
# PERFORMANCE OF QUEUE MANAGEMENT ALGORITHM INLTE NETWORK UNDER DDOS ATTACKS

**2022**
**MASTER THESIS**
**COMPUTER ENGINEERING**

**Aden ALI SAID**

**Thesis Advisor**
**Assist.Prof.Dr. Zafer ALBAYRAK**

# PERFORMANCE OF QUEUE MANAGEMENT ALGORTHIM IN LTE NETWORK UNDER DDOS ATTACKS

**Aden ALI SAID**

**T.C.**

**Karabuk University**

**Institute of Graduate Programs**

**Department of Computer Engineering**

**Prepared as Master Thesis**

**Thesis Advisor**

**Assist.Prof.Dr.  Zafer ALBAYRAK**

**KARABUK**

**January 2022**

I certify that in my opinion the thesis submitted by Aden ALI SAID titled "PERFORMANCE OF QUEUE MANAGEMENT ALGORITHM IN LTE NETWORK UNDER DDOS ATTACKS" is fully adequate in scope and in quality as a thesis for the degree of Master of Science.

Assist.Prof.Dr. Zafer ALBAYRAK .....
Thesis Advisor, Department of Computer Engineering

This thesis is accepted by the examining committee with a unanimous vote in the Department of Computer Engineering as a Master of Science thesis. January 7, 2022

| Examining Committee Members (Institutions) | Signature |
|---|---|
| Chairman : Prof.Dr. Ahmet ZENGİN (SUBU) | ..... |
| Member : Assist.Prof.Dr. Muhammet ÇAKMAK (KBÜ) | ..... |
| Member : Assist.Prof.Dr. Zafer ALBAYRAK (SUBU) | ..... |

The degree of Master of Science by the thesis submitted is approved by the Administrative Board of the Institute of Graduate Programs, Karabuk University.

Prof. Dr. Hasan SOLMAZ .....
Director of the Institute of Graduate Programs

*"I declare that all the information within this thesis has been gathered and presented in accordance with academic regulations and ethical principles and I have according to the requirements of these regulations and principles cited all those which do not originate in this work as well."*

Aden ALI SAID

## ABSTRACT

**M. Sc. Thesis**

**PERFORMANCE OF QUEUE MANAGEMENT ALGORITHM IN LTE NETWORK UNDER DDOS ATTACKS**

**Aden ALI SAID**

**Karabük University**
**Institute of Graduate Programs**
**The Department of Computer Engineering**

**Thesis Advisor:**
**Assist. Prof. Dr. Zafer ALBAYRAK**
**January 2022, 46 pages**

Cellular networks are rapidly evolving to meet the ever-increasing need for data speeds and to offer more services to mobile users everywhere. The fourth generation Long Term Evolution (LTE) network makes a significant contribution to improving the efficiency of cellular networks.

Increasing demands on existing cellular networks cause an increase in mobile traffic. This traffic is mainly generated by users equipped with smartphones, tablets and other mobile devices. LTE networks are trying to adapt to this ever-increasing number of mobile users and to offer them a higher quality service.

One of the most critical considerations for cellular network operators is whether their networks have efficient mechanisms and can manage them effectively to ensure optimal performance. One of the important elements that endanger network security

in cellular networks is Distributed Denial of Service (DDoS) attacks. These attacks cause many problems such as disabling the network, causing it to work below its capacity, disconnecting and dropping the user from the network. Active queue management algorithms (AQM) working in the Radio link control (RLC) layer of the LTE network can predict congestion, provide solutions against possible network attacks, and effectively solve the network congestion problem by reducing the transmission packet rate. The performance of AQM is directly affected by parameters such as end-to-end transfer rate, end-to-end delay, packet delivery rate and fairness index.

In this thesis, the performance of queue management algorithms such as RED, CoDel, PIE, pFIFO and Drop-Tail operating in the RLC layer of the cellular LTE network were compared in terms of end-to-end transfer rate, delay, packet delivery rate and fairness index values under DDoS attacks. The CoDel algorithm produced a better result than RED, PIE, pFIFO and DropTail algorithms, with the mechanism of early detection of packet drops.

**Key Words :** Ns-3 simulation, DDoS attacks, LTE network, Queue management algorithms.

**Science Code :** 92407

# ÖZET

**Yüksek Lisans Tezi**

**DDOS SALDIRILARINDA LTE AĞINDA KUYRUK YÖNETİMİ ALGORİTMASININ İNCELENMESİ**

**Aden ALI SAID**

**Karabük Üniversitesi**
**Lisansüstü Eğitim Enstitüsü**
**Bilgisayar Mühendisliği Anabilim Dalı**

**Tez Danışmanı:**
**Dr. Öğr. Üyesi Zafer ALBAYRAK**
**Ocak 2022, 46 sayfa**

Hücresel ağlar, sürekli artan veri hızı ihtiyacını karşılamak ve mobil kullanıcılara her yerde daha fazla servis hizmeti sunmak için hızla dönüşmektedir. Dördüncü nesil Uzun Vadeli Evrim (LTE) ağı, hücresel ağların verimliliğin artırılmasına önemli bir katkı sunmaktadır.

Mevcut hücresel ağlar üzerinde artan talepler, mobil trafiğin artmasına neden olmaktadır. Bu trafik temel olarak akıllı telefonlar, tabletler ve diğer mobil cihazlarla donatılmış kullanıcılar tarafından oluşturulur. LTE ağları, sürekli artan bu mobil kullanıcı sayısına uyum sağlamaya ve onlara daha kaliteli bir hizmet sunmaya çalışmaktadır.

Hücresel ağ operatörleri için en kritik hususlardan biri, ağlarının en iyi performansı sağlamak için verimli mekanizmalara sahip olup olmadıkları ve bunları etkin bir

şekilde yönetip yönetemeyecekleridir. Hücresel ağlarda ağ güvenliğini tehlikeye atan önemli unsurlardan bir tanesi Dağıtılmış Hizmet Reddi (DDoS) saldırılarıdır. Bu saldırılar ağı devre dışı bırakma, kapasitesinin altında çalışmaya sebep olma, bağlantı kopması ve kullanıcının ağdan düşürülmesi gibi birçok soruna neden olmaktadır. LTE ağının Radyo bağlantı kontrolü (RLC) katmanında çalışan aktif kuyruk yönetim algoritmaları (AQM) tıkanıklığı önceden tahmin edebilmekte, muhtemel ağ saldırılarına karşı çözüm üretebilmekte ve iletim paket hızını düşürerek ağ tıkanıklığı sorununu etkin bir şekilde çözebilmektedir. AQM' nin performansı, uçtan uca aktarım hızı, uçtan uca gecikme, paket teslim oranı ve adalet indeksi gibi parametrelerden doğrudan etkilenir.

Bu tezde, hücresel LTE ağının RLC katmanında çalışan RED, CoDel, PIE, pFIFO ve Drop-Tail gibi kuyruk yönetimi algoritmalarının performansını DDoS saldırıları altında uçtan uca aktarım hızı, gecikme, paket teslim oranı ve adalet indeks değerleri açısından karşılaştırılmıştır. CoDel paket düşüşlerini erken tespit etme mekanizması ile sırasıyla RED, PIE, pFIFO ve Drop-Tail algoritmalarına göre daha iyi bir sonuç üretmiştir.

**Anahtar Kelimeler :** Ns-3 simülasyonu, DDoS saldırıları, LTE ağı, Kuyruk yönetimi algoritmaları.

**Bilim Kodu** **:** 92407

## ACKNOWLEDGMENT

I extend my thanks and gratitude to:

My distinguished university "Karabuk", the teaching staff, and Computer Engineering Department for providing all possibilities and means to bring this thesis to light.

Assist. Prof. Dr. Zafer ALBAYRAK, Associate Professor in the Department of Computer Engineering at Karabuk University "my thesis supervisor" for all his time, effort, and knowledge for the sake of my education, and for all his help to make my thesis successful as you see today.

**CONTENTS**

**Page**

**Page**

**Page**

## LIST OF FIGURES

**Page**

## LIST OF TABLES

**Page**

## INDEX OF ICONS AND ABBREVIATIONS

ICONS

*avg* : Average Queue size

*Minth* : Minimum threshold value

*Maxth* : Maximum threshold value

q : Queue size

ABBREVIATIONS

| | | |
|---|---|---|
| *AQM* | : | Active Queue Managements |
| *LTE* | : | Long Term Evolution |
| *1G* | : | 1. Generation |
| *2G* | : | 2. Generation |
| *3G* | : | 3. Generation |
| *4G* | : | 4. Generation |
| *DoS* | : | Denial of Service |
| *DDoS* | : | Distributed Denial of Service |
| *RED* | : | Random Early Detection |
| *PIE* | : | Proportional Integral Controller Enhanced |
| *pFIFO* | : | Priority First In First Out |
| *CoDel* | : | Controlled Delay |
| *PDF* | : | Packet Delivery File |
| *C&C* | : | Control & Command |
| *RLC* | : | Radio Link Control |
| *RRC* | : | Radio Resource Control |
| *RNC* | : | Radio Network Control |
| *MAC* | : | Media Access Control |
| *AMPS* | : | Analog Mobile Phone Systems |

| | | |
|---|---|---|
| *E-NodeB* | : | Enhanced Node-B |
| *EPC* | : | Evolved Packet Core |
| *EPS* | : | Evolved Packet System |
| *PDCP* | : | Packet Data Convergence Protocol |
| *PCRF* | : | Policy Control Rules Function |
| *P-GW* | : | Packet Data Network Gateway |
| *QoS* | : | Quality of Service |
| *KNN* | : | K-Nearest Neighbor |
| *UDP* | : | User Datagram Protocol |
| *TCP* | : | Transmission Control Protocol |
| *UE* | : | Users Equipment |
| *UMTS* | : | Universal Mobile Telecommunications System |
| *WiMAX* | : | Worldwide Interoperability for Microwave Access |
| *VoIP* | : | Voice over IP |
| *E-UTRAN* | : | Evolved-UTRAN |
| *GPRS* | : | General Packet Radio Service |
| *GSM* | : | Global System for Mobile communications |
| *IP* | : | Internet Protocols |

# PART 1

# INTRODUCTION

## 1.1 OVERVIEW

Currently, cellular networks deliver most of the internet content. Cellular networks are required for accessing and controlling high-quality audio, video, data downloads, cloud-based apps, autonomous vehicles, and smart home management. The use of resources in cellular systems has become increasingly important as the consumption area of cellular systems has expanded, the number of internet users has rapidly increased, and the usage of mobile internet has also increased. Cellular system operators are creating network hardware, and researchers are exploring new methods to improve the efficiency of cellular network systems and satisfy the expanding needs of the mobile Internet [1].

For several years, the rise of smartphone networks has continued to accelerate. Various generations (1G, 2G, 3G, 4G, and now 5G, which is being deployed) have developed and have seen incredible evolution, providing an excellent throughput that is not decelerating, an increasingly wide bandwidth, and the number of users that can be maintained is one of the benefits of such bandwidth [2].

The 1st generation networks (also called 1G) were integrated into the telecommunications network in the 80s. These systems were, however, abandoned a few years ago, giving way to the second generation, called 2G, launched in 1991. Still active today. We can distinguish two other types of generations within the second: the 2.5 and the 2.75. The main standard for using 2G is GSM. Unlike 1G, the second generation of standards allows access to various services, such as the use of WAP to access the Internet. They said that the 3rd generation, known as 3G, allows high speeds

for internet access and data transfer [3]. Regarding the new generation of 4G (LTE), deployed so far only by a few countries, it allows very high speed, lower latency, and many other services that we will see later in the next chapter. With 5G, it will continue to develop sectors including IoT, smart homes, autonomous cars, high-resolution and high-speed data transfer, virtual and increased reality, Industry 4.0, and remote surgery apps [4].

## 1.2 PURPOSE OF THE STUDY

The major goal of this thesis is to control congested traffic management in order to reduce packet loss and transmission delay. This study analyses and compares different active queue management algorithms such as RED, CoDel, PIE, DropTail, and pFIFO according to the number of botnets. The simulation results are given in terms of delay, end-to-end throughput, pdf, and fairness index. This study aims to determine the most suitable algorithm to improve the performance of the active queue management algorithm system operating at the RLC layer to relieve congestion in the LTE network.

