An Analysis of Service Degradation Attacks against Real-Time MPLS Networks

Abdulrahman Al-Mutairi
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
Email: Abdulrahman.Almutairi.2009@live.rhul.ac.uk

Stephen D. Wolthusen
Norwegian Information Security Laboratory
Gjøvik University College
N-2818 Gjøvik, Norway
and
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
Email: stephen.wolthusen@rhul.ac.uk

***Abstract*—While the robustness of the communication network infastructure against attacks on the integrity of backbone protocols such as the *Border Gateway Protocol* (BGP) and *Multi-Protocol Label Switching* (MPLS) protocols has been the subject of significant earlier work, more limited attention has been paid to the problem of availability and timeliness that is crucial for service levels needed in areas such as some financial services and particularly for the interconnection of smart grid components requiring hard real-time communication which are not necessarily over completely isolated networks.**

In such networks, an adversary will be successful if a targeted flow or set of flows no longer meets CoS and QoS boundaries, particularly delay and jitter, even where no outright compromise of either the flow itself or the control flow is achieved. The attacker's objective can be accomplished by interfering with the operation of the control signalling protocol, but also by influencing the *policy* of MPLS nodes and the mitigation mechanisms itself.

In this paper we therefore describe an adversary model and analysis of attacks based on manipulation of *Label Distribution Protocol* (LDP) messages for the purpose of affecting the required (QoS) and *Class of Service* (CoS) for a targeted traffic where the adversary may intentionally modify the policy state of LSRs that the targeted traffic passes through.

Keywords*—*Adversary Modelling, Multiprotocol Label Switching, Real-Time Networks, Quality of Service, Class of Service, Denial of Service, Crippling Attacks

I. Introduction

One of the defining characteristics of the global Internet based on IP is that the degree of robustness to random failure in conjunction with the prerequisite cost and performance advantages has allowed it to take over a large number of functions that have previously been separate networks. The on-going migration to so-called *next generation networks* (NGN) by many carriers and inter-carrier connectivity is resulting in demands on core networks that have previously been satisfied by dedicated networks. These demands include reliability and security, but, in many cases also strict *Quality of Service* (QoS) demands including so-called *hard real-time* requirements. The mapping of hard real-time characteristics onto the core networks and differentiation into service classes relies on *policy-based routing* mechanisms rather than mere connectivity which seek to optimise resource utilisation and cost whilst guaranteeing agreed service levels. Although some mechanisms may be proprietary, Multiprotocol Label Switching (MPLS), together with the Border Gateway Protocol (BGP) is widely used both within core networks and among sites or also disparate organisation networks, typically at the network provider or carrier level.

Network operators may not wish to share policy information as this can reveal sensitive information both regarding security and reliability, but also cost structures and incentives. Policies will therefore be observable only indirectly, or can be inferred. Similarly, the service level and QoS agreements between an end user (e.g. an electric utility, a transmission/distribution grid operator interconnecting sites or sensors and actuators in a smart grid environment) and a network provider are likely to be confidential.

While problems particularly in the trust model used in MPLS and BGP and the security extensions that are currently deployed and proposed remain, the focus of this paper is to seek enhanced understanding of the threats particularly for networks relying on well-defined QoS levels, particularly regarding timing, delay, and jitter characteristics in addition to hard real-time bounds.

For this type of threats, we argue that it is desirable to explicitly construct an adversary model capturing the specific objectives of degradation and denial of service (DoS), but with limited subversion capabilities as the latter has been the focus of related work.

The remainder of this paper is structured as follows: We review related work mainly in the context of MPLS and policy-based protocol security in section II, also touching on work on realising real-time services over IP-based networks. These real-time properties and requirements are more formally described and analysed in section III before giving an overview of policy routing and the MPLS approach in section IV. We then propose a restricted model of the policy mechanism used in the subsequent analysis to minimise extraneous detail in section V, and document our adversary model in section VI, relying on these model elements for the threat analysis in section VII before a brief discussion and outlook on on-going work in section VIII.

II. Related Work

D. Guernsey et al. [1] analysed a wide range of attacks on MPLS networks for the sake of DoS or diversion of traffics. Mainly, the mentioned attacks take advantages of the adversary ability to compromise links among MPLS nodes. However, the attacks were theoretically highlighted. Alternatively, we would like to demonstrate the fears of launching similar attacks but with simulation to show the subsequent results.

M. Spainhower et al. [2] analysed the security of the signalling protocol RSVP-TE which is used to reserve resources for traffic engineering in MPLS. The authors demonstrated several exploits that could allow attacker to gain topology information by revealing the record route object (RRO) in the reservation message. Also, the authors stated that the the trust relationship between Provider Edge (PE) and Customer Edge (CE) nodes could be violated by using a fabricated RSVP-TE message to perform traffic engineering inside MPLS domain in case this type of messages is allowed at the PE node, in addition to the possibility of launching DoS attack against MPLS by misusing path messages to exhaust the node resources. However, most of the mentioned attacks could be mitigated by well configuration practises, particularly, on the MPLS edges.

MPLS VPN security was analysed by D. Grayson et al. [3], with the assumption of insider attack. They demonstrated several exploits that may cause route modification, traffic injection and DoS mainly by BGP update messages poisoning or directly injecting malicious traffic into VPNs. However, the few number of MPLS nodes and the tight security over the LSRs weaken the possibility of such attacks.

