Fault Tolerance and Security Issues in MPLS Networks

Sahel Alouneh
School of Informatic and Computing
German-Jordanian University
sahel.alouneh@gju.edu.jo

Sa'ed Abed
Computer Engineering Departemnt
Hashemite University
sabed@hu.edu.jo

***Abstract*—Multi-Protocol Label Switching (MPLS) is an evolving network technology that has been used to provide Traffic Engineering and high speed networking. There has been current demand on Internet Service Providers, which support MPLS technology, to provide Quality of Service (QoS) guarantees and security. Fault tolerance is an important QoS factor that needs to be considered to maintain network survivability. It is the property of a system that continues to operate the network properly in the event of failure of some of its parts. MPLS security has been mostly considered from the VPN point of view. However, data confidentiality, integrity, and origin authentication in MPLS networks are still main security issues under discussion by many research groups. In this paper, we review and discuss different approaches proposed in literature to provide MPLS fault tolerance and security.**

Keywords- MPLS; fault tolerance; security

I. INTRODUCTION

MPLS (*M*ulti-*P*rotocol *L*abel *S*witching) [1] is an evolving technology that facilitates several problems in the Internet, such as routing performance, speed, and traffic engineering. MPLS provides mechanisms in IP backbones for explicit routing using *L*abel *S*witched *P*aths (LSPs), encapsulating the IP packet in an MPLS packet. MPLS network combines a label-swapping algorithm, similar to that used in ATM, with network layer routing. A label is a short, fixed-length identifier that is used to forward packets. In MPLS network, the FEC (*F*orward *E*quivalence *C*lass) assignment is done just once at the ingress router. The FEC to which the packet is assigned is encoded into a *label*. The packets are labeled before they are forwarded between LSRs (MPLS core routers called *L*abel *S*witched *R*outers). In this basic procedure all packets which belong to a particular FEC and which travel from a particular node will follow the same path or LSP to the destination or the egress router, without regard to the original IP packet header information.

Fault tolerance is an important QoS factor that needs to be considered to maintain network survivability. It is the property of a system that continues to operate the network properly in the event of failure of some of its parts. MPLS network is very vulnerable to failures because of its connection oriented architecture. In this paper, we review and discuss different approaches proposed recently in literature to provide MPLS fault tolerance. We focus our analysis on three important factors, network resource utilization, recovery time, and packet loss.

The second goal of this paper covers the security issue in MPLS networks. Security considerations in MPLS networks have not been discussed thoroughly until recent demands for security have emerged by most providers and researchers. MPLS security has been mostly considered from the VPN point of view. However, data confidentiality, integrity, and origin authentication in MPLS networks are still main security issues under discussion by many research groups. In other words, there is no guarantee to users that packets do not get read or corrupted when in transit over the MPLS core. MPLS as such does not provide any of the above services.

It is important to understand that a service provider has the technical possibility to sniff data, and users can either choose to trust the service provider(s) not to use their data inappropriately, or they can use mechanisms to encrypt the traffic over MPLS core. This paper discusses most recent research proposals in literature on MPLS security combined with an analysis and comparisons of different approaches.

II. MPLS FAULT TOLERANCE

Most of the recovery approaches that have been proposed for MPLS network recovery belong to two protection models: fast restoration or pre-established protection and rerouting or dynamic protection. In fast restoration model the backup LSP is established and configured in advance, therefore bandwidth has to be reserved. In dynamic protection model the backup LSP is established after a failure occurs, and correspondingly bandwidth reservation is not applied until the failure occurs. The dynamic protection model may not be suitable for time sensitive applications because of its large recovery time [2] [3]. For this reason, in this paper we consider the fast rerouting protection recovery schemes because our main concern is to discuss fault tolerance issues in terms of recovery time delay, packet loss and network resource utilization.

