

RĪGAS TEHNISKĀ UNIVERSITĀTE

Elektronikas un telekomunikāciju fakultāte

Telekomunikāciju institūts

Arnis Ancāns

Doktora studiju programmas “Telekomunikācijas” doktorants

**AUTOTRANSPORTA BEZVADU SAKARU
TĪKLU VEIKTSPĒJAS PĒTĪŠANA UN TĀS
PAAUGSTINĀŠANA**

Promocijas darbs

Zinātniskais vadītājs
profesors *Dr. habil. sc. ing.*
ERNESTS PĒTERSONS

RTU Izdevniecība
Rīga 2021

PATEICĪBA

Vēlos pateikt lielu paldies promocijas darba zinātniskajam vadītājam profesoram *Dr. habil. sc. ing.* Ernestam Pētersonam par vērtīgajiem padomiem un rekomendācijām promocijas darba izstrādes gaitā, kas man deva neatsveramu atbalstu.

Doktorantūras laikā man bija gods strādāt kopā ar Elektronikas un telekomunikāciju fakultātes Telemātikas un transporta elektronisko sistēmu katedras un Telekomunikāciju institūta kolēģiem. Paldies par vērtīgajiem padomiem, atbalstu un draudzīgo atmosfēru.

No sirds pateicos savai sievai Anitai Geriņai-Ancānei un bērniem Aletai, Paulai un Elanam par atbalstu, sapratni, pacietību un lielo mīlestību, kas deva spēkus un motivāciju strādāt pie promocijas darba.

Paldies visiem, ar kuriem kopā esmu strādājis un kuri mani ir atbalstījuši, bet kuru vārds šeit nav minēts.

ACKNOWLEDGMENT

I would like to express my deep gratitude to the scientific supervisor of the Doctoral Thesis, to professor *Dr. habil. sc. ing.* Ernests Pētersons for the valuable advice and recommendations during the development of the Doctoral Thesis, which gave me invaluable support.

During doctoral studies, I had the honour of working with colleagues from the Department of Telematics and Transport Electronic Systems and the Institute of Telecommunications of the Faculty of Electronics and Telecommunications. Thank you for your valuable advice, support, and a friendly atmosphere.

I am incredibly grateful to my family for the support, understanding, patience, and great love that gave me the strength and motivation to work on Doctoral Thesis.

Thank you to everyone I have worked with and who have supported me, but whose name is not mentioned here.

ANOTĀCIJA

Tādas globālās attīstības tendences kā automobiļu skaita pieaugums, viedo ierīču ar bezvadu tīkla savienojumu skaita palielināšanās un pārraidāmās informācijas apjoma straužais pieaugums, veicina pieprasījumu pēc lielāka datu apmaiņas ātruma, mobilitātes un augstāka savienojamības līmeņa. Tādējādi tiek pieprasīti datu pārraides pakalpojumi arī tādos gadījumos, kad lietotāji pārvietojas ar autotransportu. Pieaugot automobiļu skaitam, jārisina arī problēmas, kas ir saistītas ar drošību uz ceļiem un transporta plūsmu vadību. Šīs problēmas akcentē nepieciešamību pēc mūsdienīgiem, tehniski un ekonomiski pamatotiem intelektuālo transporta sistēmu (*ITS*) sakaru risinājumiem. Viena no bezvadu tīklu tehnoloģijām, ko var izmantot *ITS* vajadzību nodrošināšanai, konkrēti automobiļu pasažieru nodrošināšana ar piekļuvi datu pārraides tīklam, ir *WLAN IEEE 802.11n/ac*. Realizējot šādus *WLAN* bāzētus automobiļu bezvadu sakaru piekļuves tīklus, ir jārisina vairāki jautājumi, kas galvenokārt ir saistīti ar ātri kustīgiem objektiem. Praksē izmantojams ir divrangu bezvadu sakaru tīkls, kas var nodrošināt piekļuvi interneta tīklam.

Promocijas darbā izveidotas un izpētītas vairākas divrangu autotransporta sakaru tīkla testgultnes, izmantojot *WLAN IEEE 802.11n* un *LTE* tehnoloģijas. Eksperimentāli novērtēts, kā mainās datu trafika raksturlielumi divrangu sakaru tīklā, izmantojot dažādu ražotāju *LTE* aparatūru. Pētīta šādu hibrīdu sakaru kanālu veiktspēja atkarībā no mobilo klientu pārvietošanās ātruma, klientu skaita un izmantotajiem kustības scenārijiem. Iegūtas jaunas integrētu *IEEE 802.11n* un *LTE* autotransporta sakaru tīklu veiktspēju raksturojošas likumsakarības, kas apraksta tīkla caurlaidspējas atkarību no mobilā klienta pārvietošanās ātruma. Promocijas darbā izveidota un izpētīta arī vienranga autotransporta sakaru testgultne, kas bāzēta *IEEE 802.11ac* tehnoloģijā. Pētījumā izstrādāts un realizēts uzlabots *IEEE 802.11v* standartā bāzēts pārslēgšanās procedūras (angļu val. *handover*) algoritms. Šādam vienranga automobiļu sakaru tīklam teorētiski novērtētas veiktspēju raksturojošas likumsakarības.

Darba apjoms

141 lappuses, 14 tabulas, 52 attēli, 182 literatūras avoti un deviņi pielikumi.

ANNOTATION

The global development tendencies such as the increase in the number of passenger cars, increase of smart devices with wireless network connection and the rapid increase of the data to be transmitted contribute to demand for higher data exchange speed, mobility and higher level of connectivity. Thus, the data transmission services are also required in cases when users are traveling by a car. As the number of vehicles grows, problems related to road safety and traffic flow management should also be addressed. These challenges highlight the need for modern, technically and economically justified communication solutions for Intelligent Transport Systems (*ITS*). One of the wireless network technologies that may be used for *ITS* needs, in particular for providing vehicle passengers with access to the data transmission network, is WLAN IEEE 802.11n/ac. The implementation of such WLAN based automotive wireless access networks is related to a number of issues, which mainly are related with fast moving objects. In practice a usable is a two-rank wireless network which can provide access to the Internet.

For the purpose of the Doctoral Thesis were created and studied several testbeds for the two-rank road transport network using WLAN IEEE 802.11n and LTE technologies. An experimental assessment of the change in data traffic characteristics across the two-rank network using LTE hardware from different manufacturers was made. The performance of such a hybrid communication channels was studied, depending on the velocity of mobile clients, the number of clients and used movement scenarios. The novel relationships characterizing the performance of integrated IEEE 802.11n and LTE road transport communication networks were obtained, what describe the dependence of network throughput from movement speed of the mobile client. In the thesis a single-rank IEEE 802.11ac road transport testbed was created and studied as well. Within the research was developed and realized an improved IEEE 802.11v protocol-based algorithm of handover procedure. For such a single-rank automotive communication network, performance relationships were evaluated theoretically.

Thesis contains

141 pages, 14 tables, 52 figures, 182 literature sources and 9 supplements.

SATURS

SAĪSINĀJUMU SARAKSTS	7
1. AUTOTRANSPORTA TELEKOMUNIKĀCIJU TĪKLI UN PROBLEMĀTIKA	14
1.1. Intelektuālās transporta sistēmas	16
1.2. Līdzīgu pētījumu pārskats	28
1.3. Promocijas darbā paveiktā apkopojums	31
2. INTEGRĒTU WLAN UN LTE AUTOTRANSPORTA SAKARU TĪKLU VEIKTSPĒJAS NOVĒRTĒJUMS	37
2.1. WLAN tehnoloģijas apskats	37
2.2. LTE tehnoloģijas apskats	59
2.3. WLAN un LTE tehnoloģiju apvienošana	61
2.4. Veiktspējas pētīšana, izmantojot dažādu LTE aparatūru	62
2.5. Veiktspējas pētīšana atkarībā no mobilo klientu skaita un izmantotajiem kustības scenārijiem	67
2.6. Hersta parametra noteikšana un tā analīze divrangu sakaru tīklam ar vairākiem klientiem ..	71
2.7. Veiktspējas pētīšana atkarībā no klientu skaita stacionārā režīmā	73
2.8. WLAN un LTE bāzēta automobiļu sakaru tīkla tehniski ekonomiskais novērtējums	77
2.9. Kopsavilkums un secinājumi	84
3. LIKUMSAKARĪBAS NOTEIKŠANA STARP INTEGRĒTA WLAN UN LTE SAKARU KANĀLA CAURLAIDSPĒJU UN AUTOMOBILĀ KUSTĪBAS ĀTRUMU	88
3.1. Eksperimentālo mērījumu sistēmas arhitektūra un metodoloģija	88
3.2. Nosacījumi un citi saistītie mērījumi	90
3.3. Sakaru kanāla veiktspējas mērījumu rezultāti un to novērtējums	92
3.4. Kopsavilkums un secinājumi	97
4. WLAN PĀRSLĒGŠANĀS PROCEDŪRAS UZLABOŠANAS REALIZĀCIJA UN NOVĒRTĒJUMS	99
4.1. IEEE 802.11k/r/v standartu apskats	100
4.2. Pārslēgšanās procedūras uzlabošana	104
4.3. Eksperimentālā iestatīšana	107
4.4. Veiktspējas parametru eksperimentāls novērtējums	110
4.5. Kopsavilkums un secinājumi	114
5. UZTVERTĀ WLAN SIGNĀLA JAUDAS LĪMEŅA UN CAURLAIDSPĒJAS NOVĒRTĒJUMS ATKARĪBĀ NO ATTĀLUMA LĪDZ RAIDĪTĀJAM	118
5.1. Signāla jaudas līmeņa atkarība no attāluma līdz raidītājam	118
5.2. Caurlaidspējas atkarība no uztvertā signāla jaudas līmeņa un attāluma līdz raidītājam	121
5.3. Kopsavilkums un secinājumi	123
NOBEIGUMS	125
IZMANTOTĀS LITERATŪRAS SARAKSTS	130
PIELIKUMU SARAKSTS	142

SAĪSINĀJUMU SARAKSTS

3D (*Three-dimensional*) – trīsdimensiju

3GPP (*Third Generation Partnership Project*) – trešās paaudzes sadarbības projekts

4G (*Fourth Generation*) – ceturtās paaudzes mobilie sakari

5G (*Fifth Generation*) – piektās paaudzes mobilie sakari

5G NR (*5G New Radio*) – 5G tehnoloģija NR

A

AAA (*Authentication, Authorization and Accounting*) – autentifikācija, autorizācija un uzskaitē

ACK (*Acknowledgement*) – apliecinājums

Ad-hoc (*Ad-hoc Network*) – dators-dators tīkls

AES (*Advanced Encryption Standard*) – uzlabots šifrēšanas standarts

AI (*Artificial Intelligence*) – mākslīgais intelekts

AID (*Association Identifier*) – asociācijas identifikators

AL caurlaidspēja – aplikācijas līmeņa (slāņa) caurlaidspēja

ANonce (*Authenticator Nonce*) – autentificētāja vienreizējais kods

AP (*Access Point*) – bezvadu piekļuves punkts

AQM (*Active Queue Management*) – aktīvā rindas vadība

ARIMA (*Autoregressive Integrated Moving Average*) – ARIMA statistiskās prognozēšanas modelis

ARP (*Address Resolution Protocol*) – adresu atrises protokols

B

BS (*Base Station*) – bāzes stacija

BSA (*Basic Service Area*) – pamatpakalpojumu zona

BSc (*Base Scenario*) – prognožu pamatscenārijs

BSS (*Basic Service Set*) – pamatpakalpojumu kopa

BSSID (*BSS identifier*) – BSS identifikators

BTM (*BSS Transition Management*) – BSS pārejas vadība

C

C-V2X (*Cellular-V2X*) – mobilā šūnu tīkla V2X sakari

CAN (*Controller Area Network*) – kontrolera tīkls

Cat (*Category*) – LTE UE kategorija

CAV (*Connected and Automated Vehicle*) – savienots un automatizēts transportlīdzeklis

CBC-MAC (*Cipher Block Chaining-Message Authentication Code*) – šifra blokkēdes ziņojuma autentifikācijas kods

CCKM (*Cisco Centralized Key Management*) – Cisco centralizētā atslēgu pārvaldība

CCMP (*Counter/CBC-MAC Protocol*) – skaitītāja/CBC-MAC protokols

CPU (*Central Processing Unit*) – centrālais procesors

CQI (*Channel Quality Indicator*) – frekvenču kanāla kvalitātes indikators

CRC (Cyclic-Redundancy Check) – cikliskā redundances pārbaude

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) – nesēja jušanas un sadursmju nepieļaušanas daudzpiekļuve

D

DC-HSPA (Dual Carrier High Speed Packet Access) – tehnoloģija *DC-HSPA*

DDR SDRAM (Double Data Rate Synchronous Dynamic Random Access Memory) – dubulta datu pārraides ātruma sinhronā brīvpiekļuves atmiņa

DHCP (Dynamic Host Configuration Protocol) – dinamiskā resursdatora konfigurācijas protokols

DL (Downlink) – lejuplīnija

DRAM (Dynamic Random Access Memory) – dinamiskā brīvpiekļuves atmiņa

DS (Distribution System) – sadales sistēma vai tīkls

DSRC (Dedicated Short Range Communications) – specializēti maza darbības attāluma sakari

E

E-UTRA (Evolved Universal Terrestrial Radio Access) – uzlabotā universālā zemes radiopiekļuve

EAP (Extensible Authentication Protocol) – paplašināmais autentifikācijas protokols

EAP-MSCHAPv2 (EAP-Microsoft Challenge Authentication Protocol version 2) – *EAP* Microsoft izaicinājuma autentifikācijas otrā protokola versija

EAP-TLS (EAP-Transport Layer Security) – *EAP* transporta slāņa drošība

EAPOL (EAP over LAN) – paplašināmais autentifikācijas protokols, izmantojot lokālo datortīklu

ECU (Electronic Control Unit) – elektroniska vadības ierīce

EDGE (Enhanced Data Rates for GSM Evolution) – *EDGE* tehnoloģija

EHT (Extremely High Throughput) – īpaši lielas caurlaidspējas standarts

EIRP (Equivalent Isotropically Radiated Power) – ekvivalentā izotropiski izstarotā jauda

eMBB (Enhanced Mobile Broadband) – uzlabotā mobilā platjosla

ES – Eiropas Savienība

ESS (Extended Service Set) – paplašināts pakalpojumu komplekts

ETC (Electronic Toll Collection) – elektroniskā braukšanas maksas iekasēšanas sistēma

ETSI (European Telecommunications Standards Institute) – Eiropas Telekomunikāciju standartu institūts

F

FCC (Federal Communications Commission) – Federālā sakaru komisija

FCS (Frame Check Sequence) – kadra pārbaudes secība

FDD (Frequency Division Duplex) – frekvenčdales duplexs

FSR (Fast Secure Roaming) – ātrā, drošā pārslēgšanās procedūra

FT (Fast BSS Transition) – ātrā BSS pāreja

FTAA (FT Authentication Algorithm) – *FT* autentifikācijas algoritms

FTP (File Transfer Protocol) – failu pārsūtīšanas protokols

G

GB (Gigabyte) – gigabaiti

GMK (Group Master Key) – grupas galvenā atslēga

GPS (Global Positioning System) – globālā pozicionēšanas sistēma

GTK (Group Temporal Key) – grupas pagaidu atslēga

H

HD (High Definition) – augstas izšķirtspējas

HetNet (Heterogeneous Network) – heterogēnais tīkls

HP (Hewlett-Packard) – kompānija HP

HSPA (High Speed Packet Access) – HSPA tehnoloģija

HT (High Throughput) – liela caurlaidspēja

HTC (High Throughput Control) – lielas caurlaidspējas kontrole

HTTP (Hypertext Transfer Protocol) – hiperteksta transporta protokols

I

ID (Identifier) – identifikators

IEEE (Institute of Electrical and Electronics Engineers) – Elektrotehnikas un elektronikas inženieru institūts

IETF (Internet Engineering Task Force) – interneta tehniskā uzdevumgrupa

IMT-2020 (International Mobile Telecommunications-2020) – starptautiskie mobilie telesakari 2020 (ITU termins, kas apzīmē 5G)

IoT (Internet of Things) – lietu internets

IP (Internet Protocol) – interneta protokols

IPsec VPN (Internet Protocol security VPN) – IPsec protokola VPN

ITS (Intelligent Transport Systems) – intelektuālās transporta sistēmas; intelektiskas transporta sistēmas

ITU (International Telecommunication Union) – Starptautiskā telekomunikāciju savienība

IVC (Inter Vehicle Communication) – transportlīdzekļu savstarpējā komunikācija

L

L1 (Layer 1; Physical Layer) – fizikālais (fiziskais) slānis

L2 (Layer 2; Data link Layer) – datu pārraides kanāla slānis

L3 (Layer 3; Network Layer) – tīkla slānis

L4 (Layer 4; Transport Layer) – transporta slānis

L7 (Layer 7; Application Layer) – lietojuma (aplikācijas) slānis

LAA (Licensed Assisted Access) – licencētā asistētā radiopiekļuve

LAN (Local Area Network) – lokālais datortīkls

LBT (Listen Before Talk) – “klausies, pirms runā” mehānisms

LDAP (Lightweight Directory Access Protocol) – LDAP protokols

LTE (Long Term Evolution) – starptautisko mobilo telesakaru sistēma *LTE*
LTE-A (LTE-Advanced) – *LTE* sistēmas uzlabotā versija
LTE-A Pro (LTE-Advanced Pro) – *LTE* sistēmas uzlabotās versijas paplašinājums
LTE-U (Long Term Evolution-Unlicensed) – starptautisko mobilo telekomunikāciju sistēma
LTE koplietojamām (nelicencētām) frekvenču joslām
LWA (LTE-Wi-Fi Link Aggregation) – *LTE* un *Wi-Fi* savienojumu apvienošana

M

MAC (Medium Access Control) – vides piekļuves vadības protokols
MB (Megabyte) – megabaits
MCS (Modulation and Coding Scheme) – modulācijas un kodēšanas shēma
MIC (Message Integrity Check) – ziņojuma integritātes pārbaude
MIMO (Multiple Input Multiple Output) – vairākkārtēja ievade, vairākkārtēja izvade
MIP (Mobile IP) – mobila *IP* protokols
mMTC (Massive Machine Type Communication) – masīvie mašīnu tipa radiosakari
MPDU (MAC Protocol Data Unit) – *MAC* protokola datu bloks
MPTCP (Multipath TCP) – vairākkeļu *TCP* protokols
MRC (Maximal-Ratio Combining) – maksimālās attiecības kombinēšana
MSE (Mean Squared Error) – vidējā kvadrātiskā kļūda
MSK (Master Session Key) – galvenā sesijas atslēga
MSS (Maximum Segment Size) – maksimālais segmenta izmērs
MSSHD (Mobility and Signal Strength-Aware Hand-off Decision) – *MSSHD* metode
MU-MIMO (Multi-user Multiple Input Multiple Output) – vairāku lietotāju vairākkārtēja ievade, vairākkārtēja izvade

N

NAT (Network Address Translation) – tīkla adresu translēšana
NR (New Radio) – 5G tehnoloģija *NR*

O

OBU (On-Board Unit) – transportlīdzekļa aparatūra (bortaparātūra)
OFDM (Orthogonal Frequency Division Multiplexing) – ortogonālā frekvenčdales blīvēšana
OFDMA (Orthogonal Frequency Division Multiple Access) – ortogonālā frekvenčdales daudzpiekļuve
OKC (Opportunistic Key Caching) – oportūnistiskā atslēgu uzkrāšana
OS (Operating System) – operētājsistēma
OSA (Open System Authentication) – atvērtās sistēmas autentifikācija
OSI (Open System Interconnection) – atvērto sistēmu sadarbība

P

PHY (Physical layer) – fizikālais slānis
PMK (Pairwise Master Key) – pāra galvenā atslēga

PMK-R0 (Pairwise Master Key-R0) – FT atslēgu hierarhijas pirmā līmeņa galvenā atslēga
PMK-R1 (Pairwise Master Key-R1) – FT atslēgu hierarhijas otrā līmeņa galvenā atslēga
PoE (Power over Ethernet) – ierīču elektrobarošana, izmantojot *Ethernet* kabeli
PQM (Passive Queue Management) – pasīvā rindu vadība
PRF (Pseudo-Random Function) – pseido gadījuma funkcija
PS-Poll (Power Save Poll) – enerģijas taupīšanas aptauja
PSK (Pre-Shared Key) – pirmskoplietošanas atslēga
PTK (Pairwise Transient Key) – pāra pārejas atslēga
Public APN (Public Access Point Name) – publiskais interneta piekļuves punkts mobilajos tīklos

Q

QAM (Quadrature Amplitude Modulation) – kvadrātūrā amplitūdas modulācija
QoS (Quality of Service) – pakalpojuma kvalitāte
QPSK (Quadrature Phase-Shift Keying) – kvadratūras fāzes manipulācija

R

RADIUS (Remote Authentication Dial-In User Service) – attālinātās autentifikācijas iezvanes lietotāja pakalpojums
RAM (Random Access Memory) – operatīvā atmiņa
RED (Random Early Detection) – RED algoritms
RF (Radio Frequency) – radiofrekvence
RRM (Radio Resource Management) – radio resursu vadība
RSRP (Reference Signal Received Power) – references signāla uztvertā jauda
RSRQ (Reference Signal Received Quality) – references signāla uztvertā signāla kvalitāte
RSS (Received Signal Strength) – uztvertā signāla stiprums
RSSI (Received Signal Strength Indicator) – uztvertā signāla stipruma indikators
RSU (Roadside Unit) – ceļmalas aparātūra
RTO (Retransmission Timeout) – atkārtotas pārsūtīšanas noildze
RTS/CTS (Request to Send/Clear to Send) – pieprasījums, lai sūtītu / atbrīvots, lai sūtītu
RTT (Round Trip Time) – aprites laiks (pakešu ceļošanas laiks turp un atpakaļ)

S

Sc (Scenario) – prognožu scenārijs
SCTP (Stream Control Transmission Protocol) – plūsmas vadības pārraides protokols
SDN (Software-Defined Networking) – programmatūras definēta tīklošana
SINR (Signal to Interference Noise Ratio) – signāla un traucējumi plus troksnis attiecība
SLA (Service Level Agreement) – pakalpojumu līmeņa vienošanās
SMTP (Simple Mail Transfer Protocol) – vienkāršais pasta pārsūtīšanas protokols
SNMP (Simple Network Management Protocol) – vienkāršais tīkla pārvaldības protokols
SNonce (Supplicant Nonce) – pieprasītāja vienreizējais kods
SNR (Signal to Noise Ratio) – signāla un trokšņa attiecība

SSH (Secure Shell) – SSH attālinātās piekļuves protokols
SSID (Service Set Identifier) – pakalpojumu kopas identifikators
SSR (Sum of Squared Residuals) – noviržu kvadrātu summa
STA (Station) – 802.11 darbstacija
SW (IP Switch) – IP komutators

T

TCP (Transmission Control Protocol) – pārraides vadības protokols
TDD (Time Division Duplex) – laikdales duplexs
TFTP (Trivial File Transfer Protocol) – triviālais failu pārsūtīšanas protokols
TH (Threshold) – sliekšņvērtība (robežvērtība)
TL caurlaidspēja – transporta līmeņa (slāņa) caurlaidspēja
TLS (Transport Layer Security) – transporta slāņa drošība
TM (Transition Management) – pārejas vadība
Tx (Transmitter) – raidītājs
TxBF (Transmit Beamforming) – pārraides staru formēšana

U

U-NII-1 (Unlicensed National Information Infrastructure, Band 1) – nelicenzētā nacionālā informācijas infrastruktūra, pirmā frekvenču josla
UDP (User Datagram Protocol) – lietotāja datogrammu protokols
UE (User Equipment) – galiekārta
UL (Uplink) – augšuplīnija
UMTS (Universal Mobile Telecommunications System) – universālā mobilo telesakaru sistēma
UPS (Uninterruptible Power Supply) – nepārtrauktā elektrobarošana
URL (Uniform Resource Locator) – vienotais resursu vietrādis
URLLC (Ultra-Reliable and Low-Latency Communications) – ultradroši un zemas laikaiztures radiosakari
UTP (Unshielded Twisted Pair) – neekranēts vītais pāris

V

V2I (Vehicle-to-Infrastructure) – sakari “transportlīdzeklis-infrastruktūra”
V2N (Vehicle-to-Network) – sakari “transportlīdzeklis-tīkls”
V2P (Vehicle-to-Pedestrian) – sakari “transportlīdzeklis-kājāmgājējs”
V2V (Vehicle-to-Vehicle) – sakari “transportlīdzeklis-transportlīdzeklis”
V2X (Vehicle-to-Everything) – sakari “transportlīdzeklis-viss”
VANET (Vehicular Ad-hoc Network) – transportlīdzekļu *Ad-hoc* tīkls
VCN (Vehicular Communication Network) – transportlīdzekļu sakaru tīkls
VHT (Very High Throughput) – ļoti liela caurlaidspēja
VLAN (Virtual Local Area Network) – virtuālais lokālais tīkls
VoIP (Voice over IP) – IP telefonija
VoWi-Fi (Voice over Wi-Fi) – IP telefonija *Wi-Fi* tīklā

VoWLAN (Voice over Wireless Local Area Network) – IP telefonija *Wi-Fi* tīklā

VPN (Virtual Private Network) – virtuālais privātais tīkls

W

WAN (Wide Area Network) – teritoriālais tīkls

WAVE (Wireless Access in Vehicular Environment) – bezvadu piekļuve transportlīdzekļu vidē

Wi-Fi (Wireless Fidelity) – bezvadu lokālais tīkls

WLAN (Wireless Local Area Network) – bezvadu lokālais tīkls

WLC (Wireless LAN Controller) – bezvadu tīkla kontrolieris

WNIC (Wireless Network Interface Card) – bezvadu tīkla adapteris

WNM (Wireless Network Management) – bezvadu tīkla vadība

WPA (Wi-Fi Protected Access) – *Wi-Fi* aizsargāta pieeja

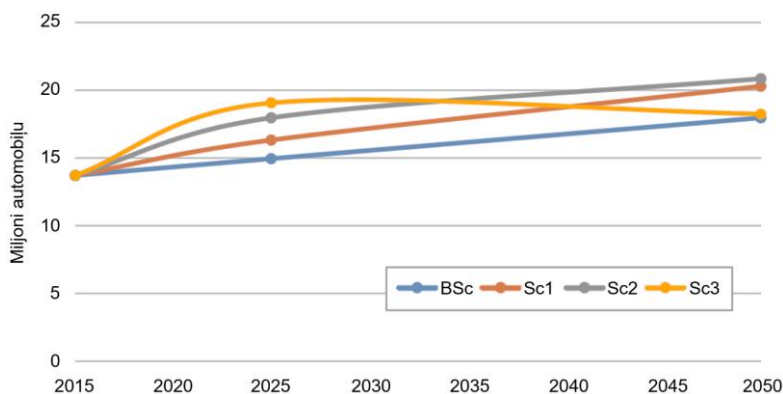
WRED (Weighted Random Early Detection) – svērtais *RED* algoritms

1. AUTOTRANSPORTA TELEKOMUNIKĀCIJU TĪKLI UN PROBLEMĀTIKA

Pieaugošais datu pārraides apjoms bezvadu sakaru tīklos un pieprasījums pēc visuresošas savienojamības un mobilitātes mūsdienu bezvadu sakaru tīkliem izvirza aizvien lielākas prasības. Informācijas sabiedrība pieprasa augsta līmeņa savienojamības risinājumus ne tikai fiksētā vidē, bet arī atrodoties ceļā, transportlīdzekļos. Viena no nozarēm, kas aktīvi piedalās prasību izstrādē nākotnes bezvadu šūnu tīkliem un tādējādi veicina jaunu tehnoloģiju un risinājumu attīstīšanu, ir autotransporta industrija. Industrijas definētās tehniskās prasības 5G tehnoloģijas datu pārraides ātrumam, pārklājumam, tīkla latentumam un tehnoloģiju līdzpastāvēšanai spēs nodrošināt tādas nākotnes pakalpojumus kā savienotais transports un autonomie automobiļi, kā arī masīvie mašīntipa *IoT* (angļu val. *Internet of Things*) sakari, mākoņbalstīta robotu vadība un industriālo risinājumu automatizācija [126]. Transporta sakaru tīkli ir viena no vadošajām pētniecības jomām, ņemot vērā tās svarīgo lomu mūsu ikdienā, tās lietojumu, augstās un specifiskās prasības [113].

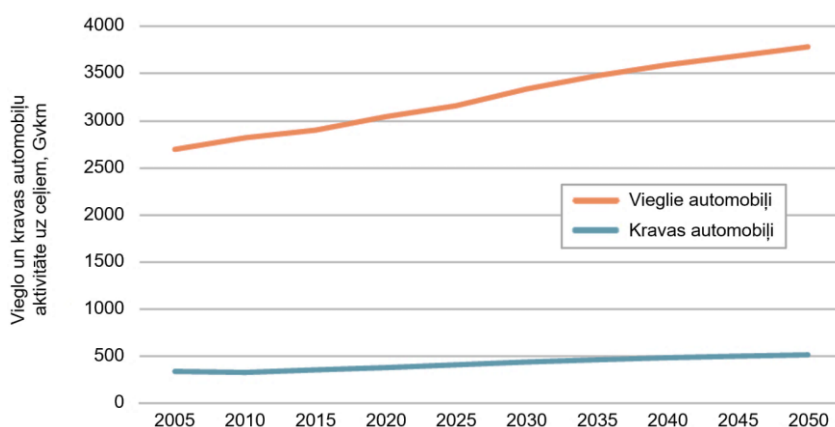
Autoražotāji strādā pie jauniem risinājumiem, pakāpeniski palielinot automobiļu automatizācijas jeb autonomijas līmeņus, sākot no automobiļa vadītāja asistenta, daļējas automatizācijas un beidzot ar ļoti augstas automatizācijas līmeni [45]. Paredzams, ka 5G tīkliem datu pārraides nodrošināšanā autonomiem automobiļiem būs noteicošā loma [175].

Automobiļu skaita pieaugums, līdz ar to arī autotransporta ceļu noslodzes palielināšanās, rada virkni problēmu, piemēram, pieaug ceļu satiksmes incidentu skaits, palielinās sastrēgumi un pieaug piesārņojuma līmenis. 1.1. attēlā redzami prognozētie pasažieru jeb vieglo automobiļu pārdošanas apjomi Eiropas Savienībā (ES) pie dažādiem scenārijiem. Pamatscenārijā jeb bāzes scenārijā (angļu val. *Base Scenario – BSc*) netiek ņemta vērā savienoto un automatizēto automobiļu (angļu val. *Connected and Automated Vehicle – CAV*) tehnoloģiju ietekme. Bāzes scenārijā tika izmantota *Eurostat* datubāzes (angļu val. *Eurostat Database*) un *ES atsaucis scenārija 2016* (angļu val. *EU Reference Scenario 2016*) informācija. *Sc1*, *Sc2* un *Sc3* scenārijos tiek ņemta vērā CAV tehnoloģiju ietekme. *Sc1*, *Sc2* un *Sc3* scenāriju līkņu raksturs mainās atkarībā no prognozētās tehnoloģiju attīstības, likumdošanas regulējuma un lietotāju gatavības (tehnoloģiju adoptācijas) līmeņa. *Sc1* scenārijs paredz zemu minēto jomu attīstības līmeni, savukārt *Sc2* paredz vidēju un *Sc3* – augstu katras jomas attīstības līmeni [140]. Atkarībā no izmantotā scenārija (*BSc*, *Sc1*, *Sc2*, *Sc3*) tiek prognozēts pasažieru automobiļu pārdošanas apjoma pieaugums: 2015.–2025. gadā no 18 % līdz 39 %; 2015.–2050. gadā no 33 % līdz 51 %. *Sc3* scenārijā ilgtermiņā prognozētais pasažieru automobiļu pārdošanas apjoma samazinājums ir saistīts ar prognozēto automobiļu koplietošanas pakalpojumu dominēšanu nākotnē [140], kas varētu veicināt pieprasījuma samazināšanos pēc privātajiem automobiļiem (1.1. att.). Savukārt kravas automobiļiem ilgtermiņā tiek prognozēta pieaugoša pārdošanas apjoma tendence visos scenārijos.



1.1. att. Prognozētie vieglo automobiļu pārdošanas apjomi ES dažādos scenārijos [140].

Saskaņā ar Eiropas Komisijas datiem ES pasažieru automobiļu aktivitāte uz ceļiem pieaugs par 9 % un 30 % attiecīgi 2015.–2025. gadā un 2015.–2050. gadā. Savukārt kravas automobiļu aktivitāte minētajā laikā uz ceļiem pieaugs par 16 % un 46 % [140] (1.2. att.). Prognozētās aktivitātes pieaugums uz autoceļiem ir saistīts ar savienoto un autonomo automobiļu pozitīvo ietekmi, automobiļu skaita pieaugumu, kā arī prognozēto ekonomiskās aktivitātes un izaugsmes pieaugumu. Tas nozīmē, ka iedzīvotāji kopumā vairāk laika pavadīs, pārvietojoties ar automobiļiem.

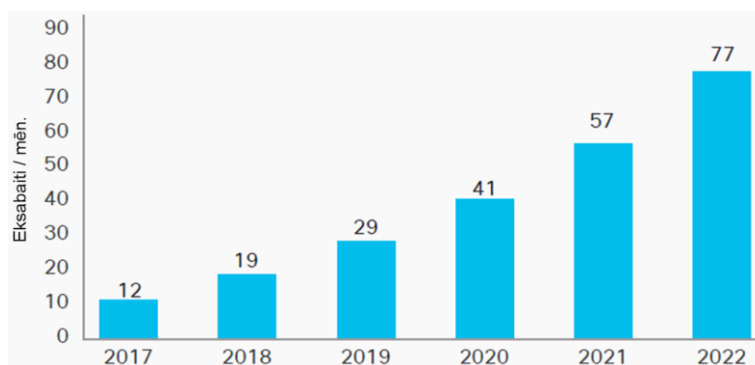


1.2. att. Vieglo un kravas automobiļu aktivitāte uz autoceļiem ES [140].

Ar automobiļu skaita pieaugumu saistītās problēmas, kas tika minētas iepriekš, efektīvi var risināt, izmantojot intelektuālās transporta sistēmas (angļu val. *Intelligent Transport Systems – ITS*), kas tiek sauktas arī par intelektiskām transporta sistēmām [95] vai automatizētām transporta sistēmām. *ITS* aptver gan privātos transportlīdzekļus, gan komerctransportu, jo kopējo satiksmes drošības līmeņa paaugstināšanu var nodrošināt, iesaistot visus ceļu satiksmes dalībniekus, arī gājējus. Papildus *ITS* risina arī problēmas, kas ir saistītas gan ar pašu transportlīdzekļu, gan ar transportlīdzekļu pasažieru piekļuvi interneta tīklam, atrodoties kustībā. Katrs automobiļa pasažieris tiek uzskatīts par mobilo klientu, kuram ir jānodrošina piekļuve datu pārraides pakalpojumiem.

Cisco globālā prognoze rāda, ka viedo ierīču ar mobilā tīkla savienojumu īpatsvars attiecībā pret vienkāršajām (angļu val. *non-smart*) ierīcēm ar mobilā tīkla savienojumu 2022. gadā pieaugs līdz 73 %, salīdzinot ar 53 % 2017. gadā [33]. *Cisco* prognozē arī to, ka globālais

mobilo datu trafīks no 2017. līdz 2022. gadam pieaugs gandrīz septiņas reizes, sasniedzot 77 eksabaitus mēnesī (1.3. att.) [33], [142].



1.3. att. Globālā mobilo datu trafīka pieaugums līdz 2022. gadam [33].

Minētās prognozes liecina par strauju pieprasījuma pieaugumu pēc datu tīkla pakalpojumiem. Izanalizējot iepriekš apskatītās tendences, var secināt, ka transportlīdzekļu pasažieri aktīvi izmantos datu pārraides pakalpojumus, arī atrodoties ceļā. Apskatītās tendences pamato nepieciešamību pēc mūsdienīgiem ITS sakaru risinājumiem.

1.1. Intelektuālās transporta sistēmas

Mobilitāte ir īpaši svarīga sabiedrības dzīves kvalitātei. Savukārt autotransporta radītās gāzes emisijas apdraud mūsu veselību un nelabvēlīgi ietekmē apkārtējo vidi, kā arī būtiski sekmē klimata pārmaiņas. Lai globāli un vietējā mērogā risinātu autotransporta plūsmas pieauguma radītās sekas, autotransporta nozarē nepieciešams ieviest augstās tehnoloģijas, gan domājot par alternatīviem transporta enerģijas avotiem, gan paaugstinot transporta plūsmu efektivitāti.

Intelektuālo transporta sistēmu (ITS) galvenais mērķis ir izstrādāt tādu autotransporta tīklošanas risinājumu, kas spētu samazināt ceļu satiksmes negadījumu skaitu un autotransporta sastrēgumus, līdz ar to uzlabojot kopējo situāciju arī piesārņojumu samazināšanas jomā. Ņemot vērā dažādu valstu nacionālās intereses un vēsturiskās iestrādes, šobrīd pasaulē tiek attīstīti vairāki ITS projekti.

Intelektuālās transporta sistēmas var iedalīt ceļu ITS un pilsētas dzelzceļa ITS. Ceļu ITS ietver jebkādas sauszemes transporta sistēmas, piemēram, automobiļi, kravas automašīnas, velosipēdi, motocikli, tramvaji, gājēji, celtniecības tehnika, lauksaimniecības tehnika u. c. Savukārt pilsētas dzelzceļa ITS ietver pilsētas vai piepilsētas dzelzceļa līnijas, kas nodalītas no ceļu un gājēju satiksmes. Promocijas darbā tiek pētīta ceļu, konkrēti – automobiļu, ITS.

Transporta mobilie objekti ir jānodrošina ar ātrgaitas datu pieslēgumiem gan transporta vajadzībām, gan pašu pasažieru vajadzībām – piekļuvei interneta tīklam. Lai to paveiktu, ir nepieciešami transporta piekļuves tīkli jeb attiecīga infrastruktūra. Pastāv vairāki risinājumi [96], kā var nodrošināt šādus datu pārraides pieslēgumu pakalpojumus, kas detalizēti tiks apskatīti šī darba attiecīgajā apakšnodaļā.

Izstrādājot intelektuālās transporta sistēmas, sākotnēji tika paredzēts, ka ar ITS palīdzību tiks nodrošināti komunikācijas kanāli galvenokārt tikai starp transportlīdzekļiem (automobiļiem) un ceļu infrastruktūru: sakari “transportlīdzeklis-transportlīdzeklis” (angļu val. *Vehicle-to-Vehicle – V2V*) un sakari “transportlīdzeklis-infrastruktūra” (angļu val. *Vehicle-to-Infrastructure – V2I*) [53], [61], [96]. Attīstoties jaunām tīklošanas tehnoloģijām, ITS tika paplašināta ar jauniem komunikācijas kanāliem starp ceļu satiksmes dalībniekiem, iekļaujot arī gājējus un tīklu: sakari “transportlīdzeklis-kājām-gājējs” (angļu val. *Vehicle-to-Pedestrian – V2P*), sakari “transportlīdzeklis-tīkls” (angļu val. *Vehicle-to-Network – V2N*) [125], [138], [147], [174], [175]. Tika ieviests arī jauns kopējs apzīmējums – sakari “transportlīdzeklis-viss” (angļu val. *Vehicle-to-Everything – V2X*), kas kalpos vēl nedefinētu nākotnes transportlīdzekļu komunikācijas kanālu apzīmēšanai [94], [164].

Autonomie automobiļi

Tiek aktīvi testēti autonomie automobiļi (angļu val. *autonomous vehicles* jeb *self-piloted cars*), un testa režīmā tie jau izbrauc ielās. Autonomie automobiļi tiek aprīkoti ar sensoriem, iebūvētām kamerām, iebūvētām datorsistēmām, augstas precizitātes GPS (angļu val. *Global Positioning System*), īsas distances radariem, dažādām datu kanālu izveidošanas tehnoloģijām un veic visus vai daļu no automobiļa vadīšanas uzdevumiem. Transportlīdzekļi ar asistēto atbalstu (1. un 2. automatizācijas līmenis) jau šobrīd ir pieejami Eiropas tirgū. Pašbraucošie automobiļi (3. un 4. automatizācijas līmenis) šobrīd tiek testēti, un plānots, ka tie būs pieejami līdz 2030. gadam, savukārt pilnīgi autonomi automobiļi (5. automatizācijas līmenis) varētu būt pieejami pēc 2030. gada [173]. Pētījumā [45] tiek apgalvots, ka automobiļu automatizācija nākotnē varētu samazināt ceļu satiksmes negadījumu skaitu vidēji par 90 %, salīdzinot ar statistikas rādītājiem, kas ir šobrīd. Galvenie faktori, kas ietekmē autonomo automobiļu ieviešanas progresu, ir mākslīgais intelekts (angļu val. *Artificial Intelligence – AI*), ar kura palīdzību notiks apkārtējās vides reāllaika atpazīšana un iegūtās informācijas konvertēšana aktuālos lēmumos, tiks risināti ētikas jautājumi par atbildību negadījumos, sabiedrības uzticēšanos, likumdošanu [175], uzkrāto personālo datu aizsardzību (kiberdrošība), piemēram, autovadītāja atrašanās vieta, izmantotie maršruti, kā arī atbilstoša autotransporta sakaru tīkla esamība un sakaru kanālu aizsardzība [45].

ITS lietojumu iedalījums

ITS lietojumi aptver ceļu satiksmes dalībnieku (transportlīdzekļu un to pasažieru, kā arī gājēju u. c. satiksmes dalībnieku), transporta ceļu infrastruktūras, ceļu satiksmes vadības un attālināto datu pakalpojumu sistēmu savstarpējās komunikācijas risinājumus [71], [147]. Ir definētas trīs galvenās pakalpojumu grupas, kur var izmantot ITS:

Ceļu satiksmes drošība un brīdināšana (angļu val. *safety applications*) ietver tādas pakalpojumus un brīdināšanu par ārkārtas situācijām kā transportlīdzekļu bīstama pietuvošanās, sadursmes risks, avarējuši transportlīdzekļi, gājēji vai dzīvnieki, kas šķērso ceļu, citu šķēršļu esamība uz ceļiem, nelabvēlīgi laika apstākļi, bīstamās zonas vai ceļa stāvoklis, glābšanas

dienestu izsaukšana, avārijas bremzēšana, nepārtrauktās sadalošās joslas šķērsošana, ceļa zīmju nolasīšana, reaģēšana uz luksofora signāliem (V2V, V2I, V2P) [113].

Transporta plūsmu vadība un transporta sistēmu pakalpojumi (angļu val. *non-safety applications*) ietver ar ceļu drošību nesaistītus pakalpojumus, tādus kā nodevu iekasēšana, operatīva transportlīdzekļa datu pārbaude (apdrošināšanas un tehniskās apskates derīguma termiņš), attālinātā transportlīdzekļu diagnostika (ikdienas tehniskās pārbaudes), autostāvvietas atrašana un rezervēšana, kravu pārvadājumi un loģistika, transportlīdzekļu programmatūras atjaunināšana, navigācijas karšu lejupielāde (piemēram, 3D HD kartes), ceļa topogrāfisko datu lejupielāde, informācija par degvielas uzpildes stacijām un autoservisiem, autoevakuācija, apziņošana, objektu atpazīšana un klasifikācija (vieglie/kravas transportlīdzekļi), kooperatīvā adaptīvā kruīza kontrole sastrēgumu mazināšanai [125], transportlīdzekļu sensoru (*IoT*) mērījumu datu (telemetrijas datu) nosūtīšana viedās pilsētas ceļu un transporta plūsmas efektīvai organizēšanai, kontrolei, plānošanai un statistikas datu iegūšanai (V2I, V2N) [19].

Informācija un izklaide (angļu val. *infotainment applications*). Pasažieri var saņemt komerciālu informāciju par tuvumā esošiem pakalpojumiem (muzeji, ievērojamas vietas, iepirkšanās centri, ekskursijas), izmantot tādus pakalpojumus kā liela datu apjoma apmaiņa un koplietošana, tiešsaistes video atskaņošana, videokonferences zvans, konferences balss sakari, tūlītēja ziņojumapmaiņa, piekļuve mākoņbalstītiem pakalpojumiem, virtuālā vai papildinātā realitāte (ekskursiju ceļveži), piekļuve interneta tīklam (V2N) [113], [124], [126].

Prasības, kas izvirzītas *ITS* ar drošību saistītām funkcijām, nosaka, ka izmantotajai sakaru tehnoloģijai jānodrošina tīkla latentums robežās 10–100 ms [29], [71]. Izvirzītās prasības saistībā ar tīkla aizturi automatizētiem un autonomiem automobiļiem paredz vēl mazākas aiztures [29].

Informācijas un izklaides pakalpojumu kategorija attiecas tieši uz pasažieriem, t. i., pasažieru nodrošināšana ar piekļuvi interneta tīklam. Informācijas un izklaides pakalpojumus nepieciešams nodalīt no ceļu satiksmes drošības, brīdināšanas un transporta sistēmu pakalpojumu funkcijām, lai neietekmētu šo kritisko funkciju izpildi [124]. To var izdarīt, informācijas un izklaides pakalpojumiem izveidojot atsevišķu bezvadu sakaru kanālu, kas var tikt organizēts, izmantojot arī atšķirīgu sakaru tehnoloģiju.

Autotransporta sakaru tīklu tehnoloģijas

Pastāv vairāki tehnoloģiski risinājumi, kā var nodrošināt datu pārraides pieslēgumu pakalpojumus automobiļiem [103]. Tālāk darbā dots aktuālo un nākotnes sakaru tehnoloģiju un standartu apskats, kas jau tiek vai arī varētu tikt izmantoti *ITS* vajadzību nodrošināšanai.

ITS-G5/WAVE

Pēdējos gados tika attīstītas vairākas specializētu, maza darbības attāluma sakaru (angļu val. *Dedicated Short Range Communications – DSRC*) tehnoloģijas, kas nodrošina datu apmaiņu starp automobiļiem (V2V), kā arī automobiļiem un infrastruktūru (V2I). Ar *DSRC* terminu tiek apzīmēta arī vecāka tehnoloģija, kas nodrošina automobiļu komunikāciju ar ceļa infrastruktūru (V2I) galvenokārt braukšanas maksas iekasēšanai (angļu val. *Electronic Toll Collection – ETC*)

[96]. Viena no specializētu, maza darbības attāluma sakaru tehnoloģijām ir WAVE (angļu val. *Wireless Access in Vehicular Environment*), ko Amerikas Savienotajās Valstīs attīsta FCC. Savukārt Eiropā ETSI attīsta intelektuālo transporta sistēmu tehnoloģiju ITS-G5 [138]. Minētās tehnoloģijas ir bāzētas transportlīdzekļu sakaru tīkla (angļu val. *Vehicular Ad-hoc Network – VANET*) IEEE 802.11p standartā [125]. ITS-G5 tehnoloģija, tāpat kā WAVE, paredzēta darbam 5,9 GHz frekvenču joslā [147]. IEEE 802.11p nodrošina datu pārraides ātrumu līdz 27 Mbit/s [23], [53]. Minētās ITS sistēmas sastāv no divu veidu iekārtām, kur viens no tiem ir transportlīdzekļa aparatūra (angļu val. *On-Board Unit – OBU*), kas ir izvietota transportlīdzeklī un kalpo par IEEE 802.11p staciju, otrs – ceļmalas aparatūra (angļu val. *Roadside Unit – RSU*), kas tiek izvietota gar ceļu vai šoseju un kalpo par IEEE 802.11p piekļuves punktu. Šāds tīkls var darboties gan infrastruktūras režīmā, gan Ad-hoc režīmā [80]. Galvenie IEEE 802.11p standartā bāzēto tehnoloģiju trūkumi ir salīdzinoši mazā caurlaidspēja un fakts, ka tīkla kopējā veiktspēja krītas, tiklīdz pieaug tīkla noslodze. Tīkla aizture jeb latentums pieaug, pieaugot lietotāju skaitam, līdz ar to maksimālo tīkla aizturi nav iespējams garantēt [138].

Latvijas teritorijā ITS vajadzībām lietošanā ir piešķirta frekvenču josla 5875–5925 MHz. Šīm sistēmām individuālās atļaujas raidītājiem nav nepieciešamas, t. i., tikai jāievēro ITS iekārtu tehnisko noteikumu izpilde, lai neradītu traucējumus citiem lietotājiem [92].

C-V2X

C-V2X (angļu val. *Cellular Vehicle-to-Everything*) ir jauna tehnoloģija, kas tika izstrādāta transportlīdzekļu ITS funkciju nodrošināšanai, izmantojot mobilos šūnu tīklus. Izstrādātā LTE C-V2X tehnoloģija, kas tiek apzīmēta arī kā LTE-V2X, ir paredzēta darbam LTE tīklā, savukārt izstrādē esošā 5G C-V2X tehnoloģija, kas tiek apzīmēta arī kā 5G-V2X vai 5G NR-V2X, ir paredzēta darbam 5G tīklā [31]. LTE bāzētā C-V2X tehnoloģija ir iekļauta 3GPP standartos Release 14 un Release 15, savukārt 5G NR-V2X ir iekļauts 3GPP standartos Release 16 un Release 17 [29].

C-V2X ir unificētas tehnoloģijas platforma, kas satur divu veidu komunikācijas metodes. Pirmā metode ir tiešas (angļu val. *direct*) vai lokālas (angļu val. *sidelink*) komunikācijas sakari starp ceļu satiksmes dalībniekiem, t. i., automobiļiem (arī motocikliem) un gājējiem (arī velosipēdistiem), kā arī starp automobiļiem un ceļmalas infrastruktūru. Tādējādi tiek izmantotas V2V, V2P un V2I komunikācijas shēmas, kas darbojas ITS frekvenču joslās (piemēram, ITS 5,9 GHz) [144] neatkarīgi no šūnu tīkla. Tie ir īsas distances (angļu val. *short-range*) sakari (<1 km), kur tiek izmantota C-V2X PC5 saskarne [90].

Otrā metode nodrošina liela attāluma (angļu val. *long-range*) mobilo šūnu tīkla komunikācijas kanālus starp ceļu satiksmes dalībniekiem un tīklu. Tādējādi tiek izmantota V2N komunikācijas shēma, kur papildus ITS izdalītajām frekvenču joslām paredzēts izmantot arī tradicionālās mobilā tīkla licencētās frekvenču joslas. Šajā gadījumā komunikācijas mērogs ir atkarīgs no mobilā šūnu tīkla pārklājuma un ir paredzēts sakaru nodrošināšanai virs 1 km, piemēram, lai ziņotu par satiksmes negadījumu izvēlētajā maršrutā. V2N sakariem tiek izmantota C-V2X Uu saskarne [90], [147].

C-V2X tehnoloģija liek pamatus 5G automobiļu savienojamībai [28], jo 5G-V2X tehnoloģija spēs nodrošināt atbalstu autonomās braukšanas pamatfunkcijām: V2V, V2P, V2N un V2I [175].

IEEE 802.11bd

Paredzēts, ka *IEEE 802.11bd* projekta standarts ar piešķirto nosaukumu “Uzlabojumi nākamās paaudzes V2X” (angļu val. *Enhancements for Next Generation V2X*) tiks izmantots transportlīdzekļu sakariem (V2X) un aizvietos esošo *IEEE 802.11p* standartu. Jaunais standarts izmantos 5,9 GHz un 60 GHz (57 GHz līdz 71 GHz) frekvenču joslas. Salīdzinot ar *IEEE 802.11p*, jaunajam standartam tiks uzlabota caurlaidspēja, nodrošināta palielināta uztvērēja jutība, lai palielinātu darbības attālumu (tas tiks dubultots, salīdzinot ar *802.11p*), atbalstāmais transportlīdzekļu braukšanas ātrums tiks palielināts līdz 500 km/h [13], [90].

IEEE 802.11n

IEEE 802.11n standarts izmanto 2,4 GHz vai 5 GHz frekvenču joslas, teorētiski spēj nodrošināt līdz 600 Mbit/s lielu datu pārraides ātrumu, lietojot lielas caurlaidspējas (angļu val. *High Throughput – HT*) tehnoloģiskus paņēmienus. Standarts izmanto vairākas radio komponentes (raidītāji, uztvērēji, antenas), formējot vairākas radio ķēdes, ko sauc par vairākkārtējas ievades, vairākkārtējas izvades (angļu val. *Multiple Input Multiple Output – MIMO*) sistēmu. *802.11n* standarts nosaka vismaz 2×2 (raidītājs $\times$ uztvērējs) līdz 4×4 radio ķēdes. Standarts ļauj izmantot 20 MHz un 40 MHz frekvenču joslu, kas ir iespējams, apvienojot divus blakus esošus frekvenču kanālus. *802.11n* standartā 20 MHz kanāla caurlaidspēja ir paaugstināta, palielinot apakšnesēju (angļu val. *subcarriers*) skaitu no 48 (*802.11a/g OFDM*) līdz 52, un 40 MHz kanāls izmanto 108 apakšnesējus. 5 GHz frekvenču joslā, izmantojot 20 MHz joslas platumu, ir 23 kanāli, kas nepārklājas (angļu val. *non-overlapping channels*). Savukārt 2,4 GHz frekvenču joslā, izmantojot 20 MHz joslas platumu, ir tikai trīs kanāli, kas nepārklājas. Apvienojot kanālus, pieejamo kanālu skaits attiecīgi samazinās, savukārt caurlaidspēja palielinās. *802.11n* ļauj ne tikai multipleksēt vai izplatīt datus starp divām vai vairākām radio ķēdēm, izmantojot vienu un to pašu kanālu, bet arī atdalīt datus, ko sauc par telpiski atdalītām neatkarīgām plūsmām (angļu val. *spatial streams*). Telpiski atdalītu neatkarīgu plūsmu skaits nav atkarīgs no raidītāju skaita, taču tas ir atkarīgs no sistēmas apstrādes veiktspējas un raidītāju tehniskajām iespējām. *802.11n* standartā ir iestrādāti bloka apliecinājumu (angļu val. *Block Acknowledgment – Block ACK*) ziņojumi kadru apstiprināšanai, kas ļauj samazināt virstēriņus, to vietā iespējams pārsūtīt vairāk lietderīgos datus un rezultātā palielināt kopējo caurlaidspēju. Standartā ir iestrādāta arī pārraides staru formēšana (angļu val. *transmit beamforming – TxBF*), kas ļauj uzlabot signāla kvalitāti un signāla un trokšņa attiecības (angļu val. *Signal to Noise Ratio – SNR*) parametru, novirzot signālu konkrētam bezvadu tīkla klientam. *802.11n* atbalsta 64-QAM modulācijas shēmu. *802.11n* iekārta spēj izmantot vairākas antenas un radio ķēdes, lai saņemtu vairākas pārsūtītas signāla kopijas. Kopijas savā starpā atšķiras un var būt cita par citu labākas. *802.11n* piedāvā maksimālās attiecības kombinēšanas (angļu val. *Maximal-Ratio Combining – MRC*) funkciju, ar kuras palīdzību var kombinēt signāla kopijas, lai izveidotu signālu, kas reprezentē vislabāko tā versiju jebkurā laika momentā. Rezultātā tiek rekonstruēts signāls ar labāku SNR attiecību. *802.11n* standarts atbalsta divu veidu starpsimbolu aizsargintervālus (angļu val. *Guard Interval – GI*), t. i., īsa aizsargintervāls 400 ns un garais aizsargintervāls 800 ns. Tas ļauj *OFDM*

signālus pārraidīt daudz biežāk, rezultātā iegūstot ~10 % caurlaidspējas pieaugumu [62]. *IEEE 802.11n* standarta specifikācijas pamatdati apkopoti 9. pielikumā.

IEEE 802.11ac

IEEE 802.11ac standarts izmanto 5 GHz frekvenču joslu, teorētiski spēj nodrošināt līdz 6,93 Gbit/s lielu datu pārraides ātrumu, izmantojot ļoti lielas caurlaidspējas (angļu val. *Very High Throughput – VHT*) tehnoloģiskus paņēmienus. Standartā ir paplašināta frekvenču kanālu apvienošana ar joslas platumu līdz 80 MHz un 160 MHz. Tiek izmantota blīvāka modulācijas shēma 256-QAM. *802.11ac* standartā var izmantot līdz astoņām telpiski izvērstām neatkarīgām datu plūsmām un ir iespēja sūtīt vairākus kadrus vairākām ierīcēm vienlaikus (angļu val. *Multi-user Multiple Input Multiple Output – MU-MIMO*). *802.11ac* standarts, tāpat kā *802.11n*, atbalsta gan 400 ns, gan 800 ns starpsimbolu aizsargintervālus [62]. *IEEE 802.11ac* standarta specifikācijas pamatdati apkopoti 9. pielikumā.

IEEE 802.11ax

IEEE 802.11ax jeb *Wi-Fi 6* ir apstiprināšanas stadijā esošs jauns standarts, kura pilnais nosaukums ir “Uzlabojumi augstai WLAN efektivitātei” (angļu val. *Enhancements for High Efficiency WLAN*). Standarts paredz daudz blīvākas modulācijas shēmas izmantošanu 1024-QAM. *802.11ax* paredzēts izmantot 2,4 GHz un 5 GHz frekvenču joslās. Standarts ļaus izmantot līdz astoņām telpiski atdalītām plūsmām ar *MU-MIMO OFDMA* tehnoloģiju. *IEEE 802.11ax* ir paplašināts darbības attālums āra apstākļos, kā arī ir iestrādāts WPA3 atbalsts un paplašinātas QoS (angļu val. *Quality of Service*) nodrošināšanas iespējas [35], [40].

IEEE 802.11be

Izstrādē esošais *IEEE 802.11be* projekta standarts, kura pilnais nosaukums ir “Īpaši augsta caurlaidspēja” (angļu val. *Extremely High Throughput – EHT*) spēs nodrošināt 4096-QAM signālu modulācijas shēmu. Paredzēts, ka *IEEE 802.11be* tiks izmantots gan iekštelpās, gan ārpus telpām, standarts izmantos 2,4 GHz, 5 GHz un 6 GHz frekvenču joslas. Tiek plānotas gan kanālu, gan dažādu frekvenču joslu (diapazonu) apvienošanas iespējas. Plānots, ka *MIMO* antenas varēs veidot līdz pat 16 telpiski atdalītām neatkarīgām datu plūsmām (angļu val. *spatial streams*). Standartā tiks iestrādāta vairāku bezvadu piekļuves punktu (angļu val. *Access Point – AP*) koordinācija, samazināta tīkla aizture, uzlabots kopējais pārklājums un nodrošināta dubleksā datu pārraide bezvadu tīklā [81].

4G LTE

4G LTE jeb *LTE* (angļu val. *Long Term Evolution*) ir mobilā tīkla tehnoloģija, ko var izmantot savienojumā ar iepriekš minētajām tehnoloģijām, lai nodrošinātu tiešu platjoslas piekļuvi interneta tīklam. *LTE* nodrošina lielu datu pārraides ātrumu (līdz 300 Mbit/s) un zemu tīkla aizturi (20 ms) [73]. *LTE* tīklos tiek izmantotas dažādas frekvences un frekvenču joslas, kas ir specifiskas konkrētām valstīm. *LTE* tehnoloģija izmanto ortogonālo frekvenčdales daudzpiekļuves metodi (angļu val. *Orthogonal Frequency Division Multiple Access – OFDMA*) metodi [36].

5G LTE/NR

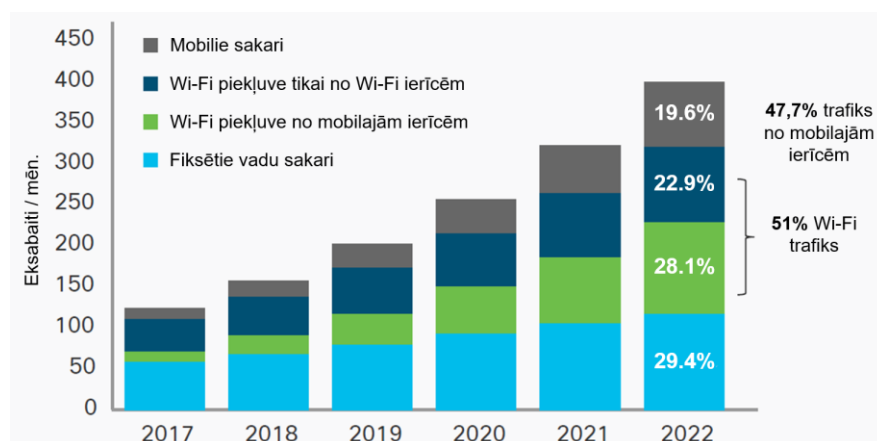
Ar 5G apzīmē ne tikai jaunu radiopiekļuves tehnoloģiju, to lieto arī daudz plašākā nozīmē, apzīmējot jaunus pakalpojumus, ko sniegs nākotnes 5G mobilo sakaru tīkli. *ITU* (angļu val. *International Telecommunication Union*) terminoloģijā 5G apzīmē ar *IMT-2020* [12]. Saskaņā ar *ITU* noteiktajām prasībām galvenie pakalpojumu veidi, kas jāspēj nodrošināt 5G sistēmām, ir [82], [126]: uzlabotā mobilā platjosla (angļu val. *Enhanced Mobile Broadband – eMBB*; vairāki Gbit/s lieli datu pārraides ātrumi tādiem pakalpojumiem kā platjoslas datu pārraide, televīzijas programmu apraides pakalpojumi, virtuālā realitāte u. c.); masīvie mašīnu tipa radiosakari (angļu val. *Massive Machine Type Communication – mMTC*; liels skaits savienoto iekārtu, zems enerģijas patēriņš, zemas izmaksas tādiem pakalpojumiem kā *IoT* (viedās pilsētas, viedās mājas, viedā satiksme), sensoru tīkli u. c.); ultradroši zemas laikaiztures radiosakari (angļu val. *Ultra-Reliable and Low-Latency Communications – URLLC*; zema laikaizture, augsta uzticamība un pieejamība tādiem pakalpojumiem kā savienotais transports, autonomie automobiļi, robotu vadība, industriālo risinājumu automatizācija u. c.) [31].

5G bezvadu piekļuve ietver gan 5G NR (angļu val. *New Radio*), gan arī *LTE* uzlabotās versijas (angļu val. *LTE Evolution*). *LTE* tehnoloģija un tās uzlabotās versijas paredzētas izmantošanai radiofrekvenču joslās zem 6 GHz, savukārt 5G NR ietver radiofrekvenču spektru līdz pat 100 GHz. Prognozējams, ka 5G radiotīklus veidos NR un *LTE* tehnoloģijās balstīti tīkli [37], [134], kā arī *WLAN* (angļu val. *Wireless Local Area Network*) tehnoloģijas [43].

Promocijas darbā ar *WLAN* vai *Wi-Fi* (angļu val. *Wireless Fidelity*) tiek apzīmētas autora veiktajos pētījumos izmantotās *IEEE 802.11n* un *IEEE 802.11ac* jeb *IEEE 802.11n/ac* standartu tehnoloģijas. Savukārt apzīmējumi 4G *LTE*, 4G un *LTE* tiek lietoti vienādā nozīmē, tie apzīmē ceturtais paaudzes mobilo sakaru *LTE* tehnoloģiju.

Datu trafika prognoze pēc piekļuves tehnoloģijas

Prognoze par *Wi-Fi* (prognozē ir iekļauti visi aktuālie *Wi-Fi* standarti) trafiku (ieskaitot trafiku no ierīcēm, kas atbalsta tikai *Wi-Fi* savienojumu) rāda, ka *Wi-Fi* un mobilais trafiks pieaugs straujāk nekā fiksētais trafiks (datu trafiks no ierīcēm, kas pieslēgtas *IP* tīklam, izmantojot *Ethernet*) (1.4. att.) [33], [142].

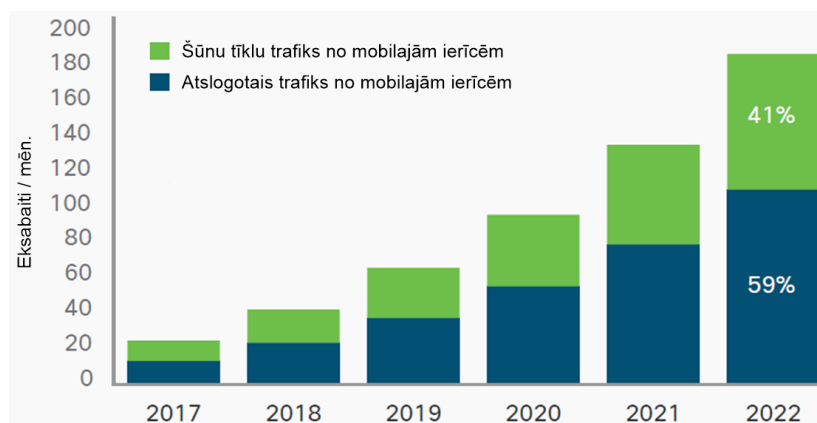


1.4. att. Globālais *IP* trafiks pēc piekļuves tehnoloģijas [142].

Līdz 2022. gadam no visa kopējā IP trafika (fiksētais un mobilais) 51 % trafika veidos datu plūsma caur *Wi-Fi* tīkliem, salīdzinot ar 43 % 2017. gadā. Datu trafiku nodrošinās gan mobilās divu režīmu viedierīces, gan tikai *Wi-Fi* ierīces. Savukārt 29,4 % trafika tiks nodrošināti caur vadu savienojumiem, 19,6 % trafika veidos mobilo tīklu savienojumi. 2022. gadā 47,7 % no visa IP trafika tiks sūtīti no mobilajām ierīcēm, tas ietvers gan mobilo, gan atslogoto trafiku (1.4. att.) [33], [142].

Atslogotā mobilā trafika prognoze

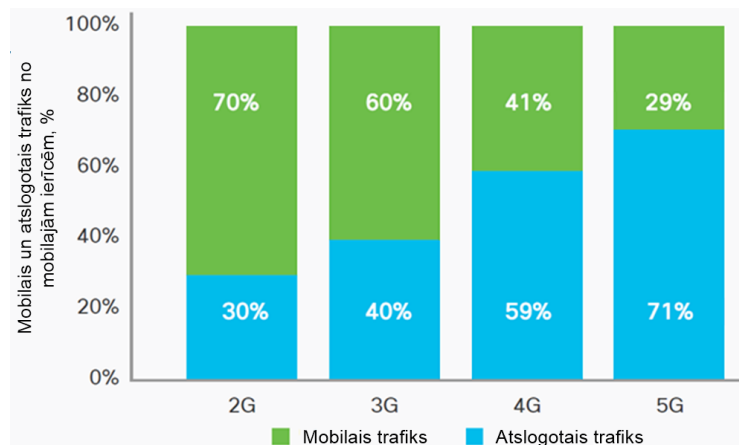
Jau 2017. gadā 54 % no visu mobilo iekārtu pārsūtītā datu trafika tika novirzīti caur *Wi-Fi* tīkliem vai femtošūnām. Saistībā ar prognozēto mobilā trafika pieaugumu (1.3.–1.4. att.) tiek prognozēts, ka šādā veidā atslogotais trafiks no mobilajām ierīcēm līdz 2022. gadam pieaugs aptuveni līdz 59 % (1.5. att.). Atslogošana (angļu val. *offloading*) attiecas uz trafiku no divu režīmu mobilajām ierīcēm (izņemot portatīvos datorus) un tiek realizēta, izmantojot *Wi-Fi* vai mazo šūnu tīklus (angļu val. *small-cell networks*) [33], [142].



1.5. att. Globālā mobilo tīklu datu trafika atslogošana caur *Wi-Fi* [33].

Tiek sagaidīts, ka *Wi-Fi* procentuāli vairāk atslogos tieši augstāku ātrumu tīklus, piemēram, 4G un 5G. 2017. gada beigās 4G tīklos atslogotais trafiks bija 57 %, un tiek prognozēts, ka līdz 2022. gadam tas sasniegs 59 % (1.6. att.) [33], [142]. Prognoze rāda, ka 5G tīklos atslogotais trafiks 2022. gadā sasniegs 71 %, tas ir saistīts ar mobilo ierīču skaita pieaugumu un jauno lietojumu augstajām prasībām pēc lieliem datu pārraides ātrumiem. 5G tīkliem sasniedzot tehnoloģisko gatavību, atslogošanas trafika īpatsvars varētu samazināties.

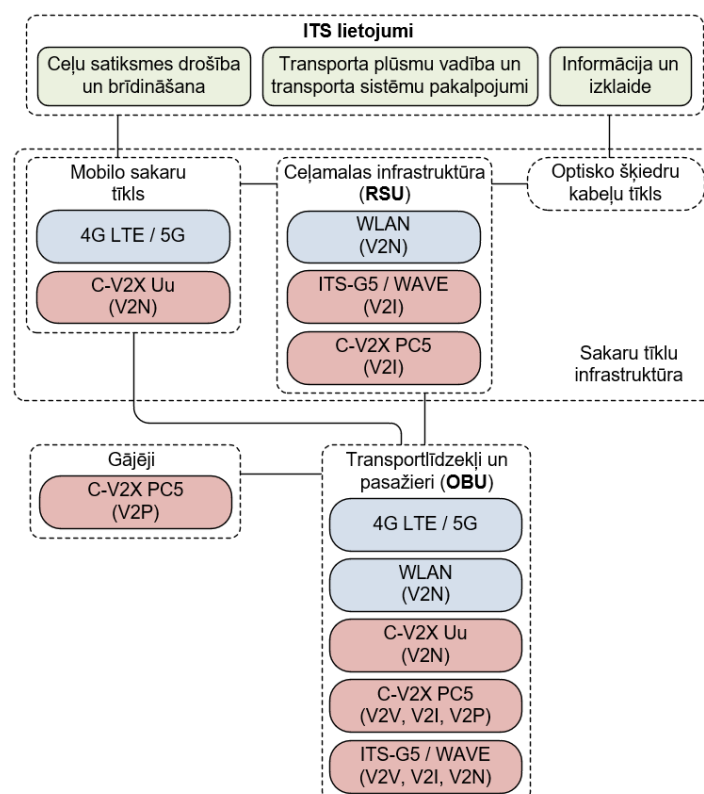
Apskatītās prognozes rāda, ka *Wi-Fi* tehnoloģija kā viena no galvenajām šūnu tīklu tehnoloģijām arī turpmāk tiks izmantota mobilo tīklu atslogošanai. *Wi-Fi* pieslēgumu skaits un tehnoloģijas nozīmība nākotnē tikai pieaugs. To arī apliecina pētījumi [11], [43], kas parāda, ka 5G tīklos paredzēts integrēt vairākas sakaru tehnoloģijas, ieskaitot *Wi-Fi* un *LTE*, tādējādi nodrošinot papildu frekvenču joslas, lai palielinātu kopējo tīkla kapacitāti.



1.6. att. Mobilo datu trafiks un atslogotais trafiks 2022. gadā [33].

Autotransporta sakaru tīklu tehnoloģiju apvienotā shēma

Saskaņā ar iepriekš apskatītajām ITS tehnoloģijām, kā arī izvērtējot datu trafika prognozes pēc piekļuves tehnoloģijas un tendencēm, kā tiks atslogoti mobilie tīkli, tika izveidota transporta sakaru tīklu tehnoloģiju apvienotā blokshēma (1.7. att.), kas apvieno 4G LTE C-V2X (LTE-V2X PC5/Uu), 5G C-V2X (5G NR-V2X PC5/Uu), ITS-G5, WAVE un WLAN tehnoloģijas.



1.7. att. ITS apvienotā sakaru tīklu tehnoloģiju shēma.

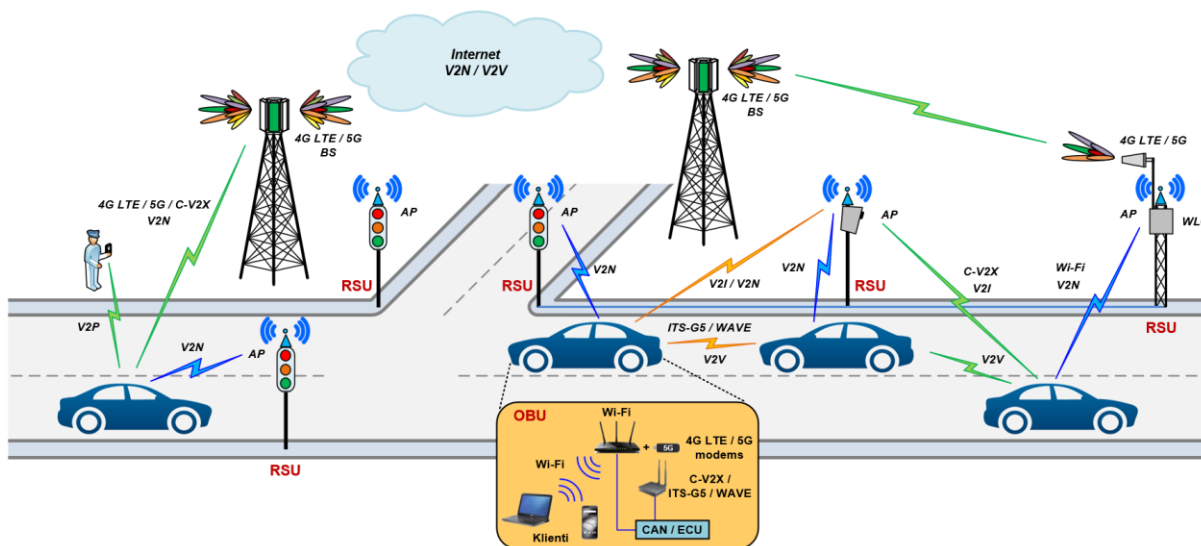
C-V2X tehnoloģija eksperimentālos testos uzrāda labākus rezultātus, salīdzinot ar IEEE 802.11p standartā bāzētām tehnoloģijām. Abas tehnoloģijas (IEEE 802.11p un C-V2X) tiek attīstītas paralēli. Paredzēts, ka IEEE 802.11p nākotnē tiks aizvietots ar izstrādē esošo IEEE

802.11bd standartu. Eiropas Savienībā ITS funkciju nodrošināšanai tiek izskatītas iespējas izmantot gan ITS-G5 (IEEE 802.11p), gan LTE-V2X tehnoloģijas [28]. Globāli automobiļu ražotāji, balstoties uz konkrētās valsts vai reģiona infrastruktūru, varēs piedāvāt ar atbilstošu ITS tehnoloģiju aprīkotos automobiļus. ITS-G5 tehnoloģiju atbalsta tādi autoražotāji kā Volkswagen (VW) and Renault. C-V2X atbalsta tādi autoražotāji kā Audi, Ducati, BMW, Ford. Savukārt abas šīs tehnoloģijas atbalsta Toyota [100].

Esošās ITS sistēmas (ITS G5/WAVE, LTE-V2X) nav paredzētas transportlīdzekļu pasažieru piekļuves organizēšanai interneta tīklam, lai pārsūtītu liela apjoma datus [29].

WLAN (Wi-Fi) tehnoloģija galvenokārt tiek izmantota piekļuvei pie informācijas un izklaides resursiem, kas tādējādi ļauj atslogot 4G LTE un 5G tīklus. Apvienotās individuālās klientu Wi-Fi plūsmas izejai uz interneta tīklu var izmantot kopīgu 4G LTE vai 5G kanālu vai arī veidot datu savienojumu caur optisko šķiedru kabeļu tīkliem.

Lai uzskatāmi parādītu apskatīto ITS tehnoloģiju 4G LTE/5G, C-V2X, ITS-G5/WAVE un Wi-Fi vietu kopējā ITS shēmā, 1.8. attēlā doti iespējamie ITS pakalpojumu V2V, V2P, V2I un V2N komunikācijas kanāli. ITS-G5/WAVE, C-V2X un Wi-Fi tehnoloģiju piekļuves punkti tiek izvietoti gar ceļmalu un tiek apzīmēti kā RSU iekārtas (1.8. att.). Automobilī tiek izvietota klienta ITS tehnoloģiju aparatūra, ko apzīmē kā OBU iekārtas.



1.8. att. Autotransporta sakaru tīkls.

Tādējādi apskatītās sakaru tehnoloģijas vai to kombinācija var tikt izmantotas, lai daļēji vai pilnā apmērā nodrošinātu ITS pakalpojumus. Gadījumā, ja automobilī tiek izvietots Wi-Fi maršrutētājs (1.8. att.), tas pilda gan ITS bezvadu klienta (OBU) funkcijas, lai nodrošinātu piekļuves pie ITS infrastruktūras tīkla (RSU), gan arī bezvadu piekļuves punkta (AP) funkcijas, lai nodrošinātu bezvadu tīkla pieslēgumu transportlīdzekļa pasažieriem. Abos gadījumos tiek izmantotas WLAN tehnoloģijas, kur katrai funkcijai tiek piešķirts savs radio kanāls. Savukārt, lai nodrošinātu automobiļa sistēmu (ECU) piekļuves datu pārraides tīklam, var tikt izmantots aprakstītais lokālais bezvadu tīkla režīms, vai arī var tikt izmantots Ethernet savienojums ar Wi-Fi maršrutētāju. Piemērā visa datu pārraide uz RSU iekārtu un tālāk uz interneta tīklu tiek nodrošināta, izmantojot automobilī izvietoto Wi-Fi maršrutētāju.

WLAN un LTE tehnoloģiju apvienotais ITS risinājums un saistītās problēmas

Izanalizējot iepriekš iegūtos faktus un tendences par aktuālajām bezvadu tīklu tehnoloģijām, var secināt, ka autotransporta pasažieru piekļuvei interneta tīklam var izmantot WLAN jeb *IEEE 802.11n/ac* tehnoloģijas. Tas saskan arī ar pētījumu [112], kura rezultāti apstiprina, ka lielāko daļu no ITS pakalpojumiem, izņemot brīdināšanu par incidentiem, ārkārtas izsaukumu (angļu val. *Emergency Call – e-Call*), kooperatīvo automobiļu vadīšanu un autonomo automobiļu atbalstu, spēj nodrošināt *IEEE 802.11ac* tehnoloģija. Savukārt AT&T kompānijas projekts *AirGig* [170] paredz izmantot kādu no *IEEE 802.11* standarta piekļuves metodēm, kur bezvadu tīkla infrastruktūras mezgli tiks izvietoti uz energokompāniju elektrības pārvades balstiem, lai nodrošinātu datu pārraides pakalpojumus mobiliem klientiem un māsaimniecībām. Savukārt elektropārvades līnijas kalpos kā atvilces tīkls (angļu val. *backhaul*), kas savienos kopā šos mezglus. Plānots, ka signāli caur elektropārvades līniju tiks pārraidīti milimetru viļņu diapazonā (60 GHz). Tālāk šādu tīklu varēs savienot ar optisko šķiedru pārraides tīklu vai pieslēgt pie 4G *LTE-A* vai 5G bāzes stacijas. Plānots, ka tīkla caurlaidspēja būs aptuveni 1 Gbit/s [162]. 5G tīklu attīstīšana lauku teritorijās ar mazu iedzīvotāju skaitu vai ārpus apdzīvotām vietām, kā arī kalnainos apgabalos nav ekonomiski pamatota, tāpēc šādu risinājumu instalācija būtu piemērota, jo tiktu izmantota esošo energokompāniju infrastruktūra. Tāpat šādu tīklu izvēršana tiktu īstenota gar ceļmalām, jo elektropārvades līnijas parasti tiek izbūvētas tieši gar tām.

Jāatzīmē, ka šobrīd esošie datu pārraides risinājumi transporta mobiliem objektiem pamatā ir bāzēti uz datu piekļuves organizēšanu caur mobilo operatoru 4G *LTE*/5G tīkliem. Šajā gadījumā galvenā problēma ir saistīta ar mobilo tīklu pārslogošanu blīvi apdzīvotos reģionos, galvenokārt pilsētās, jo pārsūtāmo datu apjoms nemitīgi pieaug. Tāpēc ir jādomā par mobilo tīklu atslogošanas risinājumiem. Nākamā problēma ir saistīta ar datu piekļuves organizēšana apgrūtinātos inženierbūves objektos, kur mobilie signāli neizplatās vai to izplatīšanās ir apgrūtināta, galvenokārt tie ir tuneļi un pazemes stāvlaukumi. Mobilo tīklu operatoriem šādos objektos un reģionos tas prasītu papildu mobilo tīklu bāzes staciju izvietošanu, lai paplašinātu vai uzlabotu pārklājuma zonu, un tās būtu ievērojamas finanšu līdzekļu investīcijas. Minētās problēmas var risināt, izmantojot WLAN tehnoloģijas. *IEEE 802.11n/ac* tehnoloģijas izmanto nelicencēto spektra daļu, kas ir bezmaksas, savukārt mobilo tīklu tehnoloģijas, piemēram, 4G *LTE* un 5G, izmanto licencēto – maksas spektra daļu. Mobilo tīklu operatori maksā arī par izmantoto tehnoloģiju patentiem. Līdz ar to mobilo tīklu pakalpojumi (atšķirībā no *Wi-Fi* tīkliem) vienmēr būs maksas [141].

Atgriežoties pie izstrādātās apvienotās ITS telekomunikāciju tehnoloģiju shēmas (1.8. att.), redzam, ka ceļmalas *Wi-Fi* bezvadu piekļuves punkti (*RSU* iekārtas) tiek pieslēgti pie centralizēta bezvadu tīkla kontroliera (angļu val. *Wireless LAN Controller – WLC*). Savukārt *WLC* var tikt pieslēgts pie 4G *LTE*/5G maršrutētāja, kas nodrošina bezvadu savienojumu ar 4G *LTE*/5G mobilā tīkla bāzes staciju (angļu val. *Base Station – BS*), kas jau tālāk nodrošina piekļuvi interneta tīklam. Realizējot WLAN un LTE tehnoloģijās bāzētu, integrētu risinājumu automobiļu piekļuvei datu pārraides tīklam, pastāv vairākas problēmas, kas tiks apskatītas tālāk.

Automobiļu sakaru tīklos mobilā klienta jeb pasažiera pārvietošanās ātrums atbilst automobiļa braukšanas ātrumam. Izmantojot *WLAN* tehnoloģiju kā mobilo klientu piekļuves metodi datu tīklam, tiek novērota veikspējas (caurlaidspējas) samazināšanās, pieaugot mobilā klienta pārvietošanās ātrumam [24]. Tas ir saistīts ar to, ka mobilais klients, pārejot uz cita bezvadu piekļuves punkta (*AP*) apkalpošanas zonu, izpilda pārslēgšanās procedūru starp *AP* (angļu val. *handover*), kas, pieaugot braukšanas ātrumam, kļūst nestabila un tiek izpildīta novēloti. Kustīgiem transportlīdzekļiem, kas pārvietojas ar lielu ātrumu (>70 km/h), ļoti svarīgs ir transporta sakaru tīkla nodrošinātais pārslēgšanās procedūras ātrums. Lai efektīvi izmantotu *IEEE 802.11* tehnoloģiju autotransporta sakaru tīklā, jāveic pārslēgšanās procedūras uzlabošana [138]. Jāņem vērā, ka pārslēgšanās procedūras ilgumu ietekmē arī *WLAN* tīklā realizētie drošības mehānismi, kas nodrošina mobilo klientu autentifikāciju [132]. Atkarībā no plānotā bezvadu tīkla mēroga un klientu skaita jāizvēlas vispiemērotākais *WLAN* tīkla drošības mehānisms un atbilstoša tīkla arhitektūra.

Bezvadu tīklos ar ātri kustīgiem objektiem lielu ietekmi uz klientu sasniedzamajiem datu pārraides ātrumiem atstāj apkārtējā vide un signālu vairākceļu izplatīšanās. Mobilajam klientam attālinoties no raidītāja, caurlaidspēja krītas. Bezvadu tīkla signāli ir jutīgi pret ārējiem traucējumu avotiem, tāpēc var tikt pazaudēti klienta sūtītie dati, kas pēc tam atkārtoti jāpārsūta, kā to paredz *802.11 MAC* un *TCP* (angļu val. *Transmission Control Protocol*) algoritmi. Tas prasa gan papildu laiku, gan pieaug virstēriņu apjoms. Līdzīgi, ietekmi uz datu trafiku atstāj arī izmantotais transporta slāņa protokols, kur *TCP* protokola gadījumā ir realizēti vairāki tīkla pārslodzes novēršanas mehānismi [123].

