Master's thesis

NTNU
Norwegian University of Science and Technology

FANKAM MAMEKONG RITA GABRIELLE

# Detecting network anomalies in Ethernet/MPLS/IP networks using Ethernet OAM performance data

Master's thesis in Communication Technology
Supervisor: Steinar Bjørnstad
June 2021

NTNU
Norwegian University of
Science and Technology

FANKAM MAMEKONG RITA GABRIELLE

# Detecting network anomalies in Ethernet/MPLS/IP networks using Ethernet OAM performance data

Master's thesis in Communication Technology
Supervisor: Steinar Bjørnstad
June 2021

Norwegian University of Science and Technology

NTNU
Norwegian University of
Science and Technology

**Title:** Detecting network anomalies in IP/MPLS/Ethernet networks using Ethernet OAM performance data

**Student:** FANKAM MAMEKONG Rita Gabrielle

**Problem description:**

The society is becoming increasingly dependent on data and telecom networks, making attacks of the networks increasingly attractive for criminal activity. The increasing complexity of the network makes it vulnerable to attacks. Ethernet is a widespread low-cost technology originating from LAN networks and now being used to create WAN networks. In this project we will analyze the Ethernet OAM performance data frame delay and frame loss to identify anomalies like, hardware fault and change in normal operation of the network. The goal is to analyze the patterns of frame loss and frame delay for identifying which type of anomaly the different patterns may indicate. E.g. how it can be differentiated between a congested network, attenuation on the optical link or a change in equipment along the monitored path.

**Date approved:** 2021-02-15

**Supervisor:** Steinar Bjørnstad

## Abstract

The effective monitoring of big data and telecom networks is becoming more and more crucial nowadays. Network anomalies can cause a decrease in performance , prevent the normal functioning of a network or put the network out of service completely. Deployment and monitoring cost of large networks are costly so network operators are constantly looking for solutions to reduce this cost. One approach employed was the enlargement of the Ethernet technology scope for use in WAN networks that run on gigabit speeds. The Ethernet became a technology used in WAN networks and now known as carrier network. The lack of Operations, Administration and Maintenance (OAM) functionalities for its management was a problem leading to the creation of Ethernet OAM which is an operation, administration and management tool for Ethernet networks.

In this thesis we evaluate the accuracy by which the Ethernet OAM can help detect anomalies in a network. we simulate a gigabit Ethernet Network and introduce common network anomalies to investigate this. A comparison is done between the loss and delay experienced by the traffic in the network and the different rates of the Ethernet OAM stream present in the network.

Results obtained show that Ethernet OAM can effectively be used at a certain rate to detect anomalies in a network. Finally, some suggestions for future work is given.

# Preface

This thesis is submitted in partial fulfillment of the requirements for the master degree of science in communication technology at the Norwegian University of Science and Technology.

I would like to thank the following people without whom this piece of work would not have been possible. To Steinar Bjørnstad for his constant supervision, guidance and availability throughout the thesis. To my friends, for their moral support, endless love and advices throughout this period. Lastly to my family, especially my departed father gone earlier this year. For his constant support, be it financially and emotionally, his endless encouragements, advices and forever love. To my mom, brother and sisters for their attention, care, support and encouragements.

# Contents

# List of Figures

# List of Tables

# List of Acronyms

**1DM** one-way frame delay measurement frame.

**API** application programmable interface.

**ARP** Address Resolution Protocol.

**BER** bit error rates.

**CAD** contextual timeseries anomaly detection.

**CCM** continuity check message.

**DDoS** Distributed denial of service.

**DMM** frame delay measurement request.

**DMR** frame delay measurement reply.

**DoS** Denial Of Service.

**EFM** Ethernet in the first mile.

**ETH-SLM** Ethernet Synthetic loss measurement.

**ETH-DM** Ethernet Frame delay measurement.

**ETH-LM** Ethernet Frame loss measurement.

**ETH-ED** Ethernet Expected Defect Function.

**ETH-BN** Ethernet Bandwidth Notification.

**ETH-CSF** Ethernet Client Signal Fail.

**ETH-VSP** Ethernet Vendor Specific.

**ETH-EXP** Ethernet Experimental OAM.

**ETH-MCC** Ethernet Maintenance Communication Channel.

**ETH-APS** Ethernet Automatic Protection Switching.

**ETH-Test** Ethernet Test.

**ETH-LCK** Ethernet Locked Signal.

**ETH-RDI** Ethernet Remote Defect Indication.

**ETH-AIS** Ethernet Alarm Indication Signal.

**ETH-LB** Ethernet loopback.

**ETH-LT** Ethernet Link Trace.

**ETH-CC** Ethernet Continuity Check.

**FCS** frame check sequence.

**FDB** forwarding database.

**FEC** Forward error correction.

**fifo** first-in first-out.

**GARP** Gratuitous Address Resolution Protocol.

**GUI** Graphical User Interface.

**HIDE** Hierarchical Intrusion Detection system.

**icmp** Internet Control Message protocol.

**IDT** interdeparture time.

**IP** Internet protocol.

**LAN** Local Area Network.

**LDP** label distribution protocol.

**LMM** loss measurement message.

**LMR** loss measurement reply.

**LOC** Loss of Continuity.

**LSTM** Long short term memory.

**MAC** Media Access Control.

**MEP** Maintenance entity group end point.

**MPLS** Multiprotocol Label Switching.

**OAM** Operations, Administration and Maintenance.

**PHAD** Packet Header Anomaly Detection.

**pps** data packets per second.

**QoS** Quality of Service.

**RTT** Round trip time.

**TCP** Transmission control protocol.

**UDP** User Datagram Protocol.

**VM** Virtual Machine.

**WAN** Wide Area Network.

# Chapter 1
# Introduction

## 1.1 Introduction

The ever-growing nature and complexity of data and telecom networks makes it prone to attacks and difficulty in monitoring. Being able to detect an abnormal behaviour during monitoring and identify it's origin or root helps keep it reliable and secure. Network anomalies can be defined as a variation or abnormal change in normal operation of a network. The increase dependency on data and telecom networks makes the detection of network anomalies necessary for several reasons, the increase dependency came about by the full digitalization of nearly every aspect of the world. Causing networks nowadays to carry a lot of critical and sensitive information for example information contained in banks, hospitals, military. These networks are also required to provide high Quality of Service (QoS) to end users and with the challenge to achieving this, network operators need to find ways in which they keep critical information safe from external attacks and a way to recognise these attacks, they should also be able to point out a decrease in network performance and its cause. These causes are known as network anomalies. Network anomalies are network failures like broadcast storms, transient congestion, babbling node, paging across the network, file server failure, crash of network nodes, faults at hardware core level, eavesdropping, Distributed denial of service (DDoS) [GGLL15]. In this work,

we would like to examine if we can discover any of these anomalies by monitoring an Ethernet network.
In today's networks, the Ethernet technology is widely spread across WAN networks due to its low cost.The transition of the Ethernet from LAN to MAN then to WAN(carrier Ethernet), was made to enable the Ethernet to provide secure communication, superior scalability, high availability and good quality of service [MSC05a]. Due to Ethernet scope enlargement, management of the Ethernet in an end-to-end manner was required bringing forth the creation of OAM functionalities leading to Ethernet OAM[HDMP11].The standardisation of Ethernet OAM was done by IEEE in IEEE 802.1ag[ag07] and ITU-T in ITU-T T.1731[Y.108]. Ethernet OAM functionalities are functions which help in administering and monitoring properly the network. Ethernet OAM functions are divided into two fault management and performance management. Fault management identifies and isolate faults in the network while performance management measures the throughput, delay etc. IEEE 802.1ag covers fault management while ITU-T T.1731 covers both fault and performance management. More details about Ethernet OAM is seen in chapter 2.

## 1.2 Background and Motivation

Anomaly detection in the area of data networks has become an area of critical research and practical importance. The network traffic contains a lot of information and these informations have been used in the search for anomalies.

Detection of network intrusion and fault detection in a network has been investigated [MP02]. This investigation involved the simulation of a wired conventional network with the presence of User Datagram Protocol (UDP) flood attack with the following data collected from the network: IP in-packet length, IP in-packet traffic, IP in-byte traffic, IP in-packet rate, IP in-byte rate, UDP in-packet length, UDP in-packet traffic, UDP in-byte traffic, UDP in-packet rate, UDP in-byte rate. For analysing this data in search of the anomalies, a framework Hierarchical Intrusion Detection system (HIDE) was developed ,which consist of: an event processor, a

statistical processor, a neural network classifier (used to identify patterns in a set of data) and a post processor.It has as input data: network traffic, system logs and hardware reports obtained from the monitored network, and as output: anomaly alarms, network reports and event log. The event processor gets the traffic input data and converts its format into one readable by the statistical processor. The statistical processor has in memory a referenced traffic profile of typical network activities and compares it with the information gotten from the event processor, it generates a stimulus vector which is fed to the neural classifier. The neural classifier analyses this stimulus and decides if the traffic is normal or not. For the accuracy of measurements, the network information was collected over different detection time windows since network traffic isn't stationary and the duration of network based attack can vary[MP02]. This proposed methodology was able to detect intrusion attack generated by UDP floods. IP flows were looked into, to tackle the issue of detecting network anomalies, with the use of IP flow graph analysis[AMP$^+$13] . This investigation involved the development of an algorithm, which collects the following IP flows:percentage of the transmitted flows, percentage of the transmitted packets, percentage of the transmitted bytes, devices that transmitted more flows, devices that transmitted more packets, devices that transmitted more bytes, from the monitored network. It groups these flows based on their source and destination addresses at regular time intervals, uses the group formed to create a directed flow graph. From the flow graph, probabilities of the selected flow properties to the grouped flows are computed, it then computes the Tsallis entropy which is a non-extensive entropy which has a strong dependence on the initial conditions of a system, to the probabilities generated from each grouped flow. A verification of the entropy values is carried out to extract features of the flow behaviour. When one or more entropy value calculated to the existing properties is dispersed, anomaly alarms are triggered. This method was proven in the analysis to be able to detect a DDoS attack, no other anomaly was tested.