## 1.3 LITERATURE REVIEW

The works presented in the literature on the examination of queue management algorithms in the LTE network under DDoS attack are reviewed in this part. A summary analysis of the problem is performed. The work of the literature and the methods used are presented. Thus, a short analysis of this work is performed.

J. Henrydoss et al. identified a few security problems in the structure of the LTE mobile network technology in [5]. A method based on ECN has been proposed to minimize congestion at the diameter interface in response to this issue. The suggested approach is investigated, and the reduction of unnecessary dropped packets is verified using the NS2 network simulation software. The quality of service of the diameter transmission interface would be improved.

W. Wei et al. examine the impact of DDoS on ad hoc networks in [6]. They used three different forms of traditional queue management algorithms: RED, Drop-Tail, and

REM. The algorithms are evaluated in an ad hoc network environment using the NS2 network simulation software under DDoS attacks. To evaluate and examine the defensive capabilities of various algorithms. As a result, Drop-Tail algorithms perform worse in small to medium-scale DDoS attacks than REM and RED Active Queue Management (AQM) algorithms. Hence, during large-scale DDoS attacks, these algorithms have limited defensive capabilities.

The author agrees in [7], to create queue management algorithms in LTE cellular networks in order to defend against DDoS attacks. In terms of packet delay, bandwidth usage, and packet dropping, the queue management algorithms perform highly. The NS-3 network simulator is utilized in this paper to investigate the active queue management technique using the LTE model. The RED algorithm, which uses probability and cut-off approaches, can be used to evaluate the data and results obtained from the simulation in LTE networks. It outperforms other algorithms in terms of efficiency.

Kumar et al. developed the smRED-4 algorithm for cellular networks in [8]. Under various load conditions, the algorithm is supposed to avoid packets from being dropped and delayed in the Evolved Node B (eNodeB) RLC buffer. The network bottleneck is overcome by adjusting the algorithm's parameters in response to different load situations.

The authors of [9], investigated several strategies for active queue management algorithms. Shodhganga et al. used the NS2 simulator to test the REM (Random Exponential Marking) and FQ (Fair Queue) active queue management algorithms in the DDoS environment under various forms of flood attacks Distribution Denial of Service (DDoS).

In [10], M. Çakmak et al. examined and compared the performance of active queue management algorithms used in mobile networks such as RED, ARED, SRED, REM, SBF, BLUE, RED, PURPLE, GREEN, and CoDel. In order to demonstrate the different types of methods and techniques for developing enhanced versions.

The authors of [11] tested the performance of the WBAN MAC standard protocols. And they used the OMNET++ simulator to compare the performance of the protocols in terms of power consumption, average delay, and packets congestion in IEEE 802.15.

The performance of the LTE PG-W and the remote host are compared in [12]. The authors of this study evaluated and demonstrated the performance of active queue management algorithms (RED, CoDel, PIE, and pFIFO) functioning between the remote host and PG-W in LTE networks in terms of average end-to-end throughput, latency, and packet loss rates.

In [13], Adesh & Renuka investigated the mobility of LTE networks under congestion and its influence on system performance. Early detection of eNodeB queue overflow and anticipation of packet delay in LTE networks is problematic. Various RED approaches attempt to resolve the queue overflow problem, while the PIE method attempts to minimize the time required to queue data packets to the eNodeB. These approaches remove data packets from the queue and wait for the congestion notification to be transmitted to the source node. Because the network layer does not support it, explicit congestion notification is not implemented in LTE networks.

In [14], Mobile Ad Hoc Networks (MANETs) determine the scheduling mechanisms that handle the buffering of packets during the wait time. Rukmani and colleagues compare between two FIFO and PQ mechanisms in a mixed traffic scenario (HTTP, FTP and VoIP applications) using OpNET Modeler simulation software. According to the research the authors have encountered some issues such as: packet dropped, packet received, and end-to-end packet delay. The results of the simulation assert that the PQ technique has higher quality than the other techniques.

In [15], Zarini and Ghasemi examined the effect of buffer size on the Quality of service of M2M traffic on 4G cellular networks. According to their simulation results, increasing the buffer size threshold does not appreciably decrease the probability of UE packet losses in the coordinated traffic model.

Ohta in [16], is evaluated the performance of a SIP signaling network under congestion situations and proposed decreasing the importance of the INVITE message to improve VoIP performance. The performance of a FIFO queue management algorithm can be tested with two distinct priority queues. However, this queuing method is easy and does not protect the system from SIP overflow attacks. The difference between a particularly saturated time and a DDoS attack on a web application, according to studies. Even on a particularly saturated time, 82.9% of IP addresses have checked the website previously. In a DDoS attack, only 0.6-14% of IP addresses were previously unknown. We can predict that this result to be unsatisfying.

In [17], Prajeet Sharma et al. evaluate traffic volume, number of packet transfers, and delay measures while identifying a DDoS attack on a MANET. These three network parameters are monitored by nodes in the current path using fixed threshold values. The packets are removed rather than transmitted to the next router if any node receives more packets than the threshold values for these three parameters. To detect DoS and DDoS, these parameters require reliable threshold values. Hence, these parameters are limited for dealing with dynamic traffic flows.

After examining all the viewpoints presented in these papers, we conclude that all the researchers investigated the AQM algorithm's performance on diverse networks such as LTE, MANET, AD HOC, and so on. However, no author has yet advised studying queue management on the RLC layer during a DDoS attack. All data packets are transferred over the RLC layer in LTE networks since it is so critical. RLC is performed via a radio interface to ensure the reliability of data transfer in packet mode. In this study, we used the NS-3 network simulator to investigate queue management in the RLC layer, in order to defend against DDoS attacks.

## 1.4 ORGANIZATION OF THESIS

The thesis work is organized in six parts. In the first part-, the purpose of the study of the thesis is explained by making a general introduction to the thesis and a review of the literature.

In the second part, the objective, general structure, operation and network layers of the LTE network are explained.

In the third part, the general structure and operation of queue management algorithms are explained.

In the fourth part, the general structure and operation of Distributed Denial of Service (DDoS) attacks are explained.

In the fifth part, network simulators are examined. The simulator selection process is explained by comparing simulators based on their characteristics.

In the sixth part, the data obtained as a result of the study are interpreted and discussed.

# PART 2

# LTE NETWORK

## 2.1 OVERVIEW

LTE (Long Term Evolution, or 4G) technology is based on an IP packet switched transport network. It has not provided any mode of routing for voice, other than VoIP, whereas 3G carries voice in circuit mode. For example, LTE uses radio frequency bands with a width that can vary from 1.4 MHz to 20 MHz, thus making it possible to obtain (for a 20 MHz band) a bit rate of up to 300 Mbit/s in the "downlink". This means that "real 4G" offers a downlink speed of up to 1 Gbit/s. LTE technology is based on a combination of improved technologies capable of significantly raising the level of performance (very high speed and low latency) compared to existing 3G networks. OFDMA (Orthogonal Frequency Division Multiple Access) multiplexing optimizes the use of frequencies while minimizing interference. The use of multiple antenna techniques (already used for Wi-Fi or WiMax) makes it possible to multiply the parallel communication channels, which increases the total speed and the range [18].

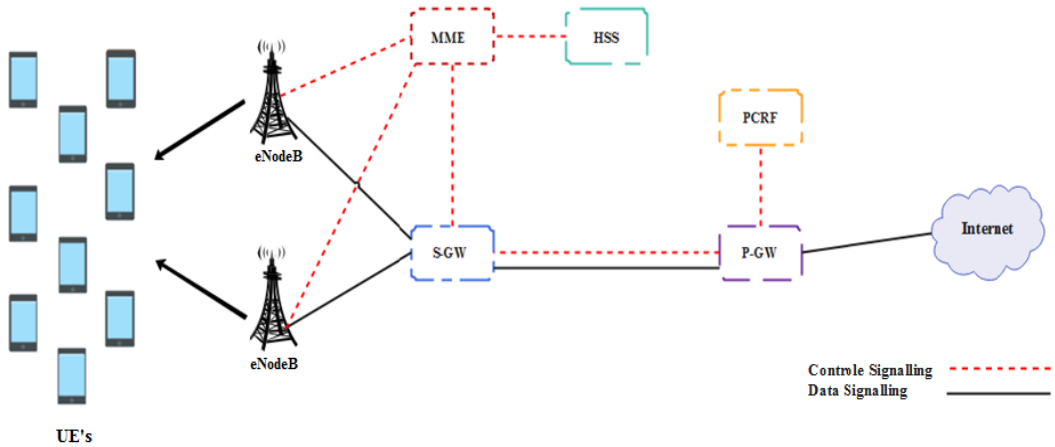


Figure 2.1 LTE Network [19]

## 2.2 MAIN PURPOSE OF LTE

The LTE (4th generation) aims to improve spectral efficiency and increase the capacity to manage the number of mobiles in a single cell. It also aims to provide high throughput in a mobile environment and full mobility to the user by developing compatibility between several existing technologies. Its goal is to make network transitions transparent to users, to prevent service disruptions during handovers, and to transition to all-IP usage [20].

The main objectives of the 4th generation networks are as follows:

- Ensure the continuity of the current session.
- Reduce traffic congestion and signaling delays.
- Provide a better quality of service.
- Optimize the use of resources.
- Reduce polling delay, end-to-end delay, jitter and packet loss.
- Minimize the cost of signage.

## 2.3 LTE NETWORK ARCHITECTURE

In comparison to previous generations of circuit-switching networks, the goal of LTE development is to establish a network architecture based only on packet switching operations. With LTE's packet switching benefits, it will offer a great internet protocol (IP) connection between the User Equipment (UE) and the PDN without producing any loss or damage to users, even when they are on the move [21].

The IP protocol is used to connect all LTE network interfaces. The All-IP protocol is a development of the 3GPP system designed to meet the growing need for cellular communication device speed. All IP network protocols are implemented to provide convenient access systems for diverse vendors and networks, with provisions for decreased system latency and customer satisfaction.

LTE consists of UE user equipment, Evolved-UTRAN Radio Access Network (E-UTRAN) evolution, and a non-radio access equivalent known as the Architecture Evolution System (SAE), which consists of LTE's Advanced Packet Core (EPC).

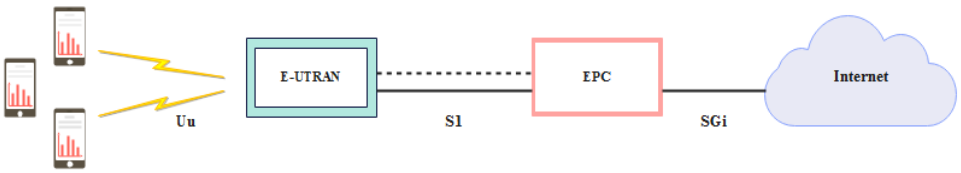


Figure 2.2 LTE Superior network architecture [21]

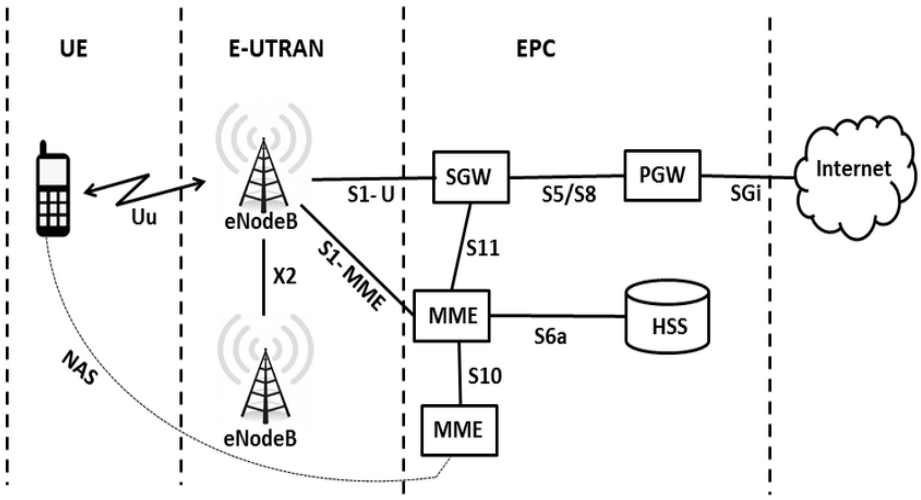


Figure 2.3 The EPS network architecture [22]

### 2.3.1 User Equipment (UE)

The user equipment for LTE has the same core architecture as UMTS and GSM, which is essentially mobile equipment (ME). The **modules** that comprise the mobile equipment are as follows:

- MT (Mobile Termination): This is where all communication operations are managed.
- TE (Terminal Equipment): This is where the data flows terminate.

