Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Hanne Malmin Bruleite

How a Control Plane Policed DDoS Attack Impacts the Latency of Time-Critical Offshore IoT Traffic

Master's thesis in Communication Technology
Supervisor: Steinar Bjørnstad
June 2020

NTNU
Norwegian University of Science and Technology

Hanne Malmin Bruleite

How a Control Plane Policed DDoS Attack Impacts the Latency of Time-Critical Offshore IoT Traffic

Master's thesis in Communication Technology
Supervisor: Steinar Bjørnstad
June 2020

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Title: Denial of Service in Offshore IoT

Student: Hanne Malmin Bruleite

Problem description:

The offshore industry is one of the most dangerous working environments that exists. People work closely to heavy machinery and in rough weather conditions far from shore. By introducing Internet of Things (IoT) to the offshore industry it is possible to monitor offshore operations from shore and with real-time IoT it is achievable to make the current processes remotely operated or autonomous. Real-time IoT technology can reduce human interaction with dangerous offshore operations.

IoT is a collection of several relatively simple devices and sensors that connect to the Internet access points using wireless connections. However, connecting this many devices to the internet increases the attack surface which is challenging for IoT and for when IoT is to be used for real-time applications. For real-time and other IoT applications the demand for secure, reliable and available services is crucial.

The problem is that in most cases IoT devices lack security mechanisms leaving the devices vulnerable to different kinds of cyberattacks. Such attacks can bring consequences such as for instance component failure, exposure of secrets, theft of information and economical loss. In the upcoming years IoT will be more and more commonly used also within real-time communication which introduce new consequences and challenges such as delay-sensitivity that potentially can cause material damage and loss of human life.

One of the more challenging kind of attacks for IoT and real-time communication is Denial of Service (DoS) attacks. A DoS attack can reduce a systems availability drastically. Availability is one of the core security concepts and can be affected during an DoS by disrupting the services and data flow by adding additional excess data traffic in the network. For real-time communication this is a crucial threat as it depends on rapid data flow when used in delay-sensitive applications.

The main challenge is that by replacing human machinery interaction with internet connected IoT devices, new challenges will occur. The idea of this project is to have a look at how a DoS attack can affect applications in an offshore IoT network, with special attention given to real-time applications.

Responsible professor: Steinar Bjørnstad, IIK

Supervisor: Steinar Bjørnstad, IIK

Abstract

Recently, 5G have been introduced as an enabler of time-critical applications with strict Ultra-Reliable Low-Latency Communication (URLLC) requirements. Several industrial sites use Internet of Things (IoT) to monitor and even control processes and objects either on site or remotely using wireless communication. However, this have yet to be deployed in the offshore industry.

There is no doubt that time-critical and mission-critical applications could be both interesting and useful for this partly isolated offshore industry. Although, several of the URLLC use cases have strict requirements with regards to latency. This is a challenge since the location of the offshore platforms are both isolated and far from *everything*. The longer the distance, the bigger the propagation delay, which further affect what applications that can be deployed at these locations.

IoT networks have been deployed successfully at several locations. Smart Power Grids and Autonomous Vehicles in Smart Cities are among the widely known IoT use cases. However, as more and more devices are connecting to the Internet, the attack surface keeps growing. It is commonly known that IoT devices are constrained in terms of resources, and hence easy for an adversary to take over and use as zombie devices that does whatever the attacker instruct them to do. Distributed Denial-of-Service (DDoS) attacks are one of the cyberattacks that is drastically increasing in both number of attacks as well as in strength. Such attacks can flood the network with excess traffic and can in many cases obstruct the legitimate data flows of reaching its destination and compromising the system's availability.

Control Plane Policing have been introduced as an mechanism that can prioritize traffic to reduce delay, allocate resources, but it can also be used to drop DDoS attack traffic and allow legitimate traffic through. By performing simulations of a router with and without a control plane policing mechanism, it is concluded that it is possible to deploy time-critical applications on offshore facilities at several locations, depending on the number of network nodes and the propagation distances in the network. The simulations also shows that Control Plane Policing can be useful to keep the time-critical data flows going for as long as possible, even during a DDoS attack.

Sammendrag

5G har nylig blitt introdusert, noe som vil gjøre det mulig å bruke tidskritiske applikasjoner som har strenge krav til pålitelighet og forsinkelse. Applikasjoner som har slike krav er også kjent som applikasjoner som krever ultra robust sanntids-kommunikasjon (URLLC) for å fungere. Flere bransjer har allerede tatt i bruk *Tingenes Internet* (IoT) og trådløs kommunikasjon for å overvåke og styre ulike prosesser og operasjoner, men dette har ikke blitt tatt i bruk i tilsvarende grad i offshore-industrien enda. Selv om platformene er delvis isolert og lokalisert langt til havs, viser det seg at tidskritiske applikasjoner kan være både aktuelle og interessante, også her. På en annen side er dette også utfordrende, grunnet applikasjonenes strenge krav til maksimal forsinkelse. Lengre avstander utgjør lenger reisetid for signalene. De lange avstandende kan i seg selv utgjøre en forsinkelse som i mange tilfeller kan overskride den maksimale toleransen til den gitte applikasjonen. Derfor er det ikke slik at alle applikasjoner kan brukes på alle lokasjoner.

IoT brukes allerede i forbindelse med førerløse kjøretøy samt i smarte strømmålere, som de fleste norske husstander har fått implementert de siste årene. I de fleste tilfeller gjør teknologien at ting blir enklere, men det følger også en bakside med slik digitalisering. Jo flere enheter som kobles til Internet, desto flere enheter kan bli brukt i nettbaserte angrep. Det er en kjent sak at enhetene som benyttes i IoT har en relativt begrenset mengde ressurser og dårlig sikkerhet, og kan enkelt bli overstyrt av en angriper. I nyere tid har antallet (distribuerte) tjenestenektangrep (DDoS) skutt i været og mange av dem er svært kraftige. Dette gjøres kun for å hindre nyttetrafikken i å nå frem til den ønskede destinasjonen og påvirker systemets tilgjengelighet og regnes som et sikkerhetsbrudd.

Control Plane Policing er introdusert som en mekanisme som kan brukes til å prioritere viktigere trafikk foran annen trafikk for å redusere forsinkelse. Dette er for eksempel også nyttig med tanke på ressursallokering i nettet og for å filtrere ut angrepstrafikk. Etter å ha kjørt simuleringer av en ruter både med og uten denne mekanismen, kan man konkludere med at det er mulig å ta i bruk tidskritiske applikasjoner offshore på flere lokasjoner, bortsett fra de lengst fra land. Reisedistanse og forsinkelse vil avhenge av lokasjon og antall noder i nettverket. Simuleringene viser også at det kan være nyttig å implementere en slik mekanisme i ruterene for å holde i gang tidskritisk datatrafikk selv under et tjenestenektangrep og for å la den tidskritiske trafikken flyte igjennom tilnærmet upåvirket av annen trafikk.

Preface

This thesis was written as the final part of the 5-year Master's degree program in Communication Technology at the Department of Information Security and Communication Technology (IIK), at the Norwegian University of Science and Technology (NTNU).

The problem description was established based on the research performed in the pre-project [13] between August and November 2019. A more specific research was carried out between January and June 2020, to explore the described problem area more in depth. And lastly, the title of the thesis was changed to make the objective of the thesis more clear and precise for the audience.

I would like to thank my responsible professor and supervisor Steinar Bjørnstad for his support and guidance throughout this semester. His feedback, suggested improvements and continuous advice have been essential for accomplishing this thesis. I would also like to thank professor Poul Einar Heegaard for answering questions when obstacles were encountered during programming in Simula and Demos.

On a personal note I would like to thank my incredible family for supporting, guiding and encouraging me through the past five years. Thank you for reading through my thesis and giving me valuable feedback, insights and a second point of view. Mom, Dad and Helleik, thank you for having the ability to withstand me leaving my computer and research material all over the house the past couple of months. You will get your house back now.

And last but definitely not least, I would like to thank my amazing friends for making my time at NTNU be five of the best years of my life. There have been challenges, opportunities and adventures, tears and laughter. Even our late nights of stressful exam preparations at have now turned into funny and long lasting memories. Thank you!

Hanne Malmin Bruleite
Trondheim, June 2020

Contents

List of Figures

List of Tables

Acronyms

5G 5th Generation Cellular Network Technology.

ACA Admission Control Algorithm.

ACK Acknowledgement.

ACL Access Control List.

AP Access Point.

AR Augmented Reality.

ARQ Automatic Repeat Request.

BLER Block Error Rate.

BS Base Station.

CAC Call Admission Control.

CE Customer Edge.

CH Cluster Head.

CIA Confidentiality, Integrity, Availability.

CPS Cyber-Physical System.

CPU Central Processing Unit.

DDoS Distributed Denial-of-Service.

DNS Domain Name System.

DoS Denial-of-Service.

DSB Norwegian Directorate for Civil Protection.

E2E End-to-end.

EDF Earliest Deadline First.

EHF Extremely-High Frequency.

eMBB enhanced Mobile Broadband.

ETSI The European Telecommunications Standards Institute.

FIFO First-In-First-Out.

Gbps Gigabits per second.

GHz Giga Hertz.

GSM Global System for Mobile Communication.

GSMA GSM Association.

HD High-Definition.

HSE Health, Safety and Environment.

iACL Interface Access Control List.

ICMP Internet Control Message Protocol.

ICPS Industrial Cyber-Physical System.

ICS Industrial Control System.

ICT Information and Communication Technology.

IDS Intrusion Detection System.

IEEE Institute of Electrical and Electronics Engineers.

IIoT Industrial IoT.

IoT Internet of Things.

IPS Intrusion Prevention System.

ISP Internet Service Provider.

LIFO Last-In-First-Out.

LSR Label-Switched Router.

LTE Long Term Evolution.

M2M Machine-to-Machine.

Mbps Megabits per second.

MEC Mobile Edge Computing.

MHz Mega Hertz.

MIMO Multiple-Input Multiple-Output.

mMTC massive Machine-type Communications.

MPLS Multi-Protocol Label Switching.

ms millisecond.

NB-IoT Narrowband-IoT.

NKOM Nasjonal Kommunikasjonsmyndighet.

NSA Non-Standalone.

NSM Nasjonal Sikkerhetsmyndighet.

NTNU Norwegian University of Science and Technology.

OS Operating System.

OT Operational Technology.

PE Provider Edge.

PER Packet Error Rate.

QoS Quality of Service.

RAM Random Access Memory.

RF Radio-Frequencies.

RO Research Objective.

RQ Research Question.

RT Round-Trip.

RTT Round-Trip Time.

SA Standalone.

SCADA Supervisory Control and Data Acquisition.

SDN Software-Defined Networking.

SHF Super-High Frequency.

SP Service Provider.

SYN Synchronize.

Tbps Terabits per second.

TCP Transmission Control Protocol.

UAV Unmanned Aerial Vehicle.

UDP User Datagram Protocol.

UE User Equipment.

UHF Ultra-High Frequency.

URCC Ultra-Reliable Critical Communication.

URL Uniform Resource Locator.

URLLC Ultra-Reliable Low-Latency Communication.

VR Virtual Reality.

WFQ Weighted Fair Queuing.

WSN Wireless Sensor Network.

Glossary

Attack Vector	Different ways to attack a target [42].
Availability	To ensure that the information or system is neither deleted nor disrupted, and avoid denial of use for authorized users [18].
Black Listing	List of entities (i.e hosts or packets) that is not allowed to use the resources in a system [126].
Botnet	Used to carry out Distributed Denial of Service attacks. Devices are infected with malware and operates under an attackers commands and instructions [19].
Bottleneck	The link the data have to go through to reach its destination, that has the smallest transmission rate (throughput) [59].
Cellular Network	A Mobile Network or Mobile Communication Network where the access link is wireless (i.e 3G, 4G or 5G).
Centralized Computing	Traditional cloud computing technique used in IoT networks, where the calculated response do not need to be immediate [3].
Confidentiality	To ensure that information is kept secret and protected from unauthorized users [18].
Control Plane Policing	Policing is a way to control or regulate what type of traffic or data packets that are allowed to enter the system. A Control Plane Policy is protecting the CPU of the network device [5].

Critical Infrastructure (Nor)	Infrastructures, both physical and technical, the society depend on to ensure the populations basic needs. Without them, the society will struggle to maintain its supply of services [94].
Critical Societal Functions (Nor)	Functions that requires critical infrastructure to provide its services for the populations basic needs (i.e banking, health services)[94].
Data Rate	The amount of traffic is estimated by the number of bits per second [59].
Decentralized Computing	Some of the easier computational tasks is moved closer to the devices, to increase speed [34].
Denial of Service (DoS) Attack	A cyberattack where the goal is to block, clogg, reduce speed or in any way obstruct a network component and this way hinder services to be performed as expected. The attack compromises the security of the system by occupying resources and hence hinder its availability [59].
Edge Computing	Cloud computing tasks performed on-site, by the devices. Similar to Fog Computing, but closer to or at the devices/object [26].
Flooding	Inserting excess traffic to a system for instance by sending multiple requests, to overwhelm the links or system resources [59].
Fog Computing	Cloud Computing tasks calculated closer to the edge of the network, for instance co-located with base stations, to increase speed [6].
Integrity	To ensure that information is kept from being modified by unauthorized users and be able to detect if data has been modified [18].
Latency	Time between request and response [37].

Chapter 1
Introduction

1.1 Motivation

The oil and gas industry is one of the six defined critical infrastructures in Norway, and these are vital for providing the basic needs for the population [94]. Most of these critical infrastructures have already transitioned into a partly or fully digital systems, such as for example *smart grids* that is being used to distribute the energy resources according to energy demands. And within the transportation sector, real-time traffic updates for traffic optimization, autonomous vehicles and more, have been introduced. In addition, industrial networks are also emerging. There is a growing desire of being more efficient and to increase production, and process automation has been and is one of the suggested and applied solutions [77].

However, the offshore industry has yet to implement IoT for operation and process related purposes. Since the offshore environment is considered as one of the most dangerous places to work, Industrial IoT (IIoT) could potentially be a suitable solution, to reduce the risk of accidents and explosions by removing people from dangerous situations and from interactions with machinery and pressured oil and gas[45][47]. IIoT could also improve operation monitoring, maintenance and allow for remote control of processes, and hence for instance make the production and maintenance work more efficient[77].

Recently, a new mobile cellular network has been introduced. 5G, is the follow up network technology after 4G, but have new features that enables and allow for more wireless and Internet-connected devices, higher data rates and higher user density than earlier network generations [67][84]. Within IoT, 5G enables wireless, real-time traffic between the network source and destination, because of 5G's support of URLLC[12]. In addition does the closer located Base Stations (BSs) decrease the delay between the end-points as well as improving security by limiting the exposure of data on the wireless link. Real-time traffic opens for several use cases that could be interesting for the offshore industry, among those is motion control of devices

and objects, handheld terminals, Virtual Reality (VR) and Augmented Reality (AR) [120]. But as the location of offshore platforms are quite isolated, is it possible to deploy use cases that require real-time data transmissions in this environment if the traffic is really sensitive to delay?

Security is an other important aspect for those who implements and deploys Internet-connected devices and IoT systems. Within the industry, process automation, autonomous operations, remote monitoring and remote control are examples of use cases that require a lot of sensors, for example at an industrial plant. Many of the sensors are wireless, for example to enable mobility, and these are all connected to the Internet. The end-devices are known to be limited in terms of resources and lacks computation power for encryption [99]. This gives a potential attacker several devices to make use of in a cyberattack. Statistics shows that IoT botnets are being frequently used to carry out Denial-of-Service (DoS) and DDoS attacks, by gathering forces and have the devices overload a specific network component with traffic, to reduce its availability [69][73].

So what happens if time-critical IoT is deployed offshore and then a component becomes a victim of a DDoS attack? Some data packets do have a quite limited timing budget between the source to its destination [37][59]. In several situations the system depends on the packets to arrive at its destination before the total packet delay exceed the absolute maximum delay. For some use cases, a packet that exceeds its maximum delay, can cause catastrophic outcomes as the decision-making or computations that needs to be done are no longer relevant, because the event may already have happened [111]. For instance, in an autonomous vehicle if a message sent from a sensor to a controller is to stop the vehicle because of an obstacle on the road, the message is not acted upon until after the vehicle have crashed into the obstacle, because it was too late to arrive at the destination. As a solution to avoid or mitigate situations like these, traffic policing has been suggested [37][59]. A policing mechanism can for instance be to prioritize traffic depending on various criteria. For instance, if the packet is a time-critical packet, it can be prioritized through a router, to minimize its queuing delay through the network node.

1.2 Research Questions

Assuming that IoT was to be deployed at offshore installations, far from shore. The following research questions (RQ) are defined:

RQ1: Would it be possible to have time-critical applications offshore that is communicating with servers on shore within the required packet delay limit and could traffic policing be a suitable solution to enable this?

RQ2: To what extent does control plane policing mitigate how a DDoS attack impacts the latency of time-critical offshore IoT traffic?

1.2.1 Research Questions and Partial Research Questions

To be able to answer the research question above, some research objectives (RO) are established.

1.2.2 Research Objectives

RO 1: Carry out a literature review on, e.g IoT systems, industrial systems and DDoS attacks, and use this as a basis for adapting known systems to a high level network architecture for an *offshore to onshore* IoT system and suggest what properties the entities should have and give reasons for the proposals.

RO 2: From the literature review, find and describe the most common DoS and DDoS attack that occurs in network systems and tie them to IoT systems. Then suggest some of these that are a potential threat to an IoT network when deployed in rural offshore locations based on the findings in published literature.

RO 3: Based on the findings in RO1 and RO2, choose a specific component of the system and show, by performing simulations of data traffic, the changes that occurs during an DDoS attack. Implement traffic policing mechanism(s) to see how this affect the data traffic delay and especially concerning traffic from and to time-critical applications.

RO 4: Use the results from the qualitative analysis and simulations and discuss if it is possible to deploy time-critical IoT offshore with special regards to how distances affect the packets End-to-end (E2E) latency.

1.3 Structure of Thesis

Following this chapter, the structure of the thesis is as follows:

Chapter 2 and **Chapter 3** holds background information and related work within the field of IoT and IIoT, DoS and DDoS attacks, current status on IoT in the offshore industry and some techniques that can be used to mitigate DoS and DDoS attacks.

Chapter 4 provides an overview of methods and techniques that are going to be used to answer the research questions and to carry out the objectives.

Chapter 5 is a qualitative analysis based on the literature review carried out in Chapter 3.

Chapter 6 holds information about and descriptions of the simulation model.

Chapter 7 that holds the results from the simulations.

Chapter 8 contains a discussion of findings done in Chapter 5 with the results of the simulations from Chapter 7.

Chapter 9 holds the findings and conclusion from the analysis and simulations carried out in earlier chapters.

Chapter 2
Background

2.1 The Offshore Industry

The offshore industry includes several internal and external human resources both in onshore offices and on offshore installations. The offshore installations are usually located between 64km and 300km from shore [47] encircled by troubled water, making the environment quite isolated in terms of everything, compared to the office buildings located in the cities or onshore. Consequently, in case of emergencies help can be far away. In addition to rural locations, the weather conditions can be harsh and in many cases hinder or postpone rescue operations with helicopters and vessels.

Working on an offshore facility is considered to be of high risk [45]. The offshore industry have a rather dark history of accidents and some of them with fatal outcomes. Unfortunately, accidents and injuries are occurring sporadically, for instance caused by explosions, uncontrolled deck operations or by human interaction directly with heavy operational equipment. High pressured oil and gas are severely explosive materials and extremely flammable [47]. Because of the occasional fires, explosions and other accidents during operation and production a major priority in this industry is Health, Safety and Environment (HSE), working towards reducing undesirable events. As a safety measure, there are also laws, regulations and standards such as a 500m safety zone surrounding each installation is established to avoid other vessels and supply ships colliding with the installation and furthermore causing major accidents [101].

2.2 Critical Infrastructure

Oil and gas is vital for production of fuel for transportation for generating electricity and energy. The industry is very important for Norway's revenue, due to the high export to other countries, which is giving high contribution to the Norwegian society to provide the basic needs for the population. Oil and gas is defined as one of the critical infrastructures in Norway. The definition of critical infrastructure states

that if one of the infrastructures fail, it will not be possible to maintain services and provide the basic needs that the society depends on [94]. Based on that it can be reasonable to assume that if Norway was subject of being attacked, an attack on one of the critical infrastructures, could harm Norway and the Norwegian population severely either economically, materialistically and/or by affecting society's basic needs, because of inter-dependencies between the different infrastructures [94]. The six critical infrastructures that are defined for Norway, are listed below;

1. Electric Power
2. Transportation
3. Communication Network
4. Satellite Communication
5. Water Supply and Wastewater
6. Oil and Gas

These infrastructures are not only susceptible to physical attacks. Cyberattacks can also be a challenge to critical infrastructures. An increasing amount of devices such as smartphones, alarms and sensors are being used and implemented *everywhere*. Such devices are expanding the cyberattack surface as they all are inter-connected through the Internet, and are relatively easy to access [99].

2.3 Internet of Things & Time-Critical Systems

IoT is a term used to describe several interconnected devices that forms a network and shares information between them [3][132].

2.3.1 Internet of Things Architecture

The IoT architecture is broadly presented in three layers which are the perception layer, the network layer and the application layer [68][77]. Figure 2.1 shows an illustration of the three IoT layers. In the perception layer, sensors, actuators and other simple devices (in terms of restrictions on Central Processing Unit (CPU) power, battery capacity and memory) are placed in the field and used to record and extract information from the environment [77]. Such information could for instance be sounds, temperatures, gas leakages or pollution levels. The collected information is transmitted over a wireless communication channel to the gateway and into the network layer. The wireless communication channel can for instance be a cellular network, where the cellular BS will act as a gateway. The gateway transmit the data

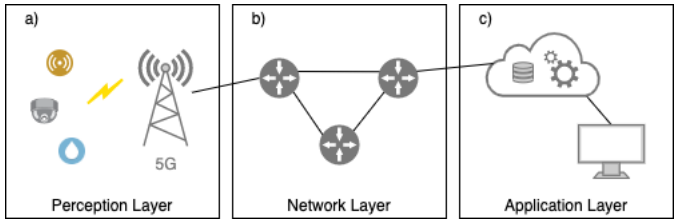

Figure 2.1: IoT Architecture

into the network, where the data is routed to its remote destination. The data is computed and stored on cloud servers, and can then be accessed by the user through smart devices. This is known as the application layer, and is where the information is presented to the user, so that the user can used the collected information to make decisions and to monitor the environment [68][132].

2.3.2 Industrial IoT & Cyber-Physical Systems

In recent years, IoT have been deployed at industrial sites to help with surveillance, computations, decision making and monitoring of physical processes. A system like this is known as a Cyber-Physical System (CPS) as it consists of both physical processes and digital computations in joint action [66]. The systems are connected to the enterprise network and over the Internet which also uses commercial IoT cloud computing services [99]. This means that on-site physical processes can be accessed over the Internet. In the industry sector this is often also referred to as IIoT [41].

IIoT provides flexibility for industrial system management and increased productivity and efficiency due to intelligent business management [99]. However, this also exposes the IIoT networks to several new security threats as these field devices and the CPSs and Industrial Control Systems (ICSs) are more exposed to the public [41][99]. The greater challenge occurs when CPSs are being used for a variety of critical services [66]. A cyberattack on such processes and critical services can cause major economic and materialistic consequences. In addition, even loss of life [54].

2.3.3 Real-Time & Time-Critical Systems

Some systems or applications are said to be safety-critical while others are mission-critical. A safety-critical system is defined as a system *"[...]whose failure could result in loss of life, significant property damage or damage to the environment"* [54]. This could for instance be a IoT system used to detect leakage on, or emissions from, an offshore installation. Whereas a mission-critical system would be a component failure or a gas leakage that causes an explosion which impacts the oil and gas production and hence affect the business significantly economically and materialistically [75].

Some services might also be categorized as both mission-critical and safety-critical, for example an autonomous vehicle that could cause loss of life and a lot of materialistic damage in case of component failure in real life traffic.