Behringer et al. [4] analysed MPLS VPN security by introducing a practical guide for MPLS security assuming the service provider is trusted. Therefore, the physical security of MPLS nodes is not included in the framework as well as the insider attack scenarios, for example, the altering of labels inside MPLS domain. The authors claimed that it is impossible to violate the separation on MPLS VPNs by implementing a practical separation on addressing, routing and traffic sides of the architecture unless it has been explicitly configured. However, the possibility of attacking VPNs by attacking the MPLS core still exists. In addition, There is a potential risk of DoS against the provider edge routers which could be mitigated by securing those routers, for example, by configuring Access Control Lists ACLs to allow traffic flow that is coming only from outside.

Moreover, the authors addressed the possibility of label spoofing which is similar to IP spoofing attack where the attacker forges the IP source address of a packet. Since the MPLS core is assumed to be trusted, the authors only discussed the possibility of passing packets with spoofed label to the MPLS domain edges which would be denied by configuring the provider edge routers not to accept labeled packets from outside.

Although the exclusion for the insider attack assumption leads to ignorance of many security issues, the scenario of compromising node in MPLS has not attracted attention. Because there are usually few MPLS nodes in the backbone domain and they are closely monitored and physically secured mostly. Moreover, the signalling protocols in such distributed environment are cooperative and coordinated to meet the required task which form a trust relationship amongst these protocols [5]. However, they suggested to use a security mechanisms such as IPsec over the MPLS infrastructure which would cause a performance problems in MPLS. As a study by Saad et al [6] showed that increasing the size of transported payload such as IPSec in MPLS reduces throughput of the total flow and introduces more overhead. Alternatively, we perform analysis of attacks that may cause service degradation for Real-Time MPLS networks.

III. Hard Real-Time Networks

Real-time traffic (hard or soft), generally, has specific characteristics differ from non-real-time traffic in the fact that messages delivery is strictly time dependant for the former. However, Hard-real-time traffic has more stringent performance requirements than soft-real-time. Therefore, high performance networks known as hard-real-time networks were designed to ensure that all messages meet their time constraints. Unlike the soft-real-time networks where meeting certain subset of messages deadlines is the main desire, all messages deadlines must be met in hard-real-time networks [7].

The main two characteristics of hard-real-time traffic are time delay and jitter. According to the definition of IPTD in ITU-T Rec. [8] time delay (packet transfer delay) is the time it takes a packet to travel between two endpoints (ingress/egress). It should be noted that we are going to use this definition for time delay throughout this paper, unless it was redefined within a specific context. Formally, let the sending time of a packet i be S_i and the receiving time of that packet be R_i therefore the time delay of that packet is expressed by the following:

$$T_i = R_i - S_i \tag{1}$$

Strict time delay is a very crucial characteristic of hard-real-time traffic. Each packet, explicitly, has a maximum time delay boundary that must be met by the underline network, however, it makes no difference how early the packet is received before the deadline. Apparently, the time delay that a packet experiences in the network could be seen as the sum up of all local time delays of a sequence of nodes on the path that the packet traverses. Setting bounds on such a path would ensure that every packet is treated according to the required time delay. Formally, let the time delay that a packet i may experience in network by T_i, the upper bound on time delay of the packet be T_i^{max} and the maximum time delay (the sum up of all maximum local delays) of a sequence of nodes along the path p that the packet traverses be T_p^{max} then the bound on the time delay that may be experienced by the packet could be expressed by the following:

$$T_i \leq T_i^{max} \leq T_p^{max} \tag{2}$$

Strict tight jitter is another characteristic of hard-real-time traffic. According to the definition of IPTD in ITU-T Rec. [9] jitter (packet delay variation) is the difference in time delay between a packet and a reference packet traverse the same end points (ingress/egress). We identify the reference packet as the previous packet sent from ingress of the same flow of the packet of concern. Formally, let the difference of packet spacing for a pair of packets i, j be Diff which is calculated as the following [10]:

$$\mathrm{Diff_{i,j}} = (R_j - R_i) - (S_j - S_i) = (R_j - S_j) - (R_i - S_i)$$

jitter J for each packet could be calculated continuously using this difference for the current packet i and the previous packet $i-1$ according to the following formula [10]:

$$J = J + (|\mathrm{Diff_{i-1,i}}| - \mathrm{J})/16 \tag{3}$$

The term $|\mathrm{diff_{i-1,i}}|$ is used because the diff may become in negative in case packet j arrives before packet i. Therefore, the underline network must ensure that the hard-real-time traffic is treated as per the jitter requirement by setting an upper bound J^{max} on jitter J as following:

$$J \leq J^{max} \tag{4}$$

Hard-real-time traffic, also, has a strict packet loss rate. Whereas, other types of traffic (e.g. soft-real-time or best effort) can tolerate some amount of loss packets to allow more network utilization, hard-real-time traffic has zero loss tolerance [11]. Another upper bound on packet loss rate L must be set for the hard-real-time traffic that traverse the underline network as following:

$$L \leq L^{max} \tag{5}$$

Generally, it is an important aspect for networks that serves traffics with certain QoS requirements such as hard-real-time traffic to offer a guaranteed bandwidth [12], [13]. Therefore, an upper bound must be set on the path that a hard-real-time traffic traverses. It should be noted that the total bandwidth of a concerned path is seen as the sum up of the links along that path. Formally, let the total bandwidth of a path p be B_p^{total} and the required bandwidth of the hard-real-time traffic is B, therefore, the upper bound for the available bandwidth to treat the hard-real-time traffic accordingly is set-up as following:

