KLAIPĖDOS UNIVERSITETAS

Jūrų technikos fakultetas

Informatikos inžinerijos katedra

EISMO SAUGUMO, INFORMACINIŲ IR MULTIMEDIJA PASLAUGŲ TEIKIMAS AUTOMOBILIŲ KOMUNIKACIJOS TINKLUOSE

SAFETY, INFORMATION AND MULTIMEDIA APPLICATIONS SUPPORT IN VEHICULAR COMMUNICATION NETWORKS

Techninių informacinių sistemų inžinerijos specialybės magistro baigiamasis darbas

Autorius: TMII-09, Mindaugas Kurmis

Vadovas: prof. dr. Arūnas Andziulis

Klaipėda, 2011

ANOTACIJA

Automobilių komunikacijos bevieliai tinklai yra viena iš sparčiausiai augančių ir daugiausiai mokslinės bendruomenės dėmesio sulaukiančių mobiliųjų technologijų. Ši nauja platforma automobiliuose leidžia teikti eismo saugumo, informacines bei multimedija paslaugas, leidžiančias keliones padaryti saugesnėmis bei komfortiškesnėmis. Šiuo metu pagrindinės automobilinės komunikacijos sritys, reikalaujančios gilesnių mokslinių tyrimų: eismo saugumo, informacinių bei multimedija paslaugų teikimas, skirtingų bevielio ryšio technologijų panaudojimas bei integravimas, privatumas ir saugumas automobilinės komunikacijos tinkluose. Šiame darbe tiriamos eismo saugumo, informacinių ir multimedija paslaugų teikimo galimybės bei perspektyvos. Atlikta išsami tiriamos srities literatūros analizė, pateikiama imitacinio modeliavimo programinės įrangos analizė. Atlikti eismo saugumo, informacinių ir multimedija paslaugų teikimo automobilių komunikacijos tinkluose tyrimai: AODV ir ADV ad-hoc maršrutizavimo protokolų efektyvumo; ryšio efektyvumo siuntėjui ir gavėjui judant priešingomis kryptimis automagistralėje; 802.11b, 802.11p ir 802.16e technologijų panaudojimo. Taip pat, sukurta nauja, pasitikėjimu grindžiama, autentifikavimo schema informacinių bei multimedija paslaugų teikimo apsaugojimui automobilinėje komunikacijoje.

Raktiniai žodžiai: VANET, automobilių komunikacijos tinklai, eismo saugumo, informacinės, multimedija paslaugos, maršrutizavimas, ad-hoc, 802.11p, V2I, V2V.

ABSTRACT

Vehicular communication networks are of the fastest growing and one of the most attention gaining mobile technologies. This new platform enables a plethora of communication-based automotive applications including road safety, information and multimedia which can make travel more safe and comfortable. At the moment, the main vehicular communication areas which need deeper scientific analysis are: road safety, information and multimedia service support, integration and employment of different wireless technologies, privacy and security in vehicular communication networks. In this work it is investigated road safety, information and multimedia service support opportunities and prospects. It was made deep analysis of literature, presented simulation software analysis. It was made road safety, information and multimedia service support in vehicular communication networks: AODV and ADV ad-hoc routing protocols performance; communication efficiency when sender and recipient are moving in opposite directions in highway; employment of 802.11b, 802.11p ir 802.16e technologies. Also it is presented new trust based authentication scheme for information and multimedia service support safety in vehicular communication.

Keywords: VANET, vehicular communication networks, road safety, informatikon, multimedia service, routing, ad-hoc, 802.11p, V2I, V2V.

SANTRUMPŲ IR TERMINŲ ŽODYNĖLIS

A

Ad-hoc – tinklo tipas, kai bevielio tinklo klientai vieni su kitais komunikuoja tik tiesiogiai „taškas į tašką“.

AC (angl. *Access* categories) – prieigos kategorijos.

ADSL (angl. *Asymmetric Digital Subscriber Line*) - asimetrinė skaitmeninė kliento linija.

ADV (angl. *Adaptive Distance Vector*) – ad-hoc maršrutizavimo protokolas. Tai hibridinis protokolas, turintis ir aktyviojo ir proaktyviojo savybių. Pagrindinės charakteristikos yra proaktyviojo, kadangi maršrutai yra atnaujinami nuolat.

AIFS (angl. *arbitration inter-frame space*) – arbitrinė kadro erdvė. Tai prieigos klasės prioritetų nustatymo metodas.

AP (angl. *Access Point*) – įrenginys skirtas bevielio vietinio tinklo įrenginių komunikavimui.

API (angl. *application programming interface*) – aplikacijų programavimo sąsaja.

AODV (angl. *On-Demand Distance Vector*) – tai reaktyvusis protokolas, kuriame maršrutai sudaromi tik tada kai reikia persiųsti duomenis. Jis prisitaiko prie dinaminių ryšio sąlygų ir tuo pačiu reikalauja nedidelių skaičiavimo ir atminties resursų.

B

BS (angl. *base station*) – bazinė stotis.

BWA (angl. *broadband wireless access*) – plačiajuosčio ryšio belaidė prieiga.

C

C2C-CC (angl. *CAR 2 CAR Communication Consortium*) – automobilio su automobiliu ryšio konsorciumas.

C3 (angl. *Car-to-Car Cooperation*) – automobilio su automobiliu kooperacija.

CA (angl. *car agent*) – automobilio agentas.

CDMA (angl. *code-division multiple access technology*) – kodo padalijimo daugialypės prieigos technologija.

CEPEC (angl. *coordinated external peer communication*) – valdomas kanalo prieigos protokolas.

CEPT (angl. *European Conference of Postal and Telecommunications Administrations*) – Europos pašto ir telekomunikacijų administracijos konferencija.

CPE (angl. *customer premise equipment*) kliento patalpos įranga.

CRN (angl. *cognitive radio networks*) – kognityvūs radijo ryšio tinklai.

CTS (angl. *clear-to-send*) – patvirtinimas siųsti.

CSMA/CD (*Carrier sence multiple Access with collision avoidance*) – protokolas, numatantis kolizijų išvengimo būdą, kurio esmė yra papildomų duomenų paketų panaudojimas

CW (angl. *contention window*) – konkuravimo langas.

D

DSL (angl. *Digital Subscriber Line*) – skaitmeninio prisijungimo linija.

DSM (angl. *Distributed Sorting Mechanism*) – paskirstytas rūšiavimo mechanizmas.

DSRC (angl. *Dedicated Short Range Communications*) – dedikuota trumpo nuotolio komunikacija.

DSSS (*Direct sequence spread spectrum*) – tiesioginės tvarkos skleisto spektro technologija.

DVB-T (angl. *Digital Video Broadcast Terrestial*) – skaitmeninė antžeminė televizija.

DTRA (angl. *dynamic transmission-range-assignment*) dinaminis perdavimo diapazono priskyrimas.

E

EAP (angl. *extended authentication protocol*) – išplėstas autentifikavimo protokolas.

EDCA (angl. *Enhanced Distributed Channel Access*) – praplėsta paskirstyta kanalo prieiga.

EDGE (angl. *Enhanced Data rates for GSM Evolution*) – skaitmeninė mobiliųjų telefonų technologija, skirta pagerinti duomenų persiuntimą.

Ethernet – kompiuterių tinklų technologija lokaliems tinklams

EvDo (angl. *Evolution Data only*) – tik evoliuciniai duomenys.

EvDv (angl. *Evolution-Data/Voice*) – evoliuciniai duomenys, balsas.

exposed terminals – atskleistieji terminalai.

F

FCC (angl. *Federal Communications Commission*) – federalinė komunikacijų komisija.

FHSS (angl. *Frequency hopping spread spectrum*) – dažnio šokinėjimo skleisto spektro technologija.

G

GPRS (angl. *General Packet Radio Service*) – bendras paketinis radijo ryšys.

GPS (angl. *Global Positioning System*) – visuotinė padėties nustatymo sistema, arba globali pozicionavimo sistema, leidžianti nustatyti objekto koordinates bet kurioje pasaulio vietoje.

GSK (angl. *Group session key*) – grupės sesijos raktas.

GUI (angl. *Graphical User Interface*) – grafinė vartotojo sąsaja.

H

hidden terminals – paslėpti terminalai.

HSPA+ (angl. *High Speed Packet Access*) – didelio greičio paketinė prieiga, leidžianti pasiekti 42 Mb/s gavimo ir 22 Mb/s išsiuntimo spartą mobiliojo ryšio tinkluose.

I

I2V (angl. *infrastructure to vehicle*) – infrastruktūros su automobiliu

IEEE (angl. *Institute of Electrical and Electronics Engineers*) – elektros bei elektronikos inžinierių institutas yra tarptautinė profesionali organizacija, užsiimanti technologijų pažanga

IEEE 1609 – bevielės prieigos automobilinėje aplinkoje standartų šeima.

IEEE 802.11 – standartų rinkinys, skirtas bevielių vietinių tinklų diegimui 2,4, 3,6 ir 5 GHz dažnių juostose.

IEEE 802.11p – tai IEEE 802.11 standartų patobulinimas, pritaikant juos bevielei prieigai automobilinėje aplinkoje 5,9 GHz dažnių juostoje. Standartas remiasi aukštesnio lygmens IEEE 1609.

IEEE 802.15.4 – standartas, aprašantis fizinį ir MAC sluoksnius žemos spartos bevieliuose personaliniuose tinkluose.

IEEE 802.16 – bevielės plačiajuostės prieigos standartų rinkinys.

IP (angl. *Internet protocol*) – Interneto protokolas. Tai tinklinio lygmens protokolas, pernešantis duomenis tarp tinklo ir vartotojo įrangos.

IPTV – televizijos paslauga, skirta transliuoti ir priimti televizinius signalus paketiniu duomenų perdavimu, panaudojant interneto protokolą (IP).

ITS (angl. *Intelligent transportation system*) – protingos transportavimo sistemos.

L

LAN (angl. *Local Area Network*) – vietinis lokalus tinklas

LLC (angl. *Logical link control*) – antrojo *OSI* modelio sluoksnio, skirto duomenų komunikavimui, posluoksnis leidžiantis nesudėtingą „*Bridge*“ tipo maršrutizavimą tarp bevielių bei laidinių „*Ethernet*“ tinklų

M

MAC (angl. *Medium Access Control*) – terpės prieigos valdymas.

MAN (angl. *Metropolitan Area Network*) – tinklas, apimantis miesto teritoriją.

MANET (angl. *mobile ad hoc network*) – mobilus *ad-hoc* tinklas.

Maršrutizatorius (angl. *Router*) – įrenginys, kuris perduoda ar paskirsto duomenų paketus per kompiuterių tinklus.

MCP (angl. *Maximum Coverage Problem*) – maksimalios aprėpties problema.

MIMO (angl. *Multiple input multiple output*) – keleto antenų naudojimas siuntimui bei priėmimui, siekiant pagerinti įrenginio savybes.

Multimedija – daugialypė terpė, kuri apima kelių tipų informaciją (garso, vaizdo, teksto ir kt.).

N

NIC (angl. *network interface card*) – tinklo sąsajos plokštė.

NLOS (angl. *non-line-of-sight*) – netiesioginis matomumas.

node-movement-scenario configuration - judėjimo scenarijaus konfigūracija

O

OBU (angl. *on board unit*) – borto įrenginys.

OFDM (angl. *Orthogonal frequency-division multiplexing*) – stačiakampis dažnių tankinimo moduliacijos metodas, naudojamas kaip skaitmeninis daugialinijinis informacijos nešėjas

OEM (angl. *original equipment manufacturer*) – originalus įrangos gamintojas.

OSI modelis (angl. *Open Systems Interconnection Reference Model*) – abstraktus ryšio protokolų, naudojamų ryšio ir kompiuteriniuose tinkluose, aprašymas

OTRP (angl. *overlay token ring protocol*) – uždengtas žiedinio tinklo protokolas.

P

PER (angl. *packet error rate*) – paketų klaidų kiekis.

PMP (angl. *point-to-multi-point*) – vieno taško su daug taškų tinklo architektūra.

packet drop attack – paketų atmetimo ataka.

PMK (angl. *Pairwise Master Key*) – porinis pagrindinis raktas.

PTK (angl. *pairwise transient key*) – porinis trumpalaikis raktas.

Q

QoS (angl. *Quality of Service*) – sąvoka, žyminti paslaugos kokybės rodiklį.

R

RERR (angl. Route Error) – kelio klaida.

RFID (angl. *radio-frequency identification*) – radijo dažnio identifikacija.

RREQ (angl. Route Request) – kelio prašymas.

RREP (angl. Route Reply) – kelio atsakymas.

RS (angl. *relay station*) – persiuntimo stotis.

RSU (angl. *road side unit*) – pakelės įrenginys.

RTS (angl. *request-to-send*) – prašymas siųsti.

S

SA (angl. *signal agent*) – signalo agentas.

SCM (angl. *Side Channel Monitoring*) stebėjimo iš šono metodas.

SE (angl. *Simulation engine*) – simuliacijos variklis.

SON (angl. *self-organizing networks*)– savaime susiorganizuojantys tinklai.

SRMA/PA (angl. *soft reservation multiple access with priority assignment*) – lengvas keleto prieigų rezervavimas su prioritetų priskyrimu.

T

TCP (angl. *Transmission Control Protocol*) – perdavimo valdymo protokolas. Vienas iš pagrindinių protokolų, esančių Internetinių protokolų rinkinyje.

TRIP (angl. *trust and reputation infrastructure-based proposal for vehicular*) – schema, pagrįsta pasitikėjimu bei reputacija

U

UDP (angl. *User Datagram Protocol*) – duomenų perdavimo protokolas. Skirtingai nei *TCP*, *UDP* nėra patikimas, neatlieka duomenų tėkmės kontrolės ir neturi klaidų atitaisymo mechanizmų.

UMTS (angl. *Universal Mobile Telecommunications System*) – universali mobiliųjų telekomunikacijų sistema.

V

V2I (angl. *vehicle to infrastructure*) – automobilis su infrastruktūra.

V2V (angl. *vehicle to vehicle*) – automobilis su automobiliu.

VANET (angl. *Vehicular Ad-Hoc Network*) – automobilinis ad-hoc tinklas.

vehicle platooning – autotraukiniai.

W

WEP (angl. *Wired Equivalent Privacy*) – algoritmas, skirtas 802.11 tinklų apsaugai, kurio rekomenduojama nenaudoti dėl saugumo spragų.

WPA (angl. *Wi-Fi Protected Access*) – algoritmas, skirtas 802.11 tinklų apsaugai, suteikiantis patikimą apsaugą, naudojant sudėtingus slaptažodžius.

WPA2 (*Wi-Fi Protected Access*) – pažangiausias 802.11 tinklų apsaugos algoritmas, užtikrinantis patikimą apsaugą.

WAVE (angl. *Wireless Access for Vehicular Environments*) bevielė prieiga automobilinėje aplinkoje.

WMN (angl. *wireless mesh network*) – bevielis *mesh* tinklas.

WSN (angl. *wireless sensor network*) – bevielis jutiklių tinklas.

WLAN (angl. *wireless local area network*) – bevielis vietinis tinklas.

WiFi – bevielio ryšio technologijos prekinis ženklas, priklausantis *Wi-Fi* aljansui.

WiMAX (angl. *Worldwide Interoperability for Microwave Access*) – bevielio ryšio technologija, kuri leidžia sparčiai perduoti duomenis radijo ryšiu.

Z

ZOR (angl. *zone of relevance*) – pavojaus zona.

Turinys

LENTELIŲ SĄRAŠAS

ILIUSTRACIJŲ SĄRAŠAS

ĮVADAS

Automobilis yra vienas iš kritinių žmogaus gyvenimo komponentų, taigi jame įdiegus programine bei technine įranga paremtą intelektą, galėtume ženkliai padidinti gyvenimo kokybę. Šiuo metu viena iš daugiausiai mokslininkų bei pramonės dėmesio susilaukiančių mobiliųjų technologijų yra automobilių komunikacijos bevieliai tinklai, kadangi yra didžiulis rinkos poreikis patikimesniems, saugesniems, ekonomiškesniems bei siūlančiais daugiau pramogų automobiliams. Šie tinklai įgauna vis didesnį komercinį aktualumą, kadangi buvo priimtas tarpautomobilinės komunikacijos *DSRC/WAVE* standartas, suteikiantis visiškai naują paslaugų, pasiekiamų automobiliuose lygį, apimantį daugybę sričių: nuo ofiso ant ratų iki pramogų, automobilių eismo saugumo didinimo, ekonomiškumo didinimo, žalos aplinkai mažinimo, mobiliojo interneto žaidimų, mobilaus apsipirkimo, nusikaltimų tyrimo, civilinės gynybos ir t.t. Automobiliai neturi griežtų elektros energijos sunaudojimo apribojimų, todėl lengvai gali būti aprūpinti galingais skaičiavimo įtaisais, bevieliais siųstuvais, sudėtingomis jutiklių sistemomis – *GPS*, foto/video kameromis, vibracijos, akustiniais, chemikalų jutikliais.

Kadangi pasaulyje dar nėra paplitusi automobilinės komunikacijos tinklų diegimo praktika, šioje kryptyje vykdomas didelis kiekis mokslinių tyrimų bei projektų. Nepaisant to, šioje srityje netrūksta ir sudėtingų mokslinių iššūkių, tarp kurių: labai dinamiškos eismo bei komunikacijos sąlygos, dažnas mazgų atsijungimas, duomenų sklaidos heterogeniškumas. Šiuo metu pagrindinės automobilinės komunikacijos sritys, užtikrinančios naudą visuomenei bei turinčios komercinį pritaikomumą, reikalauja daugiau ir gilesnių mokslinių tyrimų ir kurios buvo pasirinktos tyrimo problemomis: eismo saugumo, informacinių bei multimedija paslaugų teikimas bei integravimas įvairiomis eismo sąlygomis, skirtingų bevielio ryšio technologijų panaudojimas bei integravimas automobilinės komunikacijos tinkluose, privatumas ir saugumas automobilinės komunikacijos tinkluose.

Tyrimo objektas – heterogeninių paslaugų teikimas automobilinės komunikacijos tinkluose. Tyrimams atlikti bus naudojama imitacinio modeliavimo programinė įranga, kuri leidžia nedidelėmis laiko bei piniginėmis sąnaudomis modeliuoti, tirti bei tobulinti mobilius bevielius tinklus bei jiems taikomus metodus bei priemones.

Šio darbo tikslas – ištirti eismo saugumo, informacinių ir multimedija paslaugų teikimo galimybes bei perspektyvas automobilių komunikacijos tinkluose.

Siekiant pasiekti užsibrėžtą tikslą, suformuluoti šie darbo uždaviniai:

1. Atlikti išsamią tiriamos srities – paslaugų teikimo bevieliuose automobilių komunikacijos tinkluose literatūros analizę ir nustatyti problemines sritis.

2. Atlikti programinės įrangos, leidžiančios atlikti automobilinių tinklų imitacinį modeliavimą, kokybinę lyginamąją analizę ir parinkti tinkamiausias priemones eismo saugumo, informacinių ir multimedija paslaugų teikimo tyrimams.
3. Atlikti skirtingų ad-hoc maršrutizavimo protokolų efektyvumo tyrimą teikiant eismo saugumo, informacines ir multimedija paslaugas.
4. Atlikti eismo saugumo, informacinių ir multimedija paslaugų teikimo efektyvumo tyrimą, siuntėjui ir gavėjui judant priešingomis kryptimis automagistralėje.
5. Atlikti skirtingų bevielio ryšio technologijų panaudojimo eismo saugumo, informacinių bei multimedija paslaugų teikimui automobilių komunikacijos tinkluose efektyvumo tyrimą miesto bei greitkelio sąlygomis.
6. Sukurti naują pasitikėjimu grindžiamą autentifikavimo schemą informacinių bei multimedija paslaugų teikimo apsaugojimui automobilinėje komunikacijoje.
7. Pasiūlyti naujas naujos automobilinės komunikacijos taikymo sritis.

Darbo rezultatai buvo įdiegti įgyvendinant šiuos projektus:

- tarptautinį mokslinį projektą: LATLIT INTEREG project, code LLII-061 „Development of Joint Research and Training Centre in High Technology Area“
- nacionaliniame Aukštųjų technologijų plėtros programos projekte „Mobiliųjų ir bevielių paslaugų virtualios informacinės aplinkos sukūrimas“ (MOBAS), (paraiška Nr. B-09018, 2010 m. gegužės 19 d. tarp KTU ir Lietuvos mokslo tarybos sudarytas sutartis Nr. AUT-03/2010).

I. ANALITINĖ (LITERATŪROS ANALIZĖS) DALIS

1. *Ad-hoc* tinklų tipai

Per pastaruosius keletą metų, *ad-hoc* tinklai tapo viena labiausiai tyrinėjamų sričių tarp tinklus tyrinėjančių mokslininkų. *Ad-hoc* tinklas susideda iš tinklo mazgų, aprūpintų bevielio ryšio sąsajomis, kurios gali komunikuoti viena su kita bei jokios egzistuojančios tinklo infrastruktūros. Viena iš ryškiausių šių tinklų savybių – bevielės daugiašuolės komunikacijos sąvoka. Skirtingai nei tradiciniuose bevieliuose tinkluose, mobilūs mazgai gali siųsti žinutes ir paskirties mazgams, kurie neįeina į siuntėjo radijo aprėpties zoną. Kai paskirties mazgas yra už keleto šuolių nuo siuntėjo, tarpiniai mazgai atlieka persiuntimo funkciją ir persiunčia duomenų paketus gavėjui. Mazgai turi naudoti specialius maršrutizavimo protokolus tam, kad surasti kelią, kuriuo bus perduoti duomenų paketai iš siuntėjo gavėjui. Kadangi *ad-hoc* mazgai gali būti mobilūs, tokių protokolų kūrimas yra labai sudėtinga užduotis.

Paskutiniais metais ši bendra daugiašuolės komunikacijos sąvoka išaugo į daugybę specialių skirtingų tinklų tipų klasifikavimo variantų. Šios specializacijos skiriasi priklausomai nuo mazgų mobilumo, jų skaičiavimo resursų, energijos suvartojimo bei kitų parametrų. Šie daugiašuolės komunikacijos bevieliai tinklai skirstomi į mobilius *ad-hoc* (*MANET*), bevielius mesh (*WMN*), bevielius jutiklių (*WSN*) ir bevielius automobilių ad-hoc (*VANET*) tinklus. *ad-hoc* tinklų tipų palyginimas pateiktas 1 lentelėje.

1 lentelė. *Ad-hoc tinklų tipų palyginimas [1]*

Savybė	**MANET**	**WMN**	**WSN**	**VANET**
Tinklo dydis	Vidutinis	Didesnis už vidutinį	Didelis	Didelis
Mazgų mobilumas	Atsitiktinis	Statinis	Dažniausia statinis	Didelis, neatsitiktinis
Energijos apribojimai	Dideli	Labai maži	Labai dideli	Labai maži
Mazgų skaičiavimų resursai	—	Dideli	Labai maži	Dideli
Mazgų atminties talpa	—	Didelė	Labai maža	Didelė
Priklausomumas nuo vietovės	Mažas	Labai mažas	Didelis	Labai didelis

1.1. Mobilūs *ad-hoc* tinklai (*MANET*)

Mobilūs *ad-hoc* tinklai (angl. *MANET*) yra autonominių taškas į tašką sujungtų bevielių nepriklausomų mazgų sistema, kuri gali dinamiškai judėdama keisti prisijungimą prie tinklo. Skirtingai nuo mobiliojo telefonų ryšio, *MANET* tinkluose nėra jokios fiksuotos infrastruktūros ir centralizuoto valdymo. Tinklas gali būti sukuriamas bet kurioje vietoje, bet kuriuo metu, jei tik du ar daugiau mazgų susijungia ir komunikuoja tarpusavyje tiesiogiai, būdami radijo aprėpties zonoje arba per kitus tarpinius mobilius mazgus. Mobilieji mazgai gali atlikti tiek maršrutizatoriaus, tiek ir priimančiojo mazgo funkcijas. Didžiausios problemos su kuriomis susiduria ši technologija yra topologijos valdymas, maršrutizavimas, paslaugų kokybė (angl. *Quality of Service - QoS*), resursų

valdymas, teikiamų paslaugų aptikimas, tinklo valdymas, saugumo užtikrinimas ir kt., kadangi tradicinės tinklų schemos šiuo atveju yra nebetinkamos. Pagrindinės *MANET* taikymo sritys yra: kariuomenės ryšys, automobilinė komunikacija, stichinių nelaimių atvejai ir kt. Su naujesnių technologijų atėjimu, mobilūs *ad-hoc* tinklai tampa neatskiriama naujos kartos tinklų dalimi, dėl jų lankstumo, automatinės konfigūracijos galimybių, fiksuotos infrastruktūros nebuvimo, eksploatavimo paprastumo, ir išlaidų efektyvumo [2, 3].

1.2. Bevieliai *mesh* tinklai

Bevieliai *mesh* tinklai (angl. *Wireless Mesh Networks*) atsirado neseniai, kai naujos tinklo architektūros pradėjo sparčiai plėsti aprėptį ir didinti bevielės prieigos tinklų pajėgumus. *WMN* yra perspektyvus sprendimas suteikti plačiajuostį bevielį ryšį tiek patalpose, tiek ir lauke, be brangios laidinio tinklo infrastruktūros. *WMN* yra sudaryti iš dviejų tipų mazgų: *mesh* maršrutizatorių ir *mesh* klientų. *WMN* naudoja keletą bevielių technologijų, įskaitant *IEEE 802.11 WLAN*, *IEEE 802.16* ir ketvirtosios kartos mobiliojo ryšio. Skirtingai nuo įprastų maršrutizatorių, *mesh* tipo įrenginiai be standartinių maršrutizavimo galimybių turi papildomas maršrutizavimo funkcijas, skirtas *mesh* tinklo darbo organizavimui. Panaudojant tarpinius mazgus, galima pasiekti didelę aprėpties zoną su žema perdavimo galia. Norint dar labiau padidinti *mesh* tinklo lankstumą, *mesh* maršrutizatoriuose paprastai yra įrengtos kelios bevielės sąsajos. Nepaisant visų šių skirtumų, *mesh* ir įprasti bevieliai maršrutizatoriai paprastai gaminami remiantis panašia technine platforma. *Mesh* maršrutizatoriai suteikia minimalų mobilumą savo klientams. Nors *mesh* klientai taip pat gali veikti maršrutizatoriaus režimu, tačiau jų tiek techninė, tiek programinė įranga yra daug paprastesnė nei *mesh* maršrutizatorių. *WMN* maršrutizatorių funkcionalumas leidžia lengvai integruoti *WMN* tinklus su kitų rūšių tinklais. Įprastiniai mazgai, naudojantys bevielio ryšio plokštes (angl. *NIC*) gali tiesiogiai jungtis prie *WMN* tinklo per *mesh* maršrutizatorius, vartotojai neturintys bevielio ryšio plokštės, gali jungtis naudodami laidinę *Ethernet* prieigą.

Taigi, vietoj to, kad būtų papildomo tipo *ad-hoc* tinklais, *WMN* diversifikuoja *ad-hoc* tinklų galimybes. Ši savybė suteikia daug privalumų *WMN*, tokių kaip, maža kaina, paprasta tinklo priežiūra, stabilumas, patikima paslaugų aprėptis ir kt. Be to, kad *WMN* yra plačiai naudojami tradiciniuose *ad-hoc* tinklų taikymo sektoriuose, *WMN* sparčiai plečiasi ir kitose taikymo srityse, pvz., plačiajuosčio ryšio teikime, pastatų automatikoje, didelės spartos miestų tinkluose ir įmonių tinkluose [4, 5, 6].

1.3. Bevieliai jutiklių tinklai

Vystantis mikro-elektro-mechaninėms sistemoms, mažiems mikroprocesoriams, mažų energijos sąnaudų bevielio ryšio įrenginiams, buvo sukurti mažai kainuojantys, mažų energijos sąnaudų multifunkciniai jutiklių įrenginiai skirti stebėti įvairiems fizikiniams reiškiniams, pvz.,

temperatūrai, drėgnumui, vibracijai, seisminiams įvykiams, taršai ir kt. Sujungti tarpusavyje per bevielio ryšio sąsają, jie sudaro bevielius jutiklių tinklus, kurie susideda iš tam tikroje geografinėje zonoje išdėstytų jutiklių mazgų. Jutiklio mazgas yra nedidelis prietaisas, kuris apima tris pagrindinius komponentus: fiksavimo posistemę, skirtą duomenų gavimui iš supančios fizinės aplinkos, duomenų apdorojimo posistemę, skirtą duomenų apdorojimui ir saugojimui, ir bevielio ryšio posistemę, skirtą duomenų perdavimui. Taip pat, naudojamas energijos šaltinis, dažniausia baterija turinti ribotus energijos resursus, tiekiantis energiją, kurios reikia, kad prietaisas galėtų atlikti užprogramuotas užduotis.

Išdėstyti dideliais kiekis sensoriniame lauke, šie jutikliai gali automatiškai sudaryti *ad-hoc* tinklą bei komunikuoti tarpusavyje per vieną ar daugiau surinkimo mazgų. Nutolęs vartotojas gali įterpti komandas į jutiklių tinklą per surinkimo mazgus, ir taip priskirti duomenų surinkimo, apdorojimo ar perdavimo užduotis jutikliams bei vėliau šią informaciją persiųsti. Šių tinklų taikymas išsiplėtė į medicinos, žemės ūkio, aplinkos apsaugos, karinės pramonės, inventoriaus stebėjimo, įsibrovimų stebėjimo, judesio stebėjimo, įrenginių gedimų stebėjimo ir daugelį kitų sričių. [7, 8]

1.4. Bevieliai automobilių *ad-hoc* tinklai - *VANET*

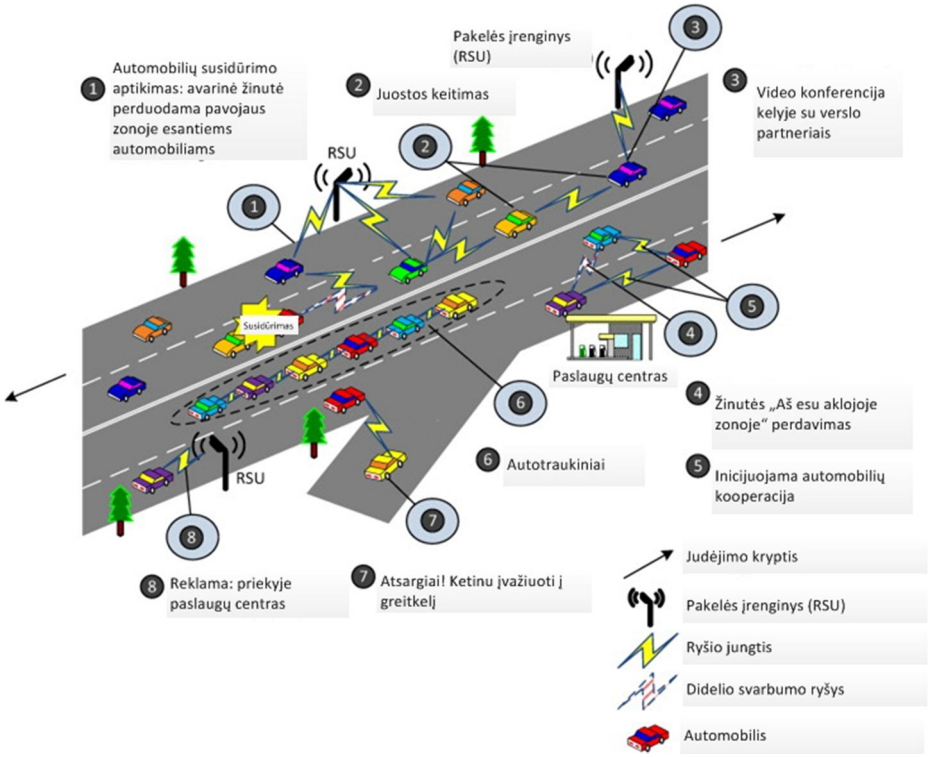
Bevieliai automobilių ad-hoc tinklai – *VANET* yra speciali *MANET* tinklų rūšis, kuriuose tinklo mazgai yra automobiliai, kurie gali judėti didžiuliu greičiu bei tinklas gali būti sudarytas tiek iš daugybės tinklo mazgų, tiek ir iš keleto. Šių mazgų mobilumas yra apribotas keliais, gatvėmis, greičio apribojimais ir t.t. Automobiliai, paprastai neturi elektros energijos suvartojimo apribojimų, todėl gali būti aprūpinti pajėgiomis skaičiavimo bei komunikacijos priemonėmis. Automobiliai siunčia signalinius paketus kas maždaug 300 ms, siekiant užtikrinti susidūrimo išvengimo programų veikimą ir perduodant pozicijos informaciją, greitį ir trajektoriją. Naudojantis signaliniais paketais, nustatoma tinklo topologija bei jos pasikeitimas laike. Daugeliu atvejų, galimas dažnas tinklo išskaidymas, kadangi automobiliai judėdami sudaro grupes, tačiau nuotolis tarp šių grupių gali būti didesnis nei ryšio aprėptis [9, 10, 11].

2. Tinklo apibrėžimas, architektūra bei diegimo scenarijai

2.1. Automobilinės komunikacijos tinklai ir jų architektūra

Automobilinės komunikacijos tinklai – tai nauja bevielių tinklų klasė, kuri sparčiai išaugo, bevielių technologijų ir automobilių pramonės naujausių mokslinių pasiekimų dėka. Automobilių tinklai yra suformuojami spontaniškai tarp judančių transporto priemonių, aprūpintų bevielėmis sąsajomis, kurios gali būti tiek homogeninės, tiek ir heterogeninės. Šie tinklai, kitaip žinomi kaip *VANET*, yra viena iš a*d-hoc* tinklų taikymo galimybių realiame pasaulyje, leidžianti tarpusavyje komunikuoti netoliese esančioms transporto priemonėms, taip pat transporto priemonėms ir

stacionariems įrenginiams. Transporto priemonės gali būti tiek privačios, tiek ir viešojo transporto (pvz. autobusai, viešųjų paslaugų transportas). Fiksuota įranga gali priklausyti valstybei, privatiems tinklų operatoriams ar paslaugų tiekėjams.



1 pav. *Praktinis automobilių komunikacijos tinklo panaudojimo pavyzdys [12]*

VANET susideda iš *OBU* – borto įrenginių (angl. *on-board units*), įmontuotų automobiliuose ir *RSU* – pakelės įrenginių (angl. *roadside units*), sumontuotų pagal gatves, greitkelius ir kitas teritorijas, kuriose važinėja automobiliai, kurie užtikrina tiek *V2V*, tiek ir *V2I* ar *I2V* komunikaciją. 1 pav. pateiktas praktinis automobilių komunikacijos tinklo panaudojimo pavyzdys. Per bevielės komunikacijos sąsajas automobiliai bendrauja su netoliese esančiais automobiliais itin dinamiškoje *ad-hoc* tinklo aplinkoje. Su eismu susijusi informacija gali būti apsikeičiama *V2V* komunikacijomis, leidžiant vairuotojams geriau suvokti eismo sąlygas. Pavojaus atveju gali būti perduodamos specialios įspėjančios žinutės pavojaus zonoje (angl. *ZOR – zone of relevance*) esantiems automobiliams. Taip pat, galima naudotis taškas į tašką principu veikiančiomis programomis, tokiomis kaip informacijos pasidalinimas ar žaidimai. *RSU* gali perduoti ne tik kelio ir eismo sąlygų informaciją (pvz. staigius posūkius, kelio dangos būklę ir kt.), bet ir užtikrinti interneto ryšį keleiviams ar teikti kitas papildomas informacines bei multimedija paslaugas, tokias kaip reklama, stovėjimo vietų informacija, mokėjimo už stovėjimą paslaugas [*12, 13*].

Prie spartaus technologijos vystymosi prisideda ne tik mokslininkai, tačiau ir automobilių pramonė. Didelį susidomėjimą rodo ir vyriausybės bei standartų organizacijos. 2003 m. *DSRC* (angl. *dedicated short-range communications*) sistema buvo sukurta JAV, kur *FCC* (angl. *Federal*

Communication Commission) skyrė 75Mhz pločio dažnių juostą skirtą automobiliniams tinklams. Europoje automobilių bei originalios automobilinės įrangos (angl. *OEM*) gamintojų buvo inicijuotas *Car-to-Car Communication* konsorciumas (*C2C-CC*), kurio pagrindinis tikslas – padidinti eismo saugumą bei efektyvumą, taprautomobilinės komunikacijos priemonėmis. *IEEE* (angl. *Institute of Electrical and Electronics Engineers*) kuria *IEEE 1609* šeimos standartus, skirtus bevielei prieigai automobilinėje aplinkoje (*WAVE*) [11].

2.2. Specifinės automobilinės komunikacijos tinklų charakteristikos

Automobilių tinklai turi specialias charakteristikas bei savybes, kurios juos skiria nuo kitų bevielių tinklų tipų. Lyginant su kitais komunikacijų tinklais, automobilių tinklai turi šias unikalias savybes [11, 9]:

- Automobiliai turi daug didesnį energijos rezervą, lyginant su įprastu mobiliu įrenginiu. Energija gali būti gaunama iš akumuliatorių bei prireikus įkraunama benzininiu, dyzeliniu ar alternatyvaus kuro varikliu.
- Transporto priemonės yra daug kartų didesnės bei sunkesnės lyginant su tradiciniais bevieliais klientais, taigi gali palaikyti gerokai didesnius ir sunkesnius skaičiavimo (jutiklių) komponentus. Automobilių kompiuteriai gali būtį didesni, greitesni bei aprūpinti itin didelės talpos atminties įrenginiais (terabaitai duomenų), taip pat galingomis bevielio ryšio sąsajomis, galinčiomis užtikrinti aukštą komunikacijos spartą.
- Transporto priemonės gali judėti dideliu greičiu (160 km/h ar daugiau), todėl sunku išlaikyti pastovią, nuoseklią *V2V* komunikaciją. Tačiau egzistuojantys statistiniai duomenys apie transporto judėjimą, tokį kaip, judėjimą kartu pagal tam tikrus šablonus arba piko metu gali padėti išlaikyti ryši tarp mobilių automobilių grupių.
- Automobiliai tinkle bet kuriuo momentu gali atsidurti už ryšio zonos (*WiFi*, mobiliojo, palydovinio ir t.t.), todėl tinklo protokolai turi būti sukurti taip, kad būtų galima lengvai prisijungti prie interneto, esant normaliam režimui.

Nepaisant daugybės unikalių teigiamų savybių, automobilių tinklų vystymasis susiduria ir su specifiniais iššūkiais, kurių pagrindiniai:

- Potencialiai didžiulio masto tinklai. Skirtingai nuo literatūroje aprašomų *ad-hoc* tinklų, kurie yra gana riboto dydžio, automobilių tinklai, iš pricipo, gali išsiplėsti visame kelių tinkle ir apimti didžiulį kiekį tinklo įrenginių (automobilių).
- Didelis mobilumas. Aplinka, kurioje veikia automobilių tinklai yra itin dinamiška ir kai kuriais atvejais gali būti ypač skirtinga, pvz. greitkeliuose greitis gali siekti iki 300 km/h, žemo apkrovimo keliuose automobilių tankumas gali tesiekti vos 1-2 automobilius kilometre. Kita

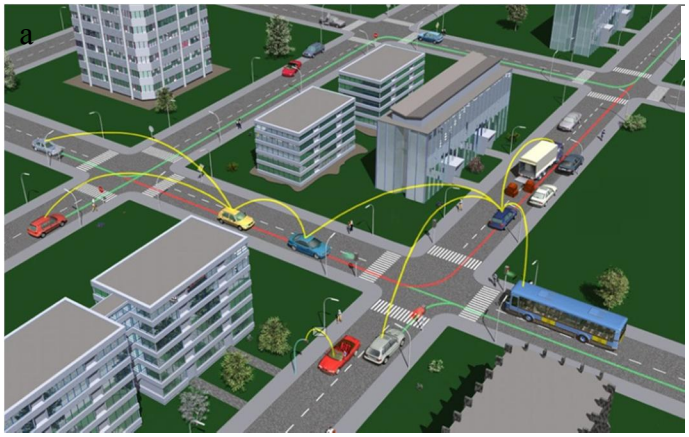
vertus, miestuose automobilių greitis siekia 50-60 km/h, o automobilių tankumas gana didelis, ypač piko metu.

- Išmėtytas tinklas. Automobilių tinklai, dažnu atveju, gali būti išmėtyti. Dinamiška eismo prigimtis gali nulemti didelius tarpus tarp automobilių retai apgyvendintose vietovėse, taip pat gali būti sukuriamas keletas izoliuotų tinklo mazgų klasterių.
- Tinklo topologija ir prisijungimas. Automobilių tinklų scenarijai labai skiriasi nuo klasikinių *ad-hoc* tinklų, kadangi automobiliai juda bei keičia pozicijas nuolatos, scenarijai yra labai dinamiški. Taip pat, tinklo topologija keičiasi labai dažnai, kadangi itin dažni prisijungimai bei atsijungimai tarp tinklo mazgų. Iš tiesų, iki kokio laipsnio tinklas yra apjungtas priklauso nuo dviejų faktorių: atstumo tarp bevielių jungčių bei automobilių, galinčių jungtis į tinklą kiekio.

2.3. Paplitusios automobilių komunikacijos schemos

Ryšiai transporto priemonėse gali būti suskirstyti į tris pagrindines grupes: automobilio ir automobilio komunikacija (*V2V*), automobilio ir infrastruktūros komunikacija (*V2I*, *I2V*) ir automobilio vidinė komunikacija. Galimas ir papildomas mišrus režimas (*V2V* ir *V2I*). Automobilinės komunikacijos tinklų sudarymo schemos pateiktos 2 pav.

a b



c

2 pav. *Tipinės VANET komunikacijos schemos: (a) automobilio su automobiliu (V2V); (b) automobilio su infrastruktūra; (c) automobilio vidinė komunikacija [14, 9, 15]*

2 pav. a ir b dalyse pateiktas tinklo schemas įgyvendinti galima ir pasitelkus komercinius *WiFi* įrenginius. Mišraus režimo tinklai yra plačiai nagrinėti mokslinės bendruomenės, ypač maršrutizavimo bei tinklo talpumo atžvilgiais. Tokiu atveju, kai automobiliai aprūpinti tik plačiajuostės interneto prieigos sąsajomis (pvz. *3G*, *WiMAX*), naudojamas scenarijus, kuriame automobiliai tarpusavyje bendrauja tik per internetą. Kai automobilis yra aprūpintas *DSRC* ir kitu plačiajuostės bevielės komunikacijos metodu, turime mišraus režimo scenarijų. Šiuo metu mokslininkai daugiausia dėmesio skiria pirmajam scenarijui, nors antrasis taip pat sulaukia nemažai susidomėjimo dėl sparčiai populiarėjančių išmaniųjų telefonų. [9, 10].

