

RĪGAS TEHNISKĀ UNIVERSITĀTE

Elektronikas un telekomunikāciju fakultāte

Telekomunikāciju institūts

Andris SKRASTIŅŠ

Doktora studiju programmas “Telekomunikācijas” doktorants

**RESURSU UN ATĻAUJU VADĪBA NĀKOŠĀS
PAAUDZES TĪKLOS**

Promocijas darba kopsavilkums

Zinātniskais vadītājs
profesors *Dr. sc. ing.*
G. LAUKS

RTU Izdevniecība
Rīga 2017

Skrastiņš A. Resursu un atļauju vadība nākošās paaudzes tīklos. Promocijas darba kopsavilkums. – R.: RTU Izdevniecība, 2017. – 49 lpp.

Iespiests saskaņā ar ETF promocijas padomes “RTU P-08” 2016. gada 8. decembra lēmumu, protokols Nr. 37.



EIROPAS SAVIENĪBA

ISBN 978-9934-10-921-8

PROMOCIJAS DARBS
IZVIRZĪTS INŽENIERZINĀTŅU DOKTORA GRĀDA IEGŪŠANAI
RĪGAS TEHNISKAJĀ UNIVERSITĀTĒ

Promocijas darbs inženierzinātņu doktora grāda iegūšanai tiek publiski aizstāvēts 2017. g. 16. martā Rīgas Tehniskās universitātes Elektronikas un Telekomunikāciju fakultātē, Āzenes ielā 12, 201. auditorijā.

OFICIĀLIE RECENZENTI

Profesors *Dr. habil. sc. ing.* Ernests Pētersons
Rīgas Tehniskā universitāte, Elektronikas un Telekomunikāciju fakultāte

Profesors *Dr. sc. comp.* Guntis Bārzdiņš
Latvijas Universitāte, Matemātikas un informātikas institūts

Pētnieks *Dr. sc. comp.* Kaspars Sudars
Elektronikas un datorzinātņu institūts

APSTIPRINĀJUMS

Apstiprinu, ka esmu izstrādājis šo promocijas darbu, kas iesniegts izskatīšanai Rīgas Tehniskajā universitātē inženierzinātņu doktora grāda iegūšanai. Promocijas darbs nav iesniegts nevienā citā universitātē zinātniskā grāda iegūšanai.

Andris Skrastiņš.....(Paraksts)

Datums:

Promocijas darbs ir uzrakstīts latviešu valodā, satur ievadu, četras nodaļas, secinājumus, literatūras sarakstu, 78 zīmējumus un ilustrācijas, kopā 162 lappuses. Literatūras sarakstā ir 116 nosaukumu.

SAĪSINĀJUMU SARAKSTS

AggSessAC	<i>Aggregated Session Admission Control</i>	Agregētu sesiju piekļuves vadība
ARP	<i>Address Resolution Protocol</i>	Adrešu atrises protokols
CAC	<i>Connection Admission Control</i>	Savienojuma piekļuves vadība
CAGR	<i>Compound Annual Growth Rate</i>	Gadskārtējais pieauguma temps
CAIDA	<i>Center for Applied Internet Data Analysis</i>	Interneta datu analīzes centrs
DiffServ	<i>Differentiated services</i>	Diferencētie pakalpojumi
DNS	<i>Domain name system</i>	Domēnu vārdu sistēma
DPI	<i>Deep Packet Inspection</i>	Padziļinātā paketes pārbaude
FAN	<i>Flow-aware networks</i>	Datu plūsmu atpazīstoši tīkli
FPGA	<i>Field-Programmable Gate Array</i>	Programmējamas ciparu integrālās shēmas
GPU	<i>Graphics Processing Unit</i>	Grafiskais procesors
HTTP	<i>Hypertext Transfer Protocol</i>	Hiperteksta pārsūtīšanas protokols
IETF	<i>Internet Engineering Task Force</i>	Interneta inženierijas uzdevumgrupa
ETSI	<i>European Telecommunications Standards Institute</i>	Eiropas telesakaru standartu institūts
ICMP	<i>Internet Control Message Protocol</i>	Interneta vadības ziņojumu protokols
IntServ	<i>Integrated Services</i>	Integrētie pakalpojumi
IoT	<i>Internet of Things</i>	Lietu internets
ISP	<i>Internet Service Provider</i>	Interneta pakalpojumu sniedzējs
ITU-T	<i>International Telecommunication Union, Telecommunication Standardization Sector</i>	Starptautiskā telekomunikāciju savienība, Telekomunikāciju standartizācijas sektors
M2M	<i>Machine-to-Machine</i>	Mašīna-mašīna datu komunikācija
MBAC	<i>Measurement-based Admission Control</i>	Mērījumu balstīta piekļuves vadība
MPLS	<i>Multiprotocol Label Switching</i>	Daudzprotokolu iezīmju komutācija
MPPS	<i>Million Packets Per Second</i>	Miljons paketes sekundē
NGN	<i>Next generation network</i>	Nākamās paaudzes tīkli
PBAC	<i>Parameter-based Admission Control</i>	Parametru balstīta piekļuves vadība
PHB	<i>Per-Hop Behaviors</i>	Pakešu virzīšanas princips, tās analizējot katrā pārsūtīšanas solī

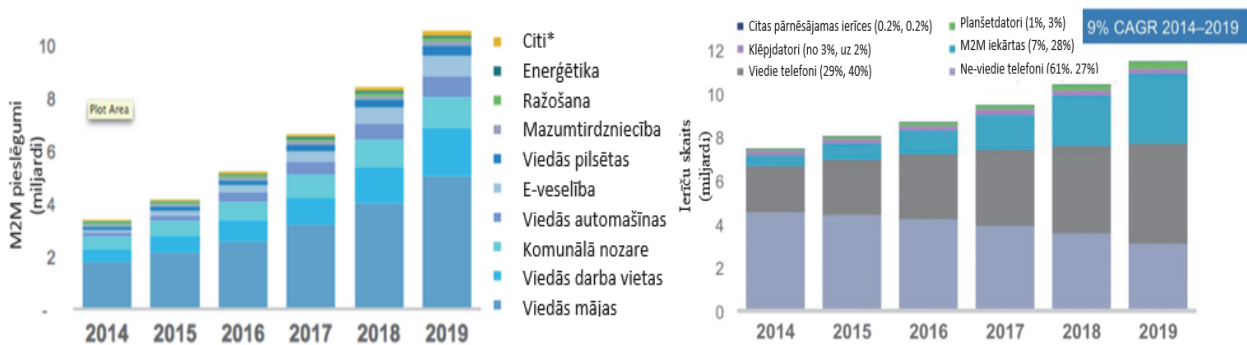
P2P	<i>Point-to-Point</i>	Vienādranga tīklošana, Punkts-punkts savienojums
QoS	<i>Quality of service</i>	Pakalpojumu kvalitāte
RACF	<i>Resource and Admission Control Functions</i>	Resursu un piekļuves vadības funkcijas
RSVP TE	<i>Resource Reservation Protocol Traffic Engineering</i>	Resursu rezervēšanas protokols ar trafika inženieriju
SLA	<i>Service Level Agreement</i>	Klienta-operatora līgums
SNMP	<i>Simple Network Management Protocol</i>	Vienkāršs tīkla pārvaldības protokols
ThresholdAC	<i>Threshold Admission Control</i>	Piekļuves vadības metodes, kas realizē secīgu, neatkarīgu, un jaunu savienojumu pieprasījumu apstrādes manieri un izvērtē caurlaides joslas resursu pieejamību
ToS	<i>Type of Service</i>	Servisa tips
TCP	<i>Transmission Control Protocol</i>	Pārraides vadības protokols
UDP	<i>User Datagram Protocol</i>	Lietotāja datagrammu protokols
VLAN	<i>Virtual local area network</i>	Virtuālais lokālais tīkls
VNI	<i>Cisco Visual Networking Index</i>	Cisco kompānijas izmantotais indekss globāla IP trafika prognozēm

VISPĀRĒJAIS DARBA RAKSTUROJUMS

Tēmas aktualitāte

Attīstības tendences. Telekomunikāciju tīklu straujā attīstība ir veicinājusi interneta servisu un tīklu konverģenci, kā rezultātā IP (Interneta protokola) balstīta datu pārraide ir kļuvusi par mūsdienu sakaru tīklu pamatu, ko bieži apzīmē arī kā “viss caur IP” (no angļu val. *everything over IP*). Vēlme pēc dažādu procesu automatizēšanas, dzīves kvalitātes un ērtuma uzlabošanas veicina arvien jaunu interneta tiešsaistes pakalpojumu parādīšanos. Katra jauna pakalpojuma parādīšanās piesaista jaunus lietotājus, palielina kopējo datu apjomu un rada arvien vairāk apkalpojamo datu sesiju. Informāciju tehnoloģiju arvien pieaugošā ienākšana ikvienā dzīves sfērā veicina arī dažādu lietu klāsta pieaugumu, kas savu funkciju pildīšanai prasa pieslēgumu pie globālā tīmekļa. Šī procesa rezultātā ir attīstījies virziens, ko dēvē par „lietu internetu” (no angļu val. *IoT – Internet of Things*), kur viena no progresējošākajām nozarēm ir M2M komunikācija [2] (skat. 1. att.). Jāsaka, ka ikviena jauna lieta ar piesaisti pie globālā tīmekļa ir jauns potenciāls datu plūsmu ģenerējošs avots.

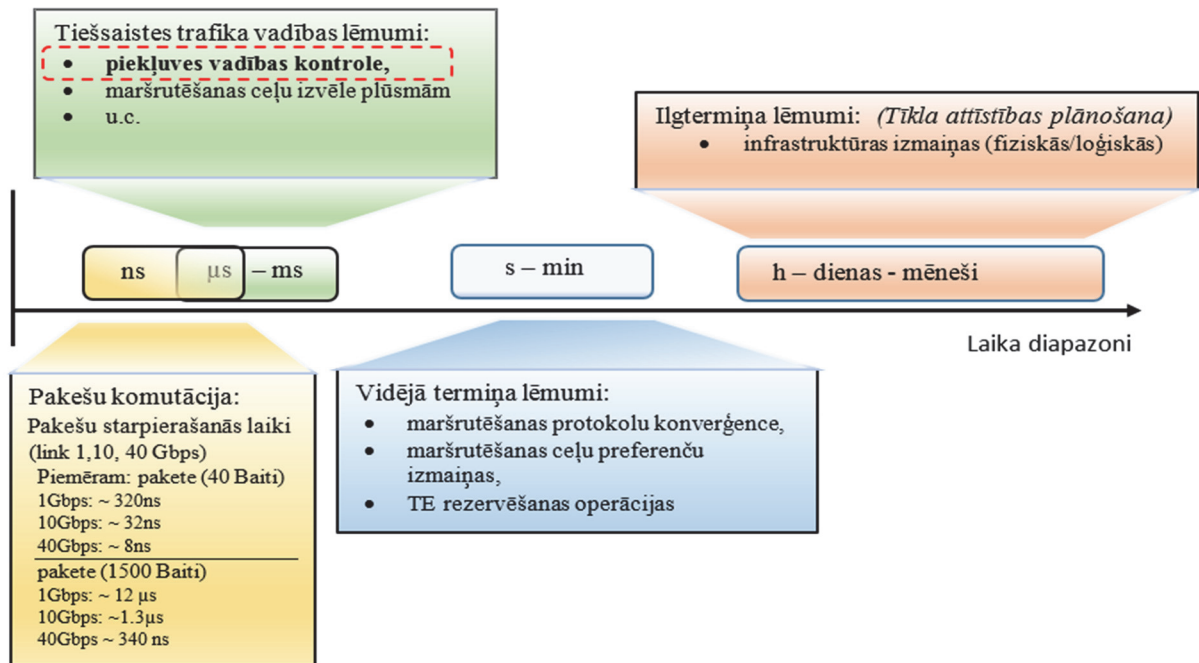
Piemēram, Cisco VNI savās prognozēs jau min, ka 2019. gadā būs ap 11 miljardu dažādu interneta tīklam piesaistītu bezvadu ierīču atšķirībā no 7.3 miljardiem 2014. gadā, kas veidos pieaugumu par 50 % (skat. 2. att.). Attiecībā uz trafika apjomu tiek prognozēts, ka 2019. gadā jau 33 % no interneta trafika veidos tieši dažāda veida bezvadu ierīces un tikai 66 % būs fiksētā pieslēguma ierīces [2], bet periodā līdz 2020. gadam tiek prognozēts trīskārtējs bezvadu ierīču radītā trafika apjoma pieaugums [7]. Šādi attīstības tempi izvirza jaunus uzdevumus trafika vadības jomā, kur attiecībā uz piekļuves vadību tas nozīmē apstrādājamo savienojumu skaita pieaugumu un jaunu servisu apkalpošanu.



1. att. Cisco VNI 2014–2019 prognozētā M2M sakaru komunikācijas attīstība un sadalījums pa nozarēm. [2]

2. att. Cisco VNI 2014–2019 globālam tīklam prognozētais piesaistīto bezvadu ierīču skaits un veidi. [6]

Laika mērogs. Mūsdienu pamattīkla šķautnes mezglos jaunu plūsmu savienojuma pieprasījumu apjomi ir mērāmi desmitos tūkstošu ik sekundi [65], [66]. Šādi un iepriekš minētie attīstības tempi palielina jaunu plūsmu intensitāti (jaunas plūsmas/s), kas piekļuves vadības risinājumiem liek darboties laika mērogā no desmitiem [μs] līdz dažām [ms] (skat. 3. att.). To vēl vairāk pastiprina pētījumu fakti, kas parāda, ka >80 % no visiem savienojumiem ilgst tikai dažas sekundes un satur līdz dažiem desmitiem pakešu [19], [34], [47], [56], [65].



3. att. Laika mērogi trafika vadības plāksnē

Servisu diferencēšana. Pēc savas būtības resursu un piekļuves pārvaldības RACF (no angļu val. *Resource and Admission Control Functions*) galvenais uzdevums ir efektīvi izdalīt pieejamos resursus, nezaudējot saistību izpildi attiecībā uz pakalpojuma saņēmējiem, un tajā pašā laikā maksimizēt pakalpojuma sniedzēja ieguvumus no izdalītajiem resursiem. Dažādie pakalpojumi un servisi nosaka vēlmi pēc to diferencēšanas piekļuves vadības līmenī ar iespēju izpildīt uz prioritātēm balstītu vadības politiku, it sevišķi brīžos, kad trūkst brīvo resursu. Visbiežāk augstākas kvalitātes prasības ir saistītas ar augstāku pakalpojuma cenu. Prioritāra piekļuves vadības politika nosaka iespēju nodrošināt plūsmu pieslēgšanu, selektīvi balstoties uz savstarpējas izvērtēšanas principiem. Tomēr, lai to realizētu, jāmaina līdzšinējo piekļuves vadības risinājumu viena izteikta un kopīga iezīme – tie visi strādā reaktīvi (momentāni) uz katru jaunu pieprasījumu, un nav iespējams tos savstarpēji izvērtēt, lai prioritātes izmantošana iegūtu savu patieso nozīmi. Šis aspekts nozīmē, ka esošos piekļuves vadības risinājumos trūkst izvēles iespējas starp viens otram tuvu sekojošiem savienojuma pieprasījumiem, jo joslas resursu trūkuma brīžos ir būtiski, kuras plūsmas tiks apstiprinātas.

ITU-T. Arī Starptautiskās telekomunikāciju savienības Telekomunikāciju standartizācijas sektors (ITU-T) ir analizējis un izstrādājis rekomendācijas [21], [22], kuras nosaka vispārēju arhitektūru, informācijas apmaiņas interfeisus un to galvenos uzdevumus tīkla resursu un piekļuves vadības funkcionālā bloka RACF realizācijai NGN tīklos. ITU-T Rec.Y2171 **ar terminu „piekļuves vadība” definē darbību un vadības politikas kopumu, lai noraidītu vai apstiprinātu jaunas sesijas iestatīšanu tīklā, izvērtējot QoS prasības, prioritāti un aktuālo resursu pieejamību.** Vadības politiku nosaka tīkla operators. Tomēr šīs rekomendācijas ir paredzētas tikai kā vadlīnijas, bet konkrētas RACF funkcionālās realizācijas ir tīkla uzturētāju, aparatūras un programnodrošinājuma izstrādātāju ziņā.

Problēmas nostādne. Viss iepriekš aprakstītais ļauj definēt problēmas nostādni. Pašreiz esošie piekļuves vadības risinājumi momentāni reaģē uz katru jaunu savienojuma pieprasījumu. Šāda nekavējoša un neatkarīga pieprasījumu apstrādes maniere to ierašanās kārtībā neļauj īstenot savstarpēji salīdzinošu, prioritāru un proaktīvu lēmuma pieņemšanu, lai savstarpēji izvērtētu vairākus pieprasījumus vienlaicīgi. Var uzskaitīt vairākas funkcijas, kuras nenodrošina esošie piekļuves vadības risinājumi:

- trūkst iespējas izpildīt patiesi selektīvu un prioritāru vadības politiku,
- neparedz iespēju uzkrāt pieprasījumus to tālākai analīzei,
- trūkst salīdzinošas izvērtēšanas starp cieši sekojošiem pieprasījumiem,
- spēju neīstenot neatkarīgu lēmumu pieņemšanu – nekavējoties uz katru jaunu pieprasījumu,
- netiek nodrošināta proaktīva rīcība piekļuves vadībā.

Turklāt secīga, momentāna un savstarpēji neizvērtējoša plūsmu apstrādes maniere veicina visu prioritāšu klašu tiekšanos saņemt vienādu atteikuma iespējamību, neveicinot prioritāru pieeju lēmumu pieņemšanas brīdī.

Izvirzās uzdevums: kā paplašināt izvēles iespējas un samazināt nepilnas informācijas apstākļus lēmuma pieņemšanas brīdī, lai veicinātu selektīvu un prioritāru lēmumu pieņemšanu un paaugstinātu gūto labumu no pieņemtajiem lēmumiem?

Viss iepriekš minētais motivēja promocijas darba autoru pievērsties piekļuves vadības problēmu risināšanai. Darbs ir veltīts jaunas piekļuves vadības metodes izstrādei un novērtēšanai. Uzdevumā ietilpa radīt risinājumu, kurš būtu efektīvs no patērēto skaitļošanas resursu viedokļa, tādējādi piemērots izmantošanai mūsdienu ātrgaitas datu pārraides tīklos un spētu nodrošināt proaktīvu, selektīvu un prioritāru piekļuves vadību.

Darba mērķis un uzdevumi

Ņemot vērā mūsdienu prasības un iepriekš minētos faktus, tika izvirzīts promocijas **darba mērķis**: izstrādāt jaunu savienojumu piekļuves vadības rīku un risinājumu, kurš spēj nodrošināt vairāku pieprasījumu savstarpēju izvērtēšanu, tādējādi paplašinot lēmumu pieņemšanas iespējas, ļaujot veidot selektīvu, prioritāru un proaktīvu piekļuves vadību, nodrošinot gūtā labuma pieaugumu no apstiprinātām plūsmām.

Promocijas darbā nosprausto mērķu sasniegšanai tika izvirzīti šādi **uzdevumi**:

- 1) novērtēt eksistējošo resursu un piekļuves vadības metožu un risinājumu piemērotību piekļuves vadības uzdevumam, iezīmējot tā galvenos trūkumus;
- 2) novērtēt mūsdienu datu plūsmu īpašības, to tendences un radītos jaunus izaicinājumus trafika vadības plāksnē;
- 3) definēt jaunu piekļuves vadības metodi, kas būtu par pamatu eksperimentāla pētāmā AggSessAC modeļa izstrādei;
- 4) izstrādāt definētajai piekļuves vadības metodei programmatisku aģentu, kuru iespējams implementēt maršrutētājos, papildinot to funkcionālās iespējas;
- 5) papildināt INET ietvarā pieejamā maršrutētāja funkcionalitāti ar izstrādāto AggSessAC programmatisko aģentu, radot eksperimentālo prototipu un dodot iespēju to novērtēt OMNeT++ simulācijas vidē;

- 6) izveidot eksperimentālu tīkla simulācijas vidi, kas ļautu analizēt jauno izstrādāto metodi un novērtēt tās efektivitāti, salīdzinot to ar piekļuves vadības metodi, kura izmanto klasisko savienojuma pieprasījumu apstrādes veidu;
- 7) analizēt AggSessAC metodē ietverto parametru ietekmi uz sasniegtajiem rezultātiem, dot rekomendācijas to robežvērtību izvēlei un adaptācijas iespējām.

Pētījumu metodika

Promocijas darbā, pamatojoties uz autora veiktajiem mērījumu rezultātiem, tika veikta plaša mūsdienu datu plūsmu analīze un gūtie secinājumi tika salīdzināti ar citiem zinātniskajos izdevumos sniegtajiem rezultātiem. Šāda mūsdienu interneta trafika analīze daudzos šķērsgriezumos – pakešu, plūsmu, protokolu – deva iespēju pamatot pētījuma virziena aktualitāti un kalpoja par pamatu jaunas piekļuves vadības paņēmiena izstrādei.

Modelēšana *Matlab* vidē tika izmantota, lai novērtētu sākotnējo projektētās piekļuves vadības koncepciju.

Jaunās piekļuves vadības metodes eksperimentāls prototips tika realizēts INET bibliotēku ietvarā esošajā maršrutētājā, papildinot tā funkcionalitāti un dodot iespēju to novērtēt OMNeT++ simulācijas vidē. Simulācijas eksperimenti veikti, lai analizētu izstrādātās metodes darbību un tās parametrus un salīdzinātu efektivitāti attiecībā pret klasisko pieprasījumu apstrādes veidu.

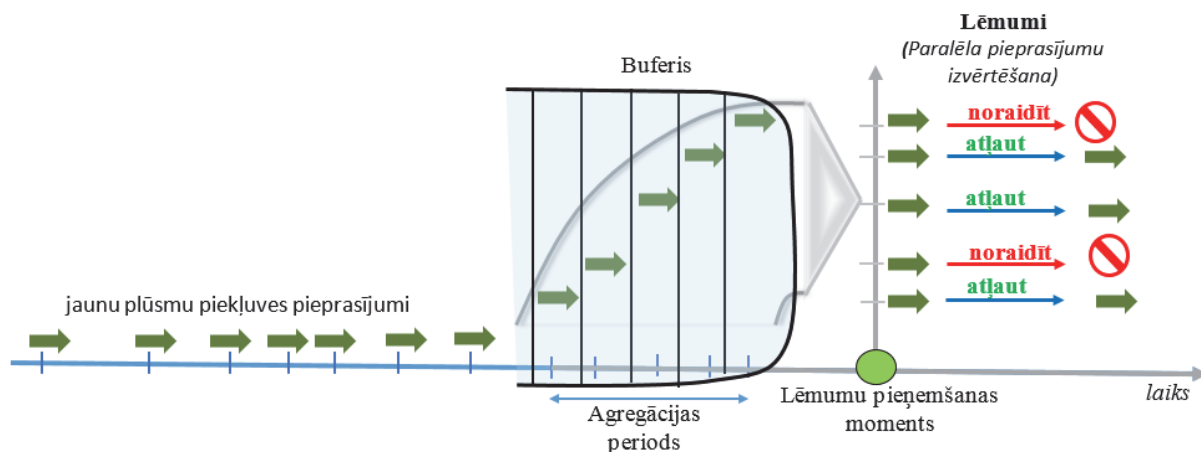
Statistiskās metodes tika izmantotas trafika mērījumu un simulācijas eksperimentu apstrādei.

Pētījumu rezultāti un zinātniskā novitāte

Promocijas darba ietvaros ir izstrādāta jauna savienojumu piekļuves vadības metode NGN ātrgaitas datu pārraides tīkliem. Izstrādāts metodei atbilstošs funkcionāls bloks, kas šajā darbā apzīmēts ar AggSessAC (no angļu val. *Aggregated Session Admission Control*), radot eksperimentālu produktu un ļaujot veikt tā novērtēšanu.