Fig.1 shows a basic recovery technique proposed by Huang et al. [3]. The authors propose a PSL (Path Switched LSR) oriented path protection mechanism that consists of three components: reverse notification tree, a hello protocol, and a

lightweight notification transport protocol. This approach targets to minimize the delay experienced by an FIS (Fault Indication Signal) message by building a fast and efficient notification tree structure and uses a lightweight transport mechanism for the notification message. Generally speaking, this approach uses 1:1 path protection (extendible to *m: n* protection) where the resources (bandwidth, buffers, processing) on the recovery path are reserved for specific application or shared with others.

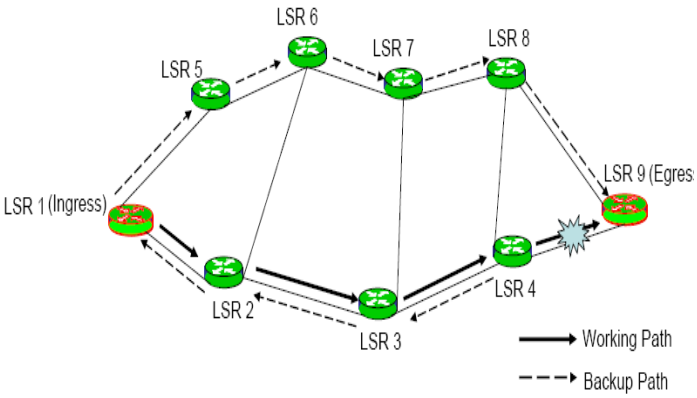

Figure 1. Path restoration example

The paper by Haskin et al. [4] introduced a simple method for setting an alternative LSP with the objective to provide a single failure protection for fast restoration. The traffic stream flowing through a working path from the ingress router towards the egress router is protected by an alternative path. In Fig. 1, if LSR4 fails, the traffic in working path is rerouted along the backup path, LSR 3-2-1-5-6-7-8-9. The backup path is comprised of two segments. The first segment is established between PML (Protection Merging LSR) and the PIL (Protection Ingress LSR) in the reverse direction of the working path. The second segment is built between PIL and PML along an LSP that does not utilize any working path. Haskin Scheme has lower packet loss rate compared to Huang's scheme because it has two backup path segments [5].

The paper by Buddhikot et al. [6] addresses the problem of distributed routing of restoration paths, which can be defined as follows: given a request for a bandwidth guaranteed LSP between two nodes, find a primary LSP, and a set of backup LSPs that protect the links along the primary LSP. A routing algorithm that computes these paths must optimize the restoration latency and the amount of bandwidth used. The authors introduce the concept of "backtracking" to bind the restoration latency. In other words, it provides algorithms that offer a way to tradeoff bandwidth to meet a range of restoration latency requirements.

Seok *et al.* proposed in [7] a fault tolerant multi-path traffic engineering scheme for MPLS networks with the objective to effectively control the network resource utilization. The proposed scheme consists of the maximally disjoint multi-path configuration and the traffic rerouting mechanism for fault recovery. The authors use the linear programming formulation to configure the maximally disjoint multi-path and the traffic rerouting solution. So when the statistical traffic demand is known between a source LSR and a destination LSR, then the traffic engineering can be applied with the following objectives: set all LSPs configuration in order to find maximally disjoint paths for each node pair, subject to minimization of the maximum of link utilization. When some link failures are detected, the proposed mechanism routes the traffic flowing on the failed LSPs into available LSPs.

The 1+1 "one plus one" protection discussed in [3, 8, and 9] can provide path recovery without packet loss or delay. However, the resources are dedicated for the recovery of the working traffic, and resources may not be used for anything else. The resources (bandwidth, buffers, and processing capacity) on the recovery path are fully reserved, and carry the same traffic as the working path. Selection between the traffic on the working and recovery paths is made at the path merge LSR (PML).