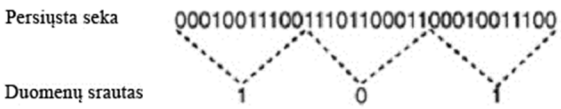
Be apžvelgtų komunikacijos schemų, bevielių komunikacijų technologijos gali būti skirstomos į tokias, kurios užmezga 1 su 1 ryšius ir tokias, kurios užmezga 1 su daug ryšius. Antruoju atveju reikalingas įrenginys, galintis padalinti turimą ryšio kanalą klientams. Šis kanalas gali tapti nepakankamas, kai aptarnaujamų mazgų skaičius aprėpties zonoje smarkiai išauga.

2.4. Bevielės prieigos ir moduliacijos technologijos

Vystantis informacinėms technologijoms, yra daug bevielių technologijų potencialiai tinkamų *V2V*, *V2I* ir *InV* komunikacijoms. Atlikus bevielių technologijų analizę buvo sudarytą pagrindinių bevielių technologijų, potencialiai tinkamų *VANET* tinklams analizė, kuri pateikta 2 priede.

2.4.1.*DSSS* – tiesioginės tvarkos skleisto spektro technologija

Naudojant tiesioginės tvarkos skleisto spektro technologiją (angl. *Direct-sequence spread spectrum*), siųstuvas pakeičia duomenų (bitų) srautą simboliais, kur kiekvienas simbolis atvaizduoja grupes iš vieno ar daugiau bitų. *DSSS* diapazoną padalina į 14 kanalų po 22 MHz, kurie iš dalies persidengia. Gaunami trys nepersidengiantys kanalai. Technologija pirmą kartą panaudota kariškių. *DSSS* itin išpopuliarėjo 1999 m., kai buvo patvirtintas *802.11b* standartas. 3 pav pavaizduotas duomenų srauto pakeitimas simboliais [16].



3 pav. *Tiesioginės tvarkos skleisto spektro technologija [16]*

2.4.2.*FHSS* – dažnio šokinėjimo skleisto spektro technologija

Naudojant dažnio šokinėjimo skleisto spektro technologiją (angl. *Frequency-hopping spread spectrum*), radijo bangų perdavimui 2,4 GHz dažnio diapazonas suskirstomas į 75 subkanalus, kiekvienas po 1 MHz. Duomenys yra siunčiami naudojant tam tikrą kanalų seką. Vienas ar keli paketai yra siunčiami vienu kanalu po to peršokama į kitą dažnį. Peršokimas į kitą dažnį nėra atsitiktinis, o naudoja siųstuvui ir imtuvui žinomą pasikartojančią tvarką, kuri sudaroma, siekiant

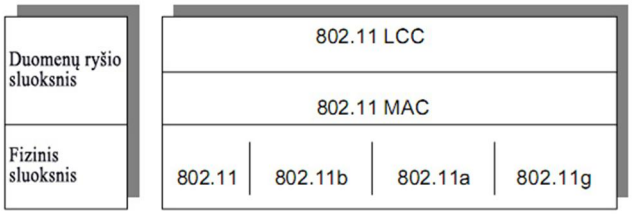
sumažinti galimybę, kad keletas radijo bangas siunčiančių įrenginių vienu metu naudos tą patį kanalą. *FHSS* greitis yra ribotas iki 2 Mbps. [2].

2.4.3.*OFDM* – stačiakampis dažnių tankinimo moduliacijos metodas

OFDM (angl. *Orthogonal frequency-division multiplexing*) – stačiakampis dažnių tankinimo moduliacijos metodas. Jis naudojamas kaip skaitmeninis daugialinijinis informacijos nešėjas. Informacijai pernešti yra naudojamas didelis kiekis šalia išdėstytų stačiakampių sub-nešėjų. Duomenys yra suskirstomi į keletą lygiagrečių srautų ar kanalų – kiekvienam sub-nešėjui po vieną. Kiekvienas sub-nešėjas yra moduliuojamas pagal tradicinę moduliavimo schemą (pvz. plotą, amplitudę, fazės poslinkį). Duomenų perdavimo sparta labai išauga, kadangi naudojami keli lygiagretūs duomenų srautai. *OFDM* itin populiarus ir dažnai naudojamas bevielių tinklų, *WiMAX*, skaitmeninių radijo transliacijų, *DVB-T*, *ADSL* moduliacijos metodas [17].

2.4.4.IEEE 802.11 standartas

802.11 darbo grupė buvo suformuota 1990 m. Jų tikslas buvo sukurti bevielių vietinių tinklų specifikaciją[18]. 802 standartai adresuoja žemesniuosius *OSI* modelio – fizinį bei duomenų ryšio (angl. *data link*) sluoksnius. *OSI* sluoksniai bei atitinkama 802 struktūra pavaizduoti 4 paveikslėlyje.



4 pav. *OSI sluoksniai ir atitinkama 802 struktūra [18]*

802.11. Pirminis *IEEE* bevielių vietinių tinklų standartas, kuris numato 1 arba 2 Mbps perdavimo greitį 2,4 GHz dažnio diapazone. Naudojama *FHSS* arba *DSSS* moduliacija. Naudojant *FHSS*, naudojamas dažnis nuo 2,4 GHz iki 2,4835 GHz. Vienas ar daugiau paketų yra perduodami vienu dažniu (diapazonas suskirstomas į 75 subkanalus, kiekvienas po 1 MHz), po to peršokama į kitą dažnį. Peršokimas į kitą dažnį nėra atsitiktinis, o naudoja siųstuvui ir imtuvui žinomą pasikartojančią tvarką. Naudojant *DSSS*, siųstuvas pakeičia duomenų (bitų) srautą simboliais, kur kiekvienas simbolis atvaizduoja grupes iš vieno ar daugiau bitų [19].

802.11a. Pirminio *IEEE 802.11* bevielių vietinių tinklų standarto praplėtimas, numatantis iki 54 Mbps pralaidumą 5 GHz dažnio diapazone. Realus pralaidumas – apie 27 Mbps. Kadangi 2,4 GHz diapazonas yra labai plačiai naudojamas ir praktiškai perpildytas, 5 GHz diapazono naudojimas suteikia labai reikšmingą privalumą. Nepaisant to, aukštas dažnis sukelia ir trūkumų: efektyvi vidutinė *802.11a* aprėptis yra mažesnė nei *802.11b/g*. Teoriškai signalas negali sklisti taip toli, todėl, kad jis yra labiau absorbuojamas sienų bei kitų stambių objektų signalo kelyje, nes

bangos ilgis yra mažesnis. Praktiškai *802.11a* aprėptis yra tokia pati arba net didesnė, dėl mažesnių trikdžių. Išleistas 1999 m. [19].

802.11b. *802.11* standarto praplėtimas, numatantis 11 Mbps pralaidumą, tačiau automatiškai galintis greitį sumažinti iki 5,5 Mbps, 2 Mbps, ar 1 Mbps, priklausomai nuo signalo stiprumo, 2,4GHz diapazone. Naudoja tik *DSSS*. 1999 m. pirminio 802.11 standarto patvirtinimas leido bevielį funkcionalumą lyginti su *Ethernet* [20].

802.11g. 2003 m. *IEEE* patvirtintas standartas, numatantis iki 54 Mbps pralaidumą 2,4 GHz diapazone. Naudojama *OFDM* moduliacija. Itin greitai išpopuliarėjo tie tarp namų vartotojų, tiek tarp verslo klientų dėl siūlomos gerokai didesnės spartos nei 802.11b standarto. Kadangi buvo didžiulis didesnės spartos poreikis, *802.11g* įranga buvo pradėta prekiauti likus metams iki oficialaus standarto patvirtinimo. Šiuo metu praktiškai visa parduodama įranga palaiko *802.11g*. [18]

802.11n. Vienas iš 802.11n reikalavimų yra patobulintos *OFDM* moduliacijos realizavimas. Vienas iš plačiausiai žinomų specifikacijos komponentų – *MIMO* (angl. *Multiple Input Multiple Output*) – sudėtinis įėjimas, sudėtinis išėjimas. Siųstuvas siunčiamą duomenų srautą padalina į keletą dalių ir kiekvieną dalį siunčia naudodamas atskirą anteną. Dabartinis standarto variantas palaiko iki keturių tokių dalių. Kiek naudojama skirtinų duomenų srautų, tiek kartų išauga duomenų perdavimo sparta [21].

2.4.5.*IEEE 802.11p*/*WAVE* sistemos

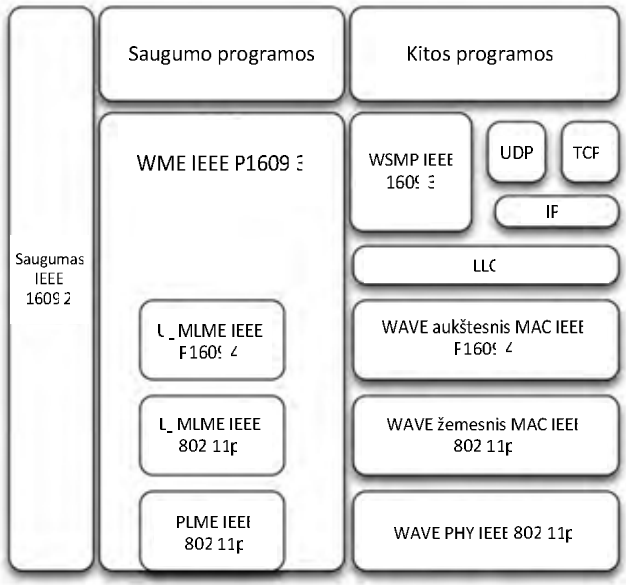
IEEE 802.11p standartas buvo pasiūlytas kaip *IEEE 802.11* standarto papildymas, siekiant užtikrinti duomenų apsikeitimą automobilių komunikacijos tinkluose. Pagrindinis *MAC* (angl. *Medium Access Control*) sluoksnio mechanizmas remiasi prioritetais ir konkurencija paremta *EDCA* (angl. *Enhanced Distributed Channel Access*) – patobulinta paskirstyta *802.11e* standarto kanalų prieigos schema [22] ir daugiakanaliu *WAVE* (angl. *Wireless Access for Vehicular Environments*) sistemos veikimu [23]. Pagal *WAVE*, automobiliai periodiškai įsijungia bendrą valdymo kanalą (*CCH*) pavojaus ir įspėjimų žinučių stebėjimui, po to persijungia į vieną iš prieinamų paslaugų kanalų (*SCH*) su saugumo nesusijusiai informacijai perduoti.

DSRC – skirtasis trumpo nuotolio ryšis (angl. *Dedicated Short Range Communications*) yra ryšys, veikiantis 5,9 GHz dažniu, palaikantis tiek viešojo saugumo, tiek ir privataus naudojimo *I2V* ir *V2V* komunikacijos aplinkas. Informacijai pernešti yra naudojamas didelis kiekis lygiagrečiai išdėstytų stačiakampių subnešėjų [13, 11].

Labai mobilioje transporto aplinkoje pagrindinė problema yra laikas, per kurį mobilus bevielis mazgas prisijungia prie bevielės stotelės. *IEEE 802.11a* standarto įrenginių kanalų skanavimo ir saugumo užtikrinimo sprendimai buvo netinkami greitai judančio transporto

priemonių saugumo užtikrinimo taikymui ir buvo reikalingi pakeitimai tiek baziniame kanalų priskyrimo lygmenyje, tiek ir paketų maršrutizavimo ir sprendimų priėmimo lygmenyje. Tokiu būdu atsirado trys standartų kūrimo ir taikymo idėjos. Pirmiausia, reikėjo atlikti *IEEE 802.11* bevielių vietinių tinklų standartų pakeitimus, kurie aprašytų *DSRC* spektrą ir juostas bei leistų greitą asociaciją, sudarančią *IEEE 802.11p* fizinį sluoksnį. Tam kad pakeisti *IEEE 802.11* sluoksnį, reikia pasiūlyti naujas saugumo ir kanalų parinkimo paslaugas aukštesniame lygmenyje. Visa tai yra įgyvendinta *IEEE 1609* standartuose – *WAVE* – bevielei prieigai automobilinėje aplinkoje [24]:

1. Resursų valdytojas – 1609.1;
2. Saugumo paslaugos ir valdymas – 1609.2;
3. Tinklo paslaugos – 1609.3;
4. Daugiakanalės operacijos – 1609.4.



5 pav. *DSRC standartai ir komunikacijos stekas [25]*

Šie standartai įgalina sistemas, kuriose automobiliai gali jungtis tiesiai į bendrą DSRC diapazono kanalą, skirtą saugumo užtikrinimui, o kiti kanalai yra prieinami mažiau svarbiems ryšiams. Aukščiausias lygmuo yra taikymo, vadinamas *SAE J2735* ir vystomas Automobilių inžinierių bendruomenės, *DSRC* techninio komiteto (angl. *Society of Automotive Engineers*, *DSRC Technical Committee*).

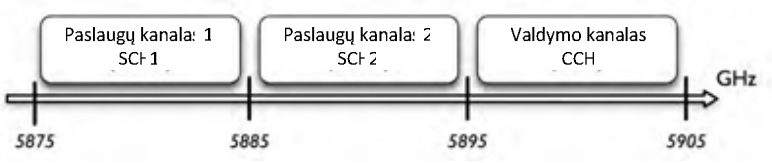
Taigi, *IEEE 802.11p* standartas (taip pat vadinamas ir *WAVE*) įneša *IEEE 802.11* standarto patobulinimus, reikalingus protingų transporto sistemų taikymui. Į jį įeina duomenų apsikeitimas tarp dideliu greičiu judančių automobilių, taip pat tarp automobilių ir *RSU* licencijuotoje 5,9 GHz dažnių juostoje iki 1000 metrų atstumu. *WAVE* apima naujas taikymo klases susijusias su saugumu keliuose (pvz. susidūrimo išvengimas) ir avarines paslaugas (policijos, greitosios pagalbos, gaisrinės ir kt. spec. tarnybų). Kai kuriais kritiniais atvejais reikia kad bendras laikas nuo *rst* signalo aptikimo iki apsikeitimo keletu kadrų neviršytų 100 ms. *WAVE* operacijoms atlikti panaudoja

valdymo kanalus ir keletą paslaugų kanalų. Fizinio sluoksnio praplėtimas remiasi *OFDM* sistema. *OFDM* sistema *WAVE* komunikacijoms suteikia 3, 4.5, 6, 9, 12, 18, 24, ir 27 Mbps spartą 10 MHz kanaluose. 3, 6 ir 12 Mbps siuntimo ir gavimo spartos palaikymas yra privalomas. Taip pat *WAVE* turi galimybę veikti 20 MHz kanaluose, tokiu atveju palaikoma 6, 9, 12, 18, 24, 36, 48 ir 54 Mbps sparta. 6, 12 ir 24 Mbps spartos palaikymas yra privalomas 20 MHz konfigūracijos atveju.

Stotelės, veikiančios pagal *WAVE*, turi sugebėti apsikeisti žinutėmis tarp *RSU* ir automobilių judančių iki 140 km/h greičiu su *PER* (angl. *packet error rate*) mažesniu nei 10%, kaip *PSDU* ilgis yra 1000 baitų; kai automobilis juda iki 200 km/h greičiu – su mažesniu nei 10% *PER*, kai *PSDU* ilgis yra 64 baitai. *V2V* atveju, turi būti užtikrinamas *PER* mažesnis nei 10% tarp automobilių, judančių 283 km/h greičiu, kai *PSDU* ilgis yra 200 baitų. Šie standartų techniniai apribojimai užtikrina saugumo paslaugų palaikymą, todėl *WAVE* susilaukia didžiulio susidomėjimo iš automobilių pramonės [15, 25].

2.4.6.Dažniai ir kanalai *WAVE* sistemose Europoje

Europoje, *ETSI* pristatė reikalavimus 5,9 GHz dažnio panaudojimo *ITS* sistemoms suderinimui Europos mastu *CEPT* (angl. *European Conference of Postal and Telecommunications Administrations*) ir Europos telekomunikacijų administracijos organizacijos. Organizacijos suteikė dažnių juostas nuo 5875 iki 5925 MHz su saugumu susijusių *ITS* sistemų vystymui, kurioms reikalinga apsauga nuo kitų paslaugų interferencijos. Su saugumu nesusijusioms sistemoms buvo paskirta dažnių juosta nuo 5855 iki 5875 MHz, kuria būtų galima naudotis nesikišimo principu. 5905-5925 MHz juosta palikta ateities *ITS* plėtimui.



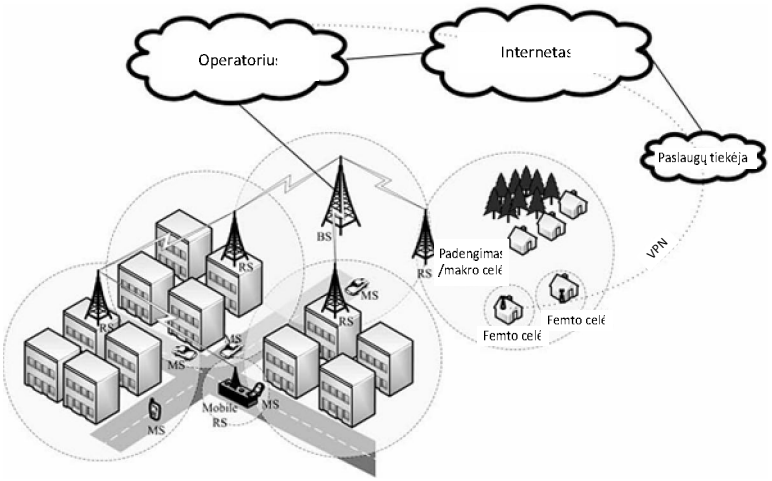
6 pav. *Į saugumą orientuotų ITS sistemų kanalai [1]*

6 pav. pateiktas dažnių juostos, skirtos į saugumą orientuotoms *ITS* sistemoms padalinimas į kanalus, kuriame 30 MHz dažnių juosta suskirstyta į tris kanalus, kur *SCH1* yra pirmasis paslaugų kanalas, *SCH2* – antrasis paslaugų kanalas ir *CCH* – valdymo kanalas [1, 15].

2.4.7.Mobilusis WiMAX – 802.16

WiMAX – yra telekomunikacijų technologija, kurios tikslas – dideliais atstumais suteikti bevielio ryšio prieigą plačiam spektrui įrenginių (nuo darbo stočių iki mobiliųjų telefonų). *WiMAX* apibūdinama kaip alternatyva kabeliniams modemams, telefonų kompanijų skaitmeninio prisijungimo linijoms (angl. *Digital Subscriber Line* (*DSL*)) arba *T1/E1* paslaugoms. [26] Paskutiniuosius keletą metų, *IEEE 802.16* yra laikoma vienu iš perspektyviausių sprendimų plačiajuosčiams miesto tinklams.

IEEE 802.16-2001 – pradinėje versijoje ryšys apibrėžiamas vieno taško su daug taškų (angl. *point-to-multi-point (PMP)*) tinklo architektūra, kurioje resursai yra paskirstomi centralizuoto mazgo, vadinamo bazine stotimi. Šiuo metu naujausias priimtas standartas yra *IEEE 802.16-2009*, tačiau yra ruošiama nauja *IEEE 802.16m* versija. Šios versijos tikslas – pakeisti tiek *IEEE 802.16-2009*, tiek *IEEE 802.16j-2009* standartus, siekiant sukurti pažangesnę licencijuojamą oro sąsają, taip pat užtikrinant suderinamumą su senesne įranga.



7 pav. *Bendroji WiMAX tinklo architektūra [27]*

7 pav. pateikta bendroji *WiMAX* tinklo architektūra. *IEEE 802.16-2009* sistemos modelyje *MS* (angl. *mobile station*) yra vartotojų įrenginiai, įskaitant mobiliuosius telefonus, delninius kompiuterius, nešiojamus kompiuterius ir pan. Bazinė stotis – BS (angl. *base station*) užtikrina *MS* interneto prieigą. *IEEE 802.16m* standarte aprašytas naujas tinklo mazgas, pavadintas *RS* – persiuntimo stotimi (angl. *relay station*), kuri gali būti tiek mobili, tiek fiksuota ir komunikuojanti su *BS*. *MS* interneto prieigą gali gauti iš vienos iš šių *RS*, kai tiesioginė komunikacija su *BS* yra neįmanoma arba yra nepatikima. Taip pat *IEEE 802.16m* standarte bus pristatytas *Femto* celių architektūros palaikymas, savaime susiorganizuojantys tinklai (*SON*) ir savaiminio optimizavimo procedūros. [27, 28]

2.4.8.*IEEE 802.16d* – fiksuotos *WiMAX* prieigos standartas

WiMAX suteikia fiksuotą, portabilų ar mobilią netiesioginio matomumo paslaugą (angl. *non-line-of-sight*) nuo bazinės stoties iki abonentinės stoties, taip pat žinoma kaip kliento patalpos įranga (angl. *customer premise equipment* (*CPE*)). *WiMAX* vienas iš tikslų yra aprėpti teritoriją 6 mylių spinduliu nuo bazinės stoties iki abonentinės įrangos, suteikti *PMP* ir paslaugas *NLOS* sąlygomis. Ši paslauga užtikrina iki 70 Mb/s mobilios bei fiksuotos prieigos greitaveiką [29].

2.4.9.*IEEE 802.16e* – mobilios *WiMAX* prieigos standartas

Mobilusis *WiMAX* perkelia fiksuotą bevielę paslaugą į naują lygmenį ir leidžia teikti paslaugas panašias, į teikiamas korinio ryšio operatorių, tuo pačiu suteikiant daug platesnes

galimybes. Mobilusis *WiMAX* užtikrina kokybišką komunikacijos ryšį judant iki 160 km/h greičiu. Technologija potencialiai gali pakeisti duomenų perdavimo koriniu ryšiu technologijas, tokias kaip *EvDo* (angl. *Evolution Data only*), *EvDv* (angl. *Evolution-Data/Voice*) ir *UMTS* (angl. *Universal Mobile Telecommunications System*). Jis taip pat suteikia geresnę skvarbą per pastatus ir pagerintas saugumo priemones nei fiksuotas *WiMAX*. Mobilus *WiMAX* puikiai tinka naujoms mobilioms paslaugoms, tokioms kaip mobilioji televizija ir žaidimai teikti. [29, 30]. Svarbu paminėti tai, kad automobilinė komunikacija greičiausiai bus vykdoma 5 GHz dažnių juostoje, kadangi JAV ir Europoje buvo rezervuota 5,9 GHz dažnių juosta *ITS* sistemoms. Dėl šios priežasties *IEEE 802.11b/g* nėra pageidaujami pasirinkimai ir galutiniai kandidatai greičiausiai bus apriboti *IEEE 802.11p*, *IEEE 802.11a* ir *IEEE 802.16e* technologijomis.

2.4.10.Mobilusis ryšys

Nors mobiliojo ryšio tinklų panaudojimas daugiausiai orientuojasi į telefoniją, duomenų perdavimas šiais tinklais itin sparčiai populiarėja. Pirmiausia siekiant padidinti *GSM* tinklu perduodamą greitaveiką (9,6 Kb/s), buvo pasiūlyta *GPRS* (angl. *General Packet Radio Service*) technologija, kuri suteikė 0,47 Mb/s greitaveiką. Po jos sekė *EDGE* technologija, užtikrinanti greitaveiką iki 1,9 Mb/s. Vėliau šios technologijos vietą užleido 3 kartos mobiliajam ryšiui. Buvo pasiūlyta *UMTS*, kuri yra labiausiai išvystyta 3 kartos mobiliojo ryšio technologija. Naujausias *UMTS* patobulinimas *HSPA+* leidžia pasiekti 42 Mb/s gavimo ir 22 Mb/s išsiuntimo spartą [31].

Mobiliojo ryšio tinklų taikymas automobilinėms sistemoms prasidėjo prieš keletą metų, kai *GSM* ir *GPRS* sistemos buvo pradėtos taikyti eismo informacijai bei pavojaus perdavimui [32]. Tačiau iki *3G* technologijų atėjimo, žema duomenų perdavimo sparta lėmė menką korinio ryšio naudojimą *ITS* sistemose. Mokslinėje literatūroje kai kurie autoriai gina *UMTS* naudojimą tiesioginėms *V2V* komunikacijoms, ši technologija taip pat taikoma stebėjimo sistemoms [33], tačiau jos taikymas *V2V* komunikacijai vis dar yra didžiulis iššūkis dėl didelio vėlinimo laiko. Kita priežastis stabdanti šių technologijų naudojimą *ITS* yra papildoma kaina, kurią reikia mokėti už naudojimąsi korine operatorių infrastruktūra. Nepaisant visų trūkumų kai kurie mokslininkai mano, kad bendra *ITS* komunikacijos technologija ir mobilusis ryšys gali būti sprendimu [15]. *3G* bevielės technologijos automobilių telematikos paslaugoms, gali pasiūlyti labai plačią aprėptį ir palaikyti didelį automobilių mobilumą. [30, 34].

2.5. Potencialios automobilinės komunikacijos taikymo sritys

Potencialios taikymo sritys automobilinėje aplinkoje gali būti suskirstytos į tris pagrindines kategorijas [35]: bendrąsias informacines – multimedija paslaugas, eismo saugumo informacines paslaugas, eismo stebėjimo ir valdymo paslaugas.

- **Bendrosios informacinės – multimedija paslaugos**. Šių paslaugų pagrindinis tikslas – vairuotojui ir keleiviams pasiūlyti patogumą ir komfortą. Pvz. *Fleetnet* [36] suteikia failų apsikeitimo bei žaidimų platformą kelyje. Lu R., et al. pasiūlė automobiline komunikacija paremtą protingą parkavimo schemą didelėms stovėjimo aikštelėms, suteikiančią realaus laiko aikštelės navigaciją, apsaugą nuo vagysčių, patogią stovėjimo informacijos sklaidą [37]. Skaitmeninės skelbimų lentos, skirtos reklamai buvo pristatytos Nandan A. et al., kurie nagrinėja reklamos platinimo galimybes automobiliniuose tinkluose, taip siūlo integruotą sistemą *AdTorrent*, skirtą turinio reitingavimui, paieškai bei pristatymui šioje architektūroje [38]. Pasinaudojant *V2I* komunikacijomis (pvz. mobiliojo ryšio tiekėjų paslaugomis) automobilyje galima atlikti tam tikrus verslo reikalus ar realizuoti mobilaus biuro idėją. Taip pat yra siūloma *CarTorrent P2P* architektūrą, panaudoti garso bei video medžiagos perdavimui automobilių tinkluose, taip ilgas keliones padarant įdomesnėmis [39]. Soldo F., et al. taip pat siūlo multimedija medžiagos transliavimo *VANET* tinklais miestuose sprendimą [40]. Šias technologijas galima panaudoti ir komerciniais garso bei video medžiagos transliavimo tikslais.
- **Eismo saugumo informacinės paslaugos**. Saugumo taikymo sritis visada yra pirmoje vietoje, siekiant ženkliai sumažinti nelaimingų atsitikimų keliuose skaičių. Panaudojus tarpautomobilinę komunikaciją, galima sukurti juostos keitimo asistavimo sistemas, adaptyvią kruizo kontrolę ir kitas sistemas padidinančias eismo saugumą ir padedančias vairuotojams įvairiose kritinėse situacijose. Sirichai P., et al. siūlo *VANET* tinklus panaudoti saugumo stebėjimo kamerų tinklo sudarymui, kuriuose stebėjimo kameros būtų sumontuotos autobusuose, taksi automobiliuose, kituose viešųjų įstaigų transporto priemonėse ir šie surinkti stebėjimų duomenys belaidės komunikacijos priemonėmis būtų perduoti į duomenų apdorojimo centrus. Tokiu būdu, būtų galima padėti užtikrinti viešąją tvarką, išaiškinti pažeidėjus, automatiškai reaguoti į nelaimes kelyje, iškviečiant specialiąsias tarnybas [41]. Dornbush S., Joshi A. [42], naudodamasi automobilinėmis komunikacijomis informuoja vairuotojus apie eismo sąlygas ir kelio apkrovimą, kas leidžia sumažinti kelionės laiką bei kuro sąnaudas. Tas pačias problemas sprendžia ir Sommer C., et al. panaudodami *UMTS* technologiją [43]. Automobilių traukinių sudarymas yra dar vienas būdas, leidžiantis padidinti eismo saugumą. Nemažai autorių siūlo savo idėjas autotraukinių (angl. *vehicle platooning*) sudarymui panaudojant *VANET* komunikacijų technologijas. Eliminuojant poreikį keisti eismo juostas, didinti ar mažinti judėjimo greitį ši technologija ženkliai gali padidinti eismo saugumą bei padėti padidinti kuro ekonomiją. Jovanović M. et al. ištyrė didelio masto autotraukinių sudarymo metodus automatizuoto

greitkelio sistemose [44]. Taip pat adaptyvią kruizo kontrolę suderinus su *V2V* komunikacijomis galima išvengti daugybės nelaimių, įvykstančių dėl žmogiškųjų faktorių.

- **Eismo monitoringas bei valdymas** yra būtini siekiant padidinti kelio pralaidumą ir sumažinti transporto spūstis. Kai kuriais atvejais, sankryžų kirtimas yra sudėtingas bei pavojingas. Tinkamas ir efektyvus šviesoforų valdymas gali palengvinti sankryžų kirtimą. Tolygus eismo judėjimas gali ženkliai padidinti gatvės pralaidumą ir sumažinti kelionės trukmę. Savaiminis paskirstytas eismo reguliavimas, panaudojant *VANET* komunikacijas išnagrinėtas Gibaud A., et al. [45]. Autorių sukurtas modeliavimo įrankis leidžia simuliuoti inovatyvių eismo valdymą bei patvirtina perspektyvią *VANET* taikymo sritį. Dresner. K., Stone P. siūlo sankryžų valdymo sistemą [46], kurioje vairuotojai ir sankryžos yra traktuojami kaip autonominiai multiagentinės sistemos agentai. Pasiūlytas naujas sankryžų valdymas panaudojant pristatytą rezervacijos sistemą. Atliktas modeliavimas patvirtino, kad ši sistema potencialiai veikia geriau už dabartines sankryžų valdymo sistemas.

2.6. Duomenų perdavimo kokybės reikalavimai eismo saugumo, informacinių bei multimedija paslaugų teikimui

Ankstesniame skyriuje aptartos galimos automobilinės komunikacijos taikymo sritys. Vienos iš pagrindinių ir galinčios atnešti realią praktinę naudą visuomenei yra eismo saugumo, informacinės bei multimedija paslaugos. Kokybiškam šių paslaugų teikimui yra keliami tam tikri duomenų perdavimo spartos, paketų pristatymo efektyvumo bei kolizijų kiekio reikalavimai. Atlikus analizę bei apibendrinus rezultatus buvo sudaryta duomenų perdavimo kokybės reikalavimų skirtingų paslaugų teikimui automobilinės komunikacijos tinkluose lentelė (2 lentelė).

2 lentelė. *Duomenų perdavimo kokybės reikalavimai skirtingų paslaugų teikimui automobilinės komunikacijos tinkluose [12, 47, 48, 50]*

Paslauga	Reikalinga minimali duomenų priėmimo sparta	Paketų praradimo įtaka
Eismo saugumo		
Juostos keitimas	1 KB/s	Vidutinė
Šviesoforų valdymo	1 KB/s	Vidutinė
Įspėjimas apie pavojų	1 KB/s	Didelė
Įspėjimas apie eismo sąlygas	10 KB/s	Vidutinė
Informacinės		
Žiniatinklis	Kuo didesnė, nėra minimalaus reikalavimo	Maža
Elektroninis paštas	Kuo didesnė, nėra minimalaus reikalavimo	Maža
Bendravimas žinutėmis (Skype, ICQ, Google Chat)	Kuo didesnė, nėra minimalaus reikalavimo	Vidutinė
Multimedija		
IPTV	500 KB/s	Vidutinė
VOIP	64KB/s	Vidutinė
Vaizdo/garso medžiagos	Kuo didesnė, nėra minimalaus	Didelė

apsikeitimas	reikalavimo	
Žaidimai	Kuo didesnė, nėra minimalaus reikalavimo	Didelė

2.7. Maršrutizavimo protokolai automobilių komunikacijos tinkluose

2.7.1.*MANET* maršrutizavimo protokolai

MANET maršrutizavimo protokolai gali būti klasifikuojami pagal daugybę skirtingų kriterijų. Vienas iš labiausiai paplitusių klasifikatorių maršrutizavimo protokolus skirsto į: proaktyviuosius, reaktyviuosius ir hibridinius. Šioje srityje daug nuveikę yra ir Lietuvos mokslininkai R. Plėštys ir R. Zakarevičius. [49] yra siūlomas *MANET* maršrutizavimo metodas, kontroliuojantis prašymo ir atsako zonas, siekiant sumažinti maršrutizavimo informacijos kiekį tinkle. Rezultatai rodo, ženklų šios informacijos sumažėjimą, naudojant šį metodą.

Skirtingų *ad-hoc* tinklų maršrutizavimo protokolų palyginimas pateiktas 3 lentelėje.

3 lentelė. *Skirtingų maršrutizavimo protokolų ad-hoc tinkluose palyginimas [1]*

Maršrutizavimo protokolai	**Proaktyvieji**	**Reaktyvieji**	**Hibridiniai**	**Geografiniai**
Ryšio užlaikymas	Labai mažas	Labai didelis	Vidutinis	Labai mažas
Mobilumo įtaka	Didelė	Didelė	Didelė	Labai didelė/labai maža
Išplečiamumas (mazgų)	Labai mažas	Mažas	Vidutinis	Labai didelis
Išplečiamumas (srautų)	Labai didelis	Labai mažas	Vidutinis	Labai didelis

2.7.2.Proaktyvieji maršrutizavimo protokolai

Proaktyvieji protokolai naudoja panašų į laidinius tinklus požiūrį. Mazgai dalyvaujantys proaktyviajame maršrutizavime, žinutėmis apsikeisdami su kitais tinklo mazgais sudaro maršrutizavimo lentelę. Keliai yra apskaičiuojami ir sudaromi iš anksto, net jei tinklu nėra perduodami duomenys.

Vienas iš pavyzdžių - *ADV* protokolas, tačiau šis protokolas yra hibridinis, t.y. turintis ir aktyviojo ir proaktyviojo savybių. Pagrindinės charakteristikos yra proaktyviojo, kadangi maršrutai yra atnaujinami nuolat. Aktyviojo savybės susideda iš dviejų aspektų: tik aktyvių imtuvų maršrutai yra aptarnaujami, maršrutų atnaujinimas vykdomas atsižvelgiant į tinklo sąlygas. Protokolas adaptyvus, nes maršrutai keičiasi dinamiškai pagal tinklo būseną. Jis remiasi nuotolio vektorių algoritmu bei naudoja sekų numerius. Šie sekų numeriai padeda sumažinti papildomų antraščių dydį, reikalingą lentelių sudarymui. Tai vienas iš pagrindinių protokolo privalumų. Protokole lentelės atnaujinamos trimis atvejais: mazgas buferyje laiko informaciją dėl nežinomo maršruto, vienas ar keli kaimynai paprašo naujo maršruto, kiti mazgai siekia nustatyti teisingus ir nebeegzistuojančius maršrutus [29, 51, 52].

2.7.3.Reaktyvieji maršrutizavimo protokolai

Reaktyvieji protokolai (taip pat žinomi kaip „pagal pareikalavimą“) kelio ieško tik tokiu atveju, kai reikia – kitaip sakant, siuntėjo mazgas nežino kelio, kuriuo bus pasiektas adresatas, todėl tai padidina duomenų perdavimo užlaikymą, kadangi siuntėjas turi laukti kol bus surastas maršruto kelias. Hibridiniais maršrutizavimo protokolais vadinami tokie, kurių negalima priskirti pastarosioms dviem grupėms. Tipinis to pavyzdys – proaktyvusis elgesys siunčiant vieniems adresatams ir reaktyvusis – kitiems.

Vienas iš populiariausių – *AODV* protokolas. Jis prisitaiko prie dinaminių ryšio sąlygų ir tuo pačiu reikalauja nedidelių skaičiavimo ir atminties resursų. Protokolas gali veikti tiek *unicast*, tiek ir *multicast* režimais. Kiekvienas tinklo mazgas turi lentelę, skirtą tinklo topologijos sekimui. Kol maršrutas yra galiojantis, jis yra nuolat atnaujinamas pagal sekos numerį. *AODV* veikia su maršruto prašymo/atsakymo ciklu, kuriam reikalingos 3 komandos: *RREQ*, *RREP* ir *RERR*. Transliacijos prašymas yra generuojamas naudojant *RREQ*. Kai adresatas yra surastas, *RREP* yra išsiunčiamas atgal siuntėjui. Jei yra aptinkama nutrūkusi jungtis – sugeneruojama *RERR* žinutė. [49, 51, 52].

2.7.4.Geografiniai maršrutizavimo protokolai

Prie šio klasifikavimo galima pridėti dar vieną kategoriją – geografinį maršrutizavimą. Jis paprastai veikia „pagal pareikalavimą“ principu, tačiau ženkliai skiriasi nuo tradicinių reaktyviųjų maršrutizavimo protokolų. Vietoj maršrutizavimo remiantis tinklo topologija, geografiniai protokolai priima maršrutizavimo sprendimus šuolis po šuolio su kiekvienu paketu. Kiekvienas persiuntėjas pasirenka sekantį šuolį remiantis jo paties pozicija, kaimynų pozicija ir paskirties pozicija [51, 52].

2.7.5.Maršrutizavimo protokolų techniniai apribojimai

Kadangi *VANET* yra viena iš *MANET* tinklų rūšių, maršrutizavimo protokolų sprendimai turėtų būti panašūs abiejų rūšių tinklams, tačiau *VANET* turi specifinius reikalavimus bei turi specifinės papildomos informacijos (pozicija, greitis, kryptis ir kt.), kurią galima panaudoti maršruto parinkimui. Susumavus visą informaciją sudaryti techniniai maršrutizavimo protokolų apribojimai [1, 53]:

1. Išplečiamumas. Dauguma maršrutizavimo protokolų, skirtų *MANET* tinklams, palaiko ribotą mobilių mazgų skaičių (apie 200). Šiuose protokoluose naudojami kelio apskaičiavimo mechanizmai yra labai reiklūs resursams dideliuose tinkluose, tokiuose, kaip *VANET*. Pvz. proaktyviuose protokoluose visuose mazguose yra saugomos maršrutizavimo lentelės, kas *VANET* atveju yra praktiškai neįmanoma.

2. Pilnas pasiekiamumas. Ši prielaida nėra realistinė *VANET* tinkluose, kadangi jei paketo siuntimo momentu paskirties adresas yra nepasiekiamas, gali būti nevienalaikis kelias tarp šaltinio ir paskirties. Tai reiškia, kad automobilis gali judėti saugodamas tą paketą, kol galiausiai paskirties adresas bus pasiekiamas. Ši paradigma vadinama užlaikymui tolerantišku tinklu (angl. *DTN – delay tolerant networking*).
3. Mobilumo spėjimas. Dauguma *MANET* maršrutizavimo protokolų neatsižvelgia į atskirus mazgų mobilumo šablonus, o atsižvelgia tik į bendruosius. Galima sukurti tokius protokolus, kurie atsižvelgtų į mobilumą, kuris tam tikrais atvejais gali būti nuspėjamas, ypač *VANET* atvejų, kur automobilių judėjimas yra apribotas gatvėmis, greičio apribojimais, ženklais, šviesoforais. Tradiciniai *MANET* maršrutizavimo sprendimai neišnaudoja apriboto mobilumo privalumų.
4. Platus užtvindymo naudojimas. Dauguma *MANET* maršrutizavimo protokolų remiasi užtvindymo metodais. Reaktyviuosiuose protokoluose duomenų siuntėjas naudoja užtvindymą tam, kad rastų kelią iki adresato. Proaktyviuosiuose protokoluose kiekvienas mazgas periodiškai siunčia kontrolines žinutes kaimyniniams arba viso tinklo mazgams. Šios operacijos sunaudoja didelę dalį kanalo pralaidumo ir stipriai sumažina viso tinklo spartą, kas itin atsiliepia didelio masto tinklams, tokiems kaip *VANET*, todėl protokolų žinučių užtvindymas turi būti apribotas.

3. Pagrindinės problemos su kuriomis susiduriama automobilinės komunikacijos tinklų moksliniuose tyrimuose

Didelio kiekio skirtingų paslaugų teikimui automobilinėje aplinkoje reikalingos veiksmingos ir efektyvios specifinės radijo resursų valdymo strategijos, tarp kurių: talpumo padidinimo, interferencijos valdymo, prieigos kontrolės, dažnių juostos rezervavimo, paketų praradimo, užlaikymo sumažinimo, paketų tvarkaraščių sudarymo, patikimumo užtikrinimo ir kt. Nepaisant fakto, kad automobiliai (tinklo mazgai) dažniausiai yra organizuojami *ad-hoc* būdu, šie tinklai iš esmės skiriasi nuo tradicinių mobilių *ad-hoc* tinklų (*MANET*), atsižvelgiant į tinklo architektūrą, naudojamus mobilumo modelius, energetinių resursų apribojimus ir kt. parametrus. [12].