Saistībā ar iepriekš aprakstītajām problēmām *WLAN* bezvadu sakaru šūnu tīkliem ir raksturīgs augsts datu pārraides kļūdu līmenis, lielas tīkla aiztures un lielas aiztures variācijas. To veicina arī *WLAN* tehnoloģijas pusduplexais darbības režīms. Šie efekti pastiprinās gadījumos ar ātri kustīgiem klientiem. Jāpiemin arī mobilā klienta relatīvi īsais savienojuma laiks ar *AP* un biežās pārslēgšanās procedūras starp *AP*. Turklāt kopējo tīkla veikspēju nosaka tīkla individuālo sakaru mezglu veikspēja.

WLAN tehnoloģija saskaras arī ar problēmām, kas ir saistītas ar tās ierobežotajām mobilitātes iespējām, īpaši aktuāli tas ir ārpus apdzīvotām vietām. Tādēļ ir jādomā arī par risinājumiem, kā var nodrošināt savienojamību, arī izbraucot ārpus *Wi-Fi* infrastruktūras pārklājuma zonas. Transporta sakaru tīkliem jāspēj nodrošināt mobilajiem klientiem (automobiļiem) visur esošā savienojamība (angļu val. *connectivity*) [97], [141].

Lai pilnvērtīgi izvērtētu *WLAN* tehnoloģijas piemērotību izmantošanai automobiļu sakaru tīklos, nepieciešams veikt šāda transporta sakaru tīkla veikspējas parametru (piemēram, caurlaidspēja, atbildes laiks, pārslēgšanās procedūras aizture) mērījumus lauka apstākļos, izmantojot dažādus kustības režīmus ar vairākiem automobiļiem dažādos braukšanas ātrumos, pēc iespējas pietuvinot mobilā klienta pārvietošanos reāliem ceļu satiksmes apstākļiem.

Praksē izmantojams ir divrangu sakaru tīkls, pirmajā rangā ir *WLAN* piekļuves tīkls, savukārt otrajā – var tikt izmantota *4G LTE*, *5G* tehnoloģija vai arī optisko šķiedru kabeļu tīkls. Tādēļ veikspējas novērtējums ir jāveic arī divrangu sakaru tīklam.

1.2. Līdzīgu pētījumu pārskats

Pētnieki visā pasaulē strādā pie jauniem zinātniskajiem projektiem saistībā ar *IEEE 802.11* standarta tehnoloģiju izmantošanas iespējām, lai nodrošinātu platjoslas bezvadu datu pārraides kanālus gan automobiļu pasažieru piekļuvei interneta tīklam, gan arī automobiļu nodrošināšanai ar bezvadu datu pārraides pieslēgumu dažādu specifisku uzdevumu risināšanai. Pētījumu rezultāti un piedāvātie risinājumi ir publiski pieejami autobūves industrijai. Bieži vien pētījumi tiek veikti sadarbībā ar auto ražotājiem vai arī to atbalstu. Rakstā [118], kas izstrādāts sadarbībā ar *Volvo Trucks*, tiek apskatīta iespēja izmantot *IEEE 802.11s* režģtīklus (angļu val. *mesh networks*), lai automobiļiem veiktu attālinātu diagnostiku, pārkonfigurētu tos, instalētu jaunāko programmatūru un tās labojumus. Pētījumā īpaša uzmanība tiek pievērsta arī drošības jautājumiem – tiek prezentēta drošības koncepcija attiecībā uz klientu autentifikāciju un datu šifrēšanu. Pētījumā [87], kas veikts ar *BMW* atbalstu, tiek novērtētas *IEEE 802.11* (2,4 GHz) tehnoloģijas izmantošanas iespējas tieši transportlīdzeklī, pilsētas vides signālu interferences un traucējumu apstākļos, ko rada citi *Wi-Fi* tīkli un tādas tehnoloģijas kā *Bluetooth*, *ZigBee* u. c.

Vairākas zinātniskās publikācijas ir veltītas automobiļu sakaru tīklu ekonomiskā pamatojuma un tehnisko raksturlielumu novērtējumam. Rakstā [78] plaši tiek analizētas tehniskās iespējas, kā arī veikts ekonomiskais novērtējums, lai, izmantojot *IEEE 802.11p* standartu un mobilo tīklu tehnoloģijas, nodrošinātu transporta sakaru sistēmas ar piekļuvei interneta tīklam. Tomēr nav pieejami pētījumi, kas būtu veltīti tieši *IEEE 802.11n/ac* un *LTE* hibrīdu sakaru kanālu ekonomiskā izdevīguma novērtējumam.

Liela uzmanība tiek pievērsta problemātikai, kas ir saistīta ar mobilo tīklu atslogošanu. Pētījumā [74] tiek parādīts, ka mobilo tīklu atslogošana, izmantojot *Wi-Fi* tehnoloģiju, ir ekonomiski pamatota un izdevīga, raugoties gan no mobilo pakalpojuma sniedzēja puses, gan arī no lietotāju skatupunkta, attiecīgi galvenie kritēriji šeit ir peļņas pieaugums un izdevumu samazināšanās. Saskaņā ar rakstā [58] izstrādāto simulācijas modeli, veicot selektīvu 5G mobilo lietotāju atslogošanu un novirzot trafiku uz *Wi-Fi* infrastruktūru, var efektīvi ietaupīt 5G tīkla resursus. Savukārt pētījumā [16] dots 3G un *Wi-Fi* tehnoloģiju apskats izmantošanai transportlīdzeklī. Praktiski realizēta transportlīdzekļu sakaru testgultne, un veikti eksperimentālie mērījumi. Piedāvāts oriģināls *Wiffler* sistēmas risinājums mobilā tīkla atslogošanai, izmantojot *Wi-Fi* infrastruktūru. Risinājumā ir iestrādāts ātrās pārslēgšanās procedūras algoritms starp pētāmajiem šūnu tīkliem, un sistēma ņem vērā arī izmantoto lietojumu toleranci uz aizturēm, lai pieņemtu atslogošanas lēmumus. Novirzot trafiku caur *Wi-Fi* tīklu, tiek papildināta 3G tīkla kapacitāte. Parādīts, ka, pārsūtot reālu, uz aizturēm tolerantu trafiku, var panākt līdz pat 45 % mobilā 3G tīkla izmantošanas samazinājumu 60 s periodā. Mobilo tīklu atslogošanas jautājumi tiek apskatīti arī pētījumos [30], [75], [102].

Vairāki raksti ir veltīti transporta sakaru tīkliem un to veiktspējas novērtēšanai. Detalizēts un visaptverošs transportlīdzekļu sakaru tīklu pētījums veikts publikācijā [71], tās autori apskata transportlīdzekļu sakaru tīklus un to galvenos raksturlielumus, sniedzot pārskatu par šādu tīklu lietojumu un definētajām prasībām pret tiem, galvenajām problēmām un iespējamajiem risinājumiem. Pētījumā [52] tiek reprezentēta bezvadu komunikāciju sistēma, kas paredzēta transportlīdzekļu sakaru nodrošināšanai un tiek bāzēta *LTE* un *IEEE 802.11p* standartos, tiek

novērtēta šāda tīkla veikspēja. Iegūtie simulāciju rezultāti rāda, ka *IEEE 802.11p* tehnoloģija nodrošina pietiekamu veikspēju tīkla topoloģijai ar ierobežotu mobilitātes atbalstu. Savukārt *LTE* tehnoloģija atbilst lielākajai daļai automobiļu lietojumu definētajām prasībām attiecībā uz uzticamību, mērogojamību un mobilitātes atbalstu. Tomēr *LTE* tīkli nevar apmierināt noteiktās prasības pret aizturēm gadījumos, kad mobilais tīkls tiek pārslogots. Rakstā [132] tiek pētīta *Wi-Fi* bāzētu transportlīdzekļu sakaru tīklu caurlaidspēja, izmantojot izstrādātu 2D Markova ķēžu (angļu val. *Markov chain*) modeli, atkarībā no definēta transportlīdzekļu kustības ātruma, pakešu kļūdu ātruma un tīkla aiztures, kā arī izmantotajām autentifikācijas metodēm (*WPA2-PSK* vai *WPA2-802.1X*). Pētījuma [129] autori eksperimentālā testgultnē ir novērtējuši *UMTS* un *WLAN* veikspēju, lai nodrošinātu transportlīdzekļu savstarpējās komunikācijas (angļu val. *Inter Vehicle Communication – IVC*) sakarus, izmantojot vairākus transportlīdzekļu trafika un mobilitātes scenārijus. Autori secina, ka atsevišķa, kontrolēta drošības kanāla definēšana, kā tas ir piedāvāts *IEEE 802.11p* standartā, ir pamats *WLAN* piemērotībai ceļu drošības lietojumiem. Testējot ar drošību nesaistītus lietojumus, kur nav definēti reāllaika ierobežojumi, iegūtie mērījumu rezultāti apliecināja šo tehnoloģiju atbilstību šādu lietojumu izmantošanai. Transporta sakaru tīkliem ir veltīti arī vairāki citi pētījumi [50], [93], kuros novērtēta un analizēta to veikspēja.

Nav atrodami pētījumi, kur eksperimentāli tiktu novērtēta ietekme uz *WLAN* trafika raksturlielumiem un kopējo bezvadu tīkla veikspēju, izmantojot vairākus mobilos klientus (automobiļus), kas pārvietojas ar ātrumu, kas lielāks par 20 km/h, realizējot dažādus mobilo klientu kustības scenārijus.

Veicot pētījumus par *TCP* protokola ietekmi uz datu tīklu trafiku, tika secināts, ka protokolā realizētās *TCP* atkārtotas pārraides un pārslodzes kontroles mehānismi izraisa sevlīdzības efektu [99], [130]. Pētījumos noskaidrots, ka *TCP/IP* datu trafiks ir korelēts [99]. Ja vadu tīkla sašaurinājumā nonāk vairākas trafika plūsmas un ja kāda no tām ir sevlīdzīga, tad šajā tīkla mezglā izejošajā apvienotā plūsma arī būs sevlīdzīga [130]. Pētījumā [48] ir parādīts, ka trafikam *802.11 MAC* līmenī piemīt sevlīdzīga trafika īpašības. Rakstā [135] tiek atklāts, ka *802.11* vadības kadru datplūsma vājina sevlīdzīguma raksturojumu un tā uzliesmojošo raksturu kopējai kadru datplūsmai sesijas sākuma un beigu fāzē, savukārt tās produkcijas fāzē ir pretējs efekts. Turpretī kontroles, datu un atkārtotas pārraides kadru datplūsma pastiprina kopējā trafika sevlīdzīgumu un tā uzliesmojošo raksturu. Taču nav pētīts, kādu iespaidu uz datu trafiku un tā raksturu atstāj dažādu *LTE* maršrutētāju izmantošana.

Rakstā [121] tiek atspoguļoti izstrādātie daudzpiekļuves transporta bezvadu tīklu (angļu val. *Drive-thru Internet systems*) analītiskie modeļi datu savienojumu veikspējas novērtēšanai. Šo modeļu pamatā ir Markova procesi (angļu val. *Markov reward process*). Rakstā piedāvātie modeļi tika pārbaudīti, veicot simulācijas, kurās tika izmantoti *IEEE 802.11* standarta protokoli.

Apskatītajos pētījumos viens no atslēgas veikspējas parametriem, kas tiek novērtēts, ir datu kanālu caurlaidspēja. Tomēr iepriekš nav veikti pētījumi, kuros būtu mēģināts eksperimentāli, lauka apstākļos noskaidrot likumsakarību starp transportlīdzekļu sakaru tīklu caurlaidspēju un mobilā lietotāja pārvietošanās ātrumu. Tas tiek atzīmēts arī rakstā [30]. Tā ir svarīga likumsakarība ar praktisku nozīmi.

Vairākas metodes un praktiski risinājumi tiek piedāvāti, lai risinātu problēmas, kas saistītas ar pārslēgšanās procedūru *Wi-Fi* tīklos. Rakstā [77] tiek paaugstināta *MAC* (angļu val. *Medium Access Control*) protokola efektivitāte transportlīdzekļu piekļuvei interneta tīklam specifiskam, maz noslogotam automaģistrāles scenārijam, kā arī izstrādāts mērogojams 2D Markova ķēdes modelis, lai pētītu tīkla caurlaidspēju, izmantojot dažādu transportlīdzekļu skaitu un atšķirīgu braukšanas ātrumu. Savukārt eksperimentālais pētījums [38] atklāj, ka cilvēki bieži brauc pa labi zināmiem maršrutiem un tādējādi ar augstu precizitāti var paredzēt informāciju, saistītu ar šo maršrutu mobilitāti un savienojamību. Izmantojot tādus vēsturiskos datus kā *GPS* ieraksti ar piefiksētu laiksپiedolu, radiofrekvenču nolasījumi (angļu val. *RF fingerprints*) un izmantotā tīkla slāņa adresācija savienojumiem ar *AP*, autori ir izstrādājuši jaunas pārslēgšanās procedūras un datu pārraides stratēģijas. Veikto eksperimentālo veikspējas mērījumu rezultāti parāda, ka piedāvātais mobilitātes un savienojamības prognozēšanas risinājums var būt noderīgs *Wi-Fi* tīklos. Raksts [22] ir fokusēts uz klienta programmiski definētu tīklošanas (angļu val. *Software-Defined Networking – SDN*) mobilitāti *IEEE 802.11* standarta tīklos. Lai nodrošinātu *SDN* tehnoloģijas principos bāzētu bezvadu tīklu funkcionalitāti, autori ierosināja uzlabot bezvadu tīkla arhitektūru, tika veiktas izmaiņas gan *AP*, gan *SDN* kontroliera komponentēs. Turklāt vadu tīkla daļā esošie *IEEE 802.11* un *SDN* kontroles kanāli tika apvienoti vienā kopējā kanālā. Lai to izdarītu, tika paplašināts esošais *OpenFlow* protokols. Piedāvātā pieeja ievērojami uzlabo bezvadu tīkla arhitektūru šādos punktos: tīkla mērogojamība; drošība; atbalsts nemanāmai pārslēgšanās procedūrai (angļu val. *seamless handover*), taču šeit netiek apspriesta jaunās mobilitātes metodes lietošana ātri kustīgiem objektiem. Publikācijā [32] tiek padziļināti pētīti prognozēšanā i datu pārraides kanāla slāņa trigeri bezvadu tīklos. Tika atklāts, ka, izmantojot statistiskās prognozēšanas modeli *ARIMA* (angļu val. *Autoregressive Integrated Moving Average*), ar lielu precizitāti var paredzēt *RSS* (angļu val. *Received Signal Strength*) vērtības, it īpaši, ja tiek prognozēts tikai viens vai divi soļi uz priekšu. Trigeru paredzēšana ir bāzēta nākotnes *RSS* vērtību prognozē, analizējot vēsturiskos datus. Atbilstoši izstrādātajiem triggeru prognozēšanas algoritmiem nepieciešams veikt agrās pārslēgšanās procedūras inicializāciju un sagatavošanos. No pētījuma izriet, ka šī metode nebūtu piemērojama ātri kustīgiem objektiem. Pārslēgšanās procedūras uzlabošanai starp bezvadu piekļuves punktiem (*AP*) rakstā [107] tiek piedāvāts risinājums *MSSHD* (angļu val. *Mobility and Signal Strength-Aware Hand-off Decision*), tā pamatā ir pārslēgšanās procedūras galveno atslēgas metriku prognozēšana, lai pieņemtu lēmumu par pārslēgšanās procedūras sākšanu un izpildi. *RSSI* (angļu val. *Received Signal Strength Indicator*) un mobilā klienta kustības virziena parametri tiek izmantoti kā ieejas dati lemjošajā faziloģikas sistēmā. Risinājums realizēts *OMNeT++* simulācijas vidē un pārbaudīts, kad mobilais klients parvietojas ar mazu ātrumu (1 m/s). Rakstā [88] tiek uzsvērts, ka galvenā problēma *IEEE 802.11* transporta sakaru tīklos ir saistīta ar pārslēgšanās procedūru, kurā ir pārāk ilgs *AP* skenēšanas process. Rakstā tiek prezentēts izstrādātais prognozē balstīts pārslēgšanās procedūras mehānisms (angļu val. *predictive handover mechanism*), kas ņem vērā automobiļa trajektoriju, autoceļu un datu tīkla topoloģiju un ļauj pieņemt lēmumu par labāko atrašanās vietu un piemērotāko *AP*, lai veiktu pārslēgšanos. Eksperimentālajos mērījumos iegūtie rezultāti uzrāda labāku vidējo uztvertā signāla stipruma vērtību, datu pārraides ātrumu un savienojuma laiku, salīdzinot ar esošajiem pārslēgšanās procedūras risinājumiem.

Izstrādātais virziena noteikšanas modulis trajektorijas analīzes veikšanai izmanto fazioloģikas (angļu val. *fuzzy logic*) matemātiskos principus. Ir veikti arī vairāki teorētiski pētījumi [84], [108], kuros izskatītas iespējas paātrināt pārslēgšanās procedūru, tādējādi samazinot pārslēgšanās aizturi un palielinot kopējo bezvadu tīkla veiktspēju, izmantojot *IEEE 802.11k/r/v* standartu kombināciju. Taču nav pieejams neviens eksperimentāls pētījums ar praktisku šo standartu realizāciju transporta sakaru tīklos.

Vairākos pētījumos tiek novērtēts *Wi-Fi* uztvertā signāla jaudas līmenis atkarībā no attāluma līdz raidītājam. Novērtējumi veikti gan teorētiskā veidā, piemēram, izmantojot divstaru zemes plakanuma (angļu val. *two-ray flat-earth*), brīvās telpas ceļa zudumu (angļu val. *free-space path loss*) vai logaritmiski normālo (angļu val. *log-normal*) modeļus [79], [83] gan arī eksperimentāli, veicot *RSS* vai *RSSI* mērījumus (jāpiebilst, ka minētajos mērījumos *RSSI* ir izteikts dBm mērvienībās un reprezentē *RSS* parametru, kas ir uztvertā signāla jauda dBm mērvienībās, šāds minēto parametru lietojums tiek izmantots arī promocijas darbā) [83], [88], [133]. Šāda signālu vairākceļu izplatīšanās dabā rada uztvertā signāla jaudas fluktuācijas. Veicot teorētisko *Wi-Fi* tīkla caurlaidspējas novērtējumu, tas būtu jāņem vērā, jo šīs jaudas fluktuācijas tiešā veidā ietekmē sistēmu veiktspēju, t. i., caurlaidspēju. Pētījumā [27] tiek piedāvāts modelis, ar kura palīdzību tiek novērtēta vairāku konkurējošu *IEEE 802.11* sistēmu kapacitāte, balstoties uz radioviļņu izplatīšanās teoriju un Šenona teorēmu. Taču nav zināma likumsakarība, kā teorētiski varētu mainīties kanāla caurlaidspēja atkarībā no attāluma līdz raidītājam, ņemot vērā uztvertā signāla fluktuācijas. Šāda likumsakarība ļautu salīdzināt teorētiski aprēķinātos caurlaidspējas datus ar eksperimentāli iegūtajiem datiem.

Ņemot vērā ierobežojumus un grūtības, ar kurām var saskarties pētnieki, realizējot eksperimentālos mērījumus lauka apstākļos (ierobežota testgultnes mērogojamība, apgrūtinātas iespējas veikt izmaiņas mērījumu scenārijos, ārējās vides faktoru ietekme u. tml.), eksperimentālie mērījumi bieži vien tiek veikti laboratorijas apstākļos, izmantojot simulācijas rīkus. Piemēram, rakstā [51] tiek piedāvāts simulācijas rīku komplekts heterogēnu transportlīdzekļu sakaru tīklu imitēšanai. Savukārt promocijas darba autora pētījumā [10] tika veikts hibrīda transportlīdzekļu bezvadu sakaru tīkla veiktspējas novērtējums nestacionārā kustības režīmā, kur tika izmantots gan analītiskais modelis, gan pielāgots *OMNeT++* simulācijas rīks, lai varētu apvienot *IEEE 802.11n* un *3GPP LTE* tehnoloģijas vienotā simulācijas modelī. Tika izmantoti *INET*, *SimuLTE* un *Veins* ietvari, un modelis tika papildināts arī ar autoceļu trafika simulācijas modeli, izmantojot *SUMO* rīku. Pielāgotā simulācijas rīka kalibrēšanai tika izmantoti šajā promocijas darbā realizētās testgultnes konfigurācijas dati un eksperimentāli iegūto mērījumu rezultāti.

1.3. Promocijas darbā paveiktā apkopojums

Apkopojot iepriekš minētos faktus un pamatojoties uz autotransporta sakaru tīklu attīstības virzienu novērtējumu, tika definēts **promocijas darba mērķis** – izpētīt un novērtēt integrētu *IEEE 802.11n/ac* un *LTE* standartos bāzētu autotransporta sakaru tīklu veiktspēju, veikt *IEEE 802.11ac* bezvadu piekļuves tīkla veiktspējas paaugstināšanu.

Definētā mērķa sasniegšanai bija jāveic vairāki **pamatuzdevumi**.

1. Veikt izpēti par autotransporta nozarē izmantotajiem un perspektīvajiem telekomunikāciju bezvadu tīklu risinājumiem pēc to lietojuma veida, veikt šādu tīklu nākotnes tendenču un attīstības virzienu novērtējumu.
2. Veikt izpēti par *WLAN* tehnoloģijas darbības principiem un realizētajiem drošības mehānismiem.
3. Veikt izpēti par *LTE* tehnoloģiju, izpētīt galvenos uztvertā *LTE* signāla parametrus. Izpētīt iespējamās *WLAN* un *LTE* konverģences risinājumus.
4. Izveidot testgultni integrētam *WLAN* un *LTE* automobiļu sakaru tīklam. Novērtēt tā veiktspēju, izmantojot dažādu ražotāju *LTE* aparatūru. Veikt šāda tīkla veiktspējas novērtējumu atkarībā no mobilo klientu skaita un izmantotajiem kustības scenārijiem.
5. Definēt parametrus divrangu *WLAN* un *LTE* autotransporta sakaru tīkla tehniski ekonomiskā pamatojuma izstrādei un saskaņā ar to veikt šāda tīkla tehniski ekonomisko novērtējumu.
6. Noteikt likumsakarību starp integrēta *WLAN* un *LTE* sakaru kanāla caurlaidspēju un automobiļa (mobilā klienta) kustības ātrumu. Minētā likumsakarība jānosaka gan transporta līmeņa (TL), gan aplikācijas līmeņa (AL) caurlaidspējai. Likumsakarību noteikšanai nepieciešams veikt eksperimentālus mērījumus. Iegūtos mērījumu datus nepieciešams apstrādāt, izmantojot statistiskās datu apstrādes metodes.
7. Izstrādāt divrangu sakaru tīkla *LTE* daļas monitoringa risinājumu statistikas datu iegūšanai par *LTE* tīkla signāla stipruma un signāla kvalitātes parametriem.
8. Izpētīt *IEEE 802.11k/r/v* standartus. Izstrādāt risinājumu pārslēgšanās procedūras uzlabošanai *WLAN* tīklā, lai paaugstinātu *WLAN* bāzēta automobiļu sakaru tīkla kopējo veiktspēju. Veikt eksperimentālu veiktspējas parametru novērtējumu izstrādātā risinājuma ietvaros.
9. Izmantojot *WLAN* testgultnē eksperimentāli iegūtos datus un veicot teorētiskos aprēķinus, novērtēt likumsakarību starp uztvertā signāla jaudas līmeni un attālumu līdz raidītājam. Novērtēt datu pārraides kanāla caurlaidspēju atkarībā no attāluma līdz raidītājam. Abos gadījumos jāņem vērā uztvertā signāla jaudas līmeņa fluktuācijas.
10. Novērtēt iegūtos rezultātus un rekomendēt integrēta *WLAN* un *LTE* bezvadu datu pārraides tīkla izmantošanu autotransporta sakaru tīklos.

Pētījumu metodika

Promocijas darbā definēto uzdevumu realizācijā un problēmu analīzē izmantoti analītiskie modeļi, veikti matemātiskie aprēķini, kā arī eksperimentāli mērījumi lauka un laboratorijas apstākļos.

Eksperimentālo mērījumu realizācijai izstrādātas vairākas autotransporta sakaru tīklu testgultnes. Mērījumos izmantota dažādu ražotāju bezvadu datu pārraides tīkla aparatūra, piemēram, *HP* (angļu val. *Hewlett-Packard*), *Cisco*, *Huawei*, *TP-Link*. *IEEE 802.11v* standarta ieviešana un tā modificētās versijas testēšana realizēta, izmantojot *TP-Link Archer C7 WLAN*

maršrutētājus, un to oriģinālā aparātprogrammatūra aizstāta ar atvērtā koda aparātprogrammatūru *OpenWrt*.

Aplikācijas līmeņa (AL) datplūsmu ģenerēšanai un AL caurlaidspējas, atbildes laika un pārslēgšanās procedūras aiztures parametru novērtēšanai izmantota *IxChariot* programmatūra, savukārt transporta līmeņa (TL) datplūsmas tika ģenerētas un mērītas, izmantojot *iPerf* programmatūru.

Eksperimentāli iegūto caurlaidspējas rezultātu aproksimācijai un paplašinātu scenāriju modelēšanai izmantots daudztermināļu sistēmas modelis. Izstrādājot likumsakarības starp datu pārraides ātrumu un mobilā klienta kustības ātrumu, eksperimentāli iegūto datu aproksimācijai izmantoti lineārie un nelineārie regresijas modeļi. Savukārt uztvertā signāla jaudas zudumu aprēķinos izmantots divstaru signālu izplatīšanās modelis, kas tika papildināts ar gadījuma signālu fluktuācijām. Rezultātā likumsakarības aprakstam izmantots logaritmiski normālais modelis. Signālu svārstību aprakstīšanai izmantots Nakagami sadalījums.

Rezultātu novērtējumam izmantoti statistikas paņēmieni, piemēram, noteikti statistikas izkļedes rādītāji un noteiktas mērījumu un datu aproksimācijas kļūdas.

Matemātiskie aprēķini veikti, izmantojot *Matlab* programmatūru, eksperimentālo mērījumu rezultātu statistiskā apstrāde veikta *Excel* vidē. *WLAN* pārklājuma plānošanai un tā novērtēšanai izmantota *EkaHau Pro* programmatūra. Testgultnes *LTE* tīkla daļā uztvertā signāla parametru statistikas datu uzkrāšana un to vizualizēšana realizēta, izmantojot *Zabbix* programmatūru.

Promocijas darba jaunieguvumi

1. Izstrādāts tehniski ekonomiskais pamatojums integrētam *WLAN* un *LTE* automobiļu sakaru tīklam. Novērtēti tādi tehniskie parametri kā caurlaidspēja un atbildes laiks. Savukārt kā efektivitātes rādītāji izmantoti tādi parametri kā risinājuma izmaksas un mobilā tīkla atslogošanas parametrs, kas ir jaunieviests lielums.
2. Izmantojot dažādu ražotāju *LTE* aparatūru, dažādu klientu skaitu un dažādus kustības scenārijus, eksperimentāli novērtēta divrangu *IEEE 802.11n* un *LTE* sakaru kanāla veiktspēja, kā arī novērtēta datplūsmu sevlīdzīguma pakāpe.
3. Iegūta likumsakarība starp sakaru kanāla caurlaidspēju un automobiļa (mobilā klienta) kustības ātrumu. Minētā likumsakarība noteikta gan transporta līmeņa (TL), gan aplikācijas līmeņa (AL) caurlaidspējai.
4. Izstrādāts “*802.11v* tīkla asistētas” pārslēgšanās procedūras risinājums, kurā modificēts un eksperimentāli realizēts *IEEE 802.11v* standarts, izmantošanai *IEEE 802.11ac* autotransporta sakaru tīklos, kas ļauj paaugstināt šādu autotransporta bezvadu sakaru tīklu veiktspēju. Izstrādātajā risinājumā *IEEE 802.11ac* autotransporta testgultnes tīklā tika palielināta vidējā AL caurlaidspēja, samazināts vidējais tīkla atbildes laiks, kā arī samazināta pārslēgšanās procedūras aizture.
5. Izmantojot eksperimentālos datus un teorētiskos aprēķinus, *IEEE 802.11ac* sakaru tīklam novērtēts uztvertā signāla jaudas līmenis un caurlaidspēja atkarībā no attāluma līdz raidītājam. Aprēķinos ņemtas vērā arī uztvertā signāla jaudas līmeņa fluktuācijas.

Promocijas darba galvenie secinājumi

1. Integrēta *WLAN* un *LTE* autotransporta sakaru tīkla izveide ir tehniski un ekonomiski pamatota gadījumā, ja tiek izmantota *WLAN* bāzēta, *LTE* koncentrēta mobilā tīkla atslogošana. Tas ir praktiski izmantojams automobiļu sakaru tīkls, lai nodrošinātu liela apjoma datu pārsūtīšanu un organizētu automobiļu pasažieru piekļuvi interneta tīklam.
2. Divrangu *WLAN* un *LTE* sakaru tīkla veiktspēja ir atkarīga no tīkla mezglu tehniskajiem veiktspējas parametriem. Izmantojot dažādus *LTE* maršrutētājus, autotransporta bezvadu sakaru tīkla AL caurlaidspēja var atšķirties par 10–20 %. Mobilo klientu pārvietošanās ātruma, klientu skaita un klientu pārvietošanās scenāriju izmaiņas ietekmē gan individuālo mobilo klientu AL caurlaidspēju, gan arī kopējo bezvadu tīkla veiktspēju.
3. Neatkarīgi no tā, kāda ražotāja *LTE* maršrutētājs tiek izmantots divrangu *IEEE 802.11n* un *LTE* tīklā, tas neietekmē datu trafika raksturu. To rāda eksperimentālo mērījumu rezultātu analīze, kur datu trafika plūsmām tika novērtēti tādi parametri kā caurlaidspēja, korelācijas koeficients, dispersija un trafika sevlīdzīguma pakāpe.
4. Pārslēgšanās procedūra starp bezvadu piekļuves punktiem ir atkarīga no klienta ierīcē realizētā pārslēgšanās procedūras algoritma, *WLAN* tīkla arhitektūras risinājuma, kā arī realizētajiem bezvadu tīkla drošības mehānismiem.
5. Integrēta *IEEE 802.11n* un *LTE* sakaru kanāla caurlaidspēja mainās atkarībā no automobiļa (mobilā klienta) kustības ātruma (0–70 km/h) pēc otrās kārtas polinomiālās funkcijas likuma.
6. Integrētā *IEEE 802.11n* un *LTE* sakaru tīklā virstēriņi starp *L7* un *L4* vidēji ir līdz 36 %, ja mobilais klients pārvietojas ar ātrumu no 0 km/h līdz 70 km/h. Tas nozīmē, ka par tīkla caurlaidspēju nevar spriest, tikai balstoties uz mērījumiem, kas ir veikti transporta (*L4*) vai zemākos slāņos.
7. *IEEE 802.11ac* tīklā ar ātri kustīgiem objektiem (>20 km/h), savlaicīgi pieņemot pārslēgšanās procedūras lēmumu un izpildot pārslēgšanās procedūru, izmantojot *IEEE 802.11v* standarta “BSS pārejas vadības vaicājuma” un “BSS pārejas vadības pieprasījuma” ziņojumus ar izstrādāto modifikāciju, var paaugstināt bezvadu tīkla kopējo veiktspēju – vidējo aplikācijas līmeņa caurlaidspēju var palielināt līdz 75 %, vidējo tīkla atbildes laiku var samazināt līdz pat 67 %, kā arī iespējams nodrošināt mazākas vidējās pārslēgšanās procedūras aiztures, salīdzinot ar “Standarta” pārslēgšanās procedūru, kurā netiek izmantots *IEEE 802.11v* standarts.
8. Teorētiski veiktie aprēķini, tāpat kā eksperimentālie novērojumi un mērījumi, rāda, ka *IEEE 802.11ac* tīklā, mobilajam klientam attālinoties no raidītāja, uztvertā signāla jauda pavājinās, kā rezultātā samazinās arī caurlaidspēja. Uztvertā signāla jauda ir laikā mainīga un fluktuējoša, uztvertā signāla jaudas svārstības izraisa konstruktīva un destruktīva interference starp vairākceļu signāla izplatīšanās komponentēm, kas savukārt izraisa arī caurlaidspējas fluktuācijas.

Promocijas darba praktiskā vērtība

- Izveidota un izpētīta integrēta autotransporta bezvadu sakaru tīkla testgultne, izmantojot *IEEE 802.11n/ac* un *LTE* tehnoloģijas.
- Eksperimentāli novērtēta dažādu ražotāju bezvadu tīkla aparatūras veiktspēja divrangu *IEEE 802.11n* un *LTE* sakaru kanālu nodrošināšanai. Eksperimenti veikti ceļu satiksmes apstākļiem pietuvinātā vidē.
- Iegūtas jaunas, kombinēta *IEEE 802.11n* un *LTE* autotransporta sakaru tīkla veiktspēju raksturojošas likumsakarības.
- Izstrādāts un *IEEE 802.11ac* tīklā eksperimentāli novērtēts *IEEE 802.11v* standarta modifikācijā bāzēts uzlabotas pārslēgšanās procedūras risinājums – “802.11v tīkla asistēta” pārslēgšanās procedūra, kas rezultātā ļāva paaugstināt kopējo bezvadu tīkla veiktspēju.

Promocijas darba zinātnisko pētījumu rezultāti tika izmantoti, sagatavojot pieteikumu ERAF projektam “Viedais savienojamības risinājums autotransporta sakaru tīkliem (SCAN)”, Nr. 1.1.1.1/20/A/007.

Promocijas darba zinātnisko pētījumu rezultāti var tik izmantoti:

- tehniski un ekonomiski pamatotu integrētu *WLAN* un *4G LTE/5G* automobiļu sakaru tīklu izveidei, kā arī *4G LTE* un *5G* tīklu atslogošanas risinājumos;
- rekomendācijas sagatavošanai ar mērķi *IEEE 802.11* standartā iekļaut realizēto *IEEE 802.11v* modifikāciju, kas ļauj nodrošināt efektīvu pārslēgšanās procedūras risinājumu ātri kustīgiem klientiem.

Promocijas darba galvenie rezultāti prezentēti septiņās starptautiskajās zinātniskajās konferencēs, kā arī atspoguļoti astoņās publikācijās zinātniskajos žurnālos, četrās publikācijās pilna teksta konferenču rakstu krājumos, vienā zinātniskās monogrāfijas nodaļā (1. pielikums).

Promocijas darba aizstāvamās tēzes

1. Realizējot integrētu, *IEEE 802.11n* un *LTE* standartos bāzētu autotransporta bezvadu sakaru tīklu, neatkarīgi no ražotāja un izmantotās *LTE* iekārtas šāda tīkla sakaru kanāla datu plūsmas raksturs nemainās.
2. Integrēta, *IEEE 802.11n* un *LTE* standartos bāzēta sakaru kanāla caurlaidspēja mainās atkarībā no automobiļa (kustīgā objekta) pārvietošanās ātruma (0–70 km/h) pēc otrās kārtas polinomiālās funkcijas likuma.
3. Izstrādātais “802.11v tīkla asistētas” pārslēgšanās procedūras risinājums *IEEE 802.11ac* tīklā ar ātri kustīgiem objektiem (>20 km/h) ļauj paaugstināt bezvadu tīkla kopējo veiktspēju, t. i., ļauj palielināt vidējo aplikācijas līmeņa caurlaidspēju līdz 75 %, samazināt vidējo tīkla atbildes laiku līdz 67 %, kā arī dod iespēju nodrošināt mazākas vidējās pārslēgšanās procedūras aiztures.

Promocijas darba apjoms ir 141 lappuses. Darbā ir piecas nodaļas, nobeigums, literatūras saraksts un deviņi pielikumi.

Pirmās nodaļas ievadā dotas galvenās tendences, kas pamato veikto pētījumu aktualitāti. Tālāk ir izveidots pārskats par *ITS* sistēmām, apskatīti galvenie jautājumi, ko tās risina. Sniegti iespējamie *ITS* attīstības virzieni un veikts perspektīvo sakaru tīklu tehnoloģiju apskats. Nodaļā ir dotas tendences, kas pamato pētījumā iekļauto bezvadu sakaru tehnoloģiju izvēli. Turpinājumā apskatītas galvenās problēmas, kas pastāv automobiļu bezvadu sakaru tīklos, ja tiek izmantotas *WLAN IEEE 802.11n/ac* un *LTE* tehnoloģijas, kā arī ir dots līdzīgu pētījumu apskats. Nodaļas noslēgumā definēti promocijas darba galvenie pētījumu virzieni, kā arī apkopota informācija par promocijas darbā paveikto.

Darba otrajā nodaļā veikts *WLAN* un *LTE* tehnoloģiju apskats. Izpētīti tādi jautājumi kā *WLAN* un *LTE* tīklu konverģences iespējas ar mērķi palielināt *WLAN* klientu mobilitāti, kā arī veikta detalizēta izpēte par pieejamiem drošības mehānismiem *WLAN* tīklos. Nodaļas turpinājums ir veltīts eksperimentālu *IEEE 802.11n* un *LTE* tehnoloģijās bāzētu autotransporta sakaru tīklu veikspējas novērtējumam. Izmantojot daudztermināļu sistēmas matemātisko modeli, veikts bezvadu tīkla veikspējas novērtējums arī stacionāram gadījumam. Nodaļas noslēgumā prezentēts izstrādātais heterogēna divrangu *Wi-Fi* un *LTE* autotransporta sakaru tīkla tehniski ekonomiskais novērtējums.

Darba trešajā nodaļā ir dotas izstrādātās likumsakarības starp integrēta *IEEE 802.11n* un *LTE* sakaru kanāla transporta līmeņa (TL) vai aplikācijas līmeņa (AL) caurlaidspēju un automobiļa (mobilā klienta) pārvietošanās ātrumiem. Nodaļas ietvaros izstrādāts *LTE* tehnoloģijas signāla stipruma un signāla kvalitātes parametru attālinātās uzraudzības risinājums un veikta iegūto rezultātu analīze.

Darba ceturtajā nodaļā novērtēti *IEEE 802.11k/r/v* standarti, ko var izmantot pārslēgšanās procedūras uzlabošanai *IEEE 802.11ac* tīklos. Nodaļas turpinājumā aprakstīts izstrādātais uzlabotas pārslēgšanās procedūras algoritms, kas balstīts *IEEE 802.11v* standartā, veikts izstrādātā risinājuma eksperimentāls veikspējas novērtējums un iegūto rezultātu analīze.

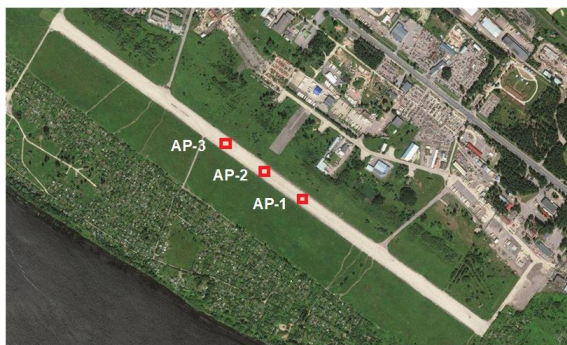
Darba piektajā nodaļā novērtēta likumsakarība starp uztvertā signāla jaudas līmeņa atkarību no attāluma līdz raidītājam. Aprēķinos izmantots logaritmiski normālais modelis, kurā tiek ņemtas vērā uztvertā signāla fluktuācijas, ko raksturo Nakagami sadalījums. Tālāk, izmantojot Šenona teorēmu un iepriekš veiktos aprēķinus, teorētiski novērtēta *WLAN* tīkla caurlaidspēja, mobilajam klientam attālinoties no raidītāja. Nodaļas noslēgumā teorētiski aprēķinātie caurlaidspējas rezultāti salīdzināti ar eksperimentāli iegūtajiem.

Promocijas darba nobeigumā apkopoti darba galvenie secinājumi un definēti turpmākie pētījumu virzieni. Pielikumos apkopoti konferenču, publikāciju un projektu saraksti, pievienoti eksperimentālos mērījumos iegūtie rezultāti, doti aprēķinos izmantotie *Matlab* kodi, kā arī atspoguļoti realizētajās testgultnēs izmantotā aprīkojuma tehniskās specifikācijas dati un mērījumu galvenie iestatījumi.

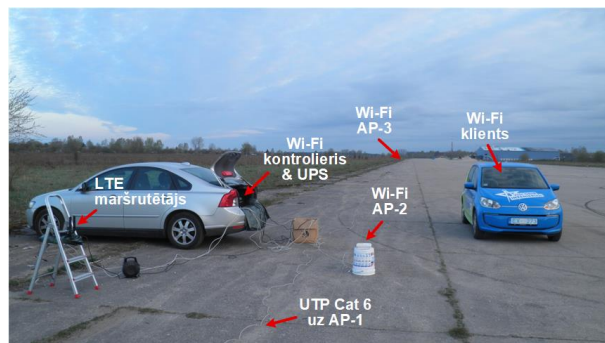
2. INTEGRĒTU WLAN UN LTE AUTOTRANSPORTA SAKARU TĪKLU VEIKTSPĒJAS NOVĒRTĒJUMS

Nodaļas sākumā dots *IEEE 802.11n* un *LTE* tehnoloģiju apskats. Apvienojot minētās datu pārraides tehnoloģijas, tiek iegūts heterogēns [60] divrangu sakaru tīkls. Tā pirmo rangu veido *IEEE 802.11n* tehnoloģija, otro – *LTE* tehnoloģija. Eksperimentāli tiek novērtētas iespējas izmantot šādu kombinētu bezvadu tīklu transportlīdzekļu sakaru nodrošināšanai. Lauka apstākļos, veicot mērījumus, tiek novērtēta divrangu sakaru tīkla veiktspēja kopā ar kustīgiem objektiem, t. i., automobiļiem un to pasažieriem, kas ir šī bezvadu tīkla klienti. Tiek pētīts, kādu ietekmi uz trafiku, tā raksturu un kopējo tīkla veiktspēju atstāj kustīgo klientu skaita izmaiņas, dažādu ražotāju *LTE* iekārtu vai dažādu kustību scenāriju izmantošana. Nodaļas noslēgumā, izmantojot *IxChariot* programmatūru, tiek simulētas vairākas bezvadu tīkla klientu plūsmas stacionārā režīmā un novērtēta pirmā ranga veiktspēja. Stacionārā režīmā iegūtie eksperimentālie rezultāti tiek pārbaudīti, izmantojot matemātisko modeli.

2.1. a–b attēlos redzama lauka apstākļos izvietotā eksperimentālā testgultne, kas atradās bijušajā Rumbulas lidlauka teritorijā.



a) Testgultnes teritorija



b) Testgultnes klienta (OBU) un ceļmalas (RSU) aparatūra

2.1. att. Eksperimentālo mērījumu iekārtas un to izvietojums.

Eksperimentālie mērījumi tika veikti, organizējot sakaru kanālu, izmantojot divrangu sakaru tīklu. Pirmā ranga galvenie eksperimentālo mērījumu iestatījumi apkopoti 8. pielikumā.

2.1. WLAN tehnoloģijas apskats

Eksperimentālajos mērījumos transporta sakaru tīkla pirmo rangu veido *Wi-Fi* tīkls, kas sastāv no bezvadu piekļuves punktiem (AP), kas atbalsta *IEEE 802.11n* standartu, bezvadu tīkla kontroliera, kā arī mobilajiem klientiem. Šajā apakšnodaļā veikts *WLAN* tehnoloģijas apskats, pievēršot uzmanību arī drošības jautājumiem.

IEEE 802.11 ir fizikālā slāņa (*PHY*) un vides piekļuves vadības (*MAC*) specifikāciju kopums *WLAN* ieviešanai 2,4 GHz, 5 GHz un 60 GHz frekvenču joslās. Šīs specifikācijas uztur *IEEE 802 LAN* standartu komisija. *WLAN* tīkliem papildus tiek plānota arī jauna 6 GHz frekvenču josla [143]. Bezvadu tīkla standarta bāzes versija pirmo reizi tika publicēta 1997. gadā. Standarts un tā papildinājumi (angļu val. *amendments*) apraksta *Wi-Fi* tehnoloģijas

pamatus. Standarta papildinājumi oficiāli tiek atcelti brīdī, kad tie tiek iestrādāti jaunākajā standarta versijā. Neskatoties uz to, iekārtu ražotāji uz savu produktu iepakojumiem norāda standarta papildinājumu apzīmējumus, jo tie kodolīgi parāda un izceļ piedāvāto produktu iespējas. Līdz ar to tīklošanas kopienā (angļu val. *networking community*) katra jauna standarta papildinājuma izdošana tiek uztverta kā jauns atsevišķs standarts [1].

Wi-Fi sakaru tīklu galvenie veiktspējas raksturlielumi ir caurlaidspēja (angļu val. *throughput*), kapacitāte jeb maksimālā caurlaidspēja (angļu val. *capacity*), aplikācijas līmeņa (AL) caurlaidspēja (angļu val. *goodput*), pakešu zudums (angļu val. *packet loss*), trīce jeb nevienmērība (angļu val. *jitter*), aizture (angļu val. *delay*) jeb latentums (angļu val. *latency*) [57], [117] vai atbildes laiks (angļu val. *response time*) un pārslēgšanās procedūras aizture (angļu val. *handover delay*) [113].

802.11 bezvadu tīklu topoloģija

Katra IEEE 802.11 standarta pamatpakalpojumu kopa (angļu val. *Basic Service Set – BSS*) sastāv no bezvadu piekļuves punkta (AP), kur tas darbojas infrastruktūras režīmā. Tas nozīmē, ka AP nodrošina pakalpojumus, kas nepieciešami, lai izveidotu bezvadu tīkla infrastruktūru. Tā ir slēgta bezvadu pakalpojumu zona, ko veido mobilo staciju grupa apkārt fiksētam bezvadu piekļuves punktam (AP). Pirms mobilā stacija var tai pievienoties, tai ir nepieciešams paziņot savas iespējas (angļu val. *capabilities*), pēc tam tiek piešķirtas pievienošanās tiesības. BSS ir ierobežots ar apraides zonu, kurā AP signāls ir izmantojams. To sauc par pamatpakalpojumu zonu (angļu val. *Basic Service Area – BSA*) jeb šūnu (angļu val. *cell*). Šūnas zonas izmēri un forma ir atkarīga no izmantotās AP antenas izstarojuma diagrammas (angļu val. *radiation pattern*). Parasti tiek izmantotas nevirzītās (angļu val. *omnidirectional*) antenas. AP kalpo par saskares punktu jebkurai iekārtai, kas vēlas izmantot BSS. Katrs AP paziņo savu BSS, tādā veidā mobilās stacijas uzzina par tā eksistenci un mēģina tam pieslēgties. BSS apziņošanai AP izmanto unikālu BSS identifikatoru (angļu val. *BSSID – BSS identifier*), kas ir bāzēts uz AP radio MAC adresi. Papildus tam AP paziņo par bezvadu tīklu, izmantojot pakalpojumu kopas identifikatoru (angļu val. *SSID – Service Set Identifier*), kas reprezentē teksta simbolu virkni, kas veido loģisku tīkla nosaukumu. Katram AP var būt definēti vairāki SSID. Tādā gadījumā AP uzrādās kā daudzkārtīgs virtuālo AP kopums, kur katrs virtuālais AP atbilst savam BSS ar unikālu BSSID.

Mobilā klienta stacijas līdzdalība konkrētā BSS tiek saukta par asociāciju (angļu val. *Association*). Stacijai ir jānosūta asociācijas pieprasījums, un AP tas ir vai nu jāpieņem, vai arī jānoraida. Pēc asociācijas mobilā stacija kļūst par BSS klientu jeb 802.11 staciju (angļu val. *Station – STA*). Kamēr 802.11 stacija paliek asociēta ar BSS, viss komunikācijas trafiks tiek sūtīts, izmantojot attiecīgo AP.

Viens AP var nodrošināt radiopārklājumu tikai konkrētai, ierobežotai zonai. Radiopārklājuma zonu var paplašināt, uzstādot papildu AP, kas tiek izvietoti ģeogrāfiski dažādās vietās. Šos AP (BSS) var savienot, izmantojot DS (angļu val. *Distribution System*) infrastruktūru, piemēram, izmantojot IP komutatorus (angļu val. *IP Switch – SW*). IEEE 802.11 standartā to sauc par paplašināto pakalpojumu komplektu (angļu val. *ESS – Extended Service*

Set). Raugoties no klienta perspektīvas, galvenā ideja ir likt vairākiem AP sadarboties tā, lai bezvadu pakalpojumi nodrošina vienlaidu savienojamību. Jebkurš SSID, kas ir definēts uz atsevišķa AP, būtu jānedefinē arī uz pārējiem AP, lai nodrošinātu pakalpojumu pieejamību visā ESS, ja vien speciāli nav noteikti ierobežojumi izplatīt konkrētu SSID. Šajā gadījumā katrai šūnai ir savs unikāls BSSID, taču vairākām šūnām var būt kopīgs SSID. Klients pārvietojas viena SSID ietvaros un tajā pašā laikā spēj atšķirt, pie kura AP tas ir pieslēdzies, izmantojot tā BSSID. ESS tīkla klients vienlaikus var asociēties tikai ar vienu AP [62].

IEEE 802.11 bezvadu tīkla arhitektūru (dizainu) lielā mērā ietekmē bezvadu tīkla mērogs, t. i., AP skaits. WLAN arhitektūru var iedalīt: autonomā; centralizētā; izkliedētā [68]. Autonomā WLAN arhitektūra raksturo autonomu AP tīklu. Centralizētā WLAN arhitektūrā visi bezvadu piekļuves punkti tiek pārvaldīti, izmantojot bezvadu tīkla kontrolieri (WLC), kur tiek nodrošinātas centralizētas vadības plaknes (angļu val. *management plane*) un kontroles plaknes (angļu val. *control plane*) funkcijas. Savukārt izkliedētā WLAN arhitektūrā WLC netiek izmantots, tā vietā savā starpā ir savienoti paplašinātas funkcionalitātes AP, kas izmanto speciālus savstarpējās komunikācijas kooperatīvos (angļu val. *cooperative*) protokolus, kas nodrošina kontroles plaknes datu apmaiņu [47], [114].

Vadības plakne sniedz iespēju veikt centralizētu WLAN tīkla konfigurēšanu, nodrošina WLAN monitoringu un pārskatus, nodrošina vienotu WLAN aparātprogrammatūras (angļu val. *firmware*) pārvaldību [35], [47].

Kontroles plakne nodrošina inteligences un tīkla iekārtu mijiedarbības funkcijas, piemēram, radio resursu vadību (angļu val. *Radio Resource Management – RRM*) (automātiska un koordinēta dinamisko frekvenču kanālu un jaudas iestatīšana starp AP), klientu slodzes balansēšanu, pārslēgšanās procedūras mehānismu darbību (vienlaidu pārslēgšanās procedūra, izmantojot ātrās pārslēgšanas paņēmienus, buferatmiņā uzkrāto klienta pakešu pārsūtīšana caur jaunās asociācijas AP) [35], [47].

802.11 pārraides vides piekļuves un kadru aizsardzības mehānisms

Bezvadu tīkla ierīces šobrīd aktuālajos IEEE 802.11n/ac standartos, ieskaitot jauno, standartizācijas procesā esošo IEEE 802.11ax standartu, strādā pusdupleksā režīmā. Tas nozīmē, ka raidošs bezvadu tīkla klients nevar noteikt, kurā brīdī tīklā notiek kolīzija, ko izraisa vairāki vienlaikus raidoši bezvadu tīkla klienti [106]. Lai nepieļautu šādas signālu kolīzijas, IEEE 802.11 standartā bāzētie bezvadu tīkli izmanto nesēja jušanas un sadursmju atklāšanas daudzpiekļuves (angļu val. *Carrier Sense Multiple Access with Collision Detection – CSMA/CA*) mehānismu [98]. CSMA/CA ir “klausies, pirms runā” (angļu val. *Listen Before Talk – LBT*) mehānisms. Raidošā stacija pirms pārraidīšanas sākšanas klausās, vai pārraides vidē nav nesēja signāls, ja kanāls ir aizņemts, tad stacija gaida, līdz nesēja kanāls atbrīvojas.

IEEE darba grupa ir iesākusi darbu pie jauna IEEE 802.11 standarta papildinājuma IEEE 802.11be izstrādes, kurā tiek plānots iestrādāt funkcionalitāti dupleksai datu pārraidei. To var panākt, izmantojot dažādas frekvenču joslas, dažādus kanālus, vai arī lietojot speciālu tehniku – izmantot vienu un to pašu kanālu vienlaicīgai datu pārraidei un saņemšanai. Tas ļautu

palielināt maksimālo kanāla caurlaidspēju un samazināt tīkla aizturi jeb latentumu (angļu val. *latency*), kā arī uzlabotu kolīziju detektēšanas shēmu [81].

Sakarā ar iespējamām kolīzijām un pārraides vides pasliktināšanos (piemēram, parādās ārējais traucējumu avots, kas rada interferenci), var tikt izkropļoti pārraidītie 802.11 kadri (angļu val. *frames*). Lai risinātu datu pazaudēšanas problēmu, MAC slānis ietver kļūdu atkopes (angļu val. *recovery*) mehānismu. 802.11 standartā ir iestrādāta apliecinājumu (angļu val. *Acknowledgment* – *ACK*) kadru un bloka apliecinājumu (angļu val. *Block ACK*) kadru izmantošana. Ja galamērķa stacija saņem uniraides (angļu val. *unicast*) kadru bez kļūdām, tad galamērķa stacija vienmēr atbild ar *ACK* kadru stacijai, kas atsūtīja šo kadru. Uztverošās stacijas neapliecina multiraides kadrus. Ja noteiktā laika periodā pārraidošā stacija nesaņem *ACK* kadru par nosūtīto uniraides kadru, tad pārraidošā stacija pieņem, ka attiecīgais datu kadrs tika bojāts un mēģina vēlreiz pārsūtīt to pašu datu kadru. Pārsūtīšanas mēģinājumi notiek vairākas reizes. Mēģinājumu skaits ir atkarīgs no ražotāja izstrādātā algoritma. Ja pārraidošajai stacijai nav izdevies veiksmīgi nosūtīt datu kadru un saņemt *ACK* kadru, tad augstāka līmeņa protokols, piemēram, *TCP*, var piedāvāt papildu kļūdu atkopes mehānismu [49].

Bezvadu tīkla veikspēju un datu trafika raksturu ietekmē 802.11 MAC līmeņa pakāpeniska datu pārraides ātruma pielāgošana sesijas izveides sākumā [50] un 802.11 MAC līmeņa atkārtotas pārraides mehānisms visas sesijas laikā.

Sakarā ar pusduplekso režīmu un obligātajiem apliecinājuma (*ACK*) kadriem datu pārraides ātrums nav pielīdzināms vadu tīklā esošajiem, tas ir daudzkārt mazāks. Apliecinājuma kadri palielina pārsūtāmo datu apjomu, kas rezultējas virstēriņos, tādējādi samazinot lietderīgo datu pārraides ātrumu.

802.11 MAC slāņa operācijas

Bezvadu klienta savienojamība

802.11 MAC protokols operē L2 (angļu val. *Layer 2*) slānī [106]. Viena no galvenajām 802.11 MAC slāņa operācijām ir klienta ierīces savienojamības nodrošināšana. Starp 802.11 tīkla klienta ierīci un *AP* ir jānotiek trīs apmaiņas procesiem, lai bezvadu klienta ierīce varētu piekļūt pie *BSS (AP)* – skenēšanas process, autentifikācijas process un asociācijas process. Klienta savienojamību papildus regulē arī diasociācijas un reasociācijas procesi [106].

Skenēšanas process

Pirms bezvadu klienta ierīce pieslēdzas pie konkrēta *BSS*, tai vispirms jānoskaidro, kādi *AP*, kas var piedāvāt bezvadu tīkla pakalpojumus, apkārtne atrodas un kādi ir to parametri. Ierīcei, iespējams, būs jāizveido pieejamo *AP* saraksts, kas nodrošina konkrētu *SSID*. Klienta ierīce var meklēt bezvadu piekļuves punktus, veicot skenēšanas operāciju divos veidos.

Pasīvā skenēšana – klienta ierīce klausās apraides bāksignālu (angļu val. *Beacon*) kadrus, kurus ar intervālu 100 ms izsūta apkārt esošie *AP*. *BSS* bāksignālu kadri satur tādu informāciju, kā to *BSSID* un piedāvātie *SSID*, kā arī atbalstītie datu pārraides ātrumi. Klienta ierīcei ir jānogaida šāds laika intervāls, lai uztvertu kārtējos bāksignālus. Tas arī ir viens no lielākajiem pasīvās skenēšanas trūkumiem, jo šis gaidīšanas laiks var būt pietiekami ilgs laika kritiskās

situācijās. Turklāt uztvertie AP bāksignāli var neietvert vajadzīgos SSID nosaukumus, tādējādi tiek tērēts laiks, tos izskatot.

Aktīvā skenēšana – ierīcei jāuzņemas aktīva loma un jāveic zondēšanas pieprasījumu (angļu val. *probe request*) kadru apraide, lai sasniegtu visus sasniedzamības zonā esošos AP, vai arī apzinātu konkrētus AP. Ierīcei šajos ziņojumos jāietver tāda informācija kā vajadzīgā SSID nosaukums un ierīces atbalstītie datu pārraides ātrumi. Kadri tiek izsūtīti visos frekvenču kanālos ar zemāko iespējamo datu pārraides ātrumu. Visiem AP, kas ir saņēmuši zondēšanas pieprasījumu ziņojumus, un kuri veiksmīgi ir izturējuši kadra pārbaudes secību (angļu val. *Frame Check Sequence – FCS*), kas norāda, ka kadrs nav bojāts [106], klienta ierīcei jāatbild ar uniraides zondēšanas atbildes (angļu val. *probe response*) kadriem, kas galvenokārt ietver bāksignāla informāciju [62]. Saņemot zondēšanas atbildes kadru, klients spēj noteikt signāla stiprumu, ar kādu šis ziņojums tika saņemts. Klients salīdzina no visiem AP saņemtos zondēšanas atbildes kadrus un pieņem lēmumu, ar kuru AP labāk asociēties. Mehānisms, ar kuru AP klientam vajadzētu asociēties, ir atstāts tīkla kartes ražotāja pārziņā, t. i., *IEEE 802.11* standartā šis mehānisms nav definēts. AP izvēles kritēriji galvenokārt ietvert tāds parametrs kā vajadzīgā SSID esamība, signāla stiprums, kā arī ražotāja iestrādātie papildu kritēriji [106].

Kamēr klients izpilda skenēšanas procedūru (aktīvā vai pasīvā), klients nevar saņemt datus no pašreizējā asociētā AP, kā arī nevar pārsūtīt datus, jo skenēšanas procedūra tiek izpildīta visos atļautajos frekvenču kanālos. Tas nozīmē, ka skenēšanas laikā klients maina frekvenču kanālus. Tas var izraisīt datu, kurus AP sūta klientam, pazaudēšanu un nepieciešamību atkārtoti tos pārsūtīt, kā arī klients var piedzīvot caurlaidspējas degradāciju [106].

Autentifikācijas process

Bezvadu tīkla klientu autentifikācijai var izmantot pirmskoplietošanas atslēgas (angļu val. *Pre-Shared Key – PSK*) autentifikāciju, *802.1X/EAP* (angļu val. *Extensible Authentication Protocol*) balstītu autentifikāciju, kā arī atvērtās sistēmas autentifikāciju (angļu val. *Open System Authentication – OSA*). Papildus var izmantot arī klienta radio MAC adreses autentifikāciju jeb MAC adrešu filtrāciju. Aktuālās autentifikācijas metodes detalizēti apskatītas šīs apakšnodaļas sadaļā “802.11 bezvadu tīklu drošība”.

Asociācijas process

802.11 asociācijas process ļauj AP sasaistīt tā loģisko portu jeb asociācijas identifikatoru (angļu val. *Association Identifier – AID*) ar bezvadu klienta staciju. *AID* unikāli identificē klienta ierīci kā AP asociēto klientu. *AID* ir klienta “dalībnieka karte”, kamēr klients paliek kā daļa no BSS. Asociācijas procesu iniciē bezvadu klienta ierīce ar asociācijas pieprasījuma (angļu val. *Association Request*) kadra palīdzību, kas satur informāciju par klienta funkcionālajām iespējām (angļu val. *capability*), piemēram, klausīšanās intervāls, izmantotais SSID nosaukums, atbalstāmo datu pārraides ātrumu un kanālu saraksts. Asociācijas procesu noslēdz AP, atbildot ar asociācijas atbildes (angļu val. *Association Response*) kadru. Asociācijas atbildes ziņojums vai nu atļauj veikt asociēšanās procesu, vai arī aizliedz to, aizlieguma gadījumā atbildē tiek norādīts iemesla kods. AP asociācijas atbildes ziņojums ietver tādu informāciju, kā statusa kods, asociācijas ID (*AID*) un atbalstītie datu pārraides ātrumi. Asociācijas ID parametra ideja ir līdzīga *Ethernet* komutatora fiziskajam portam (ligzdai).

Klienta ierīcei šī vērtība ir nepieciešama gadījumos, kad tā darbojas enerģijas taupīšanas režīmā. AP ar bāksignālu kadru palīdzību paziņo klientiem, kurā klientu AID buferatmiņā ir pienākuši tiem adresēti kadri [46], [106].

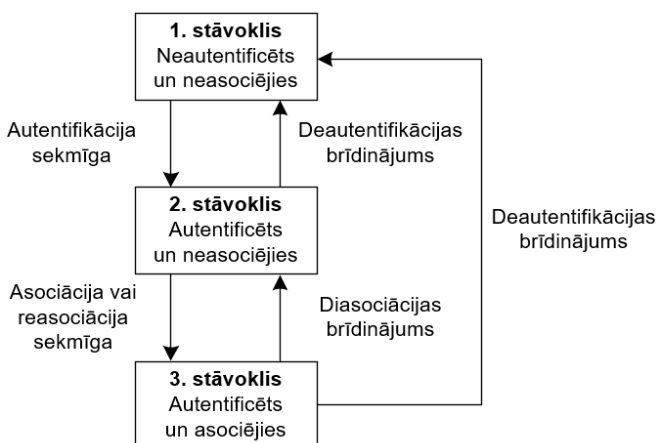
Diasociācijas process

Kad bezvadu ierīce kļūst par BSS klientu, tā saglabā savienojumu ar AP tik ilgi, kamēr tā netiek atvienota no tīkla. Klienta ierīce var tikt atvienota no AP, piemēram, ja tiek pārkāpta drošības politika, ja tā tiek atzīta par ļaunierīci (angļu val. *rogue device*) vai ja tās sesija pārāk ilgi atrodas dīkstāvē u. tml. Klienta ierīce var tikt atvienota no BSS, ja AP izsūta diasociācijas (angļu val. *Disassociation*) vai deautentifikācijas (angļu val. *Deauthentication*) kadru. Ja klients tiek diasociēts, tas zaudē tikai tā asociācijas statusu, taču joprojām paliek autentificēts. Lai klients atgrieztos atpakaļ BSS, tam vajag tikai reasociēties (angļu val. *reassociate*). Deautentifikācija ir nedaudz radikālāks process. Ja klients ir deautentificēts, tad ierīcei ir jāveic viss autentifikācijas un asociācijas process no jauna. Klienta ierīce var arī pati sevi atvienot no BSS, kad tas ir nepieciešams. Lai to izdarītu, klients brīdina AP, nosūtot tam deautentifikācijas kadru [46], [62].

Reasociācijas process

Reasociācijas (angļu val. *Reassociation*) pieprasījuma kadru izsūta klients, un tas ir gandrīz identisks asociācijas pieprasījuma kadrām, tikai papildināts ar pašreizējā AP adreses lauku. Galvenais šī kadra mērķis ir brīdināt jauno AP, ar kuru klients mēģina asociēties, ka tam vēl ir aktīva iepriekšējā asociācija. Tādējādi jaunais AP var jautāt vecajam AP, lai pārslēgšanās procedūrā esošā klienta buferētie (angļu val. *buffered*) kadri tiek retranslēti uz jauno AP. Jaunais AP atbild ar reasociācijas atbildes kadru, kas ir identisks asociācijas atbildes kadrām. Tā ir ražotāja izstrādāta specifiska implementācija, kas nav definēta IEEE 802.11 standarta specifikācijā [46], [106].

2.2. attēlā redzama IEEE 802.11 bezvadu tīkla mobilā klienta autentifikācijas un asociācijas iespējamo stāvokļu pārejas shēma [59].



2.2. att. Autentifikācijas un asociācijas stāvokļu pārejas shēma [59].

Gadījumā, ja klients fiziski pamet BSS, nonākot ārpus AP šūnas pārklājuma zonas, un par to nepaziņo AP, t. i., nenosūta tam deautentifikācijas kadru, AP šo faktu nepamanīs. Klients, arī

nepametot šūnu, var pāriet enerģijas taupīšanas režīmā un pārstāt komunicēt ar AP. Šajos gadījumos AP turpina apkalpot ierīces AID ierakstu katram gadījumam, ja nu tā tomēr atgriezīsies atpakaļ šūnā vai arī atgriezīsies no enerģijas taupīšanas režīma, taču tas tiek darīts tikai noteiktu laiku. Piemēram, Cisco bezvadu piekļuves punktus neaktīvo klientu apkalpošana tiks izbeigta pēc piecām minūtēm. Katram gadījumam, ja nu tomēr klients klausās (angļu val. *listening*), AP izsūta arī deautentifikācijas kadru [62].

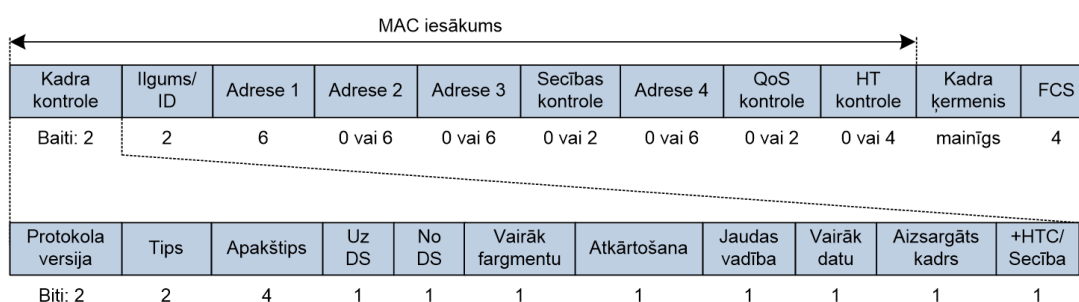
802.11 MAC kadrš

802.11 MAC kadra formāts

IEEE 802.11 standarts definē operācijas fizikālajā (fiziskajā) slānī un datu kanāla slāņa MAC apakšslānī. 2.3. attēlā redzams vispārējais MAC kadra formāts, kas ir paraugs visu IEEE 802.11-2016 standarta (tiks aizstāts ar IEEE 802.11-2020 standartu) operāciju kadriem. 2.3. attēlā atsevišķi parādīts arī kadra kontroles lauka formāts. Tehniskais apzīmējums 802.11 kadriem ir 802.11 MPDU (angļu val. *MAC Protocol Data Unit*) [67], [128].

Katrs 802.11 kadrs sastāv no vairākām komponentēm:

- MAC iesākums (angļu val. *header*), kas ietver tādus laukus kā “Kadra kontrole”, “Ilgums”, “Adrese”, “Secības kontroles informācija” (neobligāts), “QoS kontroles informācija” (neobligāts, lieto tikai QoS datu kadriem) un “HT kontrole” (neobligāts, lieto tikai +HTC (angļu val. *High Throughput Control*) kadriem);
- mainīga lieluma “Kadra ķermenis”, kurā ir specifiska informācija, kas ir atkarīga no konkrētā kadra tipa un kadra apakštipa;
- “Kadra pārbaudes secība” (FCS) ietver 32-bitu ciklisko redundances pārbaudi (angļu val. *Cyclic-Redundancy Check – CRC*), kas tiek izmantota, lai apstiprinātu saņemtā kadra integritāti.



2.3. att. IEEE 802.11-2016 MAC kadra formāts [67].

Lauks “Kadra kontrole” identificē, piemēram, kadra tipu un kadra ceļošanas virzienu, kā tas tiek sūtīts no vienas ierīces uz citu. Lauka “Kadra kontrole” pirmie trīs apakšlauki ir “Protokola versija”, “Tips” un “Apakštips”. Atlikušie kadra kontroles apakšlauki ir atkarīgi no apakšlauka “Tips” un “Apakštips” vērtībām. Ja apakšlauks “Tips” nav vienāds ar 1 vai apakšlauka “Apakštips” vērtība nav vienāda ar 6, tad atlikušie lauka “Kadra kontrole” apakšlauki ir “Uz DS”, “No DS”, “Vairāk fragmentu”, “Atkārtošana”, “Jaudas vadība”, “Vairāk datu”, “Aizsargāts kadrs” un “+HTC/Secība”. Ja apakšlauks “Tips” ir vienāds ar 1 un apakšlauka “Apakštips” vērtība ir vienāda ar 6, tad lauku “Uz DS”, “No DS”, “Vairāk fragmentu”, “Atkārtošana” vietā tiek formēts apakšlauks “Kontroles kadra paplašinājums”

(angļu val. *Control Frame Extension*) un pārējie lauki paliek tādi paši, kā pirmajā gadījumā. Apakšlaukā “Kontroles kadra paplašinājums” pieejamie 4 biti tiek izmantoti, lai palielinātu apakšlauka “Apakštips” telpu, lai definētu papildu kontroles kadrus [49], [62], [67].

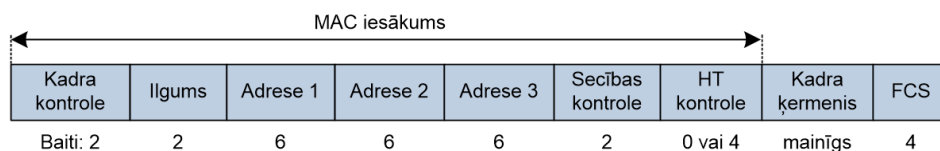
802.11 MAC kadru tipi

IEEE 802.11 standarts definē trīs dažādus kadru tipus: vadības; kontroles; datu. Katram kadra tipam ir deleģēti savi veicamie uzdevumi, tie nodrošina: vadības, kontroles un datu apmaiņas funkcijas starp bezvadu klientu stacijām un bezvadu piekļuves punktiem. *802.11* kadra tips tiek identificēts pēc kadra iesākuma lauka “Kadra kontrole” 2 bitu apakšlauka “Tips” un 4 bitu apakšlauka “Apakštips” (2.3. att.). Tas nozīmē, ka katrs no trīs kadru tipiem var ietvert vairākus apakštipes, kas paredzēti dažādu funkciju nodrošināšanai. Pēc vadības kadru apskata, tiks apskatīts vadības kadra apakštips “Darbība”.

Vadības kadri

Vadības kadri (angļu val. *Management frames*) tiek izmantoti, lai organizētu *WLAN* savienojamību, autentifikāciju un asociācijas statusu. Tie tiek izmantoti, lai sludinātu *BSS* un tā funkcionālās iespējas, vadītu klientus, kā tie pievienojas vai atstāj *BSS*. Piemēram, *802.11ac* vadības kadri ietver ļoti lielas caurlaidspējas (*VHT*) funkcionālās iespējas, tādas kā frekvenču kanāla platums, aizsargintervāls, staru formēšana (angļu val. *beamforming*) un modulācijas un kodēšanas shēmas (angļu val. *Modulation and Coding Scheme – MCS*) atbalsts. Vispirms klientam ir jānosaka kandidāta *BSS*, pie kura pievienoties, jāautentificējas ar *AP* un jāasociējas ar *BSS*. Kopumā ir definēti 14 dažādi vadības kadra apakštipi un galvenie no tiem ir: “Bāksignāls”, “Zondēšana” (angļu val. *Probe*), “Autentifikācija” un “Deautentifikācija”, “Asociācija”, “Diasociācija” un “Reasociācija”, “Darbība” (angļu val. *Action*) [49], [62]. *AP* vienmēr izsūta apraides (angļu val. *broadcast*) vadības kadrus, izmantojot zemāko obligāto datu pārraides ātrumu (angļu val. *mandatory rate* vai *802.11 BSS basic rate*), kas nodrošina labāku *SNR* vērtību un līdz ar to ļauj palielināt apraides zonu, lai droši sasniegtu un vadītu *BSS* robežās esošos klientus.

IEEE 802.11-2016 standartā (tiks aizstāts ar *IEEE 802.11-2020* standartu) definētais vadības kadra formāts redzams 2.4. attēlā. Lauki “Kadra kontrole”, “Ilgums”, “Adrese 1”, “Adrese 2”, “Adrese 3”, “Secības kontrole”, “HT kontrole”, “Kadra ķermenis” un “FCS” ir ietverti visos vadības kadru apakštipos [67].



2.4. att. *IEEE 802.11-2016* vadības kadra formāts [67].

IEEE 802.11 standartā vadības kadra apakštips “Darbība” jeb darbības kadrs (angļu val. *Action frame*) tika ieviests, lai ļautu pievienot vairāk kadru tipus saistībā ar ierobežotām iespējām definēt papildu vadības kadru apakštipes. Vadības kadriem (2.4. att.) ar apakštipes “Darbība” lauks “Kadra ķermenis” ietver kodus, kas identificē dažādus kadru formātus, kas atbalsta atšķirīgas funkcijas, piemēram, *QoS* un lielas caurlaidspējas operācijas [49]. Darbības kadrus izmanto, lai iniciētu specifiskas izpildes operācijas *BSS* šūnā [128].

Darbības kadri nodrošina paplašinātas vadības kadru iespējas. Piemēram, *IEEE 802.11k* papildinājumā bezvadu tīkla klienta stacija var izmantot darbības kadrus, lai pieprasītu radio mērījumu informāciju no citām bezvadu tīkla ierīcēm, kā arī pārskatu (angļu val. *report*) par kaimiņu *AP*, lai daudz efektīvāk pieņemtu pārslēgšanās procedūras lēmumus. *IEEE 802.11v* standarts var izmantot darbības kadrus, lai realizētu tīkla asistētu enerģijas taupīšanu, kā arī veiktu citas darbības, kas saistītas ar pārslēgšanās procedūras optimizāciju. *802.11y* papildinājums izmanto darbības kadrus, lai atļautu *AP* paziņot tā asociētajiem klientiem par gaidāmo kanāla maiņu vai kanāla joslas platuma izmaiņām [62].

Kontroles kadri

Kontroles kadrus (angļu val. *Control frames*) izmantoto pie *802.11* datu kadru apmaiņas. Kontroles kadri tiek izmantoti, lai nodrošinātu kontroli un palīdzētu piegādāt datus izmantojot datu kanālu. Kontroles kadrus ir tikai kadra iesākuma informācija bez lietderīgajiem datiem (angļu val. *payload*). Kopumā ir definēti deviņi dažādi kontroles kadru apakštipi un galvenie no tiem ir: *ACK*, *Block ACK*, *PS-Poll* un *RTS/CTS* [49], [62].

Datu kadri

Datu kadri (angļu val. *Data frames*) nodrošina datu pārsūtīšanu no klienta uz klientu. Datu kadrus ir līdz pat četriem adrešu laukiem, kas identificē sūtītāju un saņēmēju un kas identificē *BSSID* un iesaistīto bezvadu posmu, kas ir saistīts ar kadra pārsūtīšanu. *IEEE 802.11* standarts definē 15 dažādus datu kadru apakštipus [49], [62].

802.11 bezvadu tīklu drošība

Drošība bezvadu *LAN* tīklos sastāv no lietotāju autentifikācijas un pārraidīto datu šifrēšanas (angļu val. *encryption*) risinājumiem. Bezvadu tīklu drošība tiek konfigurēta atsevišķi katram *WLAN SSID*. Pārskatā netiek apskatīti *WPA* pirmās versijas drošības mehānismi.

Šifrēšana

Datu šifrēšanu ir iespējams ieviest gan *L2*, gan *L3* slānī vai arī abos slāņos vienlaikus. *L2* slāņa datu šifrēšana ir paredzēta starp klientu un *AP*. Piemēram, šobrīd aktīvi tiek izmantots *CCMP* (angļu val. *Counter/CBC-MAC Protocol*) algoritms, kas ir bāzēts *AES* (angļu val. *Advanced Encryption Standard*) šifrēšanas standartā. *L3* slāņa datu šifrēšana nodrošina datu aizsardzību starp klienta iekārtu un lietojuma serveri. *L3* slāņa datu šifrēšana parasti tiek realizēta, izmantojot virtuālo privāto tīklu (angļu val. *VPN – Virtual Private Network*), piemēram, *IPsec VPN* [35], [49].

Atvērtās sistēmas autentifikācija

Atvērtās sistēmas autentifikācija (*OSA*) nodrošina brīvu piekļuvi *WLAN*. Vienīgā prasība, kas bezvadu tīkla klientam ir jāizpilda: klientam nepieciešams noformēt un nosūtīt *802.11* autentifikācijas pieprasījumu (angļu val. *Authentication Request*) uz *AP* (vai arī uz bezvadu tīkla kontrolieri), pirms klients mēģina asociēties ar to. *AP* atbild ar autentifikācijas atbildes (angļu val. *Authentication Response*) ziņojumu. Citi akreditācijas dati (angļu val. *credentials*)

nav nepieciešami. Atvērtās sistēmas autentifikācija ir nulles autentifikācijas algoritms. Pēc atvērtās autentifikācijas un asociācijas procesa pabeigšanas klients var sākt pārraidīt un saņemt datus. Atvērtās sistēmas autentifikācijas risinājums ļauj iekārtām ātri iegūt piekļuvi bezvadu tīklam, kur klienta dati tiek sūtīti nešifrētā veidā [106], [166].

WPA2 drošības standarts

Wi-Fi alianses (angļu val. *Wi-Fi Alliance*) izstrādātajā WPA2 (angļu val. *Wi-Fi Protected Access*) versijā, pilnā apmērā ir iekļauts *IEEE 802.11i* standarts, kas specificē drošības mehānismus bezvadu tīklos, kā tiek piegādātas atslēgas, kas būtībā ir šifrēšanas atslēgu ģenerēšanas un apmaiņas mehānisms [46], [106]. WPA2 specificē *802.1X* (angļu val. *Dot1x*) porta bāzētas piekļuves kontroles standartu, kas savukārt ietver *EAP* bāzētu lietotāju autentifikācijas ietvaru, taču tas nenorāda konkrētu autentifikācijas metodi, kas būtu jāizmanto. Izmantojot WPA2 aizsardzības mehānismu, var tikt nodrošināta droša klienta pieslēgšanās *IEEE 802.11* bezvadu tīklam [40]. WPA2 izmanto *CCMP* algoritmu, kas kopā ar iekļauto *AES* šifrēšanas standartu nodrošina datu privātumu un datu integritāti. Tādējādi WPA2 ir drošības mehānisms, kas specificē klientu autentifikācijas, datu šifrēšanas un datu integritātes metodes. Atkarībā no bezvadu tīkla mēroga un nozīmes var tikt izmantoti šādi WPA2 atbalstīti drošības režīmi [35], [114]:

- *WPA2-Personal* (WPA2-PSK) jeb personālais režīms – izmanto pirmskoplietošanas atslēgu (PSK);
- *WPA2-Enterprise* (WPA2-802.1X) jeb uzņēmuma režīms – izmanto *802.1X/EAP* autentifikāciju [132].

Šobrīd *IEEE 802.11* tīklos galvenokārt tiek izmantota WPA2 versija, lai arī jau ir pieejama WPA3 versija [35], [40], [181], kas nodrošina vēl augstāku drošības līmeni, tomēr pagaidām tā netiek plaši izmantota, jo lielākā daļa esošo bezvadu tīklu un arī galiekārtu šo jauno drošības standartu neatbalsta. Lai pārietu uz WPA3 versiju, ir jāveic pakāpeniska *IEEE 802.11* bezvadu tīklu modernizācija, kas prasa lielas investīcijas uzņēmuma klases tīklos.

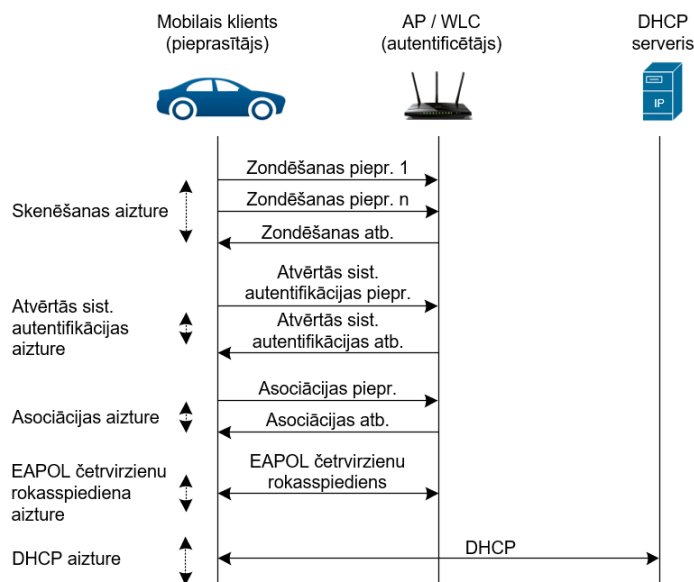
WPA2-PSK

Izmantojot PSK autentifikāciju, bezvadu tīkla klients tiek autentificēts lokāli bezvadu piekļuves punktā [40]. Tīklos ar WPA2-PSK katrā klienta ierīcē un katrā AP (vai arī WLC) ir jānokonfigurē frāzveida parole (angļu val. *passphrase*).

Pieslēgšanās pie *IEEE 802.11* BSS notiek, izejot cauri skenēšanas procesam, atvērtās sistēmas autentifikācijas, asociācijas un drošības fāzēm. Nonākot līdz drošības fāzei, tiek izpildīta četrpusīga jeb četrvirzienu rokasspiediena procedūra, kas atbild gan par lietotāja autentifikāciju, gan par datu šifrēšanu. Frāzveida parole tiek pārkonvertēta uz 256 bitu PSK atslēgu, izmantojot speciālu algoritmu. Iegūtā PSK atslēga visiem lietotājiem ir vienāda. Tā vietā, lai klients uz AP sūtītu pirmskoplietošanas atslēgu (PSK), tiek izpildīta *EAPOL* (angļu val. *Extensible Authentication Protocol over LAN*) ziņojumu apmaiņa, kuras mērķis ir apmainīties ar gala atslēgu izveidei nepieciešamo informāciju, kas nepieciešamas, lai nošifrētu uniraides jeb pāru (izmanto PTK (angļu val. *Pairwise Transient Key*) atslēgas), apraides vai multiraides trafiku (izmanto GTK (angļu val. *Group Temporal Key*) atslēgas) starp šīm ierīcēm

[35]. Savstarpēji tiek nosūtīti četri ziņojumi, kas tiek apstiprināti ar *ACK* kadriem. Tādējādi *PSK* atslēga nekad netiek pārsūtīta starp klientu un *AP*. Kad *EAPOL* procedūra veiksmīgi ir beigusies, starp *AP* un klientu ir notikusi abpusēja autentifikācija un var notikt šifrēta datu pārraide [40].

2.5. attēlā redzama pieslēgšanās procedūra *IEEE 802.11* tīklam ar nokonfigurētu *WPA2-Personal* drošības mehānismu, kas izmanto *PSK* autentifikācijas metodi [165], [167].



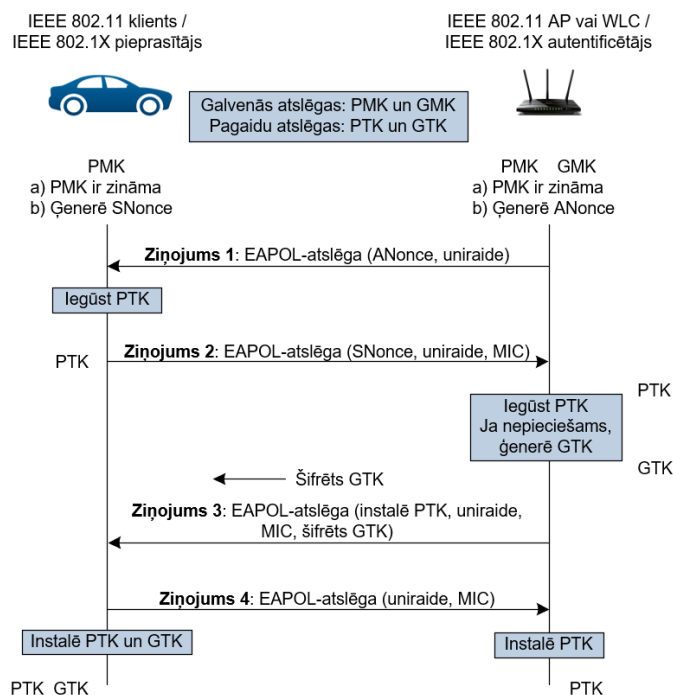
2.5. att. Pieslēgšanās pie *IEEE 802.11* infrastruktūras, izmantojot *PSK* autentifikācijas metodi.

