Proof Of Concept for Opportunistic Security in MPLS Networks

Salil Ajgaonkar B.E

A Dissertation

Presented to the University of Dublin, Trinity College

in partial fulfilment of the requirements for the degree of

Master of Science in Computer Science (Future Network Systems)

Supervisor: Stephen Farrell

August 2018

Declaration

I, the undersigned, declare that this work has not previously been submitted as an exercise for a degree at this, or any other University, and that unless otherwise stated, is my own work.

Salil Ajgaonkar

August 16, 2018

Permission to Lend and/or Copy

I, the undersigned, agree that Trinity College Library may lend or copy this thesis upon request.

Salil Ajgaonkar

August 16, 2018

Acknowledgments

...ACKNOWLEDGMENTS...

Salil Ajgaonkar

University of Dublin, Trinity College
August 2018

Proof Of Concept for Opportunistic Security in MPLS Networks

Salil Ajgaonkar, Master of Science in Computer Science

University of Dublin, Trinity College, 2018

Supervisor: Stephen Farrell

Multiprotocol Label Switching (MPLS) is a high performance packet switching technology which supports packet switching for multiple protocols and access technologies. It is a switching technology that redirects data based on short label paths rather than an IP table lookup. Each Label Switched Router in the MPLS network has this table that tells the router how to handle and redirect specific types of data. This helps the router to handle data in a consistent fashion while maintaining flexibility and congestion control at the same time.

MPLS provides networking corporations and government high speed and reliable data transfer over geographically dispersed sites as well as maintaining flexibility and high bandwidth data exchange.It is very easy to scale and can be efficiently tuned to meet service level agreements. it is primarily used to provide Virtual Private Network (VPN) capabilities for corporations who wish to transfer private data over a public network.

Such heavy reliance on MPLS by big companies and the general public to manage their data means that any forms of successful attacks often have the potential to disrupt vital everyday operations. Attacks ranging from data theft to denial of service if successful may lead to severe damages to the corporation as well as the owner of the data.

Earlier work conducted by the Internet Engineering Task Force (IETF) have analyzed the various vulnerabilities and security threats that plague the MPLS technology and have drafted a potential resolution to some of the security issues. The work proposed the implementation of Opportunistic Security in the MPLS network using payload encryption to encrypt the underlying application data and protocols using secure key exchange between end to end or hop by hop Label Switching Routers (LSR's) on an MPLS Label Switched Path (LSP).

This paper aims to provide a proof of the concept to this proposed solution by implementing it on a practical controlled environment and measuring its effects on the overall functionality and feature of the presently running MPLS technology. The aim of this paper is to provide an idea regarding the feasibility of this solution in practical commercial application in the world.

Summary

MPLS is a network routing technology which uses circuit switching and packet switched network technologies to support data routing for multiple internal protocols. It is a protocol independent and highly scalable technology whose flexibility enables efficient utilization of network resources resulting in high quality of service at low cost. MPLS relies on the use of fixed bytes of data that represent as labels for routing decisions. These labels are pushed on top of a data packet at the ingress switch of an MPLS cloud. All the succeeding Label Switching Routers (LSR's) in the MPLS cloud refer these labels to appropriately route the data to the correct destination. The path to the destination is pre-configured in the LSR's Label lookup table rather than an IP routing table. This avoids any complex lookups or reading long network addresses and implementation of longest match algorithms. Once the MPLS packet reaches the egress switch of the MPLS cloud, the MPLS label is popped off and the data packet is then transmitted as a regular IP packet along the succeeding switches. The LSRs between the ingress and the egress switch of the MPLS cloud also have the capability of pushing and popping off the MPLS labels on the data packet to efficiently engineer the network traffic.

Networking corporations and service providers can leverage this flexibility to scale their network services. Using the advantages of MPLS they are able to run high bandwidth applications over seamless IP based networks that connect multiple, remote site [2]. The reliance on MPLS VPNs by corporations and government agencies means

that attacks ranging from intercepting sensitive data to disrupting data, voice and multimedia services can significantly impact vital operations [2].

Data Security in MPLS previously mainly relied on Data security (e.g., confidentiality) in MPLS has previously relied on just two features: 1) Physical isolation of MPLS networks has been used to ensure that interception of MPLS traffic was not possible. 2) Higher-layer protocol security such as IPsec has been used whenever a particular flow has determined that security was desirable [1]. However these features have a number of vulnerabilities. The network is still vulnerable to network taps between links, misconfiguration of routers, data replication, as well as users might not enable end to end security of their applications [1].