$$B \leq B_p^{total} \tag{6}$$

All of those characteristics of hard-real-time traffic demand the underline network to manage its resources accordingly. For example, setting some bounds on buffers and schedulers. Clearly, hard real-time scheduling requires upper bounds rather than first-in first-out (FIFO) buffers. The main concern is the priority processing of the messages (given a set number of messages such that all messages are processed and delivered by their deadlines) [14]. While under the FIFO discipline, packets experience different delays depending on the length of queue they traverse in the networks, there is always a need to give some packets higher priority than others based on the involved characteristics. Therefore, there have been some priority scheduling solutions to demonstrate such needs. Depending on the required job the priority scheduling solutions include fixed priority scheduling (e.g. rate monotonic scheduling (RMS) and deadline monotonic scheduling (DMS)) [15], [16]. The other solution is dynamic priority scheduling such as earliest deadline first (EDF) [17]. Alternatively, there have been some introduced mathematical approaches to model network behaviour to allow system designer to calculates tight bounds on delay and buffer to meet the real-time requirements such as network calculus [18], [19], [20].

IV. MPLS and Policy Routing

MPLS is a connection oriented switching mechanism designed for fast routing decision based on indexed label entries instead of longest matching prefix for IP addresses. MPLS provides Traffic Engineering (TE) implicitly [21] to enable load balancing on available links and preform fast re-routing in case of link failure [22]. By guaranteeing bandwidth for various traffic flows, Traffic Engineering can satisfy the constraints bounds for QoS requirements such as bandwidth as well as administrative policies. The other main two requirements for QoS are jitter and time delay require MPLS to add class based classification to different traffic flows in order to serve each class differently. By setting the experimental filed in label headers at the ingress Label Switching Router (LSR), the core LSRs could buffer and schedule the packets accordingly. Both techniques TE and class based treatment are needed to guarantee QoS requirements (e.g. bandwidth, jitter and time delay) [23].

In MPLS, packets with the same desired treatment (e.g. same destination) are assigned to a class or what is known as Forward Equivalence Class (FEC) which represents the forwarding treatment for flow of packets in the MPLS domain. Those FECs are encoded as a 32-bit label (a short fixed-length identifier). The label is then inserted to each packet once at the MPLS edge router and forwarded to the next hop. The network layer header is not analysed at any of the subsequent hops. Actual forwarding of packets is based on labels rather than IP addresses [24]. The MPLS forwarding scheme is done by mapping the incoming label to next hop and outgoing label which replaces the incoming label when the packet is forwarded along a pre-computed label switched path (LSP). To establish such paths, MPLS uses some signalling protocols such as label distribution protocol (LDP) [25]. However, for establishing LSPs with some specific constraints (e.g. bandwidth), some signalling protocols are used such as Resource reservation protocol (RSVP) [26] and Constrained based LDP (CD-LDP) [27], [28]. The achievement of using the latter two protocols is the mapping of the available resources to the required services for the traffic flows to enable QoS routing in such environment.

The set-up LSPs then are used to map end to end QoS traffic flows using QoS routing algorithm to assure the QoS services for different traffics in case of network parameters changes (e.g. bandwidth, time delay or jitter) according to the routing/administrative polices. In addition, each flow is treated as required based on hop-by-hop basis. The main contribution by MPLS is the provision of QoS based on flow-by-flow basis rather than packet-by-packet basis. The main goal of using MPLS is the result of isolating high priority flows (e.g. real-time-traffic) from the ordinary data flow which has no strict parameters. Moreover, LSPs in MPLS could be set up with various priorities in order to serve the important LSPs better than the less important ones. Therefore, the LSPs with higher priority can pre-empt the ones with less priority. Before a new LSP is established, if there is a lack of resources, the set-up priority of the new LSP is compared with the holding priority of the other LSPs using the resources to determine the ability of the new LSP to pre-empt the exist LSPs.

V. A Simplified MPLS Policy Model

The act of routing the traffic in MPLS according to the desired QoS is subjected to a wide range of polices (e.g. routing or admission). In addition, there are different technologies which MPLS has to adopt in order to deliver QoS such as Integrated Services (IntServ) [29], Differentiated Services (DiffServ) [30] and Traffic Engineering (TE) [21]. Consequently, There are various implementations with different policies for the QoS requirements realisation. Therefore, focusing on a simplified policy model that is concerned with the QoS routing/re-routing of hard-real-time traffic in MPLS would lead to a clear security analysis process.

Our simplified model describes how the network system is supposed to treat the hard-real-time traffic as expected. Mainly, there is a need for a guaranteed QoS by establishing LSPs and bind traffic to them. We assume such LSPs are already established. However, we need to identify the QoS metrics that are considered in establishing and maintaining such paths as well as re-routing of traffic among them according to network changes. There are four metrics we deal with (bandwidth (B), time delay (T), jitter (J) and packet loss (L)).

While, bandwidth and time delay metrics are the used to establish the constrained LSPs, the time delay, jitter and packet loss metrics are used to monitor the processed hard-real-time traffic and adjust the routes according to the constraints on each of them. Therefore, bandwidth (B) to be reserved as well as using the class based treatment based on hop-by-hop for the other two requirements (time delay (T), packet loss (L)). For simplicity we are going to assume that flows are served as per Class Based Queues (CBQ). There are only two different classes as Hard-Real-Time (HRT) and Best-Efforts (BF). The network bandwidth is distributed arbitrarily among the traffic as following: 5% for signalling traffic, 25% for BE traffic and 70% for HRT traffic. Other classes may borrow bandwidth from HRT whenever it is not used but not the vice versa. The BE traffics are not sharing the same queue with the HRT traffics. However, traffics from different classes share the same queue. For simplicity, we assume that each LSP serves only one HRT traffic flow. There are back-up paths which are set-up to be used in case of failure or sudden changes in network domain shared by the LSPs.