Ņemot vērā mūsdienu trafika apjoma augošās tendences, arvien pieaugošo apstrādājamo plūsmu skaitu, kā arī maršrutētāju veiktspējas attīstību, autors izvirza ideju – veikt īslaicīgu jaunu savienojumu pieprasījumu agregāciju, novirzot jaunu savienojumu inicializācijas paketes atsevišķā rindā, lai lēmumu pieņemšanas brīdī iegūtu spējas pieņemt lēmumus proaktīvi, prioritāri, salīdzinot pieprasījumus savstarpēji, tādējādi paaugstinot gūto labumu no pieņemtajiem lēmumiem. Pēc autora ziņām, šāda pieeja resursu un piekļuves vadībā līdz šim nav pētīta.

Izstrādātā risinājuma koncepcija (skat. 4. att.) iekļauj plūsmu klasifikāciju, plūsmu stāvokļu uzturēšanu, jaunu savienojumu inicializācijas pakešu uzkrāšanu un novirzīšanu atsevišķā rindā. Pieprasījumu agregācija dod iespēju piekļuves vadībā ieviest paralēlas apstrādes virtualizāciju un samazināt nenoteiktību lēmumu pieņemšanas brīdī. Šajā promocijas darbā autors ar piekļuves pieprasījumu apzīmē jaunai individuālai datu plūsmai (sesijai) piederošas paketes, kas saņemtas piekļuves vadības modulī. Gribētu precizēt, ka darbā minētie vārdi “**pieprasījums**” un “**jaunas plūsmas pieprasījums**” ir lietoti kā sinonīmi un apzīmē jauna savienojuma prasību.



4. att. Promocijas darbā izvirzītās jaunās piekļuves vadības darbības idejiskā nostādne (pieprasījumu agregācija nodrošina paralēlas apstrādes virtualizāciju).

Darba praktiskā vērtība

- Izstrādāta jauna piekļuves vadības metode, kā arī ir veikta izveidotā modeļa verifikācija un validācija.
- Izstrādāts AggSessAC metodes funkcionālais aģents uz C++ valodas bāzes, kas ļauj papildināt maršrutētāja piekļuves vadības funkcionālās iespējas.
- Pētījumu gaitā ar izstrādāto funkcionālo bloku papildināta INET ietvarā OMNeT++ simulācijas vidē esošā maršrutētāja funkcionalitāte, ļaujot veikt metodes eksperimentālu novērtēšanu, kā arī dodot iespēju to izmantot citos pētījumos.

Aizstāvamās tēzes

1. Pieaugot datu plūsmu intensitātei (jaunas plūsmas/s), kura nākamās paaudzes tīklos ir mērāma ar kārtu 10^3 vai vairāk, un lai realizētu piekļuves vadības politikas prasības, lēmumu pieņemšanu par plūsmu apstiprinājumu var realizēt, ienesot sesijas inicializācijas aizturi; rezultātā, salīdzinot ar esošiem piekļuves vadības risinājumiem, lēmuma pieņemšanas brīdī tiek analizēta uzkrāto pieprasījumu kopa, kura nodrošina plašākas selektīvas izvēles spējas, atbilstoši uzkrāto pieprasījumu apjomam samazinot nenoteiktību lēmumu pieņemšanas brīdī.
2. AggSessAC piekļuves vadības metodes izmantošana palielina augstāko prioritāšu plūsmu pieslēgumu skaitu, nodrošinot uzstādītās vadības politikas prasību izpildi attiecībā uz apkalpošanas prioritātes līmeņiem, un palielina piekļuves vadības efektivitāti.
3. Izstrādātā AggSessAC piekļuves vadības metode, kas balstās uz īslaicīgu lēmuma pieņemšanas procesa aizturi un jaunu savienojuma pieprasījumu uzkrāšanu, ir piemērota izmantošanai tiešsaistes režīmā ātrgaitas (gigabitu) pārraides kanālos, nodrošinot to, ka ienestā aizture neietekmē jau apstiprināto plūsmu kvalitāti un nepārsniedz dažu (<5) ms robežu.

Rezultātu aprobācija

Promocijas darba galvenie rezultāti tika prezentēti 8 starptautiskās zinātniskajās konferencēs.

1. The Twentieth IEEE Symposium on Computers and Communications (ISCC 2015), Kipra, Larnaka, 6.–9. jūlijs, 2015.
2. 29th IEEE International Conference on Advanced Information Networking and Applications (AINA-2015), Korejas republika, Gwangju, 25.–27. marts, 2015.
3. 22nd Telecommunications Forum TELFOR 2014, Serbija, Belgrada, 25.–27. novembris, 2014.
4. IET International Conference on Information and Communications Technologies (IETICT 2013), Ķīna, Pekina, 27.–29. aprīlis, 2013.
5. Electronics and Electrical Engineering, Lietuva, Palanga, 17.–19. jūnijs, 2013.
6. The 20th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2012), Horvātija, Splita, 11.–13. septembris, 2012.
7. Electronics and Electrical Engineering, Lietuva, Palanga, 18.–20. jūnijs, 2012.
8. Electronics and Electrical Engineering, Lietuva, Kauņa, 17.–19. maijs, 2011.

Kopumā ir publicēti 11 zinātniski raksti dažādos zinātniskos izdevumos.

1. **Skrastiņš A.**, Jeļinskis J., Lauks G., Comprehensive analysis of AggSessAC method for revenue maximization using OMNeT++. // The Twentieth IEEE Symposium on Computers and Communications (*ISCC 2015*), Kipra, Larnaka, jūlijs, 2015, 777.–782. lpp. (***IEEE Xplore un Scopus datubāzēs.***)
2. **Skrastiņš A.**, Lauks G. Evaluation of AggSessAC Admission Control Solution to Improve Network Revenue. // *29th IEEE International Conference on Advanced Information Networking and Applications (AINA-2015)*, Korejas republika, Gwangju, marts, 2015, 23.–28. lpp. (***IEEE Xplore un Scopus datubāzēs.***)
3. **Skrastiņš A.** Admission Control Scheme for Effective Revenue Management in NGN Networks. // *22nd Telecommunications Forum TELFOR 2014*, Serbija, Belgrada, novembris, 2014, 174.–177. lpp. (***IEEE Xplore un Scopus datubāzēs.***)
4. **Skrastiņš A.**, Jeļinskis J., Lauks G. Evaluation of New Approach for Fair Downlink Bandwidth Distribution in TCP/IP Networks. // *IET International Conference on Information and Communications Technologies (IETICT 2013)*, Ķīna, Pekina, aprīlis, 2013, 117.–123. lpp. (***IEEE Xplore datubāzē.***)
5. **Skrastiņš A.**, Jeļinskis J., Lauks G. Fair Bandwidth Sharing Scheme based on Upload Traffic Control. // *Electronics and Electrical Engineering*, No. 20(1), ISSN 1392-1215, *Electronics and Electrical Engineering*, Lietuva, Palanga, jūnijs, 2013, 96.–99. lpp. (***Scopus datubāzē.***)
6. **Skrastiņš A.**, Jeļinskis J., Lauks G. Evaluation of Selective Aggregated Session CAC for QoS Provisioning in All-Optical Networks. // *The 20th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2012)*, Horvātija, Splita, septembris, 2012, 1.–5. lpp. (***IEEE Xplore un Scopus datubāzēs.***)
7. **Skrastiņš A.**, Jeļinskis J., Lauks G. Selective Aggregated Session Control with QoS Provisioning for GMPLS Networks. // *Electronics and Electrical Engineering*, No. 122(6), ISSN 1392-1215, *Electronics and Electrical Engineering*, Lietuva, Palanga 18.–20. jūnijs, 2012, 75.–78. lpp. (***Scopus datubāzē.***)

8. Lauks G., **Skrastiņš A.**, Jeļinskis J. Testing the Null Hypothesis of Stationarity of Internet Traffic. // Electronics and Electrical Engineering, No. 112(6), ISSN 1392-1215, Electronics and Electrical Engineering, Lietuva, Kauņa, maijs, 2011, 29.–32. lpp. (**Scopus datubāzē.**)
9. Jeļinskis J., **Skrastiņš A.**, Lauks G. Practical Fuzzy-CAC Realization for Effective Traffic Engineering in MPLS-TE Network. // Electronics and Electrical Engineering, No. 4(110), Kaunas: Technologija, 2011, 30.–34. lpp. (**Scopus datubāzē.**)
10. Jeļinskis J., **Skrastiņš A.**, Lauks G. Fuzzy-CAC Driven MPLS-TE Realization. // 12th IEEE International Conference on High Performance Switching and Routing, Spānija, Kartagena, jūlijs, 2011, 146.–150. lpp. (**IEEE Xplore un Scopus datubāzēs.**)
11. Jeļinskis J., **Skrastiņš A.**, Lauks G. Fuzzy-CAC based Traffic Management in MPLS-TE Networks. // 11th International Conference on Telecommunications, ConTEL 2011, Graz, Austrija, jūnijs, 2011, 389.–395. lpp. (**IEEE Xplore un Scopus datubāzēs.**)

Promocijas darba izstrādes laikā gūtie rezultāti tika izmantoti vairāku projektu pētījumu daļas realizācijā

1. “Ātrdarbīgo optisko piekļuves tīklu un elementu izstrāde.” Projekta Nr.:2010/0270/2DP/2.1.1.1.0/10/APIA/VIAA/002.
2. “Viedās pilsētas tehnoloģijas dzīves kvalitātes uzlabošanai.” Projekta Nr.:2013/0008/1DP/1.1.1.2.0/13/APIA/VIAA/016.
3. “Uz nestriktās loģikas principiem balstītu matemātisku struktūru lietojumi telekomunikāciju tīklu projektēšanas un resursu vadības tehnoloģiju attīstībai.” Projekta Nr.:2013/0024/1DP/1.1.1.2.0/13/APIA/VIAA/045.

Darba apjoms un struktūra

Promocijas darba apjoms ir 162 lappuses. Darbs sastāv no ievada, saīsinājumu saraksta, četrām nodaļām, secinājumiem un literatūras saraksta.

Darba pirmā nodaļa ir veltīta īsai esošo trafika vadības risinājumu analīzei, dots pašreizējo piekļuves vadības risinājumu novērtējums, salīdzinātas to priekšrocības un trūkumi. Nodaļā aplūkotas ITU-T izvirzītās vadlīnijas resursu un piekļuves vadībai NGN tīklos. Analizēti iespējamie virzieni, kā izstrādāto AggSessAC metodi savietot ar QoS prasību nodrošināšanas rīkiem, veidojot piemērotu risinājumu mūsdienu ātrgaitas (gigabitu) tīkliem.

Otrajā nodaļā ir demonstrētas un izceltas mūsdienu ātrgaitas datu pārraides tīklu izvirzītās prasības piekļuves vadības risinājumiem. Analizēts mūsdienu pārraides tīklos esošais trafiks no datu plūsmu viedokļa dažādos šķērs griezumos: plūsmu intensitāte, plūsmu apjomi, plūsmu izmēri, plūsmu ilgums, izmantotie protokoli, plūsmu ierašanās sadalījumi. Akcentēti plūsmu veidi, kas dominē mūsdienu interneta datu pārraides tīklos. Pamatojoties uz interneta trafika analīzes rezultātiem un iegūtajiem secinājumiem par apstrādājamo plūsmu apjomiem, promocijas darba autors veicis arī trafika klasifikatoru analīzi, novērtējot to spēju strādāt tiešsaistes režīmā ar augstiem pārraides ātrumiem un caurlaidspēju ≥ 1 Gbit/s. Visi šajā nodaļā gūtie secinājumi iezīmē pašreizējo interneta datu pārraides situāciju un to izvirzītās prasības piekļuves vadībai kā arī pamato izstrādātās AggSessAC metodes nepieciešamību priekš mūsdienu ātrgaitas datu pārraides tīkliem.

Trešajā nodaļā ir izstrādāta AggSessAC rīka un risinājuma realizācija. Nodaļā ir dotas izstrādātā AggSessAC funkcionālā bloka (aģenta) pamatfunkcijas, definēti AggSessAC risinājumā ietvertie parametri un to izvēle. Veikta izstrādātā AggSessAC funkcionālā aģenta īstenošana OMNeT++ vidē, papildinot INET ietvarā esošā maršrutētāja funkcionalitāti ar jauno darbā izstrādāto piekļuves vadības risinājumu.

Ceturtnā nodaļā ir veltīta izstrādātā AggSessAC piekļuves vadības risinājuma un izveidotā funkcionālā bloka verifikācijai un validācijai OMNet++ simulācijas vidē izveidotajā eksperimentālajā tīklā, izmantojot maršrutētāju, kura programmatūra papildināta ar izstrādāto AggSessAC piekļuves vadību. Nodaļā ir novērtēti AggSessAC risinājumā ietvertie parametri un raksturota to ietekme uz kopējo efektivitāti pie dažādiem ieejas trafikiem.

Darba noslēgumā ir apkopoti promocijas darba galvenie secinājumi.

DARBA ATSEVIŠĶO NODAĻU IZKLĀSTS

Pirmā nodaļa

Pirmā nodaļa ir veltīta esošo piekļuves vadības risinājumu analīzei, un tajā aplūkotas rekomendācijas un kritēriji, kuri jāņem vērā, plānojot jaunas piekļuves vadības realizācijas. Doti caurlaides joslas pārvaldības un QoS nodrošināšanas iespēju pētījumu rezultāti, kā arī novērtētas prognozēšanas metožu iespējas zināšanu apjoma paplašināšanai lēmumu pieņemšanas brīdī.

Piekļuves vadība ir viens no elementiem resursu un datu plūsmu pārvaldībā, kas ļauj vadīt un organizēt resursu izdali un jaunu savienojumu apstiprināšanu nepietiekamu brīvo resursu situācijās. Plānojot piekļuves risinājumu izstrādi, jāreķinās ar virkni dažādu uzdevumu, ieskaitot pakešu/plūsmu klasifikāciju, rindošanu, pieejamo resursu uzraudzību, resursu piešķiršanu un citiem uzdevumiem. Visu šo iesaistīto uzdevumu kopēja un koordinēta pārvaldība var radīt vēlamu rezultātu.

Arī ITU-T ir izstrādājusi **rekomendācijas piekļuves vadībai NGN tīklos**. Rekomendācija Y.2111 dod resursu un piekļuves vadības funkciju aprakstu un definē vispārēju RACF struktūru ar tajā ietvertiem funkcionāliem blokiem, savukārt Y.2171 definē kritērijus un vadlīnijas, kuri būtu jāievēro, veidojot prioritāšu balstītu piekļuves lēmumu pieņemšanu:

- trīs pamatkritēriji, kas jāizvērtē lēmumu pieņemšanas brīdī:
 - pieprasījuma prasītie veikspējas kritēriji (josla, aizture u. c.),
 - prioritāte,
 - aktuālā resursu pieejamība;
 - trafikam ar augstāku prioritāti jāsaņem augstākas apstiprināšanas garantijas,
 - prioritātes līmeņi nav tieši atkarīgi no ITU-T Y.1541 definētām QoS klasēm, kas balstās uz transporta slāņa metrikām,
 - prioritāšu skaits nav ierobežots un pēc vajadzības var tikt paplašināts;
- Plānojot izstrādāt piekļuves vadības metodi, tai tika izvirzīts uzdevums nodrošināt:
- selektīvu, prioritāru un savstarpēji izvērtējošu lēmuma pieņemšanu,
 - augstu veikspēju un savietojamību ar mūsdienu trafika inženierijas risinājumiem.

Darbā īsi aprakstītas divas **standartizētas QoS nodrošināšanas pieejas**:

- integrētie servisi (IntServ),
- diferencētie servisi (DiffServ).

Šie risinājumi eksistē kā trafika vadības risinājumu pamats pakešu tīklos [3], [60].

Integrētie servisi strādā plūsmu līmenī un izmanto gals–gals resursu rezervāciju. Šāds risinājums nosaka prasību uzturēt plūsmu stāvokļus uz mezgliem, kurus šķērso datu plūsma. IntServ rada mērogojamības problēmas augstā rezervējamo resursu intensitātē, ja ir liels jaunu plūsmu skaits [1], [14]. Augsta plūsmu intensitāte liek veikt ātru resursu rezervāciju, bet resursu gals–gals rezervēšana prasa laiku, lai noskaidrotu pieejamo resursu situāciju visa ceļa garumā, un ierobežo metodes izmantošanu individuālu datu plūsmu (sesiju) līmenī ātrgaitas datu pārraides tīklos.

Atšķirībā no IntServ risinājuma DiffServ strādā pakešu līmenī, pieņemot lēmumus par pakešu virzību katrā mezglā neatkarīgi pēc PHB principa. PHB vadība izmanto paketes marķējumu, kas nosaka apkalpošanas prioritāti. DiffServ gadījumā gals–gals QoS nodrošināšana būs atkarīga no noslogotākās vietas tīklā, tādējādi tas spēj nodrošināt tikai relatīvās QoS garantijas. Lai šīs problēmas risinātu, ir veikta virkne pētījumu, kuros zinātnieki centušies kombinēt gan pakešu līmeņa, gan plūsmu līmeņa pārvaldību (angļu val. *flow-aware networking*), lai varētu izpildīt gals–gals datu plūsmu QoS garantijas (skat. [28], [43], [46], [51]).

Pēc ITU-T rekomendācijas Y.2111, var nodalīt divu veidu QoS nodrošināšanas tipus [22]:

- 1) *absolūtais QoS* – vadība balstās uz QoS parametru (pakešu aizture, trīce, zudumi u. c.) mērījumiem un/vai resursu rezervāciju;
- 2) *relatīvais QoS* – vadība balstās uz prioritāru pakešu apstrādi, un tas izmantots tīklos, kur sarežģīti nodrošināt absolūtās QoS garantijas.

Absolūto QoS prasību izpildē var nodalīt divus pamata risinājumus:

- 1) *resursu rezervācija* – IntServ princips, kur galvenais trūkums ir mērogojamība attiecībā pret pienākošo plūsmu intensitāti ātrgaitas datu pārraides tīklos;
- 2) *caurlaides joslas uzraudzība/vadība* – uzturēt līnijas noslodzi definētās robežās, neļaujot līnijai pilnībā aizpildīties. Pārvaldības efektivitāti var palielināt, to izmantojot kopā ar piemērotiem piekļuves vadības risinājumiem, kuri nosaka pieejamās joslas aizpildīšanu ar datu plūsmām. Promocijas darbā izstrādātā AggSessAC piekļuves vadības metode projektēta risinājumiem ar caurlaides joslas pārvaldību.

Darbā dota arī īsa **esošo piekļuves vadības risinājumu analīze**. Esošos piekļuves vadības risinājumus pēc to funkcijām un darbības nodrošināt QoS prasību izpildi var iedalīt divās grupās:

- 1) mērījumos balstītie MBAC risinājumi,
- 2) parametros balstītie PBAC risinājumi.

MBAC gadījumā, veidojot piekļuves vadības lēmumu, tiek izmantoti kanāla QoS parametru mērījumu rezultāti. Var nodalīt divus mērījumu veidus [59]:

- 1) pasīvi mērījumi – izmanto bufera izmēra analīzi, lai noteiktu tīkla QoS parametrus, izmantojot faktu, ka starp bufera izmēru, līnijas noslodzi un pakešu zudumiem pastāv korelācija;

- 2) aktīvi mērījumi – izmantojot zondes ziņojumus, kas mēra dotā mirkļa QoS parametrus (aizturi, trīci).

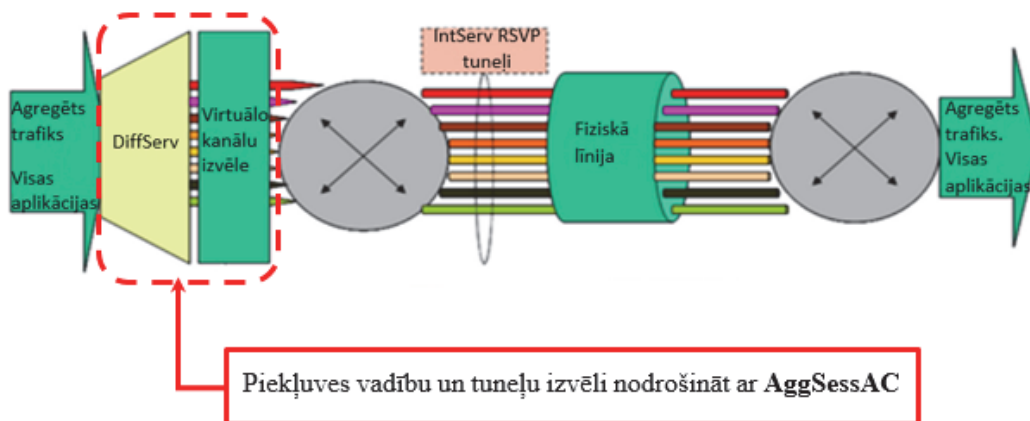
MBAC realizācija sesiju līmenī uz katru jaunu savienojuma pieprasījumu var radīt būtiskas veiktspējas problēmas un ierobežot šādas metodes izmantošanu ātrgaitas gigabitu tīklos. Šeit ļoti svarīgs kļūst mērījumu iegūšanas ātrums. Tādēļ vienmēr paliek atvērts jautājums par mērījumu biežumu – pārāk reti mērījumi var neatspoguļot tīkla patieso situāciju lēmuma pieņemšanas brīdī, kamēr ļoti bieži veikti mērījumi labāk ataino patieso situāciju tīklā, kaut gan prasa vairāk resursu to iegūšanai.

Var nodalīt PBAC risinājumus bez resursu rezervācijas un ar resursu rezervāciju. Galvenais PBAC ar resursu rezervāciju ieguvums ir spēja nodrošināt spēcīgas QoS garantijas, bet to PBAC risinājumu, kas balstīti tikai uz izejošā kanāla noslodzes kontroli un vadību, ieguvums ir salīdzinoši vienkāršā ieviešana un augstā veiktspēja, kas piemērotāka realizācijai tiešsaistes režīmā. Tomēr gadījumos ar biežiem trafika uzliesmojumiem šādi PBAC risinājumi, kas pamatojas uz izejošā kanāla noslodzi apgrūtinā pieļaujamās noslodzes sliekšņa vērtības uzturēšanu: pārāk augsta noslodze apgrūtinās QoS prasību ievērošanu, un pārāk zema noslodze izraisīs neefektīvu resursu izmantošanu. Plašāk ar MBAC un PBAC principiem var iepazīties zinātniskajos rakstos (skat., piemēram, [5], [15], [23], [24], [32], [33], [38], [41], [50], [64]).

Saistībā ar QoS prasību izpildes iespējām, kas tiek organizētas ar piekļuves vadības metodi, promocijas darba autors ir veicis pētījumus par nestriktajā loģikā balstītām piekļuves vadības iespējām MPLS-TE tīklos [25], [26], [27]. Šajos pētījumos individuālu plūsmu līmenī tiešsaistes režīmā ar RSVP-TE protokola palīdzību tika dinamiski vadīti un rezervēti jaunam savienojumam nepieciešamie resursi. Šie pētījumi uzrādīja, ka, **uzturot joslas noslodzi noteiktās robežās (<85 %) un atstājot vietu trafika uzliesmojumiem, tiks saglabātas arī QoS prasības.** Šāda pieļaujamās noslodzes sliekšņa uzturēšana vienkāršo piekļuves vadību, ļaujot izvairīties no laikietilpīgiem un nepārtrauktiem QoS parametru mērījumiem, kā, piemēram, pakešu gals–gals aiztures, un veidot risinājumu ar augstu veiktspēju. Tas samazina arī nepieciešamos skaitļošanas resursus, kas ir sevišķi svarīgi, veidojot piekļuves vadību sesiju līmenī ar augstu jaunu savienojumu pieprasījumu intensitāti. Lai efektīvāk izmantotu pieejamos resursus, šādus risinājumus var papildināt ar dinamisku sliekšņa vērtības uzturēšanu, tomēr tie būs prasīgāki pret nepieciešamajiem skaitļošanas resursiem, piemēram, izmantojot jau minēto nestrikto loģiku. Šāda pieeja principā paredz uzturēt tādu kā “buferzonu” trafika uzliesmojumiem, lai izpildītu QoS prasības, un, kombinējot ar trafika inženierijas un resursu pārdales risinājumiem, var palielināt resursu efektīvu izmantošanu, piemēram, ar MPLS-TE.