If mission-critical or safety-critical systems are to be autonomous or remotely operated, used and monitored, the response time of the system will be important. Industrial control systems, autonomous vehicles and Unmanned Aerial Vehicles (UAVs) are examples of systems that are time-critical. Such systems need to make immediate decisions, respond instantly and implement actions based on feedback from the environment in a short amount of time. Therefore, systems like these are known as real-time systems. The "degree of real-time" however, will depend on what is crucial for that exact system [123]. A system can be classified based on its real-time deadline demands, and the following categories are defined [111];

- **Hard:** If deadline is not met, the outcome can be catastrophic, and tasks and results are no longer useful.
- **Firm:** If deadline is not met, the consequences are not severe and results can still be useful.
- **Soft:** If deadline is not met, the results can be useful, but will not be as relevant over time.

Further, it is described that there are three main components that defines a real-time system [111]. These are time, system reliability and the environment of where the system operates. Time is important because of the established system deadlines, but logical correctness of tasks and computations done within that time period is just as important for the system reliability, which is the second of the three components. A real-time system failure can cause disasters, hence the system needs to be both reliable and available whenever it is needed. And, for the third component, it is necessary to evaluate the system in the environment with all the necessary actors, otherwise it will be meaningless [111].

2.3.4 Status: IoT & Real-Time Systems in the Offshore Industry

Currently, offshore processes and operations are being monitored from remote locations using cameras and video calls only. People are still working with dangerous equipment and machinery in rough weather conditions at locations far from shore. The offshore safety regulations are strict, but important to help mitigate accidents, injuries, explosions, fires and fatal outcomes among others [45][47]. Having said that, this industry could make use of IoT to improve their safety regulations and mitigate such undesirable events. By introducing "things" such as computers, sensors and

other automated tools which can communicate Machine-to-Machine (M2M) and be controlled from a distance, the workers direct interaction with physical processes and machinery could be reduced or even fully replaced [17]. In addition, the costs of using helicopters to transport industry experts to the offshore installations for maintenance could be reduced by using UAVs. An UAV, or drone, can be used for real-time video-inspections having the industry expert staying at the remote onshore office while performing the necessary check-ups. This could potentially also be more time efficient and less dangerous than using the current solutions.

2.4 5G & Ultra-Reliable Low-Latency Communication

2.4.1 5G - The New Mobile Cellular Network

The emerging new mobile cellular network, the 5th Generation Cellular Network Technology (5G), is bringing additional features to the table. In terms of speed, it will be possible to download a High-Definition (HD) movie in less than a second with 5G, compared to around ten minutes using Long Term Evolution (LTE) or 4G[84]. It is also expected that the E2E delay in 5G to be less than a millisecond (ms), compared to 70ms in the current 4G network [84].With regards to the IoT development, 5G is allowing for three new main use cases. The deployment of 5G will allow for IoT devices to communicate among each other without human interaction and support higher user density, known as massive Machine-type Communications (mMTC). It will also accept more devices to connect to the network and be able to handle more traffic, known as enhanced Mobile Broadband (eMBB) [1][139]. In addition, several new, smaller BS cells will decrease the distance between the IoT device and the BSs making the signal travel over shorter distances than what was necessary in previous versions of mobile cellular networks [50]. Shorter distances as well as higher signal frequencies are making the signal speed even faster. 5G is also said to support URLLC, which is a requirement for several future real-time applications [67][138].

The deployment of 5G is set to happen in two rounds. Firstly, the radio access is renewed in what is known as 5G Non-Standalone (NSA). Here, the network core is the same as for 4G. This deployment will only support eMBB use cases [122]. However, the second deployment of 5G, known as 5G Standalone (SA), will be enabling all the 5G features. This deployment have its own core and is not based on the old 4G network. Therefore 5G SA will provide a full 5G experience and include all the new features.

To be able to allow for an increased amount of devices that need wireless connections and following meet the increasing data capacity requirements, it is necessary to allocate additional Radio-Frequencies (RF) for 5G. Traditionally, the Ultra-High

Frequency (UHF) band, 300MHz-3GHz, have been used for mobile communication (2G to 4G) as it contains frequencies that provide great coverage and object penetration capabilities. But with 5G, it is necessary to enable even more frequencies and especially those greater than 1GHz because of its larger bandwidths [2]. For the 5G NSA edition, frequencies up to 26GHz will be enabled to allow for eMBB use cases. However, for the 5G SA edition, frequency bands between 40GHz and 71GHz will be enabled [2]. Signals (also known as mmWaves) on these frequencies do not penetrate objects easily because of shorter wavelengths and cannot travel far. This requires new BSs placed closer to the cellular devices and introduces the concepts of small cells [2][50][84].

With the increasing device density and data traffic, deploying small cells, see Table 2.1, like femtocells, picocells and microcells instead of macrocells (used in 4G). By using small cells it is possible to provide both faster connectivity, reduce signal-dropping and enhance battery duration of the already resource-constrained IoT devices [50]. This is because less battery power is needed to transmit signals over short distances. In addition, the 5G BSs will be equipped with technologies like full duplex, massive Multiple-Input Multiple-Output (MIMO) and beam-forming [84]. Massive MIMO, describes a system that enhance the BSs capabilities, allowing them to send and receive data on multiple ports at once because of an increased amount of antennas per BS. The full duplex technology makes it possible to receive and send data simultaneously on the same frequency, hence increasing the network capacity and lowering the latency between the device and the BS. Especially helpful for mmWaves, the beam-forming technology can help reduce signal interference by directing the signal to a specific user. Beam-forming is also helpful with finding the most efficient signal route [84].

Instead of using dedicated networks for different use cases, 5G network slicing will enable the use of virtual networks on one physical infrastructure, which is more cost efficient [121]. Each slice can be customized and tailored to the requirements of specific use cases [139] [121]. In other words, one slice could be tailored for IoT and mMTC use cases, one for eMBB use cases and one for URLLC or time-critical use cases. Each of the slices are isolated logically and can be prioritized [51]. They can also provide the use case specific network capabilities simultaneously [139].

2.4.2 URLLC - Ultra-Reliable Low-Latency Communication

URLLC is necessary within the industry for industrial automation and industrial control and is vital for industry automation, industrial machinery, early warning sensors, smart factories and virtual reality for instance [86]. For industrial automation the use cases can be divided into three categories; time-critical processes, non-time-critical processes and digital communication within the company [12]. Use cases such

Base Station Types	Number of Users	Coverage (km)
Femtocell	1-30	0.01-0.1
Picocell	30-100	0.1-0.2
Microcell	100-2000	1-2
Macrocell	>2000	5-32

Table 2.1: Base Station Types (from Texas Instruments [50])

as machine-vision video, motion control of robots and virtual reality with real-time data analytics are examples of time-critical processes that requires high reliability and extremely low latency. For non-time-critical processes use cases can be sensor data for environment and field monitoring and remote inspections of the facilities for instance [12]. Non-time-critical processes are examples of processes that are necessary for the industrial operations but do not have as strict requirements with regards to time. However, non-time-critical processes are producing a lot of data that are to be transmitted through the network for data analytics and to produce production insights [83].

It is possible to obtain URLLC using 5G SA as well as co-locating fog computing capabilities, or Mobile Edge Computing (MEC), with the 5G BSs [6]. Instead of using "traditional" centralized cloud computing, it is more time efficient moving some computations closer to the edge of the network [3][83]. This use of fog nodes reduce the amount of data on the transport network and makes data transmissions even faster [34] as well as reducing the distance the data has to travel before being calculated. This allows for lower latency and open for M2M time-critical communication, that is, decisions that is to be made without human interaction in a short period of time. Autonomous decision making also improves the reliability of the system as the computations are more likely to be logically correct within a timely manner compared to decision making done by humans, as we are more easily affected by other impulses [61]. By using decentralized computing, it is possible to do computations faster than before and hence reducing latency [17]. As the operational data is less exposed on the network links and not leaving the area where the data is gathered, decentralised computing is more secure than using centralized cloud computing [12].

Many of the latency, availability and reliability requirements can be met by LTE with a Block Error Rate (BLER) (or Packet Error Rate (PER)) equal to 10^{-1} and WiFi [12][17]. However, LTE and WiFi cannot meet the ultra high reliability requirements for URLLC use cases which only can be provided by 5G. In general, URLLC applications that requires high reliability, usually needs a BLER less than 10^{-5} [88]. For high reliability industrial automation and control applications it is stated that a BLER of 10^{-9} is required in most cases [17]. For real-time applications,

Use Case	E2E Latency	Reliability (BLER)	Reference
Remote Surgery	$<$ 1ms	Down to 10^{-9}	[17][89]
Automated Driving	$<$ 5-10ms	Down to 10^{-6}	[17][86]
Factory Automation	$<$ 2.5ms	Down to 10^{-9}	[17][89][137]
Virtual Reality (VR/AR)	$<$ 5ms	Down to 10^{-5}	[27][86]
Industry Control	$<$ 1ms	Down to 10^{-9}	[86][17]
Remote Robotics	$<$ 1ms	Down to 10^{-9}	[86]
Motion Control	$<$ 1ms	Down to 10^{-5}	[89]
mMTC (Non-time-critical)	$<$ 5ms	Down to 10^{-1}	[88][89]
Applications (Ctrl. to ctrl.)	$<$ 4ms	Down to 10^{-8}	[137]
eMBB (Non-time-critical)	$<$ 40ms	Down to 10^{-3}	[88][89]

Table 2.2: Latency and Reliability Requirements for Some Use Cases

or Ultra-Reliable Critical Communication (URCC) it is important that the feedback or reaction is immediate. On average, a persons reaction time is between 0.15-0.22 seconds, which includes to sense, understand, evaluate, decide and take action [116]. The E2E latency for time-critical systems needs to at least mimic human response time and preferably be as fast as less than 1ms [139]. Some URLLC use cases and its associated latency and reliability requirements can be seen in Table 2.2.

2.5 Core Security for IoT

Within cybersecurity there are established three main security objectives that needs to be achieved for the information and/or system to be considered secure. These objectives are known as the CIA-triad and consists of the three concepts Confidentiality, Integrity and Availability [18][100][130].The following protection goals applies for both information security and system security [18]:

- **Confidentiality:** To ensure that information is kept secret and protected from unauthorized users.
- **Integrity:** To ensure that information is kept from being modified by unauthorized users and be able to detect if data has been modified.
- **Availability:** To ensure that the information or system is neither deleted nor disrupted, and avoid denial of use for authorized users.

Ensuring high system availability is essential in time-critical IoT systems. The system and/or the information needs to be available and working undisrupted when it is

needed to keep the critical service persistent [86]. In addition to high availability, high reliability and low latency are also requirements for such services [86].

Ensuring confidentiality for real-time applications and services can be challenging, as the IoT devices are so simple and limited in terms of resources that they struggle with handling heavy encryption schemes [4][83]. It is also known that encryption do require some extra time for computations, meaning that for time-critical IoT services there is a trade-off between security and latency [4][26]. However, changing from centralized cloud computing to decentralized fog and edge computing allows for time-critical decisions to be made on-site, close to where the data is gathered, which reduce latency. This is also said to increase security as the information exposure in the network is reduced [34].

2.6 Time Budget of Packets

Each data packet has a time budget. From when the packets is sent from the source until it arrives at the destination, the packet will be affected by some kind of delay. The total delay of a packet depends on how many network components the packet needs to go through, as well as the medium it uses from point A to B, among others [40][59]. The number of physical mediums it goes through, the number of network nodes and their individual delays will sum up to be the total packet delay [59]:

$$Packet_{Delay} = \sum_{0}^{\infty}(Processing_{Delay} + Queuing_{Delay} + Transmission_{Delay}) + \sum_{0}^{\infty} Propagation_{Delay}$$

Some packets are more delay-sensitive than others. If the delay of a packet for any reason should exceed the maximal amount of delay it can handle it may no longer be useful, as mentioned in subsection 2.3.3. If the system in any way should be to busy with handling traffic, the availability of the system is reduced and the delay of the packets would potentially increase [86].

2.7 Denial of Service & Distributed Denial of Service

2.7.1 Denial of Service Attack

Denial of Service is a term used within communication technology and cybersecurity to describe several security threats. Such security threats will affect the service that is being provided by the system and its network components if acted upon by an

adversary. In other words, the service is overwhelmed and made unavailable and unusable for users that depend on having the system working [59]. One common way of doing this is to occupy and clog the transmission links, hindering important packets to arrive at its destination at the right time, by sending extra unnecessary data into the links [59]. A DoS attack do not necessarily mean that the information is accessed by the attackers directly [73].

In some cases the DoS attack is caused unintentionally, for instance by an configuration error or signals that interfere. This can cause the system to act the same way as it would under an attack, but this is not done to cause harm in any way. However, this can be done intentionally as well, meaning that someone is trying to obstruct and block the services on purpose. This is usually motivated by causing damage for instance economically, materialistically or as a form of "hacktivism" [19].

2.7.2 Distributed Denial of Service Attack

Norton US stated once that *"A DDoS attack is one of the most powerful weapons on the internet"* [129][22]. A DDoS attack is a more severe and intense version of a DoS attack as these attacks have multiple participating nodes and therefore can generate more data. In a DDoS attack there is one attacker, several compromised nodes like computers controlling several agent nodes that generate a lot of data and direct it towards the DDoS victim [33]. In other words, an attacker have compromised several computers and generated a botnet, where each of the compromised computers acts just as they are told by the attacker. This way, the attacker is able to generate a higher data rate than by using one single source as in a DoS attack [59] and hence easier obliterate the system [19]. In the following sections DDoS will be used to cover both DoS and DDoS attacks, unless otherwise is specified.

2.7.3 Statistics

In Norway, Nasjonal Sikkerhetsmyndighet (NSM) registered about 16000 cyberattacks in 2015, whereof only 1% was within the category of DDoS attacks [73], that is around 160 DDoS in total. However, the amount of DDoS attacks have grown quite a lot since 2015. Telenor reported a total of 3825 DDoS attacks in 2019 only affecting their organization [69]. In 2018 Telenor reported a total of 3721 such attacks [69]. Telenor also informs that the attacks are more intense and have a shorter duration than before. In 2018, the most intense attack lasted for 60 minutes and had a data transfer rate of 101 Gigabits per second (Gbps). In 2019 the numbers where changed to 18 minutes and 257 Gbps!

The number of DDoS attacks have increased with 16% from 2017 to 2018 [22] and according to Telenor and Cisco Visual Networking Index, global estimates indicates that the number of DDoS attacks will reach 14.5 millions within 2022 [69]. The trends

also shows that the attacks nowadays are more intense but shorter in duration[22]. Europe experienced an increased attack volume of 192% from 2017 to 2018 [22], which shows the same trend as the data volume reported by Telenor [69].

Statistisk Sentralbyrå (SSB) [106] states that *Statlige virksomheter*, *kommuner* and *fylkeskommuner* experienced respectively 14.7%, 11.3% and 62.5% of the registered security challenges to be in the category of DDoS in 2018. New numbers from 2019 are similar to the numbers from 2018, with 10% and 12% in *Statlige virksomheter* and *kommuner* respectively (as of 28.06.2020 the numbers for *fylkeskommuner* is not yet updated).

Considering the kind of damage that are caused by DDoS attacks, confidence loss in the business or service are estimated as the worst outcome [22][73]. But there will in many cases also be materialistically and economical damage, because of damaged components and cost of not having the service working as it should and hence missing service income.

Chapter 3
Related Work

3.1 Attack Classifications

DoS and DDoS attacks are classified in different ways. Some are classified based on how they act, that is, what kind of ways they obliterate, obstruct or hinder the service and how intense they are. Others are classified based on protocol stack layers, whether or not they make the system crash or whether or not they origin from the inside or the outside of the organization. In this section, DoS attacks will be presented, classified and described based on earlier research, to get an overview of the various types of such attacks.

3.1.1 Classifications & Types of DoS Attacks

Gavric *et.al* [33] address a part of the most common DoS attacks and how they can be mitigated. The paper focuses on attacks in Wireless Sensor Networks (WSNs) and sort them by protocol stack layers, see Table 3.1 for attack descriptions and where in the stack they occur. The DoS attacks that are referred to in this article, are all described in the terms of a WSN, however, as a WSN is a IoT perception layer network, most of the attacks are relevant to IoT networks as well.

Buch *et.al* [14] also categorize the attacks based on the protocol stack layers, just like Gavric *et.al* [33]. But in addition they add some attacks to the Link layer, Network layer, Transport layer and Application layer. The additional attacks can be seen in Table 3.2. Buch *et.al* [14] also describes that DoS attacks can be classified based on how much or what kind of destruction and damage they cause. The categories can be seen in the following list:

- Resource Consumption
- Data and Information Deletion or Alteration
- State Information Disruption

- Physical Destruction of devices
- Obstruction of communication links

In contrast to the five categories mentioned by Buch *et.al* [14], Kurose *et.al* [59] operates with three types of categories attacks. Kurose *et.al* [59] categorizes the attacks based on where the attack occurs, but also partly on what kind of damage they cause. The categories presented are listed and described below:

- Bandwidth Flooding Attacks
- Connection Flooding Attacks
- Vulnerability Attacks

A DoS *Bandwidth Flooding Attack* occurs when the link between the communicating parties is clogged with excessive packets and hence occupying the link. This clogging prevents the legitimate packets, that are needed for communication, to reach the host. Consequently the service will be fully or partially unavailable [59]. In some cases the link can handle large data rates. To cause damage, a single source is not necessarily enough to generate traffic to match or exceed the rate alone. The attacker may make use of several sources to generate the necessary traffic. In this case the Bandwidth Flooding Attack is considered a DDoS Attack [59]. The connections at the target host can also be prone to a *Connection Flooding Attack*. In a DoS Connection Flooding Attack, the attacker establish several Transmission Control Protocol (TCP) connections to the target which is overwhelmed with all the connections and hence deny real connections to be established [59].

The other type of DoS attack is the *Crashing Attack* in which the Operating System (OS) or application running on the target host is attacked, also known as *vulnerability attacks*[59], and consequently crash. Because of vulnerabilities that exists on the application layer the target host can crash or be hindered in providing the services it is supposed to. It is also possible that the attacker exploit vulnerabilities in applications by transmitting malware to make the system crash and hence causing unavailability [128].

Shahzad *et.al* [107] categorize DoS attacks as *active attacks*, that are performed successively after a *passive attack* such as data traffic analysis. An active attack is described as an attach where it occurs intentional modifications and changes to the data or the data stream by adding extra data or repeating old messages. Shahzad *et.al* [107] especially points out that attacks of this kind usually is performed by adding extra traffic on the communication links or overloading and overwhelming

the system with requests. This is the same as Kurose *et.al* calls bandwidth attack and potentially crashing attacks if the whole system goes down. It is also addressed, by Shahzad *et.al* [107], that WSNs are prone to be a victim of DoS attacks as the devices are pretty simple with regards to features [107].

Kavitha *et.al* [53] specifies that it can be interesting to look at whether the attack originates from inside the network or from the outside. Buch *et.al* [14] defines an insider attack to be whenever a node within the network is occupied and turned into a slave in the network. The behavior of the node changes to what also Kavitha *et.al* [53] describes to be a node with an unintended or abnormal behaviour. An outsider attack is opposite of an insider attack, and is performed by a third party outside the network that is attacked [14]. However, neither of the two sources states exactly which DoS attacks that can be considered as outsider attacks nor which can be considered as insider attacks.

All of the DoS attacks that are mentioned in the sources from this section, are listed and described in the two tables, 3.1 and 3.2 (*N/A* in the tables means that there are no additional attacks to the previous table).

Layer	Attack	Description
Physical	Jamming	Transmitting additional data into the network at time intervals where activity is detected.
	Interference	Radio waves and signals are generated to disturb network functionality.
	Node Tampering and Destruction	Attacker have physical access to nodes and can change information or disable functionality.
Link	Collision	Attacker sends data at the same time and on the same frequency as legitimate network nodes to obstruct traffic from reaching its destination.
	Exhaustion	Attacker sends constant collision messages that congests the network channel.
	Unfairness	Obstruction of normal activities because of constant access to channel.
Network	Sybil	Attacker hold a node with several ID's so that traffic can be routed through the malicious node.
	Selective Forwarding	Attacker decides which packets that are to be sent through or which are rejected.
	Sinkhole	All traffic is routed through the malicious node, because it is identified as the most efficient route. Traffic is then rejected.
	Hello Flooding	Broadcasting of hello-messages from attacker where the legitimate nodes answers. The answer-messages are rejected or misused.
	Wormhole	The attacker routes traffic between two malicious nodes, masqueraded as the most attractive route. The attacker however, uses connections with slow speed.
Transport	Flooding	The legitimate nodes are reduced in terms of resources because of the large amounts of connection requests sent by the attacker. (Synchronize (SYN) Flood). Other flooding attack types also exists.
	Desynchronization	Connection requests keeps coming even though connection is already established which makes it desynchronized. This also affect node resources.
Application	Sensor Overload	Attacker try to overwhelm sensors by forwarding excess data to the sink. Both bandwidth and node resources are affected.
	Path Based Attack	Attacker injects data between two nodes to affect the end-to-end connection.

Table 3.1: Protocol Stack Layers and DoS Attacks (Updated Figure from [33])

Layer	Attack	Description
Physical	N/A	N/A
Link	Interrogation	Attacker initiates the handshake using a request-to-send and ignores the clear-to-send response message, keeping the receiver busy.
	Denial of Sleep	Prevent devices of entering a sleeping state.
Network	IP Spoofing	Attacker sending ping-requests to an address, usually using the victim address as source.
	Replaying	Copy a message and sending it several times to its destination.
	Homing	Analysis of traffic to identify important nodes, to block its traffic or the node itself.
	Altering Tables	Change information in routing tables, so that traffic is wrongly transmitted onto other paths.
	Black Holes	A Black hole = malicious node which is dropping packets on a path it is not originally a part of.
	ACK Spoofing	The attacker sends packet ACKs even though the packet did not reach its destination, displaying weak paths as strong.
Transport	N/A	N/A
Application	Deluge	Reprogramming and controlling remote systems by updating the nodes with new code.

Table 3.2: Protocol Stack Layers and DoS Attacks (Updated Figure from [14])

3.1.2 Classifications & Types of DDoS Attacks

Shahzad *et.al* [107] gives an overview of DDoS attacks in WSNs in their survey paper. The categories are listed below and the description of some associated attacks can be found in Table 3.3.

- Volume Based Attacks
- Protocol Based Attacks
- Application Based Attacks

Several similarities can be found between the categories presented by Shahzad textitet.al [107] and the three categories of DoS attacks described by Kurose *et.al* [59] in the previous section. As the main goal with performing *Volume Based Attacks*

is to occupy bandwidth [48], the idea is the same as with DoS *Bandwidth Flooding Attacks*. For *Protocol Based Attacks* the main goal is to occupy and utilize resources direclty [48], similar to a where the attacker occupies the ports. For the *Application Based Attacks* the goal is to crash the web server [48], just as a *Crashing Attack* or *Vulnerability Attack*. These similarities makes sense as DDoS attacks are an extended and more distributed and intense version of a regular DoS attack. This is because there are several nodes that generates data, which increases the volume of data that can be used during the attack. The categories mentioned in the previous section could also potentially be applied to DDoS attacks. This is because of that several of the already explained attacks in Table 3.1 and Table 3.2 are similar to those examples found in Table 3.3.

Voitovych *et.al* [126] classify or group the DDoS attacks based on number of involved devices. *Group DDoS attacks* contains attacks with up to 100 devices and *Massive DDoS attacks* covers attacks with more than 100 devices. This suggestion is based on the protection mechanisms, as it is easier to block group attacks using black listing than to block every device manually in a massive DDoS attack. Another suggestion from Voitovych *et.al* [126] is to classify attacks based on the source device. For instance based on whether or not the attacker use a botnet, if the attack origins from a random computer or if the attack origins from the intruders machine directly or virtual machines. Using geographical position is also suggested as a way to group the attacks. However, Voitovych *et.al* [126] also suggest to categorize attacks based on layers, like for instance Gavric *et.al* [33] suggests for DoS attacks. Voitovych *et.al* also suggests to sort the attacks based on the effect and type of damage, like Buch *et.al* [14] for DoS attacks. The similarities of classification of DoS and DDoS attacks only shows that it is all about the same types of attacks but with a different kind of intensity with regards to volume.