***EAPOL* četrvirzienu rokasspiediena procedūra**

IEEE 802.11i autentifikācijas protokola specifikācijas procedūru, kas ir paredzēta šifrēšanas atslēgu ģenerēšanai, sauc par *EAPOL* četrvirzienu rokasspiedienu (angļu val. *four-way handshake*), vienlaikus tā pilda arī abpusējas (angļu val. *mutual*) autentifikācijas funkciju [40], [106].

2.6. attēlā redzama *EAPOL* četrvirzienu rokasspiediena (sasveicināšanās) procedūra *IEEE 802.11* tīklos [35], [67], kas ir aktuāla gan *WPA2-Personal*, gan *WPA2-Enterprise* drošības shēmām. Klients un *AP* apmainās ar četriem *EAPOL* ziņojumiem. *PSK* gadījumā pāra galvenā atslēga (angļu val. *Pairwise Master Key – PMK*) tiek iegūta no *PSK* atslēgas. Savukārt *802.1X/EAP* gadījumā *PMK* tiek iegūta *EAP* autentifikācijas procesa ietvaros, kur vispirms tiek izveidota galvenā sesijas atslēga (angļu val. *Master Session Key – MSK*), kas tālāk tiek izmantota, lai uzģenerētu *PMK* atslēgu.

Gan *WPA2-Personal*, gan *WPA2-Enterprise* autentifikācijas mehānisma gadījumā pāra pārejas atslēgas (*PTK*) iegūšanai tiek izmantota pseido gadījuma funkcija (angļu val. *Pseudo-Random Function – PRF*), kas apvieno *PMK* ar *AP* un klienta radio *MAC* adresēm un gadījumskaitļiem (angļu val. *Nonces*), tādēļ iegūtās atslēgas pāra robežās ir unikālas. Iegūto *PTK* atslēgu klienta stacija un *AP* izmanto, lai šifrētu un atšifrētu uniraides *802.11* datu kadrus [35], [165]. Atkarībā no *WLAN* tīkla arhitektūras un ražotāja drošības risinājuma realizācijas klienta trafika šifrēšana un atšifrēšana var notikt uz *AP* vai *WLC* [35]. Parasti klienta dati tiek šifrēti starp klientu un *AP*.



2.6. att. *EAPOL* četrvirzienu rokasspiediena procedūra *IEEE 802.11* tīklos [35].

Kad klienta radio veic pārslēgšanās procedūru, t. i., pārslēdzas uz citu *AP*, četrvirzienu rokasspiediena procedūra tiek izpildīta vēlreiz, taču jau ar citiem parametriem (piemēram, jaunā *AP* *MAC* adrese un citi gadījumskaitļi). Rezultātā aktuālā šifrēšanas atslēga katru reizi mainās, mobilajam klientam pārvietojoties starp *AP* (2.6. att.) [49].

802.1X/EAP autentifikācija

802.1X porta bāzētas piekļuves kontroles standarts limitē piekļuvi tīkla videi līdz brīdim, kamēr klients autentificējas. Tas nozīmē, ka bezvadu tīkla klients var asociēties ar *AP*, taču nevar sūtīt datus tīklā, kamēr nebūs pabeidzis autentifikācijas procedūru [62]. *EAP* nodrošina elastīgu autentifikācijas ietvaru, kas atbalsta vairākas autentifikācijas metodes, izmantojamā metode tiek noskaidrota pārrunu ceļā, un tā ir nepieciešama, lai savstarpēji autentificētos klients jeb pieprasītājs (angļu val. *supplicant*) un autentifikācijas serveris. *EAP* ziņojumi starp pieprasītāju un autentificētāju (angļu val. *authenticator*) tiek sūtīti datu kanāla slānī (*L2*), izmantojot *EAPOL* enkapsulāciju, kas ir definēta *802.1X* standartā. Autentificētājam no *EAPOL* kadra “jāizvelk” (angļu val. *extract*) *EAP* lietderīgie dati, tālāk tie ir jāiekapsulē *RADIUS* paketē un jāpārsūta uz autentifikācijas serveri [2]. Izmantojot *802.1X*, nepieciešams izvēlēties atbilstošu *EAP* metodi, piemēram, *EAP-TLS* (angļu val. *EAP-Transport Layer Security*), *EAP-MSCHAPv2* (angļu val. *EAP-Microsoft Challenge Authentication Protocol version 2*) [40], kas definē autentifikācijas procedūru [49].

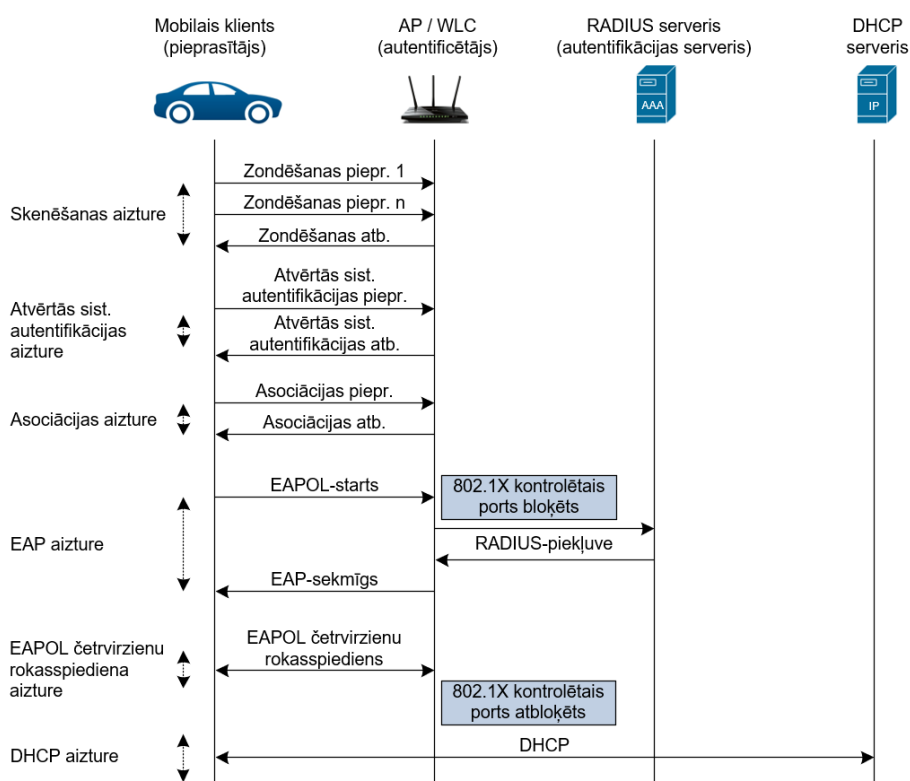
Ja tiek izmantots *802.1X* mehānisms, tad vispirms klients izmanto atvērto autentifikācijas metodi, lai asociētos ar *AP*, un pēc tam sākas faktiskais autentifikācijas process, iesaistot autentifikācijas serveri [62].

802.11 autentificētājs (*AP* vai *WLC*) izveido loģisku *802.1X* portu katrai bezvadu klienta ierīcei, balstoties uz klienta asociācijas *ID (AID)*. Loģiskais *802.1X* ports sastāv no nekontrolētā porta (angļu val. *uncontrolled port*) un kontrolētā porta (angļu val. *controlled port*).

Nekontrolētais ports ir paredzēts klienta *802.1X* autentifikācijas kadru apmaiņai, savukārt uz kontrolēto portu tiek novirzīti klienta datu kadri. *802.11* bezvadu tīklā kontrolētais ports ir bloķēts visa *EAP* autentifikācijas procesa laikā [106].

Bezvadu tīklā klienta galiekārta iniciē autentifikācijas procesu, nosūtot autentificētājam *EAPOL-starts* (angļu val. *EAPOL-Start*) ziņojumu. Bieži vien *RADIUS* serveri tiek saukti arī par AAA (angļu val. *Authentication, Authorization and Accounting*) serveriem, jo liela daļa no tiem nodrošina šo trīs pakalpojumu funkcijas [35]. *RADIUS* serveris var izmantot arī ārējo datubāzi, lai autentificētu bezvadu lietotājus, piemēram, *Microsoft Active Directory*, kas ir bāzēta uz *LDAP* (angļu val. *Lightweight Directory Access Protocol*) [35]. Autentifikācijas serveris apstrādā lietotāja jeb klienta akreditācijas datus, apstiprina galiekārtas identitāti un atļauj vai aizliedz piekļuvi bezvadu tīklam, balstoties uz lietotāju datubāzi un piemērotajām politikām. Pēc tam autentifikācijas serveris autentificētājam nodod autorizācijas rezultātus, kas atļauj vai aizliedz atvērt vajadzīgos portus. *EAP* identificēšana un autentifikācija notiek tikai starp galiekārtu un autentifikācijas serveri. Autentificētājs (*AP* vai *WLC*) nav informēts, kāda *EAP* metode tiek izmantota, tādējādi *EAP* autentifikācija ir pilnībā caurspīdīga autentificētājam.

Kad autentifikācijas serveris sūta atpakaļ *RADIUS* piekļuves apstiprināšanas ziņojumu ar iekapsulētu ziņojumu *EAP-sekmīgs* (angļu val. *EAP-Success*), tad *802.1X* autentifikācijas process ir veiksmīgi pabeigts un klients tiek autorizēts [40]. Kad četrvirzienu rokasspiediena procedūra ir veiksmīgi pabeigta, tad kontrolētais ports tiek atbloķēts un dati jau šifrētā veidā tiek pārsūtīti caur to.



2.7. att. Pieslēgšanās pie *IEEE 802.11* infrastruktūras, izmantojot *802.1X/EAP* autentifikācijas mehānismu.

2.7. attēlā redzama pieslēgšanās procedūra pie *IEEE 802.11* infrastruktūras ar nokonfigurētu *WPA2-Enterprise* drošības mehānismu, kas izmanto *802.1X/EAP* autentifikācijas mehānismu [35], [54], [67], [114], [168].

Jāatzīmē, ka *IEEE 802.11* savienojuma izveidē katrs procedūras solis (2.5. un 2.7. att.) ienes savu aizturi. Tas attiecas arī uz izmantoto drošības mehānismu [132].

Pārslēgšanās procedūras apskats

Pastāv divu veidu pārslēgšanās procedūras – homogēnā (horizontālā) pārslēgšanās un heterogēnā (vertikālā) pārslēgšanās. Viendabīgā jeb horizontālā pārslēgšanās procedūra notiek viena piekļuves tīkla robežās, piemēram, *IEEE 802.11*. Tādējādi mobilitāte ir ierobežota un atbilst tīkla mērogam. Heterogēnā jeb vertikālā pārslēgšanās procedūra notiek starp dažādām tīkla piekļuves tehnoloģijām, piemēram, no *IEEE 802.11* uz *LTE* un otrādi [32]. Promocijas darbā tiek pētīta horizontālā pārslēgšanās procedūra.

Terminiem “pārslēgšanās procedūra” jeb “pārtvere” (angļu val. *handover*), “nodošana” (angļu val. *handoff*), “viesabonēšana” (angļu val. *roaming*) vai “BSS pāreja” (angļu val. *BSS transition*) *WLAN* tīklos ir viena un tā pati nozīme, tie apraksta procedūru, kad tiek mainīta mobilā klienta piesaiste no viena *AP* uz citu, t. i., mobilajam klientam pārvietojoties no vienas *AP* šūnas uz citu [20], [158].

Atkarībā no *WLAN* arhitektūras, pārslēgšanās procedūru var iedalīt: pārslēgšanās starp autonomiem *AP*; *WLC* bāzēta pārslēgšanās; izkliedētas *WLAN* arhitektūras pārslēgšanās [35]. Savukārt *WLC* bāzēta pārslēgšanās procedūra tiek iedalīta: iekšējā viena kontroliera (angļu val. *intracontroller*) pārslēgšanās procedūrā un starpkontrolieru (angļu val. *intercontroller*) pārslēgšanās procedūrā [40].

IEEE 802.11 ir *L1* fiziskā interfeisa un *L2* datu pārraides kanāla slāņa tehnoloģija [106]. Izšķir *L2* jeb *MAC* līmeņa un *L3* jeb *IP* līmeņa pārslēgšanās procedūras. Promocijas darbā pētīta *L2* slāņa pārslēgšanās procedūra. *L2* un *L3* pārslēgšanās procedūras var tikt realizētas gan ar autonomiem *AP*, gan izmantojot bezvadu tīkla kontrolierus (*WLC*).

L2 pārslēgšanās procedūras gadījumā mobilais klients izmanto vienu un to pašu *IP* apakštīklu, kas ir piesaistīts pie konkrēta *VLAN* (angļu val. *Virtual Local Area Network*). Pēc pārslēgšanās klients var turpināt izmantot to pašu *IP* adresi, un tādējādi pārslēgšanās procedūra ir salīdzinoši ātra. *L2* starpkontrolieru pārslēgšanās procedūras laikā, kad klients izlemj pārslēgties uz citu *AP*, ko apkalpo cits *WLC*, klients reasociējas ar jauno *AP*. Tādējādi klients pārvietojas no oriģinālā (sākotnējā) *WLC* uz jauno *WLC*, un kontrolieri savā starpā nokoordinē pāreju.

L3 pārslēgšanās procedūras gadījumā klients pārvietojas starp *IP* apakštīkliem (tiek izmantoti dažādi *VLAN*). Pārejot no viena *IP* apakštīkla uz citu, klientam jāsažinās ar *DHCP* serveri un jāpieprasa jaunā apakštīkla *IP* adrese. Šī procedūra var būt laikietilpīga. Lai pārslēgšanās procedūra būtu efektīva, laiku taupoša un tādējādi vienkārša, būtu jāizvairās no jaunas *DHCP* procedūras aktivizēšanas [40]. Ja *L3* pārslēgšanās procedūra notiek starp diviem *WLC*, var tikt izmantota mobilā *IP* protokola (angļu val. *Mobile IP – MIP*) ideja [101], kur starp sākotnējo *WLC* un jauno *WLC* tiek izveidots speciāls datu tunelis [149]. Caur šo datu tuneli tiek

translēts oriģinālā kontroliera *IP* apakštīkls, un tādējādi tiek saglabāta asociācija ar oriģinālo kontrolieri. Pārslēgšanās procedūras laikā visi dati uz un no klienta bez sesijas pārtraukšanas tiek pārsūtīti caur šo tuneli [62].

IEEE 802.11 MAC protokols atbalsta *L2* pārslēgšanās procedūru, un tā ir realizēta pēc principa “pārtrauc, pirms izveido” (angļu val. *break before make*). Pašos pamatos pārslēgšanās procedūra daudz neatšķiras no 2.5. un 2.7. att. redzamajiem mobilā klienta pieslēgšanās mehānismiem *IEEE 802.11* infrastruktūrai, izņemot to, ka klients izpilda pārslēgšanās procedūru, kamēr tas ir aktīvi asociējies ar citu *BSS*. *IEEE 802.11* standarts nosaka, ka klienta mobilā ierīce vienlaikus apkalpo tās asociāciju tikai ar vienu *AP*. Tādēļ vispirms ir jāveic diasociācija ar esošo *AP*, pirms tiek izveidota asociācija ar jaunu *AP* [106]. Pārslēgšanās procedūra ir asociācijas pārvietošanas process no viena *AP* uz nākamo, uzturot bezvadu savienojumu, kamēr mobilais objekts pārvietojas. Pārslēgšanās procedūra (2.5., 2.7. att.) ietver vairākus apakšprocesus: zondēšanu (angļu val. *probing*); atvērtās sistēmas autentifikāciju; asociāciju (vai reasociāciju); *WPA2* autentifikāciju un datu šifrēšanu; *DHCP* procedūru [26], [39], [62].

Pārslēgšanās procedūra var tikt realizēta, saglabājot vai arī nesaglabājot klienta *IP* adresi. Gadījumu, kad pēc pārslēgšanās procedūras izpildes uz citu *AP* tiek saglabāta klienta *IP* adrese, sauc par vienlaidu jeb nemanāmo pārslēgšanās procedūru (angļu val. *seamless handover*) [106]. Lai varētu veikt vienlaidu pārslēgšanos starp *BSS*, mobilajam klientam vispirms nepieciešams piefiksēt, ka tas atrodas pie *Wi-Fi* šūnas robežas un tam ir nepieciešams atrast citu potenciālo šūnu vai kandidātšūnas, lai tālāk organizētu pārslēgšanos, pirms tiek pazaudēts signāls pilnībā [49]. Vienlaidu pārslēgšanās procedūra īpaši svarīga ir laika kritiskām aplikācijām, piemēram, balss trafikam [62].

Klienta izmantotās lietojumprogrammas darbības veids tieši korelē ar tās elastīgumu pārslēgšanās procedūras laikā. Lietojumprogrammas, kuru pamatā ir *TCP* protokols, ir vairāk tolerantas uz pakešu zudumiem, kas rodas pārslēgšanās laikā starp *AP*, jo *TCP* ir uzticams un uz savienojumu orientēts (angl. *connection-oriented*) protokols. *TCP* ir nepieciešami pozitīvi apstiprinājumi par ziņojumu saņemšanu, tāpat kā par *802.11 MAC* kadriem [46], [137]. Augstāka slāņa protokols *TCP* spēj atklāt pārslēgšanās procedūras laikā pazaudētos *802.11* datus (paketes) un veikt to atkārtotu pārsūtīšanu. *TCP* protokolu izmanto, piemēram, *FTP*, *HTTP*, *SMTP* un *SSH* protokoli. Tomēr daļa lietojumprogrammu balstās uz *UDP* protokolu, kas tāpat kā *TCP* ir *L4* transporta protokols. *UDP* ir zema virstēriņa, bezsavienojuma (angļu val. *connectionless*) protokols. Tas nozīmē, ka pazaudētie dati netiek pārsūtīti. Tādējādi pārslēgšanās procedūras laikā pazaudētie dati var atstāt ievērojamu ietekmi uz *UDP* bāzētiem lietojumiem. *UDP* kā transporta protokolu izmanto tādi protokoli kā *TFTP*, *SNMP*, *DHCP*, *DNS* u. c. *UDP* protokolu izmanto arī *VoIP* (angļu val. *Voice over IP*) un video pakalpojumi [20], [122].

Bezvadu piekļuves punkti atrodas vienotā pārslēgšanās domēnā (angļu val. *roaming domain*), ja tiem ir viens un tas pats apraides domēns (angļu val. *broadcast domain*), t. i., kopīgs *IP* apakštīkls, un tiem ir nokonfigurēts vienāds *SSID*. Pārslēgšanās domēnu var attiecināt arī uz *ESS*, kas ir vairāku *BSS (AP)* apvienošana, izmantojot *DS*. Mobilais klients, kurš veic pārslēgšanās procedūru, pārvietojoties pārslēgšanās domēna robežās, var uzturēt lietojuma

savienojamību tik ilgi, kamēr nemainās tā *IP* adrese. Ja klients pārvietojas no viena pārslēgšanās domēna (*IP* apakštīkla) uz citu, klienta ierīcei nomainās *IP* adrese, un tā rezultātā klienta ierīce izbeidz (angļu val. *drop*) visas aktīvās lietojuma sesijas [106].

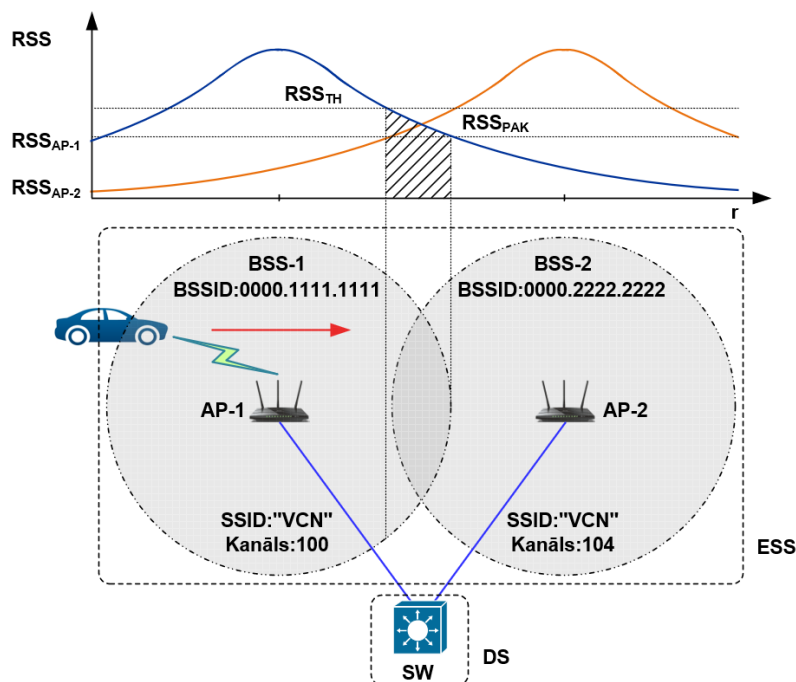
Lēmumu pārslēgties uz citu *AP* pieņem bezvadu tīkla klienta iekārta nevis bezvadu tīkla infrastruktūra. Lēmumu, tieši kurā brīdī veikt pārslēgšanos, mobilais klients pieņem, balstoties uz vairākiem nosacījumiem, galvenokārt tie ir: aktuālā savienojuma ietvaros uztvertais *RSS* signāla jaudas līmenis; *SNR*; pazaudēto *AP* bāksignālu ziņojumu skaits; pārraides kļūdas. Mehānisms, kas mobilajam klientam nosaka, kurā brīdī veikt pārslēgšanos uz citu *AP*, tāpat kā *AP* izvēles mehānisms, nav definēts *IEEE 802.11* specifikācijā, tas ir atstāts katra ražotāja pārziņā. Tādējādi aparātūras ražotāji sacenšas savā starpā, lai izstrādātu labākus un veikspējīgākus algoritmus [62], [106]. Katra pārslēgšanās procedūras risinājuma mērķis ir paātrināt pārslēgšanās procedūru, kas ļautu maksimāli samazināt pārslēgšanās procedūras aizturi (angļu val. *handover delay* vai *roaming duration*), nodrošinot savienojamību.

Nepieciešamība pēc efektīva pārslēgšanās procedūras algoritma īpaši aktuāla kļūst tad, kad bezvadu tīklā tiek izmantoti laika kritiski lietojumi un klienta pārvietošanās ātrumi ir pietiekami lieli (sākot no 20 km/h). *Wi-Fi* balss sakariem (apzīmē kā *VoWi-Fi* vai *VoWLAN*) ir nepieciešams patstāvīgs savienojums tā, lai balss plūsma netiktu izkropļota vai pārtraukta. Pārslēgšanās procedūras laikā var būt īss laika moments, kad klients nav pilnībā asociējies ar kādu *AP*. Samazinot šo laiku līdz minimumam, galiekārtas klients pat var nenojaust, ka ir notikusi pārslēgšanās starp *AP*.

Pārslēgšanās procedūra starp BSS

Mobilais klients (klienta stacija), pārvietojoties *ESS* robežās (2.8. att.) no vienas *BSS* uz citu, izpilda pārslēgšanās procedūru starp bezvadu piekļuves punktiem (*AP*). Mobilais klients nepārtraukti novērtē bezvadu savienojuma kvalitāti. 2.8. attēlā redzami divi *AP*, kas izplata vienu un to pašu *SSID*. *AP* savā starpā ir savienoti, izmantojot *DS* infrastruktūru un *IEEE 802.3 Ethernet* savienojumus. Katrs *AP* izmanto savu frekvenču kanālu, kas savā starpā nepārklājas (angļu val. *non-overlapping channels*). Tas nepieciešams, lai izvairītos no kopkanāla (angļu val. *co-channel*) un blakus esošo kanālu (angļu val. *adjacent channel*) interferences [34], [49], [62]. Mobilais klients vispirms asociējas ar *AP-1* (2.5., 2.7. att.). Ja abi *AP* strādā autonomā režīmā, tad katrs no tiem uztur savu asociēto klientu tabulu. Tālāk klients pārvietojas *AP-2* šūnas virzienā. Klientam attālinoties no *AP-1*, *RSS* signāls pavājinās. Tuvojoties *AP-1* robežai, mobilais klients, galvenokārt balstoties uz veiktajiem *RSS* un *SNR* mērījumiem, var pieņemt lēmumu par pārslēgšanās procedūras sākšanu. Šajā brīdī uztvertais signāla jaudas līmenis *RSS* ir sasniedzis definēto sliekšņvērtību (angļu val. *threshold – TH*) RSS_{TH} . *RSS* līknes iekrāsotā laukuma $RSS_{TH} - RSS_{PAK}$ (2.8. att.) robežās mobilajam klientam ir jāpaveic pārslēgšanās procedūra, t. i., kamēr klients vēl atrodas *AP-1* pārklājuma zonā un uztvertā signāla jaudas līmenis nav mazāks par datu pārraides pakalpojuma nepieciešamo minimālo vērtību RSS_{PAK} . Klients nekavējoties sāk jaunā *BSS* meklēšanu, uz kuru varētu pārslēgties (atkarībā no realizētā pārslēgšanās procedūras algoritma, skenēšanas procedūra var tikt izpildīta arī ātrāk, t. i., pirms tiek pieņemts lēmums par pārslēgšanās procedūras sākšanu) [106], [149]. Klients izsūta apraides zondēšanas pieprasījuma kadrus, lai noskaidrotu tuvumā esošos *AP*, kas var nodrošināt

prasīto *SSID*. *AP-2* saņem zondēšanas pieprasījuma kadru un atgriež zondēšanas atbildes ziņojumu, kas satur tā *BSSID* un *SSID* [62]. Citi apkārt esošie *AP* arī var dzirdēt zondēšanas pieprasījumus un atbildēt klientam ar savu zondēšanas atbildes ziņojumu. Klientam izvērtējot visus saņemtos zondēšanas atbildes ziņojumus, ir jāizlemj, kurš ir labākais *AP* kandidāts. Tālāk tas noformē un izsūta deautentifikācijas kadru *AP-1* un mēģina asociēties ar *AP-2*. Ja *ESS* infrastruktūra atbalsta reasociācijas kadrus, deautentifikācijas kadrs uz *AP-1* netiek sūtīts. Tā vietā klients nosūta reasociācijas pieprasījuma kadru uz *AP-2*, ko *AP-2* apstiprina ar *ACK* kadru. Pirms *AP-2* nosūta reasociācijas atbildes kadru klientam, *AP-2* caur *DS* infrastruktūru paziņo *AP-1* par gaidāmo asociāciju un pieprasa *AP-1* pārsūtīt visus šajā brīdī tā buferatmiņā esošos klienta datus uz *AP-2*. Kad klienta dati ir saņemti, *AP-2* atbild klientam ar reasociācijas atbildes kadru, klients atbild ar *ACK* kadru. Šajā brīdī ir nodibināta klienta asociācija ar *AP-2*, un tiek piegādāti visi klientam adresētie dati [35], [62].



2.8. att. Mobilā klienta pārvietošanās starp *AP* (*BSS*) šūnām.

Bezvadu tīkla infrastruktūras *AP*, kā arī iesaistītie komutatori atjauno savas *MAC* adrešu tabulas. *AP* atjauno savas asociēto klientu tabulas. Mobilajam klientam turpinot pārvietošanos bezvadu tīklā, līdzīgā veidā tiek izpildīta pārslēgšanās procedūra starp nākamajiem *ESS* bezvadu piekļuves punktiem.

Šāda *AP-AP* pārslēgšanās procedūras komunikācija (angļu val. *AP-to-AP handover*), kā rezultātā tiek pārsūtīti klientu dati no iepriekšējā *AP*, nav obligāta, jo tā nav definēta *IEEE 802.11* standartā, un tas ir katra ražotāja implementēts risinājums [35], [106]. Kontroliera bāzētas (centralizētas) *WLAN* arhitektūras gadījumā šāds *AP* savstarpējās komunikācijas mehānisms tiek realizēts ar *WLC* palīdzību [35].

Iesvītoto apgabalu starp RSS_{TH} un RSS_{PAK} (2.8. att.) sauc par *AP* pārslēgšanās procedūras apgabalu (angļu val. *roaming area*) [49]. Klienta atrašanās vieta šūnā, kad tiek veikta pāreja uz jaunu *AP*, tāpat kā parametra RSS_{TH} vērtība ir atkarīga no klienta ierīcē iestrādātā pārslēgšanās

procedūras algoritma. Parametra *RSS* vērtība konkrētā *BSS* šūnas lokācijā ir atkarīga no vairākiem parametriem, piemēram, *SNR* attiecības, izmantotās frekvenču joslas (2,4 GHz vai 5 GHz), attāluma līdz raidītājam un raidītāja jaudas.

Prasības kvalitatīvu sakaru nodrošināšanai *WLAN* tīklos

Signāla līmenis un pārklājums

Tipiskās *RSS* un *SNR* vērtības, kas jānodrošina *AP* pārslēgšanās procedūras apgabalā (uz šūnas robežas), tīkliem ar zemu klientu blīvumu (angļu val. *low-density*), kā arī datu pārraides lietojumiem attiecīgi ir -80 dBm *RSS* un aptuveni 20 dB *SNR* (rekomendē izmantot 2,4 GHz vai 5 GHz joslas), savukārt tīkliem ar augstu klientu blīvumu (angļu val. *high-density*), kā arī balss vai video pakalpojumiem attiecīgi ir vismaz -67 dBm *RSS* un aptuveni 33 dB *SNR* (rekomendē izmantot 5 GHz joslu) [47]. Ražotāja *Cisco* rekomendācija kvalitatīvu *Wi-Fi* balss sakaru nodrošināšanai paredz uz šūnas robežas nodrošināt vismaz -67 dBm stipru *RSS* signāla līmeni, un minimālajam *SNR* jābūt vismaz 25 dB, attiecīgi trokšņu līmenim nevajadzētu pārsniegt -92 dBm [148].

Pārslēgšanās procedūras optimālai nodrošināšanai tiek rekomendēta 10–15 % starpsūnu pārklāšanās (angļu val. *cell overlap*) vairumam datu aplikāciju un 15–20 % vai pat 30 % balss sakariem. Tas nepieciešams, lai mobilajam klientam garantētu stabilu pārklājumu arī pēc tam, kad *RSS* signāla līmenis ar asociēto *AP* nokrīt zem sliekšņvērtības RSS_{TH} un tiek aktivizēta pārslēgšanās procedūra [62], [172], [180]. Praksē drīzāk tiek realizēta pieeja, balstoties uz mērījumu, cik daudz *AP* ir redzami konkrētā dislokācijā. Tiek rekomendēts, ka balss klientam ir jābūt redzamiem un izmantojamiem (nozīmē – pietiekams *RSS* un *SNR*) vismaz diviem *AP* jebkurā vietā, kur reāllaika pakalpojuma saņēmēja ierīce varētu tikt izmantota [148].

Reāllaika pakalpojumi

Tādi reāllaika pakalpojumi kā tiešsaistes video un balss sakari (*VoWLAN*) ir vieni no jutīgākajiem pret ilgu pārslēgšanās procedūru. Abi pakalpojumi izmanto *UDP* transporta protokolu, un tiem ir izvirzītas augstas prasības, lai nodrošinātu nepieciešamo kvalitāti. *VoIP* sakaru ierīcēm nepieciešams izpildīt šādas minimālās veiktspējas prasības: pakešu zudums <1 %; kopējā vienvirziena aizture (angļu val. *one-way delay*) <150 ms [76], taču ņemot vērā pārslēgšanās procedūru starp *AP*, tiek rekomendēts nodrošināt vienvirziena aizturi <50 ms; trīce <30 ms [76] vai <50 ms [35]; pazaudēto pakešu skaits – ne vairāk kā trīs pēc kārtas [35]. Tādējādi balss datu paketes aprites laiks (angļu val. *RTT – Round Trip Time*) jeb aprites aizture (angļu val. *round trip delay*) nevar pārsniegt 300 ms [35]. Līdzīgas prasības ir arī tiešsaistes video pakalpojumiem [76].

Pārslēgšanās procedūras aizture

Pārslēgšanās procedūras aizture ir laiks, kas nepieciešams, lai izpildītu pārslēgšanās procedūru. Pārslēgšanās procedūra būtībā ir asociēšanās process, kas tika apskatīts iepriekš (2.5., 2.7. un 2.8. att.), un tas ir atkarīgs no zondēšanas, 802.11 autentifikācijas, 802.11 asociācijas un *WPA2* drošības procesa ilguma [106].

Vairāki *OSI* (angļu val. *Open System Interconnection*) modeļa slāņi rada aiztures pārslēgšanās procedūrā, piemēram, *L2*, *L3*, *L4*, *L7*. Katrs no šiem slāņiem ietver vairākas

pārslēgšanās procedūrai nepieciešamās operācijas [57]. Datu pārraides kanāla slānī (*L2*) starp skenēšanas, atvērtās sistēmas autentifikācijas un asociācijas procedūrām vislielāko papildinājumu pārslēgšanās procedūras aizturai rada tieši skenēšanas procedūra. Tā aizņem līdz pat 90 % no aiztures, ko rada šīs procedūras kopā [39]. Skenēšanas fāze var prasīt aptuveni 100 ms, atvērtās sistēmas autentifikācija aizņem aptuveni 2 ms, asociācijas process – aptuveni 20 ms. Ja tiek ņemta vērā WPA2 drošības mehānismu radītā aizture WLAN arhitektūrā, kur netiek izmantots WLC, tad kopējā *L2* aizture var sasniegt līdz pat 900 ms [39]. WPA2 autentifikācijas un datu šifrēšanas procedūra var aizņemt aptuveni 700 ms un *L3* pārslēgšanās procedūras aizture, ietverot *L2* aizturi, var sasniegt pat 4 s [39].

WLC bāzētos IEEE 802.11 bezvadu tīklos, kas atbalsta WPA2-PSK drošības mehānismu, parasti nav nepieciešami nekādi speciāli uzlabojumi, lai nodrošinātu ātru pārslēgšanās procedūru (angļu val. *fast roaming*) starp AP, un problēmas ar pārslēgšanos netiek novērotas. Kaut arī reasociējoties EAPOL četrvirzienu rokasspiediena procedūra tiek izpildīta vēlreiz [49], kopā autentifikācijas, asociācijas un četrvirzienu rokasspiediena procedūras parasti aizņem 40–60 ms [35].

Ja IEEE 802.11 tīklā ar ieviestu 802.1X/EAP autentifikāciju neizmanto ātrās pārslēgšanās procedūras (angļu val. *fast roaming*) paņēmienus (sauc arī par ātro, drošo pārslēgšanās procedūru (angļu val. *Fast Secure Roaming – FSR*)), piemēram, oportūnistiskā atslēgu uzkrāšana (angļu val. *Opportunistic Key Caching – OKC*), IEEE 802.11r un CCKM (angļu val. *Cisco Centralized Key Management*), tad katra reasociācija prasa pilnu 802.1X/EAP reaumentifikāciju. Tas parasti ir raksturīgi tīklos ar autonomiem AP, taču bieži vien attiecas arī uz kontroliera bāzētiem bezvadu tīkliem. Šajā gadījumā reasociācija var aizņemt 700 ms un pat vairāk laika [35].

Bezvadu tīklu paraugpraksēs (angļu val. *best practices*) tiek rekomendēts nodrošināt pārslēgšanās procedūras laiku, kas nav lielāks par 150 ms [35], jo pārslēgšanās procedūras aizture tiešsaistes video un VoWLAN pakalpojumiem jānodrošina ne lielāka par 150 ms [35].

802.1X/EAP autentifikācijas un *L3* pārslēgšanās procedūras gadījumā, izejot cauri skenēšanas, atvērtās sistēmas autentifikācijas un asociācijas posmiem, tiek izpildīta 802.1X/EAP reaumentifikācija. Jāņem vērā, ka bez aiztures laika starp AP un bezvadu klientu notiek komunikācija arī ar RADIUS serveri un parasti arī ar LDAP serveri. Izejot cauri 802.1X/EAP autentifikācijas fāzei, klients sāk komunikāciju ar DHCP serveri, lai iegūtu IP adresi. Noteiktos apstākļos iesaistītie serveri var tikt pārslogoti, tādējādi palielinot apstrādes aizturi, tādēļ kopējā pārslēgšanās procedūras aizture var būt ievērojama. Bezvadu tīkla klients var būt nokonfigurēts tā, lai atjaunotu tā DHCP nomas laiku (angļu val. *lease time*) esošajai IP adresei vai arī pieprasītu jaunu IP adresi [40]. DHCP procedūra, lai iegūtu dinamisku IP adresi, var aizņemt līdz pat 1,8 s [50].

Ražotājs Cisco ir paziņojis, ka, realizējot visas tā rīcībā pieejamās tehnikas (piemēram, reasociācijas procedūra, specializētie mobilitātes datu tuneļi, izvairīšanās no DHCP procedūras un IEEE 802.11r/k/v standartu izmantošana), iekšējā viena kontroliera (WLC) *L2* pārslēgšanās procedūra var aizņemt pat mazāk par 10 ms [62]. Savukārt *L2* pārslēgšanās procedūras aizture starpkontrolieru gadījumā var būt mazāka par 20 ms [62].

Pārslēgšanās procedūra var tikt kavēta, ja komunikācijas laikā tiek pazaudēti vadības kadri [35]. Šādā gadījumā tie ir jāpārsūta atkārtoti. Pēc reasociācijas, pirms klients var veikt datu pārsūtīšanu, tiek iesaistīts *ARP* (angļu val. *Address Resolution Protocol*) protokols (*L2*) un transporta līmeņa (*L4*) protokols. Jāņem vērā, ka arī *ARP* protokols rada aizturi. *ARP* komunikācijas protokola uzdevums ir noteikt adresāta *MAC* adresi, balstoties uz zināmo galamērķa *IP* adresi [116]. Kā minēts rakstā [50], *ARP* noildze (angļu val. *timeout*) *ARP* kadru atkārtotas pārsūtīšanas gadījumā ir 1 s. Tomēr pats *ARP* process netiek uzskatīts par nozīmīgu savienojuma izveides aiztures avotu [54].

Tālāk starp klientu un serveri (adresātu) atkarībā no izmantotā transporta slāņa protokola seko *TCP* sesijas nodibināšanas vai atjaunošanas fāze, vai *UDP* datu pārsūtīšana. Ja *TCP* sesija tiek veidota no jauna, *TCP* sesijas nodibināšanas laiks prasa trīs ziņojumu apmaiņu starp sūtītāju un saņēmēju, kas ir diezgan ātrs process, kas galvenokārt atkarīgs no tīkla aiztures. Ja šīs procedūras laikā kāds no ziņojumiem tiek pazaudēts, sesijas izveides laiks var ieilgt, jo pazaudētā pakete ir jāpārsūta atkārtoti, tādējādi atstājot ievērojamu ietekmi uz kopējo savienojuma izveides laiku. Tiklīdz *TCP* sesija ir izveidota, tā var sākties datu pārraide starp klientu un serveri [127]. Papildus no *L7* slāņa procesiem, kas veicina pārslēgšanās procedūras aizturi, var minēt augšējo slāņu šifrēšanas protokolus, piemēram, *TLS* (angļu val. *Transport Layer Security*) protokolu [39].

Jāatzīmē, ka literatūrā atrodamās un šajā sadaļā sniegtās pārslēgšanās procedūru aiztures attiecas uz zemas mobilitātes klientiem [54], kas pārvietojas ar nelielu ātrumu (vidēji 1,4 m/s jeb aptuveni 5 km/h).

Pārslodzes novēršanas mehānismi

TCP plūsmas sesijas laiku var iedalīt vairākas fāzēs. Sākumā ir savienojuma izveides fāze (angļu val. *TCP Connection Establishment*), pēc tās seko datu segmentu pārsūtīšanas fāze un noslēgumā ir savienojuma izbeigšanas fāze (angļu val. *TCP Connection Termination*) [85], [127]. *TCP* sesijas nodibināšana sākas ar loģiskā savienojuma izveidi starp datu sūtītāju un datu saņēmēju, izpildot trīsvirzienu rokasspiediena (angļu val. *three-way handshake*) procedūru. Savienojuma izbeigšanas fāzē tiek izpildīts četrvirzienu rokasspiediena procedūra [127]. *TCP* protokols paredz datu pakešu atkārtotu pārsūtīšanu to pazaudēšanas gadījumā.

TCP plūsma sastāv no datu segmentu (pakešu) virknes, kas tiek sūtīta no avota līdz saņēmējam. Pretējā virzienā tiek sūtīta apstiprinājuma ziņojumu (*ACK*) plūsma, kur saņēmējs katru saņemto paketi apstiprināta ar *ACK* ziņojumu. *TCP* protokols paredz iespēju nosūtīt arī vairākus segmentus pēc kārtas un saņemto porciju apstiprināt tikai ar vienu *ACK* ziņojumu.

Datu pārsūtīšanas fāzē (jebkurā tā laika momentā) sūtītājs var nosūtīt noteiktu segmentu daudzumu, kur segmenta izmērs ir atkarīgs no *MSS* (angļu val. *Maximum Segment Size*) vērtības. Vienā reizē iespējamo nosūtāmo segmentu skaitu nosaka pārslodzes logs *cwnd* (angļu val. *congestion window*). Tādējādi *cwnd* lielums kontrolē pakešu pārraides ātrumu *TCP* plūsmā. Izmantojot *TCP* pārslodzes kontroles (angļu val. *congestion control*) procedūru, sūtītājs sākumā lēni (piemēram, sākot ar vienu *MSS*) un pēc tam – strauji eksponenciālā veidā palielina plūsmas *cwnd* lielumu, sākot ar mazām vērtībām, līdz tiek detektēti zudumi (netiek saņemts *ACK*

ziņojums) vai arī tiek sasniegta sliekšņvērtība *ssthresh* (angļu val. *slow start threshold*). Šo datu pārsūtīšanas režīmu sauc par lēno startu (angļu val. *slow start*). Pēc tam, kad tiek sasniegta *ssthresh* vērtība, sūtītājs *cwnd* logu palielina daudz lēnāk, pieaugums ir lineārs. Šo datu pārsūtīšanas režīmu sauc par pārslodzes izvairīšanos (angļu val. *congestion avoidance*). Ja kāda pakete tiek pazaudēta, tad *cwnd* tiek samazināts uz pusi, pēc tam *cwnd* atkal tiek palielināts lineāri līdz brīdim, kad tiek pazaudēta nākamā pakete, un *cwnd* atkal tiek samazināts uz pusi utt. Lēnā starta procedūra tiek izpildīta sesijas sākumā, kad ir nodibināta *TCP* sesija, kā arī pēc tam, kad ir beidzies atkārtotas pārsūtīšanas laiks jeb noildze (angļu val. *Retransmission Timeout* – *RTO*), kura laikā nav saņemts *ACK* ziņojums no saņēmēja. Rezultātā iegūtā zāģveida *cwnd* diagramma izraisa attiecīgas *TCP* datu plūsmas pārraides ātruma variācijas (izmaiņas) [85], [123], [127].

Transporta bezvadu sakaru tīklos visa *TCP* savienojuma laikā, ieskaitot savienojuma izveides sākuma fāzi (iebraucot *AP* apraides zonā), pārslēgšanās starp *AP* procedūras fāzi, kad tiek atjaunota *TCP* sesija, kā arī savienojuma beigu fāzi (izbraucot no *AP* apraides zonas), *TCP* protokols var radīt ievērojamas aiztures, kas tiek atzīmēts arī pētījumos [15], [50]. Tas ir saistīts gan ar *TCP* sesijas nodibināšanai nepieciešamo laiku, gan ar plūsmas kontroles (angļu val. *flow control*) un pārslodzes kontroles algoritmiem. Izmantojot plūsmas kontroles algoritmu, tiek mainīts *TCP* loga izmērs (angļu val. *window size*) jeb slīdošais logs (angļu val. *sliding window*), kas tiek mērīts baitos, un ir nepieciešams, lai pielāgotos datu saņēmēja pieejamajam buferatmiņas apjomam. Tas tiek kontrolēts visas sesijas laikā, tādā veidā novēršot klienta buferatmiņas pārpildīšanos un tai sekojošu datu pakešu pazaudēšanu [127].

Tādējādi plūsmas kontroles algoritma uzdevums ir aizsargāt datu saņēmēju no pārslodzes, turpretim sastrēgumu kontroles algoritma mērķis ir aizsargāt tīklu no pārslodzes [123], [127].

Pazaudēto datu atkārtota pārsūtīšana ietekmē tīkla veikspēju, samazinot lietderīgo datu caurlaidspēju [123]. Arī bezvadu tīklos – tāpat kā vadu tīklos – visas pieslēguma sesijas laikā *TCP* algoritms reaģē uz jebkādiem pakešu pazaudēšanas gadījumiem un netipiskām aizturēm, un par primāro tā iemeslu tiek uzskatīti tīkla sastrēgumi jeb pārslodze [123], kā rezultātā tiek samazināts datu pārraides loga *cwnd* izmērs, pirms tiek atkārtoti pārsūtītas datu paketes. Tiek iniciēti sastrēgumu kontroles jeb izvairīšanās mehānismi, piemēram, lēnais starts, un tiek dubultota (angļu val. *exponential backoff*) atkārtotas pārsūtīšanas noildze (*RTO*) [127]. Veiktās aktivitātes samazina slodzi starpsavienojumos, tādā veidā kontrolējot sastrēgumus tīklā. Ja pakešu pazaudēšanas iemesls nav sastrēgumi tīklā, tad minētās darbības izraisa nevajadzīgu savienojuma veikspējas (caurlaidspējas) samazināšanos [120]. Datu pārraidei *IEEE 802.11* bezvadu tīklos ir raksturīga sporādiski augsta bitu kļūdu intensitāte (angļu val. *bit error rate*) un saraustīta, arī pārtraukta savienojamība (angļu val. *intermittent connectivity*), izpildot pārslēgšanās procedūru. Oportūnistiskos transporta bezvadu tīklos *TCP* protokola veikspēja cieš no nozīmīgas caurlaidspējas degradācijas un ļoti lieliem virstēriņiem [15], [50].

Pārslodzes kontroles mehānismi tiek nodrošināti gan lietotāja līmenī (angļu val. *end-to-end*), gan tīkla līmenī. Lietotāju līmenī ir izstrādāti vairāki sastrēgumu kontroles algoritmi, piemēram, *TCP Tahoe*, *TCP Reno*, *TCP Vegas*. Protokols *TCP Reno* joprojām ir viens no izplatītākajiem sastrēgumu detektēšanas un kontroles algoritmiem mūsdienās. *TCP New Reno*

ir tā uzlabotā versija. Savukārt *TCP Westwood* ir speciāli izstrādāts izmantošanai bezvadu tīklos [123].

ECN (angļu val. *Explicit Congestion Notification*) ir pārslodzes kontroles protokols, kas tiek izmantots gan lietotāja līmenī, gan tīkla līmenī, kur tīkla mezgls par tīkla pārslodzi paziņo tieši datu saņēmējam. *ECN* maršrutētājā netiek atmestas rindā esošās paketes, tā vietā *TCP IP* paketes galvenē tiek pievienota 1 bita informācija ar *ECN* marķējumu, un pakete tiek pārsūtīta saņēmējam. Saņēmējs, saņemot šādi nomarķētu paketi, pievieno *ECN* informāciju *ACK* ziņojumam un nosūta to sūtītājam. Tādā veidā tiek iniciēta pārslodzes kontroles procedūra, un saņēmējs samazina *cwnd* loga izmēru. Tas ļauj izvairīties no nevajadzīgas pakešu atmešanas un nepamatotām pakešu aizturēm [123], [127].

Tīkla līmenī realizētie pārslodzes kontroles mehānismi veido atgriezenisko saiti no tīkla, kas tiek saukti arī par rindu vadības (angļu val. *queue management* vai *buffer management*) [137] mehānismiem vai algoritmiem. Tas tiek realizēts tīkla infrastruktūras iekārtās, piemēram, maršrutētājos, bezvadu tīkla kontrolieros, komutatoros. Vienkāršākā sastrēgumu kontroles atpakaļsaite ir pakešu atmešana, tiklīdz tiek pārpildīta tīkla iekārtas buferatmiņa. Šāda procedūra tiek saukta par “astes atmešanas” (angļu val. *tail drop*) atpakaļsaiti, un tas ir pasīvās rindu vadības (angļu val. *Passive Queue Management – PQM*) mehānisms. Tas ir trigeris *TCP* sastrēgumu kontroles algoritmam, kā rezultātā *TCP* datu sūtītāja pusē tiek samazināts *cwnd* loga izmērs [123]. Daudz efektīvāki ir aktīvās rindas vadības (angļu val. *Active Queue Management – AQM*) mehānismi, piemēram, *RED* (angļu val. *Random Early Detection*) [137] vai *WRED* (angļu val. *Weighted Random Early Detection*). *RED* ir viens no visplašāk izmantotajiem tīkla pārslodzes novēršanas mehānismiem, kas ir optimāls ātrgaitas tīklos [171]. *RED* monitorē buferatmiņas aizpildījumu un veic nejauši atlasītu pakešu atmešanu brīdī, kad tiek pārsniegta minimālā definētā rindas sliekšņvērtība [120]. *WRED* kombinē *RED* algoritma iespējas ar *IP* prioritātes (angļu val. *precedence*) pazīmi, lai nodrošinātu augstākas prioritātes pakešu privilēģētu trafika apstrādi. *WRED* var selektīvi atmest zemākas prioritātes paketes gadījumā, ja tīkla iekārtas interfeiss tiek pārslogots, kā arī nodrošina diferencētas veiktspējas raksturlielumus dažādām pakalpojumu klasēm. *WRED* atšķiras no citām pārslodzes izvairīšanās tehnikām, piemēram, rindošanas stratēģijām, jo tā mēģina paredzēt un izvairīties no tīkla sastrēgumiem nevis kontrolēt tos, kad tie ir jau radušies [171]. Mūsdienās *IP* tīklos plaši tiek izmantots tieši *WRED* pārslodzes kontroles algoritms, to atbalsta tādi ražotāji kā *Cisco*, *Huawei* un *HP*. Parasti, ja *WRED* nav nokonfigurēts, tiek izmantots noklusētais “astes nomešanas” pakešu apstrādes algoritms, kas vienādi izturas pret visu datplūsmu un vienkārši nomet paketes, kad izvades rinda (angļu val. *output queue*) ir pārpildīta [120].

Vēl viens mehānisms, kas tiek izmantots tīkla pārslodzes likvidēšanai, līdz ar to efektīvi novērš arī pakešu zudumus starp serveri un tīkla infrastruktūru (parasti *IP* komutatoru), ir *IEEE 802.3x Ethernet* plūsmas kontrole (angļu val. *Ethernet Flow Control – EFC*). Mehānismā ir ieviesta pauzes (angļu val. *pause*) kadra koncepcija. Ja raidošā stacija (serveris vai tīkla komutators) raida ātrāk, nekā uztverošā stacija var apstrādāt datus, tad uztverošā stacija izsūta pauzes kadru, kas liek sūtītājam uz noteiktu laika periodu apturēt datu pārraidi [120].

Sastrēgumu jeb pārslodzes novēršanas algoritmi uzrauga tīkla noslodzi, cenšoties paredzēt un izvairīties no pārslodzes tīkla sašaurinājumos (angļu val. *bottlenecks*). Izvairīšanās no

pārslodzēm tīklā tiek panākta, veicot pakešu atmešanu [171]. Divrangu heterogēnā *Wi-Fi* un *LTE* tīklā šāds sašaurinājums ir *LTE* maršrutētāja šūnu tīkla interfeiss (angļu val. *cellular interface*), kur ir vislielākā varbūtība, ka radīsies datplūsmu sastrēgumi.

2.2. *LTE* tehnoloģijas apskats

Eksperimentālajos mērījumos transporta sakaru tīkla otro rangū veido *LTE* tīkla daļa, kas sastāv no 4G *LTE* maršrutētāja un mobilā tīkla, tāpēc šajā apakšnodaļā dots vispārīgs ieskats *LTE* tehnoloģijā un apskatīti galvenie mobilo tīklu signālu raksturojošie parametri un to iespējamās vērtības.

4G *LTE* tehnoloģija

LTE ir ceturtās paaudzes mobilo sakaru tehnoloģija, kas tiek saukta arī par *E-UTRA* (angļu val. *Evolved Universal Terrestrial Radio Access*) un ir daļa no *3GPP Release 8* specifikācijas, kas tika izdota 2008. gadā. Pēc tam sekoja pārējo saistīto *3GPP* relīžu izstrāde. *Release 8* un *Release 9* veido *LTE* standarta pamatu. Pēdējos gados *LTE* ir kļuvusi par vienu no visplašāk izmantotajām platjoslas tehnoloģijām mobilo šūnu sakaru tīklos. Kā zināms, *3GPP* izstrādā standartus, kas tiek īstenoti mobilo tīklu tehnoloģijās, un tie nosaka mobilo tehnoloģiju oficiālo attīstības virzienu.

LTE sistēma var strādāt gan frekvenčdales duplexa (*FDD* jeb *LTE FDD*), gan laikdales duplexa (*TDD* jeb *TD-LTE*) režīmos. *LTE* sistēma izmanto *OFDMA* bāzētu daudzpiekļuves shēmu gan *LTE FDD* režīmā, gan arī *TD-LTE* režīmā [161].

LTE tīkls var tikt konfigurēts, izmantojot dažādus frekvenču kanālu platumus (no 1,4 līdz 20 MHz). *LTE* sistēmā informācija tiek organizēta frekvences un laika resursu režģī, līdz ar to vairāki lietotāji vienlaikus var dalīties ar pieejamo frekvenču kanālu. Informācijas pamatvienība ir resursu elements, kas aptver vienu simbolu ar vienu apakšnesēju. Katrs resursu elements parasti nes 2, 4 vai 6 bitus atkarībā no tā, vai modulācijas shēma ir *QPSK*, *16-QAM* vai *64-QAM* [36].

LTE 3GPP Release 8 teorētiski atbalsta datu pārraides ātrumus līdz 300 Mbit/s lejuplīnijā un līdz 75 Mbit/s augšuplīnijas virzienā.

LTE nodrošina vairākas modulācijas metodes un kļūdu labošanas algoritmus, kur modulēts tiek katrs apakšnesējs. Adaptīvā modulācija un kodēšana ir efektīvs mehānisms, lai maksimāli palielinātu kanāla caurlaidspēju un efektīvi izmantotu pieejamos sistēmas resursus. Adaptācijas algoritms parasti nosaka augstāko modulācijas un kodēšanas shēmu, kas var tikt piemērota pie esošās signāla un traucējumi plus troksnis attiecības (angļu val. *Signal to Interference Noise Ratio – SINR*) uztvērējā, tādā veidā katrs lietotājs tiek nodrošināts ar konkrētajā gadījumā augstāko iespējamo datu pārraides ātrumu [36].

Lai palielinātu spektrālo efektivitāti, tiek izmantota vairāku ieeju un vairāku izeju (*MIMO*) antenu tehnika [36], tādējādi gūstot labumu no vairākceļu izplatīšanās [18] un uzlabojot radiokanāla kapacitāti bez papildu radiofrekvenču spektra izmantošanas. *MIMO* balstās uz

ideju, kur vienlaikus tiek sūtītas vairākas neatkarīgas datu plūsmas vienā un tajā pašā frekvenču kanālā. Šobrīd tiek izmantotas līdz četrām datu plūsmām [36].

LTE 3GPP Release 10 ir zināma kā *LTE-A*. Teorētiski plānots, ka ar šo tehnoloģiju varēs sasniegt datu pārraides ātrumus līdz 1 Gbit/s lejuplīnijā un līdz 500 Mbit/s augšuplīnijā [105]. *LTE-A* tehnoloģija nodrošina nesēju apvienošanu (kopumā līdz pieciem), *MIMO* paplašināšanu līdz astoņām datu plūsmām augšupvirzienā un līdz četrām datu plūsmām lejupvirzienā. *3GPP Release 10* specifikācijas izstrāde tika pabeigta 2010. gadā [161]. Savukārt *3GPP Release 13* specifikācijas izstrāde ir saistīta ar *LTE-A Pro* tehnoloģiju, un tā tika pabeigta 2016. gadā. *LTE-A Pro* tehnoloģija uzskatāma par starpposmu starp 4G un 5G [42]. Šobrīd aktuālā *3GPP* standarta relīze ir *Release 17*.

Latvijā *LTE/LTE-A* mobilo tīklu vajadzībām izmanto 800 MHz, 1800 MHz, 2100 MHz, 2300 MHz un 2600 MHz frekvenču joslas.

Testgultnes eksperimentālajos mērījumos tika izmantoti dažādu ražotāju maršrutētāji ar *LTE* (Cat. 3 un Cat. 4) un *LTE-A* (Cat. 6) modemiem.

***LTE* uztvertā signāla parametri**

LTE frekvenču kanāla mērījumos, novērtējot uztverto signālu, tiek izmantoti vairāki parametri: frekvenču kanāla kvalitātes indikators (angļu val. *Channel Quality Indicator* – *CQI*); references signāla uztvertā jauda (angļu val. *Reference Signal Received Power* – *RSRP*); references signāla uztvertā signāla kvalitāte (angļu val. *Reference Signal Received Quality* – *RSRQ*); uztvertā signāla stipruma indikators (*RSSI*); signāla un traucējumi plus troksnis attiecība (*SINR*) [36], [110]. Minētie parametri detalizēti apskatīti tālāk tekstā.

Kanāla kvalitātes indikators (*CQI*)

Kanāla kvalitātes indikatora parametrs reprezentē kvalitāti, ar kādu klienta iekārta uztver lejuplīnijas signālu no bāzes stacijas. Klienta galiekārta galvenokārt izmanto *SINR* parametru, lai aprēķinātu *CQI* parametru dekodēšanas laikā vai pēc tās. *CQI* tiek periodiski – ik pēc 2 ms – nosūtīts bāzes stacijai. *CQI* vērtības ir diapazonā no 0 (demodulācija nav iespējama) līdz 15 (labākā iespējamā signāla kvalitāte). Atkarībā no *CQI* vērtības tiek noteikta apakšnesēju modulācija un kodēšanas shēma [110].

Uztvertā signāla stipruma indikators (*RSSI*)

Uztvertā signāla stipruma indikators ir signāla jaudas vidējā vērtība no visu uztverto signālu *OFDM* simboliem (satur galiekārtu references simbolus no visiem avotiem, ieskaitot blakuskanālu neapkalpojošās un apkalpojošās šūnas, blakuskanāla traucējumus un termisko troksni mērāmā frekvenču kanāla platumā). *RSSI* izmanto arī, lai aprēķinātu *LTE* sistēmas *RSRQ* parametru [36], [110].

References signāla uztvertā jauda (*RSRP*)

References signāla uztvertā jauda ir specifisks šūnas signāla intensitātes mērījums. Ar šī parametra palīdzību var salīdzināt dažādas šūnas, kas izmanto vienu un to pašu nesējfrekvenci.

RSRP parametru izmanto pie atkārtotas šūnas izvēles un mobilo klientu pārslēgšanās procedūras lēmumu pieņemšanas. *RSRP* mērījumus izmanto arī, lai izveidotu sarakstu ar kandidātu šūnām, ņemot vērā to signālu stiprumu [110]. *RSRP* mēra tikai references signālu jaudu, neietverot traucējumu jaudu. Tādējādi *RSRP* parametrs ir tikai radiopārklājumā balstīts parametrs, kas nav atkarīgs no tīkla slodzes.

References signāla uztvertā signāla kvalitāte (*RSRQ*)

References signāla uztvertā signāla kvalitāte ir specifisks šūnas signāla kvalitātes parametrs. Līdzīgi kā *RSRP* gadījumā, šis parametrs tiek izmantots, lai veidotu sarakstu ar apkārt esošajām mobilo sakaru tīkla kandidātšūnām saskaņā ar to signālu kvalitāti. *RSRQ* ir vienāds ar *RSRP* un *RSSI* attiecību. Jo labāka ir šī vērtība, jo kvalitatīvāku signālu šūnā var uztvert, salīdzinot ar traucējumiem, kas tiek ģenerēti no blakus šūnām. Jo tuvāk negatīvā vērtība ir nullei, jo labāks ir *RSRQ*. Praksē *RSRQ*, kas ir vienāds ar -10 dB, rezultējas mazos datu pārraides ātrumos. Savukārt *RSRQ*, kas ir -3 dB vai augstāks, rezultējas lielākos datu pārraides ātrumos, ja šūnas kopējais signāla stiprums *RSRP* arī ir augsts. Tāpat kā *RSRP*, arī *RSRQ* parametrs praksē tiek izmantots mobilā klienta pārslēgšanās procedūras lēmumu pieņemšanā [36], [110].

Signāla un traucējumi plus troksnis attiecība (*SINR*)

Signāla un traucējumi plus troksnis attiecība ($S/(I + N)$) tiek mērīta mobilā klienta galiekārtā. *SINR* var tikt definēta kā signāla jaudas attiecība pret vidējo traucējumu jaudu no citām šūnām un fona trokšņa summu. Lietotāja galiekārtai attālinoties no šūnas centra, *SINR* vērtība samazinās, jo samazinās uztvertā signāla intensitāte izplatīšanās zudumu dēļ, kā arī palielinās starpsūnu traucējumi, jo, galiekārtai attālinoties no apkalpojošās bāzes stacijas, tā tuvojas kaimiņu bāzes stacijām [161].

Parametrs *RSSI* raksturo signāla stiprumu, savukārt *RSRP*, *RSRQ* un *SINR* raksturo uztvertā signāla kvalitāti [163]. Minētie parametri un to iespējamās vērtības dotas 2.1. tabulā.

2.1. tabula

LTE darbības novērtējums atkarībā no *RSSI*, *RSRP*, *RSRQ* un *SINR* [163]

Radiofrekvenču kanāla darbība	<i>RSSI</i> , dBm	<i>RSRP</i> , dBm	<i>RSRQ</i> , dB	<i>SINR</i> , dB
Teicama	> -65	> -84	> -5	$> 12,5$
Laba	-65 līdz -75	-84 līdz -102	-5 līdz -9	10 līdz $12,5$
Vidēja	-75 līdz -85	-102 līdz -111	-9 līdz -12	7 līdz 10
Vāja	< -85	< -111	< -12	< 7

2.3. WLAN un LTE tehnoloģiju apvienošana

Arvien biežāk tiek apspriestas iespējas integrēt *Wi-Fi* tehnoloģiju 4G (*LTE*, *LTE-A* un *LTE-A Pro*), kā arī 5G mobilajos tīklos [97]. Tādējādi var risināt problēmas, kas ir saistītas ar *Wi-Fi* tīklu ierobežoto mobilitāti, kas galvenokārt tiek nodrošināta pilsētvidē, kā arī šāda pieeja ļauj palielināt kopējo mobilo tīklu kapacitāti [43]. Mobilie tīkli ir projektēti darbam licencētā

frekvenču spektrā galvenokārt balss sakaru nodrošināšanai. Taču mobilajā tīklā nepārtraukti palielinās datu trafika īpatsvars attiecībā pret balss trafiku, tāpēc mobilo tīklu operatori meklē iespējas izmantot nelicencēto frekvenču spektru. Jaunākie *LTE* un *Wi-Fi* tehnoloģiju konverģences risinājumi paredz apvienošanu radio savienojuma vai *TCP* līmenī. Tālāk tekstā apskatītos risinājumus var izmantot, lai nodrošinātu transporta mobilos objektus ar ātrgaitas datu pārraides pieslēgumiem, integrējot *Wi-Fi* un *LTE* tehnoloģijas un to resursus.

LTE-U/LAA

LTE-U (angļu val. *LTE in Unlicensed*)/*LAA* (angļu val. *Licensed Assisted Access*) [89], [131] ir radio savienojumu līmeņa apvienošanas metode, ko standartizē *3GPP*. *LTE-U/LAA* datu pārraidei vienlaikus var izmantot gan licencētās *LTE* frekvenču joslas, gan nelicencēto 5 GHz frekvenču joslu. Lai ieviestu *LTE-U/LAA*, ir nepieciešama galiekārtu nomaiņa uz iekārtām, kas atbalsta *LTE* 5 GHz frekvenču joslā, kā arī mobilajam operatoram ir jāveic *LTE* 5 GHz piekļuves punktu uzstādīšana, t. i., jāveic mazizmēra šūna tīkla izveide (angļu val. *small cell*) [37], [141].

LWA

LWA (angļu val. *LTE–Wi-Fi Link Aggregation*) ir radio savienojumu līmeņa apvienošanas metode, ko standartizē *3GPP*. *LTE* trafika pārraidei *LWA* izmanto gan *LTE* frekvenču joslas, gan nelicencēto 5 GHz frekvenču joslu, kur 5 GHz joslā datu pārraide notiek, izmantojot *Wi-Fi* infrastruktūru. Tas nozīmē, ka *LWA* nav nepieciešama *LTE* 5 GHz aparatūra. *Wi-Fi AP* tiek integrēti mobilajā tīklā. Lai izmantotu *LWA* risinājumu, ir jāveic specializētas programmatūras instalēšana gan mobilā tīkla infrastruktūrai, gan *Wi-Fi AP*, kā arī klienta galiekārtai [141].

MPTCP

MPTCP (angļu val. *Multipath TCP*) ir *TCP* līmeņa datu kanālu apvienošanas metode, ko standartizē *IETF*. Ar *MPTCP* protokola palīdzību ir iespējams sadalīt trafiku tā, ka to var pārsūtīt vienlaikus izmantojot gan *LTE*, gan *Wi-Fi* tīklus. *LTE* un *Wi-Fi* kanālu apvienošana notiek klienta galiekārtā un *MPTCP* starpniekserverī (angļu val. *proxy*), tādējādi nav nepieciešamas izmaiņas tīkla aparatūrā. Lai izmantotu *MPTCP* risinājumu, interneta satura pakalpojuma sniedzēja pusē ir jāuzstāda *MPTCP* starpniekserveris un uz klienta galiekārtas jāveic specializētas programmatūras instalēšana un konfigurācijas izveide [97], [141].

Risinājums var tikt papildināts tā, lai *Wi-Fi* un 4G *LTE*/5G tehnoloģijas tiktu izmantotas pēc attiecīgā pārklājuma pieejamības. Veicot slodzes balansēšanu, priekšroka tiktu dota *Wi-Fi* pieslēgumam, un 4G *LTE*/5G savienojums tiktu uzturēts kā rezerves pieslēgums vai arī tiktu noslogots minimāli.

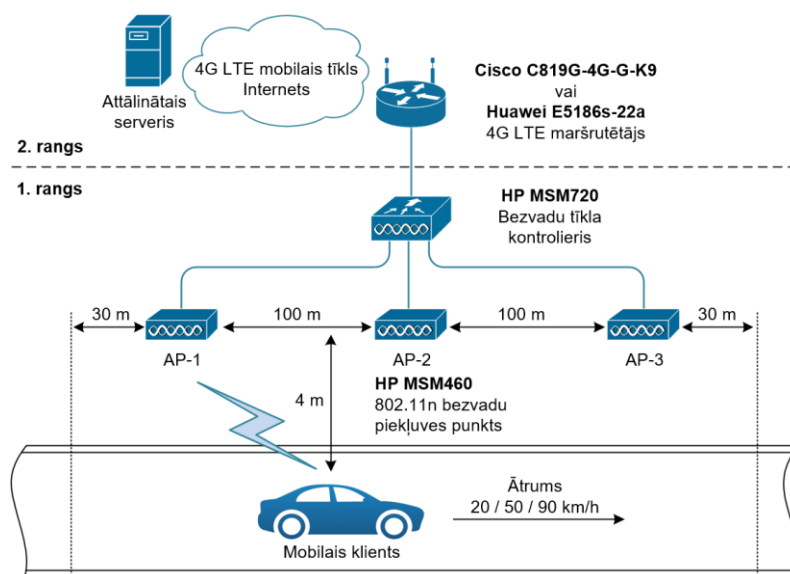
2.4. Veiktspējas pētīšana, izmantojot dažādu *LTE* aparatūru

Lai noskaidrotu integrēta *WLAN* un *LTE* transporta sakaru tīkla veiktspēju, tika veikti eksperimentāli mērījumi lauka apstākļos. Mērījumi tika veikti divrangu sakaru tīklā. Pirmajā rangā tika izmantota *IEEE 802.11n* tehnoloģija, otrajā – *LTE* tehnoloģija. Starp *IEEE 802.11n* klientu un attālināto serveri tika veikti aplikācijas līmeņa (AL) caurlaidspējas mērījumi,

mobilažam klientam pārvietojoties ar dažādiem ātrumiem, mērijumos tika izmantotas dažādu ražotāju *LTE* maršrutētāju iekārtas ar atšķirīgu veikspēju. Iegūtie rezultāti atspoguļoti publikācijā [4].

Testgultnes apraksts

Testgultni (2.9. a–b att.) veidoja pirmā ranga *IEEE 802.11* iekārtas *HP MSM460* [155] (kopā trīs) un bezvadu tīkla kontrolieris *HP MSM720* [154]. Bezvadu piekļuves punkti *HP MSM460* atbalsta *IEEE 802.11a/b/g/n* standartus. Otrajā rangā atkarībā no eksperimenta tika izmantota *LTE* aparatūra *Cisco C819G-4G-G-K9* (*Cisco LTE*) [146] vai *Huawei E5186s-22a* (*Huawei LTE*) [156].



a) Slēguma shēma



b) Izmantotā aparatūra

2.9. att. a) Testgultnes slēguma shēma; b) Eksperimentālo mērijumu iekārtu sagatavošana laboratorijā.

Testgultnes konfigurācija ļauj veikt datu pārraidi, izmantojot publisko mobilo *LTE* tīklu, līdz attālinātajam *FTP* serverim. Par mobila bezvadu tīkla klientu tika izmantota portatīvā darbstacija. Darbstacija tika izvietota automobilī, kas nodrošināja fizisku mobilitāti. Uz attālinātā servera un mobila klienta portatīvās darbstacijas tika uzinstalēta *IxChariot* programmatūra [157], ar kuras palīdzību tika ģenerēts aplikācijas līmeņa *FTP* trafiks. Mērijumos izmantotās aparatūras detalizēta specifikācija un galveno iestatījumu dati apkopoti 8. pielikumā.

Eksperimentālajos mērijumos izmantoto *LTE* maršrutētāju tehniskās specifikācijas dati apkopoti 2.2. tabulā.

LTE maršrutētāju tehniskā specifikācija [146], [156]

Parametrs	Cisco C819G-4G-G-K9	Huawei E5186s-22a
Atbalstāmās bezvadu mobilās tehnoloģijas	LTE/UMTS/HSPA/HSPA+/ DC-HSPA+/EDGE/GPRS/ GSM	LTE-A/LTE/UMTS/HSPA/ HSPA+/DC-HSPA+/EDGE/ GPRS/GSM
LTE frekvenču joslas, MHz	800/900/1800/2100/2600 (FDD)	800/900/1800/2100/2600 (FDD), 2600 (TDD)
LTE modems	Sierra Wireless MC7710	HiSilicon LTE
LTE UE kategorija	Cat 3	Cat 6
LTE DL/UL datu pārraides ātrums, Mbit/s	100/50	300/50
MIMO atbalsts	2 × 2	2 × 2
LAN Ethernet interfeisi	četri 10/100 Base-T	četri 10/100/1000 Base-T
Antena	Antenas tips: ārējā Antenas diagramma: nevirzīta Pastiprinājums: 2 dBi Polarizācija: vertikāla	Antenas tips: iebūvēta Antenas diagramma: nevirzīta Pastiprinājums: 5 dBi Polarizācija: vertikāla
Operatīvā atmiņa	1 GB DRAM	256 MB DDR SDRAM
Zibatmiņa	1 GB	512 MB

Eksperimentālo mērījumu metodoloģija

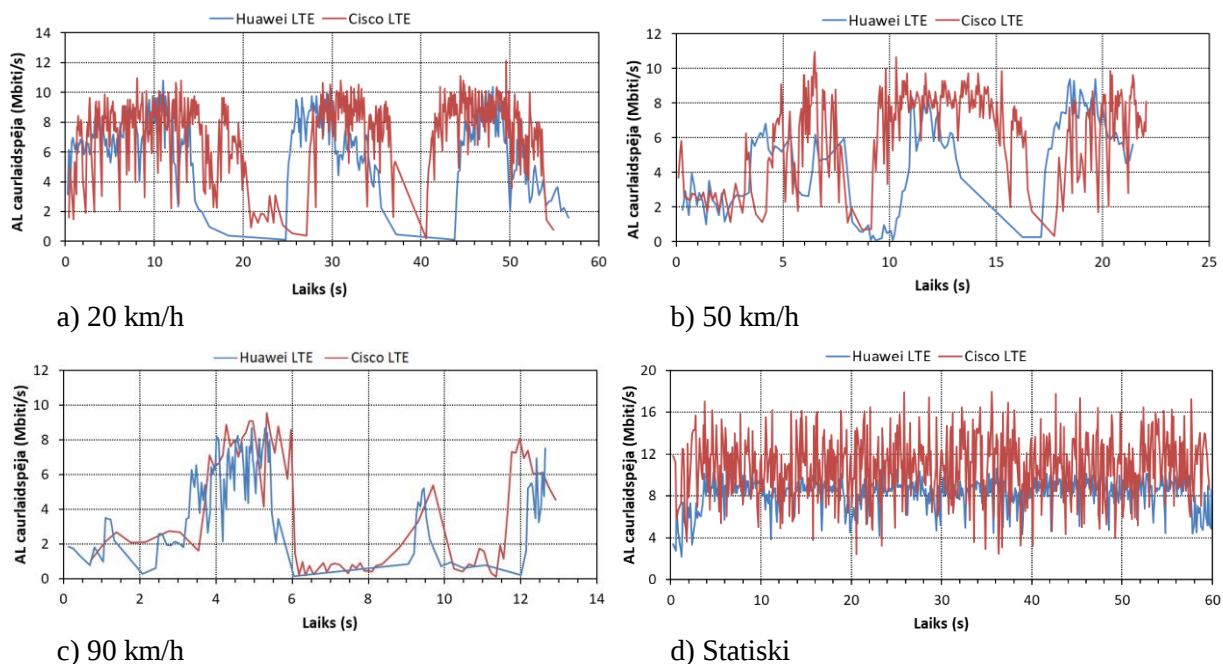
Lai novērtētu iespējamo ietekmi uz integrētā Wi-Fi un LTE kanāla AL caurlaidspēju, tika izmatoti divu dažādu ražotāju LTE maršrutētāji. Mērījumi tika veikti ar vienu transportlīdzekli dažādos braukšanas ātrumos: 20 km/h, 50 km/h un 90 km/h, kā arī automobilim atrodoties statiskā režīmā (0 km/h). Aplikācijas līmeņa FTP trafiks tika sūtīts virzienā no attālinātā servera uz mobilā klienta darbstaciju. Mērījumu laikā Huawei LTE maršrutētāja uztvertais signāla līmenis RSSI bija -64 dBm, Cisco LTE maršrutētājam attiecīgi -60 dBm.

Jāatzīmē, ka sākotnēji standarta klienta darbstacijas konfigurācija neļāva izmērīt AL caurlaidspēju, klientam pārvietojoties ar ātrumu 90 km/h. Klienta darbstacijai nomainot noklusēto bezvadu tīkla kartes iestatījumu parametru “Pārslēgšanās procedūras agresivitāte” (angļu val. *Roaming Aggressiveness*) vērtību “Vidēja” (angļu val. *Medium*) uz “Visaugstākā” (angļu val. *Highest*), to izdevās paveikt.

Eksperimentālo mērījumu rezultāti

2.10. a–d attēlā redzams eksperimentālajos mērījumos iegūto AL caurlaidspējas rezultātu salīdzinājums, izmantojot dažādus LTE maršrutētājus. Grafikos ar sarkano krāsu parādīta Cisco LTE maršrutētāja AL caurlaidspēja, ar zilo – Huawei LTE maršrutētāja AL caurlaidspēja.

Palielinot kustības ātrumu, datu pārraides ātrums samazinās. Pie mobilā klienta pārvietošanās ātruma 20 km/h pārslēgšanās procedūra starp bezvadu piekļuves punktiem (AP) tiek izpildīta korekti, ko parāda divi izteikti trafika krituma posmi (2.10. a att.). Kā redzams no mērījumu rezultātiem (2.10. b–c att.), pārvietojoties ar lielāku ātrumu, veikspēja degradējas un braukšanas ātrumā 90 km/h – pārslēgšanās starp AP kļūst nestabila.



2.10. att. Eksperimentālo rezultātu salīdzinājums. Aplikācijas līmeņa (AL) caurlaidspēja, klientam pārvietojoties dažādos ātrumos.

Izmantojot eksperimentāli iegūtos aplikācijas līmeņa (AL) caurlaidspējas grafikus (2.10. a–c att.), tika novērtēts aktīvās datu pārraides laiks τ katrā AP zonā, kā arī tika novērtēts pārslēgšanās laiks ε starp AP pāriem, rezultāti apkopoti 2.3. tabulā un grafiski atspoguļoti 2.11. a un b attēlā. AP-1 pārklājuma un datu pārraides zona apzīmēta ar 1, AP-2 zona ar 2 un AP-3 zona ar 3. Pārslēgšanās process starp pirmo un otro AP pāri apzīmēts ar 1–2, starp otro un trešo AP pāri attiecīgi 2–3.

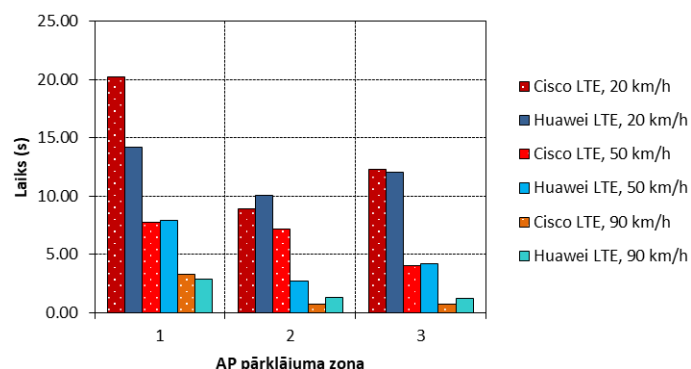
2.3. tabula

Eksperimentālo rezultātu kopsavilkums

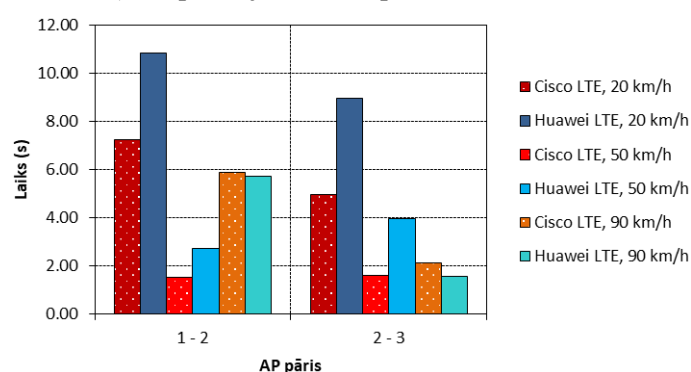
Ātrums v , km/h	LTE maršrutētājs	Datu pārraides laiks AP zonā τ , s			Pārslēgšanās laiks starp AP ε , s	
		1	2	3	1–2	2–3
20	Cisco LTE	20,21	8,94	12,31	7,25	4,97
	Huawei LTE	14,22	10,10	12,04	10,82	8,93
50	Cisco LTE	7,73	7,14	4,03	1,52	1,59
	Huawei LTE	7,89	2,74	4,21	2,72	3,95
90	Cisco LTE	3,26	0,74	0,72	5,89	2,11
	Huawei LTE	2,87	1,29	1,24	5,73	1,55

Tika novērots, ka, izmantojot dažādus LTE maršrutētājus, pārslēgšanās laiks starp AP ir atšķirīgs. AP pārklājuma zonā kopējais pavadītais laiks τ un kopējais pārslēgšanās laiks starp AP pāri ε , klientam pārvietojoties ar ātrumu 20 km/h un 50 km/h, bija labāks (attiecīgi τ lielāks, ε mazāks) mērījumos ar Cisco LTE maršrutētāju, savukārt ar ātrumu 90 km/h rezultāti bija labāki ar Huawei LTE maršrutētāju. Gan τ , gan ε vērtības ir atkarīgas no tā, cik ātri notiek pāreja no viena AP uz otru. Tas ir saistīts ar pārejas procesiem, kā rezultātā mainās kopējais

savienojuma izveides laiks. Šo pāreju var kavēt nepieciešamība veikt atkārtotu pazaudēto pakešu pārsūtīšanu.



a) AP pārkļājuma zonā pavadītais laiks



b) Pārslēgšanās laiks starp AP pāri

2.11. att. AP pārkļājuma zonā pavadītais laiks, pārsūtot datus, un pārslēgšanās laiks starp AP pāri.

Divrangu *Wi-Fi* un *LTE* sakaru kanāla sašaurinājums ir *LTE* maršrutētāja mobilā tīkla fiziskais interfeiss, kur ir vislielākā iespēja, ka radīsies sakaru kanāla pārslodze (datplūsmu sastrēgumi). Līdz ar to trafiks tiks pakļauts sastrēgumu kontroles algoritmu apstrādei [127].

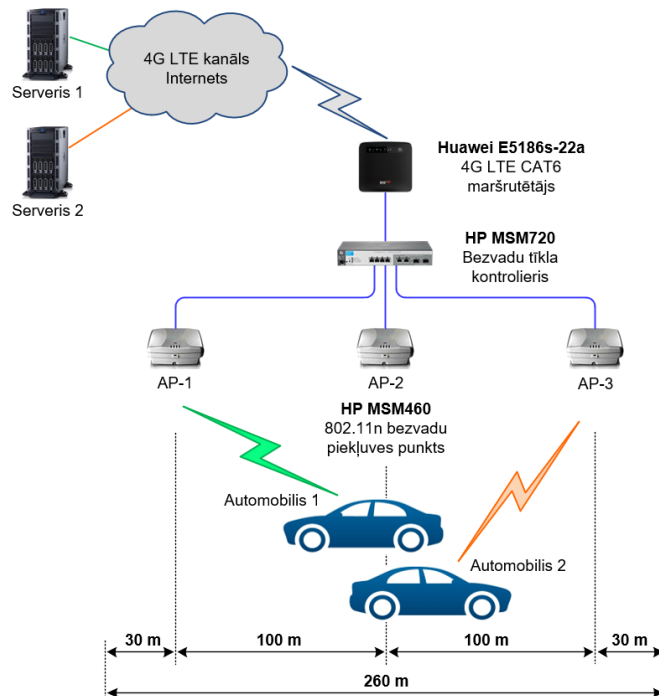
Veiktajos mērījumos pirmajā rangā *Wi-Fi* iekārtas netika mainītas, tika mainīti tikai otrā rango *LTE* maršrutētāji, tāpēc ir iespējams noskaidrot, vai *LTE* iekārtu nomaina ir ietekmējusi kopējo tīkla veiktspēju. Kā redzams no eksperimentāli iegūtajiem rezultātiem (2.10. a–d un 2.11. a–b att.), mērījumi, izmantojot dažādu *LTE* aparatūru, deva atšķirīgus veiktspējas rezultātus. Iegūto AL caurlaidspējas mērījumu rezultātu atšķirība ir 10–20 %, turklāt labāki rezultāti tika sasniegti tīkla konfigurācijā ar *Cisco LTE* maršrutētāju. Var pieņemt, ka izmantotajiem *LTE* maršrutētājiem ir atšķirīga traucējumu noturība, to parāda atšķirīgie maršrutētāju uztvertie *RRSI* līmeņi, un tas var ietekmēt veiktspējas mērījumus. Vidējā AL caurlaidspēja galvenokārt ir atkarīga no pārslēgšanās procedūras ilguma, datu pārraides laikā pazaudēto pakešu daudzuma, kas rada nepieciešamību veikt atkārtotu to pārsūtīšanu, izmantotā *TCP* pārslodzes kontroles mehānisma un pašu iekārtu veiktspējas. Pēc tehniskajiem parametriem (2.2. tab.) *Cisco LTE* maršrutētājam ir lielāka operatīvā atmiņa, kas var tikt izmantota arī kā buferatmiņa un, savienojot dažādu ātrumu tīklus (eksperimentā *Wi-Fi* un *LTE*), tas var būt izšķirošs parametrs, lai nodrošinātu augstāku sakaru kanāla veiktspēju.

