УНИВЕРЗИТЕТ „СВ. КИРИЛ И МЕТОДИЈ“ - СКОПЈЕ
Факултет за електротехника и информациски технологии
Институт за телекомуникации

АНАЛИЗА НА МРЕЖЕН СООБРАЌАЈ КАЈ SDN СЕРВИСНИ НИЗИ ВО ЦЕНТРАЛИЗИРАНА И ДИСТРИБУИРАНА NFV АРХИТЕКТУРА

- Докторска дисертација -

Кандидат:
М-р. Ѓорѓи Илиевски

Ментор:
Проф. Д-р Перо Латкоски

2022
Скопје

Овој труд го посветувам на моето семејство

СОДРЖИНА

ЛИСТА НА СЛИКИ

ЛИСТА НА ТАБЕЛИ

ЛИСТА НА КРАТЕНКИ

3GPP (3rd Generation Partnership Project)

5G (5th Generation mobile networks)

5G NORMA (5G NOvel Radio Multiservice adaptive network Architecture)

API (Application Programming Interface)

AWS (Amazon Web Services)

C-RAN (Cloud - Radio Access Network)

CDF (cumulative distribution function)

CEVPS (Cost Efficient VPS)

CAPEX (Capital Expenditures)

DC (Data Center)

D-NFV (Distributed-NFV)

DMRT_SL (Dynamic Minimum Response Time considering Same Level)

DNS (Domain Name Services)

DPI (Deep Packet Inspection)

DR (Disaster Recovery)

EMS (Element Manager System)

ETSI (European Telecommunications Standards Institute)

FIFO (First In First Out)

MC (Fixed Mobile Convergence)

GRE (Generic Routing Encapsulation)

HTTP (Hypertext Transfer Protocol)

HTTPS (Hypertext Transfer Protocol Secure)

ICMP (Internet Control Message Protocol)

IDT (Inter Departure Time)

IoT (Internet of Things)

ISG (Industry Specification Group)

IP (Internet Protocol)

K-NN (K-Nearest Neighbours)

KPI (Key Performance Indicator)

LAN (Local Area Network)

LTE (Long Term Evolution)

mMTC (massive Machine Type Communication)

MANO (Management, automation and network orchestration)

MEC (Mobile Edge Computing)

MCC (Mobile Convergence Client)

MILP (Mixed Interlinear Program)

ML (Machine learning)

MPLS (Multi-Protocol Label Switching)

NAT (Network Address Translation)

NFV (Network Function Virtualization)

NFVI (Network Function Virtualization Infrastructure)

NFVO (Network Function Virtualization Orchestrator)

NBI (NorthBound Interface)

OF (OpenFlow)

OPEX (Operational Expenditures)

OSI (Open Systems Interconnection Model)

OSS/BSS (Operation Support System/Business Support System)

PDF (probability density function)

PS (Packet Size)

QoS (Quality of Service)

RAN (Radio Access Network)

SDN (Software-Defined Networking)

SDN MA (SDN Management and Administration)

SD-WAN (Software Defined wide-area network)

SSH (Secure Shell)

TCP (Transmission Control Protocol)

TTL (Time to Live)

UDP (User Datagram Protocol)

URLLC (Ultra-Reliable and Low Latency Communications)

VIM (Virtualized Infrastructure Manager)

VLAN (Virtual Local Area Network)

VM (Virtual Machine)

VoIP (Voice over IP)

vRAN (Virtualized radio access network)

VNF (Virtual Network Function)

VNFM (Virtual Network Infrastructure Manager)

ИЗВАДОК

Преминувањето на пресметувачките околини во т.н. облак е процес кој трае. Процесот го надмина класичниот пристап на виртуелни машини (VM) и софтверски дефинирани мрежи (Software Defined Networking - SDN) и се придвижи кон контејнеризација, микросервиси, апликативни функции, виртуелни мрежни функции (Virtual Network Functions - VNF) итн. Пенетрацијата на 5G е уште еден тренд кој се гради на такви платформи. Оваа теза ги истражува перформансите на шест надгледувани алгоритми за машинско учење (ML) за класификација на мрежниот сообраќај во виртуелна средина управувана од виртуелизација на мрежни функции (Network Functions Virtualization - NFV). Анализата на перформансите се спроведува од точка на прецизност на класификација, но и од точка на временска потрошувачка (брзина) на надгледуваните алгоритми за машинско учење. Во првиот дел е направена класификација на VoIP и шифрирани VoIP сообраќај, бидејќи овој сообраќај е основата на говорните услуги кај 5G мрежите. NFV се смета за еден од фундаментите за развојот на 5G, каде традиционалните мрежни елементи се целосно виртуелизирани, најчесто изградени во мешани околини на локален и јавен облак. Виртуелните машини се заменуваат со контејнери и апликативни функции додека најголемиот дел од мрежниот сообраќај тече во насока исток-запад во облакот. Понатаму во истражувањето, мрежниот сообраќај е поделен на шест класи: VoIP, енкриптиран VoIP, DNS, управувачки, SSH, HTTP и HTTPS кои се избрани според искуството кај традиционалните мрежи и во согласност со очекуваниот мрежен сообраќај во рамките на 5G радио мрежата, како и 5G јадрената мрежа. Исто така, се оценува ефикасноста на предложените алгоритми за машинско учење во класифицирањето на избраните класи на мрежен сообраќај.

Анализата покажа дека во такво опкружување, од шесте разгледани алгоритми: BayesNet, NaiveBayes, J48, K-Nearest Neighbours (K-NN), Decision Tree и AdaBoost, алгоритамот Decision Tree има најдобра перспектива за класификација и ја има потребната брзина што ќе воведе минимално доцнење во мрежните текови, што е клучно кај 5G мрежите, каде што барањата за доцнење на пакетите се строги. Се покажа дека е сигурен и со одлични вкупни перформанси низ повеќе класи на мрежни пакети во рамките на виртуелизирана NFV мрежна архитектура. При извршувањето на класификацијата, анализата е направена само со статистички карактеристики на мрежните текови, исклучувајќи ги информациите во содржината на пакетот, изворот на мрежните пакети, дестинацијата на мрежните пакети и комуникацискиот порт, со што анализата станува валидна не само од техничка, туку и од регулаторна гледна точка.

Вториот дел од оваа теза е фокусиран на дистрибуцијата на NFV архитектурата и влијанието кое дистрибуцијата го има врз времето на престој на мрежните пакети во околината. Сметачките реурси и ресурсите за податочно складирање треба да се доведат во непосредна близина до точката на мрежен за пристап, со цел да се обезбеди сигурна, економски исплатлива и услуга со ниска мрежна латентност. Концептот за виртуелизација на мрежни функции (NFV), ја дава потребната способност за раст на мрежата кон работ. Тој ја надополнува 5G експанзијата и овозможува зголемување на мрежниот сообраќај, што е неизбежно поради зголемувањето на 5G пропусниот опсег и очекуваната експанзија на Интернетот на Нештата (Internet of Things - IoT). Дистрибуцијата на NFV

инфраструктурата го минимизира позадинскиот сообраќај, придвижувајќи ги сметачките капацитети кон мрежниот раб каде влијае на подобрување на корисничкото искуство. Со приближување на услугата до потрошувачот, доцнењето во мрежата може да се задржи под 1ms, со што случајот за употреба кај 5G мрежите е веродостоен. Дистрибуцијата на NFV инфраструктурата на повеќе локации и податочни центри е жешка тема во истражувачките и инженерските заедници. Во оваа теза, предложени се аналитички модели на мрежна архитектура базирани на NFV, со цел да се пресмета времето на престој на мрежните пакети во три различни сценарија: класична NFV средина каде што сите NFV елементи се на иста локација, дистрибуирана архитектура на податочната рамнина со централизирана средина за управување и оркестрација (MANO) и дистрибуирана средина каде што секоја локација има своја податочна рамнина и елементи за управување и оркестрација. Аналитичките модели се тестираат и дискутираат преку симулации базирани на Matlab. Преку резултатите од симулацијата, се дискутира какво е влијанието на промените на различните мрежни параметри врз времето на престој на пакетите, а архитектурите се споредуваат една со друга, со цел да се види како тие можат да се вклопат во практични услуги обезбедени во NFV околина.

Со цел експериментално да се истражи доцнењето на мрежните пакети во услугите што се протегаат на повеќе географски одвоени локации, изградени врз NFV архитектура, се користи средина со две локации, за спроведување на експерименти и на тој начин се тестира како дистрибуцијата влијае на времето на престој на пакетот во мрежата. Експериментите се прават на услуги кои работат на една локација, или се протегаат на две локации. Целта на истражувањето е да се дојде до заклучок кој ќе им помогне на мрежните архитекти да ја проценат NFV архитектурата и да направат дистрибуција на инфраструктурата врз која се изградени услугите.

ABSTRACT

Cloudification of all computing environments is an undergoing process. The process has overpassed the classical Virtual Machines (VM) and Software-Defined Networking (SDN) approach and has moved towards containerization, microservices, app functions, virtual network functions (VNF) etc. 5G penetration is another trend, and it is built on such platforms. This thesis is investigating the performance of six supervised machine learning algorithms (ML) for network traffic classification, in a virtual environment driven by Network Function Virtualization (NFV). The performance analysis is conducted from a point of classification precision, but also from a point of time consumption (speed) of the supervised ML algorithms. In the first part, classification of VoIP and encrypted VoIP traffic has been done, because this traffic is the basis of the 5G voice services. NFV is considered to be one of the fundaments of the 5G development where traditional networking elements are fully virtualized, in many cases relaying on mixed cloud solutions, both on premise and public cloud based. Virtual machines are being replaced by containers and application functions while most of the network traffic is flowing in the east-west direction within the cloud. Furthermore, the network traffic has been divided on six classes: VoIP, encrypted VoIP, DNS, Management, SSH, HTTP and HTTPS which are chosen by traditional networks experience and in alignment with the expected network traffic within the 5G radio, as well as the 5G core network. The proposed ML Algorithms are also evaluated for the efficiency in classifying these network traffic classes.

The analysis has shown that in such environment, from the six considered algorithms: Bayes Net, NaiveBayes, J48, K-Nearest Neighbours (K-NN), Decision Tree and AdaBoost, the Decision Tree algorithm has the best prospect for classification, and has the required speed that will introduce minimal delay in the network flows, which is crucial in the 5G networks, where the packet delay requirements are strict. It has proven to be reliable and with excellent overall performance across multiple network packet classes, within a virtualized NFV network architecture. While performing classification, the analysis has been done only with statistical features of the network flows, excluding the packet payload, the source of the network packets, the destination of the network packets, and the port information, thus making the analysis valid not only from technical, but also from regulatory point of view.

The second part of this thesis is focused on the distribution of the NFV architecture and the impact of the distribution on the network packets sojourn time within the environment. Compute and storage resources have to be brought at close proximity to the access networks in order to provide reliable, cost effective, and low-latency service. Network Functions Virtualization (NFV) concept, gives the needed ability for the network to grow into the edge. It complements the 5G expansion and it allows increased traffic, which is inevitable due to the 5G bandwidth and the expected IoT expansion. Distribution of the NFV infrastructure minimizes the backhaul traffic, moving the processing job at the edge, not disturbing, but rather improving the user experience. By bringing the service closer to the consumer, the latency within the network can be kept under 1ms, making the 5G use case plausible. Distribution of the NFV environment on multiple locations and datacenters is a hot topic in research and engineering communities. In this thesis, analytical models of the network architecture based upon NFV are proposed, in order to calculate the network packet sojourn time in three different scenarios: classical NFV environment where all NFV elements are on the same location, architecture wih distributed data plane and centralized Management and Orchestration (MANO) environment, and distributed environment where every location has its own data plane and MANO elements. The analytical models are tested and discussed through Matlab based simulations. Through the

simulation results, the impact of changes of different network parameters on the packet sojourn time is discussed, and the architectures are compared among each other, in order to see how they can be fitted in practical services provided in an NFV environment.

In order to experimentally investigate the network packet delay in services that span across multiple geographically separated locations, built upon NFV architecture, an environment with two locations is used to conduct experiments, and thus to test how the distribution impacts the packet sojourn time. The experiments are done upon services that work on a single location, or are spanned across two locations. The objective of the research is to come with a conclusion that will help network architects to assess the NFV architecture and to make a distribution of the infrastructure on which the services lay on.

1. ВОВЕД

Денес дигиталната индустрија се менува секојдневно. Секој мора да се трансформира и брзо да се прилагоди на промените. Оваа континуирана промена придонесува за зголемени финансиски трошоци што ги зголемуваат оперативните и капиталните расходи (OPEX и CAPEX). Ова е особено важно за бизнисите кои се примарно ориентирани кон обезбедување на дигитални услуги, телекомуникациски компании, ИТ индустријата, дигиталната забава, компаниите кои нудат интернет услуги и дигитални производи [1]. Виртуелизацијата е првиот чекор во серијата еволутивни чекори во областа, проследени со воведување на услуги во облак (cloud services), приватни и јавни, кои одат во насока на економија на обем [2]. Вмрежувањето, веројатно едно од најважните делови од мозаикот, не е исклучок. Софтверски дефинираното вмрежување (Software Defined Networking - SDN) е двигател на сценаријата за мрежна виртуелизација, што им овозможува на cloud провајдерите апстракција на мрежата, одвојување на управувачката и податочната рамнина, при што мрежните елементи се заменети со мрежни функции, кои како виртуелни машини работат на универзален хардвер [3]. Тоа ги подобрува CAPEX и OPEX [4][5] трошоците, но технолошката еволуцијата не застанува тука. Контејнерите станаа градежни блокови на микросервиси кои овозможуваат брзо распоредување, оптимална распределба на ресурсите, едноставно и автоматско скалирање. Од аспект на вмрежување, виртуелизацијата на мрежните функции (Network Functions Virtualization - NFV) [6] се појави како нов концепт на мрежна архитектура што ја надополнува SDN технологијата, создавајќи многу агилна и динамична средина [7] за поврзување на виртуелните мрежни функции (Virtual Network Functions - VNF) во сервисни низи кои обезбедуваат комплетни комуникациски услуги.

Развојот на компјутерските мрежи во насока на мрежна виртуелизација, користењето на SDN и NFV [8] базирана архитектура, текот на мрежниот сообраќај, кој во најголем дел се движи во насока исток-запад, од своја страна воведува дополнителна комплексност. Еден од проблемите кои се разгледуваат е класификацијата на мрежниот сообраќај во рамките на виртуелниот слој. Ова е особено важно за воспоставување на квалитет на сервис (Quality of Service – QoS), за подесување на соодветна мрежна безбедност, регулирање и следење на мрежниот сообраќај, особено во случаи кога низ виртуелната околина се поставени сосема различни и неповрзани сервиси. Во ваквата поставеност, често се користи вештачката интелигенција и различни алгоритми за

машинско учење, чија намена е соодветна класификација на мрежниот сообраќај. Овде, покрај техничките предизвици, во предвид треба да се имаат и правно-регулативните правила кои најчесто се мошне строги, особено кај телекомуникациските оператори кои обезбедуваат најразлични услуги користејќи една или повеќе меѓу себе поврзани системи.

VoIP (Voice over IP) комуникацијата е една од најчестите комуникациски услуги што ги користи општата популација. Повеќе системи и апликации обезбедуваат VoIP услуги кои најчесто се уред-до-уред (peer-to-peer, P2P) базирани и обезбедуваат како стандарден, така и енкриптиран сообраќај. Со оглед на тоа што системите мигрираат кон виртуелизација во облак, користејќи јавни (Amazon's AWS, Microsoft's Azure, Google Cloud), мешани или приватни облаци, класификацијата на мрежниот сообраќај е стандарден процедура во секоја организација, а класификацијата на VoIP сообраќајот е особено важна за операторите кои обезбедуваат гласовни услуги. 5G технологијата се потпира токму на овие услуги. Апликациите како Skype и Viber (и многу други) користат енкрипција на собраќајот што ја прави класификацијата на мрежниот сообраќај уште попроблематична. Освен тоа, мора да се внимава на латентноста на мрежните пакети која мора да биде минимална [9].

Поради претходното, ја истражуваме ефикасноста на некои од веќе воспоставените надгледувани алгоритми за машинско учење (supervised machine learning algorithms), во рамките на сценарио каде што класификацијата на мрежниот сообраќај и брзината на алгоритамот се подеднакво важни. Предизвикот е да се следи и долови „скриениот“ сообраќај исток-запад во рамките на NFV архитектурата и да се класифицира, но притоа да се минимизира очекуваната латентност додадена од алгоритамот за класификација. Најпрвин фокусот е на класификацијата на VoIP сообраќајот, а потоа анализата е проширена и на други типови на мрежен сообраќај.

Многу истражувања се фокусирани на аспектите на класификација и длабока инспекција на пакети (DPI-deep packet inspection) во сценарија кои вклучуваат SDN елементи [10], [11], [12]. Други ги истражуваат безбедносните аспекти при извршување на DPI [13], [14] со користење на SDN сонди за пресретнување (снифање) на мрежниот сообраќај и обработка на податоци. Некои автори ја разгледуваат класификацијата на мрежниот сообраќај во традиционалните мрежи [15], [16] без користење на виртуелизација, но овие трудови се исклучително важни за споредба на двата случаи – класични мрежи и мрежи кои се базирани на виртуелни елементи. Фокусот на

истражување во оваа дисертација е кон системите изградени врз NFV архитектура и класификацијата на мрежниот сообраќај во такво опкружување.

Мобилните мрежи од петта генерација (5G) веќе се имплементирани во многу делови на светот. Тие ќе го овозможат долгоочекуваниот пробив на „Интернет на Нештата“ (Internet of Things - IoT), со поддршката на масивен број на мрежно поврзани уреди со висок пропусен опсег. Со растот на бројот на поврзани субјекти и барањата за висок квалитет на услуга, вмрежувањето треба значително да се прошири и прилагоди на новите потреби. Спецификацијата за 5G, бара латентност на мрежните пакети во податочната раминина од само 1 ms за ултра-сигурни комуникации со мала латентност (URLLC) [9]. Токму овие сценарија бараат напредни решенија за вмрежување како што се SDN и NFV.

Апликациите и услугите побаруваат се поголема пропустност на мрежата, додека нивната достапност и сигурност мора да се зголемат. Централизираните решенија зависат од поврзувањето на крајниот потрошувач на услугата со централната локација, додека дистрибуираните средини обезбедуваат поголема приспособливост, истовремено обезбедувајќи минимизирање на позадинскиот мрежен сообраќај. За да се спроведе ова, мора внимателно да се разгледа локацијата за обработката на податоците и локацијата на системот за мрежно управување и оркестрација што се користи кај NFV архитектурата. Пресметувачките и складишните (compute and storage resources) треба да се доведат во непосредна близина до пристапната мрежа, со цел да се обезбедат мрежни услуги кои се сигурни, исплатливи и имаат ниска латентност. Концептот за виртуелизација на мрежни функции, ја дава потребната способност за мрежата да расте кон работ [17], [18]. Дел од истражувањето во оваа дисертација е во насока на пронаоѓање на можните сценарија за дистрибуција на NFV архитектурата на повеќе географски оддалечени локации. Главните недостатоци на централизираната NFV архитектура се: ограничената приспособливост, проблеми со перформансите и постоењето на единствена точка на дефект. Од друга страна, дистрибуцијата на мрежната архитектура воведува комплексност и ја афектира латенцијата во мрежата.

Латенцијата на мрежните пакети предизвикана од распределбата на виртуелните мрежни функции во рамките на NFV архитектурата [19] е една од главните грижи при дизајнирање на услуги што работат во ваква околина. Постојат многу истражувања кои се фокусирани на дистрибуираниот NFV (D-NFV) од аналитичка гледна точка и моделирање

на системите, како и врз услугите изградени на нив, за да се предвиди нивното однесување [20], [21]. Некои автори развиваат софтверски компоненти, апликации и рамки со цел да ги подобрат различните аспекти на NFV, како што е поставувањето на виртуелните мрежни функции во рамките на мрежната архитектура или да го подобрат управувањето и операциите на системот, така што услугите што работат на него да бидат оптимизирани [22], [23], [24]. Друг истражувачки тек е фокусиран на индивидуалните карактеристики на дистрибуираните SDN и NFV средини [25], [26].

Во рамките на оваа дисертација се врши на аналитичко моделирање на различни мрежни околина базирани на NFV архитектура и се анализираат факторите кои влијаат на доцнењето на пакетите во овие околини. Истражувани се три сценарија: класична NFV околина каде што сите NFV елементи се на иста локација, дистрибуирана архитектура на податочната рамнина со централизирана средина за управување, автоматизација и оркестрација (Management, automation and network orchestration - MANO) и дистрибуирана околина каде што секоја локација има своја податочна рамнина и MANO елементи. Услугите што ги обезбедува NFV може да се протегаат на повеќе локации. Комуникацијата помеѓу дистрибуираните околини може да биде на ниво на управувачката рамнина или на податочната рамнина, доколку дистрибуираните услуги се веќе воспоставени.

Аналитичкото моделирање, претежно на SDN околини, е широко користено за евалуација на мрежните перформанси [27], [28]. Различни параметри и случаи на употреба се анализирани за да се изнесат нови алгоритми и архитектури кои ги подобруваат системските перформанси [27], [29]. Некои истражувања се концентрираат на перформансите на контролерот во контролната SDN рамнина [30], додека други се фокусирани на податочната рамнината или на комутаторите во рамките на SDN [31]. Во оваа дисертација фокусот е на NFV архитектурата каде што SDN се зема како дел од целокупната NFV околина.

Други автори, исто така ги истражувале перформансите на системите кои се базирани на SDN и NFV [32], [33]. Природно доаѓа дека теоријата на редици се користи како основа за аналитичко моделирање [34], [35]. Во повеќето случаи се користи M/M/1 моделот на редици [28], [38], иако различни автори истражувале други модели на редици, како M/M/m [36] или G/G/m [37]. Поради сложеноста на целокупниот NFV процес на креирање, управување и функционирање на услугите во системот, проблемот на

аналитичко моделирање на таков систем има повеќе степени на слобода. Поголемиот дел од истражувањата кои постојат се фокусирани на некои делови од процесите во рамките на NFV архитектурата, како што е моделирањето на управувачката рамнина или распределбата и комуникацијата на виртуелните мрежни функции во рамките на сервисните низи.

1.1.Цели и мотив на истражувањето

Софтверски дефинираните мрежи и архитектурата за виртуелизација на мрежни функции имаат значително влијание во развојот на 5G мрежите и овозможуваат нивна имплементација, дозволувајќи им на мрежните компоненти, а со тоа и на целата услуга, да се доближат до крајниот корисник (потрошувач на услуга). Давателите на услуги во облак имаат проблем во имплементацијата на услуги кои се мрежно блиски до корисникот и за тоа им требаат огромни инвестиции, што ја отвора вратата за локалните даватели на ИТ решенија и телекомуникациските компании, да ја пополнат празнината и да ги искористат SDN и NFV технологиите, како и 5G пристапната мрежа, за да создадат најсовремена мрежна инфраструктура со висока достапност, приспособливост, безбедност, мало доцнење и висок пропусен опсег.

Една од целите на ова истражување е да предложи ефикасен, практично возможен и евтин начин за класификација на мрежниот сообраќај кај мрежните системи изградени врз NFV архитектура. Ефикасна класификација на мрежниот сообраќај е основа за многу процеси како што се воведувањето на висок квалитет на сервис, длабока инспекција на пакетите, мониторирање на мрежата, воспоставувањето на висока и квалитетна мрежна сигурност, управување со мрежата, усогласеност на услугите и сервисите низ мрежата со постоечката законска регулатива.

Затоа една од основите цели во ова истражување е анализа на мрежниот сообраќај во рамките на NFV систем од аспект на мрежна класификација на пакетите. За таа цел, се користат надгледувани алгоритми за машинско учење [39]. Предизвикот е да се следи и долови „скриениот“ сообраќај исток-запад во експериментална NFV средина и да се класифицира, но и да се минимизира очекуваната латентност во системот, додадена од алгоритамот за класификација. Извршени се неколку експерименти. Првиот дел се

фокусира на класификацијата на VoIP сообраќајот, користејќи ги статистичките карактеристики на мрежниот сообраќај, без да се земе предвид содржината (payload) на мрежните пакети, со цел да се избегне пробив во приватноста на информациите што би резултирало со потенцијален правен или регулаторен проблем. Со добиените резултати се оценуваат алгоритмите за надгледувано машинско учење и нивната корисност за оваа намена. Направена е споредба со слични истражувања спроведени во класичните мрежи. Ова истражување е дополнително проширено на други видови мрежен сообраќај (WEB-HTTP, WEB-HTTPS, SSH, NETMGMT, DNS, VoIP).

Уште една цел врз која се заснова трудот е воведување на ефикасен аналитички модел на NFV базирана мрежа, која може да е централизирана или дистрибуирана, со цел да се предвиде однесувањето на услугата поставена во мрежата, но и да се дизајнира мрежа која би била оптимално ефикасна од една страна и комерцијално исплатлива од друга страна. Преку моделирањето на мрежата може да се предвидат карактеристиките на услугите поставени во неа, како и да се изврши содветно поставување на мрежните функции во рамките на мрежата, со цел да се добие најефикасна сервисна низа.

Поради сложеноста на NFV архитектурата и целокупниот процес на креирање, управување и работење со мрежните услуги поставени во системот, проблемот на аналитичко моделирање на таков систем е комплексен проблем од повеќе аспекти [40]. Најголемиот дел од истражувањата во оваа област се фокусираат само на некои делови од NFV архитектурата, како што е моделирањето само на управувачката рамнина или дистрибуцијата и меѓусебната комуникација на виртуелните функции, додека во овој труд истражувачкиот проблем се состои од потребата за целосна дистрибуција, која би довела до оптимални услуги лоцирани во близина на крајниот корисник. Целта е да се процени ефикасноста на архитектурните решенија во кои ресурсите се блиску до работ на мрежата (edge computing), особено во случај на употреба во 5G. Комутаторите, контролерите и VNF менаџерите се претставуваат со M/M/1 редици, а системот е моделиран како Џексонова мрежа. Бидејќи многу услуги бараат некои од мрежните елементи да бидат блиску до потрошувачот, задача е да се процени доцнењето на пакетите во централизирани и дистрибуирани мрежни средини и факторите кои придонесуваат за доцнењето. Според наодите од истражувањето, не постои публикација која се фокусира на дистрибуирани NFV средини од аналитичка гледна точка, а во исто време ги зема предвид доцнењата на пакетите предизвикани од NFV архитектурата и доцнењата

предизвикани од растојанието помеѓу дистрибуираните средини. Темата е многу важна за идниот развој на услуги базирани на NFV архитектура.

Оваа анализа е добра основа за подготовка на адекватна мрежна архитектура во пракса, имајќи ги предвид различните типови на услуги што можат да работат на системот, особено со потенцијалот на 5G за развој на нови и иновативни мрежни услуги. Со анализа на позитивните и негативните страни на предложените сценарија, може да се избере најдобриот пристап во пракса, како и да се дизајнира најоптимална мрежна архитектура. Ова е главната мотивација на истражувањето. Истражувањето е важно во реални и практични сценарија и им овозможува на мрежните архитекти да го предвидат доцнењето мрежните пакети во модерни мрежни системи изградени врз NFV архитектура.

Експерименталниот дел во овој дел од дисертацијата служи за докажување на употребливата вредност на предложените модели, за дополнително анализирање на мрежата базирана на NFV архитектура, како и за практична проверка на потенцијалните проблеми во ваквата поставеност.

1.2.Образложение на работните хипотези и тези

Во истражувањето кое ќе биде спроведено, како главна (општа) хипотеза се јавува следнава:

SDN технологијата и NFV архитектурата се овозможувачи на напредни услуги кои мора да се доведат во непосредна близина на крајниот корисник, со цел да се запазат постоечките стандарди, а да се зголеми квалитетот на услугата. Дистрибуирањето на NFV архитектурата и разместувањето на виртуелните мрежни функции на засебни локации, во близина на крајниот корисник значително помага на таа цел.

Првата посебна теза е следнава:

1) Бидејќи модерните мрежи се имаат висок степен на виртуелизација на мрежните компоненти, ефикасна класификација на мрежните пакети претставува предизвик, како врз точноста на класификација, така и врз времето потребно за класификација кое може да доведе до значително каснење на пакетите. Ефикасна класификација на мрежниот сообраќај е основа за многу процеси како што се

воведувањето на висок квалитет на сервис, длабока инспекција на пакетите, мониторирање на мрежата, воспоставувањето на мрежна сигурност, управување со мрежата, усогласеност на услугите и сервисите низ мрежата со постоечката законска регулатива.

Втората посебна теза е следнава:

2) Преку воведување на ефикасен аналитички модел на дистрибуирани услуги базирани на NFV, можат да се изведат заклучоци за карактеристиките на услугите, особено на ефектот што оваа поставеност го има врз мрежното доцнење на пакетите.

1.3.Користени научни методи

Во првиот дел од докторската дисертација се врши анализа на мрежниот сообраќај во систем изграден врз премисите на NFV архитектурата каде услугите мрежно се воспоставени користејќи низа од меѓусебно поврзани SDN елементи. Се користат методските постапки на индукција и дедукција, а исто така особено ќе се употребуваат анализа, синтеза и компарација со други трудови кои се занимаваат со слична тематика, како и со класичните мрежи, со цел да се испитаат можностите за класификација на мрежниот сообраќај во испитуваниот NFV базиран систем. За проверка на поставената хипотеза, изложена како прва теза во претходната точка, се вршат експериментални тестирања, по што добиените податоци се анализираат користејќи шест алгоритми за надгледувано машинско учење. Врз основа на добиените резултати се пресметува ефикасноста на секој од алгоритмите и се изведуваат заклучоци.

Вториот дел од дисертацијата, содржи аналитички дел со математичка анализа. Се врши опсервација и дефинирање на проблемот што го разгледуваме – влијанието на NFV архитектурата на мрежниот проток, односно поспецифично, влијанието кое поставувањето на мрежните функции што ја формираат мрежната низа на услугата на одредена локација го има врз мрежното доцнење на пакетите. Мрежните функции, контролерите и комутаторите ги претставуваме како Марковијански редови користејќи теорија на редици, додека пак целиот систем го претставуваме како Џексонова мрежа. Целата поставка е втемелена на OpenFlow (OF) SDN елементи. Како вовед во

аналитичкиот модел ги презентираме сите претпоставки каде преовладуваат методите на апстракција, генерализација и специјализација.

За добивање на резултати, аналитичките модели се проверуваат во MatLab, по што се прави компарација на добиените резултати кај различни архитектонски решенија. Според добиените резултати се врши дискусија и се изведуваат соодветни заклучоци.

Покрај тоа, во втората фаза се врши и експериментално истражување каде се користи реална околина и услуги базирани на SDN и NFV. Се користи централизиран систем, како и дистрибуиран систем на две географски одделени локации. Во процесот се користат бројни алатки. Добиените резултати се анализираат и се споредуваат со резултатите добиени од аналитичките модели.

На крај се врши анализа и дискусија на добиените резултати со цел да се изведат заклучоци околу иницијално поставените хипотези.

1.4.Научен придонес

Придонесот на оваа дисертација е воведувањето на нов аналитички модел за претставување на систем базиран на NFV архитектура, при што овој аналитички модел може да се користи за централизирани и дистрибуирани околини. Моделот се користи првенствено за определување на доцнењето на мрежните пакети кај услуги кои се изградени со користење на SDN и NFV архитектура и нивна оптимизација, преку доближувањето на пресметувачките и складишните ресурси во близина на крајниот корисник на услугата.

Покрај тоа дисертацијата дава и значаен придонес во разбирањето на класификацијата на мрежните пакети во системи изградени во целосно виртуелна околина врз принципите на NFV архитектурата, што е основа за многу значајни процеси во пракса (QoS, DPI, мониторирање на мрежата, мрежната сигурност, управувањето и оперирањето на услугите во мрежата), при што се води сметка да се запазат правно-регулативните норми за приватност на податоците кои се движат низ мрежата.

Главните придобивки од истражувањето може да се сумираат во следните точки:

A. Докажувањето преку аналитички и експериментални методи, дека дистрибуираната NFV архитектура може значително да влијае на намалување на мрежната латентност, што игра значајна улога кај 5G базираните услуги;

B. Експериментална студија за влијанието на дистрибуцијата на архитектурата NFV врз латентноста на мрежните пакети;

C. Воведување на нови аналитички модели на мрежни системи кои се засноваат на SDN и NFV, со особен акцент на гео-локацијата на компонентите на мрежата;

D. Користење на предложените аналитички модели за анализа на доцнењето на мрежните пакети, но и на останатите карактеристики на мрежниот сообраќај, при најразлична гео-поставеност на системот. Фокусот е на дистрибуираните NFV околини, при што се разгледува доцнењето на мрежните пакети предизвикано од виртуелните елементи, но и од географската дистанца на дистрибуираните околини претставува значаен новитет во истражувањето.

E. Експериментален доказ дека алгоритмите за надгледувано машинско учење може да се користат за брза и ефикасна класификација на мрежниот сообраќај во системи изградени врз NFV архитектура, користејќи ги исклучиво статистичките атрибути на мрежниот сообраќај, без да се врши инспекција на содржината што ја носат пакетите.

1.5.Примена на резултатите од истражувањето

Изведените заклучоци имаат научна и практична примена. Аналитичките модели кои се воведуваат во докторската дисертација може да се користат за подготовка и анализа на потенцијални поставки на услуги каде што дистрибуцијата и поставувањето на пресметувачките и складишните елементи кон работ на мрежата е можно и практично. Заклучивме дека ширењето на 5G мрежите, заедно со развојот на NFV архитектурата во насока на дистрибуција кон работ, се овозможувачи на идното паметно поврзување со безбедни, функционални и целосно оптимизирани услуги. Иако е теоретска, овој дел од анализата е добра основа за подготовка на соодветна архитектура во пракса, со оглед на различните типови на услуги кои можат да работат на системот. Со анализа на услугите,

добрите и лошите страни на предложените сценарија, може да се избере најдобриот пристап во пракса. За да се потврди употребната вредност на аналитичките модели, се врши експериментално мерење на систем лоциран на две оддалечени гео-локации.

Воведувањето на повеќе мрежни локации покрај архитектурен аспект за поставување на мрежните функции на соодветна локација, има употребна вредност и при дизајнирање на локации за опоравување од катастрофа (disaster recovery sites), при што слична анализа за воспоставените услуги може да се спроведе и за ваков случај, да се добие одговор на прашањето како префрлањето на сервисната низа на секундарна локација би влијаело врз доцнењето на мрежните пакети?

Анализата на мрежниот сообраќај од аспект на негова класификација, може да се користи во пракса кај повеќе системи кои се изградени во облак, приватен или јавен. NFV елементите сега се неизбежен дел од таквите инфраструктурни решенија. 5G инфраструктурата се потпира на овие решенија, но и поврзувањето со такви системи ќе се врши преку 5G пристапната технологија. Во такви случаи, потребата за извршување QoS, проверка на пакети (DPI), безбедноста на мрежата и апликациите, управувањето со податоци, следењето и контролата на системот како целина и процесите кои се одвиваат во него, зависи од валидна класификација на мрежниот сообраќај, која треба да биде точна и брза, без притоа да се користат значителни системски ресурси. Резултатите од овој труд можат значително да помогнат во извршувањето на ваквата класификација при воведување на горенаведените услуги.

1.6.Нацрт на содржината

Воведот дава основни информации за докторската теза со осврт на целите и мотивот за овој научен труд. Накратко се образложени користените научни методи и придонесот на истражувањето, како и потенцијалната примена на добиените резултати.

Во втората глава е даден општ осврт на SDN и NFV како и принципите нsa кои тие работат, со посебен акцент на нивната примена кај мобилните мрежи од петта генерација.

Во третата глава се образложува примената на надледувани (супервизирани) алгоритми за машинско учење, кај системи изградени со помош на SDN елементи и NFV

архитектура за класификација на мрежниот сообраќај. Се образложува експерименталната поставка и се анализираат добиените резултати преку математичка анализа, со цел да се најде најефикасниот алгоритам за класификација на VoIP сообраќај. Во четвртата глава експерименталната поставка, изведените експерименти и направената анализа се проширува и на други типови на мрежен сообраќај.

Аналитички модели на систем изграден преку NFV концептот се предлагаат во петтата глава. Се анализира можноста за дистрибуција на низата од виртуелните мрежни функции на повеќе локации. Во овие околини се пресметува доцнењето на мрежните пакети и се носат заклучоци како дистрибуцијата на системот влијае на латенцијата во мрежната услуга. Се вршат симулации во MATLAB користејќи различни параметри, при што се изведуваат соодветни заклучоци. Аналитичките модели се засновани на теорија на редови, а податочната рамнина е моделирана како отворена Џексонова мрежа.

Шестата глава се надоврзува на претходната, но дистрибуцијата на виртуелните мрежни функции во рамките на NFV се разгледува од експериментален аспект. Се користи експериментален NFV систем кој се протега на две географски оддалечени локации. Се анализираат резултатите од аспект на нивната употреблива вредност во пракса и од аспект на претходно дефинираните аналитички модели.

Последната глава е резервирана за изведување на заклучоци од извршените истражувања.

2. SDN и NFV архитектура

2.1.SDN

Софтверски дефинираното вмрежување е пристап кој користи софтверски контролери или интерфејси за програмирање на апликации (Application Programming Interface - API) за да комуницира со основната хардверска инфраструктура и со цел да го насочува мрежниот сообраќај [41]. Овој модел се разликува од оној на традиционалните мрежи, кои користат дедицирани хардверски уреди (рутери и комутатори) за управување со мрежниот сообраќај. SDN може да креира и контролира виртуелна мрежа, изградена од виртуелни елементи или да контролира традиционален хардвер преку софтвер.

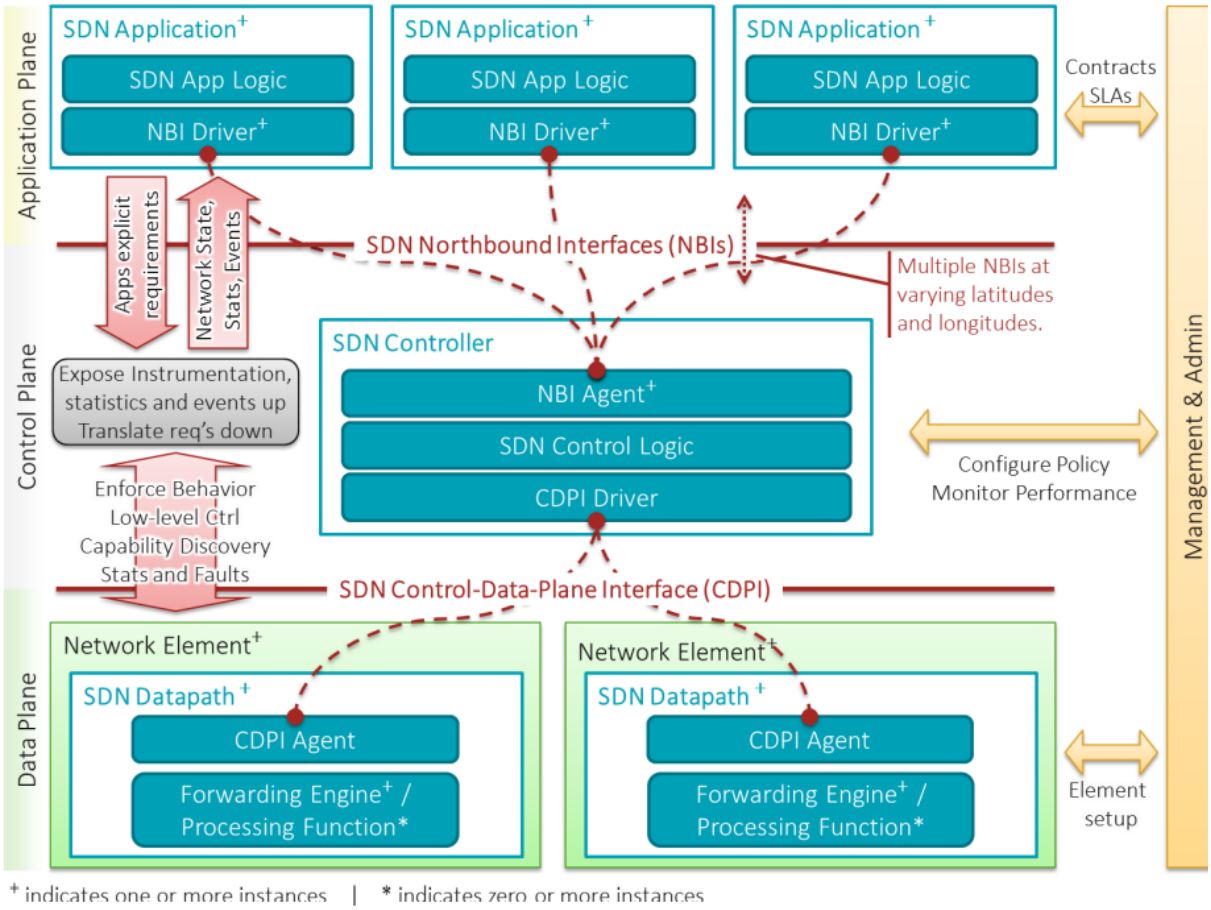
Додека мрежната виртуелизација им овозможува на организациите да сегментираат различни виртуелни мрежи во една физичка мрежа или да поврзуваат уреди на различни физички мрежи за да создадат единствена виртуелна мрежа, софтверски дефинираното вмрежување овозможува нов начин на контролирање на рутирањето на пакетите со податоци преку централизиран сервер. Со тоа се врши одвојување на управувачката рамнина од податочната рамнина, овозможувајќи мрежното управување да стане директно програмибилно. Овој пристап ја дава посакуваната агилност во управувањето и овозможува лесна и брза прилагодливост на мрежата, што го прави идеален за динамичната природа на денешните апликации кои побаруваат висока мрежна пропусност. Основната мрежна инфраструктура е абстрахирана од апликациите и мрежните функции [42].

SDN архитектурата е:

- *Програмибилна* – бидејќи го одвојува управувањето и функциите за препраќање и им овозможува на мрежните оператори да ја конфигурираат, менаџираат, обезбедуваат и оптимизираат мрежата преку апликации [43];
- *Агилна* – овозможува динамичка промена на мрежните параметри;
- *Централно управувана* – преку SDN контролерите мрежното управување е централизирано и одвоено од другите мрежни елементи, а воедно овозможува и агрегиран поглед на целата мрежна топологија:

- *Базирана на отворени стандарди (open-standard based) и неутрална во однос на производители на мрежна опрема* – со самото одвојување на управувачкиот слој и користењето на отворени стандарди, се овозможува неутралност во однос на користењето на мрежна опрема и/или софвер.

На слика 1 е даден приказ на SDN архитектурата според opennetworking.org [42].



Слика 1: Приказ на SDN архитектура [42]

Основните елементи на SDN архитектурата се:

- *SDN Контролер*. Го врши управувањето во SDN базирана мрежа. Тој е врска помеѓу апликациите и мрежните елементи во податочниот слој кои ја формираат SDN сервисната низа. Контролерот е целосно „свесен“ и ја знае мрежната топологија, распоредот и редоследот на елементите во сервисните низи.