3.2 DDoS Attacks & Future Concerns

The most common DoS and DDoS attacks, from now on referred to as DDoS attacks, are addressed in the papers that is reviewed in this chapter. These attacks can be found in the three tables; Table 3.1, Table 3.2 and Table 3.3. There are also other attacks covered in the papers, as there exists many versions of each attack with different and more describing names as well as some more general names. For instance, "Flooding attacks" as mentioned in Table 3.1 can cover different kinds of flooding attacks, for examlpe Internet Control Message Protocol (ICMP) and UDP flooding as explained in Table 3.3, just depending on how they are classified.

Fang *et.al* [30] states that DDoS attacks are likely to be a huge threat for 5G operators in the upcoming years because of the massive amount of devices that are deployed and used for IoT and communicating over wireless networks. There are also

Category	Attack	Description
Volume Based	ICMP Flooding	Also known as *Ping-flooding*. Several echo-requests are sent to overwhelm the target. [48] [78]
	UDP Flooding	Attacker sends User Datagram Protocol (UDP) packets to random ports at the target device and forces the device to check for applications that will receive UDP packets. If no applications are found, the target host have to return a message to the sender, which will generate excess network traffic. [48][79]
Protocol Based	SYN Flooding	Utilize vulnerabilities in the "three-way handshake" and sends requests (SYN) to establish an TCP connection. The target answers with an Acknowledgement (ACK) and waits for the attacker to respond to the ACK, which he does not and the system keeps waiting. [48]
	Ping of Death	IP packets are split into fragments as they are to big to send as a whole. The total packet size (sum of all fragments) cannot exceed 65 535 bytes. By manipulating the fragments the total size is changed to exceed the allowed size and hence overflows the memory of the target. [48]
	Smurf	The attacker spoof the target device's IP address and sends/broadcasts requests from that IP address (which is the attacker) causing all other network components to answer to this address and hence causing it to be overwhelmed. [49]
Application Based	Zero-day	Exploiting vulnerabilities that exist from day one that is not found by the developers, and hence have not been patched (yet).[48]
	Slowloris	By holding several connections on the target server open, an other server is able to take the target down by sending requests and not finish them. Hence, a lot of ports will be open unnecessarily and denying other connections. [48]

Table 3.3: Categories of DDoS Attacks (Updated Figure from [107])

concerns for the IoT devices as they are lacking solid security mechanisms making them vulnerable for several attacks including DDoS [23].

Frey *et.al* [31] also have concerns for the lack of security mechanisms in the really constrained nodes. Especially in terms of computational power and battery life-time. Frey *et.al* points out that the devices are *"easy victims of resource exhaustion"* [31]. This could for instance be Denial-of-Sleep [14] by keeping the node continuously active on purpose by performing a connection flooding attack, intentionally drain the battery and hence making nodes unavailable or simply by sending to many packets to the target, exceeding what the node can handle in terms of memory and processing capabilities. Buch *et.al* [14] states that the more common ways of performing an DDoS attack is to send a huge amount of requests by performing a connection flooding attack such as Interrogation attacks or SYN Flooding [107], which decrease response time and reduce the efficiency [14].

3.3 Data Traffic

3.3.1 Traffic Policing

Data traffic is routed through the network using the destination address and other information. But in some cases it might be necessary to divide the traffic into separate flows depending on the traffic content, according to Göransson *et.al* [37]. Traffic policing is a term used for an additional set of rules that are used to decide each packets forwarding path, and hence not only relying on the packets destination address alone. Traffic policing will allow the router to treat packets that match a set of rules as a separate data flow. For instance, having policies can help the router recognize whether the packets are email packets or not, and hence separate the email traffic from the rest of the traffic, by following the forwarding rules. Policies are useful in for instance Intrusion Detection Systems (IDSs), as such systems depend on inspecting packets thoroughly to decide whether or not the packet is legitimate and to provide different types of service for different packet flows [37].

Kurose *et.al* [59] states that First-In-First-Out (FIFO) is commonly used for packet transmissions and packet scheduling, meaning that the packet that arrives first, leaves first when the link is available. This can cause some queuing if there are more packets entering the queue than leaving. Kurose *et.al* [59] also wonder what could happen in cases where packets in the queues are delay-sensitive and the buffer overflows, and discuss policies and mechanisms that can help solve the potential issues. Among others they discuss packet-discarding policies, and mechanisms such as Weighted Fair Queuing (WFQ), Leaky Bucket and various combinations of these. In addition they discuss:

- **First-In-First-Out (FIFO):** First packet in is handled first, and this keeps on going for all the packets in the queue/that arrives.
- **Priority Queuing:** If a packet of higher priority is queued behind a packet with lower priority, the packet with highest priority is chosen and the other must wait.
- **Last-In-First-Out (LIFO):** Last packet in is handled first, for instance because of prioritization.

Lemeshko *et.al* [63] states the importance and the recent Quality of Service (QoS) demands that are found in multi-service networks, networks with different traffic types. Each of the traffic types require different kind of resources in terms of speed, capacity and time, among others. In the article by Lemeshko *et.al* they discuss reservation of resources in the network and describes mathematically how protection schemes can help protect network elements to improve and maintain the level QoS with the increasing amount of traffic during fast re-routing. Compared to Göransson *et.al* [37] and Kurose *et.al* [59], Lemeshko *et.al* [63] focus more on how the QoS should be handled with increasing data rates, rather than how and why it is necessary to categorize the traffic into different classes.

Xu *et.al* [133] discuss that Provider Edge (PE) routers in Multi-Protocol Label Switching (MPLS) based networks can store policies that are to be applied to traffic that passes through. They also explains that packets can contain different labels, headers, fields and sections that can be used to categorize the traffic and hence address the same as Göransson *et.al* [37] and Kurose *et.al*[59].

Alwakeel *et.al* [5] propose a Leaky Bucket scheme with the goal of achieving QoS for real-time traffic, and explains that the main idea is to look into the cause of packet delays and losses, and control a potential network congestion using traffic policing as a technique. They have performed simulations to show how traffic policing can be useful.

3.3.2 Control Plane & Data Plane

Inside a router, the control plane handles traffic where the CPU needs to be involved, whereas the data plane handles the forwarding data [103]. The way a router works is that if a packet arrives, and its forwarding destination cannot be found in the forwarding table, the control plane needs to be involved to find rules that can be applied for packets like these. The control plane evaluates the packet and updates the forwarding table for the device to use later for packets that match the previous one. The router handles most of the data in the *Data Plane*, and the *Control Plane*

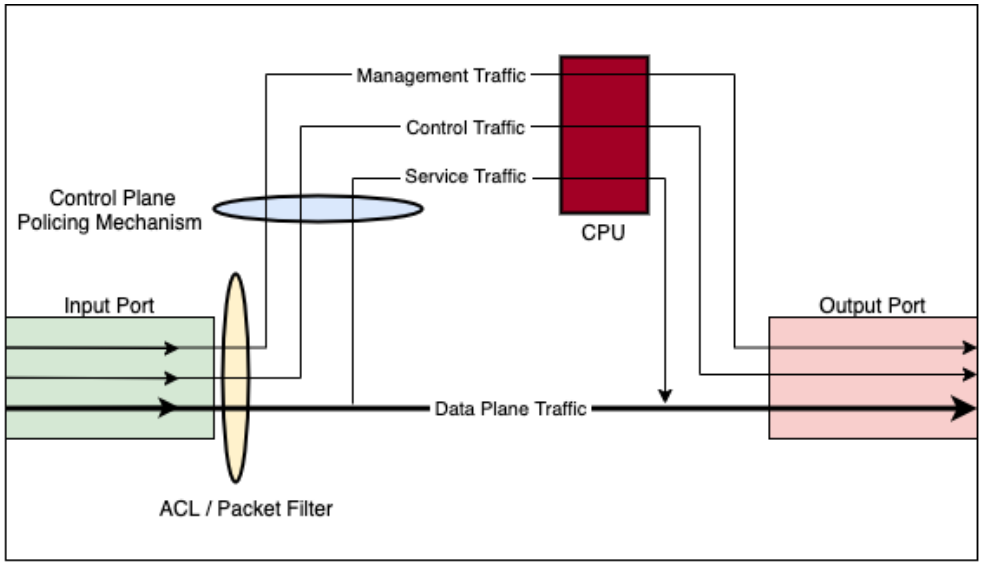

Figure 3.1: Router: Traffic Handling (Modified Fig2, Cisco Website [103])

above handles packets that are not found in the table. Above both of the previously mentioned planes, there is a third plane called the *Management Plane*. This is where administrators of the network can add policies, monitor and configure the the switch, and decide how it should handle different packets [37][59][103].

Interface Access Control List (iACL) is likely to be the first filter all packets go through when entering a network device [103], see Figure 3.1 which shows the packet handling inside a router. If the packet is denied, it is because the list contains information for instance about the source address, and that packets from this source is not to be let through. Otherwise packets are permitted and either forwarded directly to the out port or waits for the switch to ask the control plane to update the forwarding table with a suitable action. A challenge is that if the packet or source is unknown and not in the list, and packets are sent from several spoofed IP addresses, the switch have to make requests to the control plane multiple times and hence use of the already limited CPU resources. If botnet devices are instructed to target the switch with excess requests and packets, an extreme increased traffic rate occurs and the control plane resources are easily overwhelmed, which again will cause the regular updates of forwarding tables for the data plane to be delayed or not even happen at all [103].

Following from this architecture of planes there are some challenges. According to Göransson *et.al* [37], the Round-Trip (RT) latency will increase for the packets where the router have to involve the control plane, as it will wait for instructions on what to do with this packet. Another challenge they address is the *Single Point of Failure* with this topology, therefore they also address that redundancy is important in a system.

3.3.3 Alien Traffic

A DDoS attack can easily overwhelm a switch. Alien traffic is an increased volume of generated irrelevant data or excess data traffic that are routed through the network, like in a DDoS attack. Mousavi *et.al* [76] describes how a DDoS attack can exhaust the resources of a CPU in the control plane and how it can be possible to detect attack or alien traffic. They states that the biggest threat with DDoS attacks, is where the source address is spoofed, which is quite common. This is because packets from such addresses is not to be found in the forwarding tables and cause the control plane to be occupied with the alien traffic and trying to figure out what do do with it. Mousavi *et.al* [76] also points out that if the attack volume is high, most of the resources will be spent on handling alien traffic, rather than processing legitimate packets.

Mohammadi *et.al*[74] explains that the control plane is a bottleneck in the system and can be prone to a exhaustion or saturation attack which originates from a TCP SYN flooding attack, as explained in Table 3.3. The communication between the switch and the control plane is usually over a secure TCP link, and therefore can half-open connections be a challenge [37]. This can occur if the attacker intentionally sends multiple packets with different headers to the switch, forcing the switch to involve the control plane. Compared to the other authors in this section, Mohammadi *et.al*[74] explains the attack in more detail. All in all, they all agree that an attack can overwhelm the device and forcing it to drop packets, meaning that important information will be prevented from reaching its intended destination.

3.3.4 Admission Control Algorithms & Time-Critical Traffic

Chen *et.al* [16], Shakeri *et.al* [108] and Wang *et.al* [127] explains control plane and data plane traffic from a Software-Defined Networking (SDN) device point of view. These papers are used in this thesis to gain some background information on control plane and data plane policing to understand how to and why it is necessary to use prioritisation of data traffic for QoS and protect the CPU and controller as they are potential bottlenecks in the system.

Hurst *et.al* [44] carries out a simulation on how a network of critical infrastructures is affected by a DDoS attack and to calculate cascading failures and its impact in a

city. They describe that one of the main challenges with DDoS is how to identify and block the attack. That is, to allow the good requests through and block the bad traffic. Hurst *et.al* [44] use simulations to look at how a DDoS attack affect the critical telecommunication network infrastructure. Their results show that because of the inter-dependencies between the critical infrastructures some of the critical infrastructures are affected more than the others as they rely on an other critical infrastructures service to carry out their own service.

Lehoczky *et.al* [62] carried out an analysis on head-of-the-queue scheduling algorithms, like Earliest Deadline First (EDF) and FIFO, in networks with time-critical traffic and predicted the percentages of late packets. They use packet arrival rate of 0.05 packets per μs. They conclude saying that it will be necessary to analyse traffic controllers and their Admission Control Algorithm (ACA) and extend their research paper from 1998.

Ginige *et.al* [35] address the challenges with admission control in networks where eMBB and URLLC data are coexisting, as URLLC needs priority due to hard deadlines and eMBB requires high data rates. Ginige *et.al* [35] perform simulations and propose an ACA that makes it possible to make the number of eMBB users in the system as big as possible while ensuring that the URLLC packets are prioritized.

Bashar *et.al* [7] address the same challenge as Ginige *et.al* [35]. They both focus on the QoS demands of different applications, where both regular and high priority data are sharing the resources and categorizes the traffic on these grounds. As Ginige *et.al* [35] prioritize to find the optimal number of eMBB users Bashar *et.al* [7] study how they can maximize how many high priority packets that successfully pass through the system while ensuring QoS. Kumar *et.al* [58] address the same challenge as Bashar *et.al* [7], but evaluates specifically time-critical health-care applications.

Seno *et.al* [105] presents centralized scheduling of time-critical traffic, based on EDF and Automatic Repeat Request (ARQ) in ICS. They consider time-critical transmissions to be performed within its deadlines when the resources are shared among data with other priorities. They address that scheduling mechanisms performed in cycles will struggle in cases where it is being overwhelmed with excess traffic. Seno *et.al* [105] concludes that the mechanisms are more suitable for soft real-time applications, where the time deadlines are not so strict.

Neukirchner *et.al* [81] states that low priority packets should not affect high priority and time-critical traffic when the traffic coexist in a network. The show, using simulations, that admission control is useful in cases where it is necessary to dynamically manage real-time systems where the data have mixed critically.

Simon *et.al* [114] discuss admission control scheduling that admits packets in order

of deadline, or a EDF. They run simulations using this scheduling mechanism on a switching node with three input flows, where one of the flows have tight delay and high throughput demands. Lazzes *et.al* [60] perform a similar QoS study as Bashar *et.al* [7] and use a similar approach as Simon *et.al* [114] by using three traffic flows and evaluate traffic loss of time-critical data.

Kammoun *et.al* [52] focus on maximizing the QoS and the resource allocation with special regards to latency, reliability and availability, quite similar to Bashar *et.al* [7]. Kammoun *et.al* [52] performs simulations, and they are able to show that the simulated algorithm can find the available and most suitable 5G network slice matching the task requirements and hence this way be able to minimize overload of slices. In other words, Kammoun *et.al* [52] focus more on the wireless links of 5G.

Jiangzhou *et.al* [135] evaluates packet forwarding in MPLS. Their aim is to provide QoS and improve the use of resources in the network and they perform simulations in their experiment.

3.3.5 Mitigation of Control Plane DDoS Attacks

Yadav *et.al* [134] states that a DDoS attack on the control plane can harm the entire network. They specifically mentions TCP and UDP flooding as attacks that typically occurs. Further they also specifies that these attacks are hard to detect as they origin from several source devices. Their paper propose a way to mitigate a DDoS attack. Yadav *et.al* [134] propose to use the packet entropy to decide whether or not a port should be blocked. This happens if the calculation of the entropy reaches a threshold in a certain amount of time.

Deepa *et.al* [24] propose a detection mechanism that use machine learning to classify traffic. Their contribution is to combine two algorithms to better the detection rate of alien traffic. Their results shows that the hybrid-algorithm has a higher success rate of detecting malicious traffic (ca. 97%).

Shoeb *et.al* [112] address that increased latency can be caused by a DDoS attack on traffic going to the control plane. In their related work analysis they found that there are several suggested methods, most of them adding a flow monitoring layer between the data and control plane or use priority to eliminate alien packets. Shoeb *et.al* [112] proposes to use a trust list and compare trust values. This way each new host gets a trust value and the packets are prioritized based on this value. Then the packets wait in the buffer waiting for its turn.

Shim *et.al* [110] stated that the attack detection methods used earlier is no longer efficient, as the DDoS attacks usually originates form several sources. They propose

a scheme or filter to detect DDoS attacks by monitoring the destination address and show this by doing simulations.

Hu *et.al* [136] suggests a filtering mechanism that is carried out before the queue policy, to help normal and legitimate packets to reach their destination and to drop and block malicious traffic flows. They look at a couple of algorithms but suggests a filter that is active when the flow exceeds the bandwidth that is available or there are several packet drops from a queue. That is, if the packet arrival rate is too high and reach a threshold value within a time-frame several times. They find that some queuing algorithms have shortcomings with regards to protecting the legitimate traffic but also evaluates their suggested scheme, while under attack, to be suitable for its intended purposes of defending against such attacks.

Ping *et.al* [87] address that IP-spoofing in combination with DDoS attack is a challenge as it is close to impossible to trace and detect the source, hence also hard to block. They suggests a packet scheme where packets are marked by a border router either the first time the packets enter the network or when they arrive from a different domain. By collecting several packets, packet tracebacks can help recreate attack paths. Following, it is possible, based on attack signatures found by the trace, to filter the packets on the marks associated with the attack signature. Their results shows that the filtering mechanism is able to remove approximately 80% of the alien traffic.

Kolahi *et.al* [55] perform a comparison of TCP-flooding attack defense mechanisms, with listed advantages and disadvantages. They cover both Access Control List (ACL) and mechanisms for rate limiting, among others. Their related work analysis shows that there are few studies on how the legitimate throughput is affected by TCP and UDP flooding attacks. However, their results shows that both ACL and rate limiting cause high round-trip-times compared to other mechanisms. But as they evaluated other measures as well, the rate-limiting mechanism is conclusively evaluated to be the best one, as it does not affect the CPU resource as much as other mechanisms.

3.4 Examples of Recent DDoS Attacks

3.4.1 The DNS Flooding Attack on DYN in 2016

In 2016, DYN, a provider of Domain Name System (DNS) servers, became a victim to a huge DDoS attack [42][64]. A DNS server is responsible of connecting and map the Uniform Resource Locator (URL) address to the IP-address of the correct destination [21] and is crucial for the consumers to access their requested webpages. If servers like these are victims to an DDoS attack, the servers will be overwhelmed and hence

be unable to respond to legitimate requests. This will furthermore hinder the users to access the requested service [104]. The attack was a DNS Flooding Attack of where several infected devices were set to send multiple DNS lookup-requests to DYN's DNS servers [104]. This attack is special, as the botnet consisted of IoT devices, such as internet connected alarms and cameras, that where infected by the Mirai malware, and completely under the attackers control. Attacking this kind of communication related infrastructure, makes the Internet services unusable to almost everyone [21]. IoT devices that are included in the botnet are found by scanning the network. And as the IoT devices are known to have weak security mechanisms the authentications are easily breached as many of the devices have default or simple credentials that can easily be found by using brute-force techniques [77]. The newly found devices are then infected with the malware and repeats the scanning process to find new potential devices [113]. The attacker can initiate an attack by telling the commands to the control server which forward these attack instructions to the botnet devices. The devices are then generating the traffic, which in this case were lookup requests directed towards the DNS servers provided by DYN [113].

The DYN attack came in three waves, hit DNS servers on several continents and reached at its best data rates around 1.2 Terabits per second (Tbps) generated by around 100 000 devices that where geographically distributed [42]. Some of the affected websites, that were impossible to reach during the attacks, was The Guardian, CNN, Twitter, Spotify and Netflix [95][131]. Several other sites where also significantly impacted [42][64]. Analysis of the attack shows that both TCP and UDP traffic, that originated from several different source-addresses, were routed to the same port at the targets site [42]. DNS servers uses both TCP and UDP for information exchange depending on the message size. TCP is preferred to UDP if the message size exceeds 512 bytes [109]. UDP communication between a client and a server consists of requests and responses directly. Whereas for TCP, the client will need to establish a connection with the server by sending a SYN-request, of which the server will answer with a SYN-ACK. Before starting the content exchange, the client have to respond on the received SYN-ACK with an ACK. However, if the client do not send the ACK and rather send another SYN, the server will wait until the ACK arrives as well as receiving new SYNs. This will confuse the server and hence occupying its resources [48]. If the client do send the ACK, the messaging between the entities can start. As TCP is a reliable communication protocol, that provides guaranteed message delivery to its destinations, it will re-transmit the packet if there are no response from the receiver when/if the packet arrives [59]. This happened in the 2016 DYN attack. Legitimate requests, mixed with malicious requests and UDP flooding requests, were sent to the DNS. The DNS servers where pretty full on and occupied with all of the traffic generated by the botnet, that they struggled with handling the legitimate packets. And when the DNS servers were unable to handle the traffic, legitimate clients unconsciously also contributed with producing excess

traffic, because of the accumulating retry-traffic [42][109]. All of a sudden, there were several attack vectors; such as malicious nodes sending UDP traffic, malicious nodes sending TCP traffic and retry traffic as well as the legitimate clients that sent legitimate traffic and retry traffic that unfortunately also helped with the congestion [42].

3.4.2 The GitHub Smurf Attack in 2018

In 2018 GitHub [36] was a victim to an DDoS amplification attack also known as smurf attack or reflection attack. According to their incident report [56] the attack peaked at 1.35 Tbps, making it the largest DDoS attack in terms of data volume in the history [20]. The attacker spoofed the IP address of the target, and started sending GET-requests to the memcached servers, which are hosting a widely used database caching system. The memcached servers responds to the spoofed IP address with UDP packets and hence overwhelming the target with excessive traffic.

The memcached caching system is used to reduce the number of requests needed to the external data base by storing the data in the Random Access Memory (RAM) in the servers. This is done to more efficiently access information for websites driven by databases [71]. The reason this attack was possible and successful was that the memcached servers are, in addition to using TCP, also listening on UDP ports. As UDP is a connectionless communication protocol, meaning that there are no preliminary handshake between the client and host or any type of checks [59] it can help to solve potential scalability challenges, especially considering re-connections and memory consumption that occurs with increasing number of servers in combination with TCP [70]. The lack of authentication mechanisms in memcached, do not really help the case either and makes it relatively easy for an attacker to misuse. The attacker could for instance change values in the database or ask for multiple copies in one request. In combination these two could cause a lot of damage, as one request can cause the response to be sent several times over the UDP port in the memcached servers and hence generating a lot of traffic [125].

3.5 What Motivates DDoS Attacks?

3.5.1 DoS Attacks on IoT Systems

There are several known reasons for an adversary to attack IoT systems. Among them, the most obvious one, is that there exists plenty of IoT devices leaving the attackers with several attack surfaces. Everything from web-cameras, kitchen appliances, alarm systems, sensors and tablets are connected to the internet. There is more to come in the upcoming years with the enhancement of the mobile cellular network that supports higher user densities and higher data rates [1][139]. The IoT devices

are known to lack security mechanisms, especially poor authentication mechanism, leaving them easy to attack and vulnerable to be infected with malware and becoming a part of an IoT bot-network [4][83]. Examples of attacks that made use of botnets are the attacks on Imperva in 2016 and an unnamed university in 2017, which are described in the following subsections.

The Leet IoT Botnet in 2016

The Leet IoT Botnet was discovered in late 2016 [90], as an attack, that affected Imperva, peaked at 650 Gbps. The attack consisted of two waves that lasted around 20 minutes each [102][9]. According to Imperva [9], the Leet botnet attack had similarities to the Mirai botnet attack at DYN, but this attack was build to perform SYN attacks in big scale [9]. The attack was a SYN flooding attack, which contained two types of SYN packets (two sizes)[102]. The requests came from spoofed IP-addresses, meaning that the SYN requests were sent to the target, which answered with an SYN-ACK to the spoofed IP-address. The IP-addresses receiving the SYN-ACKs, have not sent any SYN request, and hence do not reply with an ACK, leaving the target on hold with half-open connections and by occupying the resources [9]. The reason for the two packet types, is that the attacker will try to achieve two things; to clog the network and to take overwhelm and take out the switches [102].

The University DDoS Attack in 2017

A university experienced a DDoS attack in 2017, where more than 5000 devices were instructed to perform DNS lookups to intentionally slow down the network speed and make websides inaccessible [90][93]. Each of the devices were, every 15 minutes, instructed to do more than hundred of lookup-requests. The IT staff at the university were not prepared to handle IoT botnets, but they managed to regain control. The botnet spread kind of similar to the botnet created by the Mirai malware [93].