2.5. Veiktspējas pētīšana atkarībā no mobilo klientu skaita un izmantotajiem kustības scenārijiem

Lai noskaidrotu divrangu *Wi-Fi* un *LTE* transporta sakaru tīkla veiktspēju atkarībā no mobilo klientu skaita un izmantotajiem pārvietošanās režīmiem, tika veikti eksperimentāli mērījumi lauka apstākļos. Eksperimentālie mērījumi tika veikti ar vienu un ar diviem kustīgiem klientiem (automobiļiem). Salīdzinot ar iepriekšējo pētījumu, iesaistot vairākus transportlīdzekļus, tika īstenoti sarežģītāki scenāriji, kas ļauj iegūt eksperimentālus mērījumu rezultātus, kas atbilst reāliem satiksmes plūsmas apstākļiem. Pētījumā iegūtie rezultāti prezentēti publikācijā [5].

Testgultnes apraksts

Eksperimentālo mērījumu veikšanai lauka apstākļos tika sagatavota testgultne. Datu pārraide no klienta uz attālināto serveri un atpakaļ tika realizēta, izmantojot bezvadu tīklu tehnoloģijas *Wi-Fi* un 4G. Testgultnes pirmo rangu veidoja *IEEE 802.11n* piekļuves tīkls, otro rang – 4G *LTE* atvilces tehnoloģija. Pirmajā rangā tika uzstādīti trīs bezvadu piekļuves punkti (AP), kas tika apvienoti, izmantojot bezvadu tīkla kontrolieri (WLC). Pie WLC augšuplīnijas (angļu val. *uplink*) interfeisa tika pieslēgts *LTE* maršrutētājs. Klienta portatīvā darbstacija (mobilais klients) tika izvietota automobilī. Testgultne aizņēma 260 m garu ceļa posmu, attālums starp AP bija 100 m.



2.12. att. Eksperimentālo mērījumu testgultne.

Mobilais klients pārvietojās gar ceļmalā izvietotajiem AP, šķērsojot to pārklājuma zonas. Iebraucot katra AP apraides zonā, mobilais klients veidoja savienojumu ar attiecīgo AP, tālāk klienta dati, izmantojot WLC, tika pārvirzīti uz *LTE* maršrutētāju un no maršrutētāja caur

mobilo tīklu līdz attālinātajam serverim. Līdzīgi, tikai apgrieztā secībā, dati tika sūtīti no attālinātā servera uz mobilā klienta darbstaciju. *LTE* bezvadu sakaru kanāls no *LTE* maršrutētāja līdz tuvākajai mobilā tīkla *LTE* bāzes stacijai var sasniegt vairākus kilometrus. Eksperimentālo mērījumu testgultnes slēguma shēma redzama 2.12. attēlā. Eksperimentos tika izmantoti viens vai divi mobilie klienti (“Automobilis 1” jeb “A1” un “Automobilis 2” jeb “A2”), tāpēc speciāli katram klientam tika sagatavoti divi neatkarīgi attālinātie serveri ar līdzīgu veikspēju. Mērījumos izmantotās aparātūras detalizēta specifikācija un galveno iestatījumu dati apkopoti 8. pielikumā.

Eksperimentālo mērījumu metodoloģija

Mērījumos tika izmantota *IxChariot* programmatūra, ar kuras palīdzību tika nodrošināta *FTP* datu plūsma (izmanto *TCP* protokolu) no attālinātā servera virzienā uz mobilo klientu. Aplikācijas līmeņa (AL) caurlaidspējas mērījumi tika veikti ar vienu un ar diviem mobilajiem klientiem dažādos to pārvietošanās ātrumos: 20 km/h un 50 km/h. Katrā mobilā klienta pārvietošanās ātrumā un pārvietošanās scenārijā tika veikti vismaz trīs mērījumi.

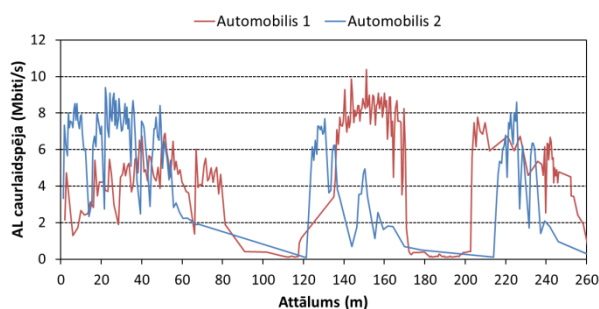
Integrēta divrangu sakaru tīkla *Wi-Fi* un *LTE* caurlaidspēja ir atkarīga no katra ranga veikspējas atsevišķi. Katra ranga maksimālā, taču savstarpēji minimālā caurlaidspēja ir šāda integrētā sakaru tīkla maksimālā iespējamā caurlaidspēja.

Pirmā ranga caurlaidspēja ir atkarīga no klientu skaita *AP* apkalpes zonā, izmantotā bezvadu tīkla kontroliera (*WLC*) un *AP* veikspējas, piemēram, atbalstītā *WLAN* datu pārraides standarta. Otrā ranga caurlaidspēja ir atkarīga no izmantotā *LTE* maršrutētāja veikspējas. Kopumā tīkla veikspēja ir atkarīga no tīkla mezglos ienākošā datu trafika intensitātes, mezglu buferatmiņas ietilpības un mezglu nodrošinātās datplūsmu apstrādes intensitātes. Datu trafiks tīkla mezglos var tikt piegādāts gan no *LTE* tīkla daļas, gan arī no *Wi-Fi* tīkla.

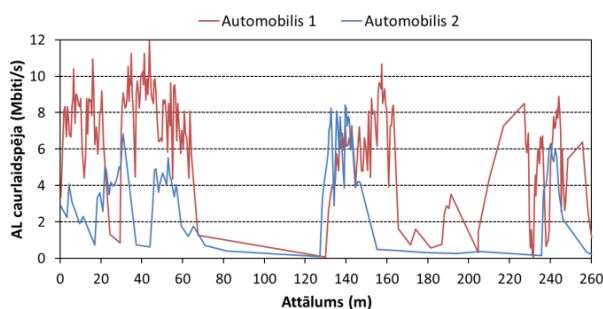
Eksperimentālo mērījumu rezultāti

2.13. a–c attēlā redzams eksperimentāli iegūto AL caurlaidspējas mērījumu rezultātu salīdzinājums ar diviem transportlīdzekļiem, kas pārvietojas ar 20 km/h lielu ātrumu, izmantojot dažādus kustības scenārijus: “viens aiz otra”, “paralēli” un “viens otram pretī”. Ja automobiļi pārvietojas paralēli, “Automobilis 1” ir tuvāk *Wi-Fi* infrastruktūrai un “Automobilis 2” ir tālāk no tās.

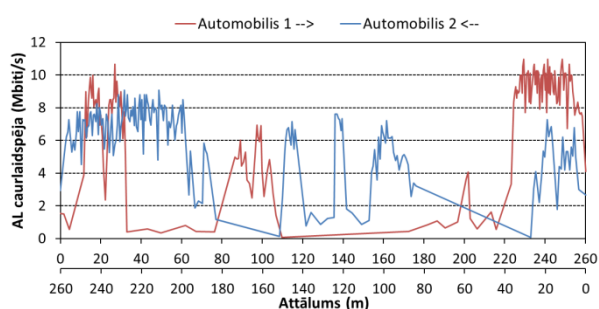
Savukārt 2.13. d–f attēlā redzams eksperimentāli iegūto AL caurlaidspējas mērījumu salīdzinājums ar diviem transportlīdzekļiem, kas pārvietojas ar 50 km/h lielu ātrumu, izmantojot dažādus kustības scenārijus: “viens aiz otra”, “paralēli” un “viens otram pretī”.



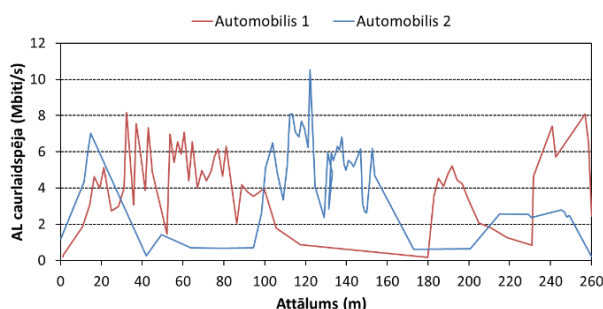
a) Scenārijs “viens aiz otra”, 20 km/h



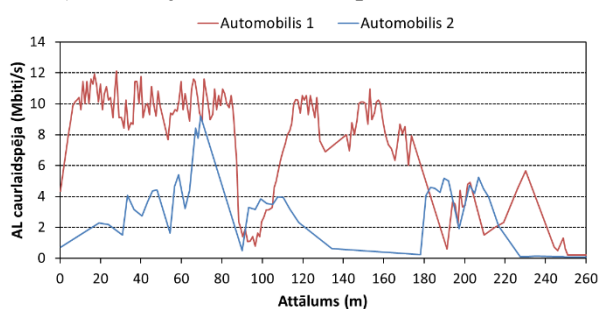
b) Scenārijs “paralēli”, 20 km/h



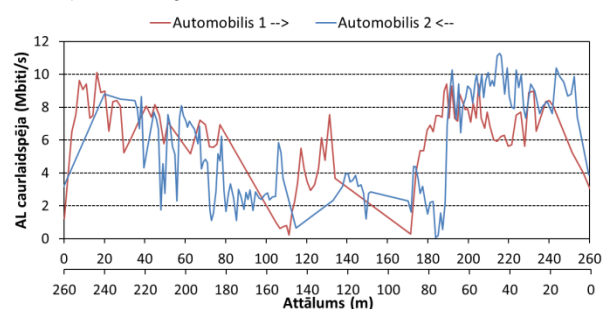
c) Scenārijs “viens otram pretī”, 20 km/h



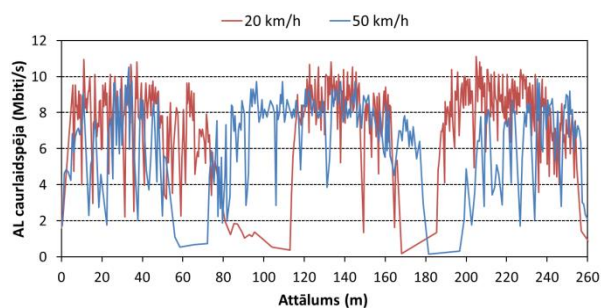
d) Scenārijs “viens aiz otra”, 50 km/h



e) Scenārijs “paralēli”, 50 km/h



f) Scenārijs “viens otram pretī”, 50 km/h



g) AL caurlaidspēja vienam klientam, braucot ar ātrumu 20 km/h un 50 km/h

2.13. att. a–f) AL caurlaidspējas salīdzinājums, diviem automobiļiem pārvietojoties dažādos braukšanas ātrumos un kustības scenārijos; g) AL caurlaidspējas salīdzinājums vienam automobilim dažādos braukšanas ātrumos.

Iegūtie rezultāti parāda katra individuālā mobilā klienta, kas pārvietojas gar bezvadu piekļuves punktiem, veikspēju. Novērtējot visu iesaistīto mobilo klientu rezultātus, var noskaidrot kopējos tīkla veikspējas ierobežojumus.

2.4. tabulā redzamas aprēķinātās vidējās AL caurlaidspējas vērtības $\bar{\eta}$ un dispersija D individuālām klientu A1 un A2 trafika plūsmām η_{A1} un η_{A2} , attiecīgi $\bar{\eta}_{A1}$ un $D_{\eta A1}$, kā arī $\bar{\eta}_{A2}$ un $D_{\eta A2}$. Tālāk tika aprēķināta kopējā vidējā AL caurlaidspēja starp abiem klientiem $\bar{\eta}_{A1A2}$, kā

arī korelācijas koeficienti $K_{\eta A1\eta A2}$ starp abu klientu AL caurlaidspējas vērtību kopām. Tika noteikta arī kopējā dispersija $D_{\eta A1\eta A2}$. Aprēķini tika veikti dažādiem automobiļu (klientu) pārvietošanās ātrumiem un dažādiem automobiļu pārvietošanās scenārijiem. Kopējā dispersija $D_{\eta A1\eta A2}$ tika noteikta, izmantojot 2.1. izteiksmi [136].

$$D[\eta_{A1} + \eta_{A2}] = D[\eta_{A1}] + D[\eta_{A2}] + 2K_{\eta A1\eta A2}, \quad (2.1.)$$

Aplūkojot iegūtās mobilo klientu A1 un A2 vidējās individuālās, kā arī vidējās kopējās AL caurlaidspējas vērtības (2.4. tab.), redzams, ka vislabākie rezultāti tika iegūti, kad automobiļi pārvietojās “viens otram pretī”. Šajā gadījumā vislielākā cīņa par piekļuvi *Wi-Fi* tīkla resursiem notiek tad, kad abi automobiļi satiekas pie *AP-2*. Scenārijā, kad transportlīdzekļi pārvietojās “paralēli” viens otram, no *Wi-Fi* infrastruktūras tālāk esošā mobilā klienta (A2) AL caurlaidspēja bija mazāka, kā jau to varēja paredzēt. Scenārijā “viens aiz otra” abu mobilo klientu AL caurlaidspējas bija diezgan līdzīgas. Pēc iegūtajiem grafikiem (2.13. a un d att.) var secināt, ka abi klienti pārsvarā vienlaikus atradās pie viena un tā paša *AP* un līdzīgi pārslēdzās uz nākamo *AP*, jo attālums starp tiem bija aptuveni 10 m.

Vidējā AL caurlaidspēja ar vienu mobilo klientu (automobili) pārvietošanās ātrumā 20 km/h bija 7,76 Mbit/s, 50 km/h attiecīgi 6,39 Mbit/s, kas kopumā dod labākus rezultātus, salīdzinot tos ar scenārijiem, kur tika izmantoti divi transportlīdzekļi. Vienā gadījumā ar diviem konkurējošiem klientiem, kas pārvietojas ar ātrumu 50 km/h, individuālā AL caurlaidspēja vienam no klientam bija lielāka, salīdzinot ar viena klienta scenāriju. To varētu skaidrot ar ārējo faktoru ietekmi – fona trokšņu līmeni, kas var radīt uztvertā signāla pavājināšanos, veicināt pakešu zudumus un līdz ar to izraisīt atkārtotu to pārsūtīšanu, kas savukārt izraisa sakaru kanāla veiktspējas degradāciju.

Brīdī, kad transportlīdzekļi pārvietojas gar *Wi-Fi* infrastruktūru un pāriet no vienas *AP* apraides zonas uz citu, datu trafiks krītas. AL caurlaidspēja no maksimālajām vērtībām samazinās praktiski līdz nullei, un, kad pārejas process ir beidzies, AL caurlaidspēja pakāpeniski atkal pieaug līdz maksimālajām vērtībām. AL caurlaidspējas vērtību svārstības ir lielas, un tas rezultātā dod lielas dispersijas vērtības (2.4. tab.).

2.4. tabula

Eksperimentāli iegūtās vidējās AL caurlaidspējas un aprēķinātās korelācijas koeficienta un dispersijas vērtības

Ātrums v, km/h	Braukšanas scenārijs	Ē, Mbit/s		Kopējā Ē _{A1A2} , Mbit/s	K _{ηA1ηA2}	D		Kopējā D _{ηA1ηA2}
		Ē _{A1}	Ē _{A2}			D _{ηA1}	D _{ηA2}	
20	viens aiz otra	4,70	5,67	5,19	-0,06	8,28	5,50	13,66
	paralēli	6,68	4,12	5,40	0,14	7,17	5,14	12,59
	viens otram pretī	7,15	5,99	6,57	0,21	9,99	4,10	14,51
50	viens aiz otra	4,25	4,41	4,33	0,19	4,06	5,31	9,75
	paralēli	7,90	3,23	5,57	0,38	10,96	4,71	16,43
	viens otram pretī	6,30	5,64	5,97	-0,23	5,53	9,32	14,39

No 2.4. tabulas datiem redzams, ka starp abu transportlīdzekļu klientu AL caurlaidspējām pastāv korelācija, lai gan tā ir vāja ($K_{\eta A1\eta A2} < 0,5$) [14]. Tas ir saistīts ar to, ka abi transportlīdzekļu klienti vēršas pie vieniem un tiem pašiem bezvadu tīkla resursiem (AP un WLC), t. i., tīkla resursi starp mobilajiem klientiem tiek koplietoti. Divos gadījumos aprēķinātā korelācija ir vāja un negatīva. Testgultnē realizētā automobiļu Wi-Fi bāzēta sakaru tīkla resursu kapacitāte ir paredzēta lielumam klientu skaitam (HP MSM720 atļauj 250 vienlaikus konkurējošas lietotāju sesijas [154]), tāpēc var paredzēt, ka, palielinot klientu skaitu, korelācijas koeficients pieaugs.

Pēc eksperimentāli iegūto AL caurlaidspējas rezultātu analīzes var secināt, ka AL caurlaidspēja ir atkarīga gan no mobilo klientu kustības scenārijiem, gan klientu pārvietošanās ātruma, kā arī no AP apkalpošanas zonā vienlaikus esošu mobilo klientu skaita. Tas atstāj iespaidu gan uz individuālajiem mobilo klientu AL caurlaidspējas rādītājiem, gan arī uz kopējo bezvadu tīkla veiktspēju.

Vienlaicīga vairāku mobilo klientu klātbūtne bezvadu tīklā nozīmē cīņu par bezvadu tīkla resursiem. Tas atspoguļojas arī iegūtajos mērījumu grafikos kā neregulāri trafika kritumi un vidējās AL caurlaidspējas samazinājums. Lielu iespaidu uz kopējo tīkla veiktspēju atstāj arī pati pārslēgšanās procedūra starp AP. Tās ir papildu problēmas un izaicinājumi, kas jārisina, lai minimizētu negatīvās sekas, ar ko saskaras mobilie klienti, izpildot biežo un laikietilpīgo pārslēgšanās procedūru.

2.6. Hersta parametra noteikšana un tā analīze divrangu sakaru tīklam ar vairākiem klientiem

Šajā apakšnodaļā tiek novērtēts un analizēts Hersta parametrs (angļu val. *Hurst parameter* – H) eksperimentāli iegūtam AL caurlaidspējas trafikam scenārijos ar vienu un diviem mobilajiem klientiem. Pētījumā iegūtie rezultāti atspoguļoti publikācijā [8].

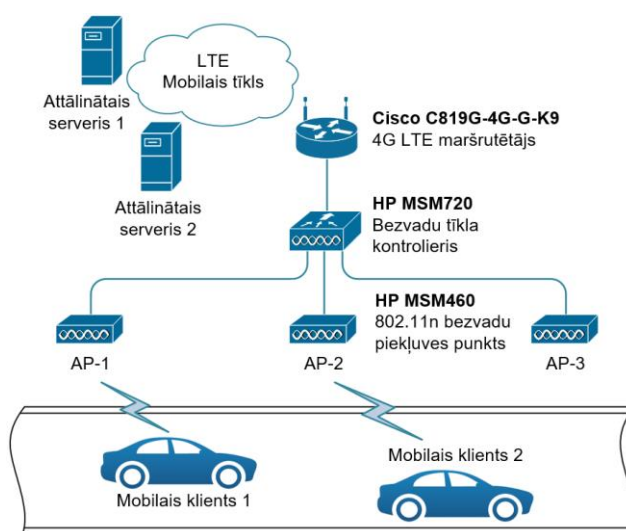
Eksperimentālo mērījumu apraksts

Testgultnes izveide un testēšana lauka apstākļos ir svarīga gan eksperimentālam sistēmas funkcionalitātes un veiktspējas novērtējumam, gan nepieciešama veiksmīgai produktu attīstīšanai. Integrētas Wi-Fi un LTE sistēmu testgultnes izveide ir laikietilpīga un komplicēta. LTE tīkla daļu var kontrolēt tikai mobilā tīkla pakalpojumu sniedzējs. Eksperimentu veicējiem šādā testgultnē pilna kontrole ir tikai pār Wi-Fi tīkla daļu, LTE daļā nav iespēju veikt kādas tehniskas izmaiņas. Turklāt mērījumi publiskos LTE tīklos ir atkarīgi no kopējās šī tīkla noslodzes.

Līdzīgi kā 2.4. apakšnodaļā attēlotajai testgultnei, arī šajā pētījumā eksperimentu vajadzībām tika realizēta integrēta Wi-Fi un LTE tehnoloģijās balstīta testgultne āra apstākļos. Testgultnes pirmajā rangā tika izmantots IEEE 802.11n bezvadu tīkla kontrolieris HP MSM720, pie kura tika pieslēgti trīs bezvadu piekļuves punkti HP MSM460, attālums starp tiem bija 100 m. Atšķirībā no iepriekšējā pētījuma testgultnes otrajā rangā tika izmantots Cisco C819G-4G-G-K9 LTE maršrutētājs. Eksperimentālajos mērījumos atkarībā no scenārija

tika izmantots viens vai divi automobiļi. Divu automobiļu realizācijā tie atradās kustībā viens aiz otra. Mobilie klienti tika nodrošināti ar biznesa klases portatīvajiem datoriem, un tika sagatavoti arī divi attālinātie serveri. Kanāls no *LTE* maršrutētāja līdz attālinātajam serverim tika organizēts, izmantojot mobilā tīkla 4G *LTE* tehnoloģiju. Tādējādi pētījuma objekts reprezentēja divrangu bezvadu tīkla testgultni (2.14. att.). Mērījumos izmantotās aparātūras detalizēta specifikācija un galveno iestatījumu dati pieejami 8. pielikumā.

Mērījumi tika veikti ar vienu un diviem automobiļiem dažādos transportlīdzekļu kustības ātrumos: 20 km/h, 50 km/h un 90 km/h. Mērījumos tika izmantota *IxChariot* programmatūra, ar kuras palīdzību tika ģenerēts *FTP* datu trafiks. Mērījumu datu trafiks tika ģenerēts attālinātajā serverī, šķērsojot testgultnes aprakstītos mezglus, nonāca klientam tuvākajā (asociētajā) *AP* un tika nosūtīts uz klienta darbstaciju. *Wi-Fi* piekļuves kontrolieris un *LTE* maršrutētājs apstrādā arī datu trafika plūsmas, kas tiek piegādātas no bezvadu piekļuves punktiem, t. i., no klientiem.



2.14. att. Testgultnes slēguma shēma.

Hersta parametra noteikšana un iegūto datu analīze

Divrangu sakaru tīklā svarīga loma ir *LTE* maršrutētājiem, jo tiem vienlaikus jāspēj komunicēt gan ar *Wi-Fi* infrastruktūru, kur pastāv *Ethernet* savienojums, gan ar mobilo tīklu. Jāņem vērā, ka *LTE* maršrutētāja šūnu tīkla interfeiss ir arī datu kanāla sašaurinājuma vieta, kur var rasties pārslodzes. Reālā tīkla vidē jāsaucas ar tīkla resursu veiktspējas ierobežojumiem, piemēram, komutatoru caurlaidspēju, ierobežotu buferatmiņas apjomu (rindu garums) un galīgu procesora apstrādes iespēju.

Mērījumos tika izmantots *FTP* datu trafiks, kas ir bāzēts uz *TCP* transporta protokolu. *TCP* protokola ietekme uz datu trafiku ir plaši pētīta, ir secināts, ka protokolā realizētās *TCP* atkārtotas pārraides un pārslodzes kontroles mehānismi var izraisīt sevlīdzības (angļu val. *self-similar*) efektu [99], [130]. Tas nozīmē, ka tīkla mezgli ietekmē datu trafika raksturu. Ja datu trafikam piemīt sevlīdzības raksturs, tad slodzes sadale atkārtojas dažādos laika periodos (dažādos laika mērogos). Tiek vērtēta informācijas plūsmas intensitātes atkarība no laika. Līdz ar trafika intensitātes palielināšanos, palielinās arī sevlīdzības pakāpe. Datu trafika sevlīdzības

pakāpes novērtēšanai tiek izmantots Hersta (H) parametrs. Sevlīdzīgam datu trafikam H mainās diapazonā 0,7–0,95 [99]. Tīklu modelēšanā jāņem vērā trafika sevlīdzības pakāpe, lai korekti varētu novērtēt šo tīklu noslodzi [99].

Eksperimentāli tika pārbaudīts, kā mainās H parametrs datu trafikam, ja pieaug klientu skaits un mainās klientu pārvietošanās ātrums. Izmantojot datorprogrammu *SELFISv.01b* [176], tika novērtēts H parametrs eksperimentāli iegūtajam viena klienta AL trafikam scenārijos ar vienu un diviem transportlīdzekļiem. Jāatzīmē, ka ir izstrādātas vairākas procesu sevlīdzības novērtēšanas metodes. Visplašāk izmantotās ir absolūto momentu (angļu val. *Absolute Moments*) un R/S (angļu val. *Rescaled Range*) metodes. Absolūto momentu metodei ir augstāka precizitāte, salīdzinot ar R/S metodi, tāpēc novērtējumam tika izmantota šī metode [99]. 2.5. tabulā dots Hersta parametra novērtējums atkarībā no klientu skaita (tīkla noslodzes) un transportlīdzekļu pārvietošanās ātruma.

2.5. tabula

Eksperimentāla Hersta parametra noteikšana

Automobiļu (klientu) skaits	Automobiļu braukšanas ātrums v , km/h	Hersta parametrs H
Viens	20	0,703
	50	0,890
	90	0,734
Divi	20	0,866
	50	0,871
	90	0,705

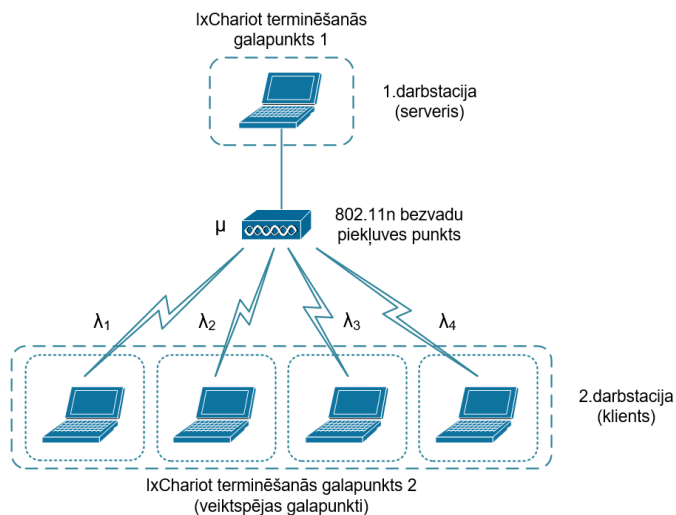
Pēc eksperimentāli iegūtajiem rezultātiem redzams, ka, pieaugot lietotāju skaitam bezvadu tīklā, Hersta parametrs mainās intervālā 0,7–0,89, tādēļ var secināt, ka mērījumos pārsūtītais datu trafiks ir sevlīdzīgs. Prognozējams, ka, tālāk pieaugot mobilo klientu skaitam, pieaugs arī H parametrs. Balstoties uz šiem rezultātiem, var novērtēt arī aparatūrai nepieciešamo buferatmiņas apjomu, jo sevlīdzīgs trafiks ir atkarīgs no buferatmiņas apjoma [99], [104]. Saskaņā ar [104] pastāv likumsakarība starp sistēmas noslodzi ρ (angļu val. *utilization*), buferatmiņas lielumu K un pakešu zudumu varbūtību P_{Loss} (angļu val. *packet loss probability*) pie dažādām Hersta parametra vērtībām. Minētā likumsakarība aprakstīta publikācijā [8]. Tādējādi ir iespējams noteikt nepieciešamo tīkla mezgla buferatmiņas apjomu dažāda sevlīdzīga trafika intensitātei, lai nepārsniegtu definēto P_{Loss} . Rezultātā tas dod iespēju plānot un attīstīt augstas veiktspējas bezvadu tīklus.

2.7. Veiktspējas pētīšana atkarībā no klientu skaita stacionārā režīmā

Šajā apakšnodaļā apkopota informācija par veiktajiem eksperimentālajiem mērījumiem un izmantoto matemātisko modeli, lai novērtētu Wi-Fi tīkla veiktspēju atkarībā no mobilo klientu skaita stacionārā režīmā. Noteikta gan katra klienta individuālā caurlaidspēja, gan kopējā tīkla caurlaidspēja. Iegūtie rezultāti atspoguļoti zinātniskajā publikācijā [8].

Eksperimenta apraksts

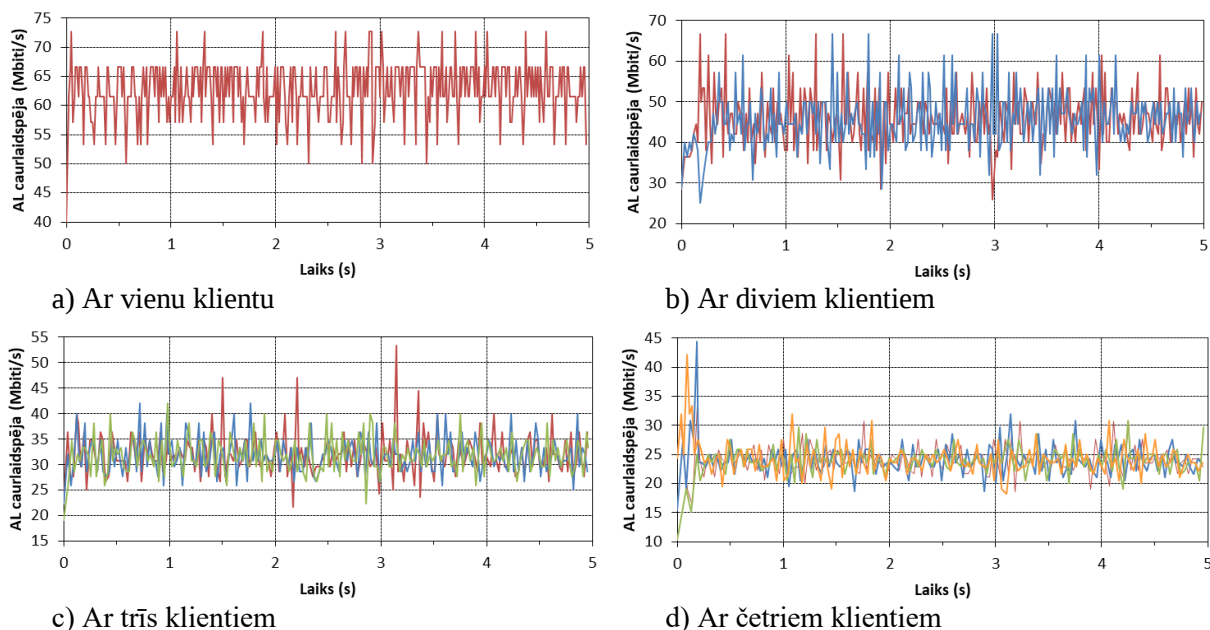
Testgultne tika realizēta, izmantojot vienu bezvadu piekļuves punktu, kas atbalsta *IEEE 802.11n* standartu, un divas darbstacijas (serveris un klients), uz kurām tika uzinstalēta *IxChariot* programmatūra (2.15. att.).



2.15. att. Eksperimentālo mērījumu shēma.

Ar *IxChariot* programmatūru ir iespējams simulēt protokolu, lietojumu un līdz ar to arī datu pārraides pakalpojumu darbību, kas tiek izmantoti dzīvē, lai prognozētu tīkla veiktspēju un nepieciešamo kapacitāti reālos slodzes apstākļos. *IxChariot* risinājums sastāv no *IxChariot* terminēšanās galapunkta 1 (servera), kas tiek terminēts servera darbstacijā un *IxChariot* terminēšanās galapunkta 2 (klienta jeb veiktspējas galapunktiem), kas tiek terminēts klienta darbstacijā. Programmatūra spēj vienlaikus simulēt dažādus komunikāciju procesus. *IxChariot* programmatūra ļauj mērīt datu pārraides tīkla aplikācijas līmeņa (AL) caurlaidspēju. Lai analizētu bezvadu tīkla veiktspēju, tika izmantots *FTP* datu pārraides scenārijs, kur datu pārsūtīšana notiek, izmantojot *TCP* transporta slāņa protokolu.

Vispirms tika noteikta bezvadu tīkla vidējā AL caurlaidspēja ar vienu tīkla klientu. Tā bija 62,55 Mbit/s. Nominālā caurlaidspēja *IEEE 802.11n* standarta piekļuves punktam ar vienu telpiski atdalītu plūsmu, modulācijas un kodēšanas shēmu *MCS7*, frekvenču kanāla platumu 20 MHz un aizsargintervālu (*GI*) 400 ns ir 72,2 Mbit/s (9. pielikums) [62]. Pēc tam pakāpeniski tika palielināts klientu skaits no viena līdz četriem. Tika iegūtas atšķirīgas vidējās AL caurlaidspējas vērtības atkarībā no klientu skaita. 2.16. a–d attēlā redzami eksperimentu rezultāti, kas iegūti ar *IxChariot* programmatūru, simulējot pie *AP* vienlaikus pieslēgtus no viena līdz četriem klientiem. Izmantoti četri klienti, jo literatūrā [69] tas tiek minēts kā vidējais prognozētais klientu (automobiļu) skaits automaģistrāļu *AP* apkalpošanas zonā, ja transporta plūsmas ātrums ir 80–90 km/h un tas pārvietojas pa trīs braukšanas joslām.



2.16. att. Eksperimentālo mērījumu rezultāti.

Vidējās eksperimentāli iegūtās AL caurlaidspējas vērtības apkopotas 2.6. tabulā. Pēc eksperimentālo datu analīzes var secināt, ka klienta individuālā caurlaidspēja samazinās, palielinoties klientu skaitam, 2.17. a attēlā redzams, ka šis samazinājums nav lineārs.

Matemātiskais modelis

Eksperimentālo rezultātu aproksimācijai vispārējam gadījumam var tikt izmantots daudztermināļu sistēmas matemātiskais modelis (angļu val. *multiterminal system model*, tiek saukts arī par *machine repairman model*) [8]. Tīklā esošo darbstaciju (klientu) skaits tiek apzīmēts ar M . Pieprasījumu (ziņojumu) pienākšanas intensitāte no vienas darbstācijas uz bezvadu piekļuves punktu tiek apzīmēta ar λ , tādējādi kopējā pieprasījumu intensitāte:

$$\Lambda = \lambda(M - i), \quad (2.2.)$$

kur M – tīkla ieeju skaits; i – pieprasījumu skaits serverī.

Par pieprasījumu plūsmu pieņem datu operāciju plūsmu (piemēram, 1500 baitu liela pakešu plūsma). Katrs pieprasījums vispirms tiek apstrādāts bezvadu piekļuves punktā, tālāk pieprasījums nonāk serverī. Pieprasījumu apstrādes intensitāte bezvadu piekļuves punktā tiek apzīmēta ar μ . Intervāli starp pieprasījumiem un to apkalpošanas ilgums ir gadījuma lielumi, un tiem ir savi varbūtību sadalījuma likumi. Tomēr saskaņā ar [72] un [55] gadījumā ar racionālu apkalpošanas laiku varbūtības sadalījums var tuvuoties eksponenciālajam sadalījumam. Tādā gadījumā minēto mainīgo lielumu vidējās vērtības būs vienādas ar $1/\lambda$ un $1/\mu$.

Tīkla veikspēju (AL caurlaidspēju) saskaņā ar šo modeli var izteikt kā:

$$\eta = (1 - p_0)\mu, \quad (2.3.)$$

kur μ – pieteikumu apstrādes intensitāte; p_0 – varbūtība, ka kanāls ir brīvs, t. i., sistēma nesaņems pieprasījumus.

AL caurlaidspēja vienam klientam atkarībā no klientu skaita M :

$$\eta_1 = (1 - p_0) \frac{\mu}{M}, \quad (2.4.)$$

kur p_0 var aprēķināt pēc izteiksmes:

$$p_0 = \left[\sum_{k=0}^M \frac{M!}{(M-k)!} \left(\frac{\lambda}{\mu} \right)^k \right]^{-1} = \left[\sum_{k=0}^M \frac{M!}{(M-k)!} \rho^k \right]^{-1}, \quad (2.5.)$$

kur ρ – sistēmas noslodzes koeficients.

Pēc modeļa izstrādes un iegūto rezultātu analīzes var noskaidrot transportlīdzekļu bezvadu sakaru tīkla caurlaidspēju un tās atkarību no ienākošo plūsmu skaita bezvadu piekļuves punkta darbības zonā.

Eksperimentālo un analītisko rezultātu salīdzinājums

2.6. tabulā un 2.17. a un b attēlā apkopoti eksperimentāli iegūtie un, izmantojot daudztermināļu sistēmas modeli, analītiski aprēķinātie AL caurlaidspējas rezultāti. Tika noteikta individuālā AL caurlaidspēja vienam klientam un kopējā bezvadu tīkla (bezvadu piekļuves punkta) AL caurlaidspēja atkarībā no klientu skaita.

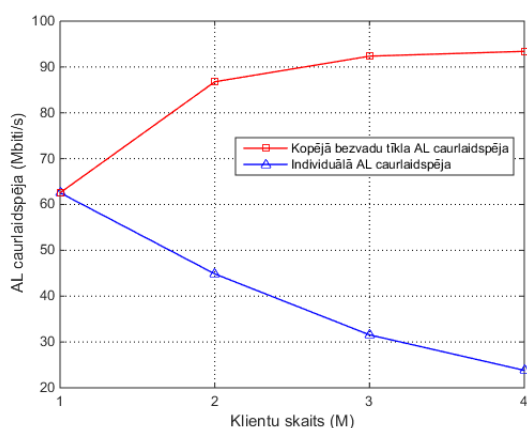
2.6. tabula

Eksperimentāli un analītiski iegūtie AL caurlaidspējas rezultāti

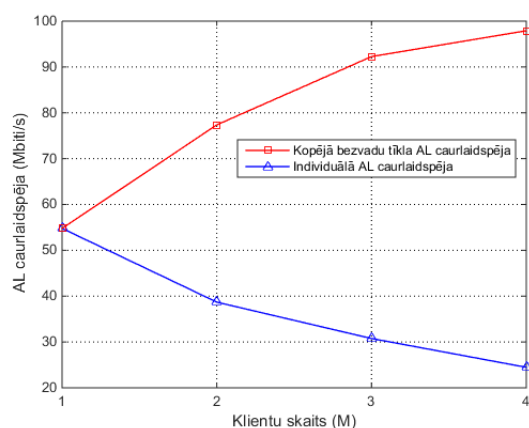
Klientu skaits	Eksperimentu vid. AL caurlaidspēja vienam klientam $\bar{\eta}_1$, Mbit/s	Eksperimentu kopējā vid. bezvadu tīkla AL caurlaidspēja $\bar{\eta}$, Mbit/s	Modeļa AL caurlaidspēja vienam klientam η_1 , Mbit/s	Modeļa kopējā bezvadu tīkla AL caurlaidspēja η , Mbit/s
1	62,55	62,55	54,78	54,78
2	44,85	86,77	38,69	77,38
3	31,55	92,36	30,76	92,27
4	23,81	93,41	24,47	97,90

No iegūtajiem rezultātiem redzams, ka starpība starp eksperimentāli iegūtajiem datiem un analītiski noteiktajiem nepārsniedz 16 %, kas ir labs rezultāts.

Iegūto likumsakarību aprēķini tika realizēti *Matlab* vidē, aprēķinu kodi apkopoti 2. pielikumā.



a) Eksperimentālie mērījumi



b) Matemātiskais modelis

2.17. att. Noteiktās likumsakarības starp kopējo un individuālo AL caurlaidspēju un klientu skaitu.

2.17. a un b attēlā redzams, ka individuālā AL caurlaidspēja vienam klientam samazinās, pieaugot klientu skaitam tīklā. Klienta individuāli sasniedzamā caurlaidspēja ir atkarīga no katra klienta iekārtas veiktspējas. Turpretī kopējā bezvadu tīkla AL caurlaidspēja, pieaugot bezvadu klientu skaitam, pieaug, jo bezvadu tīkla mezglu veiktspēja tiek projektēta lielam klientu skaitam. Sakarā ar *TCP* mehānisma darbību AL caurlaidspējas kāpums ir nelineārs. Klientu skaitam pieaugot, tiks sasniegta tīkla mezgla (*AP*) veiktspējas augšējā robeža.

2.8. WLAN un LTE bāzēta automobiļu sakaru tīkla tehniski ekonomiskais novērtējums

Promocijas darbā tiek apskatītas *Wi-Fi* un *LTE* tehnoloģijas, lai izveidotu integrētu datu pārraides risinājumu, kas ir piemērojams transportlīdzekļu (automobiļu) vajadzībām, konkrēti informācijas un izklaides, kā arī daļēji satiksmes trafika efektivitātes, vadības un transporta sistēmu komerciālu pakalpojumu nodrošināšanai, tāpēc ir svarīgi noskaidrot, vai šāda hibrīda sakaru kanāla izveide ir tehniski un ekonomiski pamatota. Apakšnodaļā vispirms tiek novērtēts datu kanāla pieslēgums, izmantojot tikai tiešo *LTE* kanālu, pēc tam – arī paplašinātais divrangu sakaru kanāls, izmantojot *Wi-Fi* un *LTE* tehnoloģijas. Apskatāmie datu pārraides risinājumi tika novērtēti, izmantojot tādus tehniskos parametrus kā aplikācijas līmeņa caurlaidspēja [6], [177] un atbildes jeb reakcijas laiks. Tika novērtēti arī tādi efektivitātes rādītāji (angļu val. *efficiency indicators*) kā izmaksas un mobilā tīkla atslogošanas (angļu val. *offloading*) parametrs. Iegūtie rezultāti ir atspoguļoti zinātniskajā publikācijā [7].

Tiešais *LTE* kanāls

Vienkāršākais veids, kā nodrošināt komunikāciju kanālu starp mobilo transportlīdzekli un attālināto serveri, piemēram, komerciālo pakalpojumu sniedzēju interneta tīklā, ir izmantot tiešo *LTE* savienojumu. Tiešā *LTE* kanāla risinājums sastāv no mobilā lietotāja *LTE* aparatūras (maršrutētāja), kas izvietota transportlīdzeklī, un mobilā 4G jeb *LTE* tīkla. Sakaru kanāls tiek terminēts attālinātajā pakalpojumu sniedzēja serverī (2.18. a att.).

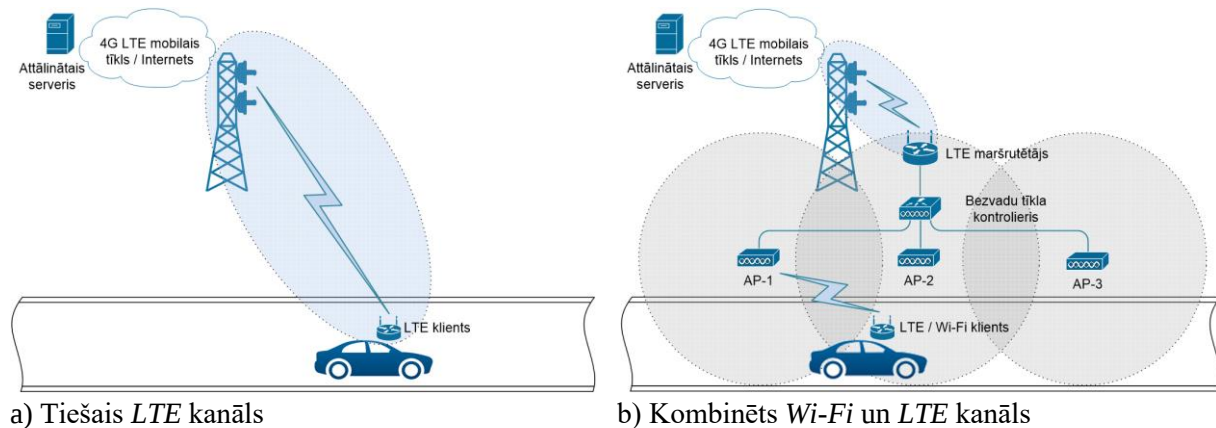
Integrēts Wi-Fi un LTE kanāls

Wi-Fi tīkli galvenokārt tiek izmantoti, lai nodrošinātu bezvadu sakarus statiskiem klientiem vai arī tādiem klientiem, kas pārvietojas ar nelielu ātrumu, t. i., kājāmgājējiem. Tomēr veiktie pētījumi un eksperimenti parāda, ka Wi-Fi tehnoloģiju veiksmīgi var izmantot arī transporta sakaru tīklos, lai nodrošinātu tādos komerciālos pakalpojumus kā piekļuve interneta tīklam, izklaide, tiešsaistes navigācijas datu nodrošināšana, liela apjoma foto un video pārsūtīšana [5], [132]. Ieinteresētās puses ir gan nekomerciālo transportlīdzekļu, gan komerciālo transportlīdzekļu turētāji tādās uzņēmējdarbības nozarēs kā pasažieru un kravu pārvadājumi.

Praksē Wi-Fi transporta sakaru piekļuves tīklu veiksmīgi var izvērst pilsētvidē, kur jau Wi-Fi tīkla pārklājums ir plaši pieejams. Wi-Fi bezvadu piekļuves punktus (AP), kas nodrošina ceļmalas aparatūras (RSU) funkcijas, var izvietot arī gar automaģistrālēm. Esošā telekomunikāciju vai enerģētikas sektora infrastruktūra, piemēram, telekomunikāciju vai elektrobarošanas līniju balsti, kā arī ceļu apgaismes laternas, var kalpot par RSU iekārtu izvietojanas punktiem [170].

Wi-Fi tīkla infrastruktūru veiksmīgi var izmantot, lai ar sakariem nodrošinātu tādas specifiskas vietas, kur mobilā tīkla pārklājums nav pieejams, piemēram, pazemes autostāvvietas un tuneli, kuru garums var pārsniegt pat vairākus desmitus kilometru.

Par atvilces tīklu šādam izvērstam Wi-Fi tīklam var izmantot LTE mobilo tīklu. Šāds integrēts divu rangu tīkla risinājums redzams 2.18. b attēlā, kur Wi-Fi klientu datu plūsma tiek apvienotas bezvadu tīkla kontrolierī un, izmantojot LTE maršrutētāju, pārsūtītas uz interneta tīklu. Tādējādi ir iespējams ietaupīt, abonējot mazāku LTE kanālu skaitu, salīdzinot ar risinājumu, kur katram mobilajam klientam individuāli tiek piešķirts tiešais LTE kanāls (2.18. a att.).



2.18. att. Piekļuve datu tīklam, izmantojot dažādas metodes.

Tehnisko parametru novērtējums

Šajā sadaļā tiek novērtēti tādi tehniskie parametri jeb rādītāji, ar kuriem var raksturot tīkla veiktspēju, un tie ir: aplikācijas līmeņa caurlaidspēja (AL) un atbildes laiks. Aproximējot eksperimentālos rezultātus vispārējam gadījumam un nosakot sistēmas aplikācijas līmeņa caurlaidspēju η un vidējo atbildes laiku $\bar{T}$, tiek izmantots daudztermināļu sistēmas modelis.

Tehniskie parametri tiek novērtēti tikai integrētam *Wi-Fi-LTE* kanālam. Šāda sistēma var tik reprezentēta kā divrangu tīkla modelis, kā tas redzams 2.18. b attēlā.

Eksperimentāli tika novērtēta testgultnes automobiļu sakaru tīkla veiktspēja, ko veidoja apvienoti *Wi-Fi* un *LTE* šūnu tīkli savienojumā ar automobili jeb mobilo klientu, kas pārvietojās gar *Wi-Fi* bezvadu piekļuves punktiem ar ātrumu 20 km/h, 50 km/h un 70 km/h. Starp automobiļa klientu un attālināto serveri tika izveidota datu sesija, nosūtot 1 MB lielus ziņojumus.

Matlab vidē realizēto tehnisko parametru un iegūto likumsakarību aprēķinu kodi apkopoti 3. pielikumā.

Aplikācijas līmeņa caurlaidspēja

Vispirms saskaņā ar [25], [91] un 2.5. izteiksmi tiek aprēķināta p_0 vērtība, tā ir varbūtība, ka kanāls ir brīvs, t. i., sistēma nesaņems pieprasījumus, ja automobiļu skaits ir M , atrodoties bezvadu piekļuves punkta *AP* pārklājuma zonā. 2.5. izteiksmē $\lambda / \mu = \rho$ ir noslodzes koeficients, kas raksturo sistēmas utilizāciju jeb noslodzi. Tālāk aprēķinos tiek pieņemts, ka $\rho = 0,5$.

Mobilo klientu (automobiļu) skaits *Wi-Fi* bezvadu punkta pārklājuma zonā tiek apzīmēts ar M . Pienākošo pieteikumu intensitāte no viena automobiļa ir λ . Pakalpojuma pieteikumu apstrādes intensitāte kontrolierī un *LTE* kanālā tiek apzīmēta ar μ . Tīkla veiktspēju, šajā gadījumā aplikācijas līmeņa caurlaidspēju η , atbilstoši izmantotajam modelim var izteikt kā:

$$\eta = \mu(1 - p_0), \quad (2.6.)$$

kur μ – pieteikumu apstrādes intensitāte.

Lai iegūtu μ vērtības, tika izmantoti eksperimentāli iegūti dati, no kuriem tika aprēķinātas vidējo datu pārraides ātrumu $\bar{\eta}$ vērtības dažādos automobiļa pārvietošanās ātrumos [6], tādējādi $\bar{\eta} = \mu$. 2.7. tabulā apkopots vidējais datu pārraides ātrums $\bar{\eta}$ jeb pakalpojumu pieprasījumu apstrādes intensitāte μ atkarībā no automobiļa pārvietošanās ātruma divrangu tīklā.

2.7. tabula

Eksperimentāli iegūto datu pārraides ātrumu vidējās vērtības

Automobiļa ātrums v , km/h	Vidējais datu pārraides ātrums $\bar{\eta}$, Mbit/s
20	12,99
50	11,39
70	10,69

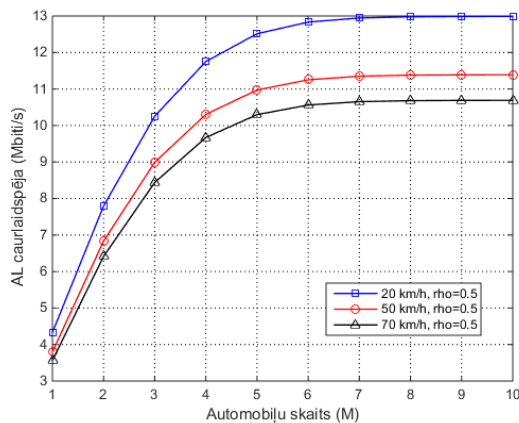
2.19. a attēlā redzama iegūtā likumsakarība starp tīkla aplikācijas līmeņa caurlaidspēju η un automobiļu skaitu M dažādos braukšanas ātrumos v (20 km/h, 50 km/h un 70 km/h) un $\rho = 0,5$. No iegūtajiem rezultātiem redzams, ka maksimālā sistēmas AL caurlaidspēja tiek iegūta, ja $M = 9$.

Atbildes laiks

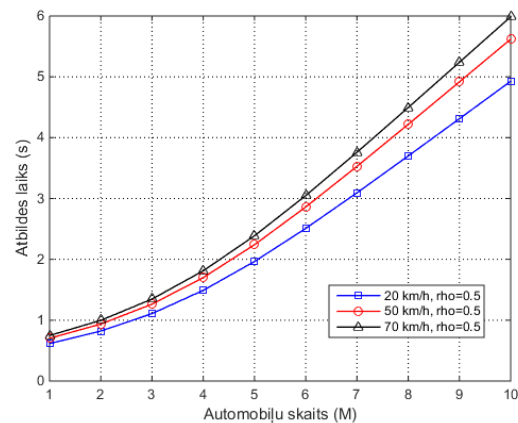
Nākamais tehniskais parametrs, kas tika novērtēts, ir sistēmas (sastāv no *Wi-Fi* kontroliera, *LTE* maršrutētāja un attālinātā servera) vidējais atbildes laiks $\bar{T}$. Saskaņā ar [25], sistēmas vidējais domāšanas laiks ir $1/\lambda$, un sistēmas vidējais atbildes laiks ir:

$$\bar{T} = \frac{M}{\mu(1 - p_0)} - \frac{1}{\lambda}. \quad (2.7.)$$

2.19. b attēlā redzama iegūtā likumsakarība starp vidējo atbildes laiku $\bar{T}$ un automobiļu skaitu M dažādos braukšanas ātrumos v (20 km/h, 50 km/h un 70 km/h) un $\rho = 0,5$, lai pārsūtītu 1 MB lielu failu.



a)



b)

2.19. att. a) Tīkla aplikācijas līmeņa caurlaidspēja atkarībā no automobiļu skaita, ātruma un tīkla noslodzes; b) Vidējais atbildes laiks atkarībā no automobiļu skaita, ātruma un tīkla noslodzes.

2.19. b attēlā redzama iegūtā atbildes laika atkarība no klientu skaita. Ir pieņemts, ka dialoga režīmā atbildes laiks nedrīkst pārsniegt trīs sekundes [72]. Tādēļ var secināt (2.19. b att.), ka sistēmā vienlaikus aktīvu klientu (automobiļu) skaits nedrīkst pārsniegt sešus.

Tehnisko parametru AL caurlaidspējas un atbildes laika likumsakarība atkarībā no automobiļu skaita uz ceļa redzama 2.20. a attēlā ($v = 20$ km/h; $\rho = 0,2$; $M = 26$; pārsūta 1 MB failu).

Efektivitātes rādītāju novērtējums

Lai novērtētu pētāmā *Wi-Fi* un *LTE* telekomunikāciju infrastruktūras risinājuma efektivitāti, tika noteikti šādi efektivitātes rādītāji: risinājuma izmaksas un mobilā tīkla *Wi-Fi* bāzētas atslogošanas parametrs.

Izmaksas tika novērtētas integrētam *Wi-Fi-LTE* kanālam, kā arī tiešajam *LTE* kanālam. Atslogošanas parametrs tika novērtēts integrētam *Wi-Fi-LTE* kanālam.

Izmaksas

Šajā sadaļā dots piedāvāto telekomunikāciju risinājumu ekonomiskais novērtējums, lai nodrošinātu datu pārraides kanālu mobiliem objektiem (automobiļiem). Izmantojot 2.8. izteiksmi, var tikt noteiktas vispārinātās izmaksas (angļu val. *generalized costs*).

$$G = k_p K_{ieg.} + U_{izm.}, \quad (2.8.)$$

kur G – vispārinātās izmaksas, kas kombinē kopā kapitālieguldījumus $K_{ieg.}$, kas reizināts ar pašizmaksas koeficientu k_p un pieskaitītas uzturēšanas izmaksas gadā $U_{izm.}$. Pašizmaksas koeficients $k_p = 1 / m$, kur m – periods gados, aprēķinos pieņemts, ka $m = 3$.

Izmaksu analīzi nepieciešams veikt fiksētam ceļa posma garumam. Testgultnes lauka mērījumi tika veikti 260 m garā ceļa posmā, tāpēc izmaksu analīze tiks veikta tieši tik garam ceļa posmam.

Veiktajos eksperimentos attālums starp bezvadu piekļuves punktiem AP bija 100 m, jo tāds ir *IEEE 802.3ab* standarta ierobežojums. Tika izmantoti trīs AP. Šāds attālums starp diviem AP ļauj nodrošināt stabilu *IEEE 802.11n/ac* bezvadu tīkla pārklājumu, kur AP strādā jau ar ievērojamu bezvadu tīkla pārklājuma rezervi (angļu val. *cell overlap*). Pēc šāda scenārija, palielinot kopējo *Wi-Fi* tīkla pārklājuma zonu, AP būtu jāizvieto ik pēc 100 m, vai arī būtu jāpāriet uz optiskajiem pieslēgumiem, kas ļautu palielināt attālumu starp AP vismaz līdz 200 m. Lai optimāli noklātu ceļa posmu līdz 1 km, būtu nepieciešams izvietot četrus līdz sešus AP, ja izmanto standarta omnivirziena (angļu val. *omnidirectional*) antenas. AP skaitu varētu samazināt, izmantojot specializētas sektora antenas (angļu val. *directional patch antennas*). Precīzs AP skaits ir atkarīgs arī no tā, kādas prasības tiek definētas datu pārraides tīklam, piemēram, datu pārraides ātrums, šūnu pārklāšanās.

Kapitālieguldījumi

Kapitālieguldījumi ($K_{ieg.}$) ietver investīcijas, kas veiktas infrastruktūrā, t. i., aparatūras un to komponentu izmaksas. Kapitālieguldījumi tiek aprēķināti pēc šādas izteiksmes:

$$K_{ieg.} = k_p (n K_{ieg.}^{AP} + K_{ieg.}^{Kontrl.} + K_{ieg.}^{LTE \text{ maršr.}}), \quad (2.9.)$$

kur n – bezvadu piekļuves punktu (AP) skaits konkrētajai distancei (aprēķinos izmantosim $n = 3$); $K_{ieg.}^{AP}$ – viena AP cena; $K_{ieg.}^{Kontrl.}$ – *Wi-Fi* bezvadu kontroliera cena; $K_{ieg.}^{LTE \text{ maršr.}}$ – *LTE* maršrutētāja cena.

Aprēķinot izmaksas, 2.9. izteiksme ir paredzēta gadījumiem, kur bezvadu tīkla virsvadība tiek deleģēta atsevišķai iekārtai, t. i., *Wi-Fi* kontrolierim ($K_{ieg.}^{Kontrl.}$). Pieejami dažādu ražotāju risinājumi, kur šo funkciju var deleģēt kādam no bezvadu piekļuves punktiem (AP), tādā veidā samazinās kopējais iegādājamo iekārtu apjoms. Savukārt *LTE* maršrutētāja iekārtu var aizvietot ar daudz lētāku risinājumu, piemēram, *LTE USB* spraudni, tādējādi var pieņemt:

$$K_{ieg.} = k_p (n K_{ieg.}^{AP} + K_{ieg.}^{LTE \text{ maršr.}}), \quad (2.10.)$$

Bezvadu piekļuves punkta cena var svārstīties. Ārpustelpu apstākļiem piemērots AP būs dārgāks, salīdzinot ar iekštelpām paredzētiem AP. Āra apstākļiem paredzētu iekārtu var izmantot mitrā un putekļainā vidē, tā spēj darboties plašā temperatūru diapazonā, vismaz sākot no $-20\text{ }^{\circ}\text{C}$ līdz $+60\text{ }^{\circ}\text{C}$. Šāda veida iekārtas atbalsta arī elektrobarošanu caur *Ethernet* kabeļiem, izmantojot *PoE* (angļu val. *Power over Ethernet*) tehnoloģiju, kas balstās, piemēram, *IEEE 802.3af* vai *802.3at* standartos. Iekārtas cena ir atkarīga arī no atbalstāmajiem *WLAN IEEE 802.11* protokoliem un citām funkcionālajām iespējām.

AP uzstādīšanai nepieciešams apmācīts personāls, kas spētu tos uzstādīt arī uz nelieliem torņiem.

Tika veikta tirgus izpēte, lai noskaidrotu minimālās aparatūras iegādes un tās montāžas izmaksas. Kopējo kapitālieguldījumu izmaksu aprēķina rezultāti apkopoti 2.8. tabulā.

Uzturēšanas izmaksas

Uzturēšanas izmaksas gadā ($U_{izm.}$) ietver tādus izdevumus, kā apkalpošanas un remonta izdevumi, elektroenerģijas izmaksas, aparatūras izvietojanas (vietas) nomas pakalpojuma izmaksas objektā un pieslēguma pie atvilces *LTE* piekļuves tīkla izmaksas gadā.

Nomas maksa par sakaru aparatūras izvietojanas laukumu (atrašanās vietu) var atšķirties atkarībā no līguma, kas noslēgts ar infrastruktūras īpašnieku. Iekārtu uzturēšanas (ekspluatācijas) izmaksas var sasniegt 5 % no kopējās infrastruktūras vērtības [7]. Elektroenerģijas patēriņa aprēķinam tika izmantoti mājas vai neliela biroja kategorijas *Wi-Fi* bezvadu piekļuves punktu vidējie elektroenerģijas patēriņa rādītāji ($\sim 9\text{ W}$), piemērojot vietējā atvērtā elektroenerģijas tirgus vidējās pieslēguma izmaksas, ieskaitot iekārtu elektroenerģijas patēriņu (3,5 EUR/mēn., 25.06.2018. dati) [7], [151].

Wi-Fi tīkla piekļuvi interneta tīklam var realizēt, gan izmantojot mobilo 4G/5G tīklu, gan optisko šķiedru kabeļu tīklu. *LTE* tehnoloģiju var izmantot, lai nodrošinātu piekļuvi interneta tīklam ceļmalā esošiem AP vietās, kur optisko šķiedru kabeļi nav pieejami vai to izbūve ir sarežģīta un dārga. Mobilie operatori piemēro *LTE* piekļuves pakalpojuma maksu atkarībā no pārsūtītā datu apjoma. Izskatot vietējo mobilo operatoru izcenojumus par *LTE* pakalpojumiem interneta piekļuvei un pieņemot, ka datu trafika apjoms šādam transporta sakaru tīklam būs konstanti vienāds ar sistēmas noslodzes koeficientu $\rho = 0,5$, tika secināts, ka visizdevīgākais interneta datu pieslēgums būtu “Mobilais internets datorā” bez datu apjoma ierobežojuma. Aprēķiniem tika izmantota mobilo operatoru piedāvātā šāda pakalpojuma vidējā cena (23,1 EUR/mēn., 25.06.2018. dati) [7].

2.8. tabulā apkopotas uzturēšanas izmaksas gan gadījumam ar tiešu, katram klientam piešķirtu individuālu *LTE* kanālu, gan gadījumam, kad datu pārsūtīšana notiek, izmantojot divrangu heterogēnu tīklu (angļu val. *HetNet – Heterogeneous Network*), t. i., *Wi-Fi* un *LTE* tīkliem. Aprēķinos netiek ņemtas vērā *Wi-Fi* un *LTE* galiekārtu iegādes izmaksas, kā arī *LTE* tīkla infrastruktūras izbūves izmaksas. Datu pārsūtīšana *Wi-Fi* tīklā ir bezmaksas, savukārt *LTE* tīklā tas ir maksas pakalpojums.

2.8. tabulā redzams, ka gadījumā ar sešiem klientiem, kur katram klientam tiek piešķirts tiešais *LTE* kanāls, šo *LTE* pieslēgumu kopējās un vispārinātās izmaksas pārsniedz *Wi-Fi* un

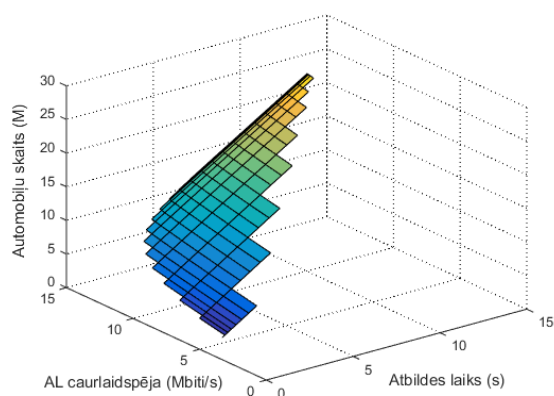
LTE bāzēta risinājuma, kur izmanto vienu LTE pieslēgumu, infrastruktūras izbūves un uzturēšanas izmaksas 260 m garā ceļa posmā.

2.8. tabula

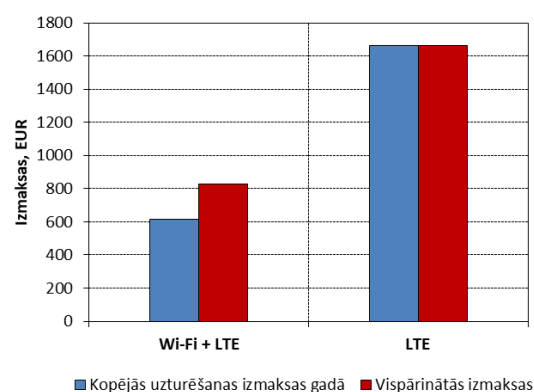
Aprēķinātās izmaksas testgultnes infrastruktūrai

Apraksts	Aptuvenās izmaksas, EUR			
	Integrēts Wi-Fi un LTE kanāls	Skaits	Tiešais LTE kanāls	Skaits
Bezvadu piekļuves punkts (AP)	147	3	–	–
LTE maršrutētājs / LTE USB spraudnis	54	1	–	–
Aparatūras uzstādīšanas izmaksas	50	3	–	–
Kopējās kapitāliegildījumu izmaksas, $K_{ieg.}$	645	–	0	–
Elektroenerģijas patēriņa izmaksas gadā	42	3	–	–
Apkalpošanas un remonta izmaksas gadā (<5 %)	32,25	–	–	–
Sakaru aparatūras lokācijas (izvietojšanas) laukuma nomas izmaksas gadā	60	3	–	–
Atvilces LTE piekļuves tīkla pakalpojuma izmaksas gadā	277,2	1	277,2	6
Kopējās uzturēšanas izmaksas gadā, $U_{izm.}$	615,5	–	1663,2	–
Vispārinātās izmaksas, G	830,5		1663,2	

Izstrādāto izmaksu aprēķināšanas metodi var izmantot arī gadījumos, kad otrā ranga tehnoloģija LTE tiek aizvietota ar pieslēgumu pie fiksētā tīkla. Šāds risinājums ir ekonomiski izdevīgs un lietojams gar ceļmalām, automaģistrālēm un autotransporta tuneļu sistēmās. Pētāmo automobiļu telekomunikāciju tīklu aprēķinātās izmaksas parādītas 2.20. b attēlā.



a)



b)

2.20. att. a) Tehnisko parametru AL caurlaidspējas un atbildes laika atkarība no automobiļu skaita; b) Automobiļu sakaru tīklu izmaksas.

Atslogošanas parametrs

Līdzās transporta telekomunikāciju tīkla ekonomiskajam pamatojumam svarīgs ir arī efekts, kas tiek iegūts, piemērojot hibrīdo Wi-Fi–LTE tīklu. Šo efektu promocijas darba autors nosauca

par “Wi-Fi bāzētu un LTE koncentrētu mobilā tīkla atslogošanu” jeb mobilā tīkla resursu atbrīvošanu, ko raksturo Wi-Fi bāzētas un LTE koncentrētas atslogošanas parametrs γ , kas arī ir saistīts ar izmaksām, un tādējādi tas ir viens no ekonomiskajiem rādītājiem.

Pēc definīcijas mobilā tīkla atslogošana ir tehnika mobilā tīkla lietotāju datu plūsmu pārslēgšanai no mobilā tīkla uz citu bezvadu tehnoloģiju tīkliem, lai nodrošinātu piekļuvi interneta tīklam. Tā paredz alternatīvu, papildinošu bezvadu tīklu izmantošanu, lai pārsūtītu datus, kas sākotnēji tika paredzēti sūtīšanai mobilajā tīklā [102]. Wi-Fi tehnoloģija tiek uzskatīta par vienu no primārajām mobilo tīklu atslogošanas tehnoloģijām [30], [75].

Atšķirībā no klasiskās mobilās tīkla atslogošanas tehnikas pētāmā automobiļu hibrīdā Wi-Fi un LTE sakaru tīkla gadījumā (2.18. b att.) LTE tīkla atslogošana izpaužas, kad mobilā tīkla klienti, t. i., automobiļi un to pasažieri, ierodoties Wi-Fi pārklājuma zonā, automātiski atslēdzas no LTE tīkla un mēģina izveidot jaunus datu savienojumus, izmantojot Wi-Fi infrastruktūru. Viss mobilo klientu datu trafiks tiek koncentrēts Wi-Fi bezvadu tīkla kontrolierī, un tad caur LTE maršrutētāju kā apvienota LTE datu plūsma tiek pārsūtīta uz interneta tīklu. Lai noteiktu, kāds ir ieguvums un cik daudz resursus var atslogot, tālāk tiek apspriesti eksperimentāli un ar modeļiem iegūtie rezultāti un novērtēts Wi-Fi bāzētas un LTE koncentrētas atslogošanas parametrs γ .

2.19. a attēlā redzams, ka, sešiem automobiļiem pārvietojoties ar ātrumu 70 km/h un $\rho = 0,5$, aplikācijas līmeņa caurlaidspēja ir 10,59 Mbit/s. Savukārt maksimālā aplikācijas līmeņa caurlaidspēja automobiļiem pārvietojoties ar ātrumu 20 km/h un $\rho = 0,5$ ir 13 Mbit/s. Sešiem klientiem pārvietojoties ar 70 km/h, LTE kanāls netiek noslogots par 2,41 Mbit/s. No otras puses, ja tīklam ir pieslēgti seši klienti, izmantojot tikai tiešos LTE kanālus ar noslodzes koeficientu $\rho = 0,5$, tad kopējie neizmantotie LTE kanālu resursi ir $13 \times 0,5 \times 6 = 39$ Mbit/s. Attiecība starp šiem neizmantotajiem resursiem pie vienādas sakaru kanālu noslodzes tika nosaukta par “Wi-Fi bāzētu, LTE koncentrētu atslogošanas parametru γ ”. Tas nozīmē, ka šajā gadījumā γ var sasniegt vērtību $39 / 2,41 = 16,2$ reizes. Tik liels ir ieguvums, pārvirzot un pēc tam apvienojot individuālu LTE klientu datu plūsmas uz integrētu Wi-Fi un LTE sakaru kanālu. Tādējādi aktīvo LTE kanālu skaits tika samazināts no sešiem līdz vienam LTE pieslēgumam, kā rezultātā mobilais tīkls tika atslogots.

Wi-Fi bāzēta un LTE koncentrēta atslogošana ļauj atslogot mobilo tīklu un samazināt ikgadējās kopējās transporta sakaru tīkla izmaksas.

2.9. Kopsavilkums un secinājumi

WLAN bāzētos transporta sakaru tīklos mobilā klienta pārvietošanās ātrums atbilst automobiļa braukšanas ātrumam. Šāda mobilā klienta vidējā bezvadu tīklā sasniedzamā caurlaidspēja būs mazāka, salīdzinot ar standarta stacionāra vai klejojoša WLAN klienta caurlaidspēju. Atšķirība sasniedzamajā vidējā veiktspējā galvenokārt saistīta tieši ar dažādiem klientu pārvietošanās ātrumiem. Pieaugot automobiļu pārvietošanās ātrumam, mobilais klients ir spiests biežāk izpildīt pārslēgšanās procedūras starp bezvadu piekļuves punktiem. Līdz ar to aktīvās datu pārraides laiks AP zonā samazinās, un proporcionāli vairāk laika tiek tērēts uz pārslēgšanās procedūras organizēšanu un tās izpildi, un tā rezultātā vidējā caurlaidspēja krītas.

Cits būtisks iemesls vidējās caurlaidspējas samazinājumam ir saistīts ar apkārtējās vides ietekmi uz bezvadu datu pārraidi, kas kļūst daudz agresīvāka, salīdzinot ar standarta klienta apstākļiem. Papildus iespējami dažādi ārējo traucējumu avoti. Pārvietojoties ar lielāku ātrumu, notiek intensīvāka radioviļņu atstarošanās, līdz ar to palielinās varbūtība, ka klienta dati var tikt pazaudēti vai bojāti, un tas savukārt nozīmē, ka pazaudētie dati būs jāpārsūta atkārtoti. Rezultātā caurlaidspēja samazinās, jo pieaug virstēriņu īpatsvars. Tas var izraisīt arī pārslēgšanās procedūras aiztures pieaugumu.

Tīkla veikspēju un trafika raksturu var ietekmēt vairāki faktori. Tīkla kopējā veikspēja ir atkarīga no datu pārraides vidē izmantotās individuālās aparatūras veikspējas, tās galvenie parametri ir procesora veikspēja, buferatmiņas apjoms, kā arī atbalstītie *IEEE 802.11* un mobilo šūnu tīklu standarti.

Divrangu *Wi-Fi* un *LTE* sakaru tīklā katrs infrastruktūras tīkla mezgls apstrādā pienākošās plūsmas ar konkrētu veikspēju, un maksimālā tīkla veikspēja (caurlaidspēja) ir tieši atkarīga no šiem mezgliem. Tā ir atkarīga gan no pirmā ranga, gan arī no otrā ranga tīkla, un maksimālā tīkla veikspēja būs šo abu divu rangu sistēmu maksimālā, taču savstarpēji minimālā veikspēja.

Bezvadu tīkla veikspēju un datu trafika raksturu ietekmē *802.11 MAC* līmeņa pakāpeniska datu pārraides ātruma pielāgošana sesijas izveides sākumā un *802.11 MAC* līmeņa atkārtotas pazaudēto kadru pārsūtīšanas mehānisms. Bezvadu tīkla veikspēja un trafika raksturs tiek ietekmēts arī *TCP* līmenī, kur ir realizēti plūsmas kontroles un tīkla pārslodzes kontroles algoritmi, kas tiek izpildīti visas sesijas laikā, kā rezultātā šie algoritmi, it īpaši *TCP* lēnā starta mehānisms, ievērojami samazina aplikācijas līmeņa caurlaidspēju.

802.11 MAC slānī, kur tiek izpildīta skenēšanas, atvērtās sistēmas autentifikācijas un asociācijas procedūras, vislielāko papildinājumu pārslēgšanās procedūras aizturai rada skenēšanas procedūra. Tā veido līdz pat 90 % no aiztures, ko rada šīs procedūras kopā.

Transporta *IEEE 802.11* bezvadu tīklos tiek rekomendēts pāriet uz centralizētu *WLAN* tīkla pārvaldību, izmantojot bezvadu tīkla kontrolierus. Centralizēta *WLAN* tīkla pārvaldība atvieglo bezvadu tīklu uzturēšanu, izmantojot vadības plaknes funkcijas, kā arī piedāvā vienotu drošības līmeni un nodrošina koordinētu kontroles plaknes funkciju darbību.

Svarīgi ir izprast *WLAN* drošības mehānismu darbības principus, kas tiek izmantoti, autentificējot mobilos klientus, jo katra drošības shēmas realizācija atstāj atšķirīgu ietekmi uz pārslēgšanās procedūras aizturi, kas īpaši kritiski ir oportunistiskos automobiļu sakaru tīklos. Dialogs starp bezvadu tīkla kontrolieri un autentifikācijas serveri, kā arī kriptogrāfisko atslēgu ģenerēšana un apmaiņa starp klientu un *AP* vai *WLC*, var aizņemt ievērojamu laiku.

Automobiļu sakaru tīklos ar centralizētu *WLAN* arhitektūru tiek rekomendēts ieviest *WPA2-Enterprise* vai *WPA3-Enterprise* drošības mehānismus, kas nodrošina visaugstāko drošības līmeni bezvadu sakaru tīklos, kas jāintegrē kopā ar ātrās pārslēgšanās procedūras risinājumiem.

Lai nodrošinātu vienlaidu jeb nemanāmo pārslēgšanās procedūru, ir jāizvairās no laikietilpīgās *DHCP* procedūras izpildes, klientam jānodrošina *IP* adreses saglabāšanas iespēja. Īpaši kritiski tas ir reāllaika pakalpojumu nodrošināšanas gadījumos.

WLAN un mobilo tīkla tehnoloģiju, piemēram, *4G LTE* vai *5G*, apvienošanas risinājumi var nodrošināt nepieciešamo mobilitāti *WLAN* bāzētos automobiļu sakaru tīklos tādās vietās, kur

WLAN pārklājums nav pieejams. Šāda pieeja ļauj palielināt arī kopējo mobilo tīklu kapacitāti un nodrošināt mobilā tīkla pamattehnoloģiju atslogošanu.

Datu savienojuma vidējā AL caurlaidspēja ir atkarīga no pārslēgšanās procedūru ilguma. Ja mobilais klients pārvietojas ar ātrumu 20 km/h, pārslēgšanās procedūra starp bezvadu piekļuves punktiem tiek izpildīta korekti. Pārvietojoties ar lielāku ātrumu, AL caurlaidspēja degradējas, un, pārvietojoties ar ātrumu 90 km/h, pārslēgšanās procedūra starp AP kļūst nestabila.

Saskaņā ar iegūtajiem eksperimentālajiem rezultātiem var secināt, ka *Wi-Fi* un *LTE* integrētā sakaru kanāla veiktspēja ir atkarīga arī no izmantotā *LTE* maršrutētāja parametriem. Izmantojot dažādus *LTE* maršrutētājus, autotransporta bezvadu sakaru tīkla AL caurlaidspēja var atšķirties par 10–20 %. To var izskaidrot ar šo tīkla mezglu veiktspēju, kā arī tiem var būt atšķirīga traucējumu noturība iekārtas *LTE* daļā.

Eksperimentāli tika īstenoti scenāriji, kuros bija iesaistīti vairāki transportlīdzekļi. Tas ļāva iegūt eksperimentālus mērījumu rezultātus, kas atbilst reāliem vai pietuvinātiem satiksmes plūsmas apstākļiem. Dažādu mobilo klientu kustības scenāriju izmantošana deva iespēju dinamiski mainīt un pārvietot mobilo klientu radīto datu trafika slodzi starp testgultnes infrastruktūras bezvadu piekļuves punktiem. Pēc eksperimentāli iegūto AL caurlaidspējas rezultātu analīzes var secināt, ka AL caurlaidspēja ir atkarīga no AP apkalpošanas zonā vienlaikus esošu mobilo klientu skaita. Tas atstāj iespaidu gan uz individuālajiem mobilo klientu AL caurlaidspējas rādītājiem, gan arī uz kopējo bezvadu tīkla veiktspēju. Ja bezvadu tīklā ir vairāki mobilie klienti vienlaikus, tas nozīmē sāncensību par bezvadu tīkla resursiem. Tas atspoguļojas arī iegūtajos mērījumu grafikos kā neregulāri trafika kritumi un vidējās individuālās AL caurlaidspējas samazinājums.

Veicot eksperimentāli iegūto mērījumu datu analīzi ar statistisku paņēmieni palīdzību, tika noteikts, ka divrangu *Wi-Fi* un *LTE* sakaru tīkla testgultnē pārsūtītais kustīgo klientu trafiks savstarpēji ir korelēts. Tas ir saistīts ar to, ka automobiļu klienti vēršas pie vieniem un tiem pašiem bezvadu tīkla resursiem, kas tiek koplietoti. Testgultnē realizētā automobiļu *Wi-Fi* bāzēta sakaru tīkla resursu kapacitāte ir paredzēta lielam klientu skaitam, tāpēc var prognozēt, ka, palielinot klientu skaitu, korelācijas koeficients pieaugs. Tika noteikts, ka klientu trafika plūsmām ir raksturīga liela dispersija – gan klientu individuālā, gan kopējā. Tas ir saistīts ar lielajām AL caurlaidspējas vērtību svārstībām, kas rodas, mobilajam klientam pārslēdzoties starp bezvadu piekļuves punktiem.

Veicot eksperimentālus mērījumus, datplūsmām, kas tika sūtītas no servera uz mobilo klientu, tika novērtēts Hersta parametrs, izmantojot absolūto momentu metodi. Tika secināts, ka pienākošais trafiks ir sevlīdzīgs un korelēts, t. i., atkarīgs no iepriekšējiem stāvokļiem. Līdz ar to var secināt, ka mērījumos realizētā divrangu *Wi-Fi* un *LTE* sakaru tīklā pārsūtītais datu trafiks ir sevlīdzīgs. Prognozējams, ka, pieaugot mobilo klientu skaitam, pieaugs arī datu trafika sevlīdzības pakāpe.

Eksperimentāli un analītiski tika novērtēta bezvadu piekļuves punkta kopējā AL caurlaidspēja atkarībā no ienākošo plūsmu (iesaistīto klientu) skaita stacionārā režīmā. Tika noteikta arī individuālā AL caurlaidspēja vienam klientam atkarībā no klientu skaita. Teorētiskajam novērtējumam tika izmantots daudztermināļu sistēmas matemātiskais modelis. Salīdzinot teorētiski iegūtos rezultātus ar eksperimentāli iegūtajiem datiem, atšķirība ir robežās

līdz 16 %, kas uzskatāms par labu rezultātu. Iegūto rezultātu analīze parāda, ka individuālā bezvadu tīkla klienta AL caurlaidspēja samazinās, pieaugot klientu skaitam tīklā. Klienta individuāli sasniedzamā caurlaidspēja ir atkarīga no klienta iekārtas veikspējas. Turpretī kopējā bezvadu piekļuves punkta AL caurlaidspēja, pieaugot bezvadu klientu skaitam, sākotnēji arī pieaug, jo AP veikspēja tiek projektēta lielam klientu blīvumam. Sakarā ar TCP mehānisma darbību AL caurlaidspējas kāpums ir nelineārs. Palielinoties klientu skaitam, tiks sasniegta AP veikspējas augšējā robeža. Līdz ar to eksperimentāli iegūtos AL caurlaidspējas mērījumu rezultātus, kas iegūti, izmantojot dažādu klientu skaitu, var izmantot, lai pārbaudītu matemātisko modeļu precizitāti, kas savukārt ir nepieciešami, lai prognozētu transporta sakaru tīklu veikspēju dažādas noslodzes apstākļos. Rezultātā tiek iegūti vērtīgi dati, kas ļauj izstrādāt augstas uzticamības un augstas veikspējas transporta sakaru tīklus.

Apkopojot iegūtos eksperimentālo mērījumu rezultātus, kur datu trafika plūsmām tika novērtēti tādi parametri kā caurlaidspēja, korelācijas koeficients, dispersija un trafika sevlīdzīguma pakāpe, var secināt, ka, izmantojot dažādu ražotāju LTE maršrutētājus, trafika raksturs nemainās.

Novērtējot transporta sakaru infrastruktūras risinājumus, nepieciešams novērtēt gan tā tehniskos veikspējas parametrus, piemēram, caurlaidspēja, atbildes laiks, gan arī tādas efektivitātes rādītājus kā izmaksas un mobilā tīkla atslogošanas parametru. Wi-Fi bāzēta un LTE koncentrēta atslogošana ļauj atslogot mobilo tīklu un samazināt ikgadējās kopējās transporta sakaru tīkla izmaksas. Wi-Fi tehnoloģija izmanto nelicencēto spektra daļu, tāpēc tā ir plaši pieejama. Veicot tehniski ekonomiskā novērtējuma rezultātu analīzi tiešam LTE kanālam un integrētam Wi-Fi un LTE sakaru kanālam, var secināt, ka hibrīda Wi-Fi un LTE autotransporta sakaru tīkla izmantošana, lai veiktu apjomīgu datu pārsūtīšanu, piemēram, transporta maršruta karšu atjaunināšana vai video informācijas pārsūtīšana, kā arī organizētu pasažieru piekļuvi interneta tīklam, ir tehniski un ekonomiski pamatota. Tādēļ var secināt, ka viens no praktiski lietojamiem autotransporta bezvadu sakaru tīkliem ir hibrīds divrangu Wi-Fi un LTE sakaru tīkls.

3. LIKUMSAKARĪBAS NOTEIKŠANA STARP INTEGRĒTA WLAN UN LTE SAKARU KANĀLA CAURLAIDSPĒJU UN AUTOMOBĪĻA KUSTĪBAS ĀTRUMU

Šajā nodaļā aprakstīti veiktie eksperimentālie mērījumi, veikta iegūto mērījumu rezultātu apstrāde un datu aproksimācija, lai noteiktu likumsakarību starp transporta sakaru tīkla caurlaidspēju un automobiļa pārvietošanās ātrumu. Tā ir svarīga likumsakarība, kurai ir praktiska nozīme, projektējot transporta sakaru sistēmas.