- *SDN Апликации*. Ова е програмибилниот дел од SDN архитектурата. Преку нив се програмира посакуваното мрежно однесување и тоа се транслира кон SDN контролерот преку таканаречен NorthBound Interface (NBI).

- *SDN податочни патеки (datapath).* Претставуваат логични мрежни уреди кои може да бидат целосни виртуелни машини, физички уреди или виртуелни мрежни функции кои се експонирани кон SDN контролерот и овозможуваат препраќање на мрежните пакети. Рутирачките елементи, односно дефинирањето на мрежната патека е целосно управувана од контролерот. Уреди се поврзани помеѓу себе во сервисни низи кои обезбедуваат соодветен мрежен сервис од крај до крај.

- *SDN Northbound Interface* е врската помеѓу апликациите и контролерот. Овозможува абстракција на мрежниот поглед. Овој интерфејс е од отворен тип и ја овозможува неутралноста во однос на мрежната опрема. Драјверите и агентите кои се дел од SDN NBI, од една страна се одговорни за преносот на информации кон контолерот во вид на мрежни подесувања и барања, а од друга вршат повратна информации од контролерот назад кон апликациите, околу мрежните параметри и настани.

- *SDN управување и администрација (SDN Management and Administration)* претставува експонираниот дел на SDN преку кој мрежните оператори ја администрираат мрежата. Овој дел може да биде мануелен, управуван од човек или преку експонирани API елементи да биде поврзан со останатите апликации во една организација.

Иако SDN контролерот има улога на централизиран управувач со мрежата, тоа во пракса не значи дека се наоѓа на една локација, напротив, честопати контролната функција може да биде распространета на повеќе физички локации. Дистрибуираната SDN архитектура е предмет на бројни публикации [44][45][46][47][48]. Во понамошниот тек во овој труд, посебен осврт ќе биде даден на дистрибуираната NFV архитектура која е целосно изградена корстејќи SDN, каде меѓу останатите ќе биде моделиран систем дистрибуирана управувачка рамнина и дистрибуирани контролери. Главните недостатоци на централизираната контролна рамнина кај SDN се ограничувањата на приспособливоста, проблемите со перформансите и единствената точка на испад. Од

друга страна, дистрибуцијата на контролната рамнина на повеќе физички локации воведува сложеност и можно каснење на пакетите што влијае на целосната латенција во мрежата.

2.1.1. OpenFlow

OpenFlow протоколот е темелот за изградба на SDN архитектурата [49]. Тој претставува основа на врската помеѓу SDN контролерот во управувачката рамнина и мрежните елементи во податочната рамнина, каде се одвиваат функциите за препраќање. Ова практично значи дека контролерот ја одредува патеката на движење на мрежните пакети низ SDN мрежата и истата ја проследува до комутаторите во податочната рамнина. Тоа го прави преку подесување на табелите за препраќање (forwarding tabels) кај комутатори од ниво 3 (layer 3) согласно OSI (Open Systems Interconnection Model) моделот. Контролерот може да додаде, избрише или промени одредено правило за препраќање, а тоа може да го прави периодично, согласно одреден распоред или ad hoc, што дава огромна функционална флексибилност на мрежата.

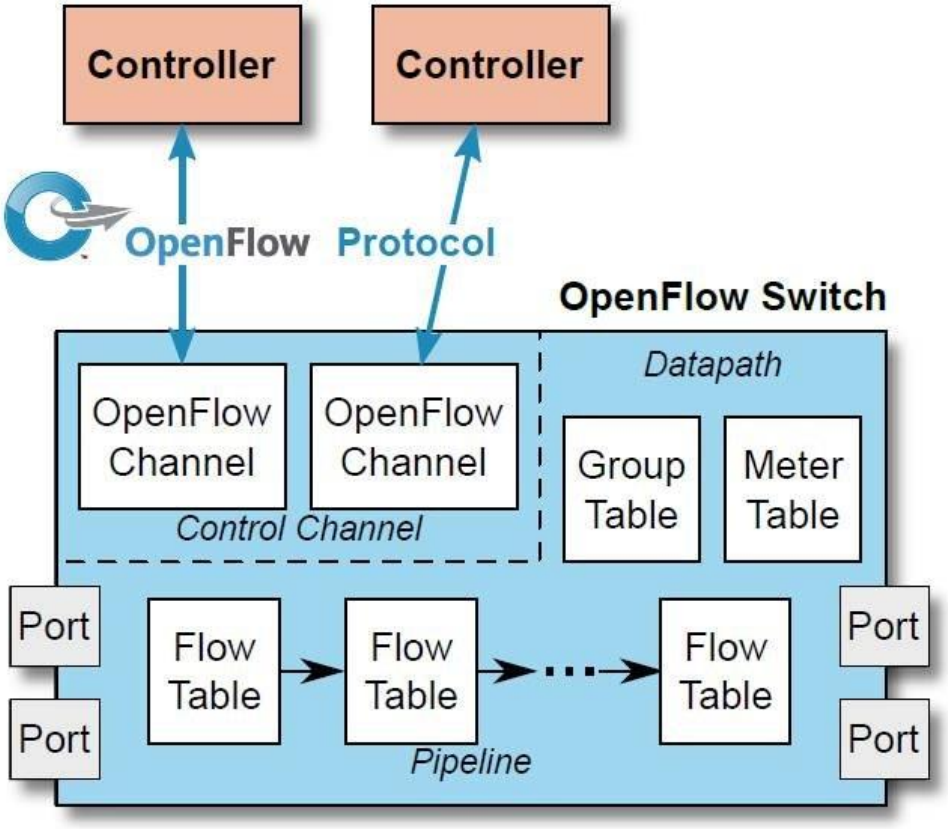
Табелите за препраќање имаат збир на инструкции или правила кои се извршуваат секој пат кога пакетот се совпаѓа со одреден запис. Мрежниот пакет треба да има извор и дестинација кои се совпаѓаат со одредено правило. Секој мрежен проток (network flow) доаѓа директно до податочната рамнина на SDN мрежата, односно до соодветен комутатор. Ако не може да се совпадне со постоечки запис за проток [50], [51], [52]:

- првиот пакет од протокот се испраќа до контролерот во контролната рамнина;
- контролерот ја пресметува оптималната патека за протокот и ги ажурира соодветните правила во табелата за проток;
- последователните пакети од истиот проток се движат директно во податочната рамнина, преку ажурираните табели на проток, без никаква интеракција со контролната рамнина.

OpenFlow протоколот може да се користи и кај централизирани и кај дистрибуирани системи со подеднаква ефикасност. Еден контролер може да управува со еден или повеќе комутатори кои пак може да бидат дистрибуирани на различни физички локации. Можно е и сценарио кога се употребуваат повеќе контролери, а дел од

комутаторите со кои управуваат да се преклопуваат. Во вакво сценарио, согласно SDN архитектурата, секој контролер во секое време мора да има информација за сите табели на проток и целосен преглед на целата мрежа. Тоа се постигнува преку комуникација помеѓу самите контролери во рамките на управувачкиот слој [53]. Експерименталните околини кои се користат, како и аналитичките модели изведени во понатамошниот текст се целосно изградени со користење на OpenFlow протоколот.

На слика 2 [54] е графички прикажана шема на еден OpenFlow комутатор.



Слика 2: Шематска архитектура на Openflow комутатор [54]

2.2.NFV

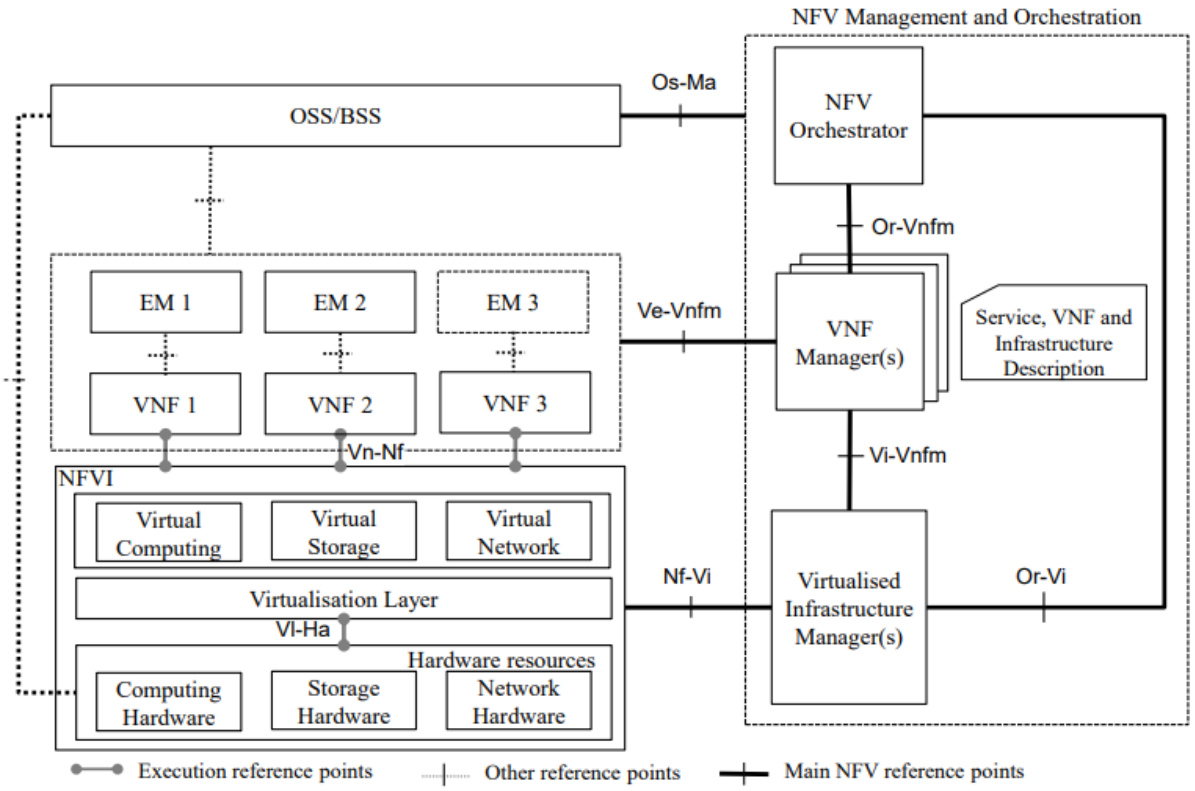
Виртуелизацијата на мрежни функции во основа ја стандардизира употребата на виртуелни елементи во рамките на компјутерските мрежи. Овие елементи се нарекуваат виртуелни мрежни функции. Секоја VNF извршува одреден мрежен сервис и може да има улога на комутатор, рутер, заштитен ѕид (firewall), SD-WAN елемент и слично. Виртуелните мрежни функции може да бидат виртуелни машини кои работат на обични хардверски сервери, но се почесто тие се апликативни контејнери или дедицирани

апликациски функции кои исто така работат на обичен хардвер, но овозможуваат уште поголема искористеност на ресурсите, сегрегација на оперативниот систем, едноставно и брзо скалирање и оперирање.

NFV архитектурата е предложена од Европскиот институт за телекомуникациски стандарди (European Telecommunications Standards Institute - ETSI) [6] кој ги дефинира стандардите за развој и употреба на NFV. Процесот се одвива и развива континуирано. Со употребата на NFV се поедноставува имплементацијата на мрежните услуги, со што се намалува времето потребно одредена услуга или производ да се исфрли на пазарот, се намалуваат капиталните и оперативните финансиски трошоци, се олеснува автоматизацијата на управувањето со мрежата и се поттикнуваат иновациите. NFV технологијата е клучен елемент во модерниот мрежен дизајн и значително влијае во развојот на новите 5G мрежи. Преглед на NFV архитектурата е даден на Слика 3 [55].

NFV архитектурата се состои од четири главни целини:

- *Слој на виртуелни мрежни функции (VNF layer)* каде се основните елементи во рамките на мрежата кои вршат одредена функција и обезбедуваат одреден сервис. Виртуелните мрежни функции ја обезбедуваат агилноста потребна за предвидување или одговор на динамичните перформанси на мрежата или барањата за проширување во хибридни и мултиоблачни средини [56]. VNF се поединечно управувани од Елемент Менаџер Систем (Element Manager System - EMS) кој што управува со конфигурацијата, грешките, перформансите и безбедноста. Во пракса EMS елементите се исто така засебни виртуелни мрежни функции.
- *NFV хардверска и софтверска инфраструктура (NFVi).* Составена е од процесирачки хардевер и софтвер, најчесто во форма на хипервизори и ги обезбедува ресурсите врз кои работат виртуелните мрежни функции. Составена е од: хардверски ресурси, виртуелизациски слој и виртуелни ресурси. NFVi е критична во градењето комплексни, широко дистрибуирани мрежи без географски ограничувања поврзани со традиционалните мрежни архитектури.



Слика 3: NFV архитектура [55]

- *Управување, автоматизација и мрежна оркестрација (Management, automation and network orchestration - MANO).* Го обезбедува фрејмворкот за управување со NFV инфраструктурата и ги координира ресурсите во NFVi делот како и кај VNF. Во NFV MANO се дефинирани стандардни темплјети за виртуелни мрежни функции што овозможува мрежните архитекти да одберат соодветни сервиси и да доделат соодветни ресурси од инфраструктурата. VNF MANO е поврзан и со слојот на виртуелни мрежни функции и со NFV инфраструктурата. Составен е од 3 компоненти:
    - *Менаџер на виртуелизираната инфраструктура (Virtualised Infrastructure Manager - VIM)* кој е врската помеѓу MANO и NFVi слојот. Управува со физичките ресурси и ја обезбедува виртуелизацијата. VIM е зависен од физичките ресурси на хардверот врз кој што работи и врши негова апстракција. Доколку ресурсите со кои располага се доволни, тој делува самостојно и не делува на квалитетот на услугата која се обезбедува преку мрежата.

- *Менаџер на виртуелни мрежни функции (Virtual Network Infrastructure Manager - VNFM)* кој е задолжен за креирање и на нови и уништување на непотребни VNF (вертикално скалирање), но по потреба и додавање и одземање на ресурси на постоечките VNF (хоризонтално скалирање).
- NFV Оркестратор (NFVO). Задолжен е за реализација на мрежните услуги, од крај до крај.

- *Оператор на систем за оперативна поддршка/систем за деловна поддршка (Operation Support System/Business Support System – OSS/BSS).* Претставува врска помеѓу OSS/BSS системи и MANO делот на NFV. Се одвива преку стандардизирани интерфејси и ја заокружува деловната употребливост на NFV архитектурата.

2.2.1. NFV и 5G

NFV архитектурата се смета за главен двигател на развојот на 5G мрежите [57]. Тие се сеуште во развој, но основните карактеристики на секоја 5G базирана мрежа се: висока приспособливост, ултра ниска латентност, способност за поддршка на голем број корисници и паралелни сесии, висока доверливост и безбедност. Овие особини се возможни преку употреба на NFV архитектурата, а главните карактеристики кои тоа го овозможуваат, според ETSI NFV Industry Specification Group (ETSI NFV ISG) се:

- *мрежното раслојување (network slicing);*
- *мрежни функции приспособени за работа во облак (cloud-native network functions);*
- *управување со сервисите од крај до крај (end-to-end service management);*
- *локација на сметачките капацитети кон мрежниот раб (edge computing);*
- *сместување на радио пристапната мрежа во облак (RAN cloudification);*
- *сервиси на повеќе локации – дистрибуција (multi site NFV);*
- *управување со NFV лиценци (NFV license management);*

- *безбедност (security);*
- *доверливост (reliability);*
- *скалабилност (scalability).*

Мрежното раслојување претставува имплеметација на „Network as a Service“ парадигмата. Тоа овозможува мрежата изградена врз NFV архитектура да се користи за повеќе независни, паралелни сервиси, кои се изолирани меѓу себе и кај кои што може да се имплеметира соодветен QoS. Иако се користат истите ресурси, мрежните слоеви може да се сметаат за сосема изолирани мрежи на логичко ниво. Честопати во пракса, мрежните слоеви кај NFV архитектурата се поистоветуваат со традиционалните VLAN-и, но тоа не е така. VLAN-ите претставуваат одделување на мрежниот сообраќај за различни корисници, но одделните VLAN-и имаат влијание еден врз друг (на пример при густ сообраќај предизвикан од еден VLAN) и комуницираат меѓу себе. Мрежното раслојување претставува комплетна изолација, секој слој е сосема различна мрежа со свои ентитети за управување и насочување, со сопствени перформанси и управување со грешки. Овие слоеви се исклучително битни при воспоставувањето на изолирани услуги, кои поминуваат низ сосема различни сервисни низи. Се смета дека NFV раслојувањето е иднината на меѓу-операторската комуникација [58], овозможувајќи пристапни пазарни цени [59].

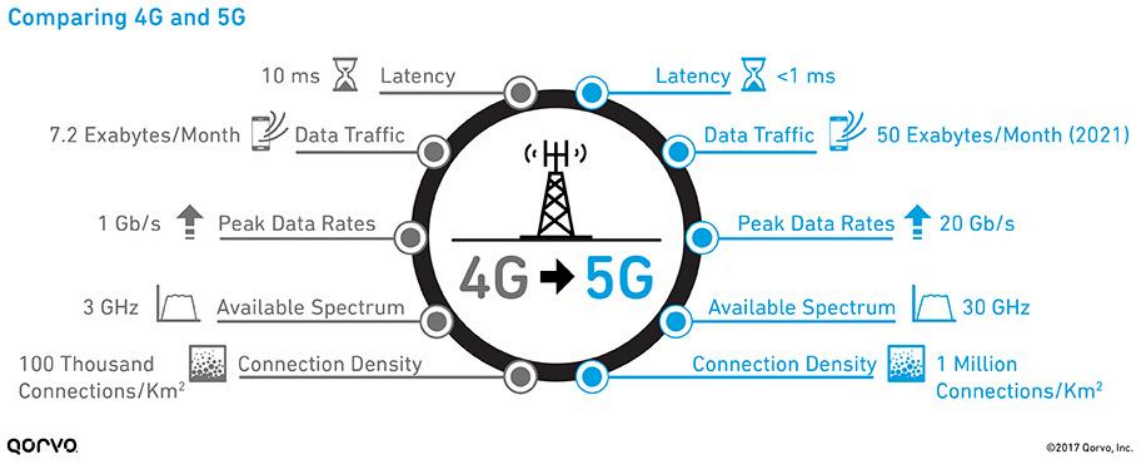
Поставувањето на сметачките и складишните капацитети кон мрежниот раб претставува предизвик кој е од исклучителна важност, со цел да се добијат сервиси кои од една страна имаат финансиска логика, а од друга страна обезбедуваат квалитетни услуги со мала латентност и висока доверливост. Токму услугите со ултра ниска латентност ја прават диференцијацијата на 5G мрежите во однос на претходните технологии. Ова значи дека виртуелните мрежни функции кои ја формираат мрежната сервисна низа, мора да работат на сметачки капацитети кои се во непосредна близина на крајниот корисник, на работ од мрежата. Тоа значи и дека самата NFV архитектура треба да се дистрибуира на повеќе географски локации. Ова претставува предизвик со позитивни и негативни страни. Повеќе автори ги испитуваат факторите кои влијаат на каснењето на мрежните пакети кај дистрибуираните NFV системи, како од експериментален [60], така и преку теоретски пристап [61]. Во главите 5 и 6 од овој труд ќе бидат анализирани токму вакви случаи. Дистрибуцијата на NFV на повеќе локации и

барањата за конективност во ваквите случаи, е предмет на истражување, како во академската средина, така и кај NFV ISG, при што се очекува спецификациите од NFV framework 3 да ги содржат протоколите за ваквата поврзаност. Во глава 6 ќе анализираме математички модели на централизирана и дистрибуирана NFV архитектура, со анализа на карактеристиките кои влијаат на мрежната латентност.

Безбедноста на сообраќајот во мрежите базирани на NFV архитектура ќе биде разгледуван од аспект на класификација на мрежните пакети во глава 3 и 4 [62][63]. Бидејќи гласовните сервиси се сеуште основа на 5G мрежите и телекомуникациските оператори, посебен осврт ќе биде даден на класификацијата на VoIP сообраќајот [64].

3. Класификација на VoIP во околина базирана на NFV архитектура

VoIP комуникацијата е еден од основните елементи на мобилните мрежи од петта генерација. Покрај повиците, технологиите во облак, IoT, социјалните мрежи и постојаната комуникација со која крајниот корисник, човек или машина, е постојано „on-line," побарува голема пропусност и мала латенција. 4G мрежите ја немаат архитектурната приспособливост која овозможува лесна приоретизација на мрежните пакети, па во моменти на висока искористеност доаѓа до висока латенција. Во ваква ситуација говорните и видео повиците може да бидат неквалитетни, со чести прекини, паузи, дисторзија и испад на повиците, односно потребни се големи инвестиции и комплицирана мрежна архитектура за избегнување на овие негативни елементи. Обезбедување на QoS кај VoIP претставува приоритет во било која мрежна поставеност. Иако 5G мрежите обезбедуваат драстично помала латенција, обезбедувањето на QoS останува висок приоритет. Самата архитектура на 5G мрежите овозможува пропусниот опсег да се прилагодува динамички. На слика 4 е дадена визуелна споредба меѓу карактеристиките на 4G и 5G [65].



Слика 4: Споредба меѓу 4G и 5G [65]

Мрежното раслојување кое го обезбедува NFV архитектурата и кое претходно го споменавме, е уште еден механизам кој овозможува изолација на различните типови на

мрежен сообраќај и соодветно доделување на ресурси, вклучително и пропусен опсег, со што се овозможува услугите кои имаат повисок приоритет да бидат со највисок квалитет. Тука, како најидеален кандидат се наметнува VoIP сообраќајот.

Класификацијата на мрежниот сообраќај претставува основа за оперирањето со мрежата. Секако тука основен елемент е обезбедување на QoS [66], но секако класификацијата на сообраќајот овозможува мрежна безбедност, управување со мрежата, соодветно насочување на сообраќајот, анализа за подобрување и оптимизација на мрежните капацитети. За таа цел во продолжение се врши анализа на можностите за класификација на мрежниот сообраќај, специфично на VoIP сообраќајот, во систем базиран на NFV архитектура, со користење на алгоритми за надгледувано машинско учење [91].

Шифрираниот мрежен сообраќај е во брз пораст. Значителен број услуги и апликации користат шифрирање како примарен метод за безбедност на информациите. Но, ова ја прави класификацијата на сообраќајот сериозен предизвик. Решението за класификација на сообраќајот што го предлагаме е применливо во пракса без да се загрози приватноста и интегритетот на податоците, дава увид во перформансите на надгледуваните алгоритми за машинско учење и одредува кој е најсоодветен за околина базирана на NFV архитектура.

Овој труд се фокусираме на 6 различни ML алгоритми: Bayes Net, Naïve Bayes, J48 (како имплементација на C4.5), K-Nearest Neighbours (K-NN), Decision Tree и AdaBoost. Овие алгоритми се избрани поради фактот што тие се најчестите ML алгоритми кои се користат во традиционалните мрежи и се докажани како сигурни во пракса. Поради механизмите за шифрирање што се користат за VoIP мрежниот сообраќај и спецификите на сообраќајот исток-запад, користењето на традиционалните механизми за класификација на сообраќајот е невозможно. Во анализата не се користат информациите за содржината на мрежните пакети (packet payload), комуникациските порти, IP адресите и MAC адресите на ентитетите на изворот и одредиштето на самите мрежни пакети. Наместо тоа се користат исклучиво статистичките карактеристики на пакетите и пакетните текови (packet flows), со цел да се креира сет за тренирање за ML алгоритмите. По тренингот се тестира прецизноста за класификација на VoIP сообраќајот на секој од алгоритмите, како и брзината со која алгоритмите го вршат процесирањето.

Создадовме средина за тестирање, во која сообраќајот се пресретнува (sniffing) во рамките на Open vSwitch [67], директно слушајќи го сообраќајот кој се движи во насока исток-запад, без воведување надворешна сонда или SDN уред што ќе ги копира податоците. Целиот мрежен сообраќај се набљудува како целина, вклучувајќи ја и комуникацијата меѓу мрежните елементи, како и податоците за управување со мрежните елементи, бидејќи ова е реално сценарио во пракса. VoIP сообраќајот (и шифриран и нешифриран) успешно се препознава под овие услови. Бидејќи ML алгоритмите го трошат процесирачкото време во виртуелизираните околини и истовремено влијаат на латентноста во мрежата додавајќи доцнење на пакетите, брзината на ML алгоритмите е многу важен аспект за севкупната ефикасност.

3.1. Поврзана работа и дискусија

Класификацијата на мрежните пакети и длабоката инспекција на пакети имаат клучно значење во мрежните средини. Бидејќи амбицијата на 5G е да се обединат многу услуги преку една платформа, со што ќе се обезбеди основа за понатамошен развој на системи и апликации, од големо значење е да се има валиден DPI што ќе обезбеди квалитетни резултати, а во исто време нема да го зголеми доцнењето на пакетите во мрежата. Постојат истражувања кои се фокусирани на DPI во SDN [10, 11, 12] додека други се фокусирани на безбедносните аспекти на DPI [13, 14]. Често се употребува принцип на додавање на сонди или SDN уреди во мрежата. Класификацијата на мрежниот сообраќај во традиционалните мрежи е истражувана во делата на [15, 16], но тие не ја разгледуваат употребата на ML алгоритми во NFV околина, што е случај во ова истражување. Со самиот факт што за класификација не ја користиме како статистичка карактеристика содржината на пакетите, нашето истражување по дефиниција не е DPI, а добиваме голем број информации кои би ги добиле вршејќи класична DPI.

Авторите на [68] предлагаат дизајн кој користи виртуелни мрежни функции, со цел, флексибилно избирање и примена на најдобрите ML алгоритми за класификација во реално време, во фазата на работа на самата мрежа. Тие анализираат повеќе ML алгоритми, како што се K-Nearest Neighbor, Support Vector Machine, Decision Tree, Ada-Boost, Naive Bayes и Multi-Layer perception. Експерименталните резултати покажуваат подобрување од 13% во точноста на класификацијата на протокот користејќи го

предложениот NFV. Споредбено со ова истражување и овие автори потврдуваат дека Decision Tree алгоритамот врши најпрецизна класификација, како што понатаму ќе видиме и во нашето истражување. Времето потребно за класификација и доцнењето кое притоа се воведува не е цел на овие автори.

Вергара-Рејес и сор. [69], градат експериментална NFV средина во која генерираат различни типови на TCP сообраќај. Мрежните пакети се анализирани со користење на три различни ML алгоритми: J48, Naive Bayes и Bayes Net, со цел да се изврши анализа на перформансите на алгоритмите. Статистичките параметри на поединечните пакети се земени во предвид за да се подготват комплетите за обука и тестирање за ML алгоритмите. Создадени се три различни сетови на податоци: традиционални, виртуелни и комбинирани за подобро да се карактеризира сообраќајот во мрежите базирани на NFV. Од друга страна, во нашето истражување работиме со статистички параметри на мрежните протоци, наместо на поединечните пакети, во експериментална околина која исто така е базирана на NFV архитектура и која е подесена да има слична поставеност со околините типични за инфраструктурите изградени во облак. Во нашето истражување се фокусираме на шифриран и нешифриран VoIP сообраќај, како основа на говорните услуги кај 5G мрежите и споредуваме повеќе ML алгоритми. Сепак добиените резултати за алгоритмите кои се преклопуваат во истражувањето на овие автори и во нашето истражување се слични и споредливи.

Алшамари и сор. [70] го покриваат DPI на VoIP сообраќајот во традиционалните мрежи, користејќи реални податоци од постојни мрежни околини со различна топологија (со и без заштитен ѕид) и различни методи за пристап (WiFi или Ethernet), за да се оцени прецизноста на три ML алгоритми: C5.0 , ADA Boost и GP класификатор. За евалуација на ML алгоритмите користат техника на земање примероци од подмножество на целиот сет на податоци врз кои се врши статистичка анализа и се одредува стапката на лажно позитивни резултати. Нивното истражување покажува дека C5.0 постигнал највисоки перформанси, со најголема прецизност и најниска стапка на лажно позитивни резултати. За споредба, нашата работа е фокусирана на околина базирана на облак, со акцент на NFV архитектура и надгледувани ML алгоритми.

[71] предлага систем за предиктивна анализа во работен режим кој работи паралелно со постоечки системи за реактивен мониторинг кои се употребуваат во рамките на мрежените оператори. Пристапот заснован на длабоко учење се користи за да се

идентификуваат аномалиските настани во логовите на NFV системот, со цел да се идентификуваат потенцијалните аномалии и да се преземат неопходните проактивни активности за нивно исправање во мрежата.

Авторите на [72] го истражуваат ефектот врз мрежниот сообраќај предизвикан од поставувањето на виртуелните мрежни функции, кои формираат SDN низа во рамките на NFV, врз зголемувањето или намалувањето на обемот на обработениот сообраќај. Развиен е алгоритам кој ја одредува патеката на проток и редоследот на мрежните функции, а потоа се предлага рутирање од тип: Најмал-Прв-Најголем-Последен (Least-First-Greatest-Last).

Работата на Бонфиљо и сор. [73] е базирана на Skype и неговиот генериран сообраќај, кој е специфичен без оглед на основната архитектура врз која работи. Се занимава со два различни пристапи за откривање на шифрираниот сообраќај на Skype во реално време, врз основа на статистичките параметри на генерираните пакети. DPI и корелацијата на протокот се користат за да се процени ефективноста на предложените пристапи. Слично на ова истражување и во нашето истражување се користи Skype, како и Viber како апликации кои користат VoIP и кои имаат енкрипција. Како што ќе видиме, надгледуваните ML алгоритми имаат висока ефикасност во класификација на енкриптираниот сообраќај кој овие апликации го користат, користејќи ги само статистичките параметри на воспоставените мрежни текови на пакетите, без потреба за пристап до содржината на пакетот (која и онака не е достапна, поради енкрипцијата).

Во [74], ML алгоритмите, платформите за анализа на големи податоци, SDN и NFV елементите се користат за да се изгради сеопфатна рамка за развој на идни апликации за самоорганизирана 5G мрежа (SON), како и рамка за групирање, предвидување и управување со сообраќајот за огромен број базни станици со различни статистички карактеристики на сообраќајот на различни типови уреди (GSM, 3G, 4G). Сообраќајните текови се анализирани и имплементирана е контрола на QoS базирана на SDN за да се овозможи гаранција за пропусниот опсег за секоја апликација. Во оваа студија, се користат 5 различни ML алгоритми за прецизна класификација на мобилните апликации. За класификација се користат различни типови на шифриран сообраќај. Се покажува дека алгоритамот Random Forrest има најдобри вкупни перформанси во однос на другите тестирани алгоритми. Споредено со ова, нашиот фокус е на перформансите на VoIP и ML алгоритмите во прецизност и брзина во средина каде што се распоредени NFV елементи,

сценарио изводливо за идниот развој на 5G. Во нашиот случај Decision Tree алгоритамот покажува најдобра ефикасност. Имајќи предвид дека тој е специфичен случај на Random Forrest алгоритамот, при што се користи само едно дрво на разгранување, нашето истражување покажува слични резултати со [74].

Генерално, во нашето истражување е воведена слична околина за тестирање како [69] и [70], при што се додадени нови елементи, како сервисни низи составени од виртуелни мрежни уреди со пристап до интернет, од кои се генерира VoIP сообраќај. Покрај шифрираниот и нешифрираниот VoIP-базиран UDP сообраќај, генерираме рандомизиран TCP и UDP сообраќај, а класификацијата ја вршиме врз основа на избрани статистички параметри на мрежните текови. Skype и Viber се избрани како најкористени peer-to-peer VoIP клиенти кои вклучуваат шифрирање. Самата тестна околина претставува новитет, бидејќи инкорпорира SDN и NFV пристап, со цел да се симулира 5G комуникација. Податоците се анализираат директно во мрежниот проток на податоци помеѓу NFV елементите, без воведување на физички или SDN сонди. Како што е прикажано во следниот дел, се оценуваат прецизноста и брзината на шест различни алгоритми во однос на тоа кој алгоритам најдобро функционира во рамките на целното сценарио.

3.2.Експериментална околина и генерирање на податочни множества

За да го симулираме мрежниот сообраќај исток-запад во виртуелизирана мрежа базирана на NFV, создадовме експериментална средина во која Oracle VirtualBox [75] е инсталиран на еден физички хост на сервер кој работи со Ubuntu 18.04 оперативен систем. Open vSwitch (OVS) [67, 76] е инсталиран на домаќинот за мрежна комуникација, овозможувајќи да се пресретнува целиот мрежен сообраќај што минува низ него. Овозможува снимање на сите преносни мрежни пакети. Ги користиме Wireshark и tshark [77] за мрежно снимање на пакетите.

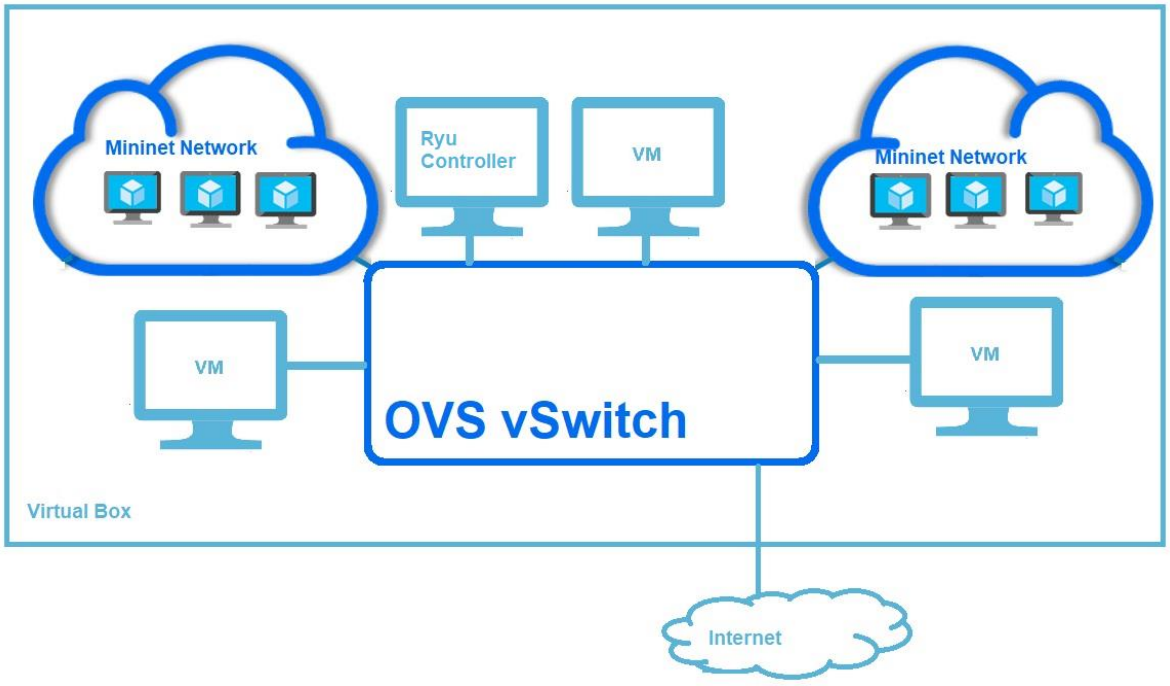
Слика 5 ја прикажува експерименталната средина што се користи. На две виртуелни машини е инсталиран мрежен симулатор Mininet [78] кој се користи за создавање на 2 мрежи со по 100 хостови, 20 комутатори и врски меѓу нив, како и кон OVS. Мининет хостовите претставуваат симулација на виртуелни мрежни функции, кои поврзани помеѓу себе формираат сервисна низа. Мрежите имаат приватни IP адреси и се способни да комуницираат една со друга користејќи GRE тунелирање, во рамките на OVS

комутаторот. Некои од симулираните хостови се NAT-ирани и имаат пристап до интернет. Симулираните мрежи се управуваат со помош на Ryu Controller [79] кој е инсталиран во дедицирана виртуелна машина.

За генерирање на TCP и UDP сообраќај, се користи генератор на дистрибуиран интернет сообраќај (D-ITG) [30] во рамките на хостовите создадени во Mininet мрежите. D-ITG произведува сообраќај на ниво на пакети, симулирајќи соодветни стохастички процеси за времето на поаѓање на мрежните пакети (IDT - Inter Departure Time) и големината на пакетите (PS - Packet Size).

Три дополнителни виртуелни машини, исто така поврзани на OVS комутаторот, со Skype и Viber клиенти инсталирани на нив, го симулираат шифрираниот UDP VoIP сообраќај во peer-to-peer комуникација. Аудио повиците се вршат меѓу клиентите со случајно времетраење. При иницирање, на VoIP сообраќајот му треба пристап до интернет, но потоа комуникацијата се одвива целосно во рамките на експерименталната средина, во правец исток-запад, целосно движејќи се низ OvS комутаторот.

Виртуелните машини во себе имаат и Python скрипта која автоматски стартува ssh сесии кон случајно одбрани Mininet хостови. Ssh сесиите се стартуваат во временски интервали кои ја следат Поасановата дистрибуција.



Слика 5: Експериментална средина

Направивме 50 експериментални итерации за да генерираме различен сообраќај (со користење на D-ITG, Skype, Viber, сопствени скрипти) и да го анализираме. Експериментите беа спроведени во временски интервали од 4 до 20 минути во кои VoIP повиците траеја од 10 секунди до 10 минути, следејќи дистрибуција по Поасон. За секоја експериментална итерација се генерира по едно податочно множество. Во секоја експериментална итерација се користеа различни D-ITG скрипти за различна симулација на сообраќај. Скриптите користеа различни Мининет хостови и различни патеки во секој обид. Просечниот број на снимени пакети беше 1.262.375, а просечниот број на мрежни текови беше 4090.

За класификација на мрежниот сообраќај, користени се 3 класи, означени како: VOIP – за нешифриран VoIP сообраќај, EncVOIP – за шифриран VoIP сообраќај и OTHER – за сите други мрежни пакети.

Кога се набљудува сообраќајот, може да се забележат повеќекратни текови во рамките на OVS комутаторот од сообраќајот кој се одвива помеѓу виртуелните мрежни функции (виртуелни хостови на Мининет), сообраќајот кој произлегува од виртуелните машини, како и управувачкиот сообраќај генериран од хипервизорот и контролерот. Карактеристиките на мрежните пакети и текови кои не се валидни во една NFV околина или пак во случаи кога сообраќајот е енкриптиран, не се користат. Такви карактеристики се изворната и дестинацискатa IP адреса и MAC адресите на уредите како и комуникацискатa порта која може да е варијабилна. За да ги генерираме податочните сетови, избравме создавање на податочни множества базирани на мрежен тек. Слично на [70], го дефинираме мрежниот тек (network flow) како двонасочна врска помеѓу два домаќини. TCP тековите завршуваат или со тајм-аут на текот или со прекин на врската помеѓу хостовите, додека UDP тековите се завршуваат со тајм-аут на протокот. За генерирање на мрежни текови од сниманиот сообраќај го користевме Argus [80].

Врз основа на искуството од традиционалните мрежи и со внимателно набљудување на добиените множества на податоци, ги избравме атрибутите дадени во Табела 1, како атрибути што ги карактеризираат мрежните текови. Содржината на мрежните пакети (ip packet payload) не се користи во анализата, поради зачувување на приватноста на сообраќајот, која честопати е и правно регулирана и не смее да се прегледува, како и поради употребата на различни методи за шифрирање во пракса, што ја прави содржината на мрежните пакети нечитлива и ирелевантна за класификацијата.

Етикетите (ip packet labels) во заглавието на транспортниот слој (на пример броевите на портите) исто така не се користат, бидејќи може лесно да се менуваат. Во табелата 1 е дадено кратко објаснување за секој од избраните атрибути.

ТАБЕЛА 1: КАРАКТЕРИСТИКИ НА МРЕЖЕН ТЕК

	КРАТЕНКА	**КАРАКТЕРИСТИКА**	**FEATURE**
1	*proto*	ТРАНСАКЦИСКИ ПРОТОКОЛ	TRANSACTION PROTOCOL
2	*rate*	БРОЈ НА ПАКЕТИ ВО СЕКУНДА	PACKETS PER SECOND
3	*srate*	БРОЈ НА ПАКЕТИ ВО СЕКУНДА НА ИЗВОРОТ	SOURCE PACKETS PER SECOND
4	*drate*	БРОЈ НА ПАКЕТИ ВО СЕКУНДА НА ДЕСТИНАЦИЈАТА	DESTINATION PACKETS PER SECOND
5	*sintpkt*	ВРЕМЕНСКИ ИНТЕРВАЛ НА ПРИСТИГАЊЕ ПОМЕЖУ ПАКЕТИТЕ НА ИЗВОРОТ	SOURCE INTERPACKET ARRIVAL TIME
6	*dintpkt*	ВРЕМЕНСКИ ИНТЕРВАЛ НА ПРИСТИГАЊЕ ПОМЕЖУ ПАКЕТИТЕ НА ИЗВОРОТ	DESTINATION INTERPACKET ARRIVAL TIME
7	*sjit*	ВРЕМЕНСКО КАСНЕЊЕ ПРИ ИСПРАЌАЊЕ НА ПАКЕТ	SOURCE JITTER
8	*djit*	ВРЕМЕНСКО КАСНЕЊЕ ПРИ ПРИМАЊЕ НА ПАКЕТ	DESTINATION JITTER
9	*moffset*	СРЕДНА ВРЕДНОСТ НА ГОЛЕМИНАТА НА TCP ХЕДЕРОТ НА ПАКЕТИТЕ ВО ЕДЕН ТЕК	MEAN OF THE DATA OFFSET VALUES OF THE PACKETS IN THE FLOW
10	*smeansz*	СРЕДНА ВРЕДНОСТ НА ГОЛЕМИНАТА НА ПАКЕТИТЕ НА ИЗВОРОТ	MEAN OF THE FLOW PACKET SIZE TRANSMITED BY THE SOURCE
11	*dmeansz*	СРЕДНА ВРЕДНОСТ НА ГОЛЕМИНАТА НА ПАКЕТИТЕ НА ДЕСТИНАЦИЈАТА	MEAN OF THE FLOW PACKET SIZE TRANSMITED BY THE DESTINATION
12	*smaxsz*	МАКСИМАЛНА ГОЛЕМИНА НА ПАКЕТ НА ИЗВОРОТ	MAX PACKET SIZE FOR SOURCE
13	*dmaxsz*	МАКСИМАЛНА ГОЛЕМИНА НА ПАКЕТ НА ДЕСТИНАЦИЈАТА	MAX PACKET SIZE FOR DESTINATION
14	*sminsz*	МИНИМАЛНА ГОЛЕМИНА НА ПАКЕТ НА ИЗВОРОТ	MIN PACKET SIZE FOR SOURCE
15	*dminsz*	МИНИМАЛНА ГОЛЕМИНА НА ПАКЕТ НА ДЕСТИНАЦИЈАТА	MIN PACKET SIZE FOR DESTINATION

За тренирање и тестирање на надгледуваните ML алгоритми, користевме Weka [81]. 2/3 од секое податочно множество беше искористено за тренирање, додека 1/3 беше искористено за тестирање на секој од алгоритмите. Бидејќи не сите атрибути имаат ист придонес во класификацијата, се користеше AttributeSelectedClassifier со Ranker како

алгоритам за рангирање на атрибути, со цел да се рангираат атрибутите според својот придонес во класификацијата. InfoGainAttributeEval се користеше како евалуатор кој ја одредува добивката на информации што ја носат атрибутите. Со овој пристап ги рангираме атрибутите кои се користат за алгоритмите, по што се оценува информацискатa добивка на секој атрибут. Овој пристап спречува можно истекување на податоци.

