KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Vytautas Dagilis

Didelio tankio belaidžių tinklų pralaidumo tyrimas

Magistro darbas

Darbo vadovas

prof. Rimantas Plėštys

Kaunas, 2011

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Vytautas Dagilis

Didelio tankio belaidžių tinklų pralaidumo tyrimas

Magistro darbas

Recenzentas

2011-05-30

Darbo vadovas

prof. Rimantas Plėštys

2011-05-30

Atliko

IFM-9/1 gr. stud.

Vytautas Dagilis

2011-05-30

Kaunas, 2011

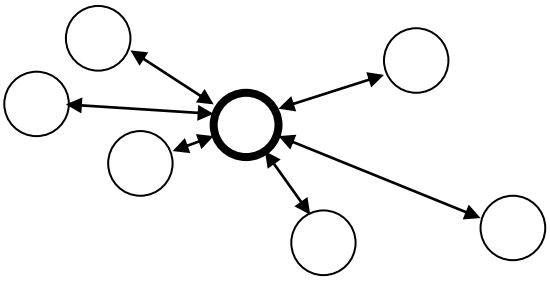
Turinys

Įvadas

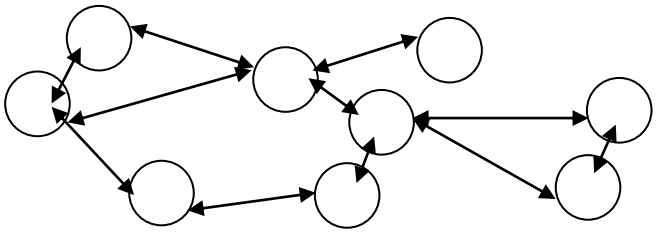
Visas pasaulinis interneto tinklas, dauguma duomenų perdavimo įrenginių naudojasi materialiomis jungtimis. Populiariausia plačiajuosčio interneto prieigos galiniams vartotojams perdavimo priemonė – vario kabeliai, kur informacija perduodama vario gyslomis tekančios srovės impulsais. Paskutiniu metu pradėta naudoti ir spartesnė bei brangesnė duomenų perdavimo terpė – optiniai kabeliai. Šiuose kabeliuose informacija perduodama šviesos impulsų pagalba, siunčiant ją optinio pluošto gyslomis.

Deja, laidinės komunikacijos priemonių pagrindinis trūkumas – įrenginių stacionarumas. Vartotojai negali naudotis internetu keisdami savo vietą (ribotai, trumpais atstumais). Beveik nėra galimybių keisti vietos nenutraukus ryšio. Dėl šios priežasties tarp vartotojų labai paplito belaidės ryšio priemones.

Šiuo metu egzistuojantys tinklų standartai remiasi centralizuotu paslaugos teikimu (pav. 1). Tai belaidžių tinklų architektūra naudojama mobiliojo ryšio operatorių bei namų belaidžiuose tinkluose, kai visi vartotojų srautai pirmiausiai turi eiti per centrinę stotį. Šiuo metu atsiranda naujų siūlymų, kaip galima patobulinti komunikaciją bei gerinti belaidžio ryšio paslaugos kokybę, pritaikant ją pagal poreikius. Belaidis ryšys gali būti panaudojamas tiesioginei komunikacijai tarp įrenginių, apeinant bazinę stotį (pav. 2), bei panaudojant kitus abonentus kaip tarpininkus, norint užmegzti tolimesnius ryšius.



Pav. 1. Centralizuoti belaidžiai tinklai



Pav. 2. Daugiašuoliai tinklai

Daugiašuolių tinklų veikimas vis dar kelia daug problemų, bet aiškiai matoma perspektyva juos panaudoti praktikoje. Geresnis resursų išnaudojimas, komunikacijos atpiginimas ar netgi naujų taikymo sričių atsiradimas skatina tolimesnius tyrimus bei sprendimų tobulinimus. Jau pradedami diegti kai kurie tinklai praktiniam panaudojimui, nors galutinių visuotinai pripažintų standartų dar nėra.

Darbe reikia išanalizuoti daugiašuolių tinklų teikiamą naudą, lyginant su dabartinėmis technologijomis. Ieškoti būdų, kaip patobulinti naujos kartos tinklų veikimą. Modeliavimo būdu nustatyti momentinę ad hoc tinklo pralaidumo reikšmę, tenkančią vienai

komunikuojančių mazgų porai. Analizei panaudoti įvairias tinklo topologijas. Duomenų analizės metu pateikti rekomendacijas tinklo veikimo optimizavimui bei diegimui.