- UICC (Universal Integrated Circuit Card): For LTE equipment, it is also known as a SIM card. It runs a program called the Universal Subscriber Identity Module (USIM).

A USIM is comparable to a 3G SIM card in that it saves user-specific data. This stores data such as the user's phone number, home network identification, security keys, and other personal information.

### 2.3.2 Access Network (E-UTRAN)

The enhanced terrestrial UMTS radio access network (E UTRAN) architecture is shown below.

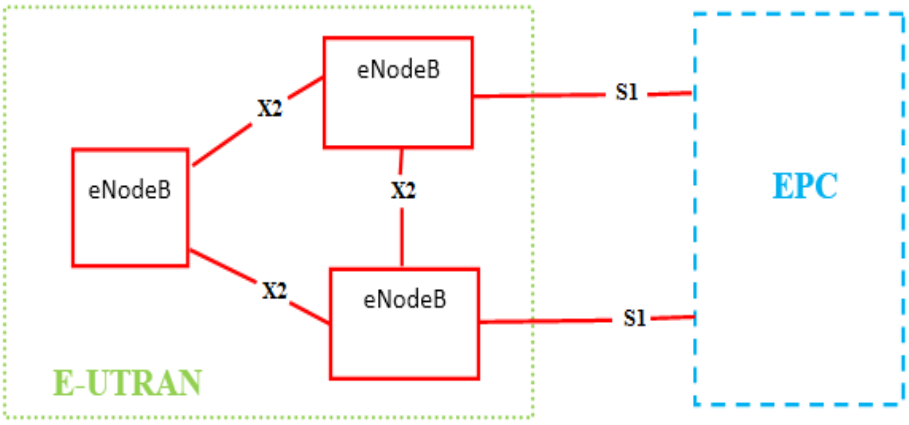


Figure 2.4 Evolved-utran (e-utran) interconnection [23]

The E-UTRAN network manages the radio transmissions across mobile devices and the evolved packet core and consists of only one component, an advanced base-station known as an eNB or eNodeB. Each eNB serves as a base station for one or more cells, controlling mobile devices. An eNB in service is a base station that connects with a mobile device [23].

LTE Mobile can only communicate with one base station and one cell at a time. The following are the two primary functions that eNB supports:

- Using the digital and analogue data transmission operations of the LTE radio interface, the eNB sends and receives radio communications to all mobile devices.
- The eNB supervises all its mobile phones' low-level functionality by giving them signaling messages like transfer requests.

Each eNB communicates with the EPC via the S1 interface and may also communicate with neighboring base stations via the X2 interface, which is primarily used for signal and packet transfer during handover. A user gets an eNB home (HeNB) base station to offer femtocell service in their home. A home eNB is part of a closed subscriber group (CSG) and can only be accessed by a mobile phone with a USIM that is also part of the CSG.

### 2.3.3 Evolved Packet Core (EPC)

The EPC (Evolved Packet Core) architecture is illustrated below. To keep it simple, a few extra components aren't included in the diagram. The Equipment Identity Registry (EIR), the Earthquake and Tsunami Warning System (ETWS), and the Policy and Billing Control Rules (PCRF) function are some of these components [24].

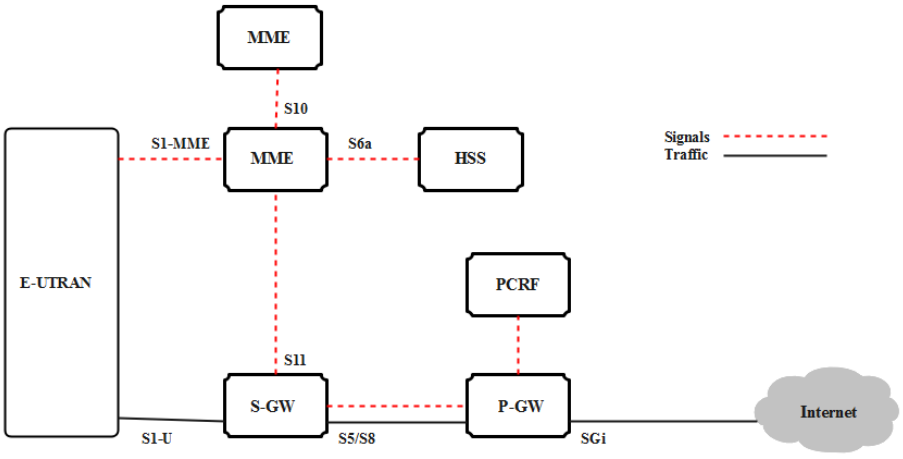


Figure 2.5 EPC Connection with RAN [25]

The Home Subscriber Server (HSS) element was migrated from UMTS and GSM systems and serves as a central database with data for all network operator users[26].

- The SGi interface is used to connect with the outside environment and PDN packet data networks by the PDN (Packet Data Network) or (P-GW) gateway. An access point name is used to identify each data packet network (APN).
- The PDN Gateway performs the same functions as the GPRS Support Node (GGSN) and the Serving GPRS Support Node (SGSN) with UMTS and GSM.
- The Serving Gateway (S-GW) is a router that connects the base station with the PDN Gateway, transmitting data.
- The mobility management entity (MME) uses signaling messages and the home subscriber server (HSS) to manage the increasing function of the mobile phone.
- The Policy and Billing Rules Control (PCRF) component isn't represented in the diagram below, but it's in charge of establishing policy control options and managing charged functionality based on those judgments. The Policy Enforcement Control Function (PCEF), which is contained in the P-GW, manages the information flow.

S5 and S8 refer to the interaction between the server and the PDN gateways. There are two distinct implementations, if the two devices are on the same network, S5 is used; if they are on different networks, S8 is used.

## 2.4 LTE RADIO PROTOCOL ARCHITECTURE

The Radio Bearer, which offers the method for transferring the EPS bearer, is set up, reconfigured, and released through LTE air-interface protocols. Layer 2 protocols, MAC protocol (Medium Access Control), RLC protocol (Radio Link Control), and PDCP protocol (Packet Data Convergence Protocol) are among the LTE air-interface protocols levels above the physical layer. The RRC protocol (Radio Resource Control) is a control plane protocol and is located on layer 3. The Non-Access Stratum (NAS)

protocol, which terminates on the core network side and was addressed in Party 2, is the protocol layer above (for the control plane).

The architecture of the generic radio interface protocol is described in this section. The essential functionalities of the MAC, RLC, PDCP, and RRC layers, as well as the concepts of ASN.1 employed in the RRC protocol, will be discussed. The radio protocol features of the X2 interface's control plane, or the interface between eNodeBs, are also discussed. The choices included for the CS fallback are explored in further depth as part of the Release 9 upgrades. The LTE Interoperability Testing (IOT) bits, which are designed for early UE handling in LTE, are introduced at the conclusion of this chapter.

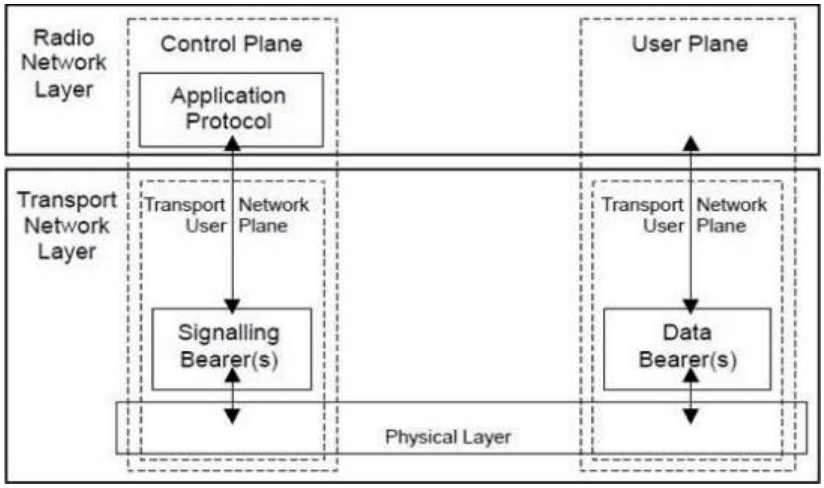


Figure 2.6 LTE radio protocol architecture

The figure shows the LTE User Plane's architectural structure, while the figure indicates the LTE Control Plane's architecture. The User and Control planes have a lot of similarities. In the next part, I'll go through each of these components in detail.

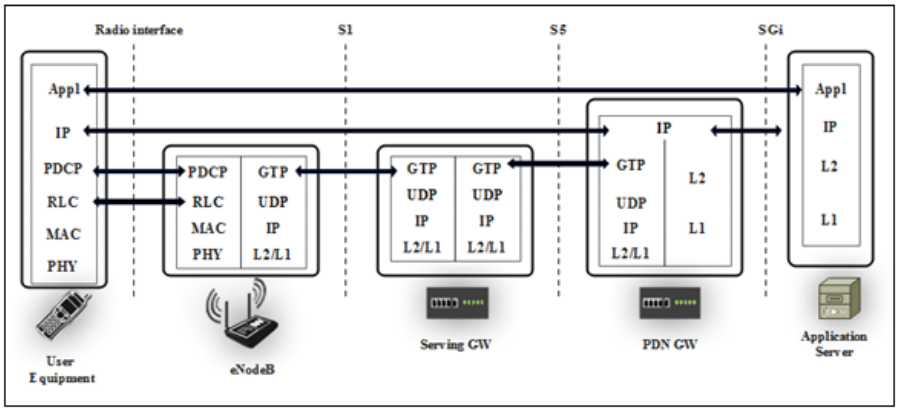


Figure 2.7 LTE user and control plane architecture [27]

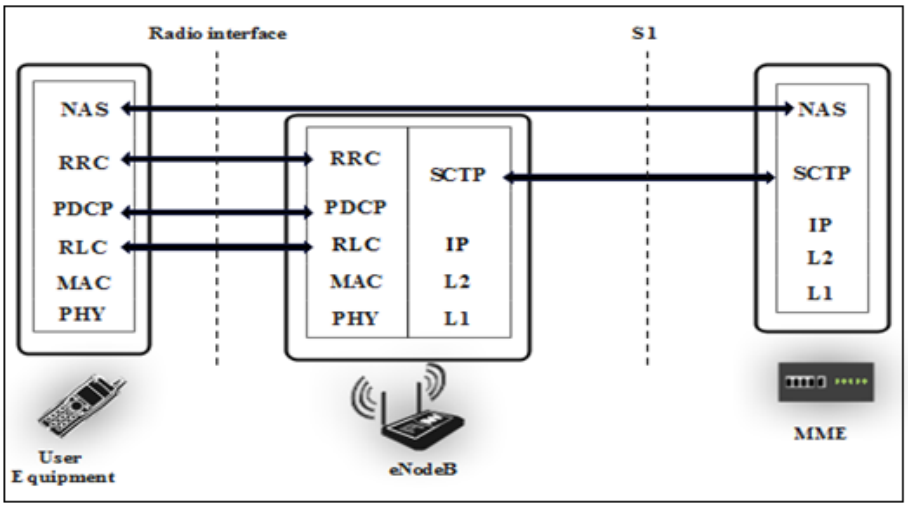


Figure 2.8 LTE user plane architecture [28]

### 2.4.1 Radio Resource Control (RRC)

All communication protocols between the UE and the eNodeB are supported by the RRC layer. Procedures for mobility and connection management are included. The RRC protocol is used to transport signals from the EPC control plane to the terminal, hence the connection between the RRC and the upper layers [29].

### 2.4.2 Packet Data Convergence Protocol (PDCP)

The PDCP layer, whose role is to provide the header compression protocol and implement data encryption. This layer supports radio carriers. Each carrier

corresponds to an information flow, such as data from the user plane or signals from the control plane. The information flows created by the "System Information Broadcast" and "Paging" operations are accessible to the PDCP layer due to their particular purpose and processing [28].