3.3.Резултати од експериментот и анализа

Подготвивме 50 експериментални множества на податоци и тестиравме 6 различни ML алгоритми врз нив. Конечните индикатори за перформанси на алгоритмите се средната вредност и статистичкото стандардно отстапување на прецизноста на алгоритмите во класификацијата, но исто така и вистинската позитивна стапка (True Positive - TP Rate) и лажно позитивната стапка (False Positive - FP Rate) на класификацијата, кои комбинирано ги даваат перформансите на класификацијата на алгоритмите.

Вистинска позитивни (True Positive – TP) е број на примери од множеството на податоци кои се правилно идентификувани во класата.

Лажно позитивни (False Positive – FP) е број на примери од множеството на податоци кои се погрешно идентификувани во класата.

Вистинска негативни (True Negative – TN) е број на примери од множеството на податоци кои се кои се вистински идентификувани дека не припаѓаат на класата.

Лажно негативни (False Negative – FN) е број на примери од множеството на податоци кои се кои се погрешно идентификувани дека не припаѓаат на класата.

Прецизноста на алгоритамот [81] се дефинира како пропорција на примери кои се правилно идентификувани во класата, поделена со вкупните примероци класифицирани како таа класа.

$$Precision = TP/(TP+FP) \quad (1)$$

Вистински позитивната стапка (TP Rate) е пропорцијата на инстанци кои се точно класифицирани и вкупниот број на инстанци кои навистина припаѓаат на таа класа.

$$TP\ Rate = TP/(FN+TP) \quad (2)$$

Лажно позитивната стапка (FP Rate) е пропорцијата на инстанци кои се погрешно класифицирани и вкупниот број на инстанци кои навистина припаѓаат на таа класа.

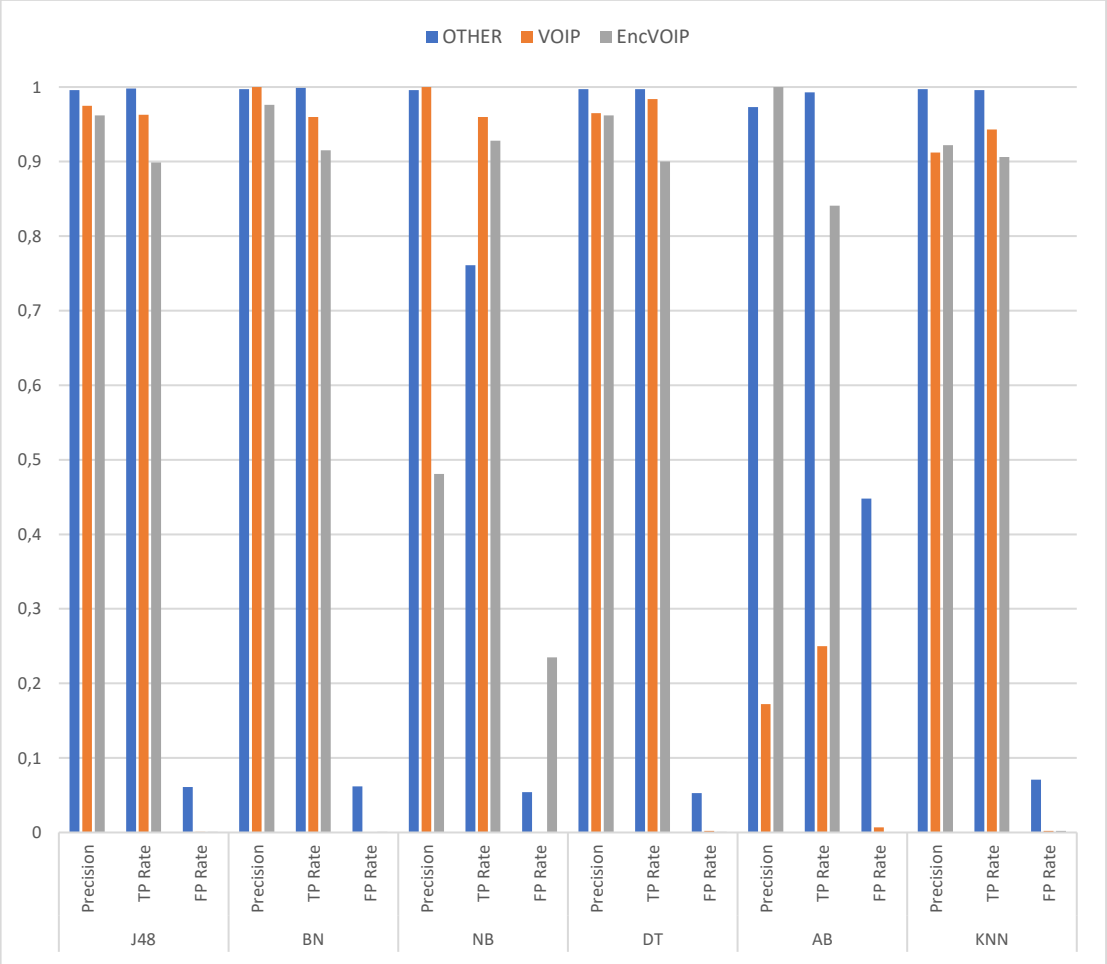
$$FP\ Rate = FP/(FP+TN) \quad (2)$$

Во Табела 2 се дадени резултатите кај шесте испитувани надгледувани ML алгоритми. Прецизноста, вистински позитивната стапка и лажно позитивната стапка се пресметани за секој алгоритам и за соодветни класи дефинирани при поделбата.

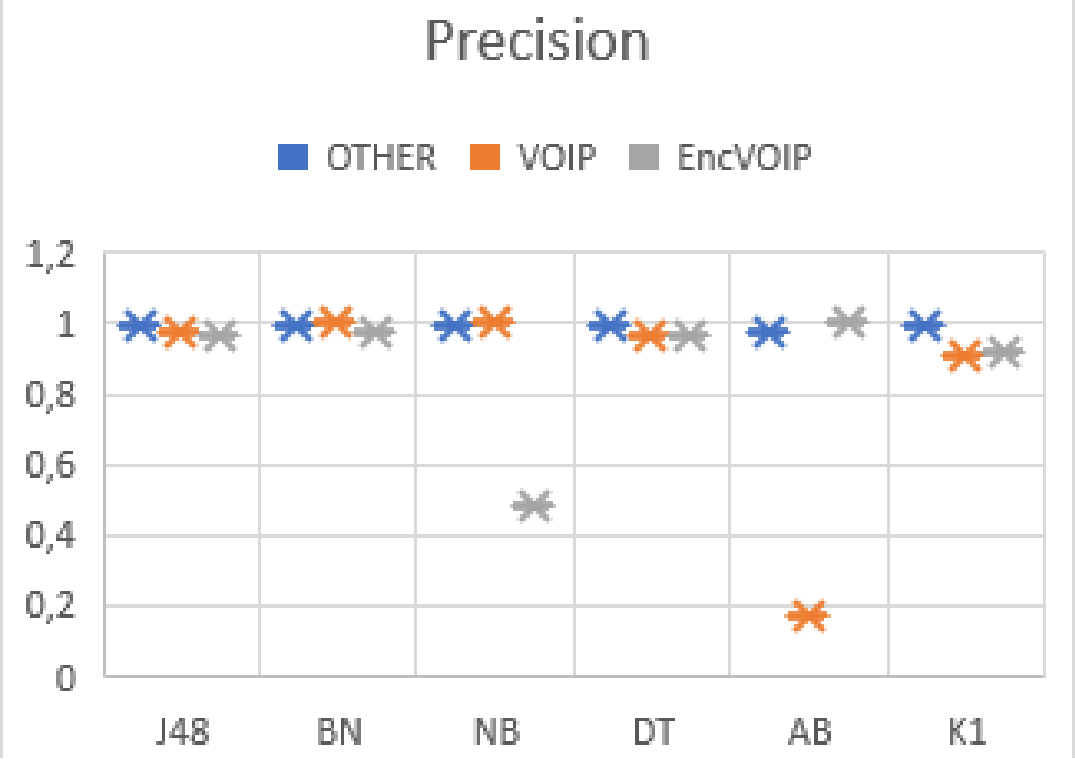
Резултатите се визуелно претставени на слика 6. Најдобрата класификација е направена од алгоритмите кои имаат поголема прецизност и TP стапка, а помала FP стапка. На сликите 7, 8 и 9, резултатите се прикажани поединечно, за ML алгоритмите во фокус.

ТАБЕЛА 2: РЕЗУЛТАТИ ПРИ КЛАСИФИКАЦИЈА

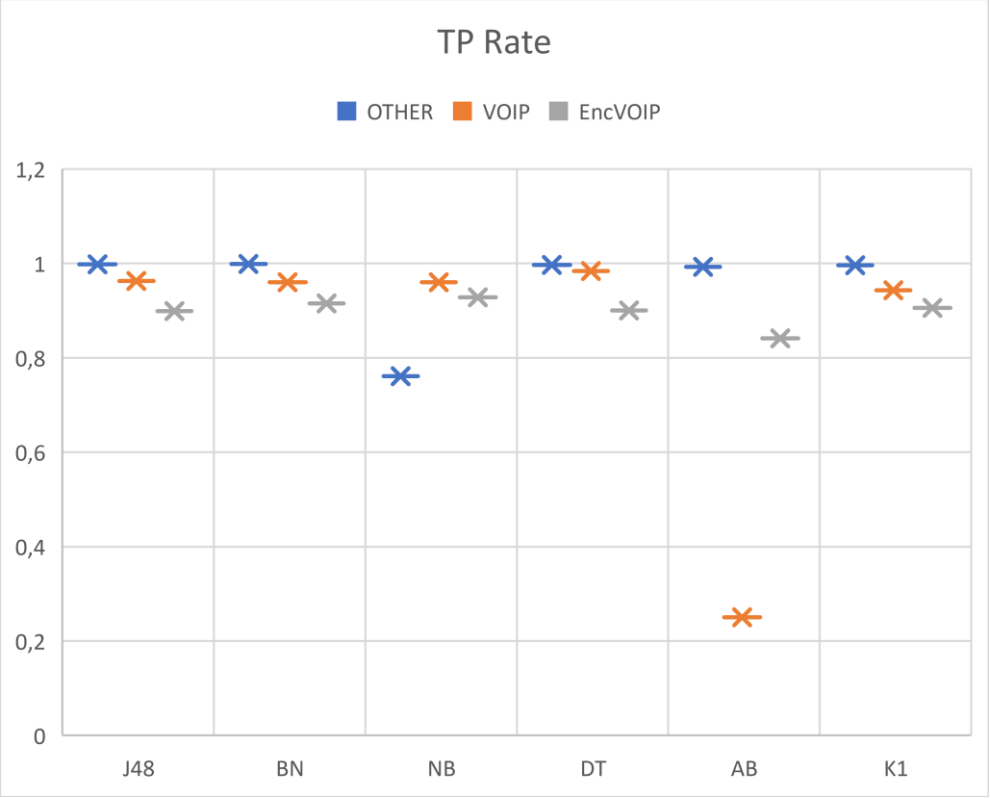
		OTHER	**VOIP**	**ENCVOIP**
J48	PRECISION	0,996±0,002	0,975±0,051	0,962±0,011
	TP RATE	0,998±0,002	0,963±0,044	0,899±0,019
	FP RATE	0,061±0,031	0,001±0,003	0,001±0,001
BayesNet	PRECISION	0,997±0,002	1,000±0,000	0,976±0,033
	TP RATE	0,999±0,001	0,960±0,080	0,915±0,077
	FP RATE	0,062±0,075	0,000±0,000	0,001±0,001
Naive Bayes	PRECISION	0,996±0,003	1,000±0,000	0,481±0,504
	TP RATE	0,761±0,276	0,960±0,080	0,928±0,070
	FP RATE	0,054±0,034	0,000±0,000	0,235±0,271
Decision Tree	PRECISION	0,997±0,001	0,965±0,047	0,962±0,044
	TP RATE	0,997±0,003	0,984±0,020	0,900±0,061
	FP RATE	0,053±0,008	0,002±0,002	0,001±0,001
AdaBoost	PRECISION	0,973±0,019	0,172±0,344	1,000±0,000
	TP RATE	0,993±0,014	0,250±0,500	0,841±0,063
	FP RATE	0,448±0,287	0,007±0,014	0,000±0,000
K-NN	PRECISION	0,997±0,002	0,912±0,084	0,922±0,042
	TP RATE	0,996±0,002	0,943±0,064	0,906±0,064
	FP RATE	0,071±0,058	0,002±0,001	0,002±0,001



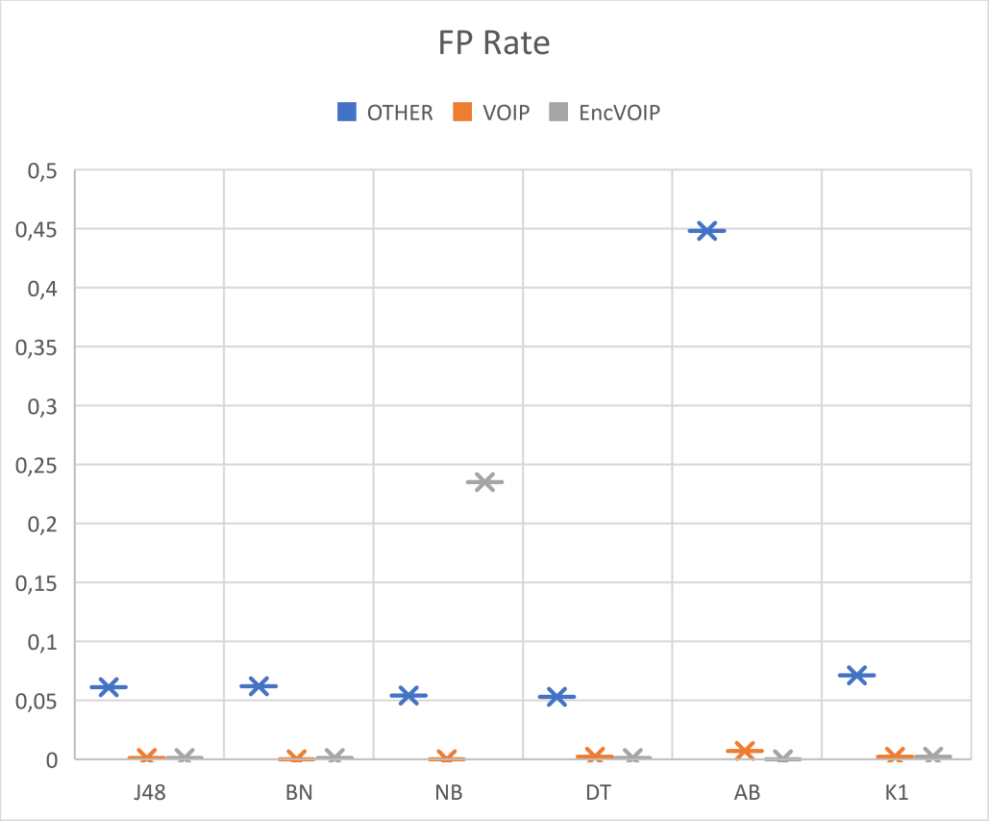
Слика 6: Резултати од класификацијата



Слика 7: Прецизност на алгоритмите



Слика 8: Вистински позитивната стапка (TP Rate)



Слика 9: Лажно позитивната стапка (FP Rate)

Кога се споредуваат резултатите за енкриптиран VoIP и класичен VoiP сообраќај, може да се види дека Decision Tree и Bayes Net алгоритмите покажуваат најдобри резултати, со најголема прецизност, висока стапка на TP и ниска стапка на FP, а по нив следат J48 и K-Nearest Neighbour алгоритмите. Перформансите на Naive Bayes и AdaBoost не се толку добри, особено во лажно позитивната стапка што ни покажува дека тие алгоритми го класифицираат другиот сообраќај како VoIP и EncVoIP.

Резултатите покажуваат дека Bayes Net има најголема вкупна прецизност, 1,35% повисока од J48 и 1,65% повисока од Decision Tree ML Algorithm. Но, во исто време Decision Tree има 0,24% подобра TP стапка од Bayes Net и 0,73% подобра од J48. Уште поважно, Decision Tree има најниска стапка на FP, која е за 1,54% пониска од Bayes Net и J48.

AdaBoost има најлоша FP стапка со 87,7% повисока вредност од Decision Tree. Naive Bayes има 51,2% повисока стапка на FP од Decision Tree.

Алгоритамот K-Nearest Neighbor е во средината со 4,78% помала прецизност, 1,25% пониска TP стапка и 4,2% повисока FP стапка од Decision Tree.

Процентите се пресметани на средните вредности на прецизноста, TP Rate и FP Rate од трите истражени класи.

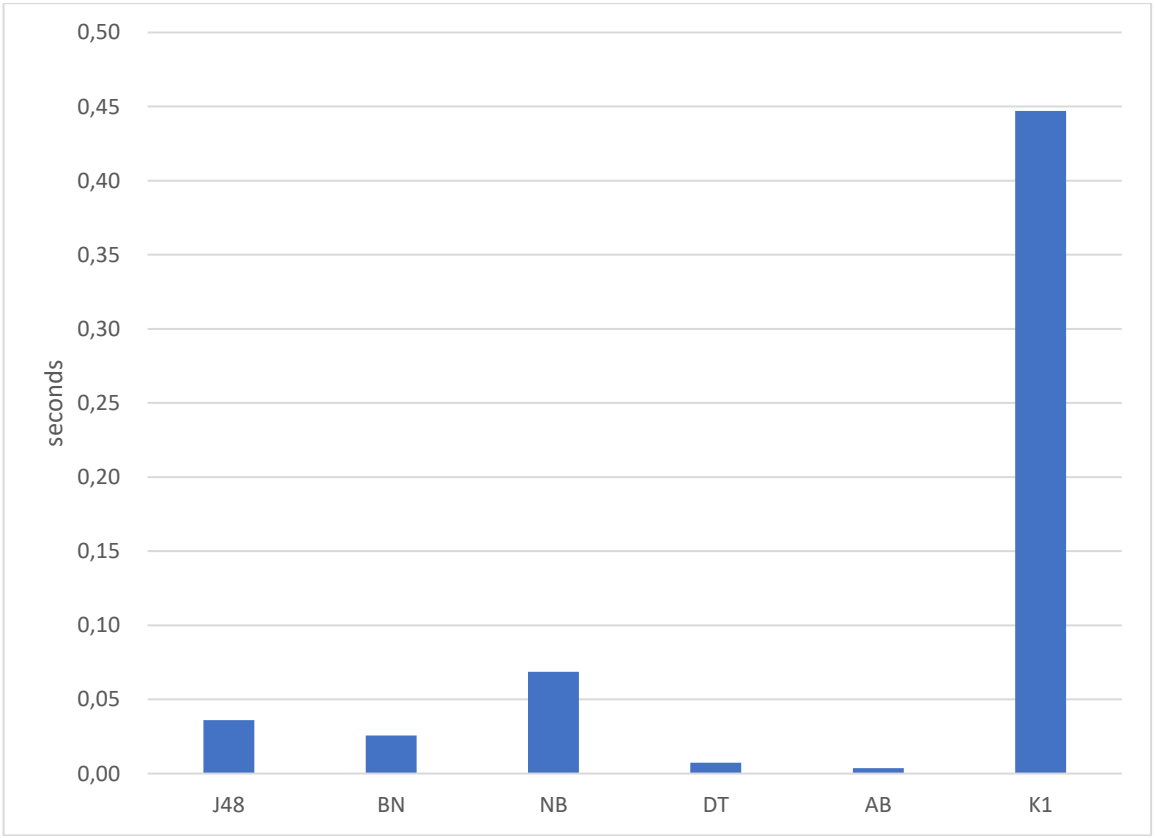
Втората карактеристика што е важна за вкупната ефикасност на алгоритмите е временскиот интервал потребен за алгоритмите да ја извршат класификацијата. Комбинираните две вредности, прецизноста и временската брзина за класификација, ќе ја дадат целата слика потребна за евалуација на ефикасноста на алгоритмите. Времето во нашиот случај е релативно на нашето експериментално опкружување, но споредбата е релевантна, бидејќи сите експерименти и мерења се направени во истата експериментална околина и истите податочни множества се користени за тренирање и тестирање на секој алгоритам. Користењето на побрзи или повеќе машини за класификација, може значително да го забрза времето потребно за евалуација, но соодносот за споредба меѓу алгоритмите се очекува да остане ист. Поради ова „трошење ресурси“ на алгоритмите, времето потребно за класификација е исклучително важно за одредување на ефикасноста.

Табела 3 покажува дека алгоритамот AdaBoost е најбрз, и одзема само 0,8% од времето кое го троши K-NearestNeighbour за класификација кој се покажува како најспор.

Поради слабите перформанси на класификација кои ги има AdaBoost, вториот најбрз алгоритам - Decision Tree има најдобра вкупна ефикасност за класифицирање на шифриран и нешифриран VoIP сообраќај во околина базирана на NFV, одземајќи само 1,66% од времето потребно на K-NN. По него следуваат Bayes Net како и J48 кои исто така имаат добро просечно време потребно за извршување на класификацијата. Бидејќи овие два алгоритма исто така добро функционираат во рамките на класификацијата, нивната вкупна изведба е задоволителна. Ова е визуелно интерпретирано на Слика 10.

ТАБЕЛА 3: ПРОСЕЧНО ПОТРОШЕНО ВРЕМЕ ЗА КЛАСИФИКАЦИЈА

ALGORITHM	AVERAGE TIME IN SECONDS
J48	0,036
BAYESNET	0,026
NAIVE BAYES	0,069
DECISION TREE	0,007
ADABOOST	0,004
K-NN	0,447



Слика 10: Просечно потрошено време за класификација

Алгоритамот K-NearestNeighbour има добри перформанси за класификација, но времето потребно за класификација е многу големо. Треба да споменеме дека резултатите прикажани овде се со користење k=1 најблизок сосед, но експериментите со повеќе (2 и 3) најблиски соседи покажале слични перформанси во експериментите во други трудови [82][83].

Naive Bayes покажа слаби перформанси на класификација и споредбено со другите алгоритми и подолго време потребно за класификацијата.

Во контекст на строгите барања на 5G за ниска латентност, поблиското набљудување на резултатите покажува дека на KNN и Naive Bayes им треба повеќе време за класификација отколку на останатите ML алгоритми кои ги разгледуваме. AdaBoost работи лошо во однос на лажно позитивните примери, додека другите имаат задоволителни перформанси за класификација, додека брзината е одлучувачки елемент за нивната употреба во 5G сценарио.

3.4.Заклучоци околу класификацијата на VoIP сообраќај во околина базирана на NFV архитектура

Во глава 3 се врши споредба на ефикасноста во класифицирањето на VoIP и шифрирани VoIP сообраќај, на шест различни надгледувани алгоритми за машинско учење, во ситуација кога мрежниот сообраќај тече во виртуелизирана средина која е поставена врз NFV архитектура. Ова сценарио има две главни цели:

1. пресретнување на мрежниот сообраќај внатре во виртуелниот слој, без потреба од воведување дополнителни надворешни мрежни сонди или SDN елементи кои би го конвертирале сообраќајот исток-запад, во сообраќај север-југ;

2. класификација на мрежниот сообраќај, со акцент на VoIP со минимална потрошувачка на ресурси, за целиот процес да не придонесе на зголемување на латентноста на пакетите.

Поради ова, ја дефинираме ефикасноста на алгоритмите како оптимална рамнотежа помеѓу перформансите за класификацијата и времето потрошено за истата. Ја

изградивме нашата експериментална средина и спроведовме повеќе тестови, генерирајќи различни групи на мрежен сообраќај, од кои ги извадивме мрежните текови на податоци. Најрелевантните статистички карактеристики на тековите, беа избрани како атрибути на податочните множества. Изворните и одредишните IP-адреси и MAC адресите, како и комуникациските порти не беа земени предвид бидејќи тие не се релевантни во виртуелизирано сценарио во кое се применува шифрирање.

Резултатите откриваат дека Decision Tree и Bayes Net алгоритмите имаат најдобра ефикасност, со J48 веднаш зад нив. K-NN (со k=1) покажа добри резултати во класификација, но потроши повеќе време за изведување на класификацијата. Naïve Bayes и AdaBoost имаат добри брзини на класификација, но имаат големи лажно позитивни стапки при класификации за VoIP сообраќајот.

3.5.Придобивки и практична примена

Придобивките од оваа анализа се во можностите за нејзината практична употреба во системи кои работат во високо виртуелизирани околини (јавни или приватни платформи во облак), каде NFV архитектурата е составен дел од решението. 5G мрежите се градат на вакви платформи и услугите кои се нудат преку 5G мрежите се високо зависни од оптимална класификација на мрежниот сообраќај. Ефикасна класификација на VoIP сообраќај, регуларен и енкриптиран, е неопходна за овозможување QoS, безбедност на податоците, управување со мрежи и апликации, следење и контрола на мрежите.

4. Класификација на мрежен сообраќај во околина базирана на NFV архитектура

Во претходната глава беше извршена експериментална класификација на енкриптиран и неенкриптиран VoIP сообраќај, користејќи надгледувани ML алгоритми. Создадовме уникатна средина за тестирање која што наликува на процесите во пракса и го симулира сообраќајот исток-запад, во виртуелната рамнина меѓу виртуелните мрежни функции, кои формираат сервисна низа во рамките на NFV. Ова претставува иновативно сценарио кое може да се искористи за споредба со нововоспоставените мрежни архитектури при имплементација на мрежите од петта генерација.

Во овој дел ќе извршиме проширување на истражувањето, преку зголемување на бројот на класи на мрежен сообраќај кои ги класифицираме. Повторно ги користиме шесте алгоритми за надгледувано машинско учење и ја споредуваме нивната ефикасност при класификацијата.

Класификацијата е направена врз основа на 6 класи, кои се избрани по искуство од традиционалните мрежи и во контекст на очекуваниот мрежен сообраќај во рамките на 5G радио, како и 5G core мрежата. Избравме 6 класи: VoIP, шифриран VoIP (EncVOIP), DNS, Управувачки (Management), SSH, HTTP и HTTPS сообраќај. NFV архитекурата станува вистински овозможувач на 5G, обезбедувајќи можност за иницијално поставување на мрежните елементи, па постепено агилно зголемување на мрежното оптоварување, истовремено насочувајќи голем дел од пресметувачките капацитети кон мрежниот раб. Со тоа се обезбедува потребниот фундамент за непречено зголемување на густината на крајни корисници, особено од делот на IoT, што се очекува со пенетрацијата на 5G. Главната цел на истражувањето е да ги испитаме и експериментално да ги потврдиме можностите на надгледуваните ML алгоритми за класификација на мрежниот сообраќај, користејќи ги најчесто употребуваните класи на сообраќај, истовремено потврдувајќи ја можноста за нивно користење кај модерните системи, кои се високо виртуелизирани.

Слично како во претходната глава, ефикасноста на алгоритмите ја дефинираме како оптимална рамнотежа помеѓу прецизноста на алгоритамот и времето потребно за вршење на класификацијата. Покрај прецизноста, брзината на ML алгоритамот во многу случаи е уште поважна. Ако времето потрошено за класифицирање на податоците додава

значително доцнење во мрежниот сообраќај и ги троши ресурсите (циклуси на процесорот, меморијата, читањето/запишувањето на тврдите дискови), прецизноста на класификацијата ја губи својата релевантност.

4.1.Поврзана работа и дискусија

Иако претходно фокусот на истражување беше на VoIP сообраќајот, кој е основа на гласовните услуги кај 5G мрежите, останатите типови на сообраќај имаат голема улога во се поголемото портфолио на сервиси кои се користат кај модерните IP мрежи. Дел од авторите се насочуваат кон испитување на мрежната безбедност, со посебен акцент на еден од најраспространетите сајбер напади – откупнината (ransomware) [84]. Други автори се фокусираат на поединечни типови на сообраќај, како на пример мултимедија сообраќајот кој зазема огромен процент од интернет сообраќајот [85].

Авторите на [84] предлагаааат современ метод за класификација на ransomware генериран сообраќај во реално време, користејќи методи на длабоко учење. Го анализираат сообраќајот, фокусирајќи се на еден од најчесто користените злонамерни софтвери: Crypto Wall, по што предлагаат модел за негова класификација. Во оваа дисертација исто така се врши класификација, на 6 различни типови на сообраќај, но со посебен акцент на поедини типови на мрежна архитектура кои се користат во пракса. Слично на овој случај и во нашето истражување се користат исклучиво статистичките карактеристики на сообраќајот.

Женг Ву и сор. [85] се насочени кон мултимедијалниот сообраќај на интернет, со цел да се обезбеди соодветен QoS за таквиот сообраќај и да се овозможи непречено мултимедијално искуство. Предлагаат нова шема CHS (chain hierarchical structure) која врши карактеризација на дистрибуцијата на класите, кои најчесто не се балансирани во рамките на мрежата. Со градење на модел на грешка, се пресметува ширењето на грешката генерирана од CHS и se анализираат факторите кои влијаат на тоа. Уште поважно, два клучни методи кои вклучуваат рангирање на класификаторите и комбинација со хиерархиската структура се осмислени за да се ублажи ширењето на грешките произведени од класификаторот. Ефективноста на развиената рамка ја потврдуваат преку експерименти, преку две множества на податоци за сообраќај од реалниот свет: во

стационарни и нестационарни средини. Експерименталните резултати покажуваат дека предложените методи се ефикасни во однос на точноста на класификацијата и времето на работа. Доколку овој пристап го споредиме со нашиот, највпечатлива сличност е пристапот кон ефикасноста на класификацијата како сплет на прецизноста и времето потребно за класификација. И овде се работи со енкриптиран и неенкриптиран сообраќај, но пристапот кој го користиме со ML алгоритми и тестирањето на најчестите видови на сообраќај е дистинкцијата на нашата работа.

Во [86] се користи мрежна архитектура која е многу слична на нашата и која во основа е изградена на SDN елементи поврзани во сервисна низа. Но, овој случај има за цел да ја оптимизира потрошувачката на енергија, во опкружување на софтверски дефинирани мрежи во податочни центри (DC-Data Center). Истражувачите развиваат нова стратегија за рутирање која може да балансира помеѓу потрошувачката на енергија и квалитетот на услугата за дојдовните сообраќајни текови. Демонстрираат како класификација на тековите на мрежниот сообраќај може да има влијание на потрошувашкаа на екектрична енергија, и истовремено ефикасно да се гарантира квалитетот на услугата на секоја класа на проток. Ова се постигнува со креирање на податочно множество кое опфаќа различни видови мрежен сообраќај како видео, VoIP, игри и ICMP. Се споредуваат перформансите на голем број техники за машинско учење и се известуваат резултатите. Принципот на разгледување на мрежни текови, наместо индивидуални пакети е ист и во нашето истражување. Класите на сообраќај се различни, како и целта, но принципите на работа се слични. Резултатите од овој труд и нашите се споделиви и се движат помеѓу 77% и 99% прецизност, во зависност од избраниот алгоритам и класа.

Трудот [87] има за цел да користи алгоритми за машинско учење при класификацијата на мрежниот сообраќај во рамките на едноставна SDN инфраструктура и да ги спореди нивните перформанси. Сообраќајот се генерира со помош на алатката „D-ITG“ која ја користиме и ние во нашето истражување. Податоците за сообраќајот се зачувуваат со помош на скрипта за обработка и потоа се користат за обука и тестирање на користените модели за машинско учење. Сообраќајот се лабелира врз основа на групите генерирани од моделот без надзор, а резултатите се користат надгледуван модел со цел да се најдат најдобрите перформанси. Пристапот резултира со просечна точност од 83,5 проценти. Во нашето истражување, лабелирањето на множеството за тестирање се врши

мануелно, што доведува до делумно подобри резултати во класификацијата и има за цел да го пронајде најдобриот надгледуван ML алгоритам за класификација. Моделот кој го предлагаат авторите на [87] има практична примена во случаи каде нема можност од претходно учење на сообраќајот или карактеристиките на истиот се менуваат често.

Во [88], класификација на мулти-сервисен интернет сообраќај, базирана на ML алгоритми, се користи за да се оцени потрошувачката на процесирачки и машински ресурси (процесорското време и користењето на системската меморија). Ние го надополнуваме ова истражување, бидејќи го проценуваме времето кое им е потребно на ML алгоритмите за извршување на класификацијата.

Мохамед Реза Парсаи и сор. [89] користат SDN за да го категоризираат сообраќајот по апликација, со примена на различни варијанти на проценител на невронска мрежа (Neural Network estimator). Тие користат техники за ископување податоци засновани на различни ML алгоритми и предлагаат контролер кој би можел динамично да распределува пропусност на мрежните текови и да ја оптимизира распределбата на ресурсите. Тие постигнуваат точност на класификација од над 97%. За разлика од нашата работа, тие користат IP-адреси на изворот и одредиштето, како и портот на транспортниот слој за класификација.

Во [90], QoS во мрежа базирана на SDN се истражува со акцент на надминување на ограничувањата на традиционалните мрежни архитектури. Се категоризираат различни механизми за рутирање на мрежниот проток. Во нашата работа, ние ја истражуваме класификацијата како основен концепт од кој QoS може значително да има корист.

Од претходно претставеното, може да се заклучи дека истражувањето на класификацијата на мрежните текови е обемно и разновидно, како од аспект на техниките кои се користат, така и од аспект на целите за се врши класификацијата. Нашата цел е да го приближиме моделот на класификација кон најчесто користените мрежни архитектури, посебно во телекомуникацискиот сектор и експериментално да ја потврдиме корисната вредност на надгледуваните ML алгоритми во обезбедувањето на таа класификација.

4.2.Одредување на карактеристики на мрежниот сообраќај

И во овој случај беше користена истата експериментална околина опишана во 3.2. Истите податочни множества од изведените 50 експериментални итерации се користат за формирање на мрежните текови користејќи го Argus. Пристапот на поделба на експерименталните множества во сооднос 1/3 наспроти 2/3, со цел да се тренираат алгоритмите и да се направат тестирањата беше идентичен со претходно. За тренирање и тестирање на податоците беше искористена Weka, секако овој пат имајќи ги во предвид шесте избрани класи на мрежен сообраќај. Атрибутите на мрежните текови од Табела 1 секако се идентични и при ова тестирање, со користење на процес на рангирање на атрибутите согласно релевантноста на информацијата што ја носат за изведување на класификацијата. Овој метод овозможува да не настане истекување на податоци (data leakage) преку формирање на моделот на соодветниот ML алгоритам преку карактеристики кои не се валидни. Како што беше и претходно истакнато, беше користен AttributeSelectedClassifier со Ranker како алгоритам за рангирање на карактеристиките и InfoGainAttributeEval како функција на Weka, за одредување на тежината на информацијата на секој атрибут.

Како што ќе се покаже во резултатите, прецизноста на класификацијата беше пресметана во целина, за сите класи, но и за секоја класа независно, со цел да се пресметаат микропросечната прецизност и макропросечната прецизност. Ова е исклучително битно, бидејќи не секоја класа на мрежен сообраќај е подеднакво застапена, па доколку се разгледува прецизноста на алгоритамот како целина, најзастапената класа ќе придонесува најмногу во конечниот резултат.

4.3.Анализа на експерименталните резултати

Бројот на вистинска позитивни (TP), лажно позитивни (FP), вистински негативни (TN) и лажно негативни (FN) класификации се дефинирани идентично како во 3.3. Повторно ги одредуваме прецизноста на алгоритмите (Precision), вистински позитивната стапка (TP Rate) и лажно позитивната стапка (FP Rate) согласно равенките (1), (2) и (3).

Табела 4 ја покажува просечната прецизност на алгоритмите во сите 50 експерименти со статистичкото стандардно отстапување низ експериментите.

Може да се види дека Decision Tree алгоритамот има најдобра прецизност. По него следат J48 и BayesNet. Од друга страна, алгоритамот AdaBoost има најлоши вкупни перформанси со најмала прецизност од 74,4%.

ТАБЕЛА 4: ПРЕЦИЗНОСТ НА АЛГОРИТМИТЕ

No.	ML Algorithm	Precision
1	AdaBoost	0.744±0.0292
2	BayesNet	0.9672±0.0189
3	J48	0.9906±0.0027
4	KNN	0.9172±0.0438
5	NaiveBayes	0.8634±0.0170
6	**Decision Tree**	**0.9914±0.0033**

За понатамошно истражување на прецизноста, ја пресметавме микропросечната прецизност, која го собира придонесот на сите класи и ја пресметува просечната метрика, како што е дадено во равенката 4. Резултатите се претставени во Табела 5.

$$Precision\_MIC = \frac{(TP1 + TP2 + \cdots + TPN)}{(TP1 + FP1 + TP2 + FP2 + \cdots + TPN + FPN)} \quad (4)$$

ТАБЕЛА 5: МИКРОПРОСЕЧНА ПРЕЦИЗНОСТ НА АЛГОРИТМИТЕ

No.	ML Algorithm	Micro Average Precision
1	AdaBoost	0.8450±0.0176
2	BayesNet	0.9954±0.0027
3	**J48**	**0.9984±0.0006**
4	KNN	0.9856±0.0073
5	NaiveBayes	0.9752±0.0027
6	**Decision Tree**	**0.9984±0.0010**

Покрај микропросечната прецизност (micro average precision), поради дисбалансот на дистрибуцијата на класите низ податочните сетови, а со цел да извлечеме валидни заклучоци, ги пресметуваме и макропросечната прецизност (macro average precision), сензитивноста (recall) и *F-1* скорот.

Макропросечната прецизност е средна вредност од прецизностите на секоја класа. Ова значи дека секоја класа ќе тежи исто во макропросечната прецизност. Следната равенка се користи за пресметување на макро просечната прецизност (*Precision_MAC*), каде што *Pr1, Pr2* итн, ја означуваат прецизноста на алгоритамот во однос на поединечните класи.

$$Precision\_MAC = \frac{Pr1 + Pr2 + \cdots PrN}{Count(Pr)} \quad (5)$$

Резултатите за макропросечната прецизност се прикажани во Табела 6. Во оваа табела е дадено и статистичкото стандардно отстапување на резултатите за секоја од класите.

Ако ја оцениме Табела 6, станува јасно дека алгоритмите не работат исто за сите класи. Decision Tree алгоритамот е најконстантен, со најголема макропросечна прецизност и најниско стандардно отстапување помеѓу класите, што покажува дека ги класифицира сите класи со слична прецизност. J48 е многу блиску до Decision Tree, со над 98% прецизност. Наспроти нив, алгоритамот AdaBoost покажува многу ниска макропросечна прецизност со високо стандардно отстапување, што значи дека работи лошо на различни класи. Алгоритамот K-Nearest Neighbours исто така слабо функционира, со малку над 82% макро просечна прецизност. Кога ќе ги споредиме овие резултати со оние во Табела 4, можеме да видиме дека алгоритмите имаат ист ред, но макропрецизноста на алгоритмите од долниот крај е полоша, извлекувајќи заклучок дека AdaBoost и KNN имаат различна прецизност за различни класи.

ТАБЕЛА 6: МАКРОПРОСЕЧНА ПРЕЦИЗНОСТ НА АЛГОРИТМИТЕ

No.	ML Algorithm	Macro Average Precision
1	AdaBoost	0.20335±0.3064
2	BayesNet	0.8899±0.1489
3	J48	0.9824±0.0148
4	KNN	0.82735±0.2202
5	NaiveBayes	0.78915±0.2048
6	**Decision Tree**	**0.9848±0.0107**

Макропросечната прецизност дава средна вредност од прецизностите за класификација на секоја од класите. За разлика од неа микропросечната прецизност го агрегира придонесот на сите класи за да ја пресмета средната метрика. Доколку прецизноста на секоја класа ни е подеднакво битна, макропросечната прецизност го дава соодветниот одговор за алгоритамот како целина. Но, доколку некоја од класите е многу повеќе застапена од другите класи микропросечната прецизност е подобриот начин за одредување на прецизноста на алгоритамот како целина.

За да се оцени влијанието на лажно негативните класифицирани примери, се користи Recall (или поинаку наречен: сензитивност). Тоа е пропорцијата на вистински позитивно класифицираните инстанци и вкупните вистински инстанци:

$$Recall = TP/(TP + FN) \quad (6)$$

Го користевме Recall за да го пресметаме *F1* скорот на надгледуваните ML алгоритми во нашите експерименти. Тоа е метрика која балансира помеѓу прецизноста и сензитивноста, така што се земаат предвид лажните негативни примери. *F1-скорот* се пресметува како хармонична средна вредност помеѓу прецизноста и сензитивноста:

$$F1 - Score = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall} \quad (7)$$

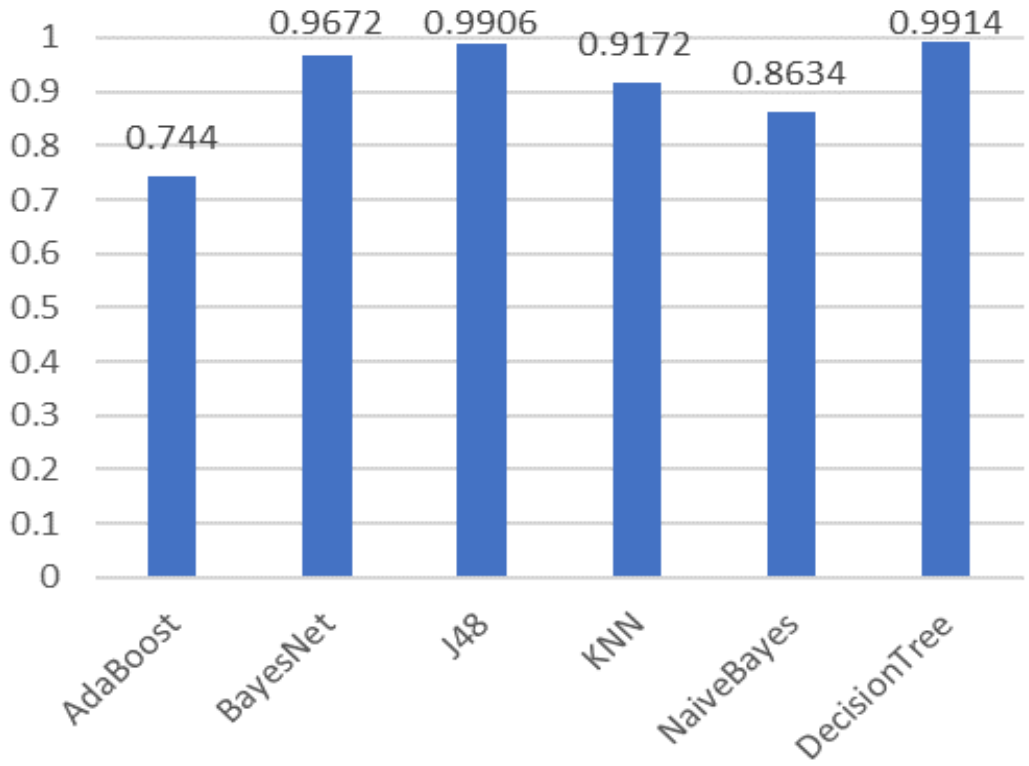
Табела 7 ги прикажува вредностите на F1 скорот пресметани за нашите експерименти.