Arī pētījumos [54], [55] to autori uzsver MPLS slāni kā vienu no potenciāli piemērotām vietām piekļuves kontroles mehānisma izvietojšanai pamattīklā un MPLS-TE virtuālo kanālu iespējas nodrošināt gals–gals QoS garantijas pamattīkla ietvaros.

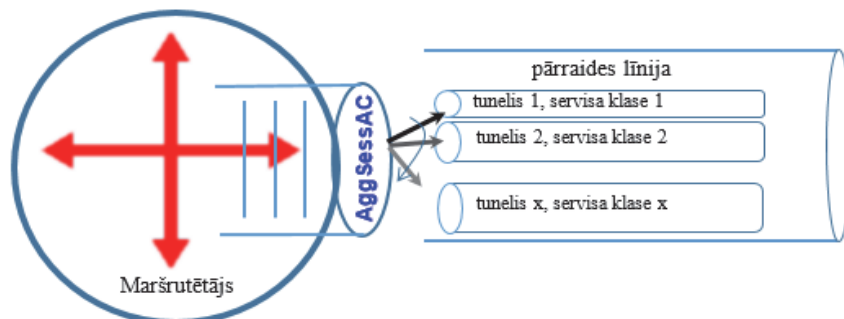
Līdzīga pieeja ir analizēta pētījumā [4], kur trafika izvietošana pa MPLS-TE tuneliem tiek organizēta, pakešu līmenī izmantojot DiffServ palīdzību, bet promocijas darba autora vēlme ir pārveidot šo principu par plūsmu līmeņa vadību. Tas liek veidot piemērotu piekļuves vadības metodi, kas prioritāri aizpildītu šos virtuālos kanālus ar datu plūsmām, aizstājot DiffServ pieeju ar šajā darbā izstrādāto AggSessAC piekļuves vadības metodi (skat. 5. att.).



5. att. AggSessAC ļauj aizstāt pakešu balstītu piekļuves vadību (DiffServ) ar plūsmu līmeņa piekļuves vadību.

Pamatojoties uz iepriekš minēto un veiktajiem pētījumiem, šī promocijas darba autors definē darbības apgabalu un izstrādā jaunu resursu un piekļuves vadības risinājumu – AggSessAC.

1. AggSessAC piekļuves vadības metode projektēta izmantošanai ātrgaitas (gigabitu) interneta pakalpojumu sniedzēju tīklos, ļaujot realizēt diferencētu un prioritāru vadību sesiju līmenī un nodrošināt selektīvas izvēles spējas lēmumu pieņemšanas brīdī.
2. AggSessAC metode strādā kā operators, kurš izvieto plūsmas pa virtuāliem kanāliem, savukārt trafika inženierija (TE) ļauj šķērsot pamattīklu ar vienu loģisko lēcieni, izpildot tikai vienu lēmuma pieņemšanu uz šķautnes maršrutētāja (skat. 6. att.).



6. att. AggSessAC metode kopā ar trafika inženierijas metodēm.

Visiem promocijas darba autoram zināmiem piekļuves vadības risinājumiem ir viena raksturīga pazīme – piekļuves pieprasījumus apstrādāt neatkarīgi, to ierašanās kārtībā, tādējādi nenodrošinot izvērtēšanu starp ļoti tuvu sekojošiem pieprasījumiem, kas rada arī problēmas realizēt selektīvu un prioritātēs balstītu piekļuves vadību. Lai to panāktu, piekļuves vadības blokam lēmuma brīdī būtu jāsaņem piekļuves pieprasījumu kopa, tādējādi nodrošinot izvēles iespējas, līdzīgi kā pakešu apstrāde rindā ar DiffServ vadības stratēģiju. Pieprasījumu kopu var iegūt:

- 1) uzkrājot savienojuma pieprasījumus – tiek iegūtas reālas pieprasījuma vērtības, tomēr jāērēķinās, ka uzkrāšanai nepieciešama aizture;
- 2) prognozējot turpmākos pieprasījumus – neprasa aizturi, bet prognozēšanas rezultāti vienmēr ir varbūtiski.

Veicot prognozēšanu ar apmācību, visbiežāk tiek izmantota vēsturiska informācija, lai prognozēšanu sasaistītu ar tīklā notiekošo procesu, bet tas nosaka, ka prognozes rezultātos vienmēr būs korelācijas ar vēstures datiem, tāpēc tā vairāk piemērota tendenču prognozēšanai nevis precīzu piekļuves pieprasījumu prasību noteikšanai. Balstoties uz darbā iegūtajiem rezultātiem prognožu jomā, promocijas darba autors nolēma neiesaistīt prognozēšanas rīkus piekļuves vadības risinājumā, lai samazināt nepilnas informācijas apstākļus un mēģinātu radīt izvēles iespējas lēmuma pieņemšanas brīdī.

Promocijas darba autors savu izstrādāto metodi varētu pieskaitīt pie parametru un plūsmu balstīta piekļuves vadības risinājuma, kas izmanto plūsmu stāvokļu tabulas un atsevišķu buferi jaunu plūsmu pakešu uzkrāšanai, lai piekļuves lēmuma brīdī nodrošinātu diferencētu vairāku pieprasījumu savstarpēju izvērtēšanu. Darbā autors abstrahējas no MPLS-TE trafika inženierijas uzdevumiem, un autora tālākie pētījumi tiek koncentrēti uz AggSessAC piekļuves risinājuma izstrādi un novērtēšanu viena kanāla ietvaros.

Otrā nodaļa

Pirms piedāvāt kādu jaunu trafika vadības paradigmu, ir svarīgi precīzi raksturot mūsdienu trafiku. Tāpēc šīs nodaļas pirmo daļu autors velta trafika analīzei dažādos šķērsgriezumos – pakešu, plūsmu, protokolu, kas ļauj sastādīt „karti” turpmākam ceļam un iespēju pamatoti pieņemt kādu jaunu vadības paņēmieni vai arī atteikties no kāda jau esošā. Trafika raksturs mainās – jo mainās protokolu algoritmi, aplikāciju veidi, to prasības, lietotāju uzvedība. Mūsdienu reālijas liecina, ka jauno plūsmu pienākšanas ātrums pamattīklos ir ievērojami audzis, parādoties daudzām mazām plūsmām ar īsu dzīves ilgumu un noslogojot arī šķautnes mezglus ar lielu datu plūsmu apstrādi. Tas rada jaunus izaicinājumus trafika vadības plāknē. Autors ir veicis plašu interneta trafika analīzi, kas dod atbildi uz autoram aktuālu pamatjautājumu: ko jāspēj nodrošināt mūsdienu prasībām atbilstošam piekļuves vadības risinājumam? Piekļuves vadībai, balstoties uz pieejamajiem resursiem, ir jānodrošina selektīva, proaktīva, prioritātēs balstīta lēmumu pieņemšana, ar augstu veikspēju un savietojamai ar trafika inženierijas risinājumiem. Nodaļas otro daļu autors velta datu plūsmu klasifikācijas iespējām un to līdzšinējo veikspējas sasniegumu novērtēšanai, izvērtējot klasifikatoru iespējas strādāt individuālu plūsmu līmenī mūsdienu pamattīklos.

Analīzei autors izmanto paša trafika trases datus, kas iegūti vienā no Latvijā strādājošiem uzņēmumiem ar plašu telekomunikāciju tīklu infrastruktūru visā valsts teritorijā. Lai veidotu plašāku priekšstatu, iegūtie mērījumu dati salīdzināti arī ar CAIDA (no angļu val. *Center for Applied Internet Data Analysis*) [57], Amerikas Savienotajās Valstīs izveidota pētniecības centra, publiski pieejamiem interneta trafika statistikas datiem.

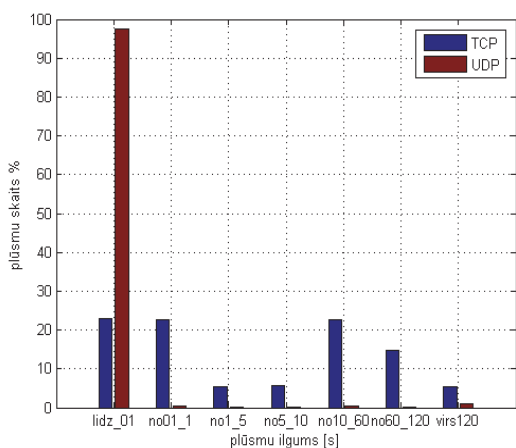
Datu plūsmu analīze

Analizējamais trases fails tika iegūts ar *tcpdump* rīku, un tika veikta plūsmu klasifikācija, izmantojot *wireshark* programmatūru [63]. Klasifikācija tika veikta pēc trijām un piecām plūsmu pazīmēm (skat. 1. tab.). Gadījumā ar piecām pazīmēm, atsevišķi nodalot UDP un TCP protokolus, analizējot porta numurus, – unikāli izšķirto plūsmu skaits palielinājās piecas reizes. Tas rāda, cik svarīgi IP plūsmu klasifikācijā ir veikt transporta slāņa informācijas analīzi, tādējādi ievērojami paaugstinot plūsmu izšķiršanas spēju, kaut arī tas prasa vairāk skaitļošanas resursu.

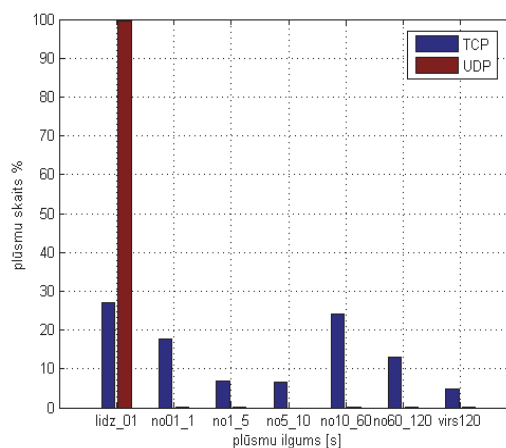
Izšķirto plūsmu skaits eksperimentālā trases failā

Plūsmas virziens	3 plūsmu pazīmes (IP protokols, avota IPv4 adrese, galamērķa IPv4 adrese)	5 plūsmu pazīmes (IP protokols avota/galamērķa IPv4 adrese, avota/galamērķa UDP/TCP porti)
Augšuplāde	10 602	
Lejuplāde	9862	
Augšuplāde TCP		31 153
Augšuplāde UDP		25 438
Lejuplāde TCP		31 015
Lejuplāde UDP		23 909

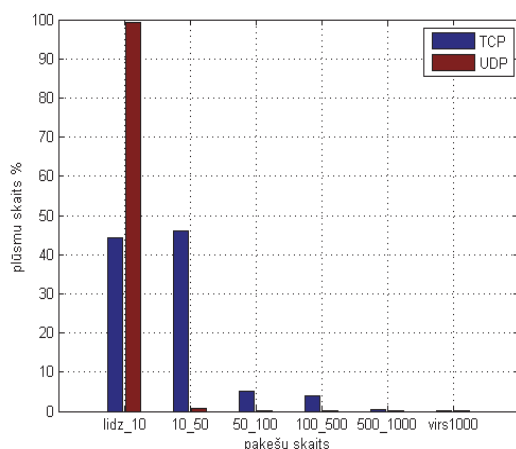
IPv6 izmantošanas gadījumā klasifikāciju atvieglo IPv6 virsrakstā ietvertais plūsmas identifikators, tādējādi līdzvērtīgai klasifikācijai pietiktu ar 3 IPv6 virsraksta lauku analīzi (attiecīgi – sūtītāja un saņēmēja IP adrese un plūsmas identifikators), izvairoties no transporta slāņa analīzes, kas atvieglo šifrēta trafika klasifikāciju.



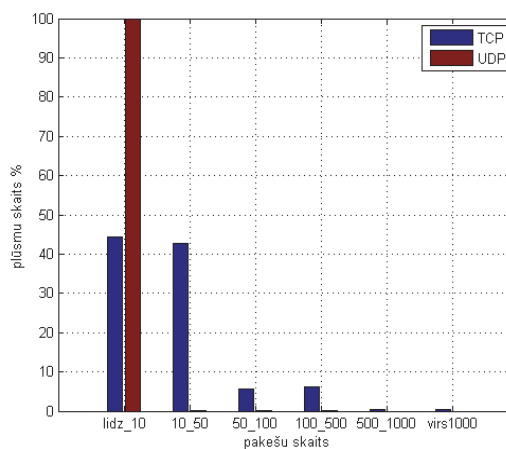
7. att. Histogramma ar augšuplādes plūsmu ilguma sadalījumu (7 laika apgabali).



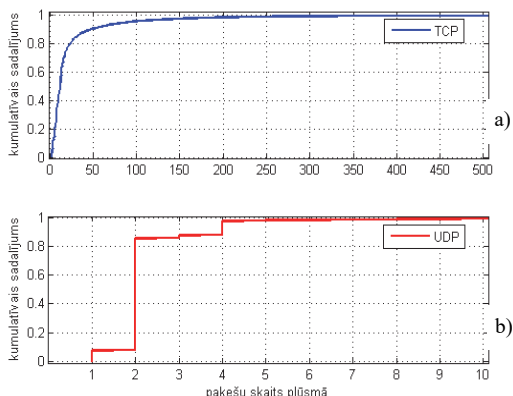
8. att. Histogramma ar lejuplādes plūsmu ilguma sadalījumu (7 laika apgabali).



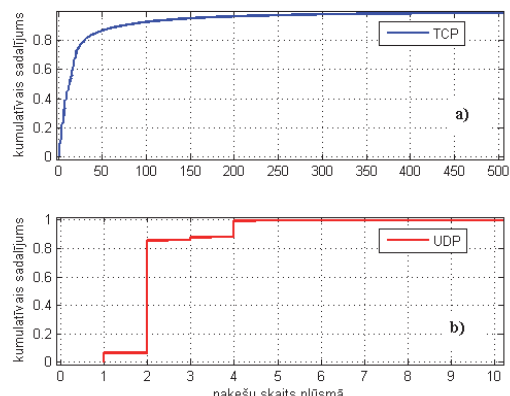
9. att. Histogramma ar augšuplādes plūsmu garumu [paketēs] (6 pakešu sk. diapazoni).



10. att. Histogramma ar lejuplādes plūsmu garumu [paketēs] (6 pakešu sk. diapazoni).



11. att. Augšuplādes plūsmu garuma kumulatīvais sadalījums: (a) pietuvinātā mērogā – līdz 500 paketēm garām TCP plūsmām, un (b) līdz 10 paketēm garām UDP plūsmām.



12. att. Lejuplādes plūsmu garuma kumulatīvais sadalījums: (a) pietuvinātā mērogā – līdz 500 paketēm garām TCP plūsmām, un (b) līdz 10 paketēm garām UDP plūsmām.

Piekļuves vadības risinājumiem svarīgi ir arī plūsmu virzieni. Uzņemtā trases faila analīze uzrāda, ka plūsmu sadalījums pēc plūsmu ilguma ietver ļoti līdzīgu ainu, gan augšupielādes, gan lejupielādes virzienam (7. un 8. att.). Attiecībā uz plūsmu ilguma noteikšanu tika nodalīti septiņi laika apgabali – attiecīgi plūsmas līdz 100 ms garas, no 100 ms līdz 1 s, no 1 s līdz 5 s, no 5 s līdz 10 s, no 10 s līdz 1 min, no 1 min līdz 2 min, un plūsmas, kas garākas par 2 minūtēm.

Galvenais, ko autors vēlas akcentēt, ir **lielais īso plūsmu skaits**, kas satur vien dažas paketes un ir ar ļoti īsu dzīves laiku. Piemēram, TCP plūsmu ilgums lejuplādes virzienā, kas dots 7. att., uzrādīja, ka ap 55 % no plūsmām nav garākas par 10 sekundēm un tikai 6 % plūsmu eksperimentālajos datos bija garākas par 2 min. Rezultāti uzrādīja, ka 44 % no TCP plūsmām nesaturēja vairāk kā 10 paketes un ap 90 % no plūsmām nesaturēja vairāk kā 50 paketes (skat. 10. att.); līdzīga aina attiecīgi ir arī augšuplādes virzienā (skat. 7. un 9. att.).

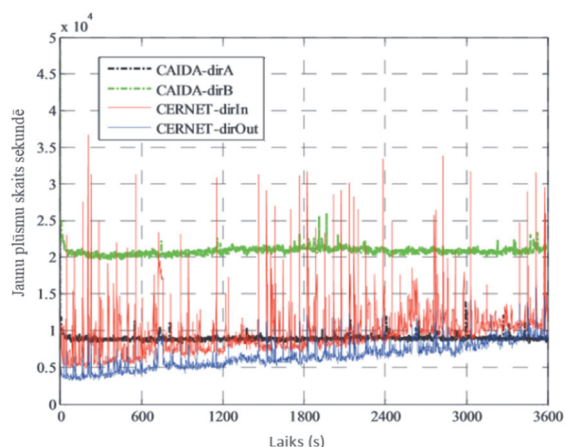
UDP plūsmu gadījumā 11. un 12. att. redzami rezultāti liecina, ka uzņemtajos eksperimentālajos trafika datos ap 99 % UDP plūsmu vienā virzienā nesatur vairāk kā 2 paketes. Šī aina ir principā identiska gan augšuplādes, gan lejuplādes virzieniem. Aplūkojot aplikācijas, kas izmantoja UDP kā transporta protokolu, tika konstatēts, ka lielākoties gandrīz visas UDP plūsmas veidoja DNS pakalpojums, kā arī tīkla monitoringa pakalpojumi, kas balstītas uz SNMP protokolu.

CAIDA datu analīze

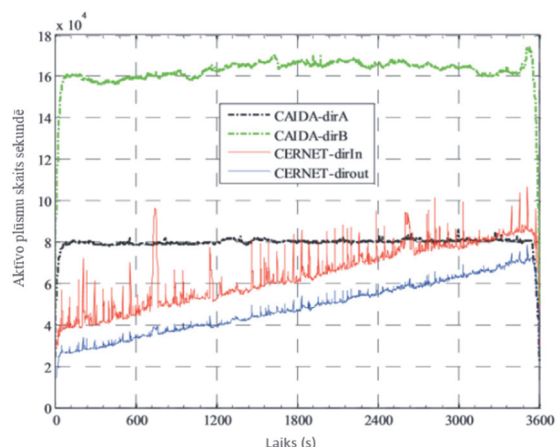
Lai noteiktu apstrādājamo plūsmu apjomu skaitļos un veidotu precīzāku priekšstatu par diapazonu, kādā jāstrādā mūsdienu piekļuves vadības risinājumiem, promocijas darba autors ir analizējis pētniecības centra CAIDA regulāri publicētos interneta trafika datus. Šie dati ir no Amerikas Savienotajās Valstīs esoša ISP pamattīkla starp Čikāgas un Sanhosē pilsētām ar kanāla ātrumu 10 Gbit/s. Dati katru mēnesi tiek regulāri atjaunināti, un tos savos pētījumos ir analizējuši arī citi pētnieki. Kā vienus no plašākajiem pētījumiem datu plūsmu jomā var izcelt [47] un [65].

Autori *X. Zhang* un *W. Ding* ir veikuši plašu pētījumu [65], kurā analizētas interneta trafika plūsmas dažādos šķērsgriezumos – aktīvo un jauno plūsmu skaits sekundē, plūsmu ātrums (paketes/s, biti/s), plūsmu apjoms (baiti), plūsmu dzīves ilgums, plūsmu sadalījums pa transporta protokoliem un citām plūsmu raksturojošām pazīmēm. Rakstā analizēti CAIDA dati, kā arī dati, kas ievākti Ķīnas izglītības un pētniecības tīklā CERNET (no angļu val. *China*

Education and Research Network), kas nodrošina 10 Gbit/s pārraides ātrumu (skat. 13. un 14. att.).



13. att. Jauno plūsmu skaits sekundē uz 10 Gbit/s līnijas pēc [65] datiem.



14. att. Aktīvo plūsmu skaits uz 10 Gbit/s līnijas pēc [65] datiem.

2. tabula

Trafika vidējās vērtības Čikāgas pilsētas tīkla mezglam 2014./2015. gada griezumā (apkopojot CAIDA piedāvātos statistikas datus)

Datu līnija	Vidējā līnijas noslodze (Gbit/s)	Vidējais pārraidīto pakešu skaits (paketes/s)	Jauno plūsmu skaits (plūsmas/s)
Čikāgas dirA	2.11	332 826	9796
Čikāgas dirB	4.42	597 480	26 097

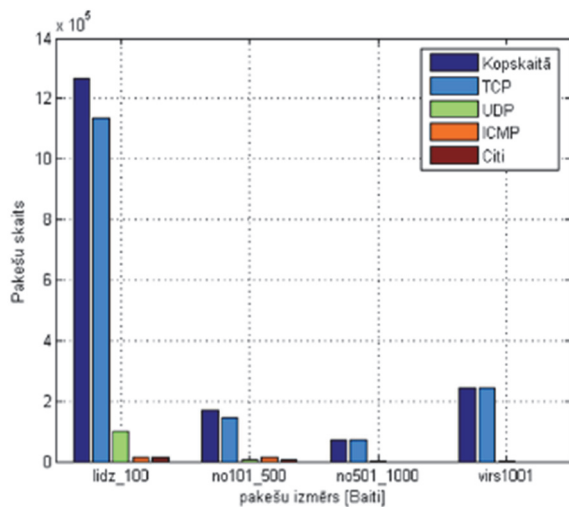
2. tabulā dotas vidējās trafiku raksturojošās vērtības 2014./2015. gada griezumā – no 2014. gada marta līdz 2015. gada martam. Virzienā dirA pie vidējās līnijas noslodzes 21 % (2.1 Gbit/s) ir vidēji 10 000 jaunu plūsmu sekundē, savukārt virzienā dirB pie 44 % noslodzes (4.4 Gbit/s) vidējais jaunu plūsmu skaits ir ap 30 000. Šie rezultāti ļauj rast priekšstatu par apkalpojamo plūsmu mērogu un iezīmē izaicinājumus plūsmu vadības jomā. Rezultāti rāda, ka **ap 80 % plūsmu dzīves ilgums ir 3–6 sekundes**. Visi iepriekš minētie rezultāti liek izdarīt secinājumus par mūsdienu interneta tīklos esošo augsto **jauno plūsmu intensitāti, kas uz 10 Gbit/s kanāla jau mērāma diapazonā no 10 000 līdz 100 000 jaunu plūsmu sekundē**.

Lielie trafika apjomi un proporcionāli liels skaits īsa dzīves laika TCP un UDP plūsmu liecina par augstu jauno plūsmu intensitāti. Jāatzīmē, ka TCP pēc to virzītā apjoma baitos internetā ir dominējošais transporta protokols, tomēr, skatoties no skaita viedokļa, UDP plūsmu skaits ir līdzvērtīgs TCP plūsmu skaitam. Augstā jauno plūsmu intensitāte ir viens no priekšnosacījumiem, kas ļāva šī promocijas darba autoram apsvērt iespēju piedāvāt jaunu pieeju piekļuves vadības risinājumam.

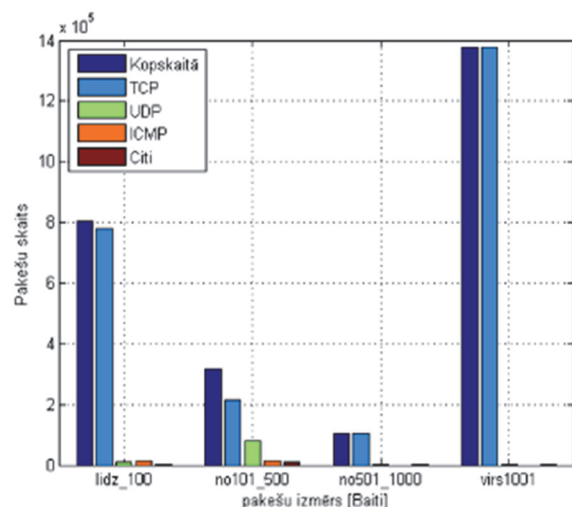
Plūsmu analīze pakešu līmenī

Trafika profilu var raksturot ar iepriekš aplūkotajiem rādītājiem – bit/s, paketes/s vai plūsmas/s. Ņemot vērā, ka šī promocijas darba autora piedāvātais piekļuves vadības risinājums izmanto atsevišķu nodalītu rindu jaunu plūsmu inicializācijas pakešu uzkrāšanai, tika veikta datu plūsmu pakešu līmeņa analīze, iegūstot tādas parametrus kā pakešu izmērs un pakešu

starp-ierašanās laika sadalījums. Analīzei tika izmantoti jau iepriekš izmantotie trases faili, un secinājumu pilnveidošanai rezultāti tika salīdzināti ar jau iepriekš minētajiem CAIDA publicētajiem mērījumu datiem.