Another approach used in detecting network anomalies was the use of log information. A model was built for basic anomaly detection based on log information

generated by network devices on an Multiprotocol Label Switching (MPLS) network [MDK+16]. The information contained in these logs are systems failures or systems malfunctioning like: user login, failed user login, raising CPU temperature, command line configuration. The model developed systematically models cumulative counts logs for the different event types of the devices found in the network with 5 minute intervals. The model collects information and establishes a normal behaviour for the network, when the information from the logs are retrieved, it calculates a mean and when this mean has an abnormal deviation from the normal mean an alarm is being raised. This method is effective in detecting point anomalies. Conclusion at the end of the study was that, further investigations needs to be done to pin point the exact anomaly which occurred.

Round trip time (RTT) can also be used to detect network anomalies. RTT was used as a parameter in a study which proposed a methodology for detecting performance anomalies with the use of contextual information [DBDL17]. Contextual information can be defined as any information known by the network in its current running state [ADB+99]. To do the authors made use of contextual timeseries anomaly detection (CAD) methodology, this method works within a constructed time window. It acts in two steps, firstly it all gathers instances within the time window in the network that exhibit comparative temporal characteristics to establish a context(contextual information). An example of an instance could be clients connecting to the same server. With this established, the standard deviation and mean of the RTT measurements of the network under investigation is generated. If a deviation is noticed from the mean this could indicate routing changes, on the other hand if a shift is noticed from the standard deviation this could indicate a congested network. This method can detect path changes and congested network accurately [DBDL17]. Another study also involved using RTT but with a different methodology for the analysis. This methodology involved the use of a pattern analysis scheme [WZL16]. RTT varies throughout the day depending on the number of users online and the load of the network. The RTT for various days over a period of time is averaged and considered as the normal pattern for a day. When monitoring a

network where the RTT has a significant deviation from this established pattern, it is considered as an anomaly.

Another approach in the literature used for the detection of network anomalies is the use of a time frequency method[JHW+10]. The authors made use of a time frequency analysis detection method based on origin-destination flows. The origin-destination flows are grouped with respect to common destination addresses. Knowing that the time and frequency properties of a network traffic can be characterized by a time-frequency analysis. This time frequency analysis is then used to obtain high frequency characteristics of the network traffic and finally, the correlation coefficients of each OD flow is compared with others in the same group. This study showed that this detection methodology could accurately detect traffic anomalies. The use of information found in packet headers of the following protocols: Ethernet, IP, UDP, Internet Control Message protocol (icmp) and Transmission control protocol (TCP), was used in a study to detect network anomalies[GM16]. The algorithm developed in this study is known as packet header algorithm detection (PHAD). It is an algorithm which is initially made to run in a network where no attack is present. This is to obtain the values of specific fields in packet headers when running in normal conditions. After this stage, it is made to run on a live network traffic and raises an alarm when it comes across a value different from that learned in the specified fields. It raises an alarm as it considers this an anomaly. Note should be taken that it also raises false alarms and assumes that the less an unusual behavior is observed, the more likely it is extremely dangerous. In the study, this method was shown to detect anomalies but not all anomalies.

From the different network traffic parameters used in the literature, none involves the use of Ethernet OAM which brings us to the motivation of this thesis. The contribution of this thesis to the detection of network anomalies is the use of frame loss and frame delay of Ethernet OAM data to detect anomalies i.e the signature these anomalies leave on Ethernet OAM frame loss and delay.

The motivation of this thesis is to analyse the pattern in Ethernet OAM frame loss and frame delay to point out which anomaly can be detected.

## 1.3 Problem statement

In this thesis, we examine whether a normally used tool in carrier Ethernet networks known as Ethernet OAM, can be used to detect network anomalies. We are investigating the extent to which Ethernet OAM frame delay and frame loss can identify anomalies. This may reduce the cost of operating networks and ease management for operators . We evaluate which network anomalies can be detected by analysing the various patterns of Ethernet OAM frame loss and frame delay. Ethernet across Wide Area Network (WAN) means bigger network, higher number of nodes, increase complexity in nodes communication, increased vulnerability. Monitoring large networks are difficult and cumbersome. To make it easier, standardisation organisations decided that network layers needed to be monitored individually, and to do so each layer needed OAM functionalities. High monitoring leads to high cost hence the need for operators to turn to deployment of carrier Ethernet solutions to reduce operation costs.

## 1.4 Objectives of the thesis

The objective of the thesis is to perform and analyse the following goals:-

- investigate which anomaly can be detected with frame delay and frame loss
- investigate patterns in frame delay and frame loss which indicates an anomaly
- identify which pattern corresponds to which specific anomaly

## 1.5 Content of Thesis

chapter 2: Elaborates about Ethernet OAM and gives an analysis of the consequences of anomalies on frame loss and delay.

chapter 3: Describes the methodology and the tools used in the study.

chapter 4: Elaborates on the topology and the simulation carried out to achieve the objectives of the thesis.

chapter 5: Presents and discuss the results of the simulation.

chapter 6: Provides a conclusion for the thesis and proposes further works .

# Chapter 2
# Ethernet OAM

This chapter presents the factors which led to the creation of Ethernet OAM. The Ethernet OAM parameters useful for anomaly detection. How Ethernet OAM measures frame loss and frame delay and finally how anomalies affect Ethernet OAM.

## 2.1 Introduction

Over the years, the most used protocol for data transmission over Local Area Networks (LANs) is the Ethernet [Baj01]. The Ethernet technology is one that was created in the mid 1970's with transmission rates of 3Mbps, it grew over the years and now has rates up to 400Gbps. It allows backward compatibility, meaning the Ethernet Frame format of the latest standard are compatible the with those of earlier standards[Wikc]. Ethernet became one of the fastest-growing technologies in WAN due to its low-cost and its ability to be easily deployed. Enterprises with simple topologies generally managed their LANs with IP protocols since they didn't have to handle thousands of customers. End-to-end customer service provision by service providers deals with different and numerous customers, also with different operators. The increase in data transport caused by the increase of enterprises and end customers demands led to the creation of Ethernet OAM[MSC05b]. A representation of Ethernet OAM from the standard ITU-T Y.1731 can be seen in figure 2.1 below.

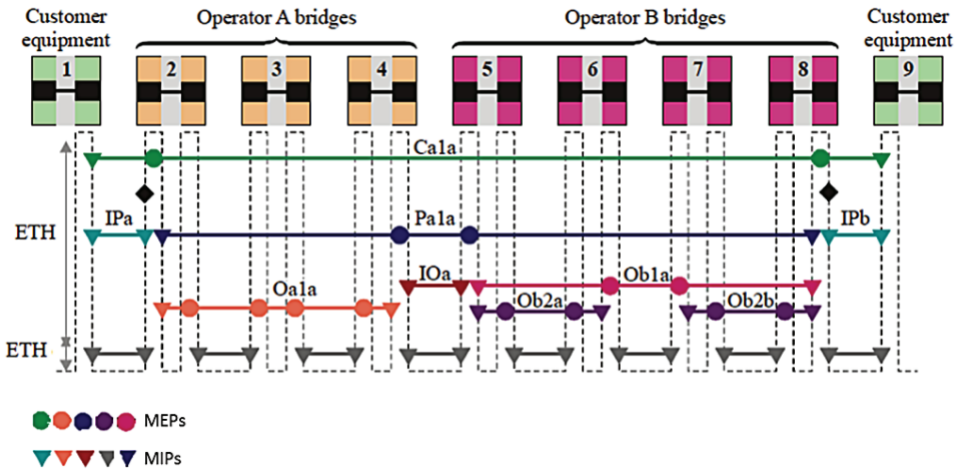



**Figure 2.1:** View of OAM with ITU-T Y.1731 from [Ham14]

## 2.2 Types of Ethernet OAM

There exist two types of Ethernet OAM. There is the link OAM and the service Ethernet OAM. Link OAM deals with Ethernet operating at single link level while service Ethernet OAM deals with connectivity provided by Ethernet on end-to-end basis and service provision guarantees [Ste06]

### 2.2.1 Link OAM

Used mainly in Ethernet in the first mile (EFM). EFM are leased lines connection of relatively low cost used to connect customers directly to their operators [swi]. This can be seen as access links. EFM generally consists of networks with simple topologies and provide direct point-to-point links between customer and service provider[Ste06]. This OAM is limited only to first mile links, provides no end-to-end service guarantee and does not provide performance measurement.Developed by the 802.3ah EFM task force.

### 2.2.2 Service Ethernet OAM

In an Ethernet based connection were we have users, service providers and network operators, each entity should have the capacity to independently monitor the layer connection under its responsibility. Service Ethernet OAM provides this independent monitoring , because it has eight OAM level. OAM level refers to the size of the managed network, the larger the managed network is, the higher its level. It assigns 3 levels to network operators, two to service providers and three to users by default. Higher-level OAM frames are transparently forwarded by lower-level devices[Ste06]. It provides end-to-end service guarantee, fault management and performance measurements.

The two Ethernet OAM's have distinct functions and could be used together. Having two running OAM protocols will burden equipment vendors and operators. Service Ethernet OAM can be restricted to a single link, this implies that link OAM is a subset of service Ethernet OAM. Causing link OAM to be used probably only in simple EFM[Ste06].

## 2.3 Useful Ethernet OAM parameters for Anomaly detection

Ethernet OAM is of interest for anomaly detection due to its ability to provide: system or network fault indication, performance monitoring, security management, diagnostic functions, configuration and user provisioning in an Ethernet network[Ham14]. It is a management tool used for the monitoring and recovery of the network in case of failure. Ethernet OAM determines the performance in the network such as wrongly configured nodes, failed nodes, frame loss, frame delay, end-to-end path identification and bit error rates with the use of its parameters. It supports fault management and performance monitoring functions. Fault management deals with the identification and isolation of faults; performance management measures throughput, delay, loss and jitter. With both functions conducted in an end-to-end manner on nodes. Nodes that initiate and terminate Ethernet OAM frames for end-to-end transmission are

known as Maintenance entity group end point (MEP)(see figure 2.1).