ТАБЕЛА 7: F1-SCORE

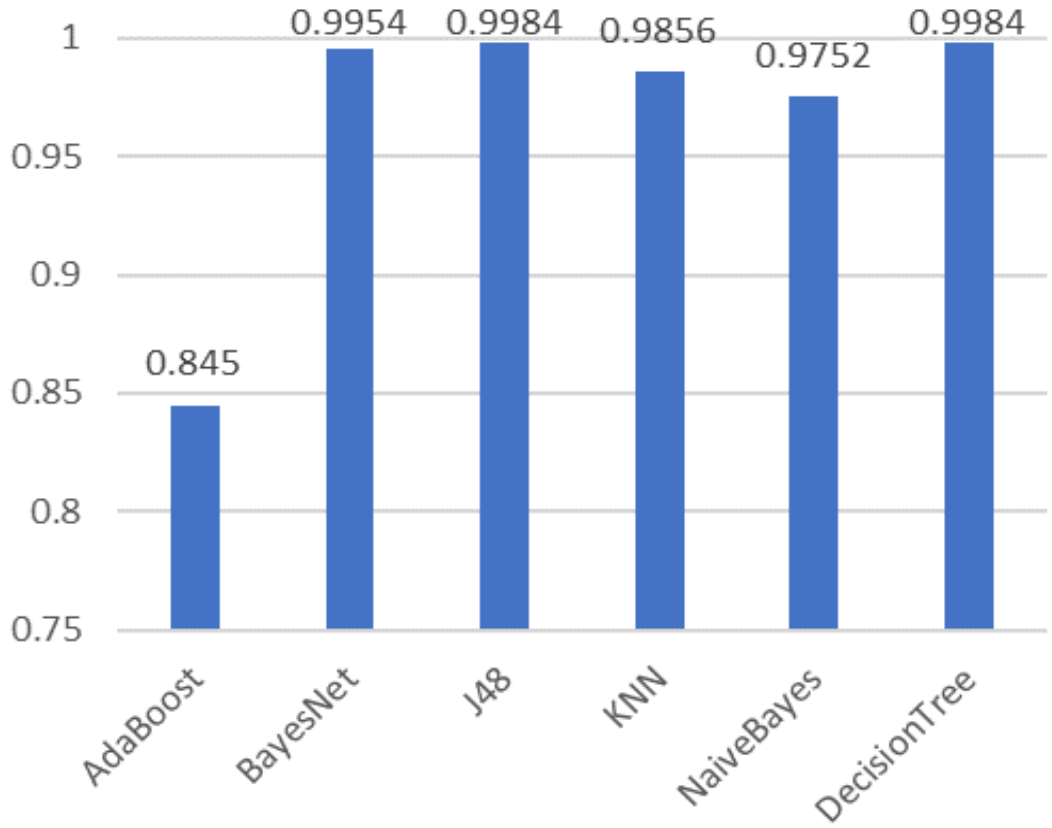
No.	ML Algorithm	F1-score
1	AdaBoost	0.231575±0.3356
2	BayesNet	0.913425±0.1055
3	J48	0.975425±0.0212
4	KNN	0.797425±0.2295
5	NaiveBayes	0.782125±0.1510
6	**Decision Tree**	**0.980475±0.0152**

Decision Tree алгоритамот има најдобар *F1-скор*, следен со J48, BayesNet, KNN, NaiveBayes и AdaBoost. Последниот има *F1-скор* од само 23,2% со многу високо стандардно отстапување.

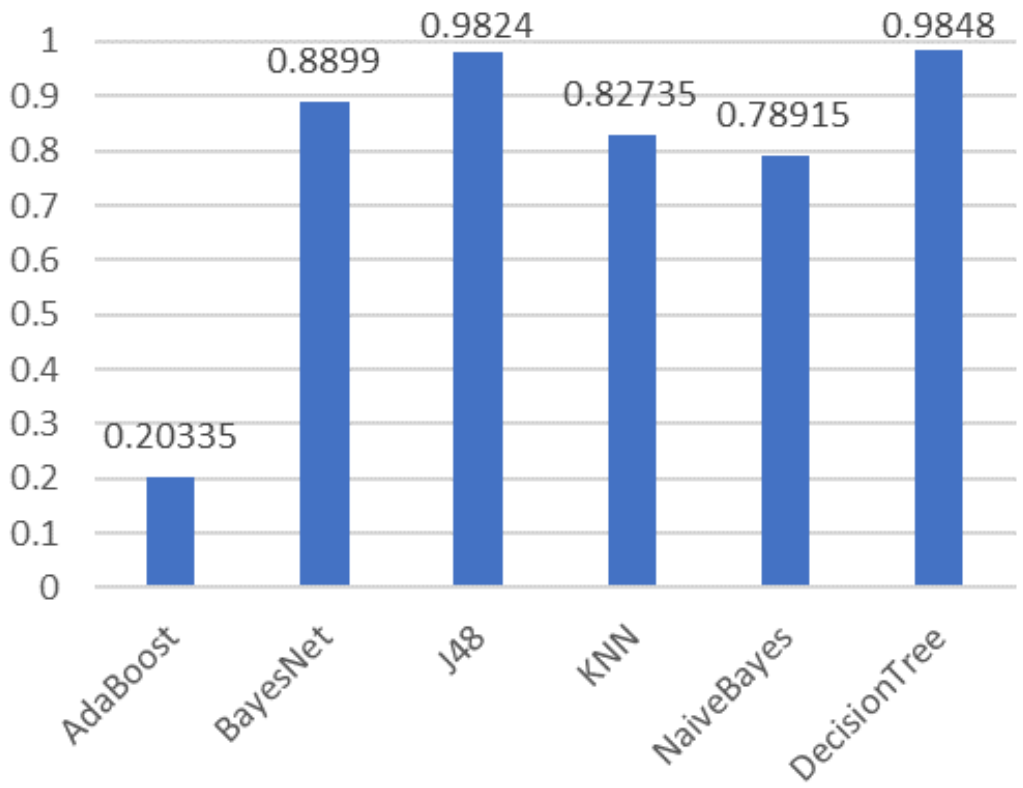
Табелите се визуелно претставени на сликите од 11 до 14.



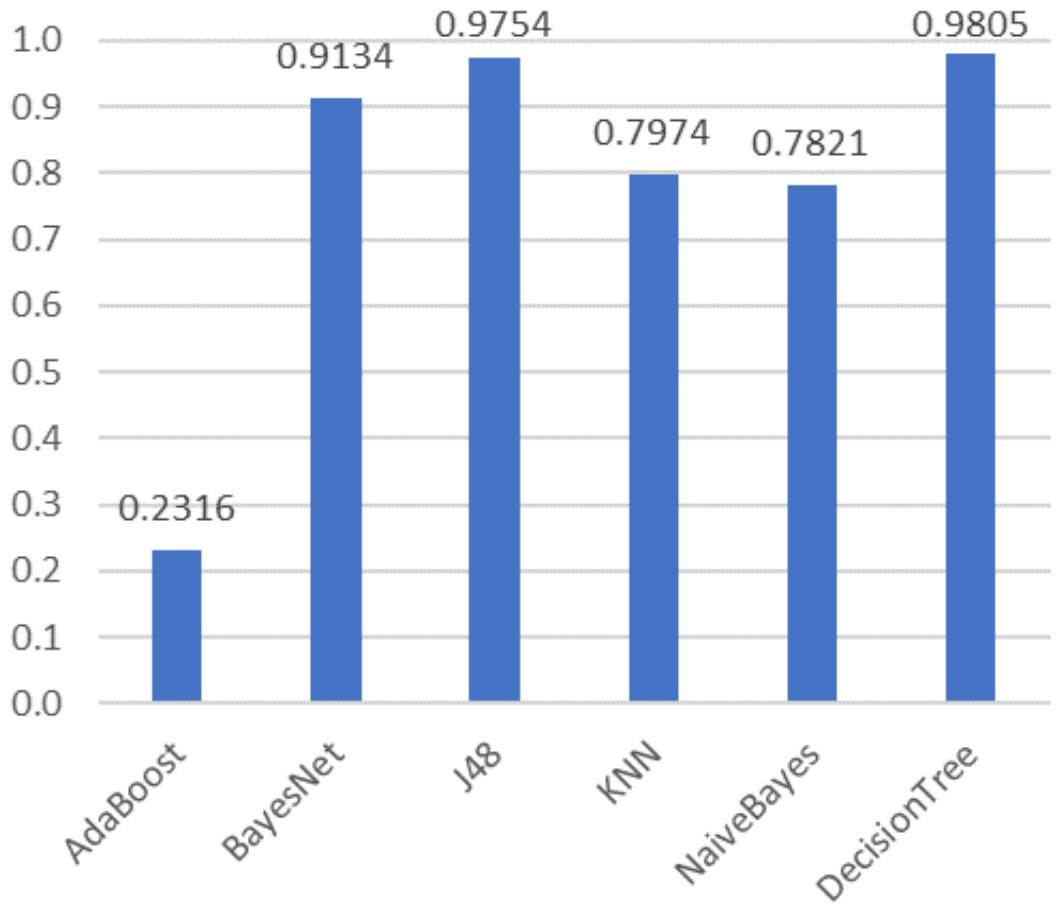
Слика 11: Прецизност на алгоритмите



Слика 12: Микропросечна прецизност на алгоритмите



Слика 13: Макропросечна прецизност на алгоритмите



Слика 14: F-1 score

Покрај прецизноста на алгоритмите и во овој случај се фокусираме и на времето кое алгоритмите го трошат за вршење на самата класификација. Пресретнувањето на мрежниот сообраќај со цел да се изврши класификација, која би се користела за било каква цел, би додало латенција во мрежата. Од оваа причина и во овој случај од голема важност е да го пресметаме времето кое секој од наведените алгоритми го троши за класификација. Најефикасен алгоритам е оној кој има оптимален сооднос помеѓу прецизноста и времето потребно за класификација.

И овде напоменуваме дека времето кое го мериме е релативно на околината во која се изведуваат експериментите. Доколку се корисни помоќна околина, времињата би биле покуси, но бидејќи за сите алгоритми се користи идентична околина, соодносот на времињата останува ист. Просечното време го пресметуваме како средна вредност од времињата за класификација од секоја итерација.

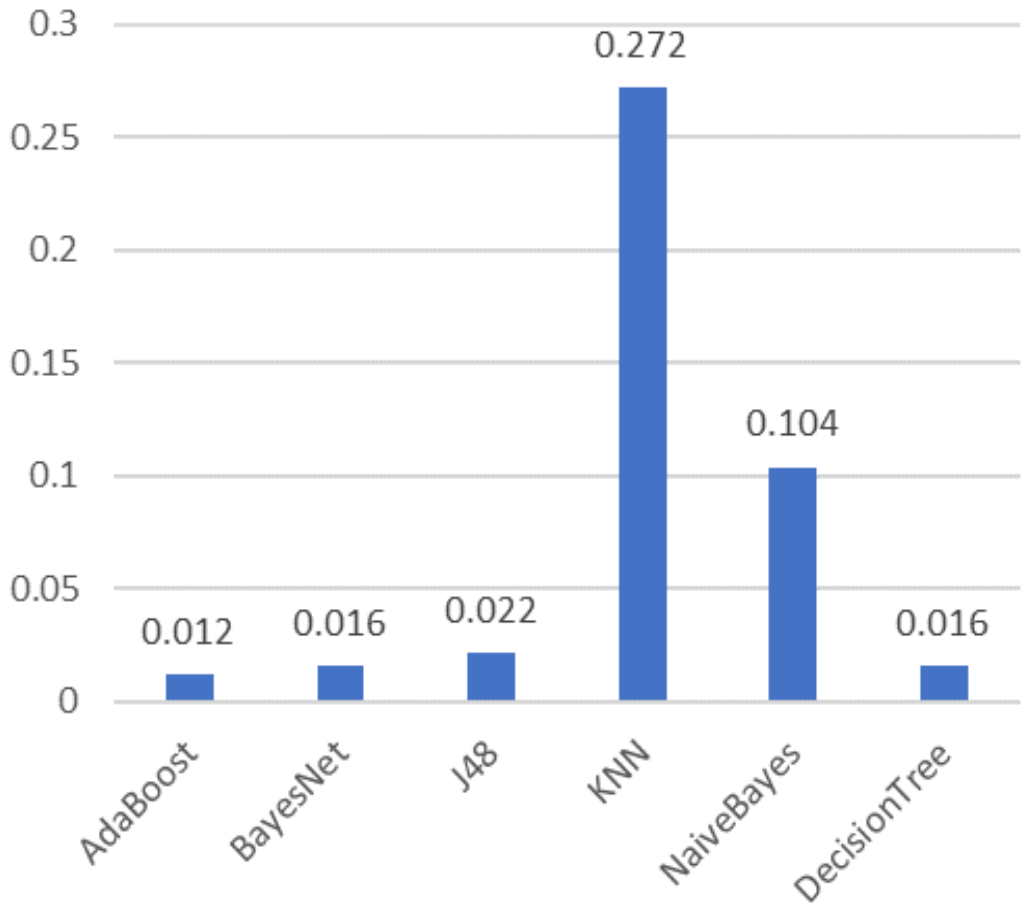
Во Табела 8 се дадени просечните времиња од изведените експериментални итерации кои беа потребни за секој од алгоритмите да ја изведе класификацијата.

ТАБЕЛА 8: ПРОСЕЧНО ПОТРЕБНО ВРЕМЕ ЗА КЛАСИФИКАЦИЈА (ВО СЕКУНДИ)

No.	ML Algorithm	Average time in seconds
1	**AdaBoost**	**0.012**
2	BayesNet	0.016
3	J48	0.022
4	KNN	0.272
5	NaiveBayes	0.104
6	Decision Tree	0.016

Резултатите за просечното време потребно за класификација покажуваат дека алгоритамот AdaBoost најдобро функционира, со најголема брзина. Decision Tree и BayesNet го делат второто и третото место и се за околу 25% побавни од AdaBoost. J48 има задоволителна брзина. NaiveBayes е скоро 9 пати побавен од AdaBoost и повеќе од 6 пати побавен од Decision Tree. KNN алгоритамот е најбавен. Decision Tree и AdaBoost трошат само 5,9% од времето потребно на KNN за извршување на класификацијата.

Слика 15 графички го прикажува просечното време потрошено од алгоритмите.



Слика 15: Време кое алгоритмите го трошат за класификација (во секунди)

Да резимираме, кога ќе ги погледнеме и прецизноста и времето потребно за класификација, Decision Tree алгоритамот има најдобри вкупни перформанси. Иако AdaBoost е најбрзиот алгоритам, прецизноста на класификацијата е слаба и нестабилна во различни класи, што го прави овој алгоритам несигурен за нашето сценарио. J48 има висока прецизност која е рамномерно распоредена меѓу класите, но е побавен од Decision Tree и BayesNet. Сепак, неговата брзина е споредлива со Decision Tree и BayesNet, што исто така го прави валиден избор како класификатор на мрежен сообраќај. BayesNet има висока прецизност, но макропросечната прецизност и F1-резултатот покажуваат дека прецизната дистрибуција меѓу класите не е толку добра како Decision Tree и J48.

NaiveBayes е во средината и од поглед на прецизност и од временска перспектива, додека алгоритамот KNN има околу 83% макропросечна прецизност и 80% F1-резултат, но тој е убедливо најбавниот алгоритам што го прави корисен само во случаи кога времето потребно за класификација има мала важност.

4.4.Заклучоци околу класификацијата на различни типови на сообраќај во околина базирана на NFV архитектура

Главната цел и идеја на оваа глава е да претставиме метод за креирање податочни множества базирани само на статистичките карактеристики на мрежните текови на сообраќај, а потоа да ги тестираме перформансите за класификација на мрежниот сообраќај кај однапред дефинирани класи, на алгоритмите за машинско учење, врз основа на креираните збирки на податоци. Сето ова е направено во експериментална околина која е креирана на основа на парадигмите за NFV архитектура.

Ефикасноста на алгоритмите се истражува од аспект на прецизност на алгоритмите, но исто така и од аспект на потрошено време за извршување на класификацијата. Ова е важно од гледна точка на виртуелизација, каде што сценарија на мрежа изградена во облак или во мешана локална и инфраструктура во облак се вообичаена практика. Тука исто така треба да се нагласи и класификацијата кај 5G мрежите, кои во најголем дел се градат користејќи NFV архитектура и каде што латентноста на мрежата е од голема важност.

При експериментирањето се вршат повеќе итерации на мерење и секоја итерација се користи за собирање податоци за мрежниот сообраќај од кој се извлекуваат IP мрежните текови. Како атрибути за класификација се користат статистичките карактеристики на тековите. Бидејќи атрибутите како што се изворната и одредишната IP и MAC адресата, како и комуникациските порти, може да се разликуваат во различни средини, тие не се земаат предвид. Поради проблеми со енкрипцијата и приватноста на податоците, носивоста (payload) на пакетите е исто така исклучена од податочните множества и не се користи за класификација.

Околината што ја користиме не воведува никаков вид мрежни сонди или засебни SDN елементи за извршување на собирањето податоци, така што сообраќајот исток-запад е целосно непроменет. Сообраќајот е целосно пресретнат во виртуелниот слој каде што природно се наоѓа. Ова, исто така, има влијание врз потрошувачката на ресурси, минимизирајќи ја дополнителната латентност што може да се додаде на мрежните пакети со пренасочување или репликација на портата што се користи во традиционалните DPI испитувања.

Резултатите покажаа дека Decision Tree алгоритамот има најдобри вкупни перформанси, и од гледна точка на прецизноста при класификацијата, и од гледна точка на потрошувачка на време. Се покажа како сигурен класификатор кој функционира рамномерно во различни класи. J48 и BayesNet исто така имаат добри перформанси, при што J48 има малку подобра прецизност, а BayesNet е побрз. K-Nearest Neighbour и NaiveBayes имаат просечна прецизност на класификација во опсег од околу 80%, но тие се бавни, особено KNN кој е скоро 20 пати побавен од Decision Tree и BayesNet. AdaBoost ги покажува најлошите перформанси со прецизност што многу варира меѓу различните класи, што може да се види од макропросечната прецизност и *F1* скорот.

4.5. Употребна вредност и идни испитувања

Анализите во оваа и претходната глава може да се користат во пракса во повеќе системи кои се изградени во виртуелни средини, без разлика дали се во облак, локални или мешани инфраструктури. Елементите на NFV сега се неизбежен дел од таквите инфраструктури. 5G мрежите се потпираат на овие типови системи, но исто така поврзувањето на различни мрежни средини, со иста или слична намена, ќе се направи преку 5G пристапната технологијата. Во вакви услови, за изведување на QoS, обезбедување на безбедноста на мрежата и апликациите кои работат во неа, управувањето со податоци, следењето и контролата на системите и процесите, зависат од валидна класификација на мрежниот сообраќај, која треба да биде прецизна и брза, без притоа да троши значителна количина на системски ресурси.

За идната работа планираме да го оцениме влијанието на бројот на класи врз резултатите од класификацијата и потрошувачката на време на надгледуваните ML алгоритми, со воведување на голем број класи или намалување на класите. Друг тек е да се прошири експерименталната тестна околина на повеќе хостови и дистрибуирани околини од географски аспект и да се оценат можностите за класификација и импактот што тоа ќе го има во овие дистрибуирани мрежи.

5. Аналитичко моделирање на дистрибуирана NFV архитектура и импактот што дистрибуцијата го прави на доцнењето на мрежните пакети

Дистрибуција на мрежите изградени врз NFV архитектура на повеќе географски локации и податочни центри е жешка тема во истражувачките и инженерските заедници. Во оваа глава, правиме аналитички модели за пресметување на времето на престој на мрежните пакети во три различни сценарија: класична NFV инфраструктура (NFVI), каде што сите NFV елементи се на иста локација, NFV инфраструктура со дистрибуирана податочна рамнина, а централизирана околина за управување и оркестрација (MANO) и целосно дистрибуирана NFV инфраструктура, каде секоја локација има своја податочна рамнина и MANO елементи. Аналитичките модели се тестираат и дискутираат преку симулации базирани на Matlab.

Ресурсите за пресметување и складирање треба да се донесат во непосредна близина до пристапните мрежи, со цел да се обезбеди сигурна, исплатлива и ниско латентна услуга. Концептот за виртуелизација на мрежни функции, ја дава потребната способност за мрежата да раст кон рабовите, преку соодветно дизајнирање на SDN сервисните елементи во сервисни низи на повеќе локации. Дистрибуцијата на NFV инфраструктурата го минимизира позадинскиот сообраќај, придвижувајќи ја обработката на податоци кон мрежниот раб, со што се подобрува корисничкото искуство. Со приближување на услугата во близина на потрошувачот, доцнењето во мрежата може да се задржи под 1ms, што го прави веродостоен случајот за употреба на оваа архитектура кај 5G мрежите.

Преку резултатите од симулацијата, го дискутираме влијанието кое го имаат промените на различни мрежни параметри врз времето на престој на пакетите и ги споредуваме инфраструктурните решенија, со цел да видиме како тие можат да се вклопат во практични услуги обезбедени во NFV околина. Нашето истражување за времето на престој на мрежните пакети е важно особено за 5G пристапната мрежа, што овозможува планирање и усогласување со потребната латентност на корисничката рамнина со 5G спецификациите. Ги симулираме моделите со MatLab и дискутираме за моделите на NFV инфраструктурата кои би овозможиле најдобро корисничко искуство и најмала мрежна латентност.

5.1.Поврзани испитувања

SDN и NFV концептите се широко истражувани во академската заедница, поради технолошките новитети кои ги овозможуваат и потенцијалот за развој на сите видови дигитални услуги. Со практичната имплементација на 5G пристапните технологии и перспективата што тие ја носат, развојот на компјутерските мрежи доби уште поголем фокус и од научната и од деловната заедница. Бидејќи полето е широко, истражувачите одат во различни насоки и различни делови од SDN и NFV концептите. За подобра читливост, поврзаната работа ја поделивме на три различни подсекции: трудови што истражуваат аналитички модели за SDN и NFV средини, трудови што ја истражуваат латентноста и трудови што ги истражуваат SDN и NFV технологиите кај 5G мрежите.

5.1.1. Аналитички модели за SDN и NFV средини

Јаршел и сор. [27] се меѓу пионерите во моделирањето на OpenFlow архитектурата. Контролерот и комутаторот ги моделираат како Марковиански сервери со M/M/1 модел на ред на чекање и M/M/1-S модел за повратната спрега. За поедноставување, тие го ограничуваат системот на еден контролер и еден комутатор. Вршат симулации на моделот за да го проценат времето на престој на пакетот во мрежата и веројатноста за загуба на пакети во таков систем. Слично на тоа, Жихао Шанг и сор. [38] анализираат како веројатноста за packet-in пораки влијае на перформансите на комутаторите и контролерите во OpenFlow SDN околина која се состои од еден контролер и повеќе комутатори. Комутаторите се моделирани како M/H2/1 редици, додека контролерот е моделиран како M/M/1 ред на чекање. Нивната анализа покажува дека постои деградација на перформансите во OpenFlow SDN мрежата која експоненцијално се зголемува со порастот OF packet-in пораки. Иако нашите модели користат Марковијански сервери со редови на чекање, ние истражуваме модерна околина базирана на SDN сервисни низи и NFV архитектура, со посебен акцент на дистрибуцијата на инфраструктурата.

Во делото на Прадос, Џонатан и сор. [37] акцентот е ставен на моделирање на низи од виртуелизирани мрежни функции (VNF) во податочниот слој. Тие користат аналитички модел базиран на мрежа на отворени редови на чекање каде VNF функциите се моделирани со G/G/m редови на чекање и вршат валидација на моделот преку симулација

за LTE виртуелизиран ентитет за управување со мобилност (LTE virtualized Mobility Management Entity) со трослојна архитектура. Во нашиот случај, ние се концентрираме на времето на престој на пакети предизвикано од мрежната архитектура во OF NFV средина, симулирајќи ги елементите со M/M/1 синџири во рамките на Џексонова мрежа.

Во работата на [92], предложен е аналитички модел за OF SDN систем заснован на M/M/1 редици. Формулирани се две различни сценарија, едно за да се истражи ограничувањето на контролерот во однос на бројот на OF комутатори со кои може да се справи, врз основа на брзината на проток и друго, да се истражи толеранцијата на OF комутаторите врз времето на престој на пакетите со цел да се одлучи кога да се префрли управувањето од еден на друг контролер, во сценарио со повеќе контролери.

Во [28] авторите размислуваат за SDN систем со еден контролер и податочна рамнина со повеќе јазли и еден комутатор во секој јазол. Слично на нашите модели, податочната рамнина е апроксимирана како отворена Џексонова мрежа каде контролерот е моделиран со M/M/1 ред на чекање. Потоа се вршат симулации за да се проценат клучните системски метрики, како што е просечното време што еден пакет го поминува во мрежата. Изведен е PDF (probability density function) и CDF (cumulative distribution function) за времето што пакетот го поминува на дадена патека од VNF елементи во OF SDN мрежата. Нашата работа исто така се заснова на модели апроксимирани како отворена Џексонова мрежа, но ги разгледуваме елементите на NFV инфраструктурата, вклучувајќи го и доцнењето предизвикано од VNF менаџерот кој е дел од NFV MANO. Исто така, ја разгледуваме дистрибуцијата не само на податочната рамнина, туку и на MANO, вклучувајќи го и доцнењето предизвикано од транспортната латентност воведена од врските помеѓу дистрибуираните средини.

5.1.2. Мрежна латенција во SDN и NFV средини

Авторите на [36] истражуваат методи за одржување на квалитетот на услугата и минимизирање на трошоците за обезбедување ресурси кај дистрибуирани SDN мрежи на повеќе географски локации. Тие предлагаат решение кое обезбедува балансирање на протокот (со гарантиран QoS) во проактивни операции на SDN контролерите, со цел да се оптимизира трошокот на ресурси при провизионирање на нови VNF елементи. Распределбата на контролерите се врши динамички, со цел да се одржат барањата за QoS, да се управува со ограничените достапни ресурси (или контролери) и да се минимизираат

оперативните трошоци. Секогаш кога ќе пристигне барање за проток до контролерот, тој одлучува каде барањето треба да се обработи, локално или на друг контролер кој може да ги задоволи барањата за QoS специфични за апликацијата. Контролерите се моделирани како M/M/1 редици. Нивната анализа покажува дека наместо да се распоредуваат повеќе ресурси во мрежата, подобро е да се распоредат контролери со висока стапка на услуга (или контролери кои имаат најниско време на одговор), за да се задоволат барањата за QoS. Во нашиот труд, вршиме анализа на времето на престој на пакети во различни NFV дистрибуирани средини, во однос на веројатноста за packet-in пораки, веројатноста за пакети до VNF менаџерот, бројот на контролери во системот и бројot на дистрибуирани локации.

Процесирањето кое се одвива на мрежните рабовите и можноста за workflow ориентирана сервисна функција, наспроти градењето на одделни сервисни низи, е разгледана во [93]. Предложено е динамичко минимално време на одговор на исто ниво (Dynamic Minimum Response Time considering Same Level - DMRT_SL) за ефикасно мапирање на workflow барањата при процесирањето на мрежниот раб, со цел да се постигне архитектура со ниска латентност.

Нова архитектура базирана на SDN-NFV е предложена во [94] која истражува шема за поврзување на повеќе кориснички уреди со користење на основна Wi-Fi мрежа. Решението покажува дека SDN-NFV архитектурата може успешно да се користи на мрежниот раб, кај крајниот корисник, со ефикасно непречено предавање, зголемувајќи ја веројатноста за испорака на пакети со минимални ефекти врз латентноста. Овој труд ја покажува разновидноста на користењето на NFV и потребата давателите на услуги да ги земат предвид дистрибуираните NFV средини што ги предлагаме и анализираме.

F.Meneses et al. [95] предлагаат рамка која користи мрежно раслојување (network slicing), овозможена од SDN и NFV, за да обезбеди беспрекорен и изолиран пристап до корпоративна содржина, додека пакетите се движат низ хетерогени мрежи. Ова решение им овозможува на операторите на мобилните мрежи динамички да инстанцираат изолирани мрежни делови за корпоративни корисници и инфраструктурно да ги соединат 3GPP (3rd Generation Partnership Project) и не-3GPP мрежите, додека логички тие се сосема изолирани, вклучувајќи ги и корпоративните мрежи. Слично на нашата работа, тие истражуваат сценарија за повеќе локации кои ќе овозможат далечинско работење во корпоративното опкружување.

5.1.3. SDN и NFV кај 5G

Во [96] SDN и NFV се идентификувани како клучни технолошки овозможувачи на архитектурата, дизајнот, работењето и управувањето со 5G мрежите. Трудот опишува како двете технологии се надополнуваат една со друга и како се очекува тие да го водат развојот на мрежите во блиска иднина. Концептот на мрежно раслојување во 5G е овозможен од SDN и NFV.

Еден од најистражените аспекти на SDN и NFV е оптимизацијата на VNF сервисните низи. Со оптимизирање на VNF низите, давателите на услуги ќе го минимизираат трошењето на ресурсите и мрежната латентност.

Во работата на [97], се споредуваат три MANO рамки: SONATA, OSM и Cloudify со цел да се идентификуваат нивните силни и слаби точки. Проценката се врши експериментално на тест околина извлечена од реални системи. Обезбедена е евалуација на главните оперативни и функционални KPI (key performance indicator), за да се добијат потребните резултати.

Авторите на [98] работат на Мулти-пристапно рабно сметање (Multi-access Edge Computing MEC) како еден од овозможувачите на 5G услугите за ултра доверливи комуникации со мала латентност (uRLLC) и предлагаат генетски алгоритам за поврзување на VNF, за да се минимизира латентноста во низата и да се максимизира достапноста на услугата. Иако нашиот пристап е значително различен, анализата што ја правиме го надополнува ова истражување во смисла на предвидување на латентноста на услугата изградена врз SDN сервисна низа од VNF, а која предизвикана од NFV архитектурата и поставеноста на нејзините елементи.

Гао, Тао и сор. [99] предлагаат економична VPS шема (CEVPS) која ја истражува дополнителната латентност настаната во потенцијална NFV средина, настаната со подигнување на VM и инсталирање на VNF инстанца. Нивната работа е цврсто поврзана со VNF менаџерот и менаџерот на виртуелна инфраструктура (VIM), и двата како дел од NFV MANO. Шемата ги разгледува VNF функциите кои вршат еден таск (single threaded) и VNF функциите кои вршат повеќе паралелни таскови (multi threaded), а нивната пропусност, како функција на доделените компјутерски ресурси, ја моделираат различно.

CEVPS е ефикасен хеуристички алгоритам кој е формулиран како мешана интерлинеарна програма (MILP). CEVPS постигнува пониска цена и помала латентност од конвенционалните шеми за проактивна поставеност на VNF елементите во сервисна низа, со најдобра достапност и економичност, што е важно за 5G средини каде што се очекува латентноста да биде минимална. Спротивно на ова, нашето истражување претпоставува дека VIM не влијае кон латентноста во мрежата, бидејќи во секое време има доволно расположливи ресурси за подигање на нови VNF и има логика која предвидува потреба од нови VNF елементи, па истите ги има спремни пред да бидат побарани во сервисната низа. Практично, истражувањето на Гао, Тао и соработниците и нашето се надополнуваат и може да се искористат во случај кога нашите претпоставки за VIM не се валидни, па има потреба да се пресметува и потенцијалната латенција предизвикана од VIM.

Во [100], предложена е колаборативна рамка која работи во реално време, свесна за контекстот во кој работи и која се наоѓа на работ на мрежата, како техника за составување на услуги, која ќе гарантира испорака на услуги специфични за корисникот во 5G мрежите. NFV низата која ја формира услугата се формира преку пристап базиран workflow, кој се потпира на претходни резултати од формирање на сервисни низи. Нашата работа се занимава и со проширување на сервисната низа, а со тоа и услугата кон работ на мрежата, но од поинаква перспектива. Ја истражуваме дистрибуцијата преметувачките елементи на повеќе локации, водени од NFV архитектурата.

Авторите на [101] се занимаваат со прашањата за приспособливост и перформанси во контекст на 5G мобилните мрежи, со воведување на нова рамка за архитектура и контролна рамнина базирана на SDN, прилагодена за системи базирани на MCC (Mobile Convergence Client), поконкретно за системи базирани на FMC (Fixed Mobile Convergence), каде што мобилните јазли и мрежните услуги се предмет на ограничувања на движењата и миграциите. Тие предлагаат дистрибуција на контролната рамнина од OF SDN на хиерархиска архитектура на две нивоа: прво ниво со глобален контролер G-FMCC и второ ниво со неколку локални контролери LFMCC. NFV се користи за распоредување на контролери од второ ниво LFMCC, по барање, врз основа на оптоварувањето на системот. Тие предлагаат алгоритам за генерирање на вектор за распоредување кој се оценува преку теоретска анализа. Ние исто така, предлагаме дистрибуирани SDN и NFV околини и го анализираме доцнењето на мрежните пакети додадено на системот поради дистрибуцијата на компонентите на повеќе локации.

Во овој контекст, нашиот труд предлага аналитички модели на три различни NFV инфраструктури, споредувајќи ги разликите меѓу нив и наведувајќи ги позитивните и негативните страни кои произлегуваат од дистрибуцијата на NFV инфраструктурата. Направивме симулации и генериравме графикони кои визуелно покажуваат како времето на престој на пакетите во NFV околината зависи од бројот на контролери во системот, стапките на услугата на NFV елементите (контролери, комутатори, VNF менаџери) и различниот број на дистрибуирани локации земајќи ги предвид врските помеѓу дистрибуираните средини.

Во следниот дел ги претставуваме нашите аналитички модели.

5.2.Дефиниции за Марковијански процес, M/M/1 ред и Џексонова мрежа

Марковијански процес или Марковијански синџир е стохастички процес со следниве карактеристики [129]:

a. Бројот на возможни состојби е конечен;

b. Исходот во која било фаза зависи само од исходот од претходната фаза;

c. Веројатните се константни со текот на времето.

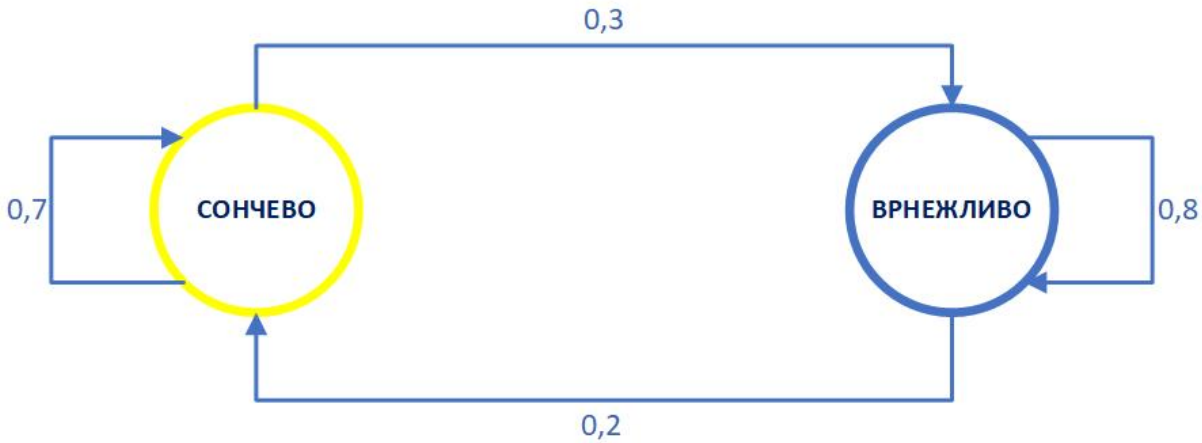
Стохастички процес е низа настани во кои исходот во која било фаза зависи од одредена веројатност.

Ако x_0 е вектор кој ја претставува почетната состојба на системот, тогаш постои матрица M таква што состојбата на системот по една итерација е дадена со векторот Mx_0. Така добиваме синџир на вектори на состојби: x_0, Mx_0, M^2x_0, . . . каде состојбата на системот по n повторувања е дадена со M^nx_0. Таквиот синџир се нарекува Марковијански синџир, а матрицата M се нарекува преодна матрица.

Векторите на состојбата можат да бидат од два вида: апсолутен вектор или вектор на веројатност. Апсолутен вектор е вектор чии записи го даваат вистинскиот број на објекти во дадена состојба. Вектор на веројатност е вектор каде што записите го даваат

процентот (или веројатноста) на објекти во дадена состојба. Сумата од вредности во еден вектор на веројатност е секогаш 1.

Марковијанскиот синџир може да се визуелизира како случаен процес кој отскокнува помеѓу различни состојби. На слика 16 е даден основен, но класичен пример за Марковијански синџир [130] со две состојби. Опишува случаен процес на временска прогноза, при што се претпоставува дека времето може да е сончево или врнежливо. Ако денес е сончево, постои 30% веројатност дека утре ќе е врнежливо, а 70% дека повторно ќе е сончево. Ако денес е врнежливо, постои веројатност од 20% утре повторно ќе е врнежливо и 80% веројатност дека утре повторно ќе е врнежливо.



Слика 16: Марковијански процес со две состојби

M/M/1 редица е специјален случај на Марковијански синџир каде што пристигнувањата го следат процесот на Поасон, времето на услугата е експоненцијално распределено и има еден сервер [131]. Претпоставките за M/M/1 редици се:

a. Бројот на клиенти кои пристигнуваат во временски интервал t следи Поасонов процес со параметар λ;

b. Интервалот помеѓу било кои две последователни пристигнувања е експоненцијално распределен со параметар λ;

c. Времето потребно за да се заврши една услуга има експоненцијална распределба со параметар μ;

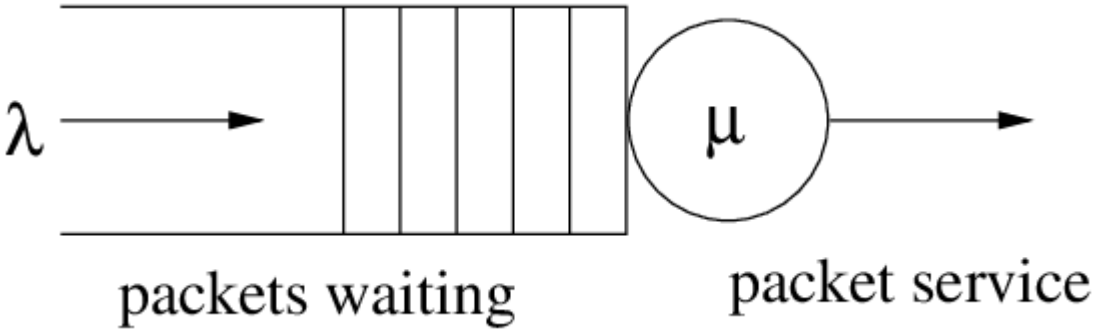
d. Времињата на пристигнување и сервисните времиња се независни едни од други;

e. Бројот на сервери е еден;

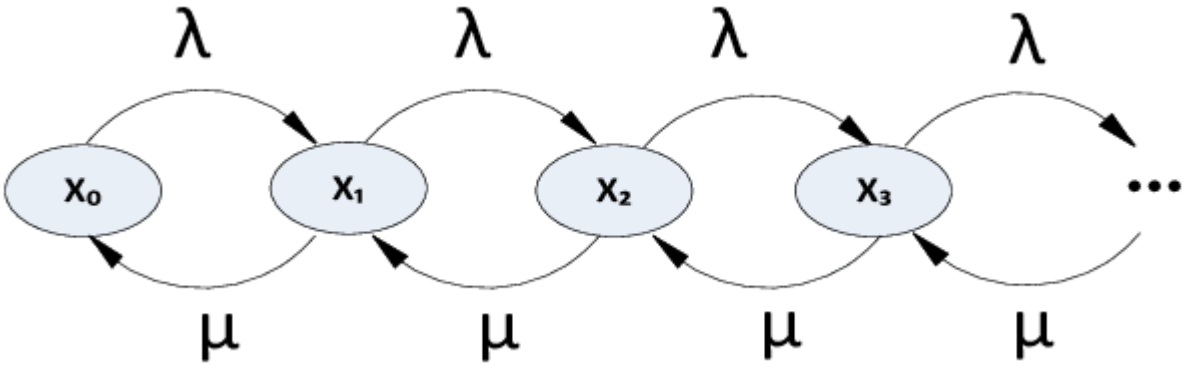
f. Големината на редот е бесконечна.

g. Редоследот на услугата се претпоставува дека е FIFO.

На слика 17 е даден шематски приказ на M/M/1 ред на чекање, а на слика 18 е претставен дијаграмот на состојби кај M/M/1 ред на чекање.



Слика 17: Шематски приказ на M/M/1 ред на чекање [132]



Слика 18: Дијаграм на состојби кај M/M/1 ред на чекање [133]

Џексонова мрежата е множество од поврзани јазли, каде што секој јазол претставува ред на чекање во кој стапката на услуга μ може да биде еднаква или различна во секој јазол и може да биде зависна од состојбата на јазолот (стапките на услугата се менува во зависност од должината на редот односно стапката на пристигање λ).

Мрежа која се состои од конечен број редици J, се нарекува Џексонова мрежа ако [134]:

a. Процесите на пристигнување во различни редици се независни Поасонови процеси. Нека λ_j ја означува стапката на надворешно пристигнување во редот j.

b. Секоја редица има еден сервер кој работи по FIFO принцип, а времињата на услуга на клиентите во секоја редица се независни и идентично дистрибуирани експоненцијални случајни променливи, со распределба $Exp(\mu_j)$. Покрај тоа, времињата на услуга во различни редици се меѓусебно независни.

c. Рутирањето е Марковијанско: клиентот кој ја завршил услугата кај редицата j се насочува кон редицата k со одредена фиксна веројатност r_{jk} и го напушта системот со веројатност $r_{j0} = 1 - \sum_{k=1}^{J} r_{jk}$. Одлуките за рутирање се меѓусебно независни и независни од претходната историја на клиентите (на пример, времето на нивното пристигнување и сервисирање и нивната рута низ мрежата до тој момент).

d. Мрежата е отворена, т.е. со веројатност една, секој клиент може да посети конечен број на редици пред да ја напушти мрежата.

