Research Article
Journal of Intelligient Systems: 7(1) (2024) 1-13
DOI: 10.38016/jista.1225716

The Impact of Denial-of-Service Attacks and Queue Management Algorithms on Cellular Networks

Muhammet Çakmak[1*]

[1]Sinop University, Department of Computer Engineering, Sinop, Türkiye

mcakmak@sinop.edu.tr

Abstract
In today's digital landscape, Distributed Denial of Service (DDoS) attacks stand out as a formidable threat to organisations all over the world. As known technology gradually advances and the proliferation of mobile devices, cellular network operators face pressure to fortify their infrastructure against these risks. DDoS incursions into Cellular Long-Term Evolution (LTE) networks can wreak havoc, elevate packet loss, and suboptimal network performance. Managing the surges in traffic that afflict LTE networks is of paramount importance. Queue management algorithms emerge as a viable solution to wrest control over congestion at the Radio Link Control (RLC) layer within LTE networks. These algorithms work proactively, anticipating, and mitigating congestion by curtailing data transfer rates and fortifying defences against potential DDoS onslaughts. In the paper, we delve into a range of queue management methods Drop-Tail, Random Early Detection (RED), Controlled Delay (CoDel), Proportional Integral Controller Enhanced (PIE), and Packet Limited First In, First Out queue (pFIFO). Our rigorous evaluation of these queue management algorithms hinges on a multifaceted assessment that encompasses vital performance parameters. We gauge the LTE network's resilience against DDoS incursions, measuring performance based on end-to-end delay, throughput, packet delivery rate (PDF), and fairness index values. The crucible for this evaluation is none other than the NS3 simulator, a trusted platform for testing and analysis. The outcomes of our simulations provide illuminating insights. CoDel, RED, PIE, pFIFO, and Drop-Tail algorithms emerge as top performers in succession. These findings underscore the critical role of advanced queue management algorithms in fortifying LTE networks against DDoS attacks, offering robust defences and resilient network performance.

Keywords: DDoS attacks, LTE network, Ns-3 simulation

DDoS Saldırılarının ve Kuyruk Yönetimi Algoritmalarının Hücresel Ağlar Üzerindeki Etkisi

Öz
Günümüzün dijital ortamında Dağıtılmış Hizmet Reddi (DDoS) saldırıları, dünyanın her yerindeki kuruluşlar için büyük bir tehdit olarak öne çıkıyor. Bilinen teknolojinin giderek ilerlemesi ve mobil cihazların yaygınlaşmasıyla hücresel şebeke operatörleri, altyapılarını bu risklere karşı güçlendirme baskısıyla karşı karşıya kalıyor. Hücresel Uzun Vadeli Evrim (LTE) ağlarına yapılan DDoS saldırıları büyük hasara, yüksek paket kaybına ve yetersiz ağ performansına yol açabilir. LTE ağlarını etkileyen trafikteki dalgalanmaları yönetmek büyük önem taşıyor. Kuyruk yönetimi algoritmaları, LTE ağları içindeki Radyo Bağlantı Kontrolü (RLC) katmanındaki tıkanıklığın kontrolünü ele geçirmek için geçerli bir çözüm olarak ortaya çıkıyor. Bu algoritmalar proaktif olarak çalışır, veri aktarım hızlarını azaltarak ve potansiyel DDoS saldırılarına karşı savunmayı güçlendirerek tıkanıklığı öngörür ve azaltır. Bu yazıda, Drop-Tail, Random Early Detection (RED), Controlled Delay (CoDel), Proportional Integral Controller Enhanced (PIE) ve Packet Limited First In, First Out queue (pFIFO) gibi çeşitli kuyruk yönetimi yöntemlerini derinlemesine inceliyoruz. Bu kuyruk yönetimi algoritmalarına yönelik titiz değerlendirmemiz, hayati performans parametrelerini kapsayan çok yönlü bir değerlendirmeye dayanır. LTE ağının DDoS saldırılarına karşı dayanıklılığını ölçüyoruz; performansı uçtan uca gecikmeye, üretime, paket dağıtım hızına (PDF) ve adalet endeksi değerlerine göre ölçüyoruz. Bu değerlendirmenin potası, test ve analiz için güvenilir bir platform olan NS3 simülatöründen başkası değildir. Simülasyonlarımızın sonuçları aydınlatıcı bilgiler sağlıyor. CoDel, RED, PIE, pFIFO ve Drop-Tail algoritmaları art arda en iyi performans gösterenler olarak ortaya çıkıyor. Bu bulgular, gelişmiş kuyruk yönetimi algoritmalarının, LTE ağlarını DDoS saldırılarına karşı güçlendirme, sağlam savunmalar ve esnek ağ performansı sunma konusundaki kritik rolünün önemini göstermektedir.

Anahtar kelimeler: DDoS atakları, LTE ağı, Ns-3 simülasyonu

* Corresponding Author.
E-mail: mcakmak@sinop.edu.tr

Recieved : 28 Dec 2022
Revision : 14 Jun 2023
Accepted : 28 Sep 2023

1. Introduction

The rapidly developing technology has increased the number of mobile phones used in cellular networks. Cellular network operators invest more in research and technology to secure against increasing data and network traffic. It is an important problem for attackers to cause network disruptions and block user services (Zenitani, 2023). DDoS attacks that occur in the LTE network cause mobile network users to disconnect or decrease the Quality of Service (QoS) (Feng et al., 2020).

DDoS attacks, which disrupt services on the network, are challenging to detect. DDoS attacks that occur in the LTE network affect all network layers but significantly affect the Radio Link Control (RLC) layer is a protocol layer in the LTE (Long-Term Evolution) wireless communication standard. It is responsible for ensuring the reliable transmission of data between the source and destination over the wireless link (Çakmak et al., 2021). One of the LTE cellular networks' main aims is developing queue management algorithms for RLC. Queue management method algorithms are used to ensure resource allocation and quality of service (QoS) during network congestion (Çakmak et al., 2022). Active Queue Management (AQM) algorithms enable efficient use of services such as delay, high bandwidth, and packet delivery speed. AQM mechanisms are used in LTE cellular networks under DDoS attacks(Wang and Wang, 2020). As a result, complete disconnection, connection slowdowns, disruptions of service, and potential data loss issues that could occur on the LTE network are prevented.

A DDoS attack occurring on a cellular LTE network can cause the entire network to go down, slowing it or preventing the use of network bandwidth. Choosing a practical algorithm for the security of the LTE network and the continuation of its services is crucial. Although DDoS attacks have been tested on the cellular LTE network to date, the performance of these attacks on queue management algorithms has not been assessed. Unlike other studies, this study evaluated the performance of queue management algorithms against DDoS attacks in the RLC layer of the cellular LTE network. Well-known Drop-Tail, RED, CoDel, PIE, pFIFO algorithms were compared under DDoS attacks in LTE networks according to end-to-end delay, throughput, PDF and fairness index values. PDF is a metric that measures the percentage of packets successfully delivered to their intended destination in a network.

DDoS attacks on LTE networks cause the network to be temporarily or completely disabled. It also causes disruption of services. Queue management algorithms create a preliminary protection area to prevent attacks and reduce their impact. It prevents congestion in queue buffers, controls packet drops, and regulates excessive demands.