Reference [10] provides a scheme that guarantees to continue the network operation with no packet loss and recovery delay, and with reasonable network resource utilization. The key idea behind this scheme is to divide an IP packet entering MPLS network at the ingress router into *n* shares. Using the Threshold Sharing Scheme in [11], the egress router should receive *k* shares when using a (*k, n*) threshold sharing level to be able to reconstruct the original IP packet. The generated MPLS packets or shares should be allocated to at least *k maximal* disjoint Label Switched Paths (LSPs) in order to make every path or LSP independent from each other.

The paper by Virk et al. [12] presents an economical global protection frame work that is designed to provide minimal involvement of intermediate LSRs, reduction in the number of PSLs (Label Switched LSRs) responsible to switch the traffic from failed working path to the backup path), fast and cost effective fault notification. The proposed scheme uses a directory service that is logically centralized and physically distributed database to provide a fast lookup of information.

In the following discussion we can summarize the main issues in MPLS fault tolerance:

- It is generally noticed that whenever path protection is required, then redundancy in network resources has to occur. In other words, the capacity share allocation is an important factor that has to be considered.
- The recovery time delay in most techniques exists and varies from one approach to another. The recovery time can be affected by the network topology and the recovery technique used. The location of link or node failure affects the recovery time.
- The packet loss factor is also exists in most techniques and varies between one approach and another. The time needed to detect a node or link failure causes packets to be dropped unless the recovery techniques use some buffering mechanisms to reduce the number of dropped packets. However, this will result in complex recovery methodology such as increasing overhead and packet reordering.

To summarize, it is seen from the previous related work in MPLS fault tolerance that recovery time, packet loss and bandwidth utilization are the main service parameters for real-time traffic. However, most of the approaches in literature focus on reducing working and recovery bandwidth utilization while considering the recovery delay. There is no scheme that can provide path protection with no packet loss and no recovery delay except the 1+1 protection at the cost of 100% redundant bandwidth reservation, and the approach presented in references [10, and 23] which have the same characteristics of the 1+1 protection scheme but with better bandwidth utilization. Also, the disperse routing approach [31] can handle single failures with lower redundant bandwidth but requires to know the location of the failure. A comparison of bandwidth utilization between the simple (1: N) protection, 1+1 protection, and the proposed work in reference [23] can be summarized as shown in Table 1.

(Φ_1, Φ_2, Φ_3) *Traffic sizes*	***Redundant Bandwidth for***		
	(1: 3)	**(1+1)**	**(3,4) TSS**
6, 6, 6	6 or 33.3 %	18 or 100 %	6 or 33.3 %
6, 6, 9	9 or 43 %	21 or 100 %	7 or 33.3 %
6, 3, 9	9 or 50 %	18 or 100 %	6 or 33.3 %
3, 3, 12	12 or 66.6 %	18 or 100 %	6 or 33.3 %

Table 1 Redundant bandwidth required for (1: 3), (1+1) and our (3, 4) TSS approach

III. MPLS SECURITY

MPLS network has security advantage as it offers VPN functionality by traffic separation. Traffic engineering in MPLS is one of the most commonly advertised features which drives a number of service providers and maintainers of large corporate network infrastructures towards MPLS-based configurations [16].

Even though security is one of the promises of MPLS, it must be noted that configuration mistakes can still have detrimental effects. In addition, MPLS suffers from a number of security issues as soon as an attacker successfully penetrates the core.

A. Security issues in MPLS

In MPLS VPNs built over MPLS infrastructure, it's relatively trivial for egress PEs (Provider Edge routers) to trust packet originators because packets arrive using encapsulations and proper PE- advertised tunnel labels.

Without this protocol demarcation, MPLS VPNs that use IP tunnels expose customer networks to the possibility of blind – insertion attacks [20], in which an attacker can circumvents a provider's defense perimeter of packet filters on edge routers and injects spoofed packets toward a PE router servicing a customer VPN. If the attacker iteratively injects packets with different 20 –bit VPN labels, it is only a matter of time until a spoofed packet matches the VPN label stored on PE router and enters the network. The spoofed packet will likely contain a bogus source IP address that a customer site device will attempt to forward, leading to black-holed or compromised data.