Јазлите (редиците) кои ја формираат Џексоновата мрежа се нарекуваат Џексонови сервери. Секој Џексонов сервер добива надворешни пристигнувања следејќи го Поасоновиот процес. Покрај тоа, клиентите исто така влегуваат во редицата откако ќе бидат опслужени на некоја друга редица и ќе бидат пренасочени. Џексоновата мрежа постигнала стабилна состојба доколку секоја редица, односно сервер во мрежата е стабилен. Тоа значи дека должината на редот не расте неограничено со текот на времето, односно Џексоновиот сервер има доволно голема стапка на услуга со која може да ја опслужи стапката на пристигнување во него . Секој клиент што влегува во редот мора на крајот да ја напушти редицата (во спротивно ќе се насобере редот). Оттука, долгорочната стапка на заминување од редот j мора да биде иста со стапката на долгорочно пристигнување, и се означува со λ_j.

Во продолжение се опишани аналитичките модели во кои се наведени претпоставките и ограничувањата со кои работиме. Користиме M/M/1 редици на чекање кои формираат Џексонова мрежа. Клиентите во нашиот случај се мрежните пакети кои се обработуваат од мрежните уреди, односно од мрежните функции.

5.3.Аналитички модели

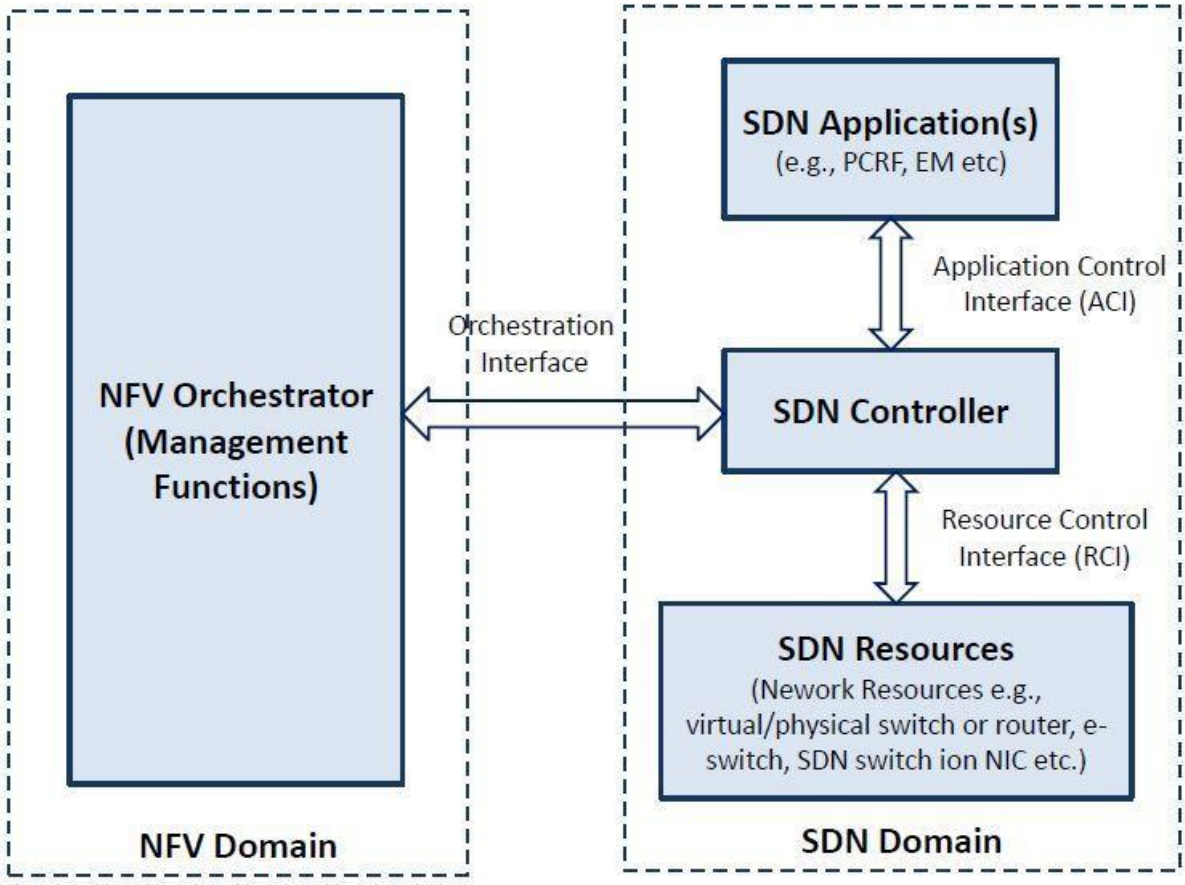
За да создадеме модели за систем изграден врз NFV архитектура, ги користиме принципите на теоријата на редици. SDN претставува неразделна компонента од модерната NFV инфраструктура и интеракцијата помеѓу SDN и NFV е дадена на слика 19. Постојат 3 модели кои се испитуваат:

- Централизиран систем каде сите елементи се на една локација (обично еден податочен центар). Системот има еден контролер, еден VNF менаџер и еден комутатор.
- Систем кој има дистрибуирана податочна рамнина, што значи дека има елементи од NFV инфраструктурата на повеќе локации. SDN низите од VNF елементи може да се протегаат во повеќе податочни центри и различни географски локации. Секоја локација има еден комутатор. MANO опкружувањето има еден контролер и еден VNF менаџер кои ги опслужуваат сите локации.
- Целосно дистрибуиран систем, каде што секоја локација ги има сите елементи на NFV архитектурата. Секоја локација има податочна рамнина направена врз NFVI со еден комутатор и MANO со контролер и VNF менаџер. Контролорите комуницираат едни со други и секој контролер е свесен за целиот систем.

5.3.1. Претпоставки

Слично на [29], ние ја моделираме податочната рамнина како Џексонова мрежа во која сите комутатори се Џексонови сервери. Секоја дистрибуирана локација има еден комутатор. Иако во пракса на една локација, еден комутатор може да се разграни на повеќе основни комутатори, за едноставност ќе претпоставиме само еден комутатор по локација. Ова нема да влијае на генерализацијата бидејќи повеќе поврзани комутатори на една локација, може да се апроксимираат како еден комутатор со соодветната стапка на пристигнување (arrival rate) и стапка на услуга (service rate). Претпоставуваме дека на секој јазол процесите на пристигнување се сметаат за Поасонови процеси. Се

претпоставува дека времето на сервисирање на пакетите следи експоненцијална дистрибуција. Второ, пристигнувањата на различни јазли и нивните соодветни времиња на услуга се независни едни од други. Трето, мрежата на редици има достигнато избалансирана состојба и искористеноста на сите редици е помала од еден. Со овие претпоставки можеме да ги моделираме сите јазли како системи со M/M/1 редици на чекање. Контролерите и VNF менаџерите се посебно моделирани како M/M/1 редици со бесконечни големини. Претпоставуваме дека сите пакети се обработени и ниту еден пакет што доаѓа до контролерот или до VNF менаџерот не е отфрлен.



Слика 19: ETSI NFV перспектива наинтеракцијата со SDN доменот [102]

Системот е базиран на OpenFlow. Контролерите се целосно свесни за мрежната топологија и се способни да прават промени во табелите на проток на комутаторите, за да се постигне оптимално проследување на податоците. Во сценарио со еден контролер, се претпоставува дека контролорот е одговорен за сите дистрибуирани локации. Во сценариото на повеќе контролери, има еден контролер по дистрибуирана локација. Секој

контролер може да направи промени во табелите на проток на комутаторите, во својата или во другите дистрибуирани околини, во случај VNF низите да се протегаат низ повеќе дистрибуирани локации. Контролерот што ја прима пораката за packet-in е одговорен за packet-out пораките и ажурирањата на табелите за проток кај комутаторите. Контролерот што ги прави промените, ги известува сите други контролери за извршените промени, така што секој контролер има ажурирани информации за мрежната топологија и табелите на проток.

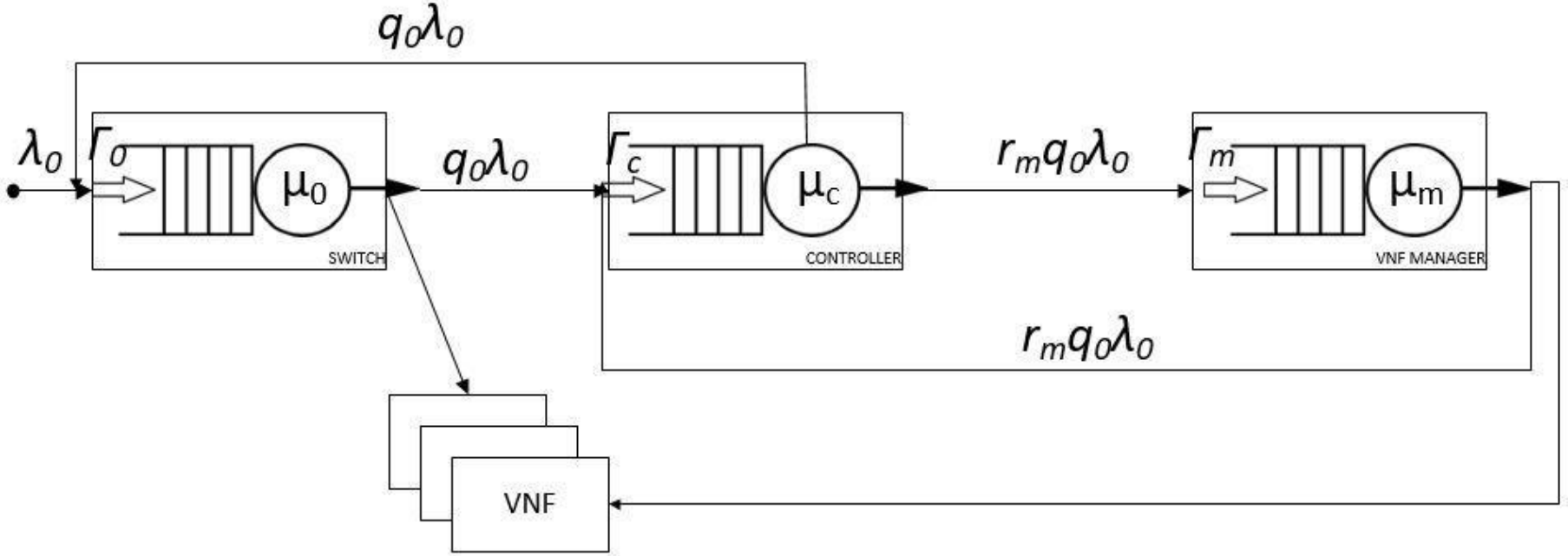
Секој контролер е поврзан со VNF менаџер кој е директно поврзан со елемент менаџерите (EM) и виртуелните мрежни функции. VNF менаџерот ја извршува работата на започнување, скалирање и продолжување на работата на VNF функциите. Добива информации од контролерот и ја извршува својата работа доколку контролорот не може да најде соодветна мрежна патека за услугата или слободни VNF функции.

Претпоставуваме дека виртуелниот менаџер на инфраструктура (VIM) не придонесува за времето на престој на пакетите во мрежата, бидејќи самостојно управува со основната инфраструктура, давајќи им ги потребните ресурси на VNF функциите во реално време. Сметаме дека основната инфраструктура секогаш има достапни ресурси. Исто така, се смета дека NFV оркестраторот не придонесува за времето на престој на пакетите поради неговата улога во NFV MANO.

5.3.2. Шематски приказ и моделирање на околините

5.3.2.1. Централизиран систем

Мрежата која е поставена на една локација изградена преку SDN елементи и NFV архитектура е дадена на слика 20. Податочната рамнина има еден комутатор со брзина на пристигнување на нови пакети λ_0. Само пакетите што не можат да се совпаднат со постоечката табела на проток во комутаторот се пренасочуваат кон контролерот. Веројатноста пакетите да бидат испратени до контролерот е означена како q_o. Објаснувањето на употребената нотација е дадено во Табела 9.



Слика 20: Централизиран систем каде сите елементи се на една локација

Искористеноста (utilization) на комутаторот, контролерот и VNF менаџерот се дадени со:

$$\rho_0 = \frac{\Gamma_0}{\mu_0} \; - the\ utilization\ of\ the\ switch \tag{8}$$

$$\rho_c = \frac{\Gamma_c}{\mu_c} \; - the\ utilization\ of\ the\ controller \tag{9}$$

$$\rho_m = \frac{\Gamma_m}{\mu_m} \; - the\ utilization\ of\ the\ VNF\ manager \tag{10}$$

Вкупната стапка на пристигнување (arrival rate) кај комутаторот е збир од стапките на пристигнување на надворешните пакети и пакетите вратени од контролерот кон комутаторот:

$$\Gamma_0 = \lambda_0 + q_0 \cdot \lambda_0 \tag{11}$$

Веројатноста за испраќање пакети од контролорот до VNF менаџерот е r_m, а вкупната стапка на пристигнување кај VNF менаџерот е:

$$\Gamma_m = r_m \cdot q_0 \cdot \lambda_0 \tag{12}$$

Вкупната стапка на пристигнување кај контролерот е збир на стапките на пристигнување од комутаторот и од VNF менаџерот:

$$\Gamma_c = q_0 \cdot \lambda_0 + r_m \cdot q_0 \cdot \lambda_0 \tag{13}$$

Просечниот број на мрежни текови во комутаторот, контролерот и VNF менаџерот се:

$$E[N_0] = \frac{\rho_0}{1 - \rho_0} \tag{14}$$

$$E[N_c] = \frac{\rho_c}{1 - \rho_c} \tag{15}$$

$$E[N_m] = \frac{\rho_m}{1 - \rho_m} \tag{16}$$

Според законот на Литл, просечното време на чекање на пакети во елементите е:

$$E[T_0] = \frac{E[N_0]}{\Gamma_0} = \frac{1}{\mu_0 - \Gamma_0} \quad (17)$$

$$E[T_c] = \frac{E[N_c]}{\Gamma_c} = \frac{1}{\mu_c - \Gamma_c} \quad (18)$$

$$E[T_m] = \frac{E[N_m]}{\Gamma_m} = \frac{1}{\mu_m - \Gamma_m} \quad (19)$$

Земајќи ги предвид горенаведените равенки, просечното време на чекање на пакетите во системот е дадено со:

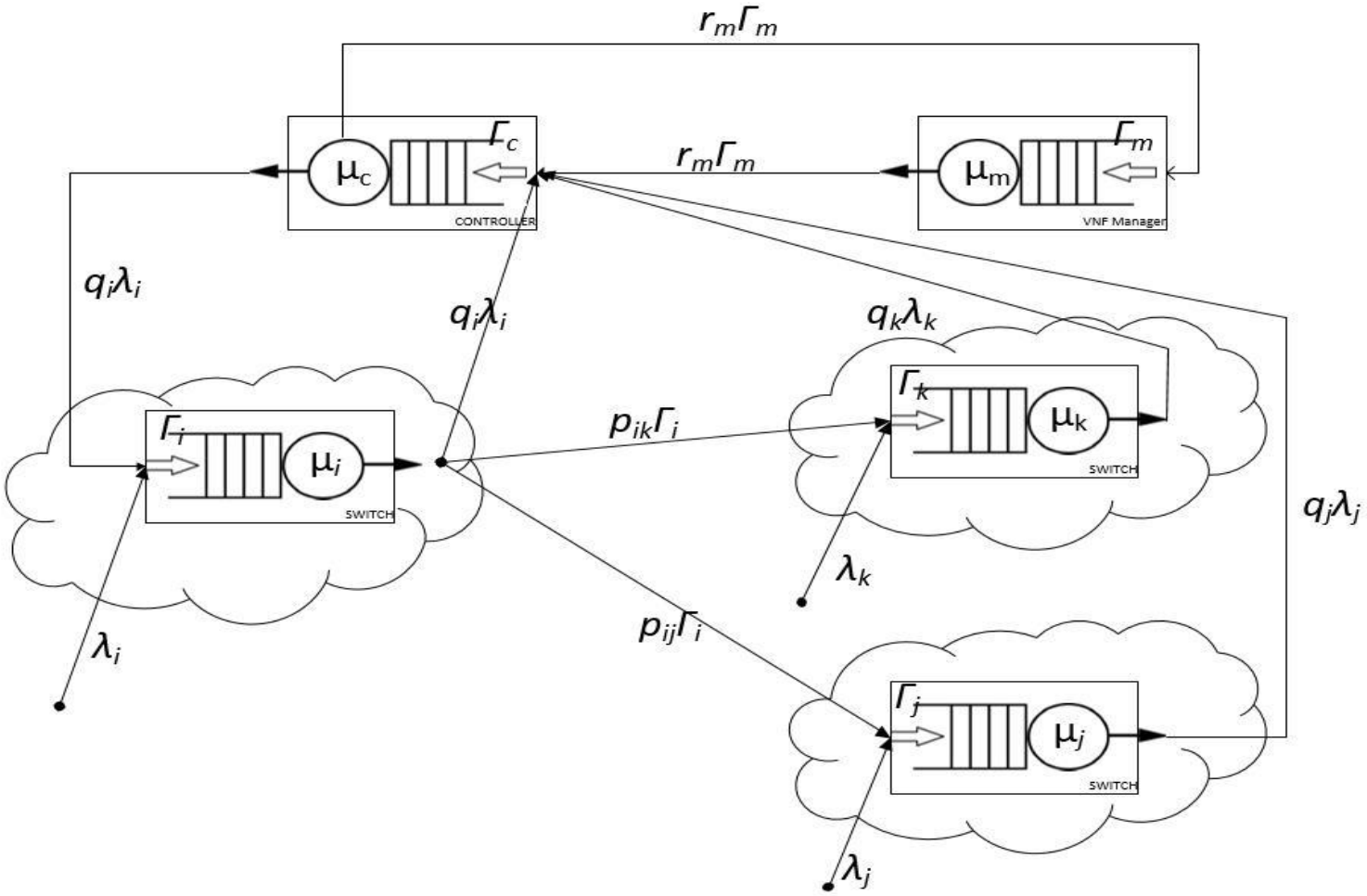
$$E[T_{tot}] = E[T_0] + E[T_c] + E[T_m] \quad (20)$$

$$E[T_{tot}] = \frac{1}{\mu_0 - \lambda_0 \cdot (1 + q_0)} + \frac{1}{\mu_c - q_0 \cdot \lambda_0 \cdot (1 + r_m)} + \frac{1}{\mu_m - r_m \cdot q_0 \cdot \lambda_0} \quad (21)$$

Во ова сценарио, претпоставуваме дека пакетите се движат во еден податочен центар, повеќето од нив во насока исток-запад, во истата виртуелизирана средина. Во ваков случај, можеме да претпоставиме дека трансмисионата латентност (transmission latency) и пропагационата латентност (propagation latency) се минимални, па затоа нема да ги земеме предвид.

5.3.2.2. Дистрибуирана податочна рамнина со централен контролер и VNF менаџер

Слика 21 покажува дистрибуирана податочна рамнина на податоци на повеќе локации со централен контролер и NFV MANO. Таквото опкружување е практично кога е неопходно некои мрежни елементи кои ја формираат корисничката услуга да бидат поблиску до потрошувачот. Мултимедијалните услуги се еден таков пример. Ова сценарио е исто така веродостојно за повеќе податочни центри во еден или повеќе географски региони. Во моментов, главните даватели на јавни услуги ги дефинираат регионите како збир на податочни центри, распоредени во периметар дефиниран според латентноста и поврзани преку дедицирана регионална мрежа со ниска латентност [103], [104].



Слика 21: Модел на дистрибуирана податочна рамнина и централен контролер и NFV MANO

ТАБЕЛА 9. ОБЈАСНУВАЊЕ ЗА НОТАЦИЈАТА

Симбол	**Параметар**
λ_i	arrival rate at switch *i*
q_i	probability of packet going from switch *i* to controller
p_{ij}	probability of packet going from switch *i* to switch *j*
r_m	probability of packet going from controller to VNF manager
μ_i	service rate of the switch *i*
μ_c	service rate of the controller
μ_m	service rate of the VNF manager
Γ_i	total arrival rate at the switch *i*
Γ_c	total arrival rate at the controller
Γ_m	total arrival rate at the VNF manager
N_i	number of packets at the switch *i*
N_c	number of packets at the controller
N_m	number of packets at the manager
T_i	sojourn time at the switch *i*
T_c	sojourn time at the controller
T_m	sojourn time at the VNF manager
$E[N]$	mean value for number of packets in M/M/1 queue
$E[T]$	mean value for the sojourn time of packets in M/M/1 queue
L_T	transmission latency
L_P	propagation latency
L_{Tij}	transmission latency from *i* to *j*
L_{Pij}	propagation latency from *i* to *j*
T_N	time spent in network
T_{NC}	time spent in the network for packets going to the controller
T_{NS}	time spent in the network for packets going between switches
$E[T_{NC}]$	mean value for the sojourn time for packets going to the controller
$E[T_{NS}]$	mean time for the sojourn time for packets going between switches
B_{ij}	number of packets on link from *i* to *j*
Bw_{ij}	bandwidth on link from *i* to *j*
d_{ij}	distance from *i* to *j*
s	speed of data in link

Имаме *k* дистрибуирани локации и *k* комутатори. Го означуваме λ_i како стапка на пристигнување на нови пакети на комутаторот *i* каде што: $i \in \{1,2,3,\ldots,k\}$

Искористеноста ја пресметуваме како:

$$\rho_i = \frac{\Gamma_i}{\mu_i} \quad - the\ utilization\ of\ the\ switch\ i \tag{22}$$

$$\rho_c = \frac{\Gamma_c}{\mu_c} \quad - the\ utilization\ of\ the\ controller \tag{23}$$

$$\rho_m = \frac{\Gamma_m}{\mu_m} \quad - the\ utilization\ of\ the\ VNF\ manager \tag{24}$$

Равенката за рамнотежа на комутаторот i е дадена збир од брзината на пристигнување на пакетите однадвор и пристигнувањето на пакетите од другите комутатори:

$$\gamma_i = \lambda_i + \sum_{j=1, j\neq i}^{k} (p_{ij} \cdot u_{ij})\gamma_j \tag{25}$$

Каде што γ_i е вкупниот влез за комутаторот i.

Користиме u_{ij} за да ги земеме предвид сервисните низи во кои нема врска помеѓу комутаторите i и j.

$$u_{ij} = \begin{cases} 1 & if\ update\ from\ j\ involves\ i \\ 0 & if\ update\ from\ j\ doesn't\ involve\ i \end{cases} \tag{26}$$

Вкупната стапка на пристигнување на комутаторот i е збирот од вкупниот влез во комутаторот (25) и пакетите што пристигнуваат до комутаторот од контролерите.

$$\Gamma_i = \gamma_i + q_i \cdot \lambda_i + \sum_{j=1, j\neq i}^{k} (q_j \cdot u_{ij})\lambda_j \tag{27}$$

Вкупните стапки на пристигнување кај VNF менаџерот и контролерот се:

$$\Gamma_m = \sum_{i=1}^{k} q_i \cdot \lambda_i \cdot r_i \tag{28}$$

$$\Gamma_c = \sum_{i=1}^{k} q_i \cdot \lambda_i + \sum_{i=1}^{k} q_i \cdot \lambda_i \cdot r_i \tag{29}$$

Со ова можеме да го пресметаме просечниот број на текови и просечното време на престој на пакетите во комутаторите, контролерот и VNF менаџерот:

$$E[N_i] = \frac{\rho_i}{1 - \rho_i} \quad (30)$$

$$E[T_i] = \frac{1}{\mu_i - \Gamma_i} \quad (31)$$

$$E[N_c] = \frac{\rho_c}{1 - \rho_c} \quad (32)$$

$$E[T_c] = \frac{1}{\mu_c - \Gamma_c} \quad (33)$$

$$E[N_m] = \frac{\rho_m}{1 - \rho_m} \quad (34)$$

$$E[T_m] = \frac{1}{\mu_m - \Gamma_m} \quad (35)$$

Просечното време што еден пакетски тек го поминува во системот, без времето поминато во линковите помеѓу дистрибуираните средини е:

$$E[T_d] = \frac{1}{\sum_{i=1}^{k} \lambda_i} \cdot \left[\sum_{i=1}^{k} E[T_i] + E[T_c] + E[T_m] \right] \quad (36)$$

$$E[T_d] = \frac{1}{\sum_{i=1}^{k} \lambda_i} \cdot \left[\sum_{i=1}^{k} \frac{1}{\mu_i - (\gamma_i + q_i \cdot \lambda_i + \sum_{j=1, j \neq i}^{k} (q_j \cdot u_{ij}) \lambda_j)} + \frac{1}{\mu_c - (\sum_{i=1}^{k} q_i \cdot \lambda_i + \sum_{i=1}^{k} q_i \cdot \lambda_i \cdot r_i)} + \frac{1}{\mu_m - \sum_{i=1}^{k} q_i \cdot \lambda_i \cdot r_i} \right] \quad (37)$$

Сега го пресметуваме времето поминато на пакетите во линковите што ги поврзуваат дистрибуираните средини:

Транспортната и пропагационата латентност се дадени со равенките:

$$L_{Tij} = \frac{B_{ij}}{Bw_{ij}} \quad (38)$$

$$L_{Pij} = \frac{d_{ij}}{s} \quad (39)$$

Во пракса, пропагационата латентност е многу помала од транспортната латентност.

Латенцијата пак, од сите комутатори до контролерот, земајќи ги предвид погорните равенки е:

$$E[T_{NC}] = \sum_{i=1}^{k} q_i \cdot (L_{Tic} + L_{Pic}) \quad (40)$$

Латенцијата од сите комутатори до комутаторот i е:

$$E[T_{Ni}] = \sum_{j=1, j\neq i}^{k} p_{ij} \cdot (L_{Tij} + L_{Pij}) \cdot u_{ij} \quad (41)$$

Вкупната латенција на сервисната низа предизвикана од транспортот на пакетите помеѓу комутаторите е:

$$E[T_{NS}] = \sum_{i=1}^{k} \sum_{j=1, j\neq i}^{k} p_{ij} \cdot (L_{Tij} + L_{Pij}) \cdot u_{ij} \quad (42)$$

Средната вредност на латенцијата за мрежните пакети кои патуваат во сервисна низа е сума од латенцијата која се појавува поради движењето на мрежните пакети помеѓу комутаторите (во различни дистрибуирани средини) и латенцијата предизвикана од потребата да се испратат пакети до контролерот.

$$E[T_N] = E[T_{NC}] + E[T_{NS}] \quad (43)$$

$$E[T_N] = \sum_{i=1}^{k} q_i \cdot (L_{Tic} + L_{Pic}) + \sum_{i=1}^{k} \sum_{j=1, j\neq i}^{k} p_{ij} \cdot (L_{Tij} + L_{Pij}) \cdot u_{ij} \quad (44)$$

Сега го имаме просечното доцнење на пакетите предизвикано од архитектурата (37) и просечното доцнење на пакетите предизвикано од транспортот на пакетите во линковите помеѓу дистрибуираните локации (44). Можеме да ја пресметаме вкупната просечна латентност на пакетите во оваа дистрибуирана околина:

$$E[T_{tot}] = E[T_d] + E[T_N] \quad (45)$$

5.3.2.3. Целосно дистрибуирана околина

Нашиот модел за целосно дистрибуирана околина е даден на слика 22. Секоја локација има податочна рамнина со еден комутатор, контролер и VNF менаџер, наменети за таа локација. Бидејќи основната физичка инфраструктура исто така треба да е дистрибуирана, секоја локација мора да има и VIM што управува со складиштето на хардверските ресурси на NFV инфраструктурата и управува со виртуелните врски,

линкови, подмрежи и порти. Слично на претходниот случај, претпоставуваме дека инфраструктурата ги има потребните ресурси и VIM управува со нив без да влијае на времето на престој на пакетите.

Дистрибуираните податочни рамнини комуницираат меѓу себе преку мрежни линкови. Сите контролери можат да комуницираат со комутаторот на нивната сопствена локација, испраќајќи packet-in пораки, со што ги менуваат табелите на проток на нивната локација. Секој контролер е целосно свесен за мрежната инфраструктура и сите сервисни услуги во NFV околината. Во случај на промена иницирана од еден контролер, тој контролер ги испраќа информациите до сите други контролери. Контролерите каде што е потребна промена на табелите на проток, дејствуваат со packet-in пораки. Секоја локација има независна стапка на пристигнување на мрежните пакети и секоја сервисна услуга, односно SDN низа од VNF функции, може да започне од која било локација. Со тоа низата може да се протега на една или повеќе локации.

Ова опкружување се препорачува доколку има потреба VNF елементите да се блиску до крајните потрошувачи, при што повеќето од сервисните услуги што се нудат користат VNF елементи главно на нивната матична локација. Како што ќе биде прикажано подоцна во овој документ, врските помеѓу дистрибуираните локации имаат големо влијание врз времето на престој на пакетите и ако сервисната услуга се протега во 3 или повеќе дистрибуирани средини, транспортното доцнење во мрежата доминира во времето на престој на пакетите.

Имаме k различни локации со k комутатори, контролери, and VNF менаџери. Во ваков случај формулите за искористеноста на комутаторот i, контролерот i и VNF менаџерот i, каде $i \in \{1,2,3,\dots,k\}$ се дадени како:

$$\rho_i = \frac{\Gamma_i}{\mu_i} \quad - the\ utilization\ of\ the\ switch\ i \tag{46}$$

$$\rho_{ci} = \frac{\Gamma_{ci}}{\mu_{ci}} \quad - the\ utilization\ of\ the\ controller\ i \tag{47}$$

$$\rho_{mi} = \frac{\Gamma_{mi}}{\mu_{mi}} \quad - the\ utilization\ of\ the\ VNF\ manager\ i \tag{48}$$

Формулата за балансирана состојба на комутаторот i е иста како и во претходното сценарио, сума од стапката на пристигање на пакетите од надвор и стапката на пристигање на пакети од другите комутатори:

$$\gamma_i = \lambda_i + \sum_{j=1, j\neq i}^{k} (p_{ij} \cdot u_{ij})\gamma_j \quad (49)$$

Каде γ_i е нето влезната стапка на пристигање на пакети во комутаторот i, која потекува од сервисот и од другите комутатори.

Вкупната стапка на пристигнување во комутаторот i е збир на нето влезот во комутаторот (49) и пакетите што пристигнуваат до комутаторот од контролорите. Ако ги споредиме (27) и (49) можеме да видиме дека веројатноста за пакети во комутаторот i од други дистрибуирани локации е c_{ij} , што е веројатноста контролерот од една локација да испрати пакет до контролер на друга локација.

$$\Gamma_i = \gamma_i + q_i \cdot \lambda_i + \sum_{j=1, j\neq i}^{k} (c_{ij} \cdot u_{ij})\lambda_j \quad (50)$$

Вкупните стапки на пристигнување кај менаџерот VNF на локација i и контролерот на локација i се:

$$\Gamma_{mi} = q_i \cdot \lambda_i \cdot r_i + \sum_{j=1, j\neq i}^{k} c_{ij} \cdot \lambda_j \cdot r_j \quad (51)$$

$$\Gamma_{ci} = q_i \cdot \lambda_i + q_i \cdot \lambda_i \cdot r_i + \sum_{j=1, j\neq i}^{k} c_{ji} \cdot \lambda_j \quad (52)$$

Сега, кога ги имаме вкупните стапки на пристигнување и сервисните стапки, можеме да го пресметаме просечниот број на текови и просечното време на престој на пакетите во комутаторите, контролорите и VNF менаџерите:

$$E[N_i] = \frac{\rho_i}{1 - \rho_i} \quad (53)$$

$$E[T_i] = \frac{1}{\mu_i - \Gamma_i} \quad (54)$$

$$E[N_{ci}] = \frac{\rho_{ci}}{1 - \rho_{ci}} \quad (55)$$

$$E[T_{ci}] = \frac{1}{\mu_{ci} - \Gamma_{ci}} \tag{56}$$

$$E[N_{mi}] = \frac{\rho_{mi}}{1 - \rho_{mi}} \tag{57}$$

$$E[T_{mi}] = \frac{1}{\mu_{mi} - \Gamma_{mi}} \tag{58}$$

Просечното време што еден пакетски тек го поминува во системот кој е целосно дистрибуиран, со контролер и VNF менаџер на секоја локација, без времето поминато во линковите помеѓу дистрибуираните средини е:

$$E[T_d] = \frac{1}{\sum_{i=1}^{k} \lambda_i} \cdot \left[\sum_{i=1}^{k} E[T_i] + \sum_{i=1}^{k} E[T_{ci}] + \sum_{i=1}^{k} E[T_{mi}] \right] \tag{59}$$

$$\begin{aligned} E[T_d] = \frac{1}{\sum_{i=1}^{k} \lambda_i} \cdot \Bigg[& \sum_{i=1}^{k} \frac{1}{\mu_i - (\gamma_i + q_i \cdot \lambda_i + \sum_{j=1, j\neq i}^{k} (c_{ij} \cdot u_{ij}) \lambda_j)} \\ & + \sum_{i=1}^{k} \frac{1}{\mu_{ci} - (q_i \cdot \lambda_i + q_i \cdot \lambda_i \cdot r_i + \sum_{j=1, j\neq i}^{k} c_{ji} \cdot \lambda_j)} \\ & + \sum_{i=1}^{k} \frac{1}{\mu_{mi} - (q_i \cdot \lambda_i \cdot r_i + \sum_{j=1, j\neq i}^{k} c_{ij} \cdot \lambda_j \cdot r_j)} \Bigg] \end{aligned} \tag{60}$$

Сега, ќе го пресметаме просечното време што еден пакет го поминува во линковите што ги поврзуваат дистрибуираните локации. Латентноста предизвикана од сите контролори со нивната меѓусебна комуникација е:

$$E[T_{NC}] = \sum_{i=1}^{k} \sum_{j=1, j\neq i}^{k} c_{ij} \cdot (L_{Tij} + L_{Pij}) \cdot u_{ij} \tag{61}$$

Латенцијата предизвикана од комуникацијата на комутаторите со комутаторот i е:

$$E[T_{Ni}] = \sum_{j=1, j\neq i}^{k} p_{ij} \cdot (L_{Tij} + L_{Pij}) \cdot u_{ij} \tag{62}$$

Латенцијата за една сервисна низа за транспортот помеѓу комутаторите е:

$$E[T_{NS}] = \sum_{i=1}^{k} \sum_{j=1, j\neq i}^{k} p_{ij} \cdot (L_{Tij} + L_{Pij}) \cdot u_{ij} \quad (63)$$

Просечното доцнење на пакетите, во случај на низа од VNF елементи кои формираат сервисна услуга на повеќе локации, е збир на латентноста предизвикана од комуникацијата помеѓу комутаторите и латентноста предизвикана од комуникацијата меѓу контролерите.

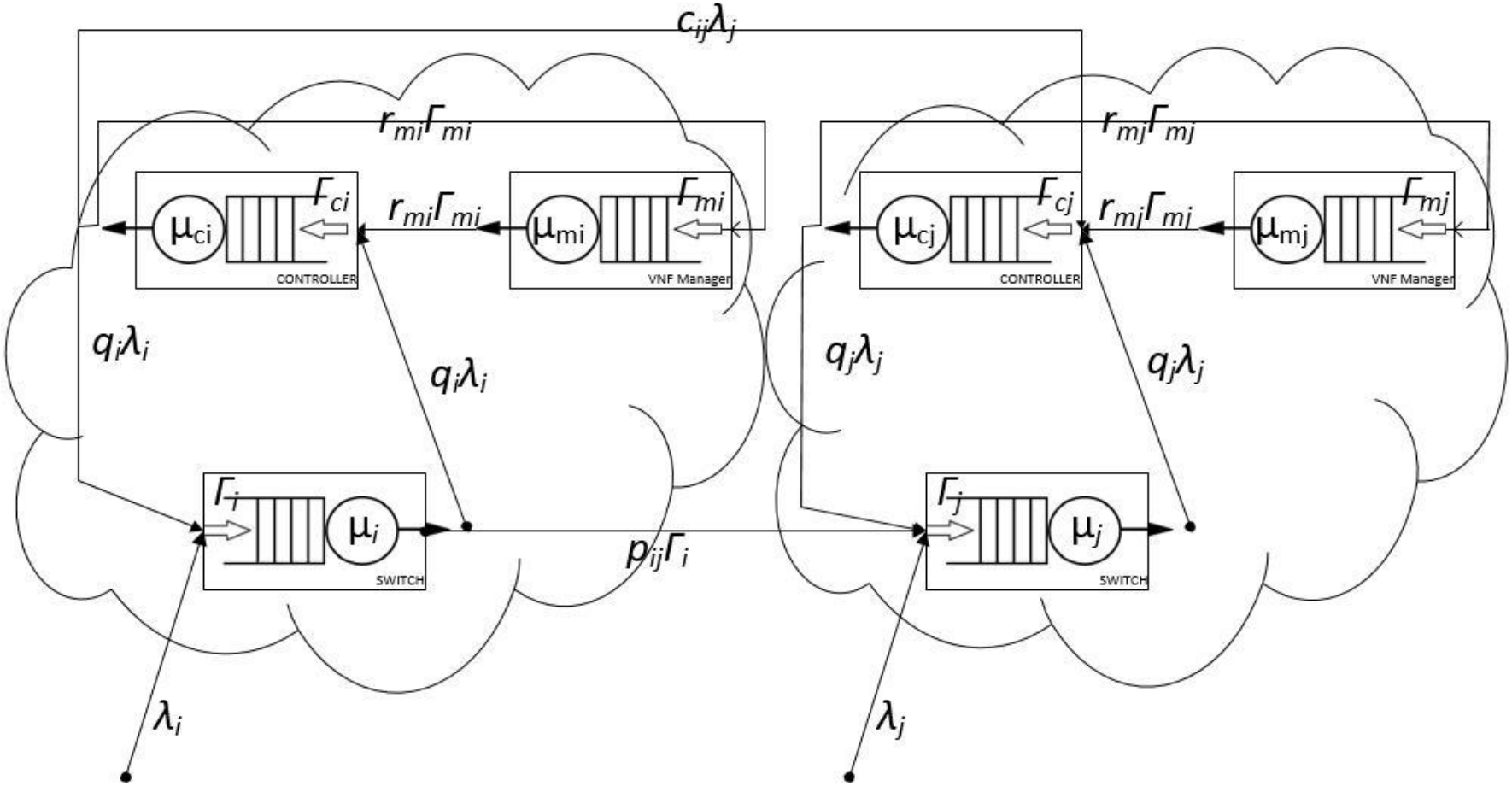
$$E[T_N] = E[T_{NC}] + E[T_{NS}] \quad (64)$$

$$E[T_N] = \sum_{i=1}^{k} \sum_{j=1, j\neq i}^{k} c_{ij} \cdot (L_{Tij} + L_{Pij}) \cdot u_{ij} + \sum_{i=1}^{k} \sum_{j=1, j\neq i}^{k} p_{ij} \cdot (L_{Tij} + L_{Pij}) \cdot u_{ij} \quad (65)$$

Според формулите (60) и (65) може да се пресмета вкупниот мрежен престој на пакетите во NFV инфраструктура која е поставена на повеќе дистрибуирани локации:

$$E[T_{tot}] = E[T_d] + E[T_N] \quad (60)$$

Во следниот дел вршиме анализа на предложените системи со аналитичките модели што ги изведовме и како тие функционираат во различни ситуации, имајќи го предвид бројот на различни локации кои можат да се користат, мрежната латентност предзивикана од линковите помеѓу нив, како и од веројатноста за пакети испратени до контролерите.



Слика 22: Модел на целосно дистрибуирана NFV околина.

5.4.Евалуација на перформанси

За да ги оцениме предложените системи со аналитичките модели опишани во претходните глави, развивме симулациски скрипти во Matlab. Ќе разговараме за секоја од околините посебно и на крајот ќе ги споредиме двете предложени дистрибуирани околини, онаа со дистрибуирата податочна рамнина, а единствена управувачка рамнина и NFV MANO и онаа со целосно дистрибуирани податочна рамнина и NFV MANO.

5.4.1. Евалуација на централизирана архитектура

Централизираната околина што ја разгледуваме има еден контролер, еден VNF менаџер и еден комутатор. Времето на престој на пакетите во системот најмногу ќе зависи од сервисната низа, но нашата цел е да оцениме како самиот систем ќе придонесе за времето на престој на пакетите.

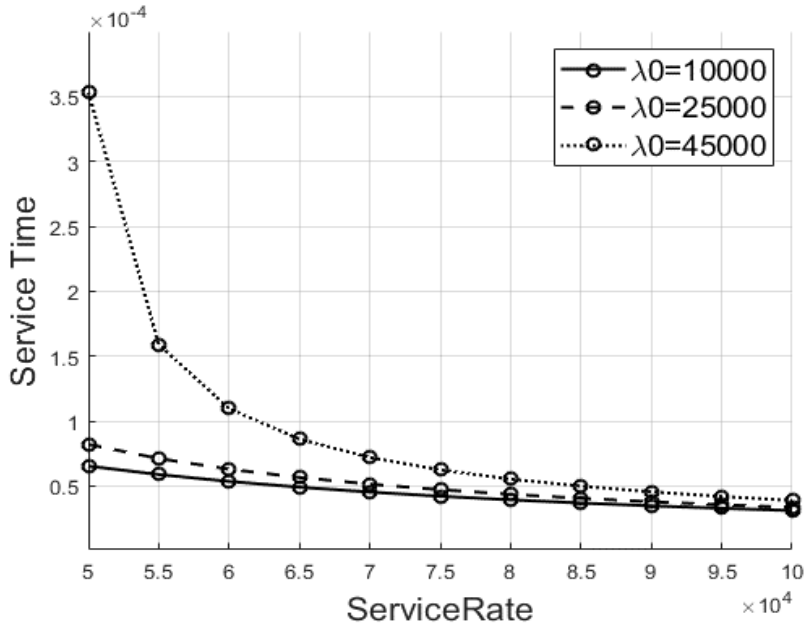
Стапката на услуга на елементите е најочигледната метрика што ќе влијае на времето на престој на пакетите. Како што може да се види на слика 23, со намалување на стапката на услуга, времето на престој на пакетите (вкупното сервисно време на системот) експоненцијално се зголемува. Слично на [27], [28], [35], [105] направивме претпоставка дека 4% од пакетите треба да одат од комутаторот до контролерот, во OF мрежата, за табелите на проток да бидат ажурирани и 4% од пакетите што стигнуваат до контролерот треба да одат до VNF Менаџерот кој комуницира со VNF во податочната рамнина.

За симулациите, зедовме основни параметри на брзината на услугата на контролорот да биде 90000 pkts/sec и стапката на услуга на VNF Менаџерот да биде 95000 pkts/sec [35]. Овие параметри се искористени во Matlab функциите.