Ethernet OAM has a broad range of parameters. Under fault management we have the parameters: Ethernet Link Trace (ETH-LT), Ethernet loopback (ETH-LB), Ethernet Alarm Indication Signal (ETH-AIS), Ethernet Continuity Check (ETH-CC), Ethernet Remote Defect Indication (ETH-RDI), Ethernet Locked Signal (ETH-LCK), Ethernet Test (ETH-Test), Ethernet Automatic Protection Switching (ETH-APS),Ethernet Maintenance Communication Channel (ETH-MCC), Ethernet Experimental OAM (ETH-EXP), Ethernet Vendor Specific (ETH-VSP), Ethernet Client Signal Fail (ETH-CSF), Ethernet Bandwidth Notification (ETH-BN), Ethernet Expected Defect Function (ETH-ED). From these parameters, only the ETH-CC is of interest to us. The study focuses on Ethernet OAM frame loss and frame delay and the continuity check message (CCM) frame which contains ETH-CC is used for the measurement of frame loss and frame and frame delay. It helps detects Loss of Continuity (LOC) between any pair of MEPs in a same network domain.

Under performance management we have: Ethernet Frame loss measurement (ETH-LM),Ethernet Frame delay measurement (ETH-DM),Ethernet Synthetic loss measurement (ETH-SLM). These are used in our study because they contain information abour Ethernet OAM frame loss and delay. ETH-LM collects ingress and egress service frames counter values which maintains counts of transmitted and received frames between a pair of MEPs. ETH-DM measures frame delay and frame delay variation. ETH-SLM measures frame loss making use of synthetic frames instead of data traffic, also used for Ethernet multi-point connectivity[Y.108].

What we obtain from the 4 parameters chosen above are measures of frame loss and frame delay. Below we have a look at how the Ethernet OAM measures frame loss and delay.

## 2.4 Measurement of Frame loss and Frame delay with Ethernet OAM

Ethernet OAM makes use of counters to measure frame loss and frame delay.

1. **Measurement of frame loss**:

   This can be performed in two ways either dual ended or single ended[Y.108]. The dual ended approach make use of CCM frames while the single ended approach makes use of loss measurement message (LMM) frames for transmission and loss measurement reply (LMR) frames for reply . Both approaches have similar schemes, below we describe the dual ended scheme: In a point-to-point connection in an Ethernet network domain, two peers MEP keep two local counters. One for the frames transmitted towards a peer MEP($TXC_i$) and the other for the frames received from a peer MEP($RXC_i$). Each MEP transmits periodically the CCM frames with the following information:

   $TXC_f$: Value of $TXC_i$ at the time of CCM frame transmission

   $RXC_b$: Value of $RXC_i$ at the time of the last CCM frame reception

   $TXC_b$: Value of $TXC_f$ in the last received CCM frame

   The number of lost frames in both directions between two consecutive arrival of CCM frames, are calculated independently by the two MEP peers at $t_{pr}$ (reception time of previous frame) and $t_{cr}$(reception time of current frame). The calculation from(far-end) and to (near-end) a MEP is expressed as:

   $FrameLoss_{far-end} = [TXC_b(t_{cr}) - TXC_b(t_{pr})] - [RXC_b(t_{cr}) - RXC_b(t_{pr})]$

   $FrameLoss_{near-end} = [TXC_f(t_{cr}) - TXC_f(t_{pr})] - [RXC_i(t_{cr}) - RXC_i(t_{pr})]$

2. **Measurement of frame delay**:

   As in frame loss, there exist two approaches : one-way and two-way. One-way makes use of one-way frame delay measurement frame (1DM) frame while two-way makes use of frame delay measurement request (DMM) and frame delay measurement reply (DMR) frames. In the one-way scheme, a MEP sends a 1DM frame

with a timestamp, and the MEP receiving the frame calculates the delay of the frame, based on the time value at which it received the frame and the timestamp from the frame. This requires synchronisation of peering MEPs [Y.108]. In two-way scheme, a MEP sends a DMM with a timestamp frame to its peer MEP.The receiving MEP generates a DMR frame containing the value of the timestamp contained in the received DMM and resend to the origin of the DMM frame. Round trip frame delay is then calculated by the MEP at the reception of the DMR frame.

## 2.5 Effects of anomalies on Frame delay and Frame loss

The disruption or deviation in patterns of frame loss and frame delay from patterns observed when the network operates under normal conditions indicates a problem. In an Ethernet WAN network, observing the changes in patterns of Ethernet OAM frame loss and frame delay, pointing out which anomaly is occurring, permits the network administrator to carry out the correct course of action. Table 2.1 lists the general observation caused by chosen anomalies on Ethernet OAM frame loss and frame delay.

1. **Overloaded network**: An overloaded network occurs when a network has more traffic that it can handle i.e incoming traffic is more than the supported bandwidth of the network. For example, an incoming traffic of rate 1Gbps on a link of rate 10Mbps. In this situation, the incoming traffic is stored in the buffers resulting in frame delay. When the buffers are full the rest of the incoming traffic is lost resulting in frame loss [JRS+15]. The degree of frame loss and delay observed depends on the level of congestion. As an example, let's have a look at figure 2.2 below. We have 2 servers A and B transmitting on the link to the switch . Both servers transmit at rate 10 Gbps while the switch transmit at 1Gbps. In a situation where both servers are transmitting simultaneously at a rate of say 2Gbps each , the outgoing link of the switch becomes overloaded and as a result, a great deal of frame loss and delay occurs[BM93].

**Table 2.1:** Effects of anomalies on frame loss and delay

| **Effect of anomalies on Frame loss and Frame delay** | | |
|---|---|---|
| **Anomalies** | Frame loss | Frame delay |
| overloaded network | increasing rates of frame loss | increase in frame delay |
| Increase in Attenuation at optical link | increasing rates of frame loss | increasing values of frame delay |
| Break of optical link | complete frame loss | timeouts since no frames received |
| Eavesdropping | no significant change in case of passive attack, little rates in case of active attacks | no significant change |
| Hardware fault | low to high ratio of frame loss depending on the hardware fault occurring | low to high values of frame delay depending on the hardware fault occurring |
| Spoofing attack | no significant change | no significant change |
| Denial of Service | High rates of frame loss | High rates of delay |

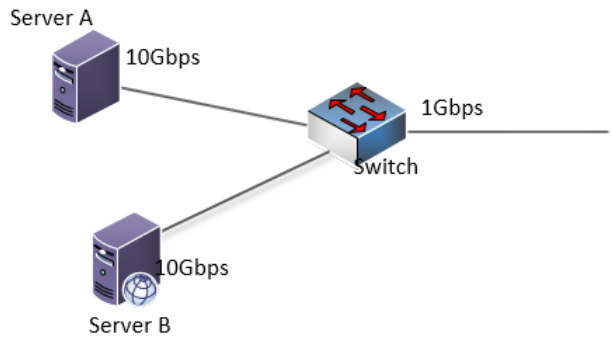



**Figure 2.2:** Overload link

2. **Sudden increase in attenuation of optical link**: The loss in signal intensity in network connection is known as attenuation[Com]. Attenuation is one of the

causes for bit error rates (BER) experienced in a received signal[SAGM14]. BER are detected at the ethernet layer by its frame check sequence (FCS) mechanism, when an FCS fails the frame is dropped causing frame loss. The degree of frame loss observed depends on the ability of the Ethernet to perform Forward error correction (FEC). The faster the rate at which the Ethernet can perform FEC the less frame loss will be observed with Ethernet OAM. Time taken to perform FEC adds delay in the network that is picked by Ethernet OAM. Let's take a simple case where the Ethernet doesn't perform any FEC, the network administrator will observe frame loss but not frame delay because, the packets transmitted will have the average values of the propagation delays in the network.

3. **Optical link break**: When a network containing optical fiber links experiences a break, there is a disruption in the data transfer[FWG+16]. This is picked up at the Ethernet layer which experiences full frame loss since it receives no signal from the physical layer.

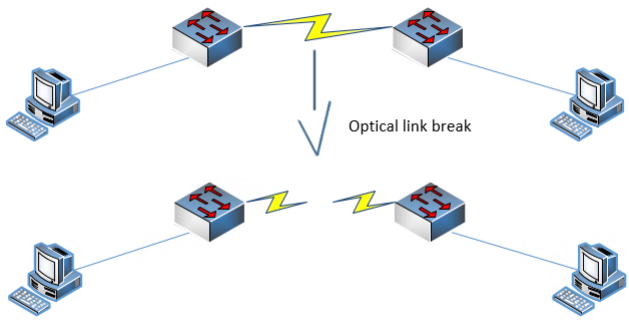



**Figure 2.3:** Optical link break

4. **Eavesdropping**: eavesdropping is an attack against the network where the attacker captures the data sent in an unsecured or weak spot of a network to read and analyse the content [Wika]. When the attack is passive i.e it doesn't transmit data, it doesn't interfere with network traffic [YA15]. Hence doesn't

affect the performance of the network, passive eavesdropping cannot be detected by analysing the frame loss and frame delay of Ethernet OAM. In an active eavesdropping attack, the attacker creates a bent in the optical link. This results in the leakage of light at the fiber core border, degrading the quality of the signal[FWG+16]. As a results the signal received at the Ethernet layer has bit errors and results in frame losses.

5. **Hardware fault**: Occurrence of hardware fault affects the performance parameters in different ways depending on which hardware fault occurred. A direct consequence of a hardware fault is a babbling node [BPZ07]. A babbling node sends repeatedly unwanted traffic, causing congestion which leads to an overloaded network, resulting in frame delay and frame loss. The degree of frame loss and delay will depend on the level of congestion created by the babbling node. Another hardware fault could be a node being completely down, this case results in full frame loss from traffic passing through this node.

6. **Spoofing attack**: Spoofing attack is an active attack where an attacker gains illegal access to a network by falsifying data i.e masquerading [DNC03]. One spoofing attack that occurs at the data link layer is MAC spoofing, here an attacker sends a false Gratuitous Address Resolution Protocol (GARP) packet containing frames with false Media Access Control (MAC) addresses in the network. GARP notifies about spoofed MAC and IP addresses to devices in the network. Due to lack of authentication for received ARP packets, the devices receiving this GARP packet change their cached entries in which the attacker made his switch the default gateway . The traffic passes through the attacker's device where the traffic is analysed before being routed to the actual network gateway[MMA20]. This introduces additional delay in the network under normal conditions due to increase in transmission path.