3.5.2 DDoS Attacks on Critical Infrastructures

Recently, there have been several cyberattacks on Critical Infrastructures, harming the electrical power system and the telecommunication networks, among others. If someone performs an attack on a critical infrastructure it will most likely affect several people and cause both materialistic and economical damage as critical infrastructures are necessary for the society to function. Such attacks can be used as leverage to blackmail someone, for instance an authority or a government in a country, to do something and in return avoid that the attacker carries out the attack, and hence spare the population for undesirable events [94]. Examples of such attacks that have been carried out is the Attack on the heating and water system in Finland in 2016 and the attack on the Iranian Telecommunication Network in 2020.

The Cold in Finland Attack in 2016

Buildings in Finland were left in the cold because of a DDoS attack on the hot water and heating control system in 2016 [90]. The shut down occurred because the devices used for the automatic systems services was accessible online and not properly protected with firewalls [95]. The system was flooded with additional traffic and hence overwhelming the system which continuously kept restarting. This caused the system to be inaccessible [57][82]. Only two buildings were affected and it only took a couple of days before it was back to normal [95]. However, the outcome could have been quite different if this attack occurred in mid-winter, had a longer duration or was targeted towards bigger buildings such as hospitals. It is suspected that the attacked devices also were a victim of the Mirai malware or something similar [95].

The Iranian Telecommunication Network Attack in 2020

In February of 2020, the telecommunication sector in Iran was a victim of a DDoS attack that caused connection errors and challenges for a number of regional Internet Service Providers (ISPs). An attack on the telecommunication network is considered as an attack on the country's critical infrastructure and can cause a crisis for everything that requires network connectivity. Luckily, the attack was reduced and eliminated by the Iranian cyber-protection group DEJFA [38].

3.5.3 DDoS Attacks on ICPS

Industrial Cyber-Physical System (ICPS) are widely used to monitor electrical power-grids, energy production and other kinds of industrial operations [32]. Attacks such as the *Cold in Finland* attack in 2016, which was mentioned earlier, is an attack on a control system, and shows that an attack on such systems can cause harm. If attacks on these kinds of systems are successful, they can cause a stop in production, and hence economical loss and damage to physical components and devices. For instance, political conflicts can drive activists into protesting against organizations, companies or operations by carrying out cyberattacks to obstruct the targets ability of performing its intended processes and operations needed to as an example produce energy. This is commonly known as *Hacktivism*, a way to digitally state an opinion and potentially a motivation to attackers. Other types of attackers can for instance be cyber criminals, who are just trying to cause damage, or it can be states and countries trying to harm each other for other political reasons [91].

3.5.4 Attack Mitigation or Detection Strategies

Some known ways of detecting and mitigating DDoS attacks can for instance be by using an traffic policing in the switch to drop packets that are not wanted, as mentioned earlier. In addition to that, Kurose *et.al* [59] and Gavric *et.al* [33] describes

an IDS. An IDS operates by obtaining information and try to identify unknown entities such as an attacker in the network. According to Kurose *et.al* [59] such a system is placed at the edge of the network and inspects the incoming packets and react if the packet is of malicious origin. The system use a database of attack signatures which it uses to compare the incoming packets to. Kurose *et.al* [59] also introduces the Intrusion Prevention System (IPS). Compared to an IDS and IPS can also block packets if the lookup in the database cause it to find a match.

Firewalls are also commonly used in between networks as a security measure [59]. A Firewall have a filtering mechanism that can be used to block certain packet types, packets to a certain address and this way only let approved packets into the network. It is for instance possible to have a list of the only packets that are allowed into the network [18]. whereas Sahu *et.al* [98] suggest a detection strategy that can block or restrain nodes that sends an abnormal and huge amount of packets within known time limit.

Kavitha *et.al* [53] suggest authentication requirements from packets as a mitigation strategy to desynchronization attacks and putting target nodes to sleep are suggested as a mitigation strategy for smurf attacks. They also suggest authentication and encryption to reduce spoofing attacks and rate limiting for exhaustion attacks, just like what was suggested by Sahu *et.al* [98]. However, Kavitha *et.al* [53] also states that these mechanisms can affect the packet delay, hence not making it as ideal for real-time communication.

Chapter 4
Methodology

This thesis consists of two parts. Part one is an analysis of how the offshore environment will be vulnerable to the cyber threats that follows a deployment of 5G and IIoT. This theoretical part will have a special regards to and focus on DDoS attacks. The second part is a simulation of DoS attacks in a router, how policies can be used to prioritize flows as well as looking into how this can affect time-critical communication in offshore IIoT. By doing the analysis and simulations described in the following sections, the research objectives listed in chapter 1 and below, will be accomplished.

RO 1: Carry out a literature review on, e.g IoT systems, industrial systems and DDoS attacks, and use this as a basis for adapting known systems, like the previously mentioned, to a high level network architecture for an *offshore to onshore* IoT system and suggest what properties the entities should have and give reasons for the proposals.

RO 2: From the literature review, find and describe the most common DoS and DDoS attack that occurs in network systems and tie them to IoT systems. Then suggest which of these that are a potential threat to an IoT network when deployed in rural offshore locations based on the findings in published literature.

RO 3: Based on the findings in RO1 and RO2, choose a specific component of the system and show by performing simulations of data traffic the changes that occurs during an DDoS attack. Implement different policies to see how this affect the data traffic throughput and have special regards to traffic from and to time-critical applications.

RO 4: Use the results from the qualitative analysis and simulations and discuss if it is possible to deploy time-critical IoT offshore with special regards to how distances affect the packets E2E latency.

4.1 Part 1: Qualitative Analysis

For the theoretical part of the thesis, the literature reviews found in the previous background and related work chapters will form the basis for a qualitative analysis of a possible offshore IIoT environment and its vulnerabilities.

4.1.1 About the Literature & Origin of Sources

A qualitative analysis is a scientific method used within science and technology. The main idea is to collect textual data, in this case through literature reviews, that can be used to answer the research questions and objectives mentioned above [39]. To answer research questions like these, there is a need for a specific, informative and descriptive context of where and why a phenomenon like a DDoS attack can occur and how they occur [39]. A literature review is a collection of sources within a relevant topic. This can be academic articles, white papers, survey papers and other published works that are specifically chosen from a critical analysis of sources [92] that are suitable to be used to create new knowledge within a new but similar field of study.

The literature review, related work and background will be based on work published by well-known and credible international and national technology organisations, technology companies and security companies to ensure that the logical reasoning, deductions and findings are correct and can be justified. Organisations such as Institute of Electrical and Electronics Engineers (IEEE), The European Telecommunications Standards Institute (ETSI), Nasjonal Kommunikasjonsmyndighet (NKOM) and ISPs such as Telenor, Telia and Tampnet. Most of the more heavily weighing sources are supported, provided or made in collaboration with the IEEE. These are chosen as they can provide different types of reliable and reasonable information and also a variation in points of view. In addition, information is also found in academic papers from different universities around the world that are working with these topics. These are included to add more resent and active research and other relevant information.

Throughout the textual data gathering, it has also been important to choose works that are of recent origin. Meaning that articles and papers written and published between 2018-2020 have been weighing more when evaluating the sources and finding information for the analysis. The reason being that there are so many changes going on within the field of technology. The technology is rapidly changing our environment and is implemented almost everywhere. To keep up with the evolution, the expansions, changes, new inventions and use cases the information needs to be up to date and modern. Technology and ideas that was proposed around 10 years ago might in many cases contain data and analysis that is outdated or soon to be outdated. By using more recently published works, it can give a better insight in trends and relevant challenges and solutions. The distribution of the sources year

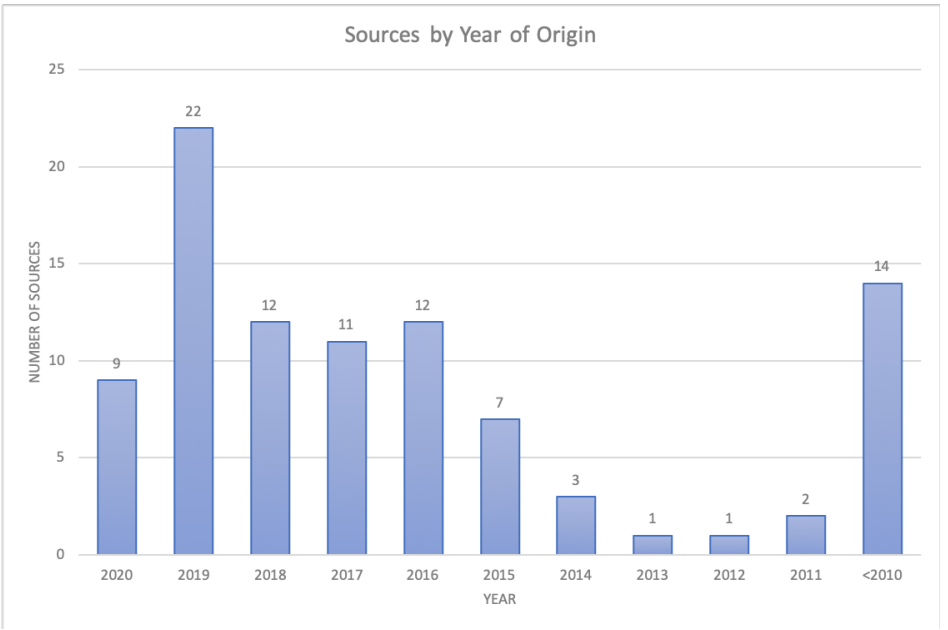

Figure 4.1: Number of sources used in the analysis by year of origin.

of origin can be seen in the diagram in Figure 4.1. However, it can be seen that several of the references are published before 2017. These sources are mostly used for definitions and as a foundation for the background and related work, hence why also listed here.

A qualitative research approach is chosen to be more suitable for this part of the thesis, as a lot of information needs to be gathered to provide and establish a more solid foundation for the following simulations. Gqibani *et.al* [39], published by IEEE, states that *"[...] a qualitative research approach would be better suited to investigating the research problem than a quantitative approach [...]"*. By doing a qualitative kind of research beforehand it can potentially help providing a more reasonable and logical description of the situation and guide the deduction of the results in an appropriate direction. This will also be easier for the reader to follow. In contrast to qualitative analysis quantitative analysis is focusing more on statistics and numbers [39]. As for this part of the thesis, there are only some statistics mentioned in the background information to give a perspective of how relevant the knowledge and results provided in this thesis is and to define what is determined as time-critical in terms of speed and data rates. This is not as relevant for the context, but potentially more interesting for the second part of the thesis.

There are different ways of performing an contextual analysis. For instance, informa-

tion gathering can be done through more direct observations, through interviews with people and experts in the industry or by using specific frameworks for for instance risk and vulnerability assessments. To start the information collecting by doing interviews would be less efficient and close to irrelevant as the interviews would have to cover a too widespread topic. Direct observations of systems and environment, especially on the offshore installations, is a bit challenging with regards to logistics. As this thesis covers a broad topic, a literature review seemed more manageable and useful to be able to grasp over a bigger amount of information before narrowing it down to a discussion and a simulation model in part 2.

4.1.2 Possible Uncertainties

Possible uncertainties with using the chosen sources and this kind of information, especially information that originates from telecommunication companies and ISPs is that there can be a touch of direct or indirect advertising. ISPs could present themselves and try to indicate that their solutions and products are to be preferred to others, to get customers and to make an appearance. There is also always uncertainty in how the authors in the published papers have been interpreting the information they have gathered. On the other side, the organisations that the literature review is based on are well-known and credible within this field of technology, and should be viable for this use. There may also be differences between the degree of development within technology on a national and international basis. The technological progress and information will be depending on what country or region the paper is for and what background it is based on. However, Norway, which is the main country of interest in this thesis, has come quite far in the technological development. Therefore, this should not be a big issue as of now.

4.1.3 Adaption of Knowledge to a new Environment

Through the literature review and background research the idea is to, more precisely, gather data from and about already existing industrial plants, smart cities, critical infrastructures and other IoT environments to compare and look at main concepts and conflicts, known challenges and what kind of DDoS attacks that exists in such systems. From this, the idea is to deduce, adapt and establish an environment or high level architecture that could be relevant for the deployment of IoT and 5G in the offshore industry and on offshore installations. This is to be done to get a better understanding of the potential effects and damage that can be caused by a intentional DDoS attack executed by an adversary, whether or not it is possible to mitigate the damage and all over increase the awareness with regards to cybersecurity. Advantages and disadvantages in, and threats to, different known systems will be used to evaluate how exposed a relatively unknown offshore 5G based IIoT system would be.

4.1.4 Step-by-Step: Qualitative Analysis

The qualitative analysis will be elaborated more thoroughly and be carried out in chapter 5, by following the following steps;

1. Gather and collect information about DoS, DDoS, critical infrastructures, IoT and the offshore industry in general by carrying out a literature review based on information from credible sources.
2. Gain an understanding of the offshore industry's HSE challenges and look at how IoT could be useful.
3. Gain an understanding of how IoT works in smart cities.
4. Gain an understanding of how IoT is used in existing industrial plants.
5. Gather information about critical infrastructures and how IoT can be useful and challenging.
6. Gather information about how a DDoS attack can be used to cause harm and kind of harm it can cause.
7. Use the gathered information to draw parallels to an IIoT system.
8. Change the newly found system to be more distributed and adapt it to an offshore environment.
9. Deduce a tailored distributed IIoT network for the offshore industry and the offshore installations.
10. Look into what kind of DDoS attacks that are more relevant to this "new" system and why.
11. Draw a conclusion on the analysis by asking questions that occurs throughout and have a deeper look into it in part two.

4.2 Part 2: Simulation

A sudden increase of DDoS attack traffic can affect the routers. The time-critical IoT traffic is supposed to be forwarded directly and depends on the routers availability. An attack on the control plane (Figure 3.1) can overwhelm the routers CPU, hence exhausting the device and impact its availability, which then again will cause delays or fully obstruct the time-critical traffic from going through.

Control Plane Policing have been implemented as a suggested solution, but how well does it really work and how does it affect real-time traffic forwarding? How much delay can an offshore IoT packet tolerate before it is no longer useful? Or is it possible to completely block the attack? This will be investigated based on the results from the simulations on a router, with and without policing mechanisms and with different types of packet flows. By inserting a DDoS attack traffic the simulations can show how the excess data traffic affects the delay of the IoT traffic and use the results and compare them to the total time-budget of a time-critical IoT packet.

A simulation is an efficient way of showing real challenges of dynamic systems and how a system will react in different circumstances using simplified models, instead of deploying systems without testing them first [11]. To look at how the router acts during an DDoS attack and by applying policing mechanisms, simulations are suitable as they can give a picture of how the delay of the packets are affected, without being expensive and demanding a lot of time. Simulations are also found to be widely used in research papers for similar purposes in the literature review carried out in chapter 3. Since several of the research papers looked into similar algorithms and policies as well as other packet delay related scenarios, it was found suitable to use the same method in this thesis.

As mentioned earlier every packet have a time-budget, whether it is really strict or not strict at all. The total delay will be the propagation delay, transmission delay, queuing delay and processing delay, where the last three adds up to be the total nodal delay [59]. The propagation delay depends on the distance the signal is to travel and what kind of medium that is being used. The number of network nodes and meters of propagation distance(s) decides the packet's total delay. In addition does time-critical data have hard, firm or soft deadlines, see subsection 2.3.3, that tells to what degree the packet is useful if it arrives too late to its destination. And some use cases have a maximum tolerable delay, see Table 2.2. These are all aspects to consider when calculating the total E2E delay of a packet in a system.

4.2.1 Tools

Simula & Demos

In the specialization project carried out on the topic from August to November 2019, Simula, with the Demos package, was considered as suitable for this project [13]. Simula is a programming language used to build simulation models, whereas Demos is a package implemented in Simula to make discrete event simulations more bearable for people new to discrete even simulation, making the Demos programs a simple version of a Simula program [11].

Simula was officially introduced in 1967 in a simulation language conference in Oslo [115][43] and have been important for the field of object-oriented programming for instance by introducing the objects, the classes and the inheritance concepts, without being widely used itself [43].

Demos is a package used with the programming language Simula, helping the user to write sufficient simulation programs without much expertise in Simula. Demos can be used to describe models using entities and resources, of which the entities competes for. Resources are used to represent smaller components, while entities are used to display entire life cycles of more important simulation components. According to Britwistle [11], even though Demos is a relatively small and simple modelling tool, it has been used to simulate realistic industrial systems in the oil and gas, telecommunication and aerospace industries as well as at universities, to mention a few [11].

The main reason for choosing to use Simula and Demos for this project the following simulations is that the language and packets are relatively easy to understand, as well as they have been used in previous projects in other units at the Norwegian University of Science and Technology (NTNU). There also exists an instruction and description manual [11] that can be used to find implementation examples and solutions as well as answers to potential challenges that can occur. To be able to use Simula, it is not necessary with any additional or expensive software or hardware, other than a computer which is easily accessible. Simula is easy to install (from [85]) and it only requires a text editor and a terminal application to run the simulations.

The main challenges that can occur during simulations is that Simula related syntax errors are close to impossible to solve using online search queries. This is a huge difference compared to what is available with other, more widely used programming languages. An other challenge is that it will require time to get the required programs

installed and read into how the programming language works to be able to model the system. Therefore some time is assumed to be used for code reviews. The examples in the Demos manual will most likely help in case something stops working. In addition there are professors at NTNU that have experience with using Simula that might be able to help, in case there are situations that occurs that is not covered in the Demos manual [11].

Draw.io

Draw.io [25] is a diagram editor that can be accessed online through Google Drive, which will be used to draw activity diagrams. This is a free tool, that has been used in previous projects to draw a variety of diagrams. The tool has been used to draw figures such as flow charts, network diagrams among others, in several units the past couple of years. The activity diagrams will be used to show how the system, that is to be simulated, is implemented. Activity diagrams are easily converted into a Demos script [11] and a great tool that can be used to show the systems functionality.

Policing Mechanisms

A policing mechanism are to be implemented in the simulation. The policing mechanism that is proposed in this thesis and used in the simulations are made with inspiration from descriptions of policing and scheduling mechanisms presented by Kurose *et. al* [59] and is similar to the mechanism Shoeb *et.al* [112] proposed in their paper. They assigned prioritization to packets to separate and prioritize packets from trusted sources over traffic from unknown sources. The policing mechanism that is used in the simulations are described in chapter 6.

4.3 Data, Accuracy & Result Validation

The parameters used in the simulation models was found during the literature review and are more thoroughly explained in chapter 5 and chapter 6. However, the numbers related to data rates, link capacity and that was used to establish threshold values was chosen from research papers in chapter 3 or very similar to what had been used in these research papers. Distributions used to mimic legitimate traffic and arrival rates was also found in those papers.

The chosen papers are research papers published by universities, other well known organizations such as IEEE or number and values found in other literature, accessible through the Norwegian University of Science and Technology (NTNU) license, from authors with great knowledge within this field of study. These works are chosen to ensure that the sources are valid and suitable for this purpose.

The model that is to be used in the simulations is a simplified version of a real-life router. It has less input ports and output ports, and it is not any specific type. Real-life routers have a specific processing capacity depending on what component is used, and is hence assumed to be added onto the results from the simulations. Therefore, there will be some deviations from a real-life system. However, that does not mean it is impossible to learn something about how a DDoS attack affect the delay of real-time traffic through simulations and how policing may or may not be efficient to mitigate it.

To ensure accuracy of the results, each of the simulations will be run with different seeds to make variations to each drawing from the distribution(s). For each scenario (with and without traffic policing and for different strengths of attack), the simulation will run ten times, where the seed is changed each time. The data that is used in the results will be the average of these ten simulations with a 95% confidence interval. The goal is to have the confidence interval as small as possible, and run the simulations with as many packets as possible to get the most accurate answers.

Before running the simulations, the model will be tested by first checking the delay of a simulation without packets, which is expected to be zero. Then, the maximum data rate the model can handle will be checked. It is expected that the simulations run with less than maximum data rate, will have lower delay that what a maximum data rate will have. If this is not the case, the model needs to be adjusted so that these simulations are behaving correctly. Otherwise the results can be faulty.

The final results from the simulations will give an indicator on how traffic policing can affect the delay of high priority traffic compared to when it is not used. Especially interesting will be to see how big the changes are when a DDoS attack is inserted to the model.

4.3.1 Step-by-Step: Simulation

1. Build the system model and draw Demos customized activity diagrams that describes the system to make it easier to implement.
2. Implement the entities and related logic into a Demos program
3. Check consistency of the model before using it in the experiment
4. Carry out simulations of different scenarios where variations are introduced.
5. Perform analysis on and discuss the results and other findings.

Chapter 5
Qualitative Analysis

5.1 5G Offshore: Importance, Possibilities and Risks

The offshore industry is a part of the oil and gas infrastructure, which in Norway is considered a critical and vital infrastructure to preserve the Norwegian societal functions and provide for the populations basic needs. The oil and gas industry is vital to the transportation sector, which for instance need fuel to deliver food to the grocery stores. It is also important as an energy source, for power and heating, as well as it generates a revenue that is used to for instance provide free health care and other benefits. A deployment of 5G and IIoT could overall improve productivity and efficiency [99]. Collecting data from several deployed sensors on the offshore installation could be used for data analytics to create better insights. This could further provide more precise calculations and better allocation of resources and more efficient productions. An interest in reforming the industry, could increase the revenue which the population could benefit from. In addition as the offshore industry is considered one of the most dangerous work places there is, a remote operated replacement of heavy human operated machinery can make the working environment more safe as the systems can be controlled from a distance, and contribute to reduce HSE risks [47].

A potential offshore IoT network could be quite similar to an industrial plant network, but most likely even more distributed and widespread in the environment. At an industrial plant, processes and operations are being closely monitored using sensors and actuators, and some systems are soon to be autonomous. The offshore industry on the other hand, have not yet implemented wireless sensors and devices for remote operations. This is most likely for instance due to the previously mentioned strict HSE management for the rural, isolated and dangerous offshore environment and/or because of cost or the long distances [47].

The features of 5G, mentioned in chapter 2, makes it possible to deploy IoT for different purposes. For example, features like tailoring the network resources, sup-

porting URLLC, handling more devices and hence also more generated data allows the network administrators to deploy and use time-critical applications, and allocate the necessary resources and prioritize the data if needed. As time-critical applications are latency-sensitive, it is necessary to be able to prioritize this data before non-latency-sensitive data, like the information used to make future predictions and normal communication data. For instance, if latency-sensitive offshore data arrived at its destination too late, it could cause dangerous situations and make the working environment more unsafe. In a smart city, if an autonomous vehicle registered that it was to close to an object and therefore sends an instruction to break, the vehicle needs to break *right now*. If the instructions arrives too late, the information is no longer relevant or useful as the accident most likely already happened. Therefore, the 5G features such as high reliability, availability and ultra low latency as well as the possibility of allocating resources, can make it possible to deploy real-time applications offshore.

There is no doubt that 5G and IoT could be important for the offshore industry's development, in terms of efficiency and safety, among others. The possibilities that follows a deployment of 5G and IoT are many, also for this industry. However, with possibilities and importance there are risks. All systems are susceptible to attacks. DDoS attacks such as those explained in chapter 3 are attacks that have occurred recently. The examples shows that the attacks described in Table 3.1, Table 3.2 and Table 3.3 are being carried out and are highly relevant. For several of them, utilizing IoT devices to affect critical infrastructures and disrupting network connectivity by flooding and exhausting the communication links is common. This shows that it is relatively normal to misuse the constrained IoT devices to cause harm. Something similar was stated in the newspaper *The Guardian*, where David Fidler said *"We have a serious problem with the cyber insecurity of IoT devices and no real strategy to combat it"* [131]. Statements like this enlightens how important it is to be aware of security and vulnerabilities of IoT devices when they are to be deployed *everywhere* [42].

The examples of attacks presented in chapter 3, shows that the motivation for attacking critical infrastructures, ICPS and IoT systems is definitely there. It is reasonable to assume that based on the motivation for attacking such systems along with other types of cyberattacks that have occurred on industrial systems recently, like the *Stuxnet* attack [66] and the attack on Hydro in 2019 [46], that an *offshore* IoT system also is prone to be a target or a victim of a cyberattack in the future.