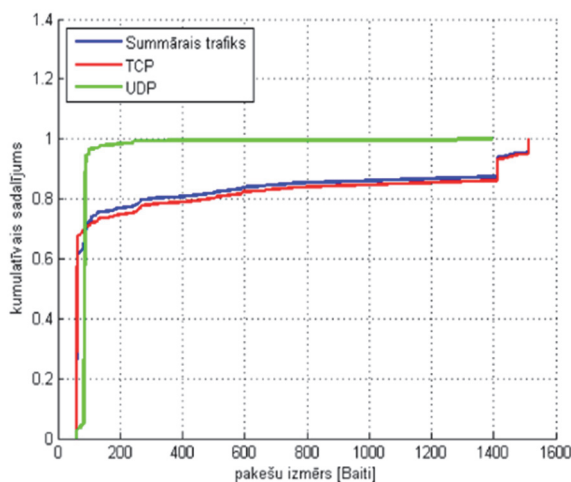
15. att. Pakešu izmēri atkarībā no izmantotā protokola augšuplādes virzienā.



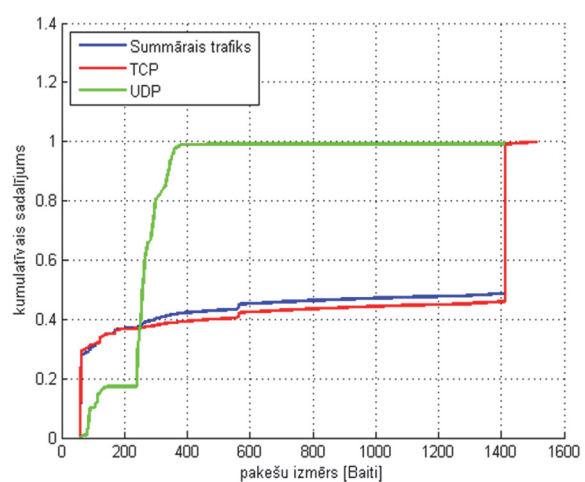
16. att. Pakešu izmēri atkarībā no izmantotā protokola lejuplādes virzienā.

15. un 16. att. var redzēt, ka TCP ir vadošais transporta protokols: augšuplādes virzienā tas veido 91.6 % no pakešu skaita, atlikušo daļu sadala UDP ar 5.7 % un ICMP ar 1.7 %, un 1 % citu protokolu. Lejuplādes virzienā ir līdzīga aina, kur TCP veido 95.3 %, UDP – 3.1 %, ICMP – 1 %, citi – 0.6 %. Rezultāti ar UDP plūsmām internetā uzrādīja, ka dominē (>90 %) plūsmas, kurās pakešu izmērs nepārsniedz 100–200 baitus. Autora uzņemto datu trases failu analīzes rezultāti doti 17. un 18. attēlā.

Jāatzīmē, ka piekļuves mezglos, kur lielu daļu trafika veido UDP balstītas P2P aplikācijas, dominējošais UDP pakešu garums lejuplādes virzienā jau ir lielāks par 1400 baitiem.



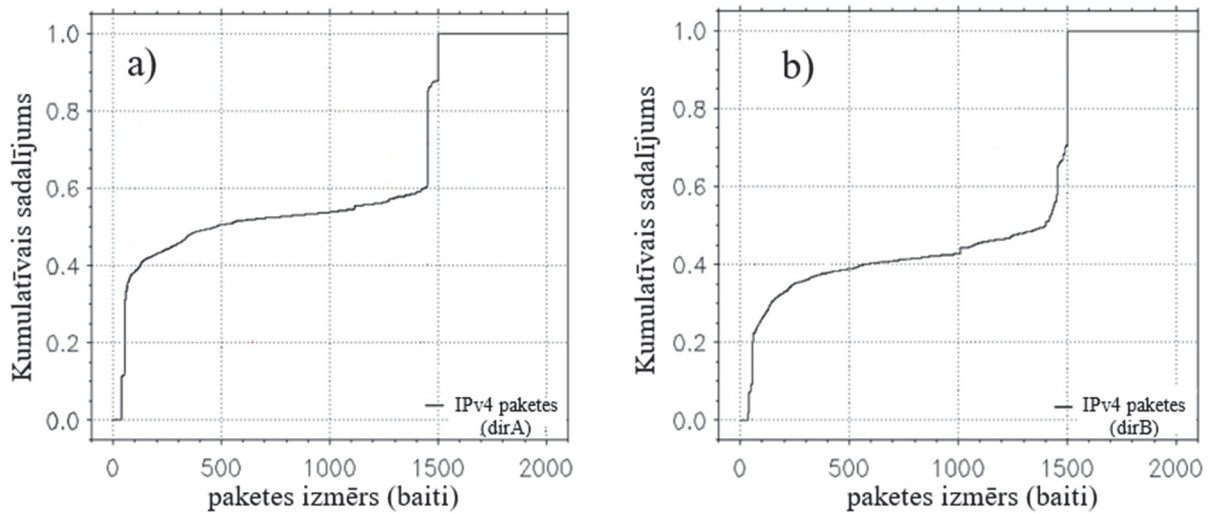
17. att. Pakešu izmēra sadalījums augšuplādes virzienā.



18. att. Pakešu izmēra sadalījums lejuplādes virzienā.

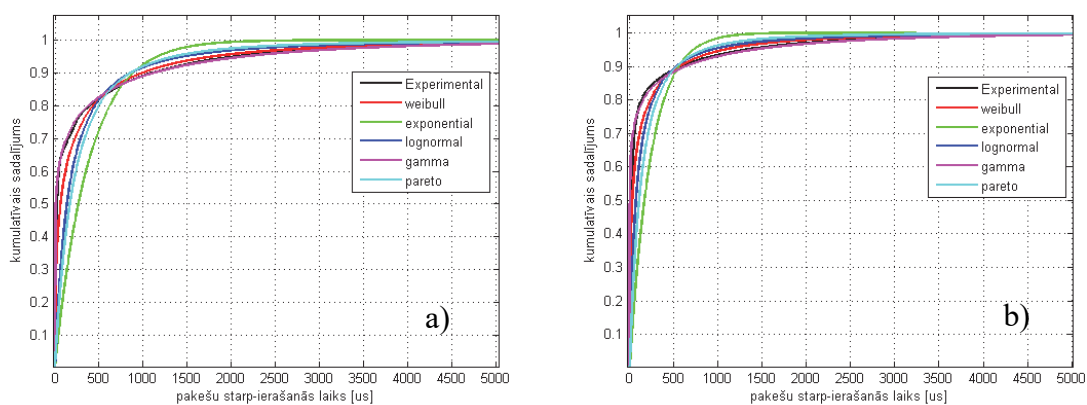
CAIDA pētniecības centrā pieejamie statistikas dati neietver dalītu informāciju par katru transporta slāņa protokolu, tomēr arī tie apstiprina secinājumus, ka galvenokārt dominē divu

veidu paketes: maza izmēra – no 100 līdz 200 baitiem, un liela izmēra – vairāk par 1400 baitiem (skat. 19. att.). Tas nozīmē, ka vidējais rēķinātais pakešu garums, kas būtu ap 500–600 baitiem, patiesībā neraksturo patieso pakešu garumu mūsdienu interneta tīklos.



19. att. Pakešu izmēra sadalījums: (a) virzienā A; (b) virzienā B [57].

Attiecībā uz pakešu starp-ierašanās laika sadalījumu rezultāti ļauj secināt, ka visi sadalījumi ir salīdzinoši tuvu, un konkrētā gadījumā kā tuvākos var nosaukt *weibull* un lognormālo (skat. 20. att.). Analizējot citus pētījumus, jāatzīmē viens no nesenajiem rakstiem [18] par pakešu starp-ierašanās laika sadalījuma novērtēšanu. Tajā kā iespējami tuvākie sadalījumi nosaukti *weibull*, Pareto, gamma, eksponenciālais un lognormālais, bet par vistuvākajiem atzīti Pareto un *weibull* sadalījums; turklāt tie ir ļoti līdzīgi gan TCP, gan UDP gadījumā. Autori secinājuši, ka iegūtie rezultāti ir tuvi un eksperimentāliem pētījumiem var izmantot jebkuru no aplūkotajiem sadalījumiem.



20. att. Pakešu starp-ierašanās laika kumulatīvā sadalījuma funkcijas pietuvinātā mērogā (līdz 5 ms):(a) augšuplādes virzienā;(b) lejuplādes virzienā.

Citu pētījumu analīze datu plūsmu jomā. Autors, apzinoties, ka eksperimentālo datu analīze nav visaptverošs interneta datu plūsmu raksturotājs, veica arī citu pētnieku gūto rezultātu analīzi, kas ļauj precīzāk novērtēt pašreizējo situāciju un iezīmēt galvenās pazīmes.

Attiecībā uz plūsmu apjomu baitos gan paketēs lielāko daļu no mūsdienu interneta trafika sesijām veido TCP protokola plūsmas, un to apstiprina arī citi pētījumi (skat. [10], [13], [31], [66]). TCP protokols ir piemērotāks interneta nepastāvīgajai videi, jo nodrošina plūsmu kontroli, kas pielāgo sūtītāja pārraides ātrumu un zaudēto pakešu atkārtotu pārsūtīšanu.

Augstu UDP plūsmu skaitu samēru mūsdienu interneta trafikā un plūsmu mazos izmērus akcentējuši arī autori no Volfsburgas universitātes [19]. Pētījums atklāja, ka 91.6 % UDP plūsmu vienā virzienā nesatur vairāk kā vienu paketi, 98.7 % satur ne vairāk kā piecas paketes, un 99.6 % nesatur vairāk kā 10 paketes.

Gribētu atzīmēt pētījumu [35], kurā autori ir novērtējuši UDP/TCP plūsmu attiecību dažādos ISP sniedzēju tīklos, gan apjoma (baitos), gan skaita, gan ilguma ziņā. UDP/TCP attiecība no apjoma viedokļa bija diapazonā no 0.02 līdz 0.11. No plūsmu skaita viedokļa UDP vidēji veidoja 15–50 % atkarībā no tīkla, kurā tas mērīts. Vidējais ilgums plūsmām, kuras lielākas par 50 paketēm, parādīja tendenci, ka aptuveni 80–90 % plūsmu neilga vairāk par vienu minūti un 50 % plūsmu neilga vairāk par 10 sekundēm. Jāatzīmē arī fakts, ka >40 % no UDP veidoja DNS pieprasījumi uz 53 portiem, kas ir īsas un maza apjoma plūsmas, kamēr līdzīgu procentuālo daļu TCP gadījumā aizņem 80 porti jeb HTTP protokols.

Arī pētījumā [66] autori veikuši UDP un TCP savstarpēju salīdzināšanu un konstatējuši, ka UDP plūsmu skaits ir trīskāršojies un sasniedzis TCP plūsmu skaitu, lai gan virzītā trafika apjoma proporcija baitos palika praktiski nemainīga, bet proporcija starp UDP un TCP pakešu skaitu pat samazinājās. Vidējais pakešu skaits UDP plūsmā ir mazāks par 10 paketēm. Pie galvenajām UDP protokola izmantošanas sfērām jāmin dažādu P2P aplikāciju signalizācijas datu transportēšana, DNS serviss, monitoringa servisi un citas aplikācijas, kuras nav jutīgas pret pakešu zudumiem.

Plūsmu klasifikatori

Visos trafika vadības uzdevumos, kas apstrādā un vada datu plūsmas, jāspēj atpazīt plūsmas un veikt to klasifikāciju. Īpaši svarīga klasifikatoru veikspēja kļūst gadījumos, kad klasifikācija jāveic tiešsaistes režīmā, kam atbilst arī šī promocijas darba autora piedāvātais savienojumu piekļuves vadības risinājums. Piemēram, pētījuma [29] autori norāda, ka, lai veiktu pakešu klasifikāciju uz OC-768 40 Gbit/s līnijas, sliktākā gadījumā ar mazu pakešu garumu (40 baiti) katras paketes apstrādes laiks nevar pārsniegt 8 ns. Tādēļ autors veica analīzi un novērtēja mūsdienu datu plūsmu klasifikatoru spējas darboties ātrgaitas datu pārraides kanālos ar ātrumu ≥ 10 Gbit/s tiešsaistes režīmā.

Augstas veikspējas sasniegumi klasifikācijā balstās uz jaunu metožu izmantošanu, specifisku programmējamo integrālo shēmu pielāgošanu klasifikācijas uzdevumam, kā arī plašāku paralēlās apstrādes izmantošanu daudzkodolu sistēmās.

Grupējot trafika klasifikatorus pēc to darbības režīmiem, izšķir trīs veidus [11]:

- bezsaistes (*offline*) – plūsmu klasifikācijai izmanto iepriekš ievāktu datu kopu. Pielietošanas sfēras ir pētniecība, statistikas iegūšana, atskaišu veidošana;
- tiešsaistes (*online*) – trafika analīze un plūsmu klasifikācija tiešsaistes režīmā. Visbiežāk izmantota tīkla vadības uzdevumos, kur nepieciešama tiešsaistes lēmuma pieņemšana un politikas īstenošana;

- cikliskā (*cyclic*) – plūsmu klasifikācija ik pēc noteikta laika intervāla. Analizēts konkrētā laika intervālā savāktais trafiks – šāda pieeja ir piemērota, lai veidotu uzskaiti un ģenerētu atskaites, kas tuvas tiešsaistes situācijai tīklā.

Ja skatās uz klasifikācijas metodes veidiem, tās pamatā var iedalīt trīs kategorijās [9], [37], [46]:

- portos balstīta klasifikācija,
- vērtuma analīzē balstīta klasifikācija (DPI),
- mašīnmācīšanās jeb automātu apmācībā balstīta klasifikācija (*machine learning*).

Trafika klasifikācija, kas balstīta uz portiem, pamatojas uz paketes virsraksta lauku analīzi, un tā ir viena no plašāk izmantotajām metodēm, jo neprasa milzīgus skaitļošanas resursus. Tā kā paketes virsraksta lauki ir standartizēti, šī metode bieži tiek iestrādāta maršrutētāju operētājsistēmu kodolos vai arī interfeisu kartēs. Vērtuma analīzes metode nodrošina augstu plūsmu izšķirtspēju, taču tai nepieciešami lieli skaitļošanas resursi un problēmas rada šifrēta trafika klasifikācija. Trafika klasifikatori, kas balstīti uz automātu apmācību, spēj veikt trafika klasifikāciju uz sākotnēji uzkrātās zināšanu bāzes ar iespējam mācīties no uzkrātās pieredzes, lai iegūtu jaunas prasmes un uzlabotu sākotnēji definēto zināšanu bāzi. Šādas metodes vairāk izmantotas bezsaistes klasifikācijas režīmā.

Pētījumā [11] arī uzskatāmi parādīts veiktspējas salīdzinājums starp portu balstītu klasifikāciju, *vienkāršoto DPI (PortLoad)*, un pilno DPI plūsmu klasificēšanas metodēm. *Vienkāršā DPI* analīzē ne tikai portus, bet arī vēl pirmos vērtuma 32 baitus. Vidējais klasifikācijas laiks ar DPI metodi bija palielinājies par 85 % salīdzinājumā ar portos balstīto metodi un par 2.8 % salīdzinājumā ar *PortLoad* metodi. CPU noslodze DPI gadījumā palielinājās piecas reizes un nepieciešamā atmiņa – sešas reizes.

Ļoti aktīvus pētījumus pakešu klasifikatoru veiktspējas jomā veic profesors *Viktor K. Prasanna* ar saviem kolēģiem no Dienvidkalifornijas universitātes [16], [17], [29], [30], [48], [49], [52], [58]. Tālāk aprakstīti vairāki no pašreizējiem sasniegumiem klasifikatoru veiktspējas jomā.

Pētījuma [39] autoru uzdevums bija nodemonstrēt, kādu veiktspēju spēj sasniegt klasifikatori, kas balstīti uz programmatūru un, kas uzstādīti uz plaši pieejamiem daudzkodolu datoriem. Uz 8 CPU kodolu platformas tika sasniegta caurlaides spēja robežās no 10 līdz 15 Gbit/s atkarībā no izmantotās klasifikācijas nosacījumu kopas garuma, kas veidoja augstu pakešu klasifikācijas veiktspēju – līdz 48 miljoni pakešu sekundē.

Pētījumā [49] uz 16 kodolu CPU tika sasniegta 60 MPPS augsta pakešu klasifikācijas veiktspēja pie 1 K (1000) lielas nosacījumu kārtulu kopas un 30 MPPS augsta veiktspēja pie 32 K (32 000) lielas nosacījumu kārtulu kopas. Šajā gadījumā tiešsaistes režīmā tika veikta pakešu klasifikācija pēc 15 virsraksta pazīmēm, un pēc tam tika analizēta arī nosacījumu kopa, kas nosaka tālāko rīcību. Šie paši autori pētījumā [58] ar reducētu nosacījumu kopas garumu sasniedz jau 98 MPPS augstu veiktspēju.

Klasifikatoru veiktspējas paaugstināšanai tiek izmantoti arī grafiskie procesori GPU. Piemēram, pētījums [36], izmantojot plaši pieejamo NVIDIA *Fermi* GPU, uzskatāmi parādīja, ka tiešsaistes režīmā pakešu klasifikators spēj sasniegt 24 Gbit/s caurlaides spēju un apstrādāt līdz pat 12 miljoniem plūsmu/s.

Kā vēl viens veiktspējas paaugstināšanas virziens jāatzīmē programmējamo ciparu integrālo shēmu FPGA izmantošana. Ir vērts pieminēt *T. Ganegedara* un *V. K. Prasanna* rakstu [39], kurā parādīta 400+ Gbit/s augsta veiktspēja; izstrādes brīdī tā bija pirmais šiem pētniekiem zināmais FPGA balstītais risinājums, kas spēj sasniegt šādu veiktspēju.

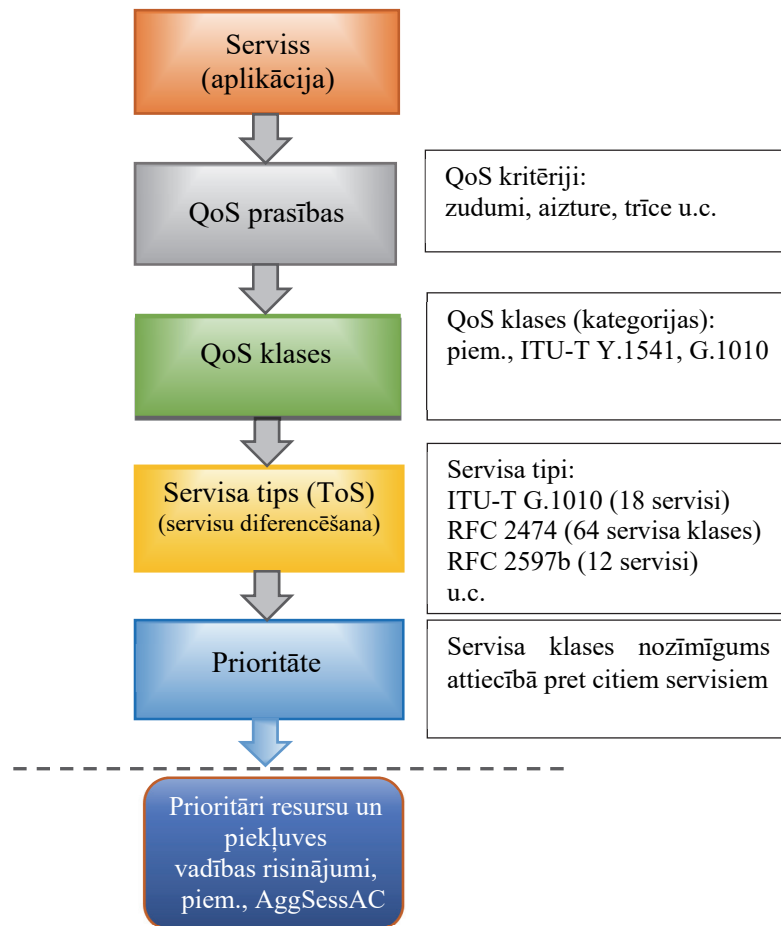
Jāatzīmē, ka promocijas darba autors, veicot plašu pētījumu analīzi klasifikācijas jomā, varēja pārliecināties, ka dažādos pētījumos gūtie rezultāti liecina par klasifikatoru piemērotību izmantošanai tiešsaistes režīmā un autora izstrādātajā piekļuves vadības risinājumā. Autors vēlas arī izcelt, ka mūsdienu tīkla aparatūra, kas paredzēta pamattīklam, tiek ražota ar daudzkodolu CPU un tiek izmantoti speciāli pielāgoti CPU veiktspējas paaugstināšanai tiešsaistes pakešu analīzes jomā. Kā piemērus var minēt *Cisco* kompānijas plaši izmantoto jaunās paaudzes procesoru *QuantumFlow processor* [58] un *MikroTik* izlaisto maršrutētāju sēriju ar daudzkodolu procesoriem [8].

Trafika vadības modelim, kas darbojas plūsmu līmenī, ir nepieciešams veikt ne tikai plūsmu klasifikāciju, bet arī uzturēt aktīvo plūsmu tabulas, tāpēc svarīgs ir arī laika parametrs, pēc kura noteikt, kad sesija ir neaktīva un kad to var dzēst no plūsmu stāvokļu tabulas. Viens no veidiem, kā uzturēt aktīvo plūsmu stāvokļu tabulas ātrgaitas datu pārraides tīklos, ir uzturēt vairāku līmeņu plūsmu tabulas. Piemēram, autori pētījumos [61] un [62] piedāvā šādu risinājumu uz augstas veiktspējas maršrutētājiem, izmantot vairākas plūsmu stāvokļu tabulas un glabāt tajās *hash* vērtības, kuras iegūtas no plūsmu pazīmēm, tādējādi paātrinot atbilstību meklēšanu. Šīs tabulas tiek dēvētas par plūsmu laika konteineriem ar attiecīgi piešķirto laika diapazonu, tādā veidā panākot, ka tiek uzturētas vairāku laika diapazonu plūsmu aktuālās tabulas (konteineri) un meklēšana vienmēr sākas ar aktuālāko (jaunāko).

Nodaļā sniegtie pētījumi spilgti parāda, ka pakešu klasifikācija tiešsaistes režīmā jau tagad ir spējīga strādāt uz līnijām ar caurlaides spēju 40 Gbit/s un augstāku, apstrādājot desmitiem un pat simtiem miljonu pakešu ik sekundi. Gan gūtie secinājumi par datu plūsmām mūsdienu interneta tīklos, gan mūsdienu klasifikatoru sasniegumi veiktspējas jomā kalpoja par nosacījumiem, kas promocijas darba autoram ļāva izvirzīt jaunu pieeju piekļuves vadībā, kuras realizācija un rezultāti ir izklāstīti nākamajās nodaļās.

Servisa tipi un prioritātes. Šajā nodaļā ir iekļauta arī plašāka analīze par iespējamām servisu klasēm un to prioritāšu līmeņiem. Prioritāšu sastādīšana ietver vairākus etapus, un vispārināta promocijas darba autora sastādīta blokshēma dota 21. attēlā. Pakalpojumu un lietotājprogrammu dažādība nosaka atšķirīgas QoS prasības, kas ietver vairākus kritērijus (piemēram, aizture, zudumi, trīce, trafika apjoms u. c.), pēc kuriem pakalpojumus sadala pa QoS klasēm (piemēram, ITU-T G.1010 un Y.1541). Tomēr QoS klase ne vienmēr ir piemērots arguments, lai norādītu kāda pakalpojuma prioritāti attiecībā pret uz citiem. Tāpēc servisi tiek iedalīti tipos un tiem tiek piešķirtas prioritātes, izvērtējot dažādus kritērijus, piemēram, QoS prasības, pakalpojumu cenu un citus, ko ISP uzskata par svarīgiem.