The following are the main security issues in MPLS network:

- *Confidentiality*: Confidentiality in MPLS networks can refer to a number of areas, including confidentiality of Label Information Base (LIB) and confidentiality of traffic passing through the infrastructure. Knowledge of LIB can lead to a number of security issues if LSR accepts labeled packets from hosts outside the core. To mitigate brute-force enumeration of label values, it must be ensured that no labeled packets are accepted from outside the MPLS infrastructure. MPLS commonly advertised as providing VPN functionality. But unlike common VPN technology, for example IPSec or SSL VPNs, MPLS VPNs do not provide any traffic confidentiality. MPLS network architecture does not provide header or payload encryption [24]. MPLS technology has emerged mainly to provide high speed packet delivery. As a result security considerations have not been discussed thoroughly until recent demands for security have emerged by most providers and researchers. The reason why MPLS does not provide encryption mechanisms is related to the purpose it was built for. In conventional IP networks, every router in the network has a role in analyzing IP packets headers, to classify, and to process every packet passing through it. This of course will add more overhead and delay in the network [14 and 15]. In MPLS network, only two routers (the ingress and egress routers) are responsible for this task. Core or LSR routers in MPLS network will only forward packets based on labels transmitted through a pre-established LSP. The use of encryption to provide privacy of data requires the core MPLS routers to analyze and process packets' header, which will result in reducing the performance of MPLS network.
- *Integrity*: MPLS relies on trusted input to build up a Label Information Base. Based on this LIB, packet forwarding decisions are made. LDP information and updates should only be accepted from trustworthy sources. This can be ensured by two mechanisms. Firstly, LDP updates must only be accepted from interfaces on which another LSR is known to reside. In other words, LDP updates should not be accepted from clients outside the MPLS core. Secondly, if core routers are not trusted or are assumed to be vulnerable to attacks, then authentication mechanisms need to be

in place to protect the Label Distribution Protocol of choice within the MPLS network.

- *Availability*: the idea of not accepting Label Distribution protocol updates from unauthorized clients is also relevant to Availability, since a malicious collaboration could redirect traffic flows inside the core by making bogus updates. Such updates should only be accepted from authorized members in the MPLS domain.

B. Related work and discussion on MPLS security issues

The following discussion provides some of the recent proposals in literature for MPLS security followed by a discussion and critique.

Behringer *et al.* [16] discussed MPLS VPN security. The authors present a practical guide to hardening MPLS networks. They assumed "zones of trust" for MPLS VPN environment. The main assumption was to assume core MPLS routers (LSRs) to be trusted or secure. This assumption led to some security concerns such as VPN data confidentiality. There is no guarantee to VPN users that packets do not get read or sniffed when they are in transit over the MPLS core. MPLS as such does not provide a mechanism for encrypting the data. The authors left the issue of securing MPLS core routers (if they are not trusted) as an open issue for more discussion.

The paper by Ren *et al.* [17] presents an implementation and analysis of MPLS VPN based on IPSec. The authors concluded that if CA (Certificate Authority), IKE (Internet Key Exchange) and IPSec are used, the security level of the VPN is higher but this will cost a lot of system resources.

Another study by T. Saad *et al.* [15] has discussed the effect of MPLS-based tunnels on end–to-end virtual connection service and security. The study shows that applying IPSec in MPLS-based tunnels reduces overall throughput of TCP flow and adds more overhead. A cryptographic protocol to protect MPLS Labels was proposed by Barlow *et al.* [18]. The design applies simple encryption technique on labels to prevent header modification. The protocol does not provide data confidentiality. Chung *et al.* [14] proposed a method for RSA algorithm suitable for multi-path topology. It was mentioned that the algorithm can be applied to MPLS networks however the details are not provided.