I. Belaidžių tinklų problematika

Dabartinės belaidės ryšio priemonės palengvino pasaulinio interneto tinklo išplitimą, paskatino mobiliųjų paslaugų paplitimą. Deja, nors ir labai patogios dabartinės belaidžių tinklų technologijos nepatenkina visų esamų vartotojų poreikių. Kuriamos naujos technologijos, kurios tiek palengvina dabartinių problemų sprendimą, tiek atveria naujas panaudojimo nišas. Žinoma, naujos technologijos susiduria su įvairiais naujais iššūkiais, kuriuos technologijų kūrėjai turi išspręsti.

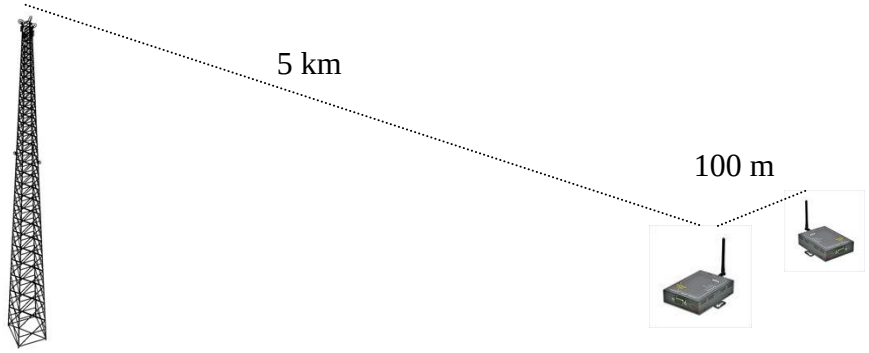
1. Šiuolaikiniai belaidžiai tinklai

Populiariausia pasaulyje GSM belaidė technologija jau pradeda diegti ketvirtosios kartos įrangą. Vietiniams tinklams naudojamos skirtingos versijos Wi-Fi standartų šeimos belaidė įranga. Į naują, miestinių tinklų nišą įsilieja WiMax standartai. Šios technologijos tenkina daugumą dabartinių vartotojų poreikių. Deja, belaidžiai tinklai vis dar turi keletą esminių trūkumų:

- Kaina - brangesnė įranga, lyginant su laidine;
- Patikimumas - jautri trukdžiams, galimi ryšio trikdžiai;
- Sparta - ne visos belaidės ryšio priemonės užtikrina pakankamą spartą kai kurioms paslaugoms (balso, vaizdo perdavimas, HD televizija);
- Poveikis aplinkai - radijo bangų poveikis aplinkai bei žmogaus organizmui iki galo neištirtas;
- Paslaugų kokybė (QoS) - jautrumas trikdžiams lemia ryšio nestabilumą;
- Saugumas - duomenų perėmimas netgi neturint fizinio priėjimo prie tinklo.

Belaidžių įrenginių kaina, lyginant su analogiška laidine tinklo įranga, yra žymiai didesnė, netgi nelyginant to, kad su paprastais laidiniais įrenginiais palaikoma duomenų sparta yra žymiai didesnė. Radijo bangomis perduodami duomenys gali būti paveikti interferencijos ar kitų pašalinių trikdžių. Šie trikdžiai gali įtakoti ne tik spartą, bet ryšio kanalo patikimumą, paslaugų kokybę. Nepakankamos kokybės ryšio paslauga, gali neleisti naudotis kitomis paslaugomis: pvz.: internetine telefonija ar televizija. Atsirandantis ryšio vėlinimas ar greičio fluktuacijos gali apriboti kai kurių internetu pasiekiamų paslaugų vartojimą. Atsiradus belaidžiams įrenginiams labai opi problema tapo fizinio tinklo saugumas. Naudojant tik laidines jungtis, fiziškai prieiti prie svetimo tinklo resursų buvo įmanoma tik turint fizinį priėjimą. Naudojant belaidį tinklą, jo veikimo ribos neretai peržengia fizinės nuosavybės ribas ir pasiekia laisvai prieinamas teritorijas. Nepakankamas belaidžių tinklų saugumo užtikrinimas kelia riziką visam tinklui, ne tik belaidei jo daliai.