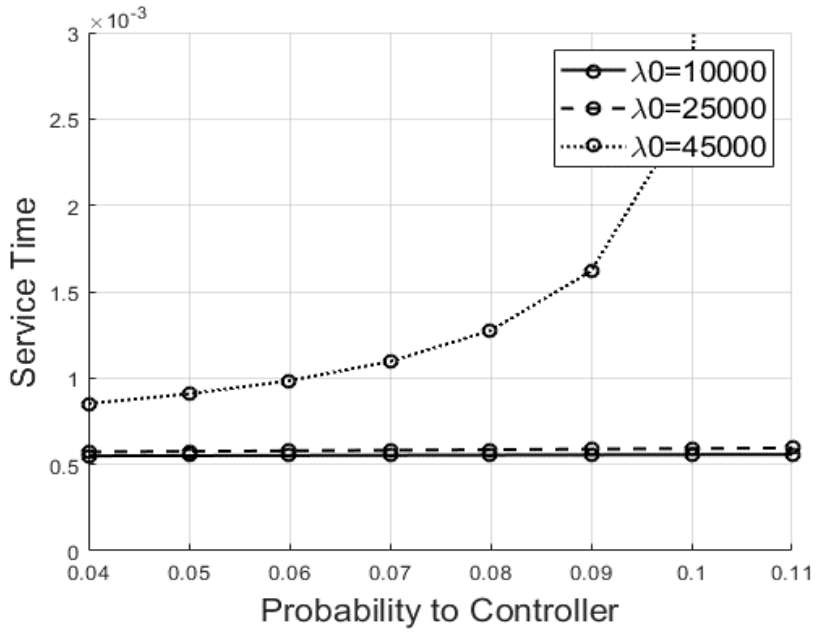
Од слика 24 можеме да видиме како системот ќе реагира во однос на средното време на престој на пакети, со различни веројатности за пакетите што треба да се испратат од комутаторот до контролерот. Очигледно, поголема веројатност за испраќање пакети до контролерот значи поголемо време на престој на пакетите. Зависноста е експоненцијална и поизразена при повисоки стапки на пристигнување.

Слика 25 ја покажува зависноста на времето на престој на пакетите од веројатноста за испраќање пакети до VNF Менаџерот. Слично на тоа, како и кај контролерот, времето на престој на пакетот расте експоненцијално како што се зголемува бројот на пакети

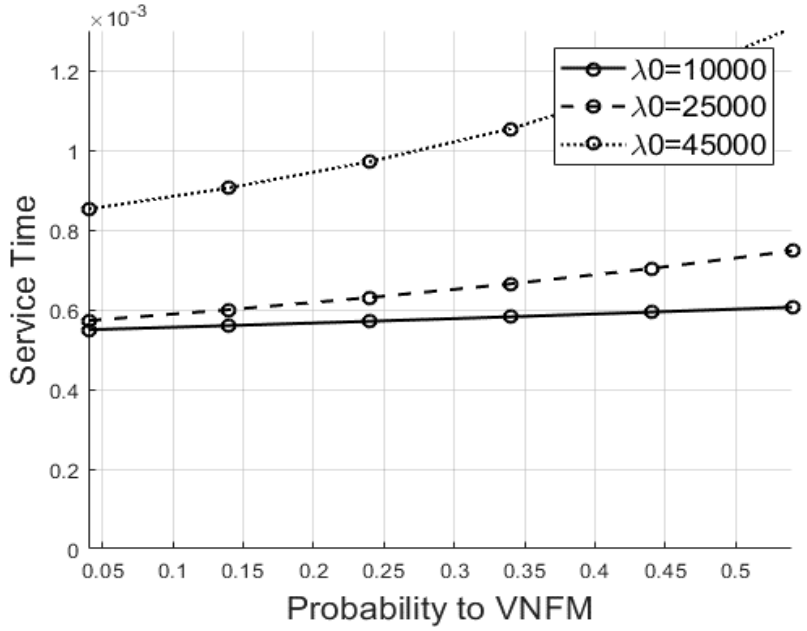
испратени до VNF Менаџерот. Ова покажува дека колку е поголема потребата за креирање и стартување на дополнителни VNF функции, толку е поголемо временското доцнење во системот. Може значително да се намали со воведување „паметни“ VNF менаџери кои можат [40] [106] [107] да ја предвидат потребата од нови VNF функции и SDN сервисни низи и да дејствуваат соодветно, со што значително ќе се намали целокупната мрежна латентност во средина базирана на NFV архитектура.



Слика 23: Зависност на сервисното време од стапката на услуга - централизиран систем



Слика 24: Зависност на сервисното време од веројатноста за праќање на пакет кон контролерот - централизиран систем



Слика 25: Зависност на сервисното време од веројатноста за праќање на пакет кон VNF Менаџерот - централизиран систем

5.4.2. Евалуација на систем со дистибуирана податочна рамнина и ценрална управувачка околина

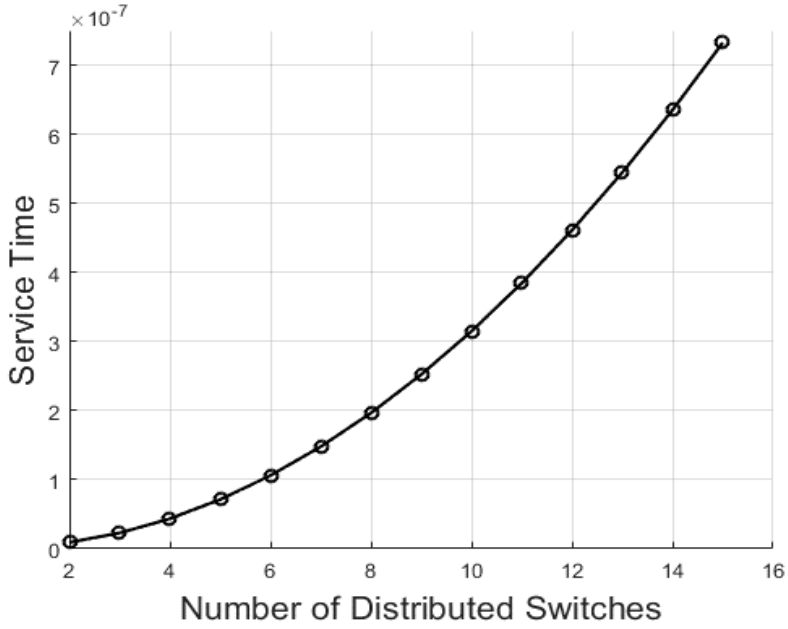
Оваа дистрибуирана околина се опслужува од еден контролер и единствен VNF менаџер, додека податочната рамнина е дистрибуираана на повеќе локации, со еден комутатор на секоја физичка локација. Како што споменавме претходно, правиме претпоставка дека 4% од пакетите одат од комутаторите до контролерот, во OF мрежата, за да се ажурираат табелите на проток и 4% од пакетите што стигнуваат до контролорет одат до VNF менаџерот. Исто така, нашата евалуација претпоставува дека физичките врски помеѓу дистрибуираните локации имаат брзини од 10 Gbps и растојанието помеѓу физичките локации е 100 km. Претпоставката за брзина на врската е направена поради фактот што оваа брзина на мрежни линкови најчесто се користи во пракса, додека физичкото растојание се зема како минимално растојание за одделни податочни центри во различни региони, но овој параметар има многу мало влијание врз целокупната латентност.

Прво, проценуваме какво е влијаниетоо на бројот на физички локации врз времето на престој на пакетите во системот, кога има стабилни стапки на пристигнување кон комутаторите од λ=50000 pkts/sec, стапка на услуга на контролорот од 90000 pkts/sec и стапка на услуга на VNF Менаџерот од 95000 pkts/сек. Слика 26 покажува дека времето

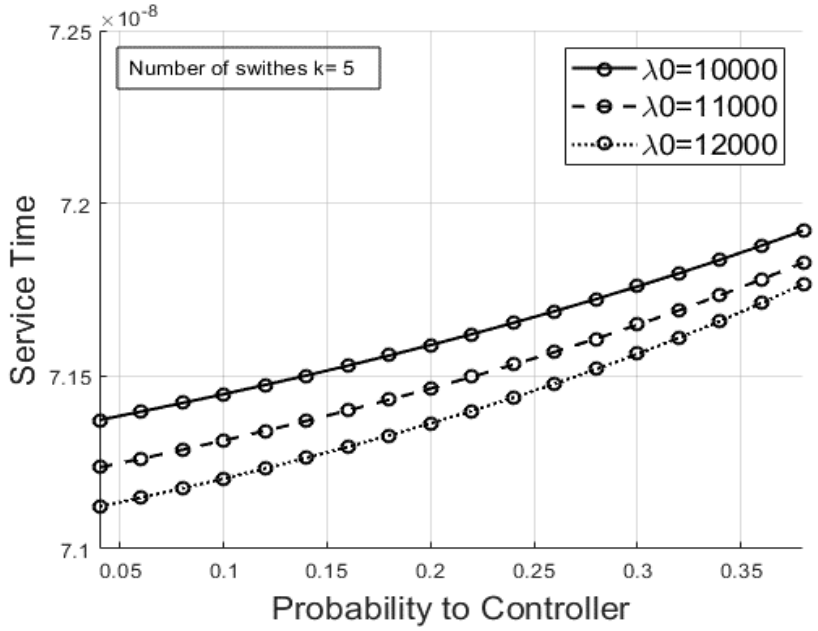
на престој на пакетите расте, како што се зголемува бројот на дистрибуирани комутатори (локации) низ кои е изградена SDN сервисната низа од VNF функции.

Сликите 27, 28 и 29 покажуваат ја покажуваат зависноста на времето на престој на мрежните пакети во системот од веројатноста за packet-in пораки што треба да се испратат до контролерот. Можеме да видиме дека времето на престој на пакетите расте побрзо кога има повеќе физички локации, што е очекувано. Додека кога имаме 5 различни физички локации, доцнењето се зголемува постабилно за различни стапки на пристигнување, кога имаме 15 различни физички локации, доцнењето расте експоненцијално. Слика 29 покажува дека за брзина на пристигнување од 12000 pkts/sec и веројатност за packet-in пораки од околу 0,36 системот колабира и пакетите не можат да се обработуваат со брзината со која пристигнуваат во системот. Исто така, може да се види дека за повисоки стапки на пристигнување, веројатноста за packet-in пораки има поголемо влијание врз времето на престој на пакетот.

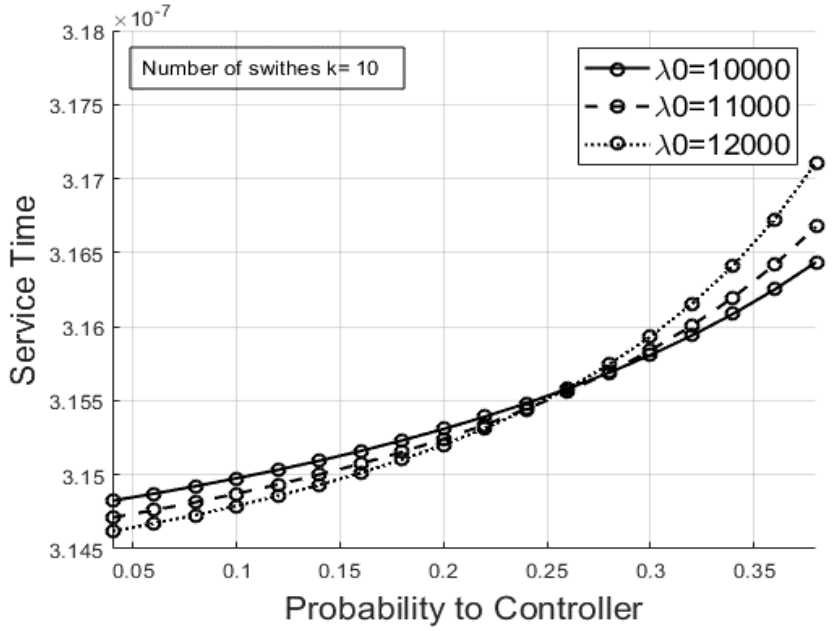
Времето на престој на пакетите во однос на веројатноста пакетите да бидат испратени на различна дистрибуирана локација, со 5, 10 и 15 дистрибуирани локации е дадено на сликите 30, 31 и 32 соодветно. Може да се види дека времето на престој на пакетите расте побрзо бидејќи се зголемува бројот на дистрибуирани локации. Можеме да видиме дека во случај на 15 дистрибуирани локации, дури и со веројатност од околу 16%, дека пакетот ќе оди на друга дистрибуирана локација и со брзина на пристигнување од 12000 pkts/sec, системот колабира и не може да ги опслужува дојдовните пакети. Во овие случаи, треба да се користат комутатори со повисоки стапки на услуги или да се имплементира различна архитектура која нема да користи толку многу дистрибуирани локации. Во нашите симулации, комутаторите имаат брзина на услуга од 90000 pkts/s.



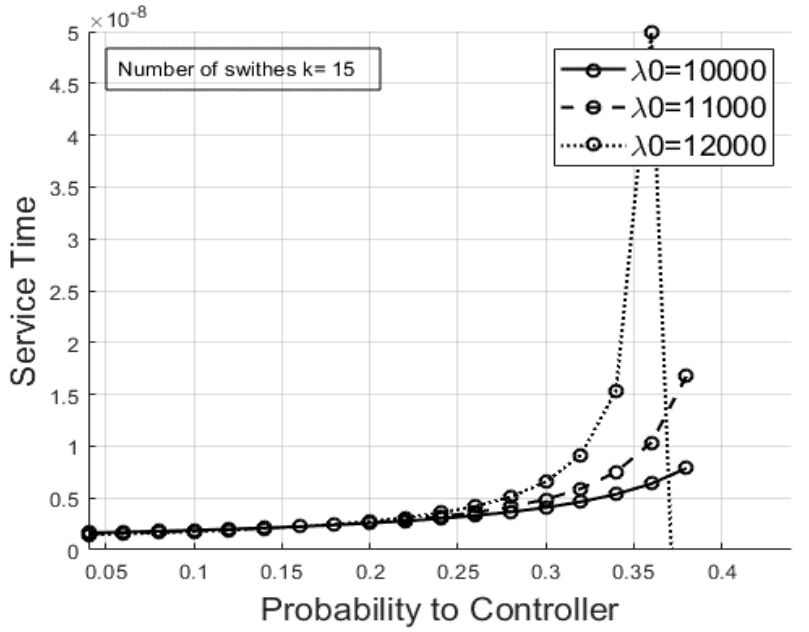
Слика 26: Зависност на сервисното време од бројот на дистрибуирани комутатори



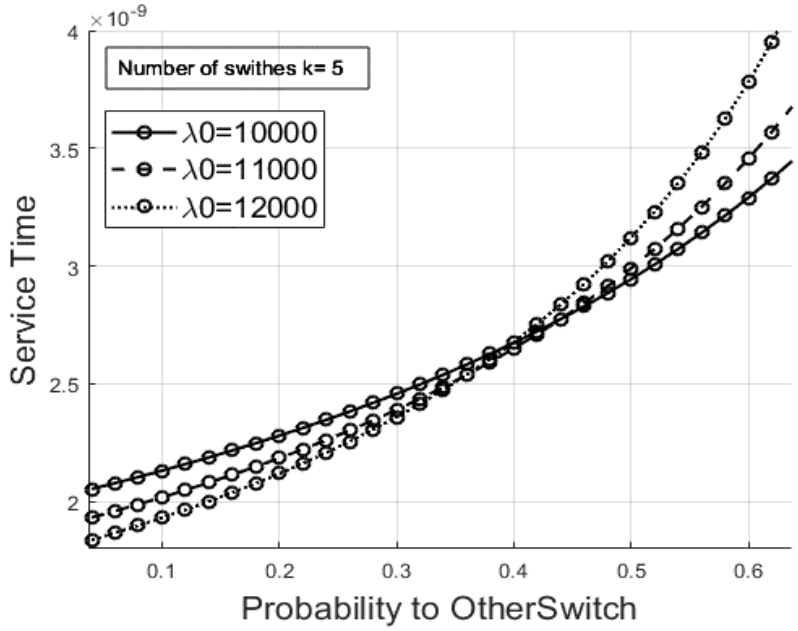
Слика 27: Зависност на сервисното време од веројатноста за OF packet-in кај дистрибуиран систем на 5 локации



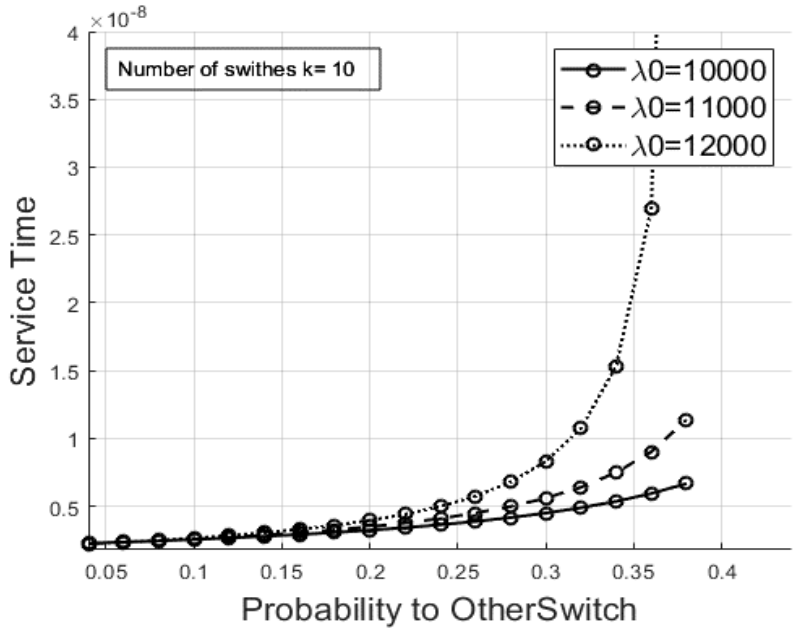
Слика 28: Зависност на сервисното време од веројатноста за OF packet-in кај дистрибуиран систем на 10 локации



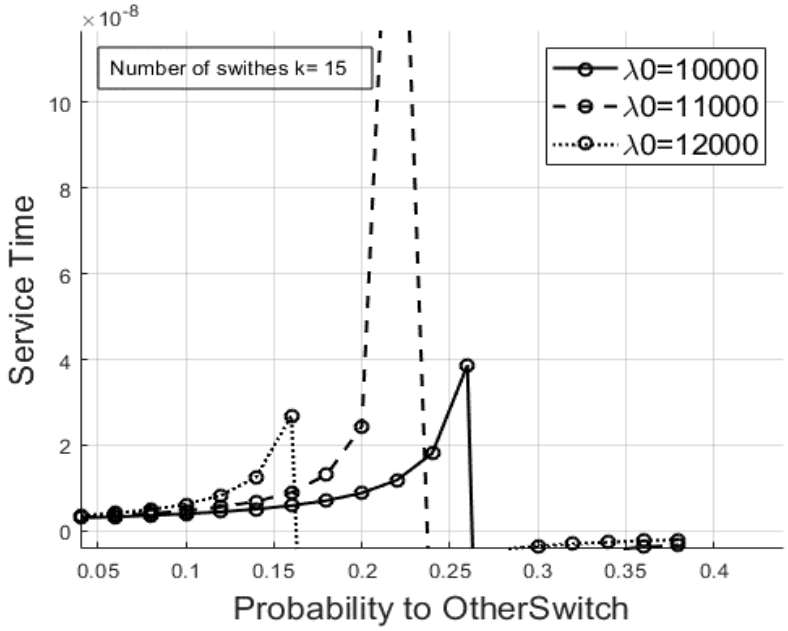
Слика 29: Зависност на сервисното време од веројатноста за OF packet-in кај дистрибуиран систем на 15 локации



Слика 30: Сервисното време кога сервисната низа е на 5 дистрибурани локации – дистрибуирана податочна рамнина



Слика 31: Сервисното време кога сервисната низа е на 10 дистрибурани локации – дистрибуирана податочна рамнина



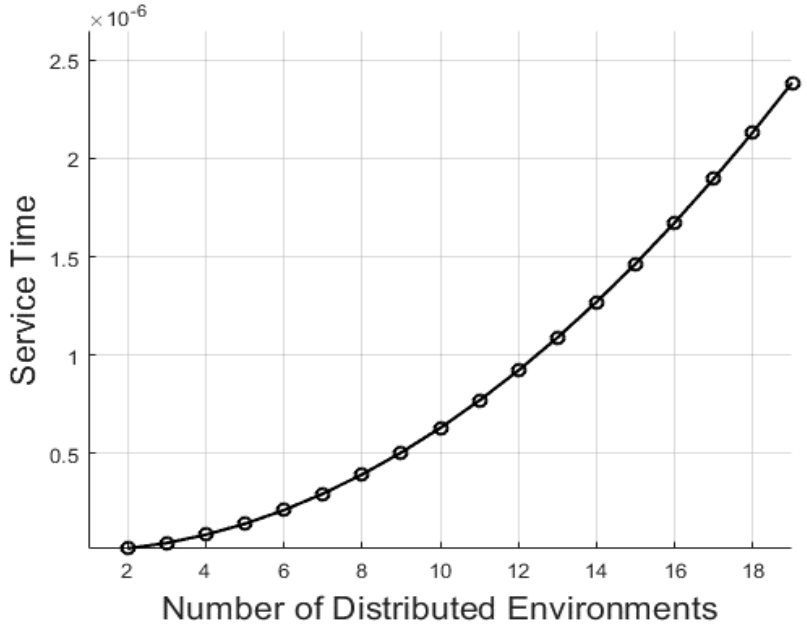
Слика 32: Сервисното време кога сервисната низа е на 15 дистрибурани локации – дистрибуирана податочна рамнина

5.4.3. Евалуација на целосно дистрибуиран систем

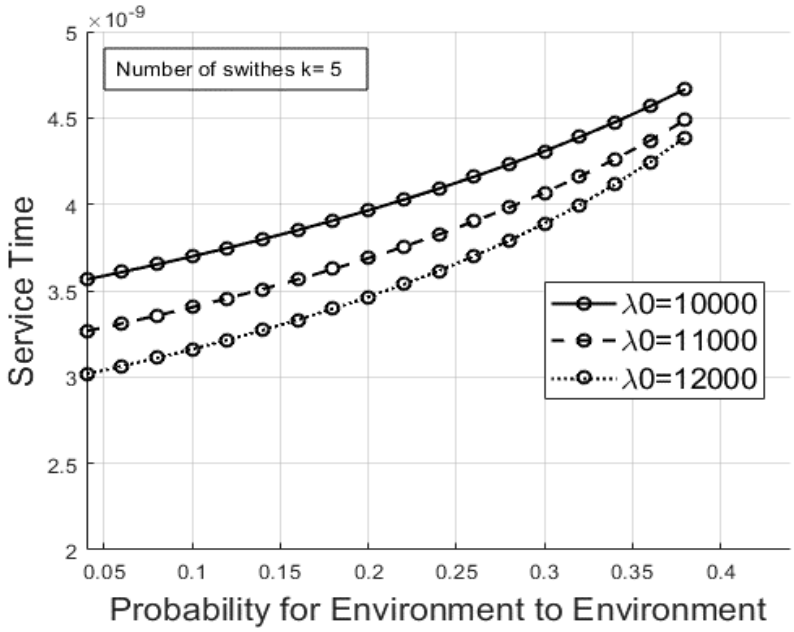
Во целосно дистрибуирана средина, секоја локација има комутатор, контролер и VNF менаџер.

Слика 33 го покажува времето на престој на пакетот во системот (сервисното време) во однос на бројот на дистрибуирани околини, при што земаме фиксна веројатност од 4% во сите случаи: дека пакетот што доаѓа во комутаторот не може да се усогласи во OF табелата и ќе треба да се пренасочи до контролерот, дека пакетот од контролорот ќе треба да пренасочи до VNF менаџерот и дека пакетот ќе оди преку мрежен линк до друга дистрибуирана локација (кога услугата се протега на повеќе локации). Очекувано, сервисното време расте со бројот на дистрибуирани локации.

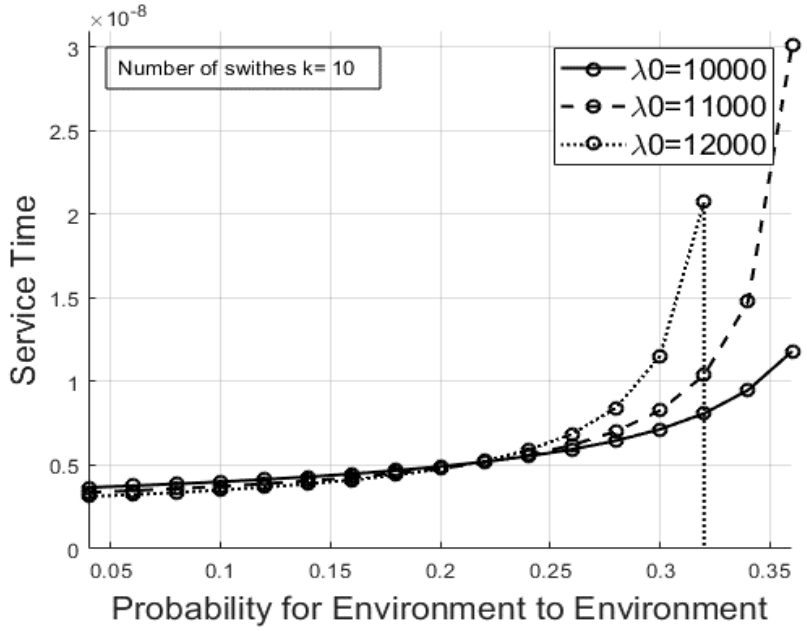
За да го провериме доцнењето предизвикано во системот од различните веројатности дека пакетот ќе оди во повеќе дистрибуирани средини, направивме симулации со 5, 10 и 15 различни дистрибуирани локации. Резултатите се дадени на сликите 34, 35 и 36. Слично на сценариото со еден контролер, времето на престој на пакетите се зголемува со зголемувањето на веројатноста пакетите да одат помеѓу различни дистрибуирани локации.



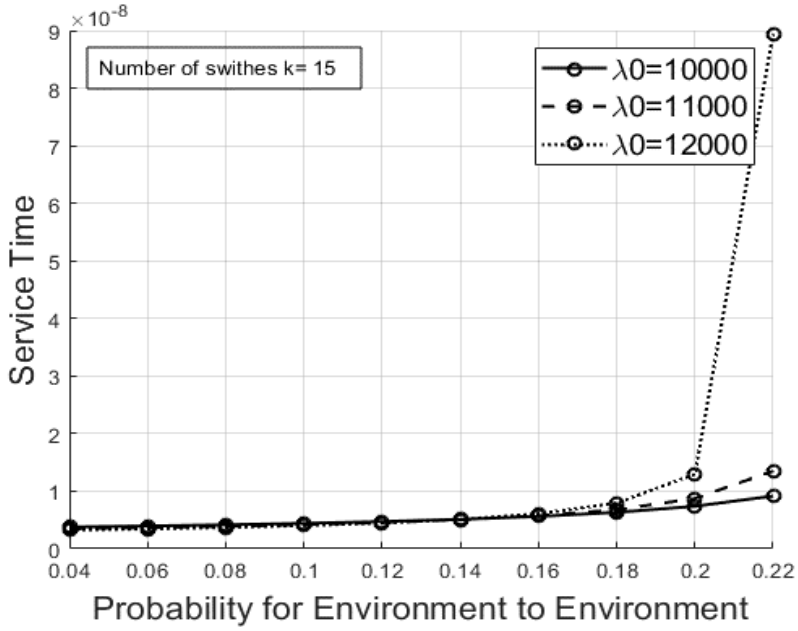
Слика 33: Време на престој релативно на бројот на дистрибуирани локации – целосно дистрибуирана околина



Слика 34: Време на престој кога сервисната низа е дистрибуирана на 5 локации – целосно дистрибуирана околина



Слика 35: Време на престој кога сервисната низа е дистрибуирана на 10 локации – целосно дистрибуирана околина



Слика 36: Време на престој кога сервисната низа е дистрибуирана на 15 локации – целосно дистрибуирана околина

5.5. Споредба помеѓу околина со дистрибуирана податочна рамнина и целосно дистрибуирана околина

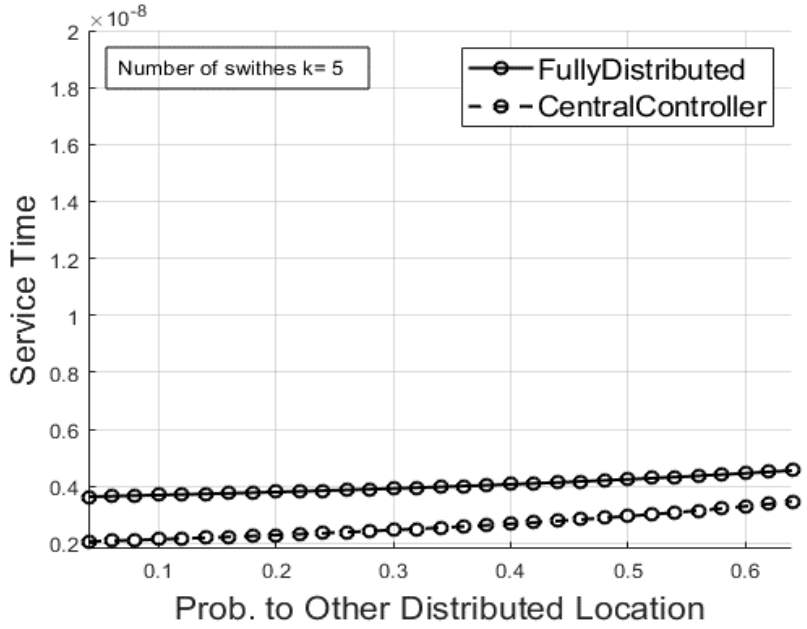
Сега можеме да ги споредиме двете различни сценарија на дистрибуирани средини. Ги проценуваме двата различни системи во сценарио каде што го проверуваме времето на престој на пакетот во однос на веројатноста дека сервисната низа што ја формира услугата се протега низ повеќе дистрибуирани околини, со што ја менуваме веројатноста пакетот да помине низ врска од еден комутатор од една локација, до друг на друга на друга локација. Веројатноста за packet-in пораки, од комутаторите до контролерот и од контролерот до VNF менаџерот се фиксирани на 4%, без оглед на сценариото (со еден или повеќе контролери). Сликите 37, 38 и 39 ја покажуваат зависноста на времето на престој на пакетите од веројатноста за движење на пакети помеѓу комутаторите (дистрибуираните локации) во случај на 5, 10 и 15 дистрибуирани локации соодветно.

Од слика 25 можеме да видиме дека при мал број на дистрибуирани локации архитектурата со централен NFV MANO работи подобро, без оглед на веројатноста за испраќање пакети на други дистрибуирани локации, иако како се зголемува веројатноста, перформансите во однос на временот на престој на пакетите стануваат слични.

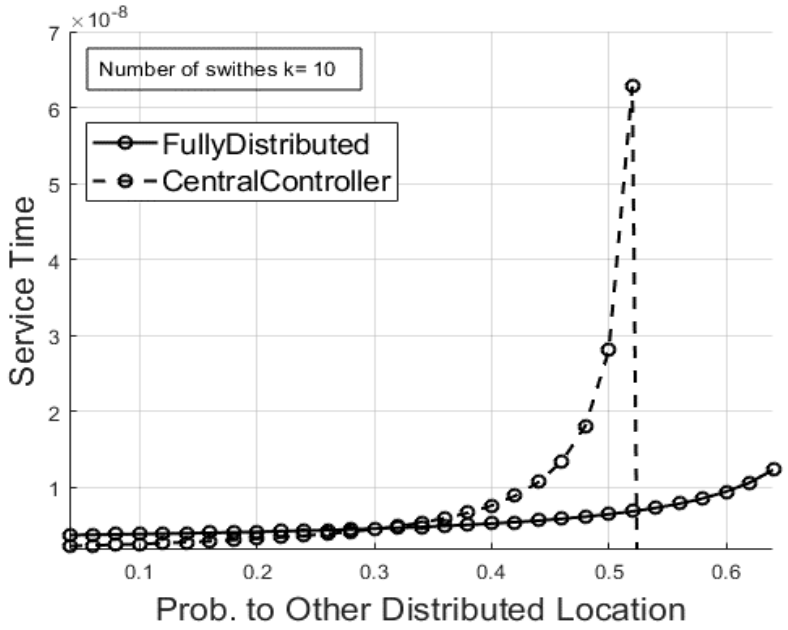
Кога ќе го анализираме сценариото за 10 локации, можеме да видиме дека за помали веројатности на пакети испратени до други дистрибуирани локации, архитектурата со централно NFV MANO работи подобро. Но, како што се зголемува веројатноста, овој пристап се влошува и времето на престој на пакетите расте експоненцијално, додека во целосно распределеното сценарио времето на престој на пакетите е стабилно. При поголеми веројатности за пакети испратени до други дистрибуирани локации, целосно дистрибуираното сценарио станува подобро. Во случај на централно NFV MANO, системот станува нестабилен многу порано отколку во случај на целосно дистрибуирана средина.

Сценариото за 15 локации е слично на претходното. Во овој случај, просечното време на престој во системот со централно NFV MANO оди повисоко над просечното време на престој во системот со дистрибуиран NFV MANO, порано со зголемувањето на веројатноста за испраќање пакети на други дистрибуирани локации. Значи, целосно дистрибуираното сценарио станува подобро при уште помала веројатост за пакети кон друга локација. Ова може да се види визуелно на слика 39.

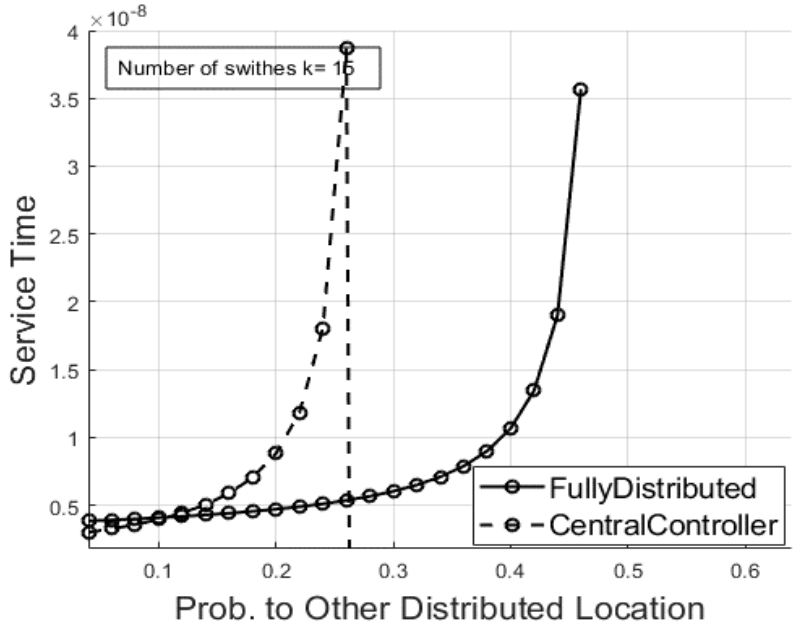
Заклучокот е дека при поголем број на локации (k>5) и при поголема веројатност за испраќање пакети кон друга локцаија, системот кој е целосно дитрибуиран работи подобро. За помал број локации, системот со централно NFV MANO работи подобро. Ваквата анализа овозможува соодветен дизајн на дистрибуираната NFV инфраструктура, според услугите кои работат на таа инфраструктура.



Слика 37: Споредба на времето на престој при 5 дистрибуирани локации



Слика 38: Споредба на времето на престој при 10 дистрибуирани локации



Слика 39: Споредба на времето на престој при 15 дистрибуирани локации

5.6. Заклучоци околу аналитичкото моделирање на дистрибуирана NFV архитектура

Во оваа глава направивме аналитички модели на три различни NFV архитектурни решенија: централизирана околина, околина со дистрибуирана податочна рамнина и централен NFV MANO (симулиран со контролер и VNF менаџер) и целосно дистрибуирана околина со NFV MANO елементи на сите локации. Податочната рамнина ја моделиравме како Џексонска мрежа со сите комутатори како Џексонови сервери. Ги поставивме претпоставките и ги моделиравме сите системски јазли како M/M/1 редици. Равенките за нашите модели го пресметуваат просечното време на престој на мрежните пакети во системите, земајќи го предвид доцнењето предизвикано од архитектонските решенија и мрежните линкови кои ги поврзуваат дистрибуираните локации.

Развивме симулациски скрипти во Matlab со цел да ги оцениме перформансите на системите под различни услови. Ги споредивме двете различни дистрибуирани средини за да видиме која од нив работи подобро и под кои услови. Кога бројот на локации е мал (до 5 дистрибуирани локации), архитектурата со централно NFV MANO работи подобро, без оглед на веројатноста за испраќање пакети на други дистрибуирани локации, иако колку е поголема веројатноста, перформансите стануваат слични. Кога бројот на локации е поголем, можеме да видиме дека за помали веројатности за испраќање пакети на други

дистрибуирани локации, архитектурата со централен NFV MANO работи подобро. Но, како што се зголемува веројатноста, овој пристап се влошува и времето на престој на пакетите расте експоненцијално, додека во целосно дистрибуираното сценарио времето на престој на пакетите е стабилно. Кога стапката на пристигнување на пакетите е поголема, разликата помеѓу две дистрибуирани сценарија е поголема, бидејќи времето на престој на пакетите во околината со централниот NFV MANO се влошува побрзо со зголемувањето на веројатноста за испраќање пакети на други дистрибуирани локации. Во случај на централно NFV MANO, системот станува нестабилен многу порано отколку во случај на целосно дистрибуирана архитектура. При голем број на локации, целосно дистрибуираната архитектура е подобра.

5.7. Употребна вредност на аналитичките модели на дистрибуирана NFV архитектура

Аналитичките модели кои ги развивме може да се користат за подготовка и анализа на потенцијални поставки на услуги каде дистрибуцијата и префрлањето на сметачките капацитети кон на работ се можни и практични. Откривме дека проширувањето на 5G заедно со развојот на NFV архитектурата во насока на дистрибуција кон работ, се овозможувачи на идното паметно поврзување со безбедни, функционални и целосно оптимизирани услуги.

Иако теоретска, нашата анализа е добра основа за подготовка на адекватна архитектура во пракса, имајќи ги предвид различните типови на услуги кои можат да работат на системот. Со анализа на услугите и позитивните и негативните страни на предложените сценарија, во пракса може да се избере најдобриот пристап и да се изгради оптимална NFV базирана мрежна архитектура.

6. Експериментална анализа на влијанието на дистрибуцијата на NFV архитектурата врз латенцијата на мрежните пакети

Во претходната глава изведовме аналитички модели на мрежни системи базирани на NFV архитектура, со акцент на влијанието што го има дистрибуцијата на системот на повеќе мрежни локации врз времето на престој на пакетоте во системот, односно латенцијата на мрежата. Експерименталното практично истражување на дистрибуцијата на NFV е исто така мошне значајна тема која ја разгледуваме. Постојат истражувања кои се фокусирани на експериментално тестирање и мерење на различни карактеристики во рамките на системите базирани на SDN и NFV [108], [109]. Направивме едноставно експериментално тестирање на средина базирана на SDN која треба да симулира можно сценарио за NFV архитектура, распоредено на две географски локации. Нашата намера е да ја предвидиме латентноста на мрежните пакети во услуга која се протега на две дистрибуирани локации и која е изградена со помош на SDN и NFV. Ја споредуваме латентноста на сервисна услуга која е изградена врз SDN сервисна низа која се протега на една локација, при што потрошувачот е блиску до примарната локација и услуга која е изградена врз SDN сервисна низа која се протега на повеќе локации. Кога потрошувачот на услугата е поблиску до секундарната локација, предизвикот е да се направи сигурна, пријателска услуга за корисниците, а притоа да се задржат трошоците на разумно ниво и да се одржат сите придобивки од NFV архитектурата. Нашето истражување е експериментално и треба да им помогне на мрежните архитекти да одлучат кој дизајн на архитектурата NFV е најсоодветен за нивната услуга.

Експериментите што ги правиме се релевантни за систем базиран на дистрибуирана NFV архитектура, но и за сценарио за враќање од катастрофа (disaster recovery), при пад на примарната локација, со цел да се предвиди доцнењето во мрежата предизвикано од промената на локацијата на сервисната услуга.

Слично на претходните експериментални анализи, за да го изградиме нашата тестна околина, користевме алатки кои се добро познати и широко користени за симулација на SDN и NFV, како што е Mininet за градење на виртуелна мрежа и поврзување на услугата, D-ITG како генератор на мрежен сообраќај. Го користевме Ubuntu 18.04 со VirtualBOX инсталиран како хипервизор на двете локации.

Во експерименталната поставка, се потпираме на SDN елементи базирани на протокол за отворен тек (OF) и Open vSwitch што се користи на хипервизорите.

Нашата главна мотивација во оваа глава е експериментално да ја потврдиме очекуваната латентност на мрежните пакети кога услугата работи на дистрибуирана мрежа која се базира на NFV архитектура. Ја споредуваме латентноста во дистрибуираниот систем со латентноста во централизирана NFV архитектура. Експериментираме со повеќе текови на податоци за да го пополниме капацитетот на линковите и да ја споредиме стабилноста на системот во таков случај.

Нашата цел е да дојдеме до заклучоци кои ќе им помогнат на идните истражувачи и мрежни архитекти да ја проценат NFV архитектурата и да направат дистрибуција доколку е потребно, со цел да изградат сигурни и исплатливи услуги со предвидливо однесување надополнувајќи ја претходната математичка анализа.

Заклучоци кои ги изведуваме се значајни од гледна точка на стабилноста на услугата, но исто така и од аспект на трошоците за CAPEX и OPEX кои се важен фактор на одлука при градење услуга во мрежа базирана на TCP/IP, особено во телекомуникациските бизниси каде 5G сè уште се планира или е во фаза на рана имплементација, така што ќе се избере најоптимизираниот и најисплатлив дизајн, во однос на доцнењето на мрежните пакети.

Експерименталните резултати ги користиме за да ги идентификуваме факторите кои влијаат на латентноста во дистрибуирана NFV средина и тоа е главниот придонес на на истражувањето во оваа глава. Резултатите може да имаат различни случаи на употреба [110], за услуги во речиси секоја област, како што се транспортот [111], [112], здравството [113], [114], производството [115], [116], преносот на енергија [117].

6.1.Поврзани испитувања

Аналитичкото моделирање кое го изведовме во глава 5 е само една од насоките во испитувањето на сложени системи и анализа на поедини карактеристики. Експерименталниот метод е сосема поинаков правец кој треба да ги потврди

математичките модели. Двата правци се надополнуваат и се често употребувани од академската и инженерската заедница.

Марио Ди Мауро и сор. [118] вршат стохастичка проценка на софтверизирана IMS (softIMS) архитектура со две главни фази: анализа на перформансите со метод на декомпозиција на мрежни редици и проценка на достапност, користејќи ја методологијата Stochastic Reward Net. Тие дизајнираат тест околина користејќи ја платформата Clearwater, за да го карактеризираат однесувањето на softIMS во однос на настаните од дефект/поправка и да извлечат сет од оптимални конфигурации кои задоволуваат дадени барања за достапност, а притоа да ги минимизираат трошоците за распоредување на мрежните елементи кои и кај нова, како и во нашата тестна околина, претставуваат SDN хост елементи. Ние, исто така, развивме тестна околина користејќи збир на добро познати и широко користени алатки, како што се Mininet, D-ITG, Open vSwitch, за да ги истражиме мрежните текови во дистрибуирана NFV архитектура.