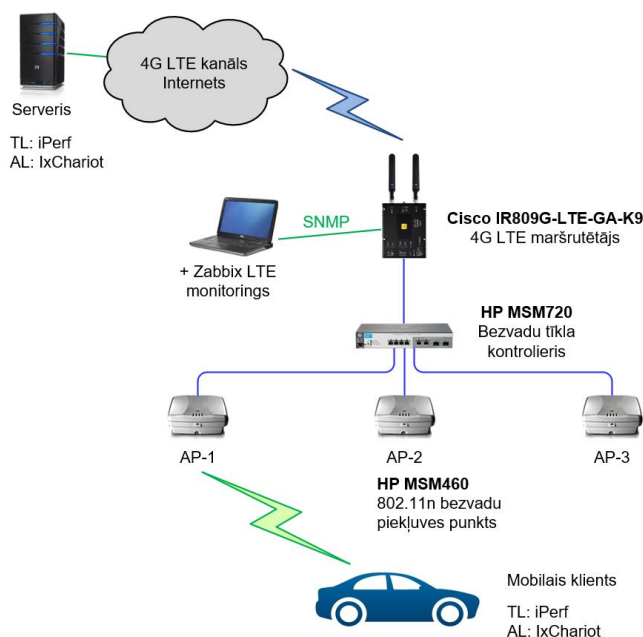
3.1. Eksperimentālo mērījumu sistēmas arhitektūra un metodoloģija

Praksē automobiļu sakaru tīklos visbiežāk ir sastopami heterogēnie sakaru tīkli. Piemēram, lai nodrošinātu tādu pakalpojumu kā datu straumēšana no servera, kas izvietots interneta tīklā, uz klientu vai arī otrādi. Eksperimentos tika izmantota *Wi-Fi* tīkla infrastruktūra savienojumā ar *LTE* tīklu. Tika pētīta kopējā šāda hibrīda tīkla caurlaidspēja. Rezultātā tika iegūtas likumsakarības starp vidējo datu pārraides ātrumu (caurlaidspēju) un mobilā klienta pārvietošanās ātrumu. Eksperimentāli tika novērtēti arī kopējie virstēriņi starp *OSI* modeļa transporta slāni (*L4*) un lietojuma jeb aplikācijas slāni (*L7*), ko rada katrs starpposma *OSI* modeļa slānis. Iegūtā likumsakarība aprakstīta zinātniskajā publikācijā [6].

Testgultnes apraksts

Eksperimentālā divrangu automobiļu sakaru tīkla slēguma shēma redzama 3.1. a attēlā. Testgultne tika realizēta lauka apstākļos. Tīkla pirmajā rangā tika izmantots bezvadu tīkla kontrolieris *HP MSM720* un trīs bezvadu piekļuves punkti *HP MSM460*, kas atbalsta *IEEE 802.11n* standartu (3.1. b att.). Tīkla otrajā rangā tika izmantots 4G maršrutētājs *Cisco IR809G-LTE-GA-K9*, kur automātiskā režīmā kā mobilā tīkla piekļuves tehnoloģija tika izmantots 4G *LTE* savienojums. *Cisco IR809G-LTE-GA-K9* ir iebūvēts *LTE* modems *Sierra Wireless MC7304*, kas atbilst *Cat 3* klasei (*DL* 100 Mbit/s un *UL* 50 Mbit/s). Maršrutētājs ir aprīkots ar iebūvēto operatīvo atmiņu *DRAM* 2 GB un zibatmiņu (angļu val. *flash memory*) 4 GB [145]. Kā bezvadu tīkla klients tika izmantota darbstacija *HP EliteBook 840 G1*, kā attālinātais serveris – darbstacija *HP ProBook 430 G2*. Mobilais klients pārvietojās, izmantojot elektromobili *VW e-UP!*, kas bija ļoti piemērots, lai īsā laika momentā sasniegtu mērījumos paredzēto braukšanas ātrumu. Attālums starp *AP* bija 100 metri, kopumā testgultnes vajadzībām tika atvēlēts 260 metrus garš ceļa posms. Mērījumos izmantotās aparatūras detalizēta specifikācija un galveno iestatījumu dati apkopoti 8. pielikumā.

Pirms eksperimentālo mērījumu veikšanas bija nepieciešams izveidot *VPN* kanālu no mobilā klienta līdz attālinātajam serverim, jo eksperimentos izmantotās mērījumu programmatūras prasību dēļ bija jānodrošina, lai mobilais klients un attālinātais serveris atrodas vienā *IP* apakštīklā.



a) Slēguma shēma



b) Izmantotā aparatūra

3.1. att. a) Testgultnes slēguma shēma; b) Eksperimentālo mērījumu aparatūras sagatavošana laboratorijā.

Iebraucot *Wi-Fi* AP apraides zonā, klients automātiski izveidoja savienojumu ar *Wi-Fi* tīklu, t. i., asociējās ar AP un piekļuva bezvadu tīkla kontrolierim. Tālāk, izmantojot 4G *LTE* maršrutētāju, kur tika lietots *NAT* (angļu val. *Network Address Translation*) protokols, tika izveidots mobilais interneta savienojums pie attālinātā servera. *Wi-Fi* tīklā tika izmantota statiski nokonfigurēta privātā *IP* adresācija. 4G *LTE* maršrutētājs kā mobilā tīkla klients saņēma publiskā *APN* (angļu val. *Public APN*) dinamisku privāto *IP* adresi. Attālinātais serveris izmantoja publisku fiksētu *IP* adresi. Pēc tam, kad piekļuve interneta tīklam tika nodrošināta, manuāli tika izveidots minētais *VPN* savienojums starp klientu un serveri. Eksperimentālo mērījumu laikā bija jāseko līdzi *VPN* kanāla statusam, jo, izbraucot ārpus testgultnes robežām, t. i., ārpus AP pārklājuma zonas, tika pazaudēts savienojums ar *Wi-Fi* tīklu un līdz ar to arī ar attālināto serveri. Atgriežoties atpakaļ *Wi-Fi* tīkla pārklājuma zonā, definētās savienojuma noildzes (angļu val. *connection timeout*) robežās *VPN* savienojums atjaunojās automātiski.

Mērījumu programmatūra un scenāriji

Eksperimentālajos mērījumos tika novērtēta gan transporta slāņa jeb transporta līmeņa (TL) caurlaidspēja, gan aplikācijas līmeņa (AL) caurlaidspēja. Transporta līmeņa (TL) maksimālās caurlaidspējas novērtēšanai tika izmantota *iPerf* programmatūra [159], savukārt aplikācijas

līmeņa (AL) maksimālās caurlaidspējas novērtēšanai – *IxChariot* programmatūra [157]. Abos scenārijos kā transporta slāņa protokols tika izmantots *TCP* [63].

iPerf programmatūra ir paredzēta maksimāli sasniedzamās caurlaidspējas mērījumu veikšanai *IPv4* vai *IPv6* tīklos, *OSI* modeļa *L4* slānī. Programmatūra atbalsta dažādu parametru pielāgošanu, kas ir saistīti ar buferatmiņas apjomu, vairāku datplūsmu vienlaicīgu ģenerēšanu un dažādu protokolu izmantošanu. Tiek atbalstīti *TCP*, *UDP* un *SCTP* transporta līmeņa protokoli [159], [160].

IxChariot programmatūru var izmantot *IPv4* un *IPv6* tīklos, lai ģenerētu dažāda tipa trafiku *OSI* modeļa *L7* slānī. Iestrādātajiem trafika šabloniem var mainīt to specifiskos parametrus. Ar *IxChariot* iespējams ģenerēt daudzveidīgu datplūsmu kopu, simulējot aplikācijas līmeņa *HTTP*, *FTP*, *VoIP*, e-pasta, video vai audio plūsmas [157]. Eksperimentālajos mērījumos, nosakot AL caurlaidspēju, tika simulēts *FTP* trafiks.

Visos mērījumos tika izmantots viens transportlīdzeklis, mērījumi tika veikti dažādos automobiļa (mobilā klienta) pārvietošanās ātrumos: 0 km/h (statisks), 20 km/h, 40 km/h, 50 km/h, 60 km/h, 70 km/h. Katrā no scenārijiem katrā braukšanas ātrumā tika veikti vismaz trīs mērījumi, tādējādi kopsummā tika veikti vismaz 36 mērījumi.

3.2. Nosacījumi un citi saistītie mērījumi

Wi-Fi frekvenču joslu izvēle

Laboratorijas apstākļos agrā rīta stundā mobilajam tīklam pieslēgts *Cisco IR809G-LTE-GA-K9* maršrutētājs spēja sasniegt lejupielādes ātrumu nedaudz virs 90 Mbit/s. Savukārt darba dienas stundās lejupielādes ātrumi, kas tika sasniegti ar šo pašu maršrutētāju, bija mainīgi un svārstījās robežās no 10 līdz 20 Mbit/s vai nedaudz virs šīm vērtībām. To var izskaidrot ar mobilā tīkla lietotāju skaita pieaugumu, kā rezultātā tīkls tika aktīvi noslogots. Papildinot stendu ar *Wi-Fi* tīkla daļu, datu pārraides ātrums var samazināties vēl par dažiem Mbit/s, to var izraisīt ārējie traucējumi, it īpaši 2,4 GHz joslā, vai arī lietotāju skaita pieaugums, jo šajā gadījumā tiek koplietota gan *Wi-Fi* tīkla daļa, gan *LTE* kanāls.

Eksperimentu veikšanai lauka apstākļos izveidotajā testgultnē dienas laikā 2,4 GHz ēters bija aizņemts, un brīvie kanāli, kas nepārklājas, nebija pieejami. Visi pieejamie brīvie kanāli bija ar lieliem blakus esošo kanālu traucējumiem. Šī iemesla dēļ mērījumi 2,4 GHz frekvenču joslā uzrādīja vājus rezultātus, un bija grūtības veikt korektu pārslēgšanās procedūras izpildi starp bezvadu piekļuves punktiem. Situācija 5 GHz frekvenču joslā bija daudz labāka. Tādēļ tika nolemts veikt mērījumus agrā rīta stundā tikai 5 GHz joslā. Veicot plānotos mērījumus divrangu tīklā (*Wi-Fi* un *LTE*), tika sasniegts maksimālais lejupielādes ātrums, kas bija tuvu 20 Mbit/s, izmantojot *IxChariot* programmatūru, un līdz 38 Mbit/s, izmantojot *iPerf* programmatūru. Vienranga tīklā (tikai *Wi-Fi*) statiskā režīmā datu pārraides ātrums tika sasniegts līdz 100 Mbit/s, jo 5 GHz ēterā traucējumi praktiski netika novēroti.

Konfigurācijas iestatījumi

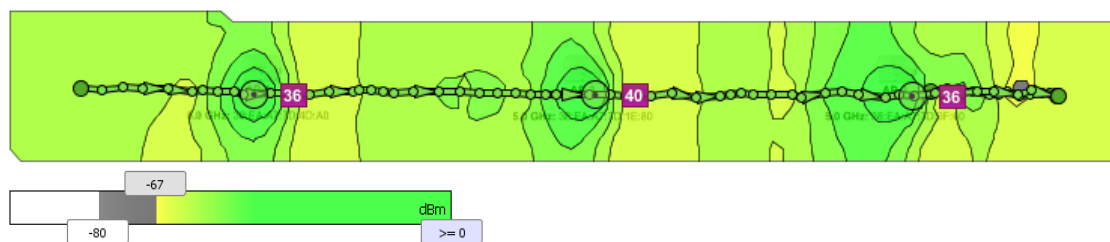
Mobilā klienta darbstacijas tīkla kartes iestatījumi: pārslēgšanās procedūras agresivitāte – visaugstākā; vēlamā frekvenču josla – 5 GHz; lielas caurlaidspējas režīms (*HT*) – iespējots; caurlaidspējas pastiprinātājs (angļu val. *booster*) – iespējots; raidīšanas jauda – augstākā.

Bezvadu tīkla kontroliera un *AP* konfigurācija: izmantotā frekvenču josla – 5 GHz (*U-NII-1*) [62]; frekvenču kanālu izvēle – manuāla; bezvadu tīkla klientu autentifikācija – *MAC* adrešu filtrs; kanāla joslas platums – 20 MHz; klienti – atļauti tikai *802.11n* klienti; datu pārraides ātrumi – atslēgti *802.11n* zemie datu pārraides ātrumi, atļauti sākot no 6 Mbit/s.

Wi-Fi tīklu plānošana un izvērsšana

Bezvadu tīkls tika plānots (prognozējošā izpēte) un analizēts (pasīvā un aktīvā izpēte) [3], izmantojot programmatūru *EkaHau Site Survey* [150]. Ar šīs programmatūras palīdzību tika veikti *Wi-Fi* tīkla pārklājuma mērījumi, tīkla konfigurācijas analīze (tīkla atbilstības novērtējums) un noteikta konkurējošo tīklu ietekme (frekvenču kanālu utilizācija, interference u. c. parametri).

3.2. attēlā redzami *Wi-Fi* tīkla pārklājuma mērījumi 5 GHz frekvenču diapazonā. Ar zaļo un dzelteni krāsu tiek apzīmēts ļoti spēcīgs *Wi-Fi* signāls (> -65 dBm), ar pelēko – signāls ir vājāks (-65 dBm līdz -75 dBm), ar balto – signāls ir par vāju (< -75 dBm) un nav pieņemams tādiem reāllaika pakalpojumiem kā *VoIP* [20], [62], [148].

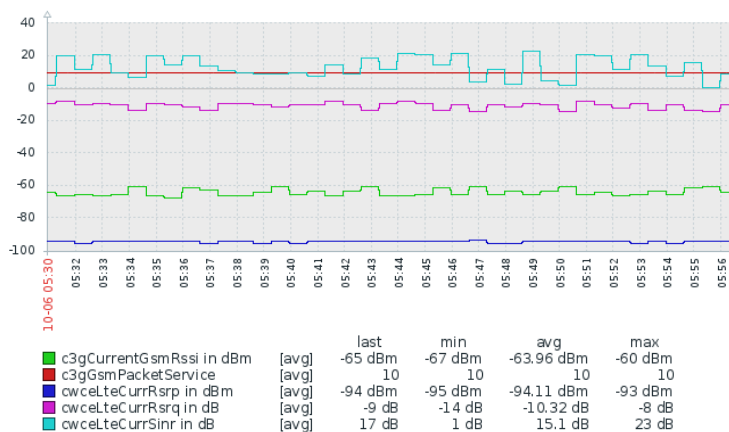


3.2. att. *EkaHau Site Survey* pārklājuma mērījumi 5 GHz frekvenču joslā.

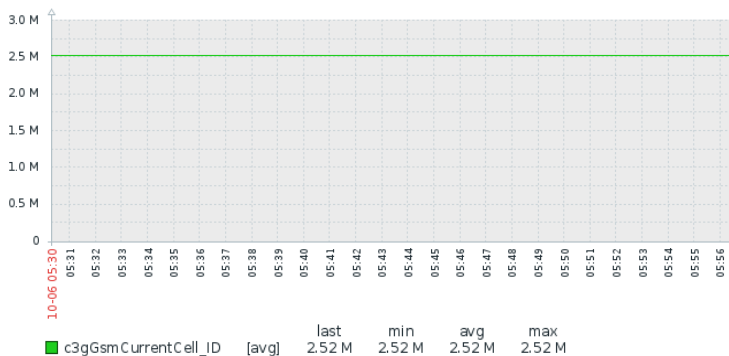
Wi-Fi un LTE tīklu uzraudzība

Programmatūra *Acrylic Wi-Fi* tika izmantota, lai uzraudzītu *Wi-Fi* tīkla pieejamību un savienojamību ar konkrēto *AP*, kā arī, lai veiktu *Wi-Fi* kanālu uzraudzību mērījumu laikā. Savukārt *LTE* mobilā tīkla signāla stipruma un tā kvalitātes parametru uzraudzība tika veikta ar speciāli mērījumiem izstrādāto “*Zabbix LTE*” monitoringa risinājumu. *Zabbix* uzraudzības sistēmā [182] tika izveidota *LTE* signāla parametru uzraudzības veidne tieši *Cisco LTE* maršrutētājiem. Tika izmantots *SNMP* (angļu val. *Simple Network Management Protocol*) protokols, lai attālināti no maršrutētāja nolasītu tā monitorējamās parametrus. Ar šī risinājuma palīdzību tika uzraudzīts *LTE* mobilā tīkla signāla stiprums *RSSI* un mobilā tīkla kvalitātes parametri *RSRP*, *RSRQ* un *SINR*, kā arī izmantotais pakešu radiopakalpojums (angļu val. *Packet Service*) jeb mobilā tīkla piekļuves tehnoloģija (angļu val. *Network Access Technology*) un šūnas identifikators (angļu val. *Cell ID*) (3.3. a–b att.). Izstrādāto veidni *Zabbix* sistēmā var izmantot arī citos pētījumos, kas saistīti ar otrā ranga tīklu, t. i., 4G *LTE* mērījumiem.

Kā redzams 3.3. a attēlā, mērījuma laikā visi novērotie *LTE* parametri bija stabili, ieskaitot izmantotās mobilā tīkla piekļuves tehnoloģijas (angļu val. *Packet Service*) parametru, kura vērtība palika nemainīga, t. i., tā mērījumu laikā bija 10, kas pēc *CISCO-WAN-3G-MIB OID* datiem nozīmē, ka tika izmantots 4G *LTE* savienojums.



a) Signāla stiprums un kvalitāte



b) Mobilā tīkla šūnas identifikators

3.3. att. Mobilā tīkla signāla parametru un šūnas identifikatora uzraudzība sistēmā *Zabbix*.

Mobilā tīkla parametrs šūnas identifikators (3.3. b att.) tika uzraudzīts, lai būtu pārliecība, ka testgultnē statistiski izvietotais *LTE* maršrutētājs neveic neplānotu pārslēgšanos uz kaimiņu šūnām. Šāda *LTE* tīkla nestabilitāte var negatīvi ietekmēt mērījumu rezultātus, jo līdz ar pārslēgšanos uz citu bāzes stacijas šūnu vai pat citu bāzes staciju var izmainīties arī mobilā tīkla pieslēguma parametri. Mērījumu laikā šūnas identifikatora parametri nemainījās.

3.3. a un b attēlā redzami iegūto *LTE* mobilā tīkla mērījumu fragmenti, līdzīgi rezultāti saglabājās visu mērījumu laiku (~3 h), tādēļ var secināt, ka veikto mērījumu laikā *LTE* mobilā tīkla pieslēgums bija stabils.

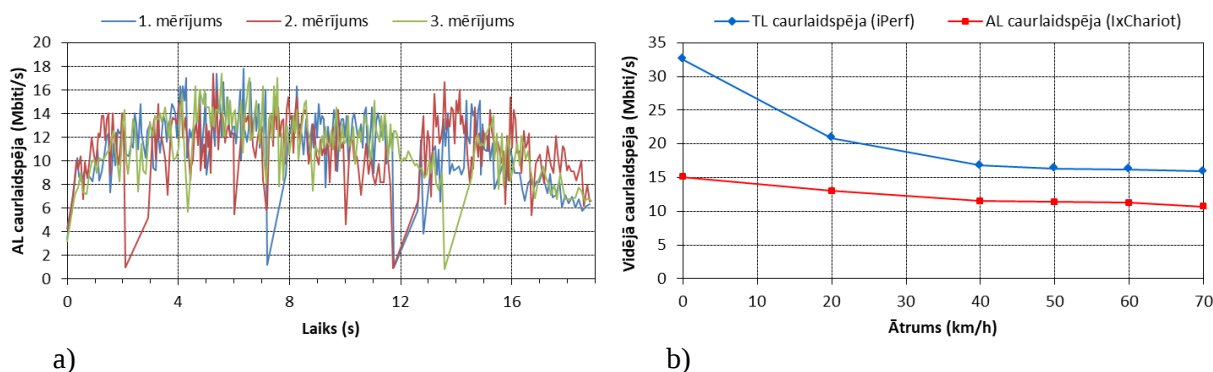
3.3. Sakaru kanāla veikspējas mērījumu rezultāti un to novērtējums

Eksperimentālo mērījumu rezultāti

Katrā automobiļa braukšanas ātrumā tika veikti trīs TL caurlaidspējas mērījumi un trīs AL caurlaidspējas mērījumi. Katram mērījumam, kas satur atsevišķas mērījumu nolases, tika

aprēķināta vidējā vērtība. Tālāk tika aprēķināta kopējā trīs iegūto rezultātu vidējā vērtība. Tādā pašā veidā tika aprēķinātas pārējās vidējās caurlaidspējas vērtības atkarībā no braukšanas ātruma un mērījumu scenārija.

3.4. a attēlā redzams ar *IxChariot* programmatūru iegūto AL caurlaidspējas mērījumu rezultātu piemērs, ja mobilais klients pārvietojas ar ātrumu 50 km/h. Eksperimentāli iegūtie TL caurlaidspējas mērījumu rezultāti ir apkopoti 4.1.–4.6. pielikumā, savukārt AL caurlaidspējas mērījumu rezultāti ir apkopoti 4.7.–4.12. pielikumā.



3.4. att. a) AL caurlaidspējas mērījumu rezultāti, ja automobiļa braukšanas ātrums ir 50 km/h;
b) Sakaru kanāla vidējā noteiktā TL un AL caurlaidspēja atkarībā no automobiļa braukšanas ātruma.

3.1. tabulā apkopota informācija par eksperimentālajos mērījumos iegūtajiem vidējiem datu pārraides ātrumiem divrangu sakaru tīklā atkarībā no transportlīdzekļa pārvietošanās ātruma un izmantotā programmnodrošinājuma, attiecīgi *iPerf* vai *IxChariot*.

3.1. tabula

Vidējā caurlaidspēja atkarībā no automobiļa braukšanas ātruma divrangu tīklā

Automobiļa braukšanas ātrums v , km/h	Vidējā caurlaidspēja un kļūdas						Procentuālā atšķirība, %
	Vidējā TL caurlaidspēja $\bar{\varphi}$ (<i>iPerf</i>), Mbiti/s	Vidējā standart kļūda $s_{\bar{\varphi}}$, Mbiti/s	Vidējā relatīvā standart kļūda $s_{\bar{\varphi}}\%$, %	Vidējā AL caurlaidspēja $\bar{\eta}$ (<i>IxChariot</i>), Mbiti/s	Vidējā standart kļūda $s_{\bar{\eta}}$, Mbiti/s	Vidējā relatīvā standart kļūda $s_{\bar{\eta}}\%$, %	
0	32,56	$\pm 0,46$	1,43	15,11	$\pm 0,06$	0,37	54
20	20,86	$\pm 0,91$	4,34	12,99	$\pm 0,10$	0,79	38
40	16,78	$\pm 1,30$	7,82	11,48	$\pm 0,18$	1,70	32
50	16,32	$\pm 1,74$	10,81	11,39	$\pm 0,17$	1,50	30
60	16,25	$\pm 1,60$	10,10	11,24	$\pm 0,22$	1,90	31
70	15,93	$\pm 1,68$	10,62	10,69	$\pm 0,24$	2,24	33

3.1. tabulā programmnodrošinājums *iPerf* reprezentē TL caurlaidspēju, *IxChariot* – AL caurlaidspēju.

Apkopojot (3.1. tab.) aprēķinātās vidējās TL un AL caurlaidspējas vērtības, 3.4. b attēlā parādītas iegūtās likumsakarības vidējai TL un AL caurlaidspējas atkarībai no mobilā klienta pārvietošanās ātruma.

Katrai 3.1. tabulā redzamajai vidējās TL un AL caurlaidspējas vērtībai papildus tika aprēķināta izlases vidējā standartklūda (absolūtā) jeb vidējā kvadrātiskā klūda (Mbit/s), kā arī izlases vidējā relatīvā standartklūda (%) [14]. No rezultātiem redzams, ka izlases vidējās standartklūdas un relatīvās standartklūdas ir mazākas AL caurlaidspējas mērījumiem, kas tika veikti, izmantojot *IxChariot* programmatūru. Tas ir saistīts ar to, ka *IxChariot* nolašu skaits viena mērījuma ietvaros ir daudz lielāks, salīdzinot ar *iPerf* programmatūru.

3.1. tabulā papildus veikta ar *iPerf* un *IxChariot* programmatūru iegūto caurlaidspējas mērījumu rezultātu un pēc tam aprēķināto vidējo caurlaidspējas vērtību salīdzināšana procentos. Gadījumā, ja mobilais klients atrodas statiskā režīmā, starpība ir izteikti liela, t. i., 54 %. Kustībā esošam klientam šī starpība ir daudz mazāka, un vidējā vērtība starp visiem mērījumiem ir 36 %.

iPerf reprezentē TL caurlaidspējas mērījumu rezultātus, un *IxChariot* attiecīgi AL caurlaidspēju, tāpēc iegūtie rezultāti parāda virstēriņu (angļu val. *overheads*) novērtējumu starp OSI modeļa aplikācijas slāni (L7) un transporta slāni (L4). Virstēriņus rada šo slāņu iesākuma jeb galvenes dati (angļu val. *header*), apliecinājuma (angļu val. *acknowledgement* – ACK) ziņojumi un TCP atkārtotas datu pārsūtīšanas mehānisms. Galvenie iemesli TCP protokola organizētai datu atkārtotai pārsūtīšanai tīklā ir datu pārraides kļūdas un datu trafika sastrēgumi tīklā, kas izraisa to pazaudēšanu [116], [177], [179]. Zemāko slāņu virstēriņi, tādi kā L3 – L2 slāņu galvenes dati un 802.11 MAC līmeņa atkārtoti pārsūtītie dati, šeit netiek ņemti vērā.

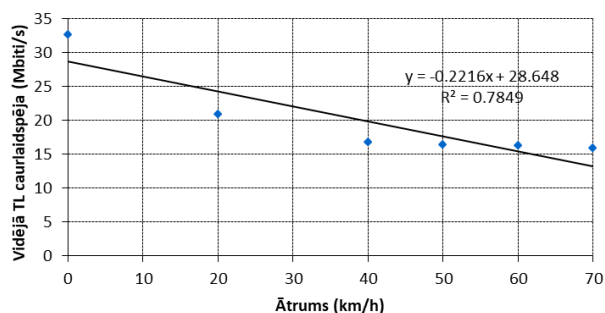
Eksperimentālo datu aproksimācija

Eksperimentālo datu aproksimācijas mērķis bija noteikt tādu funkciju, kas vislabāk apraksta iegūtos mērījumu datus (3.1. tab.), t. i., dod vismazāko aproksimācijas kļūdu. Tas ļaus secināt, pēc kāda likuma mainās TL un AL caurlaidspējas vidējās vērtības atkarībā no pārvietošanās ātruma, tādējādi tiks iegūtas jaunas likumsakarības.

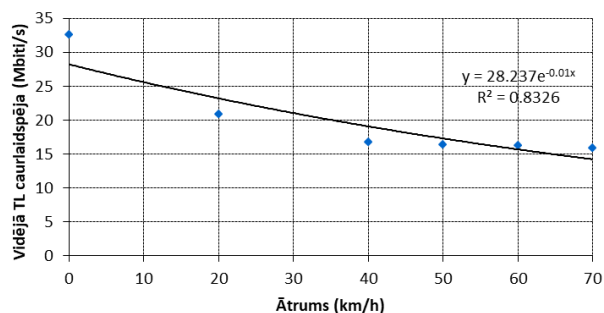
Eksperimentālo datu aproksimācija tika veikta *Excel* vidē, izmantojot lineāro un nelineāros regresijas modeļus. Vieni no visbiežāk lietotajiem regresijas modeļiem ir lineārais, eksponenciālais un polinomiālais modelis.

3.5. a–c attēlā parādīti ar *iPerf* programmatūru veiktajos eksperimentos iegūtie (3.1. tab.) un tālāk apstrādātie mērījumu rezultāti divrangu sakaru tīkla vidējai TL caurlaidspējai atkarībā no transportlīdzekļa pārvietošanās ātruma. Pēc tam, izmantojot lineāro (3.5. a att.), eksponenciālo (3.5. b att.) un polinomiālo (3.5. c att.) funkciju, dati tika aproksimēti.

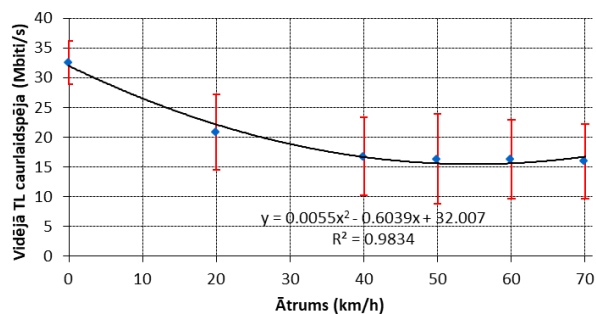
3.6. a–c attēlā redzami ar *IxChariot* programmatūru veiktajos eksperimentos iegūtie (3.1. tab.) un tālāk apstrādātie mērījumu rezultāti divrangu sakaru tīkla vidējai AL caurlaidspējai atkarībā no transportlīdzekļa pārvietošanās ātruma. Līdzīgi kā iepriekš, apstrādāto mērījumu datu aproksimācija tika veikta ar lineāro (3.6. a att.), eksponenciālo (3.6. b att.) un polinomiālo (3.6. c att.) funkciju palīdzību.



a) Aproksimācija ar lineāro funkciju

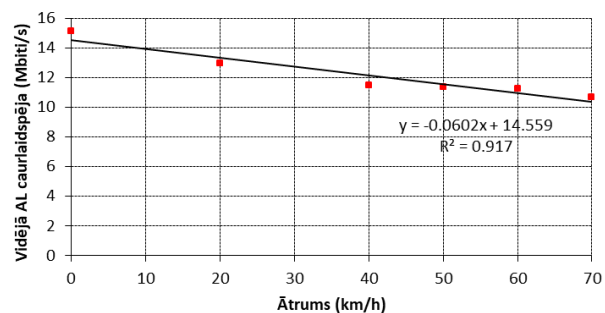


b) Aproksimācija ar eksponenciālo funkciju

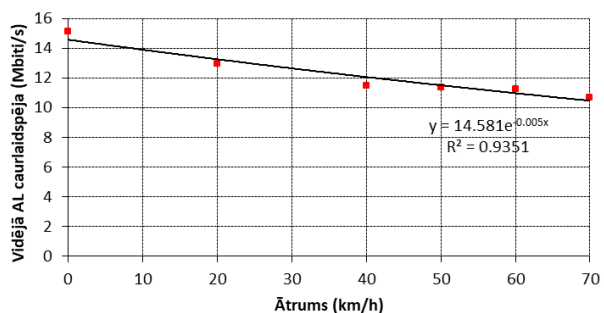


c) Aproksimācija ar polinomiālo funkciju

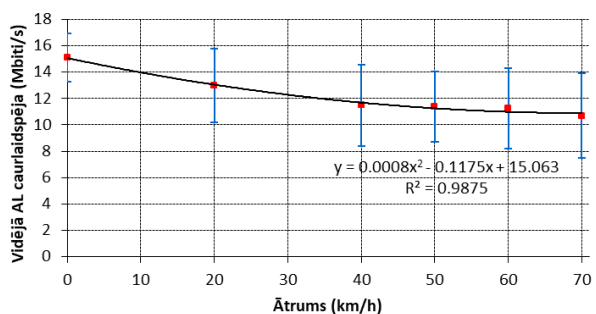
3.5. att. Vidējo transporta līmeņa (TL) caurlaidspējas eksperimentālo datu aproksimācija.



a) Aproksimācija ar lineāro funkciju



b) Aproksimācija ar eksponenciālo funkciju



c) Aproksimācija ar polinomiālo funkciju

3.6. att. Vidējo aplikācijas līmeņa (AL) caurlaidspējas eksperimentālo datu aproksimācija.

Aproksimācijas rezultātu analīze

Lai salīdzinātu iegūtās aproksimācijas funkcijas, ir jānovērtē aproksimācijas kvalitātes un precizitātes (aproksimācijas kļūdas) kritēriji. Kā aproksimācijas kvalitātes rādītājs tika

izmantots determinācijas koeficients R^2 . Jo determinācijas koeficients ir tuvāk vieniniekam, jo labāk izmantotā aproksimācijas funkcija apraksta eksperimentālos datus ($0 \leq R^2 \leq 1$). Savukārt kā aproksimācijas kļūdas kritēriji tika izmantoti parametri SSR (angļu val. *Sum of Squared Residuals*) un MSE (angļu val. *Mean Squared Error*). SSR ir noviržu kvadrātu summa [14]. MSE ir vidējā kvadrātiskā kļūda jeb vidējās kļūdas noviržu kvadrātu summa (kļūdas dispersija). Jo SSR un MSE vērtības ir mazākas, jo precīzāk aproksimācijas funkcija apraksta aproksimētos datus.

Izmantotie aproksimācijas modeļi (3.5. a–c un 3.6. a–c att.) rezultātā dod regresijas līkni ar regresijas funkcijas vienādojumu un automātiski aprēķinātu determinācijas koeficientu R^2 . SSR vērtība tika aprēķināta, izmantojot *Excel* funkciju *SUMXMY2*, funkcija izmanto 3.1. izteiksmi. MSE vērtība tika aprēķināta, izmantojot 3.2. izteiksmi [14], [86], [115].

$$SSR = \sum_{i=1}^N (E_i - R_i)^2, \quad (3.1.)$$

$$MSE = \frac{1}{z} \sum_{i=1}^N (E_i - R_i)^2, \quad (3.2.)$$

kur z – mērījumu punktu skaits ($z = 6$); E – mērījumu dati ($\bar{\varphi}$ un $\bar{\eta}$); R – aproksimācijas dati.

3.2. tabulā apkopoti aprēķinātie izmantoto aproksimācijas funkciju novērtēšanas parametri eksperimentāli iegūtajām vidējām TL un AL caurlaidspējas vērtībām atkarībā no automobiļa braukšanas ātruma divrangu tīklā

3.2. tabula

Aprēķinātie aproksimācijas funkciju novērtēšanas parametri eksperimentāli iegūtajām likumsakarībām

Aproksimācijas funkcija	Aproksimācijas novērtēšanas parametrs	Vidējās TL caurlaidspējas $\bar{\varphi}$ likumsakarība (<i>iPerf</i>)	Vidējās AL caurlaidspējas $\bar{\eta}$ likumsakarība (<i>IxChariot</i>)
Lineārā	R^2	0,78	0,92
	SSR	45,76	1,12
	MSE	7,63	0,19
Eksponeenciālā	R^2	0,83	0,94
	SSR	33,26	0,90
	MSE	5,54	0,15
Polinomiālā	R^2	0,98	0,99
	SSR	3,53	0,20
	MSE	0,59	0,03

Novērtējot parametrus R^2 , SSR un MSE (3.2. tab.), var secināt, ka vislabākos aproksimācijas rezultātus *iPerf* un *IxChariot* mērījumu datiem dod datu aproksimācija ar polinomiālo funkciju (3.5. c un 3.6. c att.). Var secināt, ka tīkla vidējās TL caurlaidspējas un AL caurlaidspējas

vērtības atkarībā no pārvietošanās ātruma mainās līdzīgi un visprecīzāk eksperimentāli iegūtās likumsakarības ar minimālu kļūdu apraksta (aproximē) otrās kārtas polinomiālā funkcija:

$$y(x) = Ax^2 + Bx + C, \quad (3.3.)$$

kur y – kopējā tīkla caurlaidspēja (TL caurlaidspēja vai AL caurlaidspēja); x – pārvietošanās ātrums v ; A , B , C – polinoma koeficienti.

Iegūtā aproksimācijas funkcija ir kvadrātiska, un datu aproksimācijai tiek izmantota aproksimācijas līknes (parabolas) krītošā segmenta daļa, kur ekstrēms ir lejā, ja pārvietošanās ātrums ir diapazonā no 0 km/h līdz 70 km/h.

Papildus iegūtajām likumsakarībām, kas redzamas 3.4. b, 3.5. c un 3.6. c attēlā, katrai aprēķinātajai vidējai TL un AL caurlaidspējas vērtībai (punktam) attiecīgajā braukšanas ātrumā tika aprēķināta vidējā standartnovirze σ , kas attiecīgi parādīta gan pozitīvā, gan negatīvā virzienā no vidējās vērtības (3.5. c attēlā – ar sarkanas krāsas vertikāliem stabiņiem, 3.6. c. attēlā – ar zilas krāsas stabiņiem). Standartnovirzes vērtības TL caurlaidspējas gadījumā vidēji ir 6,15 Mbiti/s, un AL caurlaidspējas gadījumā tā vidēji ir 2,78 Mbiti/s, kas ir salīdzinoši lielas vērtību izkliedes starp minimālo un maksimālo vērtību, un tās ir saistītas ar pārslēgšanās procedūras izpildi starp AP, kur minimālā caurlaidspējas vērtība pārslēgšanās procedūras momentā var nokrist pat līdz nullei.

3.4. Kopsavilkums un secinājumi

Eksperimentāli novērtējot integrēta, *IEEE 802.11n* un *LTE* standartos bāzēta automobiļu sakaru kanāla caurlaidspēju, secināts, ka šāda kanāla caurlaidspēja mainās atkarībā no transportlīdzekļa kustības ātruma. Transporta sakaru tīkla vidējā caurlaidspēja samazinās, pieaugot mobilā klienta kustības ātrumam. Eksperimentālie caurlaidspējas mērījumu rezultāti, mobilajam klientam pārvietojoties ar ātrumu 40 km/h, 50 km/h un 60 km/h, ir diezgan blīvi, un šeit datu pārraides ātruma samazinājums nav tik izteikts, salīdzinot ar mazākiem mobilā klienta pārvietošanās ātrumiem, taču tendence saglabājas. Jo lielāks ir automobiļa braukšanas ātrums, jo vairāk izlīdzinās tīkla vidējā caurlaidspēja.

Apstrādājot eksperimentāli iegūtos mērījumu datus, tika iegūtas likumsakarības, kas parāda, ka kopējā šāda divrangu bezvadu sakaru tīkla transporta līmeņa (TL) caurlaidspēja un aplikācijas līmeņa (AL) caurlaidspēja mainās atkarībā no mobilā klienta pārvietošanās ātruma pēc otrās kārtas polinomiālā likuma (3.3. vienādojums). Aprēķinātā un izvēlēta aproksimācijas funkcija vislabāk apraksta eksperimentāli iegūtos statistiskos datus ar vismazāko kļūdu. Iegūtā aproksimācijas funkcija ir kvadrātiska, un datu aproksimācijai tiek izmantota aproksimācijas līknes (parabolas) krītošā segmenta daļa, kur ekstrēms ir lejā, ja pārvietošanās ātrums ir diapazonā no 0 km/h līdz 70 km/h.

Jāņem vērā, ka pastāv gan aproksimācijas kļūda, kas šajā gadījumā ir minimāla, gan arī eksperimentālā kļūda, jo izvēlētie braukšanas ātrumi bija diezgan tuvi. Savukārt mērījumus, ja pārvietošanās ātrumi ir lielāki (>70 km/h), bija grūtības veiksmīgi izpildīt, jo nenotika korekta pārslēgšanās starp bezvadu piekļuves punktiem. Iemesls tam varēja būt iespējamie ārējie

traucējumu avoti, kurus mērījumu laikā nebija iespējams novērtēt, jo nebija pieejams spektra analizators, ar kura palīdzību iespējams atklāt ne tikai *IEEE 802.11* standarta traucējumu avotus.

Veicot caurlaidspējas mērījumus, tiek pārbaudīta tīkla aparatūras veiktspēja, kas apstrādā testgultnes trafiku, un gala rezultāts ir atkarīgs no visu iesaistīto mezglu maksimālās veiktspējas. AL caurlaidspēja parāda lietotāja derīgo pārsūtīto datu pārraides ātrumu.

Veicot aplikācijas līmeņa caurlaidspējas (*L7*) un transporta līmeņa caurlaidspējas (*L4*) eksperimentālo datu apstrādi un to analīzi, tika noskaidroti ienestie starpslāņu virstēriņi. Virstēriņi starp *L7* un *L4* vidēji ir līdz 36 %, ja mobilais klients pārvietojas ar ātrumu no 0 km/h līdz 70 km/h. Procentuāli tas ir diezgan liels trafika pieaugums, un praksē šie rezultāti ir jāņem vērā. Tas parāda, ka par tīkla caurlaidspēju nevar spriest, tikai balstoties uz mērījumiem, kas veikti tīkla vai transporta slāņos. Datu pārraides pakalpojumu saņēmējiem ir būtiski zināt, kāda caurlaidspēja ir reāli pieejama un kāda tā tiks sasniegta, piemēram, pārsūtot failus.

Visi mērījumi bija saistīti ar vienu kustībā esošu automobili, t. i., ar vienu mobilo lietotāju, tāpēc Wi-Fi infrastruktūras bezvadu piekļuves punktus (*AP*) nepastāvēja konkurence, nenotika cīņa par bezvadu tīkla resursiem starp bezvadu tīkla klientiem. Reālos automaģistrāles apstākļos mobilo klientu skaits ir daudzkārt lielāks. Tādēļ iegūtos caurlaidspējas mērījumu rezultātus jāuztver kā maksimālās vērtības, kas tika sasniegtas ar kustībā esošu transportlīdzekli jeb mobilo klientu, neesošas konkurences apstākļos. Lai pētītu caurlaidspēju konkurences apstākļos, kad ir vairāki transportlīdzekļi, var tikt izmantota rindošanas teorija [8]. Rezultātā caurlaidspēja katram individuālam klientam būtu proporcionāli daudz mazāka.

Lai nodrošinātu augstas kvalitātes un pieejamības divrangu sakaru tīklus, ir nepieciešams vienots Wi-Fi tīkla, kā arī LTE tīkla daļas monitoringa risinājums, kas spēj savlaicīgi atklāt un līdz ar to arī ļauj operatīvi novērst problēmas, kas saistītas ar tīkla kopējo veiktspēju.

Iegūto likumsakarību starp transportlīdzekļa pārvietošanās ātrumu un vidējo datu pārraides ātrumu var izmantot kā rekomendāciju, praksē projektējot transporta bezvadu piekļuves tīklus. Šādi tīkli var tikt izvērsti gar automaģistrālēm, lai apkalpotu kustībā esošos transportlīdzekļus un to pasažierus, nodrošinot tos ar piekļuvi interneta tīklam. Šādu tīklu projektētājiem un aparatūras ražotājiem būtu jāzina un jāņem vērā, ka, transportlīdzeklī pārvietojoties ar lielāku ātrumu, paredzams datu pārraides ātruma kritums, kas mainīsies pēc kvadrātiskās polinomiālās funkcijas likuma. Tas nozīmē, ka bezvadu piekļuves punkti un bezvadu tīkla kontrolieri būtu jāapņēma ar atbilstošu apjoma buferatmiņu, jo aparatūrā var veidoties datu trafika rindas.

4. WLAN PĀRSLĒGŠANĀS PROCEDŪRAS UZLABOŠANAS REALIZĀCIJA UN NOVĒRTĒJUMS

Šajā nodaļā vispirms sniegts *IEEE 802.11k/r/v* standartu apskats. Tālāk tiek aprakstīts izstrādātais uzlabotas pārslēgšanās procedūras risinājums *Wi-Fi* bāzētiem automobiļu sakaru tīkliem, kā arī atspoguļoti eksperimentālo mērījumu rezultāti, veikta to analīze un novērtējums. Nodaļā piedāvāts praktisks risinājums pārslēgšanās procedūras uzlabošanai datu pārraides kanāla slānī savienojumā ar ceļmalas tīkla raksturlielumiem. Lai uzlabotu pārslēgšanās procedūru, tika sagatavoti *Wi-Fi AP* un mobilais klients darbam ar *IEEE 802.11v*. Veicot eksperimentālus mērījumus, tika pārbaudīta piedāvātā risinājuma priekšrocības un efektivitāte. Tika prognozēts, ka tiks novērots *Wi-Fi* tīkla kopējās veiktspējas pieaugums. Iegūtie rezultāti atspoguļoti zinātniskajā publikācijā [70].

IEEE 802.11 tīklos ar ātri kustīgiem objektiem, kuru pārvietošanās ātrums ir lielāks par 20 km/h, pašreizējie pārslēgšanās procedūras risinājumi nenodrošina savlaicīgi pieņemtus lēmumus par pārslēgšanās procedūras sākšanu (angļu val. *handover decision*) un izpildi. Šī problēma kļūst īpaši kritiska *Wi-Fi* bāzētos transportlīdzekļu sakaru tīklos, kas tiek izvietoti gar automaģistrālēm [4], [5].

Lai veiksmīgi izmantotu *Wi-Fi* tehnoloģiju transportlīdzekļu sakaru tīklos (angļu val. *Vehicular Communication Network – VCN*), nepieciešamas izmaiņas esošajos pārslēgšanās procedūru algoritmos vai arī ir jāizstrādā pilnīgi jauns pārslēgšanās procedūras risinājums. Visas izmaiņas vēlams veikt, maksimāli izmantojot *IEEE 802.11* standartā piedāvātās iespējas, lai saglabātu jaunā risinājuma savietojamības un integrācijas iespējas. Pārslēgšanās procedūras aiztures samazināšana transportlīdzekļu kontekstā ir ļoti svarīga, lai transportlīdzekļi pēc iespējas mazāk tērētu tāpat salīdzinoši nelielo savienojuma laiku [54].

Lēmumu par nepieciešamību veikt pārslēgšanos no esošās *Wi-Fi AP* pārklājuma zonas uz kaimiņu *AP* pieņem klients patstāvīgi. Klienta pusē ir izstrādāti speciāli algoritmi, kas veic visus nepieciešamos mērījumus un aprēķinus, lai varētu realizēt pārslēgšanās procedūru. Šie algoritmi ir *Wi-Fi* aparatūras ražotāja patentēti risinājumi, un tie publiski nav pieejami. Tādējādi ar ražotāju nesaistītām ieinteresētajām pusēm šo algoritmu izmaiņas vai uzlabošana nav iespējama, un var tikt novērtēta tikai to efektivitāte, praktiski veicot eksperimentālus mērījumus. Parasti publiski tiek piedāvātas tikai fiksētas lietotāja saskarnē pieejamo *Wi-Fi* parametru pielāgošanas iespējas.

Pārslēgšanās procedūras aizturi, kas tiek novērota kā datu trafika kritumi vai ieplakas starp bezvadu *Wi-Fi* piekļuves punktiem, teorētiski var samazināt, izmantojot *IEEE 802.11* standartu kopas papildinājumus *IEEE 802.11r/k/v* [84], [108]. *IEEE 802.11k* [64], [65] un *IEEE 802.11v* [66], tāpat kā *IEEE 802.11r* jau ir iestrādāti *IEEE 802.11-2016* standartā, kas tiks aizstāts ar *IEEE 802.11-2020* standartu [67].

IEEE 802.11k/r/v standartus aktīvi testē daudzi *Wi-Fi* aparatūras ražotāji (piemēram, *Cisco*, *Aruba*, *Ruckus Networks*), taču tie nav testēti *VCN* vajadzībām. Jāatzīmē, ka *IEEE 802.11k/r/v* standarti nav obligāti, tie drīzāk ir jāuztver kā rekomendācijas aparatūras ražotājiem, tādēļ šo standartu atbalsts *Wi-Fi* tīkla infrastruktūras aparatūrā, kā arī klientu gala ierīcēs nav pietiekami izplatīts.

Pārslēgšanās procedūra notiek vairākos OSI modeļa slāņos (piemēram, datu pārraides kanāla slānī, tīkla slānī, transporta slānī, lietojuma slānī) [39], [57], tādēļ visi šie slāņi atstāj ietekmi uz kopējo pārslēgšanās procedūras aizturi. Lai nodrošinātu vienlaidu savienojamību, dažādus mehānismus vai paņēmienus var izmantot dažādos slāņos.

Mobilais klients *Wi-Fi* tīklos iziet cauri vairākiem soļiem, un katrs no tiem papildus rada savu aizturi, pirms tiek izveidota jauna asociācija ar *AP*. Tādi posmi kā kanālu skenēšana, autentifikācija un asociācija tiek izpildīti, pirms jaunais *AP* var apstrādāt un pārsūtīt klienta datus. Vislielāko pārslēgšanās procedūras aizturi apakštīkla ietvaros, kur *IP* adrese paliek nemainīga, rada datu pārraides kanāla slānis (*L2*), izpildot pasīvās vai aktīvās skenēšanas operācijas [39].

Izpildot pārslēgšanās procedūru, jānodrošina gan pakalpojumu nepārtrauktība, gan to kvalitāte (*QoS*) atbilstoši definētajām prasībām uz tīkla aizturēm.

4.1. IEEE 802.11k/r/v standartu apskats

IEEE 802.11-2016 standartā (tiks aizstāts ar *IEEE 802.11-2020* standartu) ir definēti trīs dažādi kadru tipi: vadības, kontroles un datu. Vadības kadri tiek iedalīti 14 dažādos apakštipos. *IEEE 802.11k/r/v* izmanto vadības kadrus ar apakštipu “Darbība” jeb darbības kadrus.

IEEE 802.11k

IEEE 802.11k jeb “bezvadu LAN tīklu radio resursu mērījumi” (angļu val. *Radio Resource Measurement of Wireless LANs*) ļauj klientiem no bezvadu piekļuves punkta (*AP*) pieprasīt pārskatu par kaimiņu *AP*, kas ir pārslēgšanās procedūras kandidāti. *IEEE 802.11k* kaimiņu *AP* saraksta izmantošana var samazināt nepieciešamību pēc aktīvas un pasīvas skenēšanas. Kaimiņu *AP* jeb kandidātu saraksts ietver informāciju par *BSS* identifikatoru (*BSSID*), izmantoto kanālu un blakus esošo radio darbības detaļām. Kaimiņu *AP* sarakstā ir iekļauti tikai tie *AP*, kas strādā tajā pašā frekvenču joslā (2,4 GHz vai 5 GHz), kurā ir asociējies klients. Tādējādi šī standarta izmantošana samazina visu kanālu utilizāciju, jo vairs nav nepieciešamības skenēt visus kanālus. Tas ļauj arī palielināt pieejamo raidlaiku (angļu val. *airtime*) *AP* klientiem, kā arī palielināt datu pārraides ātrumu visos kanālos, jo samazinās izsūtāmo vadības kadru apjoms, kurus *AP* vienmēr izsūta apraides režīmā, izmantojot mazāko, obligāti noteikto datu pārraides ātrumu [148]. Standarts ļauj samazināt pārslēgšanās laiku starp *AP* un palīdz klientam pieņemt lēmumu par pārslēgšanos. Turklāt tas ļauj palielināt arī klienta ierīces baterijas darbības laiku, jo katram kanālam nav jāmaina radio konfigurācija un nav nepieciešama zondes pieprasījumu kadru sūtīšana katrā kanālā. Tas ļauj izvairīties no zondes atbildes ziņojumu apstrādes [84], [108], [153].

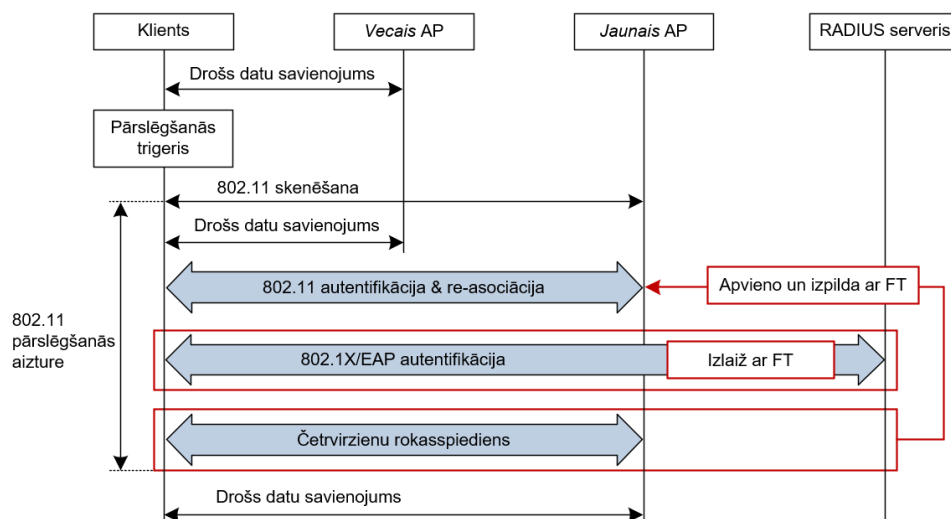
IEEE 802.11k palīdz daudz efektīvāk pieņemt pārslēgšanās procedūras lēmumus, balstoties uz saņemtajiem pārskatiem par kaimiņu bezvadu piekļuves punktiem no asociētā *AP* [35], [62].

IEEE 802.11r

IEEE 802.11r jeb “ātrā BSS pāreja” (angļu val. *Fast BSS Transition – FT*) risina problēmu, kas saistīta ar klienta pārslēgšanos no viena AP (BSS) uz citu AP vienā un tajā pašā mobilitātes domēnā (ESS robežās). Pārslēgšanās procedūras laikā tiek pazaudēta savienojamība ar tīklu (DS), tādēļ tiek meklēts veids, kā samazināt pārrāvuma laiku. FT protokols ir daļa no reasociācijas funkcijas. IEEE 802.11r specificē FT starp bezvadu piekļuves punktiem, redefinējot drošības atslēgu pārrunu protokolu. IEEE 802.11r standarts atbalsta tikai WPA2 versiju. IEEE 802.11i (WPA2) atslēgu pārrunu protokols klientam nosaka, ka gadījumā ar 802.1X/EAP bāzētu autentifikāciju pie atkārtotas atslēgu pārrunāšanas (angļu val. *renegotiate*) ar RADIUS vai citu autentifikācijas serveri katrā pārslēgšanās procedūrā nepieciešams izmantot paplašināmo autentifikācijas protokolu (EAP), kas ir laikietilpīgs process. IEEE 802.11r gadījumā pirmajā klienta asociācijas reizē 802.1X/EAP autentifikācijas procesā iegūtā galvenā sesijas atslēga (MSK) tiek izmantota daudzlīmeņu FT atslēgu hierarhijā, lai iegūtu pirmā līmeņa galveno atslēgu (PMK-R0), no kuras savukārt tiek iegūta otrā līmeņa galvenā atslēga (PMK-R1) un kas tiek izmantota, lai iegūtu PTK atslēgas, kas tiek izmantotas, lai šifrētu klienta trafiku (802.11 datu kadrus). Atkarībā no WLAN arhitektūras FT atslēgas (PMK-R0 un PMK-R1) tiek iegūtas un uzkrātas (angļu val. *cached*) dažādās WLAN iekārtās (WLC, AP, klienta stacija) [35], tas ļauj ātri izveidot turpmākos klienta pārslēgšanās procedūras savienojums, katru reizi neatkārtojot 802.1X/EAP procesu.

Gadījumā ar 802.1X/EAP autentifikāciju un realizētu FT, veicot pārslēgšanās procedūru uz citu AP, FT izpilda līdzīgu procedūru kā gadījumā ar WPA2-Enterprise drošības shēmu (2.7. att.). Vienīgi šeit tiek izlaists 802.1X/EAP autentifikācijas solis, un FT protokols apvieno IEEE 802.11i četrvirzienu rokasspiediena procedūras ziņojumus ar 802.11 atvērtās sistēmas autentifikācijas un reasociācijas ziņojumiem. Tādējādi tiek iegūti FT protokola kadri, kurus transportē FT autentifikācijas algoritms (angļu val. *FT authentication algorithm – FTAA*) kopā ar gadījumskaitļiem (angļu val. *Nonces*) un citu informāciju, kas nepieciešama, lai izveidotu beigu dinamiskās atslēgas. Apmainoties ar četriem šādiem FTAA ziņojumiem, rezultātā tiek iegūtas PTK atslēgas. Tādā veidā ir nepieciešams pārsūtīt par četriem kadriem mazāk, un pārslēgšanās procedūra tiek paātrināta, kas parasti aizņem mazāk par 50 ms [35]. 4.1. attēlā redzama klasiskā klienta pārslēgšanās procedūra gadījumā ar WPA2-Enterprise drošības mehānismu, kur tiek izmantots 802.1X/EAP autentifikācijas modelis, kā arī parādīta realizācija ar klienta ātro pāreju (FT), kad tiek izmantots IEEE 802.11r standarts [152].

IEEE 802.11r standartu var izmantot arī gadījumos ar WPA2-Personal (WPA2-PSK), ja FT atbalsta gan klients, gan AP [2]. Ja tiek izmantota klasiskā PSK autentifikācija bez FT, tad pārslēgšanās procedūra notiek ātri, parasti 40–60 ms, jo netiek izmantota 802.1X/EAP kadru apmaiņa. Izmantojot PSK autentifikāciju un FT, pārslēgšanās procedūra vēl tiek mazliet paātrināta, jo tiek izlaista WPA2 četrvirzienu rokasspiediena procedūra [35]. Jāatzīmē, ka literatūrā atrodamās un šajā sadaļā aprakstītās pārslēgšanās procedūru aiztures galvenokārt attiecas uz klasiskiem iekštelpu klientiem, kas pārvietojas ar nelielu ātrumu.



4.1. att. Pārslēgšanās procedūras shēma, izmantojot EAP autentifikāciju un FT mehānismu [152].

IEEE 802.11v

IEEE 802.11v jeb “bezvadu tīkla vadība” (angļu val. *Wireless Network Management* – WNM) bezvadu tīkla klientus nodrošina ar informāciju, lai atklātu labāko pieejamo bezvadu piekļuves punktu. Standarts ļauj IEEE 802.11 tīkla bezvadu piekļuves punktiem izsūtīt ziņojumus pieslēgtajiem klientiem par labākiem AP, kas varētu nodrošināt augstākas asociācijas kvalitātes prasības starp klientu un AP un ar kuriem klienti varētu asociēties. Tas ir noderīgi slodzes balansēšanai bezvadu tīklā, kā arī lai novirzītu vāji pieslēgtus klientus (piemēram, zems signāla līmenis, neapmierinoša SNR attiecība). IEEE 802.11v ziņojumu formāts atbilst vadības kadra (2.4. att.) apakštipam “Darbība”, atbilstoši tam tiek formēti darbības kadri.

Vairāki darbības kadra formāti ir definēti WNM vajadzībām (izmanto vadības kadra lauku “Kadra ķermenis”). Darbības kadrā lauks “WNM darbība” atrodas uzreiz pēc lauka “Kategorija” (angļu val. *Category*) un diferencē ziņojumu formātus. IEEE 802.11 standarts definē 18 dažādas lauka “WNM darbība” vērtības un tās tiek asociētas ar konkrētu kadra formātu. Detalizēti tiks aplūkoti šādi lauka “WNM darbība” formāti: “BSS pārejas vadības vaicājums” jeb “BSS TM vaicājums” (angļu val. *BSS Transition Management Query* – BSS TM Query), kuram atbilst vērtība 6; “BSS pārejas vadības pieprasījums” jeb “BSS TM pieprasījums” (angļu val. *BSS Transition Management Request* – BSS TM Request), kuram atbilst vērtība 7 un “BSS pārejas vadības atbilde” jeb “BSS TM atbilde” (angļu val. *BSS Transition Management Response* – BSS TM Response), kuram atbilst vērtība 8 [67].

IEEE 802.11v BSS pārejas vadības ziņojumi tiek piemēroti šādos gadījumos: “lūgts pieprasījums” (angļu val. *solicited request*) – klients var izsūtīt 802.11v “BSS pārejas vadības vaicājuma” ziņojumu asociētajam AP, pirms veic pārslēgšanās procedūru, lai izvēlētos labāko zināmo AP un lai noorganizētu reasociācijas procedūru; “nelūgts slodzes balansēšanas pieprasījums” (angļu val. *unsolicited load balancing request*) – ja AP ir pārslogots, tas var izsūtīt 802.11v “BSS pārejas vadības pieprasījuma” ziņojumus asociētajiem klientiem, lai

klienti varētu pārslēgties uz citiem AP; “nelūgts optimizēts pārslēgšanās procedūras pieprasījums” (angļu val. *unsolicited optimized roaming request*) – ja kāda klienta RSS un datu pārraides ātrums neatbilst prasībām, tad AP attiecīgajam klientam izsūta 802.11v “BSS pārejas vadības pieprasījuma” ziņojumu, kas ir ieteikums pārslēgties uz citu piedāvāto AP. Klients patstāvīgi pieņem lēmumu, tādējādi klients var pieņemt vai arī noraidīt šo ieteikumu. Lai piespiestu diasociēt klientu, ir iespējams izmantot “nenovēršamo diasociācijas funkciju” (angļu val. *Disassociation Imminent function*). Šī funkcija diasociē klientu pēc kāda laika perioda, ja klients neresociējas uz citu AP, taču pēc tam klients tāpat var mēģināt asociēties ar šo pašu AP [153]. Tādējādi IEEE 802.11v standartu var izmantot, lai paātrinātu jaunā AP izvēles procedūru.

“BSS pārejas vadības vaicājuma” kadra formāts

“BSS pārejas vadības vaicājuma” (angļu val. *BSS Transition Management Query*) kadrs izmanto darbības kadra (2.4. att.) lauka “Kadra ķermenis” formātu un tiek sūtīts no klienta (STA) uz AP, lai pieprasītu vai nodrošinātu informāciju par BSS pārejas kandidātu AP. WNM darbības lauka “BSS pārejas vadības vaicājums” formāts redzams 4.2. attēlā, un tajā ir šādi lauki: “Kategorija”, “WNM darbība” (angļu val. *WNM Action*), “Dialoga marķieris” (angļu val. *Dialog Token*), “BSS pārejas vaicājuma cēlonis” (angļu val. *BSS Transition Query Reason*) un “BSS pārejas kandidātu saraksta ieraksti” (angļu val. *BSS Transition Candidate List Entries*), kas ir neobligātais lauks.

Kategorija	WNM darbība	Dialoga marķieris	BSS pārejas vaicājuma cēlonis	BSS pārejas kandidātu saraksta ieraksti (neobligāts)
Baiti: 1	1	1	1	mainīgs

4.2. att. “BSS pārejas vadības vaicājuma” kadra formāts [67].

Lauks “BSS pārejas kandidātu saraksta ieraksti” satur nulles vai vairāku kaimiņu pārskatu (angļu val. *Neighbor Report*) elementus. Kaimiņu pārskatu elementus izveido klienta stacija kā daļu no tās skenēšanas procedūras, un nodrošina AP ar šo pārskatu [67].

“BSS pārejas vadības pieprasījuma” kadra formāts

“BSS pārejas vadības pieprasījuma” (angļu val. *BSS Transition Management Request*) kadrs izmanto darbības kadra (2.4. att.) lauka “Kadra ķermenis” formātu un tiek sūtīts no AP uz klientu (STA) kā atbilde uz “BSS pārejas vadības vaicājuma” kadru vai patstāvīgi.

Kategorija	WNM darbība	Dialoga marķieris	Pieprasījuma režīms	Diasociācijas taimeris	Derīguma intervāls
Baiti: 1	1	1	1	2	1

BSS izbeigšanas ilgums (neobligāts)	Sesijas informācijas URL (neobligāts)	BSS pārejas kandidātu saraksta ieraksti (neobligāts)
0 vai 12	mainīgs	mainīgs

4.3. att. “BSS pārejas vadības pieprasījuma” kadra formāts [67].

WNM darbības lauka “BSS pārejas vadības pieprasījums” formāts redzams 4.3. attēlā, un tajā ir šādi lauki: “Kategorija”, “WNM darbība”, “Dialoga marķieris”, “Pieprasījuma režīms” (angļu val. *Request mode*), “Diasociācijas taimeris” (angļu val. *Disassociation Timer*),

“Derīguma intervāls” (angļu val. *Validity Interval*), “BSS izbeigšanas ilgums” (neobligāts) (angļu val. *BSS Termination Duration*), “Sesijas informācijas URL” (neobligāts) (angļu val. *Session Information URL*), “BSS pārejas kandidātu saraksta ieraksti” (neobligāts) [67].

4.4. attēlā redzams lauks “Pieprasījuma režīms”, kas sastāv no šādiem apakšlaukiem: “Vēlamo kandidātu saraksts iekļauts” (angļu val. *Preferred Candidate List Included*), “Saīsināts” (angļu val. *Abridged*), “Diasociācija nenovēršama” (angļu val. *Disassociation Imminent*), “BSS izbeigšana ietverta” (angļu val. *BSS Termination Included*), “ESS diasociācija nenovēršama” (angļu val. *ESS Disassociation Imminent*) un pēdējais lauks ir rezervēts nākotnes vajadzībām [67].

Vēlamo kandidātu saraksts iekļauts	Saīsināts	Diasociācija nenovēršama	BSS izbeigšana ietverta	ESS diasociācija nenovēršama	Rezervēts
Biti: 0	1	2	3	4	5-7

4.4. att. Pieprasījuma režīma lauks [67].

“BSS pārejas vadības atbildes” kadra formāts

“BSS pārejas vadības atbildes” (angļu val. *BSS Transition Management Response*) kadrs izmanto darbības kadra (2.4. att.) lauka “Kadra ķermenis” formātu un neobligātā kārtā tiek sūtīts no klienta (*STA*) uz *AP* kā atbilde uz “BSS pārejas vadības pieprasījuma” kadru. *WNM* darbības lauka “BSS pārejas vadības atbilde” formāts parādīts 4.5. attēlā, un tajā ir šādi lauki: “Kategorija”, “WNM darbība”, “Dialoga marķieris”, “BTM statusa kods” (angļu val. *BTM Status Code*), “BSS izbeigšanas aizture” (angļu val. *BSS Termination Delay*), “Mērķa BSSID” (neobligāts) (angļu val. *Target BSSID*) un “BSS pārejas kandidātu saraksta ieraksti” (neobligāts) [67].

Kategorija	WNM darbība	Dialoga marķieris	BTM statusa kods	BSS izbeigšanas aizture	Mērķa BSSID (neobligāts)	BSS pārejas kandidātu saraksta ieraksti (neobligāts)
Baiti: 1	1	1	1	1	0 vai 6	mainīgs

4.5. att. “BSS pārejas vadības atbildes” kadra formāts [67].

4.2. Pārslēgšanās procedūras uzlabošana

Lēmumu izpildīt pārslēgšanās procedūru pieņem klienta bezvadu tīkla adaptera (angļu val. *Wireless Network Interface Card – WNIC*) draiveris nevis *AP*. Lēmums tiek pieņemts, ņemot vērā dažādus apstākļus. *IEEE 802.11* standartā šie apstākļi nav definēti, tāpēc pārslēgšanās procedūras algoritmi katram ražotājam ir specifiski. Precīzas sliekšņvērtības, trigeri un citi nosacījumi netiek publiski atklāti. Dažas no pārslēgšanās procedūras algoritma komponentēm ir uztvertā signāla jaudas līmenis (*RSS*), signāla un trokšņa attiecība (*SNR*), trūkstošo *AP* bāksignālu skaits, kolīziju vai interferences dēļ uzkrātās kļūdas.

Vairums bezvadu tīkla klientu veic pārslēgšanos uz citu *AP*, pirms tiek pazaudēts *Wi-Fi* signāls pilnībā, taču ir klienti, kas šādu iespēju neatbalsta. Lielai daļai klientu *WNIC* ir pieejamas uzlabotu iestatījumu opcijas. Izvēloties tādus parametrus kā pārslēgšanās procedūras agresivitāte (angļu val. *Roaming Aggressiveness*), kas ietekmē *RSS* sliekšņvērtību, un pārraides jauda (angļu val. *transmit power*), ir iespējams ietekmēt un optimizēt pārslēgšanās procedūru. Dažādi bezvadu tīkla klienti izmanto atšķirīgas sliekšņvērtības, tāpēc daļa no tiem mēģinās

veikt pārslēgšanās procedūru ātrāk nekā citi. Dažiem klientiem būs tendence uzturēt esošo asociāciju ar AP, kamēr to vairs nevarēs uztvert, turpretī citi klienti veiks pārslēgšanos, tiklīdz tiks atklāts labāks AP [62]. Tomēr gadījumā ar ātri kustīgiem objektiem šis klienta pusē pieejamās pielāgošanas iespējas neatrisina savlaicīgas un efektīvas pārslēgšanās procedūras problēmas. To pierāda iepriekš veiktie eksperimenti, kur datu trafika iekritumi saglabājas līdzīgi, neliels uzlabojums ir novērojams, ja bezvadu tīkla klients pārvietojas ar ātrumu 90 km/h [4], [5].

Viens no veidiem, kā risināt apspriestās problēmas, būtu papildus ieviest jaunas pārslēgšanās procedūras metrikas un cits – uzlabot pārslēgšanās procedūras mehānismu, izmantojot *IEEE 802.11k/r/v* standartus.

Pārslēgšanās procedūras risinājums

Tika definēts mērķis un uzdevums izveidot mehānismu, ar kura palīdzību *Wi-Fi* tīkls spētu nodot komandas mobilajam klientam, lai diasociētu klientu no esošā AP un veiktu pārslēgšanos uz labāku AP. Galvenie jautājumi ir, kurā brīdī veikt pārslēgšanās procedūru un uz kuru AP. Piedāvātais pārslēgšanās procedūras risinājums paredz *IEEE 802.11v* standarta izmantošanu. Realizācijā netika izmantoti teorētiski apskatītie *IEEE 802.11k* un *IEEE 802.11r* standarti.

Lai realizētu *IEEE 802.11v* standarta ieviešanu, adoptāciju, kā arī pārbaudītu tā efektivitāti, pakāpeniski tika realizētas vairākas *IEEE 802.11v* pārslēgšanās procedūras modifikācijas. Jāatzīmē, ka “Standarta” klienta jeb noklusētajā pārslēgšanās procedūras gadījumā lēmums par pārslēgšanās brīdi un AP izvēli, uz kuru jāpārslēdzas, ir jāpieņem klientam patstāvīgi.

Vispirms tika izstrādāts risinājums, kur pārslēgšanās procedūras lēmums vienpusēji tiek pieņemts tīkla pusē. Tas tika nosaukts par “802.11v tīkla virzīta” (angļu val. *network directed*) (manuāla) pārslēgšanās procedūra. Šī modifikācija tika realizēta izpildei manuālā režīmā. Papildus tika testēts arī automatizēts risinājums “802.11v tīkla virzīta” (automātiska) pārslēgšanās procedūra. Taču tas izrādījās samērā nestabils, jo šim risinājumam pietrūka informācija par klienta puses signāla mērījumiem, tādēļ tālāk šis variants netiek apskatīts un neparādās arī mērījumu rezultātos.

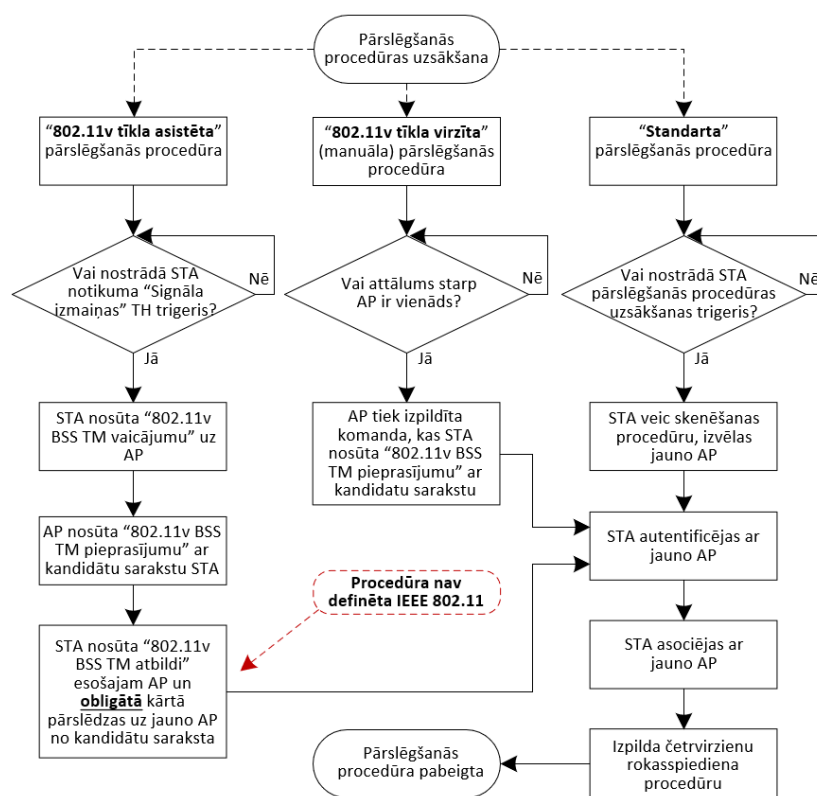
Visbeidzot tika izstrādāts risinājums, kur pārslēgšanās procedūras lēmums tiek pieņemts klienta pusē kombinācijā ar tīkla puses atbalstu. Tīkls klientam norāda, uz kuru AP klientam obligāti ir jāpārslēdzas. Risinājums tika nosaukts par “802.11v tīkla asistēta” (angļu val. *network assisted*) pārslēgšanās procedūra. Šeit klienta (*STA*) pārslēgšanās starp AP notiek automātiski.

Salīdzināšanai 4.6. attēlā parādīta apvienotā “Standarta”, “802.11v tīkla virzīta” (manuāla) un “802.11v tīkla asistēta” pārslēgšanās procedūru algoritmu shēma. Veiktajos eksperimentos katrs algoritms tika testēts atsevišķi.

Testgultnes mobilā klienta *802.11* darbstacijas (*STA*) IP adrese tika nokonfigurēta manuāli, un *DHCP* procedūra netika izmantota. Tādēļ apvienotajā pārslēgšanās procedūras algoritmu shēmā *DHCP* serviss nav iekļauts (4.6. att.).

Izstrādātā “802.11v tīkla asistēta” pārslēgšanās procedūras risinājuma principālā atšķirība un efektivitāte, salīdzinot ar “Standarta” pārslēgšanās procedūras risinājumu, slēpjas divos

aspektos: 1) asociētais AP klientam nosūta informāciju par nākamo AP, tādējādi klientam nav jātērē laiks tīkla skenēšanai; 2) asociētais AP klientam nosūta speciālu komandu veikt obligātu pārslēgšanos uz jauno AP.



4.6. att. Apvienotā pārslēgšanās procedūras algoritmu shēma.

Iekārtu programmēšana

Eksperimentos izmantotā *IEEE 802.11* tīkla infrastruktūras un klienta aparātūra pēc noklusējuma neatbalsta *IEEE 802.11v* standartu, šāda funkcionalitāte bija jāprogrammē. *IEEE 802.11 ESS* infrastruktūrā un klienta pusē tika izmantoti *TP-Link Archer C7 (AC1750)* [178] maršrutētāji (kopā četri) ar uzinstalētu atvērtā koda *OpenWrt* aparātprogrammatūru (angļu val. *firmware*), kas ir bāzēta *Linux* operētājsistēmā (angļu val. *Operating System – OS*) [169].

Visos mērījumos tika izmantots *IEEE 802.11ac* standarts. *IEEE 802.11* infrastruktūras un klienta demo aparātūra tika sagatavota darbam ar *IEEE 802.11v* standartu. Lai to paveiktu, tika izmantots maršrutētājos iebūvētais *Linux Host AP* bezvadu LAN adaptera draiveris, kas atbalsta bezvadu piekļuves punkta (AP) un *802.11* darbstacijas (STA) režīmus. Tālāk tika konfigurēti *hostapd* un *wpa_supplicant* dēmoni, kas ir fona programmas, kas nodrošina attiecīgi AP un STA pārvaldību u. c. funkcijas, ieskaitot *IEEE 802.11v* atbalstu. *hostapd* tika nokonfigurēts uz AP maršrutētājiem, savukārt *wpa_supplicant* – uz STA maršrutētāja. Abos gadījumos bija nepieciešams izlabot *IEEE 802.11v* “BSS pārejas vadības vaicājuma” kadra struktūru, kas pēc noklusējuma tika nepareizi formēta.

“Standarta” pārslēgšanās procedūras gadījumā klients var iegūt informāciju par apkārt esošajiem AP divos veidos – veicot pasīvo vai aktīvo bezvadu tīkla skenēšanu. Pirmajā

gadījumā klients klausās tuvējo AP vadības bāksignālu kadru apraidi (pasīvā skenēšana); otrajā gadījumā klients var izsūtīt vadības zondes pieprasījuma kadrus, un apkārt esošie AP atbild ar zondes atbildes kadriem (aktīvā skenēšana). Saņemot šos ziņojumus, klients patstāvīgi izlemj, pie kura AP viņam labāk pārslēgties.

Eksperimentālajos mērījumos “Standarta” risinājuma klientam tika konfigurēti šādi parametri: kanāla numurs (angļu val. *channel number*), kanāla platums (angļu val. *channel width*), SSID nosaukums, autentifikācija parametri, pārslēgšanās procedūras iniciēšanas trigeris sliekšņvērtība, un tika izmantota statiskā IP adrese. “Standarta” klienta pārslēgšanās procedūras mehānisms netika modificēts.

“802.11v tīkla virzītās” (manuāla) pārslēgšanās procedūras realizācijā tika modificēts gan AP, gan klients (STA). Klienta pusē tika izmainīts kods, kas nosaka, ka, saņemot “BSS pārejas vadības pieprasījuma” ziņojumu, klientam obligāti jāveic pārslēgšanās uz citu AP. Kad mobilais klients atradās pa vidu starp bezvadu piekļuves punktiem, uz asociētā AP manuāli tika izpildīta komanda, kas izsūtīja klientam “BSS pārejas vadības pieprasījuma” ziņojumu. Ziņojums satur lauku “BSS pārejas kandidātu saraksts” (angļu val. *BSS Transition Candidate List*) jeb nākamā AP BSSID MAC adresi. Klientam, saņemot šādi noformētu ziņojumu, obligāti ir jāpārslēdzas uz jauno AP.

“802.11v tīkla asistētās” pārslēgšanās procedūras realizācijā klients no asociētā AP uztver sūtītos apraides vadības bāksignālu kadrus (angļu val. *Management Beacon Frames*), ko AP izsūta ik pēc 100 ms. No šiem ziņojumiem tiek nolasīts RSS signāla līmenis savienojumam ar AP. Klientam tika nokonfigurēta RSS līmeņa sliekšņvērtība –62 dBm. Tas ir samērā augsts līmenis, jo mērījumos attālums starp AP bija tikai 100 m. Ja klientam, pārvietojoties AP pārklājuma zonā, divas reizes nostrādā sliekšņvērtības trigeris par zemu RSS signāla līmeni (< –62 dBm), tad mobilais klients noformē un izsūta “BSS pārejas vadības vaicājuma” ziņojumu. AP, saņemot šādu ziņojumu, noformē “BSS pārejas vadības pieprasījuma” ziņojumu. Šī ziņojuma laukā “BSS pārejas kandidātu saraksts” tiek iekļauta informācija par nākamā jeb kaimiņu AP BSSID MAC adresi, uz kuru klientam būs jāpārslēdzas. Datubāze ar nākamā AP BSSID MAC adresi tika nokonfigurēta uz katra AP lokāli. AP kandidātu saraksts ietver tikai nākamo AP, lai nodrošinātu minimālu pārslēgšanās procedūras lēmuma aizturi. Klients, saņemot no asociētā AP šādi noformētu ziņojumu, atbild ar “BSS pārejas vadības atbildes” ziņojumu un nekavējoties veic pārslēgšanos uz nākamo AP. Šī procedūra nav definēta IEEE 802.11v standartā un tika speciāli programmēta. Izstrādātie un eksperimentāli nofiksētie pārslēgšanās procedūras 802.11v BSS pārejas vadības apmaiņas ziņojumi starp klientu un AP apkopoti 6. pielikumā.

4.3. Eksperimentālā iestatīšana

Lauka apstākļos izvietotā automobiļu Wi-Fi sakaru tīkla (WLAN VCN) testgultnē tika veikti aplikācijas līmeņa (AL) caurlaidspējas, atbildes laika un pārslēgšanās procedūras aiztures eksperimentālie mērījumi. Šo raksturlielumu analīze ļauj novērtēt VCN sakaru tīklu veiktspēju un arī kvalitāti [70], [113].

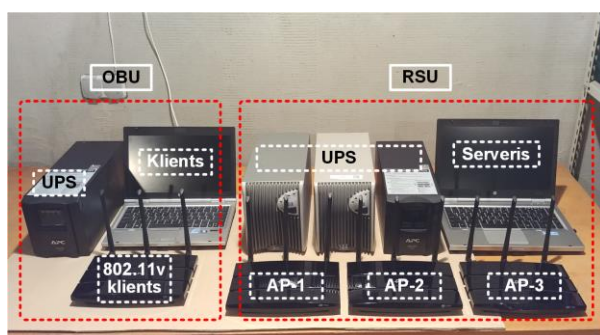
Eksperimenti tika realizēti, izmantojot trīs scenārijus: 1) “Standarta” pārslēgšanās procedūras realizācija; 2) realizācija ar izstrādāto “802.11v tīkla virzītu” (manuālu) pārslēgšanās procedūru; 3) realizācija ar izstrādāto “802.11v tīkla asistētu” pārslēgšanās procedūras metodi. Eksperimentos tika izmantots automobilis, kas pārvietojās ar dažādu ātrumu: 20 km/h, 50 km/h, 70 km/h un 90 km/h. Automobilis pārvietojās pa taisnvirziena 260 m garu ceļa posmu, kur gar ceļmalu tika izvietota testgultne. Katrā braukšanas ātrumā tika veikti vismaz trīs mērījumi.

Aplikācijas līmeņa (AL) caurlaidspējas un atbildes laika novērtēšanai mērījumos tika izmantota *IxChariot* programmatūra. Kā mobilā klienta galiekārta un attālinātais serveris tika izmantoti biznesa klases portatīvie datori, uz kuriem attiecīgi tika aktivizēta *IxChariot* programmatūra. Nepārtrauktās elektrobarošanas iekārtas (angļu val. *Uninterruptible Power Supply* – *UPS*) tika izmantotas kā elektrobarošanas avoti, lai nodrošinātu testgultnes sakaru tīkla darbību vismaz trīs stundas.

Testgultne ietvēra trīs pieslēgtus *AP*, vienu serveri un vienu mobilo klientu. *AP* režīmā tika nokonfigurēti trīs *TP-Link Archer C7* maršrutētāji ar uzinstalētu *OpenWrt* aparātprogrammatūru. Mobilā klienta galiekārtas komplektā bija portatīvais dators un *TP-Link Archer C7* maršrutētājs ar uzinstalētu *OpenWrt* aparātprogrammatūru, kas tika nokonfigurēta *STA* režīmā. Bezvadu piekļuves punkti tika uzstādīti uz statīviem 1,85 m augstumā.

Kopumā tika izmantotas četras *APC UPS* iekārtas. *Wi-Fi* ceļmalas infrastruktūras darbības nodrošināšanai tika izmantoti divi *UPS* 500 VA, kā arī viens centrālais *UPS* 1400 VA. Mobilā klienta darbības nodrošināšanai tika izmantots viens *UPS* 500 VA, iekārta tika izvietota automobilī. Eksperimentu veikšanai tika izmantots *VW e-UP!* elektromobilis, kas nodrošināja nepieciešamo paātrinājumu, lai sasniegtu attiecīgo eksperimentos izmantoto braukšanas ātrumu relatīvi īsā distancē.

4.7. a attēlā redzams automobiļu sakaru tīkla testgultnes mobilā klienta aparatūras komplekts (*OBU*), kā arī gar poligona ceļmalu izvietotā aparatūra (*RSU*).



a) Testgultnes klienta (*OBU*) un ceļmalas (*RSU*) aparatūra



b) Testgultnes ceļmalas (*RSU*) aparatūra



c) Testgultnes ceļmalas (RSU) aparatūra



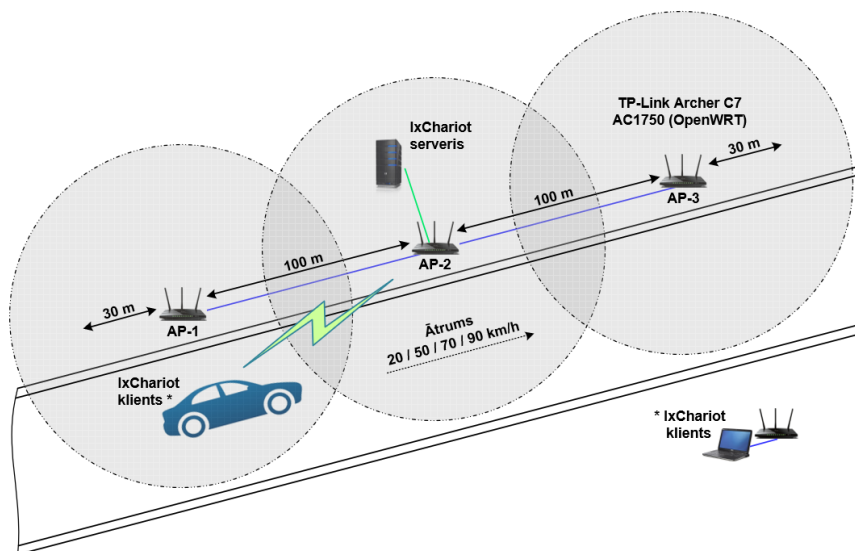
d) Testgultnes klienta (OBU) aparatūra

4.7. att. Testgultnes WLAN VCN eksperimentālo mērījumu iekārtas un to izvietojums.