Gan QoS klašu, gan servisa tipu definēšanā un rekomendāciju izstrādē ir iesaistījušās ITU-T, IETF un ETSI, kā arī IEEE organizācijas. Piemēram, RFC971 apraksta astoņus servisa tipus un iespēju definēt līdz astoņiem prioritātes līmeņiem, RFC 2474 definē 12 servisa tipus un 12 iespējamās prioritātes līmeņus. Ar plašāku dažādu rekomendāciju analīzi un iespējamām QoS klasēm, servisa tipiem un to prioritātēm var iepazīties promocijas autora pamatdarbā, kā arī vairākos literatūras avotos (skat., piemēram, [12], [42], [53]).



21. att. Vispārināta blokhēma ar prioritāšu sastādīšanā iesaistītiem elementiem.

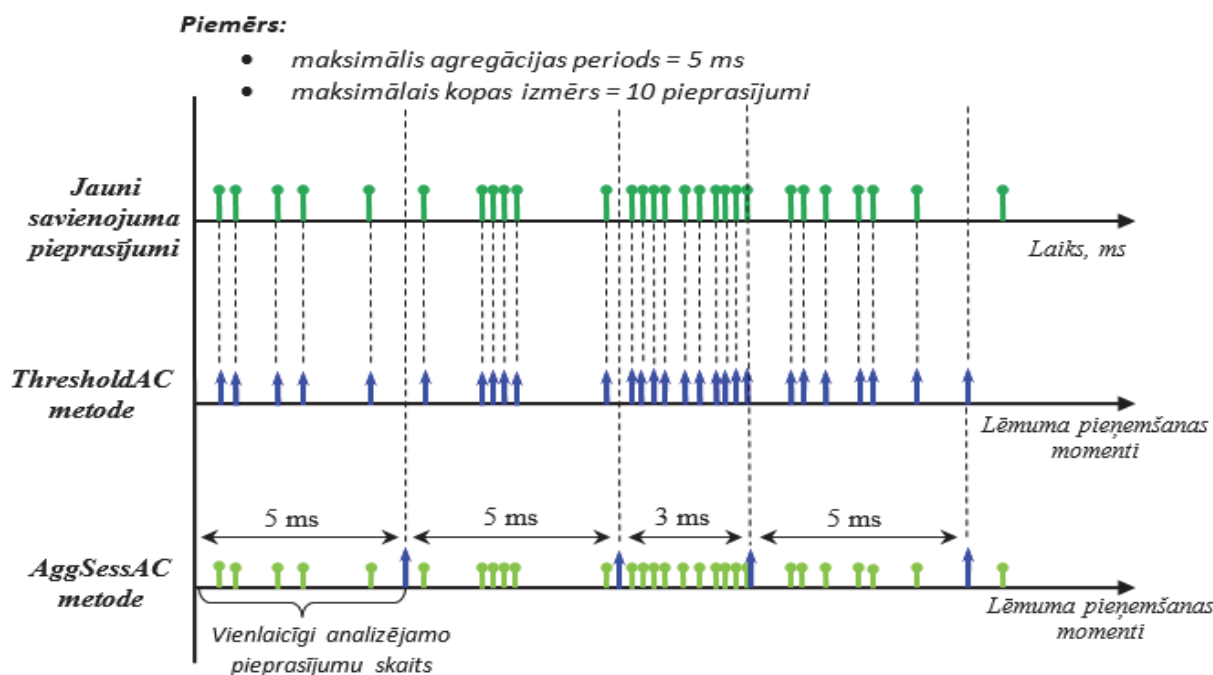
Trešā nodaļa

AggSessAC programatiskā aģenta eksperimentālā izstrāde un novērtēšana veikta OMNeT++ simulācijas vidē, izmantojot INET bibliotēku. INET ietvarā pieejamā maršrutētāja programmatūrā iestrādāta AggSessAC programatiskā aģenta funkcionalitāte.

AggSessAC koncepcija

AggSessAC darbība balstās uz koncepciju, kur tradicionālā – secīga, momentāna – savienojuma pieprasījumu apstrāde to ierašanās kārtībā tiek aizstāta ar jauno pieprasījumu uzkrāšanu jeb agregāciju atsevišķā rindā, radot savstarpējas izvērtēšanas iespējas un proaktīvu, prioritāru lēmumu pieņemšanu.

Konceptuālās pieprasījumu apstrādes atšķirības starp tradicionālo ThresholdAC un AggSessAC piekļuves vadības metodi dotas 22. attēlā.



22. att. Pieprasījumu apstrādes procesa salīdzinājums starp ThresholdAC un AggSessAC piekļuves vadības metodi.

AggSessAC metodē jaunu savienojumu pieprasījumu uzkrāšana tiek kontrolēta ar divu parametru palīdzību:

- maksimālais jaunu savienojumu pieprasījumu agregācijas periods, ko apzīmējam ar A_{\max} (ms):

$$A_{\max} \in \mathbb{R}_{>0}; \quad (1)$$

- maksimālais uzkrājamais jaunu savienojumu pieprasījumu kopas (bufera) izmērs, ko apzīmējam ar B_{\max} [jauno savienojumu pieprasījumu skaits]:

$$B_{\max} \in \mathbb{Z}_{>0} = \{1, 2, 3, \dots\}. \quad (2)$$

AggSessAC aģenta parametri kalpo par lēmuma pieņemšanas trigeru vērtībām:

IF ($A == A_{\max}$) vai ($B == B_{\max}$)

Lēmumu pieņemšana

THEN

Turpinām jauno pieprasījumu uzkrāšanu (agregāciju),

kur

A – tekošais jaunu savienojumu agregācijas ilgums, ms;

B – tekošais uzkrātais jauno savienojumu pieprasījumu skaits.

AggSessAC piekļuves vadības mērķis ir paaugstināt darbības efektivitāti pie uzdotās vadības politikas. Mūsdienu tīkli pieprasa efektīvu resursu izmantošanu un vienlaikus arī dažādu servisu prioritizēšanu. Šajā darbā izmantotā AggSessAC vadības politika noteica, ka lēmumu pieņemšanas brīžos no uzkrāto jauno pieprasījumu kopas apstiprināšanu sāk ar iespējami augstāku prioritāšu pieprasījumu apstiprināšanu, ar nosacījumu, ka to pieļauj pieejamais caurlaides joslas apjoms.

Piekļuves vadības politika izvirza divus uzdevumus.

1. **Uzturēt maksimālo vidējo kanāla noslodzi atbilstoši vadības politikā noteiktajam atļautās noslodzes līmenim.**

$$\forall t_i : \max \frac{\sum_1^n u(t_i)}{n}, \quad (3)$$

kur

t_i – lēmumu pieņemšanas moments, $i = 1, 2, 3, \dots$;

n – kopējais lēmumu pieņemšanas momentu skaits eksperimenta laikā;

$u(t_i) \in [0; 1]$ – kanāla noslodze lēmumu pieņemšanas momentā t_i .

2. **Veicināt diferencētu pieprasījumu apstrādi un augstāku prioritāšu savienojumu pieprasījumu (sesiju) apstiprināšanu katrā lēmumu pieņemšanas momentā.**

$$\forall t_i : \max_{j_{\text{accepted}}^{(p)} \in B(t_i)} \sum_0^a r(j_{\text{accepted}}^{(p)}(t_i)), \quad (4)$$

kur

$j_{\text{accepted}}(t_i)$ – apstiprinātie savienojumi (sesijas) lēmumu pieņemšanas momentā t_i ;

a – apstiprināto pieprasījumu (sesiju) skaits;

$B(t_i) \in [j(t_i)]$ – uzkrāto (agregēto) pieprasījumu kopa ar visiem uzkrātajiem jauno savienojumu pieprasījumiem $j(t_i)$ lēmumu pieņemšanas momentā t_i ;

$r(j_{\text{accepted}}^{(p)}(t_i))$ – gūtais labums no apstiprinātās sesijas j_{accepted} lēmumu pieņemšanas momentā t_i ar prioritāti p ;

$p \in \mathbb{Z}_{>0} = \{1, 2, 3, \dots\}$ – jauna savienojuma pieprasījuma prioritāte; eksperimentos tika izmantots trafiks ar trim, pieciem un astoņiem prioritāšu līmeņiem.

Šī promocijas darba ietvaros autors lieto jēdzienu “gūtais labums”, kas aizgūts no lietderības teorijas (no angļu val. *utility theory*), kura plašāku uzmanību ieguva pēc autoru *J. von Neumann* un *O. Morgenstern* publicētā raksta [44]. Šie principi tiek pārnesti arī uz inženierzinātņi (skat. [40]).

Lietderības teorija skaidro, ka, lai gan nav iespējams izmērīt lietderību jeb “gūto labumu”, kas iegūts no preces vai pakalpojuma, tomēr ir iespējams tos sarindot priekšrocību secībā attiecībā uz patērētāju. Racionāla rīcība būs tērēt līdzekļus par papildu “preces vienību” vai pakalpojumu, ja vien no tās iegūtā lietderība ir vienāda ar citas preces vai pakalpojuma lietderību vai lielāka par to. Tad, pārnesot šādu uzvedību no ekonomikas uz sakaru tīkliem, piekļuves vadības kontekstā vārdu “patērētājs” var saistīt ar “realizēto vadības politiku”, un šajā gadījumā racionāla rīcība būs nodrošināt, lai augstāko prioritāšu plūsmas saņemtu apkalpošanas priekšrocības attiecībā uz zemāko prioritāšu plūsmām. “Cena” par šādu ieguvumu būs īsa lēmumu pieņemšanas procesa aizture sesijas inicializācijas laikā.

Tāpēc piekļuves vadības spēja realizēt šādu selektīvu un prioritāru lēmumu pieņemšanu un izpildīt vadības politiku, kura nodrošina iespēju augstāku prioritāšu plūsmām saņemt apstiprināšanu ar augstāku iespējamību, šajā darbā tiek rēķināta kā gūtais labums no apstiprināto savienojumu prioritātēm. Darbā arī novērtēts, kā atbilstoši sastādītai vadības politikai izejā izmainās apstiprināto plūsmu sadalījums pa prioritātes līmeņiem.

Kopēji gūtais labums (Q) šajā darbā ir uzdots šādi:

$$Q = \sum_0^m r_{j_{\text{accepted}}}^{(p)}, \quad (5)$$

kur

m – kopējais apstiprināto sesiju skaits un $r_{j_{\text{accepted}}}^{(p)}$ – gūtais labums no apstiprinātās sesijas j_{accepted} ar prioritāti p .

Jauno pieprasījumu agregācijai nepieciešamais bufera atmiņas apjoms (B_{max}), promocijas darbā tika novērtēts, lai radītu priekšstatu par nepieciešamās buferatmiņas apjoma diapazonu. Ņemot vērā TCP savienojuma izveides procesu ar trīs ceļu rokasspiedienu (no angļu val. *three-way handshake*), tas nozīmē, ka, aizturot SYN ziņojumu agregācijas buferī, jaunas paketes no attiecīgās sesijas nepienāks. Savukārt UDP protokols darbojas bezsavienojuma režīmā (no angļu val. *connectionless mode*) un paketes tiek pārsūtītas bez apstiprinājumiem, tāpēc UDP plūsmas agregācijas perioda laikā var prasīt lielāku buferatmiņas apjomu nekā TCP. Novērtēšanai izmantota situācija, kurā visu *Ethernet* kanālu aizņem jauns savienojums ar maksimālo ātrumu. *Ethernet* pārraides vides starpkadru spraugas periodi tika izņemti no agregācijas perioda, rēķinot maksimālo iespējamo bitu pārraidi šajā periodā. 3. un 4. tabulā dotas agregācijas bufera izmēra maksimālās teorētiskās robežas.

3. tabula

Teorētiskais maksimālais agregācijas bufera izmērs pastāvot dažādiem jaunas datu plūsmas pārraides ātrumiem (pakešu izmērs **1500 B**)

Pārraides ātrums	Starpkadru spraugas, ns	Maksimālais bufera izmērs, B			
		Agregācijas periods			
		10 ms	1 ms	0.1 ms	0.01 ms
100 Mbit/s	960	124 KB (82 paketes)	12.4KB (8 paketes)	–	–
1 Gbit/s	96	1240 KB (826 paketes)	124 KB (82 paketes)	12.4 KB (8 paketes)	–
10 Gbit/s	9.6	12.4 MB (8266 paketes)	1240 KB (826 paketes)	124 KB (82 paketes)	12.4 KB (8 paketes)
40 Gbit/s	2.4	49.60 MB (33 066 paketes)	4960 KB (3306 paketes)	496 KB (330 paketes)	49.6 KB (33 paketes)
100 Gbit/s	0.96	124 MB (82 666 paketes)	12.4 MB (8266 paketes)	1240 KB (826 paketes)	124 KB (82 paketes)

Teorētiskais maksimālais agregācijas bufera izmērs pastāvot dažādiem jaunās datu plūsmas pārraides ātrumiem (pakešu izmērs **100 B**)

Pārraides ātrums	Starpkadru sprauga, ns	Maksimālais bufera izmērs, B			
		Agregācijas periods			
		10 ms	1 ms	0.1 ms	0.01 ms
100 Mbit/s	960	110 KB (1100 paketes)	11 KB (110 paketes)	1.1 KB (11 paketes)	110 B (1 pakete)
1 Gbit/s	96	1100 KB (11 000 paketes)	110 KB (1100 paketes)	11 KB (110 paketes)	1.1 KB (11 paketes)
10 Gbit/s	9.6	11 MB (110 000 paketes)	1100 KB (11 000 paketes)	110 KB (1100 paketes)	11 KB (110 paketes)
40 Gbit/s	2.4	44 MB (440 000 paketes)	4400 KB (44 000 paketes)	440 KB (4400 paketes)	44 KB (440 paketes)
100 Gbit/s	0.96	110 MB (1100 000 paketes)	11 MB (110 000 paketes)	1100 KB (11 000 paketes)	110 KB (1100 paketes)

Rezultāti rāda, ka pie 1 Gbit/s ātruma un 1 ms agregācijas perioda maksimālais teorētiski nepieciešamais bufera atmiņas apjoms nav lielāks par 124 KB, kurā ietilptu ap 82 paketēm, kas ir 1500 B garas, vai 1200 paketēm, kas ir 100 B garas.

Šī darba izstrādes rezultātā iegūtie secinājumi par mūsdienu tīklos esošo augsto jauno plūsmu intensitāti uzrāda, ka eksistē tūkstošiem jaunu savienojumu ik sekundi uz 1 Gbit/s kanāla, un uz 10 Gbit/s kanāla jaunu savienojumu intensitāte jau sniedzas desmitos tūkstošus ik sekundi. Šeit var aplūkot piemēru ar 5000 jauniem pieprasījumiem/s, kas veido vidēji 0.2 ms starp-ierašanās laiku, kas nozīmē, ka 50 pieprasījumu vienlaicīgai analīzei vajadzēs vidēji 10 ms garu agregācijas periodu. Šādam periodam teorētiski nepieciešamo maksimālo buferatmiņas izmēru ar dažādiem pārraides ātrumiem var redzēt 3. un 4. tabulā. Savukārt pie 20 000 jaunām plūsmām/s vidējais starp-ierašanās laiks būs 0.05 ms un 50 pieprasījumu uzkrāšana prasīs vidēji 2.5 ms, bet, samazinot uzkrājamo kopas izmēru uz 10 pieprasījumiem, agregācija prasīs vairs tikai 0.5 ms.

Sākotnējās agregācijas kopas izmēra izvēlei par loģiskiem apsvērumiem un priekšnosacījumiem tīkla inženieriem un projektētājiem var kalpot:

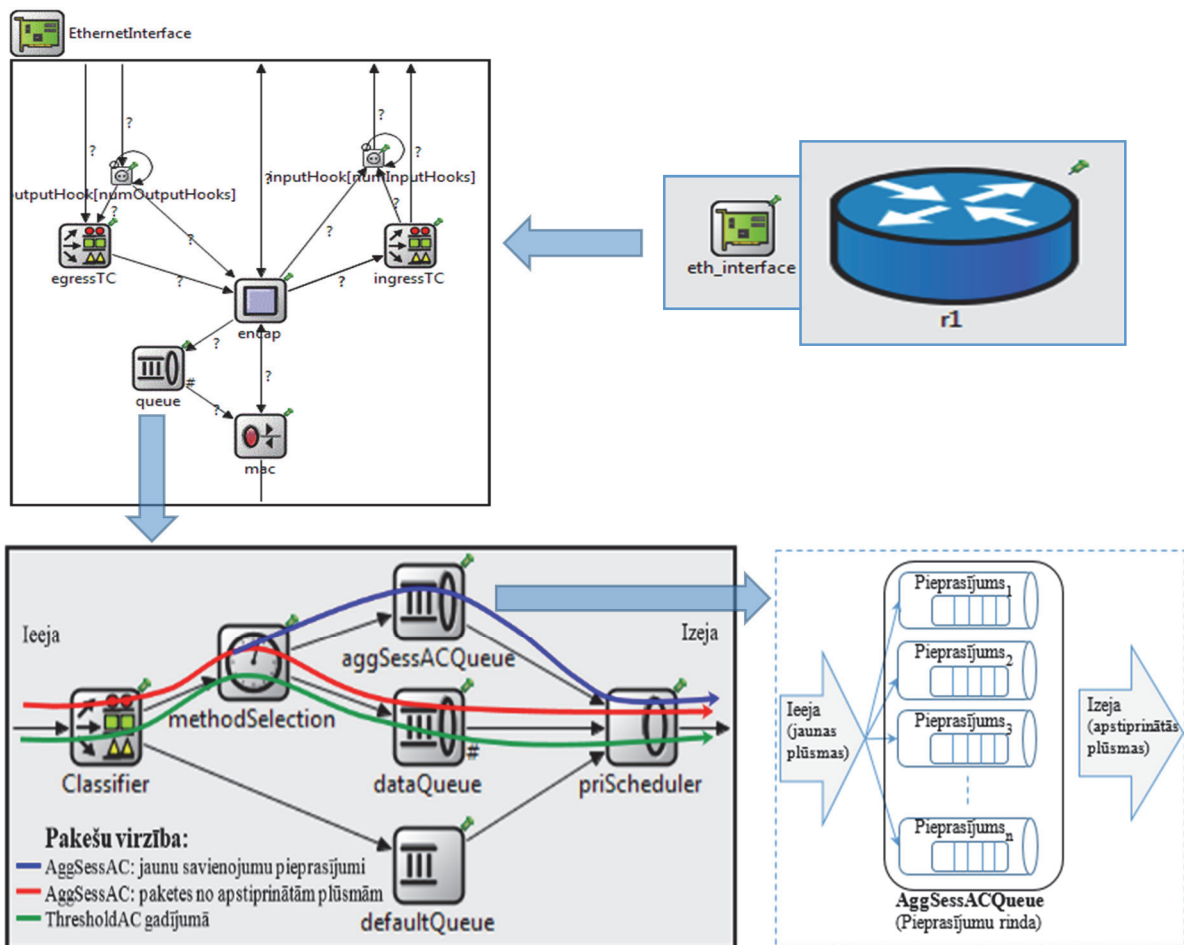
- monitoringa informācija par tīkla vidējo jauno savienojumu skaitu sekundē,
- agregācijas perioda maksimālie ierobežojumi (ienestās aiztures sliekšnis),
- ieguvumu/zaudējumu apsvērumi:
 - jo mazāks izvēlētais kopas izmērs, jo mazāks nepieciešamais agregācijas periods un ienestās aiztures,
 - nepiemēroti mazs izvēlētais kopas izmērs vai pārāk īss agregācijas periods samazina vienlaicīgi izvērtējamo pieprasījumu skaitu un rezultātā arī metodes selektivitāti lēmuma pieņemšanas brīdī.

Simulācijas rīks

Maršrutētājs pēc savas būtības ir dators ar specifiski pielāgotu operētājsistēmu. Tā kā autoram nav iespējas piekļūt maršrutētāju ražotāju operētājsistēmu avota kodiem, tika meklēti alternatīvi ceļi, rezultātā izvēloties izstrādāto resursu un piekļuves vadības risinājuma prototipu realizēt OMNeT++ moduļu balstītajā diskreto notikumu simulēšanas vidē uz INET bibliotēku bāzes [20]. OMNeT++ principā piedāvā emulēt tīkla aparatūras darbību, sākot ar pārraides kanāla fiziskā līmeņa simulēšanu, pakešu apstrādi buferī, datu un transporta līmeņa un maršrutēšanas protokoliem, līdz pat OSI aplikācijas slānim. OMNeT++ vidē pieejamā relatīvā laika skala ļāva izvērtēt arī tādus parametrus kā vidējo agregācijas perioda garuma un vidējo agregācijas rindas garuma atkarību no uzdotā vidējā plūsmu starp-ierašanās laika sadalījuma un novērtēt to dinamiku laikā.

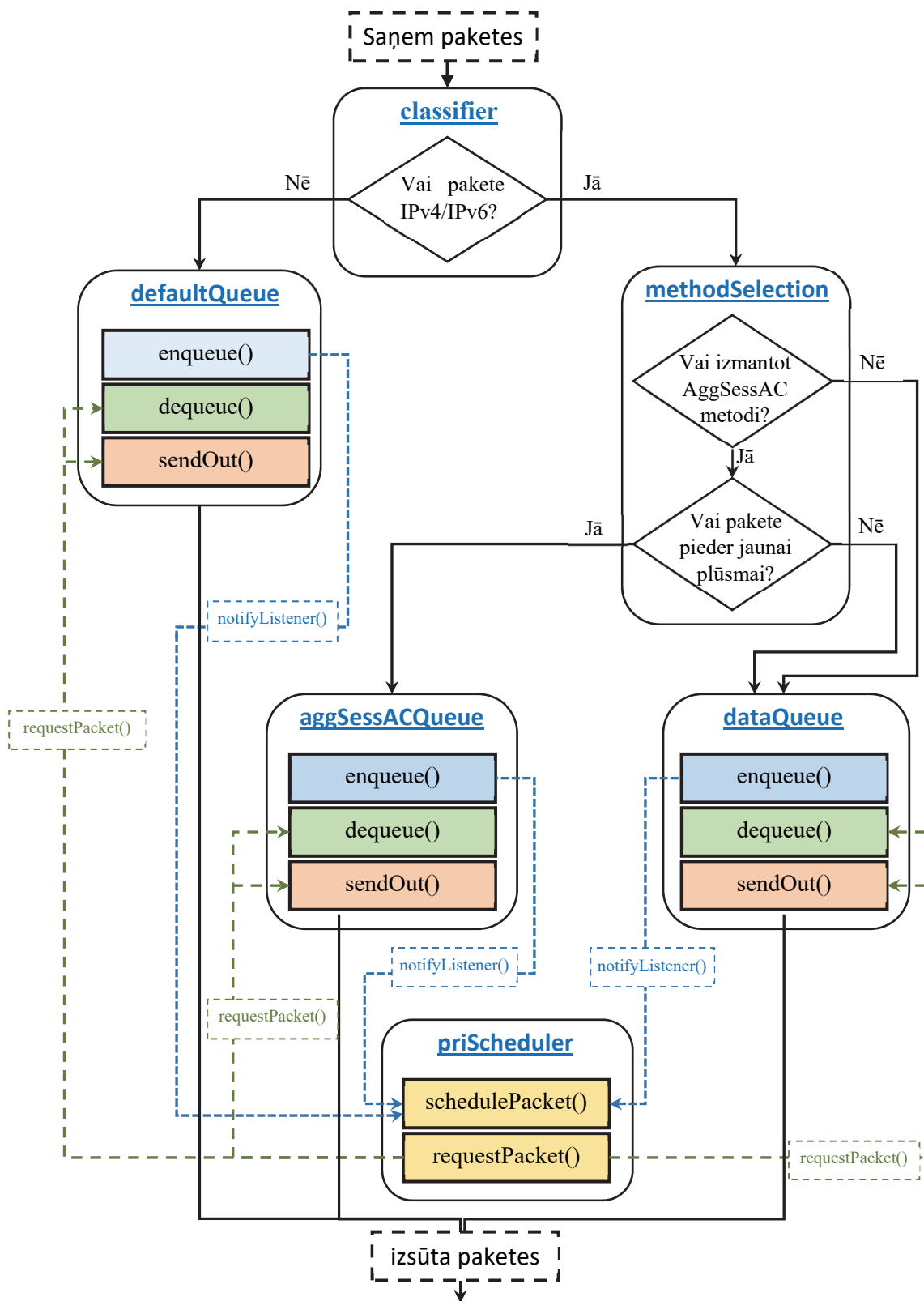
INET moduļu bibliotēkas kopa tika papildināta ar izstrādāto AggSessAC programmatisko aģentu, kas tika integrēts INET ietvarā pieejamā maršrutētājā programmatūrā kā papildu funkcionālais bloks, izveidojot AggSessAC piekļuves vadības eksperimentālu prototipu.