To mitigate these vulnerabilities to some extent, the IETF drafted an Internet-draft titled "Opportunistic Security in MPLS Networks draft-ietf-mpls-opportunistic-encrypt-03" which proposed a novel idea of implementing Opportunistic Security (OS) in the currently existing MPLS implementation. The Internet draft suggested the implementation of opportunistic encryption of data packet payload which is held by the MPLS packet. As the LSR's only rely on the information contained in the MPLS labels for routing information the contents of the MPLS packet are of no significance for the flow of traffic. Thus end-to-end or hop-by-hop encryption of the data payload of the MPLS packet by the LSRs can contribute greatly to maintain the confidentiality, integrity and authenticity of the data that flows through the MPLS network.

This paper aims to implement this proposed experimental idea in a controlled environment by simulating the flow of traffic in an MPLS network in a virtual network and comparing the difference in performance between MPLS with the OS and MPLS without the OS. This will help validate or invalidate the proposed solution experimentally and further spread more light on its impact and feasibility on real world implementation.

This experiment will be carried out using an experimental network setup consisting

of mininet as a virtualized network platform. On this virtual platform we will setup OpenVswitch (OVS) virtual switches which will simulate the flow of network traffic through the virtual switches. The MPLS flows needed to configure the OVS switches will be configured onto the switches using Software Defined Networking (SDN) Technology. The SDN is enabled using the OpenFlow communication protocol. OpenFlow configures these OVS switches to simulate the behavior of an MPLS switch. The Opportunistic Security feature in the MPLS will be implemented by coding this new feature into the existing OVS code base which would then be configured onto the OVS switches in the mininet network to simulate the behavior of the system with the OS. We would then evaluate the performance of the system by measuring certain network performance metrics and comparing them with the ones measured without the OS. This comparative analysis should give us a good idea of how the OS in MPLS fairs against MPLS without OS, if there are any room for improvements and its potential impact on practical implementation.

Contents

List of Tables

List of Figures

Chapter 1

State Of The Art

MPLS by itself is vulnerable to a number of security threats. This is primarily because MPLS in its primary idea aims to solve the problem of high speed data delivery over large geographical network while maintaining flexibility so it can be scaled to meet business requirements. Routing and traffic engineering using MPLS is very easy and service providers can leverage this benefit to provide varying levels of Quality of Service.

With the increasing deployment of MPLS, security of data passing through the MPLS network has become a grave concern for corporations and the service provider alike. Service providers are concerned with the security and confidentiality of their customers data while corporations using MPLS to share data between their geographically distributed sites demand authentication and integrity as well.

1.1 Security Requirements in MPLS

Some of the General Service Provider Security Requirements are as follows:

Protection of data at the Data-Plane

Encryption of data is not provided as a basic feature in all telecommunication protocols. Protocols like IPSEC have all the features of authentication, data integrity and confidentiality however it is not widely adopted by all applications. however, roughly 30% of web sites actually take on this burden of implementing IPSEC, even though the software required is ubiquitous [2].

Protection from attacks on Label Distribution protocol

In [16] the authors have stated that attacks on Label Distribution protocol (LDP) exploit 3 weaknesses: The LDP specification, Service provider implementation and underlying infrastructure. The authors have expressed that these attacks can lead to various DOS attacks or Route modification attacks most of which ma lead to violation of SLA for the Service provider. Naturally the Service provider would like protection against such attacks as a major requirement in implementing MPLS networks.

Prevent Malicious External Controllers from misconfiguring the SDN switches

SDN Switches are vulnerable to being misconfigured by external controller. An attacker can send malicious control-plane messages to the switches which can misconfigure them to send packets to a malicious switch, replicate the packets or drop the packets in general to trigger a Denial of service attack (DOS). Service providers expect some form of authentication of messages received from the control plane by the switches to make sure any control-plane messages received by the SDN are from a legitimate controller in the network.

Prevention of attacks that spoof IP addresses

Many attacks on protocols running in a core involve spoofing a source IP address of a node in the core (e.g., TCP-RST attacks).[3] If such a spoofed IP address gets accepted in the MPLS network, the MPLS switches can route sensitive packets to the spoofed address leading to data leakage. The attacker can then have the luxury to analyses and read the data at his leisure till the systems identifies the spoofed address.