Although loss-based, delay-based, rate based, queue-based, topology based, machine-learning based and hybrid-based studies have been carried out in LTE networks to date, the performance of DDoS attacks with queue management algorithms in LTE networks has not been examined. In this study, unlike others, the performances of the queue management algorithms in the LTE RLC layer under DDoS attacks were compared according to end-to-end delay, throughput, PDF and fairness index values using the NS-3 network simulator. Unlike others in these studies:

- The impact of queue management algorithms on the cellular LTE network under DDoS attacks was examined.
- Comparative performance of queue management algorithms against DDoS attacks in the RLC layer of the LTE network is shown.
- Well-known Drop-Tail, RED, CoDel, PIE, pFIFO algorithms were compared according to end-to-end delay, throughput, PDF and fairness index values under DDoS attacks in LTE networks.

The remainder of the study is organised as follows. In the second chapter, background and literature studies were examined. In the third section, an experimental framework and performance evaluation are provided. The results are given in the fourth section.

2. Background and Related Works

2.1. LTE Network Architecture

LTE, which stands for Long-Term Evolution, is a cellular communication standard that provides high mobile voice traffic and short messaging services (Wu et al., 2022). The LTE core network is divided into two main sections, as indicated in Figure 1, the E-UTRAN (Evolved Universal Terrestrial Access Network) and the EPC (Evolved Packet Core). The E-UTRAN disposes of an eNB (base station), which serves as the gateway between mobile terminals, radio antennas, and operators (Israr et al., 2021). eNBs are a base station that controls cell phones in the cell. It is defined as the eNB serving when the base station communicates with a mobile phone. eNBs communicate with mobile phones using analogue and digital signals via the air interface. eNB controls the operation of all mobile phones by sending signal messages (Zidic et al., 2023). eNBs are connected to the EPC via the S1 interface. The eNB accesses nearby base stations using the X2 interface for signalling and packet forwarding during transmission. EPC consists of three functional modules: Mobility Management Entity (MME), Service Gateway (S-GW), and Packet Data Network Gateway (PDN-GW). The MME delivers a paging message to the base station to provide service in the Core System (CS) domain. The S-GW connects LTE nodes and transmits user data packets. S-GW works like a router. In addition, S-GW sends the obtained data between the base station and the

PDN-GW (Mousavi et al., 2017). The Home Subscriber Server (HSS) is a central database that stores information about the cellular network operator's subscribers. The Policy Control and Pricing Rules Function (PCRF) decides on policy control. It also controls flow-based charging functions. The LTE network is connected to the rest of the Internet via PDN-GW (Oughton et al., 2022). The PDN-GW connects the EPC unit to external IP networks. PDN-GW forwards packets to external IP networks. It also allocates IP addresses to all users. It handles IP user traffic-related operations, including packet filtering.

LTE network architecture consists of Physical Layer (Layer 1), Medium Access Layer (MAC), Radio Link Control (RLC), Radio Resource Control (RRC), Packet Data Convergence Control (PDCP), and Non-Access Stratum (NAS) Protocols(Mousavi et al., 2019).

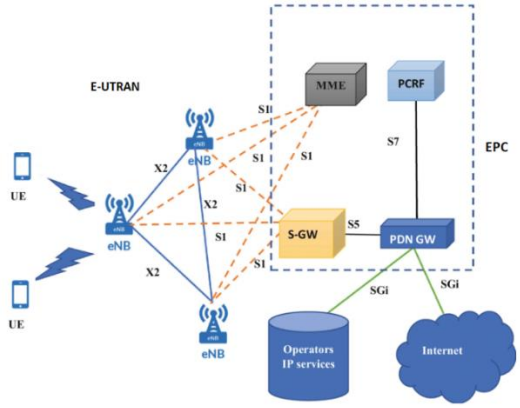

Figure 1. LTE Architecture (Gómez et al., 2014)

Figure 2 shows the data flow in the RLC, PDCP, and MAC layers.

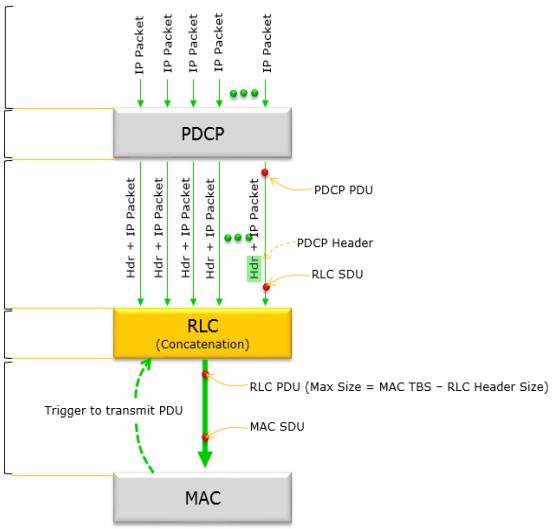

Figure 2. LTE MAC, RLC and PDCP Layers (Gómez et al., 2014)

The RLC layer is used for segmentation, efficient transport, and sequential transmission. RLC analyses the initial data units containing information of a particular type and ensures the security of the target data transmission. More control or security is needed at the RLC layer. Because the RLC layer is used in all transmission of data packets such as voice, video, and FTP, when a DDoS attack or other attack reaches the RLC level, it can cause packet loss or slow throughput, long packet delays, traffic congestion, and heavy and inefficient network performance.

2.2. DDoS Attacks

A DDoS attack is a malicious attempt to disrupt the regular traffic of the target server, service, or network by crushing it with a stream of internet traffic. DDoS attacks provide activity using multiple computer systems. These attacks can use resources such as computers, mobile phones, and IoT devices to execute an attack on the target. During a high-level DDoS attack, the victim network experiences unexpected traffic congestion, preventing regular traffic from reaching its destination. A standard method in a DDoS attack is for the attacker to send a stream of packets to a victim. This transmitted stream consumes significant resources, preventing the real user from accessing the resources (Ali et al., 2022; Said et al., 2022). Another method is to send malformed packets, which disable or blocks the application or protocol on the target machine. Some attacks block services by overloading the Internet infrastructure instead of targeting victims. A DDoS attack is also an effective attack technique to consume resources so that legitimate clients cannot receive internal or external services.

2.3. Queue Management Algorithms

Queue Management algorithms have been developed to detect and protect the network from this congestion. Queue management algorithms prevent packet loss in the network, reduce delays, detect network congestion, and recoverm congestion (Çakmak and Albayrak, 2018 ; Akhter et al., 2021). Passive queue management algorithms such as drop-tail only forward queued packets sequentially, while active queue management algorithms can pre-identify congestion and minimise packet transfer rate. This study evaluated several queue management algorithms, including well-known options like Drop-Tail, RED, CoDel, PIE, and pFIFO. Our analysis focused on their effectiveness in mitigating DDoS attacks on LTE networks.

Drop-Tail is simply the most straightforward queue management algorithm. It is often used in routers due to its simple control mechanism. Drop-Tail provides priority forwarding of the first packets to the queue. New packets are automatically rejected if the queue is full. The arrival speed of the packets can be greater than the output speed. Drop-Tail, the priority levels of all packets are the same and this causes traffic congestion and bottleneck.