### 2.4.3 Radio Link Control (RLC)

The RLC layer offers fundamental layer 2 OSI model services to the PDCP layer, such as data packet separation and Automatic Repeat Request (ARQ) for error correction. At the MAC layer, there is a one-to-one mapping between the RLC's input flow, and the logical channels supplied by the RLC.

### 2.4.4 Medium Access Control (MAC)

The MAC layer's major aim is to map and multiplex the logical channels on the transport channels once the RLC layer has performed priority modifications on the streaming data received. The MAC layer also supports Hybrid ARQ (HARQ), a high-repeat function. Finally, the MAC layer sends the transfer flows to the PHY layer, which performs channel coding and modulation before sending the data over the radio interface [30].

### 2.4.5 NAS

This is only accessible in the control plan. It's a protocol that connects MME with UE and supports bearer configuration and mobility management. It helps in the establishment of IP communication between the UE and the PDN GW. Furthermore, it is the control plane's greatest stratum [29].

## PART 3

## QUEUE MANAGEMENT ALGORITHMS

In recent years, many scientists have been studying the active queue management (AQM) technique that supports the end-to-end Transmission Control Protocol (TCP) congestion control mechanism [31]. By constantly rejecting incoming packets, the AQM mechanism manages the length of the queue in the router (that is, the quantity of packets in the buffer). Although the AQM mechanism can resolve several issues with traditional drop-tail routers, it is commonly recognized that the AQM mechanism has several vulnerabilities. First, the efficiency of the AQM mechanism is greatly determined by the control parameters selected [32]. For this reason, many experiments have been conducted to understand how the selected control parameters affect the efficiency of the AQM mechanism. Most of these simulation analyses are based on only a few simulation results. Another issue with the AQM technique is that it is unable to provide fairness among TCP connections in a general network architecture with several routers. Although numerous AQM algorithms have been developed for increasing fairness among identical TCP connections, fairness difficulties in a general network with diverse TCP connections and various routers have yet to be completely studied [33]. We concentrate on two problems indicated above, which are connected to AQM methods [34].

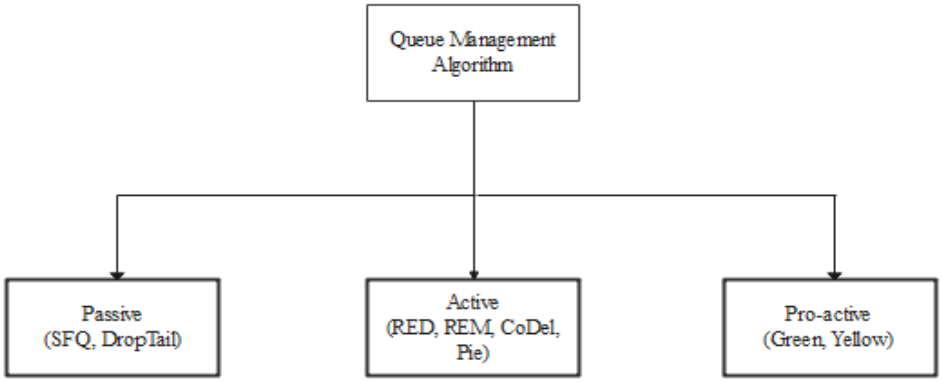


Figure 3.1 Queue management mechanisms [35]

## 3.1 DROPTAIL ALGORITHM

The principle of the DropTail Algorithm is very elementary and is frequently used for its simplicity of implementation in routers. This technique allows the packets that arrive first in the queue to be passed on as a priority. If the latter is saturated its maximum size is reached, the new packets are automatically discarded. The saturation state is trivially due to the following phenomenon: the arrival rate of packets in the file is greater than the output rate. The figure below schematizes the operating principle of this algorithm [34].

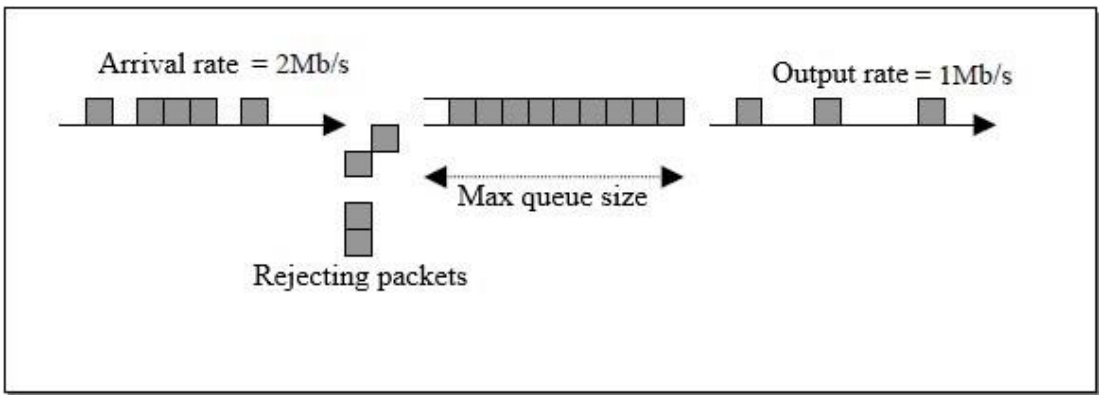


Figure 3.2 Droptail queue management algorithm

Even if the implementation is simple, this method presents vulnerabilities which do not contribute to the good use of the network, in particular the fairness of the network distribution. Indeed, a source that transmits at a higher rate than another source will be penalized for dropping the packets. Due to the important elimination, the TCP-type source adjusts its throughput according to the network load, which causes the network load to change between the two limit values (maximum and minimum), resulting in an imbalance or "inequality."

Finally, the constant charging of the queue can cause an increase in packet delay, which can seriously damage real-time applications, for example. It should also be noted that this mechanism does not distinguish the priority of the traffic, so all packets, whether the priority is required or not, are treated the same.

## 3.2 RED (RANDOM EARLY DETECTION) ALGORITHM

The Random Early Detection [36] mechanism involves the “threshold” parameter, a threshold interval in which packet elimination occurs, and is based on the average size of the queue. The algorithm developed allows to reduce the occupancy rate of the queues and tries to remain equitable between the sources in the distribution of the losses. Figure 12 illustrates how the algorithm works.

RED works according to the following principle: the probability of removing a packet is based on the interval of defined thresholds (threshold-min; threshold-max). When the queue size exceeds the minimum threshold, the RED algorithm implements its policy of discarding packets. The probability of elimination increases linearly as the queue size increases. Beyond the maximum authorized threshold, RED systematically drops all new incoming packets [7].

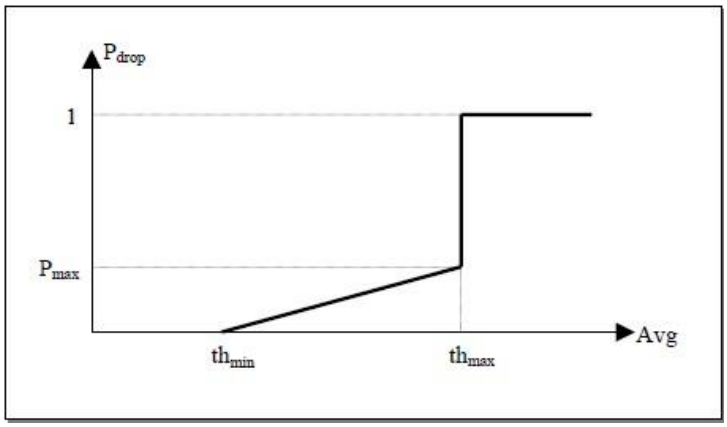


Figure 3.3 Mechanism of operation of RED [32]

This queue management algorithm is used for TCP-type flows as a congestion control mechanism. Indeed, the ECN (Early Congestion Notification) method uses the same principle adopted by RED to indicate to a TCP source that it should adapt its transmission rate according to the load of the network [33].

The problem (or inconvenience) with RED is that it's a mechanism that does not allow packet priority management, which could largely affect high-priority streams requiring high QoS.

### 3.3 CODEL (CONTROLLED DELAY) ALGORITHM

For RED queuing to perform properly, its settings must be configured for network bandwidth of various sizes. CoDel solves this problem. Unlike other AQMs, CoDel operates autonomously from network metrics including queue size, queue delay, average queue size, queue thresholds, and drop rate. CoDel does not manage the queue based on the queue size, it employs the time spent buffering packets, known as queue time [37]. The packet sojourn time parameter estimates CoDel congestion, which affects the delay in the router queue. CoDel employs packet sojourn time as a measure to anticipate network congestion. Packet sojourn time is the real-queue delay generated by a packet. The CoDel algorithm has two parameters: Target and Interval [38]. When the packet sojourn time exceeds the target value for a predefined interval of time, CoDel starts actively dropping or marking packets to control queue length. When the packet sojourn time is less than Target, no packets are dropped [39].

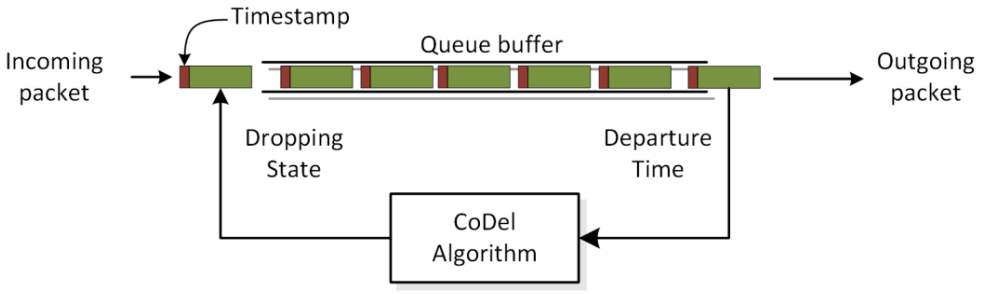


Figure 3.4 Codel algorithm [38]

### 3.4 PIE (PROPORTIONAL INTEGRAL CONTROLLER ENHANCED) ALGORITHM

Proportional Integral Controller Enhanced (PIE) is an AQM that attempts to keep the queueing delay to a configured value in time. PIE uses a Proportional Integral (PI)

algorithm as its core to maintain a target queueing delay [40]. The PIE algorithm combines the advantages of both RED and CoDel and is as simple to use as RED while managing delays effectively as CoDel. It maintains an estimation of the dequeue rate and periodically measures the queueing delay from the number of packets in the queue, which is used in the PI controller to calculate a signaling probability. For each packet enqueued, the probability is used to determine if the packet should receive a congestion signal. PIE includes several heuristics, e.g., tuning of the probability if it is low to avoid instability, limiting the change in probability, and more. PIE can manage latency around the reference over different congestion scenarios, according to the simulation and test results. It can respond rapidly and effectively to changes in network congestion. As a result, within a predefined limit, the PIE algorithm design is reliable for an approximate value of flows with diverse round-trip durations [39].

### 3.5 PFIFO (PAQUET LIMIT FIRST-IN FIRST-OUT) ALGORITHM

pFIFO queuing is the simplest mechanism to control network congestion. This algorithm queues frames in First-In-First-Out (FIFO) order, and the accumulation of the queue continues until all the buffer memory is exhausted, which is very similar to how the DropTail algorithm manages congestion [12]. In the DropTail queue management algorithm, the router drops each data packet entering the packet queue sequence when the route queue is full [7].

The loss of packets from the drop causes the TCP sender to enter slow-start, which reduces throughput in that TCP session until the sender begins to receive ACKs again and increases the cwnd. Based on scientific research, we consider PFIFO to be comparable to DropTail due to its operation being similar to DropTail.

# PART 4

# DISTRIBUTED DENIAL OF SERVICE (DDoS)

## 4.1 INTRODUCTION

Denial of Service attacks aim to consume all or part of a target's resources, in order to prevent them from being able to provide their services satisfactorily. The first types of Denial of Service attacks involved only a single attacker (DoS), but soon evolved attacks appeared, involving a multitude of "soldiers", also known as "zombies" (DDoS).