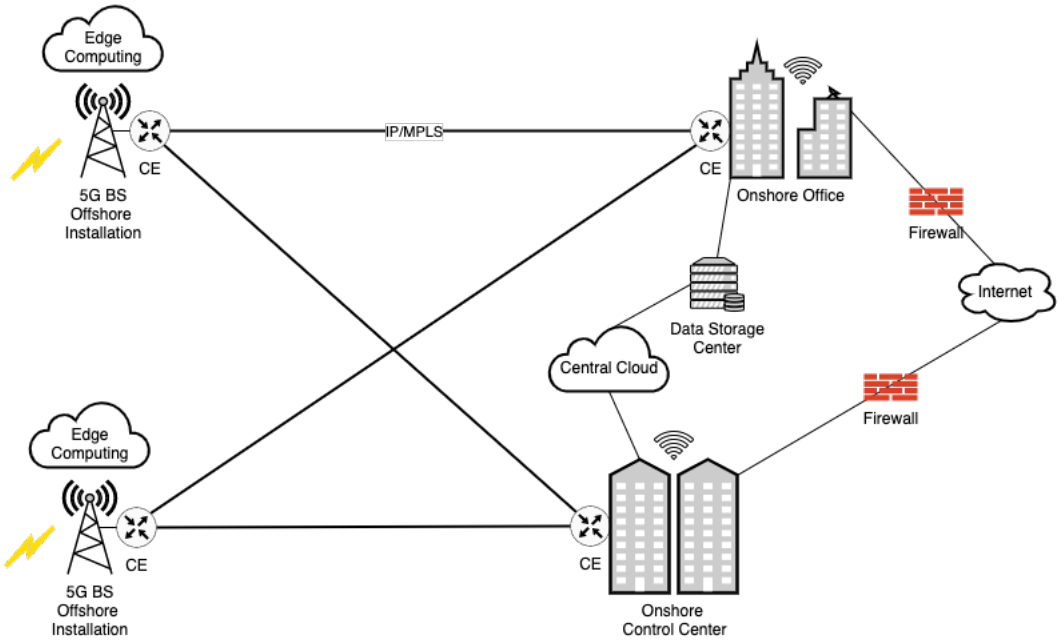

Figure 5.1: Offshore IoT Network Idea

5.2 Offshore IoT Network Setup and Traffic Prioritization

5.2.1 Similar Systems

An offshore deployment of IoT will potentially look a lot like a industrial plant network in terms of setup and required entities [31]. Therefore, the industrial plant setup found in Frey *et.al* [31] have established the foundation of what Figure 5.1 has been built upon.

5.2.2 Offshore Radio Access Network

As the main idea with the IoT deployment offshore is to simplify and defuse everyday assignments and chores, it can be necessary to monitor processes from onshore offices, make the systems make decisions on their own and use small, mobile and Internet connected devices such as cameras to communicate in real-time with industry experts and get instructions to do maintenance or tasks out of their expertise but within their capabilities. As of right now, there are wired sensors deployed and used for monitoring processes and operations as well as 4G BSs on some of the offshore installations, provided by Tampnet [118] and Telia [8]. But one of the main challenges is that 4G do not have all the features required for real-time and time-critical communication. If

the goal is to use the network connectivity for remote operations, real-time production updates, time-critical communication, real-time analytics from videos, mobility of devices (e.g for body cameras and sensors) as well as entertainment and normal data communication between onshore and offshore offices, the 4G network will not be sufficient. If the goal in the future is for example to have remotely operated processes and operations as well as be able to use UAVs for inspections and maintenance, it is necessary to take advantage of the 5G features mentioned in section 2.4.

To be able to use systems and applications that requires features like URLLC on an offshore installation, it is necessary to deploy 5G BS with co-located edge computing capabilities for faster computations, lower latency and higher reliability on the air interface between the IoT devices and the BS. 5G also comes with new features such as network slicing and eMBB which is useful in this industry. For instance, it is possible to use network slicing to separate operational URLLC from general business communication and non-time-critical monitoring data transmissions, which is already existing on the transport link. This way it is possible to allocate resources suitable for each main use case and prioritize the most time-critical transmissions over the other data.

5.2.3 Transport Network between BS and Onshore Office

Optical fibre cables provides network connectivity between onshore offices and to the offshore installations in the North Sea [119]. The Subsea fibre network infrastructure in the North Sea is provided by Tampnet [8][118]. The cables are used to provide broadband access with high capacity for huge data transmissions between offshore installations and onshore offices and to enable 4G and Narrowband-IoT (NB-IoT) offshore [119]. In addition, these fibre cables can facilitate time-critical data transmissions. because they, as Tampnet states, *"have virtually no delay"* [117]. In other words, it is not the transport network that necessarily restricts the use of URLLC offshore, but the currently used access network, 4G. Hence why, it can be possible to combine the 5G access network with the subsea optical fibre transport network and meet the URLLC requirements with regards to latency and reliability.

The optical fibre cables are connected to edge routers on each end-point. In Figure 5.1 these routers are displayed as Customer Edge (CE) routers. Label-Switched Routers (LSRs) are used with the MPLS technology as it works alongside the traditional IP-routing technology to provide faster data packet forwarding [59]. Hence, making it more compatible to being used for time-critical high-speed data transmissions [80]. The control and management planes in routers allows for network administrators to add policies to the forwarding tables and prioritize traffic, which is useful with regards to the resource consumption and making sure that the links are available when the time-critical data is arriving [37]. This could be useful for time-critical

data that is being transferred alongside other types of data packets from the offshore installations to the data center(s) at shore.

5.3 Offshore Network Attack Surface and Accessibility

Compared to 4G BSs ranges, 5G BSs have smaller signal range and support higher device density. Femtocells and picocells, see Table 2.1, would be preferred with regards to coverage, to avoid the 5G range to exceed the 500 m safety zone. If any signals was to exceed the safety zone, it could be reached and accessed by someone unknown passing by or by an attacker located onshore if the offshore installation was located close by. Small cells like, femtocells and picocells will, among others, provide faster connectivity and enhance battery duration of the IoT devices. By using small cells, unknown people or adversaries would not be able to be in range of the 5G BSs, and hence struggle to perform attacks that requires to be connected or accessing the same air interface as the constrained end-devices. Hence, the only threats for the equipment deployed on the offshore installations are assumed to be dishonest offshore workers with physical access to the IoT devices and BSs. To block data on its path from the end-device to the BS would either require that the device itself was physically tampered with or the attacker accessing the air interface to perform attacks like signal jamming, masquerading as legitimate nodes and use these to generate and send excess/alien traffic.

As mentioned by Göransson *et.al* [37], Mousavi *et.al* [76] and Li *et.al* [65] in chapter 3, the control plane can be considered as a *single point of failure* in the system. With 5G mobile networks follows real-time data transmissions. For latency-sensitive applications an attack can cause even greater harm than it could with data transmissions using 4G, namely because 5G support URLLC. A DDoS attack on a router node, could potentially overwhelm the CPU, as the device do not know where to forward the packets and have to make requests to the control plane. If the backlog of data traffic that waits on a forwarding action was to be too long, it could force the device to drop packets. This way, time-critical traffic would not be delivered on time, which then again could cause damage.

5.4 Preliminary Results

5.4.1 Offshore Systems & DDoS Attacks

The offshore industry will most likely be prone to DDoS attacks just as other systems, as argued for earlier. There are many ways to cause a DDoS attack that can affect these systems. One interesting way to carry out such attack is by overwhelming the centralized controller or CPU in a switch. The challenge occurs when the DDoS attacks origins from several hosts that are a part of a botnet.

The background research done in chapter 3 shows that there are a big risk of DDoS attacks on routers with the goal of overwhelming the CPU or controller of the switch. It is a perfect victim because it is described as a *single point of failure*, which can cause the switch or router to go down and hence not be able to carry the traffic through to the next hop. The suggestions found in the literature review on how to implement control plane policing on traffic between the data plane and the CPU, are relevant to implement on a network device also in the offshore industrial systems, especially with regards to detecting and filtering alien traffic. One of the filtering mechanisms shows a close to 97% success rate in detecting unwanted and excess traffic [24] while another conclude with an 80% success rate [87]. In addition, there are traffic priority mechanisms that can be deployed when several use cases with different QoS requirements are sharing a medium. Some of the papers in the literature review suggests solutions like blocking a port or a host for a given amount of time if there are abnormal traffic rates occurring from this source [134]. Other suggestions was for the hosts to get a trust value and use this to prioritize its packets [112]. Blocking ports can be a smart solution to protect the control plane resources, but what happens if normal and legitimate traffic passing through this port is blocked temporarily too? And what happens if a host get a low trust value because it sends packets with abnormal rates and seemingly is a part of a botnet but also transmit legitimate traffic regularly? In cases where the data packets are not time-critical, this is not as big of a challenge if the attack is not long lasting. But what happens if the suggested solutions were to be used for offshore, real-time IoT traffic that require low latency and have strict deadlines of when to reach its destination? From a security point of view, if a resource is unavailable when needed, in this case the control plane, the security of the system is compromised [18]. And if real-time traffic do not reach its destination in time, and the system have "hard deadlines", the packets are no longer useful and the outcome can be catastrophic [111].

None of the research papers that were found and is used in the literature review states anything about how a DDoS attacks on the control plane affect real-time IoT traffic through the router. Neither do they say anything of whether or not these additional policing mechanisms and filtering mechanisms affect the total delay or how much excess alien traffic a switch can handle before the time-critical data is delayed so much that it is no longer useful. Therefore, the goal in the next chapter is, by doing simulations of a DDoS attack on a router, to look into how DDoS attacks will affect the latency of time-critical offshore IoT traffic and whether or not it is possible to have use cases with strict time limits offshore because of the long distance(s) between the endpoints. A second round of simulations will be done where a Control Plane Policing mechanism is implemented to see how it can be able to mitigate how the DDoS attack impacts the latency of the real-time traffic. The main research questions (RQ) for will therefore be:

RQ1: Would it be possible to have time-critical applications offshore that is communicating with servers on shore within the required packet delay limit and could traffic policing be a suitable solution to enable this?

RQ2: To what extent does control plane policing mitigate how a DDoS attack impacts the latency of time-critical offshore IoT traffic?

5.4.2 Packet Delay

To be able to say anything about packet delay with regards to DDoS attacks, it is necessary to understand how a packet can be delayed. Packets that are time-critical can handle only a minimal amount of delay, depending on whether the deadline for the specific packet is soft, firm or hard, before it is no longer useful [111]. Industrial URLLC have requirements regarding maximum latency according to Zhang *et.al* [137]. For instance does factory automation require the end-to-end delay to be less than 2.5 ms, whereas motion control require a more strict delay maximum of 1 ms, as can be seen in Table 2.2.

According to Kurose *et.al* [59], transmission delay, queuing delay and processing delay (as well as computation delays [137]) are typically expressed in the order of milliseconds (ms), microseconds (μs) or nanoseconds (ns). The total delay of a packet will depend on those delays as well as the propagation delay which is the delay between two network components. The propagation delay depends on the distance, medium, and the propagation speed between the end points. This speed is usually in the order of meters (or kilometers) per second. In optical fibre cables the signals travels close to the speed of light, which is approximately 300 000 km/s. In other mediums the speed is not as fast, but around 200 000 km/s [59]. Packets from offshore located BSs will travel over quite long distances in subsea optic fiber cables, see section 5.3. According to a presentation given by Tampnet [118], about potential offshore IIoT use cases, the optical fibre cables used to provide Internet connectivity offshore cause a delay of 5 μs per kilometer (km) [120] which is a bit more precise for fiber optic cables than the propagation speed interval (as mentioned above) suggested by Kurose *et.al* [59].

When it comes to location of offshore platforms, Equinor states that their platforms are located approximately between 80km and 300km from shore [28][29]. Using these distances as reference, the propagation delay in fiber optic cables can be 0.4ms and 1.5ms for those locations respectively:

$$Delay = Distance(km) \times 5.0\mu s/km$$

$$Prop_{Delay_{Max}} = 300km \times 5.0\mu s/km = 1500\mu s = 1.5ms$$

$$Prop_{Delay_{Min}} = 80km \times 5.0\mu s/km = 400\mu s = 0.4ms$$

From the same presentation, Tampnet states that wireless links cause a delay of 3.6 μs per km [120]. In section 5.3 it was suggested to use small cells with a range of less than 0.2 km in an offshore deployment, as this will remain inside the offshore installations safety zone, this causes the maximum propagation delay of the air interface to be:

$$Prop_{Delay_{Air}} = Distance(km) \times 3.6\mu s/km$$

$$Prop_{Delay_{Air}} = 0.2km \times 3.6 = 0.72\mu s$$

In addition to the propagation delays of the fiber optic cable and the air interface, there will also be some time lost to processing, forwarding and queuing in the routers, switches and BSs. The delay caused by one network node will include transmission delay, queuing delay and processing delay. The transmission delay will be depending on the link rate and the packet length [124]. For instance will a 10 Gbps link cause 1.2 μs delay if the packet is of 1500 bytes, according to the following formula [59]:

$$Trans_{Delay_{Cable}} = length_{packet}/rate_{link}$$

$$Trans_{Delay_{Cable}} = 1500bytes/10Gbps$$

$$Trans_{Delay_{Cable}} = 12000bits/10Gbps = 0.0000012s = 1.2\mu s$$

Queuing delay and processing delay will be varying depending on the traffic intensity and hence how busy the CPU is [59]. The processing delay is depending on the individual network component and its specifications and will therefore be different for the various providers depending on parameters such as network interface cards among others [15]. The processing delay is therefore individual for each node, and is not included in the simulations, however it is important to keep in mind that this will be added to the total delay of each node in real-life and will be in the range of ns to μs. Additional processing delay will most likely affect the simulation results in terms of total delay, if it was to be included. In the following simulations, the processing delay is assumed to be a really small constant value. The queuing delay will be in the range of μs to ms. These two types of delays are typically harmed during an DDoS attack, as the traffic intensity is increasing and several packets have to wait in a queue to be processed. Other packets do get lost.

Figure 5.2 shows an overview of some of the delays that would be affecting the IoT packet from the offshore installation on its way to the CE router on shore, where queuing delay (QD) is to be investigated in the simulation.

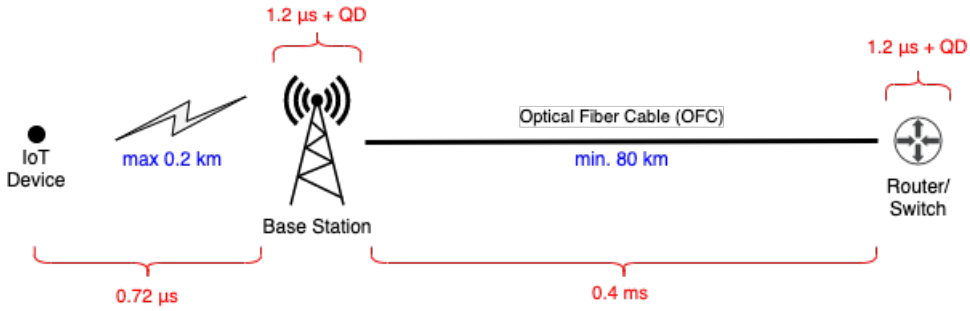

Figure 5.2: Delays in a simplified offshore network

Chapter 6
Model Description

In this chapter the simulation setup and entities are explained, the simulation parameters is presented and the reference mechanism and control plane policing mechanism are implemented and explained using figures and textual descriptions. Some assumptions are also listed as this simulation is a simplified example of a real-life situation. The results of the simulations is presented in the following chapter, chapter 7, and discussed in chapter 8. The aim of this chapter is to describe the model that is used to investigate the research questions (RQ) listed below.

RQ1: Would it be possible to have time-critical applications offshore that is communicating with servers on shore within the required packet delay limit and could traffic policing be a suitable solution to enable this?

RQ2: To what extent does control plane policing mitigate how a DDoS attack impacts the latency of time-critical offshore IoT traffic?

6.1 The System Setup

The following sections explains how the simulation is structured. Figure 6.1 gives an overview of the simulated router and its traffic flows. The traffic that enters the router is either, management traffic (red line), control traffic (blue line), service traffic (thin black line) or data plane traffic (bold black line) [37], see Figure 6.1. Service traffic is, as shown in Figure 6.1, a minor amount of the data plane traffic that needs special attention from the CPU [103]. Assuming that traffic is already filtered once by the iACL (faded yellow circle), except that the alien traffic has not been detected. The simulations will include the alien traffic as well as management, control and service traffic (*"normal"* traffic) and be performed with and without applying control plane policing (illustrated with purple and orange circles), mainly to look into how the total traffic delay is affected.

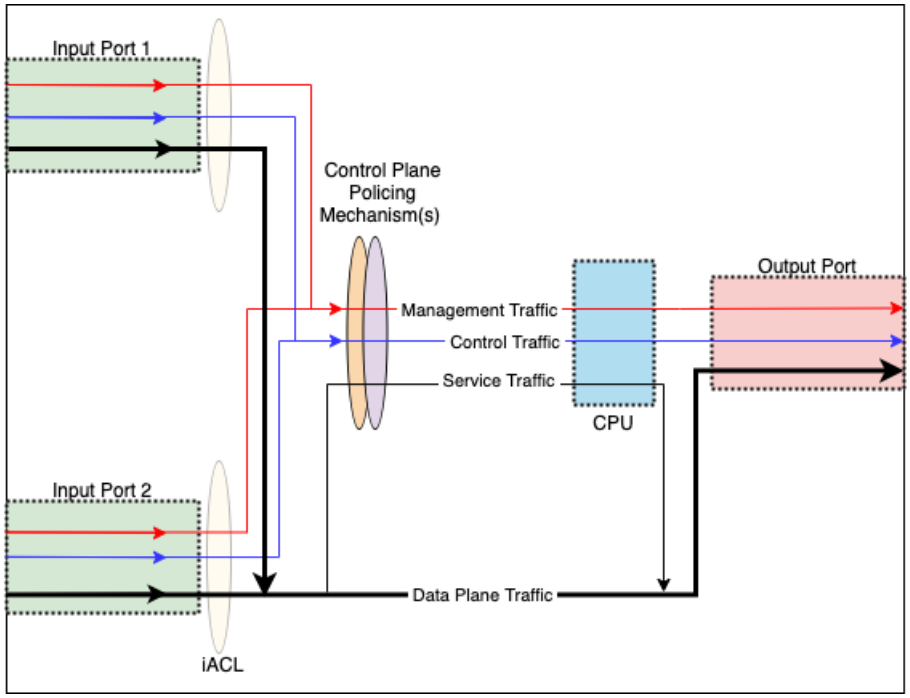

Figure 6.1: Simulation Overview (Modified version of Fig2, Cisco Website [103])

6.1.1 Assumptions

Some assumptions are made before carrying out the simulations for simplifying purposes. These assumptions are listed below:

Assumption 1: The processing delay in a router is assumed to be a really small constant value, and hence not included.

Assumption 2: The legitimate traffic and the alien traffic is being policed.

Assumption 3: The attacker generates packets with an arrival rate that is higher than the arrival rate of legitimate traffic.

Assumption 4: The models total load is 800 000 packets per second, which is 96% of the total load on a 10 Gbps link.

Assumption 5: The output link is able to handle 0.8 packets per μs and hence able to handle 96% of the load from a 10 Gbps link. (In reality the packets would queue at the output link(s) [59]).

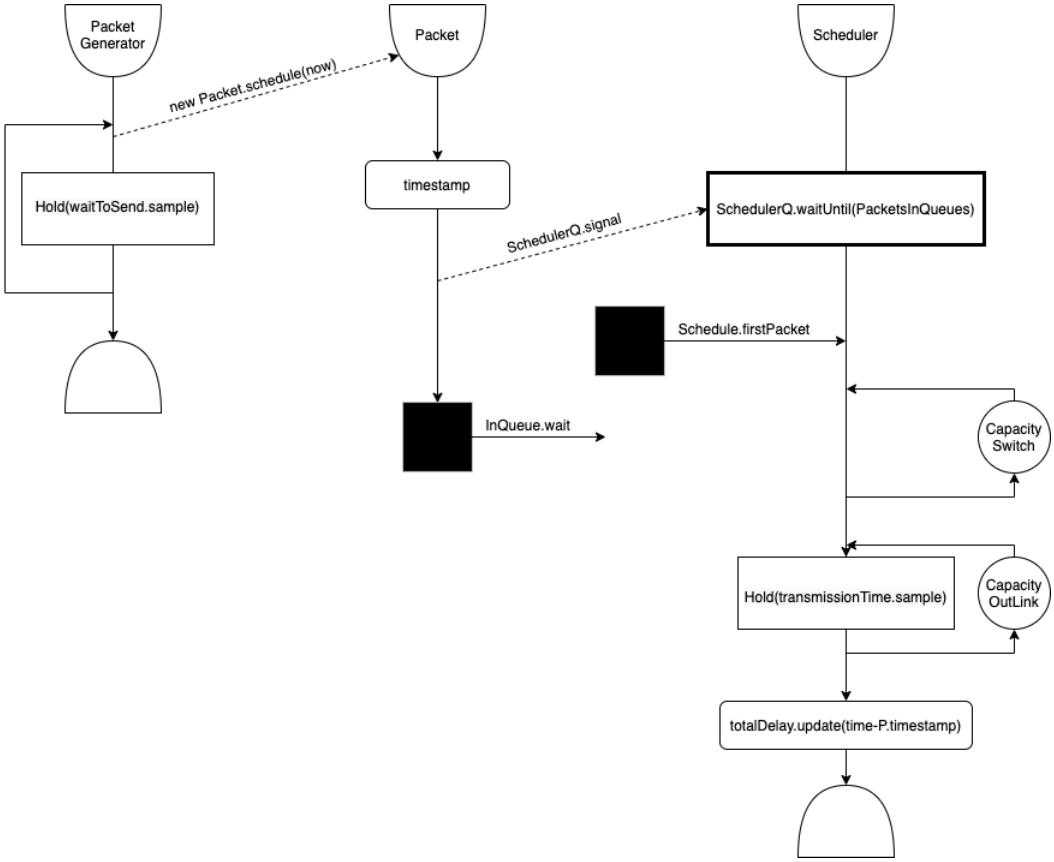

Figure 6.2: Activity Diagram of Simulation Entities excl. Attacker

Assumption 6: After exiting the switch, the packet acquire a transmission link resource, instead of queuing up.

Assumption 7: All packets are of the same size (1500 bytes).

6.2 System Entities

Figure 6.2 shows an activity diagram of the simulation with normal packet flow, whereas Figure 6.3 shows the entities used during the attack phase. Each of the entities will be described in the following subsections.