The MPLS policy model could be split into two phases the admission phase where the ingress LSR decides whether to initiate a new LSP in response to a request for HRT traffic by making the constraint computation on the available resources and the request requirements (B, L). The paths are calculated for traffics to find a set of paths that satisfies the bounds or constraints simultaneously. Firstly, finding the set of paths that satisfy the constraint B by removing the paths with residual bandwidth less than requested B using the equation-6 in section III. Then, select paths satisfy the constraint L using the equation-2 in section III. It has to be noted that if no path could be found for a new HRT request LSPs pre-emption is used. Pre-emption mechanism is included in RSVP-TE protocol [26] to allow an LSP with higher priority to pre-empt (tear down) other LSPs with lower priority. The pre-empted LSPs are then re-routed. Basically, each LSP has a set-up and holding priorities that specify the capability of an LSP to pre-empt the other LSPs and the capability of an LSP to resist such pre-emption respectively. The priority range is $0 - 7$ where the 0 is the highest priority and 7 is the lowest.

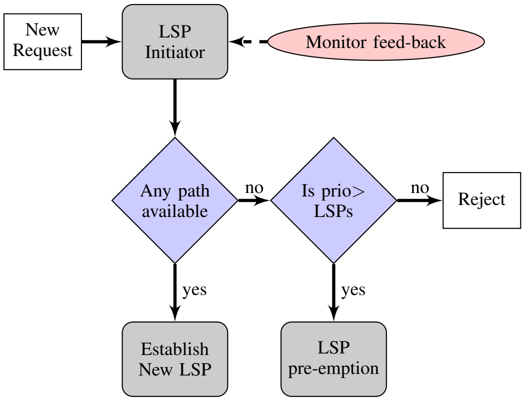

Figure 1. Admission phase for LSPs requests

The other phase is the routing phase where the traffics are forwarded along their assigned LSPs as shown in figure 2. Also, where the traffic flows status is monitored and feed-backed to the admission phase as shown in figure 1. Each traffic flow is forwarded, buffered in queues and scheduled inside MPLS domain through LSRs based on labels. As the packet received at any of the LSRs, it is checked if it has a label, otherwise, it is going to be dropped. Then, the label is processed and if it is belong to the same LSR (self label), that label is popped-up (removed) and the packet is processed again as if it is recently received as shown in figure 2. Otherwise, the LSP table (it is known as Explicit-Routes Information Base) is checked for entries for the processed label. Finally, the packet is label switched into the associated LSP if an entry is exist, otherwise, the packet is simply dropped. Moreover, we assume that the strategy to react to overload bandwidth in each LSP is limited to delay accumulation then packet discarding which could be done by assuming the queue length is limitedly fixed. However, the traffic is monitored for adjustment periodically at every time interval m to keep the three metrics L, T and J within the limits. According to A. Gurijala and C. Molina [31], QoS traffic could be monitored periodically and passively by calculating the concerned metrics averages. Hence, as the time delay is calculated for each packet using the equation-1 in section III, the average time delay for a specific flow could be calculated by dividing all received packets delays (excluding the lost packets) by the total number of the received packet delays at every time interval m. Alternatively, jitter is sampled at every time interval m as it is updated as per packet basis by the equation-3 in section III. The packet lost rate is calculated for each traffic flow at every time interval m as the ratio of lost packets to the total sent packets. Whenever, one of the monitored metrics at least exceeds the threshold and the assigned bandwidth was not violated, the traffic flow is re-routed to another path that satisfies the specified QoS requirement. Otherwise, a signalling message is sent to sender to block the most recent flow [32]. The boundaries on L, T and J are arbitrarily set as 0.80%, $80ms$ and $3ms$ respectively.

VI. An Adversary Model for MPLS LDP and Policy Attacks

A. Adversary Goal and Motivations

The main goal for our adversary is to affect the QoS parameter of a targeted traffic in order to degrade the service

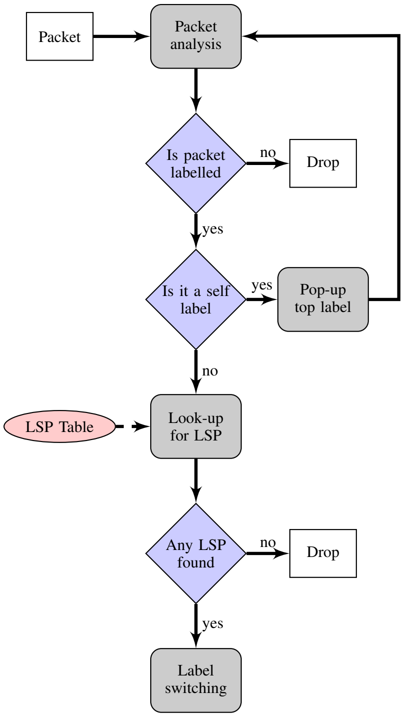

Figure 2. Routing phase for packets

it is supposed to receive inside MPLS domain and/or upgrade a targeted traffic to enhance the service it is received on the starvation of others. However, the adversary aims to minimise the ability of network operators to notice that the system is under attack in order to take advantage of such attacks. Moreover, the motivations of launching attacks against MPLS domain could explains and justify the risk it takes and/or the ability of the adversary could gain in order to affect such backbone infrastructure that carries highly time sensitive traffic for various military, financial, health and critical infrastructure organisations. Therefore, the motivations are highly classified as economical and political driven.