AggSessAC funkcionālā bloka (aģenta) realizācija tika iestrādāta OMNeT++ INET ietvarā pieejamā maršrutētāja *Ethernet* interfeisa buferī kā papildu funkcionālais bloks (23. att.). Izstrādātais projekts un tā pirmkods ir publiski pieejams <https://github.com/askrastins/aggssessac>.



23. att. Izstrādātā AggSessAC funkcionālā aģenta struktūra maršrutētāja *Ethernet* saskarnes rindas modulī un pakešu virzības atkarība no izmantotās piekļuves vadības metodes.

Atbilstoši 23. att. izstrādāto AggSessAC aģentu veido vairāki funkcionālie moduļi, un katram modulim atbilst savs C++ avota fails. Plašāk ar galvenajām izstrādāto klašu funkcijām var iepazīties pamatdarba 3. nodaļā.



24. att. Vispārināta AggSessAC funkcionālā aģenta darbības blokhēma.

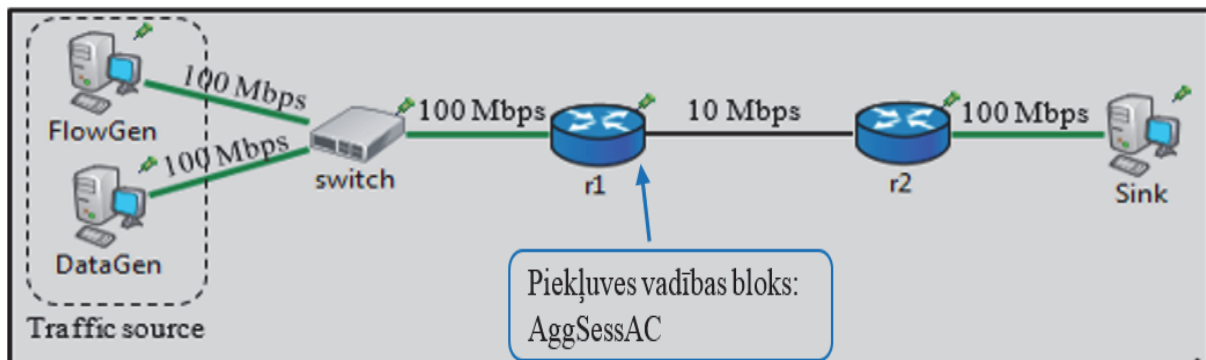
Vispārinātajā AggSessAC funkcionālā aģenta blokshēmā (sk. 24. att.) klasifikatora (*classifier*) galvenais uzdevums ir noskaidrot, vai saņemtais kadsrs ietver IP paketi, un to novirzīt uz *methodSelection* moduli, bet, ja tas ir kas cits (piemēram, ARP ziņojums), – uz *defaultQueue* rindu. *MethodSelection* modulis ļauj iestatīt izvēlēto piekļuves vadības metodi *ThresholdAC* vai *AggSessAC*, kā arī īstenot aktuālās un pieejamās caurlaides joslas monitoringu un uzskaiti. Tiek izmantoti trīs rindas moduļi – attiecīgi *defaultQueue*, *dataQueue* un *aggSessACQueue* (skat. 23. un 24. att.). *DataQueue* modulis spēj realizēt *ThresholdAC* piekļuves vadību, savukārt *aggSessACQueue* realizē izstrādāto *AggSessAC* savienojumu piekļuves vadību, nodrošinot gan jaunu savienojumu pieprasījumu pakešu uzkrāšanu, gan pieprasījumu analīzi un vadības lēmumu pieņemšanu. Rindu moduļu galvenās pamatfunkcijas ir mantotas no bāzes klases *PassiveQueueBase.cc* un nodrošina pakešu ievietošanu rindā – *enqueue()*, pakešu izņemšanu no rindas – *dequeue()*, nosūtīšanu tālāk – *sendOut()*, kā arī paziņošanu par jaunas paketes ierašanos rindā *notifyListener()*. Rindas darbība nosaka, ka ik reiz, parādoties jaunai paketei rindā, tas caur rindas mantoto *notifyListener()* metodi tiek paziņots *priScheduler* modulim, kurš spēj izsaukt rindas *enqueue()* un pēc tam *sendOut()* metodi, kas savukārt attiecīgi nodrošina paketes izņemšanu no rindas un nosūtīšanu tālāk sakaru kanālā. *PriScheduler* modulis seko pakešu esamībai rindās un to aktuālajam garumam; reaģēšana uz *notifyListener()* ziņojumiem ir pakārtota un vadīta ar moduļiem, kas simulē sakaru kanālu. *AggSessAC* gadījumā *priScheduler* un *notifyListener()* metode ir pakļauta arī agregācijas periodam, un tā pie *aggSessACQueue* rindas vēršas atbilstoši šim periodam vai arī ja pieprasījumu agregācijas kopa ir sasniegusi iepriekš uzstādīto maksimālo vērtību. Rindas ir apkalpotas prioritāšu secībā, kur visaugstākā prioritāte ir *defaultQueue* rindai, otra augstākā – *aggSessACQueue* rindai, un zemākā prioritāte ir *dataQueue* rindai. Tas nodrošina, ka lēmumu pieņemšanas procesa beigās jaunie savienojumi tiek apstrādāti pirmieun pēc iespējas ātrāk virzīti tālāk, pēc tam vēršoties pie *dataQueue* rindas un apstiprinot paketes no jau apstiprinātajām sesijām.

Rezumējot gribētu atzīmēt, ka promocijas autora piedāvātais *AggSessAC* risinājums balstās uz vienkāršu, bet efektīvu pieeju, kur vairākas plūsmas lēmumu pieņemšanas brīdi tiek apstrādātas vienlaicīgi, kas nodrošina savstarpējas izvērtēšanas un selektīvas plūsmu apstiprināšanas iespējas, aizpildot sakaru kanālus ar jaunām datu plūsmām. Lai to realizētu, *AggSessAC* risinājumā savienojuma pieprasījumi tiek uzkrāti un, veicot plūsmu klasifikāciju, jauno savienojumu pieprasījumu inicializācijas paketes tiek atšķirtas no jau apstiprinātajām datu plūsmām. Risinājums liek uzturēt plūsmu stāvokļus un ienest sistēmas arhitektūrā jaunu plūsmu pieprasījumu inicializācijas pakešu buferi, kurā novirzīt jauno savienojumu pieprasījumu paketes. Agregācijas ilguma kontrolei risinājums nosaka ieviest un sekot līdzīgi tādiem parametriem kā maksimālais kopas izmērs un maksimālais agregācijas periods. Rezultātā tiek iegūts, kas līdzīgs rindošanas algoritmu realizētai diferencētai pakešu vadībai, tikai šajā gadījumā selektīvas izvēles iespējas notiek plūsmu līmenī un nonāk piekļuves vadības “rokās”, kā arī dod iespēju darboties ar pilnībā ticamu pieprasījumu vērtību kopu.

Ceturrtā nodaļa

Nodaļa veltīta izstrādātā *AggSessAC* funkcionālā aģenta novērtēšanai un simulēšanas procesā iegūto rezultātu analīzei, lai pārliecinātos par autora piedāvātā *AggSessAC* risinājuma darbības efektivitāti un iegūtu tā darbību raksturojošos datus.

Lai novērtētu izstrādātā AggSessAC funkcionālā aģenta darbību un izdarītu secinājumus, tika izveidota OMNeT++ vidē simulācijas eksperimentiem nepieciešamā tīkla topoloģija, kas dota 25. attēlā.



25. att. Simulēšanas eksperimentos izmantotā tīkla shēma OMNeT++ vidē.

Eksperimentu scenāriji un to rezultāti

Simulācijas eksperimentu scenāriji ietver šādu parametru analīzi:

- gūtais labuma novērtējums, ja ir dažādi izvēlētie AggSessAC parametri,
- vidējais *aggSessACQueue* rindas garums lēmuma pieņemšanas brīdī,
- vidējais pieprasījumu pavadītais laiks *aggSessACQueue* rindā lēmumu pieņemšanas momentā,
- ietekme uz kanāla noslodzi,
- gūtā labuma novērtējums, pastāvot dažādiem ieejas prioritāšu sadalījumiem,
- apstiprināto savienojumu prioritāšu kumulatīvais sadalījums izejā (selektivitāte).

AggSessAC metodē sākotnēji iestatāmo parametru novērtējums

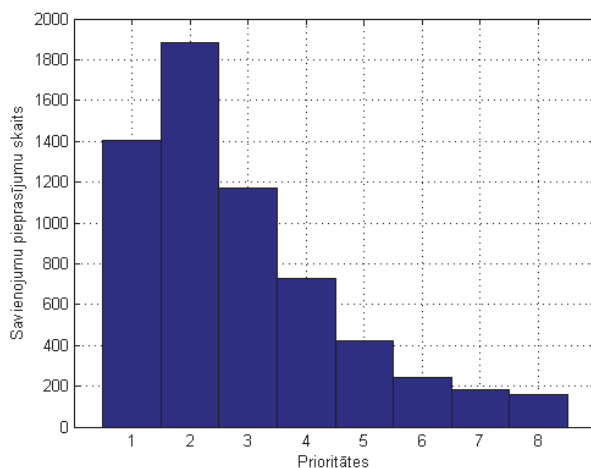
Šajā punktā tiks analizēts AggSessAC metodē sākotnēji iestatāmo parametru – maksimālā kopas izmēra un maksimālā agregācijas perioda – izvēle, to savstarpējā atkarība un ietekme uz gūto labumu.

Ieejā ģenerētais trafiks:

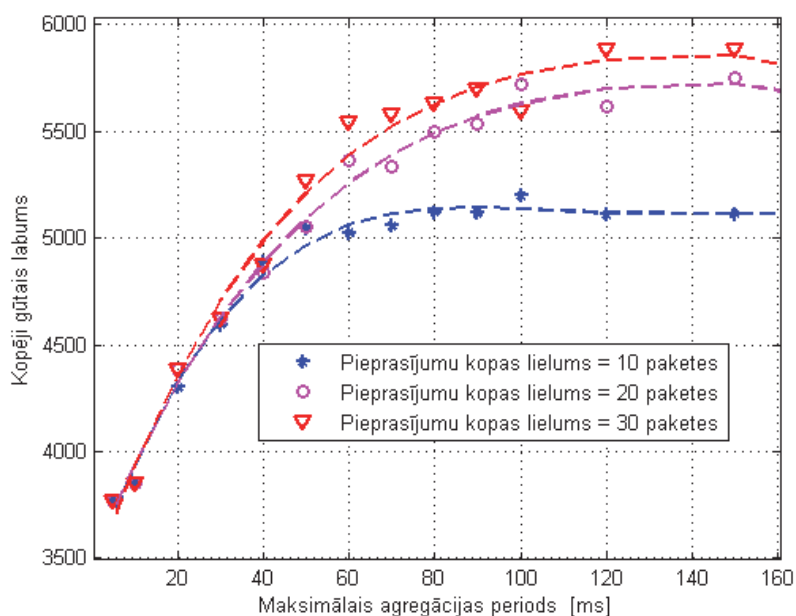
- jaunu savienojumu starp-ierašanās sadalījums – eksponenciāls ar vidējo vērtību 5 ms (~200 plūsmas/s);
- plūsmu izmērs – gamma sadalījums ar vidējo vērtību 450 Kbit/s (plūsmas no 50 Kbit/s līdz 2000 Kbit/s). Tika izmantots visos turpmākajos simulācijas eksperimentu pētījumos;
- jaunu plūsmu pieprasījumi ar astoņiem prioritātes līmeņiem, kur attiecīgi pirmais ir zemākā prioritāte un astotais ir augstākā prioritāte (skat. 26. att.).

Jauno plūsmu pieslēguma pieprasījumi ir piecas reizes biežāki par pieslēgto plūsmu deaktivēšanas gadījumiem, lai kanāls atrastos pārslodzes režīmā.

AggSessAC parametru novērtējuma rezultāti, simulējot 30 s ilgu sastrēgumu, kura laikā tika apstrādāti 5917 savienojuma pieprasījumi, doti 27., 28. un 29. attēlā.



26. att. Ieejas plūsmu sadalījums pa prioritātēm (trafiks ar izteikti vairāk zemas prioritātes pieprasījumiem).



27. att. Kopēji gūtais labums ar trīs pieprasījumu kopas izmēriem atkarībā no izvēlēta agregācijas perioda.

Rezultāti 27. att. uzskatāmi rāda, kā sākotnēji strauji palielinās gūtais labums pie dažādiem kopas izmēriem, palielinoties agregācijas periodam. Tas izskaidrojams ar selektīvas izvēles pieaugumu lēmumu pieņemšanas brīdī. Rezultāti rāda, kā strādā agregācijas kopas robeža, kuru sasniedzot gūtais labums pie noteikta agregācijas perioda vairs nepalielinās, jo uzkrāto pieprasījumu skaits sasniedz uzstādītās kopas izmēru. Tas nozīmē, ka, zinot vidējo jauno pieprasījumu intensitāti, var noteikt agregācijas periodu, kurš piemērots uzstādītajam agregācijas kopas izmēram, lai lēmumu pieņemšanas brīdī pieprasījumu kopa vairumā gadījumu būtu aizpildīta (skat. 28. att.). Rezultāti, kas atspoguļoti 28. att., parāda vidējo *AggSessACQueue* rindas (*AggSessACQueue* rindas modulis dots 23. att.) garumu pie dažādiem kopas izmēriem un tā izmaiņas atkarībā no uzstādītā agregācijas perioda.

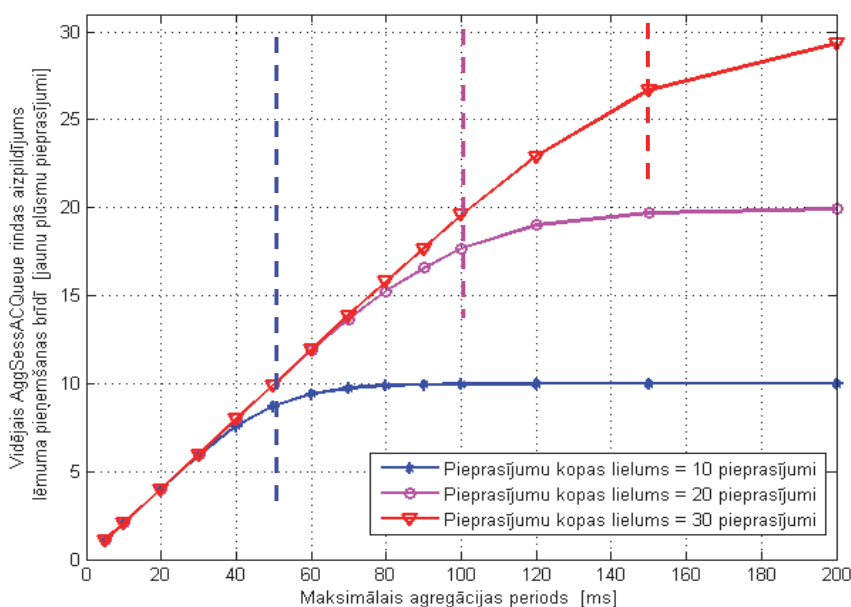
Šajā scenārijā vidējais jauno plūsmu ierašanās laiks ir 5 ms. Tas nozīmē – lai uzkrātu vidēji 10 pieprasījumus, ir nepieciešamas vidēji 50 ms, lai uzkrātu 20 nepieciešamas ~100 ms, un 30 prasa ~150 ms, kas arī ir piemērotas robežas agregācijas perioda izvēlei. Tas ļauj arī apgalvot, ka pie izvēlēta pieprasījumu kopas izmēra un sekojot līdzīgai vidējai jaunu pieprasījumu ierašanās intensitātei, ir iespējams veidot arī adaptīvus risinājumus, kas pielāgo agregācijas periodu tiešsaistes režīmā. Uzstādot tīklā AggSessAC risinājumu, svarīgas ir zināšanas par vidējo jaunu plūsmu intensitāti, kas dod iespēju jau sākotnēji daudz precīzāk izvēlēties AggSessAC sākotnējās parametru vērtības – nepieciešamo agregācijas kopu un nepieciešamo agregācijas periodu.

Skaitliskās vērtības trijos gadījumos pie trīs dažādiem agregācijas kopas izmēriem ar piemēroti izvēlētu agregācijas periodu dotas 5. un 6. tabulā.

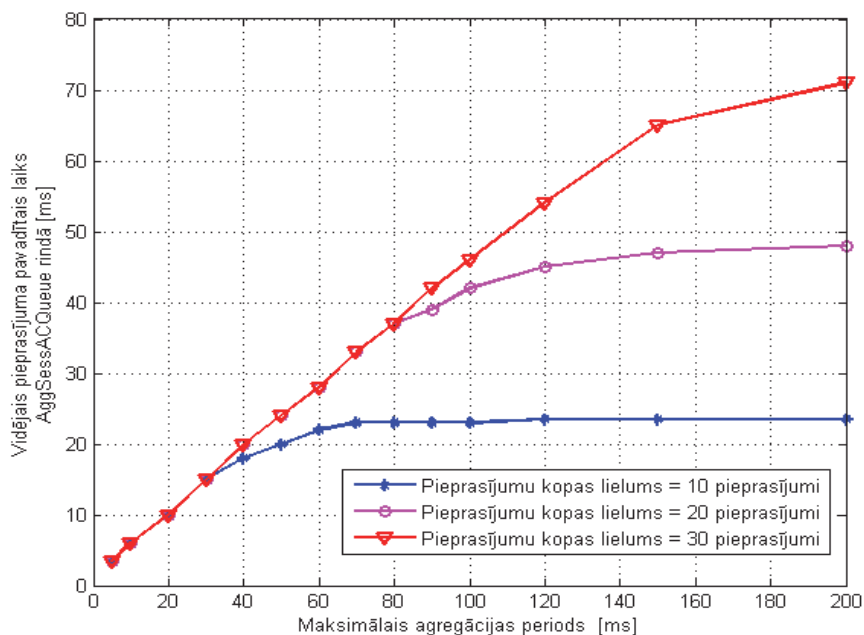
5. tabula

Skaitliskie rezultāti ar AggSessAC risinājumu pie trīs agregācijas kopas izmēriem.

<i>Tīkla sastrēguma simulācijas laiks 30 s</i>					
Izvēlētais pieprasījumu kopas lielums, pieprasījumi	Agregācijas periods, ms	Kopēji apstrādāto plūsmu skaits	Noraidīto plūsmu skaits	Apstiprināto plūsmu skaits	Lēmumu pieņemšanas brīžu skaits
10	50	5917	4676	1241	680
20	100	5917	4747	1170	335
30	150	5917	4785	1131	222



28. att. Vidējais *AggSessACQueue* rindas garums lēmumu pieņemšanas momentā pie trīs pieprasījumu kopas izmēriem atkarībā no izvēlēta agregācijas perioda.



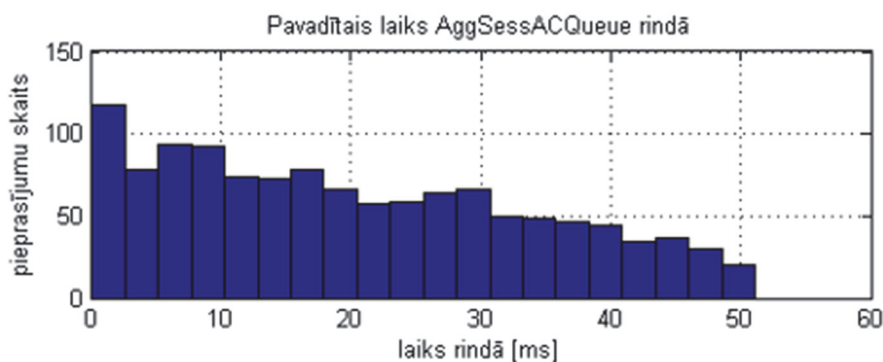
29. att. Vidējais pieprasījumu pavadītais laiks *AggSessACQueue* rindā pie trīs pieprasījumu kopas izmēriem atkarībā no izvēlēta agregācijas perioda.

6. tabula

Skaitliskie rezultāti – vidējais *AggSessACQueue* rindas garums un vidējais pieprasījumu pavadītais laiks *AggSessACQueue* rindā lēmumu pieņemšanas momentā

AggSessAC metodes skaitliskās vērtības			
Izvēlētais pieprasījumu kopas lielums, pieprasījumi	Agregācijas periods, ms	Vidējais <i>AggSessACQueue</i> rindas garums, pieprasījumu skaits	Vidējais pieprasījumu pavadītais laiks <i>AggSessACQueue</i> rindā, ms
10	50	8.7	21
20	100	17.7	42
30	150	26.9	65

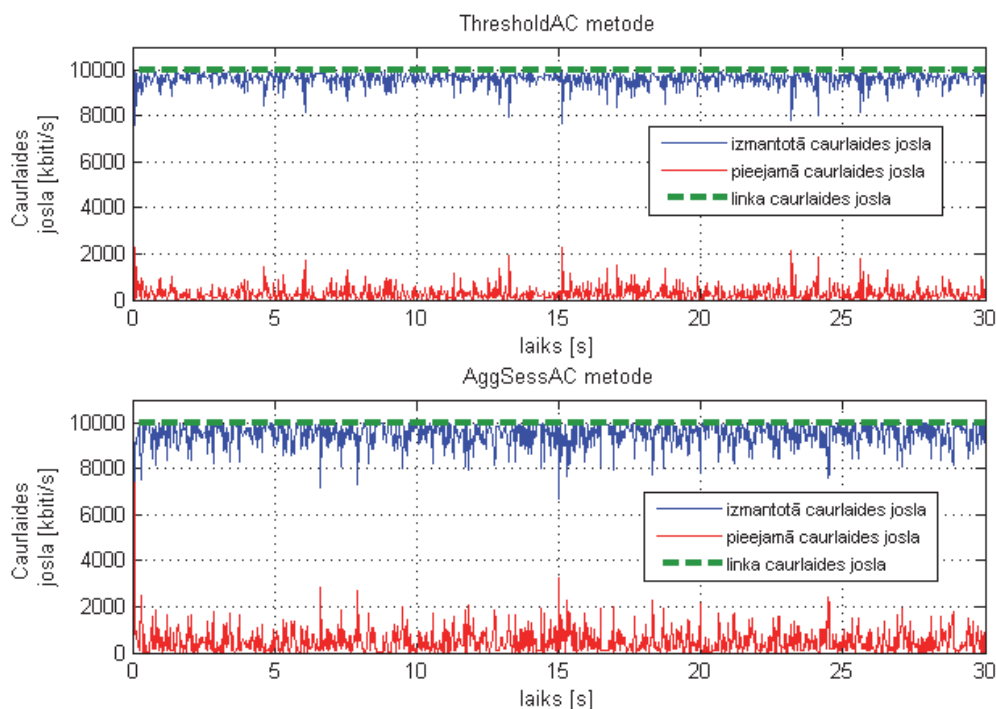
29. att. parādīts vidējais jauno savienojuma pieprasījumu pakešu pavadītais laiks *AggSessACQueue* rindā. **Jauno pieprasījumu pavadītais laiks rindā veido “cenu”, kas AggSessAC risinājumā “jāmaksā” par iespējam lēmumu pieņemšanas brīdī analizēt pieprasījumu kopu, nodrošinot izvēles iespējas un ļaujot realizēt pro-aktīvu un prioritāru vadības politiku.** No 6. tabulā apkopotajiem rezultātiem var secināt, ka vidējais pieprasījumu pavadītais laiks rindā nav lielāks kā puse no izvēlēta maksimālā agregācijas perioda, ja agregācijas periods aprēķināts, balstoties uz zināšanām par vidējo jauno pieprasījumu intensitāti. Apliecinājumu tam var redzēt arī 30. attēlā, kas iegūts simulācijas eksperimenta scenārijā ar kopas izmēru 10 un agregācijas periodu 50 ms. Pieprasījumi, kas agregācijas perioda laikā pienāk vēlāk, arī *AggSessACQueue* rindā uzskatās īsāku laiku.