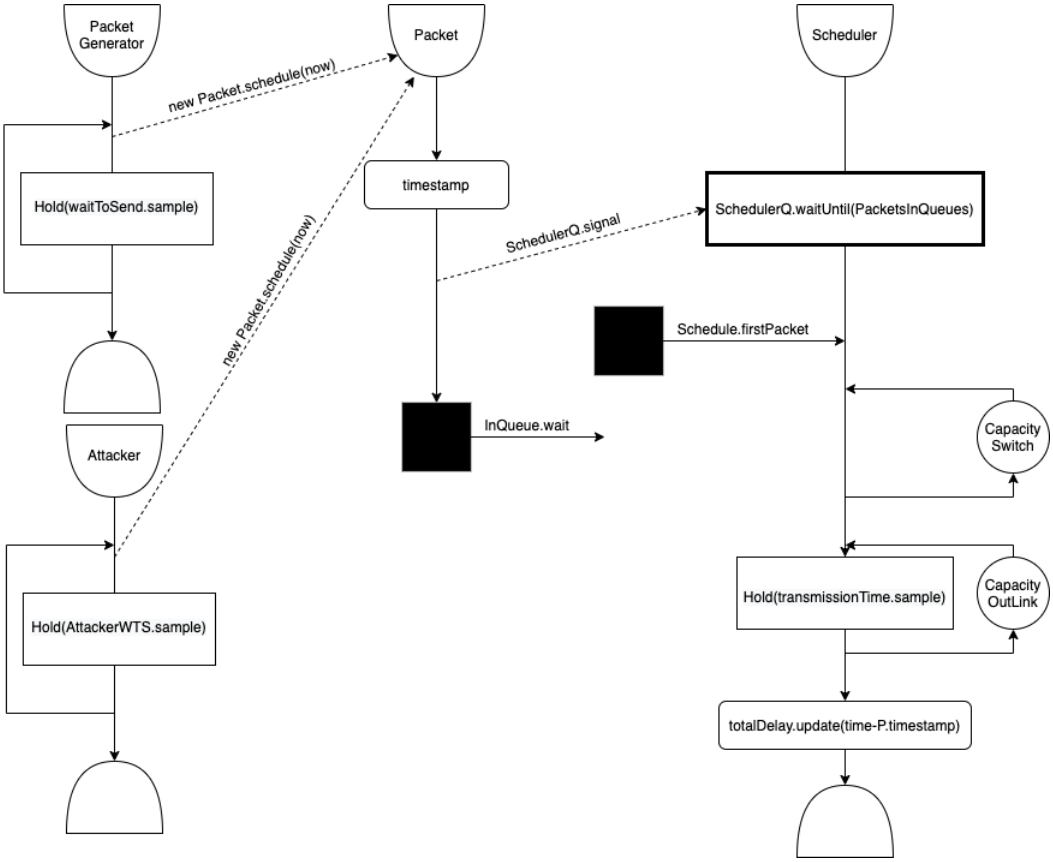

Figure 6.3: Activity Diagram of Simulation Entities incl. Attacker

6.2.1 Packet Entity

The *Packet* entity is assigned a total of four attributes Figure 6.4. When a packet is generated, it gets a port number (1 or 2) and a signature based on what entity that have generated the packet (either attacker, a legitimate packet generator or time-critical packet generator). For policing mechanism, see Figure 6.6, the packets are also assigned a priority. When the packet arrives at the input port, it gets an arrival timestamp. The timestamp is used to measure the packet delay. The packets are all of the same size (1500 bytes).

6.2.2 Packet Creation Entities

Packets are originating from three different sources, one attacker and two legitimate, that transmit the packets to two input ports. The input ports are chosen for each

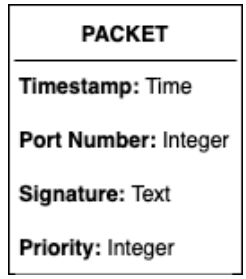

Figure 6.4: Packet Entity and its Attributes

packet using the built-in pseudo-random integer generator in Demos. This generates a uniform distribution of the integers 1 and 2. The uniform distribution makes it as likely for a packet to go to input port 1 as input port 2, spreading the traffic equally on the two ports. It is important to keep in mind that random generators are not truly random, but for this simulation it is useful as it generates numbers relatively fast.

Each packet is also assigned a signature. This is simplified from a real-life situation, as these signatures is not as obviously marked. However, the signatures added to the packets in this setup makes it possible to distinguish the alien packets from the legitimate packets for counting purposes and to generate results based on how many successful packets that is processed successfully. When a packet is created, whether it is malicious or not, it signals the switching mechanism that a packet is now put in a queue (Queue 1 or 2, depending on the assigned port number) waiting to be processed.

For the policing mechanism, the packets are assigned a *Priority*. All packets that is time-critical gets priority = 2, other legitimate packets gets priority = 1, whereas alien packets gets priority = 0. When packets are put in queues, packets with higher priorities are put in front of packets with lower priority.

6.2.3 The Scheduler Entity

The *Scheduler*, as can be seen in both Figure 6.2 and Figure 6.3, its main task is to wait until there are any packets in any of the queues, then if the switch resource is available, it schedules the packet located first in any of the queues (depending on the rules set for when to pick from each queue), and transmit it onto the output link. In reality, the packets would be processed in the switch as well, hence causing a processing delay, which is neglected in these simulations, as explained in subsection 5.4.2. The final step of the scheduler is to update the timestamp of the packet, and log when the packet was finished. However, in this simulation there are two different mechanisms

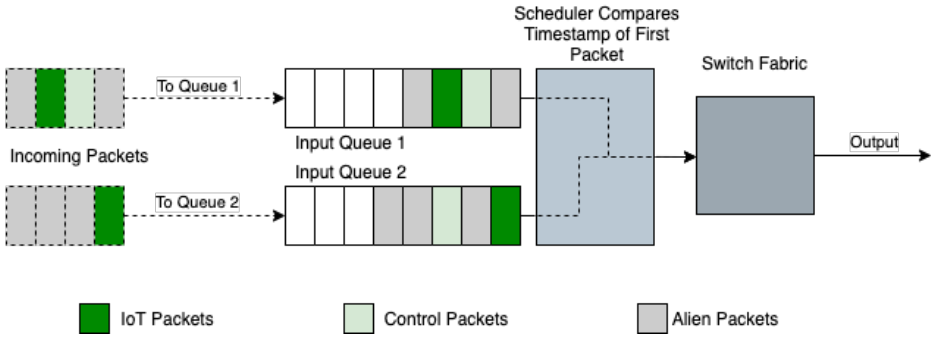

Figure 6.5: Reference Mechanism, State Diagram

used to schedule the next packet. One of the mechanisms is the reference mechanism with no policing mechanisms implemented, where the scheduler alternate the queues its picking from. The second mechanism has policing implemented. Here the packets are prioritized and the packet with the highest priority are the packets mimicking time-critical packets.

The Reference Mechanism

This mechanism[1] is meant to be mimicking a router without any control plane policing mechanisms. The only thing this mechanism do, is to check whether or not there are any packets in any of the queues, and process the packet first in the queue. If there are packets in both queues, it draws a random number 1 or 2, and chooses the first packet in the queue. This mechanism is not concerned with either priorities or timestamps. Figure 6.5 shows how the reference mechanism works.

[1] https://github.com/HanneB/MasterProject/blob/master/ReferenceMechanism.sim

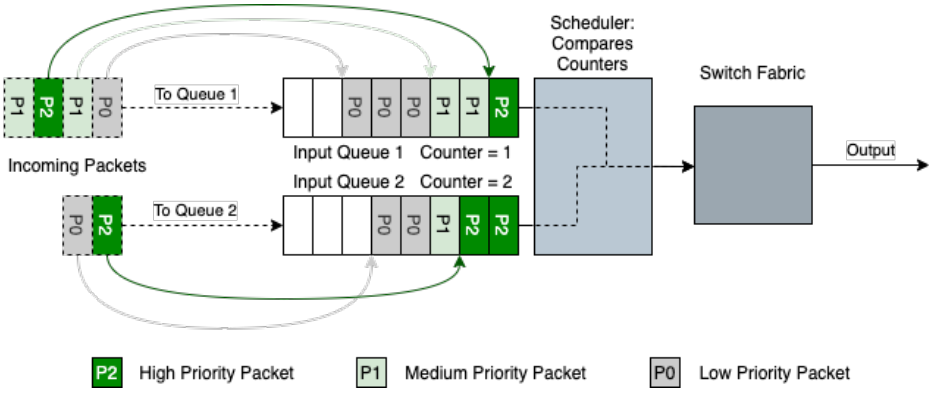

Figure 6.6: The Implemented Policing Mechanism, State Diagram

The Proposed Policing Mechanism

The second mechanism prioritize a bit different[2]. Here each packet gets a priority 0, 1 or 2 and each time a time-critical or legitimate packet is added to a input queue, a counter (respectively to each of the queues and each of the packet types) is incremented by one. This way, this scheduler keeps track of how many legitimate and time-critical (medium and high priority, respectively) packets are waiting in front of each of the queues and picks the queue containing the highest number of high priority packets. If both of the high-priority counters equals zero, it checks the medium priority counters. For the other packets the scheduler compares the timestamps of the first packet in each of the queue and chooses the packet that have most elapsed time. The moment a high-priority (priority = 2) packet enters a queue, this packet is guaranteed to be processed before packets with lower priority, but after packets with the same priority that is already placed in the queue, see Figure 6.6. If both queues contains the same amount of prioritized packets, the scheduler compares the timestamps of the first packet in each queue and process the one that have the highest timestamp because if they both are time-critical packets, the packet with the highest elapsed time is the packet that is closest to its deadline, and hence it is necessary to minimize any additional delay. This also goes for medium-priority and low priority packets.

[2]https://github.com/HanneB/MasterProject/blob/master/CoppMechanism.sim

Chapter 7
Simulation Results

7.1 The Simulation Parameters

Mills *et.al* [72] operates with a network link speed of approximately 10 Gbps. Which according to Ruud *et.al* [97] also is common for optical fiber cables. Mills *et.al* [72] further chooses the top speed to be 800 000 packets per second, and justify their choice by showing that

$$8 \times 10^5 \times 12000 = 9.6Gbps$$

where 12000 is the number of bits in a packet of 1500 bytes. 9.6Gbps is 96% of the total load on a 10Gbps link. In other words, the maximum arrival rate, in the order of μs as stated by Kurose *et.al* [59], is 0.8 packets per μs. The correlation between arrival rate ($R_{Arrival}$) and inter-arrival time ($T_{Arrival}$) is given by the following formula [96]:

$$T_{Arrival} = 1/R_{Arrival}$$
$$T_{Arrival} = 1/0.8$$
$$1.25\mu s = 1/0.8$$

causing the minimum amount of time between each packet is $1.25\mu s$, which is the input in the simulation model. Gyires *et.al* [40] describes that the exponential distribution and the *Poisson Process* are used to model the time between arrivals of events that are independent of each other. This distribution is therefore suitable for modelling packet generations. This distribution model is also used by Shakeri *et.al* [108], Lehoczky *et.al* [62] and Jiangzhou *et.al* [135], where Lehoczky *et.al* [62] suggest a packet arrival rate of 0.05 packets per μs. Following the formula above [96], the inter-arrival time is 20 μs. This forms the basis of the parameter choices

found in Table 7.1. Other information with regards to the simulations can be seen in Table 7.2.

The time to get the packet onto the output link, or the transmission time, is set to be equal to the maximum arrival rate of 0.8 packets per μs. For the legitimate traffic, the mean time between when each packet is generated is set to be $50\mu s$(0.02 packets per μs) following a negative exponential functionality in the Demos program [11]. For the time-critical IoT traffic the packet generation rate is assumed to be more intense with a new packet generated with a mean of $20\mu s$ and an arrival rate of 0.05 packets per μs. Some sample simulations will also be performed with a higher arrival rate on (normal) legitimate packets (that is, the same arrival rate as for time-critical packets) to see if it makes any difference to the results.

The reason for choosing these arrival rates is to be able to perform simulations for attacks that is up to ten times more intense than the legitimate traffic. In the description of the Leet botnet attack at Imperva [9], the attack caused the data rate to be changed from the normal rate of 20 million packets per second to 170 million packets per second, and even more. This is an 8.5 times higher rate than whats seems to be the normal rate for that network.

The link (10 Gbps) is used because there will be scenarios where the link is close to fully occupied with legitimate data. The corresponding data rates for the legitimate traffic chosen above is meant to be mimicking only a few devices sending data. The data link of choice is prepared to handle traffic when all the information gathering devices are sending bits at the same time. Otherwise, if this (0.05 and 0.02 packets per μs) was to mimic maximum legitimate traffic on the link, it would be more cost efficient to choose a link with a lower bit rate, especially from an economical perspective [10].

The alien traffic can have a maximum arrival rate of 0.73 packets per μs. Because the total load of the model can be calculated as follows:

$$\begin{aligned} Load_{Total} &= Load_{TimeCritical} + Load_{Normal} + Load_{Alien} \\ 0.8 - (0.05 + 0.02) &= Load_{Alien} \\ 0.73 &= Load_{Alien} \end{aligned}$$

where the time-critical and other legitimate traffic is held at a constant arrival rate and the intensity of the attack traffic is changed from no attack to an attack of up to 95% of the possible load of alien traffic (which is 0.73 packets per μs). The reason for changing the attack intensity is to see how the intensity of the attack affects the legitimate traffic, and especially the time-critical traffic.

Parameter	Value	Ref.
Mean time between each legitimate packet	50 μs	section 7.1
Mean time between each time-critical packet	20 μs	[62]
Mean time to transmit to output link	1.25 μs	[59]
Arrival Rate, legitimate packets	0.02 packets per μs	section 7.1
Arrival Rate, time-critical packets	0.05 packets per μs	[62]
Transmission rate	0.8 packets per μs	[59]
Threshold Value, E2E Delay	1 ms	section 7.2
Arrival Rate(s), alien packets	0% to 95% of 0.73	

Table 7.1: Simulation Parameters

Simulation Information
Simulation ends when 100 000 time-critical packets are successfully switched
10 independent simulation runs for each of alien attack rates

Table 7.2: Other Simulation Related Information

The parameters chosen in the previous paragraphs are listed in Table 7.1.

7.2 Threshold Values

To cover the various use cases, in terms of their latency requirements, it is necessary to establish some threshold values. To be able to have motion control of for instance robots and drones it is necessary with a E2E latency lower than 1 ms, see Table 2.2. VR and other real-time video streaming also requires less than 1ms delay, potentially less than 5 ms for some use cases. When using AR such as head-mounted displays, it is necessary with E2E latency than 10 ms [120], whereas other use cases such as video operated remote control, process automation and process monitoring are not as strict with regards to latency and usually can handle delays up to 100 ms [120]. Table 2.2 lists some other use cases and their demanded E2E latency. It is important to also keep in mind that some use cases may be more strict with regards to latency and may require a 1 ms *Round-Trip Time (RTT)*, as they need an acknowledge when the message has arrived at its destination. Tele-surgery is mentioned by Popovski *et.al* [89], that have such restrictions. In Table 2.2 it is listed with "<1ms" E2E latency. If it was to meet the RTT requirements, the one-way latency would be around 0.5ms. However, tele-surgery precision is not as relevant in the offshore industry just yet, according to Tampnet [120]. The use cases with one-way latency of 1ms are the ones that is accounted for by choosing the threshold value to be 1ms here.

Since Tampnet presents some use cases that could be useful offshore, such as control of drones, remote worker (using VR), handheld terminals, motion control and real-time streaming of data or video the E2E latency in the offshore network system should ideally be less than 1 ms to enable such applications [120]. In other words, time-critical IoT packets should not have more than 1ms of latency before it is no longer useful. The formula in section 2.6 is then limited to be less than 1 ms:

$$\sum_{0}^{\infty} Nodal_{Delay} + \sum_{0}^{\infty} Link_{Delay} = Packet_{Delay}$$

$$\sum_{0}^{\infty} Nodal_{Delay} + \sum_{0}^{\infty} Link_{Delay} \leqslant 1ms$$

The simulation results are presented, compared and discussed with regards to this time limit in this chapter and further discussed in chapter 8.

7.3 Preliminary Findings

From the previous section (section 7.2), the time limit of a time-critical packet was set to be 1ms, to enable use cases with such demands. And as some offshore installations are located around 80km from shore (or more), this is chosen to be a minimum propagation distance. In addition, as several use cases can be enabled by deploying 5G offshore, the data from the installed, wireless sensors are sent across a wireless link of minimum 10m. The threshold values will in the following sections be used in calculations and simulations to show how and why control plane policing can be useful, when deploying 5G including URLLC applications this far from shore.

7.3.1 Individual Delays

System component characteristics affecting the system latency:

Optical Fiber Cable Length

Having a 1ms (= $1000\mu s$) E2E time limit is necessary to cover some of the time-critical use cases, as described in section 7.2. Given that there are no other network components in the system, the maximum length of optical fibre cables can be 200km. For longer distances, the system latency will exceed the time limit of 1 ms, as can be seen below:

$$Prop_{Delay} = Distance(km) \times 5.0\mu s/km$$

$$Prop_{Delay} = Distance(km) \times 5.0\mu s/km \leqslant 1000\mu s$$

$$Distance(km) \leqslant 1000\mu s \div 5.0\mu s/km$$
$$Distance(km) \leqslant 200km$$

The numbers and values used in the calculations above and below are the same as found and established in subsection 5.4.2.

Wireless Propagation Link

If the wireless link was the only component in the system, it could be up to 277km, given that there are no other propagation links or other components, as this will cause the latency to be more than 1ms:

$$Prop_{Delay} = Distance(km) \times 3.6\mu s/km$$
$$Prop_{Delay} = Distance(km) \times 3.6\mu s/km \leqslant 1000\mu s$$
$$Distance(km) \leqslant 1000\mu s \div 3.6\mu s/km$$
$$Distance(km) \leqslant 277km$$

Based on the BSs mentioned in Table 2.1, the macrocell, which is the cell with the widest range, can only cover up to 32km. From a security point of view, if there was to be any BSs that would cover this kind of range, it would possibly not be clever to use. The reason being that a BS range of up to 277km would handle time-critical data on a BSs that could easily be accessed by the public, as it would exceed the 500m safety zone (as discussed in section 2.1) and in some cases also reach shore.

Network Nodes

However, there will most likely be multiple network nodes (i.e routers, BSs) on the way between the two system end-points (offshore and onshore), to forward or store the sensor generated data [59]. From subsection 5.4.2, the propagation delay caused by the fiber optic cable is 0.4ms for the offshore installations located approximately 80km from shore. Assuming that the offshore installation *is* 80km from shore and that the minimum BS range to be used is 10m (that is, $3.6\mu s/km \times 0.01km = 0.036\mu s = 0.000036ms$) gives that the number of any additional propagation links and network node delays needs to fulfill the following equation:

$$\sum_{0}^{\infty} Nodal_{Delay} + 0.4ms + 0.000036ms + \sum_{0}^{\infty} Link_{Delay} \leqslant 1ms$$
$$\sum_{0}^{\infty} Nodal_{Delay} + \sum_{0}^{\infty} Link_{Delay} \leqslant 1ms - 0.4ms - 0.000036ms$$

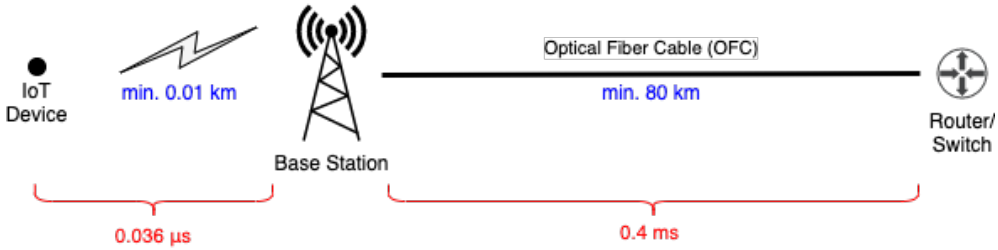

Figure 7.1: Minimum propagation distance and corresponding latency

$$\sum_{0}^{\infty} Nodal_{Delay} + \sum_{0}^{\infty} Link_{Delay} \leqslant 0.599964ms = 0.6ms$$

Figure 7.1 shows the minimum propagation distance that is required to have Internet connectivity on an offshore installation, given that the platform is located 80km from shore and the BS of choice has a 10m range. The new time limit is $= 599.964\mu s$ or approximately $600\mu s$, which is the total time it can take to pass through any additional components.

How many network nodes can be added in this network without having the total latency exceed the absolute maximum of 1 ms, which is a requirement for some of the use cases that could be useful in the offshore industry and enabled by a 5G deployment? And how many nodes can be added to this network if one of the routers becomes a victim of a DDoS attack?

7.4 Simulation Results

By performing simulations of a router with two input ports and one output port, with and without control plane policing mechanism and with and without attack, the results in Table 7.3 were obtained. The simulations was first run on the system with only the reference mechanism to see what kind of improvement it could be possible to make by applying policing mechanisms. Figure 7.2 shows the maximum measured delays for each of the DDoS attacks and its 95% confidence interval. The simulations were run with variations in attack packet arrival rate, from 0% and up to 95% of 0.73 packets per μs, which is the maximum data rate of alien traffic in this model. A 100% arrival rate of alien traffic would mean that 96% of the total load on a 10 Gbps link was occupied, see section 7.1. At 0% alien traffic, the only delay is the delay caused by the legitimate traffic. The idea with these simulations are not to see when the system crash, rather look at how the delay changes for time-critical packets with different attack intensities. Figure 7.2 shows that with more traffic and more packets arriving closer together, the maximum delay increases similar to an curve

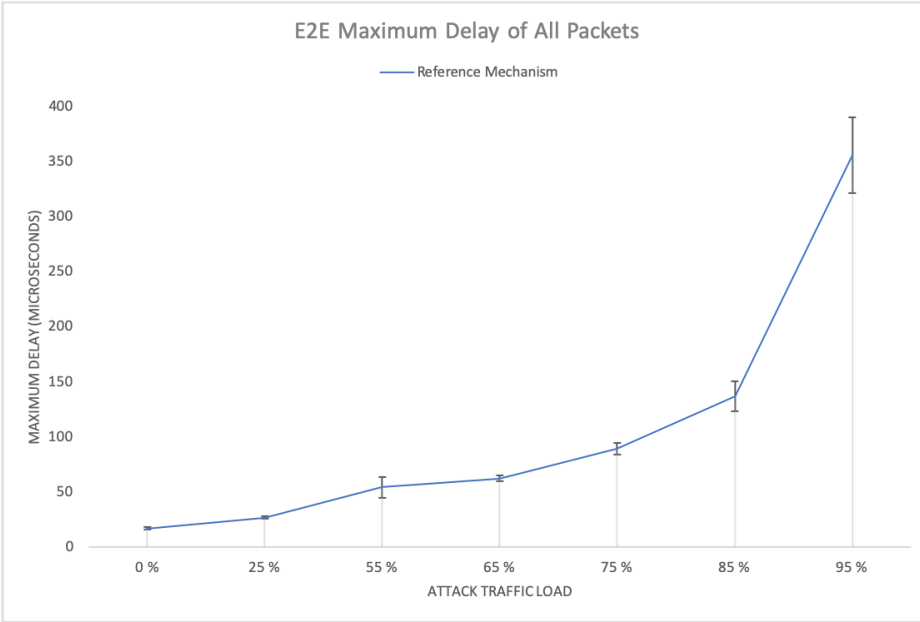

Figure 7.2: Max. delay of traffic before applying policing mechanism

with exponential growth. The vertical lines (black) in the figure(s) shows the 95% confidence interval. It is similar to the curve used to show the dependency between queuing delay and intensity of data traffic [59].

The comparison of the two mechanisms with regards to the maximum E2E delay can be seen in Figure 7.3. Due to greater deviations in the measures of maximum delay, these are not overlapping *all* the time. The difference is only a couple of microseconds, and not of significant matter. It is the delay of the time-critical packets that are interesting to investigate.

Some packets are time-sensitive and some are time-critical depending on the use case. It is preferable to have the delay of all such packets as low as possible through each network node. If one of the time-critical packets is the packet with maximum delay of approximately $350\mu s$, as in Figure 7.2, a packet with a time limit of 1 ms, could only make it through two network nodes, and potentially not travel far across a propagation link. From section 7.3.1, a packet in an offshore-onshore system, would only be able to successfully pass through one node as its remaining time is $= 600\mu s$.