RED is the first AQM algorithm for congestion. It calculates network congestion using the average queue

size to avoid congestion in RED packet switched networks. The RED algorithm manages the queue size using four parameters: the minimum threshold (Minth), the maximum threshold (Maxth), the maximum probability, and the weighting factor. The minimum and maximum points determine the queue sizes within which packets are marked. In contrast, the maximum likelihood sets the maximum drop probability for packets exceeding the maximum threshold. The weighting factor controls the rate at which the average queue size is computed over time, with higher values giving greater weight to recent samples. The algorithm works to maintain an average queue size. The packet drop probability value, Pd, varies linearly between zero and Pmax as the mean queue size changes between the Minth and Maxth values. All incoming packets are dropped if the average queue size value exceeds Maxth (Paul et al., 2017). The RED algorithm controls the congestion structure due to packet drop because the packet drop mechanism operates according to the moving average of the past values.

CoDel was developed to solve the bottleneck problem in the network (Raghuvanshi et al., 2013). Congestion is detected by CoDel when the packet transmission time exceeds the set target value. After the congestion is detected, the signal is sent to drop the packet to avoid clutter in the queue. CoDel detects congestion in the network using the packet delay time. Buffer bloat causes packet losses to increase in the queue even when the buffer size is large. The CoDel algorithm efficiently controls the buffer-bloat problem. Unlike RED, CoDel is independent of parameters such as queue size and average, queue delay, and drop rate.

pFIFO is an active queue management algorithm based on the FIFO algorithm (Bisoy and Pattnaik, 2016). It is classified by considering different channels for network traffic. High-priority traffic is processed earlier. Its main purpose is a simple method to support differentiated service classes. The advantage of pFIFO is low computational load and traffic transmission generated in real-time applications. The most critical problem in the network is that the volume of high-priority traffic is high, the buffer space allocated for low-priority traffic is reduced, and overflow occurs. This causes packet drop on the network and slows down the network (Low et al., 2002).

PIE is designed to control latency in the network effectively (Pan et al., 2013). In PIE, the average queue rate is estimated relative to the non-moving queue. The speed is used to calculate the available delay. Then, the delay is periodically used to calculate the probability of falling. Finally, when the packet arrives at the destination, a packet is dropped (or flagged) based on that probability. PIE adjusts probability based on latency trend. Alpha and beta are statically selected parameters chosen to control the fall probability increase and are determined by control theoretical approaches. Alpha determines how the deviation between the current and target delay changes the probability. The beta makes additional adjustments based on the lag trend. PIE is designed to improve time-sensitive performance and strives to provide interactive traffic and network stability while maintaining high connection usage. Adapting the control parameters in small increments voids large oscillations leading to unbalance(Pan et al., 2013).

2.4. Related Works

Researchers and developers have proposed various queue management algorithms to address congestion and performance issues in wired and wireless networks. These algorithms aim to improve network performance by managing the flow of packets in the network queues. These algorithms aim to improve features like network utilisation, packet loss, and adaptability for different traffic loads.

The proposed AQMs aim to solve problems such as loss-based congestion control (Verma et al., 2022) delay-based congestion control and rate-based congestion control (Amer et al., 2020). For eNB on LTE, smRED (smart-RED), a smart AQM that works by adjusting the variance value in RED to prevent buffer congestion and packet drop in variable traffic loads at the RLC layer, enables packet programmers to work through single-cell and multicell handover and no failover. The study investigated the effects of the queue management algorithms on the network performance metrics, including throughput, delay, and deviation values. The adjusted variance value *i* of RED took different values in low and high-load situations, affecting the drop of packets accumulated in RCL buffers (Paul et al., 2017).

The authors introduced an innovative machine learning-based intrusion detection system to mitigate Distributed Denial of Service (DDoS) attacks within the LTE-A network. The proposed model effectively identifies DDoS flows targeting the eNB and utilises the random forest algorithm for attack classification. Remarkably, the system achieved an impressive accuracy rate of 99.95% in accurately identifying and classifying DDoS attacks (Gong et al., 2019).

In a separate study, the authors introduced the DDoS Threat Analysis and Response Framework (DTARS), which encompasses distributed real-time threat identification, behavioural monitoring, and validation of control plane operations specifically tailored for LTE networks (Krishnan et al., 2019).

In another study, the authors proposed an improved Neural Network (NN) model for intrusion detection, which identifies authenticated nodes and cluster heads (CH) using elliptic curve cryptography (ECC) in the LTE network for Machine Type Communication (MTC) devices. In case of an attack, the proposed model imposes a penalty and restricts the affected nodes from participating in MTC communication. Specifically, the improved NN was created using a new optimisation

algorithm called Whale with Three-Level Update (WTU) (Jyothi and Chaudhari, 2020).

The packet congestion feedback mechanism proposed by the authors was developed to avoid queue overflow in the LTE networks and reduce queuing delays. With the QoS value of the packets in the network, the packet is defined as TCP or UDP. An average value was calculated to estimate full queues, and low ranges for TCP and high ranges were determined for UDP. Setting the sender congestion window to high, medium and low according to the network traffic situationit has been tried to prevent the queue overflow in Evolved Node B (eNB) (Adesh and Renuka, 2019).

In another study, the authors classified DDoS attacks in the LTE network with logistic regression and decision tree machine learning algorithms (Ashfaq et al., 2022).

The authors examined the performance of AQMs operating in the RLC layer of the cellular LTE network according to end-to-end delay, throughput, PDF and fairness index values. The study has shown that the selection of the right queue management algorithm directly affects the performance of the network (Çakmak et al., 2021; Çakmak and Albayrak, 2022). The authors proposed an adaptive queue management algorithm operating at the RLC layer of the cellular LTE network. The proposed algorithm adaptively adjusts the network's throughput according to low, medium and high network load (Çakmak and Albayrak, 2022).

Praveen and Pratap (2021) proposed a congestion-sensitive resource allocation and routing protocol (CRR) based on hybrid optimisation techniques for IoT devices in smart city infrastructure. The proposed method uses a meta-heuristic algorithm to reduce total congestion and allocate IoT gateways. It also uses a swarm optimisation algorithm for the route discovery mechanism. The proposed ECRR technique was designed and implemented with the NS-2 simulator. The authors examined the AQM mechanism based on neural networks. The study aims to employ machine learning techniques to learn the behaviour of the Active Queue Management (AQM) mechanism. Specifically, the study seeks to develop a model that can predict the behaviour of the AQM mechanism in response to changes in network traffic conditions, such as variations in traffic volume or type, to improve network performance and reduce congestion. Obtains training examples considering the similarity of network traffic. The model uses the Gaussian method. The study demonstrates the effectiveness of the active queue management mechanism based on neural networks (Szyguła et al., 2021). In another study, the authors proposed the Federated Intelligence (FIAQM) architecture for AQM, using the Federated Learning approach. The proposed method dynamically adjusts the AQM parameters for a multi-domain environment, which is difficult to achieve with conventional AQM. The proposed FIAQM method uses a trained feedforward neural network trained on a network traffic dataset to predict the behavior of the Active Queue Management (AQM) mechanism in response to changes in traffic conditions. In addition, the developed method improves the performance of FIAQM's inter-domain connections by reducing congestion in its connections while keeping the network data private in each participating domain (Gomez et al., 2021).