Network operators should ensure that all devices and interfaces that are accessible by customers should be adequately hardened with respect to security to ensure that excessive information leakage associated with the network infrastructure is minimized.

Multi-path routing has been mainly used to improve network performance by providing multiple paths between source-destination pairs. Multi-path routing has a potential to aggregate bandwidth on various paths, allowing a network to support data transfer rates higher than what is possible with any single path [14 and 21]. There have been few works investigating the use of multi-path routing to improve MPLS network security.

In reference [21], this paper proposes a mechanism to enhance the security in MPLS networks by using multi-path routing combined with a modified (*k, n*) Threshold Secret Sharing scheme. An IP packet entering MPLS ingress router can be partitioned into *n* shadow (share) packets, which are then assigned to maximally-node disjoint paths across the MPLS network. The egress router at the end will be able to reconstruct the original IP packet if it receives any *k* share packets. The attacker must therefore tap at least *k* paths to be able to reconstruct the original IP packet that is being transmitted, while receiving *k-1* or less of share packets makes it hard or even impossible to reconstruct the original IP packet. From a network point of view, if the whole message follows the same path to the destination, the chance of risk that an attacker could intercept all information in the message is large. However by using a multi-path routing protocol combined with (*k, n*) Threshold Secret Sharing scheme makes it hard for the attacker to intercept all the information. This procedure requires the attacker to compromise at least *k* different nodes on *k* disjoint paths (here two paths are considered independent if no shared nodes exist between a source and destination) to be able to reconstruct the original IP.

From the previous discussion on related work of MPLS security we notice that most of the research proposals concentrate on MPLS-VPN point of view. In other words, the domain of a MPLS network is assumed to be trusted. The security control measurements are mainly applied to MPLS-VPN edge routers. It is also seen that the application of IPSec to provide confidentiality and integrity of data inside MPLS domain is accompanied by significant overhead. It is important to take into account not to reduce the performance of the MPLS network such as high speed networking when applying security protocols. The security of the MPLS domain may not always be assumed to be trusted. Therefore, in this thesis we tackle this case where we assume that the MPLS domain is not trusted. It is worth to note that the MPLS security subject is still a work in progress in IETF MPLS Working Group.

Finally, network operators should maintain devices within the core infrastructure at the most recent security patch level, as new vulnerabilities are constantly discovered in software and hardware. Vulnerabilities might also be identified within MPLS switches even though they might affect non-MPLS functionality of the same device. However, it should be mentioned that when providing more security solution, this should not be on the price of MPLS architecture. In other words, attention should be paid to the fact that the more complex an MPLS infrastructure becomes, the more protocols are likely to be involved which tends as a result to make MPLS networking a classical IP-based network.

IV. CONCLUSIONS

This paper provides an overview of potential fault tolerance and security issues in MPLS network and make suggestions about how to mitigate the corresponding issues. In this paper, we focused on fault tolerance schemes related to path protection. The dynamic rerouting is out the scope of this paper since we are targeting fault recovery for time and data sensitive applications. Generally, path protection adds redundancy in

terms of network resource utilization. Recovery schemes discussed in this paper have different recovery time delay and packet loss ratios.

Additionally, this paper addresses MPLS security issues and provides suggestions to be considered when security protocols are needed to be integrated with MPLS. Whenever a solution to MPLS security has to be provided, it should be kept in mind not to add more burdens on its basic architecture.

REFERENCES

[1] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," IETF, RFC 3031, 2001.

[2] L. Hundessa and J. D. Pascual, "Optimal and Guaranteed Alternative LSP for Multiple Failures," in Proceeding ICCCN 2004, Chicago, USA, Oct 2004, pp. 59- 64.

[3] C. Huang, and V. Sharma, "Building Reliable MPLS Networks Using a Path Protection Mechanism," IEEE Communication Magazine, March 2002, pp. 156 – 162.

[4] D. Haskin, "A method for setting an Alternative Label Switched Paths to Handle Fast Reroute," Internet Draft, July 2001.