4.7. b–d attēlā redzams OBU un RSU aparatūras izvietojums eksperimentu laikā. Mērījumos izmantotās aparatūras detalizēta specifikācija un galveno iestatījumu dati apkopoti 8. pielikumā.

“Standarta” pārslēgšanās procedūra

Izmantotā automobiļu sakaru tīkla, kas bāzēts *Wi-Fi* tehnoloģijā un tika detalizēti aprakstīts 4.3. apakšnodaļas ievadā, “Standarta” pārslēgšanās procedūras scenārija testgultnes slēguma shēma redzama 4.8. attēlā. Eksperimentā tika izmantotas standarta nemodificētas AP un STA iekārtas bez *IEEE 802.11v* atbalsta.

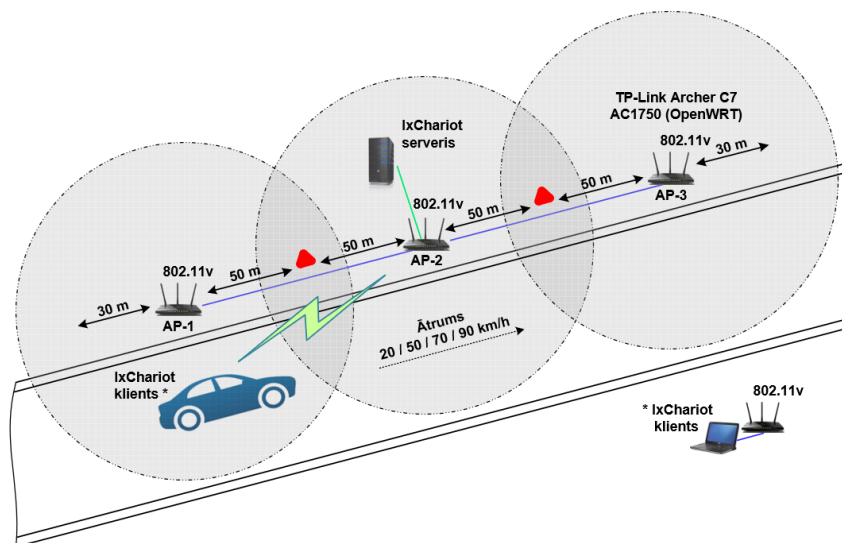


4.8. att. Testgultnes slēguma shēma nemodificētam WLAN VCN, bāzēts *802.11ac* standartā.

“802.11v tīkla virzība” (manuāla) pārslēgšanās procedūra

Šajā scenārijā izmantotā VCN testgultne aprakstīta 4.3. apakšnodaļas ievadā. VCN *Wi-Fi* tīkla maršrutētāji (AP) un mobilā klienta maršrutētājs (STA) tika modificēti, lai implementētu *IEEE 802.11v* standartu un realizētu iepriekš aprakstīto “802.11v tīkla virzību” (manuālu) pārslēgšanās procedūras funkcionalitāti. Testgultnē pa vidu starp AP tika izvietoti marķieri, kas slēguma shēmā (4.9. att.) atzīmēti ar sarkaniem trijstūriem. Kad mobilais klients atradās tieši pretī marķierim, uz asociētā AP manuāli tika izpildīta komanda, kas izsūtīja mobilajam

klientam “BSS pārejas vadības pieprasījuma” ziņojumu, tādējādi iniciējot pārslēgšanās procedūru, lai pārslēgtos uz nākamo AP.



4.9. att. Testgultnes slēguma shēma modificētam WLAN VCN, bāzēts 802.11ac un 802.11v standartos.

“802.11v tīkla asistēta” pārslēgšanās procedūra

Šajā scenārijā izmantotā VCN testgultne aprakstīta 4.3. apakšnodaļas ievadā un redzama 4.9. attēlā. Atšķirībā no iepriekšējā scenārija jaunajā realizācijā pārslēgšanās procedūra notiek pilnīgi automātiski, un ceļmalas marķieri nav nepieciešami. VCN Wi-Fi tīkla maršrutētāji (AP) un mobilā klienta maršrutētājs (STA) tika modificēti, lai implementētu IEEE 802.11v standartu un realizētu iepriekš aprakstīto “802.11v tīkla asistētu” pārslēgšanās procedūras funkcionalitāti.

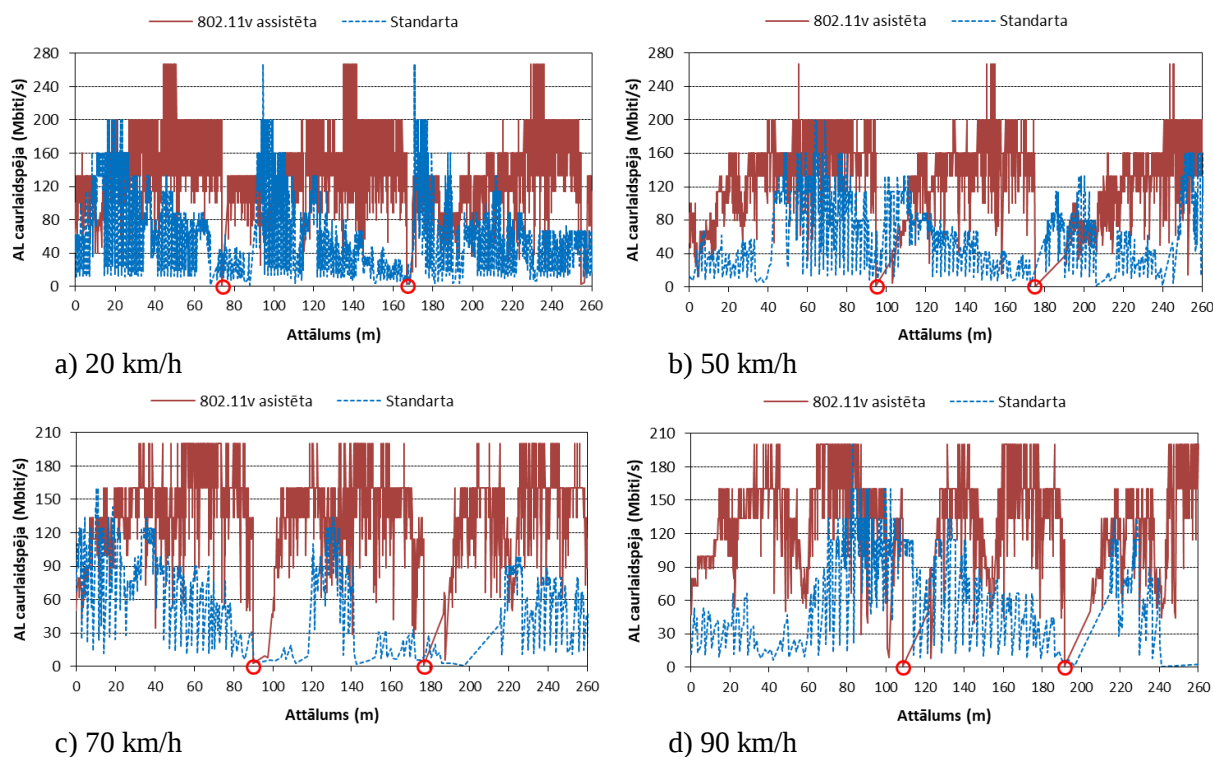
4.4. Veiktspējas parametru eksperimentāls novērtējums

Šajā apakšnodaļā tiek veikts eksperimentāajos mērījumos iegūto veiktspējas parametru (AL caurlaidspēja, atbildes laiks un pārslēgšanās procedūras aiztures) novērtējums. Eksperimentālie mērījumu dati “Standarta”, “802.11v tīkla virzītai” (manuālai) un “802.11v tīkla asistētai” pārslēgšanās procedūrām attiecīgi apkopoti 5.1.–5.5., 5.6.–5.10. un 5.11.–5.15. pielikumā.

Aplikācijas līmeņa caurlaidspēja

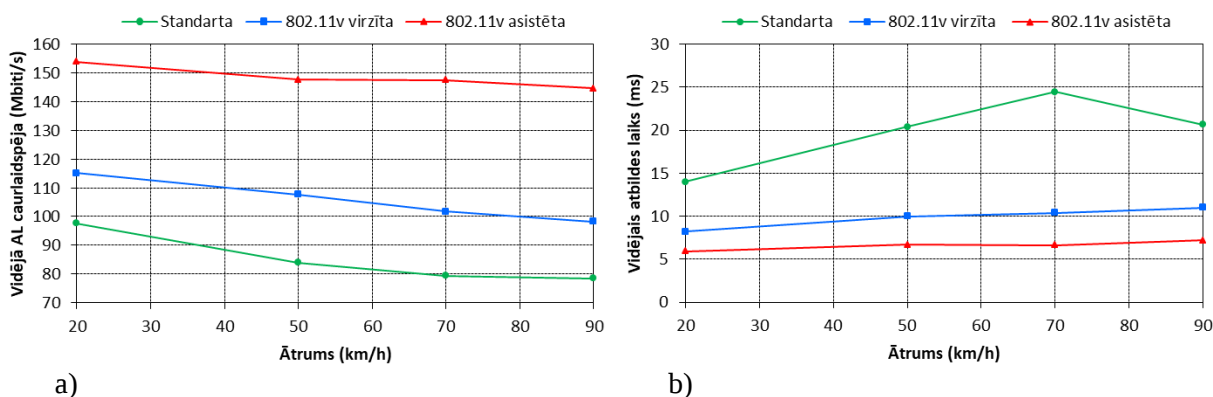
Salīdzināšanai (4.10. a–d att.) ir parādīti eksperimentāli iegūtie AL caurlaidspējas grafiki “Standarta” un “802.11v tīkla asistētas” pārslēgšanās procedūras mehānismiem, ja automobilis pārvietojas ar dažādu ātrumu, IEEE 802.11ac tīklā. Pārslēgšanās starp AP scenārijā ar “802.11v tīkla asistētu” pārslēgšanās procedūru, kas 4.10. a–d attēla grafikos uz horizontālās ass atzīmēta ar sarkaniem apliem, tiek izpildīta diezgan precīzi – aptuveni pa vidu starp bezvadu piekļuves punktiem. Scenārijā ar “802.11v tīkla virzītu” (manuālu) pārslēgšanās procedūru (5.16. pielikums) pārslēgšanās moments starp AP notiek tieši pa vidu starp AP (~80 m un ~180 m), jo

pārslēgšanās komandas tiek izpildītas manuāli, tieši pretī gar ceļmalu izvietotajiem marķieriem. Tika novērots, ka “Standarta” pārslēgšanās procedūras gadījumā, ja pārvietošanās ātrums ir lielāks par 20 km/h, pārslēgšanās procedūra notiek nokavēti, ja pārvietošanās ātrums ir 90 km/h – nekorekti, jo kāds no testgultnes AP var tikt ignorēts un izlaists.



4.10. att. AL caurlaidspēja, ja braukšanas ātrums ir 20 km/h, 50 km/h, 70 km/h un 90 km/h, izmantojot “802.11v tīkla asistētu” un “Standarta” pārslēgšanās procedūras metodes.

4.11. a attēlā redzamas aprēķinātās vidējās AL caurlaidspējas raksturlīknes, to aprēķiniem tika izmantoti eksperimentāli iegūtie mērījumu dati, klientam pārvietojoties dažādā ātrumā un izmantojot dažādas pārslēgšanās procedūras metodes.



4.11. att. a) Vidējā AL caurlaidspēja; b) Vidējais atbildes laiks.

4.1. tabulā apkopots iegūto AL caurlaidspējas raksturlīkņu (4.11. a att.) novērtējums. Virspirms tika aprēķinātas iegūto AL caurlaidspējas līkņu vidējās vērtības starp visiem braukšanas ātrumiem, tālāk – novērtēti tādi izkliedes rādītāji kā standartnovirze σ un variācijas koeficients.

Vidējā aplikācijas līmeņa caurlaidspēja un izkliedes rādītāji

Pārslēgšanās metode	Vidējā AL caurlaidspēja $\bar{\eta}$, Mbit/s	Standartnovirze, σ	Variācijas koeficients K_v , %
Standarta	84,80	7,70	9,09
802.11v virzīta	105,67	6,42	6,07
802.11v asistēta	148,44	3,43	2,31

Pēc iegūtajiem rezultātiem redzams, kā vislielāko AL caurlaidspējas vidējo vērtību un vismazākos izkliedes rādītājus dod izstrādātais “802.11v tīkla asistētas” pārslēgšanās procedūras risinājums. Īpaši ir jāpievērš uzmanība iegūtajiem izkliedes rādītājiem, jo tie raksturo likumsakarību, kā mainās AL caurlaidspējas vidējā vērtība atkarībā no pārvietošanās ātruma. Jo mazāki ir izkliedes rādītāji, jo mazāks ir AL caurlaidspējas vidējās vērtības kritums, pārvietojoties ar lielāku ātrumu.

Atbildes laiks

Atbildes laiks ir kopējais nepieciešamais laiks, lai sāktu datu pārraidi, tas ir laiks no brīža, kad klients veic pieprasījumu, līdz tiek saņemta atbilde. Atbildes laiku var ietekmēt attālinātā servera pieprasījumu apstrādes laiks (angļu val. *processing time*) izmaiņas un tīkla aiztures izmaiņas, kas ir atkarīgas no servera un tīkla noslodzes, pieejamajiem servera un tīkla aparatūras operacionālajiem resursiem. Jāņem vērā arī pārslēgšanās procedūra un tās radītā aizture, kas palielina kopējo tīkla aizturi. Tādējādi atbildes laikā ietilpst tīkla aizture, sistēmu pieprasījumu apstrādes laiks un pārslēgšanās procedūras aizture.

4.11. b attēlā redzamas aprēķinātās vidējās atbildes laika raksturlīknes, aprēķiniem tika izmantoti eksperimentāli iegūtie mērījumu dati, mobilajam klientam pārvietojoties dažādā ātrumā un izmantojot dažādas pārslēgšanās procedūras metodes. Pieaugot mobilā klienta kustības ātrumam, pieaug arī tīkla atbildes laiks. “Standarta” pārslēgšanās procedūras gadījumā vidējā atbildes laika raksturlīknes kritumu, kad pārvietošanās ātrums bija 90 km/h, var izskaidrot ar faktu, ka šajā gadījumā mobilais klients nav veicis pārslēgšanos starp visiem AP. Katra pārslēgšanās procedūra palielina kopējo tīkla atbildes laika vērtību. Tas uzskatāmi parāda iepriekš minēto problēmu, ka *IEEE 802.11* tīklos ar “Standarta” pārslēgšanās procedūras realizāciju, ja braukšanas ātrums ir, sākot no 90 km/h, parādās problēmas korekti pārslēgties starp bezvadu piekļuves punktiem.

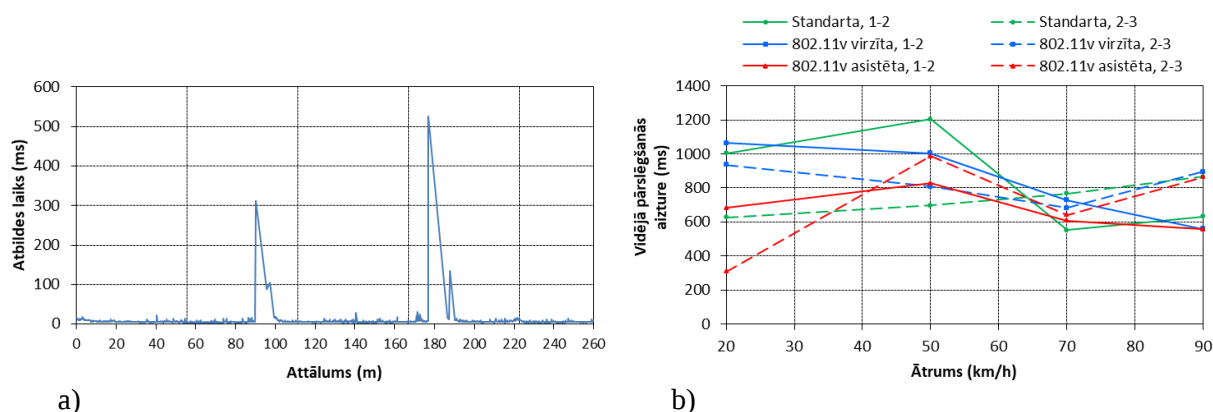
4.2. tabulā apkopots iegūto atbildes laika raksturlīkņu novērtējums. Tika aprēķinātas atbildes laika raksturlīkņu vidējās vērtības starp visiem braukšanas ātrumiem un novērtēti tādi izkliedes rādītāji kā standartnovirze σ un variācijas koeficients. Kā redzams (4.2. tab.), vismazāko atbildes laika vidējo vērtību un vismazākos izkliedes rādītājus nodrošina izstrādātais “802.11v tīkla asistētas” pārslēgšanās procedūras risinājums.

Vidējais atbildes laiks un izkliedes rādītāji

Pārslēgšanās metode	Vidējais atbildes laiks $\bar{T}$, ms	Standartnovirze, σ	Variācijas koeficients K_v , %
Standarta	19,87	3,75	18,89
802.11v virzīta	9,90	1,04	10,54
802.11v asistēta	6,60	0,44	6,73

Pārslēgšanās procedūras aizture

Izpētot eksperimentāli ar *IxChariot* programmatūru iegūtos atbildes laika grafikus, tika noteikts aptuvenais katras pārslēgšanās procedūras ilgums jeb aizture. Iegūtajos grafikos (5. pielikums) pārslēgšanās procedūras aiztures tiek novērotas kā izteikti atbildes laika vērtību pieaugumi (pīķi), un to laika momenti precīzi sakrīt ar AL caurlaidspējas grafikos novērotajiem datu trafika kritumiem. Kā piemērs 4.12. a attēlā redzams atbildes laika grafiks “802.11v tīkla asistētas” pārslēgšanās procedūras gadījumam, ja klients pārvietojas ar ātrumu 70 km/h (arī 4.10. c att.).



4.12. att. a) Atbildes laiks, ja braukšanas ātrums ir 70 km/h un izmanto “802.11v tīkla asistētu” pārslēgšanās procedūru; b) Vidējās pārslēgšanās aiztures starp AP pāri, izmantojot dažādas pārslēgšanās procedūras metodes.

4.12. b attēlā parādītas eksperimentāli novērtētās vidējās pārslēgšanās procedūras aiztures starp AP-1 un AP-2, kā arī starp AP-2 un AP-3, izmantojot dažādas pārslēgšanās procedūras metodes, mobilajam klientam pārvietojoties dažādā ātrumā. Katrā braukšanas ātrumā tika izpildīti trīs mērījumi. Pārslēgšanās procedūras aiztures visiem mērījumiem detalizēti apkopotas 5.17. pielikumā.

4.3. tabulā apkopots iegūto pārslēgšanās procedūru aiztures raksturlīkņu novērtējums. Tika aprēķinātas pārslēgšanās procedūru aiztures raksturlīkņu vidējās vērtības starp visiem braukšanas ātrumiem un novērtēti tādi izkliedes rādītāji kā standartnovirze un variācijas koeficients. No iegūtajiem rezultātiem redzams, ka vismazākās vidējās pārslēgšanās procedūras aiztures vērtības ir, izmantojot “802.11v tīkla asistētas” pārslēgšanās procedūras risinājumu.

Vislielākās pārslēgšanās procedūras aiztures rada autentifikācijas, asociācijas, četrvirzienu rokasspiediena un *DHCP* operācijas, kas kopā veido savienojuma nodibināšanas laiku.

Mērījumos tika izmantota *WPA2-PSK* jeb *WPA2-Personal* autentifikācija, tādēļ pie pārslēgšanās procedūras tika izpildīts *EAPOL* process (četrvirzienu rokasspiediena procedūra), kas aizņēma aptuveni 100 ms.

Jāņem vērā, ka pārslēgšanās procedūras aiztures vērtības tika iegūtas no tīkla atbildes laika mērījumiem, līdz ar to tās varēja ietekmēt gan tīkla aiztures, gan klienta un servera pieprasījumu apstrādes laika aiztures.

4.3. tabula

Vidējā pārslēgšanās aizture starp *AP* un izkliedes rādītāji

Pārslēgšanās metode starp <i>AP</i>	Vidējā pārslēgšanās aizture $\bar{\delta}$, ms	Standartnovirze, σ	Variācijas koeficients K_v , %
Standarta, 1-2	848,42	266,61	31,42
Standarta, 2-3	739,79	87,92	11,88
802.11v virzīta, 1-2	838,67	205,20	24,47
802.11v virzīta, 2-3	831,08	97,67	11,75
802.11v asistēta, 1-2	669,25	102,00	15,24
802.11v asistēta, 2-3	700,58	257,88	36,81

Lai ar augstu precizitāti noteiktu pārslēgšanās procedūras aiztures parametru, var izmantot vairākas citas metodes. Piemēram, mērījumu laikā uz klienta (*STA*) vai *AP* nepieciešams aktivizēt notikumu reģistrēšanu (angļu val. *logging*) par klienta *MAC* adresi asociācijas un diasociācijas notikumiem ar ieslēgtu laikspiedolu (angļu val. *timestamp*) vai arī jāveic 802.11 kadru tveršana (angļu val. *packet capture*), piemēram, izmantojot *Wireshark* vai līdzīgu aplikāciju, un pēc tam jāveic iegūto datu analīze.

4.5. Kopsavilkums un secinājumi

Klienta savlaicīgi pieņemts pārslēgšanās procedūras lēmums par pārslēgšanās procedūras sākšanu starp bezvadu piekļuves punktiem un savlaicīgi izpildīta pārslēgšanās procedūra *IEEE 802.11 ESS* infrastruktūras tīklā ar ātri kustīgiem objektiem var efektīvi samazināt caurlaidspējas degradāciju un datu pārraides pārtraukumus, kas novēroti kā datu trafika kritumi vai ieplakas.

Pārslēgšanās procedūras sākšanas lēmuma pieņemšana ir atkarīga no šīs procedūras algoritmā iekļautajiem kritērijiem, tādiem kā *RSS* līmenis, *SNR*, savienojuma datu pārraides ātrums, sakaru kanāla noslodze, kā arī definētajām šo kritēriju trigeru sliekšņvērtībām.

Plānojot *Wi-Fi* infrastruktūru taisnos ceļa posmos un uz automaģistrālēm, būtu jāvadās pēc principa, ka pārslēgšanās procedūrai jānotiek orientējoši pa vidu starp *AP*. Lai nodrošinātu optimālu pārslēgšanos starp *AP*, nepieciešams pieskaņot *AP* raidītāju jaudu atbilstoši *Wi-Fi* infrastruktūras plānojumam (*AP* izvietojums un attālums starp tiem) un definētajām datu pārraides pakalpojumu prasībām, ietverot prasības par šūnu pārklāšanos. Atsevišķos gadījumos

var būt nepieciešama klienta pārslēgšanās procedūras mehānisma RSS trigeru sliekšņvērtības piešķiršana.

No eksperimentos iegūtajiem rezultātiem ir redzams, ka ražotāju piedāvātais ("Standarta") *IEEE 802.11* pārslēgšanās procedūras mehānisms tīklā ar ātri kustīgiem klientiem nenodrošina savlaicīgu pārslēgšanos starp bezvadu piekļuves punktiem. Pārslēgšanās procedūras lēmuma pieņemšanā jāiesaista abas puses – gan *Wi-Fi* tīkls, gan mobilais klients. Tīkls var sniegt atbildi, pie kāda *AP* slēgties, savukārt klients var sniegt atbildi, kurā brīdī iniciēt pārslēgšanās procedūru.

Pārslēgšanās procedūra notiek vairākos *OSI* modeļa slāņos, piemēram, datu pārraides kanāla slānī, tīkla slānī, lietojuma slānī. Tādējādi katrs no šiem slāņiem rada savu laika aizturi un rezultātā veido kopējo pārslēgšanās procedūras laika aizturi. Vislielāko papildinājumu pārslēgšanās procedūras aiztūrei rada datu pārraides kanāla slāņa aktīvās vai pasīvās skenēšanas operācijas, kad tiek noskaidrots jaunais *AP*, uz kuru nepieciešams pārslēgties. Skenēšanas fāze aizņem pārāk ilgu laiku, un tās rezultātā netiek savlaicīgi izpildīta pārslēgšanās procedūra, tādēļ tiek novērots uztvertā signāla līmeņa un līdz ar to arī datu pārraides ātruma straujš kritums.

AP skenēšanas fāzi var aizstāt ar *IEEE 802.11v* standartā iestrādāto funkcionalitāti, kur tiek izmantoti *802.11v* *BSS* pārejas vadības ziņojumi, ar kuru palīdzību ir iespējams mobilajam klientam nodot *AP* kandidātu sarakstu. Lai risinājums būtu piemērots izmantošanai automobiļu sakaru tīklos, kur iespējami lieli klienta pārvietošanās ātrumi, nepieciešams modificēt izmantoto *802.11v* "*BSS* pārejas vadības pieprasījuma" ziņojumu tā, lai klients, to saņemot, obligāti veiktu pārslēgšanos uz norādīto *AP*, jo *WLAN IEEE 802.11* standartā šis lēmums ir atstāts klienta pārziņā.

Izmantojot *IEEE 802.11v* standartu un modificējot to, tika izstrādāts automātiskās "*802.11v* tīkla asistētas" pārslēgšanās procedūras risinājums, kas ietver "tīkla virzītas" pārslēgšanās procedūras elementus, un ļauj tīklam (*AP*) izpildīt komandas un ietekmēt klienta pārslēgšanās procedūru, lai nodrošinātu klienta pārslēgšanos uz noteiktu *AP*.

Tika secināts, ka "*BSS* pārejas vadības pieprasījuma" ziņojumos pieejamais "nenovēršamās diasociācijas funkcijas" karogs, kur tiek izmantots ziņojuma lauks "*ESS* diasociācija nenovēršama", klientam tikai rekomendē veikt pārslēgšanos uz citu *AP*. Klients šo rekomendāciju var arī neņemt vērā un nepārslēgties uz citu *AP*, tādējādi var tikt ignorēts piedāvātais bezvadu piekļuves punktu kandidātu saraksts.

Lai paātrinātu un garantētu veiksmīgu pārslēgšanās procedūras izpildi, bezvadu tīklā ar ātri kustīgiem objektiem, promocijas darba autors rekomendē "*BSS* pārejas vadības pieprasījuma" ziņojumā ieviest jaunu karogu. Saņemot no *AP* "*BSS* pārejas vadības pieprasījuma" ziņojumu ar jauno karogu, klientam būs obligāti jāpārslēdzas uz to *AP*, kas norādīts "*BSS* pārejas vadības pieprasījuma" laukā "*BSS* pārejas kandidātu saraksta ieraksti". Speciālā karoga ieviešanai var izmantot "*BSS* pārejas vadības pieprasījuma" ziņojuma lauka "Pieprasījuma režīms" apakšlauku "Rezervēts", t. i., 5. līdz 7. bitu (4.4. att.). Šāda procedūra nav definēta *IEEE 802.11v* standartā, un tas ir jauns pārslēgšanās procedūras koncepts.

Eksperimentāli tika noteikts, ka vislabākos aplikācijas līmeņa caurlaidspējas un atbildes laika rezultātus ar vismazākajiem izkliedes rādītājiem dažādos automobiļa pārvietošanās ātrumos dod metode ar automātisko "*802.11v* tīkla asistētas" pārslēgšanās procedūras

risinājumu. Tika parādīts, ka šajā režīmā var nodrošināt optimālu un precīzu pārslēgšanos starp infrastruktūras AP. Galvenie pārslēgšanās procedūras uzdevumi ir minimizēt pārslēgšanās procedūras aizturi un atjaunot datu pārraidi, minimizējot savienojuma dīkstāves vai izveides laiku. Tīkla atbildes laika parametram tā vērtību vislielāko pieaugumu rada tieši pārslēgšanās procedūra. *IEEE 802.11* bāzētos automobiļu sakaru tīklos nepieciešams samazināt pārslēgšanās procedūras aiztures, lai nodrošinātu nepārtrauktus, kvalitatīvus datu pārraides pakalpojumus automobiļu sistēmām un to pasažieriem.

Pēc eksperimentāli iegūto rezultātu analīzes var secināt, ka savlaicīgi pieņemot pārslēgšanās procedūras lēmumu un izmantojot *IEEE 802.11v* standarta “BSS pārejas vadības vaicājuma” un “BSS pārejas vadības pieprasījuma” ziņojumus ar izstrādāto modifikāciju savienojumā ar *IEEE 802.11ac* standartu, var izmantot ātri kustīgu objektu (>20 km/h) pārslēgšanās procedūras nodrošināšanai. Rezultātā vidējā aplikācijas līmeņa caurlaidspēja tika palielināta par 75 %, salīdzinot ar “Standarta” pārslēgšanās procedūru, kur netika izmantots *IEEE 802.11v* standarts. Kā arī par 67 % tika samazināts vidējais tīkla atbildes laiks un tika nodrošinātas mazākas vidējās pārslēgšanās procedūras aiztures. Mērījumi tika veikti, mobilajam klientam pārvietojoties ar ātrumu no 20 km/h līdz 90 km/h. *IEEE 802.11ac* standarta vietā var izmantot arī *IEEE 802.11-2016* standartā iekļautos *IEEE 802.11a/b/g/n* standartus, kuriem ir jābūt savietojamiem ar *IEEE 802.11v*. Tāpat savietojamam vajadzētu būt arī jaunajā standarta versijā *IEEE 802.11-2020* iekļautajam standarta papildinājumam *IEEE 802.11ax*. Jāatzīmē, ka šāds eksperimentāls risinājums iepriekš nav realizēts.

Lai papildus paātrinātu pārslēgšanās procedūru, kad ir ieviests “802.11v tīkla asistētas” pārslēgšanās procedūras risinājums, klienta pusē var tikt atslēgta “BSS pārejas vadības atbildes” ziņojuma izsūtīšana, kas ir atbilde uz saņemto “BSS pārejas vadības pieprasījuma” ziņojumu.

Lai praksē realizētu piedāvāto “802.11v tīkla asistētas” pārslēgšanās procedūras risinājumu, ir jāmodificē *Wi-Fi* infrastruktūras un tīkla klienta aparatūras programmatūra. Tas ir izdarāms, atjauninot iekārtu aparātprogrammatūru ar specializētu tās versiju. *IEEE 802.11v* standartu būtu jāizmanto apvienojumā ar *IEEE 802.11k* un *IEEE 802.11r* standartiem. *IEEE 802.11k* standarts ir jāievieš, lai nodrošinātu automātiski sastādītu AP datubāzi ar “BSS pārejas kandidātu sarakstu”, kas tiek iegūts, izmantojot kaimiņu AP pārskata datus.

Papildu metrikas, kuras var iekļaut pārslēgšanās procedūras lēmuma pieņemšanā, ir mobilā klienta kustības virziena un ātruma dati, lai *Wi-Fi* tīkls dinamiski un savlaicīgi spētu piedāvāt kandidātu sarakstu ar kaimiņu AP. Datu iegūšanai var izmantot tādas metodes kā tiešsaistes GPS dati, GPS inerciālā navigācija, AP triangulācija. Savukārt automaģistrālēs vai klientam jau zināmos ceļa posmos var izmantot jau iepriekš sastādītu AP datubāzi, kas pasīvā režīmā tiek atjaunota, lai paātrinātu klienta pārslēgšanos starp AP. Ja mobilā klienta kustības ātrums ir lielāks par 90 km/h un attālums starp AP ir <150 m, pārslēgšanās procedūras algoritmā var iestrādāt noteikumu, kur pārslēgšanās procedūra tiek izpildīta, izlaižot vienu AP, tā nodrošinot ilgāku savienojuma laiku. Prognozējams, ka tādā veidā būtu iespējams paaugstināt vidējos tīkla veikspējas parametrus.

Realizējot “802.11v tīkla asistētas” pārslēgšanās procedūras risinājumu *Wi-Fi* tīklos ar ātri kustīgiem objektiem, pārslēgšanās procedūras aizture starp AP joprojām saglabājas ievērojama, t. i., aptuveni 0,68 s. Šo aizturi papildus var samazināt, ieviešot centralizētas automobiļu

bezvadu sakaru tīkla infrastruktūras pārvaldības modeli, t. i., ieviešot centralizētu *Wi-Fi* kontrolieri, kas pārslēgšanās procedūras brīdī organizētu klienta datu uzkrāšanu vecajā *AP* un tālāk organizētu to pārsūtīšanu uz jauno *AP*. Projektējot *WLAN* bāzētus automobiļu sakaru tīklus, jāņem vērā arī aiztures, ko var radīt izvēlētais tīklu drošības risinājums. Lai minimizētu pārslēgšanās procedūras aiztures, kas saistītas ar klientu autentifikāciju un datu šifrēšanu *L2* slānī, tiek rekomendēts tīklos ar iestrādātu *WPA2* drošības mehānismu ieviest *IEEE 802.11r* standartu, kas nodrošina ātrās *BSS* pārejas funkcionalitāti drošai un ātrai klientu autentifikācijai. Tādējādi tiek organizēta klienta autentifikācijas datu izplatīšana starp bezvadu piekļuves punktiem. Rezultātā, klientam pārslēdzoties uz jauno *AP*, atliktu izpildīt tikai reasociācijas procedūru, t. i., šajā gadījumā klientam no jauna nav jāatkārto pilnā autentifikācijas un asociācijas procedūra.

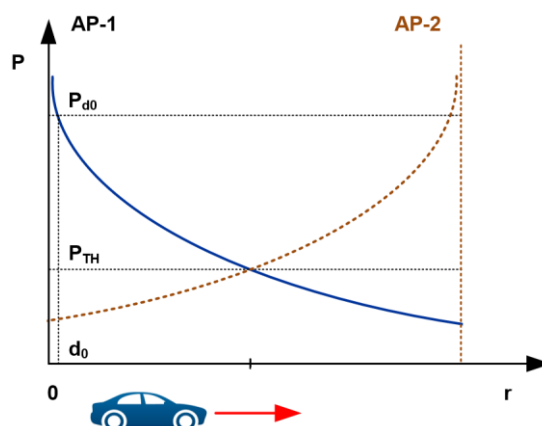
Sakarā ar to, ka tika pārbaudītas “*802.11v BSS pārejas vadības*” funkcionalitātes iespējas un *IEEE 802.11v* standarta modifikācijas efektivitāte, kas sekmēja pārslēgšanās procedūras paātrināšanu, paaugstināja *AL* caurlaidspējas vidējās vērtības un ļāva samazināt tīkla atbildes laika vidējās vērtības, tāpēc piedāvātais pārslēgšanās procedūras risinājums uzskatāms par perspektīvu un attīstāmu. Promocijas darba autors rekomendē automobiļu sakaru tīklos, kas bāzēti *IEEE 802.11ac* standartā, iekļaut *IEEE 802.11v* standarta atbalstu ar izstrādāto modifikāciju. Šī rekomendācija attiecas arī uz automobiļu sakaru tīkla klientiem.

5. UZTVERTĀ WLAN SIGNĀLA JAUDAS LĪMEŅA UN CAURLAIDSPĒJAS NOVĒRTĒJUMS ATKARĪBĀ NO ATTĀLUMA LĪDZ RAIDĪTĀJAM

Šajā nodaļā, izmantojot gan eksperimentālos datus, gan teorētiskos aprēķinus, noteikti tādi transportlīdzekļu sakaru kanālu veiktspējas parametri kā uztvertā signāla jaudas līmenis un sakaru kanāla caurlaidspēja atkarībā no transportlīdzekļa attāluma līdz raidītājam. Aprēķinos ņemtas vērā arī uztvertā signāla fluktuācijas, kas ir saistītas ar signāla vairākceļu izplatīšanos. *Matlab* kodi izstrādāto likumsakarību aprēķiniem apkopoti 7. pielikumā. Iegūtie rezultāti atspoguļoti zinātniskajā publikācijā [9].

5.1. Signāla jaudas līmeņa atkarība no attāluma līdz raidītājam

Mobilajam klientam pārvietojoties starp *Wi-Fi* tīkla pārklājuma zonām, mainās piesaiste pie bezvadu piekļuves punktiem (AP). 5.1. attēlā atspoguļota eksperimentāli novērota likumsakarība starp uztverto signāla jaudas līmeni, kas apzīmēts ar P (tiek izmantots RSS parametrs), un attālumu līdz bezvadu piekļuves punktam r . Uztvertā signāla stipruma parametrs RSS raksturo uztverto signāla jaudu P [110]. 5.1. attēlā parādīts mobilais klients, kurš sāk kustību no AP-1 un pārvietojas nākamā bezvadu piekļuves punkta AP-2 virzienā. P_{d0} ir uztvertā signāla jaudas līmenis pie minimālā attāluma d_0 no klienta līdz AP-1, un P_{TH} jeb RSS_{TH} ir sliekšņvērtība, pie kuras mobilais klients izpilda pārslēgšanās procedūru uz nākamo AP. Novērots, ka, mobilajam klientam attālinoties no AP, uztvertā signāla jaudas līmenis P jeb RSS samazinās, turklāt RSS signāla līmenis ne tikai samazinās, bet arī fluktuē ap tā vidējo vērtību.



5.1. att. Uztvertā signāla jaudas parametra P izmaiņas atkarībā no attāluma līdz raidītājam.

Veicot eksperimentālos mērījumus, tika konstatēts, ka uztvertā signāla RSS jaudas līmeņu straujas fluktuācijas izraisa laikā nobīdītu pārslēgšanās procedūras inicializāciju. Tā var tikt sākota vai nu pārāk ātri vai arī novēloti atkarībā no tā, kad tiek pārsniegta RSS_{TH} vērtība. Tas pats attiecas arī uz pieslēgšanos *Wi-Fi* tīklam mērījumu sākuma fāzē. Tādēļ šādas signālu fluktuācijas ir jāņem vērā, izstrādājot pārslēgšanās procedūras algoritmus, lai nodrošinātu

korektu un efektīvu šo algoritmu darbību. Līdzīgi eksperimentālie novērojumi un ar to saistītās problēmas ir aprakstītas arī pētījumā [50].

Šajā apakšnodaļā plānots pārliecināties, vai eksperimentālie novērojumi saskan ar teoriju un citu pētījumu rezultātiem [20], [111], [119]. Teorētiski tiks aprēķināta likumsakarība starp signāla jaudas līmeņa izmaiņām un attālumu līdz raidītājam, kā arī tiks ņemtas vērā uztvertā signāla fluktuācijas. Šie dati būs nepieciešami turpmākajos aprēķinos, lai noteiktu teorētisko sakaru kanāla caurlaidspēju.

Transportlīdzekļa infrastruktūras sakaru kanāla modelis

Viens no V2I sakaru kanāla (sakaru kanāls starp automobili un fiksēto ceļmalas infrastruktūru) ģeometriskajiem modeļiem, kas ņem vērā vairāk nekā vienu iespējamo signāla izplatīšanās ceļu ir divstaru plakanas zemes virsmas (angļu val. *two-ray flat-earth*) modelis [41]. Šajā modelī uztvertais signāls tiek veidots no tieši uztvertā signāla un zemes virsmas atstarotā signāla. Mazos attālumos šis modelis dod ātras signāla fluktuācijas, jo no zemes virsmas atstarotais signāls nobīdās fāzē attiecībā pret tieši uztverto signālu. Lielos attālumos starp raidītāju un uztvērēju tieši uztvertā un no zemes virsmas atstarotā signālu izplatīšanās ceļi kļūst gandrīz vienādi. Robežu starp šiem diviem apgabaliem d_c nosaka pēc 5.1. izteiksmes. Izmantojot 5.1. tabulā apkopotos eksperimentāli iegūtos datus [41], [70], tika veikti aprēķini un noteikts parametrs $d_c = 191$ m.

$$d_c = \frac{4h_t h_r}{\lambda_v}, \quad (5.1.)$$

kur h_t – raidošās antenas augstums, m; h_r – uztverošās antenas augstums, m; λ_v – viļņa garums, m.

Divstaru modelī tiek pievienotas gadījuma fluktuācijas, kuru statistika ir atkarīga no fizikālās staru izkliedes vidē, tiek pieņemts Gausa sadalījums, kura vidējā vērtība ir nulle, kas dod pieņemamu rezultātu un saskan ar mērījumiem. To sauc par logaritmiski normālo (angļu val. *log-normal*) modeli. Modeļa pieraksts vispārīgā formā dots 5.2. vienādojumā. Modelis ļauj noteikt uztvertā signāla jaudas līmeni P atkarībā no attāluma r starp raidītāju un uztvērēju. Promocijas darbā apskatīts gadījums, ja signāli izplatās nelielos attālumos, t. i., ja $d_0 \leq r \leq d_c$ [41], [44], [54].

$$P(r) = P(d_0) - 10u \log_{10} \left(\frac{r}{d_0} \right) + X_\sigma, \quad (5.2.)$$

kur $P(r)$ – uztvertā signāla jaudas līmenis (atbilst RSS) atkarībā no r , dBm; d_0 – attālums no bezvadu piekļuves punkta (AP) līdz transportlīdzeklim, m; r – attālums starp raidītāju un uztvērēju, m; $P(d_0)$ – uztvertā signāla jaudas līmenis, kad klients atrodas tieši pretī bezvadu piekļuves punktam, dBm; u – trases zudumu rādītājs (angļu val. *path loss exponent*); X_σ – gadījuma izlases mainīgais, dB.

Eksperimentāli iegūtie dati

Parametrs	Vērtība
h_t	1,85 m
h_r	1,5 m
λ_v	0,058 m
d_0	3,5 m
$P(d_0)$	-49 dBm
r	3,5–100 m
u	1,9
σ	5,9 dB

Parametru u un σ (kur σ – standartnovirze gadījuma izlases mainīgajiem X_σ) vērtības automaģistrāles gadījumam ir eksperimentāli iegūtas pētījumā [41] un apkopotas 5.1. tabulā. Eksperimentālajos mērījumos izmantotais raidītājs un uztvērējs atbalsta *IEEE 802.11ac* standartu, kas arī tika izmantots [70].

Uztvertā signāla jaudas līmenis bez fluktuācijām

Izmantojot 5.2. izteiksmi, tika aprēķinātas $P(r)$ vērtības, neņemot vērā X_σ . 5.2. attēlā redzams iegūtais grafiks uztvertā signāla jaudas atkarībai no attāluma līdz raidītājam bez signāla fluktuācijām (sarkanā līkne).

Uztvertā signāla jaudas līmenis ar fluktuācijām

Sakarā ar nelieliem attālumiem, kas ir raksturīgi V2I/V2X savienojumos, precīzāku signālu svārstību aprakstu dod maza mēroga rimšanas modeļi, kur svārstības izraisa konstruktīva un destruktīva interference starp vairākceļu (angļu val. *multipath*) signāla izplatīšanās komponentēm. Ja fāzē esošās un kvadrātiskās signāla komponentes svārstās kā neatkarīgi Gausa sadalījuma izlases mainīgie, tad tas dod Releja (*Rayleigh*) vai Raiza (*Rician*) statistikas rezultātus atkarībā no tā, ir vai nav tiešā redzamība. Uztvertā signāla sadalījums, ar kuru iespējams modelēt abu veidu statistiku, ir Nakagami sadalījums (5.3. vienādojums).

$$f(x; \alpha, \omega) = \frac{2\alpha^\alpha x^{2\alpha-1}}{\omega^\alpha \Gamma(\alpha)} e^{-\frac{\alpha x^2}{\omega}}, \quad (5.3.)$$

kur α – formas (angļu val. *shape*) parametrs; ω – vidējās jaudas novērtējums rimšanas apliecējā (angļu val. *fading envelope*); x – vispārīgs gadījumskaitlis, kas pakļauts Nakagami sadalījumam.

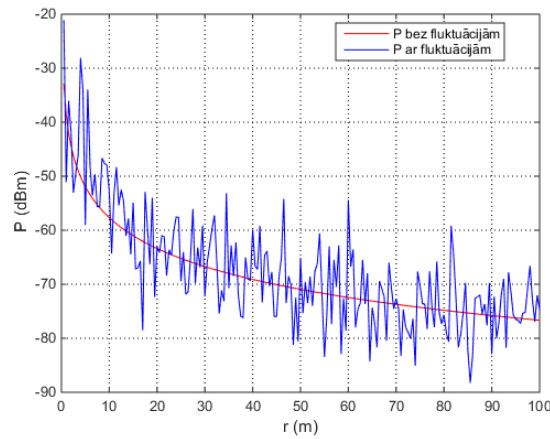
Gadījumā, ja $\alpha = 1$, Nakagami sadalījums apraksta Releja sadalījumu. Savukārt, ja $\alpha > 1$, tad tas ir Raiza sadalījums. Vidējā uztvertā signāla jaudas svārstību vērtība aprēķināma pēc 5.4. izteiksmes.

$$\bar{X}_\sigma = \int_0^\infty xf(x; \alpha, \omega)dx = \int_0^\infty x \left(\frac{2\alpha^\alpha x^{2\alpha-1}}{\omega^\alpha \Gamma(\alpha)} e^{-\frac{\alpha x^2}{\omega}} \right) dx. \quad (5.4.)$$

Aprēķinos tiek pieņemts, ka $\alpha = 1$, tādējādi 5.4. izteiksme vienkāršojas:

$$\bar{X}_\sigma = \int_0^\infty \frac{2x^2}{\omega} e^{-\frac{x^2}{\omega}} dx. \quad (5.5.)$$

Izmantojot 5.5. izteiksmi, tika noteikta ienestā signāla fluktuāciju ietekme uz $P(r)$ (5.2. izteiksme). Aprēķinos tika izmantots $\omega = 1$. Vispirms tika aprēķināta jaudas svārstību vidējā vērtība $\bar{X}_\sigma$. Tālāk tika uzģenerētas gadījuma vērtības ar Gausa jeb normālo sadalījumu, kur tika izmantotas iegūtās $\bar{X}_\sigma$ vērtības un eksperimentāli iegūtā standartnovirze σ gadījuma izlases mainīgajiem X_σ , kas atbilst automaģistrāles scenārijam (5.1. tab.) [41]. 5.2. attēlā redzami iegūtie rezultāti (zilā līkne).



5.2. att. Teorētiski aprēķinātā uztvertā signāla jauda P atkarībā no attāluma līdz raidītājam bez un ar jaudas fluktuācijām.

5.2. Caurlaidspējas atkarība no uztvertā signāla jaudas līmeņa un attāluma līdz raidītājam

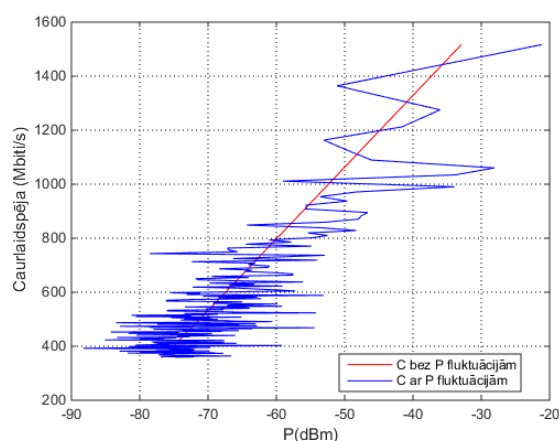
Sakaru kanāla caurlaidspējas augšējās robežas jeb kanāla kapacitātes C (biti/s) aprēķinam tiek izmantota Šenona frekvenču kanāla kapacitātes teorēma (turpmāk tekstā – Šenona teorēma) (5.6. vienādojums). Tā raksturo fizikālā slāņa caurlaidspēju, kas dod iespēju novērtēt kanāla ideālo lielumu, t. i., maksimālo teorētiski iegūstamo caurlaidspēju [12], [57], [109]. Tā reprezentē ideālo sistēmu ar Gausa troksni [17], [21], kur bitu kļūdu līmeni var samazināt līdz nullei, piemērojot atbilstošas kodēšanas shēmas, ja lietotāja datu pārraides ātrums ir mazāks par kanāla kapacitāti. Tomēr šādi kodi vēl nav izstrādāti, tas ir arī viens no iemesliem, kāpēc praksē tiek iegūti vairākas reizes mazāki datu pārraides ātrumi.

$$C = B \log_2 \left(1 + \frac{S}{N} \right), \quad (5.6.)$$

kur C – frekvenču kanāla kapacitāte, biti/s; B – frekvenču kanāla joslas platums, Hz; S – uztvertā signāla vidējā jauda kanālā, W; N – trokšņa vai traucējumu signāla vidējā jauda kanālā, W.

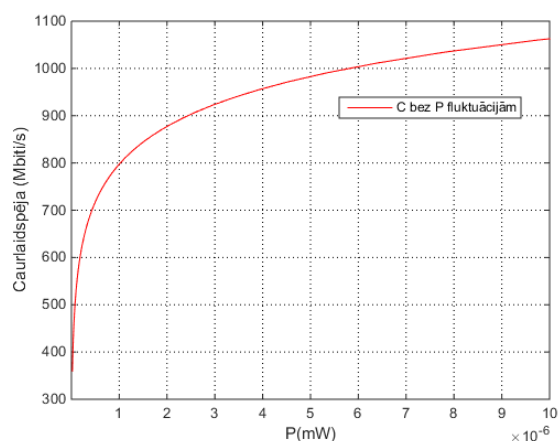
Izmantojot 5.6. un 5.2. izteiksmi, tika aprēķināta teorētiskā caurlaidspēja C ideālam sakaru kanālam. Aprēķinos tika izmantotas parametru vērtības $B = 80$ MHz un $N = -90$ dBm, kur parametrs N tika pārkonvertēts uz milivatiem (mW). Mainīgais S atbilst 5.2. izteiksmes parametram $P(r)$ un tika izteikts mW.

5.3. attēlā redzams iegūtais aprēķinu rezultāts, kā mainās sakaru kanāla maksimālā caurlaidspēja (kapacitāte) C atkarībā no uztvertā signāla jaudas līmeņa P (dBm) ar uztvertā signāla jaudas līmeņa fluktuācijām un bez tām.



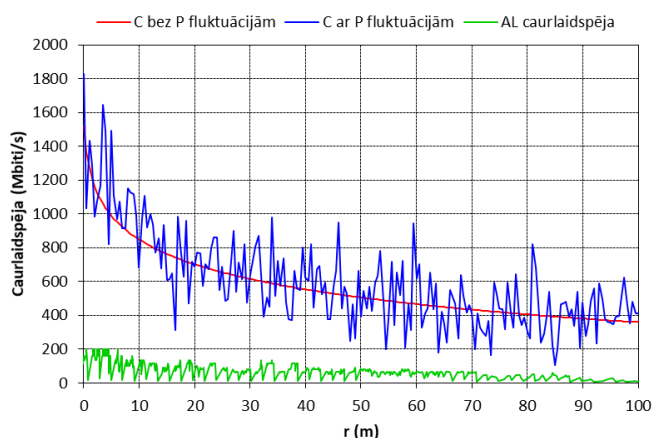
5.3. att. Teorētiski aprēķinātā caurlaidspēja C atkarībā no uztvertā signāla jaudas P (dBm) bez un ar jaudas fluktuācijām.

5.4. attēlā papildus dota teorētiski aprēķinātā signāla jauda P (mW) atkarībā no sakaru kanāla caurlaidspējas C . Parametrs P tika ielikts robežās 10^{-9} – 10^{-5} mW, kas dod praktiski sasniedzamus rezultātus.



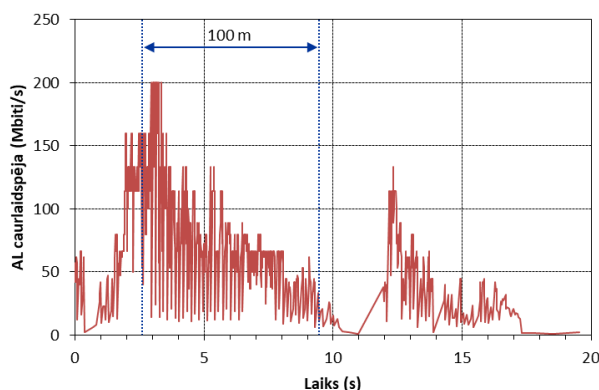
5.4. att. Teorētiski aprēķinātā caurlaidspēja C atkarībā no uztvertā signāla jaudas P (mW) bez jaudas fluktuācijām.

Tālāk tika aprēķināta sakaru kanāla caurlaidspēja C atkarībā no attāluma līdz raidītājam. Teorētiski iegūtie caurlaidspējas C rezultāti (sarkanā un zilā līkne) tika apvienoti vienā grafikā ar eksperimentāli iegūtajiem AL caurlaidspējas rezultātiem (zaļā līkne) (5.5. att.).



5.5. att. Teorētiski aprēķinātā caurlaidspēja C bez un ar P fluktuācijām un eksperimentāli iegūtā AL caurlaidspēja atkarībā no attāluma līdz raidītājam.

Zaļā līkne 5.5. attēlā reprezentē eksperimentāli iegūto AL caurlaidspēju, kur izmantoti mērījumu dati no 5.6. attēla, ja kustības ātrums ir 50 km/h, laika intervālā, kad *Wi-Fi* mobilais klients sākumā atrodas pretī *AP*, pēc tam attālinās no tā par 100 m (laika izteiksmē tas atbilst 7,2 s). Mērījumi tika veikti vienranga *IEEE 802.11ac* tīklā, izmantojot standarta bezvadu tīkla klientu. Atrodoties tieši pretī *AP*, klients sasniedz maksimālo AL caurlaidspēju. Attālinoties no *AP*, attālums r palielinās, un AL caurlaidspēja krītas.



5.6. att. Eksperimentāli iegūtā AL caurlaidspēja, ja klienta pārvietošanās ātrums ir 50 km/h.

5.3. Kopsavilkums un secinājumi

Teorētiskie aprēķini, tāpat kā veiktie eksperimentālie novērojumi un mērījumi, rāda, ka *WLAN* tīklā, mobilajam klientam attālinoties no raidītāja, uztvertā signāla jauda pavājinās un rezultātā samazinās arī caurlaidspēja. Uztvertā signāla jauda P ir laikā mainīga un fluktuējoša. Uztvertā signāla jaudas svārstības izraisa konstruktīva un destruktīva interference starp vairākceļu signāla izplatīšanās komponentēm. Tas izraisa arī caurlaidspējas fluktuācijas. Jāņem vērā, ka, izmantojot teorētiskos aprēķinus, iegūtie grafiki (5.3.–5.5. att.) ir saistīti ar idealizāciju, jo aprēķinos tiek izmantota Šenona teorēma [12], [56]. Teorētiskajos aprēķinos

netika ņemts vērā klienta pārvietošanās ātrums. Pētījuma mērķis bija pārlicināties, vai eksperimentāli iegūtie dati atbilst klasiskiem secinājumiem, kas izriet no Šenona teorēmas.

Teorētiski aprēķinātā bezvadu kanāla kapacitāte jeb maksimāli iespējamā caurlaidspēja C ir vairākas reizes lielāka, salīdzinot ar eksperimentāli iegūto aplikācijas līmeņa (AL) caurlaidspēju. Līkņu tendence un raksturs ir līdzīgs, taču absolūtās vērtības atšķiras, jo Šenona teorēma paredz datu pārraides ātruma noteikšanu ideālam kanālam, tā ir fizikālā vide, un aprēķinos netiek ņemta vērā augstāku *OSI* modeļa slāņu ietekme. Jāatzīmē, ka eksperimentālie mērījumi gadījumā ar stacionāru bezvadu tīkla klientu, kur pakāpeniski tiktu palielināts tā attālums līdz raidītājam, uzrādītu labākus aplikācijas līmeņa caurlaidspējas rezultātus, salīdzinot ar kustībā esošu klientu. Pētījumā izmantotā *Wi-Fi* tehnoloģija spēj nodrošināt eksperimentāli iegūtos aplikācijas līmeņa caurlaidspējas rezultātus konkrētos lauka apstākļos, redzams, ka joprojām ir liela rezerve līdz teorētiskajiem “griestiem”. Pilnveidojot atklādošanas protokolus, var palielināt kopējo tīkla caurlaidspēju. Augstāki *OSI* modeļa slāņi spēj atpazīt datus tikai tad, ja tie ir loģiski noformēti. Tādēļ ir nepieciešama, piemēram, kadru, *IP* pakešu un *ACK* ziņojumu formēšana. Ja tiek izmantots *TCP* transporta protokols, nepieciešams veikt papildu uzdevumus, lai pārraidītu datus. Piemēram, *TCP* sesijas nodibināšanas laikā notiek trīsvirzienu rokasspiediena procedūra, savukārt pakešu pazaudēšanas gadījumā tiek veikta atkārtota datu pārsūtīšana. Katrs *OSI* slānis (no *L7* līdz *L2*) rada papildu trafiku jeb virstēriņus, tādus kā informācija par izmantotā lietojuma (aplikācijas) slāņa protokolu (piemēram, *FTP*), *TCP* iesākums, *IP* iesākums, *Ethernet* iesākums u. c. komunikācijas dati, kas ir jāpārsūta, un Šenona teorēmā tas netiek ņemts vērā. Veiktie teorētiskie aprēķini pamato iepriekšējās nodaļās eksperimentāli iegūtos rezultātus.

NOBEIGUMS

Strauji pieaugošais datu trafika apjoms un klientu skaita palielinājums bezvadu sakaru tīklos [33] veicina pieprasījumu pēc lielas caurlaidspējas bezvadu sakaru tīkliem un to sniegtās mobilitātes. Līdz ar to klienti pieprasa augsta līmeņa savienojamības risinājumus, ne tikai izmantojot fiksētus bezvadu tīkla savienojumus, piemēram, atrodoties mājās vai birojos, bet arī atrodoties ceļā. To apstiprina arī prognozes [140], kas parāda, ka tuvākajos gados aizvien pieaugs gan privāto automobiļu, gan komerctransporta skaits uz ceļiem, kā arī pieaugs šo transportlīdzekļu pārvietošanās intensitāte. Tas nozīmē, ka automobiļu pasažieri aktīvi izmantos datu pārraides pakalpojumus brauciena laikā. Minētās tendences pamato nepieciešamību pēc mūsdienīgiem, tehniski un ekonomiski pamatotiem intelektuālo transporta sistēmu sakaru risinājumiem.

Promocijas darba **1. nodaļā** apskatīti vairāki tehnoloģiski risinājumi, kas var tikt izmantoti, lai nodrošinātu automobiļus ar datu pārraides pieslēgumu pakalpojumiem. ITS vajadzībām tiek izmantotas WAVE un ITS-G5 tehnoloģijas, kas izmanto IEEE 802.11p protokolu ar salīdzinoši nelielu datu caurlaides joslu. Tiek strādāts arī pie 5G C-V2X risinājuma, savukārt LTE C-V2X risinājums jau ir izstrādāts. Minētās ITS tehnoloģijas ir paredzētas drošības uzlabošanai uz ceļiem, komunikācijai starp transportlīdzekļiem, pārejām ceļu satiksmes dalībniekiem un infrastruktūru, apziņošanai un brīdināšanai. Tomēr šīs tehnoloģijas nav paredzētas transportlīdzekļu pasažieru piekļuves organizēšanai interneta tīklam. Veicot teorētisko izpēti, tika secināts, ka WLAN IEEE 802.11n/ac tehnoloģijas var izmantot autotransporta jomā, lai nodrošinātu datu pārraides kanālu pieslēgumus automobiļu pasažieriem, kas atbilst ITS pakalpojumu grupai “Informācija un izklaide”, it īpaši vietās, kur ir spēkā pilsētvidei raksturīgie braukšanas ātrumi un ir pieejams plašs bezvadu tīkla pārklājums vai jau pastāv infrastruktūra šāda tīkla izvēršanai. WLAN piekļuves tīklus var izmantot arī citu ITS pakalpojumu atbalstam, kas ir ietverti pakalpojumu grupā “Transporta plūsmu vadība un transporta sistēmu pakalpojumi”, piemēram, liela datu apjoma pārsūtīšanai (tiešsaistes video trafiks par stāvvkli uz ceļa, navigācijas karšu atjaunošana, automobiļu programmatūras atjaunošana u. c.). Promocijas darba pētījumiem izvēlēto WLAN tehnoloģiju kā ITS datu pārraides piekļuves risinājumu pamato arī datu trafika prognoze pēc piekļuves tehnoloģijas, kā arī atslogotā mobilā trafika prognoze [33], [142]. Jāatzīmē, ka 5G tīkli paredz izmantot vairākas tehnoloģijas, ieskaitot WLAN [11], [43].

WLAN tīklu izmantošana ātri kustīgiem objektiem saskaras ar vairākām problēmām. Novērots, ka, pieaugot WLAN klientu kustības ātrumam, samazinās klientu sasniedzamā maksimālā caurlaidspēja [24]. Tas galvenokārt ir saistīts ar pārslēgšanās procedūru izpildi, kas, pieaugot klientu pārvietošanās ātrumam, kļūst nestabilas un tiek izpildītas novēloti, kā arī pieaug pārslēgšanās procedūru biežums. Jāņem vērā, ka pārslēgšanās procedūras ilgumu var ietekmēt arī WLAN tīklā realizētie drošības mehānismi. WLAN bezvadu sakaru šūnu tīkliem ir raksturīgs augsts datu pārraides kļūdu līmenis un lielas tīkla aiztures. Bezvadu tīkla signāli ir jutīgi pret ārējiem traucējumu avotiem, rezultātā var tikt pazaudēti klienta sūtītie dati, kas pēc tam atkārtoti jāpārsūta, kā to paredz 802.11 MAC un TCP protokolu algoritmi. TCP protokolā realizētie tīkla pārslodzes novēršanas mehānismi var negatīvi ietekmēt arī bezvadu tīklu

veiktspēju [123]. Gadījumos ar ātri kustīgiem klientiem šie efekti tikai pastiprinās. Kopējo tīkla veiktspēju nosaka arī tīkla individuālo sakaru mezglu veiktspēja. *WLAN* tehnoloģija saskaras arī ar problēmām, kas ir saistītas ar tās ierobežotajām mobilitātes iespējām, īpaši aktuāli tas ir ārpus apdzīvotām vietām. Lai risinātu iepriekš minētās problēmas, kas ir saistītas ar *WLAN* veiktspējas samazināšanos ātri kustīgiem klientiem, ir jāveic padziļināti pētījumi.

Atrisinot problēmas, kas ir saistītas ar *WLAN* tīklos pārāk ilgo un nekorekto pārslēgšanās procedūru ātri kustīgiem objektiem (>70 km/h), *WLAN* tehnoloģiju veiksmīgi var izmantot arī gar automaģistrālēm, kur ir raksturīgi lieli pārvietošanās ātrumi (>90 km/h), lai nodrošinātu datu pārraides pakalpojumus autotransportam

Papildinot *WLAN* piekļuves tīklu ar *LTE* tīkla tehnoloģiju, tiek iegūta funkcionāla, praksē izmantojama divrangu sakaru sistēma, kas veido integrētu *WLAN* un *LTE* sakaru kanālu un spēj nodrošināt piekļuvi interneta tīklam. Tādēļ veiktspējas pētījumi ir jāveic arī divrangu sakaru tīklam. Lai pilnvērtīgi izvērtētu apvienotā *WLAN* un *LTE* tehnoloģiju risinājuma piemērotību izmantošanai automobiļu sakaru tīklos, nepieciešams veikt šāda transporta sakaru tīkla veiktspējas parametru mērījumus lauka apstākļos, tādējādi pēc iespējas pietuvinot mobilā klienta pārvietošanos reāliem ceļu satiksmes apstākļiem.

Bieži vien bezvadu sakaru tīklu eksperimentālie veiktspējas mērījumi lauka apstākļos nav iespējami savas specifikas dēļ, jo nav pieejama nepieciešamā mēraparatūra un atbilstoša testgultnes infrastruktūra vai arī jāpielāgojas laikapstākļiem. Tādu mērījumu veikšana ir sarežģīts, organizatorisks pētniecības darbs, kas prasa padziļinātas tehnoloģiskas zināšanas, lielus resursus, kā arī tas ir laikietilpīgs process un prasa lielu sagatavošanās laiku. Strādājot pie testgultnes izveides, ir jādoma par tās atrašanās vietu un mērogu, kā tiks nodrošināta fiziskā drošība mērījumu laikā, risināts elektrobarošanas avotu pieejamības jautājums testgultnes vajadzībām u. tml. Neskatoties uz ierobežojumiem un grūtībām, ar kurām saskaras pētnieki, eksperimentālo mērījumu laikā strādājot jau ar nofiksētas arhitektūras un konfigurācijas testgultnēm, tas tikai parāda šādu pētījumu nozīmību. Šādas testgultnes ir izveidotas konkrētu, definētu pētījuma mērķu sasniegšanai. Lauka apstākļos iegūtie eksperimentālie mērījumu rezultāti ir ļoti svarīgi un nepieciešami definēto teoriju un izstrādāto analītisko modeļu pārbaudei, simulācijas sistēmu kalibrēšanai un jaunu likumsakarību atklāšanai, kā arī jaunu produktu un risinājumu testēšanai un uzlabošanai.

Promocijas darba **2. nodaļā** veikts *WLAN* un *LTE* tehnoloģiju apskats, pētīti tādi jautājumi kā *WLAN* un *LTE* tīklu konverģences iespējas ar mērķi palielināt *WLAN* klientu mobilitāti, kā arī veikta detalizēta izpēte par pieejamiem drošības mehānismiem *WLAN* tīklos. Nodaļā izstrādātas vairākas automobiļu sakaru tīklu testgultnes, un lauka apstākļos veikti vairāki eksperimentāli mērījumi, izmantojot dažādus mērījumu scenārijus, piemēram, dažāds mobilo klientu skaits, vairāku ražotāju sakaru aparatūra, atšķirīgi kustības scenāriji. Mērījumu mērķis bija novērtēt hibrīdu, *IEEE 802.11n* un *LTE* tehnoloģijās bāzētu autotransporta sakaru tīklu veiktspēju, novērtējot tādos parametrus kā caurlaidspēja, pārslēgšanās laiks, datu pārraides laiks *AP* zonā, trafika sevlīdzības pakāpe un tīkla atbildes laiks. Izmantojot daudzterminālu sistēmas matemātisko modeli, veikts bezvadu tīkla veiktspējas novērtējums arī stacionāram gadījumam. Nodaļā izstrādāts divrangu *Wi-Fi* un *LTE* autotransporta sakaru tīkla tehniski ekonomiskais novērtējums.

Promocijas darba **3. nodaļā** izstrādātas likumsakarības starp integrēta *IEEE 802.11n* un *LTE* sakaru kanāla transporta līmeņa un aplikācijas līmeņa caurlaidspēju un automobiļa (mobilā klienta) pārvietošanās ātrumiem. Pētījuma ietvaros realizēta divrangu sakaru tīkla testgultne, kur eksperimentāli iegūtie mērījumu dati tika izmantoti minēto likumsakarību izveidē. Aproximējot eksperimentāli iegūtos mērījumu datus, tika izmantoti lineārie un nelineārie regresijas modeļi. Nodaļas ietvaros izstrādāts *LTE* tehnoloģijas signāla stipruma un signāla kvalitātes parametru uzraudzības risinājums, kā arī novērtētas mērījumu un aproksimācijas kļūdas.

Promocijas darba **4. nodaļā** novērtēti *IEEE 802.11k/r/v* standarti, ko var izmantot pārslēgšanās procedūras uzlabošanai *WLAN* tīklos. Detalizēti izpētīts *IEEE 802.11r* standarts, kas nodrošina ātro *BSS* pārejas procedūru, kas ir kritiski gadījumos, ja tiek izmantota *802.1X/EAP* bāzēta klientu autentifikācija. Padziļināti izpētīts arī *IEEE 802.11v* standarts. Pētījuma ietvaros realizēta *IEEE 802.11ac* standartā bāzēta autotransporta sakaru tīkla testgultne. Izstrādāts uzlabots pārslēgšanās procedūras algoritms, kas ir balstīts *IEEE 802.11v* standarta modifikācijā. Testgultnē eksperimentāli novērtēta bezvadu tīkla veikspēja, izmantojot “Standarta” pārslēgšanās procedūru, izstrādāto manuālo “*802.11v* tīkla virzītu” pārslēgšanās procedūru un izstrādāto automātisko “*802.11v* tīkla asistētu” pārslēgšanās procedūru. Eksperimentāli novērtēti tādi parametri kā aplikācijas līmeņa caurlaidspēja, atbildes laiks un pārslēgšanās procedūras aizture.

Promocijas darba **5. nodaļā** novērtēta likumsakarība starp uztvertā signāla jaudas līmeņa atkarību no attāluma līdz raidītājam. Aprēķinos izmantots logaritmiski normālais modelis, kurā tiek ņemtas vērā uztvertā signāla fluktuācijas, ko raksturo Nakagami sadalījums. Veiktajos aprēķinos izmantoti arī *IEEE 802.11ac* automobiļu sakaru tīkla testgultnē eksperimentāli iegūtie rezultāti. Izmantojot Šenona teorēmu un iepriekš veiktos aprēķinus, teorētiski novērtēta *WLAN* tīkla caurlaidspēja, mobilajam klientam attālinoties no raidītāja. Teorētiski aprēķinātie caurlaidspējas rezultāti salīdzināti ar eksperimentāli iegūtajiem. Eksperimentāli iegūtie rezultāti ir vairākas reizes mazāki par teorētiski iegūtajiem rezultātiem, jo teorētiskajos aprēķinos izmantotā Šenona teorēma paredz caurlaidspējas noteikšanu ideālam kanālam, tā ir fizikālā vide, līdz ar to aprēķinos netiek ņemta vērā augstāku *OSI* modeļa slāņu ietekme.

Veiktie divrangu *IEEE 802.11n* un *LTE* sakaru kanālu veikspējas pētījumi un sasniegtie rezultāti, kā arī izstrādātais pārslēgšanās procedūras risinājums *IEEE 802.11ac* bāzētam automobiļu sakaru tīklam, izmantojot speciāli modificētu *IEEE 802.11v* funkcionalitāti, ir liels ieguldījums Latvijas intelektuālo transporta sistēmu (*ITS*) un ar to saistīto datu pārraides pakalpojumu attīstībai.

Perspektīvā, ieviešot jaunus *WLAN* standartus, piemēram, *IEEE 802.11ax* savienojumā ar izstrādāto uzlabotas pārslēgšanās procedūras risinājumu, var tikt pārskatītas iespējas nodrošināt arī pārējās ar ceļu satiksmes drošību saistītās *ITS* funkcijas, kas tiek iekļautas *ITS* pakalpojumu kategorijā “Ceļu satiksmes drošība un brīdināšana”, jo *IEEE 802.11ax* risina tādas problēmas kā klientu blīvums, tīkla pārklājums, tīkla aiztures un citu *QoS* parametru nodrošināšana.

Veiktie eksperimenti parādīja, ka caurlaidspējas ziņā “šaurā vieta” šādā eksperimentālā transportlīdzekļu sakaru tīklā ir *LTE* kanāls. Praksē *LTE* tīkla daļu var aizvietot ar jebkuru

aktuālo mobilo tīklu tehnoloģiju, piemēram, 5G vai arī optisko šķiedru kabeļu tīklu, lai palielinātu kopējo transporta sakaru tīkla caurlaidspēju.

Promocijas darbā apkopoti pabeigtu pētījumu rezultāti un definēti iespējamie **turpmākie pētījumu virzieni**.

1. Mobilitātes paplašināšanas risinājumu izstrāde *WLAN* bāzētu autotransporta sakaru tīklu klientiem, izstrādāto risinājumu veikspējas novērtēšana. Savienojamības risinājums paredzētu adaptīvu *WLAN* un 4G *LTE*/5G sakaru kanālu izmantošanu problemātiskajās pārklājuma zonās. Piedāvātais risinājums *ITS* tīklos ļautu nodrošināt stabilus platjoslas datu pārraides pakalpojumus un būtu vērsts uz multimediju datu pārraidi.
2. *IEEE 802.11k* standarta padziļināta izpēte un risinājuma izstrāde, lai nodrošinātu automātiski aizpildāmu datubāzi ar bezvadu piekļuves punktu (*AP*) kandidātu sarakstu, kas iekļautu arī *AP GPS* datus. Pārslēgšanās procedūras algoritms varētu tikt papildināts ar jaunām *AP* izvēles metrikām, piemēram, klienta pozicionēšanas dati, kustības virziens un ātrums. Izstrādāto risinājumu veikspējas un efektivitātes novērtēšana.

Promocijas darba izstrādes laikā tika iegūti vairāki galvenie secinājumi.

Integrēta *WLAN* un *LTE* autotransporta sakaru tīkla izveide ir tehniski un ekonomiski pamatota gadījumā, ja tiek izmantota *WLAN* bāzēta, *LTE* koncentrēta mobilā tīkla atslogošana. Tas ir praktiski lietojams automobiļu sakaru tīkls, lai nodrošinātu liela apjoma datu pārsūtīšanu un organizētu automobiļu pasažieru piekļuvi interneta tīklam.

Divrangu *WLAN* un *LTE* sakaru tīkla veikspēja ir atkarīga no tīkla mezglu tehniskajiem veikspējas parametriem. Izmantojot dažādus *LTE* maršrutētājus, autotransporta bezvadu sakaru tīkla AL caurlaidspēja var atšķirties par 10–20 %. Mobilo klientu pārvietošanās ātruma, klientu skaita un klientu pārvietošanās scenāriju izmaiņas ietekmē gan individuālo mobilo klientu AL caurlaidspēju, gan arī kopējo bezvadu tīkla veikspēju.

Neatkarīgi no tā, kāda ražotāja *LTE* maršrutētājs tiek izmantots divrangu *IEEE 802.11n* un *LTE* tīklā, tas neietekmē datu trafika raksturu. To parāda eksperimentālo mērījumu rezultātu analīze, kur datu trafika plūsmām tika novērtēti tādi parametri kā caurlaidspēja, korelācijas koeficients, dispersija un trafika sevlīdzīguma pakāpe.

Pārslēgšanās procedūra starp bezvadu piekļuves punktiem ir atkarīga no klienta ierīcē realizētā pārslēgšanās procedūras algoritma, *WLAN* tīkla arhitektūras risinājuma, kā arī realizētajiem bezvadu tīkla drošības mehānismiem.

Integrēta *IEEE 802.11n* un *LTE* sakaru kanāla caurlaidspēja mainās atkarībā no automobiļa (mobilā klienta) kustības ātruma (0–70 km/h) pēc otrās kārtas polinomiālās funkcijas likuma.

Integrētā *IEEE 802.11n* un *LTE* sakaru tīklā virstēriņi starp *L7* un *L4* vidēji veido līdz 36 %, ja mobilā klienta pārvietošanās ātrums ir no 0 km/h līdz 70 km/h. Tas nozīmē, ka par tīkla caurlaidspēju nevar spriest, tikai balstoties uz mērījumiem, kas ir veikti transporta (*L4*) vai zemākos slāņos.

IEEE 802.11ac tīklā ar ātri kustīgiem objektiem (>20 km/h), savlaicīgi pieņemot pārslēgšanās procedūras lēmumu un izpildot pārslēgšanās procedūru, izmantojot *IEEE 802.11v*

standarta “BSS pārejas vadības vaicājuma” un “BSS pārejas vadības pieprasījuma” ziņojumus ar izstrādāto modifikāciju, var paaugstināt bezvadu tīkla kopējo veikspēju – vidējo aplikācijas līmeņa caurlaidspēju var palielināt līdz 75 %, un vidējo tīkla atbildes laiku var samazināt līdz pat 67 %, kā arī iespējams nodrošināt mazākas vidējās pārslēgšanās procedūras aiztures, salīdzinot ar “Standarta” pārslēgšanās procedūru, kur netiek izmantots *IEEE 802.11v* standarts.

Teorētiski veiktie aprēķini, tāpat kā eksperimentālie novērojumi un eksperimentāli veiktie mērījumi, rāda, ka *IEEE 802.11ac* tīklā, mobilajam klientam attālinoties no raidītāja, uztvertā signāla jauda pavājinās, un tā rezultātā samazinās arī caurlaidspēja. Uztvertā signāla jauda ir laikā mainīga un fluktuējoša, uztvertā signāla jaudas svārstības izraisa konstruktīva un destruktīva interference starp vairākceļu signāla izplatīšanās komponentēm, kas savukārt izraisa arī caurlaidspējas fluktuācijas.

Definētais promocijas darba mērķis – izpētīt un novērtēt integrētu, *IEEE 802.11n/ac* un *LTE* standartos bāzētu autotransporta sakaru tīklu veikspēju un veikt *IEEE 802.11ac* bezvadu piekļuves tīkla veikspējas paaugstināšanu – ir sasniegts.

Nobeigumā jāuzsver, ka iegūtos divrangu *WLAN* un *LTE* autotransporta sakaru tīklu veikspējas pētījumu rezultātus, kā arī *WLAN* pārslēgšanās procedūras uzlabošanas risinājuma rezultātus var izmantot gan jau ekspluatācijā esošu *WLAN* piekļuves pārraides sistēmu uzlabošanai, gan arī jaunu, *WLAN* un 4G *LTE* / 5G tehnoloģijās bāzētu ITS izstrādei un ieviešanai.

IZMANTOTĀS LITERATŪRAS SARAKSTS

- [1] Abdelgader A. M. S., Lenan W. The Physical Layer of the IEEE 802.11p WAVE Communication Standard: The Specifications and Challenges // WCECS, San Francisco. – 2014. – Vol. 2. – pp. 691–698.
- [2] Alcantara C., Darchis N., Henry J., Jimenez J., Ziliotto F. CCIE Wireless v3 Study Guide. – Cisco Press, 2019. – p. 520.
- [3] Alexander B. 802.11 Wireless Network Site Surveying and Installation. – Cisco Press, 2004. – p. 456.
- [4] **Ancans A.**, Bogdanovs N., Petersons E., Ancans G., Umanskis A., Vishnevskiy V. Evaluation of Wi-Fi and LTE Integrated Channel Performance with Different Hardware Implementation for Moving Objects // *Procedia Computer Science*. – 2017. – Vol. 104. – pp. 493–500.
- [5] **Ancans A.**, Bogdanovs N., Petersons E., Ipatovs A. Integrated Wireless Network Performance Estimation for Moving Vehicles // *Conference on Advances in Wireless and Optical Communications (RTUWO)*, Riga. – 2017. – pp. 203–207.
- [6] **Ancans A.**, Petersons E. The Relationship between Transport Wireless Network Throughput and Vehicle Speed // *Automatic Control and Computer Sciences (AC&CS)*. – 2018. – Vol. 52, Iss. 4. – pp. 297–305.
- [7] **Ancans A.**, Petersons E., Ancans G., Stetjuha M., Ipatovs A., Stankevicius E. Technical and Economic Analysis of Transport Telecommunication Infrastructure // *Procedia Computer Science*. – 2019. – No. 149. – pp. 206–214.
- [8] **Ancans A.**, Petersons E., Ipatovs A. Vehicular Wireless Network Access Controller Parameter Estimation // *Progress in Electromagnetics Research Symposium (PIERS)*, Singapore. – 2017. – pp. 2152–2159.
- [9] **Ancans A.**, Petersons E., Jerjomins R., Grabs E., Ancans G., Ipatovs A. Evaluation of received signal power level and throughput depending on distance to transmitter in testbed for automotive WLAN IEEE 802.11ac communication network // *Latvian Journal of Physics and Technical Sciences (apstiprināta publicēšanai)*.
- [10] **Ancans A.**, Petersons E., Umanskis A. Hybrid Vehicular IEEE 802.11n and LTE Wireless Network Performance Evaluation in Non-Stationary Mode of Motion // *Proceedings of Advances in Wireless and Optical Communications (RTUWO)*. – 2018. – pp. 213–213.
- [11] Ancans G., Bobrovs V., **Ancans A.**, Kalibatiene D. Spectrum Considerations for 5G Mobile Communication Systems // *Procedia Computer Science*. – 2017. – Vol. 104. – pp. 509–516.
- [12] Ancans G., Stafecka A., Bobrovs V., **Ancans A.**, Caiko J. Analysis of Characteristics and Requirements for 5G Mobile Communication Systems // *Latvian Journal of Physics and Technical Sciences*. – 2017. – Vol. 54, Iss. 4. – pp. 69–78.
- [13] Anwar W., Trasl A., Franchi N., Fettweis G. On the Reliability of NR-V2X and IEEE 802.11bd // 2019 IEEE 30th Annual International Symposium on Personal, Indoor and

- Mobile Radio Communications (PIMRC), Istanbul. – 2019. – Vol. 2019-September. – pp. 1–7.
- [14] Arhipova I., Bāliņa S. Statistika ekonomikā un biznesā. Risinājumi ar SPSS un Microsoft Excel. – Datorzinību Centrs, 2006. – 352 lpp.
 - [15] Balakrishnan H., Padmanabhan V.N., Seshan S., Katz R.H. A comparison of mechanisms for improving TCP performance over wireless links // IEEE/ACM Transactions on Networking. – 1997. – Vol. 5, Iss. 6. – pp. 756–769.
 - [16] Balasubramanian A., Mahajan R., Venkataramani A. Augmenting Mobile 3G Using WiFi // MobiSys'10 - Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services. – 2010. – pp. 209–222.
 - [17] Balodis G. Diskrētā signālu apstrāde. – RTU Izdevniecība. Radioiekārtu katedra, Elektronikas un telekomunikāciju fakultāte, Rīgas Tehniskā universitāte, 2011. – 130 lpp.
 - [18] Balodis G. Mobilie sakari. – RTU Izdevniecība. Radioiekārtu katedra, Elektronikas un telekomunikāciju fakultāte, Rīgas Tehniskā universitāte, 2003. – 111 lpp.
 - [19] Barton R., Grossetete P., Hanes D., Henry J., Salgueiro G. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. – Cisco Press, 2017. – p. 576.
 - [20] Beard C., Stallings W. Wireless Communication Networks and Systems. – Pearson Higher Education, Inc., 2016. – p. 640.
 - [21] Beķeris E. Signālu teorijas pamati. – RTU Izdevniecība. Elektronikas pamatu katedra, Elektronikas un telekomunikāciju fakultāte, Rīgas Tehniskā universitāte, 2010. – 229 lpp.
 - [22] Bencel R., Kostal K., Kotuliak I., Ries M. Common SDN control channel for seamless handover in 802.11 // 2018 Wireless Days (WD). – 2018. – pp. 34–36.
 - [23] Bilgin B. E., Gungor V.C. Performance Comparison of IEEE 802.11p and IEEE 802.11b for Vehicle-to-Vehicle Communications in Highway, Rural, and Urban Areas // International Journal of Vehicular Technology. – 2013. – Vol. 2013. – pp. 1–10.
 - [24] Bogdanovs N., **Ancans A.**, Martinsons K., Petersons E. Estimating the Speed of an Integrated Wireless Network for Transportation Applications // Automatic Control and Computer Sciences (AC&CS). – 2014. – Vol. 48, Iss. 5. – pp. 274–281.
 - [25] Bolch G., Greiner S., De Meer H., Trivedi K. S. Queueing Networks and Markov Chains: Modeling and Performance Evaluation With Computer Science Applications. Second Edition. – John Wiley & Sons, Inc., 2006. – p. 896.
 - [26] Bouras C. J. Trends in Telecommunications Technologies. – In-Teh, 2010. – p. 768.
 - [27] Brodsky M. Z., Morris R.T. In defense of wireless carrier sense // Conference on Data Communication, ACM SIGCOMM 2009, Barcelona. – 2009. – Vol. 39, Iss. 4. – pp. 147–158.
 - [28] CEPT Report 71. Report from CEPT to the European Commission in response to the Mandate to study the extension of the Intelligent Transport Systems (ITS) safety-related band at 5.9 GHz // Electronic Communications Committee (ECC) within the European Conference of Postal and Telecommunications Administrations (CEPT). 2019. – p. 42.