The authors propose an algorithm for fair bandwidth distribution, considering traffic class priority, connected loads of a node, and average queue size. The average queue size across the nodes is adjusted based on the gradient suggested for the Global Priority (GP) differential, which is a metric that assigns priorities to different types of network traffic based on their importance. Specifically, the proposed mechanism uses the GP differential to determine the relative importance of different traffic flows in the network and adjusts the average queue size accordingly. This allows for more efficient allocation of network resources and improved Quality of Service (QoS) for critical traffic flows. The node's speed is calculated based on the node's average queue size and GP. The proposed routing protocol is designed for Wireless Sensor Networks (WSN), networks of small, low-power devices equipped with sensors that collect and transmit data wirelessly. The protocol is optimised for WSNs, which typically have limited resources such as bandwidth, energy, and computational power and operate in environments where the network topology may change frequently. The proposed method is applied to a tree topology that deals with both Real-Time (RT) and Non-real-time (NRT) traffic classes (Swain and Nanda, 2021). Table 1 shows control mechanism literature for LTE networks.

Table 1. Control mechanism literature for LTE networks

Study	Year	Reference
Loss-based congestion control	2022	(Verma et al., 2022)
Delay-based congestion control	2021	(Lin et al., 2021)
Rate-based congestion control	2020	(Amer et al.)
	2019	(Paul et al.)
Topology-based mechanism	2021	(Swain and Nanda)
Machine-learning based control	2019	(Gong et al.)
	2020	(Jyothi and Chaudhari)
	2021	(Szyguła et al.)
	2021	(Gomez et al.)
Hybrid control mechanism	2021	(Praveen and Pratap)
	2022	(Çakmak and Albayrak)

Although loss-based, delay-based, rate-based, queue-based, topology-based, machine-learning-based, and hybrid-based studies have been carried out in LTE networks, the performance of DDoS attacks with queue management algorithms in LTE networks has not been examined. A DDoS attack on a cellular LTE network can cause a temporary disruption and potentially degrade the network's performance, as it overwhelms the network with many requests, making it difficult for

legitimate users to access network resources. However, it does not permanently turn off the entire network. Although security studies have been done in the cellular LTE network, the security of the RCL layer has not been directly tested. Preventing DDoS attacks that may occur at the RCL layer will increase the performance of cellular network security. In this study, unlike others, the versions of the queue management algorithms in the LTE RLC layer under DDoS attacks were compared according to end-to-end delay, throughput, PDF and fairness index values using the NS-3 network simulator.

3. Experimental Framework and Performance Assessment

In this section, the network topology and system parameters for the LTE network are determined. Then the simulation results were analysed and evaluated according to the end-to-end average throughput, delay, PDF and fairness index.

For the experimental environment,

* Firstly, eNB and nodes are created in the NS3 environment.

*Parameter of eNB is set.

*BotNets are placed according to the specified numbers in accordance with the topology.

*Simulation starts

*Drop-tail, RED, CoDel, pFIFO and PIE algorithms are run separately at simulation time.

*Test results are saved as end-to-end average throughput, delay, PDF and fairness index

*Simulation is terminated.

3.1. Network Topology and Simulation Environment

One of the easiest and most effective ways to empirically observe traffic on the network is to use simulation. Using simulation, network nodes, connections and network traffic can be designed similarly to the real world (Jevtić et al., 2009) and (Weingärtner, et al., 2009). In addition, simulation makes it cheaper and easier to implement systems that are difficult and very expensive to implement in the real world. Ns3 network simulator is free open-source software developed for educational and research purposes and works on a discrete event basis. Parameter settings for the Ns3 simulation environment were made as follows:

*Basic eNB added

*MTU value for SGW and PDN-GW is set to 1500 bytes

*Inter-unit data rate was selected as 100 Gbps, which is the maximum supported by eNB

* eNB delay set to optimum value 0.01s

* eNB connection latency set to 2ms.

*TCP New Reno module was used as TCP traffic type

*Attackers' displacement feature was selected as RandomWalk2D

*For Droptail's package, a maximum of 50 packages, 100 ms interval and 5ms target value were selected

*For RED, the minth value for sending 50 packets of data is determined as 20 and the maximum value is 50. Queue weight value was determined as 0.002s

*Limit package setting for pFIFO was set as 50 packages

*Average queue delay value for PIE was set to 0.01s

*Simulation completed between 0.1s and 100s.

This study designed an LTE network structure and attack scenario suitable for the actual situation. Thus, the obtained data is more similar to the actual system. In the experimental environment, 1 eNB is attacked by DDoS with 10, 20, 40, 60, and 100 attackers, respectively. In simulation, data traffic starts from 0.1 seconds and the simulation takes 100 seconds. Drop-tail, RED, CoDel, pFIFO and PIE algorithms were run in each attack. The results were compared to the average end-to-end throughput, delay, PDF and fairness index. The simulation parameters showed in Table 2.

3.2. Experimental Results

The simulation results were analysed using average end-to-end delay, throughput, PDF, and fairness index values. For the real-world simulation environment, a DDoS attack is carried out on 1 eNB by 10, 20, 40, 60 and 100 attackers, respectively.

Table 2. Simulation Parameters

	SGW and PDN-GW Gateway	
	Parameters	**Value**
LTE	MTU (Maximum Transmission Unit)	1500 Bytes
	Data Rate	100 Gbps
	Delay	0.010 s
	Wired Link Capacity	100 Mbps
	Data Rate	100 Gbps
	Delay	2 ms
	Botnet Number	10, 20, 40, 60, and 100
	TCP Traffic Type	TCP New Reno
	Mobility	RandomWalk2D
	Queue Algorithms	
Drop-tail	Mode (Bytes, Packets)	Packets
	Max Packets	50
Codel	Mode	Packets
	Max Packets	50
	Interval	100 ms
	Target	5 ms
RED	Mode	Packets
	MeanPktSize	50
	IdlePktSize	1500*1000bytes
	MinTh, MaxTh	20,50
	Queue Limit	50
	Queue weight	0,002s

	Link Delay	20ms
pFIFO	Limit	50 packets
PIE	Average Queue Delay	0.01 s
Simulation Time		
Simulation Start Time		0.1 s
Total Simulation Time		100 s

Figure 3 shows the packet control flow structure of the Drop-tail RED, CoDeL, PIE and pFIFO algorithms for the simulation environment.

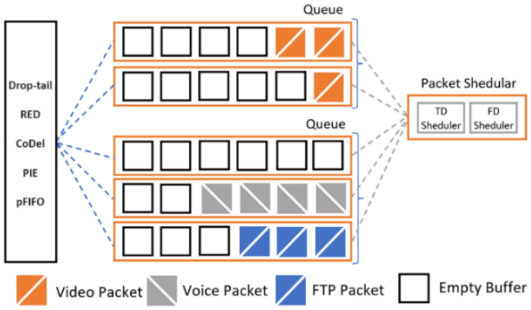

Figure 3. Simulation Packet Controller

Figure 4 shows the network topology of the simulation.