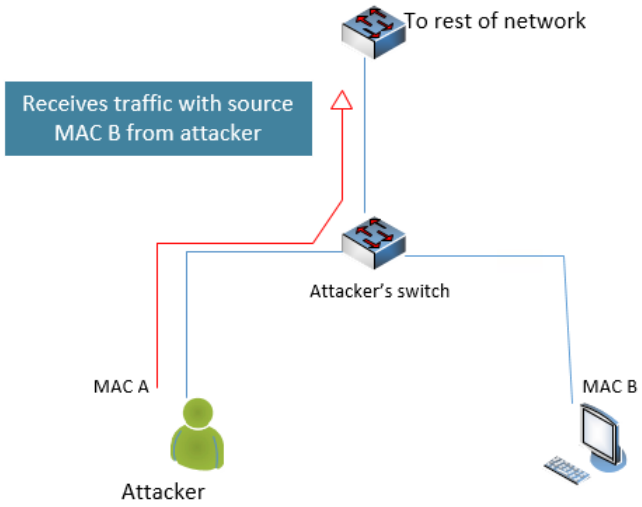



**Figure 2.4:** MAC Spoofing attack

7. **Denial of Service**: Denial Of Service (DoS) is an attack which aims at the exhaustion of network resources [KBT15]. DoS can be performed at the physical layer and at the link layer. At the link layer it makes use of ARP flooding as explained in spoofing attack above, the difference is that, the attacker disables its IP packet routing[EHT07]. Meaning after the attacker receives the traffic he doesn't forward it to the actual network gateway causing and interruption in data transfer and the network experiences full frame loss or high rates of frame loss. At the physical layer, a break/cut in the optic fiber will cause DoS[FSK11] as explained in the case of optical fiber break above.

From table 2.1 above, we observe different anomalies affecting frame loss and delay in a similar way. A more detailed analysis is needed in order to point out which pattern represents which exact anomaly. One way to do this is by examining the correlation between the occurrence of the frame loss and frame delay. From the above discussion the anomalies with similar patterns on frame loss can be grouped

as seen in table 2.2 below.

**Table 2.2:** Grouping of anomalies with similar effects on frame loss

| **Anomalies with similar frame loss pattern** | | |
|---|---|---|
| -Overloaded network | -break of optical link | -passive eavesdropping |
| -Hardware fault(babbling node) | -Hardware fault (node down) | -Spoofing attack |
| -Increase in attenuation at optical link | -Denial of service | |

**Table 2.3:** Grouping of anomalies with similar Frame delay pattern

| **Anomalies with similar frame delay pattern** | | | |
|---|---|---|---|
| -break of optical link | -Overloaded network | -active eavesdropping | -passive eavesdropping |
| -Hardware fault (node down) | -Hardware fault (babbling node) | -spoofing attack | |
| -Denial of service | | -Increase in attenuation at optical link | |

From the classification above, we can extract some observed patterns in frame delay and frame loss according to the different anomalies. Observing a simultaneous increase in frame loss and delay, could indicate a congestion which points to either an overloaded network or a babbling node. A simultaneous increase in frame loss and little or no increase in frame delay, could indicate an increase in attenuation at the optical link or active eavesdropping. A simultaneous increase in frame delay with slight increase or no frame loss could indicate a spoofing attack. Observing no data transfer i.e no packet going through the network, points out to either a DoS attack, a node down or a break in the optical link.

# Chapter 3
# Methodology and tools Used

In this chapter, the methodology used in the thesis to address its objectives is presented. Why this methodology was chosen and a brief description of the tools used during the study. Two methods were used in this thesis; a literature review and a simulation.

## 3.1 Literature review

This is an important part in the research because it helps gather information available on the subject, acquire new knowledge and information about the topic under study. Conference papers, White papers, research publication were studied to understand : Ethernet OAM and its use, anomalies that can occur in a network and patterns of delay and loss in data-packet switched networks. These papers and publications were found on google, digital libraries like : google scholar, IEEE, researchgate, ITU. They were chosen based on their relevance, state of art and publication date.

## 3.2 Simulation

This method was chosen because it is difficult to carry out this investigation in a real environment. It was not conducted in the lab because of the lack of necessary equipment's to carry out this investigation. It wasn't carried out analytically because

simulation gives a more realistic approach and creates a base or foundation for when the network becomes more complex. With the analytical approach if factors are added to the network, a new analytical approach will need to be carried out. Whereas with a simulation platform, only the integration of this factors are required. Simulation also provides us with a flexible and malleable environment were we can carry out many test in seconds or minutes and be able to collect a great load of data. The simulation is described in chapter 4.

## 3.3 Tools

The platforms used to carry out the simulations are described below

### 3.3.1 GNS3

GNS3 is a free and open source software used for the configuration, testing, troubleshooting and emulation of real and virtual networks. It gives the possibility to run small topologies as well as big topologies( i.e many devices on servers). It has an architecture which consists of two software components, the all-in-one and the virtual machine. The all in one consist of a graphical user interface and is the client part of the software while the Virtual Machine (VM) is the server part of the software. It permits to build real life scenario topologies as seen in figure3.1below. emulated and simulated devices are supported on this platform. Emulation is when actual images of real routers or switches are run on a virtual device in this case real cisco ios. Simulation is the mimicking of functionalities of the hardware device( i.e either switch or router etc)[gnsb]. This platform was used to build the network topology used for the simulation, see figure 4.1.

For the simulation, there was the need of a traffic generator that generates traffic reflecting realistic traffic flows in real networks. We had to choose between ostinato and D-ITG. We chose D-ITG because it is a traffic generator which gives us the possibility to generate traffic following stochastic processes. In real networks, traffic arrivals are not constant. For example when the computer is in standby, the arrival

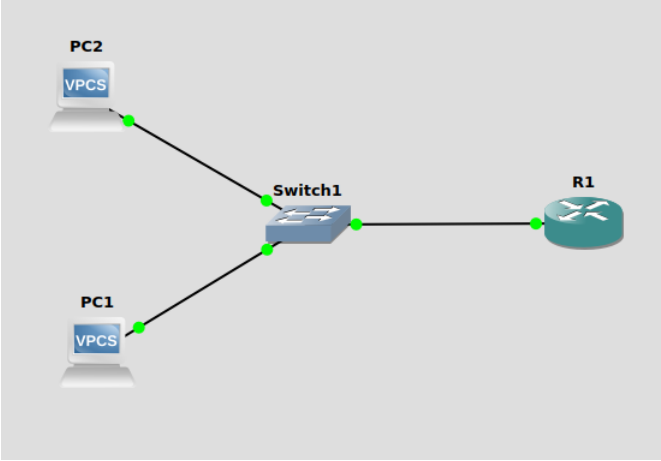



**Figure 3.1:** simple topology in gns3

rate is not the same as when the computer is performing file sharing or when the computer is downloading on peer-to-peer applications. Ostinato was used in the simulation setup to provide the interfering traffic creating the anomalies. D-ITG and Ostinato are described below:

### 3.3.2 D-ITG

D-ITG is a platform for generating network traffic packets and also a tool used for measurement of network performance parameters(i.e delay, throughput, jitter, frame loss). It gives the possibility to generate traffic with interdeparture time (IDT) and packet size which follows stochastic models. The architecture of D-ITG is presented below.

The main components for traffic generation are ITGRecv and ITGSend, ITGSend is the component generating the traffic. ITGSend and ITGRecv produce log files containing informations about the packets being sent. ITGSend can send multiple flows simultaneously to ITGRecv which can also receive them simultaneously. The generation of traffic between ITGSend and ITGRecv is controlled by a signalling channel. These two instances, produces log informations which can be saved locally or sent to the ITGlog instance. ITGlog collects and save all the measures from a

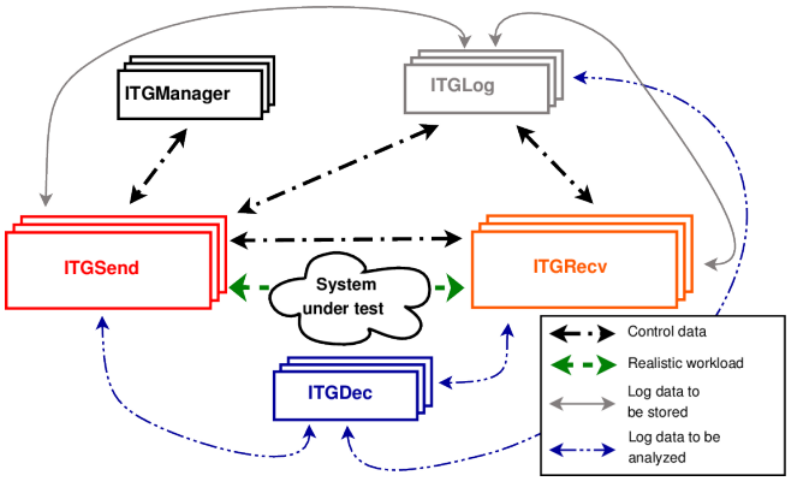



**Figure 3.2:** D-ITG architecture from [AGE+04]

single point. ITGDec produces performance metrics from the logs after analyzing them. The ITGmanager is representative of the fact that ITGSend can be remotely controlled by the D-ITG application programmable interface (API), permitting the user to control a large scale distributed experiment from a single point[AGE+04]. For delay measurements, it computes the difference between the transmission time and reception time of each frame. For frame loss measurements, it computes the difference between the number of frames generated by the ITGSend instance and the frames received at the ITGRecv instance.

### 3.3.3 Ostinato

Ostinato is a traffic generation tool, with a Graphical User Interface (GUI). It supports a wide range of protocols like: Ethernet, VLAN with QinQ, 802.3, LLC SNAP, ARP, IPv4, IPv6, TCP, UDP, ICMPv4, ICMPv6, IGMP, HTTP, SIP . It carries out automated tasks with the help of Python API. It has a simple architecture made of two binaries: a controller and a drone, as seen in figure 3.3 below[PMM+17].