Atliktuose tyrimuose [52, 53, 54, 56, 55] buvo įrodyta, kad didelio masto automobilinės komunikacijos tinklams su dideliu greičiu judančiais automobiliais, tiesiogiai taikant metodus, sukurtus *MANET* tinklams yra neveiksminga ir neefektyvu. Taigi, norint pasiekti gerų rezultatų, masiniam automobilinės komunikacijos tinklų įdiegimui būtina sukurti naujas efektyvesnes, būtent šiems tinklams skirtas strategijas. Pateikiamos pagrindinės problemos su kuriomis susiduriama automobilinės komunikacijos tinklų moksliniuose tyrimuose:

- **Dažnas mazgų atsijungimas**. Dėl didžiulio automobilių mobilumo, automobilinės komunikacijos tinklų topologija dažnai keičiasi, tuo pačiu sukelianti komunikacijų nutrūkimą. Skirtingai nuo *MANET*, automobiliai juda dideliu greičiu (100 km/h ar daugiau užmiestyje), todėl resursų paskirstymas ar jų teikimas tampa sudėtingas, dėl dažnai nutrūkstančio ryšio tarp siuntėjo ir gavėjo [57]. Pvz., jei siuntėjas juda 120 km/h, o gavėjas – 100 km/h greičiu ta pačia kryptimi, o duomenų perdavimo nuotolis yra 300 metrų, ryšys tarp šių mazgų gali būti apie minutę laiko. Tiems patiems automobiliams judant priešingomis kryptimis, komunikacija gali trukti vos mažiau nei 5 s. Taigi, prisijungimo galimybių analizės bei į mobilumą orientuotas resursų paskirstymas yra ypač svarbūs.
- **Labai dinamiškos eismo sąlygos**. Automobilių tankumas automobilinės komunikacijos tinkle gali kisti nuo labai mažo (užmiestyje) iki labai didelio (transporto kamščiuose). Transporto srautas tam tikroje vietoje taip pat gali labai skirtis skirtingu paros metu. Greitai kintančios eismo sąlygos vis dar yra itin sudėtingas uždavinys, ypač atsižvelgiant į tai, kad pradinėse *VANET* diegimo stadijose tik maža dalis automobilių bus aprūpinta prisijungimo prie šio tinklo galimybėmis. Mažas tinkle veikiančių automobilių skaičius gali sąlygoti dažno tinklo fragmentavimo problemas, kur *VANET* pasiekiamumas gali būti prastas. Dar vienas susirūpinimą keliantis faktas yra dėl dinamiškų eismo variacijų galimas lėtas arba greitas fedingas (radijo bangų priėmimo susilpnėjimas arba visiškas nutrūkimas dėl pakitusių radijo bangų sklidimo sąlygų). Greitas fedingas gali pasireikšti situacijose su mažu automobilių tankumu, kai jie juda dideliu greičiu. Lėtas fedingas gali pasireikšti situacijose su dideliu automobilių tankumu, pvz. eismo kamščiuose. Kanalo sąlygos gali smarkiai varijuoti laiko ir erdvės atžvilgiu, taigi labai svarbūs ir reikalingi adaptyvūs kanalų pasiekimo protokolai, atsparūs kanalų suprastėjimui [53, 58, 59, 60, 61].
- **Duomenų sklaidos heterogeniškumas**. *VANET* apima platų eismo saugumo bei multimedija paslaugų spektrą. Eismo saugumo užtikrinimo paslaugoms būtinas žemas vėlinimo laikas, bei aukštas patikimumas, tuo tarpu, multimedija paslaugoms – duomenų perdavimo sparta, žemas paketų praradimas, resursų panaudojimas. Heterogeninės informacijos paslaugoms teikti reikalingos kanalų pasiekimo bei resursų paskirstymo strategijos, kurios turi būti adaptyvios ir užtikrinti efektyvią, organizuotą komunikaciją tarp automobilių bei *RSU*. Yra aišku, kad automobilių komunikacijos tinkluose su saugumo susijusioms žinutėms turi būti priskirtas aukštas prioritetas. Reikalingi efektyvūs ir veiksmingi komunikacijos požiūriai, galintys užtikrinti eismo saugumo bei multimedija paslaugų teikimą itin dinamiškoje automobilinėje aplinkoje [12, 62].

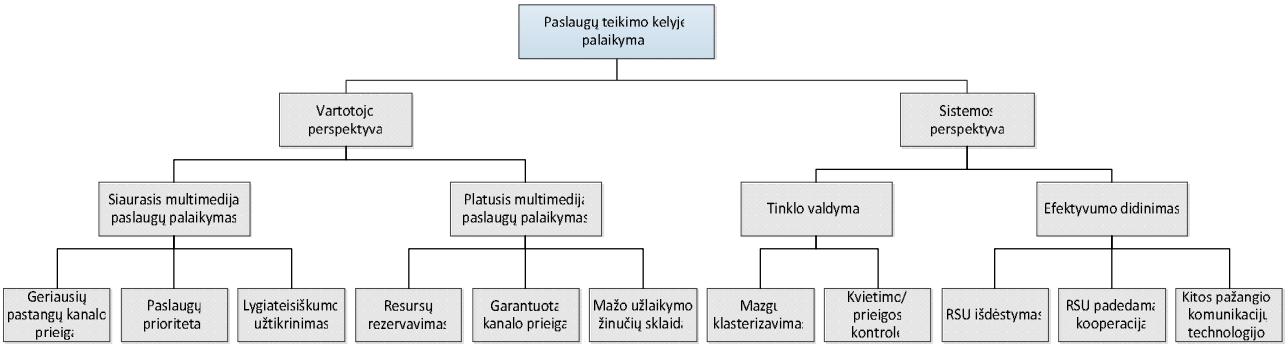
Reikia pažymėti tai, kad ryšio sluoksnio protokolų bei metodų lygmenyje negalima visiškai išspręsti specifinių aukščiau nagrinėtų automobilių komunikacijos techninių problemų. Tam reikalingas holistinis sprendimas, apimantis atskirų *VANET* protokolo steko savybes.

4. Paslaugų teikimas VANET tinklais iš vartotojo perspektyvos

4.1. Mokslinių tyrimų probleminės sritys

Bevielėse sistemose, yra būtinas apibrėžti būdus, kuriais bevieliai mazgai turi bendrauti tarpusavyje bei dalintis tinklo resursais. Be tinkamo *MAC* sluoksnio koordinavimo gali kilti paketų kolizijos, sumažinančios duomenų perdavimo spartą, padidinančios paketų atmetimo kiekį bei lemiančias prastą radijo resursų panaudojimo lygį. Avarinėse situacijose įspėjančių žinučių perdavimo nesėkmės gali lemti katastrofiškas pasekmes. Nors egzistuoja daug vertingų mokslinių tyrimų susijusių su *MAC* protokolais, tačiau dauguma iš jų yra netinkami automobilinei aplinkai. Pastaraisiais metais buvo publikuoti tyrimai, kuriuose nagrinėjami konkrečiai *VANET* pritaikyti *MAC* protokolai. [63] siūlomi du dinaminiai konkurencinių langų mechanizmai, leidžiantys sumažinti spartos kritimą esant dideliam mobilumui. Pirmoji schema užtikrina dinamišką paslaugų prioritetų nustatymą panaudojant kaimyninius mazgus, o antroji – paslaugų prioritetus pagal mazgų santykinį greitį.

Kadangi automobilių komunikacijos tinklu bus teikiamos heterogeninės paslaugos, yra būtinas sisteminio lygmens resursų valdymo schemų sukūrimas šiems tinklams. Visų pirma, turi būti sukurtos efektyvios tinklo planavimo bei efektyvios sistemos resursų padidinimo metodikos, kurios leistų pagerinti tiek multimedija, tiek ir eismo saugumo paslaugų teikimo kokybę. Šiuo atveju, kanalų prieigos kandidatai padalinti į dvi kategorijas, atsižvelgiant į jų sukūrimo tikslą bei metodiką: siaurąjį multimedija paslaugų palaikymą ir platųjį multimedija paslaugų palaikymą. Siaurojoje kategorijoje yra nagrinėjamas ne realaus laiko eismas bei realaus laiko eismas be griežtų *QoS* reikalavimų, o plačiojoje – reikalingas tikslus *QoS* palaikymas. 8 pav. pateikta nagrinėjimo metu egzistuojančių komunikacijos požiūrių taksonomija.



8 pav. *Kelyje teikiamų paslaugų komunikacijos požiūrių taksonomija [12]*

Bevielės komunikacijos sistemose *QoS* spartos metrikos gali būti suskirstytos į tris kategorijas [64]: bitų lygio *QoS*, paketų lygio *QoS* ir iškvietimo lygio *QoS*. Skirtingoms

programoms, paprastai reikia skirtingo *QoS* lygio atitikimo. Realaus laiko programos (pvz. balso perdavimo) yra jautrios užlaikymui, kuriose paketai turi būti perduodami su mažu paketų atmetimo dažnumu, tačiau gali toleruoti aukštą bitų klaidų kiekį. Iš kitos pusės, duomenų perdavimo programos (pvz. taškas į tašką duomenų apsikeitimo) yra nejautrios užlaikymams, tačiau joms reikalingas itin auštas duomenų perdavimo tikslumas.

4.2. Siaurasis multimedija paslaugų palaikymas

Vienas iš minimalių *MAC* reikalavimų siaurajam multimedija paslaugų palaikymui *VANET* tinkluose yra palaikyti geriausių pastangų (angl. *best-effort*) paslaugas, tokias kaip interneto naršymas, apsikeitimas failais, reklama. Šio tipo protokolai yra skirti pigiems *VANET* su homogeninės informacijos paslaugomis. Heterogeninės informacijos paslaugoms teikti yra reikalingas paslaugų prioritetų nustatymas pagal paslaugų pobūdį. Pvz. video perdavimui priskiriamas aukštas prioritetas, o el. paštui – žemas [12].

4.2.1.Geriausių pastangų kanalo prieiga

Geriausių pastangų kanalo prieigos kūrimo tikslas – pralaidumo padidinimas, tuo pačiu kolizijų kiekį sumažinant iki minimumo. Šių paslaugų palaikymui plačiausiai naudojami yra *IEEE 802.11a*, *802.11b* ir *802.11g*. Kaip minėta ankščiau, remiantis šiais standartais buvo sukurtas *DSRC* standartas, skirtas *WAVE*, kitaip žinomas kaip *802.11p*. Šiame standarte naudojama patobulinta paskirstyta kanalo prieiga, kuri pirmiausia buvo aprašyta *IEEE 802.11e* [65] standarte. Terpės (angl. *medium*) prieigos metodai remiasi *CSMA* (angl. *carrier sense multiple access*) technologija [63]. Technologijos esmė – jei yra aptinkama, kad kanalas laisvas – automobilis siunčia paketus, kitų atveju siuntimas yra sustabdomas. *CSMA* taikymas didelio masto daugiašuoliuose tinkluose yra problemiškas dėl paslėptų terminalų (angl. *hidden terminals*), kas sukelia perdavimo kolizijas, bei atskleistų terminalų (angl. *exposed terminals*). kurie bereikalingai nuslopina radijo signalą, taip sukeldami sistemos spartos sumažėjimą [63]. Šioms problemoms spręsti bei pralaidumui padidinti, gali būti panaudojamas prašymo siųsti (angl. *request-to-send* (*RTS*))/ patvirtinimo siųsti *CTS* (angl. *clear-to-send*) mechanizmas. Siuntėjas pirmiausia išsiunčia *RTS* kadrą gavėjui. Jei *RTS* gautas sėkmingai, gavėjas atsako *CTS* kadru. Visi aplinkiniai automobiliai, girdintys *RTS* ar *CTS* kadro perdavimą, atideda savo paketų perdavimą.

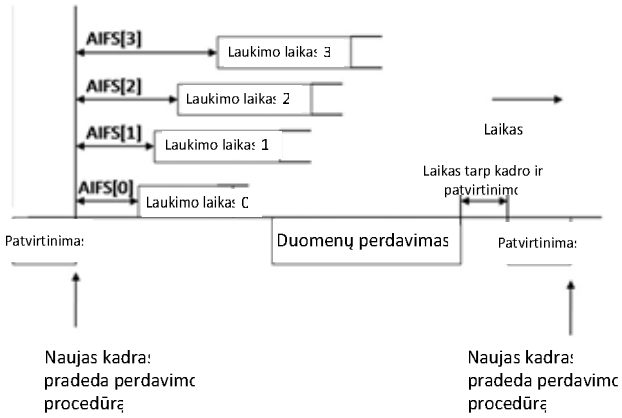
Kitas efektyvus metodas išvengti paketų kolizijoms *VANET* tinkluose yra signalų fliuktuacija. Naudojant šį metodą, gavėjas išsiunčia užimtumo signalą paketų priėmimo metu, kuris atlieka dvi funkcijas – siuntėjui patvirtina duomenų perdavimo galimybę, bei sustabdo paslėptų terminalų galima siuntimą. Šis metodas nėra toks populiarus kaip *CSMA* paremti metodai, kadangi sunaudoja daug elektros energijos. Kaip minėta anksčiau, energijos sunaudojimas yra svarbus

tradiciniuose *MANET*, tačiau *VANET* šio apribojimo neturi, todėl signalų fliuktuacija paremti protokolai gali būti vertingi praktiniame *VANET* įgyvendinime [12, 59, 66].

Šie išnagrinėti protokolai gali būti taikomi *VANET* tinklams su nedideliu-vidutiniu automobilių judėjimo greičiu, tačiau šių protokolų taikymas didelio mobilumo automobiliams yra neefektyvus. Be to, geriausių pastangų protokoluose nėra atsižvelgiama į prioritetus.

4.2.2.Paslaugų prioritetai

Vienas iš būdų pasiekti paslaugų diferencijavimą yra kanalo prieigos prioritetų nustatymas skirtingo tipo duomenų srautui [12]. *IEEE 802.11p/WAVE* standarte naudojama patobulinta paskirstytos kanalo prieigos (angl. *enhanced distributed channel access (EDCA)*) schema, kuri prioritetus suteikia pagal statistinius duomenis. Skirtingiems duomenų srautams yra priskiriamos skirtingos prieigos kategorijos (angl. *Access categories (AC)*). Aukštesnio prioriteto srautui yra priskiriamas mažesnis konkuravimo langas ir trumpesnis *AIFS* (angl. *arbitration inter-frame space*) [22].



9 pav. *Kanalo prieiga pagal skirtingus prioritetus EDCA mechanizme [24]*

9 pav. pateikta supaprastinta *EDCA* mechanizmo schema. Jei to paties tinklo mazgo, bet skirtingų eilių paketai konkuruoja dėl kanalo prieigos, virtuali sprendimų funkcija išsprendžia konfliktą ir siuntimo galimybę suteikia aukščiausio prioriteto eilei, o paketai iš žemesnio prioriteto yra persiunčiami pakartotinai arba atmetami [24].

Pastaruoju metu buvo pristatyta keletas mokslinių darbų, siekiančių patobulinti *EDCA* taikymui *VANET* sistemose. [67] siūlomas paskirstytas rūšiavimo mechanizmas (angl. *Distributed Sorting Mechanism (DSM)*), pagerinantis komunikacijos efektyvumą tarp automobilio bei *RSU*. *DSM* mechanizme, kiekvienas automobilis gali individualiai apskaičiuoti savo komunikacijos prioritetus, todėl laikas reikalingas pasiekti kanalą gali būti sumažintas. *DSM* naudojimas supaprastina *handoff* procedūrą ir sumažina tinklo apkrovą. [68] siūlo nesudėtingą, intraklasterinį resursų paskirstymo algoritmą, atsižvelgiantį į galios, subnešėjų priskyrimą bei paketų eilių sudarymą. [69] siūlomas panašus resursų paskirstymo algoritmas, pasiekiantis Pareto optimumą, ir

įrodantis metodo efektyvumą. Didelio masto *VANET* tinkluose su dideliu greičiu judančiais automobiliais kanalų priskyrimas, kur dažnių panaudojimas gali būti maksimizuojamas paskirstytu būdu išlieka atviru tyrimų klausimu. *SMUG* – hibridinis *MAC* protokolas siūlomas [40], suteikiantis prieigą prie transliuojamos medžiagos konkuravimu paremtu metodu automobilių komunikacijos tinkluose.

Praktiškai absoliučią paslaugų diferenciaciją garantuojančią schemą, palaikančią multimedija paslaugų teikimą su skirtingais *QoS* reikalavimais autoriai siūlo [70]. Paketų eilės sudarymas yra formuluojamas kaip optimalaus valdymo problema. *QoS* diferencijavimas yra parametrinis, kuris gali būti pasiektas paprasčiausiai iteraciniu būdu išsprendžiant apribotą kvadratinę optimizacijos problemą. Šis sprendimas gali būti įdiegtas į *EDCA* mechanizmą *IEEE 802.11p/WAVE* standarte, siekiant užtikrinti vėlinimui jautrių duomenų perdavimą. Šio metodo trūkumas – optimalaus valdymo problemos sprendimas naudoja daug skaičiavimo resursų.

Kaip matome iš išnagrinėtų schemų, paketų prioritetų sudarymas yra būtinas, norint pasiekti paslaugų diferenciaciją *VANET* tinkluose su heterogeninės informacijos srautais. Neatsižvelgus į nešališkumą, kai kurios žemo prioriteto paslaugos gali būti užgožtos per didelio kiekio aukšto prioriteto paslaugų. Šiai problemai išspręsti turėtų būti atsižvelgiama į teisingą prioritetų paskirstymą, kuriant kanalo prieigos protokolus.

4.2.3.Lygiateisiškumo užtikrinimas

Lygiateisiškumas yra svarbus efektyvumo matas, įvertinantis kaip teisingai tarp tinklo mazgų yra paskirstomi tinklo resursai. Yra nustatyta, kad *IEEE 802.11e* (*CSMA/CA*) *MAC* protokolas, kuris buvo patobulintas, negali pasiekti gerų efektyvumo rezultatų dėl binarinio eksponentinio *backoff* mechanizmo, kuriame naudojamas trumpesnis konkuravimo langas (angl. *contention window (CW)*). Trumpesnis *CW* sukelia rimtų problemų *multi-hop* automobilių tinkluose su dideliu kiekiu automobilių aprėpties zonoje, kur yra daug paslėptų terminalų (automobilių). Taigi, tokiu atveju gali būti šimtai automobilių, interferuojančių tarpusavyje, taip sukeldami didelį kiekį kolizijų ir lemdami sumažėjusią duomenų perdavimo pralaidumą [76]. *CSMA/CA* paremtas *MAC* protokolas, kuriame atsižvelgiama į resursų paskirstymo lygiateisiškumą buvo pasiūlytas [72]. Šioje schemoje kiekvienam mazgui pagal judėjimo greitį yra suderinama duomenų perdavimo tikimybė laiko atkarpoje. Tai atliekama keičiant *CW* dydį. Rezultatai rodo, kad ši schema iš dalies padeda išspręsti lygiateisiško resursų paskirstymo problemą. Ši problema taip pat plačiai išnagrinėta [63]. Darbe atliekamas išsamus mobilumo įtakos *IEEE 802.11p MAC* protokolo efektyvumui tyrimas. Taip pat, siūlomi du dinaminių langų mechanizmai, leidžiantys sumažinti tinklo spartos kritimą, esant dideliam mobilumui. Lygiateisiškai kanalo prieigai užtikrinti gali būti pasitelkta ir neraiškioji logika (angl. *fuzzy logic*). Yra pasiūlytas konkuravimu paremtas *MAC* protokolas, kuris

remiasi neraiškiosios logikos taisyklių rinkiniu, siekiant užtikrinti teisingą resursų panaudojimą tarp automobilinių mazgų [73].

Taigi, geriausių pastangų kanalų prieiga yra būtina, siekiant užtikrinti pagrindines informacines-pramogines paslaugas be *QoS* reikalavimų. Norint užtikrinti siaurąjį heterogeninės informacijos multimedija paslaugų palaikymą, yra reikalinga paslaugų diferenciacija. Teisingam resursų paskirstymui tarp automobilių yra reikalingi kanalų prieigos algoritmai, atsižvelgiantys į lygiateisiškumą. Norint pasiekti aukštą *QoS* tikslumą plačiam multimedija paslaugų palaikymui ir garantuoti prieigą eismo saugumo programoms yra būtini *MAC* sluoksnio resursų rezervavimo mechanizmai [12].

4.3. Platusis multimedija paslaugų palaikymas

Be siaurųjų multimedija paslaugų palaikymo, tikimasi, kad *VANET* ateityje palaikys platų spektrą multimedija ir eismo saugumo programų pritaikymą: nuo interaktyvių žaidimų iki auto įvykių išvengimo įspėjimų. Šioms sritims reikalingi itin griežti *QoS* reikalavimai, tokie kaip vėlinimo laikas ir patikimumas, kas reiškia, kad ankstesniame skyriuje išanalizuoti kanalų prieigos metodai yra nebetinkami. Visais atvejais resursų rezervavimas išlieka pagrindiniu tikslaus *QoS* užtikrinimo elementu. Siekiant toliau užtikrinti eismo saugumo efektyvumą, reikalingi nekonkurenciniai kanalų prieigos metodai, skirti periodiniam su eismu susijusiai informacijai perduoti ir patikimi mechanizmai – galinio taško į galinį tašką (angl. *end-to-end*) paketų perdavimui su minimaliu vėlinimu, skirti itin jautrioms vėlinimui avarinių situacijų įspėjimo žinutėms [12].

4.3.1.Resursų rezervavimas per konkuravimą

Konkuravimas dėl kanalų yra dažniausiai naudojamas resursų rezervavimo realizavimo būdas [71]. Jei rezervacijos prašymas yra patvirtinamas, automobilis gali užsirezervuoti tam tikrą resursų kiekį (pralaidumo, kanalų) paketų perdavimui. Naudojant *SRMA/PA* (lengvą keleto prieigų rezervavimą su prioritetų priskyrimu (angl. *soft reservation multiple access with priority assignment*)) resursai gali būti rezervuojami tiek realus laiko srauto, tiek ir ne realaus laiko per sėkmingus konkuravimo bandymus. Šiame protokole, aukštesnio prioriteto srautas gali užimti žemesnio prioriteto srauto rezervuotus resursus. Šio metodo taikymas parodė teigiamus ir daug žadančius rezultatus, kadangi jį naudojant yra sumažinamas atmestų paketų skaičius realaus laiko sraute. Kadangi šis protokolas yra paskirstytas, reikalingas tikslus laiko sinchronizavimas. Tam galima panaudoti pozicionavimo sistemas, kadangi šiuo metu itin plačiai paplitę ir toliau sparčiai populiarėja *GPS* imtuvai, leidžiantys labai tiksliai sinchronizuoti laiką [74]. Šis metodas automobiliniuose tinkluose susiduria su dažno sąsajų atsijungimo problemomis. Jungiamumo kokybės pagerinimui yra siūlomas dinaminis perdavimo diapazono priskyrimo (*DTRA* - angl. *dynamic transmission-range-assignment*) algoritmas paremtas eismo srautų teorijomis. Žinant

automobilių tankumą, automobiliai perdavimo diapazoną gali suderinti taip, kad prailgintų ryšio laiką, taip pat pagerinant resursų rezervavimą [75].

Resursų rezervavimas per konkuravimą yra perspektyvus metodas, užtikrinantis aukšto detalumo *QoS* palaikymą realaus laiko srautams. Šis metodas yra mažiau efektyvus užtikrinant kritines eismo saugumo taikymo sritis. Itin jautrioms užlaikymui su eismo saugumo susijusioms žinutėms perduoti turi būti garantuota kanalo prieiga [12].

4.3.2.Garantuota kanalo prieiga

Saugumui užtikrinti reikalinga kanalo prieiga be konkuravimo, kurioje su eismu susijusios žinutės būtų perduodamos tiesiogiai automobiliams. Su periodiniu signalinių žinučių be kolizijų perdavimu, kiekvienas automobilis galėtų atnaujinti ir stebėti kaimyninių automobilių statusą: poziciją, greitį, pagreitį. Šioms idėjoms realizuoti, literatūroje buvo pasiūlyti centralizuoti resursų rezervavimo metodai, nukreipti į eismo saugumą. [76] pasiūlytas valdomas interneto prieigos protokolas su *QoS* palaikymu (*CVIA-QoS*), skirtas garantuoti *QoS* reikalavimų palaikymą realaus laiko srautui ir maksimizuoti pralaidumą priskiriant laisvą pralaidumą geriausių pastangų srautui. [77] pasiūlytas taip pat valdomas kanalo prieigos protokolas – *CEPEC* (angl. *coordinated external peer communication*). Šis protokolas pagerina *IEEE 802.16* savybes padidindamas duomenų perdavimo spartą, tuo pačiu užtikrindamas teisingą resursų paskirstymą tarp į segmentus suskirstytų automobilių. *CEPEC* yra nesudėtingas ir gali būti taikomas vėlinimui jautrioms saugumo užtikrinimo programoms.

Kaip bebūtų, dauguma mokslinių tyrimų orientuoti į *V2I* komunikacijas. Siekiant užtikrinti garantuotą kanalo prieigą *V2V* komunikacijose, galima pasitelkti *token ring* technologija paremtą *MAC* protokolą periodiškai be konkurencijos perduoti su eismu susijusioms žinutėms. [78] siūlomas *OTRP* (angl. *overlay token ring protocol*) protokolas, kuriame automobilių tinklas traktuojamas kaip iš dalies persiklojantys žiedai, kurių kiekvienas pasiunčia užimtumo signalą žiedais, užtikrinant duomenų perdavimo teisę. Žiedo struktūra yra dinamiškai reguliuojama pagal automobilių judėjimą. *OTRP* turi du veikimo režimus: normalų ir avarinį. Simuliacijų metu įrodyta, kad šis protokolas yra tinkamas su saugumo susijusioms žinutėms perduoti, tačiau nagrinėjama tik vieno kanalo prieiga ir visi automobiliai vertinami kaip vienodos svarbos.

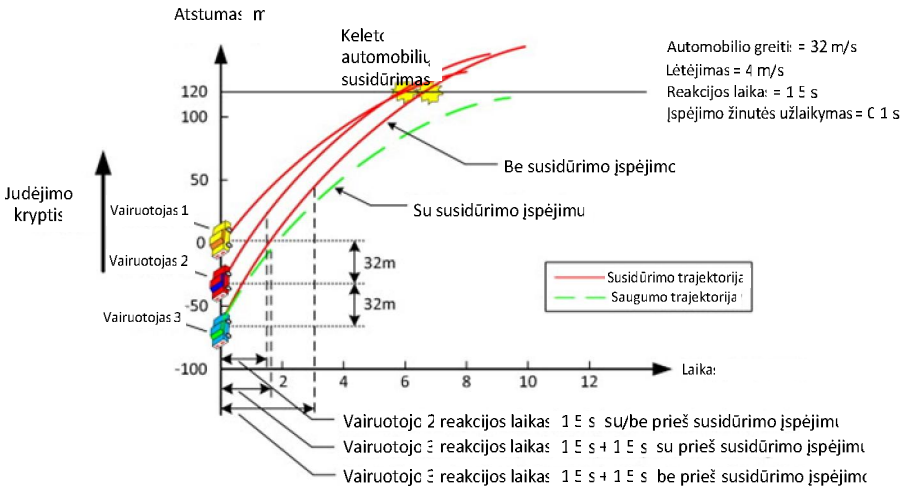
Dėl savo patikimumo, *CDMA* paremti kanalų prieigos metodai gali būti tinkami kandidatai aktyvioms ryšiu paremtoms saugumo priemonėms. [79] siūloma *MM-SA* (angl. *multicarrier multicode spread Aloha*) sistema paremta kodo padalijimo daugialypės prieigos technologija (angl. *code-division multiple access technology*) ir leidžia padidinti mazgų tankumą bei išspręsti paslėptų terminalų problemą. Rezultatai rodo, kad ši sistema gali užtikrinti eismo saugumo programoms reikiamą spartą. Nors saugumo žinutės gali būti paskleistos be užlaikymo, signalų išsklaidymas,

mažinantis duomenų perdavimo spartą stabdo *CDMA* technologijų panaudojimą *VANET* tinkluose. Norint šią technologiją sėkmingai pritaikyti plačiajam multimedija paslaugų palaikymui, reikalingi papildomi tyrimai. Saugumo žinučių ir kitų resursų panaudojimo dažnumas turi būti nustatomas pagal kelio bei eismo sąlygas. Dinaminio resursų rezervavimo schema prisitaikanti pagal situaciją pasiūlyta [80]. Tyrimas atskleidė, kad norint išlaikyti aukštą eismo saugumo lygmenį, periodinis signalinių žinučių perdavimas turi būti adaptyvus, atsižvelgiantis į kiekvieno bei aplinkinių automobilių judėjimą. Eismo saugumo bei multimedija paslaugų efektyvumo padidinimui reikalingi papildomi erdvės-laiko resursų rezervavimo tyrimai.

Vis dėlto, duomenų perdavimo užlaikymas gali atsirasti ir naudojant nekonkurencinius protokolus. Dėl didelio automobilių mobilumo, pavojaus zona (angl. *zone of danger (ZOR)*) gali būti pakankamai didelė. Eismo įvykio atveju reikalingos efektyvios *multi-hop* žinučių perdavimo schemos su mažu užlaikymo laiku.

4.3.3.Mažo užlaikymo žinučių sklaida

Nors šiandienos automobiliai yra aprūpinti daugybe aktyvaus saugumo užtikrinimo priemonių tokių kaip: žibintai, signalai, veidrodėliai, aktyvios stabdžių sistemos ir kt., tačiau dauguma avarijų įvyksta dėl žmogaus klaidų, todėl yra reikalingi pasyvūs saugumo užtikrinimo mechanizmai: saugos diržai, oro pagalvės, susilankstančios vairo kolonėles, šoninio smūgio saugos sistemos, apsaugančios vairuotojus bei keleivius avarijos atveju. Todėl, komunikacija paremtos aktyvios saugumo priemonės, aptartos ankstesniuose skyriuose gali tik iš anksto įspėti vairuotojus apie gresiantį pavojų. Kadangi šios priemonės vairuotojus turi įspėti kuo anksčiau, su saugumo susijusios žinutės turi būti perduotos su kuo mažesniu užlaikymu. Efektyvus būdas to pasiekti, avarinių žinučių perdavimui panaudoti atskirą kanalą. Vienas iš tokių pavyzdžių siūlomas [59], kur, kaip ir anksčiau minėtame metode, taikomas daugiakanalis *token ring* paremtas kanalų prieigos protokolas. Aptikus avarinę situaciją, žiedu dedikuoti kanalu perduodama avarinė žinutė visiems žiedo nariams be užlaikymo. Avarijos tikimybei sumažinti [81] siūloma prieš-susidūrimo įspėjimo sistema. Jei susidūrimas yra neišvengiamas, automobilis išsiunčia prieš-susidūrimo įspėjimo signalą aplinkiniams automobiliams, todėl netoliese esantys vairuotojai turi daugiau laiko sureaguoti bei išvengti susidūrimo. 10 paveiksle pateiktas prieš-susidūrimo įspėjimo sistemos schemos grafikas. Pvz. 1 vairuotojas 0 pozicijoje supranta, kad susidūrimas neišvengiamas ir ima staigiai stabdyti. Be prieš-susidūrimo įspėjimo sistemos, 2 ir 3 vairuotojai stabdyti pradėtų tik pamatę 1 automobilio stabdžių žibintus, kas sąlygotų 3 automobilių susidūrimą. Panaudojant tokią sistemą, į susidūrimą patektų tik 2 pirmieji automobiliai. Taip pat, kuo anksčiau vairuotojai būtų įspėti, tuo būtų mažesni avarijos padariniai.



10 pav. *Prieš-susidūrimo įspėjimo sistemos schemos grafikas [12]*

Komunikacijų aprėpčiai padidinti gali būti panaudotas galios valdymas, kuriame didesnė perdavimo galia būtų rezervuota avarinių žinučių perdavimui. Dėl maksimalios perdavimo galios ribojimų, ne visi automobiliai esantys *ZOR* galės būti informuoti apie pavojų. Efektyviam pavojaus zonoje esančių automobilių įspėjimui, reikalingi į vietovę atsižvelgiantys sklaidos protokolai. [82] atliko išsamią susidūrimo išvengimo pagalbos sistemų analizę, kurioje išnagrinėtos literatūroje siūlomos sistemos bei autorių pasiūlyta nauja sistema. [83] nagrinėjamas įvykių laikas ir kaip jis veikia programine įranga paremtas susidūrimo išvengimo strategijas *DSRC* komunikacijoje. Nustatyta, kad pagrindiniai apribojimai yra ryšio vėlinimas, aptikimo nuotolis, kelio sąlygos, vairuotojo reakcija ir lėtėjimo greitis. [84] siūlomas vienos krypties eismo transliacijos (angl. *broadcast*) avarinių žinučių sklaidos protokolas, kuriame prieš išsiunčiant žinutę, automobilis pirmiausiai patikrina ar iš priešais važiuojantis automobilis neišsiuntė tos pačios žinutės, taip siekiant sumažinti žinučių užtvindymą.

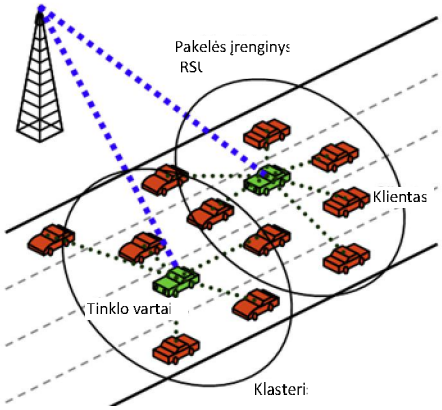
5. Kelyje teikiamų paslaugų palaikymas automobilinės komunikacijos tinkluose iš sistemos perspektyvos

5.1. Mokslinių tyrimų probleminės sritys

Ankstesniame skyriuje buvo išanalizuotas eismo saugumo ir multimedija paslaugų palaikymas iš vartotojo perspektyvos, tačiau be puikiai organizuoto sisteminio lygmens resursų valdymo šie pasiūlyti metodai būtų mažiau efektyvūs arba visai netinkami. Šiame skyriuje nagrinėjami du pagrindiniai paslaugų teikimo kelyje uždaviniai iš sistemos perspektyvos: tinklo valdymas ir efektyvumo didinimas. Paslaugų tiekėjui pagrindiniai sisteminio lygmens tikslai yra padidinti vartotojų skaičių ir pagerinti eismo saugumą. Kaštų sumažinimui ir įdiegimo paspartinimui dažniausiai pasirenkamas decentralizuotas valdymas, kur duomenų mainai gali būti palengvinami klasterizuojant tinklo mazgus. Norint patenkinti vis didėjančius *VANET* taikymo sričių reikalavimus, reikia didinti tinklo efektyvumą, įskaitant vėlinimo mažinimą bei

komunikacijos patikimumą. Sistemos efektyvumas gali būti padidintas optimaliai išdėstant *RSU*, bendradarbiaujant tinklo mazgams bei kitomis pažangiomis komunikacijų technologijomis [12].

Siekiant efektyviai valdyti didelio masto bevielius tinklus, buvo pasiūlyta tinklo mazgus klasterizuoti. Šiuo atveju, bevielis tinklas yra padalinamas į keletą klasterių, į kuriuos įeina pagal tam tikrus parametrus atrenkami mobilūs mazgai. Įvairūs pasikeitimai yra perduodami lokaliai klasteryje. Tai sumažina perduodamų žinučių kiekį, taip padidinant tinklo stabilumą bei efektyvumą, kadangi naudojant nekonkurencinį paketų perdavimą yra efektyviai sumažinamas užlaikymas ir žinutės yra perduodamos efektyviau [85, 86, 87]. 11 pav. pateiktas klasterizavimu paremtas duomenų perdavimo V2I komunikacijoje modelis.



11 pav. *Klasterizavimu paremtas duomenų perdavimas V2I komunikacijoje [30]*

Mokslinėje literatūroje yra daug tyrimų apie bevielių tinklų klasterizavimą. Klasterizavimas bevieliuose jutiklių tinkluose buvo tirtas [69], [88], [89]. [90] buvo atlikta šiems tinklams skirtų klasterizavimo algoritmų analizė. [86], [87], [91] buvo tirtas klasterizavimas mobiliuose *ad-hoc* tinkluose. Keletas naujausių tyrimų analizuoja klasterizavimą būtent *VANET* tinkluose, nors tai išlieka rimta tyrimų tema. [85] siūlomas klasterizavimo algoritmas remiasi kaimynais, esančiais dinaminėje aprėpties zonoje, automobilių judėjimo kryptimi, entropija. [92] siūlomas paprastas ir efektyvus duomenų sklaidos protokolas skirtas tankiems automobilių tinklams. Šiame protokole išvengiame transliacijos audros problemos, kylančios tankiuose tinkluose. Taip pat siūlomas pasisveikinimo žinučių mechanizmas, kuriame dalyvauja tik dalis tinklo automobilių. [93] siūlomas klasterizavimu paremtas metodas, kuriame yra laviruojama tarp nekonkurencinio ir konkurencija paremtų *MAC*, siekiant palaikyti skirtingus saugumo ir ne saugumo žinučių reikalavimus. [94] yra pasitelkiamos transporto srautų teorijos, siekiant nustatyti avarinių žinučių užlaikymą klasterizuotuose tinkluose.

Efektyvaus kanalų priskyrimo ir mazgų klasterizavimo algoritmai, kurie atsižvelgtų į tikslius *QoS* reikalavimus reikalauja papildomo tyrinėjimo. Didelio mobilumo aplinkoje, klasteriai gali gyvuoti labai trumpai, tuo sumažindami duomenų sklaidos efektyvumą.

5.2. Našumo didinimas

5.2.1. *RSU* išdėstymas

Optimalus *RSU* išdėstymas yra efektyvus būdas, leidžiantis ženkliai padidinti *VANET* efektyvumą bei sumažinti sistemos įdiegimo kaštus, kadangi *RSU* yra labai brangūs įrenginiai. Strategiškai išdėsčius *RSU* pagal greitkelį arba miesto gatves, galima ne tik išspręsti dažno tinklo fragmentavimo problemą, bet ir užtikrinti efektyvią ir patikimą eismo saugumo, informacinės bei multimedija informacijos sklaidą. Svarbi eismo informacija, tokia kaip kelio sąlygos, gali įspėti vairuotojus apie gresiančius pavojus: prastas kelio sąlygas, slidžią kelio dangą ar kelio remontą. Taip pat, naudojant *RSU*, vėlinimo laikas ir komunikacijos patikimumas gali būti pagerinti, dėl didesnės aprėpties zonos. [95] buvo nustatyta, kad tinkamai išdėsčius *RSU*, sėkmingai perduotų žinučių skaičius išauga 13%. *RSU* tinkamiausią išdėstymą galima nustatyti ir sprendžiant optimizacijos uždavinius. Tokius uždavinius, pasinaudojant genetiniais algoritmais sprendė [96]. [97] buvo įrodyta, kad optimalaus *RSU* išdėstymo uždavinys gali būti išspręstas klasikiniu aproksimacijos algoritmu. [98] sprendžiama maksimalios aprėpties problema (*MCP* - angl. *Maximum Coverage Problem*), tuo pačiu siekiama maksimizuoti automobilių, kontaktuojančių su *RSU* skaičių. Problemos sprendžiamos euristiniais algoritmais. Autoriai nustatė, kad optimalus *RSU* išdėstymas įmanomas tik žinant automobilių mobilumo charakteristikas. [99] autoriai analizuoja mobilaus sensorių tinklo architektūrą, kurioje itin didelis kiekis mobilių sensorių, judančių pagal atsitiktinio žingsnio bei Gauso-Markovo mobilumo modelius, kurių informaciją surenka vienas mazgas. Buvo įrodyta, kad sistemos efektyvumas priklauso ne tik nuo mobilumo ir aprėpties, tačiau ir nuo surinkimo mazgų išdėstymo.

Nors optimalaus *RSU* išdėstymo problemų sprendimai gana dažnai sutinkami literatūroje, tačiau jų išdėstymas, atsižvelgiant į multimedija paslaugų teikimą nėra plačiai išnagrinėtas. [100] nagrinėjamas *RSU* išdėstymas, kuriame būtų galima maksimaliai užtikrinti *QoS* palaikymą. Siekiama minimizuoti vidutinį šuolių kiekį nuo *RSU*, taip sumažinant vėlinimo laiką ir padidinant komunikacijos efektyvumą. [28] nagrinėjamas optimalus persiuntimo stočių išdėstymas *802.16* tinkle, pasitelkiant greitkelio mobilumo modelius. Persiuntimo stočių parinkimas formuluojamas, kaip netiesinės optimizacijos problema, kurios tikslas rasti optimalią persiuntimo stotį, norint pasiekti maksimalų abonentinių stočių skaičių. Naudojant šį metodą, abonentinių stočių skaičių galima padidinti 49,86%. [101] analizuojama, kurioje moduliacijos zonoje nuo bazinės stoties reikia statyti retransliacijos stotis, norint turėti maksimalų tinklo pralaidumą. Siekiant užtikrinti aukščiausios kokybės interneto ryšį buvo išanalizuotas abonentų skaičiaus poveikis tinklo pralaidumui, bei slotų užimtumas kadre, o taip pat nustatytas optimalus, prijungtų prie vienos bazinės stoties retransliacijos stočių skaičius.

5.2.2.*RSU* padedama kooperacija

Tinkamas mazgų bendradarbiavimas gali padidinti sistemos efektyvumą bei padidinti perduodamų duomenų tikslumą. [102] nagrinėjamas bendradarbiavimu paremtas resursų priskyrimo modelis su *QoS* palaikymu. Siūlomi du nesudėtingi, bet efektyvūs metodai, paremti *Karush-Kuhn-Tucker* [103] interpretacijomis ir skirti bevieliams mesh tinklams. Dėl didelio automobilių mobilumo, komunikacijos kanalai yra linkę į greitą fedingą ir tokiu atveju negali būti užtikrintas patikimas ryšys [104]. [105] analizuojamas bendradarbiavimo diversiškumas, paremtas Nakagami fedingu [106]. Tiriama pastiprinimo ir persiuntimo schema, kurioje *RSU* padeda kiti automobiliai, veikiantys kaip persiuntėjai. Rezultatai rodo, kad ryšio kokybė gali būti pagerinta aukšto triukšmo lygio aplinkoje.

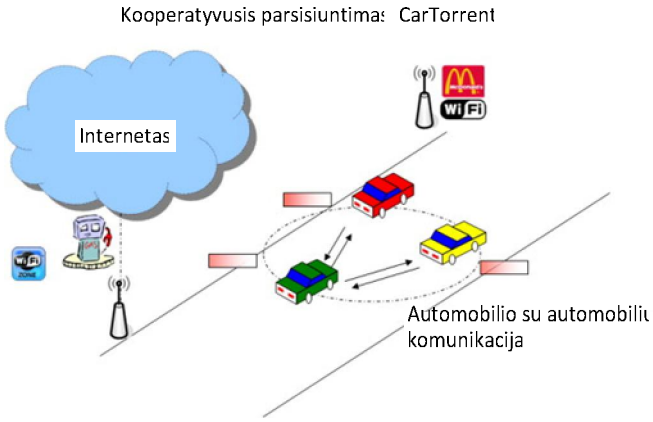
Kooperatyvus protokolas siūlomas [60], kurio tikslas – sumažinti atmestų paketų kiekį ir minimizuoti perdavimų kiekį. Tam pasitelkiama dvigubos fazės transliavimo strategija. Rezultatai rodo, kad šis metodas leidžia pasiekti beveik 100% pakėtų priėmimo santykį. Kitas kooperatyvus protokolas siūlomas [107]. Protokolas inicijuoja žinučių apsikeitimą su *RSU* ir pradeda mazgų kooperaciją tarp kaimyninių automobilių, siekiant padidinti tinklo efektyvumą. Nors tyrimų šia kryptimi daugėja, tačiau dar trūksta žinių apie tai, kada automobilių kooperacija yra naudinga ir kada – ne. Kaip integruoti automobilinius traukinius į automobilių kooperaciją taip pat įdomi bei reikalaujanti tolimesnių tyrimų sritis.