30. att. Apstiprināto pieprasījumu pavadītais laiks *AggSessACQueue* rindā (histogramma no 20 intervāliem pie pieprasījumu kopas izmēra 10 un agregācijas perioda 50 ms).

Ietekme uz kanāla noslodzi

Salīdzinoši rezultāti ar ietekmi uz kanāla noslodzi, izmantojot *AggSessAC* un salīdzinot ar klasisko *ThresholdAC* metodi, novērtēti 31. att. un to skaitliskās vērtības dotas 7. tabulā.



31. att. Kanāla noslodzes atšķirības 30 sastrēguma simulācijas periodā uz 10 Mbit/s kanāla ar *ThresholdAC* un *AggSessAC* metodi pie kopas izmēra 10 un agregācijas perioda 50 ms.

AggSessAC metodes gadījumā vidējā izmantotā caurlaides josla ir nedaudz mazāka kā *ThresholdAC* metodes gadījumā. Tā galvenais iemesls – plūsmas, kuras kļūst neaktīvas un tiek atslēgtas agregācijas perioda laikā, netiek tik ātri aizstātas ar jaunām plūsmām, jo jaunu plūsmu pieslēgšana notiek agregācijas perioda beigās. Tomēr šeit svarīgi atzīmēt, ka nozīmīga ietekme veidojas tikai gadījumā, kad *AggSessAC* metode ir uzstādīta tīklā ar šai metodei nepiemērotiem kvantitatīviem rādītājiem:

- 1) kopējais caurlaides joslas izmērs attiecībā uz atslēgtās plūsmas ātrumu (bit/s),
- 2) izvēlētā agregācijas perioda attiecība pret jauno pieprasījumu intensitāti.

Pirmkārt, šajā simulācijas scenārijā tika izmantots 10 Mbit/s caurlaides kanāls ar vidējo plūsmas pieprasījuma lielumu 450 Kbit/s, kas nozīmē, ka vidēji vienas atslēgtas plūsmas ietekme veido 4.5 % no kopējās caurlaides joslas; savukārt, ja to attiecina uz 1 Gbit/s kanālu, ietekme sastādīs 0.045 %; ja attiecina uz 10 Gbit/s kanālu, tas veidos 0.0045 %. Otrkārt, palielinoties kanāla caurlaides joslai, sastrēguma brīžos visbiežāk būs arī augstāka jauno plūsmu intensitāte, un tas prasīs īsākus agregācijas periodus. Šie rezultāti apstiprina promocijas autora apgalvojumu, ka metode ir projektēta izmantošanai ātrgaitas (>1 Gbit/s) datu pārraides tīklos, reaģējot uz mūsdienu tīklos esošo augsto jauno savienojumu intensitāti un plašo dažādo servisu klāstu un prasībām.

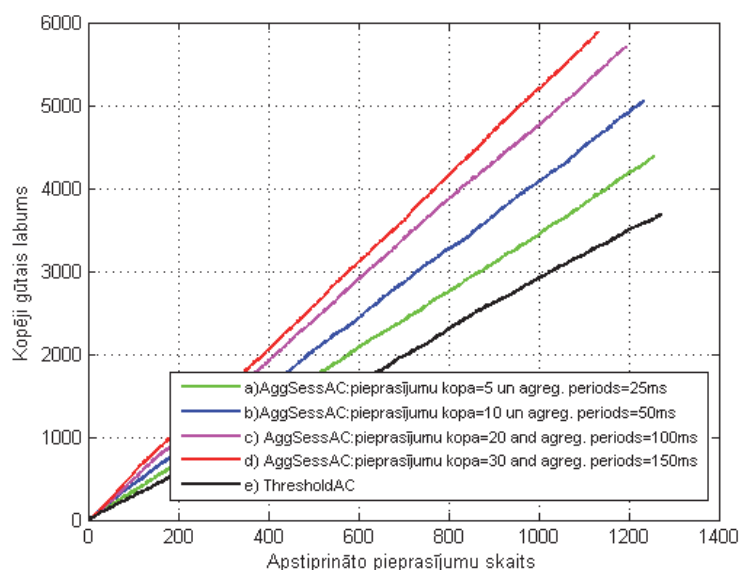
7. tabula

Kanāla noslodzes atšķirības AggSessAC un ThresholdAC metodes gadījumā

AggSessAC metodes skaitliskās vērtības			
Izvēlētais pieprasījumu kopas lielums, pieprasījumi	Agregācijas periods, ms	Vidējā kanāla noslodze, Mbit/s	Atšķirība no ThresholdAC, %
5	25	9.61	-0.6
10	50	9.42	-2.6
20	100	9.05	-6.4
30	150	8.54	-11.7
ThresholdAC metode			
–	–	9.67	–

Gūtā labuma novērtējums

Šajā gadījumā “gūtā labuma” aprēķins tiek balstīts uz vēlmi sasniegt prioritāru piekļuves vadību, kura nosaka, ka augstāku prioritāšu plūsmām jāsaņem augstāka apstiprināšanas priekšrocība.



32. att. Kumulatīvi gūtā labuma pieaugums ar ThresholdAC un AggSessAC metodi.

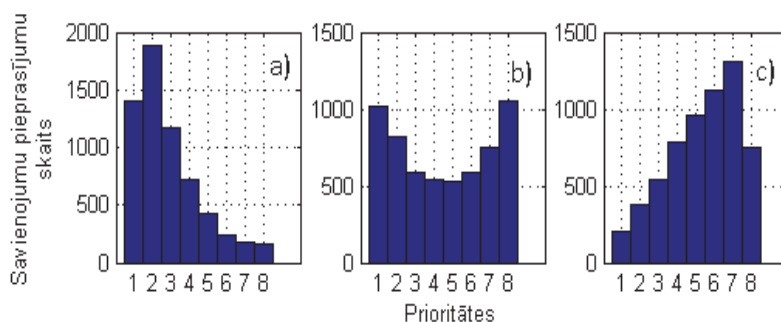
Iegūtie rezultāti šajā konkrētā simulācijas scenārijā parādīja, ka kumulatīvi gūtais labums ar AggSessAC risinājumu ir par 15–37 % augstāks salīdzinājumā ar ThresholdAC risinājumu. Kopēji gūta labuma pieauguma temps ir atkarīgs no vienlaicīgi izvērtējamo pieprasījumu skaita lēmumu pieņemšanas momentā. 32. attēlā redzams, kā, palielinot selektīvās izvēles iespējas, lēmumu pieņemšanas brīžos pieaug pieņemto lēmumu kvalitāte. Rezultātā tiek apstiprināts arvien vairāk augstāku prioritāšu plūsmu, kas veicina gūta labuma pieaugumu un definētās vadības politikas izpildi.

Jāuzsver, ka sasniegt šādu efektivitāti un izpildīt prioritāru, proaktīvu vadības politiku ir iespējams, pateicoties AggSessAC metodei, kas lēmumu pieņemšanas brīdī lēmumu pieņemšanas aģentam nodrošina iespēju analizēt pieprasījumu kopu, nevis vienu individuālu pieprasījumu, kā tas ir esošajās piekļuves vadības metodēs.

Gūta labuma novērtējums pie dažādiem ieejas prioritāšu sadalījumiem

Šajā simulācijas scenārijā izmantoti trīs dažādi ieejas trafika modeļi:

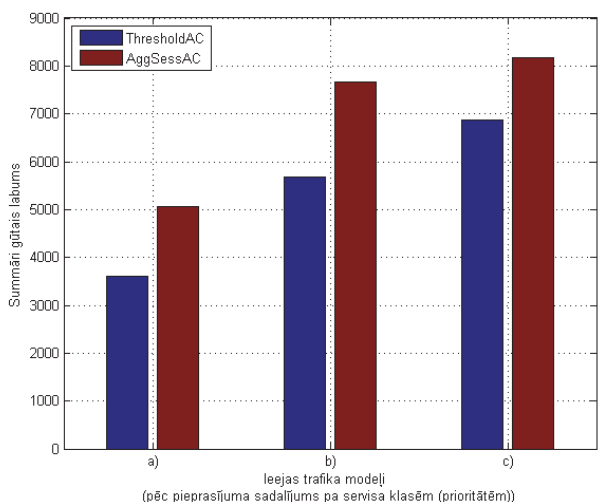
- trafiks, kurš ietver tendenci saturēt daudz vairāk zemu prioritāšu plūsmu nekā augsto prioritāšu plūsmu (33.a att.);
- trafiks, kurš ietver vienlīdz daudz gan zemāko, gan augstāko prioritāšu plūsmu, bet salīdzinoši mazāk vidējo prioritāšu plūsmu (33.b att.);
- trafiks, kurš ietver tendenci saturēt daudz vairāk augsto prioritāšu plūsmu nekā zemo prioritāšu plūsmu (33.c att.).



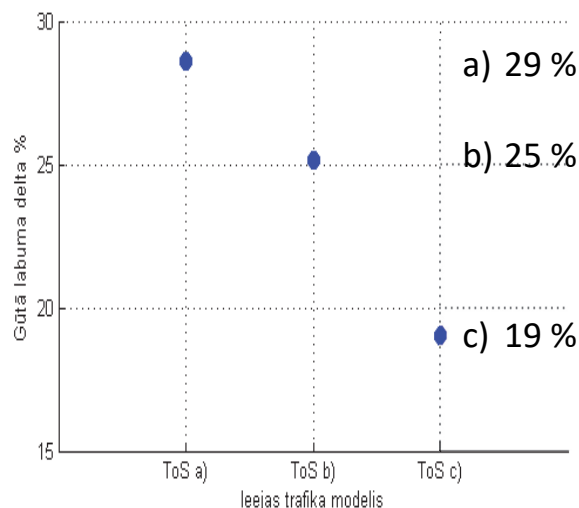
33. att. Prioritāšu sadalījuma histogrammas ieejā ģenerētiem pieprasījumiem.

34. att. uzskatāmi parāda summāri gūto labumu ar AggSessAC un ThresholdAC metodi ar trīs dažādiem ieejas prioritāšu sadalījumiem (skat. 33. att.) un izmantojot eksponenciālu jaunu savienojumu starp-ierašanās laika sadalījumu. Jāatzīmē, ka, aprēķinot procentuāli gūto labumu starp ThresholdAC un AggSessAC metodēm, pēc 35. att. var secināt, ka vislielākā atšķirība veidojas tieši gadījumā, kad ieejas trafiks satur daudz zemu prioritāšu plūsmu, kā tas ir atbilstoši 33.a att. Tas liecina par AggSessAC risinājuma efektivitāti realizēt prioritāru vadības politiku un spēju izcelt mazo skaitu augstāku prioritāšu plūsmu liela zemu prioritāšu plūsmu fona apstākļos.

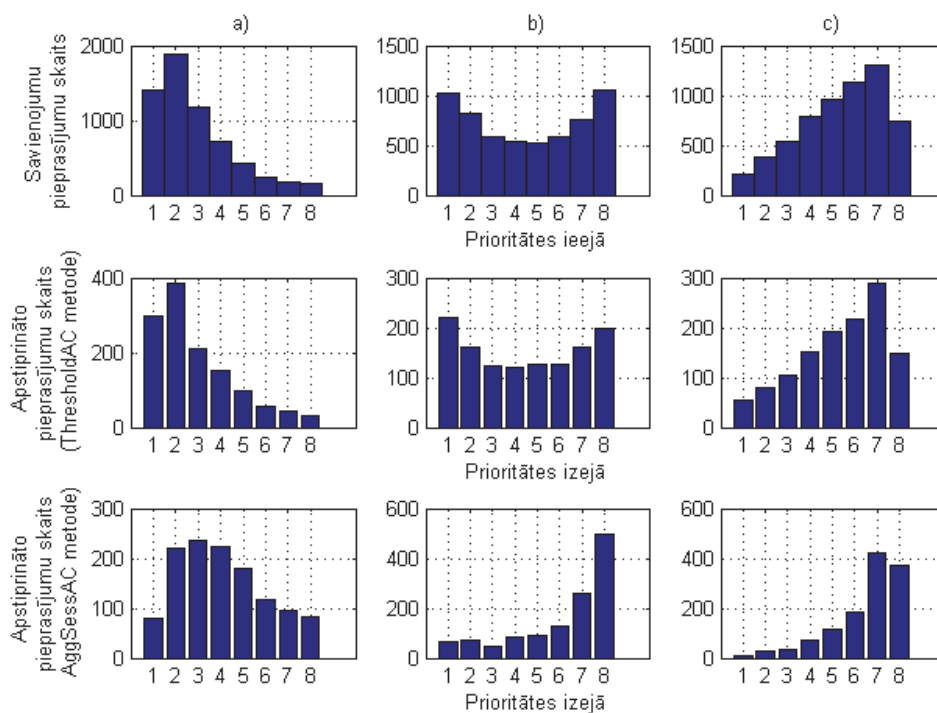
Apstiprināto plūsmu sadalījums pēc prioritātēm 36. att. ļauj secināt, ka tradicionālā ThresholdAC metode izejā dod ļoti līdzīgu ainu ieejai, kam iemesls ir izvēles neesamība lēmumu pieņemšanas brīdī, savukārt AggSessAC gadījumā apstiprināto plūsmu aina izejā ievērojami atšķiras, demonstrējot AggSessAC spēju realizēt uzdoto vadības politiku.



34. att. ar ThresholdAC un AggSessAC metodi ar pieprasījumu kopas garumu 10 un agregācija periodu 50 ms.



35. att. Summāri gūtais labums ar ieejas trafika paterniem atbilstoši delta (procentuālā atšķirība starp ThresholdAC un AggSessAC metodēm ieejas prioritāšu sadalījumiem atbilstoši 33. att.).

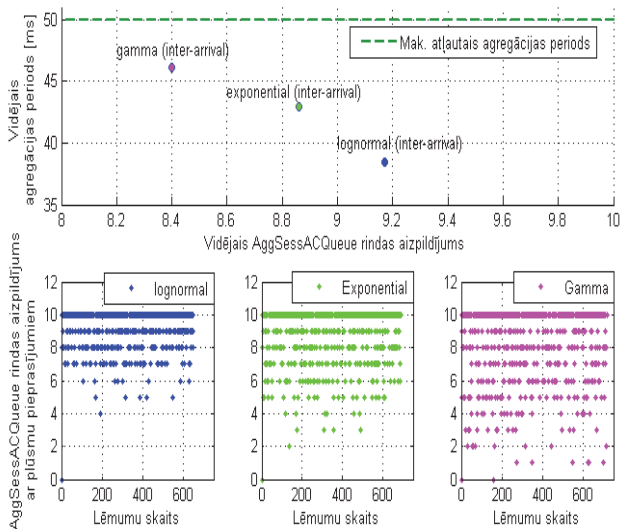


36. att. Apstiprināto pieprasījumu skaita sadalījums pa prioritāšu līmeņiem ar ThresholdAC un AggSessAC metodi ar dažādiem ieejas trafika prioritāšu sadalījumiem.

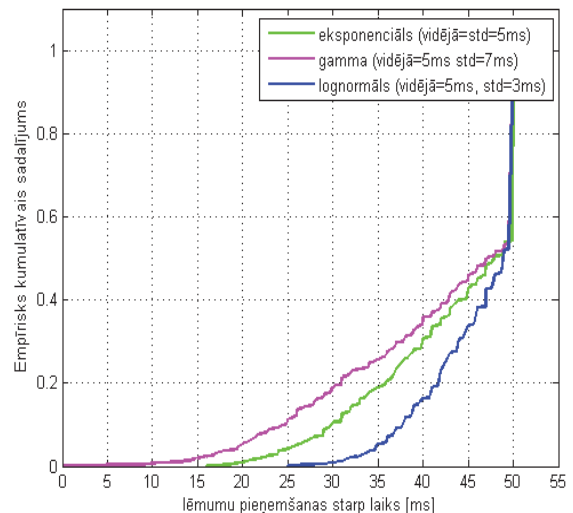
Ieejas plūsmu starp-ierašanās sadalījuma ietekme uz AggSessAC rezultātiem

Darbā novērtēta arī izstrādātās piekļuves vadības metodes darbība pie dažādiem jaunu plūsmu sadalījumiem un novērtēta ietekme uz iegūtajiem rezultātiem. Novērtēšanai izmantoti lognormālais, eksponenciālais un gamma sadalījums ar vidējo vērtību 5 ms, bet ar dažādām dispersijām – attiecīgi 3 ms, 5 ms, 7 ms.

Mazākā jaunu plūsmu starp-ierašanās laika dispersija dod lielāku *AggSessACQueue* rindas garumu lēmumu pieņemšanas brīdī, kā rezultātā iegūst vairāk pieprasījumu vienlaicīgai izvērtēšanai (skat. 37. att.). 38. att. redzams, kā pienākošo pieprasījumu starp-ierašanās laika dispersija ietekmē lēmuma pieņemšanas brīžu izkliedi. Lielāka plūsmu starp-ierašanās laika dispersija apgrūtina piemērotu *AggSessAC* parametru vērtību izvēli. Kopumā no 8. tabulā atspoguļotajiem rezultātiem var secināt, ka nelielās dispersijas izmaiņas pie dažādiem sadalījumiem neatstāj būtisku ietekmi uz gūtā labuma pieaugumu, un tas ir ļoti tuvs pie visiem sadalījumiem.



37. att. Vidējais agregācijas periods un *AggSessACQueue* rindas garums lēmumu pieņemšanas brīdī (kopas izmērs 10 un agregācijas periods 50 ms).



38. att. Empīrisks lēmumu pieņemšanas starplaiku kumulatīvais sadalījums (kopas izmērs 10 un agregācijas periods 50 ms).

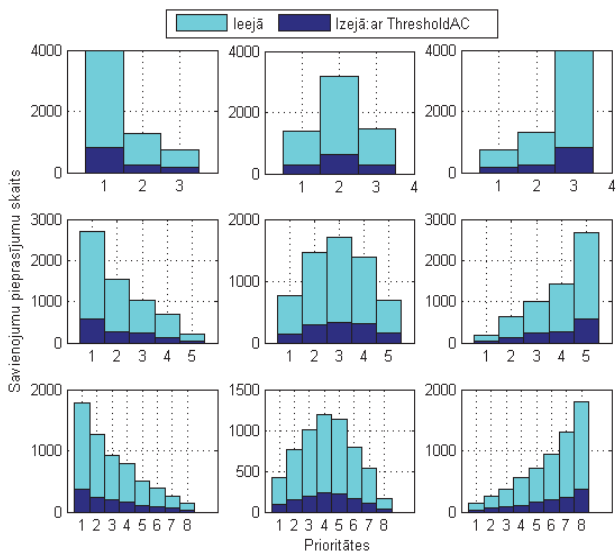
8. tabula

Rezultātu skaitliskās vērtības *AggSessAC* un *ThresholdAC* metodes gadījumā

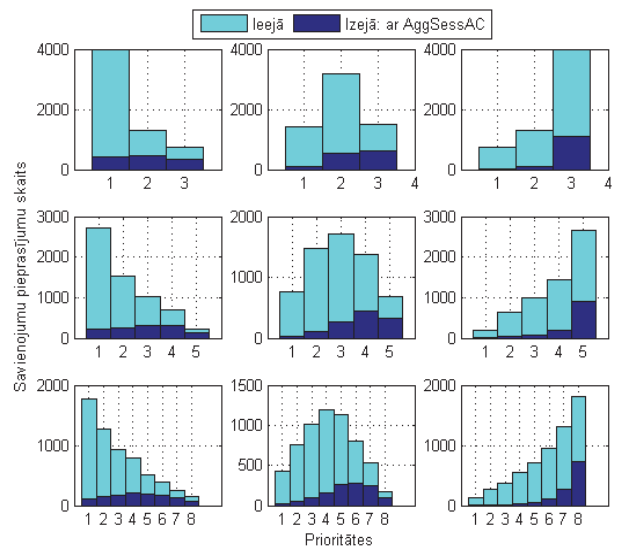
Tīkla sastrēguma simulācijas laiks 30 s							
Savienojuma pieprasījumu pienākšanas sadalījums	<i>ThresholdAC</i> risinājums		<i>AggSessAC</i> risinājums				
	Gūtais labums	Lēmumu skaits	Gūtais labums	Lēmumu skaits	Vid. agregācijas periods, ms	Vidējais <i>AggSessACQueue</i> rindas garums lēmuma momentā, jauns pieprasījums	Gūtā labuma pieaugums
lognormāls	3616	5960	5050	649	46	9.17	+28.4 %
eksponenciāls	3592	6014	5032	688	44	8.86	+28.6 %
gamma	3519	6035	4965	718	42	8.40	+29.1 %

Selektivitāte

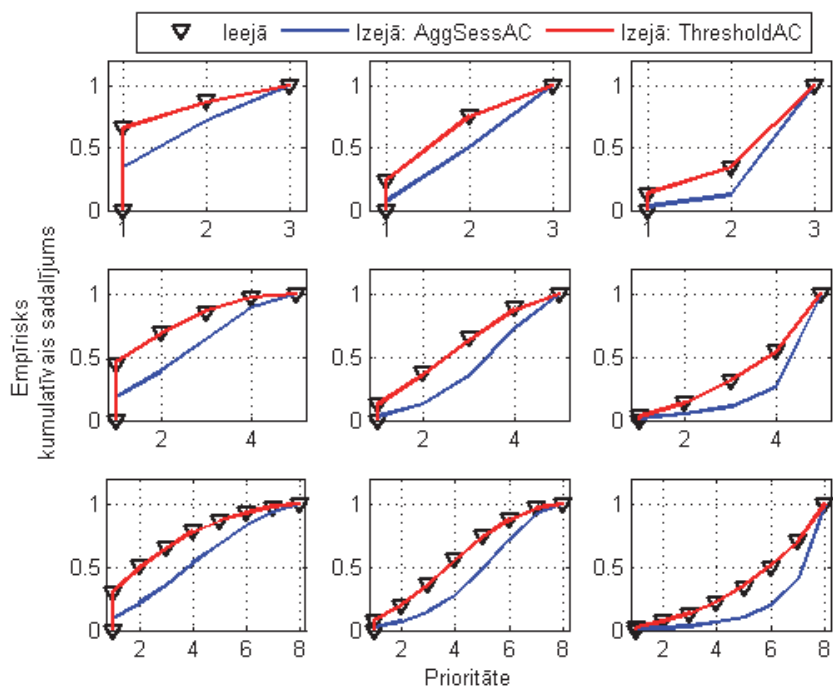
Šajā etapā tika novērtētas *AggSessAC* risinājuma spējas pie dažāda trafika prioritāšu līmeņu skaita ar dažādiem prioritāšu sadalījumiem. Ieejas trafiks ar eksponenciālu plūsmu starp-ierašanās laiku un gamma sadalījumu plūsmu izmēriem pie pieprasījumu kopas izmēra 10 pieprasījumi un agregācijas perioda 50 ms.



39. att. Ieejas ģenerētās un izejā iegūtās apstiprināto savienojumu prioritāšu sadalījuma histogrammas ar ThresholdAC risinājumu.