Simulations shows great improvements in keeping the delay from increasing drastically, when using the control plane mechanism (Table 7.4) where time-critical packets are prioritized before other packet types. The arrival timestamp of the packet is

Mechanism	% Alien	Avg.	Conf. 95%	Max.	Conf. 95%
Reference Mechanism	0%	1.36μs	$\pm$0.001μs	16.79μs	$\pm$1.19μs
	25%	1.81μs	$\pm$0.003μs	26.76μs	$\pm$0.93μs
	55%	3.03μs	$\pm$0.010μs	54.36μs	$\pm$9.57μs
	65%	3.84μs	$\pm$00.015μs	62.17μs	$\pm$2.73μs
	75%	5.58μs	$\pm$0.028μs	89.34μs	$\pm$5.49μs
	85%	9.15μs	$\pm$0.069μs	136.84μs	$\pm$13.44μs
	95%	25.62μs	$\pm$0.705μs	355.71μs	$\pm$34.25μs
Control Plane Policing Mechanism	0%	1.36μs	$\pm$0.001μs	18.00μs	$\pm$2.15μs
	25%	1.81μs	$\pm$0.003μs	29.21μs	$\pm$2.21μs
	55%	3.03μs	$\pm$0.010μs	53.14μs	$\pm$7.69μs
	65%	3.84μs	$\pm$0.015μs	61.75μs	$\pm$2.98μs
	75%	5.58μs	$\pm$0.028μs	97.06μs	$\pm$8.42μs
	85%	9.15μs	$\pm$0.069μs	141.37μs	$\pm$23.33μs
	95%	25.62μs	$\pm$0.705μs	353.32μs	$\pm$41.31μs

Table 7.3: E2E Delay - All traffic types

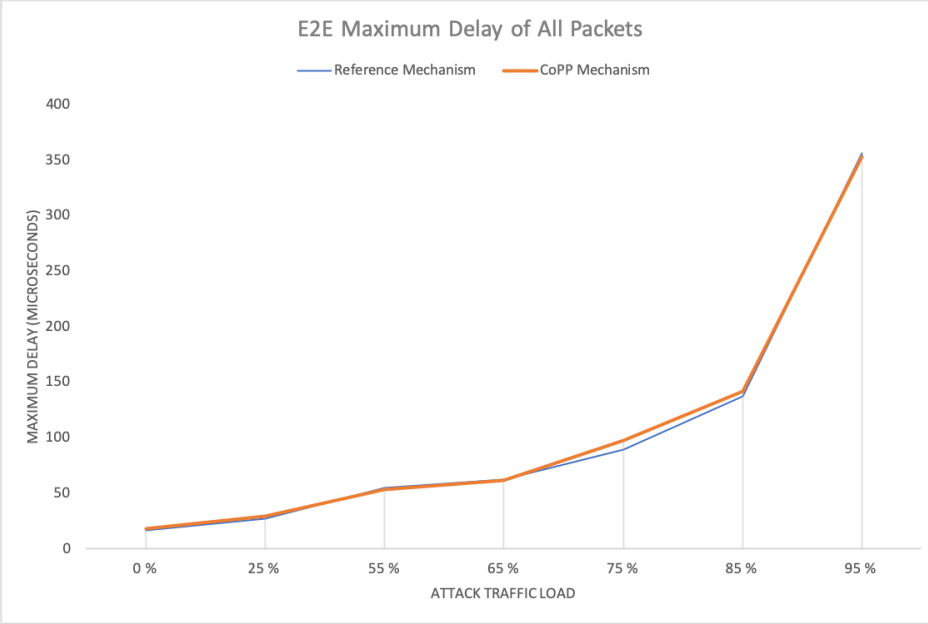

Figure 7.3: Overlapping max. delay of traffic in both mechanisms

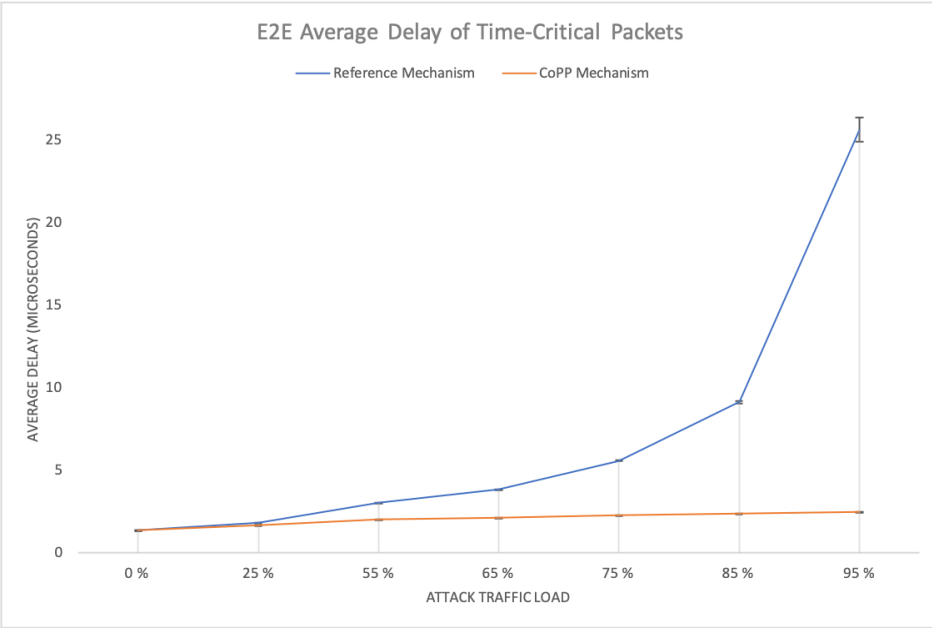

Figure 7.4: Avg. delay of time-critical traffic after applying policing mechanism

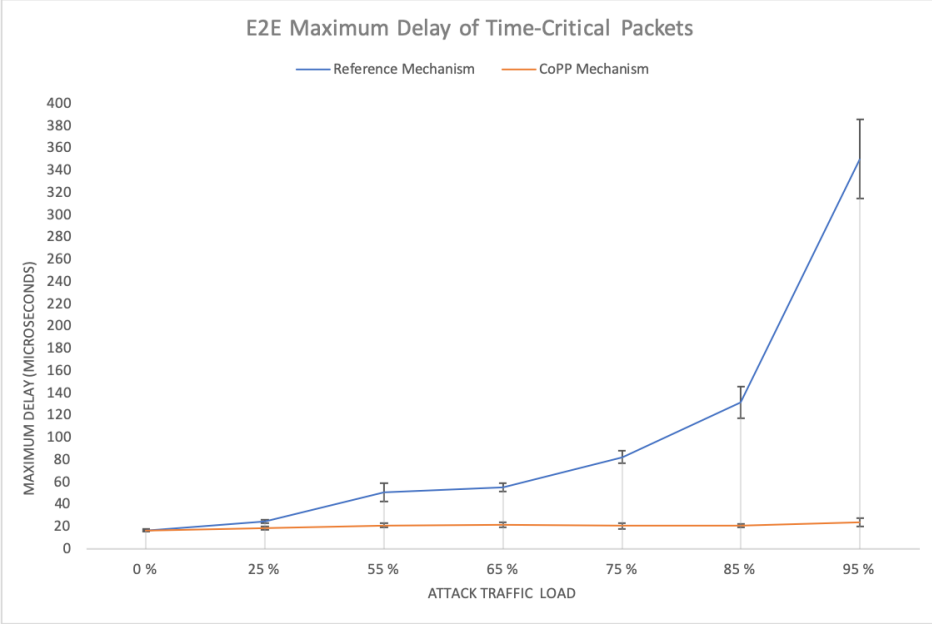

Figure 7.5: Max. delay of time-critical traffic after applying policing mechanism

Mechanism	% Alien	Avg.	Conf. 95%	Max.	Conf. 95%
Reference Mechanism	0%	1.36μs	$\pm$0.001μs	16.64μs	$\pm$1.26μs
	25%	1.81μs	$\pm$0.003μs	24.77μs	$\pm$1.31μs
	55%	3.03μs	$\pm$0.012μs	50.92μs	$\pm$8.43μs
	65%	3.85μs	$\pm$0.017μs	55.30μs	$\pm$4.09μs
	75%	5.59μs	$\pm$0.039μs	82.55μs	$\pm$5.51μs
	85%	9.14μs	$\pm$0.0683μs	131.62μs	$\pm$14.14μs
	95%	25.62μs	$\pm$0.728μs	350.08μs	$\pm$35.58μs
Control Plane Policing Mechanism	0%	1.36μs	$\pm$0.001μs	16.41μs	$\pm$0.93μs
	25%	1.66μs	$\pm$0.002μs	18.69μs	$\pm$1.77μs
	55%	2.03μs	$\pm$0.005μs	21.31μs	$\pm$1.75μs
	65%	2.15μs	$\pm$0.003μs	21.46μs	$\pm$2.15μs
	75%	2.28μs	$\pm$0.006μs	20.62μs	$\pm$2.39μs
	85%	2.40μs	$\pm$0.004μs	21.02μs	$\pm$1.66μs
	95%	2.51μs	$\pm$0.003μs	23.86μs	$\pm$3.85μs

Table 7.4: E2E Delay - Time-critical traffic

considered if the packets in front of each of the queues are both of the same priority. The packet that has been waiting the longest amount of time, is prioritized among them, to help the packet reach its destination before its deadline, as mentioned earlier in section 6.2.3.

The two figures, Figure 7.4 and Figure 7.5, shows how the delay of the time-critical packets are barely increasing (orange curve) when using control plane policing and prioritization. From when there is no attack until the attack is at 95%, there is not any big changes. In a router without such policing, the time-critical packets disappear among the alien traffic and other traffic and have to queue up like the other packets. In a router without policing, the time-critical traffic follows the exponential curve (blue curve), and from no attack until 95% attack, the delay increases extensively.

In section 7.1 the arrival rate of the time-critical and the normal legitimate packets were set to 0.05 and 0.02 packets per μs respectively. If both arrival rates are set to 0.05 packets per μs and by performing the simulations with 0%, 55% and 95% attack traffic, the results shows that the policing mechanism still is able to keep the maximum delay of the time-critical packets to be around 25 μs. Because of that the attack rate is so much higher than the arrival rate of the legitimate packet types, it causes the results to be similar whether the packet rate is 0.02 or 0.05 packets per μs for the non-time-critical packets.

Chapter 8
Discussion

"It's about to get a lot worse" [9]. The quote was the conclusion on a blog post that described the Leet botnet attack in 2016 section 3.5.1 and what to expect with regards to DDoS attacks in the future. According to the description by Imperva, the botnet flooded the server with around 150 million packets each second, compared to *"normal"* packet rates of less than 25 million packets each second [9]. The simulations performed earlier, was scaled down and smaller in size than this real attack, but the result, see Figure 7.5 gives an indicator on how a DDoS attack of different strengths affect the total delay of the traffic and how traffic policing can be a useful solution.

8.1 Time Budgeting before applying Traffic Policing

For some time-critical data it is crucial to arrive at its destination within a settled deadline, otherwise it may no longer be useful [111]. Therefore, even though the average delays can give some interesting information about how traffic policing can improve the average delay, it can for some real-time packets be more important to look at the maximum delay instead. This is because a series of packets could be unusable and irrelevant if a packet was to late or lost on the way. If the delay of a packet is exceeding the time constraint or if there is no more room in the queue(s) the packet could in reality be considered as lost or actually be lost [59].

In Figure 7.5 when no alien packets are in the system, the maximum delay was on average approximately $17\mu s$, see Table 7.4 (alien traffic is at 0%). Given the minimum propagation distance (80km fiber + 10m wireless) and that all nodes can cause packets to have this maximum delay, the number of nodes in the network can at most be approximately 35, as seen in the following calculation:

$$\sum_{0}^{\infty} Nodal_{Delay} \leqslant 0.599ms$$

$$\sum_{0}^{\infty} Nodes \leqslant 0.599ms \div 17 * 10^{-3}ms$$

$$\sum_{0}^{\infty} Nodes \leqslant \lfloor 35.3 \rfloor = 35$$

The total network is then consisting of 35 nodes, 80km of optical fiber cables and 10m of wireless transmission link(s). This could however be budgeted differently. Less number of nodes could allow for longer propagation distances.

8.2 Time Budgeting with Traffic Policing

By implementing a control plane policing mechanism such as traffic prioritization, the maximum delay of the time-critical packets are held close to linear with a minor growth, reaching its maximum at around 24 μs during a 95% attack, even though the attack intensity is increasing as in the previous scenarios. The results obtained after running simulations with and without attacks on the router, with the implemented control plane policing, can be seen in the lower section of Table 7.4. Figure 7.5 clearly shows that the policing mechanism can help solve some of the delay issues given that it is possible to separate/find the time-critical traffic and give them a high-priority stamp.

Without attack, the maximum delay can be around 17 μs. Assuming that all of the nodes in the network have a packet with 17 μs as the maximum delay, it is possible to have 35 such nodes with the implemented policing mechanism:

$$\sum_{0}^{\infty} Nodes \leqslant 0.599ms \div 17 * 10^{-3}ms$$

$$\sum_{0}^{\infty} Nodes \leqslant \lfloor 0.599ms \div 17 * 10^{-3}ms \rfloor$$

$$\sum_{0}^{\infty} Nodes \leqslant 35$$

As found in subsection 5.4.2, some offshore facilities are located at least 80km from shore. However, as found in section 7.3.1, the maximum distance of an optical fiber cable is around 200km with this time constraint and no other components. The network needs at least two nodes, one at each end of the propagation link, hence offshore installations located further away, is not able to use applications with these time requirements or this kind of delay-sensitivity. Although, assuming that the offshore IoT network would have one or two nodes on the offshore installation and

two or three onshore, a total of five nodes, then the total distance of additional optical fiber cable could be:

$$\sum_{0}^{\infty} Link_{Delay} \leqslant 0.599ms - 5 * 17 * 10^{-3}ms$$

$$\sum_{0}^{\infty} Link_{Delay} \leqslant 0.51ms$$

$$Distance(km) \leqslant 0.51 \div 5 \times 10^{-3}ms/km = 102km$$

which in total leaves the system with approximately 182km of optical fiber cables. Similarly, if ten routers were to be used in the network, the additional distance of optical fiber cable would be around 85km. This leaves the offshore network system with a total of between 165km (80km + 85km) and 182km (80km + 102km) of optical fiber cable depending on the amount of network nodes. This could allow several offshore installations, even those located a bit further away, to deploy and make use of time-critical and delay-sensitive (IoT) applications.

There are advantages and disadvantages with time constraints and propagation distance limits, when the use cases and applications are needed in such rural and isolated environments. In addition, in the offshore networks, the data needs to travel further than in for example industrial plant networks. At industrial plants, sensors, BSs and other fog nodes, routers and end devices are not as widespread as it realistically could be in an offshore-onshore network. Hence, the data do not have to spend as much time the propagating through physical links. If the same amount of network nodes were to be used in a smaller area, with shorter propagation links, the data packets would have a greater time margin and could potentially handle more delay than the offshore data packets, in case it was to be affected by a DDoS flooding attack in any of the nodes or links. And from the offshore packets point of view, the data packets have traveled several kilometers when reaching the onshore edge routers, hence they are more vulnerable to a potential DDoS attack, as they have spent more time on propagating between two destinations and have shorter time until they reach their limit.

8.2.1 A Network under Attack

A challenge occurs if there is more traffic in the network. In the scenarios above, the data rate is around 70 000 packets per second (of 800 000 packets per second), leaving space for more traffic. In comparison, during an intense DDoS attack that is pushing the total traffic rate close to the link's maximum, the delay is approximately $350\mu s$.

This scenario is without any traffic policing mechanisms in the router and where the alien traffic is at 95%, see Table 7.4. With traffic policing, the corresponding delay is approximately $24\mu s$.

Given a network of 5 nodes, 182km of fiber optic cables and 10m of wireless link, having one of the nodes become a victim of a DDoS attack:

No Traffic Policing

If the routers do not have traffic policing, it is reasonable, from the results, to assume that time-critical packets may have a delay of up to around $350\mu s$:

$$\sum_{0}^{\infty} Nodal_{Delay} + \sum_{0}^{\infty} Link_{Delay} = ?$$

$$4 \times 17 \times 10^{-3}ms + 1 \times 350 \times 10^{-3}ms + 182km \times 5 \times 10^{-3}ms + 0.00036ms = 1.33ms$$

which exceeds the 1ms end-to-end time limit.

With Traffic Policing

The maximum delay measured from the time-critical packets with traffic policing is around 24 μs.

$$\sum_{0}^{\infty} Nodal_{Delay} + \sum_{0}^{\infty} Link_{Delay} = ?$$

$$4 \times 17 \times 10^{-3}ms + 1 \times 24 \times 10^{-3}ms + 182km \times 5 \times 10^{-3}ms + 0.000036ms = 1.00ms$$

This shows that traffic policing can be useful to keep time-critical traffic prioritized and within the limit even during a heavy DDoS attack.

8.3 Alternative Solution

1ms is not a lot of time. In an earlier subsection 5.4.2 it was stated that Equinor also have oil and gas platforms around 300km from shore [28][29]. If it should be desirable to deploy time-critical applications on platforms located further away, control rooms could be established closer to where the applications are used and where monitoring processes and operations are carried out. This would distance the workers from the dangerous situations which was considered as a potential risk in chapter 2 and section 2.1, and the operations would be controlled and monitored from a remote, more safe location. The propagation distance for the time-critical data would be reduced, as the control room could be located closer to where the data is generated.

From a security point of view, if the time-sensitive data was only handled offshore, it could potentially improve the security, as the vulnerable devices would be harder for the attacker to both find and reach. However, the cost of establishing and placing an offshore platform for monitoring purposes, could potentially be cost inefficient, but this is not further discussed in this thesis.

8.4 Key Findings

DDoS attacks are a widely known challenge within different industrial cyber-physical systems and it will likely be challenging for offshore networks as well. It is necessary to be aware of that offshore networks are prone to DDoS attacks, if an implementation of IoT networks was to happen.

The results shows that traffic policing can be useful to keep the data flows from time-critical applications going during a intense DDoS flooding attacks. From a security point of view, it will be vital for mission-critical offshore applications to run until anyone are able to reduce the attack volume, and this way avoid any production reductions or undesired stops for as long as possible.

Some of the mitigation strategies suggested in chapter 3 and subsection 3.3.5 can be useful. However, both Deepa *et.al* [24] and Hu *et.al* [136] suggest to block the malicious packets by either blocking the port the data arrives at or by examine at the arrival rate. Blocking a port because alien traffic is detected, will also block time-critical traffic arriving at that port, and hence potentially cause damage. By comparing all the different arrival rates with expected normal rates, the router can decide to block the traffic flows that could be a threat. Ping *et.al* [87] addressed that is almost impossible to detect the attack source when IP-addresses are spoofed, but have suggested a solution that can filter out 80% of the alien traffic. That solution could potentially be helpful to reduce the attack.

However, the attack volume may come to a point where it could be necessary to have a controlled temporary reduction or shut down of the time-critical traffic flow to regain control and traffic balance in the system. If the goal is to keep the offshore IoT systems run for as long as possible, it may be necessary to consider and evaluate the criticality among the time-critical packets. Potentially could traffic with hard deadlines have a priority over traffic with firm and soft deadlines respectively. This way, the hard deadline traffic would continue on its path, whereas packets with established firm and soft deadlines could be rerouted, as they could still be useful to some degree even if they arrive after the preferred deadline [111]. Although, this would require pre-implemented system parallelism and redundancy that also could handle time-critical data sufficiently, so that traffic could arrive at its destination within a timely manner.

An alternative is to leave all time-critical M2M communication at the offshore installation, and within the safety zone, by co-locating MEC with the BS. This way, only periodical updates from such applications would leave the offshore platform and propagate to shore. However, this would most likely require that offshore use cases was to be autonomous and that they would only be remotely monitored and not controlled.

From the calculations of propagation distances based on the simulation results, not all platforms can be remotely operated and controlled because of the distances between shore and where the operations takes place, as of right now. However, use cases with less restrictions with regards to latency, could be usable on offshore installations located further away.

8.5 The Future of Time-Critical IoT Offshore

Based on the simulation results described in chapter 7, it seems possible to deploy 5G offshore with the goal of enabling time-critical applications demanding a maximum of 1ms end-to-end latency, on the offshore installations closest to shore with the current network topology. However, the margins in terms of delay in case of a DDoS attack are small.

In the pre-project from 2019 [13], which formed the basis for this project, the offshore IoT network environment was considered to be less vulnerable to some kinds of cyberattacks than in IoT networks located in urban areas. Mostly because of the physical distance from shore and hence that the network components are not as easily reached when deployed in such rural and isolated environments.

One of the main concerns was and is the rapidly increasing amount of DDoS attacks utilizing the constrained IoT devices to build botnets with the goal of harming the availability of industrial control systems and other cyber-physical systems, by flooding the links and overwhelming the network nodes and their CPUs. It is reasonable to assume that the offshore industry is no different, and hence also a potential victim of such attacks.

A mitigation strategy of DDoS attacks that is useful, for instance in the offshore industry, and that can minimize the queuing delay caused by a potential DDoS attack, is to implement traffic policing. The traffic policing can allow high priority and time-critical packets pass through the router as fast as possible, with minimal queuing delay and at the same time downgrade unknown, and potentially dangerous, traffic. The simulations performed earlier, is a simplified setup of a real-life router, where several assumptions are made. However, the results shows that if it is possible to identify time-critical traffic, it is possible to obstruct, reduce or hold back "normal" traffic to

let the delay-sensitive packets have priority. If such traffic policing mechanisms are used, the delay is kept low, even during an attack, which gives room for the traffic to propagate over longer distances of fiber cable(s) and hence making it useful for offshore platforms located even further away.

Chapter 9
Conclusion

Through the analysis and simulations performed in this thesis, the objective was to study how a control plane policing mechanism can affect DDoS attacks and to protect time-critical data. The research questions were defined as follows:

RQ1: Would it be possible to have time-critical applications offshore that is communicating with servers on shore within the required packet delay limit and could traffic policing be a suitable solution to enable this?

RQ2: To what extent does control plane policing mitigate how a DDoS attack impacts the latency of time-critical offshore IoT traffic?

From the background study it is found that there is a potential to deploy and use 5G and time-critical IoT applications in the offshore industry. The working environment offshore is considered as risky because of its isolated location, the high pressure liquid and gas, and explosion hazards, among others. In addition, people do interact with process and safety systems on a daily basis. The potential is to remotely operate offshore installations now that 5G technology will become available, to control the risk of undesired events. In the analysis it was also found that there are challenges with regards to the technology. IoT systems are vulnerable to DDoS attacks which also is a potential risk for offshore IoT systems and applications. Such attacks can affect the systems availability and is found to be a challenge especially for time-critical applications where catastrophes can be caused if the data traffic arrives at its destination too late.

Simulations shows that the offshore industry are able to deploy and use time-critical IoT applications that requires an end-to-end latency of down to 1ms. For example, a network that consists of between five and ten network nodes and a wireless propagation distance of 10m, a packet can travel between 165km and 182km in a optical fiber cable. Because of the propagation delay in the transportation link(s),

offshore facilities that are located further from shore cannot use applications that requires a maximum of 1ms end-to-end latency. However, a possible solution can be to operate these platforms from another offshore facilities, to reduce the propagation distance.

With control plane policing mechanism introduced, the results shows that if time-critical traffic is prioritized through a router, the delay is kept at a low level. This is because when a time-critical (high-priority) packet arrives at the input port, the packet is put in front of the queue and will be processed before lower priority packets. The results shows that in case of a DDoS attack, the maximum delay is increasing depending on the strength of the attack and will have a close to exponential growth. Whereas when the policing mechanism is implemented the maximum delay is close to linear with a minor increase in delay. During the strongest attack the delay of the time-critical packets were reduced from $350.08\mu s$ to $23.86\mu s$ by using the mechanism. With control plane policing introduced, the time-critical traffic can be kept close to unaffected during a DDoS flooding attack. Control plane policing mechanisms can also be used to mitigate DDoS attack traffic.

References

[1] European Telecommunications Standards Institute (ETSI). *Why Do We Need 5G?* https://www.etsi.org/technologies/5g. Accessed: 30.10.2019. 2019.

[2] NorskKommunikasjonsmyndighet (NKOM). *Frekvenskompass for mobilkommunikasjon*. Accessed: 20.05.2020. Sept. 2019. URL: https://www.nkom.no/teknisk/frekvens/frekvensstrategi/frekvenskompass/_attachment/41462?_ts=16d1f297902.

[3] Mamta Agiwal, Navrati Saxena, and Abhishek Roy. "Towards connected living: 5g enabled internet of things (iot)". In: *IETE Technical Review* 36.2 (2019), pp. 190–202.

[4] Arwa Alrawais et al. "Fog computing for the internet of things: Security and privacy issues". In: *IEEE Internet Computing* 21.2 (2017), pp. 34–42.

[5] S. S. Alwakeel and S. S. AlGhanmi. "A real time leaky bucket based admission control scheme for VoIP networks". In: *2012 International Conference on Multimedia Computing and Systems*. 2012, pp. 651–656.

[6] AB Asrar, NA Malek, and AA Sharaf. "Fog Computing for Network Slicing in 5G Networks: An Overview". In: *Journal of Telecommunication Systems and Management* 7 (2018), p. 172.

[7] S. Bashar and Z. Ding. "Admission control and resource allocation in a heterogeneous OFDMA wireless network". In: *IEEE Transactions on Wireless Communications* 8.8 (2009), pp. 4200–4210.

[8] Telia Bedrift. *Smartere Oljeplattformer*. Accessed: 17.04.2020. May 2018. URL: https://www.telia.no/magasinet/smartere-oljeplattformer-med-ny-teknologi/.