Dar viena architektūrinė dabartinių tinklų problema - komunikacija tik per centrinį tašką. Dvejų arti esančių įrenginių priverstinė komunikacija per nutolusią bazinę stotį be reikalo užteršia didesnį ryšio kanalo kiekį. Pavyzdyje (Pav. 3) pavaizduota situacija, kai 100 m atstumu esantys mazgai komunikacijai būtinai turi naudoti už 5 km esančią bazinę stotį. Netgi 100 vartotojų, išsidėsčiusių poromis 100 metrų atstumu tarpusavyje, optimaliai parinkę siunčiamo signalo stiprumą, komunikacijai išnaudotų tik apie 3 km^2 plotą. Tuo tarpu dviems abonementams, komunikuojantiems per bazinę stotį, esančią už 5 km, komunikacijos išnaudojama teritorija pakiltų bent iki 75 km^2 ploto. Netgi tuo atveju, kai bazinė stotis naudotų keturių sektorių antenas, aptarnaujančias po 90^0 laipsnių kampu apribotą teritoriją, kuri siektų bent 18 km^2 ploto. Apeinant bazinę stotį ir panaudojant tiesioginės komunikacijos galimybę, galima stipriai pagerinti to paties dažninio radijo bangų kanalo išnaudojimą. Tokiu būdu visoje bazinės stoties aptarnaujamoje teritorijoje tuo pačiu metu galėtų pasinaudoti kiti abonentai, kuriems komunikacija su bazine stotimi yra neišvengiama. Bazinės stoties panaudojimas tik esant būtinybei stipriai pagerintų resursų išnaudojimą.



Pav. 3. Banginių resursų neoptimalus panaudojimas centralizuotuose tinkluose

Nepaisant nemažo kiekio neigiamų belaidžio tinklo savybių, teigiami šių tinklų aspektai skatina jų plėtimąsi bei tolimesnes investicijas į jų tobulinimą. Be mobilumo šie tinklai pasižymi šiomis savybėmis:

- Lankstumas - platus panaudojimo galimybių spektras;
- Atsparumas - mažiau fizinės infrastruktūros, kuri gali būti fiziškai pažeista;
- Patogumas - įrenginių mobilumas, visur prieinamas ryšys;
- Mažesni diegimo kaštai - nebūtina infrastruktūra iki pat galinio vartotojo;
- Paprastumas - įranga projektuojama taip, kad galutiniam vartotojui reikėtų konfigūruoti kuo mažiau parametrų;

Pagrindinė ir labiausiai akcentuojama belaidžių tinklų savybė yra mobilumas. Ne tik mobilumas yra stiprioji belaidžių technologijų pusė. Nors galinės įrangos kaštai yra didesni, bet naujų vartotojų prijungimas prie tinklo tampa pigesnis. Nėra poreikio diegti infrastruktūrą,

taigi galutiniai kaštai yra žymiai mažesni. Infrastruktūros nebuvimas žymiai kelia atsparumą – įvykus bet kokiam įvykiui ar stichinei nelaimei galinė infrastruktūra lieka nepažeista, o pagrindinė infrastruktūra dažniausiai būna žymiai atsparesnė nei „paskutiniosios mylios“ įranga (angl. last mile). Daugumos belaidžių įrenginių sąsaja padaryta nesudėtinga ir yra lengvai suprantama bet kuriam vartotojui. Gana dažnas šiai įrangai keliamas reikalavimas, kad kiekvienas norintis vartotojas, netgi neturintis specialių žinių apie telekomunikacijas sugebėtų pajungti šią įrangą savo reikmėms.

Mobilumas bei kitos vartotojams patinkančios savybės skatina šių technologijų plitimą bei tolimesnę evoliuciją. Spartus mobiliojo interneto plitimas skatina tobulinti technologijas. Ateityje belaidžių mobiliųjų tinklų svarba tik didės. Technologijų tobulinimas dažniausiai remiasi į dabartinės įrangos tobulinimą bei tolimesnį vystymą, taip taupant diegimo kaštus. Ateities tinklų evoliucija remsis į dabartines technologijas.

GSM

Turbūt pats populiariausias belaidės įrangos standartas paplitęs visame pasaulyje. Šio standarto dėka išplito mobilieji telefonai. Plačiai išplitęs telefonų tinklas, jau egzistuojanti infrastruktūra buvo pritaikyta ir atsirandančiam duomenų perdavimo poreikiui.