5.2.3.Kitos pažangios komunikacijų technologijos

Pažangios komunikacijos technologijos yra dažnai naudojamos bevieliuose tinkluose, siekiant padidinti komunikacijos efektyvumą. *MIMO* (angl. *multiple-input–multiple-output*) technologija gali būti panaudota siekiant padidinti sistemos pajėgumą (informacinėms, multimedija paslaugoms) ir spartą (eismo saugumo paslaugoms). [108] autoriai parodo, kad automobilių komunikacijoje naudojamas *MIMO* kanalų modelis, ženkliai skiriasi nuo įprastų bevielių tinklų. [109] siūlomas daugiakanalis *MAC* protokolas, skirtas didelio tankumo *VANET* tinklams, naudojant kryptines antenas. Rezultatai rodo, kad pasiūlyta schema užtikrina patikimą duomenų perdavimą. Kadangi automobilių judėjimas yra apribotas, yra tikimasi, kad kryptinėmis antenomis paremti komunikacijų protokolai gali būti tinkami praktiniame diegime.

Pastaruoju metu, nemažai dėmesio susilaukė tinklo kodavimo koncepcija. Pasitelkiant tinklo kodavimu paremtą informacijos sklaidą, gali būti padidintas sistemos efektyvumas: padidinta sparta bei sumažintas vėlinimo laikas [9]. Pirmiausia buvo pasiūlytas *SPAWN* [110] *BitTorrent* paremtas failų apsikeitimo protokolas *VANET* tinklams. Šiame protokole failas yra padalijamas į dalis ir įkeliamas į *RSU* serverį arba mobiliuosius mazgus. Kiekvienas failas turi unikalų *ID* ir kiekviena dalis turi unikalų sekos numerį. Mazgai kooperuodami apsikeičia turimomis dalimis.

Išplėsdami *SPAWN*, autoriai pasiūlė *CarTorrent* protokolą [111]. Šiame protokole mazgo artumas buvo pasirinktas pagrindiniu siuntimo mazgo pasirinkimo kriterijumi. *CarTorrent* naudojamas k-šuolių ribotas tikimybinis ir artimiausias-rečiausias pirmas metodai failo dalies pasirinkimui. Lee U., et al. pasiūlė *CodeTorrent* [48], tinklo kodavimu paremtą turinio sklaidos protokolą, kuris rėmėsi tuo, kad tinklo kodavimas gali išspręsti retų failo dalių problemą. 12 pav. pateiktas kooperatyvaus duomenų atsisiuntimo *CarTorrent* modelis.



12 pav. *Kooperatyvaus duomenų atsisiuntimo CarTorrent modelis [39]*

Kognityvūs radijo tinklai (angl. *cognitive radio networks - CRN*) yra plačiai tiriami, kaip galimas sprendimas dėl spektro perkrovimo ir licencijuotų vartotojų žemo spektro panaudojimo lygio [112]. Darbe analizuojamos efektyvaus maršrutizavimo *CRN* tinkluose problemos, atliekama išsami *CRN* maršrutizavimo apžvalga, siūlomos ateities tyrimų kryptys. [113] pristatoma technologija, kuri leidžia skirtingiems resursų apribotiems mazgams bendradarbiauti tarpusavyje, sprendžiant sudėtingas užduotis paskirstytu būdu. [114] analizuojami *CRN* tinklų uždaviniai, pricipai ir iškylančios problemos multimedija ir vėlinimui jautrios informacijos perdavime. Taip pat apibrėžiami atviri realaus laiko transporto tyrimų klausimai. [115] siūlomas autorių sukurtas reaktyvusis maršrutizavimo protokolas *CRN* tinklams, leidžiantis pasiekti 3 tikslus: išvengti interferencijos, atlikti bendrą kelio ir kanalo parinkimą, panaudoti keletą kanalų ir taip padidinti tinklo spartą. [116] yra analizuojamos *CRN ad-hoc* tinklų mokslinių tyrimų problemos, siūlomos naujos spektro valdymo funkcijos, nagrinėjamas paskirstytas koordinavimas.

Taigi, sisteminio lygmens resursų valdymas *VANET* tinkluose yra svarbus palaikant eismo saugumo bei multimedija paslaugų teikimą. Kaip bebūtų, reikalingi papildomi moksliniai tyrimai, nustatantys sisteminio lygmens resursų valdymo metodų efektyvumą *VANET* tinkluose su dideliu greičiu judančiais automobiliais [12].

6. Papildomų mokslinių tyrimų reikalaujančios probleminės sritys

6.1. Eismo saugumo, informacinių bei multimedija paslaugų teikimas bei integravimas įvairiomis eismo sąlygomis

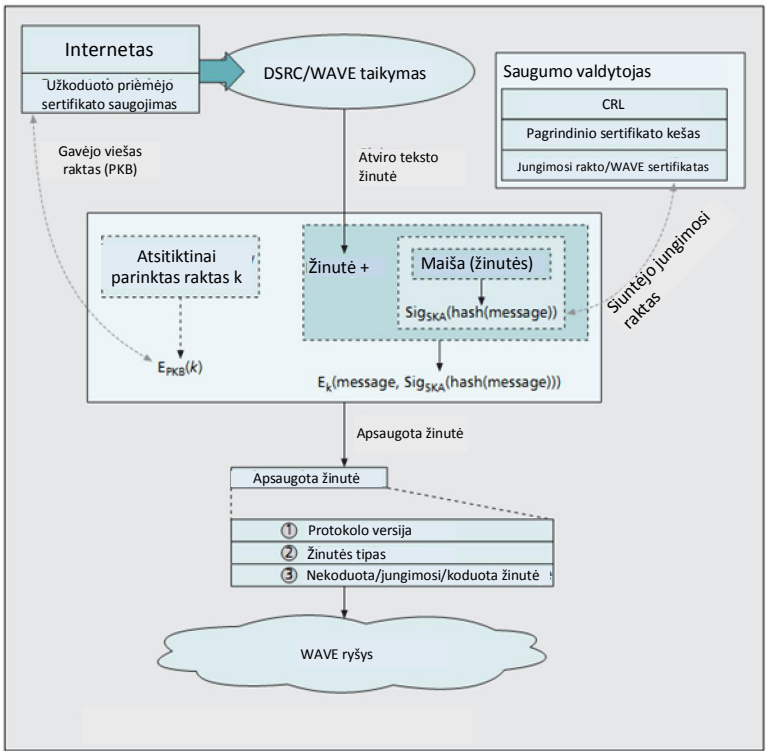
VANET tinkluose, palaikančiuose eismo saugumo, informacines ir multimedija paslaugas, yra būtina saugumo žinutėms priskirti aukščiausią prioritetą ir garantuoti prieigą prie resursų. Didelio masto tinkluose, eismo sąlygos bei vartotojų reikalavimai gali itin skirtis tiek laiko, tiek erdvės atžvilgiu. Deterministiniai kanalų prieigos protokolai yra mažiau efektyvūs, kur reikia aukšto tikslumo *QoS* palaikymo. Reikalingi nauji adaptyvūs resursų rezervavimo metodai bei tyrimai, pritaikyti didelio mobilumo *VANET* tinklams, palaikantys įvairias skirtingas programų kelyje kombinacijas.

6.2. Bevielio ryšio technologijos automobilinės komunikacijos tinklams

Šiuo metu viena iš aktualiausių bei gilesnių mokslinių tyrimų reikalaujančių sričių – bevielio ryšio technologijų panaudojimas automobilinės komunikacijos tinklams. Pastaruoju metu gana daug dėmesio susilaukė ir *VANET* integravimas su kitomis mobilaus ryšio sistemomis. Šių hibridinių *VANET*/*LTE*/mobiliojo ryšių sistemų priežastis ta, kad pradinėse *VANET* diegimo stadijose, tik maža dalis automobilių bus aprūpinta *OBU* įrenginiais. Vienas iš būdų padidinti šį skaičių – panaudoti paplitusią ryšių platformą kaip papildomą tinklą. Buvo nustatyta, kad kai kuriais atvejais mobiliuoju ryšiu paremtas *VANET* gali lenkti įprastus *VANET* pagal paketų pristatymo santykį. Efektyvių ir veiksmingų resursų valdymo metodų kūrimas integruotiems tinklams reikalauja papildomų tyrimų [12, 39, 117].

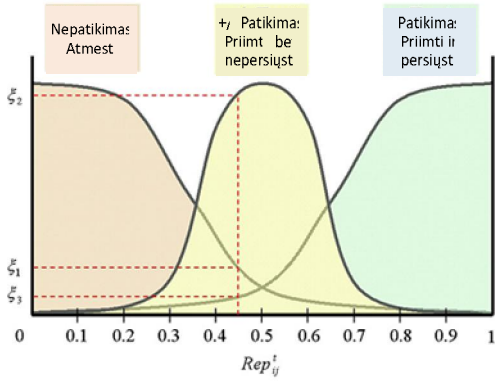
6.3. Privatumas ir saugumas automobilinės komunikacijos tinkluose

Nepaisant visų automobilinės komunikacijos tinklų suteikiamų privalumų, šie tinklai susiduria su įvairaus aspekto saugumo ir privatumo grėsmėmis. Kadangi tai yra specialios paskirties *MANET* tinklai, jie paveldi visus žinomus ir dar nežinomus *MANET* tinklų saugumo trūkumus. Vienų vartotojų vykdomos atakos, tokios kaip žinučių turinio pakeitimas, ar persiuntimo atakos, gali turėti fatališkas pasekmes kitiems vartotojams. Saugumo problemos *VANET* tinkluose yra dar sudėtingesnės dėl unikalių šių tinklų savybių, tokių kaip: didelis mobilumas, itin didelis kiekis tinklo mazgų, greitai besikeičianti topologija. Taip pat būtinas asmens duomenų privatumo užtikrinimas: asmens vardo, automobilio valstybinių numerių, greičio, pozicijos, maršruto ir kt., tuo pačiu paliekant galimybę valdžios institucijoms pasinaudoti šia informacija, esant svarbioms priežastims (nusikaltimo išaiškinimo ir pan.) [118]. 13 pav. pateikta *IEEE 1609.2* standarto saugumo paslaugų užtikrinimo konstrukcija, skirta apsikeisti žinutėmis tarp *WAVE* įrenginių.



13 pav. *IEEE 1609.2 standarto saugumo paslaugų užtikrinimo konstrukcija, skirta apsikeisti žinutėmis tarp WAVE įrenginių [118]*

Iki dabar, saugumo ir privatumo klausimai *VANET* tinkluose susilaukė gana nedidelio dėmesio mokslinėje literatūroje. [119] yra siūloma saugumo infrastruktūra *VANET* tinklams, kuri naudoja asimetrinę ir simetrinę kriptografiją bei sugadinimui atsparią įrangą. Rezultatai rodo, kad siūlomas metodas yra nereiklus skaičiavimo resursams ir nesunaudoja daug kanalo pralaidumo. [120] yra siūloma *TRIP* (angl. *trust and reputation infrastructure-based proposal for vehicular*) schema, pagrįsta pasitikėjimu bei reputacija. Taip pat, yra atliekama saugumo ir privatumo užtikrinimo sistemų analizė, siūloma reikalavimų specifikacija pasitikėjimo ir reputacijos modeliams. [121] yra siūloma pasitikėjimu ir biologija paremta schema, naudojanti *fuzzy* taisykles sprendimų priėmimui. 14 paveiksle pateiktas šio metodo panaudojimas pasitikėjimo lygių nustatymui.



14 pav. *Fuzzy logikos taisyklių panaudojimas pasitikėjimo lygių nustatymui [120]*

[122] yra siūlomas naujas portatyvus privatumą išsaugantis autentifikavimo ir prieigos kontrolės protokolas *PAACP* ne saugumo užtikrinimo programoms. [123] siūloma autentifikavimo schema, skirta sumažinti perdavimo (angl. *handoff*) vėlinimui. Schemoje *RSU* yra padalinti į pasitikėjimo grupes ir autentifikavimas yra atliekamas grupiniu metodu. [124] siūlomas programine įranga paremtas sprendimas, naudojantis tik du pasidalintus slaptus raktus ir užtikrinantis privatumą. Rezultatai rodo, kad su šiuo mechanizmu 45% yra padidinamas sėkmingai verifikuotų žinučių kiekis. Taip pat, siūlomas grupinės komunikacijos protokolas, leidžiantis autentifikuotis ir saugiai komunikuoti žinomos grupės automobiliams. Galiausiai, [125] yra siūloma privatumo nustatymo metrika *VANET* sistemoms. Autoriai atsižvelgia į tai, kad automobiliai dažniausiai važiuoja tuo pačiu maršrutu kasdien ir tokiu būdu, apie juos gali būti surenkama privati informacija. Darbe siūlomi algoritmai ir metodai, leidžiantys užtikrinti šios informacijos privatumą.

Saugumo ir privatumo srityje, ypač pastaraisiais metais daug nuveikė Xuemin S. su autorių kolektyvu. [126] siūloma saugi viešo rakto kodavimo schema, paremta kodavimo teorija, [127] siūloma pseudonominė autentifikavimo schema su stipriu privatumo išlaikymu, [128] siūloma robastinė parašo schema, naudojanti binarinius autentifikavimo medžius, [129] siūloma viešo rakto infrastruktūra, skirta apsaugoti bevielei automobilių komunikacijai, [130] pristatomas saugus viešo rakto kriptografijos protokolas multi-hop tinklams, [131] pateikiama į paslaugų saugumą orientuota schema, kuri remiasi automobilių mobilumo nuspėjimu, ir infrastruktūra paremta trumpalaikių sertifikatų schema, [132] nagrinėjama viena iš pavojingiausių atakų – paketų atmetimo ataka (packet drop attack). Siūlomas *SCM* (angl. *Side Channel Monitoring*) metodas, galintis aptikti šios atakos panaudojimo atvejus. [133] siūloma pasitikėjimu grindžiama autentifikavimo schema, *V2V* ir *V2I* komunikacijai, leidžianti sumažinti persijungimą tarp *RSU* įrenginių *802.11p* tinkluose.

Taigi, nors pastaraisiais metais padaugėjo mokslinių tyrimų saugumo ir privatumo užtikrinimo *VANET* tinkluose srityje, tačiau vis dar reikalingi *VANET* specializuoti sprendimai ir gilesni moksliniai tyrimai, galintys užtikrinti tiek eismo saugumo, tiek informacinių ir multimedija paslaugų saugumą bei privatumą.

6.4. Mobilumo modeliai

Tikslioms automobilių komunikacijos simuliacijoms reikalingi tikslūs, lengvai konfigūruojami mobilumo modeliai, atspindintys realią automobilinę aplinką. Nemažai darbų, nagrinėjančių realistišką mobilumą sutinkami literatūroje. Pvz. [1], [9], [63], [51] yra nagrinėjami mobilumo modeliai, tačiau jie apima tik nedidelę dalį komunikacinių scenarijų. Reikalingi papildomi mobilumo automobilinėje aplinkoje tyrimai, atsižvelgiantys į dinaminius erdvės ir laiko parametrus, laikinas kelio sąlygas ir t.t.

7. Mokslinių tyrimų projektai *ITS* ir automobilių komunikacijos srityse

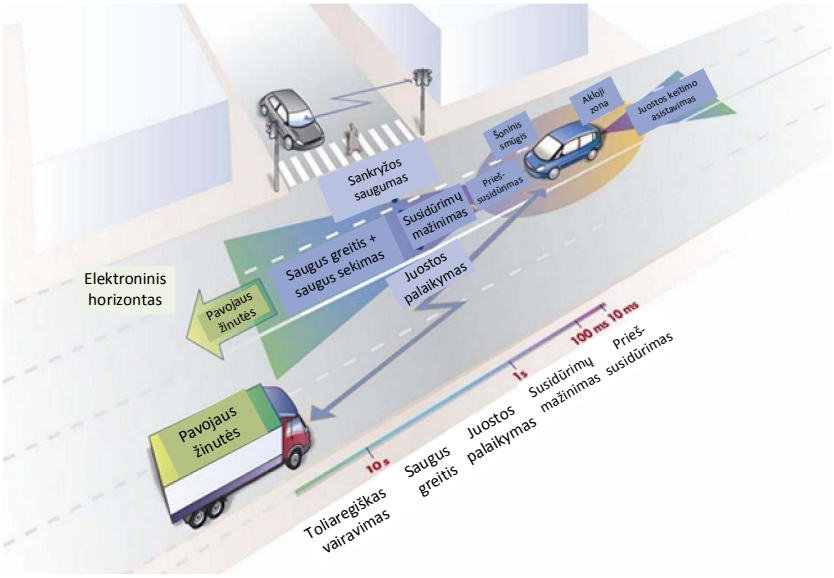
Tobulėjant bevielėms technologijoms, automobilinė komunikacija pastūmėjo didelį kiekį mokslinių tyrimų *ITS* srityje. Pirmieji tyrimų šioje srityje projektai buvo pradėti 1980 metais Japonijoje [12]. 1987 metais panašių *ITS* iniciatyvų buvo imtasi ir Europoje bei buvo pradėtas didelio masto projektas: *PROMETHEUS* – didžiausias visų laikų tyrimų ir plėtros *ITS* projektas, orientuotas į žmogaus nevaldomų automobilių sritį. Bendra projekto vertė – 749 milijonai eurų, įgyvendinime dalyvavo automobilių gamintojai iš 6 valstybių, elektronikos pramonės įmonės, universitetai, mokslinių tyrimų institutai, eismo inžinieriai ir valdžios institucijos. Buvo sukurtos eismo saugumo koncepcijos, bei pasiekti pionieriniai autonominio vairavimo rezultatai, kai du žmogaus nevaldomi automobiliai nukeliavo daugiau nei 1000 km, pasiekdami iki 130 km/h greitį, o vėliau ir sukonstruotas autonominis Mercedes-Benz automobilis, kuris nevaldomas nukeliavo 1600 km – iš Miuncheno į Kopenhagą. Maksimalus pasiektas greitis – 175 km/h su žmogaus įsikišimu vidutiniškai kas 9 minutes. Šio projekto pasiekimai davė pradžią visiems kitiems žmogaus nevaldomų automobilių tyrimams. Nepaisant visų pasiekimų, projektas susidūrė su iššūkiais, kadangi tuo metu dar nebuvo pigios radijo įrangos, navigacijos technologijų. Šiuo metu mobiliųjų technologijų bei pozicionavimo sistemų pasiekimai lėmė *V2X* tyrimų projektų atgijimą pastarajame dešimtmetyje [1, 10, 12].

Pagrindiniai V2X projektai Europoje:

FleetNet – Internet on the Road (2000 -2003). Vokietijos tyrimų projektas (partneriai: *Daimler Chrysler*, *FhG Fokus*, *NEC*, *Bosch*, *Siemens*, *Temic*). Vietoj *single-hop* transliavimo metodo, projekte buvo pasitelkti ad-hoc pricipai bei *multi-hop* tarpautomobilinė komunikacija. Nors idėja buvo naudotis ad-hoc komunikacijomis, orientuojantis į eismo saugumą, tačiau *Fleetnet* taip pat siekė sukurti komunikacijos platformą, paremtą *IP* protokolu ir tinkamą multimedijapaslaugų teikimui. Pagrindiniai sukurti metodai yra aktualūs ir šiandieną. Buvo nagrinėjamos įvairios, automobilinei komunikacijai preliminariai tinkamos radijo ryšio sistemos: *ULTRA-TDD*, duomenų perdavimas 24 GHz dažniu, *IEEE 802.11* technologija. Galiausiai buvo pasirinkta pastaroji, kadangi ji suteikė kompromisą tarp suteikiamos spartos, įrangos kainos ir prognozuojamos rinkos dalies. Buvo sukurti nauji pozicionavimu paremti maršrutizavimo protokolai, leidžiantys perduoti su saugumu susijusias žinutes visiems automobiliams, panaudojant vieną ar kelis automobilius kaip persiuntėjus [36].

CarTALK 2000 (2001-2004). Projektas buvo finansuojamas ES (partneriai: *CRF*, *Daimler*, *TNO*, *Bosch*, *Siemens*, *Cologne* ir *Stuttgart* universitetai). Pagrindinis tikslas – vairuotojui padedančių programų tyrimai, paremti ad-hoc tinklais. Šiam tikslui buvo sukurti specialūs savaime susiorganizuojančių ad-hoc tinklų protokolai. Kaip ir *Fleetnet* buvo remiamasi *WLAN* technologija. Buvo tiriama: automatinis įsiliejimas į eismą bei autotraukinių sudarymas [135].

IP PReVENT (2004-2006). Pagrindinis ES finansuojamo projekto tikslas – sukurti naują vairuotojų asistavimo sistemą, kuri leistų dvigubai sumažinti eismo įvykių skaičių iki 2010 metų. Buvo siekiama ne tik suteikti daugiau informacijos vairuotojui, bet ir sukurti visiškai automatizuotą eismo įvykių išvengimo mechanizmą [136]. 15 paveiksle pateikta *PReVENT* saugumo zonos apie automobilį vizija realizuojama viena kitą papildančiomis saugumo funkcijomis



15 pav. *PReVENT saugumo zonos apie automobilį vizija realizuojama viena kitą papildančiomis saugumo funkcijomis [136]*

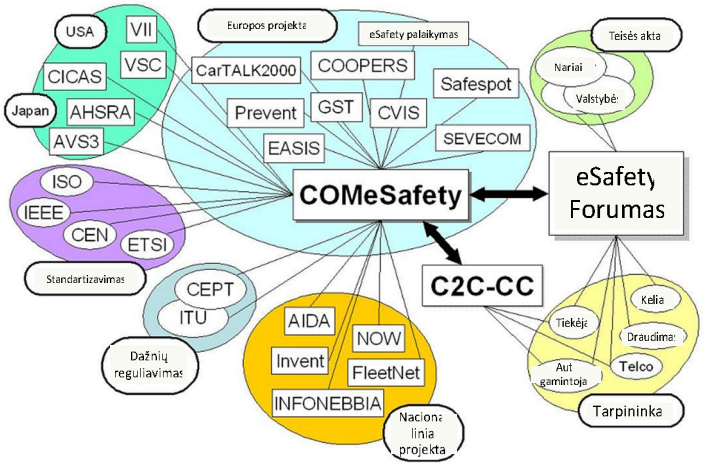
Network on Wheels (2004-2008). Projektas buvo *Fleetnet* pasekėjas, kuris rėmėsi pagrindiniais IEEE802.11 ir ad-hoc komunikacijos, skirtos saugumo ir mobilumo bei *IP* protokolu paremtoms taikymo sritims, pasiekimais. Pagrindinė idėja – sukurti atvirą komunikacijos platformą saugumo, eismo efektyvumo ir komforto/informacinėms taikymo sritims. Buvo pasiekta nemažai techninių pasiekimų, tarp kurių: saugumo informacijos sklaidos schema tinklo ir taikymo lygmenyse, pasiūlyta saugumo architektūra [137].

SAFESPOT (2006-2010). ES finansuojamas projektas, kurį vykdė 51 partneris, įskaitant automobilių gamintojus bei tiekėjus, kelių operatorius, tyrimų institucijas. Projekto tikslas – sukurti komunikacija paremtas sistemas, kurios pagerintų eismo saugumą. Buvo sukurta pavojaus įspėjimo „*Safety Margin Assistant*“ sistema, kuri apjungė automobilio sensorių, iš kitų automobilių gautą informaciją, dinaminę eismo informaciją ir pavojaus taškus. Žinučių apsikeitimui buvo remiamasi *Car-2-Car Communication Consortium ad-hoc* tinklo koncepcijomis [138].

PRE-DRIVE C2X (2008-2010). Projekto tikslas – paruošti *V2X* komunikacijos platformą, paremtą *COMeSafety* [139] architektūra. Panašiai kaip ir *Network on Wheels*, *PRE-DRIVE* prisideda prie *V2X* komunikacijų standartizavimo *ETSI* [140].

COMeSafety (2008-2013) (partneriai: *Audi*, *BMW*, *Daimler Chrysler*, *Fiat*, *Renault*, *Volkswagen*). Projekto tikslas – apjungti visus vykdytus ir ateityje vyksiančius *ITS* projektus. Projekto uždaviniai: ES mastu koordinuoti tyrimų rezultatus ir jų įgyvendinimą, *eSafety Forum*

palaikymas, dažnių juostų priskyrimas, informacijos sklaida, standartizavimo derinimas pasauliniu mastu [139]. 16 paveiksle pateiktas *COMeSafety* ir susijusių projektų sąryšis.



16 pav. *COMeSafety ir susijusių projektų ryšys [139]*

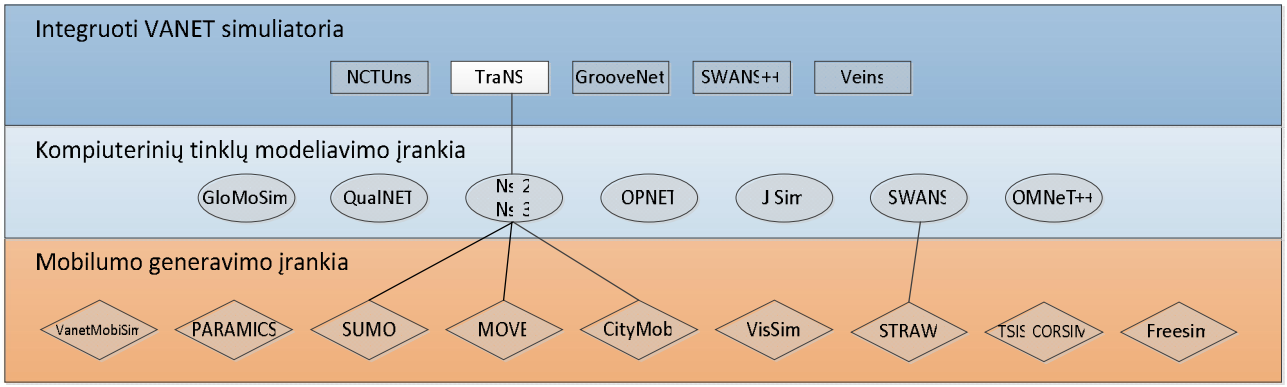
Neišnaudotas automobilinės komunikacijos potencialas lėmė didelį kiekį bendradarbiavimo iniciatyvų, siekiant eismo saugumo užtikrinimo ir multimedija paslaugų palaikymą kelyje. Kadangi bendradarbiavimas tarp vyriausybės organizacijų, automobilių pramonės ir mokslo institucijų nuolat auga, nauji ir inovatyvūs mokslinių tyrimų projektai leidžia ir leis ateityje nustatyti naujas automobilių komunikacijos tinklų panaudojimo sritis bei rinkas.

II. METODINĖ DALIS

8. Automobilių komunikacijos tinklų modeliavimo programinės įrangos analizė

Yra sukurtas ir siūlomas gana didelis automobilių komunikacijos imitacinio modeliavimo programinės įrangos (simuliatorių), leidžiančios tirti bei įvertinti įvarius prieigos, maršrutizavimo bei įspėjimų perdavimo protokolus, pasirinkimas. Automobilių komunikacijos modeliavimas fundamentaliai skiriasi nuo *MANET* modeliavimo, kadangi automobilinė aplinka sukelia naujų problemų bei reikalavimų, tokių kaip: apribota kelių topologija, pakelės kliūtys, eismo srauto modeliai, kintantis automobilių greitis ir mobilumas, šviesoforų signalai, eismo spūstys, vairuotojų elgesys ir t.t. Automobilių komunikacijos tinklų kūrimas ir testavimas sunaudoja daug laiko bei piniginių resursų, todėl dažnu atveju sistemas tirti tikslinga panaudojant modeliavimą bei simuliavimą.

Atlikus analizę, automobilių komunikacijos tinklų modeliavimo bei simuliavimo programinė įranga buvo suskirstyta į 3 skirtingas kategorijas: (a) automobilių mobilumo generatoriai, (b) tinklų simuliatoriai ir (c) automobilių komunikacijos tinklų simuliatoriai. 17 pav. pateikta šios programinės įrangos klasifikacija.



17 pav. *VANET modeliavimo bei simuliavimo programinės įrangos klasifikacija*

8.1. Automobilių eismo ir mobilumo modeliai

Automobilių eismo modeliavimas yra plačiai žinoma sritis civilinėje inžinerijoje ir yra esminis, norint tinkamai sumodeliuoti automobilių eismą projektuojant naujus kelius, sankryžas ar kitą transporto infrastruktūrą. Transporto ir eismo moksluose yra išskiriami 3 eismo modeliai, atsižvelgiant į modelių detalumą pagal kurį eismo srautai yra analizuojami: makroskopinis, mezoskopinis ir mikroskopinis [141].

Makroskopiniuose modeliuose eismas yra modeliuojamas dideliu masteliu, eismą laikant skysčiu, kuriam taikomi hidrodinaminiai judėjimo dėsniai. Simuliavimas vyksta nuo atkarpos iki atkarpos, nenagrinėjant atskirų automobilių. Šio tipo modeliavimas sunaudoja kur kas mažiau skaičiavimo resursų negu mikroskopiniai modeliai, tačiau neužtikrina galimybių analizuoti transporto patobulinimų dideliu detalumu [142].

Mezoskopiniuose modeliuose (angl. *Continuous Traffic Assignment Model* (*CONTRAM*)) yra apjungiamos tiek makroskopinių, tiek ir mikroskopinių modelių savybės. Kaip ir miksroskopiniuose modeliuose, eismo srauto vienetas yra vienas automobilis. Vis dėlto, automobilių judėjimas remiasi makroskopiniu modeliu ir yra lemiamas vidutinio greičio bei nėra atsižvelgiama į individualaus automobilio dinaminį greitį bei tarpusavio ryšius [10].

Kadangi automobilių komunikacijos tinklų simuliavimas remiasi tiksliu radijo bangų perdavimu tarp mazgų, yra būtinos tikslios šių mazgų pozicijos. Tiek makroskopiniai, tiek mezoskopiniai modeliai negali užtikrinti tokio detalumo lygio, todėl automobilių komunikacijos tinklų modeliavimui labiausiai tinka mikroskopiniai modeliai, kurie aprašo atskirų automobilių elgesį bei jų tarpusavio sąveiką. Transporto ir eismo mokslininkų buvo sukurta daug specialių modelių, iš kurių kiekvienas pritaikytas tam tikram atvejui. Mokslinės bendruomenės plačiausiai naudojami „*Cellular Automaton*“ (*CA*), „*Stefan Krauss*“ (*SK*) ir „*Intelligent Driving Model*“ (*IDM*) modeliai. Mikroskopinių modelių simuliacija užima daug laiko ir reikalauja daug darbinės atminties, todėl tai riboja modeliuojamo tinklo dydį ir simuliacijų kiekį [141].

8.2. Mobilumo generavimo įrankiai

Automobilių mobilumo generatoriai reikalingi realizmo lygio padidinimui automobilių komunikacijos tinklų stimuliatoriuose. Jie generuoja realistiškus automobilių judėjimo kelius, kurie vėliau naudojami kaip įėjimas tinklų simuliatoriui. Kaip įėjimai gali būti panaudojami kelių modeliai, scenarijų parametrai (automobilio greitis, atvykimo ir išvykimo laikai ir kt. Šiame skyriuje aptariami skirtingi automobilių eismo modeliai, egzistuojantys mobilumo generatoriai. 3 priede pateiktas kokybinis mobilumo generatorių palyginimas, kuris buvo suskirstytas į 5 kategorijas: programinės įrangos charakteristikos, žemėlapių tipas, palaikomi mobilumo modeliai, naudojami eismo modeliai, palaikomi žymių užrašymo formatai. Pagrindiniai automobilių komunikacijos tinklų tyrimuose naudojami mobilumo generavimo įrankiai: *TSIS-CORSIM, VisSim, PARAMICS, VanetMobiSim, SUMO, MOVE*, *STRAW, FreeSim*, *CityMob*.

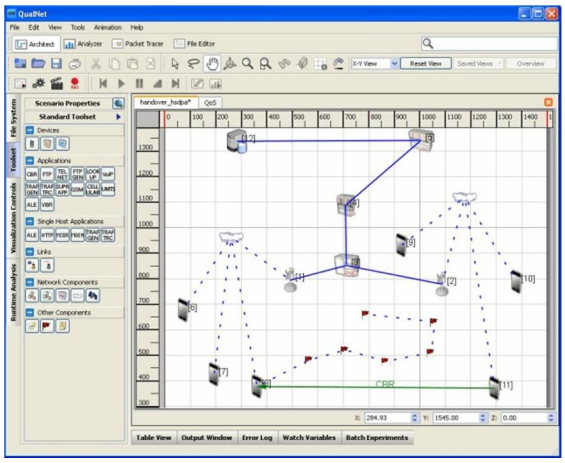
8.3. Kompiuterinių tinklų modeliavimo įrankiai

Tinklų modeliavimo įrankiai ir simuliatoriai mokslininkams leidžia tyrinėti kaip tinklas elgsis, esant skirtingoms sąlygoms. Palyginus resursus, reikalingus realiam tinklui įrengti bei jame atlikti bandymus, tinklų simuliatoriai yra pigus ir greitas sprendimas atliekant mokslinius tyrimus, ypač tokiomis aplinkybėmis kai sudėtinga ar itin brangu tai atlikti naudojantis technine įranga, kas itin aktualu automobilių komunikacijos tyrimuose. Šiame skyriuje aptariami šiuo metu populiariausi tinklų modeliavimo bei simuliavimo įrankiai, naudojami automobilių komunikacijos tinklų tyrimuose:

ns-2 yra atvirojo kodo diskretinis įvykių simuliatorius, sukurtas *VINT* projekto tyrimų grupės *Berkeley* universitete ir skirtas tiek laidinių, tiek bevielių tinklų modeliavimui. Simuliatorius buvo praplėstas *Monarch* tyrimų grupės, kuri įtraukė: mazgų mobilumą, realistinį fizinį sluoksnį su radijo sklidimo moduliu, radijo tinklų sąsajas ir *IEEE 802.11 MAC* protokolą naudojant paskirstytų koordinačių funkciją (angl. *distributed coordination function* (*DCF*)). *ns-2* apima daugybę *MANET* maršrutizavimo protokolų ir yra plačiai naudojamas įrankis akademiniuose tinklų tyrimuose. Simuliatoriuje yra realizuota keletas mobilumo modelių, tarp kurių: *Random Trip Mobility* ir *Semi-Markov Smooth Mobility*. Įvykdžius simuliaciją yra sugeneruojami rezultatų ir animacijos failai, kuriuose yra informacija apie paketų perdavimą, paketų persiuntimą ir paketų praradimus [143].

GloMoSim yra bevielių bei laidinių kompiuterinių tinklų modeliavimo bei simuliavimo įrankis, specialiai sukurtas *MANET* tyrimams, apimantis daugybę maršrutizavimo protokolų ir keletą fizinio sluoksnio realizacijų. Kadangi tai integruotas simuliavimo įrankis, jis suteikia galimybes sugeneruoti žymes ir pagal kai kuriuos mobilumo modelius: *Random Waypoint*, *Random Drunken*, taip pat importuoti sugeneruotus kitais įrankiais. *GloMoSim* vystymas buvo nutrauktas 2000 metais, tačiau vis dar įmanoma ją parsisiųsti, tačiau tik mokymo tikslais. Komercinė *GloMoSim* versija tapo *Qualnet* simuliatoriumi, vystomu *Scalable Network Technologies*. [15, 141]

QualNET yra itin galingas bei detalus tinklų modeliavimo bei simuliavimo paketas, palaikantis didelį rinkinį bevielių fizinių ir *MAC* sluoksnių modelių bei mobilumo modelių, mokslininkams leidžiantis sukurti bei lengvai simuliuoti įvairius tinklų protokolus. Paketas veikia *Windows* ir *Unix/Linux* platformose. *QualNet* užtikrina didelio tikslumo tinklo įrenginių, transmiterių, antenų, žemės paviršiaus, žmonių simuliaciją realiu laiku, nepriklausomai nuo to ar simuliuojama 50 ar 5000 tinklo mazgų. Su programa pateikiamas modulių bibliotekų pirminis kodas, leidžiantis eksperimentuoti su tinklų funkcionalumu [144]. *QualNET* grafinės vartotojo sąsajos pvz. pateiktas 18 pav.



18 pav. *QualNET paketo veikimas Design Mode režimu [144]*

OPNET yra komercinis bevielių bei laidinių tinklų modeliavimo paketas, kuris palaiko platų bevielių technologijų spektrą: *MANET*, *IEEE 802.11*, *WiMAX*, *Bluetooth* ir palydovinius

tinklus. Modelių kūrimui naudojamas grafinis redaktorius, kuriuo gali būti kuriami įvairūs modeliai nuo fizinio lygio moduliacijos iki taikymo procesų. Pateikiami grafiniai paketai bei moduliai simuliacijos rezultatų pateikimui [145].

J-Sim yra atvirojo kodo simuliacijos aplinka. Programoje naudojami du mobilumo modeliai: trajektorija paremtas ir *random waypoint*. Įrankis pristatomas kaip *ns-2* alternatyva, kadangi jo naudojimas yra gerokai paprastesnis. *J-Sim* aplinkoje programos yra kuriamos kaip atskirų komponentų rinkiniai, kurie gali būti kuriami ir testuojami atskirai [146].

OMNeT++ yra atvirojo kodo simuliacijos aplinka, taikoma interneto, mobilumo ir ad-hoc simuliacijoms. Programa palaiko tinklų ir mobilumo modelius per atskirai sukurtas mobilumo bei *INET* struktūrų modulius (angl. *frameworks*) [147].

8.4. Integruoti automobilių komunikacijos tinklų simuliatoriai

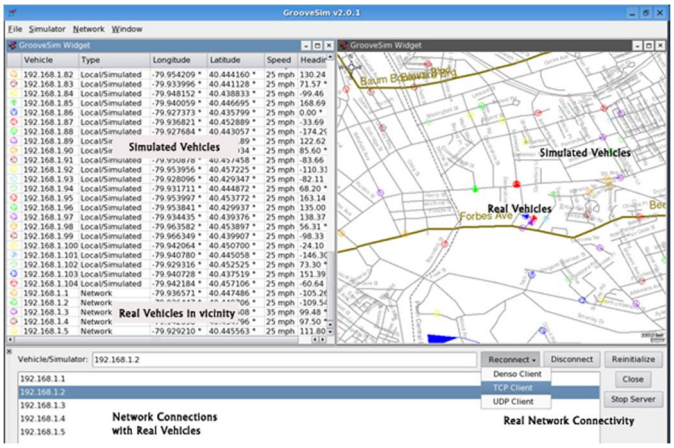
Kaip buvo minėta ankstesniuose skyriuose, automobilių komunikacijos tinklų simuliacijai neužtenka simuliuoti tik bevielę komunikaciją tarp automobilių, tačiau reikia simuliuoti ir jų judėjimą. Deja, tačiau *VANET* simuliacijose šie du aspektai dažnai yra atskirti. Pagrindinė problema yra šių dviejų tipų simuliatorių apjungimas. Paprasčiausias sprendimo būdas – į tinklų simuliatorių integruoti mobilumo modelius, tačiau tokiu atveju, tinklo duomenys nėra perduodami atgal mobilumo modeliui, todėl galima tik vienakryptė komunikacija (iš mobilumo modelio į tinklą). Šio tipo modeliavimo įrankiai leidžia simuliuoti informacines automobilių komunikacijos tinklų aplikacijas (interneto ryšys, multimedija, taškas į tašką programos), kur komunikavimas neįtakoja automobilio judėjimo.

Integruoti *VANET* simuliatoriai, kurie užtikrina dvikryptę komunikaciją, paprastai susideda iš dviejų sub-simuliatorių (tinklo ir mobilumo), kurie gali komunikuoti vienas su kitu. Šie simuliatoriai labiau tinkami su saugumu susijusios ir eismo informacijos aplikacijoms, kurios gavusios atsaką iš tinklo įtakoja automobilių judėjimą. Šio tipo aplikacijose, eismo simuliatorius perduoda tinklo simuliatoriui tam tikrą informaciją (poziciją, greitį, pagreitį, kryptį ir t.t.). Automobilių komunikacijos tinklų aplikacija, veikianti viršutiniame tinklų simuliatoriaus lygmenyje, šią informaciją apjungia su aplinkinių automobilių pateikiama informacija, taip perspėdamas vartotojus apie netoliese esančias spūstis ar galimus susidūrimus. Remiantis šia informacija vairuotojas gali keisti vairavimo veiksmus – gali pakeisti eismo juostą, pasirinkti kitą kelią. Šie galimi sprendimai turi būti perduoti atgal mobilumo simuliatoriui, kuris atitinkamai koreguoja automobilių judėjimą [141]. Toliau pateikti pagrindiniai automobilių komunikacijos tinklų modeliavimui naudojami integruoti modeliavimo įrankiai:

SWANS++ praplečia tinklų simuliatorių *SWANS*, pridėdamas grafinę vartotojo sąsają scenarijų ir mobilumo (*STRAW*) modelių vizualizavimui. *STRAW* naudoja paprastą „random

waypoint“ mobilumo modelį, tačiau automobilių judėjimas yra apribotas realių gatvių ribomis, įkeltomis iš *TIGER/Line* duomenų bazės. Nors *SWANS++* yra glaudžiai integruotas simuliatorius, tačiau jis nepalaiko atgalinio ryšio tarp mobilumo ir tinklo modulių [148].

GrooveNeT yra integruotas tinklų bei mobilumo simuliatorius, leidžiantis komunikuoti realiems ir simuliuojamiems automobiliams. Simuliatoriuje galima naudoti realius gatvių žemėlapius iš *TIGER/Line* duomenų bazės, simuliuoti automobilių judėjimą realiose gatvėse, įskaitant fiksuotą mobilumą, greitį gatvėse, pastovų greitį, automobilių sekimo modelius. *GrooveNeT* turi unikalią galimybę integruoti realius automobilius su simuliuojamu tinklu, todėl tai kartu yra realaus tinklo testavimo bei simuliavimo įrankis [*149*]. *GrooveNeT* grafinės vartotojo sąsajos pvz. pateiktas 19 pav.



19 pav. *GrooveNeT paketo grafinė vartotojo sąsaja. [149]*

TraNS (angl. *Traffic and Network Simulation Environment*) gali būti vadinamas pirmuoju *VANET* simuliatoriumi, kadangi jame pirmą kartą buvo apjungtas tinklų simuliatorius *ns-2* su automobilių eismo simuliatoriumi *SUMO* bei buvo sukurtas grįžtamasis ryšys iš tinklo simuliatoriaus į mobilumo [150].

Veins (angl. *Vehicles in Network Simulation*) yra dar vienas simuliatorius, integruojantis mobilumo bei tinklo simuliatorius į vieną: *SUMO* yra apjungiamas su *OMNeT++* per *TCP* ryšį. *Veins* simuliatoriuje yra valdymo modulis, kuris atsakingas už dviejų simuliatorių sinchronizavimą. Reguliariais laiko tarpais valdymo modulis įvykdo vieną mobilumo modulio laiko žingsnį, priima rezultatą (mobilumo žymę) ir įvykdo pozicijos atnaujinimus visiems moduliams. Kaip ir *TraNS*, *Veins* turi dvi atskiras įvykių eiles [151].