B. Adversary Knowledge and Limitation

The MPLS nodes in the network backbone are closely monitored and most of the time physically secured. Therefore, the compromised node scenario is excluded form our adversary model, however, the adversary still can read/write at most one link of choice. In other means, the adversary could drop, intercept and fabricate messages on the compromised link.

Furthermore, MPLS domain is usually well configured and administrated on MPLS edges. For example, packets enter the MPLS domain will be subjected to various access checks. Therefore, miss-configuration attacks analysed in [2], [4] are not going to be overseen here as the ability of the adversary is restricted by the well configuration of MPLS nodes and edges. Moreover, the protocol signalling messages are assumed to be readable and possible to be fabricated by the adversary.

In addition, we would like to add more restriction on our adversary by excluding the assumption of compromising link that are attached directly to the MPLS edges. Because compromising one of the links attached to the edges increases the ability to affect the edges themselves as well as the ability to affect most of the routed traffic, especially, on links attached to the egress LSR where packets are sent in layer 3 format because of the penultimate hop popping mechanism [33]. The adversary has the knowledge of the topology either as initial power or by exploiting the exist security vulnerabilities such as revealing the addresses in MPLS domain by capturing the Record Route Object RRO in the reservation message addressed by M. Spainhower et al. [2]. In addition, we assume that the adversary could identify the targeted traffic flows in the MPLS domain.

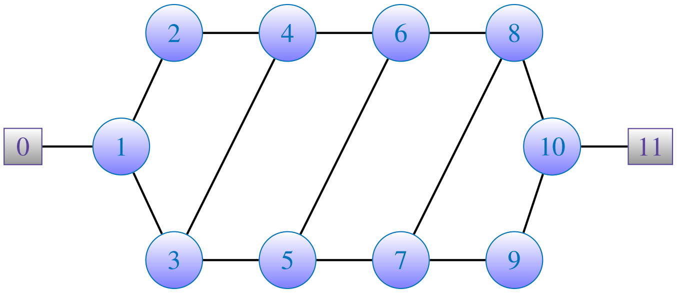

Figure 3. MPLS Network Topology

VII. Threat Analysis

In this paper we show how our adversary is able to affect QoS of a traffic flow of choice and minimize the opportunity of attack discovery by manipulating policy engines or how they are implemented in order to affect the HRT traffic in MPLS domain. We used network simulator NS (version 2) [34] to demonstrate some of the presented attacks. NS-2 is a popular and powerful simulation tool that includes MPLS simulation. Our simulated network is composed of the Provider Edge (PE) and the customer edge (CE) as shown in figure 3. The PE represents the MPLS domain which is made up of multiple LSRs (LSR-1,...,9) represented by node-2,..,9 accordingly. The LSRs are bounded by two MPLS edges (ingress and egress LSRs) represented by node-1 and node-10 respectively. The CE is made up of a sender or source node (node-0) and a receiver or destination node (node-11) for simplicity. Each two adjacent nodes are connected by at most one link. Each node can implement the QoS scheduling for the treated traffic on the attached links. For simplicity, we assume that there is only one HRT traffic flow at source rate of $290kbps$ which is attached to an LSP takes the shortest path on LSR-1→ LSR-2 → LSR-4 → LSR-6 → LSR-8 → LSR-10 with a guaranteed bandwidth of $300kbps$ those are chosen arbitrarily. Our analysis has revealed the following attacks:

A. QoS Treatment Level Disable

Attacks under this category are concerned with disabling HRT traffic from getting the guaranteed QoS either by manipulation of LSRs policy engines or by manipulation of labels belong to the traffic itself. First of all, whereas, the initiation of LSPs and the binding of specific traffic flows to them is done at the ingress LSR as mentioned in section V, any changes done to the policies of LSRs or traffic flows inside the MPLS domain may not be reported to or received by ingress LSR.

For example, if a resource release message was sent from one of the LSRs downstream of the ingress LSR (e.g. from

LSR-3) which is happened to be along one of the set-up LSPs then the resources will be released from the LSRs downstream that LSRs and the treatment of the underline traffic flow of the released LSP will be no longer subjected to the desired QoS and such action may not be reported to the ingress LSR neither to egress LSR as stated in section VI-B. Our adversary has the ability to fabricate such resource release messages to downgrade QoS treatment for the affected traffic. It should be noted that LSPs are assumed not to be updated by the status of label distributed bindings, otherwise, manipulation of LDP messages such as label release messages, would affect a wide range of LSPs based on those signalled labels due to the propagating nature of such messages.

The second attack under this category takes advantages of the independent processing of flows on LSRs and because the decisions of binding flow to LSPs are based on labels as mentioned in section V, the adversary could only replace labels belong to the concerned LSP on label stack of HRT traffic of concern to a label of choice that redirect traffic of concern into another LSP that does not comply with required QoS in order to assure its delivery to the egress LSR to minimize the probability of discovery, therefore, the affected traffic is not going to be attached to the assigned LSP in the downstream LSRs and hence the required QoS treatment is no longer applied to that traffic.