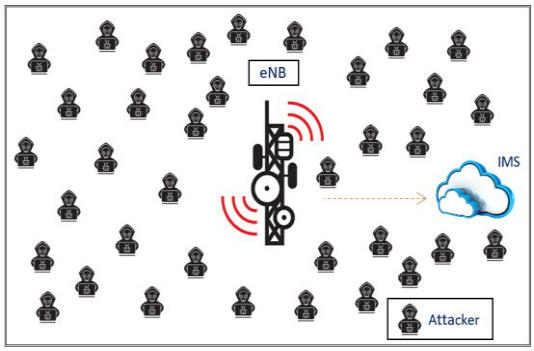

Figure 4. Simulation network topology

Pseudo code of the system.

1: procedure enodeb (parameters)
2: Initialize variable
3: Arrive packets on RLC
5: Attack on system
4: (Droptail, RED, CoDel, PIE, and pFIFO) apply on RLC
5: Check the packets
6: End the process

3.2.1 Average End-to-end Throughput

Drop-tail, RED, CoDel, pFIFO and PIE algorithms were compared using 10, 20, 40, 60 and 100 botnets in the LTE network environment. Table 3 shows the average throughput values of the LTE RLC layer under DDoS attacks. The variation of the end-to-end average throughput values according to the number of botnets is shown in Figure 5.

Table 3. End-to-end Throughput

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

The average end-to-end output throughput values obtained with the increase in the number of botnets showed a natural decrease. CoDel algorithm showed the best performance in terms of end-to-end throughput value even in high botnet attack. Other best performing algorithms are listed as RED, PIE, pFIFO, and Drop-Tail respectively. The CoDel algorithm gives the best results due to early detection of packet drops and processing according to the queuing time of packets. Drop-Tail algorithm, which dropped incoming packets after the queue is full, gives the worst result among all algorithms. This shows that Drop-tail is the most vulnerable algorithm for high traffic.

The presented data outlines the Average Throughput (measured in Kbps) achieved by various AQM (Active Queue Management) algorithms across different scenarios involving varying numbers of BotNets. When confronted with 10 BotNets, the CoDel algorithm exhibits the highest throughput at 2914.524 Kbps, closely followed by the PIE algorithm at 2756.93 Kbps. The RED algorithm also demonstrates commendable performance, achieving a throughput of 2793.681 Kbps. In contrast, both Drop-Tail and pFIFO algorithms yield lower throughputs at 2492.157 Kbps and 2554.671 Kbps respectively. As the number of BotNets increases to 20, 40, 60, and eventually 100, a discernible pattern emerges. CoDel consistently maintains its lead in throughput across all scenarios, showcasing its superior ability to handle network congestion, even in high-stress situations with a substantial number of BotNets. RED

and PIE algorithms also exhibit competitive performance, with both consistently achieving noteworthy throughput values. Conversely, Drop-Tail and pFIFO face considerable challenges, with their respective throughputs experiencing significant drops as the number of BotNets increases. This comparative analysis underscores the efficacy of CoDel in managing network congestion and maximising throughput, particularly in scenarios with a high BotNet count.

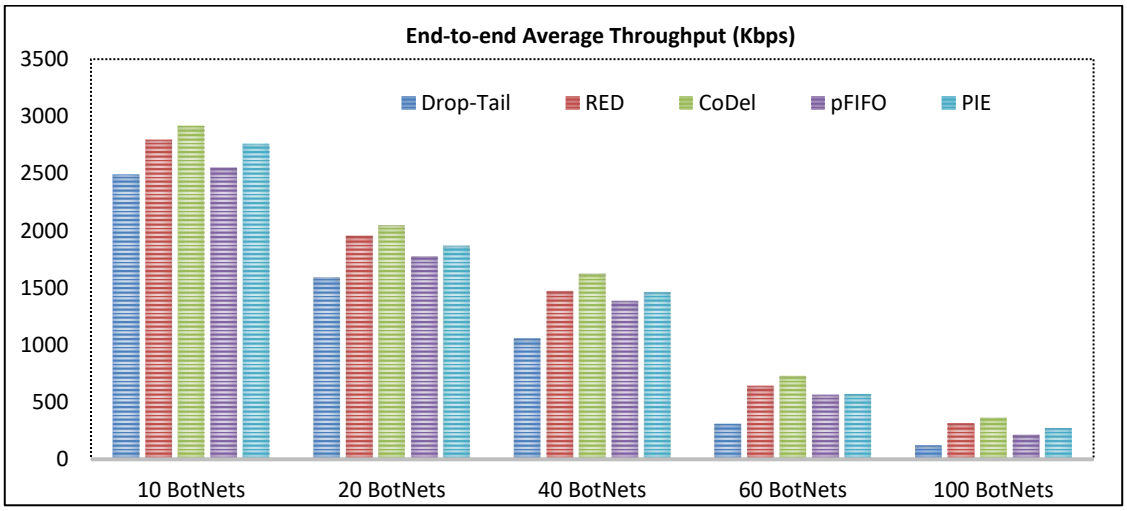

Figure 5. Average End-to-end Throughput Under DDoS Attacks

3.2.2 Average End-to-end Delay

Drop-tail, RED, CoDel, pFIFO and PIE were compared in an LTE network environment using 10, 20, 40, 60 and 100 botnets. Table 4 shows the average throughput values of the LTE RLC layer under DDoS attacks.

Table 4. End-to-end Delay

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

Figure 6 shows the aveage end-to-end delay based on the number of botnets. Packets coming from the PDN-GW router significantly affect parameters such as modulation, encoding, and packet creation time. These parameters are adversely affected in a DDoS attack. CoDel does not use the size of the queue to manage the queue, it uses the queuing time of the packets. This ensures that the packet drop value of the CoDel algorithm is low. Thus, the end-to-end delay value of CoDel is lower than other algorithms. Dropping more packets due to a DDoS attack caused more delay. The CoDel algorithm has the best end-to-end delay performance, with the lowest packet loss rate under DDoS attack. The Drop-Tail drops the packets arriving to the queue from the front if the queue is full. Therefore, Drop-tail has the worst performance among all algorithms. This algorithm is followed by RED, PIE, pFIFO and Drop-Tail, respectively. The CoDel algorithm is followed by RED, PIE, pFIFO and Drop-Tail, respectively.

Average Delay (measured in milliseconds) experienced with various AQM (Active Queue Management) algorithms across different scenarios involving varying numbers of BotNets. With 10 BotNets, the CoDel algorithm demonstrates the lowest delay at 26.751 ms, closely followed by the RED algorithm at 29.193 ms. In contrast, Drop-Tail experiences significantly higher delays at 74.686 ms. As the number of BotNets increases to 20, 40, 60, and eventually 100, a clear trend emerges. CoDel consistently maintains its lead in minimising delay across all scenarios, showcasing its superior ability to manage network congestion, even in high-stress situations with a substantial number of BotNets. RED and PIE algorithms also exhibit competitive performance, with both consistently achieving lower delay values. Conversely, Drop-Tail and pFIFO face

considerable challenges, with their respective delays experiencing substantial increases as the number of BotNets escalates. This comparative analysis underscores the effectiveness of CoDel in reducing network delay and enhancing overall performance, particularly in scenarios with a high BotNet count.