- [29] Chen S., Hu J., Shi Y., Zhao L., Li W. A Vision of C-V2X: Technologies, Field Testing and Challenges with Chinese Development // IEEE Internet of Things Journal. – 2020. – Vol. 7, Iss. 5. – pp. 3872–3881.
- [30] Cheng N., Lu N., Zhang N., Shen X. S., Mark J. W. Vehicular WiFi offloading: Challenges and solutions // Vehicular Communications. – 2014. – Vol. 1, Iss. 1. – pp. 13–21.
- [31] Cheng X., Zhang R., Yang L. 5G-Enabled Vehicular Communications and Networking. – Springer, 2019. – p. 177.
- [32] Chien S. F., Liu H., Low A. L. Y., Maciocco C., Ho Y.L. Smart Predictive Trigger for Effective Handover in Wireless Networks // IEEE International Conference on Communications, Beijing. – 2008. – pp. 2175–2181.
- [33] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022. White paper. – Cisco, 2019. – p. 33.
- [34] Coleman D. D., Westcott D. A. CWNA Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106. – Sybex, John Wiley & Sons, 2014. – p. 912.
- [35] Coleman D. D., Westcott D. A., Harkins B.E. CWSP Certified Wireless Security Professional Study Guide: Exam CWSP-205. 2nd Edition. – Sybex, John Wiley & Sons, 2017. – p. 701.
- [36] Dahlman E., Parkvall S., Skold J. 4G: LTE/LTE-Advanced for Mobile Broadband. 2nd Edition. – Academic Press, 2014. – p. 544.
- [37] Dahlman E., Parkvall S., Skold J. 5G NR: The Next Generation Wireless Access Technology. – Academic Press, 2018. – p. 466.
- [38] Deshpande P., Kashyap A., Sung C., Das S.R. Predictive Methods for Improved Vehicular WiFi Access // Proceedings of the 7th ACM International Conference on Mobile Systems, Applications, and Services. –2009. – pp. 263–276.
- [39] Dutta A., Schulzrinne H. Mobility Protocols and Handover Optimization: Design, Evaluation and Application. – John Wiley & Sons Ltd., 2014. – p. 442.
- [40] Edgeworth B., Rios R. G., Hucaby D., Gooley J. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide. – Cisco Press, 2020. – p. 1073.
- [41] Emmelmann M., Bochow B., Kellum C. C., eds. Vehicular Networking: Automotive Applications and Beyond. – John Wiley & Sons Ltd, 2010. – p. 296.
- [42] Fattah H. 5G LTE Narrowband Internet of Things (NB-IoT). – CRC Press, Taylor & Francis Group, 2019. – p. 263.
- [43] Fei H., eds. Opportunities in 5G Networks: A Research and Development Perspective. – CRC Press, Taylor & Francis Group, 2016. – p. 577.
- [44] Fei H., eds. Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communications: A Technical Approach. – CRC Press, Taylor & Francis Group, 2018. – p. 346.
- [45] Frisoni R., Dall'Oglio A., Nelson C., Long J., Vollath C., Ranghetti D., McMinimy S. Research for TRAN Committee – Self-piloted cars: The future of road transport? – European Parliament's Committee on Transport and Tourism, 2016. – p. 106.
- [46] Gast M. S. 802.11 Wireless Networks: The Definitive Guide. 2nd Edition. – O'Reilly Media, 2005. – p. 656.

- [47] Gast M. S. 802.11ac: A Survival Guide. – O'Reilly Media, 2013. – p. 152.
- [48] Ge X., Yang Y. Characteristics of Frame Traffic in 802.11 Wireless Networks // The 4th International Conference on Mobile Ad-hoc and Sensor Networks, Wuhan. – 2008. – pp. 295–298.
- [49] Geier J. Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks For Enterprise-Based Applications. 2nd Edition. – Cisco Press, 2015. – p. 512.
- [50] Hadaller D., Keshav S., Brecht T., Agarwal S. Vehicular opportunistic communication under the microscope // MobiSys '07 Proceedings of the 5th international conference on Mobile systems, applications and services, San Juan, Puerto Rico. – 2007. – pp. 206–219.
- [51] Hagenauer F., Dressler F., Sommer C. A Simulator for Heterogeneous Vehicular Networks // Proceedings of 6th IEEE Vehicular Networking Conference (VNC 2014), Poster Session. – 2014. – pp. 185–186.
- [52] Hameed M. Z., Filali F., LTE and IEEE 802.11p for vehicular networking: a performance evaluation // Eurasip Journal on Wireless Communications and Networking. – 2014. – Vol. 2014, Iss. 1. – pp. 1–15.
- [53] Hartenstein H., Laberteaux K. P., eds. VANET: Vehicular Applications and Inter-Networking Technologies. – JohnWiley & Sons, 2010. – p. 466.
- [54] Hasan S. F., Siddique N., Chakraborty S. Intelligent Transport Systems: 802.11-based Vehicular Communications. Second Edition. – Springer International Publishing, 2018. – p. 183.
- [55] Haverkort B. R. Performance of Computer Communication Systems: A Model-Based Approach. – John Wiley & Sons, Ltd, 1999. – p. 488.
- [56] Haykin S. Digital Communication systems. – John Wiley & Sons, Inc. 2014. – p. 700.
- [57] Higginbottom G.N. Performance Evaluation of Communication Networks. – Artech House, 1998. – p. 366.
- [58] Ho J., Zhang J., Jo M. Selective offloading to WiFi devices for 5G mobile users // 13th International Wireless Communications and Mobile Computing Conference (IWCMC 2017). – 2017. – pp. 1047–1054.
- [59] Holt A., Huang C. H. 802.11 Wireless Networks: Security and Analysis. – Springer-Verlag London Limited, 2010. – p. 236.
- [60] Hu R. Q., Qian Y., eds. Heterogeneous Cellular Networks. – John Wiley & Sons, 2013. – p. 379.
- [61] Huang C. M., Chen Y.S., eds. Telematics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications. – Information Science Reference, IGI Global, 2010. – p. 438.
- [62] Hucaby D. CCNA Wireless 200-355 Official Cert Guide. – Pearson Education, Cisco Press, 2016. – p. 570.
- [63] Huston G. TCP Performance // The Internet Protocol Journal. – 2000. – Vol. 3, No. 2. – pp. 2–24.
- [64] IEEE Computer Society: IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and

- metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 1: Radio Resource Measurement of Wireless LANs, IEEE Std 802.11k-2008, 12 June 2008.
- [65] IEEE Computer Society: IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 2: Fast Basic Service Set (BSS) Transition, IEEE Std 802.11r-2008, 15 July 2008.
- [66] IEEE Computer Society: IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 8: IEEE 802.11 Wireless Network Management, IEEE Std 802.11v-2011, 9 February 2011.
- [67] IEEE Computer Society: IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2016, 7 December 2016. – p. 3534.
- [68] Jackman S. M., Swartz M., Burton M., Head T. W. CWDP Certified Wireless Design Professional Official Study Guide: Exam PW0-250. – Sybex, Wiley Publishing, 2011. – p. 871.
- [69] Jansons J. IEEE 802.11n Evaluation in Vehicular Communication Systems // 52nd International Scientific Conference of Riga Technical University, Riga. – 2011. – pp. 1–8.
- [70] Jerjomins R., **Ancans A.**, Petersons E., Gerina-Ancane A. Improving Handover Mechanism in Vehicular WiFi Networks // ICTE in Transportation and Logistics 2019, Lecture Notes in Intelligent Transportation and Infrastructure (ICTE ToL 2019, LNITI). – Springer Nature Switzerland AG, 2020. – pp. 243–261.
- [71] Karagiannis G., Altintas O., Ekici E., Heijenk G., Jarupan B., Lin K., Weil T., Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions // IEEE Communications Surveys & Tutorials. – 2011. – Vol. 13, Iss. 4. – pp. 584–616.
- [72] Kleinrock L. Queueing Systems, Volume I: Theory. – John Wiley & Sons, 1975. – p. 417.
- [73] Lauridsen M., Gimenez L.C., Rodriguez I., Sorensen T.B., Mogensen P. From LTE to 5G for Connected Mobility // IEEE Communications Magazine. – 2017. – Vol. 55, Iss. 3. – pp. 156–162.
- [74] Lee J., Yi Y., Chong S., Jin Y. Economics of WiFi Offloading: Trading Delay for Cellular Capacity // IEEE Transactions on Wireless Communications. – 2014. – Vol. 13, Iss. 3. – pp. 1540–1554.
- [75] Lee K., Lee J., Yi Y., Rhee I., Chong S. Mobile data offloading: how much can WiFi deliver? // IEEE/ACM Transactions on Networking. – 2013. – Vol. 21, Iss. 2. – pp. 536–550.

- [76] Lewis C., Pickavance S. Selecting MPLS VPN Services. – Cisco Press, 2006. – p. 456.
- [77] Li B.Z., Luan T.H., Hu B., Chen S.Z. Efficient MAC protocol for drive-thru Internet in a sparse highway environment // IET Communications. – 2017. – Vol. 11, Iss. 3. – pp. 428–436.
- [78] Ligo A. K., Peha J. M., Ferreira P., Barros J. Throughput and Economics of DSRC-Based Internet of Vehicles // IEEE Access. – 2017. – Vol. 6. – pp. 7276–7290.
- [79] Lim C. B., Kang S. H., Cho H. H., Park S. W., Park J. G. An Enhanced Indoor Localization Algorithm Based on IEEE 802.11 WLAN Using RSSI and Multiple Parameters // 5th International Conference on Systems and Networks Communications, Nice. – 2010. – pp. 238–242.
- [80] Lin W. Y., Li M. W., Lan K. C., Hsu C. H. A. Comparison of 802.11a and 802.11p for V-to-I Communication: A Measurement Study // LNICST. – 2012. – Vol. 74. – pp. 559–570.
- [81] Lopez-Perez D., Garcia-Rodriguez A., Galati-Giordano L., Kasslin M., Doppler K. IEEE 802.11be Extremely High Throughput: The Next Generation of Wi-Fi Technology Beyond 802.11ax // IEEE Communications Magazine. – 2019. – Vol. 57, Iss. 9. – pp. 113–119.
- [82] Marsch P., Bulakci O., Queseth O., Boldi M., eds. 5G System Design. Architectural and Functional Considerations and Long Term Research. – John Wiley & Sons, 2018. – p. 608.
- [83] Mazuelas S., ABahillo A., Lorenzo R. M., Fernandez P., Lago F. A., Garcia E., Blas J., Abril E.J. Robust Indoor Positioning Provided by Real-Time RSSI Values in Unmodified WLAN Networks // IEEE Journal on Selected Topics in Signal Processing. – 2009. – Vol. 3, Iss. 5. – pp. 821–831.
- [84] Meschke R., Krohn M., Daher R., Gladisch A., Tavangarian D. Novel handoff concepts for roadside networks using mechanisms of IEEE 802.11k & IEEE 802.11v // ICUMT. – 2010. – pp. 1232–1238.
- [85] Mills K. L., Filliben J. J., Cho D. Y., Schwartz E., Genin D. Study of Proposed Internet Congestion Control Mechanisms. – National Institute of Standards and Technology (NIST), U. S. Department of Commerce, 2010. – p. 570.
- [86] Mood A. M., Graybill F. A., Boes D. C. Introduction to the theory of statistics, 3rd ed. – McGraw-Hill, 1974. – p. 564.
- [87] Mourad A., Heigl F., Hoeher P. A. Performance Evaluation of Concurrent IEEE 802.11 Systems in the Automotive Domain // 41st IEEE Conference on Local Computer Networks, Dubai. – 2016. – pp. 655–661.
- [88] Mouton M., Castignani G., Frank R., Engel T. Enabling vehicular mobility in city-wide IEEE 802.11 networks through predictive handovers // Vehicular Communications. – 2015. – Vol. 2, Iss. 2. – pp. 59–69.
- [89] Mukherjee A., Cheng J. F., Falahati S., Koorapaty H., Kang D. H., Karaki R., Falconetti L., Larsson D. Licensed-Assisted Access LTE: Coexistence with IEEE 802.11 and the Evolution toward 5G // IEEE Communications Magazine. – 2016. – Vol. 54, Iss. 6. – pp. 50–57.

- [90] Naik G., Choudhury B., Park J. M. IEEE 802.11bd & 5G NR V2X: Evolution of Radio Access Technologies for V2X Communications // IEEE Access. – 2019. – Vol. 7. – pp. 70169–70184.
- [91] Ng C. H., Soong B. H. Queueing Modelling Fundamentals: With Applications in Communication Networks. Second Edition. – John Wiley & Sons, Ltd, 2008. – p. 271.
- [92] Noteikumi par radiofrekvenču spektra joslu sadalījumu radiosakaru veidiem un iedalījumu radiosakaru sistēmām, kā arī par radiofrekvenču spektra joslu izmantošanas vispārīgajiem nosacījumiem (Nacionālais radiofrekvenču plāns). Latvijas Republikas Ministru kabineta noteikumi Nr. 1151. Pieņemti Latvijas Republikas Ministru kabinetā 06.10.2009.; stājās spēkā 10.10.2009. Latvijas Vēstnesis, 09.10.2009., Nr.161.
- [93] Papadimitratos P., La Fortelle A. D., Evenssen K., Brignolo R., Cosenza S. Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation // IEEE Communications Magazine. – 2009. – Vol. 47, Iss. 11. – pp. 84–95.
- [94] Papathanassiou A., Khoryaev A. Cellular V2X as the Essential Enabler of Superior Global Connected Transportation Services // IEEE 5G Tech Focus. – 2017. – Vol. 1, No. 2. – pp. 1–4.
- [95] Par konceptuālo ziņojumu “Par intelektisko transporta sistēmu ieviešanu Latvijas autotransporta jomā un to saskarnēm ar citiem transporta veidiem”. Latvijas Republikas Ministru kabineta rīkojums Nr. 396. Pieņemts Latvijas Republikas Ministru kabinetā 17.07.2020.; stājās spēkā 17.07.2020. Latvijas Vēstnesis, 21.07.2020., Nr. 138.
- [96] Paul A., Chilamkurti N., Daniel A., Rho S. Intelligent Vehicular Networks and Communications: Fundamentals, Architectures and Solutions. – Elsevier, 2017. – p. 229.
- [97] Perez A. Wi-Fi Integration to the 4G Mobile Network. – ISTE, John Wiley & Sons, 2018. – p. 288.
- [98] Pētersons E. Bezvadu lokālo tīklu pamati. – RTU Izdevniecība. Transporta elektronikas un telemātikas katedra, Elektronikas un telekomunikāciju fakultāte, Rīgas Tehniskā universitāte, 2005. – 41 lpp.
- [99] Pētersons E. Sevlīdzīgs trafiks telekomunikāciju un datoru tīklos. – RTU Izdevniecība. Transporta elektronikas un telemātikas katedra, Elektronikas un telekomunikāciju fakultāte, Rīgas Tehniskā universitāte, 2005. – 61 lpp.
- [100] Pujol F., Manero C., Ropert S., Enjalbal A., Lavender T., Jervis V., Rudd R., Marcus J. S. Study on using millimetre waves bands for the deployment of the 5G ecosystem in the Union. – European Commission, IDATE DigiWorld, 2019. – p. 134.
- [101] Raab S., Chandra M. Mobile IP Technology and Applications. – Cisco Press, 2013. – p. 290.
- [102] Rebecchi F., Dias de Amorim M., Conan V. et al. Data Offloading Techniques in Cellular Networks: A Survey // IEEE Communication Surveys & Tutorials. – 2015. – Vol. 17, No. 2. – pp. 580–603.
- [103] Recommendation ITU-R M.2084-1. Radio interface standards of vehicle-to-vehicle and vehicle-to-infrastructure two-way communications for Intelligent Transport System applications // International Telecommunication Union (ITU). – 2019. – p. 26.

- [104] Rodriguez-Dagnino R. M. Some Remarks Regarding Asymptotic Packet Loss in the Pareto/M/1/K Queueing System // IEEE Communications Letters. – 2005. – Vol. 9, No. 10. – pp. 927–929.
- [105] Roessler A., Schlien J., Merkel S., Kottkamp M. LTE-Advanced (3GPP Rel.12) Technology Introduction. White Paper. – Rohde & Schwarz, 2014. – p. 60.
- [106] Roshan P., Leary J. 802.11 Wireless LAN Fundamentals. – Cisco Press, 2004. – p. 312.
- [107] Sadiq A. S., Abu Bakar K., Ghafoor K. Z., Gonzalez A. J. Mobility and Signal Strength – Aware Handover Decision in Mobile IPv6 based Wireless LAN // International Multiconference of Engineers and Computer Scientists. – 2011. – Vol. 1. – pp. 664–669.
- [108] Sanchez M. I., Boukerche A. On IEEE 802.11k/r/v amendments: Do they have a real impact? // IEEE Wireless Communications. – 2016. – Vol. 23, Iss. 1. – pp. 48–55.
- [109] Saunders S. R., Aragon-Zavala A. Antennas and Propagation for Wireless Communication Systems. – John Wiley & Sons Ltd, 2007. – p. 516.
- [110] Sauter M. From GSM to LTE-Advanced Pro and 5G. An Introduction to Mobile Networks and Mobile Broadband. Third Edition. – John Wiley & Sons Ltd., 2017. – p. 523.
- [111] Sharp I., Yu K., eds. Wireless Positioning: Principles and Practice. – Springer Nature Singapore, 2019. – p. 626.
- [112] Siegel J., Erb D., Sarma S. Algorithms and Architectures: A Case Study in When, Where and How to Connect Vehicles // IEEE Intelligent Transportation Systems Magazine. – 2018. – Vol. 10, Iss. 1. – pp. 74–87.
- [113] Singh P. K., Chattopadhyay S., Bhale P., Nandi S. Fast and Secure Handoffs for V2I Communication in Smart City Wi-Fi Deployment // International Conference on Distributed Computing and Internet Technology. – 2018. – Vol. 10722. – pp. 189–204.
- [114] Smith J., Woodhams J., Marg R. Controller-Based Wireless LAN Fundamentals: An end-to-end reference guide to design, deploy, manage, and secure 802.11 wireless networks. – Cisco Press, 2010. – p. 315.
- [115] Smotrovs J. Varbūtību teorija un matemātiskā statistika. 2. daļa. – Zvaigzne ABC, 2007. – 136 lpp.
- [116] Stallings W. Data and Computer Communications. Tenth Edition. – Pearson Education, 2014. – p. 912.
- [117] Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. – Addison-Wesley Professional, 2016. – p. 560.
- [118] Steger M., Karner M., Hillebrand J., Rom W., Boano C., Romer K. Generic framework enabling secure and efficient automotive wireless SW updates // 21st IEEE International Conference on Emerging Technologies and Factory Automation, Berlin. – 2016. – pp. 1–8.
- [119] Sveccko J., Malajner M., Gleich D. Distance estimation using RSSI and particle filter // ISA Transactions. – 2015. – Vol. 55. – pp. 275–285.
- [120] Sziget T., Barton R., Hattingh C., Briley K. End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks. 2nd Edition. – Cisco Press, 2014. – p. 1040.

- [121] Tan W. L., Lau W. C., Yue O. C., Tan H. H. Analytical Models and Performance Evaluation of Drive-thru Internet Systems // IEEE Journal on Selected Areas in Communications. – 2011. – Vol. 29, Iss. 1. – pp. 207–222.
- [122] Tanenbaum A. S., Wetherall D. J. Computer Networks. Fifth Edition. – Pearson Education Limited, 2014. – p. 803.
- [123] Varma S. Internet Congestion Control. – Elsevier, 2015. – p. 286.
- [124] Vegni A. M., Loscri V., V. Vasilakos A. V., eds. Vehicular Social Networks. – CRC Press, 2017. – p. 208.
- [125] Wang X., Mao S., Gong M. X. An Overview of 3GPP Cellular Vehicle-to-Everything Standards // GetMobile: Mobile Computing and Communications. ACM Digital Library. – 2017. – Vol. 21, Iss. 3. – pp. 19–25.
- [126] Warren D., Dewar C. Understanding 5G: Perspectives on future technological advancements in mobile. – GSMA Intelligence, 2014. – p. 26.
- [127] Welzl M. Network Congestion Control: Managing Internet Traffic. – John Wiley & Sons, 2005. – p. 282.
- [128] Westcott D. A., Coleman D. D., Miller B., Mackenzie P. CWAP Certified Wireless Analysis Professional Official Study Guide: Exam PW0-270. – Sybex, Wiley Publishing, 2011. – p. 702.
- [129] Wewetzer C., Caliskan M., Meier K., Luebke A. Experimental Evaluation of UMTS and Wireless LAN for Inter-Vehicle Communication // Volkswagen Group, ITST 2007 - 7th International Conference on Intelligent Transport Systems Telecommunications. – 2007. – pp. 287–292.
- [130] Wisitpongphan N., Peha J. M. Effect of TCP on self-similarity of network traffic // Proceedings. 12th International Conference on Computer Communications and Networks. – 2003. – pp. 370–373.
- [131] Xu S., Li Y., Gao Y., Liu Y., Gacanin H. Opportunistic Coexistence of LTE and WiFi for Future 5G System: Experimental Performance Evaluation and Analysis // IEEE Access. – 2017. – Vol. 6. – pp. 8725–8741.
- [132] Xu W., Zhou H., Shi W., Lyu F., Shen X. Throughput Analysis of In-Vehicle Internet Access via On-Road WiFi Access Points // 86th IEEE Vehicular Technology Conference (VTC-Fall). – 2017. – Vol. 9. – pp. 1–5.
- [133] Yamamoto B., Wong A., Agcanas P. J., Jones K., Gaspar D., Andrade R., Trimble A. Z. Received Signal Strength Indication (RSSI) of 2.4 GHz and 5 GHz Wireless Local Area Network Systems Projected over Land and Sea for Near-Shore Maritime Robot Operations // Journal of Marine Science and Engineering (JMSE). – 2019. – Vol. 7, Iss. 9. – pp. 290–306.
- [134] Zaidi A., Athley F., Medbo J., Gustavsson U., Durisi G., Chen X. 5G Physical Layer: Principles, Models and Technology Components. – Academic Press. Elsevier, 2018. – p. 322.
- [135] Zhang K., Ge X., Liu C., Xiang L. Analysis of Frame Traffic Characteristics in IEEE 802.11 Networks // Fourth International Conference on Communications and Networking in China, Xian. – 2009. – pp. 1–5.

- [136] Вентцель Е. С., Теория вероятностей. Изд. 4-е. – Наука, 1969. – 576 с.
- [137] Кучерявый Е. А. Управление трафиком и качество обслуживания в сети Интернет. – Наука и Техника, 2004 – 336 с.
- [138] 5G Automotive Vision. European Commission, 2015. / Internets. – <https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf>, skatīts 17.04.2020.
- [139] 802.11n/HT and 802.11ac/VHT, MCS, SNR and RSSI. / Internets. – <https://wlanprofessionals.com/laminated-card-802-11n-ht-and-802-11ac-vht-mcs-snr-and-rssi/>, skatīts 31.05.2020.
- [140] Alonso Raposo M., Grosso M., Despres J., Fernandez Macias E., Galassi C., Krasenbrink A., Krause J., Levati L., Mourtzouchou A., Saveyn B., Thiel C., Ciuffo B. An analysis of possible socio-economic effects of a Cooperative, Connected and Automated Mobility (CCAM) in Europe. European Commission, 2018. / Internets. – <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111477/kjna29226enn.pdf>, skatīts 12.04.2020.
- [141] Analysis of LTE – WiFi Aggregation Solutions. Netmanias Report, 2016. / Internets. – <https://www.netmanias.com/en/post/reports/8532/laa-lte-lte-u-lwa-mptcp-wi-fi/analysis-of-lte-wifi-aggregation-solutions>, skatīts 13.04.2020.
- [142] Barnett T., Jain S., Andra U., Khurana T. Cisco Visual Networking Index (VNI) Global and Americas/EMEAR Mobile Data Traffic Forecast, 2017–2022. Cisco, 2019. / Internets. – https://www.cisco.com/c/dam/m/en_us/network-intelligence/service-provider/digital-transformation/knowledge-network-webinars/pdfs/190320-mobility-ckn.pdf, skatīts 28.04.2020.
- [143] Blanchard S. Understanding IEEE 802.11 and Wi-Fi Standards / Internets. – <https://www.microwavejournal.com/articles/34582-understanding-ieee-80211-and-wi-fi-standards>, skatīts 25.10.2020.
- [144] Cellular-V2X Technology Overview. Qualcomm Technologies, 2019. / Internets. – <https://www.qualcomm.com/media/documents/files/c-v2x-technology-overview.pdf>, skatīts 23.04.2020.
- [145] Cisco 809 Industrial Integrated Services Routers Data Sheet. / Internets. – <https://www.cisco.com/c/en/us/products/collateral/routers/809-industrial-router/datasheet-c78-734980.html>, skatīts 17.10.2020.
- [146] Cisco 819 4G LTE M2M Gateway Integrated Service Routers Data Sheet. / Internets. – https://www.cisco.com/c/en/us/products/collateral/routers/819-integrated-services-router-isr/data_sheet_c78-678459.html, skatīts 17.10.2020.
- [147] Coexistence of C-V2X and ITS-G5 at 5.9GHz. 5GAA, 2018. / Internets. – <https://5gaa.org/wp-content/uploads/2018/10/Position-Paper-ITG5.pdf>, skatīts 18.04.2020.
- [148] Croak P., Kim Y. Site Survey Guidelines for WLAN Deployment. Cisco, 2020. / Internets. – <https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html>, skatīts 18.02.2020.

- [149] Dondurmacioglu O. Handover mechanics for Wi-Fi phones, Rev. 1, 2012. / Internets. – <https://community.arubanetworks.com/t5/Community-Tribal-Knowledge-Base/Handover-mechanics-for-Wi-Fi-phones/ta-p/25696>, skatīts 18.02.2020.
- [150] Ekahau Site Survey. / Internets. – <https://www.ekahau.com/products/ekahau-connect/pro/>, skatīts 06.09.2020.
- [151] Elektroenerģijas tarifu salīdzinājums mājsaimniecībām. / Internets. – <https://www.elektroenerģija.lv>, skatīts 27.05.2020.
- [152] Enhanced Roaming Algorithm. – 2019. / Internets. – <https://support.samsungknox.com/hc/en-us/articles/115013403768-Enhanced-Roaming-Algorithm>, skatīts 01.03.2020.
- [153] Enterprise Mobility 8.1 Design Guide, 802.11r, 802.11k, 802.11v, 802.11w Fast Transition Roaming. Cisco, 2018. / Internets. – https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide/Chapter-11.pdf, skatīts 18.02.2020.
- [154] HPE MSM Controller Series. Overview. / Internets. – <https://h20195.www2.hpe.com/v2/getdocument.aspx?docname=c04111705>, skatīts 03.11.2020.
- [155] HPE MSM-802.11n Dual Radio Access Point Series. Overview. / Internets. – <https://h20195.www2.hpe.com/v2/getdocument.aspx?docname=c04111126#>, skatīts 03.11.2020.
- [156] HUAWEI E5186s-22a LTE CPE. Product Description. / Internets. – <https://usermanual.wiki/Pdf/HuaweiE5186Datasheet.94928258/view>, skatīts 17.10.2020.
- [157] Instant performance assessment of complex networks from pre- to post-deployment. Keysight Technologies. / Internets. – <https://www.keysight.com/zz/en/products/network-test/performance-monitoring/ixchariot.html>, skatīts 11.09.2020.
- [158] Interworking Wi-Fi and Mobile Networks. Ruckus Wireless, Inc., 2013. / Internets. – <http://c541678.r78.cf2.rackcdn.com/wp/wp-interworking-wi-fi-and-mobile-networks.pdf>, skatīts 18.02.2020.
- [159] iPerf - The ultimate speed test tool for TCP, UDP and SCTP. / Internets. – <https://iperf.fr/>, skatīts 27.05.2020.
- [160] Iperf for Bandwidth Testing / Internets. – <https://www.sd-wan-experts.com/blog/iperf-bandwidth-testing/>, skatīts 14.09.2020.
- [161] LTE / LTE-Advanced Fundamentals. Rohde & Schwarz. / Internets. – https://www.rohde-schwarz.com/lv/technologies/cellular/lte/lte-technology/lte_information_52292.html?change_c=true, skatīts 05.10.2020.
- [162] Lum E. Project AirGig: What is it really and why do you care? RCR Wireless, 2017. / Internets. – <https://www.rcrwireless.com/20170419/analyst-angle/20170419wireless-project-airgig-what-is-it-really-and-why-do-you-care>, skatīts 22.10.2020.
- [163] Modem Signal Strength and Signal Quality / Internets. – <https://customer.cradlepoint.com/s/article/Modem-Signal-Strength-and-Signal-Quality#quality>, skatīts 05.10.2020.
- [164] Molinaro A., Campolo C. 5G for V2X Communications. / Internets. – <https://www.5gitaly.eu/2018/wp-content/uploads/2019/01/5G-Italy-White-eBook-5G-for-V2X-Communications.pdf>, skatīts 10.11.2020.

- [165] Nayanajith R. CWSP – 4 Way Handshake. / Internets. – <https://mrncciew.com/2014/08/19/cwsp-4-way-handshake/>, skatīts 09.10.2020.
- [166] Nayanajith R. WLC Client Debug – Part 1. / Internets. – <https://mrncciew.com/2014/10/15/wlc-client-debug-part-1/>, skatīts 09.10.2020.
- [167] Nayanajith R. WLC Client Debug – Part 2. / Internets. – <https://mrncciew.com/2014/10/17/wlc-client-debug-part-2/>, skatīts 09.10.2020.
- [168] Nayanajith R. WLC Client Debug – Part 3. / Internets. – <https://mrncciew.com/2019/06/03/wlc-client-debug-part-3/>, skatīts 09.10.2020.
- [169] OpenWrt Documentation. / Internets. – <https://openwrt.org/docs/start>, skatīts 27.05.2020.
- [170] Project AirGig: 500 Patents and Applications, One Great Idea. AT&T, 2019. / Internets. – https://about.att.com/innovationblog/2019/03/project_airgig.html, skatīts 22.10.2020.
- [171] QoS: Congestion Avoidance Configuration Guide. / Internets. – https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/xs-16/qos-conavd-xe-16-book/qos-conavd-overview.html, skatīts 15.10.2020.
- [172] Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide. Cisco, 2014. / Internets. – https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RTowLAN/CCVP_BK_R7805F20_00_rtowlan-srnd/CCVP_BK_R7805F20_00_rtowlan-srnd_chapter_010.html, skatīts 18.02.2020.
- [173] Self-driving cars in the EU: from science fiction to reality. European Parliament, 2019. / Internets. – <https://www.europarl.europa.eu/news/en/headlines/economy/20190110STO23102/self-driving-cars-in-the-eu-from-science-fiction-to-reality>, skatīts 12.04.2020.
- [174] Springer J. Connectivity Standards in the Automotive Industry. / Internets. – https://www.itu.int/en/ITU-T/extcoop/cits/Documents/Meeting-20191028-e-meeting/18_5GAA_ITS-status-update.pdf, skatīts 10.11.2020.
- [175] The Mobile Economy 2020. / Internets. – https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf, skatīts 12.04.2020.
- [176] The SELFIS Tool. / Internets. – <http://alumni.cs.ucr.edu/~tkarag/Selfis/Selfis.html>, skatīts 07.11.2020.
- [177] The truth about throughput / Internets. – <https://www.excentis.com/blog/truth-about-throughput>, skatīts 14.09.2020.
- [178] TP-Link Archer C7 AC1750. Technical Data. / Internets. – <https://openwrt.org/toh/tp-link/archer-c7-1750>, skatīts 03.11.2020.
- [179] Understanding Carrier Ethernet Throughput. Am I getting the throughput I should be getting? Version 2, July, 2010. / Internets. – https://www.mef.net/Assets/White_Papers/Understanding_Carrier_Ethernet_Throughput_-_v14.pdf, skatīts 18.02.2020.
- [180] Wi-Fi Location-Based Services 4.1 Design Guide. Cisco, 2014. / Internets. – <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/WiFiLBS-DG/wifich5.html>, skatīts 18.02.2020.
- [181] WPA3 – Improving your WLAN security. / Internets. – <https://wlan1nde.wordpress.com/2018/09/14/wpa3-improving-your-wlan-security/>, skatīts 10.11.2020.
- [182] Zabbix Documentation 3.0, Zabbix appliance. / Internets. – <https://www.zabbix.com/documentation/3.0/manual/appliance>, skatīts 05.09.2020.

PIELIKUMU SARAKSTS

1. pielikums

Ziņojumu starptautiskās konferencēs, publikāciju zinātniskajos žurnālos, rakstu pilna teksta konferenču rakstu krājumos, zinātniskās pētniecības projektu saraksts.

2. pielikums

Matlab kodi AL caurlaidspējas aprēķiniem.

3. pielikums

Matlab kodi AL caurlaidspējas un atbildes laika aprēķiniem.

4. pielikums

Eksperimentāli iegūtie TL un AL caurlaidspējas mērījumu rezultāti.

5. pielikums

Eksperimentāli iegūtie AL caurlaidspējas, atbildes laika un pārslēgšanās procedūras aiztures mērījumu rezultāti.

6. pielikums

IEEE 802.11v BSS pārejas vadības ziņojumi.

7. pielikums

Matlab kodi uztvertā signāla jaudas līmeņa un caurlaidspējas aprēķiniem.

8. pielikums

Testgultnes specifikācijas dati un mērījumu iestatījumi.

9. pielikums

IEEE 802.11n/ac standartu specifikācija.

Ziņojumu un publikāciju saraksts

Ziņojumi starptautiskajās konferencēs

1. **Ancans A.**, Petersons E., Umanskis A. Hybrid Vehicular IEEE 802.11n and LTE Wireless Network Performance Evaluation in Non-Stationary Mode of Motion // *Advances in Wireless and Optical Communications (RTUWO)*. **Latvija**, Rīga, 15.–16. novembris, 2018.
2. **Ancans A.**, Petersons E., Ipatovs A. Vehicular Wireless Network Access Controller Parameter Estimation // *Progress in Electromagnetics Research Symposium (PIERS)*. **Singapūra**, 19.–22. novembris, 2017.
3. **Ancans A.**, Bogdanovs N., Petersons E., Ipatovs A. Integrated Wireless Network Performance Estimation for Moving Vehicles // *Advances in Wireless and Optical Communications (RTUWO)*. **Latvija**, Rīga, 2.–3. novembris, 2017.
4. **Ancans A.**, Petersons E. Wireless LAN and LTE Unified Data Channel Performance Evaluation at Various Types of Equipment and Measurement Methods of a Moving Object // *Riga Technical University 57th International Scientific Conference*. **Latvija**, Rīga, 14.–18. oktobris, 2016.
5. Ancans G., Stankevicius E., Bobrovs V., **Ancans A.** Analysis on Interference Impact of Wi-Fi on Digital Terrestrial Television Broadcasting // *Wireless Telecommunications Symposium (WTS)*. *Global Wireless Communications: Europe and Beyond*. **Lielbritānija**, Londona, 18.–20. aprīlis, 2016.
6. **Ancans A.**, Petersons E., Ipatovs A. Development of a Measurement System for Evaluation of Heterogeneous Wireless Networks Performance Parameters // *Riga Technical University 56th International Scientific Conference*. **Latvija**, Rīga, 14.–16. oktobris, 2015.
7. **Ancans A.**, Ipatovs A. Analysis of Routing Protocols in Wireless Networks with Moving Objects // *Riga Technical University 55th International Scientific Conference*. **Latvija**, Rīga, 14.–16. oktobris, 2014.

Nodaļa zinātniskajā monogrāfijā

1. Jerjomins R., **Ancans A.**, Petersons E., Gerina-Ancane A. Improving Handover Mechanism in Vehicular WiFi Networks. In: *ICTE in Transportation and Logistics 2019, Lecture Notes in Intelligent Transportation and Infrastructure (ICTE ToL 2019, LNITI)*. Ginters E., Ruiz Estrada M., Piera Eroles M., eds. **Switzerland**, Cham: Springer, 2020, pp. 243–261.

Publikācijas zinātniskajos žurnālos

1. **Ancans A.**, Petersons E., Jerjomins R., Grabs E., Ancans G., Ipatovs A. Evaluation of received signal power level and throughput depending on distance to transmitter in testbed for automotive WLAN IEEE 802.11ac communication network // *Latvian Journal of Physics and Technical Sciences* (apstiprināta publicēšanai).

2. **Ancans A.**, Petersons E., Ancans G., Stetjuha M., Ipatovs A., Stankevicius E. Technical and Economic Analysis of Transport Telecommunication Infrastructure // *Procedia Computer Science*. 2019, No. 149, pp. 206–214.
3. **Ancans A.**, Petersons E. The Relationship between Transport Wireless Network Throughput and Vehicle Speed // *Automatic Control and Computer Sciences (AC&CS)*. 2018, Vol. 52, Iss. 4, pp. 297–305.
4. Ancans G., Stafecka A., Bobrovs V., **Ancans A.**, Caiko J. Analysis of Characteristics and Requirements for 5G Mobile Communication Systems // *Latvian Journal of Physics and Technical Sciences*. 2017, Vol. 54, Iss. 4, pp. 69–78.
5. Ancans G., Bobrovs V., **Ancans A.**, Kalibatiene D. Spectrum Considerations for 5G Mobile Communication Systems // *Procedia Computer Science*. 2017, Vol. 104, pp. 509–516.
6. **Ancans A.**, Bogdanovs N., Petersons E., Ancans G., Umanskis A., Vishnevskiy V. Evaluation of Wi-Fi and LTE Integrated Channel Performance with Different Hardware Implementation for Moving Objects // *Procedia Computer Science*. 2017, Vol. 104, pp. 493–500.
7. Ancans G., Stankevicius E., Bobrovs V., **Ancans A.** Analysis on Interference Impact of Wi-Fi on Digital Terrestrial Television Broadcasting // *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)*. 2016, Vol. 8, Iss. 1, pp. 35–44.
8. Bogdanovs N., **Ancans A.**, Martinsons K., Petersons E. Estimating the Speed of an Integrated Wireless Network for Transportation Applications // *Automatic Control and Computer Sciences (AC&CS)*. 2014, Vol. 48, Iss. 5, pp. 274–281.

Publikācijas pilna teksta konferenču rakstu krājumos

1. **Ancans A.**, Petersons E., Umanskis A. Hybrid Vehicular IEEE 802.11n and LTE Wireless Network Performance Evaluation in Non-Stationary Mode of Motion // *Proceedings of Advances in Wireless and Optical Communications (RTUWO)*. Latvia, Riga, 15–16 November, 2018, pp. 213–213.
2. **Ancans A.**, Petersons E., Ipatovs A. Vehicular Wireless Network Access Controller Parameter Estimation // *Progress in Electromagnetics Research Symposium (PIERS)*. Singapore, 19–22 November, 2017, pp. 2152–2159.
3. **Ancans A.**, Bogdanovs N., Petersons E., Ipatovs A. Integrated Wireless Network Performance Estimation for Moving Vehicles // *Proceedings of Advances in Wireless and Optical Communications (RTUWO)*. Latvia, Riga, 2–3 November, 2017, pp. 203–207.
4. Ancans G., Stankevicius E., Bobrovs V., **Ancans A.** Analysis on Interference Impact of Wi-Fi on Digital Terrestrial Television Broadcasting // *Proceedings of Wireless Telecommunications Symposium (WTS). Global Wireless Communications: Europe and Beyond*. United Kingdom, London, 18–20 April, 2016, p. 13.

Dalība projektos

Starptautiskais zinātniskās pētniecības projekts

Promocijas darba rezultāti tika izmantoti ERAF projekta pieteikuma sagatavošanā:
“Viedais savienojamības risinājums autotransporta sakaru tīkliem (SCAN)”,
Nr. 1.1.1.1/20/A/007.

Matlab kodi AL caurlaidspējas aprēķiniem**Analītiskā modeļa aprēķini**

```

max_M = 4; % klientu skaits
M      = 1:max_M;

lambda = zeros(1,4) + lambda2; % ziņojumu pienākšanas intensitāte
mu      = zeros(1,4) + mu2; % ziņojumu apstrādes intensitāte

p0      = zeros(1,max_M);
for num = M
    % p0 varbūtības noteikšana
    p0cur = 0;
    for k = 0 : num;
        p0cur = p0cur + (factorial(num)/factorial(num-
k)*(lambda(num)/mu(num))^k);
    end
    p0cur = 1/p0cur;
    p0(num) = p0cur
end

performance_goodput = (1 - p0).*mu % kopējā bezvadu tīkla aplikācijas līmeņa
caurlaidspēja, Mbiti/s
goodput = (1 - p0).*mu./M % aplikācijas līmeņa caurlaidspēja vienam klientam,
Mbiti/s

```

Matlab kodi AL caurlaidspējas un atbildes laika aprēķiniem**a) Aplikācijas līmeņa (AL) caurlaidspēja**

```

% v1 = 20 km/h
mu1 = 12.99; % Mbiti/s
rho = 0.5;
lambda1 = rho*mu1;
lambda = zeros(1,10) + lambda1; % ziņojumu pienākšanas intensitāte
mu_v1 = zeros(1,10) + mu1; % ziņojumu apstrādes intensitāte
max_M = 10;
p0 = zeros(1,max_M);
M = 1:max_M;
for num = M
    p0cur = 0;
    for k = 0 : num;
        p0cur = p0cur + (factorial(num)/factorial(num-
k)*(lambda(num)/mu_v1(num))^k);
    end
    p0cur = 1/p0cur;
    p0(num) = p0cur;
end
performance_goodput_v1 = (1 - p0).*mu_v1; % aplikācijas līmeņa caurlaidspēja,
Mbiti/s

% v2 = 50 km/h
mu2 = 11.39; % Mbiti/s
lambda2 = rho*mu2;
lambda = zeros(1,10) + lambda2;
mu_v2 = zeros(1,10) + mu2;
max_M = 10;
p0 = zeros(1,max_M);
M = 1:max_M;
for num = M
    p0cur = 0;
    for k = 0 : num;
        p0cur = p0cur + (factorial(num)/factorial(num-
k)*(lambda(num)/mu_v2(num))^k);
    end
    p0cur = 1/p0cur;
    p0(num) = p0cur;
end
performance_goodput_v2 = (1 - p0).*mu_v2; % aplikācijas līmeņa caurlaidspēja,
Mbiti/s

% v3 = 70 km/h
mu3 = 10.69; % Mbiti/s
lambda3 = rho*mu3;
lambda = zeros(1,10) + lambda3;
mu_v3 = zeros(1,10) + mu3;
max_M = 10;
p0 = zeros(1,max_M);
M = 1:max_M;
for num = M
    p0cur = 0;
    for k = 0 : num;
        p0cur = p0cur + (factorial(num)/factorial(num-
k)*(lambda(num)/mu_v3(num))^k);
    end
    p0cur = 1/p0cur;
    p0(num) = p0cur;
end
performance_goodput_v3 = (1 - p0).*mu_v3; % aplikācijas līmeņa caurlaidspēja,
Mbiti/s

```

b) Atbildes laiks

```
% v1 = 20 km/h
goodput_vid_v1 = 12.99; % Mbiti/s
T_1MB = 1*8/goodput_vid_v1; % 1 MB faila pārsūtišanas laiks, s
mul = 1/T_1MB;
rho = 0.5;
lambda1 = rho*mul;
lambda = zeros(1,10) + lambda1;
mu_v1 = zeros(1,10) + mul;

max_M = 10;
p0 = zeros(1,max_M);
M = 1:max_M;
for num = M
    p0cur = 0;
    for k = 0 : num;
        p0cur = p0cur + (factorial(num)/factorial(num-
k)*(lambda(num)/mu_v1(num))^k);
    end
    p0cur = 1/p0cur;
    p0(num) = p0cur;
end
response_time_v1 = M./(mu_v1.*(1-p0))-1./lambda % atbildes laiks, s

% v2 = 50 km/h
goodput_vid_v2 = 11.39; % Mbiti/s
T_1MB = 1*8/goodput_vid_v2;
mu2 = 1/T_1MB;
lambda2 = rho*mu2;
lambda = zeros(1,10) + lambda2;
mu_v2 = zeros(1,10) + mu2;
max_M = 10;
p0 = zeros(1,max_M);
M = 1:max_M;
for num = M
    p0cur = 0;
    for k = 0 : num;
        p0cur = p0cur + (factorial(num)/factorial(num-
k)*(lambda(num)/mu_v2(num))^k);
    end
    p0cur = 1/p0cur;
    p0(num) = p0cur;
end
response_time_v2 = M./(mu_v2.*(1-p0))-1./lambda % atbildes laiks, s

% v3 = 70 km/h
goodput_vid_v3 = 10.69; % Mbiti/s
T_1MB = 1*8/goodput_vid_v3;
mu3 = 1/T_1MB;
lambda3 = rho*mu3;
lambda = zeros(1,10) + lambda3;
mu_v3 = zeros(1,10) + mu3;
max_M = 10;
p0 = zeros(1,max_M);
M = 1:max_M;
for num = M
    p0cur = 0;
    for k = 0 : num;
        p0cur = p0cur + (factorial(num)/factorial(num-
k)*(lambda(num)/mu_v3(num))^k);
    end
    p0cur = 1/p0cur;
    p0(num) = p0cur;
end
response_time_v3 = M./(mu_v3.*(1-p0))-1./lambda % atbildes laiks, s
```

c) Aplikācijas līmeņa caurlaidspējas un atbildes laika atkarība no automobiļu skaita

```
% v1 = 20 km/h
goodput_vid_v1 = 12.99; % Mbiti/s
rho = 0.2;
mul = goodput_vid_v1;
lambdal = rho*mul;

lambda = zeros(1,26) + lambdal;
mu_v1 = zeros(1,26) + mul;

max_M = 26;
p0_v1 = zeros(1,max_M);
M = 1:max_M;
for num = M
    p0cur_v1 = 0;
    for k = 0 : num;
        p0cur_v1 = p0cur_v1 + (factorial(num)/factorial(num-
k)*(lambda(num)/mu_v1(num))^k);
    end
    p0cur_v1 = 1/p0cur_v1;
    p0_v1(num) = p0cur_v1;
end
performance_goodput_v1 = (1 - p0_v1).*mu_v1; % aplikācijas līmeņa caurlaidspēja,
Mbiti/s

T_1MB = 1*8/goodput_vid_v1; % 1 MB faila pārsūtīšanas laiks
mul = 1/T_1MB;
lambdal = rho*mul;

lambda = zeros(1,26) + lambdal;
mu_v1 = zeros(1,26) + mul;

max_M = 26;
p0_v1 = zeros(1,max_M);
M = 1:max_M
for num = M
    p0cur_v1 = 0;
    for k = 0 : num;
        p0cur_v1 = p0cur_v1 + (factorial(num)/factorial(num-
k)*(lambda(num)/mu_v1(num))^k);
    end
    p0cur_v1 = 1/p0cur_v1;
    p0_v1(num) = p0cur_v1;
end
response_time_v1 = M./(mu_v1.*(1-p0_v1))-1./lambda % atbildes laiks, s

[X, Y] = meshgrid(response_time_v1, performance_goodput_v1);
Z = griddata(response_time_v1, performance_goodput_v1, M, X, Y)
surf(X,Y,Z), grid on
```

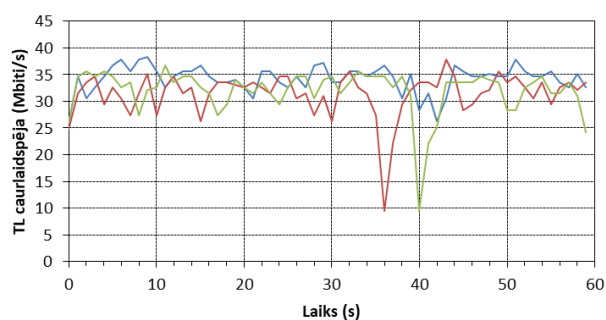
4. pielikums

Eksperimentāli iegūtie TL un AL caurlaidspējas mērījumu rezultāti

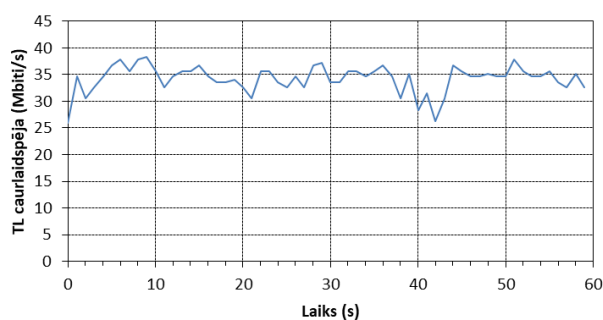
Divrangu sakaru tīklā eksperimentāli iegūtie mērījumu rezultāti likumsakarībai starp mobilā klienta braukšanas ātrumu un transporta līmeņa (TL) vai aplikācijas līmeņa (AL) caurlaidspēju, kuru apkopojums ir pieejams promocijas darbā.

4.1. pielikums

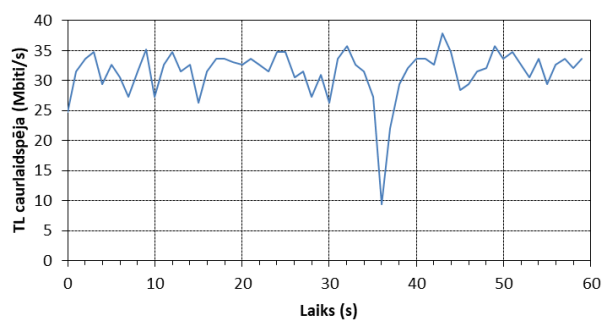
TL caurlaidspēja, 0 km/h



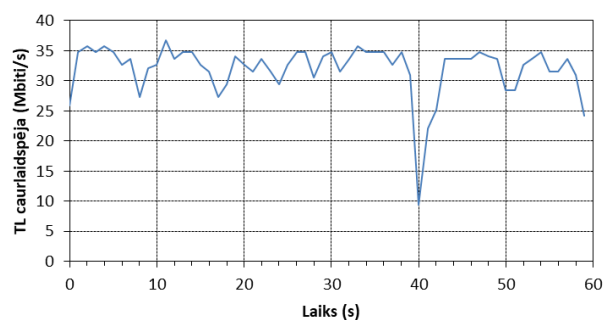
a) Apvienotie mērījumi



b)



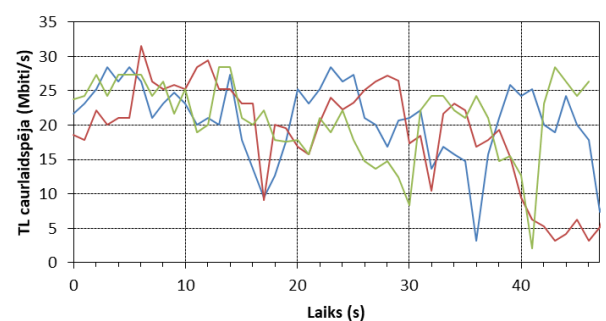
c)



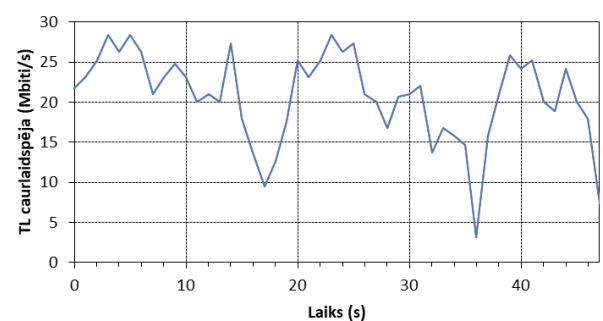
d)

4.2. pielikums

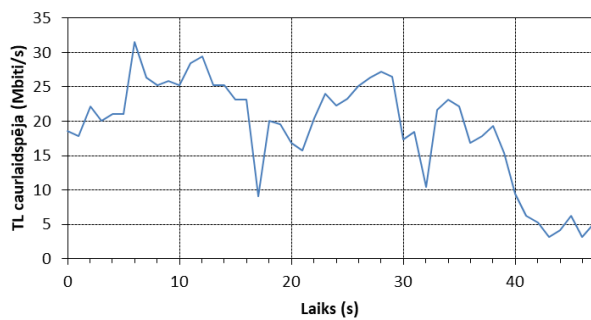
TL caurlaidspēja, 20 km/h



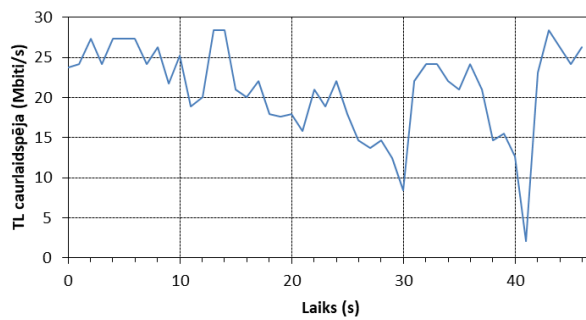
a) Apvienotie mērījumi



b)



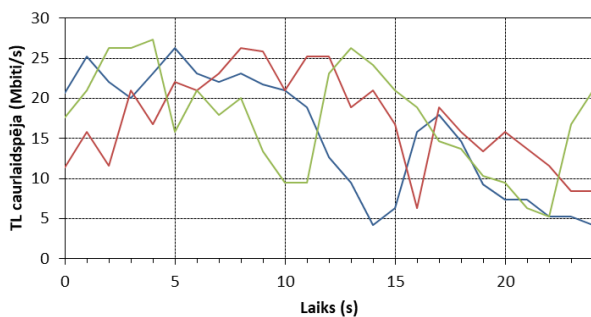
c)



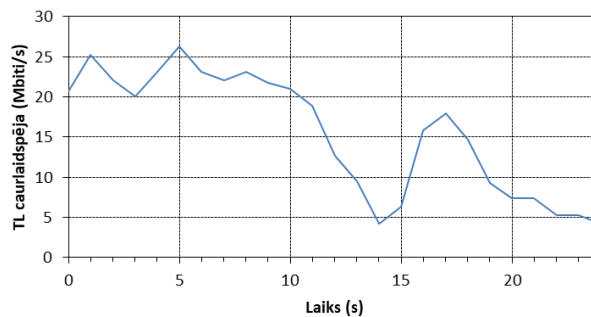
d)

4.3. pielikums

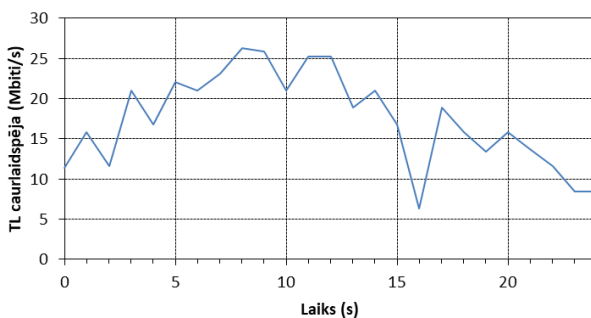
TL caurlaidspēja, 40 km/h



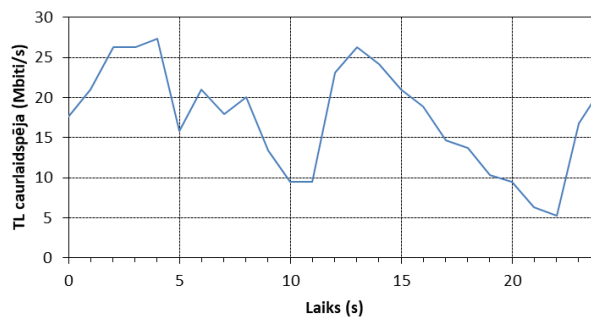
a) Apvienotie mērījumi



b)



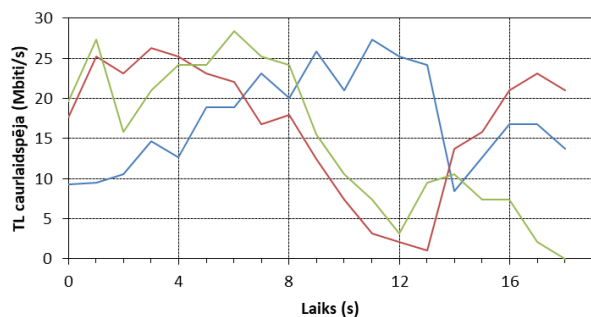
c)



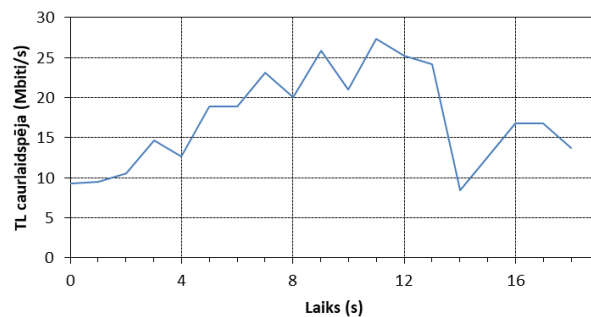
d)

4.4. pielikums

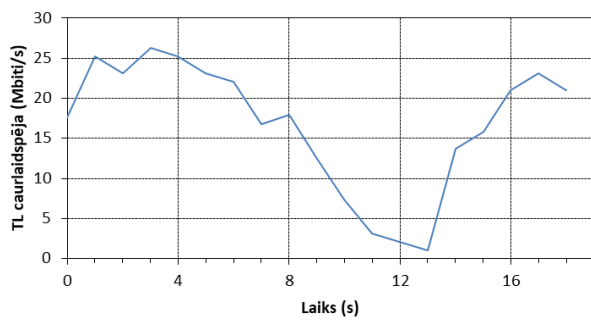
TL caurlaidspēja, 50 km/h



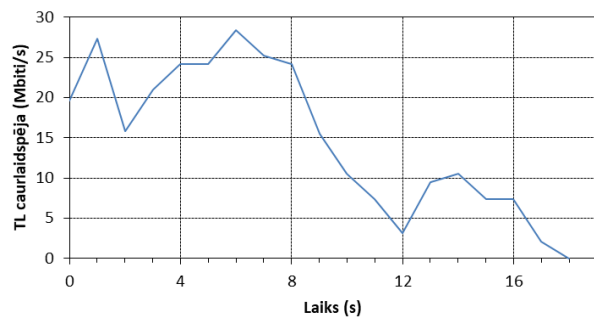
a) Apvienotie mērījumi



b)



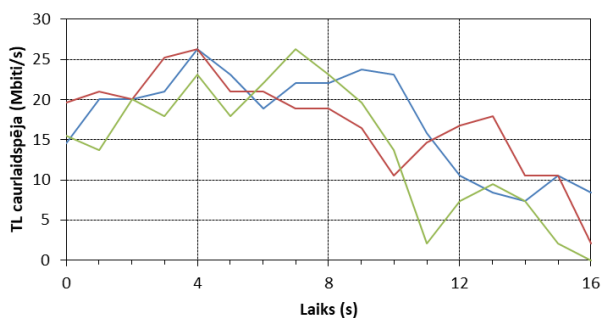
c)



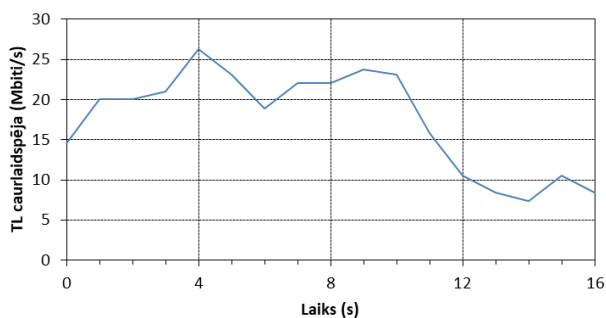
d)

4.5. pielikums

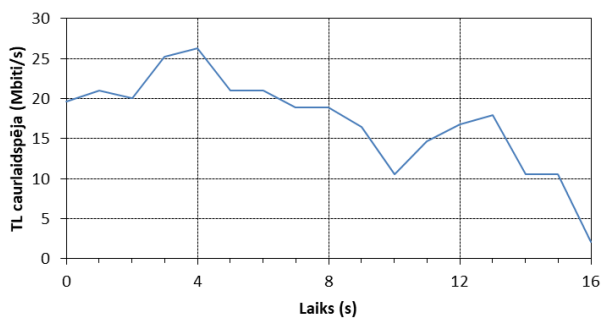
TL caurlaidspēja, 60 km/h



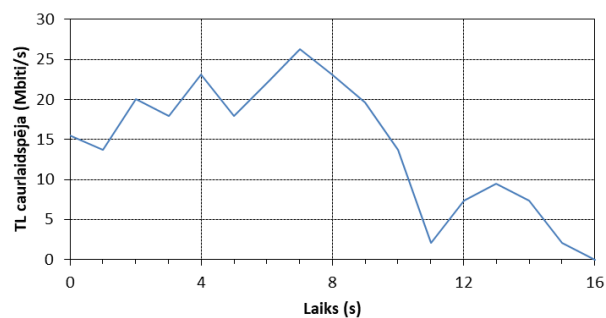
a) Apvienotie mērījumi



b)



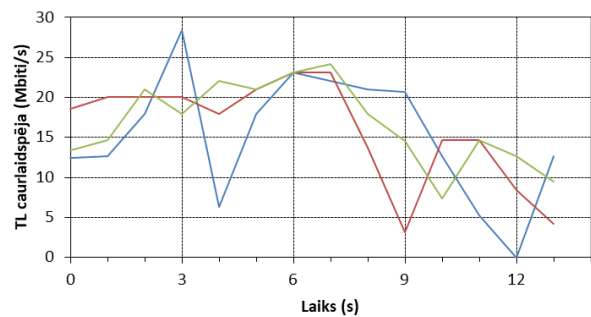
c)



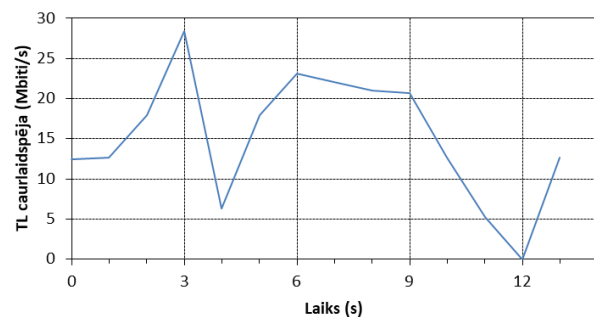
d)

4.6. pielikums

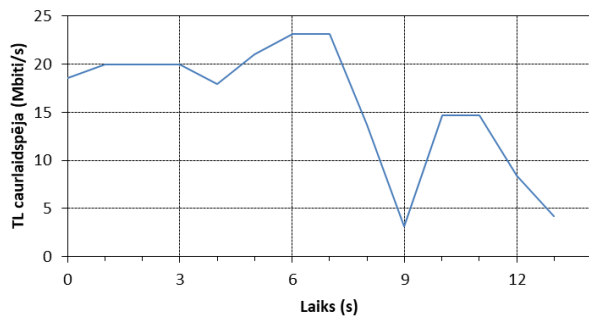
TL caurlaidspēja, 70 km/h



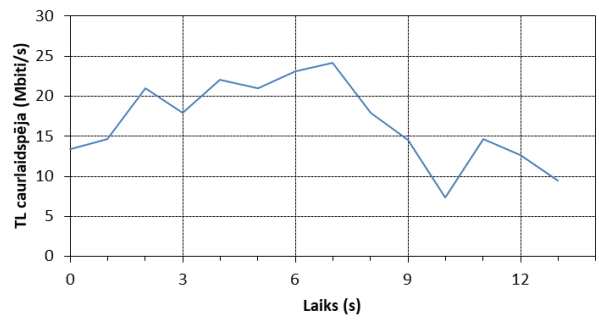
a) Apvienotie mērījumi



b)



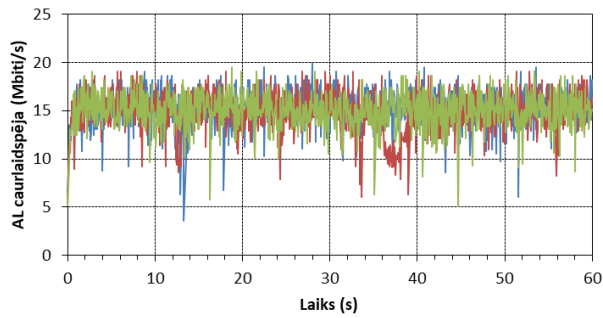
c)



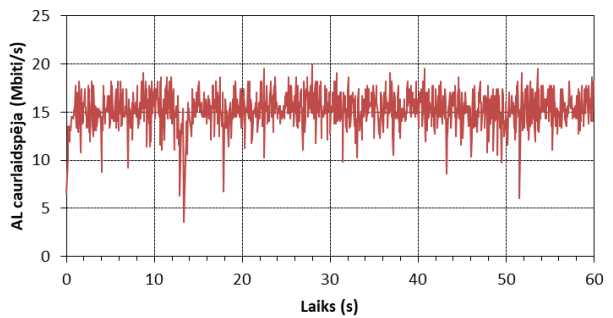
d)

4.7. pielikums

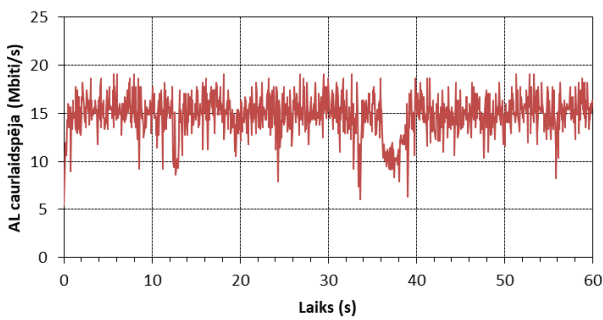
AL caurlaidspēja, 0 km/h



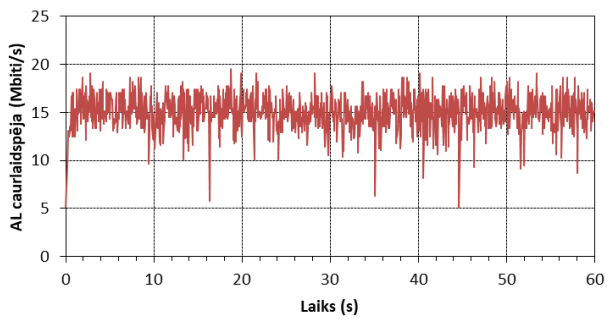
a) Apvienotie mērījumi



b)



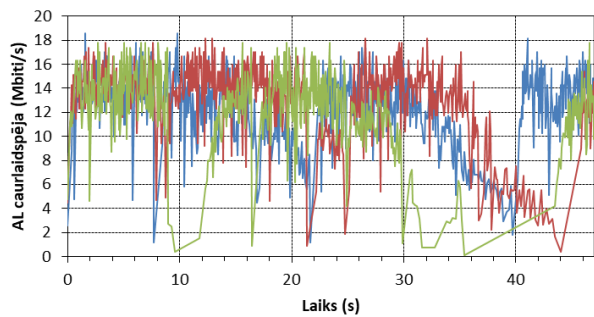
c)



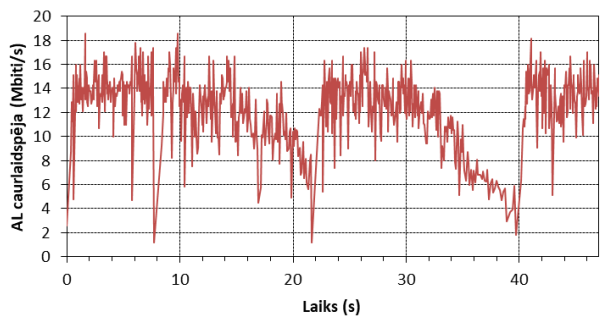
d)

4.8. pielikums

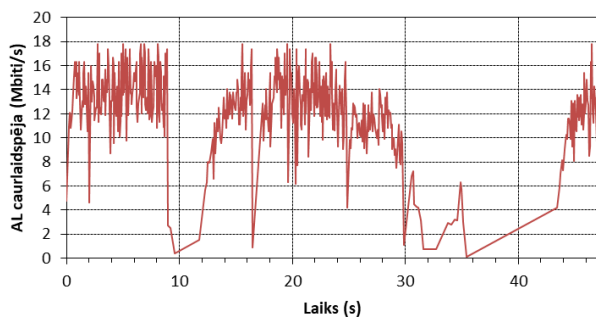
AL caurlaidspēja, 20 km/h



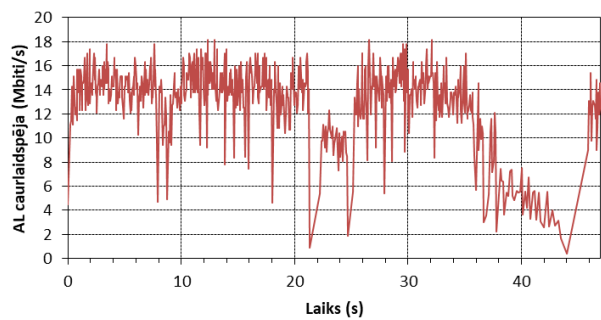
a) Apvienotie mērījumi



b)



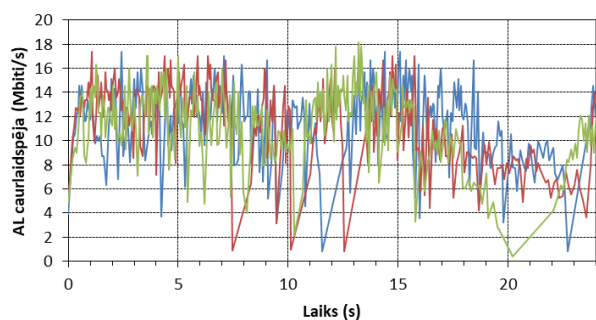
c)



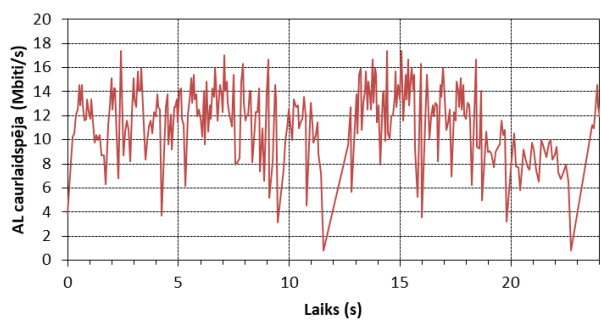
d)

4.9. pielikums

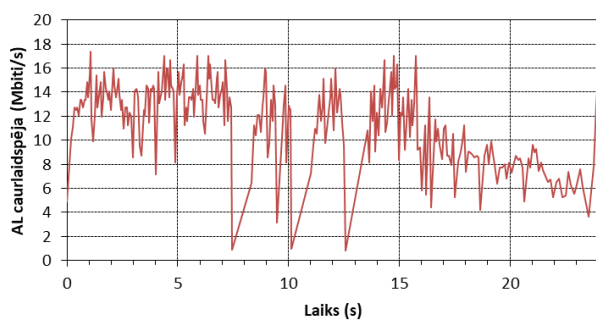
AL caurlaidspēja, 40 km/h



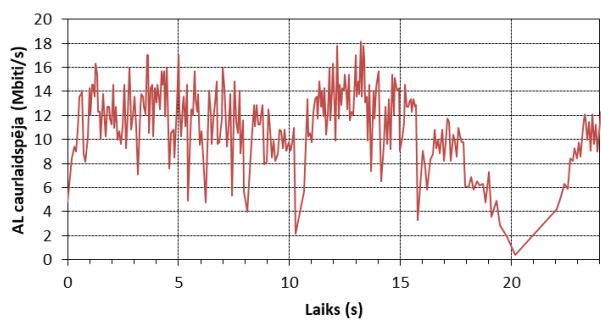
a) Apvienotie mērījumi



b)



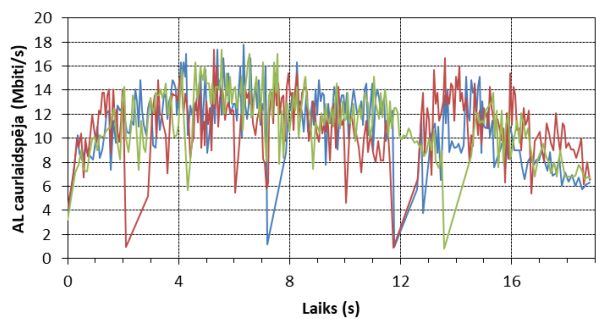
c)



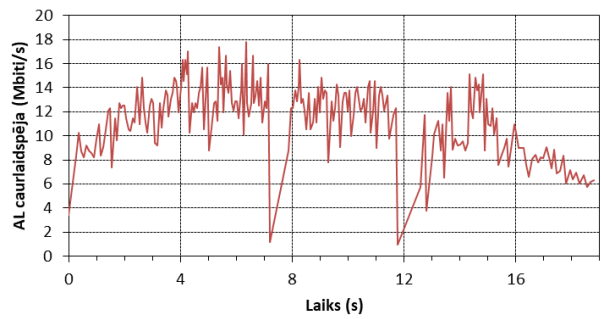
d)

4.10. pielikums

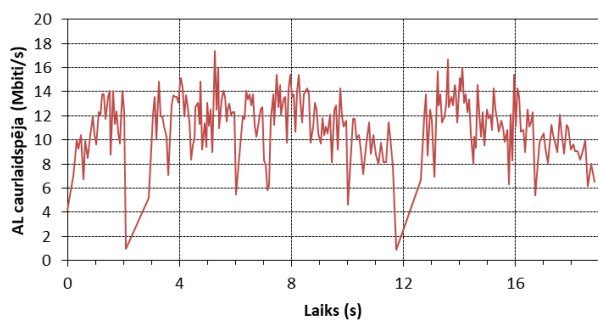
AL caurlaidspēja, 50 km/h



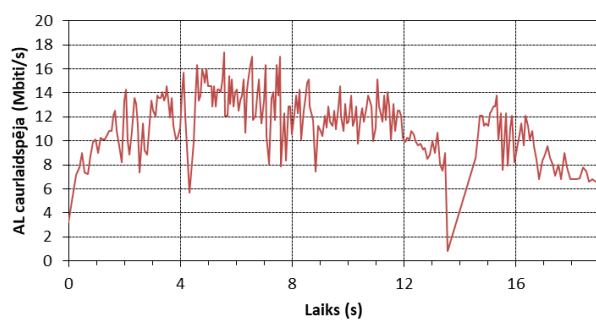
a) Apvienotie mērījumi



b)



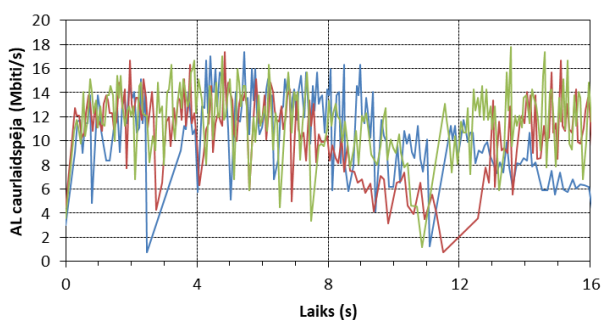
c)



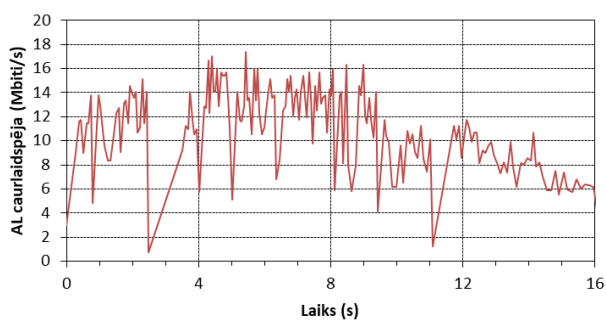
d)

4.11. pielikums

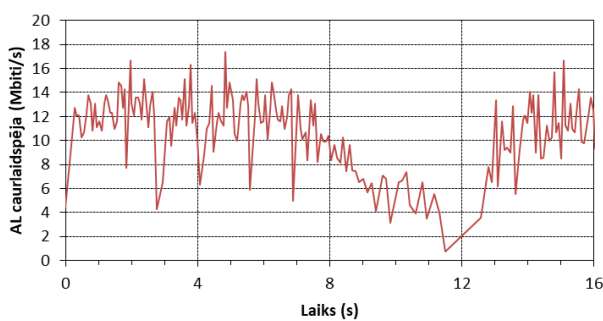
AL caurlaidspēja, 60 km/h



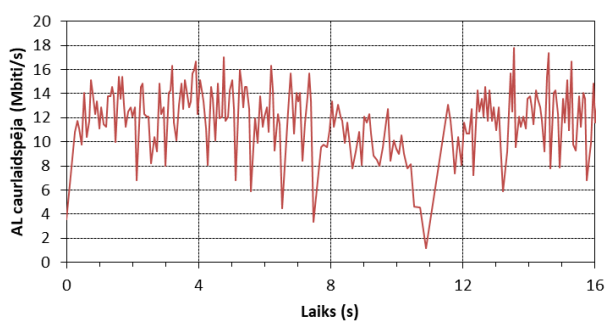
a) Apvienotie mērījumi



b)



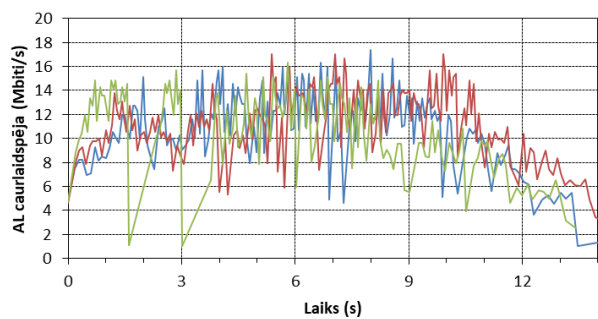
c)



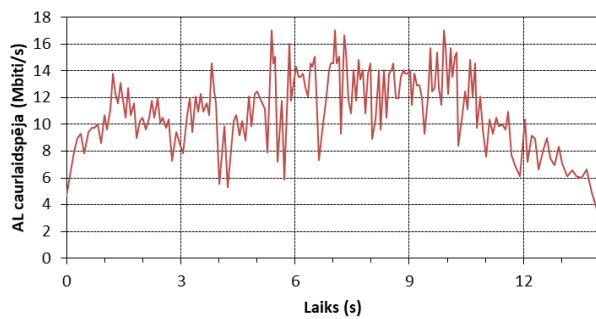
d)

4.12. pielikums

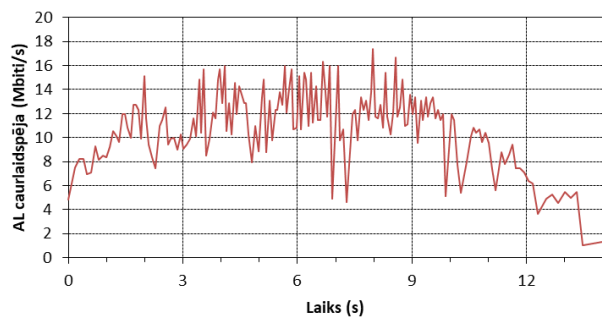
AL caurlaidspēja, 70 km/h



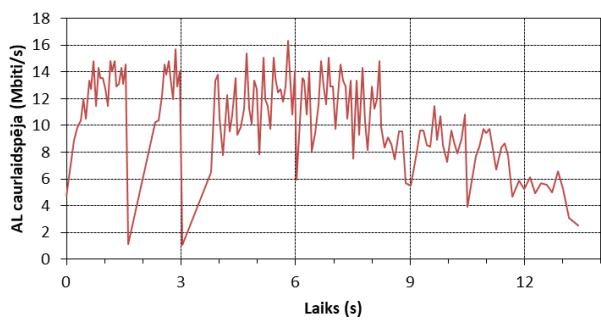
a) Apvienotie mērījumi



b)



c)



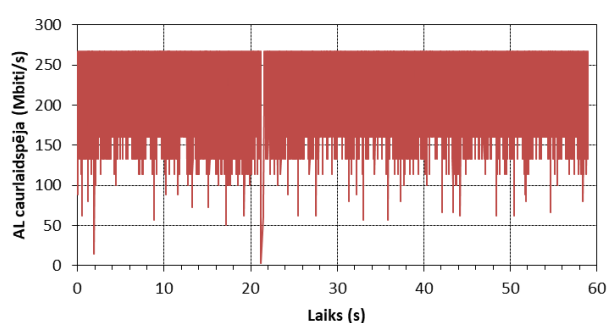
d)

Eksperimentāli iegūtie AL caurlaidspējas, atbildes laika un pārslēgšanās procedūras aiztures mērījumu rezultāti

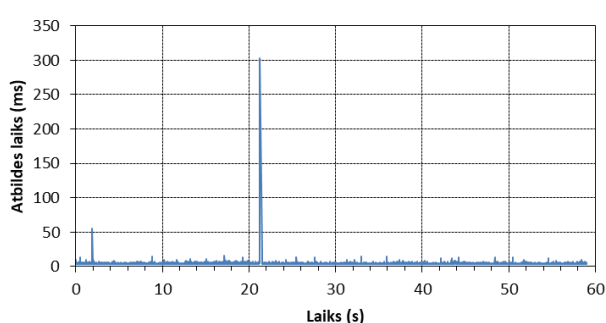
AL caurlaidspējas un atbildes laika mērījumu rezultāti *IEEE 802.11ac* tīklā, izmantojot “Standarta”, “802.11v tīkla virzītu” (manuālo) un “802.11v tīkla asistētu” pārslēgšanās procedūras metodes.

5.1. pielikums

AL caurlaidspēja un atbildes laiks, izmantojot “Standarta” pārslēgšanās procedūru, 0 km/h



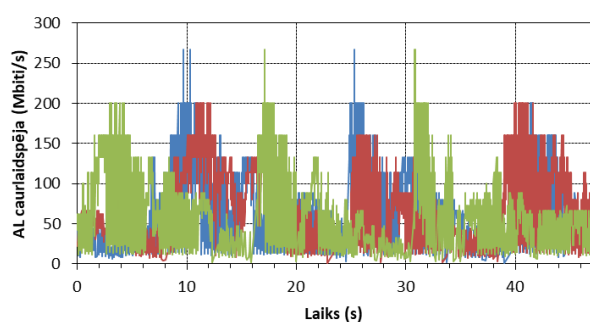
a) Apvienotie mērījumi



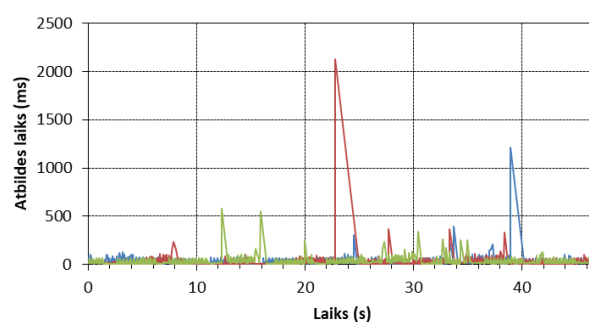
b)

5.2. pielikums

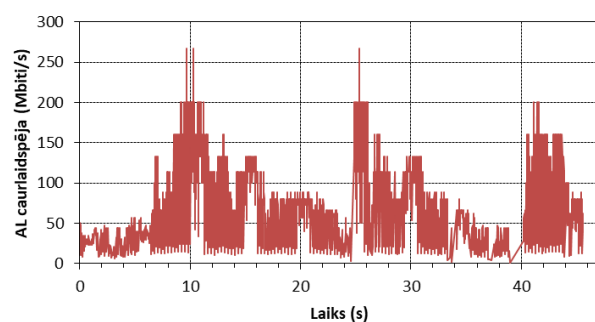
AL caurlaidspēja un atbildes laiks, izmantojot “Standarta” pārslēgšanās procedūru, 20 km/h



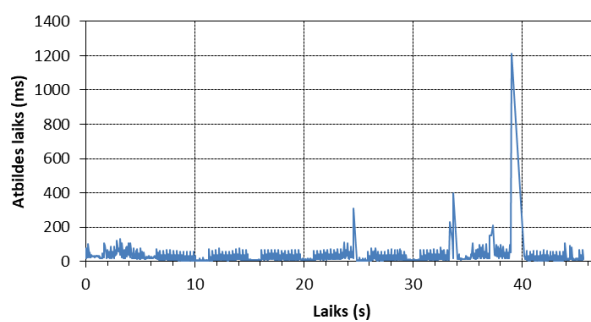
a) Apvienotie mērījumi



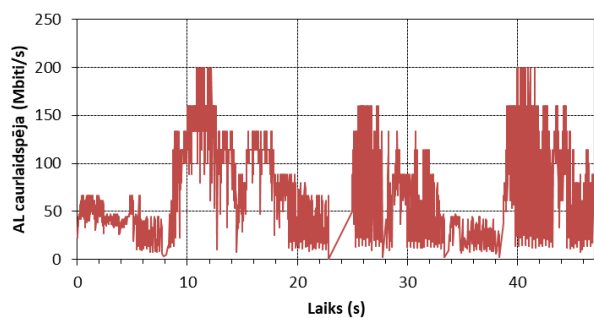
b) Apvienotie mērījumi.