B. *Traffic Fluctuation*

According to T. Bilski [35], the mitigation procedure to re-route the high bandwidth traffic around the affected cables in the Mediterranean Sea which have suffered cuts in 2008 did not consequently affected only the QoS of the re-routed connections, but, the QoS of connections from other parts of the world to unacceptable level and such deterioration of QoS may last for months.

Our adversary could initiate a longer and wider LSP with highest priority to make sure it crosses almost all of the other LSPs and utilize most of the network resources. In our network the ideal path for this type of attacks is the path on LSR-3 → LSR-4 → LSR-6 → LSR-5 → LSR-7 → LSR-8 → LSR-10. Consequently, according to the MPLS model in section V, almost all of the initiated LSPs are going to be torn down and re-established because of the LSPs pre-emption mechanism. The sudden tear down of almost all of the initiated LSPs, the re-establishing procedure and re-routing of the traffics among them would affect almost all of the HRT traffic inside the MPLS domain. It could disable most of the LSPs from being re-established as long as that fabricated LSP keeps occupying the network resources. Alternatively, the adversary could only initiate a longer LSP that interferes with most of the established LSPs discretely. The main idea here is to created a flapping environment inside the MPLS domain.

A fabricated LSP with a guaranteed bandwidth of $200kbps$ was initiated over the the path that passes through LSR-3→LSR-4→LSR-6→LSR-5→LSR-7→LSR-8→LSR-10). Then, a traffic at source rate of $200kbps$ was attached at the time $5sec$ to the fabricated LSP in order to show how a slight flapping situation could affect the other traffic flows even if they are not sharing the same LSP. Our results show a slight changes in the time delay as it reached $75ms$ as shown in figure 4 with no changes to the packet loss value as the bandwidth was not violated, however, the HRT traffic jitter violated the specified bound in section V which is $3ms$ and reached $3.4ms$ as shown in figure 5 compared to the HRT traffic jitter on normal operation.

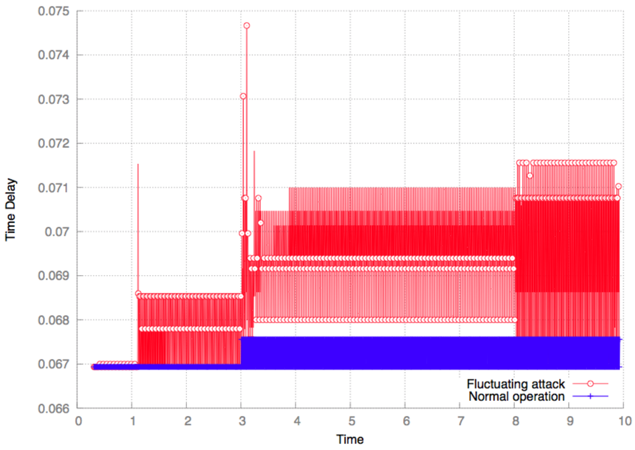

Figure 4. HRT traffic time delay in fluctuating attack

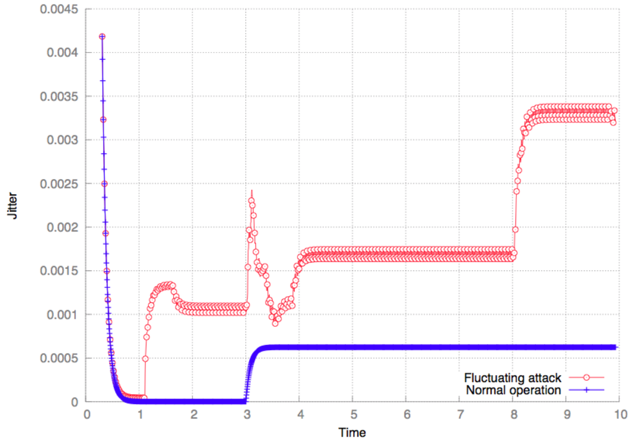

Figure 5. HRT traffic Jitter in fluctuating attack

C. *LSP Injection*

The main goal of deliberately injecting traffic flows into other LSP s is to affect the QoS of the traffic flows already attached into those LSPs. Using the label manipulation attack mentioned in section VII-A, our adversary could inject other traffic flows into any LSP passes through the compromised link. More interestingly, this attack could be launched against any HRT traffic flow in the MPLS domain by fabricating the label stack for LSP that serves the HRT traffic flow of concern and push a top label belong to the LSR's label that the HRT traffic flow passes through. The targeted LSR then pop-up (remove) the label on top and process the next label on label stack according to the policy engine in figure 2.

More interestingly, we have demonstrated by simulation how injection of even a low rate traffic could hugely affect the QoS of the HRT traffic flow that traverses the attacked LSP. Even by injecting a traffic at source rate of $10kbps$ into the LSP