[119] предлагаат архитектура базирана на мрежни слоеви за 5G мобилни мрежи што вклучува радио пристапна мрежа во облак (C-RAN), мобилно сметање на работ (MEC) и податочен центар во облак. Мрежата е моделирана со користење на систем на мрежни слоеви базиран на теорија на редици, кој може да се користи за да се изведат главните индикатори за перформанси како што се искористеноста на процесорот, пропусната моќ на системот, стапката на испади на системот, просечниот број на барања за пораки, просечното време на одговор и просечното време на чекање на мрежните пакети. Обезбедени се квантитативни примери за да се покаже како овој модел може да се примени за да се проценат перформансите на системот и трошоците за систем за мрежно раслојување кај мобилните 5G мрежи, како и бројот на C-RAN и MEC процесирачки јадра кои се потребни под различни услови кај 5G сообраќајот.

S. Mustafiz и сор. [120] предлагаат пристап за моделирање на апликативни процеси каде NFV систем се смета за апликативен домен на работа. За таа цел ја користат апликацијата MAPLE [121] за математичка анализа и Papyrus [122] за дизајнирање на апликативните процеси, а моделирањето на процесите се врши со дијаграми на активност на UML (Unified Modeling Language). Наша цел се системи базирани на NFV архитектура, но акцентот е на нивната дистрибуција, при што користиме експериментален пристап.

Авторите на [123] создаваат целосно оперативно експериментално сценарио, со главна цел да се интегрираат различните достигнувања на проектот H2020 5G-RANGE, за да можат да се испробаат заедно во случај за користење 5G мрежа. Сценариото опфаќа (i) нова радио пристапна мрежа која цели на пропусен опсег од 100 Mb/s во радиус на ќелија од 50 km и (ii) мрежа на мали беспилотни воздушни возила (SUAV). Овој сет на SUAV уреди е овозможен од NFV, над кој може автоматски да се распоредат виртуелни мрежни функции (VNF) за поддршка на повремени мрежни комуникации надвор од опсегот на 5G радио ќелиите. Целото распоредување подразбира употреба на виртуелна приватна мрежа која овозможува прелиминарна валидација на компонентите од нивните соодветни оддалечени локации и поедноставување на нивната последователна интеграција во еден локален демонстратор, конфигурација на потребните GRE/IPSec тунели, интеграција на новите 5G физички, MAC и мрежни слоеви и валидација на гласовните и податочните услуги. Експериментот е наменет за рурални подрачја, кои немаат пристап до интернет. Ова сценарио е многу покомплицирано од нашето, но ја докажува подобноста на NFV архитектурата при градењето на 5G базирани мрежи и потврдува дека ваквата констелација има неограничени можности.

Во [124] се дискутира за ограниченоста на експерименталните средини во однос на реалните околини базирани на NFV архитектура. Се предлага платформа за дизајнирање и тестирање на NFV инфраструктура и едноставно креирање на низи од виртуелни мрежни функции. Платформата е емулатор и е означена како NIEP, со намена да се провери одреден мрежен дизајн пред да се изгради во пракса. Идејата на нашето експериментирање е слична, да се покаже влијанието на мрежниот дизајн и дистрибуцијата на NFV базиранат мрежа, врз движењето и каснењето на мрежните пакети.

Molka Gharbaou и сор. [125] вршат експериментална студија во која се предлага систем за оркестрација на виртуелни мрежни функции кои формираат соодветна SDN сервисна низа во рамките на мрежа изградена врз дистрибуирана NFV архитектура. Нивната експериментална околина репродуцира типична 5G мрежа во која виртуелните функции се поставени на дистрибуирани локации, на мрежниот раб. Системот за оркестрација е наречен LASH-5G и е изграден како интеграција меѓу различни решенија за оркестрација и распоредување во околини на облак. Има за цел да обезбеди ниска латентност, адаптивна и сигурна оркестрација на сервисна низа распоредена низ

податочни облаци и локални мрежни ресурси, меѓусебно поврзани преку SDN. Авторите вршат проценка на ефективноста на предложениот пристап за оркестрација. Во нашата експериментална околина е спроведен сличен експериментален пристап, но акцентот е врз доцнењето на мрежните пакети во рамките на дистрибуираната околина, а не на оркестрацијата на виртуелните мрежни функции.

Во основа, нашата работа е чисто експериментална и се фокусираме првенствено на латентноста на мрежните пакети во рамките на дистрибуираниот систем. Фокусот е на факторите кои можат да влијаат на времето на престој на пакетите во системот, со цел да се посочат можните дистрибуирани NFV имплементации. Експерименталната околина е детален објасната во следната точка.

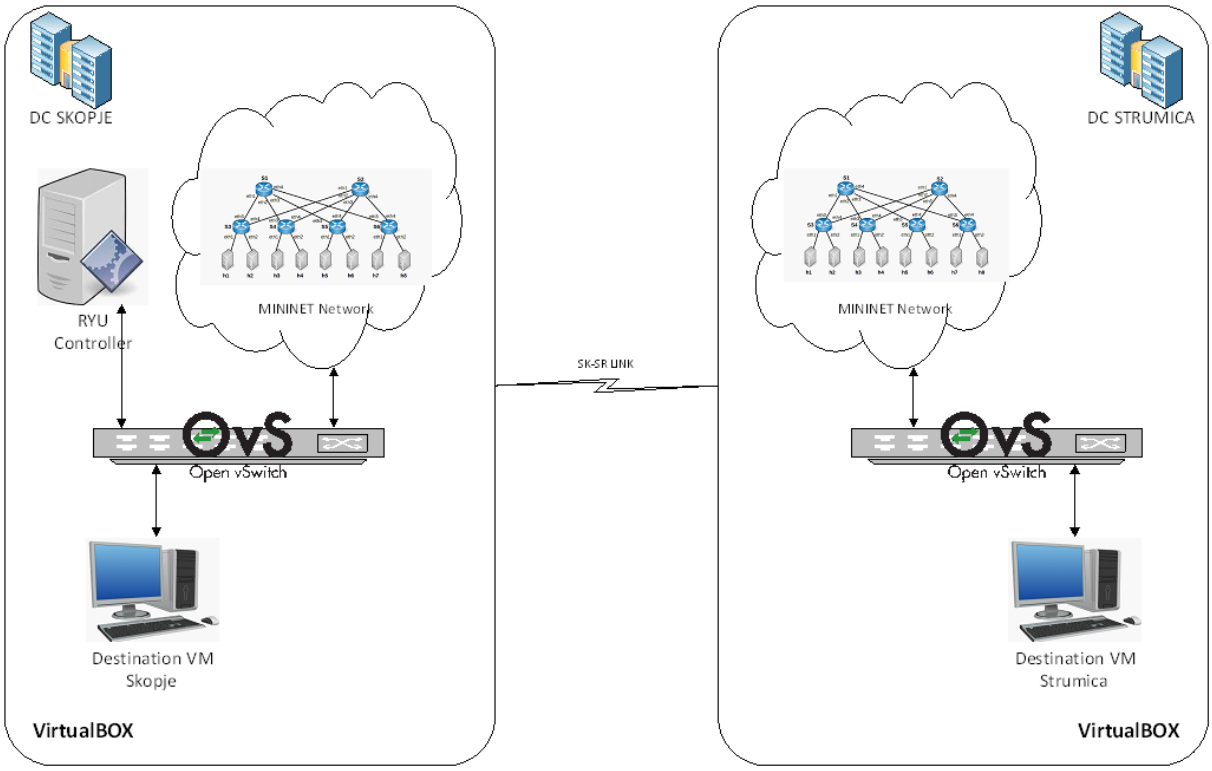
6.2.Експериментална околина на дистрибуиран NFV систем

Експерименталната околина се заснова на две физички одвоени локации кои се оддалечени 160 километри една од друга. Тие се поврзани со линк со брзина од 10 Gbps. Пропагационата латентност е многу мала, додека трансмисионата латентност предизвикана од линкот е главниот фактор што влијае на целокупното доцнење на мрежните пакети кај мрежните сервисни низи кои се протегаат на двете локации.

На двете локации имаме хипервизор базиран на Ubuntu 18.04 OS и VirtualBox. Серверите што се користат како хипервизори имаат мрежни интерфејси од 1Gbps. Се користи Open vSwitch (OVS). Мрежниот симулатор Mininet е инсталиран на секоја локација во одделна виртуелна машина. Се користи за создавање SDN мрежи со повеќе хостови, комутатори и линкови меѓу нив. Мрежите имаат приватни IP адреси. Тие комуницираат една со друга користејќи GRE тунелирање, во рамките на OVS комутаторот. Симулираните мрежи се управуваат со помош на Ryu Controller, кој се наоѓа на првата локација и се користи за двете локации, во дедицирана виртуелна машина.

Генератор на дистрибуиран интернет сообраќај (D-ITG) се користи за генерирање на TCP и UDP мрежен сообраќај. D-ITG произведува сообраќај на ниво на пакети, реплицирајќи соодветни стохастички процеси за случајните променливи IDT (Inter Departure Time) и PS (Packet Size).

Спроведувавме експерименти со 4, 8, 12 и 16 истовремени мрежни текови на податоци. Беа направени 30 различни експериментални итерации за секоја ситуација соодветно. Итерациите беа спроведени во временски интервали од 20 секунди до 10 минути следејќи ја дистрибуцијата на Поасон. Го пресметавме средното време на испорака на пакети за секој експеримент. Просечниот број на заробени пакети беше 1.862.225. Ние користевме стандардни информации во носивоста на генерираниот сообраќај како што е дефинирано од D-ITG. Користевме и TCP и UDP сообраќај. Времето меѓу поаѓање во тековите беше поставено да има нормална распределба. На слика 40 е прикажана експерименталната околина.

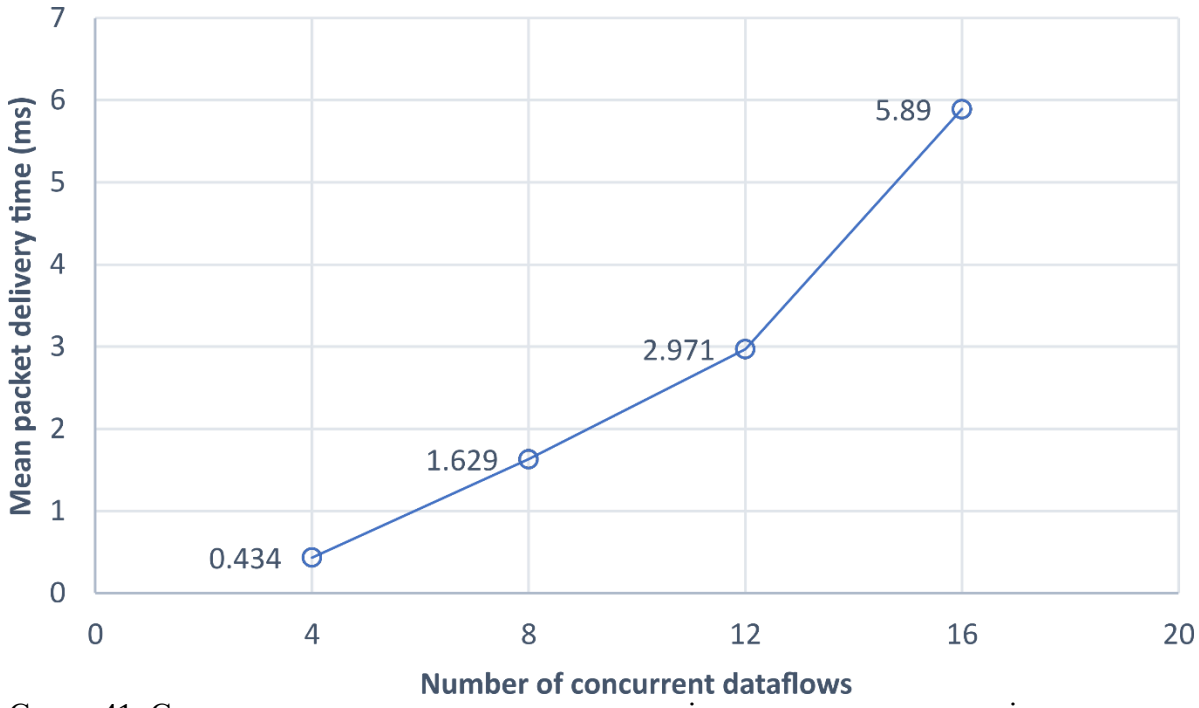


Слика 40: Експериментална околина за D-NFV систем

6.3.Резултати од експериментите

Нашиот прв експеримент беше со мрежна патека која симулира сервисна низа што се протега само на една локација. Создадениот сообраќај е целосно во рамките на примарната локација, со дестинација поставена на локалната виртуелна машина, симулирајќи корисник во непосредна близина на давателот на услугата. Како што е

очекувано, бројот на истовремени текови на податоци има влијание врз средното време на испорака на пакети, но порастот на времето за испорака на пакетите е мал.



Слика 41: Средно време на испорака на пакети кај сервис на една локација

Табела 10 ги прикажува резултатите од средното време на испорака на пакети земени од 30 мерни повторувања за секој експеримент, користејќи 4, 8, 12 и 16 истовремени текови на податоци. Слика 41 графички ги прикажува резултатите.

ТАБЕЛА 10: СРЕДНО ВРЕМЕ НА ИСПОРАКА НА ПАКЕТИ КАЈ СЕРВИС НА ЕДНА ЛОКАЦИЈА.

Flows	***4***	***8***	***12***	***16***
Mean packet delivery time(ms)	0,434	1,629	2,971	5,86

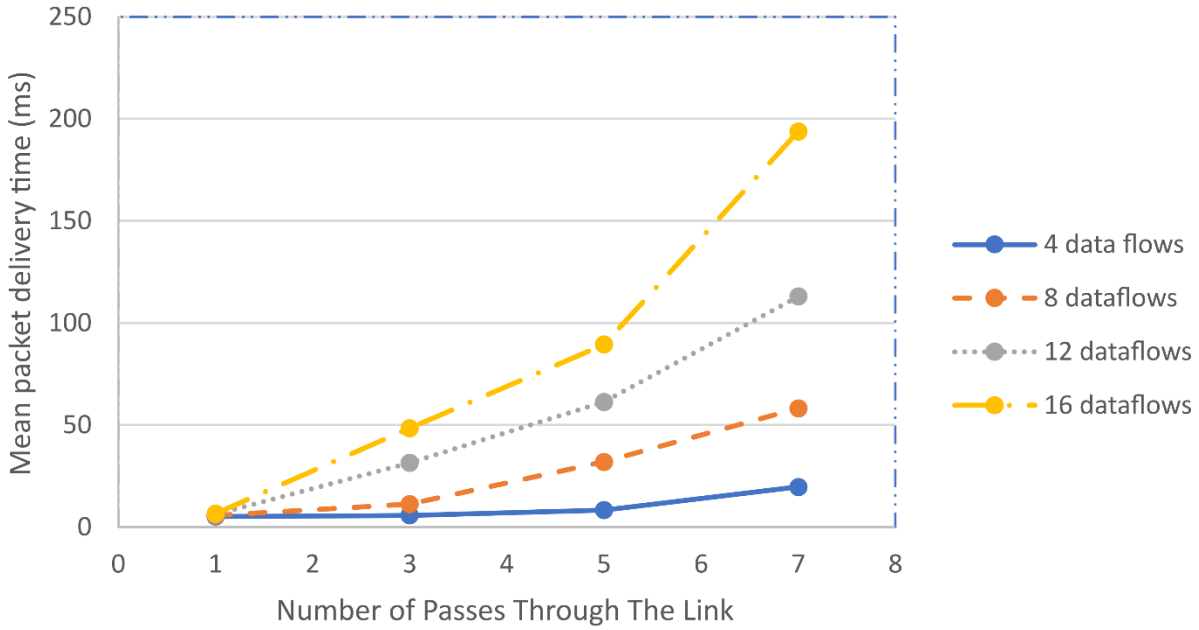
Кога сервисната низа се протега на две локации, со некои од VNF на примарната, а некои на секундарната локација, мрежните пакети може да течат помеѓу двете локации повеќе пати. Во ова сценарио го меревме средното време за испорака на пакети со симулирање на сообраќај што тече 1, 3, 5 и 7 пати преку линкот што ги поврзува

дистрибуираните околини. Експериментот го направивме 4 пати, повторно користејќи 4, 8, 12 и 16 паралелни текови на податоци. Изворот на мрежниот сообраќај е секогаш на примарната локација, додека дестинацијата (на пример, потрошувачот) е секогаш на секундарната локација. Просечното време за испорака на пакети беше пресметано врз основа на 30 повторувања за секоја ситуација.

ТАБЕЛА 11: СРЕДНО ВРЕМЕ НА ИСПОРАКА НА ПАКЕТИ КАЈ СЕРВИС НА ДВЕ ЛОКАЦИИ

Passes through the link	***Concurrent flows***			
	4	***8***	***12***	***16***
1	5,121ms	5,67ms	6,195ms	6,634ms
3	5,72ms	11,21 ms	31,461ms	48,389ms
5	8,432ms	31,961ms	61,31ms	89,455ms
7	19,651ms	58,12ms	112,942ms	193,82ms

Како што покажуваат резултатите од Табела 11, влијанието од преминувањето на пакетите низ линкот има значително влијание врз средното време на испорака на пакетите, а влијанието е поголемо за поголем број истовремени текови, што се очекува. Визуелно ова може да се види на Слика 42.



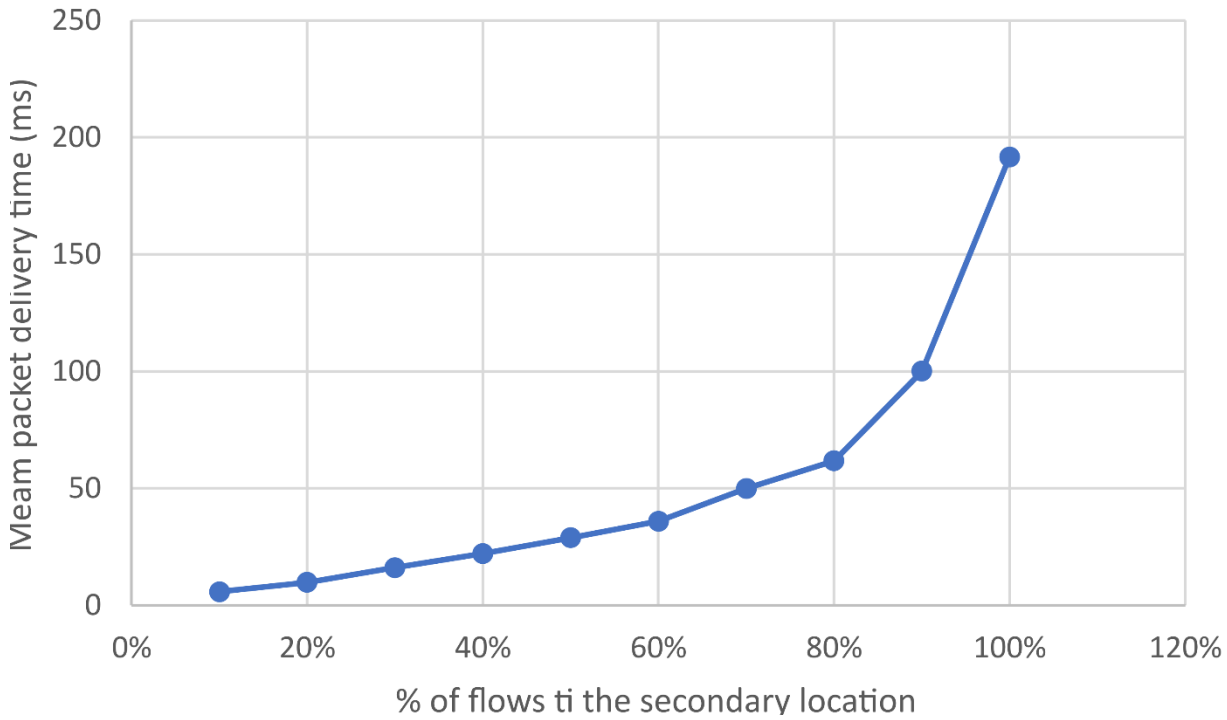
Слика 42: Средно време на испорака на пакети кај сервис на две локации

Ако ги споредиме сценаријата, можеме да заклучиме дека просечното време на испорака на пакети расте експоненцијално и во двата случаи, но во случајот на две локации, латентноста на мрежата е многу поголема, достигнувајќи скоро 200 ms, додека во сценариото за една локација латентноста е значително помала. Ова доцнење е предизвикано главно поради сетирањата на комутаторите кои работат во режим на „обликување на сообраќајот (traffic shaping)“ кој што е вообичаен кога сообраќајот е и TCP и UDP базиран. Наспроти ова, друг вообичаен режим на работа на комутаторите е „водење на сообраќајот (traffic policing)“ при што се врши отфрлање или прекласификација на мрежните пакети. Обликувањето на сообраќајот се обидува да го направи сообраќајот усогласен со одредена стапка (traffic rate) со одложување на пакетите во бафер и нивно испраќање во моментот кога „просторот“ станува достапен. Ова докажува дека близината на VNF кои се дел од сервисната низа и крајниот потрошувач има значително влијание врз латентноста на мрежата, со што се потврдува дека мрежните архитекти мора внимателно да размислат за поставувањето на мрежните елементи при дизајнирањето на услугата низ мрежата.

Како трета експериментална поставка, истражуваме ситуација во која изворот на пакетите е секогаш на примарната локација, додека дестинацијата може да биде на примарната или секундарната локација. Тестните итерации се засноваат на одреден процент од сообраќајот што оди до секундарните локации, мерејќи го средното време на испорака на пакети кога 10%, 20% и до 100% од тековите одат до секундарната локација. Користевме 40 истовремени текови на податоци. Кога целиот сообраќај минува низ линкот, мрежните интерфејси на хипервизорите достигнуваа искористеност и до 97%. Резултатите може да се видат во Табела 12 и Слика 43.

ТАБЕЛА 12: СРЕДНО ВРЕМЕ НА ИСПОРАКА НА ПАКЕТИТ КОГА ОДРЕДЕН ПРОЦЕНТ НА СООБРАЌАЈ ОДИ НИЗ ЛИНКОТ

% of flows through the link	***10%***	***20%***	***30%***	***40%***	***50%***	***60%***	***70%***	***80%***	***90%***	***100 %***
Mean Packet delivery time (ms)	***5,86***	***9,82***	***16,13***	***22,07***	***28,91***	***35,87***	***50,05***	***61,81***	***100,12***	***191,58***



Слика 43: Средно време на испорака на пакети релативно на процентот на пакети кои поминуваат низ линкот.

Резултатите од претходниот експеримент може да се искористат и за сценарио за враќање од катастрофа (disaster recovery), каде што ќе претпоставиме дека примарната локација има испад, а секундарната локација е единствената локација што ги обезбедува VNF функциите и сервисната низа врз која е изградена услугата. Потрошувачот (дестинацијата) е во непосредна близина на примарната локација. Претпоставуваме дека линкот функционира, што може да се третира како ситуација во која врската не е засегната од катастрофата, или секундарна врска постои и е во функција. Нема да го земеме предвид времето потребно за повторно воспоставување на линкот бидејќи тоа може да варира во зависност од ситуацијата и може да се третира како константа што ќе воведе дополнителна мрежна латентност. Тоа е сценарио во кое 100% од мрежните текови одат од секундарната, назад кон примарната локација.

Од резултатите можеме да видиме дека иако бројот на мрежните пакети расте линеарно, латентноста на мрежата расте експоненцијално. Резултатите може да бидат важни за мрежните архитекти кои можат да имаат корист од можноста за дистрибуција на услугата на повеќе географски одвоени локации, имајќи предвид дека близината на мрежните елементи до крајниот потрошувач на услугата има големо влијание врз

перформансите на мрежата. Но, ако сообраќајот на една услуга е пренасочен на повеќе локации, латентноста на мрежата е многу засегната. Со ова може да се дизајнира оптимално сценарио од точка на перформанси на латентност на мрежата, но и од точка на цена на инфраструктурата.

6.4.Заклучок од експериментите

Направивме експериментална околина за тестирање и симулација на систем заснован на SDN и дистрибуирана NFV архитектура, со цел да се оцени латентноста на мрежата што ќе се појави под различни околности. Користивме две географски оддалечени локации поврзани со линк кој има пропусен опсег од 10 Gbps. Физичките комутатори што ги поврзуваат локациите користат политика за обликување на сообраќајот и линкот нема поставен QoS. Го пресметувавме средното време за испорака на пакети со извршување на 30 повторувања од секој експеримент.

Како што се очекуваше, експериментите го докажаа заклучокот дека кога услугата се протега на повеќе локации, линкот меѓу нив има значително влијание врз латентноста на мрежните пакети. Бројот на поминувања на пакетите низ линкот има значително влијание врз целокупното време на испорака на пакети.

Заклучоците што ги направивме може да се користат од истражувачи и мрежни архитекти за планирање на инфраструктурата и за предвидување на латентноста на услугите кои работат врз таа инфраструктура. Доближувањето на мрежните елементи до потрошувачот е од суштинско значење доколку латентноста на мрежата е од голема важност. Овие сценарија се исклучително важни кога се користи 5G мрежа за имплементација на услугите. Распределбата на сервисната низа на повеќе локации може да има финансиска смисла ако латентноста предизвикана од неа е внимателно пресметана и не влијае на услугата. Заклучуваме дека дистрибуцијата на NFV архитектурата може да биде корисна за доближување на услугата до крајниот потрошувач, но кога сообраќајот треба да минува низ повеќе податочни центри поставени на различни локации, користа од близината на услугата до крајниот корисник може да биде уништена.

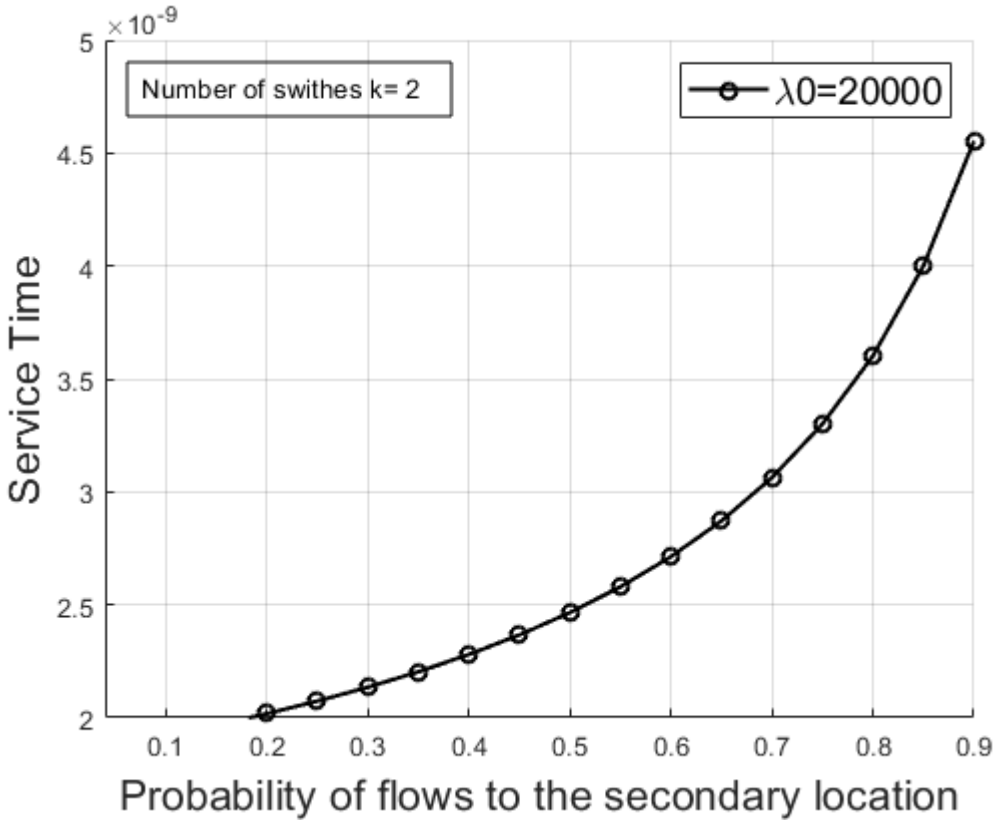
6.5.Споредба на експериметалните и аналитичките резултати

Експериментот е изведен на систем распространет на две дистрибуирани локации, при шти контролерот е на примарната локација. Ова ќе го искористиме за да направиме споредба со аналитичкиот модел на мрежа изградена користејќи SDN сервисни низи поставени врз NFV архитектура во случај кога MANO елементите се централизирани, односно на примарната локација и ги опслужуваат сите локации. Аналитичкиот модел кој го изведовме е универзален и може да се искористи за број на дистрибуирани локации по избор, но за споредба ќе земеме дека има само две локации, за да соодветствува на експерименталната околина.

Направена е MatLab симулација на аналитички модел со две локации, при што е земено дека линкот е со големина од 1GBps, а просечната големина на пакетите е 1400bytes. Иако големината на пакетите може да варира значително, во зависност од апликацијата или системот каде се одвива сообраќајот, повеќе автори [126][127] и комуникациски компании [128] експериментално утврдуваат дека во моментов просечната големина може да се смета дека е 1400 бајти.

За спроведување на аналитичката пресметка, земено е дека во системот со 2 околини (2 комутатора) линкот е со пропустност од 1Gbps, стапка на пристигнување од $\lambda=10000$ пакети во секунда, максимална искористеност (utilization) на комутаторите од $\rho_0 = 90000$ пакети во секунда, максимална искористеност на контролерот од $\rho_c = 50000$ пакети во секунда и максимална искористеност на VNF менаџерот од $\rho_v = 2000$ пакети во секунда. Како и претходно земаме дека 4% од пакетите се упатуваат до комутаторите до контролерот и 4% од пакетите што стигнуваат до контролерот се упатуваат до VNF менаџерот.

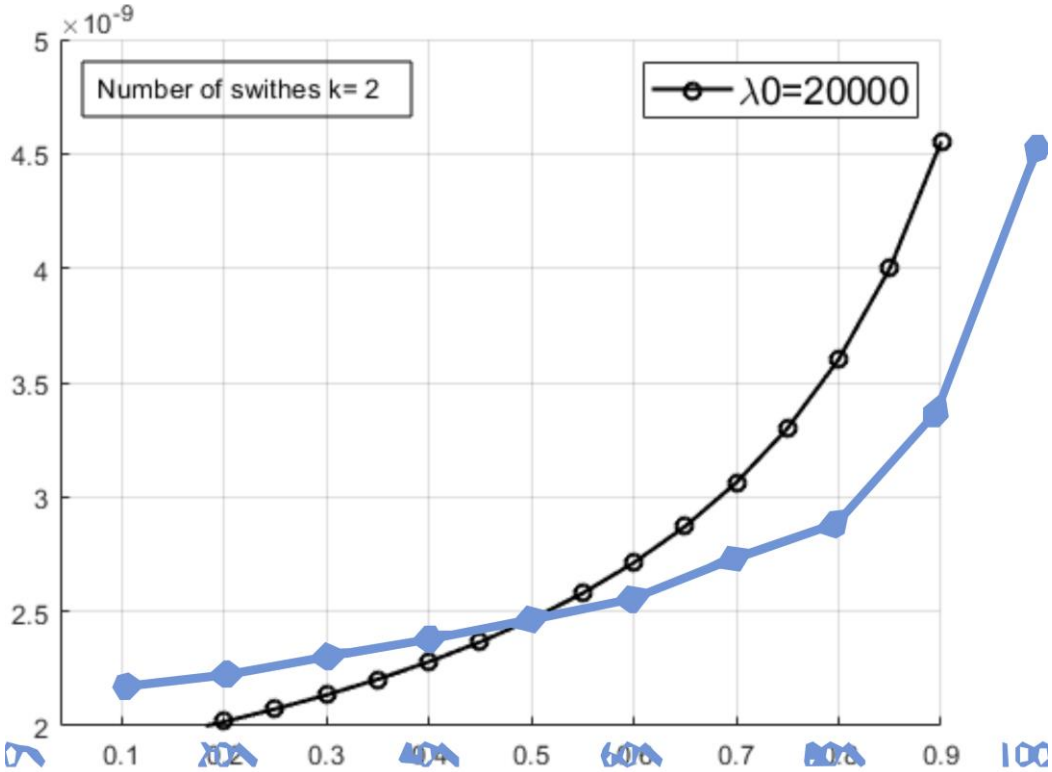
Најпрвин преку аналитичкиот модел, ќе го видиме просечното време што пакетот го поминува во рамките на сервисната низа, која може да се протега на две локации, во зависност од веројатноста пакетот да поминува низ линкот. Веднаш се забележува тенденцијата на кривата која е експоненцијален раст во ситуација кога веројатноста за поминување од една на друга локација расте линеарно. Ако ги споредиме сликите 39 и 40 се гледа огромна сличност помеѓу нив. Во експериметалниот случај, при помали веројатности кривата е порамна, но при повисоки и таа се стреми кон високо сервисно време.



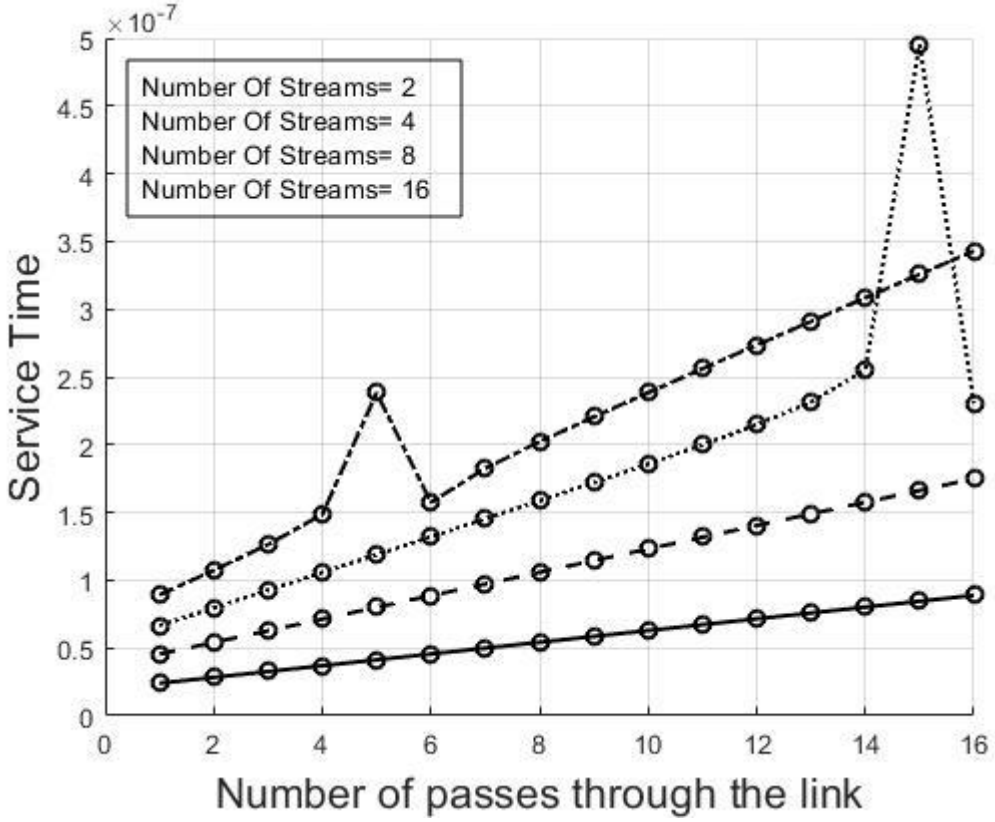
Слика 44: Аналитичка пресметка на просечното време што пакетот го поминува во рамките на сервисната низа, релативно на процентот на пакети кои поминуваат низ линкот.

Ако ги преклопиме слика 43 и 44 една врз друга, може визуално да ги споредиме. Тоа е направено во слика 45.

Втората споредба која може да ја направиме помеѓу аналитичкиот модел и експерименталните истражувања е да разгледуваме број на поединечни мрежни текови кои поминуваат низ линкот и број на пати што поминуваат низ самиот линк. Станува збор за сложени сервисни низи кои се протегаат на двете локации и сообраќајот теоретски може да поминува повеќе пати низ самиот линк. Соодветната експериментална поставка, односно експерименталните резултати се дадени на слика 38. Слика 46 е добиена од аналитичкиот модел со централизирана MANO околина, при што се земени 2, 4, 8 и 16 мрежни текови, при што секој однив поминува одреден број пати низ линкот што ги поврзува локациите. Останатите параметри се земени идентично како во претходниот случај.



Слика 45: Споредба на аналитичкиот модел и експерименталните резултати при соодветна веројатност за пакети кон втората локација



Слика 46: Резултати од аналитичкиот модел за средно време на испорака на пакети кај сервис на две локации со соодбветен број на мрежни текови

Ако ја анализираме слика 46, се гледа дека доколку имаме голем број на мрежи текови, односно 16 во нашиот случај, системот станува нестабилен и не може да го опслужува сообраќајот, доколку секој тек поминува низ линкот 5 пати. Кај експериментот, гледаме дека тоа ќе се случи при 16 истовремени текови кои низ линкот поминуваат 7 пати, но имајќи ги предвид претпоставките кои ги воведовме, за големината на пакетите, растојанието помеѓу околините и искористеноста на елементите, резултатите како и изгледот на добиената крива се доволно блиски и покажуваат сличности, што ја потврдува веродостојноста на аналитичкиот модел. Слични резултати се добиваат и за 2, 4 или 8 мрежни текови. Гледаме дека за 8 мрежни текови, системот станува нестабилен, доколу секој од нив помине низ линкот по 15 пати. За помал број на паралални мрежни текови, аналитичкиот модел покажува дека системот е стабилен и при поголем број на минувања на тековите низ мрежниот линк.

Заклучокот од споредбата е дека аналитичките модели може да се споредат со експериментално добиените резултати и истите може да се користат во пракса, со соодветно подеување на претпоставките во моделот.

7. Заклучок

Телекомуникациската индустрија веќе распоредува мрежи базирани на 5G стандард, но процесот има многу предизвици, од технолошка перспектива, но и од финансиска гледна точка. Процесот е неизбежен бидејќи густината на корисници се зголемува со неверојатна брзина, но со непредвидливо групирање, поради мобилноста на корисниците. Се очекува дека потрошувачката на мрежен сообраќај ќе се зголеми експоненцијално со масивната машинска комуникација (massive machine type communication - mMTC) [135] што ќе биде наметната од пенетрацијата на Интернет на нештата, а со тоа и потребата за зголемен капацитет на сообраќајот, како на 5G радио пристапната мрежа, така и на основната јадрена 5G мрежа. Но, предизвикот дополнително се зголемуна ако ги имаме во предвид проблемите со потрошувачка на електрична енергија, како и обезбедување ниски цени на услугите достапни на потрошувачите.

Последната деценија беше фокусирана на технологиите за виртуелизација кои беа двигател за услугите во облаци, како приватни, така и јавни. Повеќето од услугите се виртуелизирани со користење на виртуелни машини, проследено со контејнеризација, што дополнително ги подобри сценаријата за користење, овозможувајќи сложени услуги од крај до крај, со намалено економско влијание предизвикано од економијата на обем. Концептите за вмрежување не се исклучок од овој тек. Софтверски дефинираните мрежи овозможија одвојување на контролната рамнина и податочната рамнина и значително ја подобрија оркестрацијата на мрежите, како изградени локални, така и во облак. Архитектурата за виртуелизација на мрежни функции овозможи функционирање на виртуелни на мрежни функции на регуларен хардвер, формирање и управување на SDN сервисни низи, подобрувајќи го финансискиот аспект на новите мрежни концепти, но исто така овозможувајќи агилен пристап кон градење скалабилни и прилагодливи мрежни услуги. Иако се различни, SDN и NFV се надополнуваат еден со друг и станаа клучни технолошки овозможувачи на 5G мрежите. Токму затоа во овој труд се разгледувани овие два концепти од неколку аспекти: можноста за класификација на мрежниот сообраќај во мрежите кои се високо виртуелизирани и кај кои класичните методи за следење на мрежниот сообраќај не се апликабилни, како и методите за аналитичко моделирање на мрежите изградени користејќи SDN технологија и NFV архитектура, со цел да се извршат математички анализи за карактеристиките на мрежниот сообраќај.

Гласовните услуги кои се даваат на корисниците кај 5G мрежите се базирани на VoIP. Покрај тоа во оптек постојат голем број на апликации кои се користат, а кои овозможуваат VoIP мрежен сообраќај (Viber, Skype, WhatsApp, Facebook Messenger, Zoiper итн). Сообраќајот кој се одвива помеѓу овие апликации, скоро без исклучок е енкриптиран и најчесто откако ќе се воспостави, се одвива директно помеѓу корисниците (peer-to-peer), во самата мрежа. Самото следење на овој сообраќај најчесто е и регулаторен проблем, а сепак операторите имаат потреба од класификација на овој тип на сообраќај од најразлични причини, обезбедување на QoS, обезбедување на мрежна безбедност, имплементација на регулаторни правила и слично. Поради тоа императив е овој сообраќај да биде класифициран, во рамките на системите кои се високо виртуелизирани, а притоа да се зачува приватноста на корисниците и секако да не се наруши латентноста на мрежата. Токму ова е целта во првиот дел од нашето истражување. Главната цел и идеја е да претставиме метод за креирање на множества од податоци базирани само на статистичките карактеристики на тековите на мрежниот сообраќај, а потоа и да извршиме тестирање на перформансите на шест алгоритми за надгледувано машинско учење врз основа на креираните збирки на податоци. Сето ова е направено во иновативна експериментална тест околина каде што се користи NFV архитектура. Ги користиме алгоритмите Bayes Net, Naïve Bayes, J48, K-Nearest Neighbours (K-NN), Decision Tree и AdaBoost. Овие алгоритми се избрани поради фактот што тие се најчестите ML алгоритми кои се користат во традиционалните мрежи и се докажани како сигурни во пракса, но и бидејќи истите имаат истечени патенти, па може слободно да се користат од потенцијалните имплементатори на системи за класификација.

Ефикасноста на алгоритмите се истражува од точка на прецизност на алгоритамот, но и од точка на временска потрошувачка потребна за извршување на класификацијата. Ова е важно поради виртуелизацијата, каде што мешаните сценарија на облак се вообичаена пракса, но и за 5G, каде што латентноста на мрежата е од голема важност.

Нашата експериментална тестна околина ја користиме за извршување на повеќе експерименти и за собирање податоци за мрежниот сообраќај од кои се извлекуваат IP мрежните текови. Како атрибути за класификација се користат статистичките карактеристики на тековите. Бидејќи атрибутите како што се изворната и дестинацискатa IP и MAC адреса, како и комуникациските порти може да варираат во виртуелизирана средина, тие не се земаат предвид. Поради проблеми со енкрипцијата и приватноста на

податоците, содржината на пакетите со податоци е исто така исклучена од збирките на податоци и не се користи за класификација.

Околината што ја користиме не воведува никаков вид мрежни сонди или SDN елементи за извршување на собирањето податоци, така што сообраќајот исток-запад е целосно непроменет. Сообраќајот е целосно пресретнат во виртуелниот слој при што внимаваме да не воведеме дополнителна латентност во мрежата или потреба за користење на големи ресурси од виртуелната околина за самата класификација. Традиционалните методи за DPI најчесто функционираат со репликација на сообраќајот на засебна порта и негово испитување. Ваквиот метод е непрактичен и не го користиме.