Hiding Service Infrastructure

In general the service provider would like to hide his service infrastructure from the external network. An MPLS/GMPLS provider may make its infrastructure routers unreachable from outside users and unauthorized internal users. For example, separate address space may be used for the infrastructure loopbacks [3]. A service that is hidden

to the external network has less chances of being targeted by attackers.

Protection from mis-merging of LSP

Care needs to be taken that any implementation of security procedures do not alter the the MPLS Label stacking logic which then becomes vulnerable to mis-merging of LSPs. LSP mis-merging has security implications beyond that of simply being a network defect. LSP mis-merging can happen due to a number of potential sources of failure, some of which are due to MPLS label stacking [17].

Link Authentication

Service providers would prefer to authenticate a site before linking a connection. this helps validate the site based on certain security protocols like IPSEC. If the user wishes to hold the authentication credentials for access, then provider solutions require the flexibility for either direct authentication by the PE itself or interaction with a customer authentication server [3].

Security Considerations in Operations, Administration, and Maintenance messages

Operations, Administration, and Maintenance (OAM) messages are messages that are used for the internal functionality of the MPLS switches. OAM messages help in monitoring devices and implementing data transport mechanisms on a network level. They are responsible for the overall performance of the network device. On a service-oriented functionality they provide monitoring services to end users which is vital to keep a track of the performance so as to make sure the SLAs are met.The nature of OAM therefore suggests having some form of authentication, authorization, and encryption in place. This will prevent unauthorized access to MPLS-TP equipment and it will prevent third parties from learning about sensitive information about the transport network [18]

Meeting these requirements can easily fail if the system in place is vulnerable to any security threatening attacks. With the intention of securing these vulnerabilities we first need to analyze what are the different forms of attacks and how we can resolve

them. A number of research has been conducted in analyzing the various security threats that plague the MPLS networks.

1.2 Security threats in MPLS

[1] has analysis a number of security threats to MPLS in VPN. In this work the authors have discussed the principal security issues in MPLS related to Network separation, Inter-provider connectivity and MPLS packet labeling. In [2] the authors have stated that security in MPLS previously relied only on the physical isolation of the MPLS network and High-layer protocol security like IPSec. The authors have also gone further as to why these features fall short of being the ideal solutions to current network attacks.In [3] the authors have elaborated on specific types of exploits that threaten the MPLS/GMPLS network. The authors have segregated the attacks in the form of attacks on the data plane, attacks on the control plane, attacks on the operation and management plane and insider attacks. they have also recommended defensive techniques for MPLS against these forms of attacks. In [2] the author has suggested a mechanism to enhance the security in MPLS networks by using multi-path routing using a threshold secret sharing scheme. In [8] has elaborated the security issues that are inherent in the MPLS architecture. The authors state that some routers may implement security procedures relying on certain headers being in fixed place relative to a certain layer header in the IP stack. Another security issue mentioned was that the MPLS routers agree on the meaning of the labels and thus work upon a chain of trust to transfer data in the network and that if packets from untrusted sources are accepted then they may get routed illegitimately.

In this section we will try to list out the various security attacks that the MPLS network is vulnerable to. The Security attacks have been categorised into 4 types: Attacks on the Data Plane, Attacks on the Control Plane, Attacks on Operational and Management of the MPLS Network and Insider attacks.

1.2.1 Attacks on the Data Plane

Attacks that are mainly aimed at the User's or the Service Provider's data are categoried into Data-plane security attacks. These attacks aim to either manipulate the

data flowing through the MPLS network, delete the data flowing through the MPLS network, inject malicious data or just plain observe data unauthorized data all with malicious intent.

Plain IP forwarding

MPLS Switches can forward un-labelled IP packets as normal IP packets if they are configured to do so. An attacker already inside the core can exploit this information to reach other core devices compromising them. It is difficult to manage this type of attack by just traffic engineering or implementing any VPN service.

Forwarding captured packets from the core to the outside network

An attacker inside the core can capture the data sensitive packets and forward them to any destination he desires even if IP traffic is not being forwarded. This can be done by encapsulating the captured packet in the payload of a UDP packet. The source IP address can be spoofed and the detination IP address can be set to whever the attacker may wish to forward the packet. This however is only possible if the attacker is already aware of the Labels needed to route through the LSP.