GSM dar vadinamas 2G - antrosios kartos korinio ryšio standartas daugiausiai vis dar orientuotas tik į telefoninių paslaugų (balso) perdavimą. Keletas patobulinimų leidžia persiųsti labai ribotą duomenų kiekį, kas taip pat labai atsiliepia duomenų persiuntimo kainai.

Tolimesni GSM atnaujinimai įeina į 3G - trečiosios kartos mobiliųjų telekomunikacijų karta. Tokie standartai kaip UMTS, HSPA, HSDPA dar labiau praplėtė vartotojų mobiliąją prieigą prie duomenų resursų. Spartų palyginimas pateiktas Lentelė 1.

Lentelė 1. GSM standartų spartos

Technologija	Dažninio kanalo plotis	Vartotojui skirta sparta (teorinė)	Vartotojui skirta sparta (Reali)
GSM	200 kHz	9,6 kbps	9,6 kbps
GPRS	200 kHz	172 kbps	40 kbps
EDGE	200 kHz	474 kbps	100 kbps
UMTS	3,75 MHz	2 Mbps	384 kbps
WCDMA	5 Mhz	2 Mbps	1 mbps
HSDPA		17 Mbps	14,4 Mbps

Šios technologijos panaudojimas vartotojų atžvilgiu yra labai nepatogus, kadangi vartotojai yra pririšami prie centrinio operatoriaus. Naudojami licencijuoti dažniniai kanalai draudžia bet kokios asmeninės įrangos naudojimą šiuose kanaluose negavus operatoriaus sutikimo.

Dviems greta esantiems įrenginiams neleidžiama tiesiogiai komunikuoti tarpusavyje. Šiuose tinkluose labiausiai pasireiškia neoptimalus greta esančių įrenginių tarpusavio komunikacijos poveikis visam tinklui, dėl pakankamai didelio veikimo atstumo. Didelis padengiamas plotas bei šiuo metu jau įdiegta infrastruktūra ateityje neleis šiems tinklams greitai išnykti iš rinkos. Turėtų keistis šio tinklo paskirtis iš tiesioginio paskutinės mylios prieigos suteikimo į ryšio šaltinį kitiems, mažesniems, tinklams.

IEEE802.11 - Wi-Fi

Labiausiai paplitęs vietinio tinklo (WLAN - wireless local area network) standartas [13]. Šie tinklai neapima didelių teritorijų, ir yra taikomi namų ar pastato viduje esančių įrenginių prijungimui prie tinklo. Naudojant brangesnes antenas bei įrangą taikomi ir tolimesniais atstumais.

Stiprioji šio standarto savybė - išnaudojamas nelicencijuojamas 2,4 GHz dažnis (yra ribojamas tik įrangos signalo stiprumas). Paskirtis - asmeniniams vartotojų poreikiams namų ar biuro aplinkoje.

Žemiau pateikiamoje Lentelė 2 palyginamos skirtingais metais išleistos skirtingos standarto versijos. Visose versijose, išskyrus 802.11n variantą, naudojamas "Half-Duplex" režimas, reiškiantis kad vienu metu įrenginys gali vykdyti arba siuntimą arba priėmimą. Tik paskutiniojoje 802.11n versijoje yra realizuojamas "Full-Duplex" režimas, kai abipusiai srautai į vieną sąsają gali egzistuoti vienu metu.

Lentelė 2. IEEE 802.11 standarto savybės

Standartas	Dažnis	Dažninio kanalo plotis	Vartotojui skirta sparta (teoriškai)	Veikimo nuotolis (lauke)
802.11a	5* GHz	20 MHz	54 Mbit/s	120 m
802.11b	2.4 GHz	20 MHz	11 Mbit/s	140 m
802.11g	2.4 GHz	20 MHz	54 Mbit/s	140 m
802.11n	2.4 GHz	20/40 MHz	72,2/150 Mbit/s	230 m

* Licencijuojamas dažnis, reikalingi leidimai

Nelicencijuoto dažnių diapazono panaudojimas palengvino šio standarto įrenginių skverbimąsi į rinką. Vartotoji netrukdomai gali pirkti ir naudotis šia įranga. Tai labai atpigino šios įrangos gamybos kaštus ir dar labiau skatino įsigalėjimą namų vartotojų rinkose. Panaikinamas operatoriaus poreikis naudojant šią įrangą, kas labai pravartu eiliniams vartotojams.