Atlikus integruotų automobilių komunikacijos tinklų simuliatorių analizę buvo sudarytas kokybinis palyginimas (4 lentelė)

4 lentelė. *Integruotų simuliatorių palyginimas [15, 141, 148, 149, 150, 151, 152, 154]*

Atributas	Swans++	GrooveNeT	TraNS	Veins	NCTuns
Mobilumo funkcijos					
Vartotojo grafikai	*Palaikoma*	*Palaikoma*	*Palaikoma*	*Palaikoma*	*Palaikoma*
Atsitiktiniai grafikai	*Random*	*Voronoi*	*Tinkleliu*	*Random*	*Figūrų failai*

	waypoint	*grafikai*	*paremti*	*waypoint*	
Žemėlapiais paremti grafikai	*Tiger duomenų bazė*	*GDF*	*Tiger duomenų bazė*	*OpenStreetMap DB*	*Figūrų failai*
Keletas eismo juostų	*Palaikoma*	*Palaikoma*	*Palaikoma*	*Palaikoma*	*Palaikoma*
Pradžios/pabaigos pozicija	*Atsitiktinis*	*AP, atsitiktinis*	*AP, atsitiktinis*	*Atsitiktinis*	*Atsitiktinis*
Kelias	*Atsitiktinio kelio*	*Atsitiktinio kelio, Dijkstra*	*Atsitiktinio kelio, Dijkstra*	*Atsitiktinio kelio*	*Atsitiktinio kelio*
Greitis	*Pastovus*	*Priklausantis nuo sąlygų, pastovus*	*Priklausantis nuo sąlygų, pastovus*	*Pastovus*	*Priklausantis nuo sąlygų, pastovus*
Sankryžų valdymas	*Nepalaikomas*	*Šviesoforai, ženklai*	*Nepalaikomas*	*Nepalaikomas*	*Šviesoforai*
Juostų keitimas	*Nepalaikomas*	*Palaikomas*	*Nepalaikomas*	*Nepalaikomas*	*Palaikomas*
Radijo kliūtys	*Nepalaikomas*	*Palaikomas*	*Nepalaikomas*	*Palaikomas*	*Palaikomas*
Kitos funkcijos					
Grafinė vartotojo sąsaja	*Palaikoma*	*Palaikoma*	*Nepalaikoma*	*Palaikoma*	*Palaikoma*

Įvertinus modeliavimo programinės įrangos analizės rezultatus buvo nustatyta, kad eismo saugumo, informacinių ir multimedija paslaugų teikimo automobilių komunikacijos tinkluose tyrimams geriausiai tinka glaudžiai integruotas modeliavimo paketas *NCTUns*, ypač dėl naudojamų realių TCP/UDP/IP protokolų.

8.5. *NCTUns* integruotas tinklų bei mobilumo simuliatorius ir emuliatorius

NCTUns (angl. *National Chiao Tung University Network Simulator*) yra aukšto tikslumo, praplečiamas integruotas tinklų bei mobilumo simuliatorius ir emuliatorius, leidžiantis modeliuoti daugybę įvairių protokolų, naudojamų tiek laidiniuose, tiek bevieliuose tinkluose. Jis remiasi moderniu pakartotinio kreipimosi į branduolį (angl. *kernel re-entering*) metodu, kuris *NCTUns* suteikia daugybę unikalių privalumų, kurių neturi plačiai paplitę simuliatoriai, pvz. *ns-2* ar *OPNET*. Naudojama intuityvi vartotojo sąsaja, kuri panaikina sudėtingo skriptų rašymo būtinybę. Netrukus bus išleista komercinė šio simuliatoriaus versija *EstiNet 7.0* [152, 153].

Pagrindiniai *NCTUns* privalumai [154]:

Gali būti naudojamas kaip emuliatorius. Išorinis realaus pasaulio tinklo įrenginys gali apsikeisti paketais (pvz. užmegzti *TCP* ryšį) su mazgais (kompiuteriais, maršrutizatoriais, mobiliosiomis stotelėmis) *NCTUns* simuliuojamame tinkle. Taip pat galimas ir keleto realių tinklo įrenginių ryšys per *NCTUns* simuliuojamą tinklą. Ši savybė yra labai naudinga, kadangi realūs įrenginiai gali būti išbandomi prie įvairių sąlygų.

Palaiko paskirstytą didelio tinklo emuliaciją keliuose kompiuteriuose. Kai emuliuojamame tinkle yra daug mazgų, kuriuose turi veikti daugybė realaus pasaulio programų, arba yra labai didelis apsikeičiamų paketų kiekis, vienam kompiuteriui dažnai nepakanka procesoriaus skaičiavimo resursų bei operatyviosios atminties tam, kad emuliaciją vykdyt realiu laiku. Tokiu atveju, *NCTUns* gali išdalinti emuliuojamą tinklą į keletą mažesnių dalių ir kiekvienos

dalies emuliaciją vykdyti kitame kompiuteryje. Paskirstyto emuliavimo naudojimas yra visiškai automatinis, nereikalaujantis vartotojo įsikišimo.

Tiesiogiai naudojamas realus *Linux TCP/IP* protokolo stekas, leidžiantis gauti aukšto tikslumo rezultatus. Naudojant modernų pakartotinio kreipimosi į branduolį metodą, panaudojamas realus *Linux* branduolio protokolo stekas.

Galima naudoti bet kokią realią *UNIX* taikomąją programą simuliuojamame mazge be jokių papildomų modifikacijų. Bet kokia reali programa (*P2P BitTorrent*, *Java* ir kt. programos) gali būti naudojamos simuliuojamame kompiuteryje, maršrutizatoriuje, mobiliame mazge tam, kad sugeneruoti realistišką tinklo duomenų srautą. Ši galimybė leidžia tyrėjams įvertinti paskirstytos programos ar sistemos funkcionalumą ir efektyvumą esant įvairioms sąlygoms.

Galima naudoti bet kokius realius *Unix* tinklų konfigūravimo ir stebėjimo įrankius. Pvz. *UNIX route*, *ifconfig*, *netstat*, *tcpdump*, *traceroute* ir kt. komandos gali būti panaudotos sukonfigūruoti ar stebėti simuliuojamą tinklą.

Simuliuojami įvairūs svarbūs tinklai. Tarp palaikomų tinklų: *Ethernet* fiksuoti tinklai, *IEEE 802.11(b) wireless LAN*, mobilūs *ad-hoc* (sensorių) tinklai, *GPRS*, optiniai, *IEEE 802.11(b) dual-radio wireless mesh* tinklai, *IEEE 802.11(e) QoS wireless LAN*, *Tactical* ir *active* mobilūs *ad-hoc* tinklai, *IEEE 802.16 WiMAX* tinklai, *DVB-RCS* palydoviniai, *IEEE 802.11(p)/1609 WAVE* bevieliai automobilių tinklai (*V2V* ir *V2I*) ir kt.

Simuliuojami įvairūs svarbūs protokolai. Pvz. *IEEE 802.3 CSMA/CD MAC*, *IEEE 802.11 (b) CSMA/CA MAC*, *IEEE 802.11(e) QoS MAC*, *IEEE 802.11(b) wireless mesh* tinklų maršrutizavimo, *IEEE 802.16(d)(e)(j) WiMAX MAC* ir *PHY*, *DVB-RCS satellite MAC* ir *PHY*, *IP*, *Mobile IP*, *Diffserv (QoS)*, *RIP*, *OSPF*, *UDP*, *TCP*, *RTP/RTCP/SDP*, *HTTP*, *FTP*, *Telnet*, *BitTorrent*, ir kt.

Sugeneruojami pakartotini simuliacijos rezultatai. Simuliacijos rezultatai gali būti pakartojami vykdant simuliacijas keletą kartų. Rezultatams įtakos neturi kitos simuliacijos kompiuterio atliekamos veiklos jo apkrovimas.

Patogi vartotojo sąsaja. Ji leidžia greitai ir paprastai: nubrėžti tinklų topologijas, sukonfigūruoti mazgo naudojamus protokolų modulius, nurodyti mobilių mazgų judėjimo trajektorijas, braižyti efektyvumo grafikus, peržiūrėti paketų perdavimo animacijas.

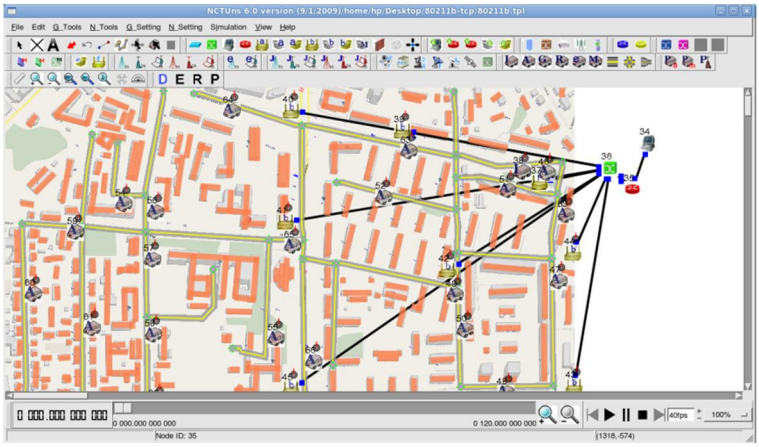
Atvira sistemos architektūra ir atviras kodas. Naudojant modulių *API* rinkinius gali būti kuriami ir integruojami protokolai. Yra galimybė tyrėjams išbandyti naujus, nenumatytus įrenginius bei konfigūracijas įvykdyti apeinant grafinę vartotojo sąsają.

NCTUns ypač daug dėmesio susilaukė iš *ITS* tyrinėtojų, kai 2007 metais sukūrė *ITS* automobilinių tinklų palaikymą *NCTUns 4.0* versijoje. *NCTUns p*alaiko: pagrindinius vairuotojo elgesio modelius, bazinę kelių tinklo konstrukciją, *RSU* (*road side unit*) simuliavimą, *OBU* (*on-*

board unit) įrenginių, kurie gali būti aprūpinti bevielėmis *IEEE 802.11(b)* infrastruktūros režimo, *ad-hoc* režimo, *GPRS*, *802.16(e) mobile WiMAX* ryšio technologijomis, *DVB-RCST* palydovinio ryšio, arba visų galimų bevielės prieigos metodų simuliavimą. Kadangi šis simuliatorius yra glaudžiai integruotas, juo gali būti tiriamos sudėtingos *ITS* situacijos, kuriose reikalingi automobilio vairavimo elgsenos pasikeitimai gavus tam tikras žinutes iš tinklo. *NCTUns 5.0* versijoje buvo įdiegti svarbūs *VANET* tinklų simuliavimo patobulinimai: efektyvus mazgų mobilumo valdymas itin didelės apimties automobiliniuose tinkluose, automatinis kelių tinklo konstravimas iš *SHAPE* formato žemėlapių failų ir svarbiausia, pilnas *IEEE 802.11(p)/1609* standartų, skirtų automobilių komunikacijos tinklų, palaikymui.

8.5.1.*NCTUns* architektūra

***GUI* (grafinė vartotojo sąsaja)** suteikia 5 pagrindines funkcijas, kurios vartotojams padeda lengvai sugeneruoti konfigūracijos failus reikalingus įvykdyti simuliacijai. Simuliacijos pradžioje šie failai yra nuskaitomi kitų programos komponentų. Kelių tinklo konstravimo įrankiai suteikia aplinką, kurioje vartotojas lengvai gali konstruoti pasirinktą kelių tinklą. Palaikomi skirtingi kelių tipai: vienos eismo juostos keliai, keleto juostų keliai, sankryžos, T-formos keliai, juostas sujungiantys keliai. 20 pav. pateiktas sudarytas Klaipėdos miesto žemėlapio fragmentas su kelių tinklu bei pastatais.



20 pav. *Sudarytas realaus miesto žemėlapis NCTUns pakete*

Sudarytuose kelių tinkluose galima nurodyti matomumo/radijo kliūtis, kurios gali blokuoti vairuotojo matomumą, ir/arba gali blokuoti arba sumažinti galią bevielio ryšio signalams [152, 154].

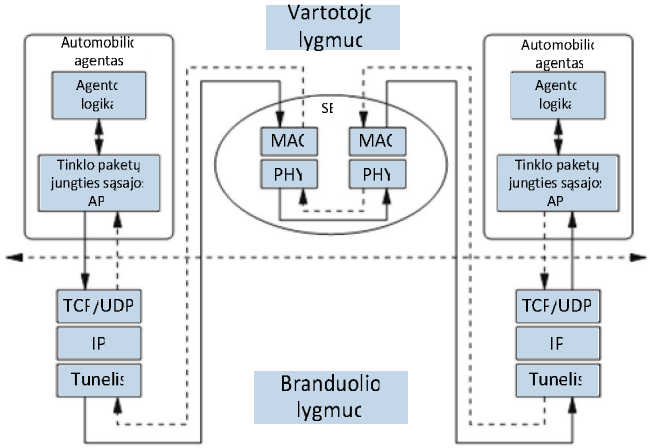
Automobilio profilio nustatymai. Norint nustatyti skirtingas judėjimo charakteristikas skirtingiems automobiliams, vartotojo sąsaja leidžia vartotojams sudaryti automobilių profilius. Profilyje galima nurodyti automobilio maksimalų greitį, maksimalų pagreitį, maksimalų pagreičio mažėjimą. Galima nustatyti procentinį tam tikro profilio automobilių kiekį ir automatiškai priskirti profilius automobiliams [157].

Automobilio judėjimo nustatymai. *NCTUns* palaiko du automobilių judėjimo valdymo metodus: pirmasis – iš anksto nustatytas; antrasis – autopiloto. Naudojantis pirmuoju metodu, vartotojas naudodamasis grafine vartotojo sąsaja, nurodo automobiliu judėjimo trajektorijas ir jų greitį prieš prasidedant simuliacijai. Grafinė vartotojo sąsają šią informaciją įrašo į mazgo judėjimo scenarijaus konfigūracijos failą. Simuliacijos metu automobiliai juda pagal nustatytą trajektoriją kelių tinkle. Naudojantis autopiloto metodu, vartotojui nereikia nurodyti kiekvieno automobilio konkrečių trajektorijų ir greičio, tačiau reikia nustatyti kiekvieno automobilio profilį. Simuliacijos metu automobilio agentas automatiškai valdo judėjimo elgseną. Kiekvienas automobilis dinamiškai gali keisti judėjimo kryptį ir greitį simuliacijos metu. Agentai yra priskiriami automatiškai.

Tinklo protokolų nustatymas. *NCTUns* programoje skirtingų tipų bevielio ryšio prieiga yra realizuota simuliuojant skirtingus tinklo protokolų stekus. Automobilis su radijo ryšio prieiga yra susietas su atitinkamu tinklo protokolu. Kiekvieno protokolo stekas yra įgyvendintas kaip protokolų modulis. Į protokolų steką gali būti žiūrima kaip į seriją tarpusavyje sujungtų protokolų modulių. Vartotojo sąsaja leidžia vartotojams lengvai pasirinkti/pakeisti protokolų modulius, tokius kaip mobilių ad-hoc maršrutizavimo protokolų modulius bei nustatyti su kiekvienu moduliu susijusius parametrus. Informacija apie naudojamus protokolų stekus ir modulių parametrus yra įrašoma į protokolų modulių specifikacijos konfigūracijos failą. Taip pat grafinėje vartotojo sąsajoje galima peržiūrėti animuotus paketų perdavimus bei automobilių judėjimą tiek simuliacijos metu, tiek ir po simuliacijos. Šis simuliacijos rezultatų vizualizavimas leidžia greitai ir lengvai patikrinti ir ištaisyti tinklo protokolų klaidas bei automobilių judėjimo elgseną [152, 157].

Simuliacijos variklis (*SE*). Paleidus programą, *SE* atlieka nukreipimą į *CA* (angl. *car agent*) arba *SA* (angl. *signal agent*), priklausomai nuo parinktos taikomosios programos. Kaip ir kitos *SE* paleistos programos, *CA* arba *SA* procesai gali būti paleisti ir nutraukti bet kuriuo simuliacijos metu. *SE* sukuria *TCP* paremtą komandų serverį (kuris yra periodiškai iškviečiama SE proceso funkcija) skirtą priimti komandas iš *CA* arba *SA*. Pagal komandos tipą, komandų serveris gali išsaugoti/išrinkti duomenis iš/į signalų duomenų bazę arba automobilių informacijos duomenų bazę.

Į tinklo protokolo steką, simuliuojamą *NCTUns* įeina *Linux* branduolio protokolo stekas, įskaitant *TCP/IP* ir *UDP/IP*, vartotojo lygio *SE* protokolo stekas, įskaitant *MAC* ir *PHY* sluoksnio protokolus (21 pav.).



21 pav. *IP paketų perdavimo vieno automobilio kitam simuliacijos procesas [157]*

Turėdamas galimybę panaudoti realius *Linux* branduolio *TCP/UDP/IP* protokolų stekus, *NCTUns* generuoja realistiškus *TCP/UDP/IP* protokolų automobilių bevielės komunikacijos simuliacijos rezultatus.

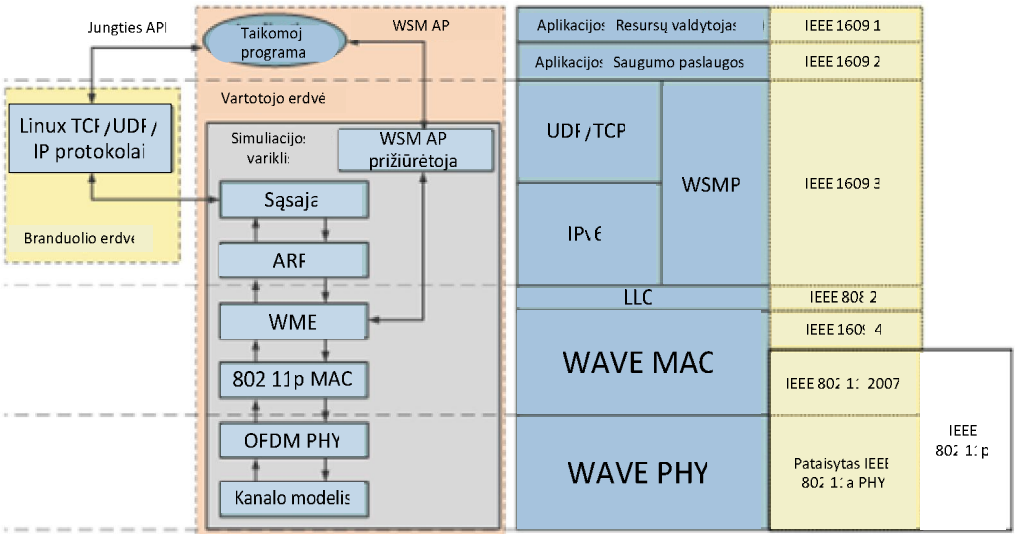
***CA* – automobilio agentas** (angl. *car agent*). *CA* yra *SE* simuliuojamo ir su juo asocijuoto automobilio valdiklis. Agento logika, esanti *CA* yra sprendimų priėmėjas, kuris nustato kada reikia imtis tam tikrų veiksmų. Vykstant simuliacijai, agento logika periodiškai atnaujina automobilio ir signalų informacijos duomenų bazes per jungties sąsajos *API*. Komandų serveris suteikia ne tik atnaujinimą ar prieigą prie paslaugų, tačiau atlieka ir duomenų analizę, pvz. šviesoforų ženklų nustatymo atveju.

Taip pat, yra įdiegtos papildomos agento funkcijos skirtos surinkti visapusiškai informacijai, pagal kurią priimami vairuotojo sprendimai. Pvz., agentas gali nustatyti priešais esančio kelio eismo kryptį ir pagal tai pasirinkti tinkamą judėjimo kryptį. Kitas pvz. – agentas gauna informaciją iš gretimų eismo juostų, pagal kurią keičia eismo juostas arba lenkia kitus automobilius. Vartotojas gali papildyti standartinį autopiloto agento intelektą savo sukurtu [152, 154, 157].

***SA* – signalo agentas** (angl. *signal agent*). Jis yra atsakingas už visų keturių šviesoforų ženklų pasikeitimą. Grupės identifikatorių naudojant kaip indeksą, SA agento logika panaudoja signalo informacijos jungties sąsajos *API* specifinio tipo eismo signalų informacijai gauti, pvz. pradinė signalo būsena. Komandų serveris gauna reikiamą informaciją iš signalų informacijos duomenų bazės ir išsiunčia ją atgal agentui [152, 154, 157].

8.5.2.*IEEE 802.11(p)/1609 OBU* ir *RSU* architektūra *NCTUns* simuliatoriuje

NCTUns palaiko dviejų tipų *IEEE 802.11(p)/1609* protokolo mazgus: *802.11(p) RSU* ir *802.11(p) OBU*. Abu mazgai naudoja tą pačią protokolo steko konfigūraciją, kuri pateikta 22 pav.



22 pav. *IEEE 802.11(p)/1609 protokolo architektūra NCTUns programoje [152]*

IEEE 802.11(p)/1609 protokolo architektūros *NCTUns* programoje paaiškinimai [155]:

Taikomoji programa (angl. *Application Program*). *NCTUns* tiesiogiai vykdo vartotojo lygmens taikomuosius procesus, kad realizuotų taikymo funkcijas, reikalingas *IEEE 802.11(p)/1609* protokolo mazgui. Tokia programa gali perduoti arba priimti: 1) *IP* paketus per standartinę lizdo sąsają, 2) *WAVE* trumpąsias žinutes per specialią *WSMP* taikomojo programavimo sąsają (*API*).

WSMP. Skirtingai nei *TCP/UDP/IP* protokolų rinkinys, kuris buvo standartizuotas prieš daug metų ir įdiegtas *Linux* branduolyje, *WSMP* yra naujas tinklo lygio protokolas, kuris nėra palaikomas *Linux* operacinės sistemos. *NCTUns* programoje *WSMP* yra integruotas simuliacijos variklyje kaip protokolo modulis. Jei ateityje *WSMP* bus integruotas į *Linux* operacinę sistemą, bet kuri vartotojo lygio programa galės tiesiogiai naudotis pastarąja.

***MAC* ir fizinio sluoksnių moduliai.** Šie moduliai yra įgyvendinti kaip simuliacijos protokolų moduliai. *WME* funkcionalumas, aprašytas *IEEE 1609.3* yra įgyvendintas WME modulyje, o *WAVE* režimo *MAC* sluoksnio funkcijos, tokios kaip kanalų perjungimas ir *802.11(e)* kanalų prioritetų nustatymas yra įgyvendinti *802.11(p) MAC* modulyje. *OFDM* kanalų charakteristikos simuliuojamos *OFDM* modulio.

III. EKSPERIMENTINĖ DALIS

9. Skirtingų ad-hoc maršrutizavimo protokolų efektyvumo eismo saugumo ir multimedija paslaugų teikimo įvertinimas

Egzistuoja nemažai mokslinių tyrimų, analizuojančių maršrutizavimą *ad-hoc* tinkluose, tačiau protokolai dažniausiai skirti *MANET* tinklams, o *VANET* tinklai, kaip minėta anksčiau turi specifinius reikalavimus. Šio tyrimo tikslas – ištirti trijų ad-hoc maršrutizavimo protokolų: *AODV* (angl. *On-Demand Distance Vector*), *ADV* (angl. *Adaptive Distance Vector*) ir *GOD* (režimas, kai maršrutai parenkami iš anksto prieš pradedant simuliaciją), efektyvumą, teikiant eismo saugumo ir multimedija paslaugas esant skirtingoms automobilinės komunikacijos sąlygoms: miesto bei greitkelio. Protokolų efektyvumo įvertinimui buvo pasirinktos šios metrikos:

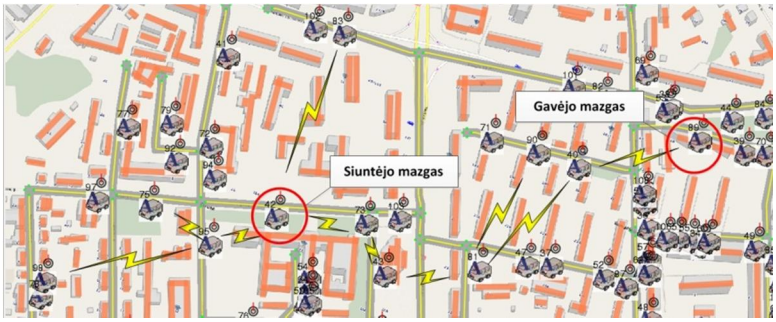
Paketų kolizijos. Kolizijos lemia bendrą tinklo spartos sumažėjimą bei gali lemti paketų integralumo praradimą. Dviem ar daugiau mazgų bandant siųsti paketus tuo pačiu metu gali įvykti kolizija. Žemas kolizijų skaičius lemia gerą tinklo darbo efektyvumą, kuris automobilinėje komunikacijoje itin svarbus tiek eismo saugumo, tiek ir multimedija paslaugų teikimui.

Paketų atmetimo skaičius. Tai paketų kiekis, kurie negali būti sėkmingai perduodam siuntėjo gavėjui ir viename iš mazgų yra atmetami ir sunaikinami. Eismo saugumo paslaugų užtikrinime tai gali lemti katastrofiškas pasekmes, kadangi gali būti nepristatytos avarinės žinutės.

Tinklo pralaidumas. Pralaidumas nurodo tinklo efektyvumą perduodant duomenų paketus. Multimedija paslaugų teikimui tinklo sparta yra itin svarbi, ypač perduodant didelio pralaidumo reikalaujančius duomenis: vaizdo, garso medžiagą, IP telefonijai ir kt.

9.1. Eksperimento sudarymas

Eksperimentas buvo atliktas *NCTUns 6.0* programiniu paketu, kuris buvo įdiegtas *Fedora 12 Linux* operacinėje sistemoje. Buvo atlikti bandymai tinkle modeliuojant 30, 50 ir 75 automobilių judėjimą. Buvo sudarytas miesto mobilumo modelis, naudojant Klaipėdos miesto žemėlapį. Vidutinis automobilių judėjimo greitis – 35 km/h, tačiau jis yra adaptyvus ir kintantis pagal eismo sąlygas, šviesoforų ženklus ir kitų automobilių judėjimą. Eksperimento atlikimo schema pateikta 23 paveiksle.



23 pav. *Skirtingų ad-hoc maršrutizavimo protokolų efektyvumo eismo saugumo ir multimedija paslaugų teikimo VANET tinkle miesto sąlygomis tyrimo atlikimo schema*

Simuliacija buvo atliekama 120 sekundžių. Bandymas buvo pakartotas naudojant ankščiau aptartus maršrutizavimo protokolus bei tinkle veikiant skirtingam automobilių kiekiui. Eksperimento atlikimui naudojami simuliacijos parametrai pateikti 5 lentelėje.

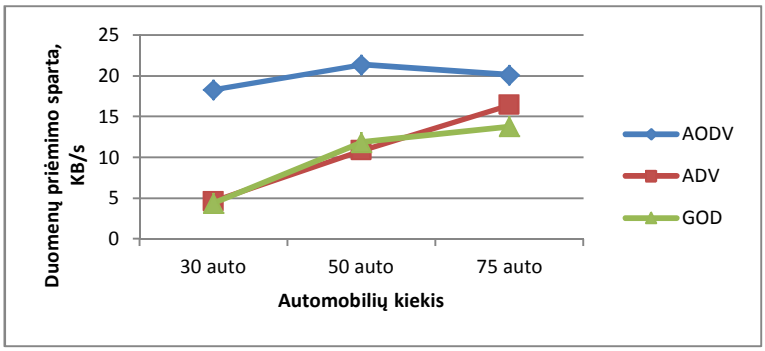
5 lentelė. *Eksperimentui atlikti naudojami simuliacijos parametrai*

Parametras	**Reikšmė**
Simuliacijos laikas	120 s
Fizinio sluoksnio protokolas	802.11b
Automobilių skaičius	Nuo 30, 50, 75
Mazgų judėjimas	Atsitiktinis, miesto mobilumo modelis
Kanalo dažnis	2,4 GHz
Maršrutizavimo protokolas	AODV, ADV, GOD

9.2. Eksperimento rezultatai

Atlikus tyrimą ir apdorojus gautus duomenis, buvo gauti ir toliau pateikiami šie eksperimentų rezultatai: vidutinės duomenų priėmimo bei siuntimo spartos priklausomybė nuo automobilių kiekio, duomenų priėmimo bei siuntimo spartos priklausomybė nuo laiko, tinkle veikiant 50 automobilių, kolizijų kiekio gavėjo bei siuntėjo mazguose priklausomybė nuo automobilių kiekio, kolizijų kiekio gavėjo bei siuntėjo mazguose priklausomybė nuo laiko, tinkle veikiant 50 automobilių, atmestų paketų gavėjo bei siuntėjo mazguose priklausomybė nuo automobilių kiekio bei laiko.

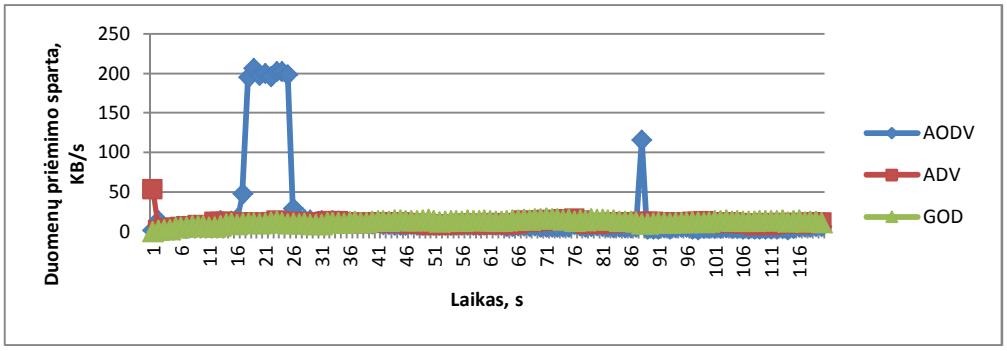
24 pav. pateiktas duomenų priėmimo spartos priklausomybės nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus grafikas. Iš grafiko matome, kad naudojant *ADV* ir *GOD* maršrutizavimo protokolus, duomenų priėmimo sparta yra tiesiogiai proporcinga automobilių kiekiui ir yra panaši abiems protokolams. Naudojant *AODV* maršrutizavimo protokolą, didžiausia duomenų priėmimo sparta yra tinkle veikiant 50 automobilių.



24 pav. *Vidutinės duomenų priėmimo spartos priklausomybė nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus*

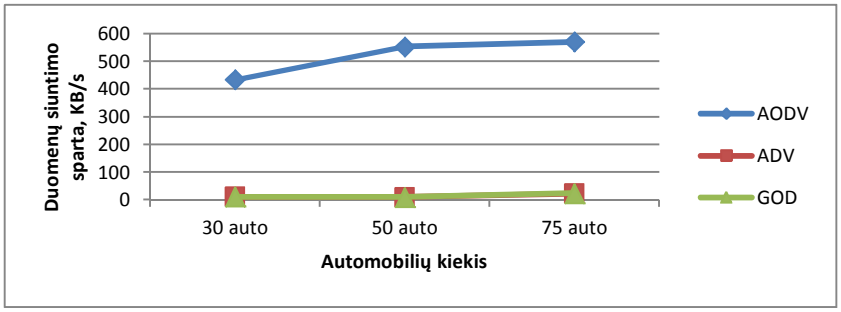
24 pav. pateiktas duomenų priėmimo spartos priklausomybės nuo laiko, tinkle veikiant 50 automobilių, naudojant skirtingus maršrutizavimo protokolus grafikas. Iš pateikto grafiko matome, kad laikui bėgant veikiant *ADV* ir *GOD* maršrutizavimo protokolams duomenų priėmimo sparta yra

labai žema, tai reiškia, kad tinklas yra užtvindytas maršrutizavimo žinutėmis, ir tai sąlygoja žemą tinklo efektyvumo lygį. Naudojant *AODV* maršrutizavimo protokolą, iki 14 s rezultatas yra panašus į ankščiau aptartų protokolų, o nuo 14 s iki 28 s duomenys yra priimami maždaug 200 KB/s sparta. 130 KB/s sparta yra pasiekiama ir 88 sekundę. Šie trumpi spartos padidėjimai lėmė didesnę vidutinę duomenų priėmimo spartą, tačiau, kaip matome iš rezultatų, visais trimis atvejais duomenų priėmimo sparta yra žema ir netinkama multimedija paslaugų teikimui VANET tinkluose.



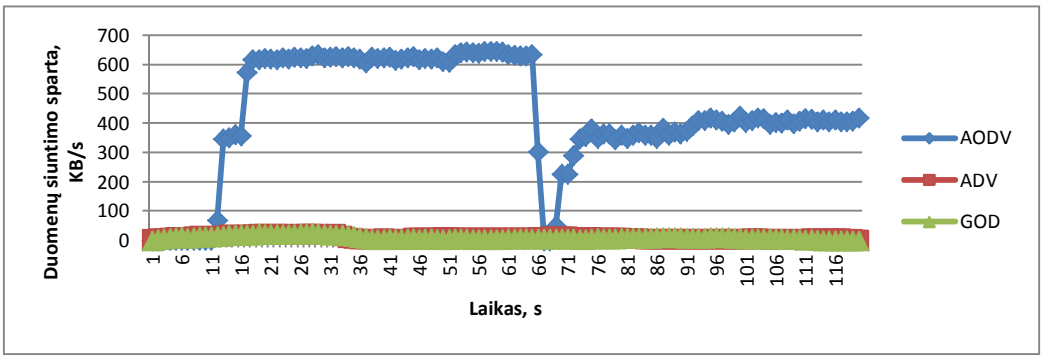
25 pav. *Duomenų priėmimo spartos priklausomybė nuo laiko, tinkle veikiant 50 automobilių, naudojant skirtingus maršrutizavimo protokolus*

25 pav. pateiktas duomenų siuntimo spartos priklausomybės nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus grafikas, kuris rodo analogiškus ankščiau aptartiems rezultatams duomenis. Aukščiausia vidutinė duomenų išsiuntimo sparta pasiekiama naudojant *AODV* maršrutizavimo protokolą – iki 570 KB/s tinkle veikiant 75 automobiliams, o naudojant *ADV* ir *GOD* duomenų išsiuntimo sparta yra itin žema ir siekia vos 10 – 20 KB/s, tačiau šios spartos pakanka eismo saugumo paslaugoms teikti.



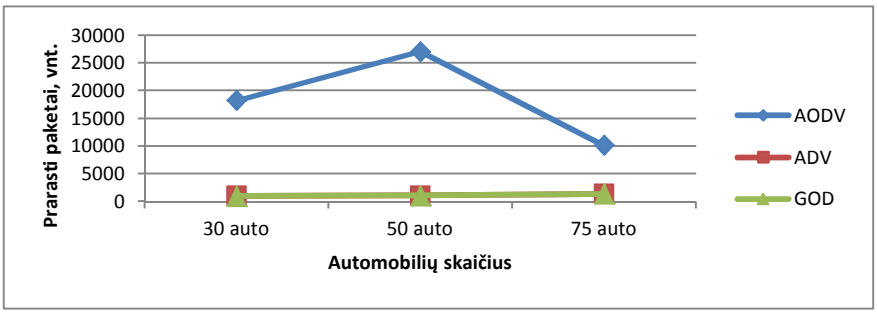
26 pav. *Duomenų siuntimo spartos priklausomybė nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus*

27 pav. pateiktas duomenų siuntimo spartos priklausomybės nuo laiko, tinkle veikiant 50 automobilių bei naudojant skirtingus maršrutizavimo protokolus grafikas, kuriame matome, kad naudojant *AODV* maršrutizavimo protokolą nuo 9 s iki 65 s yra išlaikoma pastovi aukšta (apie 630 KB/s) duomenų išsiuntimo sparta, nuo 65 s iki 69 s duomenų siuntimas nutrūksta, o nuo 70 s iki 120 s – apie 400 KB/s sparta.



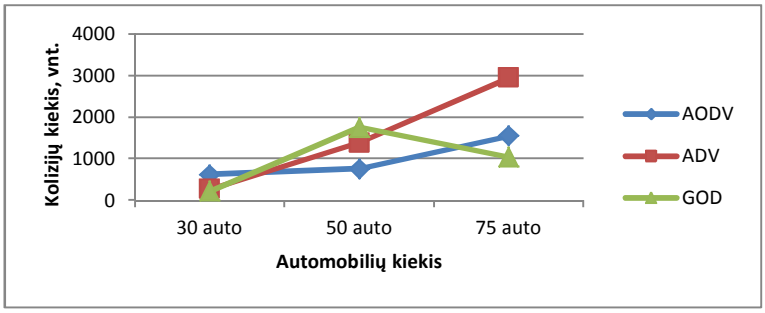
27 pav. *Duomenų siuntimo spartos priklausomybė nuo laiko, tinkle veikiant 50 automobilių, naudojant skirtingus maršrutizavimo protokolus*

27 pav. pateiktas prarastų paketų priklausomybės nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus grafikas, kuriame matome, kad naudojant *ADV* ir *GOD* maršrutizavimo algoritmus yra praktiškai tokie patys rezultatai ir paketų praradimas žemas, kadangi ir duomenų perduodama labai mažai, o naudojant *AODV* – didžiausias paketų praradimas kai tinkle 50 automobilių, mažiausias – kai 75 automobiliai.



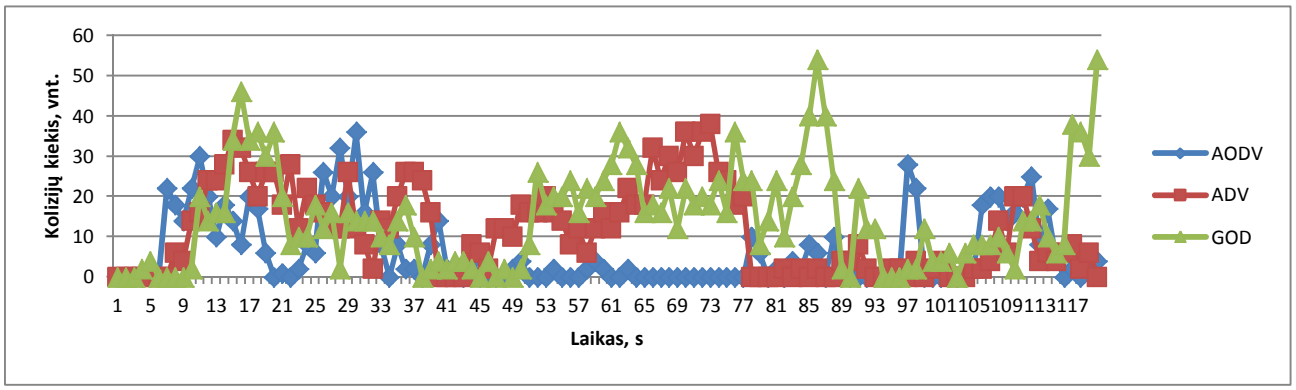
28 pav. *Prarastų paketų priklausomybė nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus*

28 pav. pateiktas kolizijų kiekio gavėjo mazge priklausomybės nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus grafikas. Iš grafiko galime matyti, kad naudojant *ADV* ir *AODV* maršrutizavimo protokolus, kolizijų skaičius gavėjo mazge auga tiesiškai ir yra tiesiogiai proporcingi automobilių kiekiui tinkle. Naudojant *GOD* protokolą, daugiausia kolizijų – kai tinkle veikia 50 automobilių, o mažiausia – kai 30.



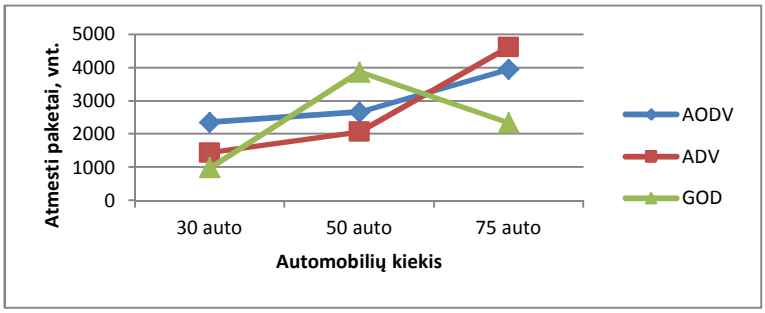
29 pav. *Kolizijų kiekio gavėjo mazge priklausomybė nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus*

29 pav. pateiktame grafike matome kolizijų kiekio gavėjo mazge priklausomybę nuo laiko, tinkle veikiant 50 automobilių bei naudojant skirtingus maršrutizavimo protokolus.

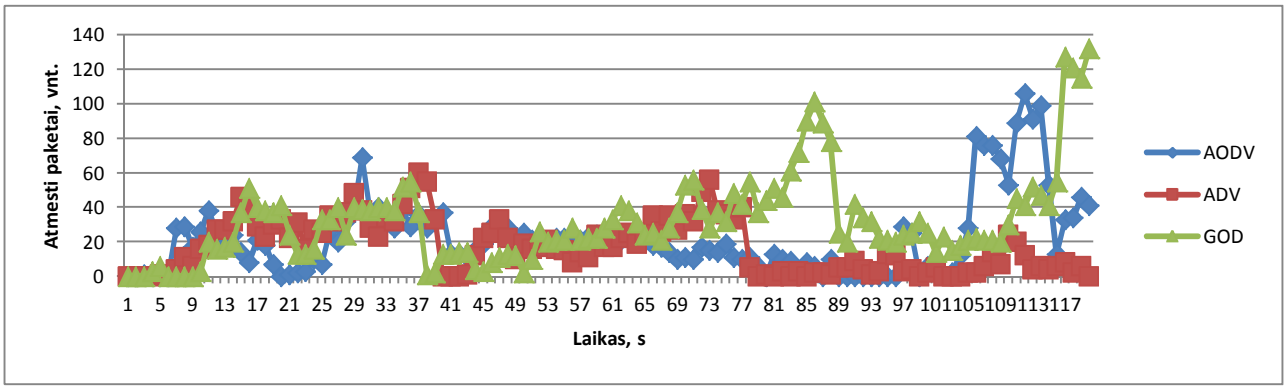


30 pav. *Kolizijų kiekio gavėjo mazge priklausomybė nuo laiko, tinkle veikiant 50 automobilių, naudojant skirtingus maršrutizavimo protokolus*

30 pav. pateiktas atmestų paketų gavėjo mazge priklausomybės nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus grafikas, o paketų atmetimo gavėjo mazge priklausomybė nuo laiko pateikta 31 pav. Šiuo atveju gavėjo mazge daugiausia paketų atmetama naudojant *ADV* maršrutizavimo algoritmą bei tinkle veikiant 75 automobiliams. Mažiausiai – *GOD* su 30 automobilių. Naudojant *AODV*, paketų atmetimas tiesiogiai proporcingas automobilių kiekiui.