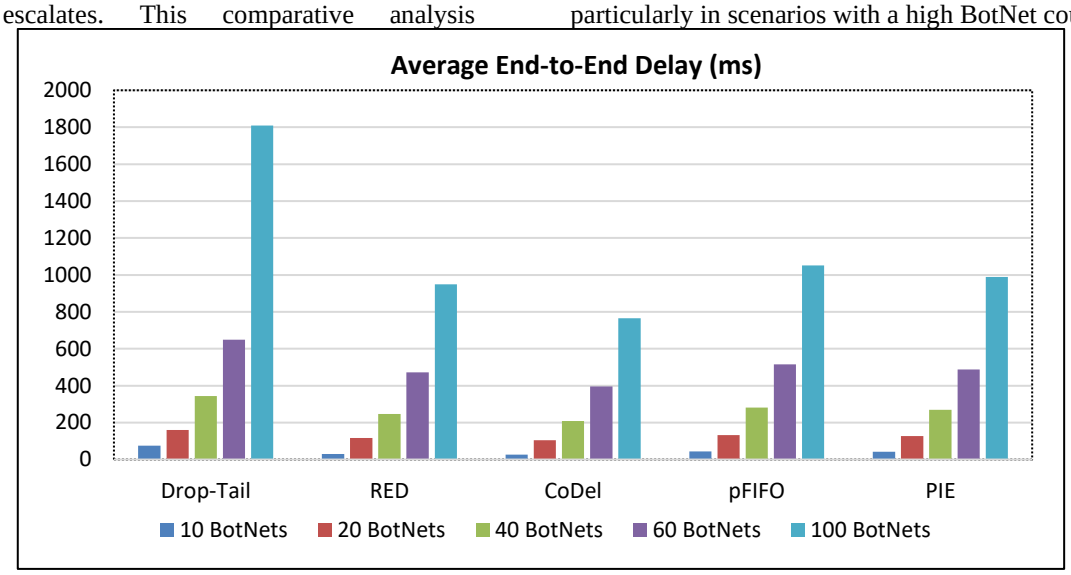

Figure 6. Average End-to-end Delay Under DDoS Attacks

3.2.3 Average End-to-end PDF

Drop-tail, RED, CoDel, pFIFO and PIE were compared using 10, 20, 40, 60 and 100 botnets in the LTE network environment. Table 5 shows the average PDF values of the LTE RLC layer under DDoS attacks.

Table 5. End-to-end PDF

AQM	Average PDF(%)				
	10 BotNets	**20 BotNets**	**40 BotNets**	**60 BotNets**	**100 BotNets**
Drop-Tail	89	81	64	54	8
RED	97	87	75	69	51
CoDel	98	89	76	72	57
pFIFO	93	83	71	59	38
PIE	95	86	73	61	42

The packet delivery rate, PDF, is calculated as the ratio of the total packets sent to the total packets received. The PDF value is an important parameter that shows the network's performance. Figure 6 shows the end-to-end average PDF based on the number of botnets. As the number of botnets increases, the demanded amount of resources also increases. User packets are accumulated in the queues of the RLC layer. Accumulated packets are held for resource allocation. Due to the DDoS attack, there is a decrease in PDF value because the resource allocation is not sufficient. With an increasing number of botnets, all algorithms get lower PDF values due to excessive packet drop. CoDel, RED, PIE, pFIFO ,and Drop-Tail get the best PDF values, respectively. Figure 7 shows the average end-to-end PDF values. The provided data illustrates the Average PDF percentages for various AQM (Active Queue Management) algorithms under different scenarios involving varying numbers of BotNets. When faced with 10 BotNets, the CoDel algorithm outperforms its counterparts, achieving an impressive 98% Average PDF. Following closely behind, the PIE algorithm demonstrates substantial efficiency with a PDF of 95%. Meanwhile, Drop-Tail and pFIFO exhibit decreasing performance with PDF values of 89% and 93% respectively. As the BotNet count escalates to 20, 40, 60, and eventually 100, a clear trend emerges. Across all scenarios, CoDel consistently maintains its lead, demonstrating superior PDF percentages compared to other AQM strategies. RED and PIE algorithms also exhibit competitive performance, with both showcasing robust PDF percentages. Conversely, Drop-Tail and pFIFO face significant challenges as the number of BotNets increases, with notable reductions in their respective PDF values. This comparative analysis highlights the effectiveness of CoDel in managing network congestion, particularly in high-stress scenarios with a substantial number of BotNets.

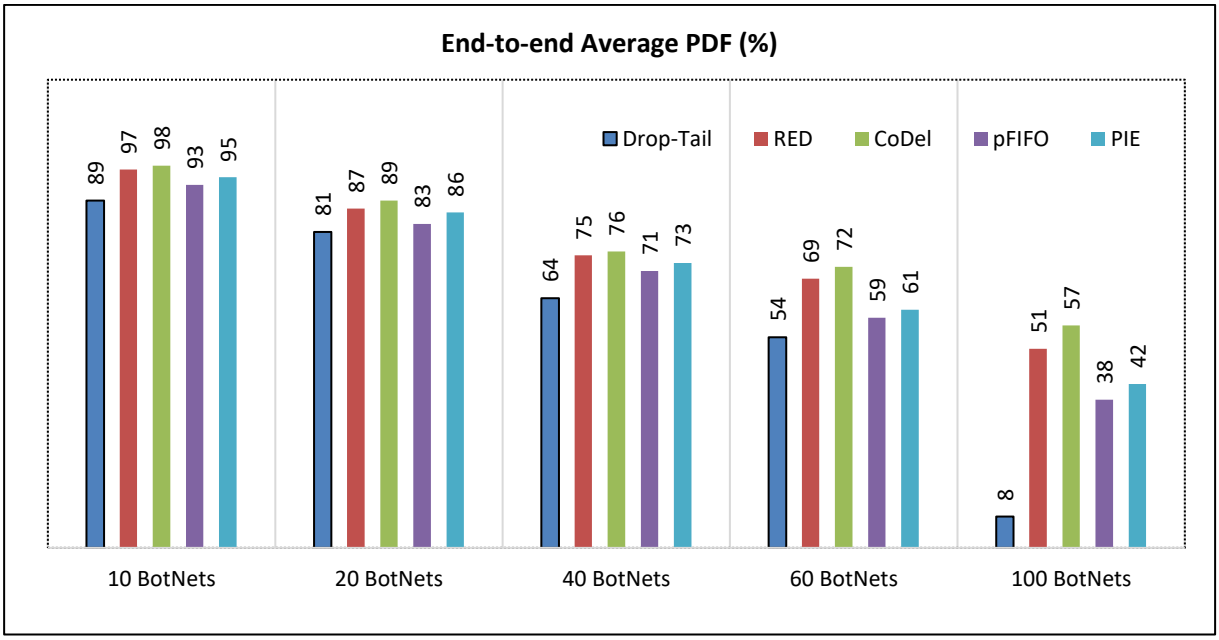

Figure 7. Average End-to-end PDF Under DDoS Attacks

3.2.4 Average End-to-end Fairness Index

Drop-tail, RED, CoDel, pFIFO and PIE were compared using 10, 20, 40, 60 and 100 botnets in the LTE network environment. Table 6 shows the average fairness index values of the LTE RLC layer under DDoS attacks.