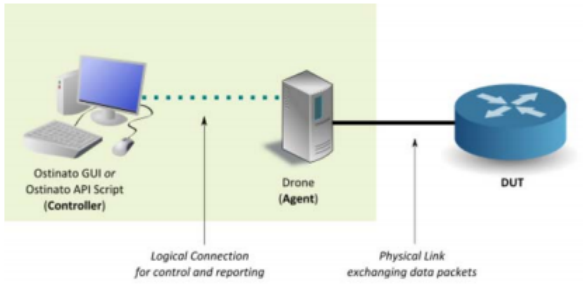



**Figure 3.3:** Ostinato architecture from [PMM+17]

# Chapter 4

# Network Anomaly Simulation Set-up

This chapter presents the simulation scenario used to investigate the objectives of the thesis.

## 4.1 Simulation aim

The aim of the simulation is to observe the variation of Ethernet OAM frame loss and delay when an anomaly is present in the network. The degree and accuracy by which Ethernet OAM can detect anomalies is being tested. This is done by deploying a gigabit Ethernet network in GNS3 and simulating anomalies scenarios with D-ITG and Ostinato.

## 4.2 Topology

The topology used for the simulation is depicted in figure 4.1. It is a switch based network consisting of 3 traffic generators and an EtherSwitch connected with gigabit Ethernet links. The transmission rates of the links are shown in table 4.1. These were chosen based on transmission rates of real Ethernet networks. D-ITG1 is generating the useful traffic in the network, along side with the Ethernet OAM packet stream. Ostinato-1 injects interfering traffic in the network. A representation of the traffic stream flow scenario can be seen in figure 4.2.

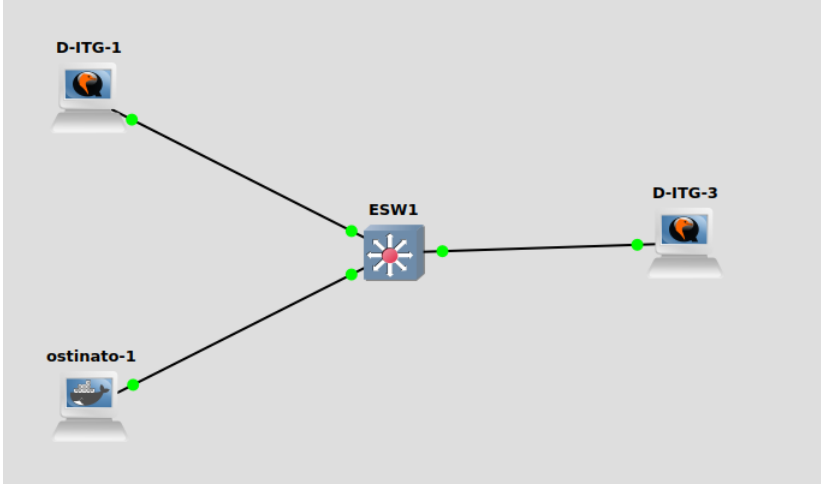



**Figure 4.1:** Simulation topology

**Table 4.1:** Links transmission rates

| Links | rates |
|---|---|
| D-ITG1 - ESW1(Fa0/0) | 1Gbps |
| ostinato1 - ESW1(Fa0/1) | 1Gbps |
| D-ITG3 - ESW1(Fa0/2) | 1Gbps |

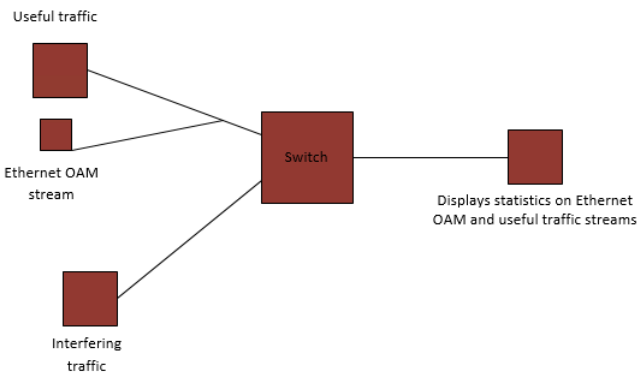



**Figure 4.2:** traffic flow

## 4.3 Hardware

The version of GNS3 used for the simulation was 2.2.10. The built in switches in GNS3 does not permit any network configuration and have 100Mbps ethernet interfaces. So, there was a need to add an Etherswitch which is configurable and contains 1Gbps interfaces. This was done by configuring an Etherswitch with the use of c3725 cisco IOS image following the installation guide in [gnsa]. The D-ITG version 2.6.1d added to a linux microcore 2.11.5 running on Qemu was added to the simulator. There was no installation guide for this, so it was installed following the steps as those for the Etherswitch. Ostinato is used on the docker platform, version 0.7.1 was integrated for use in GNS3 following the instructions in [Ber]. This topology was built in Oracle VM virtualbox 6.1.12 [Vir], running on linux mint 20 OS with kernel 5.4.0-40 and architecture: x86-64.

## 4.4 Simulation scenario

The network configuration and traffic characteristics are shown in table 4.2 and table 4.3 respectively. The run time of the simulation was set to 60 seconds because, there is total control of traffic behaviour making 60s enough time to get accurate information. The arrival rate of the normal traffic is Poisson, because it represents the nature of arrival rates of real traffic in networks. The transmission rates of the Ethernet OAM frames were chosen as stated in ITU-T Y.1731 [Y.108]. The transmission rates and frame sizes of Ethernet OAM are varied, to test which rate and frame size is suitable for detecting network anomalies. Ethernet OAM frames can have frames size ranging from 64 to 1518bytes [Jun]. The Ethernet OAM frame sizes were varied between 64 to 84bytes because, being a probe frame it shouldn't have large frame sizes that create overheads in the network. An assumption made was that, the Ethernet OAM frames shouldn't have larger frame sizes than those of useful traffic which is 128bytes. The frame size for the useful traffic was chosen arbitrarily between the possible frame range of an Ethernet packet[Wikb]. The mean arrival rate of the useful traffic was chosen so as to provide a flow of 0.5Gbps in the

network. The queueing strategy used in the switch is the first-in first-out (fifo). The result obtained from the Ethernet OAM stream will be compared to those of the useful traffic to see how accurately Ethernet OAM can detect anomalies.

The setup runs two type of anomaly scenario, an overloaded network and a DoS. Anomalies like hardware fault (node down) and break in optical fiber were not simulated because of the obvious outcome of complete frame loss. The simulation case for overloaded network is representative of 2 anomalies; an overloaded network and a babbling node. This is because, both anomalies result in the same effect i.e congestion.

**Table 4.2:** Network configuration

| devices | IP address | Subnetmask |
|---|---|---|
| SW1 - vlan2 | 192.168.0.1 | 255.255.255.0 |
| SW1 - vlan3 | 192.168.1.1 | 255.255.255.0 |
| D-ITG1 | 192.168.0.2 | 255.255.255.0 |
| D-ITG3 | 192.168.1.2 | 255.255.255.0 |
| Ostinato-1 | 192.168.0.6 | 255.255.255.0 |

**Table 4.3:** Traffic characteristics

| **traffic characteristics** | | | | |
|---|---|---|---|---|
| **Traffic type** | **Normal** | **Ethernet OAM payload** | **interfering overloaded payload** | **interfering DoS payload** |
| arrival rate | poisson | constant | constant | bursts |
| packet size(bytes) | 128 | 64, 74, 84 | 128 | 512 |
| transmission rate(pps) | mean=480000 | 10, 100 | 500000 | 200000 |
| simulation run time(s) | 60 | 60 | 60 | 60 |

1. **Overloaded network**: D-ITG1 and ostinato-1 transmit simultaneously to D-ITG3 . Ostinato-1 transmits at a rate of 0.6Gbps.

2. **DoS**: Ostinato-1 transmits bursts of traffic with 512 bytes at 200000pps(0.82Gbps), throughout the transmission time, to flood the network and exhaust network resources. The data frame size chosen is larger than the frame size of the useful traffic to hinder the passage of useful traffic.

## 4.5 Measurements

D-ITG3 uses its measurement functionalities to measure the frame delay and frame loss experienced by the normal and Ethernet oam traffic stream going through the network. This is stored in a log file and decoded with ITGDec.

# Chapter 5
# Results and Discussion

This chapter presents the results and discussion obtained from running the simulation performed above.

## 5.1 Results from overloaded network

An initial run without the interfering traffic was performed to get the normal running conditions of the traffic in the designed network. An observation of zero frame (0%) loss and an average delay of 0.15s, was made both for the useful traffic and the Ethernet OAM stream . The results obtained when running the simulation parameters for the overloaded network case in table 4.2, are presented in table 5.1. The different flows experience different frame delay and loss in the network. The interfering traffic cause the occurrence of frame loss and an increase in frame delay experienced by both the Ethernet OAM stream and the useful traffic. With regard to the case where the Ethernet OAM stream traffic operates at a rate of 10pps, Ethernet OAM experiences more loss than the actual traffic, but these two streams experience approximately same delay in the order of .26s to .28s (an increase in the range 60ms to 80ms). When Ethernet OAM is transmitted at a rate of 100pps, it experiences approximately same loss from 9.62% to 23.68% and same delay(an increase of 60ms to 80ms) as the useful traffic. Comparison bar chart of the frame loss and frame

delay are shown in figure 5.1, 5.4, 5.2 and 5.3.