40. att. Ieejas ģenerētās un izejā iegūtās apstiprināto savienojumu prioritāšu sadalījuma histogrammas ar AggSessAC risinājumu.



41. att. Ieejā ģenerētais un izejā iegūtais apstiprināto prioritāšu empīriskais kumulatīvais sadalījums ar ThresholdAC un AggSessAC risinājumiem.

Atšķirīgo prioritāšu plūsmu pieslēgumu skaitliskās vērtības un tendenci var redzēt, salīdzinot 39. un 40. attēlu. Rezultāti 39. att. demonstrē, ka ThresholdAC metode, izvērtējot tikai vienu pieprasījumu katrā lēmumu pieņemšanas momentā, izejā veido tādu pašu struktūru ar apstiprināto plūsmu prioritāšu veidiem, kā tika uzdots ieejā. Tas liecina, ka klasiskā (ThresholdAC) pieprasījumu apstrādes maniere nespēj nodrošināt prioritāru vadības politikas izpildi – visu prioritāšu klases tiecas saņemt vienādu atteikuma iespējamību.

AggSessAC risinājuma spēju izteikti izmainīt kopējo apstiprināto plūsmu struktūru izejā var redzēt 40. attēlā. Kā izmanījies prioritāšu empīriskā kumulatīvā sadalījuma līkne izejā

AggSessAC gadījumā no ieejas sadalījuma var redzēt 41. attēlā. Izejā iegūtās līknes izmaiņu virziens ir atkarīgs no izmantotās vadības politikas, un atšķirība AggSessAC risinājumā ir sasniegta, pateicoties spējai nodrošināt vairāku vienlaicīgu pieprasījumu savstarpēju izvērtēšanu un rezultātā atšķirīgu plūsmu pieslēgšanu.

Neatkarīgi no ieejas trafika prioritāšu skaita un ieejas plūsmu sadalījuma pa prioritātes līmeņiem **AggSessAC risinājums, pateicoties spējai nodrošināt selektīvas izvēles iespējas, paaugstina pieņemto lēmumu kvalitāti – palielināt gūto labumu atbilstoši sastādītās vadības politikas mērķiem.**

PROMOCIJAS DARBA GALVENIE REZULTĀTI

Veicot darba ievadā definēto uzdevumu izpildi, iegūti galvenie promocijas darba secinājumi un rezultāti.

- Augošais IT pakalpojumu klāsts nosaka, ka jaunās paaudzes tīkli attiecībā uz jebkuru iepriekšējo paaudzi būs aizvien prasīgāki pret resursu pieejamību tiešsaistes pakalpojumiem un nospraustās vadības politikas izpildi. Jaunās paaudzes tīkli savā būtībā nosaka dalītus vadības un transporta slāņus. Jebkura nākamā tīklu paaudze izvirzīs aizvien lielākas prasības pret vadības slāni, kas ietver resursu un piekļuves vadības uzdevumus, – tiem jāklūst ātrākiem, efektīvākiem un selektīviem.
- Plūsmu skaits tīklos nemitīgi palielinās, kas šodien resursu un piekļuves vadībai liek strādāt μs – ms diapazonā. Saskaņā ar Cisco CARG pētījumiem mobilo ierīču pieslēgumu skaits caur IEEE802.11 piekļuves punktiem nemitīgi palielinās, apejot mobilo operatoru tīklus un noslogojot fiksētos piekļuves punktus. Augstā jauno plūsmu intensitāte noslogoto piekļuves mezglus. Turklāt jau šodien 80 % no TCP plūsmām nav garākas par 3–10 sekundēm! Lai arī UDP trafika apjoms (biti/s) internetā veido 10 %, tomēr no plūsmu skaita viedokļa UDP plūsmu skaits ir līdzvērtīgs TCP plūsmu skaitam un vairāk nekā 80 % UDP plūsmu garums ir samazinājies līdz minimumam un satur vien dažas paketes.
- Esošie piekļuves vadības risinājumi reaģē momentāni, secīgi un neatkarīgi uz katru jaunu pienākošo savienojuma pieprasījumu, samazinot iespējas pieņemt lēmumus selektīvi un prioritāri. Šādā gadījumā iespēja selektīvi izvēlēties prioritāras vienības un realizēt diferencētu apkalpošanas stratēģiju var balstīties tikai uz resursus prasīgiem apstrādes algoritmiem – prognozēšanas, nestriktās loģikas vai citiem kompleksiem risinājumiem. Prognozēšanas risinājumi var būt efektīvi turpmāko tendenču noteikšanā, tomēr vāja un apšaubāma ir momentāno vērtību (μs – ms), tādu kā savienojumu pieprasījumu prasību prognozēšana, lai iegūtu kaut cik ticamu rezultātu.
- Neviens no autoram zināmajiem pētījumiem neizskata iespēju atteikties no momentānas un neatkarīgas jaunu plūsmu savienojumu pieprasījumu apstrādes manieres un *lēmuma pieņemšanas brīdī analizēt agregētu jaunu savienojumu pieprasījumu kopu ar nolūku iegūt selektīvu un prioritāru resursu un piekļuves vadību.*
- Izstrādātais AggSessAC risinājums, kurš balstās uz īslaicīgu jaunu savienojumu pieprasījumu agregāciju, nodrošina iespēju piekļuves vadībā ienest savienojumu paralēlas apstrādes virtualizāciju, tādējādi ļaujot apskatīt pieprasījumus kā notikumu kopu, radot iespēju tos savstarpēji salīdzināt un izvērtēt lēmumu pieņemšanas brīdī.

- Darbā izstrādātā AggSessAC metode ir realizēta kā funkcionāls vadības aģents, kurš integrēts OMNeT++ simulācijas vidē INET ietvarā pieejamā maršrutētāja programmatūrā kā jauns resursu un piekļuves vadības rīks, radot eksperimentālu produktu. Dotais programmnodrošinājums ir pieejams studentiem un pētniekiem ar iespēju to integrēt citos trafika vadības uzdevumos/pētījumos.
- Izstrādātajā AggSessAC risinājumā jaunu pieprasījumu novirzīšana atsevišķā rindā nodrošina, ka lēmumu pieņemšanas brīžu aizture neietekmē iepriekš apstiprināto plūsmu kvalitāti, un, ņemot vērā, ka plūsmu intensitāte (jaunas plūsmas/s) ātrgaitas (gigabitu) interneta datu pārraides kanālos mērāma ar kārtu 10^3 vai vairāk (interneta trafika analīze uzrādīja, ka uz 10 Gbit/s kanāla pat ar kārtu 10^4), tas ļauj izvēlēties pieprasījumu uzkrāšanas kopas izmēru tā, lai aizture jauno sesiju apstiprināšanai nepārsniegtu dažu (<5) ms robežu.
- Pie izvēlētas pieprasījumu uzkrāšanas kopas izmēra maksimālās robežvērtības, zinot kanālā vidējo jauno plūsmu starp-ierašanās laiku, ir iespējams noteikt nepieciešamo uzstādāmo agregācijas perioda robežvērtību, lai vidējais uzkrātais jauno pieprasījumu skaits *AggSessACQueue* rindā būtu tuvs uzstādītajam rindas garumam (kopas izmēram).
- Pārmērīgi īss izvēlētais agregācijas periods attiecībā uz jaunu plūsmu intensitāti un izvēlēto pieprasījuma kopas izmēru samazina gaidāmo AggSessAC metodes efektivitāti, ja lēmumu pieņemšanas brīdī uzkrāto pieprasījumu skaits nav tuvs izvēlētajam pieprasījuma kopas izmēram.
- Ņemot vērā, ka AggSessAC metode ir projektēta tīkla mezgliem ar kanāla caurlaidspēju ≥ 1 Gbit/s un jaunu plūsmu intensitāti (jaunas plūsmas/s), kas mērāma ar kārtu 10^3 vai vairāk, ietekme uz kanāla utilizāciju nepārsniedz procentu simtdaļas no kopējās caurlaides spējas.
- Rezultāti rāda, ka selektivitāte un izvēles iespējas lēmumu pieņemšanas brīdī veicina atšķirīgu (alternatīvu) plūsmu apstiprināšanu un nodrošina izteiktu spēju realizēt prioritāru vadības politiku, pieslēdzot lielāku skaitu augstas prioritātes plūsmu, pat gadījumā, kad ienākošais trafiks satur izteikti lielāku skaitu zemu prioritāšu plūsmu salīdzinājumā ar secīgu un neatkarīgu pieprasījumu apstrādes veidu.
- AggSessAC risinājums nodrošina vadību plūsmu līmenī un, patiecoties selektīvai izvēlei, pie jebkuras uz prioritātēm definētas vadības politikas spēj palielināt gūto labumu no pieņemtajiem lēmumiem atbilstoši sastādītās vadības stratēģijai. Šādi pieņemti lēmumi paaugstina kopējo piekļuves vadības efektivitāti. Kvantitatīvi rezultāti vienmēr būs atkarīgi no trafika sastāva plūsmu līmenī, izvēlētas vadības politikas, plūsmu sadalījuma pa prioritātes līmeņiem un citiem datu plūsmu raksturojošiem parametriem.

Darbā izvirzītais mērķis sasniegts, un darba uzdevumi izpildīti. Sasniegtie promocijas darba rezultāti ir daudzsološi. Izstrādātais AggSessAC risinājums pie augstās jaunu plūsmu intensitātes, kāda eksistē mūsdienu datu pārraides tīklos, izmantojot īslaicīgu jaunu savienojumu pieprasījumu uzkrāšanu, nodrošina selektīvu, prioritāru un pro-aktīvu resursu un piekļuves vadību. AggSessAC strādā, neietekmējot apstiprināto plūsmu kvalitāti un neizmantojot resursu prasīgus skaitļošanas līdzekļus vai prognozēšanas risinājumus papildu informācijas iegūšanai, lai realizētu efektīvu piekļuves vadību.

INFORMĀCIJAS AVOTI

1. J. Baraković, H. Bajrić, and S. Baraković, "Priority Level Configuration for Signaling Service Class," *2010 Third International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ)*, 2010, pp. 122–127.
2. T. Barnett, Cisco VNI Complete Forecast Update: Key Trends Include Mobility, M2M and Multimedia Content, May 27, 2015. Source – Cisco VNI: *Global IP Traffic Forecast, 2014–2019*. Internet: <http://blogs.cisco.com/sp/2015-cisco-vni-complete-forecast-update-key-trends-include-mobility-m2m-and-multimedia-content>
3. S. Blake *et. al.*, "An Architecture for Differentiated Services," IETF RFC 2475, Dec. 1998.
4. P. Carvalho, P. Solis, B. Queiroz, B. Carneiro, and M. Deus, "A Traffic Analysis per Application in real IP/MPLS Service Provider Network," in: *Broadband Convergence Networks, BcN '07. 2nd IEEE/IFIP International Workshop*, 2007, pp. 1–5.
5. B. K. Choi, D. Xuan, C. Li, R. Bettati, and Wei Zhao, "Utilization-Based Admission Control for Scalable Real-Time Communications," in: *Journal of Real-Time Systems*, Vol. 24, No. 2, 2003, pp. 171–202.
6. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014–2019, White Paper. Internet: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html
7. Cisco Visual Networking Index: Forecast and Methodology, 2015–2020, White paper. Internet: <http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf>
8. Cloud Series Devices. Internet: <http://cloudcorerouter.com/>
9. A. Dainotti, A. Pescapè, and K. Claffy, "Issues and future directions in traffic classification." *IEEE Network*, Vol. 26, No. 1, pp. 35–40, Jan 2012.
10. I. Din, N. Saqib, and A. Baig, "Passive analysis of web traffic characteristics for estimating quality of experience," *GLOBECOM Workshops, 2008 IEEE*. IEEE, 2008, pp. 1–5.
11. W. de Donato, A. Pescapè, and A. Dainotti, "Traffic Identification Engine: An Open Platform for Traffic Classification", *IEEE Network*, Vol. 28, No. 2, March 2014, pp. 56–64.
12. H. Ekström, "QoS Control in the 3GPP Evolved Packet System," *IEEE Commun. Mag.*, Vol. 47, No. 2, Feb. 2009, pp. 76–83.
13. M. Feknous, T. Houdoin, B. Le Guyader, J. De Biasio, A. Gravey, and J. A. Torrijos Gijon, "Internet traffic analysis: A case study from two major European operators," in: *Proceedings of the 2014 IEEE Symposium on Computers and Communication (ISCC)*, Funchal, 23–26 June 2014, pp. 1–7.
14. P. Flavius, and P. Ferdi, "Internet Service Delivery Models: Evolution and Current Issues," *2011 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2011, pp. 146–153.
15. S. Floyd, "Comments on Measurement-based Admissions Control for Controlled-Load Service," *Submitted to Computer Communication Review*, 1996.
16. V. R. Gandhi, Y. R. Qu, and V. K. Prasanna, "High-throughput hash-based online traffic classification engines on FPGA," in: *Proc. 2014 International Conference on ReConFigurable Computing and FPGAs (ReConFig14)*, Cancun, Dec. 2014, pp. 1–6.
17. T. Ganegedara, and V. K. Prasanna, "StrideBV: Single Chip 400G+ Packet Classification," in: *13th IEEE International Conference on HighPerformance Switching and Routing (HPSR)*, 2012, pp. 1–6.
18. E. Garsva, N. Paulauskas, G. Grazlevicius, and L. Gulbinovic, "Packet Inter-arrival Time Distribution in Academic Computer Network," *Electronics and Electrical Engineering*, No. 20(3), ISSN 1392-1215, Lithuania, Kaunas, 2014, pp. 87–90.

19. S. Gebert, R. Pries, D. Schlosser, and K. Heck, "Internet Access Traffic Measurement and Analysis," in: *Proceedings of the 4th International Conference on Traffic Monitoring and Analysis*, Vienna, Austria, 2012, pp. 29–42.
20. INET Framework. Internet: <http://inet.omnetpp.org/>
21. Recommendation ITU-T Y.2001, "General overview of NGN", 2004.
22. Recommendation ITU-T Y.2111, "Resource and Admission Control Functions in NGN", 2011.
23. S. Jamin, P. B. Danzig, S. Shenker, and L. Zhang, "A Measurement-based Admission Control Algorithm for Integrated Services Packet Network," *IEEE/ACM Transactions on Networking*, Vol. 5, Iss. 1, 1997, pp. 56–70.
24. S. Jamin, S. Shenker, and P. Danzig, "Comparison of Measurement-based Admission Control Algorithms for Controlled-Load Service," in: *Proc. of INFOCOM '97*, Vol. 3, April 1997, pp. 973–980.
25. J. Jelinskis, A. Skrastins, and G. Lauks, "Fuzzy-CAC Driven MPLS-TE Realization," *12th IEEE International Conference on High Performance Switching and Routing*, Spain, Cartagena, July 4–7, 2011, pp. 146–150.
26. J. Jelinskis, A. Skrastins, and G. Lauks, "Practical Fuzzy-CAC Realization for Effective Traffic Engineering in MPLS-TE Network," *Electronics and Electrical Engineering. Kaunas: Technologija*, 2011, No. 4(110), pp. 30–34.
27. J. Jelinskis, A. Skrastins, and G. Lauks, "Fuzzy-CAC based Traffic Management in MPLS-TE Networks," *11th International Conference on Telecommunications, ConTEL 2011*, Graz, Austria, June 1517, 2011, pp. 389–395.
28. Y. Jia, and M. Chen, "A new architecture of providing end-to-end quality-of-service for differentiated services network," in: *Proc. of IEEE Military Communications Conference 2001(MILCOM 2001)*, No. 1, Oct. 2001, pp. 1451–1456.
29. W. Jiang, and V. K. Prasanna, "Large-scale wire-speed packet classification on FPGAs," in: *Proc. FPGA '09. ACM*, 2009, pp. 219–228.
30. W. Jiang, and V. K. Prasanna, "Scalable Packet Classification on FPGA," *IEEE Trans. VLSI Syst.*, Vol. 20, No. 9, 2012, pp. 1668–1680.
31. W. John, and S. Tafvelin, "Analysis of internet backbone traffic and header anomalies observed," in: *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. ACM*, 2007, pp. 111–116.
32. M. Kuļikovs, and E. Pētersons, "Real-Time Traffic Analyzer for Measurement-Based Admission Control," in: *Proceeding of The Fifth Advanced International Conference on Telecommunications AICT2009*, Venice/Mestre, Italy, 2009, pp. 72–75.
33. M. Kuļikovs, E. Pētersons, and S. Šarkovskis, "Integral measurement process of incoming traffic for Measurement-Based Admission Control," in: *Proceedings, 2010 IEEE Region 8 International Conference on Computational Technologies in Electrical and Electronics Engineering*, Russia, Irkutsk, Listvyanka, Vol. 1, 2010, pp. 183–186.
34. K. C. Lan, and J. Heidemann, "A measurement study of correlations of Internet flow characteristics," *Computer Networks*, Vol. 50, No. 1, Jan. 2006, pp. 46–62.
35. D. Lee, B. E. Carpenter, and N. Brownlee, "Media Streaming Observations: Trends in UDP to TCP Ratio", *International Journal on Advances in Systems and Measurements*, Vol. 3, No. 3 and 4, April 2011, pp. 147–162.
36. R. Leira, P. Gomez, I. Gonzalez, and J. E. Lopez de Vergara, "Multimedia flow classification at 10 Gbps using acceleration techniques on commodity hardware," in: *Proc. of SaCoNeT*, Vol. 3, Paris, 2013, pp. 1–5.
37. B. Li, J. Springer, G. Bebis, and M. H. Gunes, "A survey of network flow applications," *Journal of Network and Computer Applications*, Vol. 36, No. 2, 2013, pp. 567–581.
38. X. Li, and S. Paul, "Class-based Bandwidth Allocation and Admission Control for QoS VPN with DiffServ," *Comsware 2006*, New Delhi, 2006, pp. 1–10.

39. Y. Ma, S. Banerjee, S. Lu, and C. Estan, "Leveraging Parallelism for Multi-dimensional Packet Classification on Software Routers," *SIGMETRICS Perform. Eval. Rev.*, Vol. 38, No. 1, 2010, pp. 227–238.
40. M. Marston, and F. Mistree, "An implementation of expected utility theory in decision based design," in: *Proc. 10th International Conference on Design Theory and Methodology (DETC)*, Atlanta, GA, USA, 1998, pp. 1–11.
41. K. Mase, and Y. Toyama, "End-to-End Measurement Based Admission Control for VoIP Networks," *IEEE ICC*, 2002, pp. 1194–1198.
42. A. Meddeb, "Internet QoS: Pieces of the puzzle," *IEEE Communications Magazine*, Vol. 48, No. 1, January 2010, pp. 86–94.
43. N. Moghim, S. M. Safavi, and M. R. Hashemi, "Evaluation of a new end-to-end quality of service algorithm in differentiated services networks," *IET Communications Magazine*, Vol. 4, No. 14, Sep. 2010, pp. 1687–1695.
44. J. von Neumann, and O. Morgenstern, "The Theory of Games and Economic Behavior", New York, USA: Princeton University Press, 1944.
45. T. Nguyen, and G. Armitage, "A Survey of Techniques for InternetTraffic Classification Using Machine Learning," *IEEE Comm. Surveys Tutorials*, Vol. 10, No. 4, 2008, pp. 56–76.
46. S. Oueslati, and J. Roberts, "A new direction for quality of service: Flow aware networking," NGI 2005, Rome, April 18–20, 2005, pp. 226–232.
47. T. Pan, X. Guo, C. Zhang, J. Jiang, H. Wu, and B. Liuy, "Tracking millions of flows in high speed networks for application identification," in: *INFOCOM, 2012 Proceedings IEEE*, March 2012, pp. 1647–1655.
48. Y. R. Qu, and V. K. Prasanna, "Compact Hash Tables for High-performance Traffic Classification on Multi-core Processors," *2014 IEEE 26th International Symposium on Computer Architecture and High Performance Computing (SBAC-PAD 2014)*, France, 2014, pp. 17–24.
49. Y. Qu, S. Zhou, and V. K. Prasanna, "Scalable Many-Field Packet Classification on Multi-core Processors," in: *Proc. of SBAC-PAD*, Porto de Galinhas, Oct. 2013, pp. 33–40.
50. Y. Saito, M. Hasegawa, and Y. Murata, "A Fast and Efficient End-to-End QoS Measurement Scheme for Real Seamless Handover," *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications. PIMRC 2007*, Athens, Sept. 2007, pp. 1–5.
51. R. Sharma, N. Kumar, and S. Talabattula, "Performance of New Dynamic Benefit-Weighted Scheduling Scheme in DiffServ Networks," in: *Proc. Advances in Computing, Communications and Informatics (ICACCI 2014)*, Sept. 2014, pp. 2578–2583.
52. Z. Shijie, P. R. Nittoor, and V. K. Prasanna, "High-Performance Traffic Classification on GPU", in: *Proc. IEEE 26th International Symposium on Computer Architecture and High Performance Computing (SBAC-PAD 2014)*, Jussieu, Oct. 2014, pp. 97–104.
53. R. Stankiewicz, P. Cholda, and A. Jajszczyk, "QoX: what is it really?," *Communications Magazine*, Vol. 49, Iss. 4, Apr. 2011, pp. 148–158.
54. B. Statovci-Halimi, "Adaptive admission control for supporting class-based QoS," *2010 6th EURO-NF Conference on Next Generation Internet (NGI 2010)*, Paris, 2–4 June, 2010, pp. 1–8.
55. B. Statovci-Halimi, and V. C. Emeakaroha, "Framework for multi-class and dynamic flow-aware admission control," in: *Proc. of the 34th Annual IEEE Conference on Local Computer Networks (LCN 2009)*, Zurich, Oct. 2009, pp. 344–347.
56. Y. Sun, Z. Zhang, L. Guo, S. Bai, and J. Tan, "An Effective Algorithm for Counting Active Flows Based on Loop Bloom Filter," in: *Proc. of IEEE International Conference on Networking, Architecture, and Storage (NAS)*, Chongqing, China, June 2008, pp. 104–109.
57. The CAIDA UCSD Statistical information for the CAIDA Anonymized Internet Traces, Internet: http://www.caida.org/data/passive/trace_stats/

58. D. Tong, Y. R. Qu, and V. K. Prasanna, "High-throughput traffic classification on multi-core processors," *2014 IEEE 15th International Conference on High Performance Switching and Routing (HPSR)*, Canada, 2014, pp. 138–145.
59. A. A. Wahid, and J. Schormans, "Bounding the maximum sampling rate when measuring PLP in a packet buffer," *Computer Science and Electronic Engineering Conference (CEEC)*, Colchester, Sept. 2013, pp. 115–118.
60. P. White, "RSVP and Integrated Services in the Internet: A tutorial," *IEEE Communications Magazine*, Vol. 35, No. 5, 1997, pp. 100–106.
61. B. Whitehead, C.-H. Lung, and P. Rabinovitch, "Tracking Per-Flow State – Binned Duration Flow Tracking," in *Proc. of SPECTS*, Ottawa, July, 2010, pp. 73–80.
62. B. Whitehead, Chung-Horng Lung, and P. Rabinovitch, "An Efficient Approach to Per-Flow State Tracking for High-Speed Networks", in: *Proc. of GLOBECOM 2010*, 6–10 Dec. 2010, pp. 1–6.
63. Wireshark network protocol analyzer. Internet: <https://www.wireshark.org/>
64. Z. Yongqing, M. Maode, and C. Tee-Hiang, "A Novel Multiple Access Scheme for Ethernet Passive Optical Networks," *IEEE GlobeComm '03*, Vol. 5, Dec. 2003, pp. 2649–2653.
65. X. Zhang, and W. Ding, "Comparative Research on Internet Flows Characteristics," in: *Proc. Networking and Distributed Computing (ICNDC 2012)*, Hangzhou, Oct. 2012, pp. 114–118.
66. M. Zhang, M. Dusi, W. John, and C. Chen, "Analysis of udp traffic usage on internet backbone links," in *Ninth Annual International Symposium on Applications and the Internet, 2009. SAINT '09*, IEEE, Bellevue, WA, 2009, pp. 280–281.