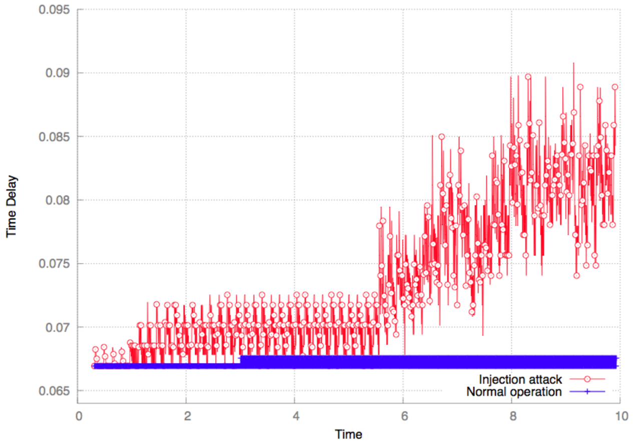

Figure 6. HRT traffic time delay in injection attack

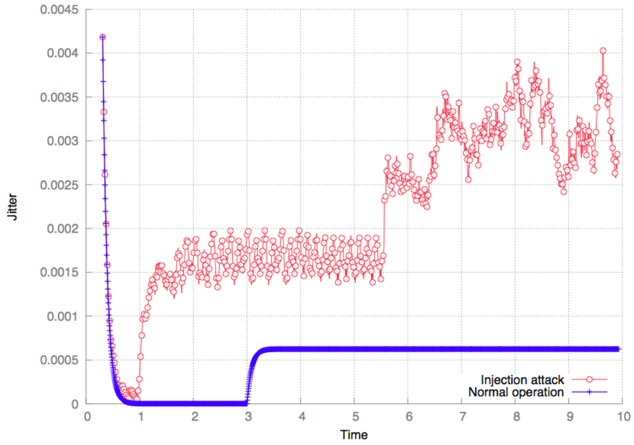

Figure 7. HRT traffic jitter in injection attack

that serves the HRT traffic flow only to fill up the allowed bandwidth for that LSP which is $300kbps$, the time delay and jitter of the HRT traffic flow have increased dramatically to exceed $90ms$ and $4ms$ compared to $67ms$ and $0.6ms$ in normal operation as shown in figures 6 and 7 respectively. However, the packet loss value was not changed because the bandwidth was not violated.

D. Attacks Concealment

Covering attacks and traces are so important for attackers in general. However, the notion of attack concealment is more important for QoS degradation attacks mainly because the attacks are only successful as they are periodically being launched in network domain to degrade the QoS of the targeted traffic. Also, attacks concealment is useful to make it harder for the network operator to track down the source of attacks or problem such as the compromised link.

Because QoS monitoring in our simplified MPLS policy model in section V are mainly based on the analysis of the mean values of time delay and packet loss or the current value of jitter, the implementation of our attacks could not be discovered or mitigated if they were periodically launched to affect the HRT traffic flow of concern partially on packet basis. For illustration, lets arbitrarily assume that the metrics samples are taken periodically every $60sec$, then if both of our simulated attacks only lasts for $5sec$ the sampling results for packet loss rate, average delay time and jitter in the traffic fluctuation attack are 0%, $68m$ and$0.9ms$ respectively which is close to the sampling results for the LSP injection attack as 0.3%, $69ms$ and $1.2ms$ respectively.

VIII. Conclusions

The demands for a guaranteed QoS for diversity of applications and the degree of criticality of those applications (e.g financial services or critical mission communications) increasingly force the Internet Service Providers (ISPs) to adopt, develop and secure their networks accordingly.

Securing the underlying networks is the most important step in providing QoS because any violation to the QoS deadlines or the so called service-Level Agreement (SLA) may not be detected, mitigated or subjected to further assessment in design process as the case with other elements.

Therefore, some efforts have been made to study the security of main elements of such networks, mainly, protocols. For example, analysing the security of signalling protocols such as LDP or BGP and the resource managing protocols such as RSVP. However, analysing the security of individual protocols solely and the ability which is given to the adversary may ignore the vulnerabilities of the system to certain type of attacks such as those targeting the policy model.

This paper provides analysis of the real-time networks security mainly in the context of MPLS core networks. In this paper we illustrated the mapping of hard real-time characteristics onto the core networks and differentiation into service classes.

Furthermore, an adversary model is introduced in order to highlight the ability of limited resources to take advantages of potential vulnerabilities of distributed systems. These limitation and restrictions on the adversary model are important to direct the security study of real-time systems correctly from the common security issues into the availability and stability of the networks operation. Furthermore, some practical attacks have been demonstrated using the network simulator NS (version 2) which is a discrete event simulator targeted at networking research that has the ability to simulate MPLS networks and QoS mechanisms. Our simulation scenarios showed how different techniques could be applied by an adversary with a limited resources to affect the QoS of traffic of choice. Finally, we explain how such attacks might not be reported to network operators or trigger the monitoring servers. We hope that the introduced adversary model and the revealed attacks results raise the concerns about QoS security in the backbone networks as well as the security of control protocols used at core systems.

References

[1] D. Guernsey, A. Engel, J. Butts, and S. Shenoi, “Security analysis of the mpls label distribution protocol,” in *Critical Infrastructure Protection IV: Proceedings of the Fourth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*, vol. 342, Washington D.C., USA, Mar. 2010, pp. 127–139.

[2] M. Spainhower, J. Butts, D. Guernsey, and S. Shenoi, “Security analysis of rsvp-te signaling in {MPLS} networks,” *International Journal of Critical Infrastructure Protection*, vol. 1, no. 0, pp. 68–74, 2008.

[3] 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.

[4] M. H. Behringer, "Analysis of the security of bgp/mpls ip virtual private networks (vpns)," IETF, RFC 4381, Feb. 2006.

[5] F. Palmieri and U. Fiore, "Securing the mpls control plane," in *High Performance Computing and Communications*, 2005, vol. 3726, pp. 511–523.

[6] T. Saad, B. Alawieh, H. T. Mouftah, and S. Gulder, "Tunneling techniques for end-to-end vpns: generic deployment in an optical testbed environment," *Communications Magazine, IEEE*, vol. 44, no. 5, pp. 124–132, 2006.