Sniffing of Data

Data sniffing can be explained as the action of capturing data packets and analyzing its contents to understand what they contain. Private corporations and Users in general often transfer confidential and sensitive data over the internet. If this data is not sufficiently encrypted before forwarding them onto the internet then an attacker can use the wide variety of packet sniffing tools to sniff these data sensitive packets and use the sensitive information in them for malicious purposes. Unauthorized packet sniffing can also be a first step in other attacks in which the recorded data is modified and re-inserted, or simply replayed later [3]. Unauthorized packet sniffing is one of the most commonly faced security issue in any network system including and especially the MPLS network considering its wide spread use for mission critical systems and reliance of both common users as well as Multi national corporations.

Modification of Data Packets

If an attacker is able to manipulate the contents of the data passing through the MPLS network then he has the potential to initiate a wide range of security attacks on the network. Though not as easy as it sounds the attacker must first be aware of the internal configurations of the MPLS netowork which more often than not is more difficult than the actual manipulation of packets. MPLS often has an "egg-shell" security model where it is very difficult to penetrate the internal network core, but once inside the attacker can cause a lot of damage to the service provider and the network service as a whole [1]. Some of the potential attacks that can be triggered by data manipulations are:

Route modification attacks

Once inside the network an attacker can manipulate the data flowing through the network and route them to any destination he desires, provided he has the information necessary to route the information correctly through the network. Route modification attacks enable an attacker to gain access to certain traffic (e.g., maneuver traffic through a compromised link); affect accounting (e.g., trigger automatic financial transactions among cooperating providers); or route traffic across domains (e.g., send one customers traffic to another customers network) [16].

1. Path Switching: A normal traffic flowing through the MPLS network ideally follows a fixed set path or to be more precise an Label Switched Path (LSP). The LSP is determined by the initial traffic engineering setup done by the service provider. The traffic engineering primarily relies on the label configuration of the packets. If an attacker were to modify this label information of a data packet, then he may be able to route the data packet that it was not intended to. Such a path is called a rogue path. By doing this the attacker can deceive the traffic engineering and reap benefits out of it. For example an attacker can forward his online gaming data packets via the live video conferencing path to get better speed advantage and disrupting the video conferencing quality of service.

2. Destination Switching: Just like Path switching, an attacker is also able to modify the destination of a packet if he modifies the label configurations appropriately.

This can fool the MPLs network into forwarding the packet to a rogue destination where the attacker can further conduct malicious operations on the packet which he wasn't able to do while inside the MPLS network.

3. Brute-Force Label Prediction: An attacker can deduce the LSP of an MPLS network if the destination address is known. He can target this address and pass data packets into the MPLS with an initial label value. He can then test out the Label with incremental values till he receives a reply from the destination address. The reply from the destination address can help him deduce the LSP for the destination address and thus reuse the label information to further pass data to the destination.

4. Brute Force Target Location: Similar to label prediction, the target can also try to identify what type of service lies at the end of an LSP, for example if the user were trying to identify if a web service lies at the end of an LSP then he can set the target tcp port to 80 and incrementally try out the IP address for a successful hit. This however is a very time consuming process considering the probabilities of getting the correct IP address compared to the total combination of IP addresses possible.

5. Forward Equivalency Class (FEC) Specificity Exploitation: When configuring the MPLS network Packets are configured in such a way that packets of similar type are routed through the same LSP. These packets are thus bound by the same MPLS label and routed through the same path as designated for labels of that value. Such classification of packets is termed as Forward Equivalency Class. This attack takes advantage of the most specific or longest match rule applied by ingress routers to incoming IP packets. An attacker needs access to a link or a connection to an interface to establish an LDP session. The attacker identifies a target FEC and advertises label bindings for more specific FECs. LSRs that receive the label mappings distribute them throughout the network, thereby building new LSPs toward the compromised link [16].

6. Label Mapping Messages Modification: An attacker can modify the Label values of a datapacket inside the MPLs network. He can thus reroute the traffic or create loops within the MPLS network. This modified message is sent on to the next

MPLS switch. When the upstream LSR receives a packet for the target FEC, it applies the incorrect label, which causes the downstream router to mistakenly recognize the packet as belonging to a different FEC. The packet is then forwarded along the desired LSP [16].