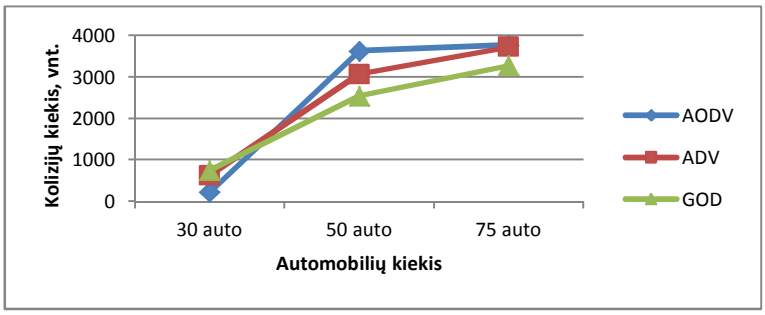


31 pav. *Atmestų paketų gavėjo mazge priklausomybė nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus*



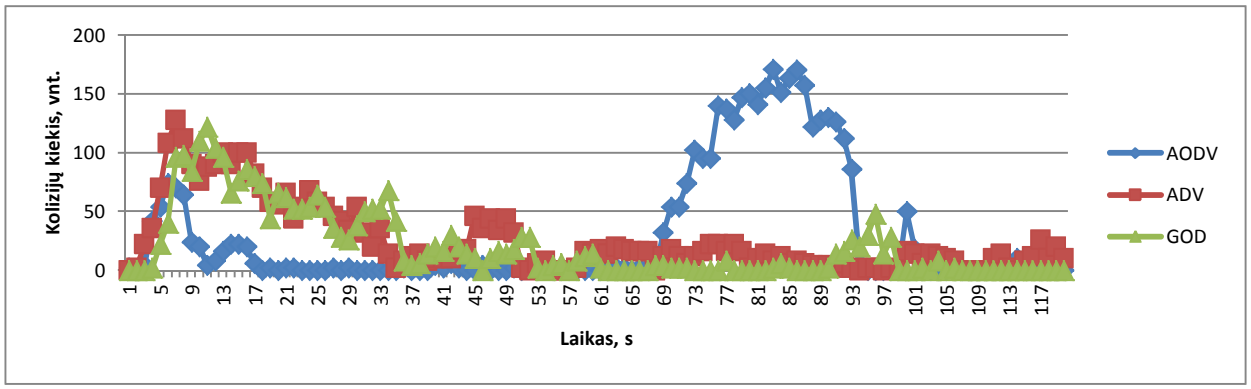
32 pav. *Atmestų paketų gavėjo mazge priklausomybė nuo laiko, tinkle veikiant 50 automobilių, naudojant skirtingus maršrutizavimo protokolus*

Kaip ir gavėjo mazge, taip ir siuntėjo, naudojant *AODV* ir *ADV* maršrutizavimo protokolus, kolizijų kiekis siuntėjo mazge tiesiogiai proporcingas automobilių kiekiui. Šiuo atveju tokia pati priklausomybė galioje ir *GOD* protokolui (31 pav.). Taip yra todėl, kad didėjant automobilių kiekiui, didėja ir kolizijų tikimybė, kadangi didėja kanalo apkrova.



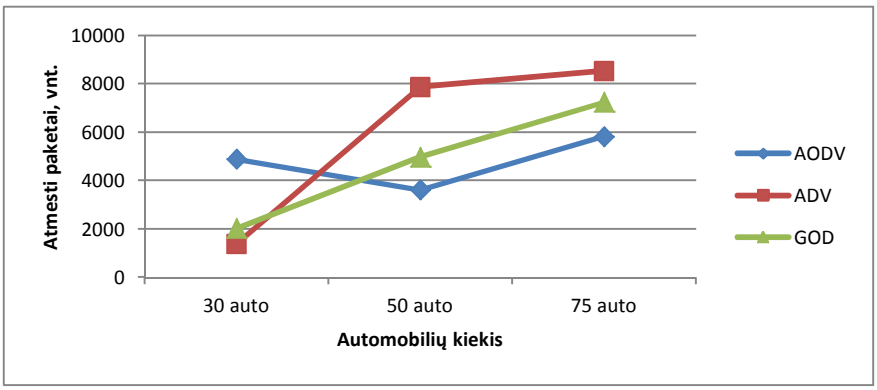
33 pav. *Kolizijų kiekio siuntėjo mazge priklausomybė nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus*

33 pav. parodyta kolizijų kiekio siuntėjo mazge priklausomybė nuo laiko, tinkle veikiant 50 automobilių, naudojant skirtingus maršrutizavimo protokolus. Matome, kad iki 65 s kolizijų kiekis buvo panašus naudojant visus protokolus, o nuo 65 s iki 95 s, *AODV* protokolo kolizijos sparčiai išauga. Tai lėmė sumažėjusią duomenų siuntimo ir priėmimo spartą (25 ir 27 pav.)

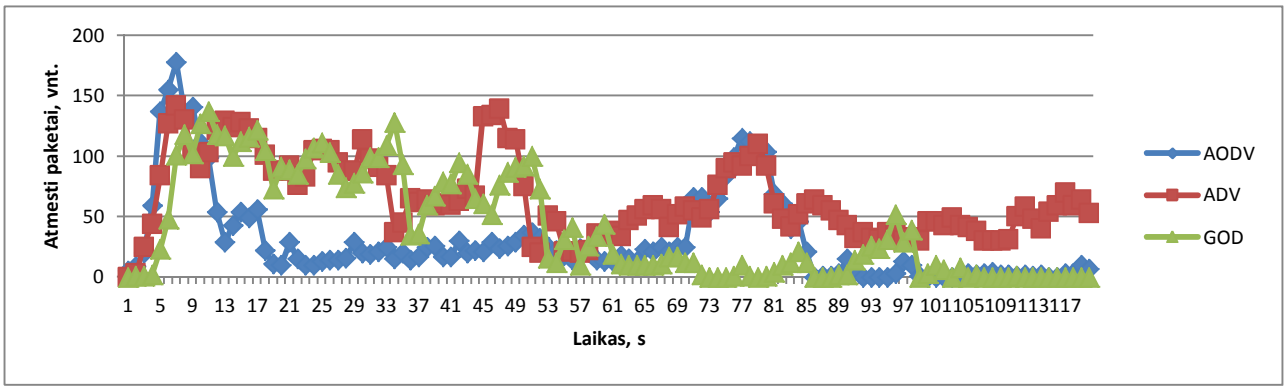


34 pav. *Kolizijų kiekio siuntėjo mazge priklausomybė nuo laiko, tinkle veikiant 50 automobilių, naudojant skirtingus maršrutizavimo protokolus*

35 ir 36 pav. pavaizduotos atmestų paketų siuntėjo mazge priklausomybės nuo automobilių kiekio bei priklausomybės nuo laiko, naudojant skirtingus maršrutizavimo protokolus. Naudojant *AODV* maršrutizavimo protokolą mažiausias atmestų paketų kiekis yra tinkle veikiant 50 automobilių, didžiausias – 75 automobiliams. Naudojant *ADV* ir *GOD*, mažiausias – tinkle veikiant 30 automobilių, didžiausias – 75 automobiliams.



35 pav. *Atmestų paketų siuntėjo mazge priklausomybė nuo automobilių kiekio, naudojant skirtingus maršrutizavimo protokolus*



36 pav. *Atmestų paketų siuntėjo mazge priklausomybė nuo laiko, tinkle veikiant 50 automobilių, naudojant skirtingus maršrutizavimo protokolus*

9.3. Eksperimento apibendrinimas

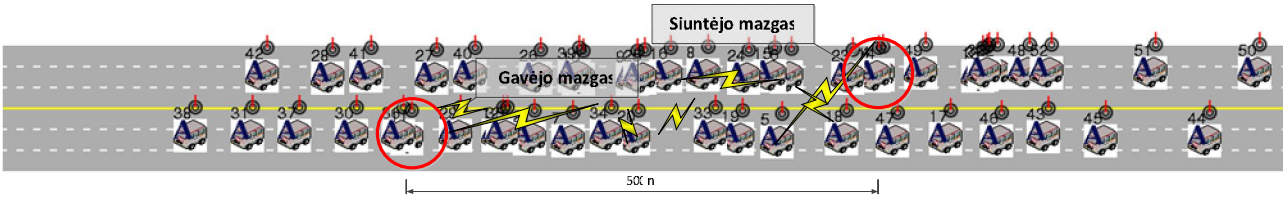
Buvo atliktas skirtingų ad-hoc maršrutizavimo protokolų efektyvumo eismo saugumo ir multimedija paslaugų teikimui tyrimas. Ištirti 3 *ad-hoc* maršrutizavimo protokolai automobilinėje komunikacijoje miesto sąlygomis. Tyrimo metu nustatyti bevielės komunikacijos kokybiniai parametrai ir surastos priklausomybės nuo automobilių kiekio bei laiko. Rezultatai rodo, kad geriausi rezultatai pasiekiami naudojant *AODV* ad-hoc maršrutizavimo protokolą, kadangi šiuo atveju buvo pasiekta didžiausia duomenų išsiuntimo ir priėmimo sparta, mažiausias procentas prarastų paketų (vidutiniškai 32%). Šis maršrutizavimo protokolas yra potencialiai tinkamas didelio tikslumo nereikalaujančioms multimedija (*IP* telefonija, vaizdo medžiagos transliacija) bei eismo saugumo paslaugoms teikti miesto sąlygomis. Naudojant *ADV* protokolą, gaunami prasti duomenų perdavimo spartos rezultatai ir praktiškai visas ryšio kanalas sunaudojamas maršrutizavimo žinutėms perduoti. Šis protokolas netinkamas multimedija paslaugų teikimui miesto sąlygomis, iš dalies juo naudojantis galima teikti nekritines eismo saugumo paslaugas. *GOD* režimo tinkamumas nėra vertinamas, kadangi tai nėra realus maršrutizavimo protokolas, kuris buvo tiriamas palyginimo tikslais. Atsižvelgiant į gautus rezultatus, galima daryti išvadą, kad norint teikti kokybiškas multimedija bei eismo saugumo paslaugas yra reikalingi nauji, specialiai pritaikyti automobilinei komunikacijai ad-hoc maršrutizavimo protokolai.

10. Eismo saugumo ir multimedija paslaugų teikimo efektyvumo, siuntėjui ir gavėjui judant priešingomis kryptimis automagistralėje, tyrimas

10.1.Eksperimento sudarymas

Šio eksperimento tikslas – ištirti eismo saugumo ir multimedija paslaugų teikimo efektyvumą, siuntėjui ir gavėjui judant priešingomis kryptimis automagistralėje. Eksperimentas vykdytas, kai automobilių kiekis tinkle yra nuo 10 iki 100 automobilių, siekiant nustatyti automobilių kiekio įtaką duomenų perdavimo efektyvumui. Automobiliai juda dideliu greičiu (130 km/h) priešingomis kryptimis. Likę automobiliai, juda skirtingais greičiais: nuo 90 km/h iki 150

km/h, o jų judėjimo kryptys pasiskirsčiusios tolygiai. Automobilio (4) yra siunčiami duomenys automobiliui (11). Komunikacija vyksta *801.11b* ryšiu bei yra naudojamas *multi-hop* duomenų perdavimas. Eksperimento metu buvo įvertinamas duomenų perdavimo efektyvumas – siuntimo sparta, priėmimo sparta, paketų atmetimas, kolizijų kiekis esant skirtingam automobilių skaičiui tinkle. Duomenys perduodami *UDP* protokolu, vieno paketo dydis – 1000 baitų. Simuliacija vykdoma 60 sekundžių. Sudarant eksperimentą remiamasi prielaidomis, kad komunikacijos laikas tarp siuntėjo ir gavėjo yra tiesiogiai proporcingas automobilių kiekiui tinkle. Taip pat didėjant automobilių kiekiui turėtų išaugti kolizijų kiekis bei atmetamų paketų skaičius. 37 pav. pateiktas eksperimento scenarijus.



37 pav. *Duomenų perdavimo efektyvumo automagistralėse eksperimentų scenarijus*

Eksperimento atlikimui naudojami simuliacijos parametrai pateikti 6 lentelėje.

6 lentelė. *Eksperimentui atlikti naudojami simuliacijos parametrai*

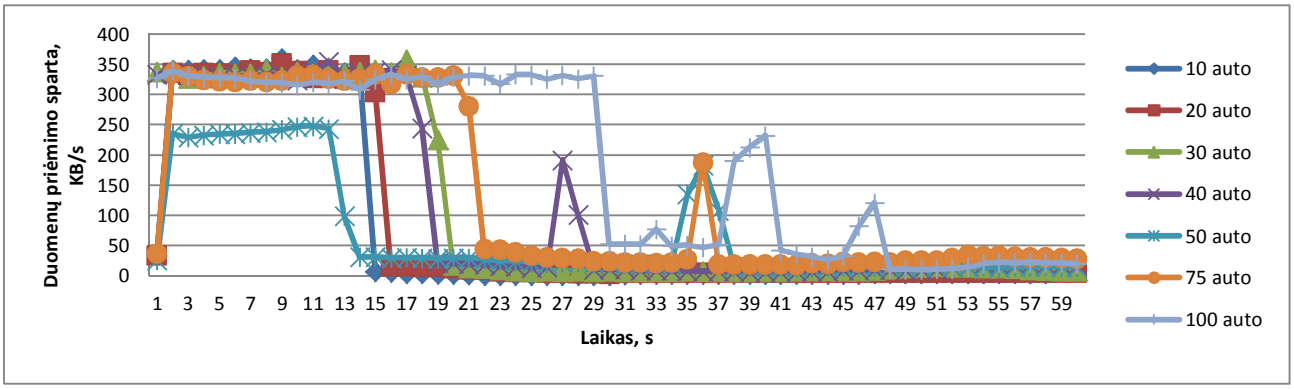
Parametras	**Reikšmė**
Simuliacijos laikas	60 s
Fizinio sluoksnio protokolas	802.11b
Automobilių skaičius	Nuo 10 iki 100
Mazgų judėjimas	Atsitiktinis, greitkelio mobilumo modelis
Kanalo dažnis	2,4 GHz
Maršrutizavimo protokolas	AODV

10.2.Eksperimento rezultatai

Atlikus tyrimą ir apdorojus gautus duomenis, buvo gauti ir toliau pateikiami šie eksperimentų rezultatai: duomenų priėmimo spartos priklausomybė nuo laiko, esant skirtingam automobilių skaičiui tinkle, vidutinės duomenų siuntimo ir priėmimo spartos priklausomybė nuo automobilių skaičiaus tinkle, prarastų paketų priklausomybė nuo automobilių skaičiaus tinkle, atmestų paketų kiekio priklausomybė nuo automobilių skaičiaus tinkle siuntėjo ir gavėjo mazguose, kolizijų priklausomybė nuo automobilių kiekio siuntėjo ir gavėjo mazguose.

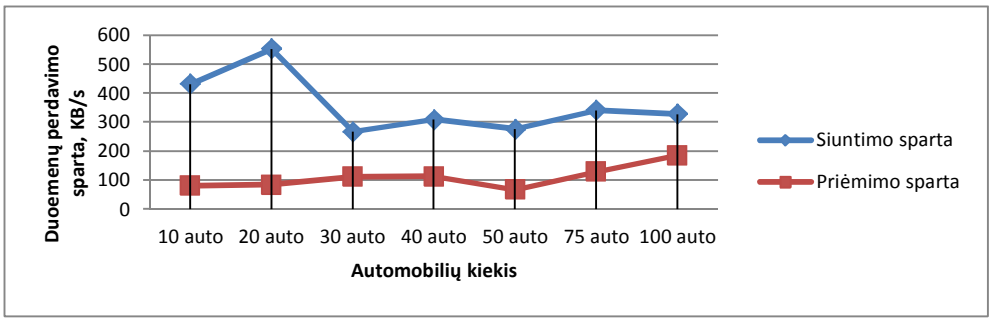
38 paveiksle pateiktas duomenų priėmimo spartos priklausomybės nuo laiko, esant skirtingam automobilių skaičiui tinkle grafikas. Iš grafiko matome, kad ilgiausias komunikacijos laikas yra pasiekiamas tinkle veikiant didžiausiam automobilių skaičiui – 100. Dėl didžiausio automobilių kiekio, tinklo aprėptis išauga, todėl duomenis galima perduoti ilgesnį laiko tarpą. Esant 100 automobilių su maždaug 330 KB/s duomenų perdavimo sparta, komunikaciją pavyko išlaikyti 30 sekundžių, nuo 31 s sparta nukrito iki 50 KB/s, tačiau nuo 37 iki 41 s sparta pakyla iki 230 KB/s,

o nuo 46 s iki 48 s – iki 130 KB/s. Vėliau automobiliams pravažiavus vieniems pro kitus ryšys nutrūksta. Mažiausias duomenų perdavimo spartos pikas pasiekiama tinkle veikiant 50 automobilių. Taip pat, šiuo atveju yra išlaikoma trumpiausia komunikacija. Esant mažam automobilių skaičiui (10 – 30) yra išlaikoma gana didelė duomenų perdavimo sparta, dėl nedidelio kolizijų kiekio.



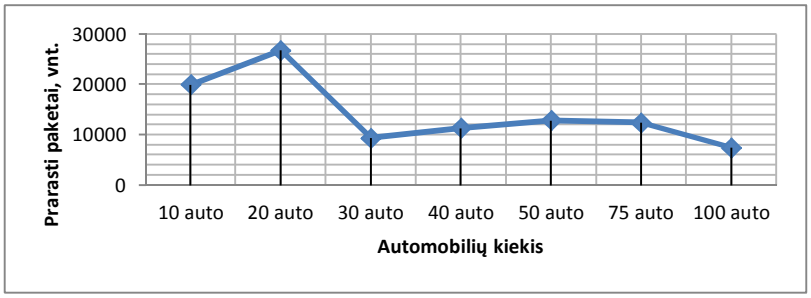
38 pav. *Duomenų priėmimo spartos priklausomybė nuo laiko, esant skirtingam automobilių skaičiui tinkle*

39 pav. pateikta vidutinės duomenų siuntimo ir priėmimo spartos priklausomybė nuo automobilių skaičiaus tinkle. Šiuo atveju didžiausia vidutinė siuntimo sparta pasiekiama tinkle veikiant 20 automobilių, o mažiausia – 30. Didžiausia vidutinė duomenų priėmimo sparta – tinkle veikiant 100 automobilių, o mažiausia – 50.



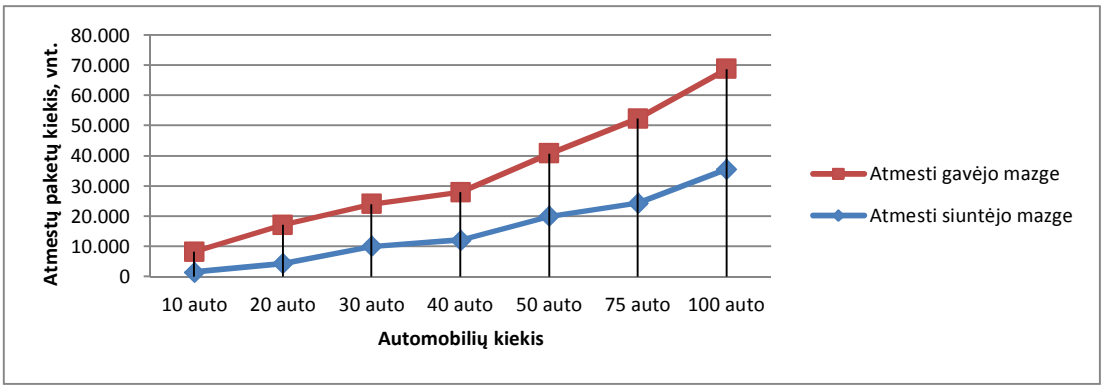
39 pav. *Vidutinės duomenų siuntimo ir priėmimo spartos priklausomybė nuo automobilių skaičiaus tinkle*

Nors iš 39 pav. matome, kad didžiausia vidutinė duomenų išsiuntimo sparta pasiekiama tinkle veikiant 20 automobilių, tačiau 40 pav. galime matyti, kad šiuo atveju yra didžiausias prarandamų paketų skaičius – 26761. Mažiausiai paketų prarandama tinkle veikiant 100 automobilių. Nuo 30 iki 50 automobilių paketų praradimas po truputį auga, o nuo 50 iki 100 – ima mažėti.



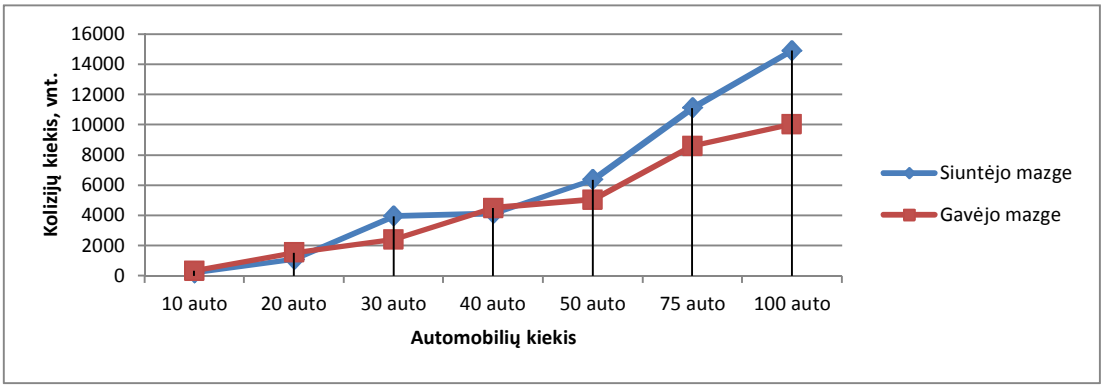
40 pav. *Prarastų paketų priklausomybė nuo automobilių skaičiaus tinkle*

41 pav. pateikta atmestų paketų kiekio priklausomybė nuo automobilių skaičiaus tinkle siuntėjo ir gavėjo mazguose. Iš grafikų matome, kad atmestų paketų skaičius didėja tiesiogiai proporcingai pagal automobilių kiekį. Taip yra todėl, kad didėjant automobilių kiekiui, didėja ir tų pačių paketų gavėjo mazgui, atsiunčiamų skirtingų tarpinių mazgų. Siuntėjo mazge paketai yra atmetami dėl įvykstančių kolizijų, dėl netinkamai veikiančių kanalo prieigos paskirstymo mechanizmų. Didesnė dalis paketų yra atmetama gavėjo mazge. 45% paketų atmetama siuntėjo mazge ir 55% - gavėjo.



41 pav. *Atmestų paketų kiekio priklausomybė nuo automobilių skaičiaus tinkle siuntėjo ir gavėjo mazguose*

42 pav. pateikta kolizijų priklausomybė nuo automobilių kiekio siuntėjo ir gavėjo mazguose. Kolizijų kiekis tiesiogiai proporcingas automobilių skaičiui. Iki 40 automobilių tiek gavėjo, tiek siuntėjo mazguose jis yra panašus, o nuo 50 automobilių kolizijų skaičius yra didesnis siuntėjo mazge dėl automobilinei komunikacijai nepritaikytų kanalo prieigos užtikrinimo mechanizmų.



42 pav. *Kolizijų priklausomybė nuo automobilių kiekio siuntėjo ir gavėjo mazguose*

10.3.Eksperimento apibendrinimas

Buvo ištirtas eismo saugumo ir multimedija paslaugų teikimo efektyvumas automagistralėje, siuntėjui ir gavėjui judant priešingomis kryptimis dideliu greičiu. Nustatyta, kad ilgiausiai komunikacija gali būti išlaikoma esant didžiausiam automobilių skaičiui tinkle, tačiau šios komunikacijos kokybė yra atvirkščiai proporcinga automobilių skaičiui, kadangi didėjant automobilių skaičiui – didėja tinklo užliejimas duomenimis bei įvyksta daug kolizijų. Norint teikti kokybiškas multimedija bei eismo saugumo paslaugas yra reikalingi nauji maršrutizavimo

protokolai bei kanalo prieigos užtikrinimo metodai, skirti dideliam kiekiui didžiuliu greičiu judančių mazgų bei greitai kintančios topologijos *VANET* tinklams.

11. Skirtingų bevielio ryšio technologijų panaudojimo eismo saugumo bei multimedija paslaugų teikimui automobilių komunikacijos tinkluose efektyvumo tyrimas miesto bei greitkelio sąlygomis

11.1.Eksperimento sudarymas

Šiuo metu egzistuoja keletas bevielio ryšio technologijų potencialiai tinkamų automobilinės komunikacijos tinklams. Pagrindinės iš jų: *802.11a/b/g/n*, *802.11p* bei *802.16e*. šio tyrimo tikslas nustatyti kuri iš bevielio ryšio technologijų geriausiai tinka eismo saugumo bei multimedija paslaugų teikimui automobilinės komunikacijos tinklais.

Eksperimentų metu buvo tiriamas *802.11b*, *802.11p* bei *802.16e* duomenų perdavimo efektyvumas tarp *RSU* ir automobilio. Bandymai buvo atliekami miesto ir automagistralės sąlygomis. Miesto sąlygomis automobilis judėjo vidutiniu 35 km/h greičiu, o automagistralės – 130 km/h greičiu. Eksperimento metu buvo įvertinamas duomenų perdavimo efektyvumas – siuntimo sparta, priėmimo sparta, paketų atmetimas, kolizijų kiekis. Simuliacija vykdoma 120 sekundžių.

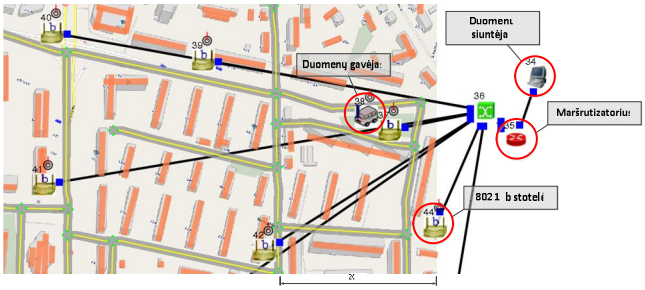
Eksperimentų atlikimui naudojami simuliacijos parametrai pateikti 7 lentelėje.

7 lentelė. *Eksperimentams atlikti naudojami simuliacijos parametrai*

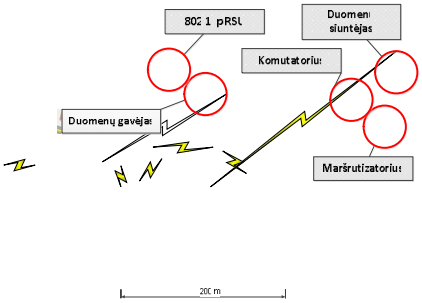
Parametras	**Reikšmė**
Simuliacijos laikas	120 s
Fizinio sluoksnio protokolas	802.11b, 802.11p, 802.16e
Automobilių skaičius	1
Mazgų judėjimas	Atsitiktinis, miesto mobilumo modelis, greitkelio mobilumo modelis
Kanalo dažnis	2,4 GHz

11.2.Eksperimentai miesto sąlygomis

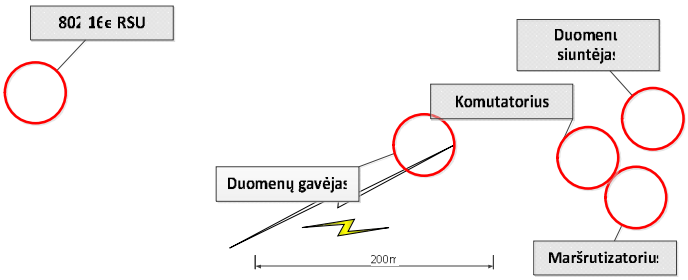
Pirmiausia, eksperimentai vykdomi miesto sąlygomis. Naudojamas realus miesto žemėlapis, kuriame išdėstyti namai, blokuojantys signalą bei vairuotojo matomumą. Simuliuojamas vieno automobilio judėjimas bei komunikavimas su *802.11b*, *802.11p* ir *802.16e RSU*. Duomenys yra perduodami iš serverio pažymėtu „Duomenų siuntėjas“. Serveris prijungtas prie maršrutizatoriaus, o pastarasis prie komutatoriaus, prie kurio prijungti visi *RSU*. Duomenys siunčiami TCP protokolu, vieno paketo dydis – 1000 baitų. 43-45 pav. pateikti eksperimento vykdymo scenarijai, naudojant *802.11b*, *802.11p*, *802.16e* bevielio ryšio technologijas.



43 pav. *802.11b bevielio ryšio technologijos tyrimo miesto sąlygomis scenarijus*



44 pav. *802.11p bevielio ryšio technologijos tyrimo miesto sąlygomis scenarijus*



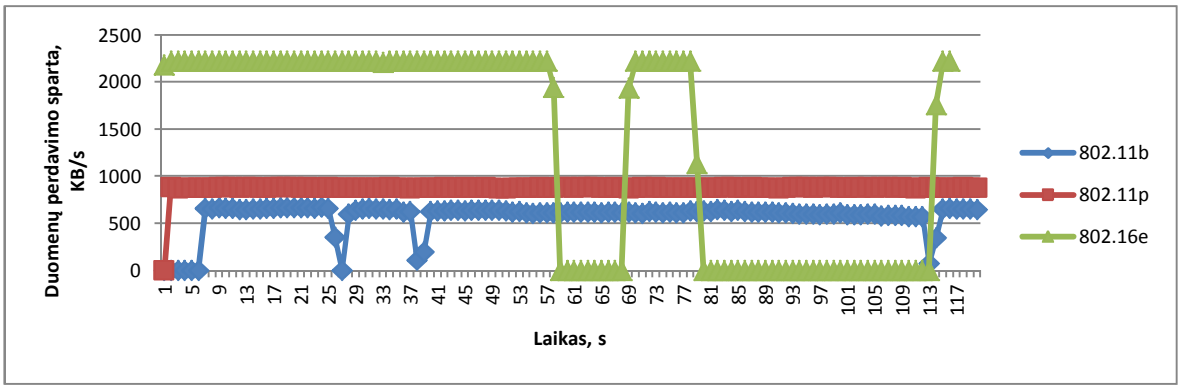
45 pav. *802.16e bevielio ryšio technologijos tyrimo miesto sąlygomis scenarijus*

11.3.Eksperimentų rezultatai miesto sąlygomis

Atlikus tyrimą ir apdorojus gautus duomenis, buvo gauti ir toliau pateikiami šie eksperimentų rezultatai: duomenų priėmimo bei išsiuntimo spartos priklausomybės nuo laiko, naudojant *802.11b*, *802.11p* ir *802.16e* bevielio ryšio technologijas, paketų praradimo priklausomybė nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio technologijas, paketų atmetimo gavėjo mazge priklausomybė nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio technologijas, kolizijų kiekio gavėjo mazge priklausomybė nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio technologijas miesto sąlygomis.

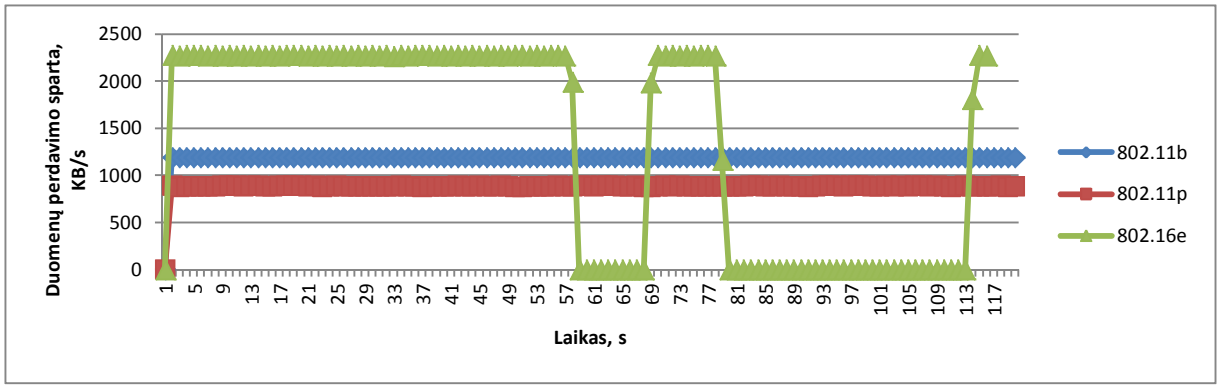
46 pav. pateiktas duomenų priėmimo spartos priklausomybės nuo laiko, naudojant *802.11b*, *802.11p* ir *802.16e* bevielio ryšio technologijas grafikas. Iš gautų rezultatų matome, kad didžiausia duomenų priėmimo sparta buvo pasiekta naudojant *802.16e* mobilaus *WiMAX* technologiją. Ši technologija leidžia pasiekti aukštą duomenų perdavimo spartą tiek tiesioginio, tiek netiesioginio matomumo sąlygomis [158]. Naudojant šią technologiją buvo pasiekta apie 2200 KB/s duomenų priėmimo sparta, kas leidžia užtikrinti tiek didelio duomenų srauto reikalaujančių multimedija paslaugų, tiek ir eismo saugumo užtikrinimo paslaugų teikimą automobiliniame tinkle. Nuo 60 s iki 69 s ir nuo 80 s iki 110s duomenų perdavimo sparta krito, dėl dingusio signalo tarp automobilio ir *RSU*. Tą galėjo sąlygoti netinkamai išdėstyti *RSU* tankiai apstatyto miesto sąlygomis. Šias problemas galėtų išspręsti tinkamas *IEEE 802.16j* standarto retransliacijos stočių išdėstymas, leidžiantis minimaliomis sąnaudomis maksimizuoti tinklo aprėpties zoną ir pasiekti maksimalią greitaveiką [101]. Naudojant 802.11p bevielio ryšio technologiją, specialiai sukurtą automobilinei

komunikacijai, matome, kad duomenų perdavimo sparta išlieka stabili ir siekia apie 900 KB/s, ko užtenka net didelio duomenų srauto reikalaujančioms multimedija bei eismo saugumo užtikrinimo paslaugoms. Šiuo atveju nėra spartos kritimo, kaip naudojant mobilaus *WiMAX* prieigą. Naudojant *802.11b* technologiją, duomenų priėmimo sparta yra žemiausia iš tirtų technologijų – siekia apie 600 KB/s, ko taip pat užtenka patikimam multimedija bei eismo saugumo užtikrinimo paslaugų veikimui. Šiuo atveju matome ryšio dingimą 4 vietose – iki 6 s, ties 26 s, 38 s bei 113 s. Tą lėmė persijungimo prie kitos bevielio ryšio stotelės laikas (*handoff*).



46 pav. *Duomenų priėmimo spartos priklausomybė nuo laiko, naudojant 802.11b, 802.11p ir 802.16e bevielio ryšio technologijas miesto sąlygomis*

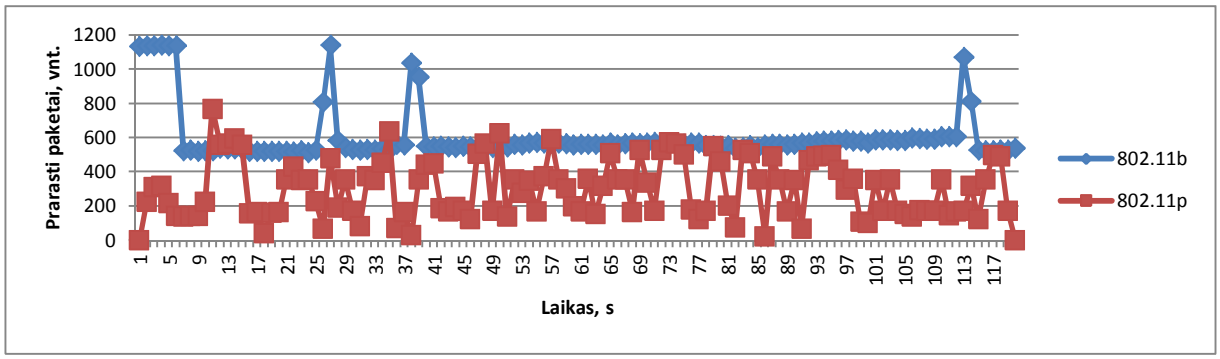
47 pav. pateiktame duomenų siuntimo spartos priklausomybės nuo laiko, naudojant *802.11b*, *802.11p* ir *802.16e* bevielio ryšio technologijas grafike matome kaip kinta duomenų išsiuntimo sparta laiko atžvilgiu. Kaip ir duomenų priėmimo atveju, didžiausia sparta pasiekiama naudojant mobiliojo *WiMAX* prieigą – 2270 KB/s, tačiau kaip ir ankstesniu atveju matome ryšio dingimą tuo pačiu metu. 1200 KB/s greitaveika pasiekiama naudojant *802.11p* technologiją. Duomenų perdavimo sparta išlieka stabili visą simuliacijos laiką. 890 KB/s greitaveika pasiekiama naudojant *802.11b*. duomenų perdavimo sparta taip pat pastovi.



47 pav. *Duomenų siuntimo spartos priklausomybė nuo laiko, naudojant 802.11b, 802.11p ir 802.16e bevielio ryšio technologijas miesto sąlygomis*

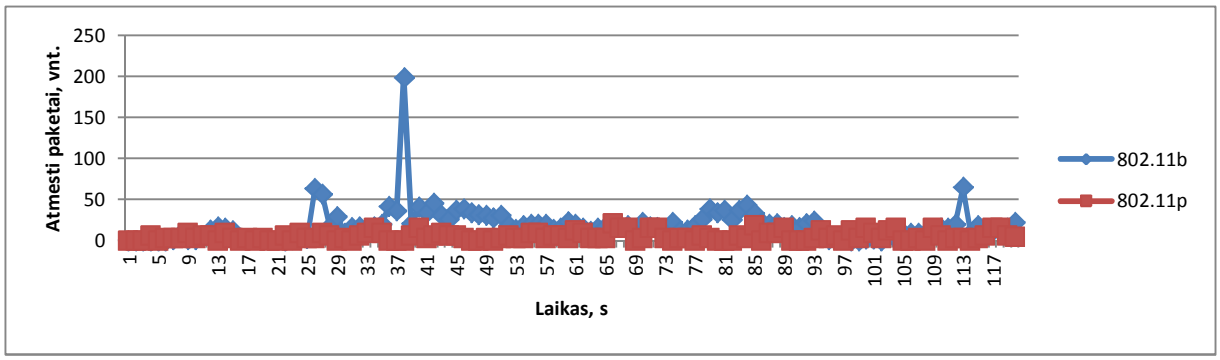
48 pav. pavaizduota paketų praradimo priklausomybė nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio technologijas. Iš pateikto grafiko matome, kad ženkliai daugiau paketų prarandama naudojant *802.11b* bevielio ryšio technologiją. Naudojant *802.11p* paketų praradimas

svyruoja. Dėl simuliavimo programinės įrangos apribojimų, negalima įvertinti 802.11e ryšio paketų praradimo bei kolizijų.



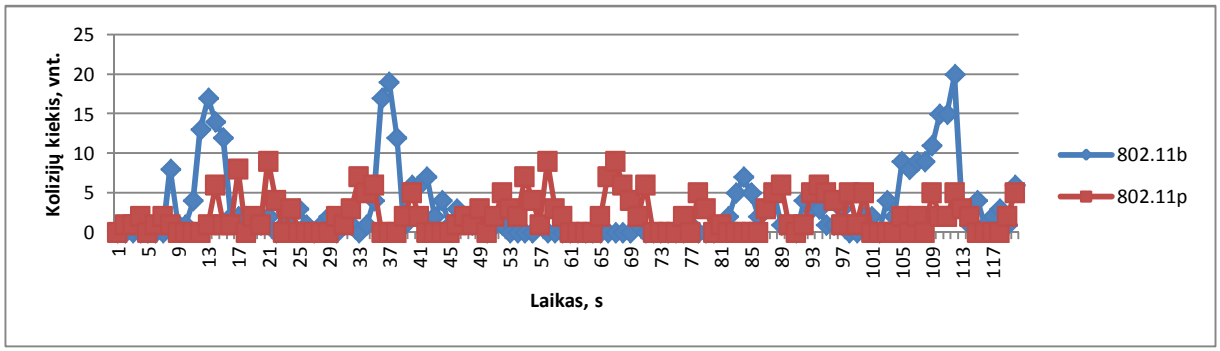
48 pav. *Paketų praradimo priklausomybė nuo laiko, naudojant 802.11b ir 802.11p bevielio ryšio technologijas miesto sąlygomis*

49 pav. pateikta paketų atmetimo gavėjo mazge priklausomybė nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio technologijas. Rezultatai rodo, kad gavėjo mazge mažiau paketų atmetama naudojant 802.11p technologiją – 36%, o 802.11b – 53%, kas patvirtina ir 48 pav. pateiktus rezultatus. Naudojant *802.11b* technologiją išryškėja paketų atmetimo pikai 25, 38 ir 113 sekundėmis. Galima daryti prielaidą, kad tuo metu vyko „*handoff*“ procedūra.



49 pav. *Paketų atmetimo gavėjo mazge priklausomybė nuo laiko, naudojant 802.11b ir 802.11p bevielio ryšio technologijas miesto sąlygomis*

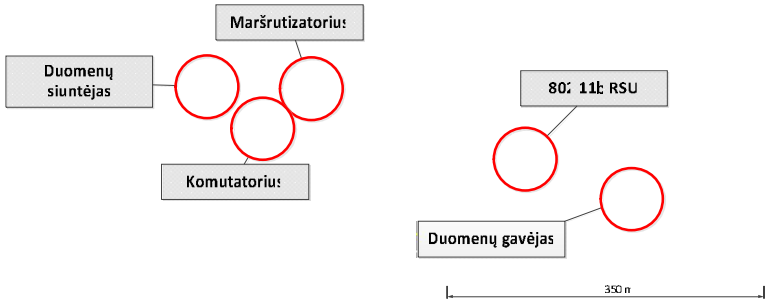
50 pav. pateiktas kolizijų kiekio gavėjo mazge priklausomybės nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio technologijas grafikas. Grafike matomi ryškūs kolizijų pikai, duomenis perduodant *802.11b* ryšiu.