**Table 5.1:** frame loss and delay from overloaded network scenario

| E-OAM Packet size (bytes) | Frequency of E-OAM (pps) | E-OAM frame loss (%) | Useful traffic frame loss (%) | Avg delay E-OAM (s) | Avg delay useful traffic (s) |
|---|---|---|---|---|---|
| 64 | 10 | 14.74 | 12.21 | 0.28 | 0.28 |
| | 100 | 9.62 | 9.71 | 0.27 | 0.27 |
| 74 | 10 | 11.39 | 10.73 | 0.27 | 0.27 |
| | 100 | 23.51 | 23.20 | 0.26 | 0.26 |
| 84 | 10 | 21.89 | 21.06 | 0.26 | 0.26 |
| | 100 | 22.34 | 23.68 | 0.26 | 0.26 |

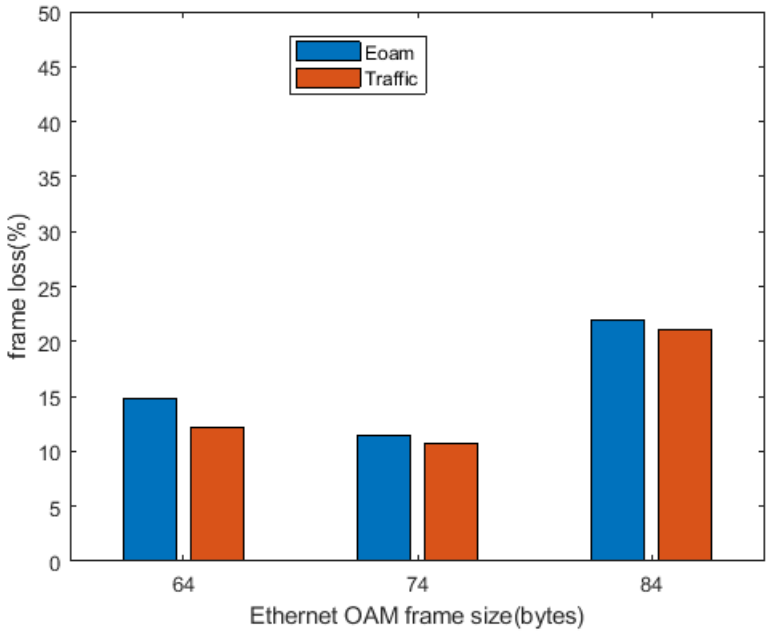



**Figure 5.1:** Frame loss experienced by Ethernet OAM 10pps stream compared to Useful Traffic loss

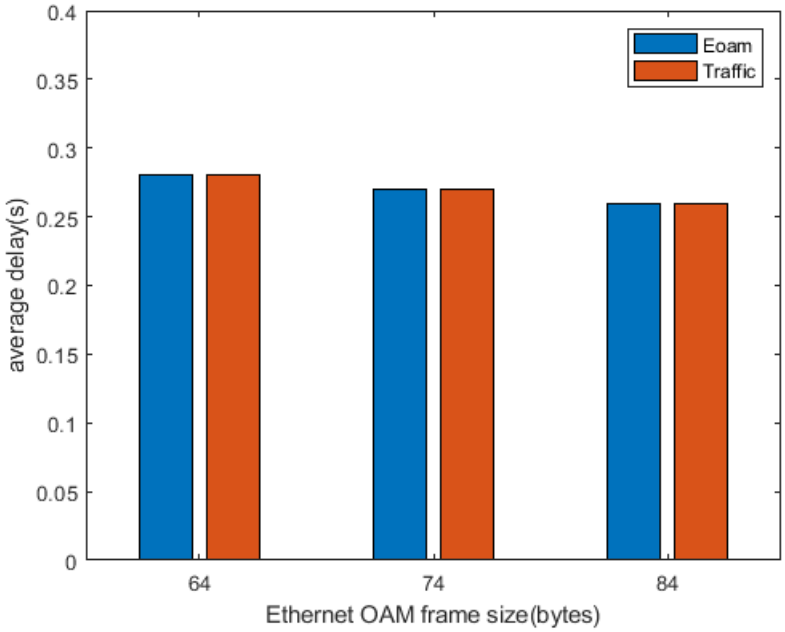



**Figure 5.2:** Delay experienced by Ethernet OAM 10pps stream compared to Useful Traffic delay

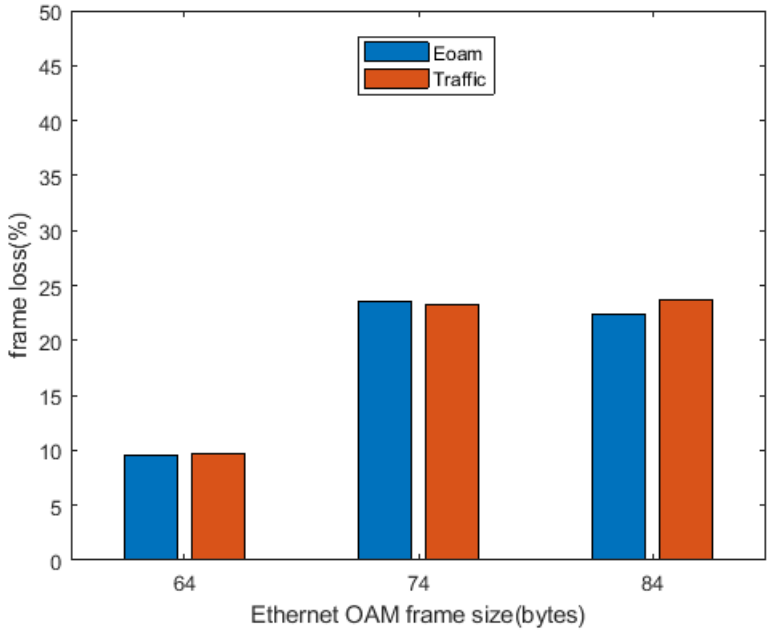



**Figure 5.4:** Frame loss experienced by Ethernet OAM 100pps stream compared to Useful Traffic loss

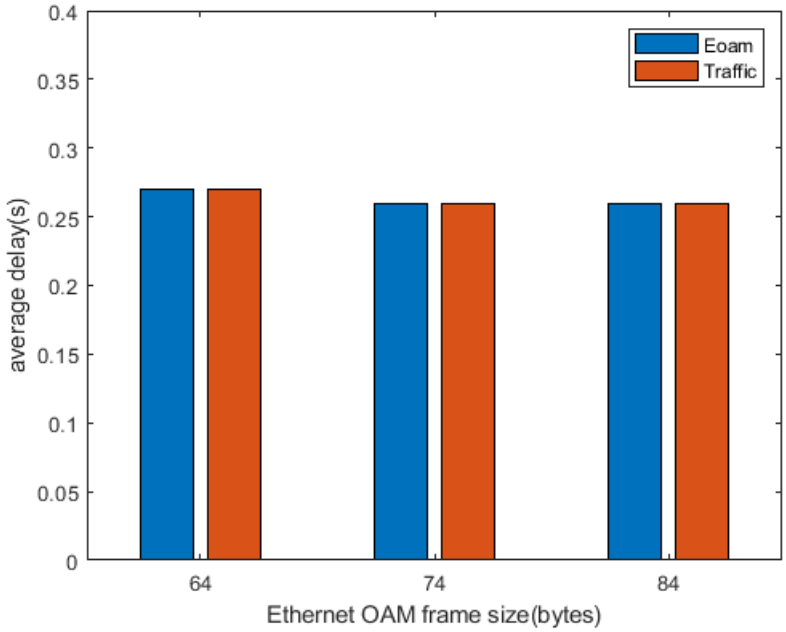



**Figure 5.3:** Delay experienced by Ethernet OAM 100pps stream compared to Useful Traffic delay

## 5.2 Results from DoS

Normal running conditions are the same as that observed in section 5.1. The results obtained when running the simulation parameters for the DoS case is presented in table 5.2. Here we observe really high rates of frame loss, over 55% for Ethernet OAM stream and over 65% for the useful traffic. Both traffics experience similar delay in the network. With regard to the transmission rate of Ethernet OAM data stream, in the 10pps case, the Ethernet OAM stream experiences 10% less frame loss than the useful traffic. At 100pps Ethernet OAM streams experiences 5% less frame loss than the useful traffic. Both traffic experience similar delay(an increase in the range 60ms to 80ms). A graphical representation of comparison between the frame loss and delay experienced by the Ethernet OAM stream and useful traffic in figure 5.5, 5.6 , 5.7 and 5.8.

**Table 5.2:** frame loss and delay from DoS scenario

| E-OAM Packet size (bytes) | Frequency of E-OAM (pps) | E-OAM frame loss (%) | Useful traffic frame loss (%) | Avg delay E-OAM (s) | Avg delay useful traffic (s) |
|---|---|---|---|---|---|
| 64 | 10 | 55.54 | 65.85 | 0.24 | 0.25 |
| | 100 | 64.63 | 71.71 | 0.24 | 0.24 |
| 74 | 10 | 63.19 | 73.01 | 0.23 | 0.24 |
| | 100 | 63.95 | 68.88 | 0.23 | 0.24 |
| 84 | 10 | 58.28 | 65.67 | 0.23 | 0.23 |
| | 100 | 63.23 | 68.37 | 0.23 | 0.23 |