7. Address Messages Modification: Similar to label modification an attacker can redirect a data packet by spoofing the the destination IP address. This attack, also known as Fabricating Address Messages, reroutes traffic or creates loops by manipulating the least cost mechanism used to select the next hop. Traffic can be redirected using access to a compromised link adjacent to an LSR along a selected LSP. This modified message forces the LSR to adjust its local label information base and generate a Label Request message.Thus, a new LSP is constructed that forces the targeted traffic along the compromised link [16].

8. Label Edge Router (LER) label Modification: Label Edge Router (LER) are routers situated at the end of an MPLS network. These routers are the final routers in the MPLS network that pop the final MPLS Label off the data packet and forward the data packet its original form before entering the MPLS network. This attack requires access to a link along the path between VPN sites. Redirection of packets to a different site in the same VPN requires the attacker to know the routes and labels corresponding to that site. The attack is executed by modifying the topmost label of a transit packet (before the penultimate pop) to another label. If the new label is valid at the next hop, the packet is forwarded to a different LER [1]. This new LER may or may not be connected to the destination. It could either drop the packet as a whole which could lead to denial of service if the attacker modified to many of the packets or the LER may forward the IP packet as a normal IP packet, depending on its configuration.

9. VPN label Modification: VPN label modification is similar to the LER Label Modification. In this type of attack two VPNs are involved. One is the legitimate source VPN and the other is the destination VPN which is incorrect. The attacker captures and modifies the datapacket label of the source VPN and redirects it to the incorrect VPN. When this modified data packet reaches the LER, the LER redirects it to the incorrect VPN. If the LER doenot have a VRPN routin gand

Forwarding (VRF) Table then the LER may forward the packet as a regular IP packet. Given knowledge of routes and VPN labels in the network core, the combination of VPN label modification with LER label modification (previous attack) enables an attacker to redirect and/or drop any traffic passing through the compromised link [1].

10. VRF table Modification: A more serious issue is if the attacker is able to modify the VRF tables themselves. This would grant the user the ability to control the traffic from the LER. The attacker can change outgoing LER labels and outgoing VPN labels to impact QoS. More over, the attacker can control the routes taken by ingress VPN traffic and divert it to the wrong VPNs [1].

Data Insertion attacks

Insertion of Inauthentic Data Traffic: Spoofing and Replay Injection Based on VPN Labels: Injection Based on LER Labels:

Unauthorized Deletion of Data Traffic Unauthorized Traffic Pattern Analysis Misconnection

Denial-of-Service Attacks Modifying the Community Attribute in LERs: Fabricating Notification Messages: Blocking KeepAlive Messages: Fabricating Address Withdraw Messages Fabricating Label Withdraw Messages: Exhausting Label Memory: Creating Loops: LSP Deletion. Path State Resource Exhaustion. Excessive LSP ID Allocation.

1.2.2 Attacks on the Control Plane

LSP Creation by an Unauthorized Element LSP Message Interception Attacks against RSVP-TE Attacks against LDP Denial-of-Service Attacks on the Network Infrastructure Attacks on the SPs MPLS/GMPLS Equipment via Management Interfaces Cross-Connection of Traffic between Users Attacks against Routing Protocols

1.2.3 operation and managemnet

MAlicious collaborator Unauthorizd access to LER misconfiguration 6

1.2.4 insider attacks

19)

1.2.5 Enumeration attacks

Ingress Probing Record Route Object Access.

1.2.6 Cross domain attacks

Promiscuous Path Acceptance. PreLabeled Traffic Acceptance.

refer the book number 5 for ending paragraph

Most of the literature covering MPLS security usually concerned itself with a certain use case. [1] [11][12][15] analyzed the security issues of MPLS VPN. [3] concerned with the security framework to be implemented for the MPLS network. [8] elaborated on the security concerns in implementing label stack encoding. We therefore need to summarize a set of security threats that is commonly faced by MPLS network as well as the existing security tools to identify the pros and cons of implementing them and determine if the implementation of the OS in MPLS is justifiable or not.