Until recently, DoS and DDoS attacks were carried out by "hackers" looking for exploits and fame. Today, real criminal organizations have sprung up around these tools. A recent McAfee study estimates that 70% of Internet attacks are carried out by organized crime groups. For example, some hackers have specialized in raising "zombie" armies, which they can then hire out to other hackers to attack a target [41]. With the sharp increase in the number of commercial exchanges on the Internet, the number of Denial of Service blackmail cases is also increasing very strongly: a hacker launches a DoS or DDoS attack on a company in order to saturate the network's resources and cause network congestion, which will increase packet loss, long delay, and inefficient network performance. All these examples show how essential it has become to be able to effectively detect these attacks (by establishing an active queue management mechanism) [42].

## 4.2 DENIAL OF SERVICE (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

A denial of service is a network attack aimed at preventing a server or a network from satisfactorily providing its services. A denial of service attack is conducted by

consuming a large portion of the victim's resources. These resources can be network (bandwidth, buffers, etc.) or software (flaws in applications or operating systems). In all cases, the goal is to consume all or part of the resources that the victim needs to provide his services [43].

### 4.2.1 Definition of DoS and DDoS Attacks

There are two main types of denials of service: denials of service "simple" (DoS) and distributed denials of service (DDoS). DoS attacks are the first to appear. In this type of attack, the hacker alone launches his attack against the victim (or target) [44]. Most of the time, the hacker hides his network identity (IP address and UDP / TCP ports) by pretending to be one or even several other machines (spoofing). Thus, it cannot be recognized by the victim (or target) (fig. 4.1).

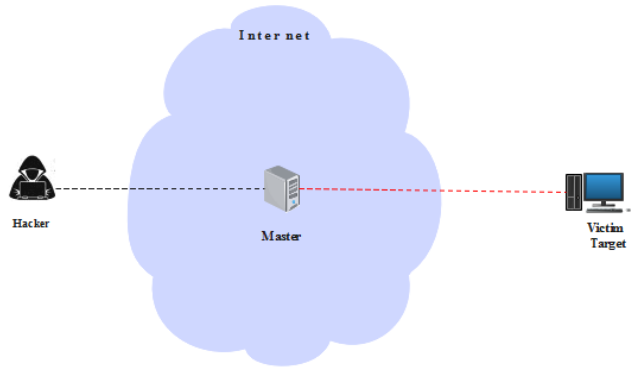


Figure 4.1 Dos attack [45]

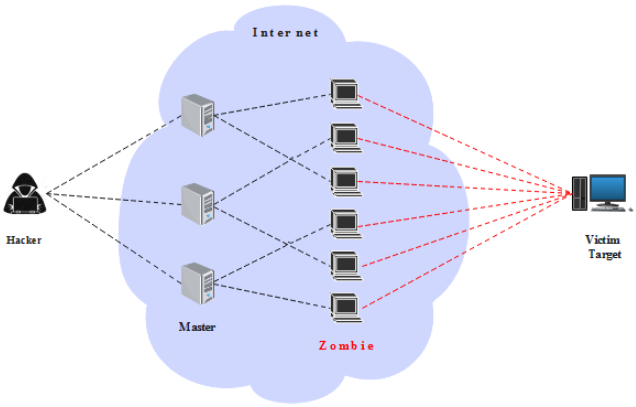


Figure 4.2 Ddos attack [45]

Distributed denials of service are more complex. They deploy an army of attackers (called "agents" or "zombies"), controlled by one or more "generals" (called "masters"). Each agent generates a simple DoS attack on the target. The "generals" give the attack orders to the agents and are piloted by one or more hackers (Fig. 4.1 and Fig. 4.2). Such an architecture makes it possible to multiply the power of the attack. It complicates the identification of hackers by the victim (or target). But such attacks first require a phase of corrupting machines on the Internet in order to install agents there and later to be able to use this army of attackers. Note that some hackers have specialized in corruption and raising an army of attackers, which they then give to other hackers who want to execute attacks. Hence, the same attacking army can be used for several attacks [45].

## 4.3 DOS AND DDOS ATTACKS IN LTE MOBILE NETWORK

The emergence of mobile devices with access to data, as well as sophisticated services such as websites, video streaming, and mobile apps for use on wireless networks, unlike the enormous Internet, such as Google, Yahoo, and Amazon, most mobile operators are unequipped and unprepared for large-scale security threats. Mobile operators are vulnerable to security attacks due to the large-scale security of the 4G LTE network, and DDoS attacks are increasing on mobile networks. For this reason, DDoS is the most dangerous security attack on network infrastructure. These DDoS attacks may be categorized depending on attack volume. A single attacker can create a small amount of traffic (DoS), and multiple attackers using agents coordinated by the Botnet Command and Control Center (C & C) can create a large amount of traffic (DDoS attacks using botnet clusters, for example) [46].

Additionally, a UE botnet could also be used to amplify the impact of a DDoS attack on a particular internet target. When botmasters use cellphones to construct a botnet, they may either use a command to activate all the botnet nodes or configure the nodes to wake up at a specific time. At the time of the attack, any botnet node can either begin downloading a huge file (such as a YouTube movie) to cause downlink congestion or transmit fake (or false) data to an arbitrary recipient to cause uplink

congestion. Congestion has the consequence of making most clients unable to utilize the cellular network successfully [5].

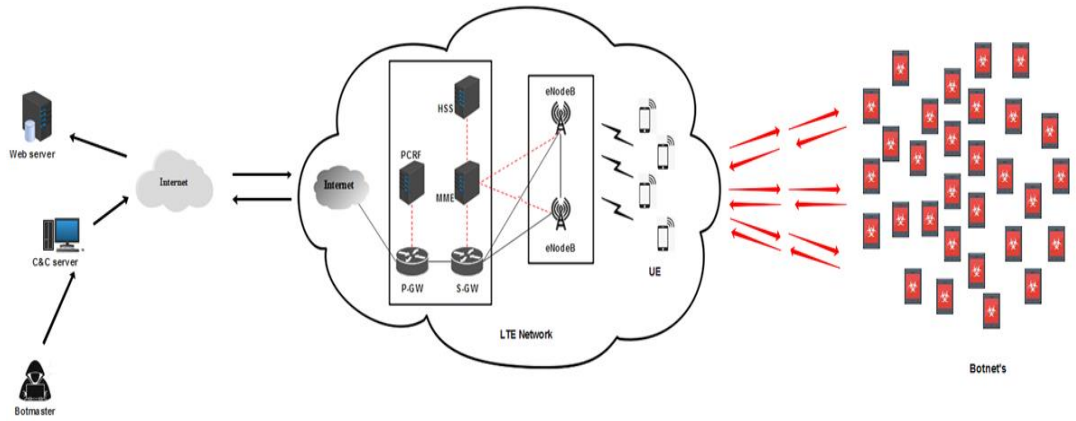


Figure 4.3 Botnet in 4g cellular network

# PART 5

# NETWORK SIMULATORS

The Network Simulator is a simulation program, ready to use and primarily for wired and wireless computer networks. In this study, we want to simulate an LTE network. For this purpose, we aim to use the famous NS-2 simulator or its successor, NS-3 [47]. So far, it is not possible to simulate this type of network. In this sense, a project to extend the NS-3 to simulate LTE networks is underway. On this basis, we decided to carry out a study on the use of different computer network simulation tools for the simulation of wireless sensor networks. This study, in the end, allows us to choose a suitable simulation tool to carry out our simulation project. We have recorded, in research work based on the simulation of computer networks, the use of a multitude of simulation tools (OMNET++, OPNET++, QualNet... etc.), some of which have advantages that others do not. Hence, they need to be able to compare them [48]. But before that, it is necessary to mention the interest of these simulators: what can they be used for?

## 5.1 THE UTILITY OF SIMULATOR

Network simulators are used by people from different fields, such as academic, industrial, and quality assurance (QA) researchers, to design, simulate, verify, and analyze the protocol performance of different networks. The simulations are performed in a simulated environment, not a real one. They can also be used to assess the effects of different parameters of the protocols studied. Some simulators are more complete in their results than others, but all allow the behavior of a network with a specific topology and characteristics to be studied. Simulators thus make it possible to anticipate the topology of a network. When the results of a simulation are not satisfactory, it is easy to modify the topology to correct the problems put forward by

the previous simulation. For example, if a simulation indicates from its results that the location of an AP (Access Point) is not correct (the coverage area is not optimal), we can easily modify its location via the simulator to predict the behavior of the network if the AP is moved.

Simulation is also interesting for creating the topology of a network before setting it up. And this is possible because the simulators integrate numerous tools, making it possible to carry out realistic simulations. You can also use a simulator to test a new protocol (ease of integration depends on the simulator used) before using it (a network topology).

## 5.2 NETWORK SIMULATORS

There are several network simulators available, including NS3, NS2, OPNET, OMNET++, and others. Among these simulators, we will focus on the most widespread simulators, such as NS3, NS2 , OPNET, and the OMNET++ simulator that we have chosen for the development of our application [49].

### 5.2.1 The OMNET ++ Simulator (Objective Modular Network Testbed)

OMNeT++ is a free and open-source simulation environment that includes a simulation core and has a solid graphical interface. It's a discrete event simulation program written in C++ that's free for academic research. Although there is a commercial version named "OMNEST" that is not free, It was developed to simulate [50]:

- ✓ Systems for communication networks.
- ✓ Systems for multi-processor.
- ✓ Distributed systems of many types.
- ✓ Currently it is used in universities for the validation of new software and hardware, as well as for the analysis and evaluation of transmission protocols.
- ✓ Queue networks.

OMNET ++ was realized thanks to the study project of the Technical University of Budapest in 1992 and has been improved over the years. However, the simulation of computer networks is the main area of application. For this, there are frameworks that provide modules for wired and wireless simulation or for mobility. OMNET++ is known for its ease of learning, integrating new modules and modifying those already implemented. The architecture of the OMNeT++ model consists of several nested hierarchically (visualized in the figure below) modules which are [51]:

- **The system module**.
- **Simple modules** (sheets): programmed in C ++ encapsulating the behavior of a real system. For each simple module corresponds a .cc file and a .h file.
- **Compound modules**: made up of one or more simple modules or compound modules linked together. The parameters, ports and modules for each module are specified in an *.ned* file. the architecture of OMNET ++ is visualized in the following figure:

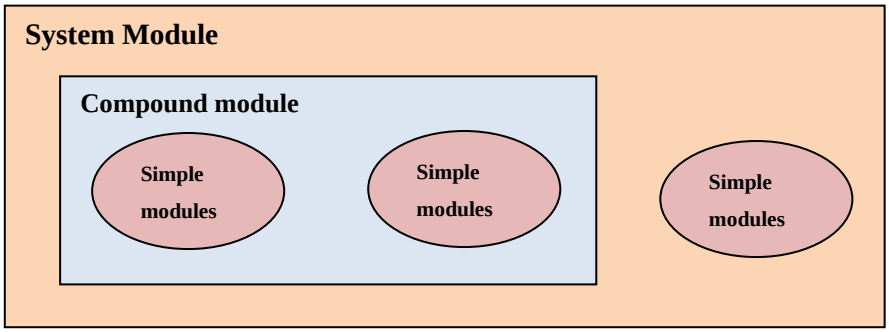


Figure 5.1 The architecture of the OMNeT ++ simulator modules

### 5.2.2 The OPNET++ Simulator (Optimum Network Performance)

The OPNET simulation tool allows you to simulate powerful network infrastructures coded in C++ and designed in an object-oriented way [52]. It also makes it possible to design and study communications networks. We use this simulator especially for wireless sensor networks, new technologies, etc. But it takes a long time to learn. It is made up of several editors: the nodes module, the process module, and the simulation module (execution of the simulation which will bring changes to the nodes). OPNET

includes various proprietary functions. It also manages certain types of objects, such as links and packet formats. OPNET is quite a complex simulator, which results in learning difficulties. It is based on two methods, which are the use of programmed nodes and the definition of models. OPNET can be used in [14]:

- Traffic modeling of telecommunication networks.
- Protocol modeling.
- Modeling of network tails.
- Hardware architecture validation.
- Evaluation of complicated software systems in terms of performance.