[7] N. Malcolm and W. Zhao, "Hard real-time communication in multiple-access networks," *Real-Time Systems*, vol. 8, no. 1, pp. 35–77, 1995.

[8] *Recommendation ITU-T Y.1540, Internet protocol aspectsQuality of service and network performance-Internet protocol data communication service IP packet transfer and availability performance parameters*, nt'l Telecommuncation Union, 2011.

[9] *ITU-T Recommendation Y.l541, Internet protocol aspectsQuality of service and network performance-Network performance objectives for IP-based services*, nt'l Telecommuncation Union, 2011.

[10] V. Jacobson, R. Frederick, S. Casner, and H. Schulzrinne, "Rtp: A transport protocol for real-time applications," IETF, RFC 3550, Jul. 2003.

[11] C. M. Aras, J. F. Kurose, D. S. Reeves, and H. Schulzrinne, "Real-time communication in packet-switched networks," *Proceedings of the IEEE*, vol. 82, no. 1, pp. 122–139, 1994.

[12] S. Kashihara and M. Tsurusawa, "Dynamic bandwidth management system using ip flow analysis for the qos-assured network," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, Dec. 6–10, 2010, pp. 1–5.

[13] S. Chong, S. Li, and J. Ghosh, "Predictive dynamic bandwidth allocation for efficient transport of real-time vbr video over atm," *Selected Areas in Communications, IEEE Journal on*, vol. 13, no. 1, pp. 12–23, 1995.

[14] L. Thiele, S. Chakraborty, and M. Naedele, "Real-time calculus for scheduling hard real-time systems," in *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, vol. 4, Geneva, May 2000, pp. 101–104.

[15] J. P.Lehoczky, "Fixed priority scheduling of periodic task sets with arbitrary deadlines," in *Real-Time Systems Symposium, 1990. Proceedings., 11th*, Dec. 5–7, 1990, pp. 201–209.

[16] N. C. Audsley, A. Burns, R. I. Davis, K. W. Tindell, and A. J. Wellings, "Fixed priority pre-emptive scheduling: An historical perspective," *Real-Time Systems*, vol. 8, no. 2-3, pp. 173–198, 1995.

[17] T. M. Chen, J. Walrand, and D. G. Messerschmitt, "Dynamic priority protocols for packet voice," *Selected Areas in Communications, IEEE Journal on*, vol. 7, no. 5, pp. 632–643, 1989.

[18] R. L. Cruz, "A calculus for network delay. i. network elements in isolation," *Information Theory, IEEE Transactions on*, vol. 37, no. 1, pp. 114–131, 1991.

[19] R. Agrawal, R. L. Cruz, C. Okino, and R. Rajan, "Performance bonds for flow control protocols," *IEEE/ACM Transactions on Networking (TON)*, vol. 7, no. 3, pp. 310–323, 1999.

[20] C. Li, A. Burchard, and J. Liebeherr, "A network calculus with effective bandwidth," *IEEE/ACM Transactions on Networking (TON)*, vol. 15, no. 6, pp. 1442–1453, 2007.

[21] D. O. Awduche and J. Agogbua, "Requirements for traffic engineering over mpls," IETF, RFC 2702, Sep. 1999.

[22] T. Usui, Y. Kitatsuji, and H. Yokota, "A study on traffic management cooperating with ims in mpls networks," *Telecommunication Systems*, pp. 1–10, Feb. 2011.

[23] V. Fineberg, "Qos support in mpls networks," White Paper, Frame Relay Forum, May 2003.

[24] L. He and P. Botham, "Pure mpls technology," in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, Mar. 4–7, 2008, pp. 253–259.

[25] L. Andersson, P. Doolan, N. Feldman, A. Fredette, and B. Thomas, "Ldp specification," IETF, RFC 5036, Oct. 2007.

[26] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "Rsvp-te: extensions to rsvp for lsp tunnels," IETF, RFC 3209, Dec. 2001.

[27] B. Jamoussi, L. Andersson, R. Callon, R. Dantu, L. Wu, P. Doolan, T. Worster, N. Feldman, A. Fredette, and M. Girish, "Constraint-based lsp setup using ldp," IETF, RFC 3212, Jan. 2002.

[28] J. Ash, M. Girish, E. Gray, B. Jamoussi, and G. Wright, "Applicability statement for cr-ldp," IETF, RFC 3213, Jan. 2002.

[29] B. Braden, D. Clark, and S. Shenker, "Integrated service in the internet architecture: an overview," *Program on Internet and Telecoms Convergence*, May 1994.

[30] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An architecture for differentiated services," IETF, RFC 2475, Dec. 1998.

[31] A. Gurijala and C. Molina, "Defining and monitoring qos metrics in the next generation wireless networks," in *Telecommunications Quality of Services: The Business of Success, 2004. QoS 2004. IEE*, Mar. 2–3, 2004, pp. 37–42.

[32] J. L. Chen, M. C. Chen, and Y. R. Chian, "Qos management in heterogeneous home networks," *Computer Networks*, vol. 51, no. 12, pp. 3368–3379, 2007.

[33] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol label switching architecture," IETF, RFC 3031, Jan. 2001.

[34] Network simulator ns (version 2). [Online]. Available: http://www.isi.edu/nsnam/ns/

[35] T. Bilski, "Fluctuations and lasting trends of qos on intercontinental links," in *Quality of Service in Heterogeneous Networks*, 2009, vol. 22, pp. 251–264.