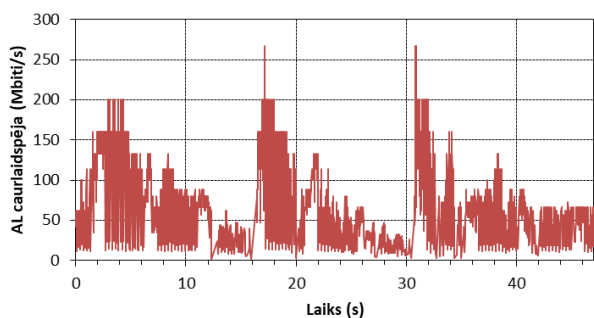
c)



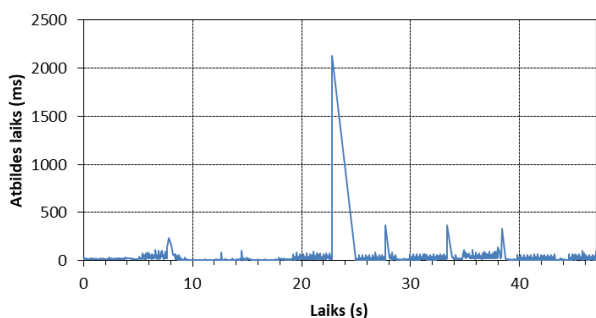
d)



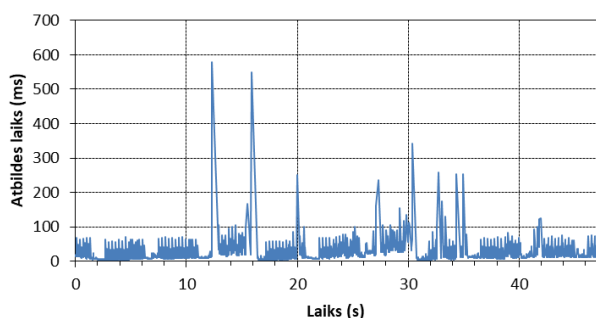
e)



g)



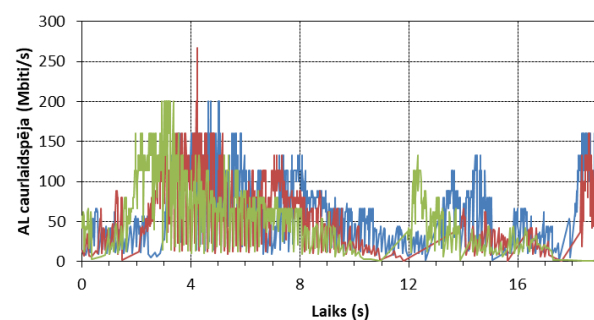
f)



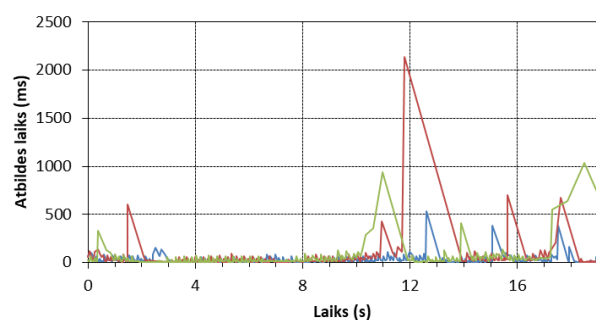
h)

5.3. pielikums

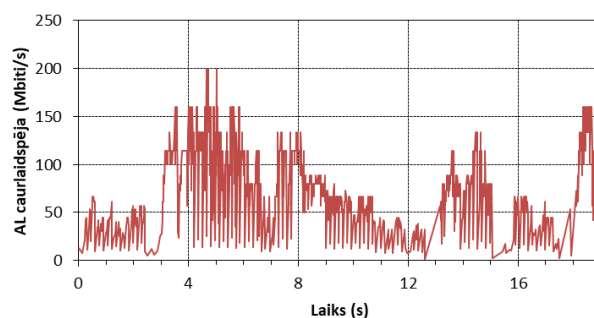
AL caurlaidspēja un atbildes laiks, izmantojot “Standarta” pārslēgšanās procedūru, 50 km/h



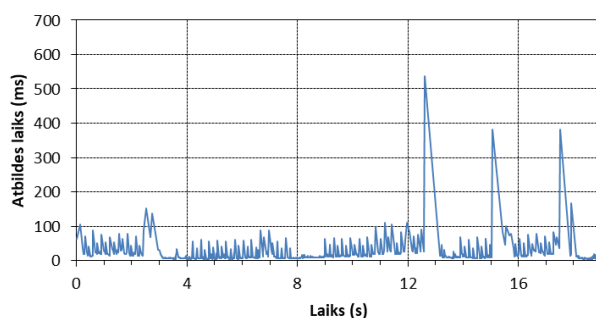
a) Apvienotie mērījumi



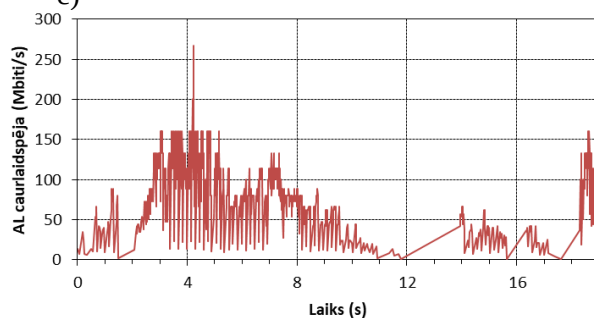
b) Apvienotie mērījumi



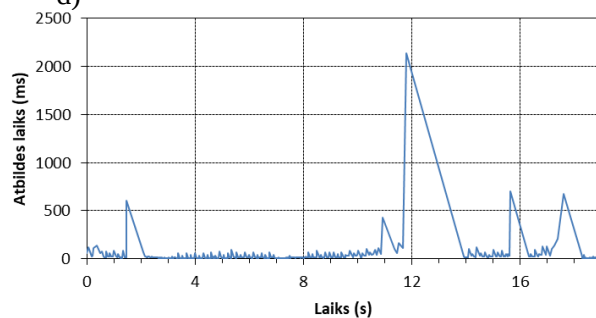
c)



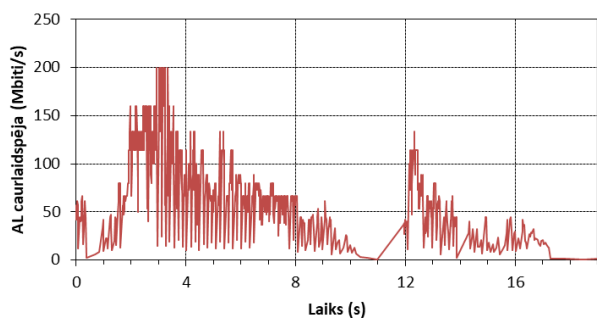
d)



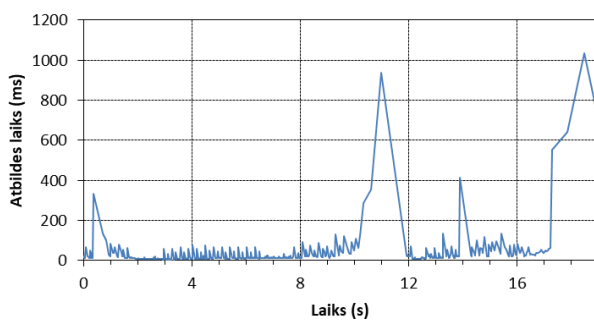
e)



f)



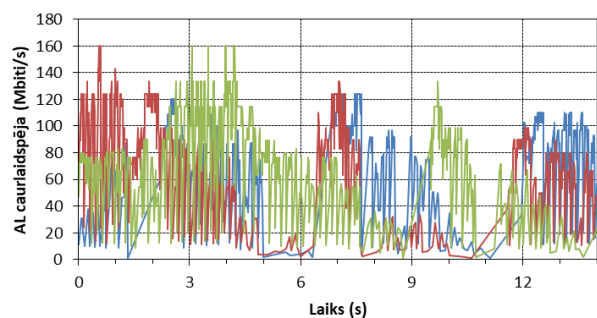
g)



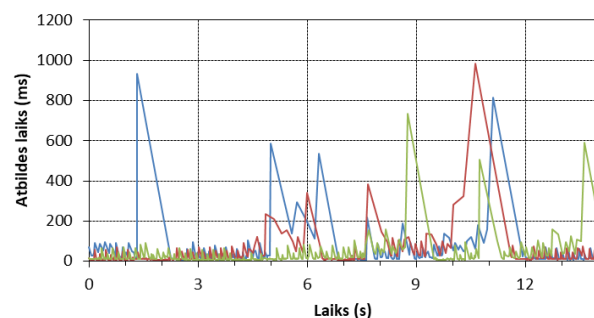
h)

5.4. pielikums

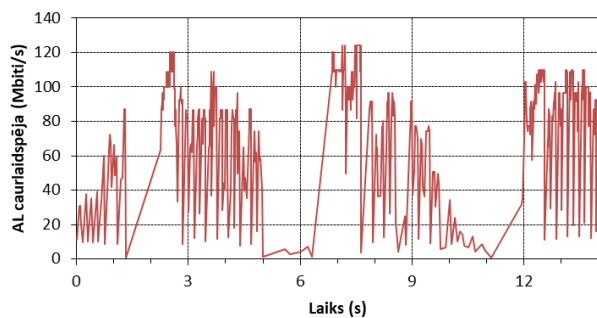
AL caurlaidspeja un atbildes laiks, izmantojot “Standarta” pārslēgšanās procedūru, 70 km/h



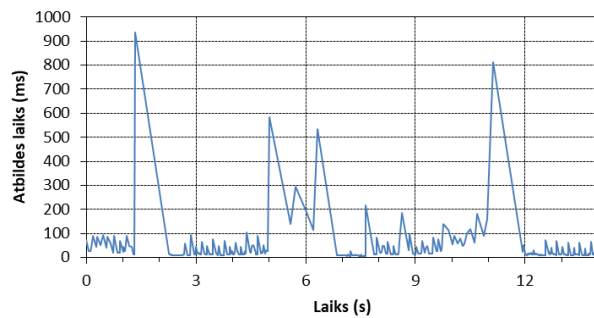
a) Apvienotie mērījumi



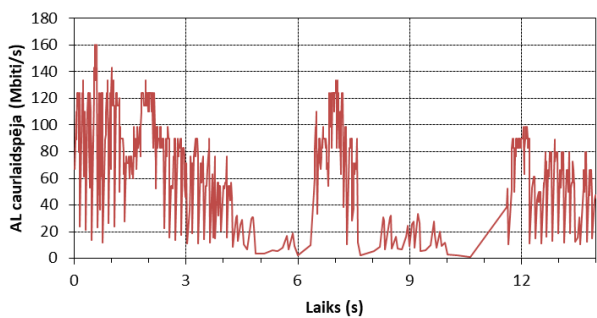
b) Apvienotie mērījumi



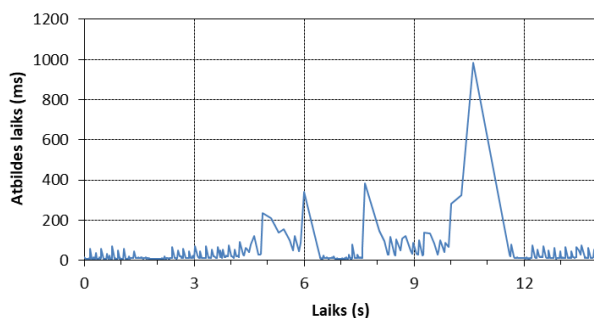
c)



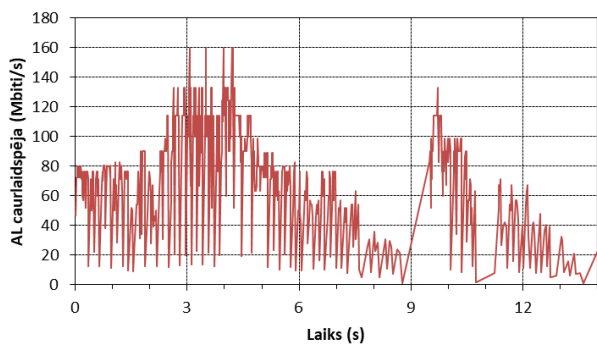
d)



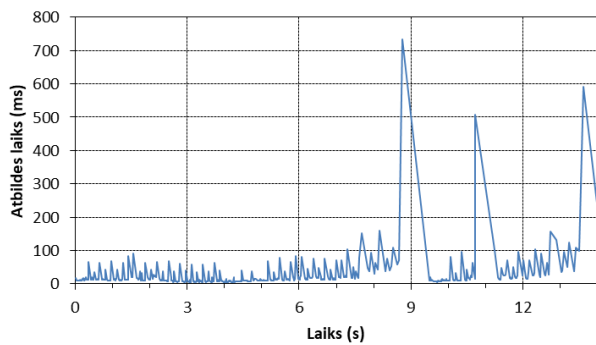
e)



f)



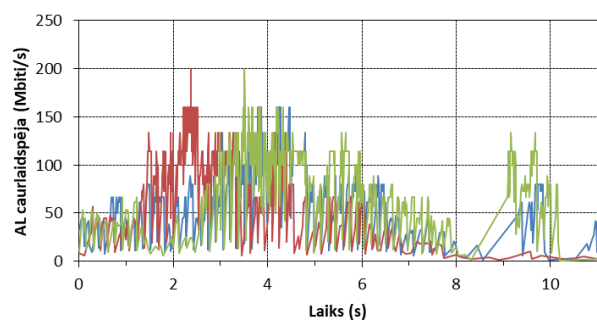
g)



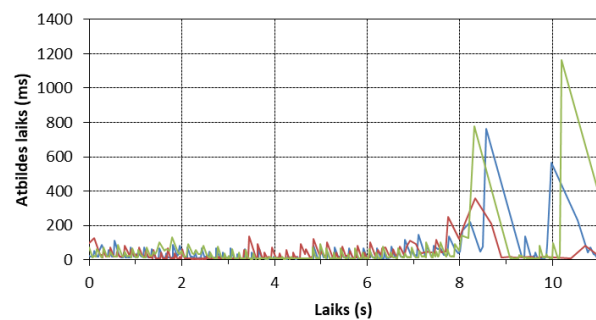
h)

5.5. pielikums

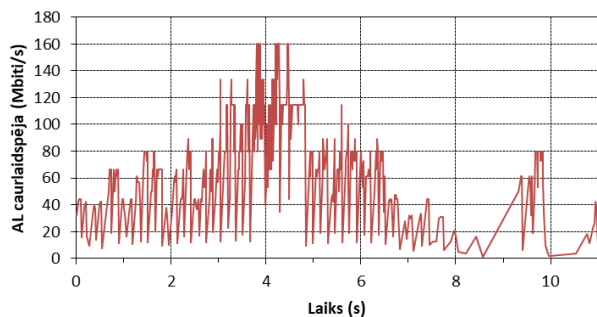
AL caurlaidspēja un atbildes laiks, izmantojot “Standarta” pārslēgšanās procedūru, 90 km/h



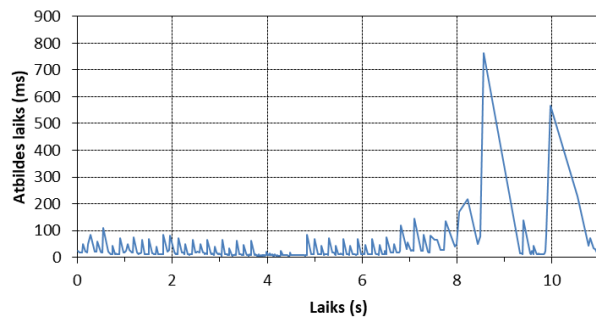
a) Apvienotie mērījumi



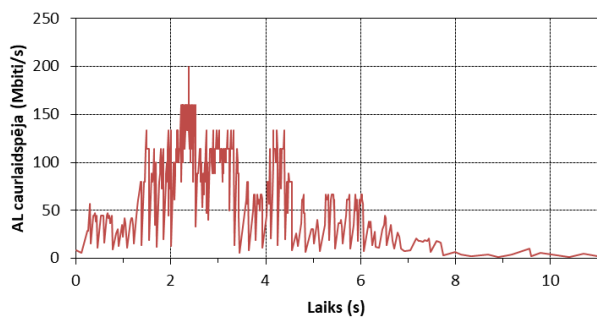
b) Apvienotie mērījumi



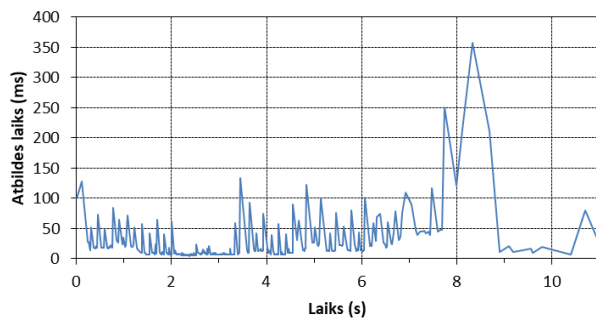
c)



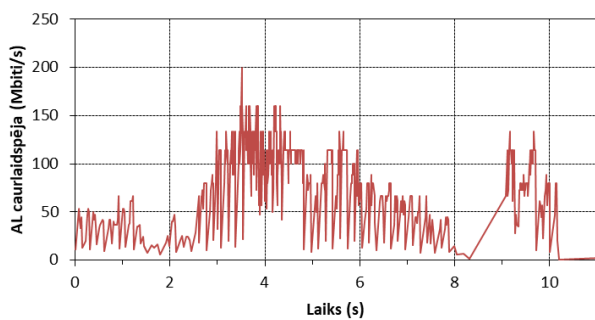
d)



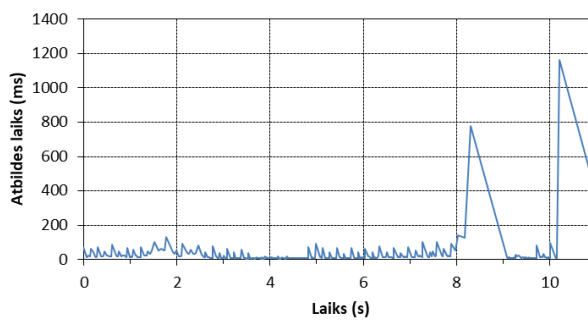
e)



f)



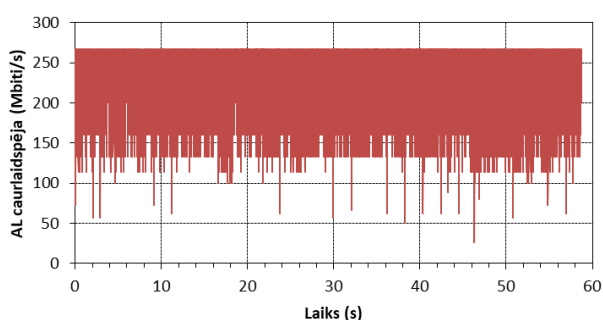
g)



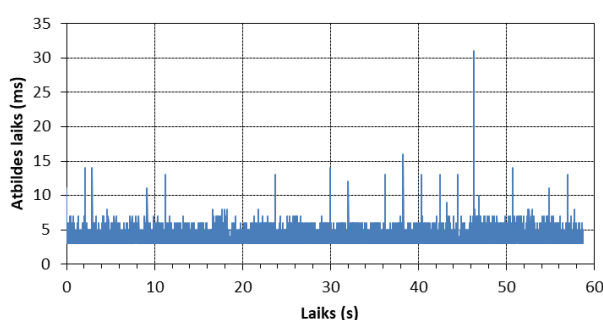
h)

5.6. pielikums

AL caurlaidspēja un atbildes laiks, izmantojot “802.11v tīkla virzītu” (manuālo) pārslēgšanās procedūru, 0 km/h



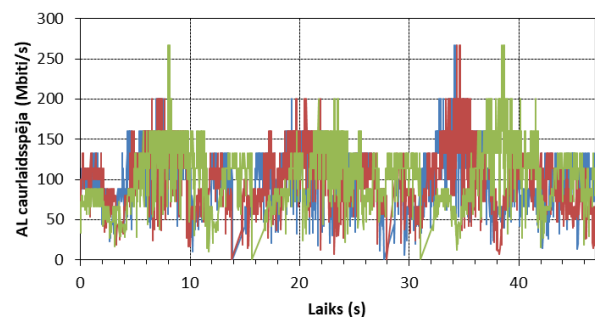
a)



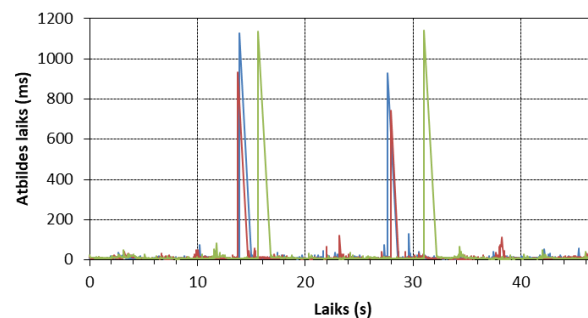
b)

5.7. pielikums

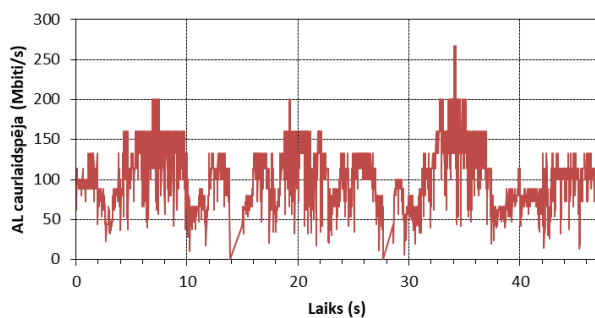
AL caurlaidspēja un atbildes laiks, izmantojot “802.11v tīkla virzītu” (manuālo) pārslēgšanās procedūru, 20 km/h



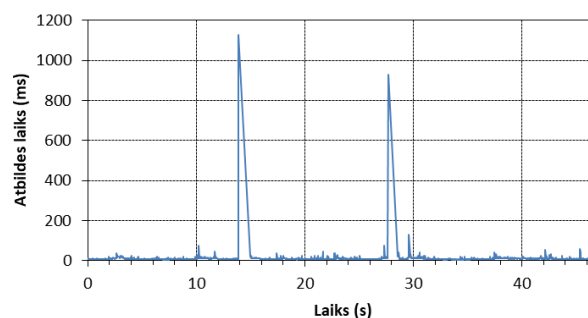
a) Apvienotie mērījumi



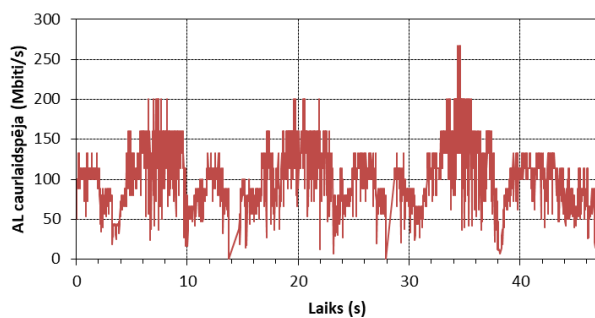
b) Apvienotie mērījumi



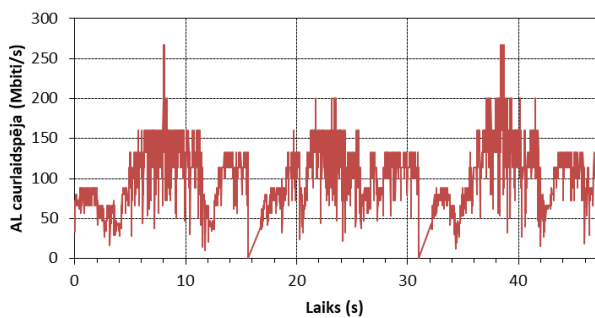
c)



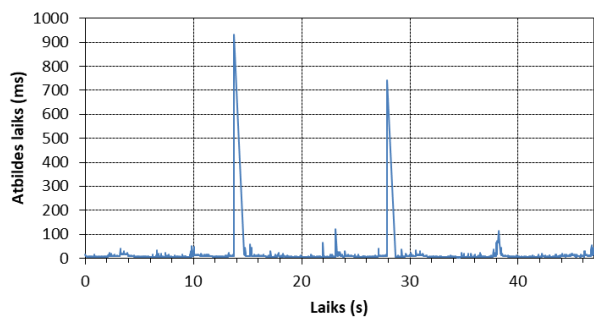
d)



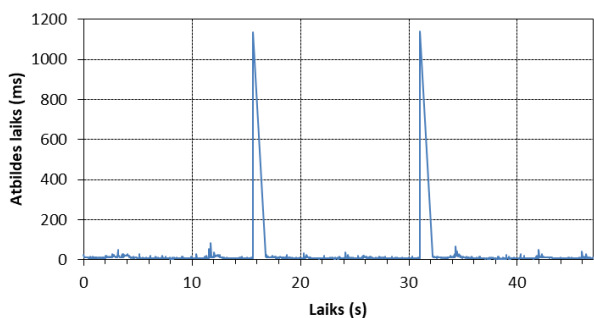
e)



g)



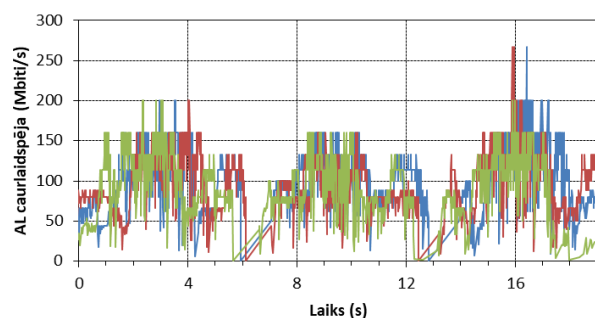
f)



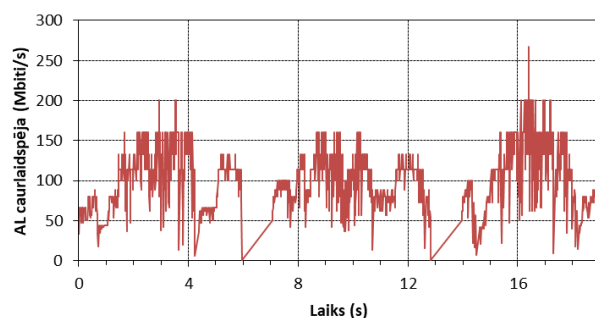
h)

5.8. pielikums

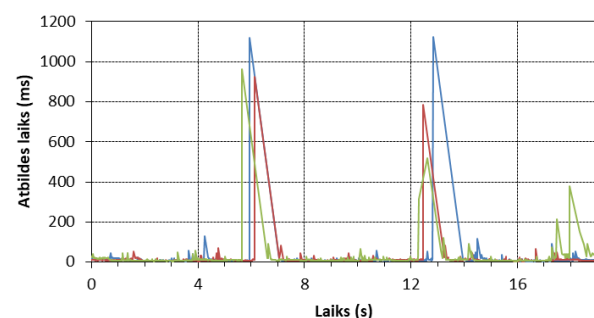
AL caurlaidspēja un atbildes laiks, izmantojot “802.11v tīkla virzītu” (manuālo) pārslēgšanās procedūru, 50 km/h



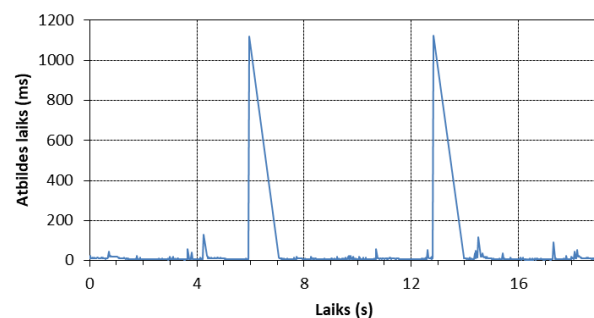
a) Apvienotie mērījumi



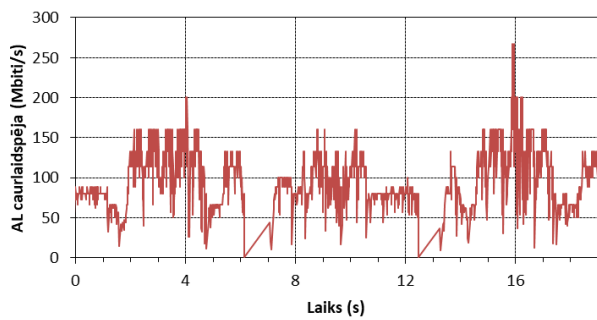
c)



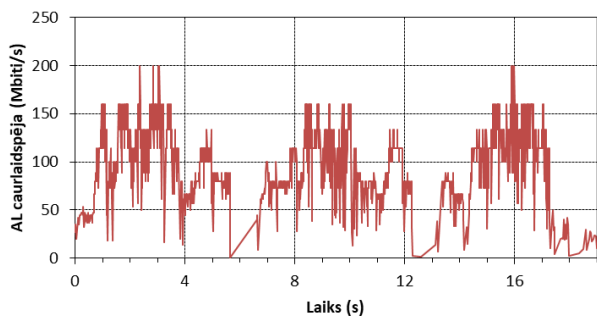
b) Apvienotie mērījumi



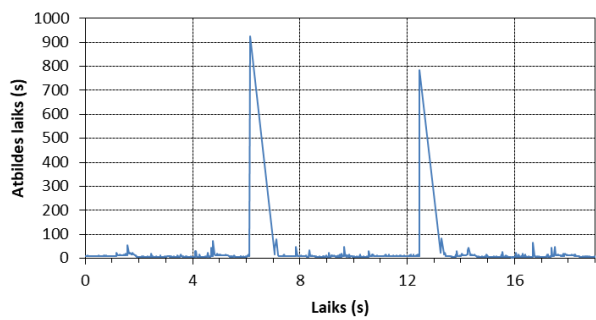
d)



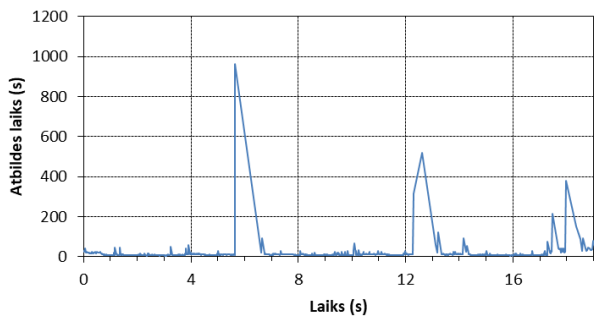
e)



g)



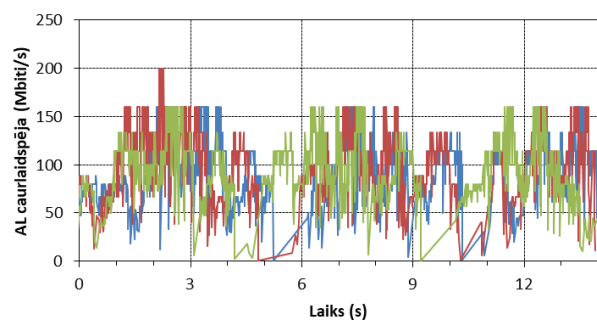
f)



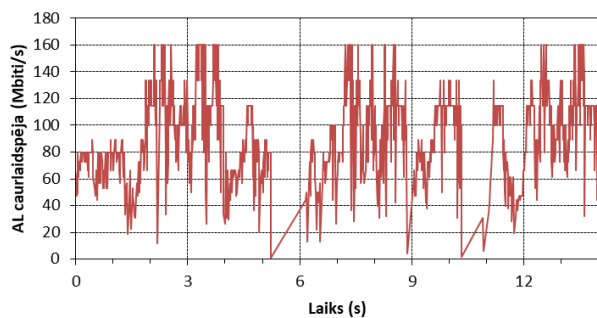
h)

5.9. pielikums

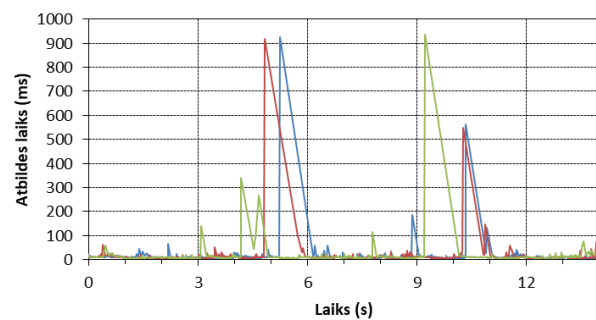
AL caurlaidspēja un atbildes laiks, izmantojot “802.11v tīkla virzītu” (manuālo) pārslēgšanās procedūru, 70 km/h



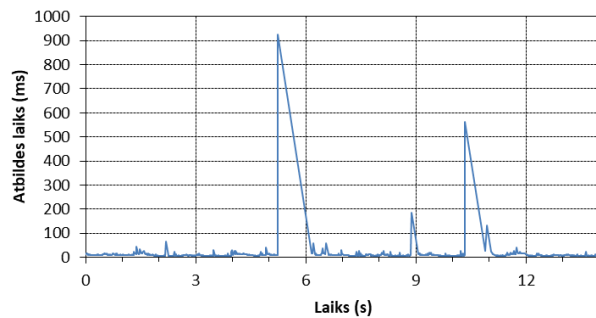
a) Apvienotie mērījumi



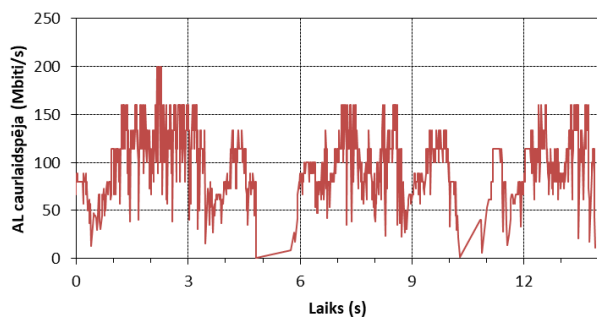
c)



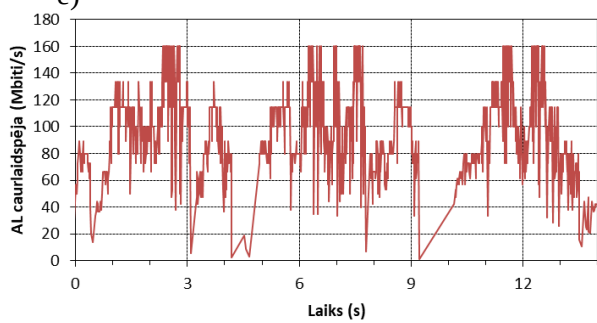
b) Apvienotie mērījumi



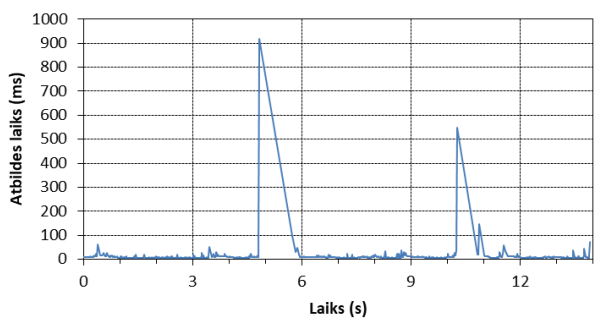
d)



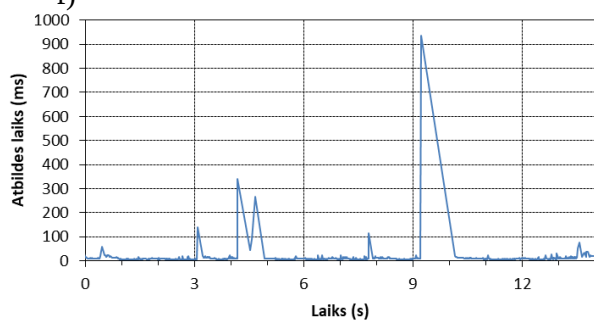
e)



g)



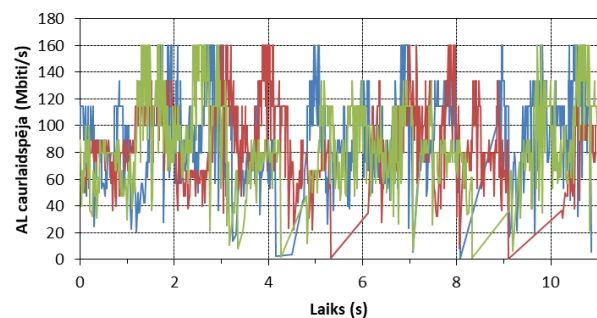
f)



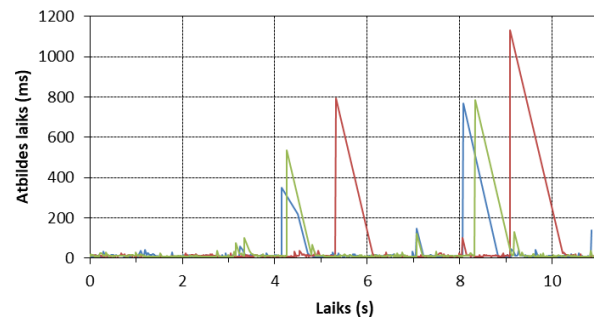
h)

5.10. pielikums

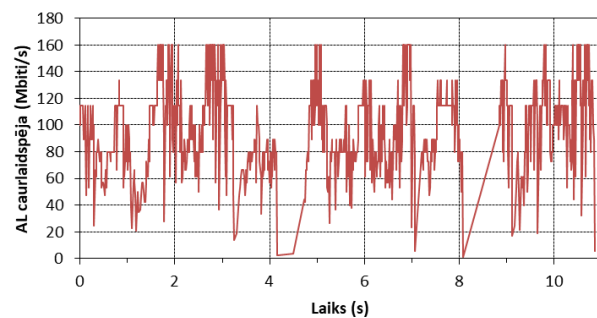
AL caurlaidspēja un atbildes laiks, izmantojot “802.11v tīkla virzītu” (manuālo) pārslēgšanās procedūru, 90 km/h



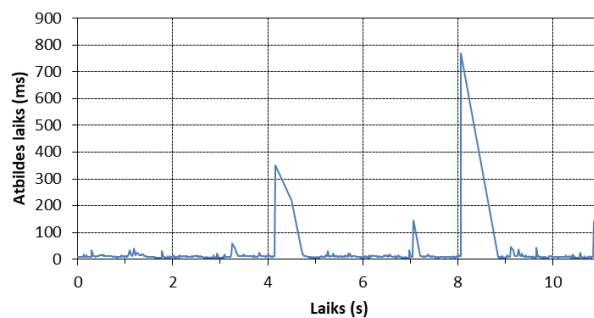
a) Apvienotie mērījumi



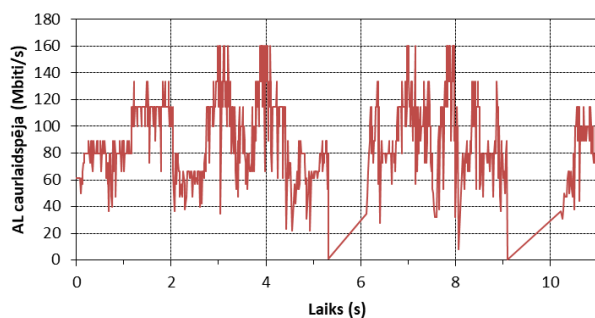
b) Apvienotie mērījumi



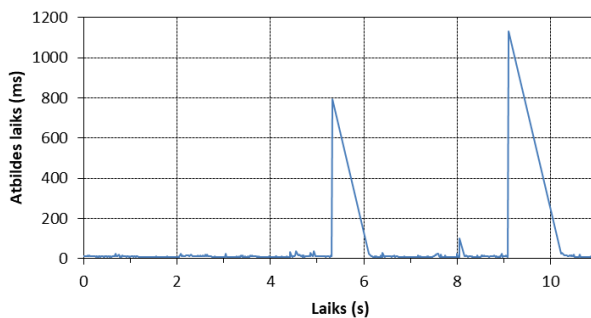
c)



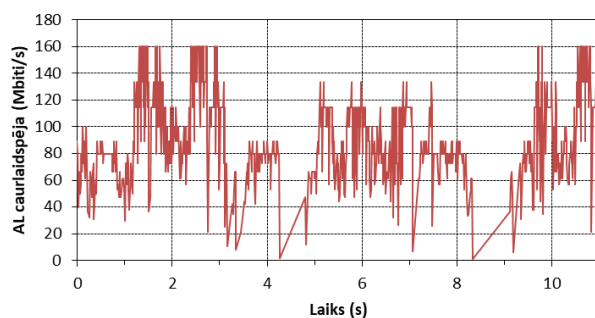
d)



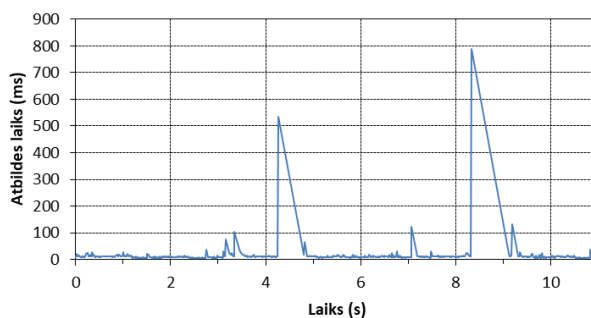
e)



f)



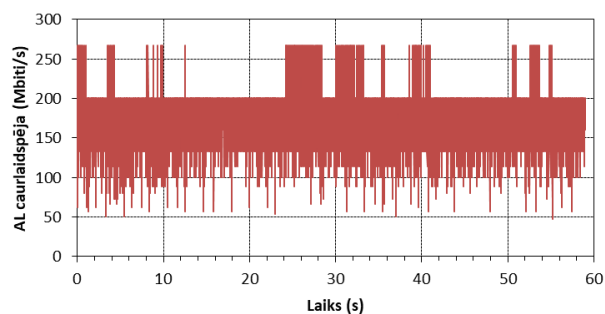
g)



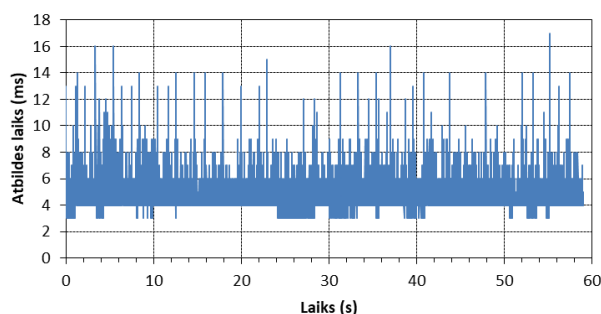
h)

5.11. pielikums

AL caurlaidspēja un atbildes laiks, izmantojot “802.11v tīkla asistētu” pārslēgšanās procedūru, 0 km/h



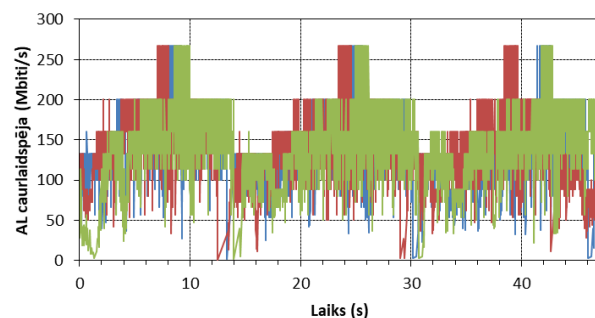
a) Apvienotie mērījumi



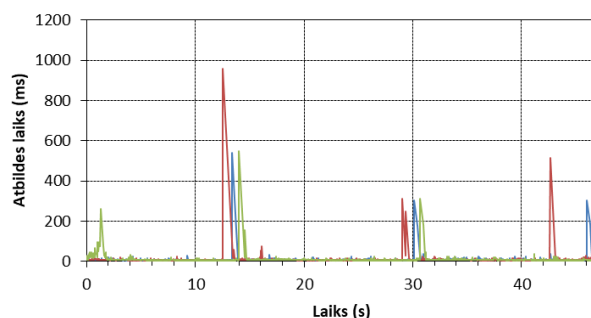
b) Apvienotie mērījumi

5.12. pielikums

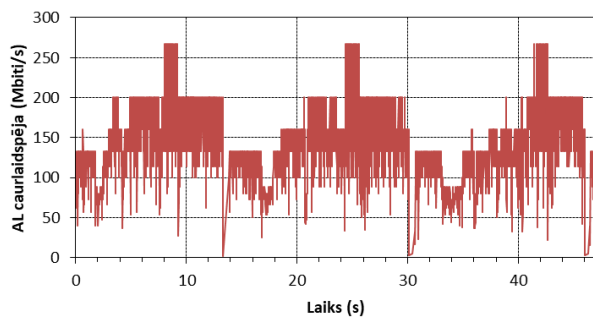
AL caurlaidspēja un atbildes laiks, izmantojot “802.11v tīkla asistētu” pārslēgšanās procedūru, 20 km/h



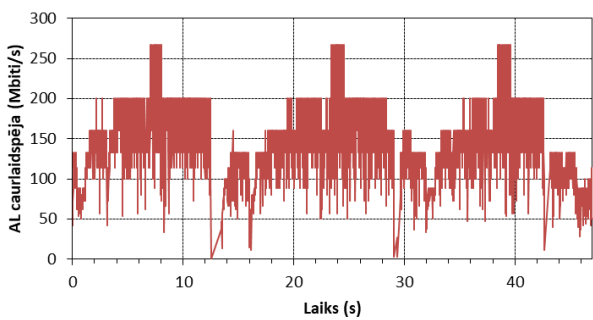
a) Apvienotie mērījumi



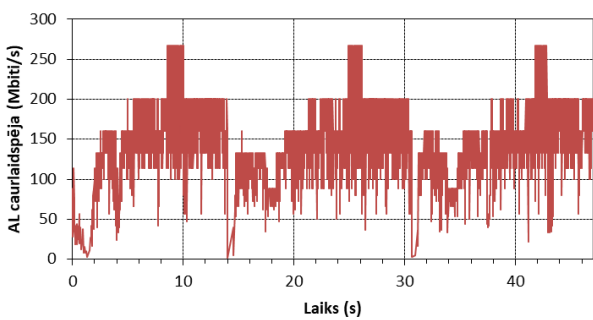
b) Apvienotie mērījumi



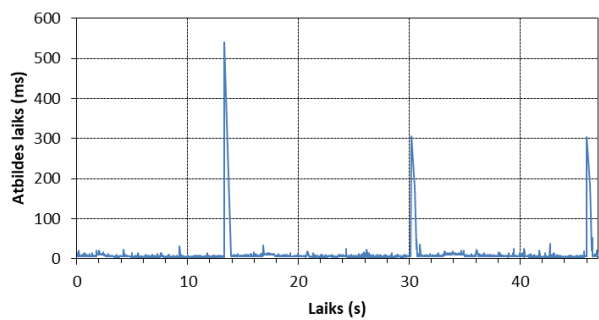
c)



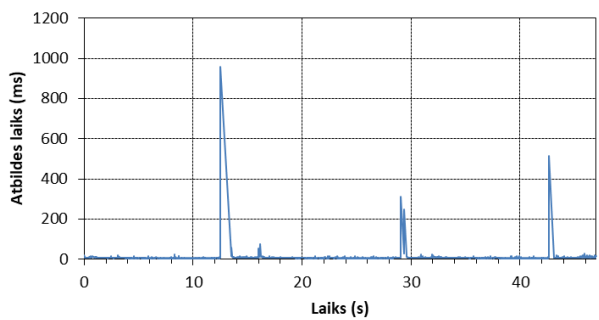
e)



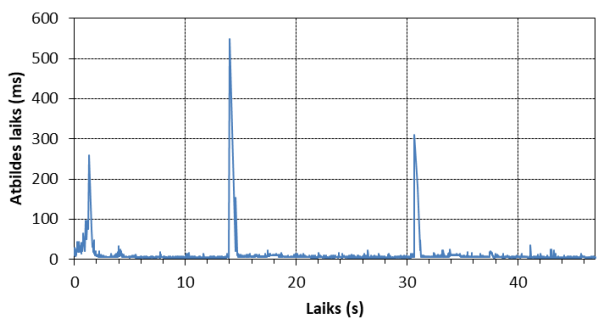
g)



d)



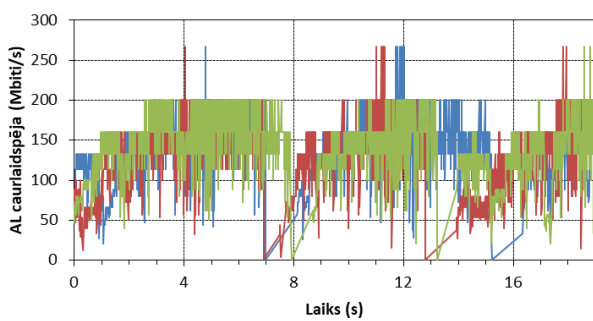
f)



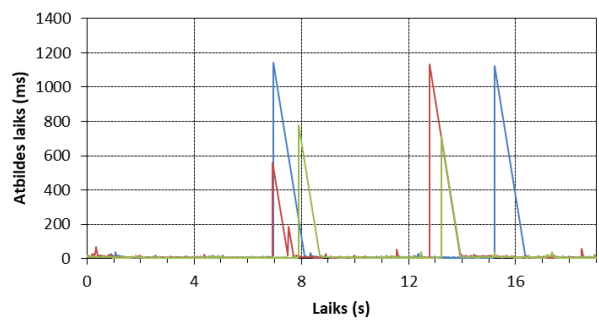
h)

5.13. pielikums

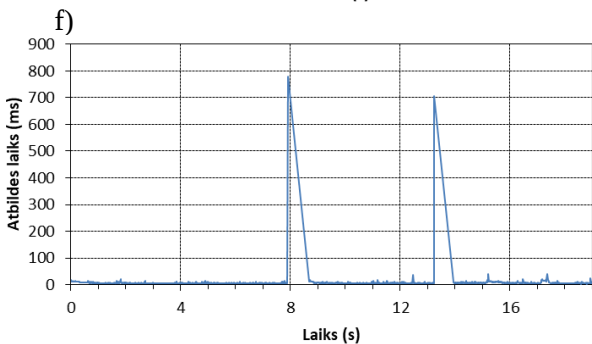
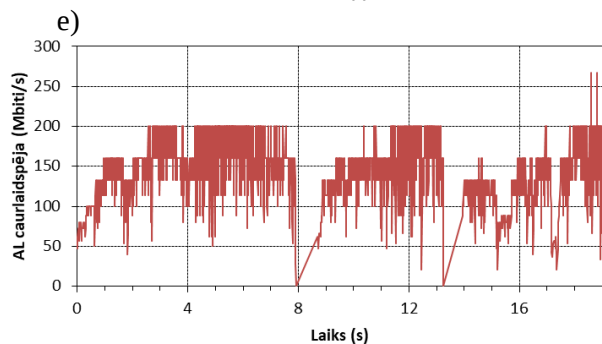
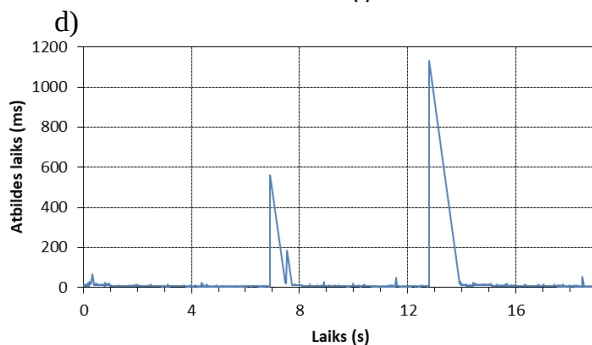
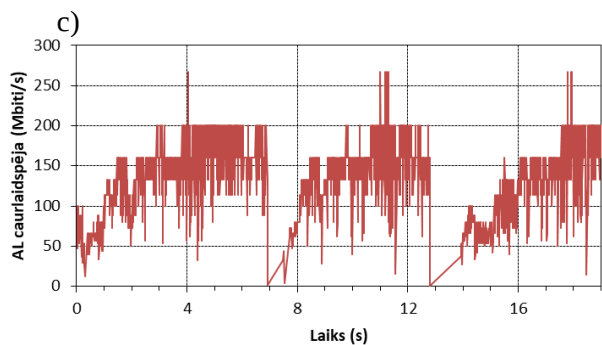
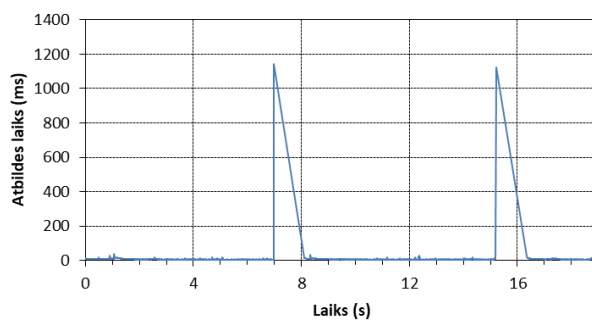
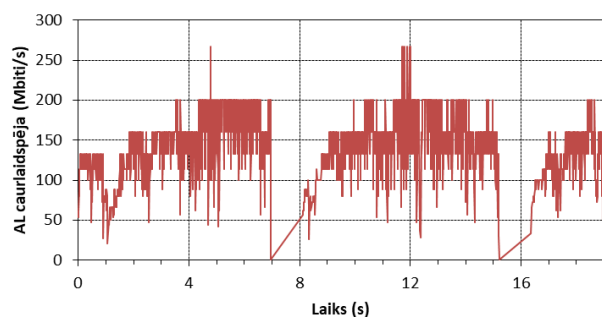
AL caurlaidspēja un atbildes laiks, izmantojot “802.11v tīkla asistētu” pārslēgšanās procedūru, 50 km/h



a) Apvienotie mērījumi



b) Apvienotie mērījumi

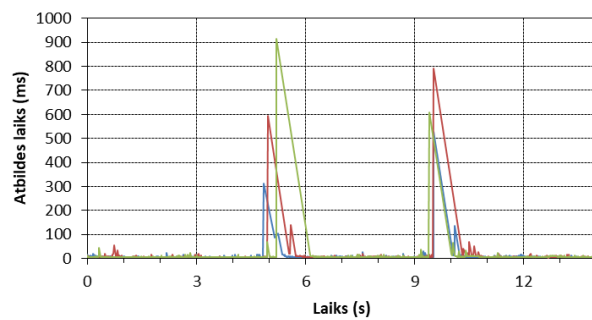
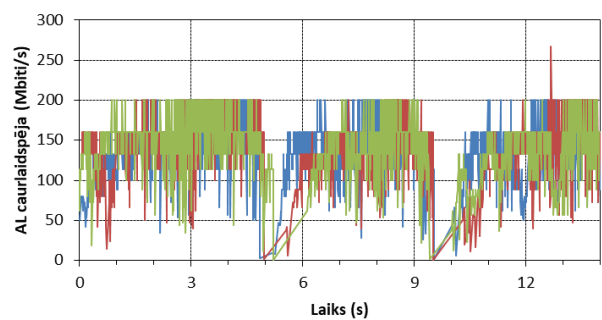


g)

h)

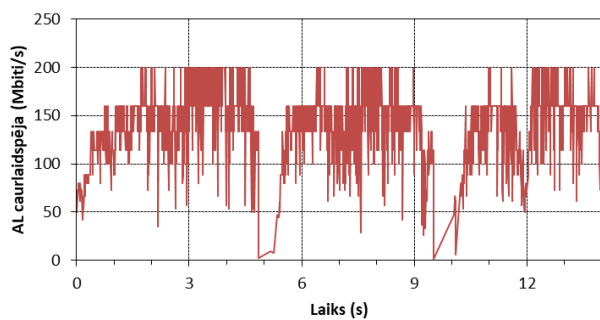
5.14. pielikums

AL caurlaidspēja un atbildes laiks, izmantojot “802.11v tīkla asistētu” pārslēgšanās procedūru, 70 km/h

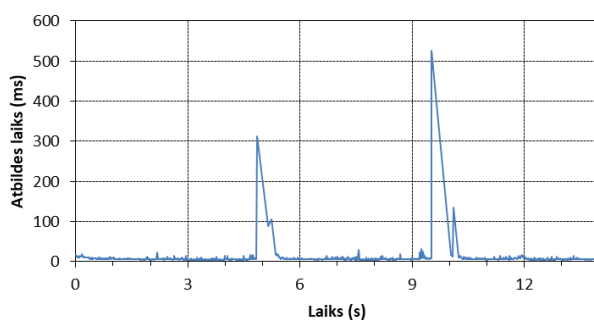


a) Apvienotie mērījumi

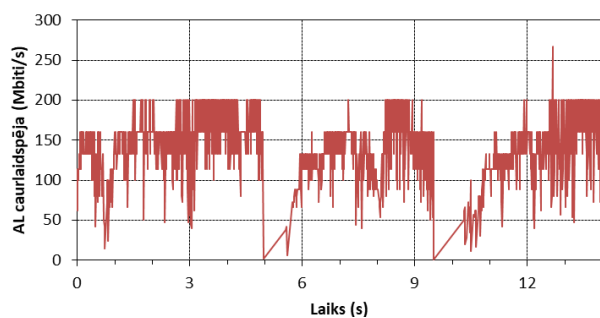
b) Apvienotie mērījumi



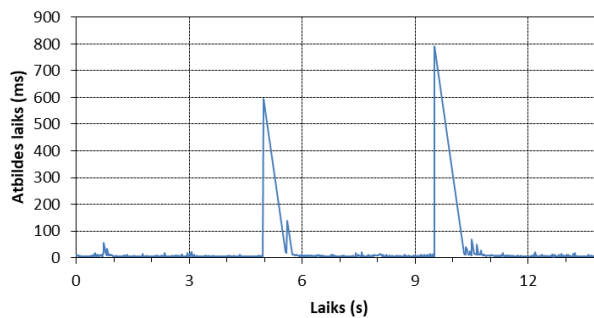
c)



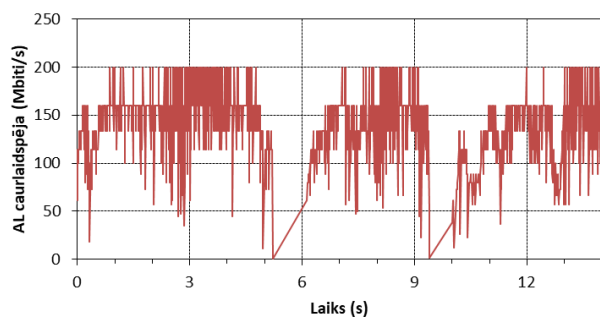
d)



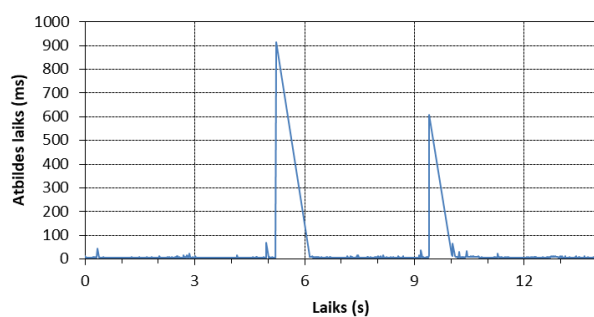
e)



f)



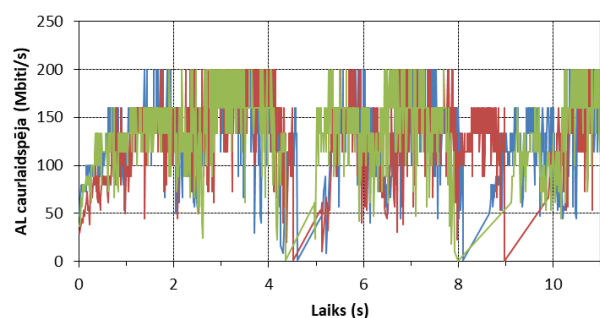
g)



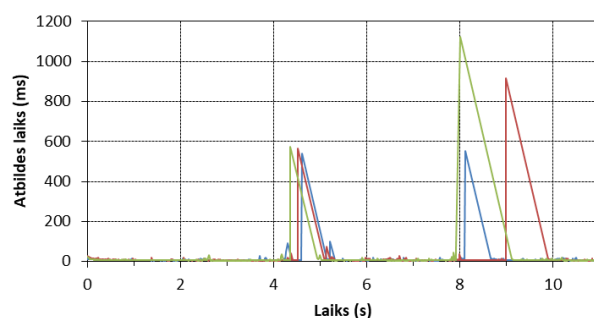
h)

5.15. pielikums

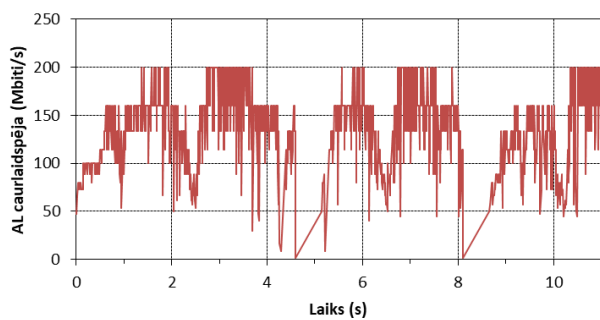
AL caurlaidspēja un atbildes laiks, izmantojot “802.11v tīkla asistētu” pārslēgšanās procedūru, 90 km/h



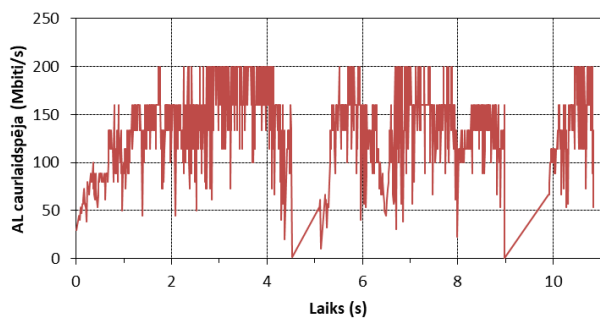
a) Apvienotie mērījumi



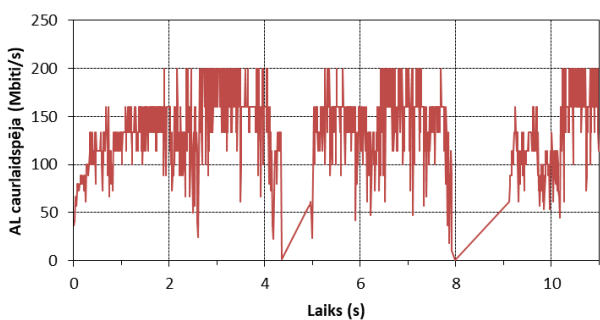
b) Apvienotie mērījumi



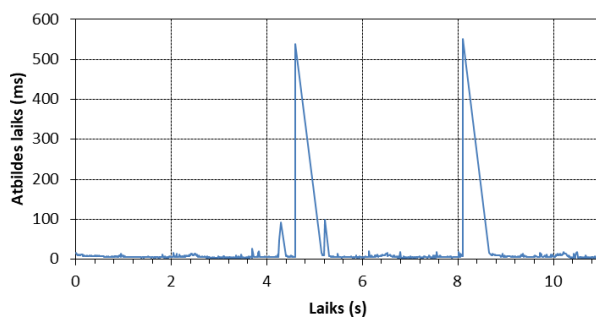
c)



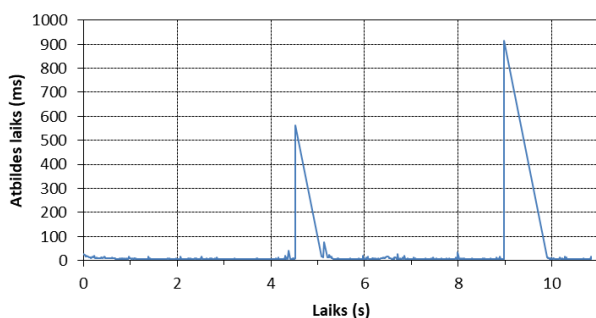
e)



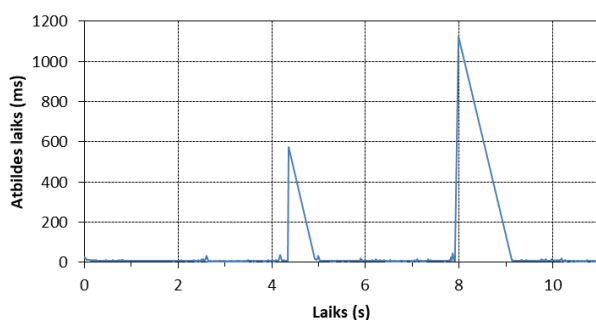
g)



d)



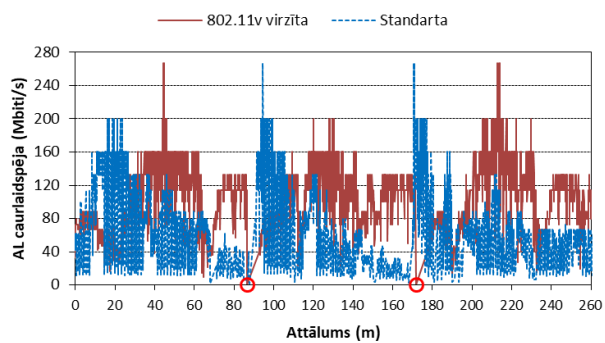
f)



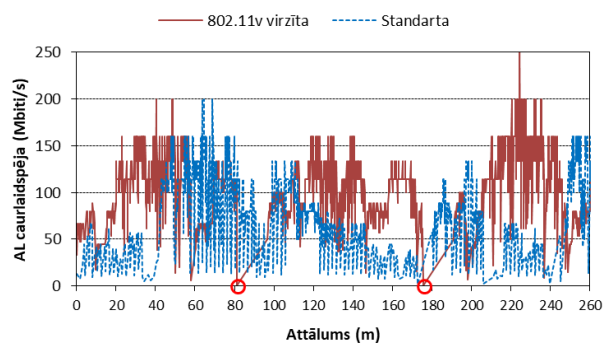
h)

5.16. pielikums

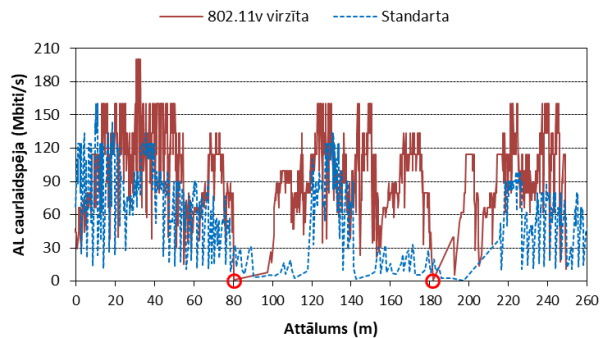
Apvienoti eksperimentāli iegūtie AL caurlaidspējas mērījumu rezultāti, izmantojot “Standarta” un “802.11v tīkla virzītu” (manuālo) pārslēgšanās procedūras metodi, dažādos mobilā klienta pārvietošanās ātrumos



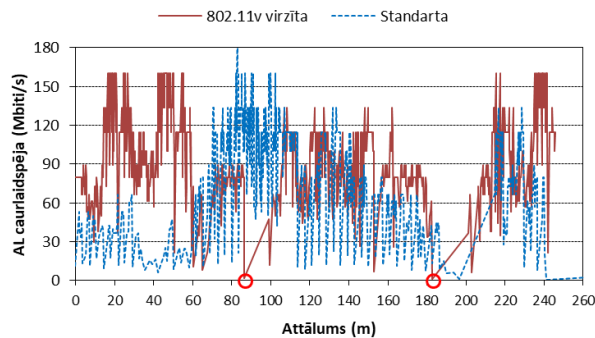
a) 20 km/h



b) 50 km/h



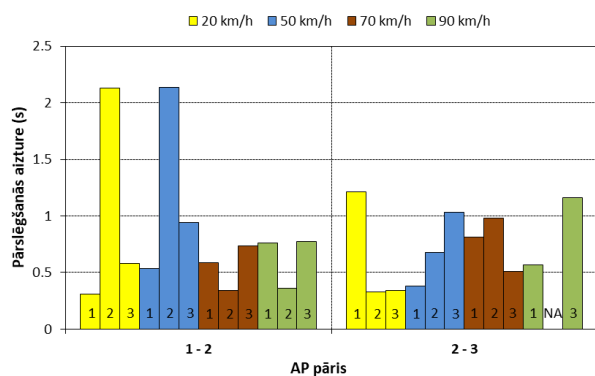
c) 70 km/h



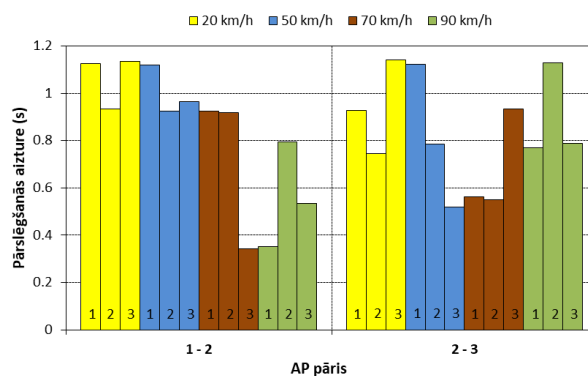
d) 90 km/h

5.17. pielikums

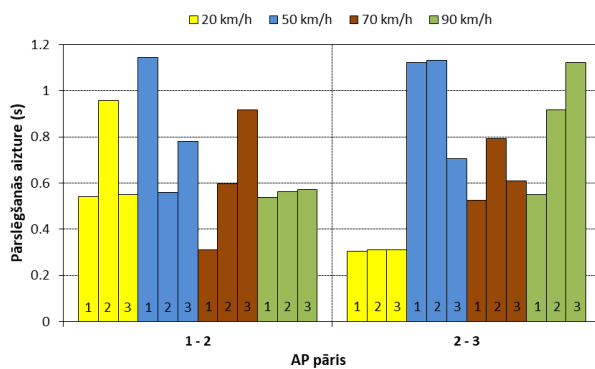
Pārslēgšanās procedūras aiztures starp *AP-1* un *AP-2*, *AP-2* un *AP-3*, izmantojot “Standarta”, “802.11v tīkla virzītu” (manuālo) un “802.11v tīkla asistētu” pārslēgšanās procedūras metodes, kur katrā automobiļa braukšanas ātrumā (20 km/h, 50 km/h, 70 km/h un 90 km/h) tika veikti trīs mērījumi (atzīmēts ar 1, 2, 3)



a) Standarta



b) 802.11v tīkla virzīta (manuālā)



c) 802.11v tīkla asistēta

802.11v BSS pārejas vadības ziņojumi

802.11v BSS pārejas vadības ziņojumi starp klientu un bezvadu piekļuves punktiem AP-2 un AP-3

No.	Time	Source	Destination	Protocol	Length	Info
358	10.687829	Tp-LinkT_56:d4:ec	Tp-LinkT_ae:b5:b4	802.11	57	BSS Transition Management Query
360	10.688511	Tp-LinkT_ae:b5:b4	Tp-LinkT_56:d4:ec	802.11	75	BSS Transition Management Request
380	10.842240	Tp-LinkT_56:d4:ec	Tp-LinkT_ae:b5:b4	802.11	118	BSS Transition Management Response
1048	19.013356	Tp-LinkT_56:d4:ec	Tp-LinkT_bb:a4:99	802.11	57	BSS Transition Management Query
1050	19.014261	Tp-LinkT_bb:a4:99	Tp-LinkT_56:d4:ec	802.11	75	BSS Transition Management Request
1052	19.016333	Tp-LinkT_56:d4:ec	Tp-LinkT_bb:a4:99	802.11	118	BSS Transition Management Response

a) 802.11v “BSS pārejas vadības vaicājuma” ziņojums

```
> Frame 358: 57 bytes on wire (456 bits), 57 bytes captured (456 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Action, Flags: .....C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters
    Category code: WNM (10)
    Action code: BSS Transition Management Query (6)
    Dialog token: 0x01
    BSS Transition Query Reason: Low RSSI (16)
```

b) 802.11v “BSS pārejas vadības pieprasījuma” ziņojums

```
> Frame 360: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Action, Flags: .....C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters
    Category code: WNM (10)
    Action code: BSS Transition Management Request (7)
    Dialog token: 0x01
    ....1 = Preferred Candidate List Included: 1
    ....0. = Abridged: 0
    ....0.. = Disassociation Imminent: 0
    ....0... = BSS Termination Included: 0
    ...0 .... = ESS Disassociation Imminent: 0
    Disassociation Timer: 0
    Validity Interval: 1
    BSS Transition Candidate List Entries: 340db04e26bba499000000000002400
  ▼ Tag: Neighbor Report
    Tag Number: Neighbor Report (52)
    Tag length: 13
    BSSID: Tp-LinkT_bb:a4:99 (b0:4e:26:bb:a4:99)
  > BSSID Information: 0x00000000
    Operating Class: 0
    Channel Number: 36 (iterative measurements on that Channel Number)
    PHY Type: 0x00
```

c) 802.11v “BSS pārejas vadības atbildes” ziņojums

```
> Frame 380: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Action, Flags: .....C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters
    Category code: WNM (10)
    Action code: BSS Transition Management Response (8)
    Dialog token: 0x01
    BSS Transition Status Code: 0
    BSS Termination Delay: 0
    BSS Transition Target BSS: Tp-LinkT_bb:a4:99 (b0:4e:26:bb:a4:99)
    BSS Transition Candidate List Entries: 3410b04e26aeb5b4020c00008024090301ff3410b04e26bb...
  ▼ Tag: Neighbor Report
    Tag Number: Neighbor Report (52)
    Tag length: 16
    BSSID: Tp-LinkT_ae:b5:b4 (b0:4e:26:ae:b5:b4)
    > BSSID Information: 0x00000c02
      Operating Class: 128
      Channel Number: 36 (iterative measurements on that Channel Number)
      PHY Type: 0x09
    > Subelement: BSS Transition Candidate Preference
  ▼ Tag: Neighbor Report
```

Matlab kodi uztvertā signāla jaudas līmeņa un caurlaidspējas aprēķiniem

a) Uztvertā signāla jaudas zudumu P atkarība no attāluma r līdz raidītājam

```
d0 = 3.5; % m
Pd0 = -49; % dBm
u = 1.9;
sigma = 5.9; % dB
r=(0:0.5:100)'; % m
alfa = 1;
w = 1;

fun = @(x) x.*(2.*alfa.^alfa.*x.^(2.*alfa-1)/(w.^alfa.*(factorial(alfa)))).*
exp((-alfa.*x.^2)./w);
Xsigma = integral(fun,0,Inf);

rng(0,'twister');
Xshad = sigma.*randn(201,1) + Xsigma;
Xfade = abs(randn(201,1) + 1i*randn(201,1));
Xsigma_rand = Xshad + sigma*10*log10(Xfade);
Pr = Pd0 - 10*u*log10(r/d0); % dBm
PrX_rand = Pd0 - 10*u*log10(r/d0) + Xsigma_rand; % dBm
```

b) Caurlaidspējas aprēķināšana ideālam kanālam atkarībā no attāluma r līdz raidītājam

```
B = 80; % MHz
N = -90; % dBm

Pr2 = 10.^(Pr./10); % mW
N2 = 10^(N/10); % mW
C = B.*log2(1+Pr2./N2); % Mbiti/s
PrX2_rand = 10.^(PrX_rand./10); % mW
CX2_rand = B.*log2(1+PrX2_rand./N2); % Mbiti/s
```

Testgultnes specififikācijas dati un mērījumu iestatījumi

a) Testgultnē izmantotā aprīkojuma specififikācija

Aprīkojums	Specifikācija
4G LTE maršrutētājs	Cisco C819G-4G-G-K9; Huawei E5186s-22a; Cisco IR809G-LTE-GA-K9 (atkarībā no eksp.)
Bezvadu tīkla kontrolieris	HP MSM720 (atkarībā no eksp.)
Bezvadu piekļuves punkts	HP MSM460 (3 gab.); TP-Link Archer C7 AC1750 (V2, 1. gab.; V4, 3 gab.) (atkarībā no eksp.)
Nepārtrauktās elektrobarošanas iekārtas	APC UPS 500 VA (3 gab.); APC UPS 1400 VA (1 gab.)
Attālinātais serveris 1	Intel Xeon E5335 CPU 2,0 GHz, 4 GB RAM, 64-bit OS Windows Server 2008 R2 Standard
Attālinātais serveris 2	HP ProBook 430 G2, Intel Core i5-5200U CPU 2,2 GHz, 8 GB RAM, HDD 500 GB, 64-bit OS W7
Mobilais klients 1	EliteBook 840 G1, Intel Core i5-4310U CPU 2,0 GHz, 8 GB RAM, SSD 128 GB, 64-bit OS W7, Intel Dual Band Wireless-N 7260 WNIC
Mobilais klients 2	EliteBook 8470p, Intel Core i5-3360M CPU 2,8 GHz, 4 GB RAM, SSD 128 GB, 64-bit OS W7, Intel Centrino Advanced-N 6205 WNIC
Automobilis	VW e-UP!; Volvo S40 (atkarībā no eksp.)

b) Eksperimentālo mērījumu galvenie iestatījumi

Parametrs	Vērtība
Bezvadu tehnoloģija	IEEE 802.11n/ac
Frekvenču kanāli	fiksēti
Frekvenču kanālu platums	20 MHz; 80 MHz (atkarībā no eksp.)
Frekvenču diapazons	5 GHz
Raidītāja jauda (EIRP)	5 dBm; adaptīva (atkarībā no eksp.)
Klienta pārslēgšanās procedūras RSS sliekšņvērtība	noklusētā; -62 dBm (atkarībā no eksp.)
Ethernet savienojumu datu pārraides ātrums	līdz 1 Gbit/s
Bezvadu piekļuves punktu maksimālais nodrošinātais datu pārraides ātrums	līdz 450 Mbit/s; līdz 1300 Mbit/s (atkarībā no eksp.)
LTE lejupielādes datu pārraides ātrums (otrais rangs)	līdz 100 Mbit/s; līdz 300 Mbit/s (atkarībā no eksp.)
MIMO pārraides iestatījumi	automātisks (3 × 3 : 3)
OFDM aizsargintervāls	400 ns
Nosūtāmā faila izmērs	100000 baiti
Transporta līmeņa protokols	TCP
IP adresācija Wi-Fi tīklā	fiksēta, privātā
SSID klientu autentifikācija	atslēgta; ieslēgta (atkarībā no eksp.)
Programmatūra trafika ģenerēšanai un analīzei	IxChariot v. 6.70; iPerf 3.1.2 (atkarībā no eksp.)
Klienta pārvietošanās ātrums	20 km/h; 40 km/h; 50 km/h; 60 km/h; 70 km/h; 90 km/h (atkarībā no eksp.)

IEEE 802.11n/ac standartu specifikācijaa) *IEEE 802.11n/ac* standartu kopsavilkums [62]

IEEE standarts	Frekvenču josla, GHz	Frekvenču kanāla platums, MHz	Modulācija	Telpiski atdalītu plūsmu skaits	Maksimālais datu pārraides ātrums
<i>802.11n</i>	2,4 vai 5	20 vai 40	<i>BPSK, QPSK, 16-QAM, 64-QAM</i>	1–4	600 Mbiti/s
<i>802.11ac</i>	5	20, 40, 80, 160	<i>BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM</i>	1–8	6,933 Gbiti/s

b) IEEE 802.11n / HT MCS un IEEE 802.11ac / VHT MCS standartu datu pārraides ātrumu specifikācija līdz trīs telpiski atdalītām plūsmām [139]

HT MCS	VHT MCS	Modulācija	Kodēšana	20 MHz				40 MHz				80 MHz				160 MHz			
				Pārraides ātrums*		Min. SNR	RSSI	Pārraides ātrums		Min. SNR	RSSI	Pārraides ātrums		Min. SNR	Pārraides ātrums		Min. SNR	RSSI	
				800 ns**	400 ns			800 ns	400 ns			800 ns	400 ns		800 ns	400 ns			
viena telpiski atdalīta plūsma																			
0	0	BPSK	1/2	6,5	7,2	2	-82	13,5	15	5	-79	29,3	32,5	8	-76	58,5	65	11	-73
1	1	QPSK	1/2	13	14,4	5	-79	27	30	8	-76	58,5	65	11	-73	117	130	14	-70
2	2	QPSK	3/4	19,5	21,7	9	-77	40,5	45	12	-74	87,8	97,5	15	-71	175,5	195	18	-68
3	3	16-QAM	1/2	26	28,9	11	-74	54	60	14	-71	117	130	17	-68	234	260	20	-65
4	4	16-QAM	3/4	39	43,3	15	-70	81	90	18	-67	175,5	195	21	-64	351	390	24	-61
5	5	64-QAM	2/3	52	57,8	18	-66	108	120	21	-63	234	260	24	-60	468	520	27	-57
6	6	64-QAM	3/4	58,5	65	20	-65	121,5	135	23	-62	263,3	292,5	26	-59	526,5	585	29	-56
7	7	64-QAM	5/6	65	72,2	25	-64	135	150	28	-61	292,5	325	31	-58	585	650	34	-55
-	8	256-QAM	3/4	78	86,7	29	-59	162	180	32	-56	351	390	35	-53	702	780	38	-50
-	9	256-QAM	5/6	-	-	31	-57	180	200	34	-54	390	433,3	37	-51	780	866,7	40	-48
divas telpiski atdalītas plūsmas																			
8	0	BPSK	1/2	13	14,4	2	-82	27	30	5	-79	58,5	65	8	-76	117	130	11	-73
9	1	QPSK	1/2	26	28,9	5	-79	54	60	8	-76	117	130	11	-73	234	260	14	-70
10	2	QPSK	3/4	39	43,3	9	-77	81	90	12	-74	175,5	195	15	-71	351	390	18	-68
11	3	16-QAM	1/2	52	57,8	11	-74	108	120	14	-71	234	260	17	-68	468	520	20	-65
12	4	16-QAM	3/4	78	86,7	15	-70	162	180	18	-67	351	390	21	-64	702	780	24	-61
13	5	64-QAM	2/3	104	115,6	18	-66	216	240	21	-63	468	520	24	-60	936	1040	27	-57
14	6	64-QAM	3/4	117	130,3	20	-65	243	270	23	-62	526,5	585	26	-59	1053	1170	29	-56
15	7	64-QAM	5/6	130	144,4	25	-64	270	300	28	-61	585	650	31	-58	1170	1300	34	-55
-	8	256-QAM	3/4	156	173,3	29	-59	324	360	32	-56	702	780	35	-53	1404	1560	38	-50
-	9	256-QAM	5/6	-	-	31	-57	360	400	34	-54	780	866,7	37	-51	1560	1733,3	40	-48
trīs telpiski atdalītas plūsmas																			
16	0	BPSK	1/2	19,5	21,7	2	-82	40,5	45	5	-79	87,8	97,5	8	-76	175,5	195	11	-73
17	1	QPSK	1/2	39	43,3	5	-79	81	90	8	-76	175,5	195	11	-73	351	390	14	-70
18	2	QPSK	3/4	58,5	65	9	-77	121,5	135	12	-74	263,3	292,5	15	-71	526,5	585	18	-68
19	3	16-QAM	1/2	78	86,7	11	-74	162	180	14	-71	351	390	17	-68	702	780	20	-65
20	4	16-QAM	3/4	117	130	15	-70	243	270	18	-67	526,5	585	21	-64	1053	1170	24	-61
21	5	64-QAM	2/3	156	173,3	18	-66	324	360	21	-63	702	780	24	-60	1404	1560	27	-57
22	6	64-QAM	3/4	175,5	195	20	-65	364,5	405	23	-62	-	-	26	-59	1579,5	1755	29	-56
23	7	64-QAM	5/6	195	216,7	25	-64	405	450	28	-61	877,5	975	31	-58	1755	1950	34	-55
-	8	256-QAM	3/4	234	260	29	-59	486	540	32	-56	1053	1170	35	-53	2106	2340	38	-50
-	9	256-QAM	5/6	260	288,9	31	-57	540	600	34	-54	1170	1300	37	-51	-	-	40	-48

* datu pārraides ātrums, Mbit/s

** aizsargintervāls