The architecture of OPNET is hierarchical nested, with the highest level being the network domain, which allows to define the topology of the latter. The simulation under OPNET is based on two methods: either by using the programmed nodes provided by OPNET, or by defining a link model, protocols, and process models.

### 5.2.3 Ns-3 Network Simulator

NS3 consists of a tested and validated kernel and various modules. The kernel is made up of the scheduler and classes defining the key objects, namely: packets, nodes, channels, applications, and network elements.

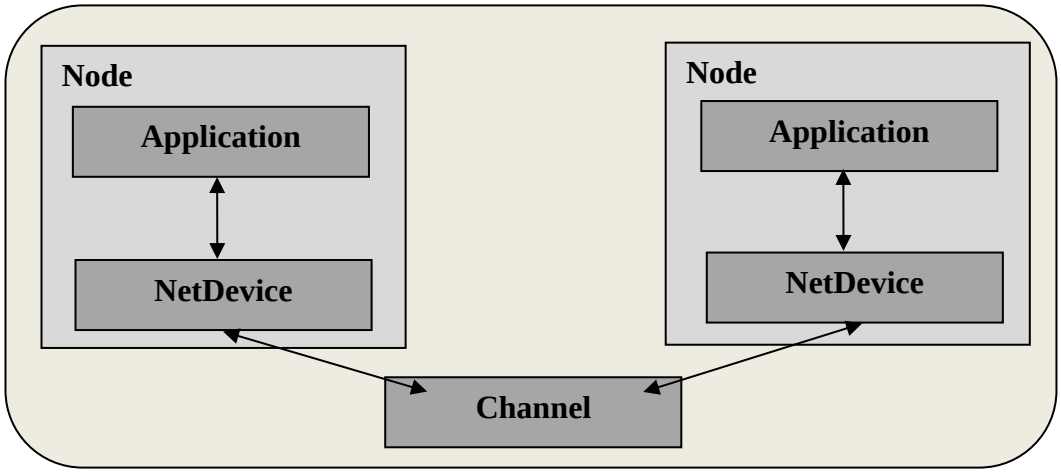


Figure 5.2 Basic components of NS3

All of these elements are used in scripts to perform the simulations. Figure 5.2, which shows the basic components of NS3 from NS3. The languages supported by NS3 are C++, Python, and NS2, unlike NS-2, which uses TCL. It is designed with an emphasis on all layers 2-4 of the OSI model, thus enabling it to support IP addresses. It has a modular, scalable, and realistic architecture, with better performance. This feature allows it to support large-scale network simulation efficiently with better performance compared to other existing simulators. It generates packet capture type files (Packet Capture, PCAP, traces) and log files as output. For visualization and analysis of results. The NS3 also offers the possibility of integrating other free software, such as the Wireshark packet capture and analysis software. It is made by and for the research community.

## PART 6

# PERFORMANCE OF QUEUE MANAGEMENT ALGORITHMS IN LTE NETWORK UNDER DDOS ATTACKS

To resolve the congestion problems that a rise in LTE cellular networks, the efficiency of active queue management algorithm systems operating at the RLC layer must be increased. In addition, the balanced operation of the RLC buffer must be guaranteed at different load values. We offer some algorithms such as RED, DropTail, PIE, CoDel and pFIFO. After comparing all the algorithms which provide higher end-to-end throughput and lower delay in LTE networks and to resolve congestion issues.

## 6.1 SIMULATION ENVIRONMENT

In this section, first of all, the network model was created for the experimental study and the simulation parameters were adjusted. Then the simulation results were evaluated. For the performance evaluation, first the different queue management algorithms such as RED, Drop-tail, PIE, pFIFO, and CoDel were compared and analyzed. Then, the simulation studies are then examined and compared on LTE networks under DDoS attacks in terms of end-to-end average throughput, delay, pdf, jitter, and fairness index. To test the performance of each method on LTE networks, we utilized the NS-3 network simulator software. The first section presents the LTE application scenario, and the second section explains the system parameters. Then, in the third section, the simulation results are explained and evaluated. Finally, the last section concludes the simulation study, or conclusion.

## 6.2 SIMULATION SCENARIO

The simulation model is one of the most efficient decision-making applications accessible to complicated network architects and managers. It includes creating a

model of a real network and performing tests on this model in order to study the system's performance and comportment. In addition, there are various network simulators available, including OPNET, OMNET ++, Qualnet, GloMoSim, NS2, and NS3. Unlike previous simulators, NS3 is a free and open-source simulator that was designed for educational and research purposes and is licensed under the GNU and GPLv2 licences. Its performance is based on discrete events.

In order to test or evaluate the queue management algorithms in this thesis, an LTE network design needs to be established in our research using a Ns3 simulator. Figure 6.1 shows the topology employed in this simulation model.

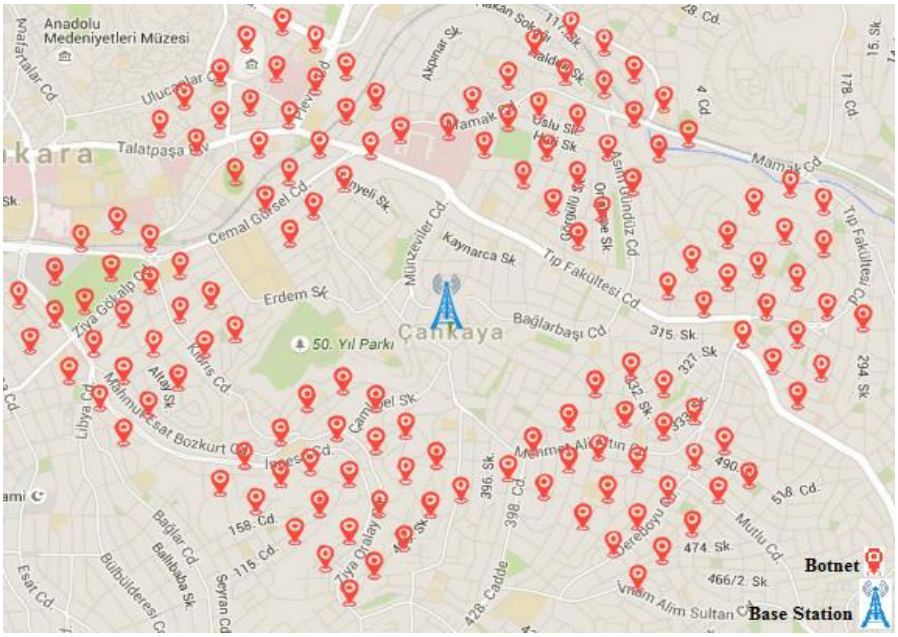


Figure 6.1 Topology lte network

Figure 6.1 shows the LTE model, which includes 100 botnets, 1 eNodeB to which these botnets are linked, S-GW and P-GW nodes for connecting to the internet and services, and an internet node.

### 6.3 SIMULATION PARAMETER

For LTE models, the parameters in table 1 are used. The interconnection between the Internet node and the S-GW and P-GW nodes has a data rate of 100 Gbps. Ethernet

networks have a maximum transmission unit (MTU) of 1500 bytes. This indicates that in an Ethernet network, the maximum size of an incoming packet is 1500 bytes. There is a 0.010 second delay between these nodes. The data rate is 100 Gbps with a delay of 2 ms between the S-GW/P-GW node and the eNodeB node. RandomWalk2D is the user mobility type. The wired link capacity is 100 Mbps. TCP NewReno is the TCP traffic type. These are the interface parameter values in the LTE architecture.

Table 6.1. LTE model parameters.

| Parameter | Value |
|---|---|
| Internet-S-GW/P-GW Node; | |
| Maximum Transmission Unit (MTU) | 1500 |
| Data Rate | 100 Gbps |
| Delay | 0.010 s |
| S-GW/P-GW-eNodeB Node; | |
| Wired Link Capacity | 100 Gbps |
| Data Rate | 100 Gbps |
| Delay | 2 ms |
| Number of Botnets | 20, 40, 60, 80, 100 |
| Type of TCP Traffic | TPC New Reno |
| Mobility | RandomWalk2D |

The DropTail queue management algorithm was tested using the parameters listed in Table 6.2. The DropTail mode option is used to process the queue as packets or bytes. Max-Packets determines the maximum number of packets that a queue can accept.

Table 6.2. DropTail queue management algorithm parameters.

| Parameter | Value |
|---|---|
| Mode (Bytes, Packets) | Packets |
| Max Packets | 50 |

The CoDel queue management algorithm was tested using the parameters listed in Table 6.3. The CoDel mode option is used to process the queue as packets or bytes. The maximum number of packets that a queue can receive is specified by Max-

Packets. The interval parameter specifies how long packets can wait in the queue. The target parameter is used to delay or extend the target queue by 5 milliseconds.

Table 6.3. CoDel queue management algorithm parameters.

| Parameter | Value |
|---|---|
| Mode (Bytes, Packets) | Packets |
| Max Packets | 50 |
| Interval | 100ms |
| Target | 5ms |

The RED queue management algorithm was tested using the parameters listed in Table 6.4. The RED mode option is used to process the queue as packets or bytes. The average queue size is represented by MeanPktSize. IdlePktSize is the average packet size used when the system is idle. The RED algorithm uses the Link Delay parameter to calculate the link delay value, which is measured over 20 ms.

Table 6.4. RED queue management algorithm parameters.

| Parameter | Value |
|---|---|
| Mode (Bytes, Packets) | Packets |
| MeanPktSize | 50 |
| IdlePktSize | 1500*1000bytes |
| MinTh, MaxTh | 20,50 |
| Queue Limit | 50 |
| Queue weight | 0,002s |
| Link Delay | 20ms |

The pFIFO queue management algorithm was tested using the parameters listed in Table 6.5. The size of the queue is determined by the limit parameter. it is measured at 50.

Table 6.5. pFIFO queue management algorithm parameters.

| Parameter | Value |
|---|---|
| Limit | 50 |

## 6.4 SIMULATION STUDY

In this section, we compared various algorithms, such as RED, DropTail, CoDel, PIE and pFIFO algorithms, in terms of delay, end-to-end average throughput, Package Delivery Fraction (PDF), and fairness-index, using 10, 20, 40, 60, and 100 botnets in an LTE network environment.

The average end-to-end throughput values for the different algorithms are shown in Tab 6.6. The CoDel algorithm gives better values than other algorithms in terms of average end-to-end throughput. The lowest-level algorithm is the DropTail algorithm.

Table 6.6. Average throughput values for various AQM.

| AQM | Performance of Average Throughput (Kbps) | | | | |
|---|---|---|---|---|---|
| | 10 BotNet | 20 BotNet | 40 BotNet | 60 BotNet | 100 BotNet |
| DropTail | 2492,157 | 1593,321 | 1058,988 | 310,52 | 123,963 |
| PIE | 2756,93 | 1866,50 | 1462,62 | 571,65 | 275,244 |
| pFIFO | 2554,671 | 1777,167 | 1386,537 | 566,55 | 217,539 |
| RED | 2793,681 | 1953,759 | 1473,846 | 643,13 | 317,061 |
| CoDel | 2914,524 | 2047,491 | 1623,633 | 730,35 | 365,868 |

A graph of the average throughput value is shown in Figure 6.2. In terms of end-to-end efficiency, the CoDel algorithm achieves the best result of all the algorithms. CoDel gives the highest average throughput with Target and Interval, followed by packet delays. The closest result of the CoDel is the RED algorithm. The DropTail algorithm achieves the worst results of all the algorithms, dropping entering packets when the queue is full. Also, as the quantity of botnets expands, DropTail performs

poorly. This indicates that DropTail is the algorithm that is most sensitive to high traffic.