1.3 Exisiting security tools

Several Security tools already exists to make MPLS more secure. Each tool having its own set of features and complexities to make data transmission over MPLS network more secure. A thorough analysis needs to be made regarding which tool to be used based on the operational requirements and feasibility of its implementation in the current scenario. There is no one single tool that solves all the security issues plaguing the MPLS network, however proper consideration and analysis of the security requirements of the system and using the appropriate tool to mitigate them is more than enough to make MPLS secure enough for business requirements. Based on this idea it is best to have a suitably large number of security tools in the arsenal to fight off the possible security threats. Security tools range from a wide variety of mechanism to make MPLS secure. some of which are described in the following.

1.3.1 Payload Encryption

One of the ways to make MPLS more secure is to encrypt the data that is to be passed through it. This prevents any sniffing attacks from sniffing any confidential data that a company or service provider may be transmitting via the MPLS network. Packet Encryption is ideally a responsibility of the application that is sending or receiving the data. Applications can use security tools like Transport Layer Security (TLS) which is an Internet standard to implement privacy and data integrity between communicating computer applications.

IPsec is another tool which can be applied end-to-end or hop-by-hop applications to maintain privacy and data integrity. It is mainly used to encrypt IP packets that flow through the network. IPSec can be used to encrypt the IP packets before they are passed onto the MPLS network. IPsec has historically placed a heavy "full-mesh" configuration burden on implementation although this is now ease with the introduction of the NULL Authentication Method in the Internet Key Exchange Protocol Version 2 allows for opportunistic key exchange to support IPsec [1].

1.3.2 Link layer security

Moving down the IP stack, encryption is also possible in the Layer 2 (Link Layer). Packets can be encrypted on a hop by hop basis between two communicating routers using MACsec. MACsec encrypts Ethernet frames that transmit across ethernet network. Thus end to end security can be implemented by creating a chain of trust between all the participating routers in the network path.

1.3.3 Pseudowires

MPLS is used to transport data of multiple protocols like Ethernet, ATM, TDM along with IP. Security tools limited by protocol types often don't help in fully leveraging the strengths of MPLS networks. Security tools that work for all types of protocols go well with MPLS implementation. Such a tool is pseudowire (PW) encryption. PW security is carried out by setting up pseudowires that tunnel the native service through the MPLS core by encapsulating at the edges [13]. The benefits of PW encryption is that compromising of edges or routers becomes very difficult. Protection of control

plane messages means protection from majority of attacks.PEs are usually configured to reject MPLS packets from outside the service provider network, thus ruling out insertion of PW packets [1] from the outside [13]

The reason why MPLS does not provide encryption or any other data confidentiality features is because in a conventional IP networks, every router in a network ideally analyses IP packet headers to process it. Encryption will add additional overhead and delay in the network [10x]. However with the increasing implementation of MPLS in mission critical applications the added data integrity, confidentiality and authentication may outweigh the overhead introduced. To get a better judgment of the cost to benefit ratio this project aims to calculate the overhead cost involved in implementing this opportunistic security in MPLS networks which can further strengthen or weaken the case of its feasibility in real life implementation.

1) payload encryption 1 2) Link layer security 1 3) Encryption on Pseudowires 1 4) Management System Authentication 13 5) p2p authentication 13 6) IPSEC in MPLS 13 7) Diffserv 13 8) Encryption for Device Configuration and Management 13 9) Access Control Techniques, Filtering,

1.4 Section 1.1

Chapter 2

Design

2.1 Description

2.2 Mininet

2.3 OpenVSwitch (OVS)

2.4 Network Setup

2.5 OS changes in OVS

mininet OVS mininet + ovs = h1,h2,h3,s1,s2,s3 mpls setup changes in ovs (CW, encryption GCMAES, DECRYPTION)

Chapter 3

Implementation

3.1 Server setup

3.2 Mininet Setup

3.3 Open vSwitch (OVS) setup

3.4 Code Changes in OVS

Chapter 4

Experiment

4.1 Running the system

4.2 Logging the metrics

Chapter 5

Results

5.1 Analysis of the metrics

5.2 Results

Works

Chapter 6

Conclusion

Appendix

...

Bibliography

[1] Denise Grayson, Daniel Guernsey, Jonathan Butts, Michael Spainhower, and Sujeet Shenoi, "Analysis of security threats to mpls virtual private networks", *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 146 – 153, 2009.

[2] Sahel Alouneh, Abdeslam En-Nouaary, and Anjali Agarwal, "Mpls security: an approach for unicast and multicast environments", *annals of telecommunications - annales des télécommunications*, vol. 64, no. 5, pp. 391–400, Jun 2009.

Appendix

...