Didelis populiarumas taip pat skatina šio standarto pritaikymo kitais vartojimo scenarijais tyrimus. Dėl šios priežasties dauguma tyrimų, susijusių su ad-hoc ar mesh tinklais yra daromi naudojant šio standarto įranga, bei atsižvelgiant į šio standarto modelius.

Dabar egzistuojantis šio standarto "ad-hoc" režimas vis dar nepalaiko daugiašuolių srautų perdavimų belaidėje terpėje. Tai yra pirmas žingsnis einant link centralizuoto prieigos taško panaikinimo iš komunikacijos. Tai ir lemia šios įrangos panaudojimą naujos kartos tinklų tyrimams.

Esminis šio standarto trūkumas - tinkle turi būti bazinė stotelė (angl. Access point), kuri dirba arba kaip šliuzas arba kaip maršrutizatorius. Kaip ir GSM atveju, dažniausiai greta esantys įrenginiai negali komunikuoti be iš anksto įdiegtos infrastruktūros. Kitaip nei GSM atveju, kai kurie šio standarto įrenginiai palaiko ad hoc režimą. Šio režimo pagalba keli įrenginiai gali komunikuoti tarpusavyje, nenaudodami bazinės stotelės. Šis režimas palengvina apsikeitimą duomenimis tarp gretimų įrenginių, bet kol kas nėra išvystytas integravimo į IP bei interneto tinklus mechanizmas, kas apsunkina prieigos prie interneto dalijimąsi tarp šiuo režimu veikiančių įrenginių.

Nepaisant trūkumų, šiuo metu atliekama daugybė tyrimų, kaip šio standarto įrangą pritaikyti įvairiose naujose srityse: transporto tarpusavio komunikacija, miestų tinklai (MAN - metropolitan area networks) bei kiti. Galimybė apsieiti be prieigos taško, nelicencijuoto dažnio naudojimas bei spartus ryšys yra labai svarbios savybės, kurių pagalba šis standartas gali būti panaudotas kaip pagrindas tolimesniam naujos kartos tinklų vystymui.

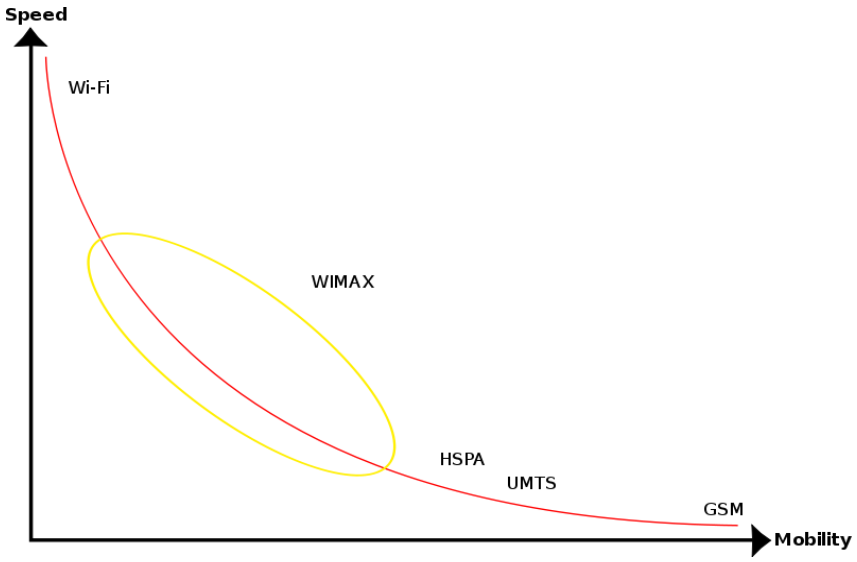
IEEE802.16 - WiMax

Šiuo metu sparčiai plintančios naujos kartos belaidžių tinklų standartas IEEE802.16 [1, 14] skirtas miesto ar platesnių teritorijų aprūpinimui plačiajuosčiu ryšiu. Vienas iš tikslų - plačiajuosčio tinklo prieiga mobiliesiems vartotojams - priešingai nei IEEE802.11 standartas, kuris buvo daugiau orientuotas į statinius vartotojus. Šis standartas priskiriamas 4G ryšio technologijų kartai, kaip ir naujai kuriamas LTE (GSM įpėdinis).