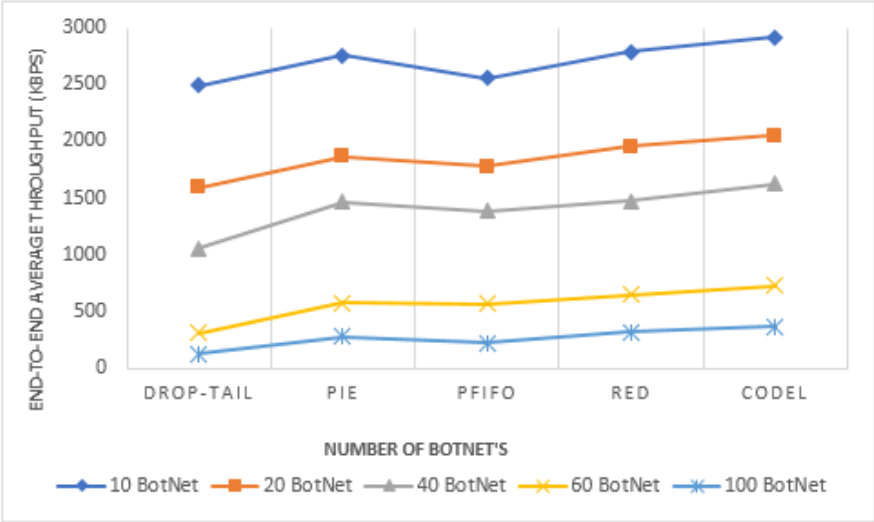


Figure 6.2 Average end-to-end throughput values

In the LTE network, the low end-to-end delay allows users to get data more efficiently. The average end-to-end delay improves as the number of botnets rises, as seen in Tab. 6.7. Due to the extended demand time of the packet drop mechanism, the DropTail, PIE, and pFIFO algorithms have long delays. The CoDel algorithm reduces latency by rejecting packets based on their queue delay. Additionally, the CoDel algorithm drops fewer packets than other algorithms, which reduces network latency.

Table 6.7. Average end-to-end delay/ms.

| AQM | Average end-to-end Delay (ms) | | | | |
|---|---|---|---|---|---|
| | 10 BotNet | 20 BotNet | 40 BotNet | 60 BotNet | 100 BotNet |
| DropTail | 74,686 | 160,86 | 343,04 | 648,45 | 1809,8 |
| PIE | 41,59 | 126,50 | 268,73 | 488,34 | 988,104 |
| pFIFO | 44,6405 | 131,68 | 280,81 | 514,69 | 1050,6 |
| RED | 29,193 | 117,40 | 246,27 | 472,62 | 949,679 |
| CoDel | 26,751 | 104,43 | 208,85 | 395,81 | 766,104 |

The average end-to-end delay time, dependent on the number of botnets, is shown in Fig 6.3. The router numbers in the connection between the sender and receiver determines the end-to-end delay. End-to-end delay is extremely improved by router mechanisms such as transition, encoding, packet generation time, and queue management. Hence, the CoDel algorithm has the lowest average end-to-end delay and the least packet loss.

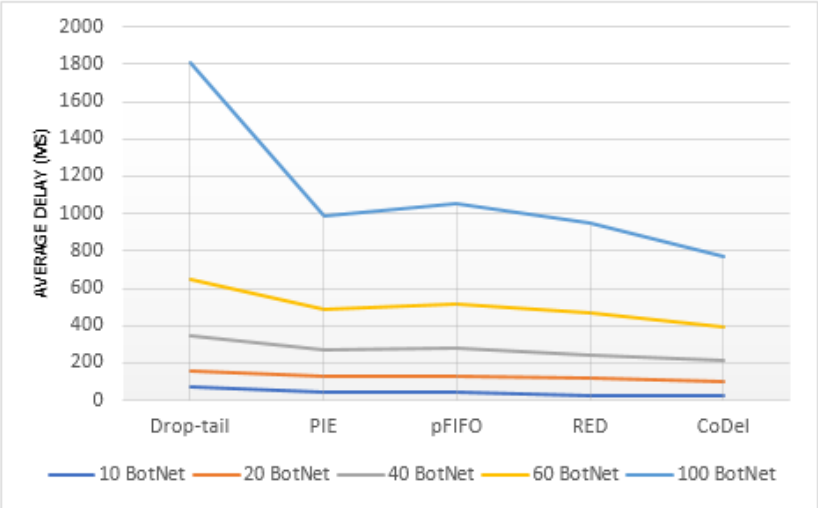


Figure 6.3 Average end-to-end delay (kbps)

The variation in the Packet Delivery Fraction (PDF) as a function of the number of botnets is represented in Tab. 6.8. The PDF is a crucial ratio for assessing network performance. Because it determines the ratio of total packets sent to total packets received.

Table 6.8. Average PDF rate.

| AQM | Average PDF (%) | | | | |
|---|---|---|---|---|---|
| | 10 BotNet | 20 BotNet | 40 BotNet | 60 BotNet | 100 BotNet |
| DropTail | 89% | 81% | 64% | 54% | 8% |
| PIE | 95% | 86% | 73% | 61% | 42% |
| pFIFO | 93% | 83% | 71% | 63% | 45% |
| RED | 97% | 87% | 75% | 69% | 51% |
| CoDel | 98% | 89% | 76% | 72% | 57% |

CoDel is an algorithm that optimizes the number of packets in the eNodeB buffer, as shown in Fig 6.4. The CoDel algorithm removes packets from the queue depending on the queue delay. For this cause, CoDel is the algorithm with the largest percentage of packets at source and destination. According to the PDF values, CoDel performs better than other methods. When the queue is full, DropTail drops directly the collected packets in the queue, for this reason it is an algorithm with the least PDF value.

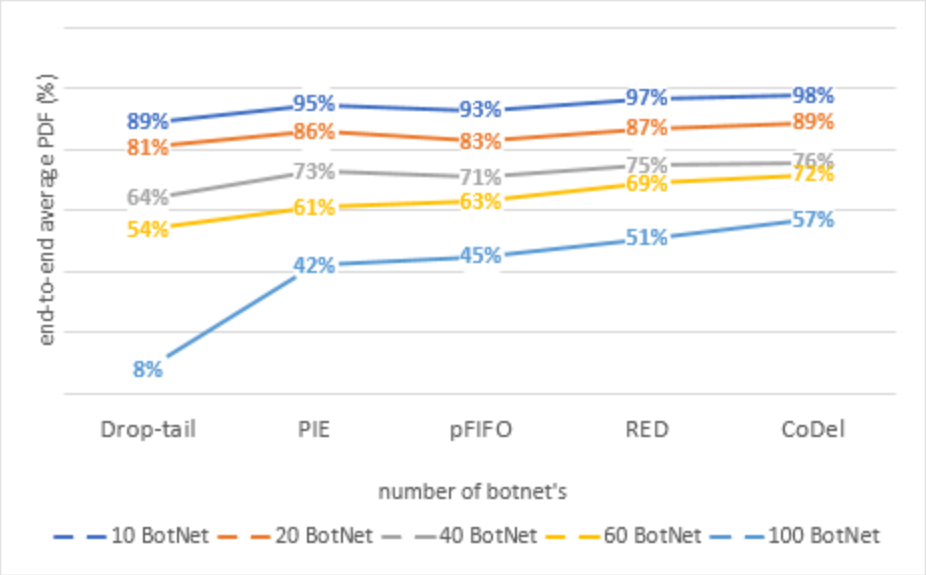


Figure 6.4 Average end-to-end PDF

Tab. 6.9 Fairness Index for algorithm

| AQM | Fairness Index | | | | |
|---|---|---|---|---|---|
| | 10 BotNet | 20 BotNet | 40 BotNet | 60 BotNet | 100 BotNet |
| DropTail | 0,79 | 0,65 | 0,41 | 0,23 | 0,09 |
| PIE | 0,89 | 0,78 | 0,63 | 0,51 | 0,31 |
| pFIFO | 0,87 | 0,77 | 0,65 | 0,56 | 0,38 |
| RED | 0,88 | 0,81 | 0,66 | 0,58 | 0,41 |
| CoDel | 0,91 | 0,84 | 0,78 | 0,61 | 0,49 |

For the LTE network, any transmission protocols or P2P implementations that operate well with packet congestion control systems. The fairness index necessitates a protocol

that does not utilize more network resources than identical flows. The fairness index values for the CoDel, PIE, pFIFO, RED, and DropTail algorithms are distributed by the number of botnets in Tab. 6.9.

The CoDel algorithm has the highest fairness index value (see Figure 6.5). The reduced waiting time in the queue allows RED to make the maximum of network resources. The distribution of resources on the LTE network has a major influence on the time and quality of service. CoDel improves network quality of service by dropping fewer packets. Due to the uncontrolled package drop mechanism, DropTail achieves poor performance in terms of fairness index value.

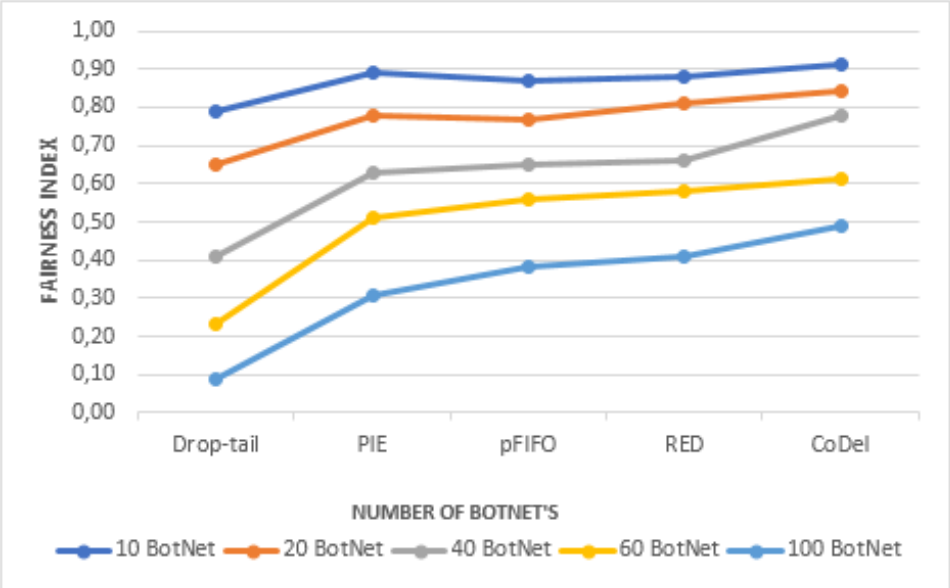


Figure 6.5 Fairness index on the number of botnets with different algorithms

## 6.5 SIMULATION RESULT

According to the simulation results, the CoDel queue management algorithm has a lower packet delay rate than other algorithms that use various queue lengths and botnet numbers. The packet drop procedure is performed by the CoDel queue management algorithm based on the real queue wait time. The packet is only dropped if the packet waiting in the queue exceeds its separation time, even though there is a probability that the queue will be overloaded, and any entering packets will be dropped. RED is the

algorithm that produces the most similar results to the CoDel algorithm. Followed by the Pie, DropTail, and pFIFO algorithms. The RED queue management algorithm controls the queue size in real time and determines whether or not to drop a packet based on the defined minimum and maximum threshold values. The DropTail and pFIFO algorithms are queue management algorithms that function in a conventional way, and whether a packet is dropped or not depends on whether the queue is full or not. This is why the CoDel queue management algorithm performs better than the other four algorithms (RED, DropTail, PIE, pFIFO).

The CoDel algorithm aims to identify a remaining queue by recording the minimal queuing delay packets encounter over a specified time interval using timestamps. To ensure better connection usage, CoDel believes that a low target remaining queue is sufficient. A packet is dropped from the queue if the minimum queuing delay exceeds the target delay value by one interval, and the next dropping time is determined by a control rule. The controller stops rejecting packets when the queuing delay is less than the target time.

# PART 7

# CONCLUSION

The issue of identifying anomalies in network congestion traffic caused by DDoS attacks has mainly been studied in terms of detecting illegal DDoS traffic provided by traditional connected devices (such as PCs, laptops, servers, and mobile devices). To manage congestion traffic, researchers and equipment developers have created queue management algorithms. Active queue management algorithms have been developed for the purpose of managing proximate average queue lengths, detecting traffic congestion in advance and preventing DDoS attacks. When evaluating the impact of network queue management algorithms, it is considered that the key measures of network performance are latency and packet loss rate. The NS3 program has full capabilities for simulating computer networks using models of traffic generators, protocols like IP and TCP, channels, and devices like LTE and Wi-Fi, and examines and visualizes the results. In addition, the results produced in the simulation must be represented as if they were in a real system.

In this thesis, several traditional or basic queue management algorithms are analyzed and compared in terms of delay, end-to-end throughput, pdf and fairness index, using several botnets.