Table 6. End-to-end Fairness Index

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

As the number of botnets connecting to eNB increases, the amount of resources also demanded increases. Normal users expect resource allocation, and a fair allocation of resources is required for requested resources. Figure 8 shows the end-to-end average fairness index values according to the number of botnets. As the DDoS attack increases, the packets coming into the queue begin to drop. Excessive packet drops reduce the fairness index value of the network. Also, the attack causes network latency. CoDel does not use the size of the queue to manage the queue; it uses the queue time of the packets. This ensures that the fairness index value of the CoDel algorithm is high. The CoDel algorithm is followed by RED, PIE, pFIFO, and Drop-Tail, respectively.

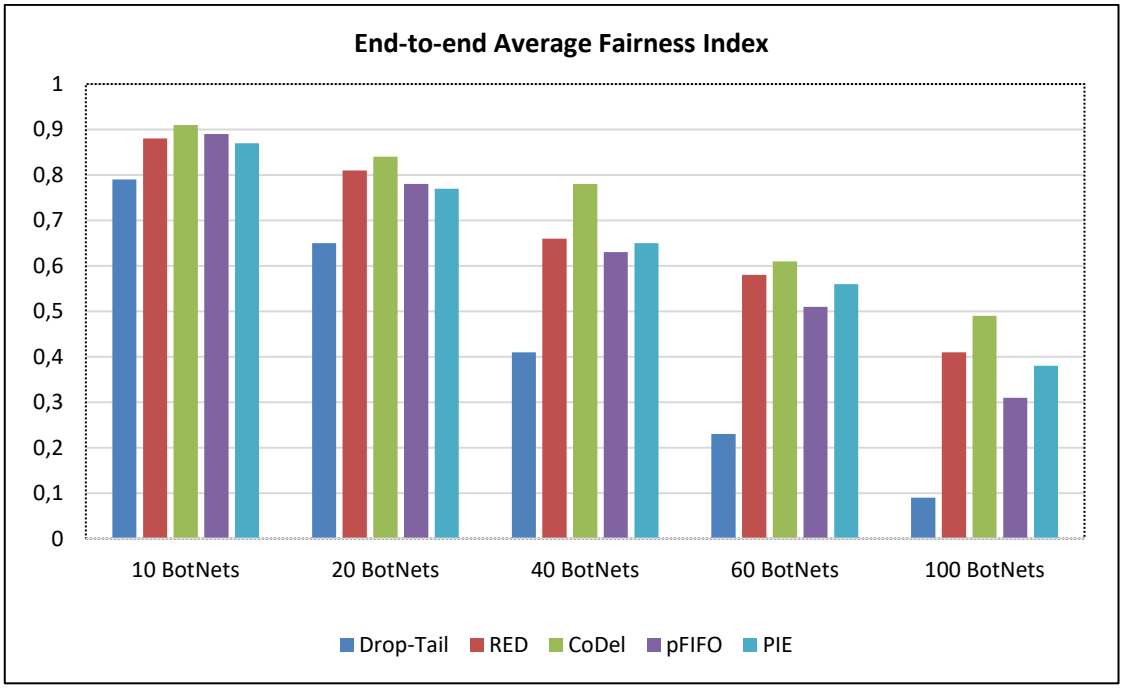

Figure 8. Average End-to-end Fairness Index Under DDoS Attacks

Packets coming from the PDN-GW router significantly affect parameters such as modulation, coding, and packet generation time. These parameters are negatively affected in a DDoS attack. CoDel does not use the size of the queue to manage it; it uses the time it takes for packets to queue. This ensures that the packet drop rate of the CoDel algorithm is low. Therefore, the end-to-end delay value of CoDel is lower than that of other algorithms. More packets dropped due to a DDoS attack cause more delay. The CoDel algorithm yields the best results due to its early detection of packet drops and processing of packets according to their queue time. As the number of botnets increases, the amount of requested resources also increases. User packets are collected in the queues of the RLC layer. The accumulated packets are retained for resource allocation. Due to the DDoS attack, the PDF value decreases because the resource allocation is insufficient. With the increase in the number of botnets, all algorithms obtain lower PDF values due to excessive packet drops. As the DDoS attack escalates, the packets arriving in the queue begin to drop. Excessive packet drops reduce the fairness index value of the network. Additionally, the attack causes network delay. CoDel does not use the size of the queue to manage it; it uses the queue time of the packets. This ensures that the fairness index value of the CoDel algorithm is high.

4. Conclusion

In conclusion, our research underscores the paramount importance of robust queue management algorithms in fortifying LTE networks against the disruptive impact of DDoS attacks. Through a comprehensive examination of various techniques, our study extends the existing body of knowledge in network security beyond conventional paradigms. We have systematically evaluated the performance of CoDel, RED, PIE, pFIFO, and Drop-Tail algorithms under simulated DDoS scenarios, shedding light on their respective strengths and weaknesses. Notably, the CoDel algorithm emerges as the standout performer, leveraging packet waiting time to optimize packet loss, latency, and end-to-end transmission. The RED algorithm also demonstrates commendable performance, strategically regulating packet drop thresholds. Conversely, PIE, pFIFO, and Drop-Tail algorithms face notable challenges in packet control during DDoS attacks, with Drop-Tail exhibiting a pronounced vulnerability. These findings provide critical insights for network administrators and security experts in devising robust defenses against escalating DDoS threats in LTE networks.

Furthermore, this study contributes significantly to the broader discourse on network security. By elucidating the nuanced interplay between LTE architecture and DDoS attacks, our research highlights the pivotal role of effective queue management in thwarting and mitigating such assaults. This comprehensive evaluation of queue management algorithms fills a notable gap in the current literature, offering practical guidance for implementing tailored security measures. Looking ahead, future research endeavors could focus on the development of AI-driven queue management algorithms fine-tuned for LTE networks, further enhancing the resilience of these crucial communication systems in the face of evolving cyber threats.

References

Albayrak, Z., Çakmak, M., 2018. A Review: Active Queue Management Algorithms in Mobile Communication. International Conference on Cyber Security and Computer Science 180–184.

Ali, S.M., Çakmak, M., Albayrak, Z., 2022. Security Classification of Smart Devices Connected to LTE Network, in: Lecture Notes in Networks and Systems. https://doi.org/10.1007/978-3-030-94191-8_91

Amer, H., Al-Kashoash, H., Khami, M.J., Mayfield, M., Mihaylova, L., 2020. Non-cooperative game based congestion control for data rate optimization in vehicular ad hoc networks. Ad Hoc Networks 107. https://doi.org/10.1016/j.adhoc.2020.102181

Ashfaq, M.F., Malik, M., Fatima, U., Shahzad, M.K., 2022. Classification of IoT based DDoS Attack using Machine Learning Techniques, in: 2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM). IEEE, pp. 1–6. https://doi.org/10.1109/IMCOM53663.2022.9721740

Bisoy, S.K., Pattnaik, P.K., 2016. Design of feedback controller for TCP/AQM networks. Engineering Science and Technology, an International Journal 20. https://doi.org/http://dx.doi.org/10.1016/j.jestch.2016.10.002

Çakmak, M., Albayrak, Z., 2022. AFCC-r: Adaptive Feedback Congestion Control Algorithm to Avoid Queue Overflow in LTE Networks. Mobile Networks and Applications 27. https://doi.org/10.1007/s11036-022-02011-8