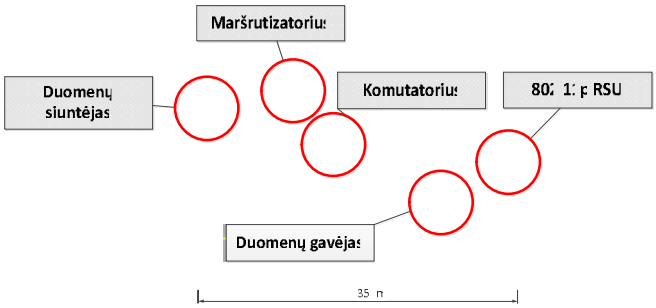
50 pav. *Kolizijų kiekio gavėjo mazge priklausomybė nuo laiko, naudojant 802.11b ir 802.11p bevielio ryšio technologijas miesto sąlygomis*

11.4.Eksperimentai automagistralės sąlygomis

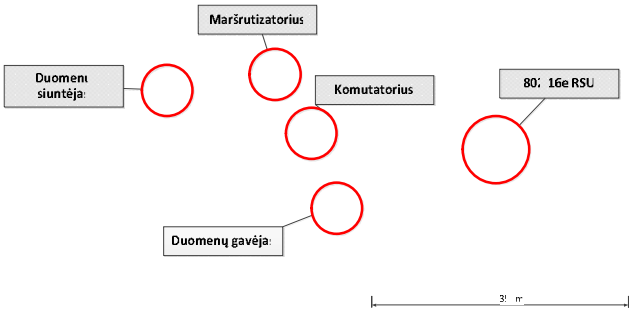
Analogiški prieš tai aptarti eksperimentai buvo vykdomi ir automagistralės sąlygomis. Naudojamas magistralės žemėlapis, kuriame nėra objektų, blokuojančių bevielio ryšio signalą. Simuliuojamas vieno automobilio judėjimas bei komunikavimas su *802.11b*, *802.11p* ir *802.16e RSU*. Duomenys yra perduodami iš serverio pažymėtu „Duomenų siuntėjas“. Serveris prijungtas prie maršrutizatoriaus, o pastarasis prie komutatoriaus, prie kurio prijungti visi *RSU*. Duomenys siunčiami *TCP* protokolu, vieno paketo dydis – 1000 baitų. 51-53 pav. pateikti eksperimento vykdymo scenarijai, naudojant *802.11b*, *802.11p*, *802.16e* bevielio ryšio technologijas.



51 pav. *802.11b technologijos tyrimo automagistralės sąlygomis scenarijus*



52 pav. *802.11p technologijos tyrimo automagistralės sąlygomis scenarijus*



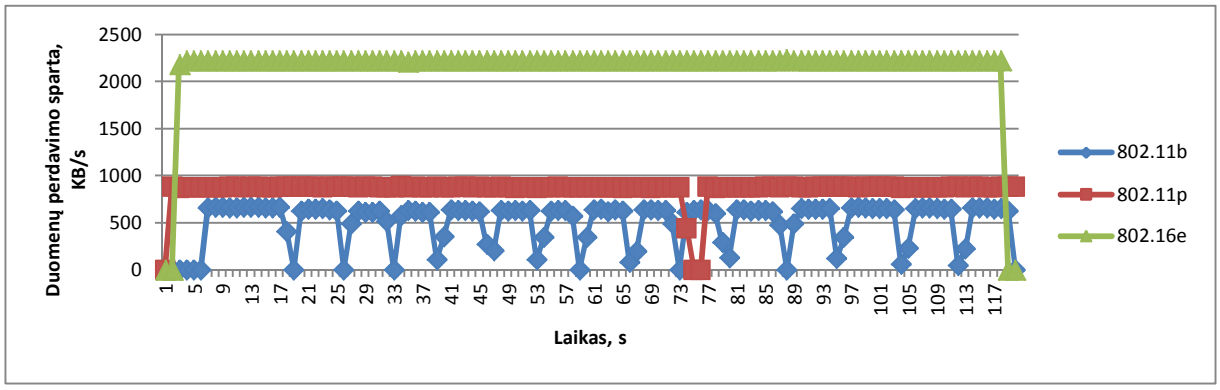
53 pav. *802.16e technologijos tyrimo automagistralės sąlygomis scenarijus*

11.5.Eksperimentų rezultatai automagistralės sąlygomis

Atlikus tyrimą ir apdorojus gautus duomenis, buvo gauti ir toliau pateikiami šie eksperimentų rezultatai: duomenų priėmimo bei išsiuntimo spartos priklausomybės nuo laiko, naudojant *802.11b*, *802.11p* ir *802.16e* bevielio ryšio technologijas, paketų praradimo priklausomybė nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio technologijas, paketų atmetimo gavėjo mazge priklausomybė nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio

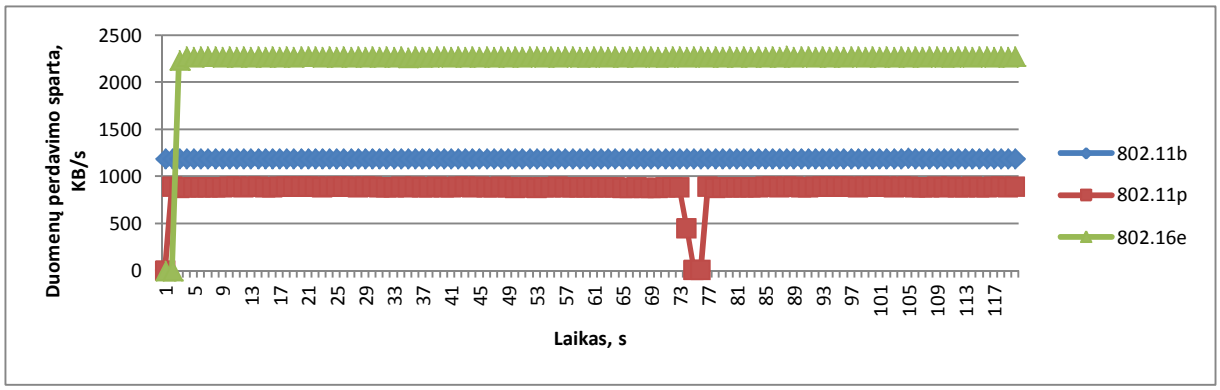
technologijas, kolizijų kiekio gavėjo mazge priklausomybė nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio technologijas miesto sąlygomis.

54 pav. pateiktas duomenų priėmimo spartos priklausomybė nuo laiko, naudojant *802.11b*, *802.11p* ir *802.16j* bevielio ryšio technologijas automagistralės sąlygomis grafikas. Iš grafiko matome, kad aukščiausia duomenų priėmimo sparta pasiekiama naudojant *802.11e* bevielio ryšio technologiją. Automagistralėje pasiekiama 2200 KB/s pastovi duomenų priėmimo sparta. Nors šis standartas skirtas mobiliems mazgams, kurių judėjimo greitis yra iki 120 km/h, tačiau kaip matome iš rezultatų ryšys yra patikimas ir judant 130 km/h greičiu, kuris yra maksimalus leistinas važiavimo greitis daugelyje valstybių. Duomenų priėmimo sparta išlieka pastovi visą simuliacijos laiką, nes šiuo atveju nėra trukdžių, kurie sudarė ryšio problemas miesto sąlygomis. Ši sparta leidžia užtikrinti aukštos kokybės multimedija bei eismo saugumo užtikrinimo paslaugų teikimą. *802.11p* ryšio technologija perduodami duomenys buvo priimami vidutine 880 KB/s sparta, kas yra pakankama tiek multimedija, tiek ir eismo saugumo paslaugų palaikymui. Ties 75s matomas spartos kritimas, kuris galėjo įvyko dėl „*handoff*“ procedūros arba dėl neoptimaliai išdėstytų *RSU*. Naudojant *802.11b* technologiją, buvo pasiekta 660 KB/s duomenų priėmimo sparta, kurios pakanka tiek multimedija, tiek ir eismo saugumo paslaugų palaikymui. Maždaug kas 5 s matomas duomenų priėmimo spartos kritimas, kuris vyko dėl „*handoff*“ procedūros, kuri dėl mažesnio ryšio nuotolio yra gerokai dažnesnė nei naudojant *802.11p* standartą.



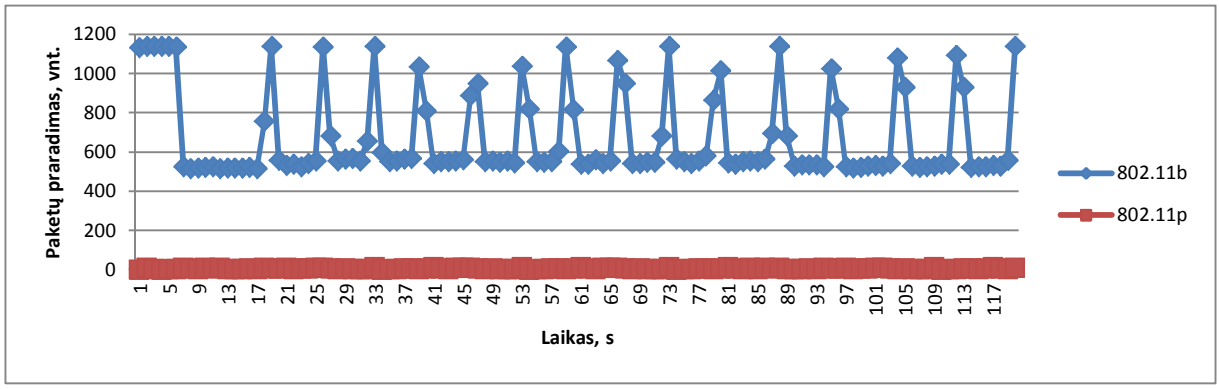
54 pav. *Duomenų priėmimo spartos priklausomybė nuo laiko, naudojant 802.11b, 802.11p ir 802.16j bevielio ryšio technologijas automagistralės sąlygomis*

55 pav. pateiktas duomenų siuntimo spartos priklausomybė nuo laiko, naudojant *802.11b*, *802.11p* ir *802.16j* bevielio ryšio technologijas automagistralės sąlygomis. Rezultatai rodo, kad visų trijų standartų perduodamos spartos pakanka tiek multimedija, tiek ir eismo saugumo paslaugų palaikymui. Naudojant mobilų *WiMAX* yra pasiekiama 2270 KB/s sparta, 802.11b – 1190 KB/s, 802.11p – 890 KB/s.



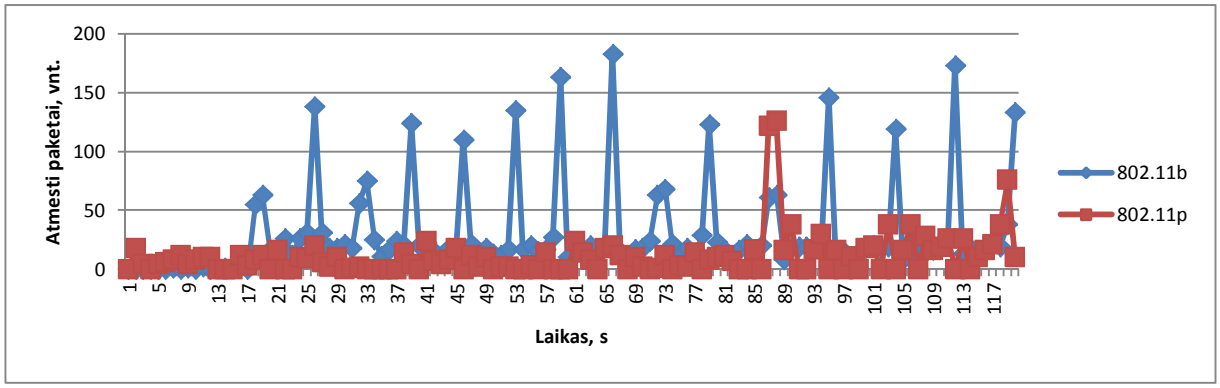
55 pav. *Duomenų siuntimo spartos priklausomybė nuo laiko, naudojant 802.11b, 802.11p ir 802.16j bevielio ryšio technologijas automagistralės sąlygomis*

56 pav. pateiktame paketų praradimo priklausomybės nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio technologijas automagistralės sąlygomis grafike matome, kad naudojant *802.11p* ryšio standartą yra ženkliai mažesnis paketų praradimas, lyginant su *802.11b* standartu. Naudojant *802.11p* prarandama 0,65% perduodamų paketų, o naudojant *802.11b* – net 59%. Taigi, *802.11p* užtikrina 90 kartų mažesnį paketų praradimą magistralės sąlygomis nei *802.11b*.



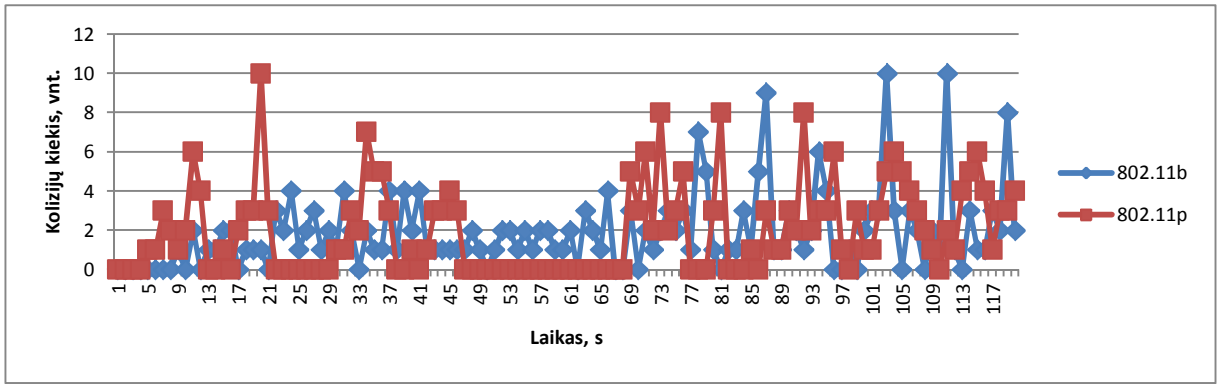
56 pav. *Paketų praradimo priklausomybė nuo laiko, naudojant 802.11b ir 802.11p bevielio ryšio technologijas automagistralės sąlygomis*

Panašius rezultatus rodo ir 57 pav. pateiktas paketų atmetimo gavėjo mazge priklausomybės nuo laiko, naudojant *802.11b* ir *802.11p* bevielio ryšio technologijas automagistralės sąlygomis grafikas. Ženkliai didesnis paketų skaičius atmetamas gavėjo mazge naudojant *802.11b* nei *802.11p*.



57 pav. *Paketų atmetimo gavėjo mazge priklausomybė nuo laiko, naudojant 802.11b ir 802.11p bevielio ryšio technologijas automagistralės sąlygomis*

58 pav. pateiktas grafikas rodo panašią kolizijų kiekio gavėjo mazge priklausomybę nuo laiko, naudojant tiek *802.11b*, tiek ir *802.11p* bevielio ryšio technologijas automagistralės sąlygomis.



58 pav. *Kolizijų kiekio gavėjo mazge priklausomybė nuo laiko, naudojant 802.11b ir 802.11p bevielio ryšio technologijas automagistralės sąlygomis*

11.6.Eksperimento apibendrinimas

Atlikus *802.11b*, *802.11p* bei *802.16e* duomenų perdavimo efektyvumo tarp *RSU* ir automobilio tyrimą miesto bei automagistralės sąlygomis bei įvertinus duomenų perdavimo efektyvumą – siuntimo spartą, priėmimo spartą, paketų atmetimą bei kolizijų kiekį galima daryti išvadas, kad visi trys metodai tinkami multimedija bei eismo saugumo užtikrinimo paslaugų teikimui. Geriausi duomenų perdavimo spartos rezultatai buvo pasiekti naudojant *802.16e* bevielio technologiją, tačiau šiuo atveju miesto sąlygomis buvo pastebimas ryšio dingimas, kurį galimą išspręsti optimizuojant retransliacijos stočių išdėstymą mieste. Dėl techninių simuliavimo paketo galimybių nebuvo įvertintas mobilaus *WiMAX* paketų praradimas bei kolizijų kiekiai, todėl šios technologijos panaudojimas reikalauja tolimesnių tyrimų.

802.11p bevielio ryšio technologijos naudojimo tiek miesto, tiek automagistralės sąlygomis parodė geriausią duomenų perdavimo bei paketų praradimo santykį. Šiuo atžvilgiu pastarajai technologijai gana ženkliai nusileidžia *802.11b* standartas, kurį naudojant buvo gana aukštas paketų praradimo skaičius.

Taigi, atliktas tyrimas parodė, multimedija bei eismo saugumo paslaugų teikimui automobilinėje komunikacijoje miesto bei automagistralės sąlygomis efektyviausia naudoti specialiai tam sukurtą *802.11p* technologiją, kuri užtikrina tiek aukštą duomenų perdavimo spartą, tiek žemą paketų praradimo lygį. Šios technologijos įdiegimui, taip pat, reikia įrengti mažiau infrastruktūros įrenginių, kadangi jos veikimo nuotolis yra didesnis.

12. Siūloma pasitikėjimu grindžiama autentifikavimo schema

Viena iš pagrindinių *VANET* problemų yra perduodamų duomenų saugumas bei anonimiškumas. Itin svarbu užtikrinti, tik autorizuotą prieigą prie tinklo, kadangi neapsaugotas tinklas gali būti pažeidžiamas įsilaužėlių, o tai, eismo saugumo situacijose gali turėti fatališkas

pasekmes. Įprastiems bevieliams tinklams sukurti saugumo mechanizmai netinka automobilinei komunikacijai, kadangi, kaip aptarta ankstesniuose skyriuose, mobilūs mazgai šiuose tinkluose juda žymiai didesniu greičiu, todėl labai svarbu kad mazgai galėtų kuo greičiau persijungti nuo vieno RSU ar ad-hoc režimu veikiančio automobilio kuo greičiu, taip sumažinant tam reikalingą laiką, vadinamą „*handoff*“. Šiame skyriuje pristatoma nauja pasitikėjimu grindžiama autentifikavimo schema, leidžianti ženkliai sumažinti „*handoff*“ laiką.

12.1.Autentifikavimas *802.11* tinkluose

802.11 tinkluose yra naudojamos dvi autentifikavimo schemos: atviros sistemos ir pasidalinto rakto. Atviros sistemos autentifikavime yra dvi autentifikavimo žinučių sekos. Pirmoji seka skirta identifikacijai ir autentifikavimo prašymui. Antroji – grąžina autentifikavimo rezultatą. Jei rezultatas yra teigiamas – klientui yra suteikiamas leidimas prisijungti prie sistemos [159]. Naudojant pasidalinto rakto autentifikavimą, pirmiausia yra išsiunčiamas prašymas prisijungti prie tinklo. Kai *AP* gauna autentifikavimo prašymą, ji išsiunčia kvietimo žinutę mobiliam mazgui. Mobilusis mazgas panaudodamas pasidalintą raktą, užkoduoja gautą žinutę ir išsiunčia atgal *AP*. *AP* taip pat užkoduoja tą pačią žinutę ir palyginą ją su gautąja iš mobilaus mazgo. Jei užkoduotos žinutės sutampa, mobilus mazgas gauna teisę prisijungti prie tinklo [95].

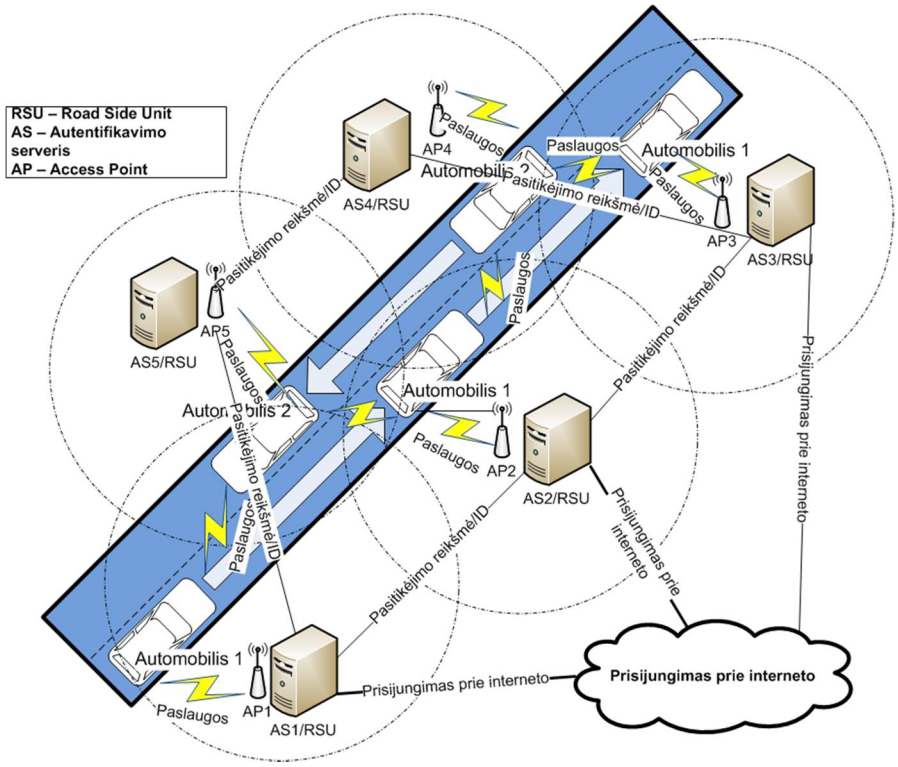
Kadangi *WEP* saugumo užtikrinimo bevieliuose vietiniuose tinkluose protokolas yra nesaugus, buvo sukurta naujas protokolas – *802.11i*. naudojant šį protokolą, tinklo mazgai yra padalinti į 3 grupes: prašytojus, autentifikatorius ir autentifikavimo serverius. Gavęs autentifikavimo prašymo žinutę, autentifikuotojai, naudodami išplėstą autentifikavimo protokolą (*EAP*) raktų sudarymui ir paskirstymui. *EAP* procesui pasibaigus yra sugeneruojamas *Pairwise Master Key* (*PMK*) ir perduodamas mobiliam mazgui. Tuomet, prašytojas ir autentifikuotojas, naudodamas keturių krypčių „handshake“ procesą sugeneruoja *PTK* (angl. *pairwise transient key*). Nors šie procesai gali būti pritaikomi *VANET* tinkams, dėl autentifikavimo vėlinimo jie yra netinkami.

12.2.Siūloma autentifikavimo schema

Dėl infrastruktūros nebuvo *ad-hoc* režimu veikiančiuose tinkluose, dėl didelio automobilių judėjimo greičio ir nuolat kintančios tinklo topologijos yra reikalingi nauji saugumo mechanizmai, galintys užtikrinti patikimą veikimą tokiomis sudėtingomis sąlygomis [133]. Siūlomos sistemos esmė – autentifikavimo mechanizmas yra grindžiamas pasitikėjimu tarp tinklo mazgų. Autentifikavimo procesas yra inicijuojamas tik į tinklą jungiantis naujam automobiliui. Visi automobiliai ir *RSU* yra suskirstyti į pasitikėjimo grupes. Kiekvienam automobiliui yra priskiriama pasitikėjimo reikšmė ir *ID*, kuriais nuolat apsikeičia autentifikavimo serveriai. Vienos pasitikėjimo grupės automobiliai ir *RSU* kitus šios grupės narius laiko patikimais. Kai naujas automobilis nori

prisijungti prie tinklo, jis turi įvykdyti visą *802.11i* standarte aprašytą autentifikavimo procedūrą ir jam turi būti sugeneruotas grupės sesijos raktas. Autentifikavimo serveriai nuolat apsikeičia reguliariai atnaujinama saugumo lentele, kurioje nurodomos mazgų pasitikėjimo vertės, mazgų *ID*, informacija apie sėkmingai autentifikuotus ir į juodąjį sąrašą įtrauktus mazgus. Kai automobilis nori prisijungti pries tinklo, kuris jau turi informaciją apie šį mazgą, automobilis gali pasinaudoti ankščiau sugeneruotu grupės sesijos raktu ir sugeneruoti *PTK*. Naudojant šią schemą, nereikia atlikti viso *802.11i* autentifikavimo proceso. Naudojant šią schemą, gali būti ženkliai sumažinamas persijungimo prie kitų *RSU* ar *ad-hoc* tinklų laikas. 59 paveiksle pateiktas galimas siūlomos autentifikavimo schemos panaudojimo scenarijus.

Tokiame automobilių komunikacijos tinkle, prašytojai yra automobiliai, aprūpinti *802.11p* bevielio ryšio sąsajomis. Šie automobiliai gali komunikuoti su *RSU* arba vienas su kitu *ad-hoc* režimu. Autentifikatoriai yra *RSU*, kuris tuo pačiu užtikrina prieigą prie interneto, arba kiti tinklo automobiliai (*ad-hoc* tinklo atveju). Pateiktame scenarijuje yra 2 automobiliai, 5 *AP* ir 5 autentifikavimo serveriai/*RSU*. Automobilių judėjimo kryptis parodyta rodyklėmis. Jungtys rodo paslaugas teikiamas *RSU* ir kitų automobilių. Pateiktame scenarijuje *AP1*, *AP2*, *AP3* ir Automobilis 1 yra vienoje, o *AP4*, *AP5* ir Automobilis 2 – kitoje pasitikėjimo grupėje. Automobilis 1 jungdamasis prie tinklo pasirenka *RSU* su stipriausiu signalu – *AP1*, kuris inicijuoja pilną autentifikavimo procedūrą, siekiant sugeneruoti grupės sesijos raktą (*GSK*) ir *PTK*.

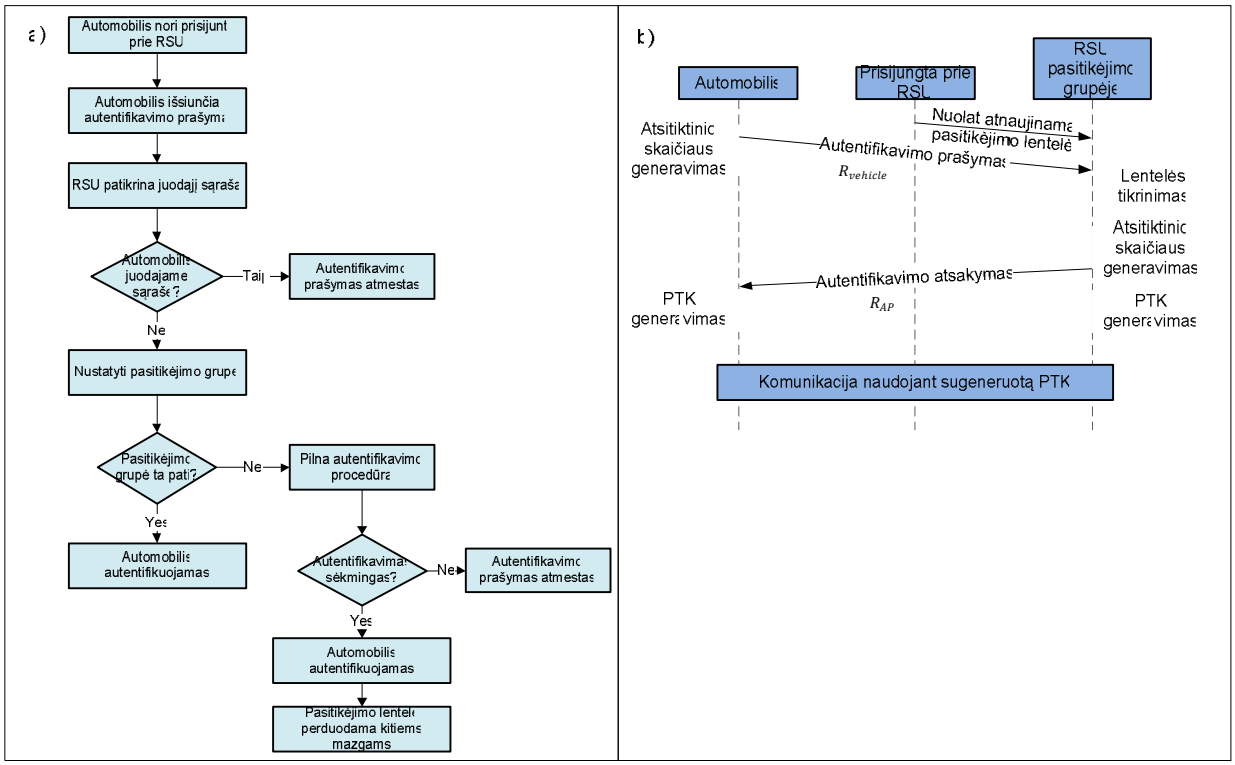


59 pav. *Siūlomos autentifikavimo schemos panaudojimo scenarijus*

Jei automobilis sėkmingai autentifikuojamas, *AS1* apskaičiuoja pasitikėjimo reikšmę ir *ID* bei šiuos duomenis perduoda kitiems pasitikėjimo grupėje esantiems mazgams. Automobiliui toliau

judant ir signalo stiprumui nukritus žemiau užduotos vertės, yra skenuojamas tinklas ir surandamas kitas stipriausią signalą turintis ir pasitikėjimo grupėje esantis *RSU*. Jei *AS* identifikuoja automobilį kaip iš jo pasitikėjimo grupės, jis autentifikuojamas be pilnos procedūros.

60 pav. a) pateiktas automobilio autentifikavimo toje pačioje pasitikėjimo grupėje ir kitoje pasitikėjimo grupėje algoritmas ir b) sekos diagrama



60 pav. *Automobilio autentifikavimo toje pačioje pasitikėjimo grupėje ir kitoje pasitikėjimo grupėje: a) algoritmas; b) sekos diagrama*

12.3.Pasitikėjimo vertės skaičiavimas

Pasiūlytoje autentifikavimo schemoje pasitikėjimo reikšmė turi esminę reikšmę, „*handoff*“ laiko sumažinime. Automobiliai prisijungdami prie tos pačios grupės *RSU* ar kitų automobilių neturi kartoti visos autentifikavimo procedūros, taip ženkliai sumažinant prisijungimo laiką. Pasitikėjimo reikšmė yra maišos funkcija, kuri V2I atveju apskaičiuojama pagal 1 lygtį.

$$T_{ID_{vehicle}} = \left(t_1\left(hash\left(R_{vehicle}\right)\right) \cap t_1\left(hash\left(R_{trustRSU}\right)\right)\right) \cap t_3 \left(hash\left(PTK\left(ID_{trust}, ID_{vehicle}, GSK_{vehicle}, R_{vehicle}, R_{trustRSU}\right)\right)\right) \quad (1)$$

Kai automobilis nori prisijungti prie *RSU* savo pasitikėjimo grupėje, jis sugeneruoja atsitiktinį skaičių $R_{vehicle}$ ir išsiunčia autentifikavimo prašymą *RSU*. *RSU* pirmiausia patikrina pasitikėjimo lentelę, siekiant išsiaiškinti ar automobilis priklauso tai pačiai pasitikėjimo grupei. RSU atsako išsiųsdamas autentifikavimo atsakymo paketą (*ASP*) su sugeneruotu atsitiktiniu skaičiumi $R_{trustRSU}$. Automobiliui gavus autentifikavimo prašymo paketą, tiek automobilis, tiek RSU

žino atsitiktinius sugeneruotus skaičius. Tuomet, abu mazgai gali sugeneruoti *PTK*, naudodami *GSK*, automobilio *ID*, *RSU ID* ir du sugeneruotus skaičius.

Automobilio pasitikėjimo autentifikavimas *V2V* komunikacijai gali būti užrašytas kaip 2 lygtis.

$$T_{ID_{vehicle}} = t_1\left(RTV\left(mean\left(R_e, O_{sc}, ID_{vehicle}\right)\right)\right) \cap t_2\left(hash\left(PTK\left(ID_{trust}, ID_{vehicle}, GSK_{vehicle}\right)\right)\right). \quad (2)$$

Kur R_e yra resursai panaudoti $ID_{vehicle}$ mazgo ir O_{sc} yra sėkmingai įvykdytos operacijos (remiantis istorija). Pasiūlyta autentifikavimo schema gali ženkliai sumažinti „*handoff*“ procedūros laiką ir būti efektyvesnė lyginant su kitomis *VANET* autentifikavimo sistemomis.

IŠVADOS

Atlikus išsamią tiriamos srities literatūros analizę ir nustačius šiuo metu aktualiausios problemines sritiss: eismo saugumo, informacinių bei multimedija paslaugų teikimas bei integravimas įvairiomis eismo sąlygomis, skirtingų bevielio ryšio technologijų panaudojimas bei integravimas automobilinės komunikacijos tinkluose, privatumas ir saugumas automobilinės komunikacijos tinkluose. Atsižvelgus į šių temų aktualumą, buvo atlikti sekantys moksliniai tyrimai:

1.Atlikus programinės įrangos, leidžiančios atlikti automobilinių tinklų imitacinį modeliavimą, kokybinę lyginamąją analizę buvo parinktas tinkamiausias probleminės srities tyrimams modeliavimo programinis paketas – *NCTUns 6.0*, leidžiantis tiksliai modeliuoti realistišką automobilių judėjimą bei panaudoti realius Linux operacinės sistemos *TCP/UDP/IP* protokolus, užtikrinant gautų rezultatų patikimumą bei realistiškumą.

2.Atliktas *AODV* ir *ADV ad-hoc* maršrutizavimo protokolų efektyvumo tyrimas teikiant eismo saugumo, informacines ir multimedija paslaugas, kurio metu nustatyta, kad geriausi rezultatai pasiekiami naudojant *AODV* maršrutizavimo protokolą, kadangi šiuo atveju buvo pasiekta didžiausia duomenų išsiuntimo ir priėmimo sparta (vidutiniškai 20 KB/s), mažiausias procentas prarastų paketų (32%, *ADV* – 42%, *GOD* – 42%). Šis maršrutizavimo protokolas yra tinkamas aukštos perdavimo spartos nereikalaujančioms multimedija ir informacinėms bei eismo saugumo paslaugoms teikti miesto sąlygomis. Naudojant *ADV* protokolą, gaunami prasti duomenų perdavimo spartos rezultatai ir praktiškai visas ryšio kanalas sunaudojamas maršrutizavimo žinutėms perduoti. Šis protokolas netinkamas multimedija paslaugų teikimui miesto sąlygomis, iš dalies juo naudojantis galima teikti nekritines eismo saugumo paslaugas.

3.Atliktas eismo saugumo, informacinių ir multimedija paslaugų teikimo efektyvumo tyrimas, siuntėjui ir gavėjui judant priešingomis kryptimis automagistralėje, kurio metu buvo nustatyta, kad ilgiausiai komunikacija gali būti išlaikoma esant didžiausiam automobilių skaičiui tinkle, tačiau šio ryšio kokybė yra atvirkščiai proporcinga automobilių skaičiui, kadangi didėjant automobilių skaičiui – didėja tinklo užliejimas duomenimis bei įvyksta daug kolizijų.

4.Atliktas *802.11b*, *802.11p* ir *802.11e* bevielio ryšio technologijų panaudojimo eismo saugumo, informacinių bei multimedija paslaugų teikimui automobilių komunikacijos tinkluose efektyvumo tyrimas miesto bei greitkelio sąlygomis, kurio metu buvo nustatyta, kad visos trys technologijos yra tinkamos informacinių, multimedija bei eismo saugumo paslaugų teikimui. Geriausi duomenų perdavimo spartos rezultatai buvo pasiekti naudojant *802.16e* bevielio technologiją, tačiau šiuo atveju miesto sąlygomis buvo pastebimas ryšio dingimas, kurį galimą išspręsti optimizuojant retransliacijos stočių išdėstymą mieste. *802.11p* bevielio ryšio technologijos

naudojimo tiek miesto, tiek automagistralės sąlygomis parodė geriausią duomenų perdavimo bei paketų praradimo (36% ir 0,65%) santykį. Šiuo atžvilgiu pastarajai technologijai gana ženkliai nusileidžia *802.11b* standartas, kurį naudojant buvo itin aukštas paketų praradimo skaičius (53% ir 59%). Rezultatai rodo, kad informacinių, multimedija bei eismo saugumo paslaugų teikimui automobilinėje komunikacijoje miesto bei automagistralės sąlygomis efektyviausia naudoti specialiai tam sukurtą, *802.11p* technologiją, kuri užtikrina tiek aukštą duomenų perdavimo spartą, tiek žemą paketų praradimo lygį. Šios technologijos įdiegimui, taip pat, reikia įrengti mažiau infrastruktūros įrenginių, kadangi jos veikimo nuotolis yra didesnis.

Įvykdžius visus užsibrėžtus uždavinius buvo pasiektas darbo tikslas – ištirtos eismo saugumo, informacinių ir multimedija paslaugų teikimo galimybės bei perspektyvos automobilių komunikacijos tinkluose. Sukurta nauja pasitikėjimu grindžiama autentifikavimo schema, skirta informacinių bei multimedija paslaugų teikimo apsaugojimui automobilinės komunikacijos tinkluose, teoriškai galinti sumažinti persijungimo tarp bevielių stočių laiką. Taip pat, atsižvelgiant į gautus rezultatus, galima teigti, kad norint teikti kokybiškas multimedija bei eismo saugumo paslaugas yra reikalingi nauji, automobilinei komunikacijai skirti ad-hoc maršrutizavimo protokolai.

Šie rezultatai sudaro prielaidas tolimesniems aukštesnio lygio tęstiniams tyrimams, todėl autorius sieks šiuos tyrimus tęsti doktorantūroje.

LITERATŪRA

1. Olariu S., Weigle M. C. 2009. Vehicular Networks: From Theory to Practice. USA: Chapman & Hall/CRC, Taylor & Francis Group, p. 472.
2. Roy R. R. 2011. Handbook of Mobile Ad Hoc Networks for Mobility Models. London: Springer, p. 1090.
3. Amri H. A., Abolhasan M., Wysocki T. 2010. Scalability of MANET routing protocols for heterogeneous and homogenous networks. Computers & Electrical Engineering, vol. 36, No. 4, p. 752-765.
4. Akyildiz I. F., Wang X. 2005. A Survey on Wireless Mesh Networks. IEEE Radio Communications, vol. 43, No. 9, p. 23-30.
5. Akyildiz I. F., Wang X., Wang W. 2005. Wireless mesh networks: a survey. Computer Networks, vol. 34, No. 1, p. 445-487.
6. Capone A., et al. 2010. Routing, scheduling and channel assignment in Wireless Mesh Networks: Optimization models and algorithms. Ad Hoc Networks, vol. 8, No. 6, p. 545-563.
7. Anastasi G., et al. 2009. Energy conservation in wireless sensor networks: A survey. Ad Hoc Networks, vol. 7, No. 3, p. 537-568.
8. Baronti P., et al. 2007. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. Computer Communications, vol. 30, No. 7, p. 1655-1695.
9. Lee U., Gerla M. 2010. A survey of urban vehicular sensing platforms. Computer Networks, vol. 54, No. 4, p. 527-544.
10. Zeletin R., Radusch I., Rigani M. A. 2010. Vehicular-2-X Communication: State-of-the-Art and Research in Mobile Vehicular Ad hoc Networks. Berlin: Springer, p. 156.
11. Moustafa H., Zhang Y. 2009. Vehicular Networks: Techniques, Standards, and Applications. USA: Auerbach Publications, Taylor & Francis Group, p. 450.
12. Cheng H. T., Shan H., Zhuang W. 2011. Infotainment and road safety service support in vehicular networking: From a communication perspective. Mechanical Systems and Signal Processing, vol. 25, No. 6, p. 2020-2038.
13. Hartenstein H., Laberteaux K. 2010. VANET Vehicular Applications and Inter-Networking Technologies. UK: John Wiley & Sons Ltd, p. 466.
14. CAR 2 CAR Communication Consortium. Mission & Objectives [interaktyvus]. [žiūrėta 2011-03-21]. Prieiga per Internetą: <http://www.car-to-car.org/>.
15. Grilli G. Data dissemination in vehicular networks. 2010. PhD dissertation. University of Rome, p. 198.
16. Sahu P. P., Singh M. 2009. Multichannel direct sequence spectrum signaling using code phase shift keying. Computers & Electrical Engineering, vol. 35, No. 1, p. 218-226.
17. Kattoush A. H., et al. 2010. The performance of multiwavelets based OFDM system under different channel conditions. Digital Signal Processing, vol. 20, No. 2, p. 472-482.
18. IEEE. IEEE 802 Working Group. [interaktyvus]. [žiūrėta 2011-03-23]. Prieiga per Internetą: <http://www.ieee802.org/dots.shtml>.
19. Holt A., Huang C. Y. 2010. 802.11 Wireless Networks: Security and Analysis. London: Springer, p. 212.
20. Schaar M., Chou P. A. 2007. Multimedia over IP and Wireless Networks: Compression, Networking, and Systems. USA: Elsevier, p. 712.
21. IEEE. 802.11n-2009 - IEEE Standard for Local and Metropolitan Area Networks - Telecommunications and Information Ixchange between Systems -- Local and Metropolitan Area Networks -- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput, 2009, p. 502.
22. IEEE. 802.11p-2010 - IEEE Standard for Local and Metropolitan Area Networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. 2010, p. 51.

23. IEEE. 1609.3-2010 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services. 2010, p. 144.
24. Amadeo M., Campolo C., Molinaro A. 2010. Enhancing IEEE 802.11p/WAVE to provide infotainment applications in VANETs. Ad Hoc Networks, In Press.
25. Weil T. 2009. Service Management for ITS Using WAVE (1609.3) Networking. IEEE GLOBECOM Workshops 2009, p. 1-6.
26. Carames T. M., Gonzalez-Lopez M., Castedo L. 2011. Mobile WiMAX for vehicular applications: Performance evaluation and comparison against IEEE 802.11p/a. Computer Networks, In Press.
27. Bacioccola E., et al. 2010. IEEE 802.16: History, status and future trends. Computer Communications, vol. 33, No. 2, p. 113-123.
28. Ge Y., Wen S., Ang Y. H. 2009. Analysis of Optimal Relay Selection in IEEE 802.16 Multihop Relay Networks. IEEE Transactions on Vehicular Technology, vol. 59, No. 5, p. 2198 – 2206.
29. Jang J., Kimb S. W., Lee J. H. 2010. Performance evaluation of a new QoS packet-scheduler for VoIP service in IEEE 802.16-based WMAN systems. Computer Communications, vol. 33, No. 5, p. 589-594.
30. Hossain E., et al. 2010. Vehicular telematics over heterogeneous wireless networks: A survey. Computer Communications, vol. 33, No. 7, p. 775-793.
31. Reid N. 2010. Wireless Mobility: The Why of Wireless. USA: McGraw-Hill Osborne Media, p. 320.
32. Masini B. M., Fontana C., Verdone R. 2004. Provision of an emergency warning service through GPRS: performance evaluation. IEEE Conference on Intelligent Transportation Systems, p. 1098–1102.
33. Santaa J., Skarmetaa A. F., Artigas M. S. 2008. Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks. Computer Communications, vol. 31, No. 12, p. 2850-2861.
34. Deruyck M., et al. 2011. Modelling and optimization of power consumption in wireless access networks. Computer Communications, In Press.
35. Willke T. L., Tientrakool P., Maxemchuk N. F. 2009. A survey of inter-vehicle communication protocols and their applications. IEEE Communications Surveys & Tutorials, vol. 11, No. 2, p. 3-20.
36. Fleetnet - Internet on the road. [interaktyvus]. [žiūrėta 2011-03-21]. Prieiga per Internetą: <http://www.netlab.nec.de/Projects/fleetnet.htm>.
37. Lu R., et al. 2009. SPARK: A New VANET-Based Smart Parking Scheme for Large Parking Lots. IEEE INFOCOM 2009, p. 1413–1421.
38. Nandan A., et al. 2005. AdTorrent digital billboards for vehicular networks. Proceedings of the IEEE/ACM V2VCOM, p. 1-20.
39. Gerla M., Kleinrock L. 2011. Vehicular networks and the future of the mobile internet. Computer Networks, vol. 55, No. 2, p. 457-469.
40. Soldo F., et al. 2008. Streaming Media Distribution in VANETs. IEEE Global Telecommunications Conference, IEEE GLOBECOM 2008, p. 1-6.
41. Sirichai P., et al. 2011. Smart Car with Security Camera for Road Accidence Monitoring. Procedia Engineering, vol. 8, p. 308-312.
42. Dornbush S., Joshi A. 2007. StreetSmart Traffic: Discovering and Disseminating Automobile Congestion Using VANET's. IEEE Vehicular Technology Conference, p. 11–15.
43. Sommer C., et al. 2010. On the feasibility of UMTS-based Traffic Information Systems. Ad Hoc Networks, vol. 8, No. 5, p. 506-517.
44. Jovanovic M. R., et al. 2008. On the peaking phenomenon in the control of vehicular platoons. Systems & Control Letters, vol. 57, No. 7, p. 528-537.
45. Gibaud A., Thomin P., Sallez Y. 2011. Foresee, a fully distributed self-organized approach for improving traffic flows. Simulation Modelling Practice and Theory, vol. 19, No. 4, p. 1096-1117.
46. Dresner K., Stone P. 2008. A Multiagent Approach to Autonomous Intersection Management. Journal of Articial Intelligence Research, vol. 31, No. 1, p. 591-656.