[5] G. Ahn, and W. Chun, "Simulater for MPLS path restoration and performance evaluation," Joint 4th IEEE International Conference on High Speed Intelligent Internet Symposium, Korea, April 2001, pp.32-36.

[6] L. Buddhikot, M. Chekuri, "Routing bandwidth guaranteed paths with local restoration in label switched networks," IEEE Journal on Selected Areas in Communications, Feb, 2005. pp. 437 – 449.

[7] Y. Seok, Y. Lee, and N. Choi, "Fault-tolerant Multipath Traffic Engineering for MPLS Networks," IASTED International Conference on Communications, Internet, and Information Technology, USA, Nov 2003, pp. 91-101.

[8] A. Autenrieh, "Recovery Time Analysis of Differentiated Resilience in MPLS," Proceeding of DRCN/ IEEE, Alberta, Canada, 2003, pp. 333-340.

[9] V. Sharma, and F. Hellstrand, "Framework for Multiprotocol Label Switching (MPLS)-based Recovery," IETF, RFC 3469, Feb 2003.

[10] S. Alouneh, A. Agarwal, and A. En-nouaary, " A Novel Aprroach for Fault Tolerance in MPLS Networks," The Third IEEE international conference in Innovations in Information Technology, Dubai, UAE, Nov. 2006.

[11] A. Shamir, "How to share a secret," Communications of ACM, vol. 24, Nov. 1979.

[12] A. Virk, and R. Boutaba, "Economical protection in MPLS networks," Computer Communications, Vol. 29, Issue 3, February 2006, pp. 402-408.

[13] W. Grover, "Mesh-Based Survivable Networks, Options and Strategies for Optical, MPLS, SONET, and ATM Networking," Prentice Hall PTR, 2004.

[14] J. Chung, "Multiple LSP Routing Network Security for MPLS Networking," IEEE-MWSCAS, 2002.

[15] T. Saad, B. Alawieh and H. Mouftah, "Tunneling Techniques for End-to-End VPNs: Generic Deployment in an Optical Testbed Environment," IEEE Communication Magazine, 2006.

[16] M. Behringer and M. J. Morrow, "MPLS VPN- Security," Cisco Press, 2005.

[17] R. Ren, D. Feng and K. Ma, " A Detailed Implement and Analysis of MPLS VPN based on IPSEC," in Proceeding of the IEEE Third International Conference on Machine Learning and Cybernetics, Shanghai, August 2004.

[18] D. Barlow, V. Vassilio, H. Owen, "A cryptographic protocol to protect MPLS Labels", Proceeding of IEEE Workshop of Information Assurance, 2003.

[19] D.Awduche et al., "Requirements for Traffic Engineering over MPLS", IETF, RFC 2702.

[20] B. Daugherty and C. Metz, "Multiprotocol label switching and IP. Part I. MPLS VPNs over IP tunnels," IEEE Internet Computing, Vol. 9, Issue 3, June 2005, pp. 68-72.

[21] S. Alouneh, A. En-Nouaary, A. Agarwal, "A Multiple LSPs Approach to Secure Data in MPLS Networks", Journal of Networks, Vol 2, Issue 4, pp 51-58, August 2007.

[22] D. Grayson, D. Guernsey,J. Butts, M. Spainhower, and S. Shenoi, "Analysis of security threats to MPLS virtual private networks", International Journal of Critical Infrastructure Protection, Vol. 2, No. 4, pp. 146-153, 2009.

[23] S. Alouneh, A. Agarwal, and A. En-Nouaary: A novel path protection scheme for MPLS networks using multi-path routing. Computer Networks, Vol. 53, No. 9, pp. 1530-1545, 2009.

[24] S. Alouneh, A. En-Nouaary, and A. Agarwal: MPLS security: an approach for unicast and multicast environments. Annales des Télécommunications, Vol. 64, No.5-6, pp. 391-400, 2009.