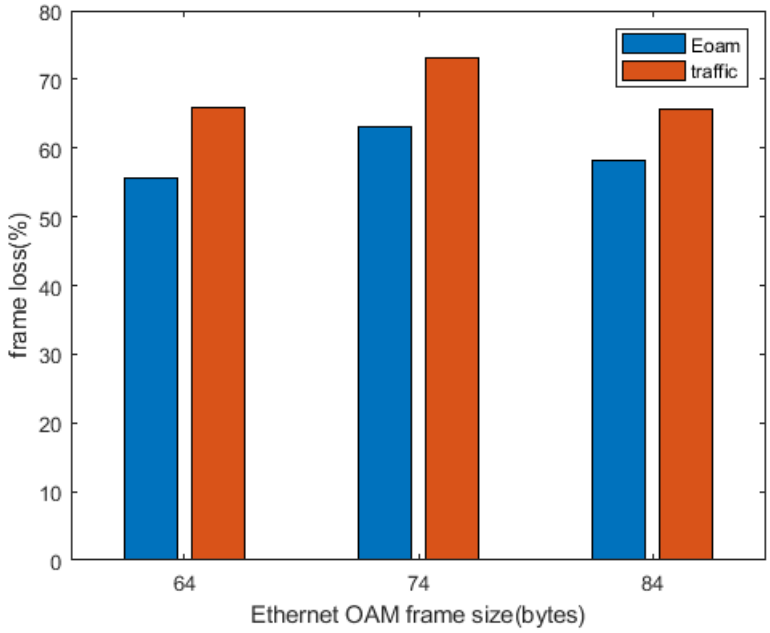



**Figure 5.5:** Frame loss experienced by Ethernet OAM 10pps stream compared to Useful Traffic loss

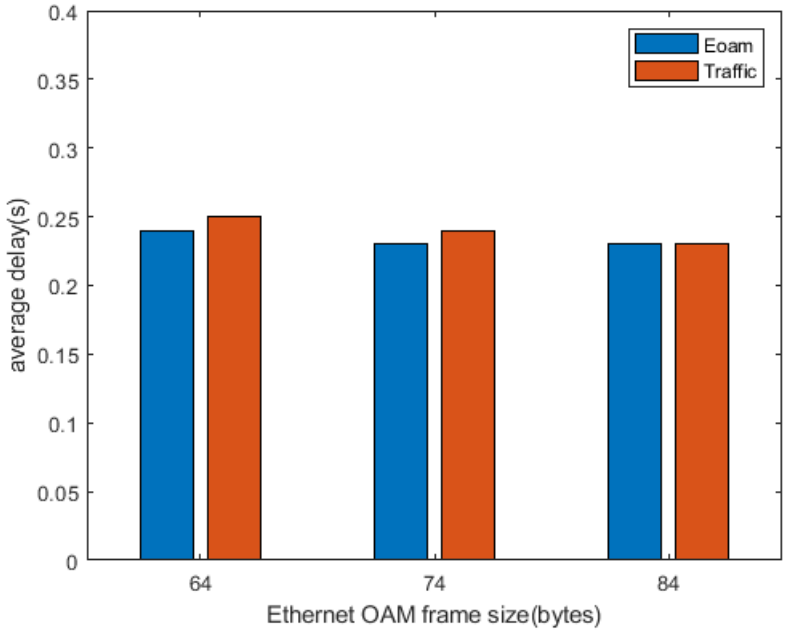



**Figure 5.6:** Delay experienced by Ethernet OAM 10pps stream compared to Useful Traffic delay

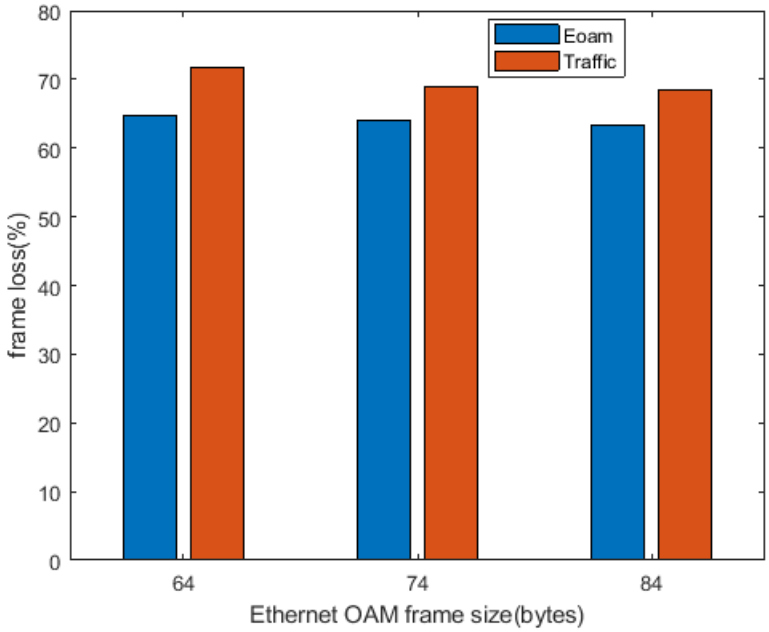



**Figure 5.8:** Frame loss experienced by Ethernet OAM 100pps stream compared to Useful Traffic loss

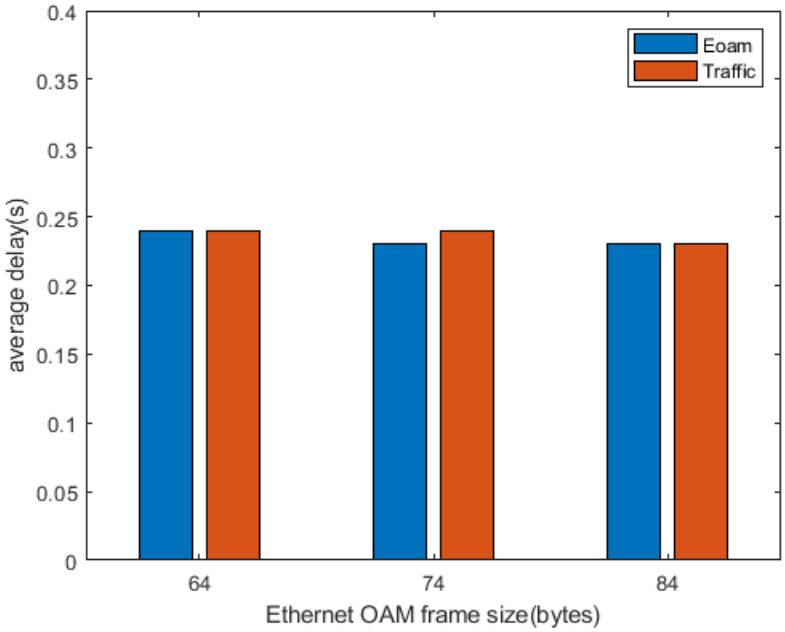



**Figure 5.7:** Delay experienced by Ethernet OAM 100pps stream compared to Useful Traffic delay

The frame sizes of the Ethernet OAM don't affect the loss and delay in the traffic because, they are small packets with low transmission rates i.e 51.2 Kbps, 59.5 Kbps and 67.2Kbps. The variation in frame loss and delay observed is due to the processing overhead that occur in the switch. Comparing the plots from Overloaded and DoS anomaly scenario, a pattern of simultaneous increase in delay and frame loss is observed. In both scenarios, the Ethernet OAM frames experience approximately similar delays, but the distinction of the anomaly is made regarding the degree of frame loss experienced by the traffic. In the DoS attack case, there is an abrupt change from zero frame loss to high rates of frame loss rate (55.54% to 73.01%). Whereas in the overloaded network case, the change is from zero frame loss to rates of 9.62% to 23.68%.

## 5.3 Discussions

In this simulation, Ethernet OAM packet sizes and transmission rate are varied to see how accurate one can use these data to detect anomalies in an Ethernet/IP/MPLS network. From table 5.1 and table 5.2, the variation between the delay and loss experience by the Ethernet OAM data is some what proportional to that experienced by the traffic. Probing the network with Ethernet OAM at a rate of 100pps gives more accurate results than probing with 10pps. The loss and delay obtained with 100pps Ethernet OAM traffic is representative of what the useful traffic is experiencing as can be seen by the results of the simulation above. Varying the size of the Ethernet frame in this case is shown to not matter when it has sizes less than the sizes of the traffic because the queue of the switch works on an first-in-first-out basis. Meaning that in case of congestion it drops frames that arrive when the queue is full not based on the type of frames. Also, the portion of the Ethernet OAM stream in the traffic is extremely small (51.2 Kbps, 59.5 Kbps, 67.2 Kbps), merged with traffic transmitted at 0.5Gbps. This simulation shows us that monitoring a live network with Ethernet OAM at a rate of 100pps in presence of an anomaly, can accurately depict the state of the network. With these values the network administrator can point out if an anomaly is occurring. An observation of abrupt raise from zero loss to high values loss values and increase in delay indicates to the network administrator that a DoS might be happening in the network. A mild increasing rate in frame loss and increase in delay indicates either an overloaded network or a babbling node.

# Chapter 6
# Conclusion and Future works

## 6.1 Conclusion

In this thesis, we presented a background on the traffic parameters used to detect network anomalies. A description of what is Ethernet OAM and how it came about. An analysis of how the different anomalies affect frame loss and delay in data switched networks. A simulation to investigate the effect of network anomalies on streams of Ethernet OAM frames, with different frame sizes and different transmission rates is carried out.

The simulation produced results for gigabit Ethernet network environments which have OAM functionalities. The results obtained demonstrated that a stream of Ethernet OAM packets with bit rate of 51.2 Kbps, 59.5 Kbps, 67.2 Kbps can accurately represent the loss and delay experienced by the traffic in a network transmitting at 0.5Gbps.

## 6.2 Future works

This section present suggestions of further work that could be done on this project. An algorithm that runs in the network and automatically collects the data from Ethernet OAM, analyses them and displays the corresponding anomalies could be developed.

# References


[ADB+99] Gregory D. Abowd, Anind K. Dey, Peter J. Brown, Nigel Davies, Mark Smith, and Pete Steggles. Towards a better understanding of context and context-awareness. In Hans-W. Gellersen, editor, *Handheld and Ubiquitous Computing*, pages 304–307, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[ag07] IEEE: 802.1 ag. Connectivity fault management. December 2007.

[AGE+04] S. Avallone, S. Guadagno, D. Emma, A. Pescape, and G. Ventre. D-itg distributed internet traffic generator. In *First International Conference on the Quantitative Evaluation of Systems, 2004. QEST 2004. Proceedings.*, pages 316–317, 2004.

[AMP+13] Alexandre A. Amaral, Leonardo S. Mendes, Eduardo H. M. Pena, Bruno B. Zarpelão, and Mario Lemes Proença. Network anomaly detection by ip flow graph analysis: A ddos attack case study. In *2013 32nd International Conference of the Chilean Computer Science Society (SCCC)*, pages 90–94, 2013.

[Baj01] Nijaz Bajgoric. Information technologies for virtual enterprise and agile management. In A. Gunasekaran, editor, *Agile Manufacturing: The 21st Century Competitive Strategy*, pages 397–416. Elsevier Science Ltd, Oxford, 2001.

[Ber] Bernhard. https://www.b-ehlers.de/projects/ostinato4gns3/index.html.

[BM93] L. Benmohamed and S.M. Meerkov. Feedback control of congestion in packet switching networks: the case of a single congested node. *IEEE/ACM Transactions on Networking*, 1(6):693–708, 1993.