According to the simulation result, the CoDel algorithm is the most efficient algorithm compared to other algorithms because it gives the lowest packet loss rate values and low delay. RED is the algorithm that produces the closest results to the CoDel algorithm. Followed, respectively, by the Pie, DropTail, and pFIFO algorithms. Since the CoDel algorithm evaluates the queue delay for each entering packet and determines whether or not to drop the packet based on the current queue time. As traditionally, queue management algorithms such as pFIFO and DropTail drop packets when the queuing router is full.

## REFERENCES


1. Soh, Y. S., Member, S., Quek, T. Q. S., and Member, S., "Energy Ef fi cient Heterogeneous Cellular Networks", 31 (5): 840–850 (2013).

2. Çakmak, M., and Albayrak, Z., "Mobile Communication - Past, Present and Future: a Review", ***International Conference on Advanced Technologies, Computer Engineering and Science***, 18 (2): 12–29 (2018).

3. Khare, V., Garg, S., Shukla, S., and Sharma, P., "Comparative Study of 1G, 2G, 3G and 4G", ***Journal Of Engineering Computers & Applied Sciences***, 2 (4): 55–63 (2013).

4. Lopa, M. and Vora, J., "Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G", ***International Journal Of Modern Trends In Engineering And Research***, 2 (10): 282–283 (2015).

5. Henrydoss, J. and Boult, T., "Critical security review and study of DDoS attacks on LTE mobile network", ***Proceedings, APWiMob 2014: IEEE Asia Pacific Conference On Wireless And Mobile 2014***, 194–200 (2014).

6. Wei, W., Song, H., Wang, H., and Fan, X., "Research and Simulation of Queue Management Algorithms in Ad Hoc Networks under DDoS Attack", ***IEEE Access***, 5: 27810–27817 (2017).

7. Çakmak, M., Albayrak, Z., and Torun, C., "Performance comparison of queue management algorithms in lte networks using NS-3 simulator", ***Tehnicki Vjesnik***, 28 (1): 135–142 (2021).

8. Paul, A., Kawakami, H., Tachibana, A., and Hasegawa, T., "Effect of AQM-Based RLC Buffer Management on the eNB Scheduling Algorithm in LTE Network", ***Technologies***, 5 (3): 59 (2017).

9. Singh, H., and Bansal, A., " Various Active Queue Management Techniques", ***International Journal of Scientific Research in Computer Science Applications and Management Studies***, 2 (5): (2011).

10. Albayrak, Z. and Çakmak, M., "A Review: Active Queue Management Algorithms in Mobile Communication", ***International Conference On Cyber Security And Computer Science***, (October 2018): 180–184 (2018).

11. Albayrak, Z., Musa, H., and Çakmak, M., "Performance Evaluation of WBANs MAC Protocols in Different dBm and OMNet++", ***Journal Of Intelligent Systems: Theory And Applications***, 4 (1): 1–7 (2021).

12. Çakmak, M. and Albayrak, Z., "LTE Ağlarda Remote-Host ile PG-W arasındaki Kuyruk Yönetim Algoritmalarının Performans Analizi", ***Academic Platform Journal Of Engineering And Science***, 456–463 (2020).

13. N.D., A. and A., R., "Avoiding queue overflow and reducing queuing delay at eNodeB in LTE networks using congestion feedback mechanism", ***Computer Communications***, 146 (July): 131–143 (2019).

14. Rukmani, P. and Ganesan, R., "Scheduling algorithm for real time applications in mobile ad hoc network with opnet modeler", ***Procedia Engineering***, 64: 94–103 (2013).

15. Zhang, G. A., Gu, J. Y., Bao, Z. H., Xu, C., and Zhang, S. B., "Joint routing and channel assignment algorithms in cognitive wireless mesh networks", ***Transactions On Emerging Telecommunications Technologies***, 25 (3): 294–307 (2014).

16. Ohta, M., "Overload control in a SIP signaling network", ***Transactions On Engineering Computing And Technology V***, 12 (12): 87–92 (2009).

17. Sharma, P., "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network", ***International Journal Of Computer Applications***, 41 (21): 16–21 (2012).

18. Sevindik, V., Wang, J., Bayat, O., and Weitzen, J., "Performance evaluation of a real long term evolution (LTE) network", ***Proceedings - Conference On Local Computer Networks, LCN***, 679–685 (2012).

19. Nossenson, R., "Long-term evolution network architecture", ***2009 IEEE International Conference On Microwaves, Communications, Antennas And Electronics Systems, COMCAS 2009***, (2009).

20. Park, E. and Del Pobil, A. P., "Modeling the user acceptance of long-term evolution (LTE) services", ***Annales Des Telecommunications/Annals Of Telecommunications***, 68 (5–6): 307–315 (2013).

21. Kim, Y. H., Han, Y. H., Kim, M., Park, Y. S., Moon, S. J., Lee, J. H., and Choi, D. K., "Distributed PDN gateway support for scalable LTE/EPC networks", ***2014 IEEE 11th Consumer Communications And Networking Conference, CCNC 2014***, (Ccnc): 139–144 (2014).

22. Rost, P., Banchs, A., Berberana, I., Breitbach, M., Doll, M., Droste, H., Mannweiler, C., Puente, M. A., Samdanis, K., and Sayadi, B., "Mobile network architecture evolution toward 5G", ***Infocommunications Journal***, 9 (1): 24–31 (2017).

23. Palat, S. and Godin, P., "Network Architecture", ***LTE - The UMTS Long Term Evolution: From Theory To Practice***, 21–50 (2009).

24. Hayashi, T., "Evolved Packet Core (EPC) network equipment for Long Term Evolution (LTE)", ***Fujitsu Scientific And Technical Journal***, 48 (1): 17–20 (2012).

25. Ouzzif, M., "4G System : Network Architecture and Performance", ***International Journal Of Innovatice Research In Advanced Engineering***, 2 (4): 215–220 (2015).

26. Kim, Y. hwan, Lim, H. kyo, Kim, K. han, and Han, Y. H., "A SDN-based distributed mobility management in LTE/EPC network", ***Journal Of Supercomputing***, 73 (7): 2919–2933 (2017).

27. Atayero, A. A., Luka, M. K., Orya, M. K., and Iruemi, J. O., "3GPP Long Term Evolution: Architecture, Protocols and Interfaces", ***International Journal Of Information And Communication Technology Research***, 1 (7): 306–310 (2011).

28. Rinne, M. and Tirkkonen, O., "LTE, the radio technology path towards 4G", ***Computer Communications***, 33 (16): 1894–1906 (2010).

29. Lo, A. and Niemegeers, I., "Multi-hop relay architectures for 3GPP LTE-advanced", ***Proceedings - MICC 2009: 2009 IEEE 9th Malaysia International Conference On Communications With A Special Workshop On Digital TV Contents***, (December): 123–127 (2009).

30. Chen, Y. and Lagrange, X., "Architecture and Protocols of EPC-LTE with relay", (January): (2013).

31. Dzivhani, M. and Ouahada, K., "Performance Evaluation of TCP Congestion Control Algorithms for Wired Networks using NS-3 Simulator", ***IEEE AFRICON Conference***, 2019-Septe: (2019).

32. Hamdi, M. M., Rashid, S. A., Ismail, M., Altahrawi, M. A., Mansor, M. F., and Abufoul, M. K., "Performance Evaluation of Active Queue Management Algorithms in Large Network", ***ISTT 2018 - 2018 IEEE 4th International Symposium On Telecommunication Technologies***, (May): 1–6 (2018).

33. Ryu, S., Rump, C., and Qiao, C., "Advances in internet congestion control", ***IEEE Communications Surveys & Tutorials***, 5 (1): 28–39 (2009).

34. Dergisi, F. B., "Evaluation of Active Queue Management Algorithms", ***İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi***, 4 (7): 123-139–139 (2005).

35. Mahida, P. T., "A Comparative Analysis of Queue Management Techniques", ***P. T. Mahida***, 65 (6): 2–5 (2013).

36. Karmeshu, Patel, S., and Bhatnagar, S., "Adaptive mean queue size and its rate of change: queue management with random dropping", ***Telecommunication***

***Systems***, 65 (2): 281–295 (2017).

37. Shnain, A. H. and Shaheed, S. H., "A comparative study of active queue management algorithms for network performance evaluation", ***International Journal Of Supply Chain Management***, 7 (3): 107–112 (2018).

38. Cip, C., Expertise, C., Networks, H., Science, B., and Transfers, D., "Lab 18 : Controlled Delay ( CoDel ) Active Queue Management", 11–18 (2019).

39. Kundel, R., Blendin, J., Viernickel, T., Koldehofe, B., and Steinmetz, R., "P4-CoDel: Active Queue Management in Programmable Data Planes", ***2018 IEEE Conference On Network Function Virtualization And Software Defined Networks, NFV-SDN 2018***, 1–4 (2018).

40. Kua, J., Nguyen, S. H., Armitage, G., and Branch, P., "Using Active Queue Management to Assist IoT Application Flows in Home Broadband Networks", ***IEEE Internet Of Things Journal***, 4 (5): 1399–1407 (2017).

41. Altunay, H. C., Albayrak, Z., Ozalp, A. N., and Cakmak, M., "Analysis of Anomaly Detection Approaches Performed through Deep Learning Methods in SCADA Systems", ***HORA 2021 - 3rd International Congress On Human-Computer Interaction, Optimization And Robotic Applications, Proceedings***, (June): (2021).

42. Rekhis, S., Chouchane, A., and Boudriga, N., "Detection and reaction against DDoS attacks in cellular networks", ***2008 3rd International Conference On Information And Communication Technologies: From Theory To Applications, ICTTA***, 1–6 (2008).

43. Michalas, A., Komninos, N., and Prasad, N. R., "Mitigate DoS and DDoS attack in mobile ad hoc networks", ***International Journal Of Digital Crime And Forensics***, 3 (1): 14–36 (2011).

44. Prasad, K. M., Reddy, A. R. M., and Rao, K. V., "DoS and DDoS Attacks: Defense, Detection and TracebackMechanisms -A Survey", ***Global Journal Of Computer Science And Technology***, 14 (7): 19 (2014).

45. Elleithy, K. and Blagovic, D., "Denial of Service Attack Techniques: Analysis, Implementation and Comparison", ***Journal Of Systemics, …***, 3 (1): 66–71 (2006).

46. Khosroshahy, M., Qiu, D., and Mehmet Ali, M. K., "Botnets in 4G cellular networks: Platforms to launch DDoS attacks against the air interface", ***2013 International Conference On Selected Topics In Mobile And Wireless Networking, MoWNeT 2013***, 30–35 (2013).

47. Gupta, S. G., Ghonge, M. M., Thakare, P. D., and Jawandhiya, P. M., "Open-Source Network Simulation Tools: An Overview", ***International Journal Of Advanced Research In Computer Engineering & Technology (IJARCET)***, 2

(4): 1629–1635 (2013).

48. Thapar, V., "A Comparative Study of Cloud Simulation Tools", ***International Journal On Computer Science And Engineering (IJCSE)***, 9 (06): 385–392 (2017).

49. Albayrak, Z. and Torun, C., "Recent LTE Simulation Tools", ***International Conference on Engineering and Naturel Sciences***, (September 2016): (2018).

50. Varga, A., "Using the OMNeT++ Discrete Event Simulation System in Education", ***IEEE Transactions On Education***, 42 (4): 372 (1999).

51. Mayer, C. P. and Gamer, T., "Integrating real world applications into OMNeT++", ***Technical Report TM-2008-2***, 1–9 (2008).

52. Schilling, B., "Qualitative Comparison of Network Simulation Tools", ***Qualitative Comparison Of Network Simulation Tools - Modeling And Simulation Of Computer Systems***, 1–15 (2005).

## RESUME

Aden ALI SAID graduated first and elementary education in Djibouti. He completed high school education at Gabode High School,then, he obtained bachelor's degree from University of Djibouti of Computer sciences and IUT (University Institute of Technologies) department of Sciences in 2017. Education, he studied Turkish Language from Çankırı/Turkey in 2018-2019. To complete M.Sc. education, he moved to Karabük/Turkey in 2019. He started his master education at the department of computer engineering in Karabuk University.