[9] Dima Bekerman and Avishay Zawoznik. *650Gbps DDoS Attack from the Leet Botnet*. Accessed: 09.05.2020. 2016. URL: https://www.imperva.com/blog/650gbps-ddos-attack-leet-botnet/.

[10] Jim Boyce and Rob Tidrow. *Windows 8 Bible*. Vol. 785. John Wiley & Sons, 2012, p. 1006.

[11] Graham Britwistle. *DEMOS - a system for Discrete Event Modelling on Simula*. University of Sheffield, 2003.

[12] Gabriel Brown. "Ultra-reliable low-latency 5G for industrial automation". In: *Heavy Reading white paper for Qualcomm* (2018).

[13] Hanne Malmin Bruleite. *Identifying Mission Critical IoT Vulnerabilities in the Rural Offshore Environment*. Project report in TTM4502. Department of Information Security, Communication Technology, NTNU - Norwegian University of Science, and Technology, Dec. 2019.

[14] Dhara Buch and Devesh Jinwala. "Denial of Service Attacks in Wireless Sensor Networks". In: Dec. 2010.

[15] Patrik Carlsson et al. *Delay Performance in IP Routers*. http://www.diva-portal.org/smash/get/diva2:837930/FULLTEXT01.pdf. Accessed: 15.06.2020.

[16] G. Chen et al. "Joint resource allocation and admission control mechanism in software defined mobile networks". In: *China Communications* 16.5 (2019), pp. 33–45.

[17] He Chen et al. "Ultra-reliable low latency cellular networks: Use cases, challenges and approaches". In: *IEEE Communications Magazine* 56.12 (2018), pp. 119–125.

[18] Markus Christen, Bert Gordijn, and Michele Loi. *The Ethics of Cybersecurity*. Springer, 2020.

[19] Cisco. *What Are the Most Common Cyber Attacks?* Accessed: 17.04.2020. URL: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks.

[20] Cloudflare. Accessed: 08.05.2020. 2018. URL: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/.

[21] Cloudflare. Accessed: 08.05.2020. URL: https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/.

[22] Sam Cook. *DDoS attack statistics and facts for 2018-2019*. Accessed: 17.04.2020. Aug. 2019. URL: https://www.comparitech.com/blog/information-security/ddos-statistics-facts/.

[23] Casey Crane. *The Top 15 DDoS Statistics You Should Know in 2020*. Accessed: 07.05.2020. 2019. URL: https://cybersecurityventures.com/the-15-top-ddos-statistics-you-should-know-in-2020/.

[24] V. Deepa, K. M. Sudar, and P. Deepalakshmi. "Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques". In: *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)*. 2018, pp. 299–303.

[25] Google Draw. *Draw.io*. URL: https://app.diagrams.net/.

[26] Schahram Dustdar, Cosmin Avasalcai, and Ilir Murturi. "Edge and Fog Computing: Vision and Research Challenges". In: *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*. IEEE. 2019, pp. 96–9609.

[27] M. S. Elbamby et al. "Toward Low-Latency and Ultra-Reliable Virtual Reality". In: *IEEE Network* 32.2 (2018), pp. 78–84.

[28] Equinor. *Field and Platforms*. https://www.equinor.com/en/what-we-do/fields-and-platforms.html. Accessed: 18.11.2019. 2019.

[29] Equinor. *Kjente og ukjente oljerekorder*. Accessed: 09.06.2020. 2020. URL: https://www.equinor.com/no/magazine/industry-world-records.html.

[30] D. Fang, Y. Qian, and R. Q. Hu. "Security for 5G Mobile Wireless Networks". In: *IEEE Access* 6 (2018), pp. 4850–4874.

[31] Michael Frey et al. "Security for the Industrial IoT: The Case for Information-Centric Networking". In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. IEEE. 2019, pp. 424–429.

[32] Jianlei Gao et al. "Research about DoS Attack against ICPS". In: *Sensors* 19.7 (2019), p. 1542.

[33] Zeljko Gavric and Dejan Simic. "Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks". In: *Ingeniería e Investigación* 38.1 (2018), pp. 130–138.

[34] Sunil Ghildiyal, Anupam Semwal, and Surender Kumar. "Enhancing Security of Internet of Things (IoT) using Fog Computing". In: *Available at SSRN 3402922* (2019).

[35] Nipuni Uthpala Ginige et al. "Admission Control in 5G Networks for the Coexistence of eMBB-URLLC Users". In: *arXiv preprint arXiv:1910.13855* (2019).

[36] GitHub. Accessed: 08.05.2020. 2020. URL: https://github.com/.

[37] Paul Goransson and Chuck Black. *Software defined networks: a comprehensive approach*. Morgan Kaufmann, 2016.

[38] Naveen Goud. *DDoS Cyber Attack on Iran's Internet and Telecom sector*. Accessed: 08.05.2020. 2020. URL: https://www.cybersecurity-insiders.com/ddos-cyber-attack-on-irans-internet-and-telecom-sector/.

[39] S. Gqibani, N. Clarke, and A. L. Nel. "Motivation for developing a qualitative methodological basis for the analysis of historical curriculum changes". In: *2016 IEEE Global Engineering Education Conference (EDUCON)*. 2016, pp. 637–644.

[40] Tibor Gyires. *Algorithms of Informatics, Chapter 5: Network Simulation*. Accessed: 08.06.2020. 2007. URL: https://bit.ly/30oUe1L.

[41] Mohammad Hassan et al. “Increasing the trustworthiness in the Industrial IoT Networks through a reliable cyber-attack detection model”. In: *IEEE Transactions on Industrial Informatics* (2020).

[42] Scott Hilton. *DYN Analysis Summary of Friday October 21 Attack*. Accessed: 09.05.2020. URL: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

[43] Jan Rune Holmevik. *Compiling Simula*. Accessed: 04.06.2020. Jan. 1993. URL: http://staff.um.edu.mt/jskl1/simula.html.

[44] W. Hurst, N. Shone, and Q. Monnet. “Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures”. In: *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*. 2015, pp. 1697–1702.

[45] Talal Husseini. *Most Dangerous Offshore Jobs*. Accessed 23.10.2019. 2018. URL: https://www.offshore-technology.com/features/most-dangerous-offshore-jobs/.

[46] Hydro. *Cyberangrep på Hydro*. Accessed: 21.05.2020. 2019. URL: https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/.

[47] Dordi Høivik et al. “What is most important for safety climate: The company belonging or the local working environment?–A study from the Norwegian offshore industry”. In: *Safety science* 47.10 (2009), pp. 1324–1331.

[48] Imperva. *DDoS Attacks*. Accessed: 07.05.2020. URL: https://www.imperva.com/learn/application-security/ddos-attacks/.

[49] Imperva. *Smurf Attack DDoS*. Accessed: 07.05.2020. URL: https://www.imperva.com/learn/application-security/smurf-attack-ddos/.

[50] Texas Instruments Incorporated. *Small Cells, Big Impact: Designing Power Solutions for 5G Applications*. http://www.ti.com/lit/wp/slyy166/slyy166.pdf. Accessed: 15.11.2019. 2019.

[51] Menglan Jiang, Massimo Condoluci, and Toktam Mahmoodi. “Network slicing management & prioritization in 5G mobile systems”. In: *European Wireless 2016; 22th European Wireless Conference*. VDE. 2016, pp. 1–6.

[52] A. Kammoun et al. “Admission Control Algorithm for Network Slicing Management in SDN-NFV Environment”. In: *2018 6th International Conference on Multimedia Computing and Systems (ICMCS)*. 2018, pp. 1–6.

[53] T Kavitha and D Sridharan. “Security vulnerabilities in wireless sensor networks: A survey”. In: *Journal of information Assurance and Security* 5.1 (2010), pp. 31–44.

[54] J. C. Knight. “Safety critical systems: challenges and directions”. In: *Proceedings of the 24th International Conference on Software Engineering. ICSE 2002*. May 2002, pp. 547–550.

[55] S. S. Kolahi et al. “Performance comparison of defense mechanisms against TCP SYN flood DDoS attack”. In: *2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. 2014, pp. 143–147.

[56] Sam Kottler. *February 28th DDoS Incident Report*. Accessed: 08.05.2020. 2018. URL: https://github.blog/2018-03-01-ddos-incident-report/.

[57] Mohit Kumar. *DDoS Attack Takes Down Central Heating System Amidst Winter In Finland*. Accessed: 09.05.2020. 2016. URL: https://thehackernews.com/2016/11/heating-system-hacked.html.

[58] S. Kumar and M. S. Gaur. “Handoff Prioritization to Manage Call Admission Control in Mobile Multimedia Networks for Healthcare”. In: *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. 2019, pp. 1–7.

[59] James F. Kurose and Keith W. Ross. *Computer Networking: A Top-Down Approach*. sixth. Pearson, 2013.

[60] A. Lazzez and N. Boudriga. “Admission Control in OBS Networks: A Real Time QoS-Oriented Approach”. In: *2007 IEEE International Conference on Signal Processing and Communications*. 2007, pp. 931–934.

[61] Min Xiang Lee. *The Art of Decision Making: Machines vs Humans*. Accessed: 20.05.2020. Sept. 2018. URL: https://medium.com/@minxianglee/the-art-of-decision-making-machines-vs-humans-149ec02eb0fd.

[62] J. P. Lehoczky. “Scheduling communication networks carrying real-time traffic”. In: *Proceedings 19th IEEE Real-Time Systems Symposium (Cat. No.98CB36279)*. 1998, pp. 470–479.

[63] Oleksandr Lemeshko et al. “Quality of Service Protection Scheme under Fast ReRoute and Traffic Policing Based on Tensor Model of Multiservice Network”. In: *2019 International Conference on Information and Digital Technologies (IDT)*. IEEE. 2019, pp. 288–295.

[64] Dave Lewis. *The DDoS Attack Against DYN One Year Later*. Accessed: 09.05.2020. 2017. URL: https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/#185cc3db1ae9.

[65] R. Li and B. Wu. “Early detection of DDoS based on φ-entropy in SDN networks”. In: *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*. Vol. 1. 2020, pp. 731–735.

[66] Magdi S Mahmoud, Mutaz M Hamdan, and Uthman A Baroudi. "Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges". In: *Neurocomputing* 338 (2019), pp. 101–115.

[67] Rwan Mahmoud et al. "Internet of things (IoT) security: Current status, challenges and prospective measures". In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE. 2015, pp. 336–341.

[68] Rwan Mahmoud et al. "Internet of things (IoT) security: Current status, challenges and prospective measures". In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE. 2015, pp. 336–341.

[69] Hilde Martinsen. *Bruk av IKT i offentlig sektor*. Accessed: 17.04.2020. Feb. 2020. URL: https://blogg.telenor.no/tjenestenektangrep-angrepet-som-kan-lamme-nettjenesten-din-totalt.

[70] Jamie Medrano. Accessed: 08.05.2020. 2011. URL: https://corporate.tuenti.com/en/dev/blog/using-udp-in-memcached.

[71] Memcached. Accessed: 08.05.2020. URL: https://memcached.org/.

[72] K Mills et al. "Study of Proposed Internet Congestion-Control Mechanisms". In: *NIST Special Publication* 500 (2010), p. 282.

[73] Sigrid Moe and Cecilie Storbråten Gjendem. *Evry-kunder ble rammet av 88 store Ddos-angrep i fjor*. Accessed: 20.05.2020. Jan. 2016. URL: https://e24.no/teknologi/i/3J1Jq0/evry-kunder-ble-rammet-av-88-store-ddos-angrep-i-fjor.

[74] R. Mohammadi, R. Javidan, and M. Conti. "SLICOTS: An SDN-Based Lightweight Countermeasure for TCP SYN Flooding Attacks". In: *IEEE Transactions on Network and Service Management* 14.2 (2017), pp. 487–497.

[75] N. A. Mohammed, A. M. Mansoor, and R. B. Ahmad. "Mission-Critical Machine-Type Communication: An Overview and Perspectives Towards 5G". In: *IEEE Access* 7 (2019), pp. 127198–127216. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2894263.

[76] S. M. Mousavi and M. St-Hilaire. "Early detection of DDoS attacks against SDN controllers". In: *2015 International Conference on Computing, Networking and Communications (ICNC)*. 2015, pp. 77–81.

[77] Nataliia Neshenko et al. "Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations". In: *IEEE Communications Surveys & Tutorials* (2019).

[78] NetScout. *ICMP Flood*. Accessed: 07.05.2020. URL: https://www.netscout.com/what-is-ddos/icmp-flood.

[79] NetScout. *UDP Flood*. Accessed: 07.05.2020. URL: https://www.netscout.com/what-is-ddos/udp-flood.

[80] Metaswitch Networks. *MPLS in Optical Networks*. Accessed: 17.04.2020. Oct. 2001. URL: http://www.olddog.co.uk/opticalmpls2-2.pdf.

[81] M. Neukirchner et al. "Contract-based dynamic task management for mixed-criticality systems". In: *2011 6th IEEE International Symposium on Industrial and Embedded Systems*. 2011, pp. 18–27.

[82] NextGov. *Cyberattack Leaves Finnish Apartment Dwellers in the Cold*. Accessed: 09.05.2020. 2016. URL: https://www.nextgov.com/cybersecurity/2016/11/denial-service-attack-cyberattack-leaves-finnish/143997/.

[83] Jianbing Ni, Xiaodong Lin, and Xuemin Sherman Shen. "Toward Edge-Assisted Internet of Things: From Security and Efficiency Perspectives". In: *IEEE Network* 33.2 (2019), pp. 50–57.

[84] Amy Nordrum, Kristen Clark, and IEEE Spectrum Staff. *Everything You Need to Know About 5G*. Accessed: 20.05.2020. Jan. 2017. URL: https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g.

[85] Universitet i Oslo. *Install Simula*. Accessed: 04.06.2020. Feb. 2020. URL: http://simula67.at.ifi.uio.no/cim.shtml.

[86] Evelina Pencheva et al. "5G System Support for Mission Critical Communications". In: (2019).

[87] S. Y. Ping and Lee Moonchuen. "IP traceback marking scheme based packets filtering mechanism". In: *2004 IEEE International Workshop on IP Operations and Management*. 2004, pp. 253–260.

[88] Petar Popovski et al. "5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view". In: *IEEE Access* 6 (2018), pp. 55765–55779.

[89] Petar Popovski et al. "Wireless access in ultra-reliable low-latency communication (URLLC)". In: *IEEE Transactions on Communications* 67.8 (2019), pp. 5783–5801.

[90] Ramjee Prasad and Vandana Rohokale. *Cyber Security: The Lifeline of Information and Communication Technology*. Springer, 2020.

[91] Ramjee Prasad and Vandana Rohokale. "Internet of Things (IoT) and Machine to Machine (M2M) Communication". In: *Cyber Security: The Lifeline of Information and Communication Technology*. Springer, 2020, pp. 125–141.

[92] Queensland University of Technology QUT. *Writing a literature review*. Accessed: 02.05.2020. URL: https://www.citewrite.qut.edu.au/write/litreview.jsp.

[93] Sri Ravipati. *University Hackers Attacked 5,000 IoT Devices on Campus*. Accessed: 09.05.2020. 2017. URL: https://campustechnology.com/articles/2017/02/13/university-hackers-attacked-5000-iot-devices-on-campus.aspx.

[94] Norwegian Government - Regjeringen. *Cyber Security Strategy Norway*. Accessed: 20.12.2019. Jan. 2019. URL: https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber%5C_security%5C_strategy%5C_norway.pdf.

[95] Paul Roberts. *Let's Get Cyberphysical: Internet Attack shuts off the Heat in Finland*. Accessed: 09.05.2020. 2016. URL: https://securityledger.com/2016/11/lets-get-cyberphysical-ddos-attack-halts-heating-in-finland/.

[96] Raquel Roman. *What's The Difference Between Arrival Rates and Inter Arrival Times?* Accessed: 20.05.2020. June 2012. URL: https://blog.simul8.com/simul8-tip-whats-the-difference-between-arrival-rates-and-inter-arrival-times/.

[97] Jan Morten Ruud et al. *Nexia Statnett Submarine Fiber Evaluation*. Accessed: 08.06.2020. 2015. URL: https://www.statnett.no/globalassets/her-er-vare-prosjekter/mellomlandsforbindelser/north-sea-link/nexia-fiber-evaluation-report.pdf.

[98] S. S. Sahu, P. Priyadarshini, and S. Bilgaiyan. "Curbing Distributed Denial of Service attack by traffic filtering in Wireless Sensor Network". In: *Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*. 2014, pp. 1–6.

[99] Anam Sajid, Haider Abbas, and Kashif Saleem. "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges". In: *IEEE Access* 4 (2016), pp. 1375–1384.

[100] Spyridon Samonas and David Coss. "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security." In: *Journal of Information System Security* 10.3 (2014).

[101] Hilde Sandhåland, Helle Oltedal, and Jarle Eid. "Situation awareness in bridge operations–A study of collisions between attendant vessels and offshore facilities in the North Sea". In: *Safety science* 79 (2015), pp. 277–285.

[102] Tara Seals. *Leet IoT Botnet Bursts on the Scene with Massive DDoS Attack*. Accessed: 09.05.2020. 2017. URL: https://www.infosecurity-magazine.com/news/leet-iot-botnet-bursts-on-the-scene/.

[103] Cisco Security. *Control Plane Policing Implementation Best Practices*. Accessed: 25.05.2020. URL: https://tools.cisco.com/security/center/resources/copp_best_practices.

[104] Red 5 Security. Accessed: 09.05.2020. URL: http://www.red5security.com/news_media_34_3921121624.pdf.

[105] L. Seno et al. “Bandwidth Management for Soft Real-Time Control Applications in Industrial Wireless Networks”. In: *IEEE Transactions on Industrial Informatics* 13.5 (2017), pp. 2484–2495.

[106] Statistisk sentralbyrå. *Bruk av IKT i offentlig sektor*. Accessed: 17.04.2020. Apr. 2019. URL: https://www.ssb.no/teknologi-og-innovasjon/statistikker/iktbruks.

[107] Furrakh Shahzad, Maruf Pasha, and Arslan Ahmad. “A survey of active attacks on wireless sensor networks and their countermeasures”. In: *arXiv preprint arXiv:1702.07136* (2017).

[108] S. Shakeri, S. Parsaeefard, and M. Derakhshani. “Proactive admission control and dynamic resource management in SDN-based virtualized networks”. In: *2017 8th International Conference on the Network of the Future (NOF)*. 2017, pp. 46–51.

[109] Nirmal Sharma. *DNS or other Services works on both TCP and UDP*. Accessed: 09.05.2020. 2017. URL: https://support.microsoft.com/en-us/help/556000.

[110] S. Shim et al. “Destination Address Monitoring Scheme for Detecting DDoS Attack in Centralized Control Network”. In: *2006 Asia-Pacific Conference on Communications*. 2006, pp. 1–5.

[111] Kang G Shin and Parameswaran Ramanathan. “Real-time computing: A new discipline of computer science and engineering”. In: *Proceedings of the IEEE* 82.1 (1994), pp. 6–24.

[112] A. Shoeb and T. Chithralekha. “Resource management of switches and Controller during saturation time to avoid DDoS in SDN”. In: *2016 IEEE International Conference on Engineering and Technology (ICETECH)*. 2016, pp. 152–157.

[113] Andrew Shoemaker. *How to Identify a Mirai-Style DDoS Attack*. Accessed: 09.05.2020. 2017. URL: https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/.

[114] R. Simon and T. Znati. “A probabilistic analysis of admission control policies for deadline-driven service disciplines”. In: *Proceedings 31st Annual Simulation Symposium*. 1998, pp. 110–117.

[115] Jaroslav Sklenar. *Introduction to OOP in Simula*. Accessed: 04.06.2020. 1997. URL: http://staff.um.edu.mt/jskl1/talk.html#History_67.

[116] SNL Store Norske Leksikon. *Reaksjonstid*. Accessed: 13.04.2020. Apr. 2020. URL: https://sml.snl.no/reaksjonstid.

[117] Tampnet. *Fibre Optics*. Accessed: 17.04.2020. URL: https://www.tampnet.com/solutions/fibre-optics/.

[118] Tampnet. *Tampnet*. Accessed: 17.04.2020. URL: https://www.tampnet.com/.

[119] Tampnet. *Tampnet in the North Sea*. https://www.tampnet.com/north-sea/. Accessed: 17.04.2020. 2019.

[120] Tampnet. *Usecase Low Latency Offshore*. PowerPoint Presentation from Tampnet. Accessed: 01.09.2019. Aug. 2019.

[121] Telenor. *Network slicing: realising the benefits of 5G by tailored use of network capabilities*. Accessed: 12.04.2020. URL: https://www.telenor.com/media/public-policy/capturing-the-societal-benefits-of-5g/network-slicing-realising-the-benefits-of-5g-by-tailored-use-of-network-capabilities/.

[122] Stephane Teral. "5G best choice architecture". In: *IHS Markit Technology* (2019).

[123] IEEE Design & Test. *Call for Contributions Special Issue on Time-Critical Systems Design*. Accessed: 20.05.2020. 2017. URL: https://www.comp.nus.edu.sg/~tulika/special-issue-time-critical.pdf.

[124] F. Tonini et al. "A Traffic Pattern Adaptive Mechanism to Bound Packet Delay and Delay Variation in 5G Fronthaul". In: *2019 European Conference on Networks and Communications (EuCNC)*. 2019, pp. 416–420.

[125] Steven J. Vaughan-Nichols. Accessed: 08.05.2020. 2018. URL: https://www.zdnet.com/article/memcached-ddos-the-biggest-baddest-denial-of-service-attacker-yet/.

[126] Olesya Voitovych et al. "Investigation of simple Denial-of-Service attacks". In: *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*. IEEE. 2016, pp. 145–148.

[127] Y. Wang et al. "SGS: Safe-Guard Scheme for Protecting Control Plane Against DDoS Attacks in Software-Defined Networking". In: *IEEE Access* 7 (2019), pp. 34699–34710.

[128] Steve Weisman. *What are Denial of Service (DoS) attacks? DoS attacks explained*. Accessed 17.04.2020. Feb. 2020. URL: https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html.

[129] Steve Weisman. *What is a distributed denial of service attack (DDoS) and what can you do about them?* Accessed 18.04.2020. URL: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html.

[130] Paul S Wooley. "Identifying cloud computing security risks". In: (2011).

[131] Nicky Woolf. *DDoS attack that disrupted internet was largest of its kind in history, experts say*. Accessed: 09.05.2020. 2016. URL: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[132] Jacob Wurm et al. “Security analysis on consumer and industrial IoT devices”. In: *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE. 2016, pp. 519–524.

[133] Fengman Xu et al. *Traffic policing for MPLS-based network*. US Patent 9,059,912. June 2015.

[134] S. K. Yadav, P. Suguna, and R. L. Velusamy. “Entropy based mitigation of Distributed-Denial-of-Service (DDoS) attack on Control Plane in Software-Defined-Network (SDN)”. In: *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. 2019, pp. 1–7.

[135] Yan Jiangzhou and Liu Zengji. “Resource allocation and admission control based on flow congestion probability in MPLS networks”. In: *2009 11th International Conference on Advanced Communication Technology*. Vol. 01. 2009, pp. 694–697.

[136] Yen-Hung Hu, Hongsik Choi, and Hyeong-Ah Choi. “Packet filtering to defend flooding-based DDoS attacks [Internet denial-of-service attacks]”. In: *2004 IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communications*. 2004, pp. 39–42.

[137] Lei Zhang, Guodong Zhao, and Muhammad Ali Imran. “Internet of Things and Sensors Networks in 5G Wireless Communications”. In: (2020).

[138] Qi Zhang and Frank HP Fitzek. “Mission critical IoT communication in 5G”. In: *Future Access Enablers of Ubiquitous and Intelligent Infrastructures*. Springer. 2015, pp. 35–41.

[139] S. Zhang. “An Overview of Network Slicing for 5G”. In: *IEEE Wireless Communications* 26.3 (2019), pp. 111–117.

Hanne Malmin Bruleite

How a Control Plane Policed DDoS Attack Impacts the Latency of Time-Critical Offshore IoT Traffic

NTNU
Norwegian University of
Science and Technology