Според добиените резултати, Decision Tree и BayesNet алгоритмите имаат највисока прецизност во класификацијата на VoIP сообраќајот, без разлика дали е енкриптиран или неенкриптиран. По нив се J48 и K-Nearest Neighbor алгоритмите. Naive Bayes и AdaBoost покажаа висока лажно позитивна стапка, класифицирајќи друг тип на сообраќај како VoIP што покажува дека не се доволно добри во делот на прецизноста. Од аспект на времето потребно за класификација AdaBoost алгоритамот е најбрз, но поради лошата прецизност не е соодветен за намената. DecisionTree алгоритамот има слични перформанси во однос на брзината и поради својата висока прецизност е најдобар избор, односно е најефикасен за класификација на VoIP. BayesNet и J48 исто така се извршуваат брзо и може да се користат за намената.

Истражувањето го проширивме и на други типови на мрежен сообраќај со цел да ја утврдиме употребната вредност на испитуваните алгоритми за општа класификација на сообраќајот. Избравме 6 класи, имајќи ги во предвид досегашните практики кај класичните мрежи, како типови на сообраќај каде најчесто е потребна класификација: VoIP, шифриран VoIP (EncVOIP), DNS, Управувачки (Managment), SSH, HTTP и HTTPS сообраќај. Резултатите и во овој случај покажаа дека алгоритамот Decision Tree има најдобри вкупни перформанси, и од гледна точка на прецизноста на класификацијата и од гледна точка на потрошувачка на време. Се покажа како сигурен класификатор на VoIP, но и на останатите класи на мрежен сообраќај. J48 и BayesNet исто така имаат добри перформанси, при што J48 има малку подобра прецизност, а BayesNet е побрз. K-Nearest Neighbor и NaiveBayes имаат просечна прецизност на класификација во опсег од околу 80%, но тие се бавни, особено KNN кој е скоро 20 пати побавен од Decision Tree и BayesNet. AdaBoost ги покажува најлошите перформанси со прецизност која многу варира

меѓу различни класи, што може да се види од макропросечната прецизност и *F1* скорот . Анализата во која ја изведовме може да се користи во пракса и покажа дека алгоритмите за надгледувано машинско учење може да имаат важна примена за класификација на мрежниот сообраќај кај модерните компјутерски мрежи.

Понатаму во овој труд се фокусираме на математичка анализа на мрежите изградени користејќи ги SDN и NFV технологиите. Поточно, целта е да ја предвидиме латенцијата што се појавува во мрежата, а која доаѓа од самата архитектура. Модерните мрежи функционираат на принципот на поврзување на виртуелни мрежни функции во сервисни низи, кои од една страна го следат SDN концептот на поделба на управувачкиот и податочниот слој и од друга страна се изградени користејќи ја NFV архитектурата која станува стандарден модел во телекомуникациската област, посебно со развојот на 5G мрежите. Токму кај 5G мрежите (но и кај останатите) каснењето на мрежните пакети, односно обезбедувањето на ниска латентност на услугите, игра главна улога во дизајнот и развојот на сервисите кои се нудат. Затоа се повеќе се настојува мрежните функции да се донесат во близина на крајниот потрошувач на услугата. Намерно го употребуваме зборот потрошувач, бидејќи се повеќе тенденцијата е потрошувачот да биде одреден уред, а не личност. Бројот на потрошувачи се зголемува, а се зголемува и конзумацијата на сообраќај по единка, што секако го афектуира и вкупниот обем на мрежен сообраќај. Покрај тоа се забележува и тенденција на групирање на потрошувачите на одредена географска локација, односно кластерирање, тие не се подеднакво распоредени на целата географска територија. Од овие причини, во нашето истражување даваме акцент на дистрибуцијата на мрежата на повеќе географски локации и го испитуваме влијанието што дистрибуцијата го има врз каснењето на мрежните пакети. Овој модел покрај намалување на трошоците за процесирачка моќ (хостовите врз кои работат виртуелните мрежни функции) дава значително подобрување на услугата за крајниот корисник. Од една страна може да се каже дека дистрибуираната NFV архитектура ја надополнува инфраструктурата во облак, но од друга страна се смета дека таа претставува тивок убиец на јавните облаци. Овозможува заштеда во делот на мрежна инфраструктура, линкови (кои во случаите на јавни облаци се меѓународни), ја поедноставува топологијата, дава поголема флексибилност во креирањето на сервисните низи и секако со самата близина до корисникот дава минимално мрежно доцнење на пакетите.

За да го изведеме истражувањето, односно за креирање на аналитичките модели користевме теорија на редици во која елементите ги апроксимиравме со M/M/1 редици, а целата мрежаа ја сметаме за Џексонова мрежа. Секоја географска локација е апроксимирано дека има еден комутатор. Претпоставуваме дека процесите на пристигнување во секој јазол имаат Поасонова распределба, а времето на сервисирање на пакетите следи експоненцијална дистрибуција. Мрежата на редици има достигнато избалансирана состојба и искористеноста на сите редици е помала од еден. Сметаме дека сите пакети се обработуваат и нема загуба од пакети во мрежата. Системот е целосно базиран на OpenFlow протоколот.

Изведовме 3 аналитички модели, на три различни архитектурни решенија:

- Централизиран систем, востпоставен на една локација, при што самиот систем има еден комутатор, еден контролер и еден VNF менаџер. Податочната рамнина се смета дека е воспоставена во еден податочен центар и лежи на виртуелизирана околина, најчесто приватен облак;
- Систем со дистрибуирана податочна рамнина на повеќе географски локации, која го содржи слојот на виртуелни мрежни функции (VNF layer) и NFV инфраструктурата, додека MANO елементите се централизирани и управуваат со системот од примарната локација. MANO опкружувањето има еден контролер и еден VNF менаџер кои ги опслужуваат сите локации;
- Целосно дистрибуиран систем, каде што секоја локација ги има сите елементи на NFV архитектурата.

За анализа на карактеристиките на вака дефинираните околини, поточно за анализа на латенцијата направени се MatLab апликации.

Кај централизираниот систем увидовме дека колку е поголема веројатноста за испраќање пакети до контролерот или пак до VNF Менаџерот, времето на престој на пакетите, а со тоа и комплетната латенција се зголемува. Доколку сите елементи се во непосредна мрежна близина, латенцијата не е голема. Но доколку крајниот потрошувач е оддалечен од примарната локација, линковската поврзаност односно транспортната и пропагационата латентност се зголемува. Оваа архитектура е задоволителна доколку

локацијата на мрежните функции кои ја креираат сервисната низа и крајниот потрошувач се близу од мрежен аспект.

Кај двете дистрибуирани архитектури, времето на престој на пакетите расте, како што се зголемува бројот на дистрибуирани комутатори (локации) низ кои е изградена SDN сервисната низа од VNF функции. При помал број на дистрибуирани локации архитектурата со централен NFV MANO работи подобро, без оглед на веројатноста за испраќање пакети на други дистрибуирани локации, но како се зголемува веројатноста, перформансите во однос на времето на престој на пакетите стануваат слични кај двете архитектури. Колку е поголем бројот на дистрибуирани локации низ кои се протега сервисната низа, така архиотектурата која е комплетно дистрибуирана станува подобра. Точката на пресек на графиците на каснење завиосно од бројот на дистрибуирани локации зависи од стапките на пристигнување на мрежен сообраќај и стапките на обработка на подаци кои ги имаат елементите, а секако и од транспортната и пропагационата латентност на линковите помеѓу дистрибуираните локации, но останува заклучокот дека за помал број на локации (во нашиот случај к<5) делумно дистрибуираната околина е подобра, но за поголем број на локации целосно дистрибуирана околина е подобра. Изведените равенки може да се искористат за пресметка на каснењето на мрежните пакети при различни параметри.

Во пракса логично е да се изврши заштеда на ресурси така што сервисната низа ќе биде целосно или во најголем дел на дистрибуирана локација која е во непосредна близина на потрошувачот. Користење на централизиран MANO кој би бил поврзан со брзи линкови со гео-локациите е логичниот след. Доколку понудените услуги, достапните ресурси или процесирачките елементи не овозможуваат ваква поставеност на сервисната низа, тогаш целосно дистрибуирана околина е логичен след.

Вреди да се напомене дека при голем број на дистрибуирани локации и комплицирани сервисни низи кои се протегаат на голем број од нив, централизирана околина може да даде и подобри резултати и би ја поедноставила мрежната архитектура.

Покрај теоретските испитувања и анализата во MatLab, истражувањето го проширивме и на експериментална околина која симулира дистрибуирана NFV архитектура на две засебни географски локации. Локациите се оддалечени 160км и се поврзани со 10Gbps линк. Направивме испитувања за мрежни низи кои се протегаат на

двете локации и мрежни патеки кои се така поставени, што сообраќајот повеќекратно поминува низ линкот. Експериментално добиените резултати ги поврдија резултатите од аналитичките модели, што докажува дека и покрај ограничувањата кои ги поставивме со претпоставките, аналитичките модели и равенките се соодветна појовна точка за пресметување на времето на каснење на пакетите во мрежата.

Крајната цел е аналитичките модели да може да се искористат за симулација на мрежниот сообраќај и естимација на мрежното доцнење во различни архитектурни решенија, со што теоретски мрежните архитекти може да ја одредат најдобрата околина за градење на мрежата низ која ќе се градат сервисните низи и услугите кон крајните потрошувачи.

РЕФЕРЕНЦИ

[1] J. Reis, M. Amorim, N. Melao, P. Matos, “Digital Transformation: A Literature Review and Guidelines for Future Research”, 2018, doi:10.1007/978-3-319-77703-0_41.

[2] J. Reis, M. Amorim, N. Melao, Y. Cohen, M. Rodrigues, “Digitalization: A Literature Review and Research Agenda”, 2020, doi:10.1007/978-3-030-43616-2_47.

[3] J. H. Cox, J. Chung, "Advancing Software-Defined Networks: A Survey," IEEE Access, vol 5, pp 25487 - 25526, 2017.

[4] H. Yeganeh, E. Vaezpour, “Fronthaul network design for radio access network virtualization from a CAPEX/OPEX perspective”, Ann. Telecommun. 71, pp. 665–676, 2016, doi:10.1007/s12243-016-0538-3

[5] C. L. Navarrete Hernández, C. A. Calderón, "Selection of NFV Test Platforms for the Service Provider." EAC [online]. 2021, vol.42, n.2, pp.89-99. ISSN 1815-5928.

[6] ETSI - Standards for NFV - Network Functions Virtualisation, NFV Solutions, https://www.etsi.org/technologies/nfv, cited 04.04.2022

[7] M. Chiosi et. al., “Network Functions Virtualisation - Introductory White Paper”, 2015. URL ⟨https://portal.etsi.org/nfv/nfv_white_paper.pdf⟩.

[8] D. Huang, A. Chowdhary, S. Pisharody, “SDN and NFV: From Theory to Practice”, 2018, doi:10.1201/9781351210768-4.

[9] M. Eiman, “Minimum Technical Performance Requirements for IMT-2020 Radio Interface(s)”, Presentation, 2018. [Online] Cited 2019-10-10. Available at https://www.itu.int/en/ITU-R/studygroups/rsg5/rwp5d/imt-2020/Documents/S01-1_Requirements%20for%20IMT-2020_Rev.pdf

[10] U. Huang, P. Li, S. Gu, “Traffic scheduling for deep packet inspection in software-defined networks.” Concurrency and Computation: Practice and Experience. 2017, doi:10.1002/cpe.3967.

[11] M. Mousa, A. Bahaa-Eldin, M. Sobh, “Software Defined Networking concepts and challenges.” In 11th International Conference on Computer Engineering & Systems (ICCES), 2016, pp 79-90. doi:10.1109/ICCES.2016.7821979

[12] L. Polčák et al, “A. High Level Policies in SDN”. In International Conference on E-Business and Telecommunications, 2016, pp. 39-57, doi:10.1007/978-3-319-30222-5_2.

[13] J. Arevalo Herrera, Camargo, J. E. “A Survey on Machine Learning Applications for Software Defined Network Security”. Applied Cryptography and Network Security Workshops. ACNS 2019. Lecture Notes in Computer Science, vol 11605. Springer, Cham. DOI: 10.1007/978-3-030-29729-9_4

[14] A. Chowdhary, D. Huang, A. Alshamrani, A. Sabur, M. A. Kang Kim, A. Velazquez, “SDFW: SDN-based Stateful Distributed Firewall”, 2018, doi:10.13140/RG.2.2.11001.93281.

[15] S. Choudhury, A. Bhowal, “Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection.” In ICSTM, Tamil Nadu, India, 2015, pp. 89–95, doi:10.1109/ICSTM.2015.7225395

[16] M. Shafiq, X. Yu, A. A. Laghari, et al., “Wechat text and picture messages service flow traffic classification using machine learning technique.” In IEEE HPCC/SmartCity/DSS, 58-62, 2016, pp. 58–62, doi:10.1109/HPCC-SmartCity-DSS.2016.0019

[17] Ericsson Publishing, “Edge computing and 5G - Harnessing the distributed cloud for 5G success”, [Online], 2020, https://www.ericsson.com/en/edge-computing/forms/ericsson-edge-computing-paper

[18] G. Honghao, Y. Yuyu, H. Guangjie, Z. Wenbing, “Edge computing: Enabling technologies, applications, and services”, Transactions on Emerging Telecommunications Technologies, Vol32, Issue6, 2021, doi:10.1002/ett.4197

[19] M. Alenazi, A. Almutari, S. Almowuena, W. Abdul, E. Cetinkaya, “NFV Provisioning in Large-Scale Distributed Networks With Minimum Delay”, IEEE Access, 2020, pp. 1-1, doi:10.1109/ACCESS.2020.3017667.

[20] Z. Zhang, Z. Li, C. Wu and C. Huang, "A Scalable and Distributed Approach for NFV Service Chain Cost Minimization," 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017, pp. 2151-2156, doi:10.1109/ICDCS.2017.210.

[21] A. Huff, G. Venâncio, V. F. Garcia, E. P. Duarte, "Building Multi-domain Service Function Chains Based on Multiple NFV Orchestrators," 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2020, pp. 19-24, doi:10.1109/NFV-SDN50289.2020.9289849.

[22] A. Khalid, F. Esposito, "Optimized Cuckoo Filters for Efficient Distributed SDN and NFV Applications," 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2020, pp. 77-83, doi:10.1109/NFV-SDN50289.2020.9289870.

[23] X. Fu, R. Yu, J. Wang, Q. Qi, J. Liao, "Performance Optimization for Blockchain-Enabled Distributed Network Function Virtualization Management and Orchestration,” IEEE Transactions on Vehicular Technology, 2020, pp. 1-1, doi:10.1109/TVT.2020.2985581.

[24] H. Feng, J. Llorca, A. Tulino, D. Raz, A. Molisch, "Approximation Algorithms for the NFV Service Distribution Problem, " 2021. Preprint, unpublished.

[25] W. Chiang, J. Wen, "Design and Experiment of NFV-Based Virtualized IP Multimedia Subsystem," 2018 3rd International Conference on Computer and Communication Systems (ICCCS), 2018, pp. 397-401, doi:10.1109/CCOMS.2018.8463235.

[26] A. Jain, N. S. Sadagopan, S. K. Lohani, M. Vutukuru, "A comparison of SDN and NFV for re-designing the LTE Packet Core," 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2016, pp. 74-80, doi:10.1109/NFV-SDN.2016.7919479.

[27] M. Jarschel, S. Oechsner, D. Schlosser, R. Pries, S. Goll and P. Tran-Gia, "Modeling and performance evaluation of an OpenFlow architecture," 2011 23rd International Teletraffic Congress (ITC), 2011, pp. 1-7.

[28] M. Jarschel, O. Østerbø, A. Chilwan, K. Mahmood, "Modelling of OpenFlow-based software-defined networks: The multiple node case," IET Networks, 2015, doi:4.10.1049/iet-net.2014.0091.

[29] M. Iushchenko, V. Shuvalov and B. Zelentsov, "Modeling the Software Dependability For a SDN/NFV Controller," 2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON), 2019, pp. 0134-0139, doi: 10.1109/SIBIRCON48586.2019.8958337.

[30] B. Xiong, X. Peng, J. Zhao, "A Concise Queuing Model for Controller Performance in Software-Defined Networks," Journal of Computers 11, 2016, pp. 232-237, doi: 10.17706/jcp.11.3.232-237.

[31] W. Saied, N. B. Youssef Ben Souayeh, A. Saadaoui and A. Bouhoula, "Deep and Automated SDN Data Plane Analysis," 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2019, pp. 1-6, doi: 10.23919/SOFTCOM.2019.8903846.

[32] C. Bouras, A. Kollia and A. Papazois, "SDN & NFV in 5G: Advancements and challenges," 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), 2017, pp. 107-111, doi: 10.1109/ICIN.2017.7899398.

[33] R. Muñoz et al., "SDN/NFV orchestration for dynamic deployment of virtual SDN controllers as VNF for multi-tenant optical networks," 2015 Optical Fiber Communications Conference and Exhibition (OFC), 2015, pp. 1-3.

[34] S. Azeem and S. Sharma, Satyendra, "Advanced Technologies Involved In Network Convergence: Sdn & Nfv," International Journal of Development Research, vol. 7, 2019.

[35] A. Fahmin, Y. -C. Lai, M. S. Hossain, Y. -D. Lin and D. Saha, "Performance Modeling of SDN with NFV under or aside the Controller," 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2017, pp. 211-216, doi: 10.1109/FiCloudW.2017.76.

[36] K. Sood, S. Yu, Y. Xiang and H. Cheng, "A General QoS Aware Flow-Balancing and Resource Management Scheme in Distributed Software-Defined Networks," in IEEE Access, vol. 4, pp. 7176-7185, 2016, doi: 10.1109/ACCESS.2016.2621770.

[37] J. Prados-Garzon, P. Ameigeiras, J. J. Ramos-Munoz, P. Andres-Maldonado and J. M. Lopez-Soler, "Analytical modeling for Virtualized Network Functions," 2017 IEEE International Conference on Communications Workshops (ICC Workshops), 2017, pp. 979-985, doi: 10.1109/ICCW.2017.7962786.

[38] Z. Shang, and K. Wolter, "Delay Evaluation of OpenFlow Network Based on Queueing Model.", 2016, ArXiv abs/1608.06491

[39] E. Frank, M. A. Hall, I. H. Witten. The WEKA Workbench. Online Appendix for "Data Mining: Practical Machine Learning Tools and Techniques", Morgan Kaufmann, Fourth Edition, 2016

[40] T. Subramanya and R. Riggio, "Machine Learning-Driven Scaling and Placement of Virtual Network Functions at the Network Edges," 2019 IEEE Conference on Network

Softwarization (NetSoft), Paris, France, 2019, pp. 414-422, doi: 10.1109/NETSOFT.2019.8806631

[41] V. Rajamani, E. Francy, E. Rani, and M. Theepa, “Study and Analysis of Software Defined Networking (SDN) using Open Source Tools and Techniques,” Asian Journal od applied Science and Technology, volume 2, Issues 2, 2020, pp. 508-514

[42] Software-Defined Networking (SDN) Definition. Opennetworking.org. Cited: June 2022.

[43] A. Montazerolghaem, M. H. Yaghmaee and A. Leon-Garcia, "Green Cloud Multimedia Networking: NFV/SDN Based Energy-Efficient Resource Allocation," in IEEE Transactions on Green Communications and Networking, vol. 4, no. 3, pp. 873-889, Sept. 2020, doi: 10.1109/TGCN.2020.2982821.

[44] G. ILIEVSKI and P. LATKOSKI, “Network Functions Virtualization - Distributed network environment to provide state of the art customer services,” PRESING, Chamber of certified Architects and Certified Engineers of R. Macedonia, year IX, No. 54, December 2021.

[45] D. Levin, A. Wundsam, B. Heller, N. Handigol, and A Feldmann, “Logically centralized? State distribution trade-offs in software defined networks.” HotSDN'12 - Proceedings of the 1st ACM International Workshop on Hot Topics in Software Defined Networks, 2012, doi:10.1145/2342441.2342443.

[46] Z. Zhang, L. Ma, K. Leung, F. Le, S Kompella, and L. Tassiulas, “How Better is Distributed SDN? An Analytical Approach,” 2017, Doi:10.48550/arXiv.1712.04161

[47] R. Firouzi and R. Rahmani, "A Distributed SDN Controller for Distributed IoT," in IEEE Access, vol. 10, pp. 42873-42882, 2022, doi: 10.1109/ACCESS.2022.3168299.

[48] Y. Jeon, S. Jang, S. Pack, K. Kim, and H. Park, “Mobility-Aware Leader Controller Selection in Distributed SDN,” The Journal of Korean Institute of Communications and Information Sciences, vol 47, 2022, pp. 76-78, doi:10.7840/kics.2022.47.1.76.

[49] Open Networking F.. OpenFlow switch specification version 1.3.1. Tech. Republic; 2012.

[50] W. Braun, M. Menth, “Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices,” Future Internet, vol 6 , 2016, pp. 302-336, doi:10.3390/fi6020302.

[51] A. Kalyaev, I. Korovin, M. Khisamutdinov, G. Schaefer and M. A. R. Ahad, "A hardware approach for organisation of software defined network switches based on FPGA," 2015 International Conference on Informatics, Electronics & Vision (ICIEV), 2015, pp. 1-4, doi: 10.1109/ICIEV.2015.7334067.

[52] S. Panev, P. Latkoski, “Handover analysis of openflow-based mobile networks with distributed control plane,” Computers & Electrical Engineering, vol.81, 2020, doi:10.1016/j.compeleceng.2019.106546.

[53] G. ILIEVSKI, P. LATKOSKI, “Evaluation of Distributed NFV Infrastructures for Efficient Edge Computing in 5G,” ETAI, 2021, Online Conference

[54] B. Goswami, “Software Defined Network, Controller Comparison,” International Journal of Innovative Research in Computer and Communication Engineering, Vol.5, Special Issue 2, April 2017

[55] https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_White_Paper_Network_Transformation_2019_N32.pdf

[56] EQUINIX, “Defining The Elements of NFV Architectures - Interconnections - The Equinix Blog,” https://blog.equinix.com/blog/2019/10/17/networking-for-nerds-defining-the-elements-of-nfv-architectures/, cited: 2022-06-19

[57] ETSI, “Network Functions Virtualisation – White Paper on NFV priorities for 5G,” Issue 1, https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf. cited: 2022-06-19

[58] B. Chatras, U. S. Tsang Kwong and N. Bihannic, "NFV enabling network slicing for 5G," 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), 2017, pp. 219-225, doi: 10.1109/ICIN.2017.7899415.

[59] Z. Chen, F. Lin, CH Yu, WH Hu, “Pricing 5G Network Slices Based on NFV MANO,” In book: Proceedings of the Future Technologies Conference (FTC) 2022, Volume 3, pp.237-250, 2022, doi:10.1007/978-3-030-89912-7_19.

[60] G. ILIEVSKI, P. LATKOSKI, “Experimental evaluation of network packet latency within a distributed NFV Infrastructure,” 29th Telecommunications Forum (TELFOR), 2021, pp. 1-4. doi:10.1109/TELFOR52709.2021.9653395.

[61] G. ILIEVSKI, P. LATKOSKI, “Analytical modeling of distributed NFV architectures and the impact of the distribution on the packet sojourn time,” Transactions on Emerging Telecommunications Technologies, In Press, 2022, doi: 10.1002/ett.4559.

[62] G. ILIEVSKI, P. LATKOSKI, “Network traffic classification using supervised machine learning algorithms in systems with NFV architecture,” COMPLEX SYSTEMS: SPANING CONTROL AND COMPUTATIONAL CYBERNETICS, Dedicated to Professor Georgi M. Dimirovski on his anniversary. Peng Shi (Editor), Jovan Stefanovski (Editor), Janusz Kacprzyk (Editor), 2022

[63] G. ILIEVSKI, P. LATKOSKI, “Network Traffic Classification in an NFV Environment using Supervised ML Algorithms,” Journal of Telecommunications and Information Technology, National Institute of Telecommunications – Poland, Instytut Łączności - Państwowy Instytut Badawczy, ISSN:1509-4553, 2021, doi:10.26636/jtit.2021.153421

[64] G. ILIEVSKI, P. LATKOSKI, “Efficiency of Supervised Machine Learning Algorithms in Regular and Encrypted VoIP Classification within NFV Environment,” Radioengineering, Společnost pro radioelektronické inženýrství, 2020, 29(1), pp. 243-250, ISSN 1210-2512, doi:10.13164/re.2020.0243

[65] Qorvo, “Getting to 5G: Comparing 4G and 5G System Requirements,” https://www.qorvo.com/design-hub/blog/getting-to-5g-comparing-4g-and-5g-system-requirements

[66] T. Daengsi, P. Ungkap, P. Pornpongtechavanich and P. Wuttidittachotti, "QoS Measurement: A Comparative Study of Speeds and Latency for 5G Network Using Different Speed Test Applications for Mobile Phones," 2021 IEEE 7th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), 2021, pp. 206-210, doi: 10.1109/ICSIMA50015.2021.9526296.

[67] M. V. Bernal, I. Cerrato, F. Risso and D. Verbeiren, "Transparent Optimization of Inter-Virtual Network Function Communication in Open vSwitch," 2016 5th IEEE

International Conference on Cloud Networking (Cloudnet), 2016, pp. 76-82, doi: 10.1109/CloudNet.2016.26.

[68] L. He, C. Xu, Y. Luo, “vTC: Machine Learning Based Traffic Classification as a Virtual Network Function.”, 2016, pp. 53-56, doi: 10.1145/2876019.2876029.

[69] J. Vergara-Reyes, M. C. Martinez-Ordonez, A. Ordonez and O. M. Caicedo Rendon, "IP traffic classification in NFV: A benchmarking of supervised Machine Learning algorithms," 2017 IEEE Colombian Conference on Communications and Computing (COLCOM), 2017, pp. 1-6, doi: 10.1109/ColComCon.2017.8088199.

[70] R. Alshammari, A. Nur Zincir-Heywood “Identification of VoIP encrypted traffic using a machine learning approach” Journal of King Saud University - Computer and Information Sciences archive, Volume 27 Issue 1, 2015, pp 77-92

[71] Z. Li, Z. Ge, A. Mahimkar, J. Wang, B.Y. Zhao, H. Zheng, J. Emmons, L. Ogden, “Predictive Analysis in Network Function Virtualization”, Proceedings of the Internet Measurement Conference 2018, pp 161-167

[72] W. Ma, O. Sandoval, J. Beltran, D. Pan and N. Pissinou, "Traffic aware placement of interdependent NFV middleboxes," IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 2017, pp. 1-9, doi: 10.1109/INFOCOM.2017.8056993.

[73] D. Bonfiglio, M. Mellia, M. Meo, D. Rossi, P. Tofanelli, "Revealing skype traffic: when randomness plays with you" SIGCOMM Comput., 2007, pp 37–48.

[74] L. Le, B. Pail Lin, D. Sinh, “Applying Big Data, Machine Learning, and SDN/NFV for 5G Early-Stage Traffic Classification and Network QoS Control,” Transactions on Networks and Communications, vol. 6, 2018, doi: 10.14738/tnc.62.4446.

[75] Oracle VirtualBox. 2019 Cited 2019-09-10. Available at: https://www.virtualbox.org

[76] Linux Foundation, Open vSwitch Project, 2016 [Online]. Available: http://www.openvswitch.org

[77] Wireshark, 2006 Cited 2019-09-10. Available at: https://www.wireshark.org/

[78] M. Team, 2017 Mininet: An instant virtual network on your laptop (or other pc) - mininet. Cited 2019-09-12. Available at: http://mininet.org

[79] Ryu Framework, 2019. Cited 2019-09-10. Available at: http://osrg.github.io/ryu/

[80] Argus Quosient, 2015. Cited 2019-09-10. Available at: https://qosient.com/argus/

[81] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, I. H. Witten, “The WEKA Data Mining Software: An Update,” in SIGKDD Explorations Newsletter, Volume 11, Issue 1. pp. 10-18, 2009, doi: 10.1145/1656274.1656278

[82] S. Zhang, X. Li, M. Zong, X. Zhu and R. Wang, "Efficient kNN Classification With Different Numbers of Nearest Neighbours," in IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 5, pp. 1774-1785, May 2018, doi: 10.1109/TNNLS.2017.2673241.

[83] S. Zhang and J. Li, "KNN Classification with One-step Computation," in IEEE Transactions on Knowledge and Data Engineering, doi: 10.1109/TKDE.2021.3119140.

[84] D. Arivudainambi, K. A. Varun, R. Vinoth and P. Visu. “Ransomware Traffic Classification Using Deep Learning Models: Ransomware Traffic Classification,” in International Journal of Web Portals, vol. 12, pp. 1-11, 2020, 10.4018/IJWP.2020010101.

[85] Z. Wu, Y. -n. Dong, J. Jin, H. -L. Wei and G. Xie, "Multimedia Traffic Classification for Imbalanced Environment," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 3, pp. 1838-1852, 1 May-June 2022, doi: 10.1109/TNSE.2022.3153925.

[86] M. Nsaif, G. Kovásznai, M. Abboosh, A. Malik, R. de Fréin, “ML-Based Online Traffic Classification for SDNs,” 2022, pre-press

[87] A. Vulpe, I. Girla, R. Craciunescu and M. G. Berceanu, "Machine Learning based Software-Defined Networking Traffic Classification System," 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2021, pp. 1-5, doi: 10.1109/BlackSeaCom52164.2021.9527861.

[88] S. Zander, G. Armitage, "Practical machine learning based multimedia traffic classification for distributed QOS management.” In IEEE LCN, Bonn, Germany, 2011, pp. 399–406. DOI: 10.1109/LCN.2011.6115322

[89] M. Reza, M. J. Sobouti, S. ,Raouf, R. Javidan, “Network Traffic Classification using Machine Learning Techniques over Software Defined Networks,“ in International Journal of Advanced Computer Science and Applications, 2017, DOI: 8.10.14569/IJACSA.2017.080729.

[90] M. Karakus, A. Durresi, “Quality of Service (QoS) in Software Defined Networking (SDN): A survey,” in Journal of Network and Computer Applications, 2016, DOI: 80. 10.1016/j.jnca.2016.12.019

[91] G. ILIEVSKI, P. LATKOSKI, “Classification of Network Traffic Using Supervised Machine Learning Algorithms within NFV environment,” in Serbian Journal of Electrical Engineering, Vol. 18, No. 2, 2021, doi: 10.2298/SJEE2102237I

[92] C. Sarkar, S.K. Setua, “Analytical model for openflow-based software-defined network,” in Progress in computer, analytics and networking, 2018, pp. 583–592.

[93] G. Sun, Y. Li, D. Liao, V. Chang, “Low-latency orchestration for workflow-oriented service function chain in edge computing,” in Future Generation Computer Systems, vol. 85, 2018, doi: 10.1016/j.future.2018.03.018.

[94] R. S. Guimaraes, V. M. G. Martínez, R. C. Mello, D. R. Mafioletti, M. Martinello and M. R. N. Ribeiro, "An SDN-NFV Orchestration for Reliable and Low Latency Mobility in Off-the-Shelf WiFi," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148900.

[95] F. Meneses, R. Silva, D. Santos, R. Corujo, and L. Aguiar L, “An integration of slicing, NFV, and SDN for mobility management in corporate environments,” in Transactions on Emerging Telecommunications Technologies, vol. 31(1), 2020, doi: 10.1002/ett.3615

[96] W. Braun, M. Menth, “Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices,” in Future Internet, 2014, pp. 302-336, doi: 10.3390/fi6020302.

[97] T. Panagiotis, K. Panagiotis, L. Helen, T. Zahariadis, F. Vicens, A. Zurita, P. Alemany, T. Soenen, C. Parada, J. Bonnet, E. Fotopoulou, S. Zafeiropoulos, E. Kapassa,

M. Touloupou, and D. Kyriazis, “Comparison of Management and Orchestration Solutions for the 5G Era,” in Journal of Sensor and Actuator Networks, vol. 9, 2020, doi: 10.3390/jsan9010004.

[98] L. Yala, P. A. Frangoudis and A. Ksentini, "Latency and Availability Driven VNF Placement in a MEC-NFV Environment," 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1-7, doi: 10.1109/GLOCOM.2018.8647858.

[99] T. Gao et al., "Cost-Efficient VNF Placement and Scheduling in Public Cloud Networks," in IEEE Transactions on Communications, vol. 68, no. 8, pp. 4946-4959, Aug. 2020, doi: 10.1109/TCOMM.2020.2992504.

[100] I. Al Ridhawi, M. Aloqaily, Y. Kotb, Y. Al Ridhawi, and Y. Jararweh, “A collaborative mobile edge computing and user solution for service composition in 5G system,” in Transactions on Emerging Telecommunications Technologies, vol. 29(11), 2018, doi: 10.1002/ett.3446

[101] A. Aissioui, A. Ksentini, A. Gueroui, T. Taleb, “Towards Elastic Distributed SDN/NFV Controller for 5G Mobile Cloud Management Systems,” IEEE Access, vol. 3, 2015, doi: 10.1109/ACCESS.2015.2489930.

[102] ETSI NFV ISG, “GS NFV-EVE 005 V1.1.1 Network Function Virtualization (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework,” Dec. 2015.

[103] Microsoft Azure, (2020), [Online], Cited 2020-06-09, https://azure.microsoft.com/en-us/global-infrastructure/regions/

[104] Amazon AWS, (2020), [Online], Cited 2020-06-09, https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html

[105] J. R. Jackson, “Networks of waiting lines,” Operations research, vol. 5, no. 4, pp. 518–521, 1957.

[106] A. Bikakis, X. Zheng, “Multi-disciplinary Trends in Artificial Intelligence”, 9th International Workshop, MIWAI 2015, Fuzhou, China, November 13-15, 2015, Proceedings, pp. 390-403, 2015

[107] P. Gope, I. Pedone, A. Lioy, F. Valenza, “Towards an Efficient Management and Orchestration Framework for Virtual Network Security Functions, Security and Communication Networks,” in Hindawi, 2019, doi: 10.1155/2019/2425983

[108] W. Chiang and J. Wen, "Design and Experiment of NFV-Based Virtualized IP Multimedia Subsystem," 2018 3rd International Conference on Computer and Communication Systems (ICCCS), 2018, pp. 397-401, doi: 10.1109/CCOMS.2018.8463235.

[109] A. Jain, N.S. Sadagopan, S. K. Lohani and M. Vutukuru, "A comparison of SDN and NFV for re-designing the LTE Packet Core," 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2016, pp. 74-80, doi: 10.1109/NFV-SDN.2016.7919479.

[110] W. Lei, A. Soong, L. Jianghua, W. Yong, B. Classon, W. Xiao, D. Mazzarese, Z. Yang, and T. Saboorian, “From 4G to 5G: Use Cases and Requirements,” in Springer, Cham, 2021, doi: 10.1007/978-3-030-73703-0_1.

[111] A. Gohar, G. Nencioni, “The Role of 5G Technologies in a Smart City: The Case for Intelligent Transportation System,” In Sustainability, vol 13, 2021, doi: 10.3390/su13095188.

[112] J. F. Monserrat, A. Diehl, C. Bellas Lamas, S. Sultan, Sara, “Envisioning 5G-Enabled Transport, World Bank, Washington, DC., 2020, doi: 10.1596/35160.

[113] T. Neumuth, C. Bulitta, S. Hamm, F. Edelmann, A. Mittermaier, M. Rockstroh, C. Thuemmler, “5G Health - The need for 5G technologies in healthcare,” 2020, doi: 10.13140/RG.2.2.10915.27687.

[114] A. Ahad, M. Tahir and K. -L. A. Yau, "5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions," in IEEE Access, vol. 7, pp. 100747-100762, 2019, doi: 10.1109/ACCESS.2019.2930628.

[115] J. Lee, M. Azamfar, M. Miller, “5G and Smart Manufacturing,” in Manufacturing and Leadership, Manufacturing and Leadership Council, 2020

[116] A. Chehri, A. Zimmermann, “5G Assisted Smart Manufacturing and Industrial Automation,” in International Conference on Applied Human Factors and Ergonomics, pp. 385-393, 2021, doi: 10.1007/978-3-030-80840-2_44.

[117] L. Helen, T. Zahariadis, L. Sarakis, E. Tsampasis, A. Voulkidis, T-H. Velivasaki, “Smart Grid: a demanding use case for 5G technologies, 2018, pp. 215-220, doi: 10.1109/PERCOMW.2018.8480296.

[118] M. Di Mauro, G. Galatro, F. Postiglione and M. Tambasco, "Performability of Network Service Chains: Stochastic Modeling and Assessment of Softwarized IP Multimedia Subsystem" in IEEE Transactions on Dependable and Secure Computing, vol. , no. 01, pp. 1-1, 5555. doi: 10.1109/TDSC.2021.3082626

[119] S.A. AlQahtani, W.A. Alhomiqani, "A multi-stage analysis of network slicing architecture for 5G mobile networks," in Telecommun Syst 73, 2020, pp. 205–221, doi: 10.1007/s11235-019-00607-2

[120] M. Sadaf, H. Omar, D. Guillaume, K. Ferhat, T. Maria, "Model-Driven Process Enactment for NFV Systems with MAPLE”, Springer Nature, 2020

[121] Mathematics-based software & services for education, engineering, and research, MAPLE, https://www.maplesoft.com/

[122] ISIS Papyrus Software, https://www.isis-papyrus.com/

[123] V. Sanchez-Aguero, I. Vidal, F. Valera, B. Nogales, L. Mendes, W. Dias, A. Ferreira, “Deploying an NFV-Based Experimentation Scenario for 5G Solutions in Underserved Areas,” Sensors, 2021, doi: 10.3390/s21051897.

[124] F. De Turck, A. Schaeffer-Filho, L. Granville, M. Franco, L. Bondan, C. R. Paula dos Santos, L. Marcuzzo, E. Duarte Jr, T. Tavares, G. Souza, V. Garcia, “On the design and development of emulation platforms for NFV-based infrastructures,” in International Journal of Grid and Utility Computing, vol. 11, 2020, doi: 10.1504/IJGUC.2020.10026553.

[125] M. Gharbaoui, C. Contoli, G. Davoli, D. Borsatti, G. Cuffaro, F. Paganelli, W. Cerroni, P. Cappanera, B. Martini, “An experimental study on latency-aware and self-adaptive service chaining orchestration in distributed NFV and SDN infrastructures,” in Computer Networks 208, 2022, doi: 10.1016/j.comnet.2022.108880.

[126] W. Xiao-Long, W-M Li, F. Liu, and H. Yu, "Packet size distribution of typical Internet applications," 2012 International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP), 2012, pp. 276-281, doi: 10.1109/ICWAMTIP.2012.6413493.

[127] S. Dong , Y. Xia, "Network traffic identification in packet sampling environment, Digital Communications and Networks," Sciense Direct, 2022, doi: doi.org/10.1016/j.dcan.2022.02.003

[128] Cisco, "Packet Size of Internet Traffic", 2022, https://community.cisco.com/

[129] B. Husen, "Math Teachings, Department of Mathematics," Ohio State University, https://people.math.osu.edu/husen.1/teaching/571/markov_1.pdf

[130] M.D. DiSorbo, J. Blitzstein, J. Hwang, "Probability! An interactive introduction," Harvard University Archives, 2022

[131] P.C. Tulasian, V. Pandey, "Quantitative Techniques: Theory and Problems," Pearson India, SBN:9788131701867, 2006

[132] R. Sehgal, "Modeling And Analysis Of Delay Tolerant Networks," 2016, doi: 10.13140/RG.2.2.29407.92328.

[133] A. Obiniyi, M. Soroyewun, M. Abur, "New Innovations in Performance Analysis of Computer Networks: A Review, in International Journal of Applied Information Systems, vol 6, 2014, doi: 10.5120/ijais14-451085.

[134] H. Chen, D. D. Yao, "Jackson Networks," inn: Fundamentals of Queueing Networks, Stochastic Modelling and Applied Probability, vol 46. Springer, New York, NY, 2001, doi:10.1007/978-1-4757-5301-1_2

[135] C. Bockelmann et al., "Massive machine-type communications in 5g: physical and MAC-layer solutions," in IEEE Communications Magazine, vol. 54, no. 9, pp. 59-65, September 2016, doi: 10.1109/MCOM.2016.7565189.

ОБЈАВЕНИ ТРУДОВИ

[1] G. ILIEVSKI, P. LATKOSKI, "Efficiency of Supervised Machine Learning Algorithms in Regular and Encrypted VoIP Classification within NFV Environment," Radioengineering, Společnost pro radioelektronické inženýrství, 2020, 29(1), pp. 243-250, ISSN 1210-2512, doi:10.13164/re.2020.0243. **Impact Factor: 0.951**

[2] G. ILIEVSKI, P. LATKOSKI, "Analytical modeling of distributed NFV architectures and the impact of the distribution on the packet sojourn time," Transactions on Emerging Telecommunications Technologies, Volume 33, Issue 9, 2022, doi: 10.1002/ett.4559. **Impact factor: 2.638**

[3] G. ILIEVSKI, P. LATKOSKI, "Network Traffic Classification in an NFV Environment using Supervised ML Algorithms," Journal of Telecommunications and Information Technology, National Institute of Telecommunications – Poland, Instytut Łączności - Państwowy Instytut Badawczy, ISSN:1509-4553, 2021, doi:10.26636/jtit.2021.153421. **Index Copernicus, ICV2018=114,89; Scopus Impact Factor: 0.722, SJR 2019: 0.182; SNIP 2019: 0.421; CiteScore 2019: 1.1**

[4] G. ILIEVSKI, P. LATKOSKI, "Classification of Network Traffic Using Supervised Machine Learning Algorithms within NFV environment," in Serbian Journal of Electrical Engineering, Vol. 18, No. 2, 2021, doi: 10.2298/SJEE2102237I

[5] G. ILIEVSKI, P. LATKOSKI, "Network traffic classification using supervised machine learning algorithms in systems with NFV architecture," COMPLEX SYSTEMS: SPANING CONTROL AND COMPUTATIONAL CYBERNETICS, Dedicated to Professor Georgi M. Dimirovski on his anniversary. Peng Shi (Editor), Jovan Stefanovski (Editor), Janusz Kacprzyk (Editor), 2022

[6] G. ILIEVSKI and P. LATKOSKI, "Network Functions Virtualization - Distributed network environment to provide state of the art customer services," PRESING, Chamber of certified Architects and Certified Engineers of R. Macedonia, year IX, No. 54, December 2021.

[7] G. ILIEVSKI, P. LATKOSKI, "Evaluation of Distributed NFV Infrastructures for Efficient Edge Computing in 5G," ETAI, 2021, Online Conference

[8] G. ILIEVSKI, P. LATKOSKI, "Experimental evaluation of network packet latency within a distributed NFV Infrastructure," 29th Telecommunications Forum (TELFOR), 2021, pp. 1-4. doi:10.1109/TELFOR52709.2021.9653395.