[BPZ07] Giuseppe Buja, Juan R. Pimentel, and Alberto Zuccollo. Overcoming babbling-idiot failures in can networks: A simple and effective bus guardian solution for the flexcan architecture. *IEEE Transactions on Industrial Informatics*, 3(3):225–233, 2007.

[Com] Comptia. https://www.comptia.org/content/guides/what-is-attenuation.

[DBDL17] G. Dimopoulos, P. Barlet-Ros, C. Dovrolis, and I. Leontiadis. Detecting network performance anomalies with contextual anomaly detection. In *2017 IEEE International Workshop on Measurement and Networking (M N)*, pages 1–6, 2017.

[DNC03] R. Thompson Dale, Chaudhry Neeraj, and W. Thompson Craig. Rfid security threat model. pages 1–7, 2003.

[EHT07] Wassim El-Hajj and Zouheir Trabelsi. Using a fuzzy logic controller to thwart data link layer attacks in ethernet networks. In *2007 IEEE Wireless Communications and Networking Conference*, pages 2547–2552, 2007.

[FSK11] M. Furdek and N. Skorin-Kapov. Physical-layer attacks in all-optical wdm networks. In *2011 Proceedings of the 34th International Convention MIPRO*, pages 446–451, 2011.

[FWG+16] Marija Furdek, Lena Wosinska, Róża Goścień, Konstantinos Manousakis, Michał Aibin, Krzysztof Walkowiak, Sashko Ristov, Marjan Gushev, and José L. Marzo. An overview of security challenges in communication networks. In *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, pages 43–50, 2016.

[GGLL15] Anteneh Girma, Moses Garuba, Jiang Li, and Chunmei Liu. Analysis of ddos attacks and an introduction of a hybrid statistical model to detect ddos attacks on cloud computing environment. In *2015 12th International Conference on Information Technology - New Generations*, pages 212–217, 2015.

[GM16] Akash Garg and Prachi Maheshwari. Phad: Packet header anomaly detection. In *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, pages 1–5, 2016.

[gnsa] gns. https://docs.gns3.com/docs/using-gns3/beginners/switching-and-gns3/.

[gnsb] gns3. https://docs.gns3.com/docs/.

[Ham14] Dicko Hammadoun. Understanding ethernet oam. *IEEE Communications magazine*, pages 1–6, 2014.

[HDMP11] Rick Hofstede, Idilio Drago, Giovane Cesar Moreira Moura, and Aiko Pras. Carrier ethernet OAM: an overview and comparison to IP OAM. In Isabelle Chrisment, Alva L. Couch, Remi Badonnel, and Martin Waldburger, editors, *Managing the Dynamics of Networks and Services - 5th International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2011, Nancy, France, June 13-17, 2011. Proceedings*, volume 6734 of *Lecture Notes in Computer Science*, pages 112–123. Springer, 2011.

[JHW+10] Dingde Jiang, Yang Han, Xingwei Wang, Zhengzheng Xu, Hongwei Xu, and Zhenhua Chen. A time-frequency detecting method for network traffic anomalies. In *International Conference on Computational Problem-Solving*, pages 94–97, 2010.

[JRS+15] Wanchun Jiang, Fengyuan Ren, Ran Shu, Yongwei Wu, and Chuang Lin. Sliding mode congestion control for data center ethernet networks. *IEEE Transactions on Computers*, 64(9):2675–2690, 2015.

[Jun] Juniper. https://www.juniper.net/documentation/en_US/junose15.1/topics/concept/ethernet-oam-lfm-messages.html.

[KBT15] Christophe Kiennert, Samia Bouzefrane, and Pascal Thoniel. 3 - authentication systems. In Maryline Laurent and Samia Bouzefrane, editors, *Digital Identity Management*, pages 95–135. Elsevier, 2015.

[MDK+16] Muhammet Macit, Emrullah Delibaş, Bahtiyar Karanlık, Alperen İnal, and Tevfik Aytekin. Real time distributed analysis of mpls network logs for anomaly detection. In *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, pages 750–753, 2016.

[MMA20] Shahid Mahmood, Syed Muhammad Mohsin, and Syed Muhammad Abrar Akber. Network security issues of data link layer: An overview. In *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pages 1–6, 2020.

[MP02] C. Manikopoulos and S. Papavassiliou. Network intrusion and fault detection: a statistical anomaly approach. *IEEE Communications Magazine*, 40(10):76–82, 2002.

[MSC05a] M. McFarland, S. Salam, and R. Checker. Ethernet oam: Key enabler for carrier class metro ethernet services. *IEEE Communications Magazine*, 43(11):152–157, November 2005.

[MSC05b] M. McFarland, S. Salam, and R. Checker. Ethernet oam: key enabler for carrier class metro ethernet services. *IEEE Communications Magazine*, 43(11):152–157, 2005.

[PMM+17] Bharat Rahuldhev Patil, Minal Moharir, Pratik Kumar Mohanty, G. Shobha, and S. Sajeev. Ostinato - a powerful traffic generator. In *2017 2nd International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS)*, pages 1–5, 2017.

[SAGM14] Jahangir S.M., M. Alam, Hu Guoqing, and Md Mehrab. Improvement of bit error rate in fiber optic communications. *International Journal of Future Computer and Communication*, 3:281–286, 01 2014.

[Ste06] Yaakov Jonathan Stein. Ethernet oam. (20), 2006.

[swi] swiftinter. https://www.swiftinter.net/efm-broadband/#:~:text=Ethernet%20First%20Mile%20(EFM%20or,20%20Mbps%20with%20no%20contention.

[Vir] Virtualbox. https://www.virtualbox.org/.

[Wika] Wikipedia. https://en.wikipedia.org/wiki/Eavesdropping.

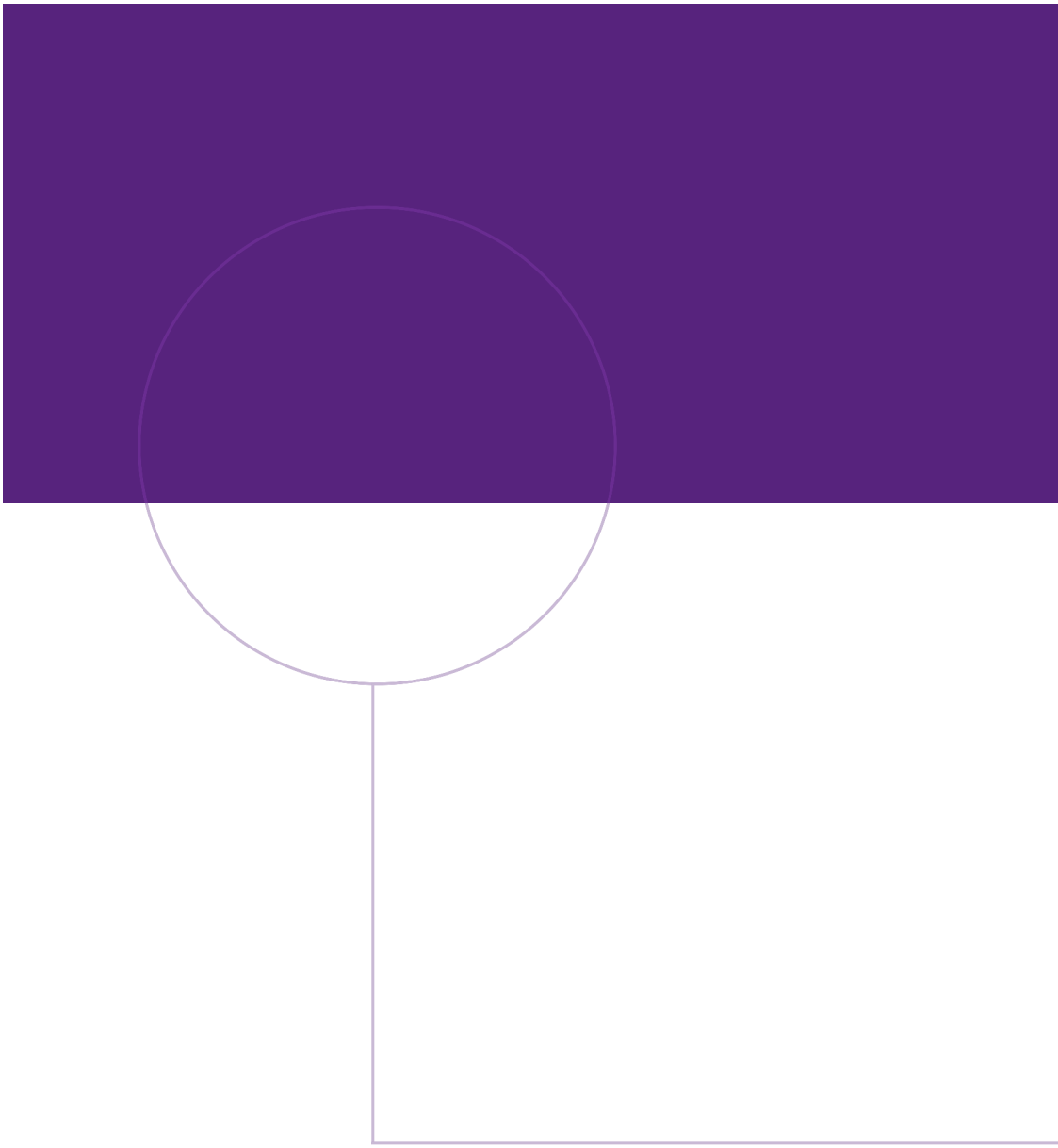
[Wikb] Wikipedia. https://en.wikipedia.org/wiki/Maximum_transmission_unit.

[Wikc] Wikipedia1. https://en.wikipedia.org/wiki/Ethernet#cite_note-29.

[WZL16] Jia-Qi Wei, Qian-Li Zhang, and Xing Li. Network anomaly detection and localization. In *2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pages 8–13, 2016.

[Y.108] ITU-T: Y.1731:. Oam functions and mechanisms for ethernet based networks. February 2008.

[YA15] Mustafa Harun Yılmaz and Hüseyin Arslan. A survey: Spoofing attacks in physical layer security. In *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, pages 812–817, 2015.



NTNU

Norwegian University of
Science and Technology