Çakmak, M., Albayrak, Z., 2020. Performance Analysis of Queue Management Algorithms Between Remote-Host and PG-W in LTE Networks. Academic Platform Journal of Engineering and Science 456–463. https://doi.org/10.21541/apjes.662677

Çakmak, M., Albayrak, Z., Torun, C., 2021. Performance comparison of queue management algorithms in lte networks using NS-3 simulator. Tehnicki Vjesnik 28. https://doi.org/10.17559/TV-20200411071703

F. M. Suaib Akhter, A., F. M. Shahen Shah, A., Ahmed, M., Moustafa, N., Çavuşoğlu, U., Zengin, A., 2021. A Secured Message Transmission Protocol for Vehicular Ad Hoc Networks. Computers, Materials & Continua 68, 229–246. https://doi.org/10.32604/cmc.2021.015447

Gomez, C.A., Wang, X., Shami, A., 2021. Federated intelligence for active queue management in inter-domain congestion. IEEE Access 9, 10674–10685. https://doi.org/10.1109/ACCESS.2021.3050174

Gómez, G., Pérez, Q., Lorca, J., García, R., 2014. Quality of service drivers in LTE and LTE-A networks. Wirel Pers Commun 75, 1079–1097. https://doi.org/10.1007/s11277-013-1409-0

Gong, Y., Cao, J., Fu, Y., Guo, M., 2019. A DDoS attack detection model for LTE-A network. Journal of Cyber Security 4. https://doi.org/10.19363/J.cnki.cn10-1380/tn.2019.01.03

Israr, A., Yang, Q., Li, W., Zomaya, A.Y., 2021. Renewable energy powered sustainable 5G network infrastructure: Opportunities, challenges and perspectives. Journal of Network and Computer Applications. https://doi.org/10.1016/j.jnca.2020.102910

Jevtić, M., Zogović, N., Dimić, G., 2009. Evaluation of Wireless Sensor Network Simulators. Proceedings of the 17th Telecommunications Forum TELFOR 2009 Belgrade Serbia.

Jyothi, K.K., Chaudhari, S., 2020. Optimized neural network model for attack detection in LTE network. Computers & Electrical Engineering 88, 106879. https://doi.org/10.1016/j.compeleceng.2020.106879

Krishnan, P., Duttagupta, S., Achuthan, K., 2019. SDNFV Based Threat Monitoring and Security Framework for Multi-Access Edge Computing Infrastructure. Mobile Networks and Applications 24. https://doi.org/10.1007/s11036-019-01389-2

Lin, Y., Li, L., Ren, P., Wang, Y., Szeto, W.Y., 2021. From aircraft tracking data to network delay model: A data-driven approach considering en-route congestion. Transp Res Part C Emerg Technol 131. https://doi.org/10.1016/j.trc.2021.103329

Low, S.H., Paganini, F., Jiantao Wang, Adlakha, S., Doyle, J.C., n.d. Dynamics of TCP/RED and a scalable control, in: Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, pp. 239–248. https://doi.org/10.1109/INFCOM.2002.1019265

Mousavi, H., Amiri, I.S., Mostafavi, M.A., Choon, C.Y., 2019. LTE physical layer: Performance analysis and evaluation. Applied Computing and Informatics 15. https://doi.org/10.1016/j.aci.2017.09.008

Mousavi, H., Amiri, I.S., Mostafavi, M.A., Choon, C.Y., 2017. LTE physical layer: Performance analysis and evaluation. Applied Computing and Informatics. https://doi.org/10.1016/j.aci.2017.09.008

N.D., A., A., R., 2019. Avoiding queue overflow and reducing queuing delay at eNodeB in LTE networks using congestion feedback mechanism. Comput Commun 146, 131–143. https://doi.org/10.1016/j.comcom.2019.07.015

Oughton, E.J., Comini, N., Foster, V., Hall, J.W., 2022. Policy choices can help keep 4G and 5G universal broadband affordable. Technol Forecast Soc Change 176. https://doi.org/10.1016/j.techfore.2021.121409

Pan, R., Natarajan, P., Piglione, C., Prabhu, M.S., Subramanian, V., Baker, F., VerSteeg, B., 2013. PIE: A lightweight control scheme to address the bufferbloat problem. IEEE International Conference on High Performance Switching and Routing, HPSR 148–155. https://doi.org/10.1109/HPSR.2013.6602305

Paul, A., Kawakami, H., Tachibana, A., Hasegawa, T., 2017. Effect of AQM-Based RLC Buffer Management on the eNB Scheduling Algorithm in LTE Network. Technologies (Basel) 5, 59. https://doi.org/10.3390/technologies5030059

Praveen, K. v., Prathap, P.M.J., 2021. Energy Efficient Congestion Aware Resource Allocation and Routing Protocol for IoT Network using Hybrid Optimization Techniques. Wirel Pers Commun 117. https://doi.org/10.1007/s11277-020-07917-8

Raghuvanshi, D.M., Annappa, B., Tahiliani, M.P., 2013. On the effectiveness of CoDel for active queue management. International Conference on Advanced Computing and Communication Technologies, ACCT 107–114. https://doi.org/10.1109/ACCT.2013.27

Said, A.A., Çakmak, M., Albayrak, Z., 2022. Performance of Ad-Hoc Networks Using Smart Technology Under DDoS Attacks, in: Lecture Notes in Networks and Systems. https://doi.org/10.1007/978-3-030-94191-8_92

Swain, S.K., Nanda, P.K., 2021. Adaptive queue management and traffic class priority based fairness rate control in wireless sensor networks. IEEE Access 9. https://doi.org/10.1109/ACCESS.2021.3102033

Szyguła, J., Domański, A., Domańska, J., Marek, D., Filus, K., Mendla, S., 2021. Supervised learning of neural networks for active queue management in the internet. Sensors 21. https://doi.org/10.3390/s21154979

Verma, H., Chauhan, N., Chand, N., Awasthi, L.K., 2022. Buffer-loss estimation to address congestion in 6LoWPAN based resource-restricted 'Internet of Healthcare Things' network. Comput Commun 181, 236–256. https://doi.org/10.1016/j.comcom.2021.10.016

Wang, T., Wang, M., 2020. Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding. Opt Laser Technol 132, 106355. https://doi.org/10.1016/j.optlastec.2020.106355

Weingärtner, E., vom Lehn, H., Wehrle, K., 2009. A performance comparison of recent network simulators, in: IEEE International Conference on Communications. https://doi.org/10.1109/ICC.2009.5198657

Wu, Z., Zhu, M., Li, Q., Xue, L., Yang, J., Chen, Z., Cao, Y., Cui, Y., 2022. Design of power monitoring system for new energy grid-connected operation based on LoRa and 4G technology. Energy Reports 8, 95–105. https://doi.org/10.1016/j.egyr.2022.10.038

Zenitani, K., 2023. From attack graph analysis to attack function analysis. Inf Sci (N Y) 119703. https://doi.org/10.1016/j.ins.2023.119703

Zidic, D., Mastelic, T., Nizetic Kosovic, I., Cagalj, M., Lorincz, J., 2023. Analyses of ping-pong handovers in real 4G telecommunication networks. Computer Networks 227. https://doi.org/10.1016/j.comnet.2023.109699