47. Ramos F. M. V., et al. 2011. Reducing channel change delay in IPTV by predictive pre-joining of TV channels. Signal Processing: Image Communication, In Press.
48. Lee U., et al. 2006. CodeTorrent: Content Distribution using Network Coding in VANET. MobiShare'06, p. 1-6.
49. Plėštys R., Zakarevičius R. 2010. Request and Response Zone Control for Routing in MANET. IEEE Electronics Conference (BEC), p. 219-222.
50. Karapantazis S., Pavlidou F. N. 2009. VoIP: A comprehensive survey on a promising technology. Computer Networks, vol. 53, No. 12, p. 2050-2090.
51. Ho Y. H., Ho A. H., Hua K. A. 2008. Routing protocols for inter-vehicular networks: A comparative study in high-mobility and large obstacles environments. Computer Communications, vol. 31, No. 3, p. 2767-2780.
52. Bernsen J., Manivannan D. 2009. Unicast routing protocols for vehicular ad hoc networks: A critical comparison and classification. Pervasive and Mobile Computing, vol. 5, No. 1, p. 1-18.
53. Benslimane A., Barghi S., Assi C. 2011. An efficient routing protocol for connecting vehicular networks to the Internet. Pervasive and Mobile Computing, vol. 7, No. 1, p. 98-113.
54. Rezende C., et al. 2010. The impact of mobility on Mobile Ad Hoc Networks through the perspective of complex networks. Journal of Parallel and Distributed Computing, In Press.
55. Abdou W., et al. 2011. Using an evolutionary algorithm to optimize the broadcasting methods in mobile ad hoc networks. Journal of Network and Computer Applications, In Press.
56. Correia F., Vazao T. 2010. Simple ant routing algorithm strategies for a (Multipurpose) MANET model. Ad Hoc Networks, vol. 8, No. 8, p. 810-823.
57. Bi Y., et al. 2009. A Multi-Channel Token Ring Protocol for QoS Provisioning in Inter-Vehicle Communications. IEEE Transactions on Wireless Communications, vol. 8, No. 11, p. 5621-5631.
58. Shafiee K., Leung V. 2011. Connectivity-aware minimum-delay geographic routing with vehicle tracking in VANETs. Ad Hoc Networks, vol. 9, No. 2, p. 131-141.
59. Jarupan B., Ekici E. 2011. A survey of cross-layer design for VANETs. Ad Hoc Networks, vol. 9, No. 5, p. 966-983.
60. Li M., Zeng K., Lou W. 2011. Opportunistic broadcast of event-driven warning messages in Vehicular Ad Hoc Networks with lossy links. Computer Networks, In Press.
61. Wang S. C., Tsao Y. L., Chen H. H. 2010. Doppler-resistant column-wise complementary coded CDMA technology for V2V communications. Ad Hoc Networks, In Press.
62. Leontiadis I., Costa P., Mascolo C. 2009. A hybrid approach for content-based publish/subscribe in vehicular networks. Pervasive and Mobile Computing, vol. 5, No. 6, p. 697-713.
63. Alasmary W., Zhuang W. 2010. Mobility impact in IEEE 802.11p infrastructureless vehicular networks. Ad Hoc Networks, In Press.
64. Jiang H., et al. 2006. Quality-of-service provisioning and efficient resource utilization in CDMA cellular communications. IEEE Journal on Selected Areas in Communications, vol. 24, No. 1, p. 4-15.
65. IEEE Standard. 802.11e-2005 - IEEE Standard for Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment: Medium Access Method (MAC) Quality of Service Enhancements. 2005, p. 212.
66. Chrichigno J., Wu M. Y., Shu W. 2008. Protocols and architectures for channel assignment in wireless mesh networks. Ad Hoc Networks, vol. 6, No. 7, p. 1051-1077.
67. Wu T. Y. 2010. Improving RSU service time by Distributed Sorting Mechanism. Ad Hoc Networks, In Press.
68. Cheng H. C., Zhuang W. 2008. Joint Power-Frequency-Time Resource Allocation in Clustered Wireless Mesh Networks. IEEE Network, vol. 22, No. 1, p. 45-51.
69. Cheng H. T., et al. Pareto optimal resource management for wireless mesh networks with QoS assurance: Joint node clustering and subcarrier allocation. IEEE Transactions on Wireless Communications, vol. 8, No. 3, p. 1573-1583.

70. Alcaraz J. J., Vales-Alonso J., García-Haro J. 2009. Control-based scheduling with QoS support for vehicle to infrastructure communications. IEEE Wireless Communications, vol. 16, No. 6, p. 32-39.
71. Alsabaan M., Zhuang W., Wang P. 2011. Link layer solutions for supporting real-time traffic over CDMA wireless mesh networks. Wireless Communications and Mobile Computing, vol. 11, No. 5, p. 644–653.
72. Karamad E., Ashtiani F. 2008. A modified 802.11-based MAC scheme to assure fair access for vehicle-to-roadside communications. Computer Communications, vol. 31, No. 12, p. 2898-2906.
73. Abdelkader T., et al. 2009. Adaptive Backoff Scheme for Contention-based Vehicular Networks Using Fuzzy Logic.Proceedings of IEEE International Conference on fuzzy Systems, Korea, p. 1621-1626.
74. Kumar S., Raghavan V. S., Deng J. 2006. Medium Access Control protocols for ad hoc wireless networks: A survey. Ad Hoc Networks, vol. 4, No. 3, p. 326-358.
75. Artimy M. 2007. Local Density Estimation and Dynamic Transmission-Range Assignment in Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems, vol. 8, No. 3, p. 400-412.
76. Korkmaz G., Ekici E., Ozguner F. 2010. Supporting real-time traffic in multihop vehicle-to-infrastructure networks. Transportation Research Part C: Emerging Technologies, vol. 18, No. 3, p. 376-392.
77. Yang K., et al. 2007. A Multihop Peer-Communication Protocol With Fairness Guarantee for IEEE 802.16-Based Vehicular Networks. IEEE Transactions on Vehicular Technology, vol. 56, No. 6, p. 3358-3370.
78. Zhang J., Liu K., Shen X. 2008. A Novel Overlay Token Ring Protocol for Inter-Vehicle Communication. In IEEE Proceedings of ICC'2008, p. 4904-4909.
79. Yomo, H., et al. 2009. Development of a CDMA intervehicle communications system for driving safety support. IEEE Wireless Communications, vol. 16, No. 6, p. 24-31.
80. Schmidt R., et al. 2010. Exploration of adaptive beaconing for efficient intervehicle safety communication. IEEE Network, vol. 24, No. 1, p. 14-19.
81. Adams F. Y., et al. 2008. V2V Wireless Communication Protocol for Rear-End Collision Avoidance on Highways. IEEE International Conference on Communications Workshops,. ICC Workshops '08, p. 375-379.
82. Santa J., et al. 2010. An analysis of communication and navigation issues in collision avoidance support systems. Transportation Research Part C: Emerging Technologies, vol. 18, No. 3, p. 351-366.
83. Tang A., Yip A. 2010. Collision avoidance timing analysis of DSRC-based vehicles. Accident Analysis & Prevention, vol. 42, No. 1, p. 182-195.
84. Biswas S., Tatchikou R., Dion F. 2006. Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. IEEE Communications Magazine, vol. 44, No. 1, p. 74-82.
85. Daeinabi A., Rahbar A. G. P., Khademzadeh A. 2011. VWCA: An efficient clustering algorithm in vehicular ad hoc networks. Journal of Network and Computer Applications, vol. 34, No. 1, p. 207-222.
86. Konstantopoulos C., Gavalas D., Pantziou G. 2008. Clustering in mobile ad hoc networks through neighborhood stability-based mobility prediction. Computer Networks, vol. 52, No. 9, p. 1797-1824.
87. Taheri J., Zomaya A. Y. 2007. Clustering techniques for dynamic location management in mobile computing. Journal of Parallel and Distributed Computing, vol. 67, No. 4, p. 430-447.
88. Liu C. M., Lee C. H., Wang L. C. 2007. Distributed clustering algorithms for data-gathering in wireless mobile sensor networks. Journal of Parallel and Distributed Computing, vol. 67, No. 11, p. 1187-1200.
89. Dimokas N., Katsaros D., Manolopoulos Y. 2010. Energy-efficient distributed clustering in wireless sensor networks. Journal of Parallel and Distributed Computing, vol. 70, No. 4, p. 371-383.

90. Abbasi A. A., Younis M. 2007. A survey on clustering algorithms for wireless sensor networks. Computer Communications, vol. 30, No. 15, p. 2826-2841.
91. Zhang Y., et al. 2009. A distributed group mobility adaptive clustering algorithm for mobile ad hoc networks. Computer Communications, vol. 32, No. 1, p. 189-202.
92. Schwartz R. S., et al. 2011. A directional data dissemination protocol for vehicular environments. Computer Communications, In Press.
93. Rawashdeh Z. Y., Mahmud S. M. 2008. Media Access Technique for Cluster-Based Vehicular Ad Hoc Networks. IEEE 68th Vehicular Technology Conference, VTC 2008-Fall, p. 1-5.
94. Abboud K. et al. 2009. Modeling and Analysis for Emergency Messaging Delay in Vehicular Ad Hoc Networks. IEEE Global Telecommunications Conference GLOBECOM 2009, p. 1-6.
95. Lee J., et al. 2009. Design of Intersection Switches for the Vehicular Network. 12th Asia-Pacific Network Operations and Management Symposium, APNOMS 2009, vol. 5787, p. 523-526.
96. Lochert C., Scheuermann B., Wewetzer C. 2008. Data aggregation and roadside unit placement for a vanet traffic information system. VANET '08 Proceedings of the fifth ACM international workshop on Vehicular Inter-NETworking, p. 58-65.
97. Sun Y., et al. 2010. Roadside Units Deployment for Efficient Short-Time Certificate Updating in VANETs. IEEE International Conference on Communications (ICC), p. 1-5.
98. Trullols O., et al. Planning roadside infrastructure for information dissemination in intelligent transportation systems. Computer Communications, vol. 33, No. 4, p. 432-442.
99. Hu Y., et al. 2009. The Sink Node Placement and Performance Implication in Mobile Sensor Networks. ACM/Springer Journal on Mobile Networks and Applications (MONET), Special Issue on New Advances in Heterogeneous Networking for Quality, Reliability, Security and Robustness, vol. 14, No. 2, p. 230-240.
100. Li P., et al. 2007. Optimal Placement of Gateways in Vehicular Networks. IEEE Transactions on Vehicular Technology, vol. 56, No. 6, p. 3421–3430.
101. Bulbenkienė V., Pareigis V., Andziulis A., Kurmis M., Jakovlev S. 2011. Simulation of IEEE 802.16j mobile WiMAX relay network to determine the most efficient modulation zone to deploy relay station. Electronics and Electrical Engineering, In Press.
102. Cheng H. T., Zhuang W. 2009. QoS-driven MAC-layer resource allocation for wireless mesh networks with non-altruistic node cooperation and service differentiation. IEEE Transactions on Wireless Communications, vol. 8, No. 12, p. 6089-6103.
103. Wu H. C. 2009. The Karush–Kuhn–Tucker optimality conditions in multiobjective programming problems with interval-valued objective functions. European Journal of Operational Research, vol. 196, No. 1, p. 49-60.
104. Molisch A., et al. 2009. A survey on vehicle-to-vehicle propagation channels. IEEE Wireless Communications, vol. 16, No. 6, p. 12-22.
105. Ilhan H., Uysal M., Altunbas I. 2009. Cooperative Diversity for Intervehicular Communication: Performance Analysis and Optimization. IEEE Transactions on Vehicular Technology, vol. 58, No. 7, p. 3301-3310.
106. Yilmaz A., Kucur O. 2011. Performance of rotated PSK modulation in Nakagami-m fading channels. Digital Signal Processing, vol. 21, No. 2, p. 296-306.
107. Zhou L., et al. 2008. Cross-layer rate control, medium access control and routing design in cooperative VANET. Computer Communications, vol. 31, No. 12, p. 2870-2882.
108. Abdalla G. M. T., Abu-Rgheff M. A., Senouci S. M. 2009. An Adaptive Channel Model for VBLAST in Vehicular Networks. EURASIP Journal on Wireless Communications and Networking, vol. 2009, No. 1, p. 1-8.
109. Xie Xu., et al. 2008. Adaptive Multi-channel MAC Protocol for Dense VANET Using Directional Antennas. Second International Conference on Future Generation Communication and Networking, 2008. FGCN '08, p. 398–401.
110. Nandan A., et al. 2005. Co-operative Downloading in Vehicular Ad-hoc Wireless Networks. IEEE Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services, p. 32-41.

111. Lee K. C., et al. 2007. First Experience with CarTorrent in a Real Vehicular Ad Hoc Network Testbed. 2007 Mobile Networking for Vehicular Environments, p. 109–114.
112. Cesana M., Cuomo F., Ekici E. 2011. Routing in cognitive radio networks: Challenges and solutions. Ad Hoc Networks, vol. 9, No. 3, p. 228-248.
113. Datla D., et al. 2011. Wireless distributed computing in cognitive radio networks. Ad Hoc Networks, In Press.
114. Bicen A. O., Gungor V. C., Akan O. B. 2011. Delay-sensitive and multimedia communication in cognitive radio sensor networks. Ad Hoc Networks, In Press.
115. Cacciapuoti A. S., Caleffi M., Paura L. 2011. Reactive routing for mobile cognitive radio ad hoc networks. Ad Hoc Networks, In Press.
116. Akyildiz Y. F., Lee W. Y., Chowdhury R. 2009. CRAHNs: Cognitive radio ad hoc networks. Ad Hoc Networks, vol. 7, No. 5, p. 810-836.
117. Lequerica I., Ruiz P. M., Cabrera V. 2010. Improvement of vehicular communications by using 3G capabilities to disseminate control information. IEEE Network, vol. 24, No. 1, p. 32 – 38.
118. Lin X., et al. 2008. Security in Vehicular Ad Hoc Networks. IEEE Communications Magazine, vol. 46, No. 4, p. 88-95.
119. Plößl K., Federrath H. 2008. A privacy aware and efficient security infrastructure for vehicular ad hoc networks. Computer Standards & Interfaces, vol. 30, No. 6, p. 390-397.
120. Marmol F. G., Perez G. M. 2011. TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of Network and Computer Applications, In Press.
121. Marmol F. G., Marin-Blazquez J. G., Perez G. M. 2010. Linguistic Fuzzy Logic Enhancement of a Trust Mechanism for Distributed Networks. 10th IEEE International Conference on Computer and Information Technology (CIT 2010), p. 838-845.
122. Yeh L. Y., Chen Y. C., Huang J. L. 2011. PAACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks. Computer Communications, vol. 34, No. 3, p. 447-456.
123. Zhang Z., Boukerche A., Ramadan Z. 2011. Design of a lightweight authentication scheme for IEEE 802.11p vehicular networks. Ad Hoc Networks, In Press.
124. Chim T. W., et al. 2011. SPECS: Secure and privacy enhancing communications schemes for VANETs. Ad Hoc Networks, vol. 9, No. 2, p. 189-203.
125. Ma Z., Kargl F., Weber M. 2010. Measuring long-term location privacy in vehicular communication systems. Computer Communications, vol. 33, No. 12, p. 1414-1427.
126. Lu R., et al. 2010. An efficient and provably secure public key encryption scheme based on coding theory. Security Comm. Networks, p. 1939-1947.
127. Sun Y., et al. 2010. An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications. IEEE Transactions on Vehicular Technology, vol. 59, No. 7, p. 3589–3603.
128. Jiang Y., et al. 2009. BAT: A robust signature scheme for vehicular networks using Binary Authentication Tree . IEEE Transactions on Wireless Communications, vol. 8, No. 4, p. 1974–1983.
129. Wasef A., et al. 2010. Complementing public key infrastructure to secure vehicular ad hoc networks. IEEE Transactions on Wireless Communications, vol. 17, No. 5, p. 22–28.
130. Mahmoud M., Shen, X. 2010. ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multihop Wireless Networks. IEEE Transactions on Mobile Computing, In Press.
131. Zhu H., et al. 2009. Security in service-oriented vehicular networks. IEEE Wireless Communications, vol. 16, No. 4, p. 16-22.
132. Li X., et al. 2011. Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks. IEEE ICC 2011, In Press.
133. Andziulis A.; Kurmis M., Vaupsas J., Jakovlev S., Pareigis V. 2011. Trust Based Authentication Scheme for Latency Reduction in Vehicular Ad-Hoc Networks (VANETs). The 7th International

Conference on New Electrical & Electronic Technologies & Their Industrial Implementation (NEET 2011), Accepted Manuscript.
134. Jarupan B., Ekici E. 2011. A survey of cross-layer design for VANETs. Ad Hoc Networks, vol. 9, No. 5, p. 966-983.
135. CarTalk. The European Project CarTALK 2000. [interaktyvus]. [žiūrėta 2011-03-26]. Prieiga per Internetą: <http://www.cartalk2000.net/>.
136. Schulze M., et al. 2008. PReVENT Final Report. PReVENT Consortium 2008, p. 198.
137. Festag A., et al. 2008. 'NoW – Network on Wheels': Project Objectives, Technology and Achievements. Proceedings of 5rd International Workshop on Intelligent Transportation (WIT), p. 211-216.
138. SAFESPOT Integrated Project. [interaktyvus]. [žiūrėta 2011-03-26]. Prieiga per Internetą: <http://www.safespot-eu.org/>.
139. The COMeSafety Project. [interaktyvus]. [žiūrėta 2011-03-26]. Prieiga per Internetą: <http://www.comesafety.org/>.
140. The European project PRE-DRIVE C2X. [interaktyvus]. [žiūrėta 2011-03-26]. Prieiga per Internetą: <http://www.pre-drive-c2x.eu/>.
141. Martinez F. J. 2011. A survey and comparative study of simulators for vehicular ad hoc networks (VANETs). Wireless Communications and Mobile Computing, In Press.
142. López-Neria E., Ramírez-Treviño A., López-Mellado E. 2010. A modeling framework for urban traffic systems microscopic simulation. Simulation Modelling Practice and Theory, vol. 18, No. 8, p. 1145-1161.
143. Font J. L., et al.. 2011. Analysis of source code metrics from ns-2 and ns-3 network simulators. Simulation Modelling Practice and Theory, Vol 19, No 5, p. 1330-1346.
144. Scalable Networks. Qualnet Developer. [interaktyvus]. [žiūrėta 2011-02-18]. Prieiga per Internetą: <http://www.scalable-networks.com/products/qualnet/>.
145. Opnet. The OPNET Modeler® Wireless Suite. [interaktyvus]. [žiūrėta 2011-02-18]. Prieiga per Internetą: <http://www.opnet.com/solutions/network_rd/modeler_wireless.html>.
146. J-Sim. General Information about J-Sim. [interaktyvus]. [žiūrėta 2011-02-18]. Prieiga per Internetą: <http://www.j-sim.zcu.cz/>.
147. Omnet++. OMNeT++ Network Simulation Framework. [interaktyvus]. [žiūrėta 2011-02-18]. Prieiga per Internetą: <http://www.omnetpp.org/>.
148. SWANS++ - Extensions to the Scalable Wireless Ad-hoc Network Simulator. [interaktyvus]. [žiūrėta 2011-02-18]. Prieiga per Internetą: <http://www.aqualab.cs.northwestern.edu/projects/swans++/>.
149. GrooveNet: Vehicular Network Virtualization Platform. [interaktyvus]. [žiūrėta 2011-02-18]. Prieiga per Internetą: <http://www.seas.upenn.edu/~rahulm/Research/GrooveNet/>.
150. TraNS. Traffic and Network Simulation Environment. [interaktyvus]. [žiūrėta 2011-02-18]. Prieiga per Internetą: <http://lca.epfl.ch/projects/trans>.
151. Veins - Vehicles in Network Simulation. [interaktyvus]. [žiūrėta 2011-02-18]. Prieiga per Internetą: <http://veins.car2x.org/>.
152. Wang S. Y., Chou C. L.. 2009. NCTUns tool for wireless vehicular communication network researches. Simulation Modelling Practice and Theory, Vol. 17, No. 7, p. 1211-1226.
153. Vindašius A. 2010. Tinklų modeliavimas ir emuliavimas NCTUns aplinkoje. Electronics and electrical engineering, vol. 2, No. 1, p. 73-76.
154. Simreal Technology. NCTUns. [interaktyvus]. [žiūrėta 2011-02-18]. Prieiga per Internetą: <http://nsl10.csie.nctu.edu.tw/>.
155. Wang S. Y., Lin C. C. 2008. NCTUns 5.0: A Network Simulator for IEEE 802.11(p) and 1609 Wireless Vehicular Network Researches. 2nd IEEE International Symposium on Wireless Vehicular Communications, Canada, p. 1-2.
156. Wang S. Y., et al. 2011. Design and Implementation of A More Realistic Radio Propagation Model for Wireless Vehicular Networks over the NCTUns Network Simulator. IEEE WCNC 2011 (Wireless Communications and Networking Conference 2011), p. 1937-1942.

157. Wang S. Y., et al. 2007. NCTUns 4.0: An Integrated Simulation Platform for Vehicular Traffic, Communication, and Network Researches. 1st IEEE International Symposium on Wireless Vehicular Communications, p. 2081-2085.
158. Andziulis A., Pareigis V., Bulbenkiene V., Adomaitis D., Kurmis M., Jakovlev S. 2010. WiMAX Technology Application Research in the Klaipeda Region. 16th Internation Conference on Information & Software Technologies (IT2010). Research Communications. p. 48-52.
159. Kurmis M., Adomaitis D., Pareigis V., Jakovlev S., Andziulis A. 2010. Bevielių vietinių tinklų saugumo tyrimas. VII Mokslinė Konferencija „Technologijos Mokslo Darbai Vakarų Lietuvoje“, p. 186-189.

SUMMARY

Vehicular communication networks are acquiring more and more commercial relevance because of recent advances in inter-vehicular communications via the DSRC/WAVE standard, which stimulates a brand new family of visionary services for vehicles, from road safety to entertainment and multimedia applications. After deep analysis of the literature it was chosen to investigate road safety, information and multimedia service support opportunities and prospects in vehicular communication networks.

After careful analysis of the simulation tools, it was chosen NCTUns 6.0 software package for planned investigations. The results of the first investigation: AODV and ADV ad-hoc routing protocols performance evaluation showed that the best results are achieved when using AODV protocol because it is the highest throughput and lowest packet loss rate. It was found that for quality multimedia and road security services support the new protocols are needed.

The results of investigation: road safety, information and multimedia service support in highway fast moving vehicles in opposite direction showed that the longest communication can be maintained with the largest number of cars, but the quality of the communication is inversely to vehicles number.

The results of investigation: 802.11b, 802.11p and 802.11e technologies employment for road safety, information and multimedia service support in city and highway conditions showed that all three technologies are suitable for the investigated service support. The best throughput results were achieved when using the 802.11e technology. 802.11p showed the best results in throughput and packet loss ratio.

Kurmis M. Eismo saugumo, informacinių ir multimedija paslaugų teikimas automobilių komunikacijos tinkluose. Techninių informacinių sistemų inžinerijos magistro baigiamasis darbas. Darbo vadovas prof. A. Andziulis, Klaipėdos universitetas: Klaipėda, 2011. – 98 p.

PRIEDAI

1 priedas. Parengtos publikacijos

1. A. Andziulis; **M. Kurmis**; J. Vaupsas; S. Jakovlev; V. Pareigis. Trust Based Authentication Scheme for Latency Reduction in Vehicular Ad-Hoc Networks (VANETs).. The 7th International Conference on New Electrical & Electronic Technologies & Their Industrial Implementation (NEET 2011). Zakopane, Poland, June 28 – July 01, 2011. [ISI Proceeding; Accepted Manuscript]
2. A. Andziulis; R. Plestys; S. Jakovlev; D. Adomaitis; K. Gerasimov; **M. Kurmis**; V. Pareigis. Priority Based Tag Authentication and Routing Algorithm for Intermodal Containers RFID Sensor Network. Transport, 2011. Taylor&Francis. [ISI Web of Knowledge; Accepted Manuscript; In Press]
3. V. Bulbenkiene; V. Pareigis; A. Andziulis; **M. Kurmis**; S. Jakovlev. Simulation of IEEE 802.16j Mobile WiMAX Relay Network to Determine the Most Efficient Modulation Zone to Deploy Relay Station. Electronics & Electrical Engineering. 2011. [ISI Web of Knowledge; Accepted Manuscript; In Press]
4. A. Andziulis; S. Jakovlev; D. Adomaitis; R. Steponavicius; **M. Kurmis**; V. Pareigis. Integration of Information system Models in Intermodal Container Transportation Systems. Proceeding of the 14th International Conference. Transport Means 2010. Kaunas, Lithuania, October 21-22, 2010, [ISI Proceeding]
5. A. Andziulis; V. Pareigis; V. Bulbenkiene; D. Adomaitis; **M. Kurmis**; S. Jakovlev. WiMAX Technology Application Research in the Klaipeda Region. 16th Internation Conference on Information & Software Technologies (IT2010). Research Communications. Kaunas, Lithuania, April 21-23, 2010, p. 48-52.
6. S. Jakovlev; A. Andziulis; K. Gerasimov; **M. Kurmis**. The Software Architecture of an Information System for Monitoring Containers Cargo Conditions. IFIP Advances in Information & Communication Technology. The 11th International IFIP Conference on e-Business, e-Service, e-Society (I3E2011). Kaunas, Lithuania, October 12-14, 2011. Springer-Verlag. [ISI Proceedings; Received Manuscript]
7. **M. Kurmis**; D. Adomaitis; V. Pareigis; S. Jakovlev; A. Andziulis. Bevielių vietinių tinklų saugumo tyrimas. VII Mokslinė Konferencija „Technologijos Mokslo Darbai Vakarų Lietuvoje“. Klaipėda, Lietuva, 2010, p. 186-189.
8. V. Pareigis; **M. Kurmis**; A. Andziulis; A. A. Bielskis. Adaptyvaus protingo ekologiško socialinio būsto automatinio valdymo bevieliu ryšiu sistemos koncepcija. VII Mokslinė Konferencija „Technologijos Mokslo Darbai Vakarų Lietuvoje“. Klaipėda, Lietuva, 2010, p. 226-230.

2 priedas. Pagrindinių bevielių technologijų, potencialiai tinkamų VANET tinklams palyginimas

Technologija	Nuotolis	Ryšio tipas	Sparta (Mbps)	Dažnių juosta	IEEE standartas	Tinkamumas automobilių tinklams		
						V2V	V2I	I2V
Bluetooth	100 m	1 su n	1	2,4 Ghz	IEEE 802.15.1	+	-	-
WLAN	200 m	1 su 1 1 su n	10-150	2,4; 5 Ghz	IEEE 802.11 a/b/g/n	++	+	+
802.11p	1 km	1 su 1	50	5,9 Ghz	IEEE 802.11p	++	++	++
WiMAX	10 km	1 su n	~20	2,4; 5 Ghz	IEEE 802.16e	-	++	++
GPRS	10 km	1 su n	~0,2	700-2600 Mhz	-	-	++	++
GSM	10 km	1 su n	0,02	900, 1800 Mhz	-	-	++	++
3G	10 km	1 su n	Iki 56	įvairus	-	-	++	++
LTE	10 km	1 su n	Iki 1000	728-3600 Mhz	-	-	++	++
Palydovinis	>10000km	1 su n	0,3	950-1450 Mhz	-	-	+	++

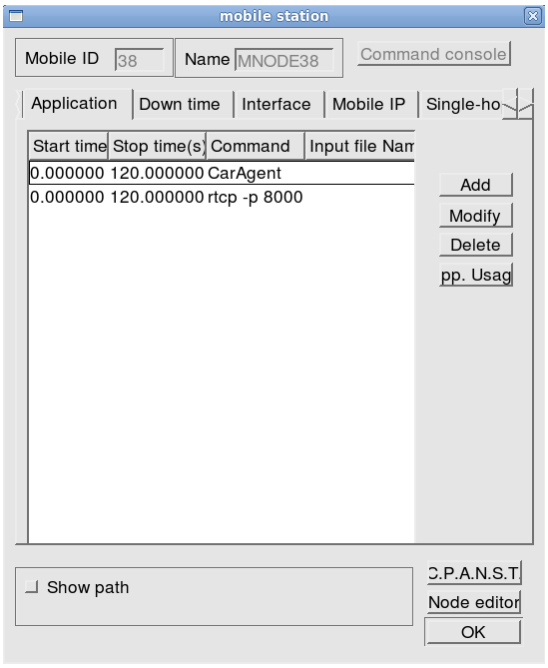
3 priedas. Kokybinis mobilumo generatorių palyginimas

	VanetMobiSim	SUMO	MOVE	STRAW	FreeSim	TSIS	VISSIM	SmartAHS
Programinės įrangos charakteristikos								
Nemokama	+	+	+	+	+	-	-	+
Atviras kodas	+	+	+	+	+	-	-	+
Konsolė	-	+	+			+	-	+
Grafinė vartotojo sąsaja	+	+	+	+	+	+	+	-
Tęsiamas vystymas	-	+	-	-	-	+	+	-
Diegimo sudėtingumas	vidutinis	vidutinis	lengvas	vidutinis	lengvas	lengvas	lengvas	sudėt.
Naudojimo sudėtingumas	vidutinis	sudėt.	vidutinis	vidutinis	lengvas	sudėt.	vidutinis	sudėt.
Žemėlapių tipas								
Realūs	+	+	+	+	+	+	+	-
Sukurti vartotojo	+	+	+	-	-	+	+	-
Atsitiktiniai	+	+	+	-	-	-	+	+
Palaikomi mobilumo modeliai								
Atsitiktinio judėjimo	+	+	+	-	-	+	+	+
Manhattan	-	+	+	-	-	-	-	-
Naudojami eismo modeliai								
Makroskopiniai	-	-	-	-	+	+	+	-
Mikroskopiniai	+	+	+	+	+	-	-	+
Kelios eismo juostos	+	+	+	+	-	+	+	-
Juostų keitimas	+	+	+	+	-	+	+	-
Atskirų krypčių srautai	+	+	+	+	-	+	+	-
Greičio apribojimai	+	+	+	+	+	+	-	-
Šviesoforai	+	+	+	+	-	+	+	+
Dideli kelių tinklai	-	+	+	+	-	+	-	-
Judėjimas be susidūrimų	-	+	+	-	-	-	-	-
Skirtingi automobilių tipai	-	+	+	-	-	+	+	-
Hierarchinės sankryžos	-	+	+	-	-	+	-	-
Palaikomi žymių užrašymo formatai								
ns-2	+	-	+	-	-	-	-	-
GloMoSim	+	-	+	-	-	-	-	-
QualNet	+	-	+	-	-	-	-	-
XML paremtas	+	-		-	-	+	-	-
OS suderinamumas								
Windows	-	-	-	-	-	-	+	-
Unix	+	+	+	+		+	-	+

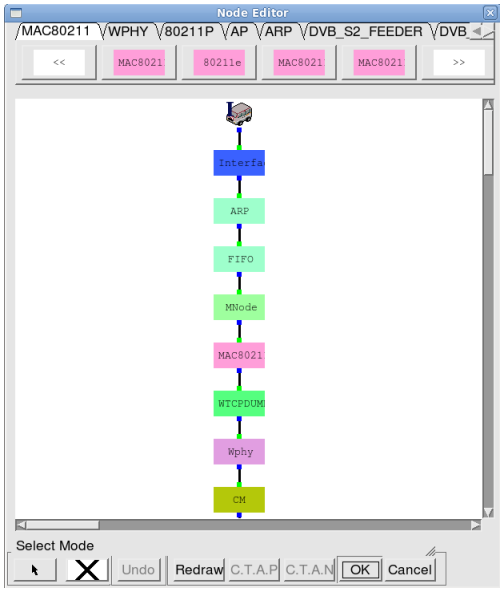
4 priedas. NCTUns programa sudaryto modelio kodo fragmentas

```
                </Application>
                 <Application>
                  <BeginTime>0</BeginTime>
                  <EndTime>120</EndTime>
                  <Command>stg -u 1000 120 1.0.1.1 -p
8000</Command>
                  <File></File>
                  <SrcPort>0</SrcPort>
                  <DstPort>0</DstPort>
                  <ProtocolType>0</ProtocolType>
                  <DirectionType>0</DirectionType>
                  <TrafficStreamID>0</TrafficStreamID>
                  <TrafficType></TrafficType>
                  <Mean_Data_Rate>0</Mean_Data_Rate>

<Nominal_Packet_Size>0</Nominal_Packet_Size>
                  <DelayBound>0</DelayBound>

<Maximum_Service_Inteval>0</Maximum_Service_Inteval>
                 </Application>
                </ApplicationList>
                <Host_conf>
                 <m_RO>0</m_RO>
                 <m_port></m_port>

<System_Routing_Table_Mode>3</System_Routing_Table_M
ode>

<System_Routing_Deamon></System_Routing_Deamon>
                </Host_conf>
                <MInterfaceList Number="1" >
                 <MInterface InterfaceID="1" Type="0" ID="1"
>
                  <Pos>
                   <X>905</X>
                   <Y>150</Y>
                   <Z>0</Z>
                   <CX>910</CX>
                   <CY>155</CY>
                   <CZ>0</CZ>
                   <Left>905</Left>
                   <Right>915</Right>
                   <Top>150</Top>
                   <Bottom>160</Bottom>
                  </Pos>
                  <Size>
                   <Width>10</Width>
                   <Height>10</Height>
                  </Size>
                  <Visible>True</Visible>
                  <VisibleID>True</VisibleID>
                  <DownTime Number="0" />
                  <Antenna>
                   <AngularSpeed>0.000000</AngularSpeed>
                   <BeamWidth>6.283185</BeamWidth>
                   <PointDirection>1.570796</PointDirection>
                  </Antenna>
                 </MInterface>
                </MInterfaceList>
                <VisibleInteface>True</VisibleInteface>
                <DefaultGateway>1.0.1.254</DefaultGateway>
                <Show>
                 <ShowMobility>False</ShowMobility>

<ShowReceiveThreshold>False</ShowReceiveThreshold>

<ShowCSThreshold>False</ShowCSThreshold>
                </Show>
                <Mobility>

<KeepMovingSpeed>True</KeepMovingSpeed>
                 <MoveSpeed>10</MoveSpeed>
                 <PauseTime>0</PauseTime>
                </Mobility>
                <MobileIP>
                 <UseMobileIP>False</UseMobileIP>
                 <HA></HA>
                 <MN></MN>
                </MobileIP>
                <car_info>
                 <road_type>0</road_type>
                 <road_ID>0</road_ID>
                 <group_ID>0</group_ID>
                 <large_scale>0</large_scale>
                 <change_road>0</change_road>
                 <leader_id>0</leader_id>
                </car_info>
                <TrafficUnit>
                 <isroadsideunit>0</isroadsideunit>
                 <iscontroller>0</iscontroller>
                </TrafficUnit>
               </Node>
               <Node Type="ID_NODE_CAR_ADHOC"
ID="42" >
                <Pos>
                 <X>266</X>
                 <Y>166</Y>
                 <Z>0</Z>
                 <CX>282</CX>
                 <CY>182</CY>
                 <CZ>0</CZ>
                 <Left>266</Left>
                 <Right>298</Right>
                 <Top>166</Top>
                 <Bottom>198</Bottom>
                </Pos>
                <Size>
                 <Width>32</Width>
                 <Height>32</Height>
                </Size>
                <Visible>True</Visible>
                <VisibleID>True</VisibleID>
                <DownTime Number="0" />
                <IDAccumulator>2</IDAccumulator>
                <InterfaceList Number="0" />
                <ApplicationList Number="1" >
                 <Application>
                  <BeginTime>0</BeginTime>
                  <EndTime>120</EndTime>
                  <Command>CarAgent</Command>
                  <File></File>
                  <SrcPort>0</SrcPort>
                  <DstPort>0</DstPort>
                  <ProtocolType>0</ProtocolType>
                  <DirectionType>0</DirectionType>
                  <TrafficStreamID>0</TrafficStreamID>
                  <TrafficType></TrafficType>
                  <Mean_Data_Rate>0</Mean_Data_Rate>

<Nominal_Packet_Size>0</Nominal_Packet_Size>
                  <DelayBound>0</DelayBound>

<Maximum_Service_Inteval>0</Maximum_Service_Inteval>
                 </Application>
                </ApplicationList>
                <Host_conf>
                 <m_RO>0</m_RO>
                 <m_port></m_port>

<System_Routing_Table_Mode>3</System_Routing_Table_M
ode>

<System_Routing_Deamon></System_Routing_Deamon>
                </Host_conf>
                <MInterfaceList Number="1" >
                 <MInterface InterfaceID="1" Type="0" ID="1"
>
```

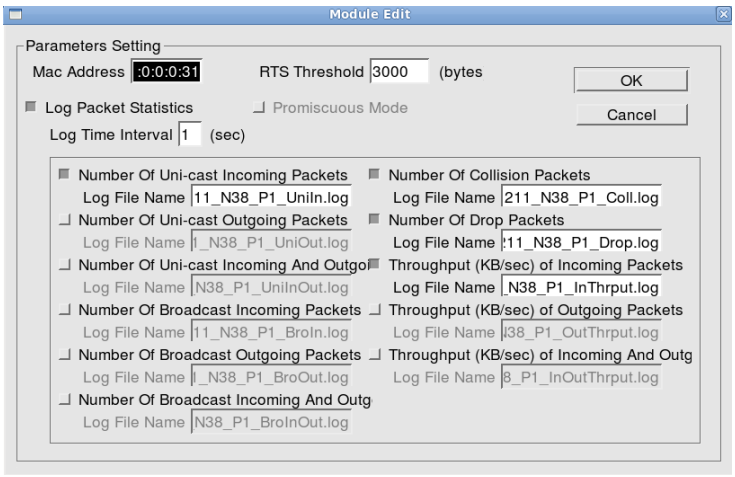
5 priedas. NCTUns programinio paketo dialogo langai



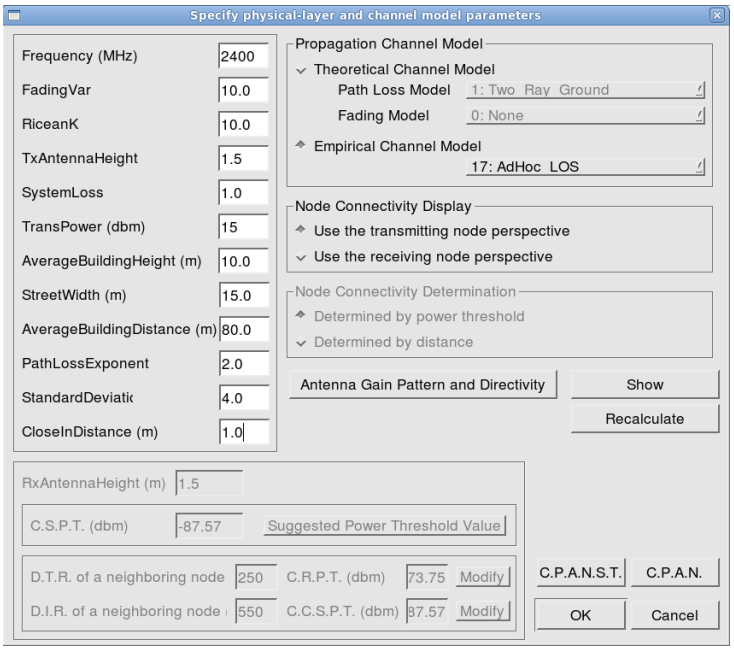
1 pav. *Mobilaus mazgo nustatymų langas, kuriame nurodytos mazgo vykdomos programos*



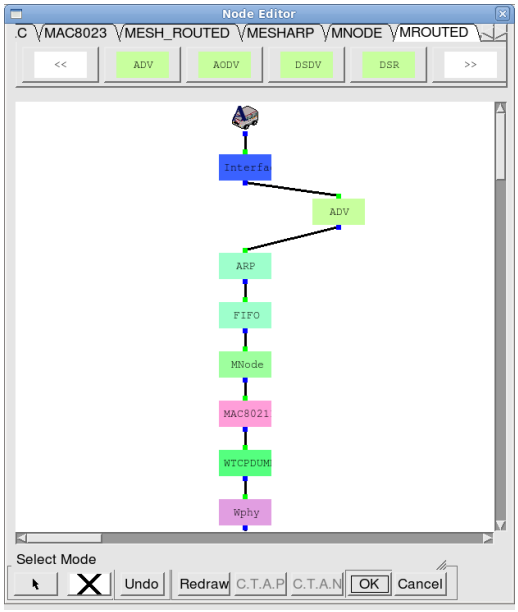
2 pav. *Mobilaus mazgo protokolo stekas*



3 pav. *Simuliacijos rezultatų užrašymo pasirinkimų langas*



4 pav. *Fizinio kanalo parametrų nustatymų langas*



5 pav. *Mobilaus ad-hoc mazgo maršrutizavimo protokolo keitimas*