Šiuo metu daugiausiai medžiagos randama apie du šio standarto variantus: 802. 16d bei 802. 16e. Pirmasis yra statinis WiMax, antrasis yra pritaikytas mobiliesiems vartotojams. Dokumentacijoje [1] minimas maksimalus 70 Mbit/s greitis. Veikimo atstumas iki 50 km. Naudojamas iki 20 MHz kanalo plotis. Žinoma, ši technologija, kaip ir Wi-Fi turi adaptyvią moduliaciją, kurios pagalba reguliuojama sparta, atsižvelgiant į ryšio parametrus. Dėl šios priežasties, prie maksimalaus atstumo gaunama sparta yra žymiai mažesnė, kaip ir judančių mazgų gaunama sparta bus visuomet žemesnė už maksimalią galimą. Dažnių diapazonai iki galo nėra nusistovėję - tarptautinės ryšių reguliavimo tarnybos kol kas nėra rezervavę

dažninio diapazono šiai technologijai. Galima rasti įrangos dirbančios 2,4; 3,5 bei 10,5 GHz dažnių diapazone, priklausomai nuo regiono bei šalies licencijavimo tvarkos.

WiMax tiesiogiai nekonkuruoja su Wi-Fi standartu. Tai standartas užimantis tarpinę poziciją tarp GSM (ar 3G) sprendimų, suteikiantis žymiai didesnes spartas nei GSM, bei didesnes mobilumo galimybes nei WiFi Pav. 4.



Pav. 4. WiMax pozicionavimas tarp standartų[1]

Šis standartas yra labai artimas Wi-Fi standartų šeimai. Šie standartai pirmiausiai buvo projektuojami duomenų perdavimui, o ne balso komunikacijai, kaip GSM. Kuriant buvo panaudotas labai didelis kiekis gerųjų Wi-Fi standarto savybių, kurios šį standartą padaro lengviau pritaikomą daugiašuoliams tinklams. Deja, kol kas jo veikimas taip pat paremtas vieno šuolio belaidės komunikacijos principu, kai visi vartotojai turi būtinai komunikuoti su bazine stotimi, norėdami persiųsti duomenis greta esančiam įrenginiui ar kitiems tinklams. Nors, vartotojo požiūriu, daugiašuoliai tinklai nėra prieinami, bet 2004 metais į standartą buvo įtrauktas neprivalomas mesh topologijos palaikymas (plačiau kitame skyriuje), kai bazinės stotys gali tarpusavyje bendrauti naudodamos daugiašuolius belaidžius tinklus [8]. Tai atpigina operatoriui diegimo kaštus, kadangi nėra poreikio prie kiekvienos bazinės stoties įdiegti laidinio ryšio, taip pat kyla patikimumas, kadangi mesh tipo tinkluose dažnai taikomas jungčių dubliavimas bei srauto balansavimas tarp jų. Esant apkrovai ar neveikiant vienam įrenginiui, tinklas išlieka gyvybingas. Nemažas kiekis tyrimų atlikta ir šio tinklo pritaikymui ad hoc tinklams. Įdomių technologinių sprendimų siūloma tiek miesto tinklo kūrimui, tiek laivyno komunikacijos sistemoms [12].

Didelis dėmesys šio standarto atėjimui į rinką skatina tiek platesnius tyrimus tiek ir vartotojų susidomėjimą. Ieškomi nauji panaudojimo būdai bei tolimesnės pačio standarto

vystymo kryptys. Galimybė naudotis VoIP bei vaizdo perdavimo paslaugomis iš mobiliųjų įrenginių yra labai paklausi, dėl to tikimasi didelio šios technologijos augimo.

Visi šiuo metu naudojami tinklai pasižymi ta pačia problematika - vartotojai, nors ir būdami greta, privalo naudotis santykinai toli esančia bazine stotimi.Tai labai neoptimaliai išnaudoja radijo bangų resursus - du šalia esantys mobilieji telefonai užima tam tikrą kanalo dalį, kuri galėtų būti panaudota kitų įrenginių komunikacijai, kol jie bendrautų tarpusavyje. Taip pat patikimumas visiškai priklauso nuo bazinės stoties įrangos. Esant bet kokiems sutrikimams, visi vartotojai, esantys bazinės stoties aptarnavimo zonoje lieka be galimybės naudotis ryšio priemonėmis. Galimybė komunikuoti tiek tiesiogiai, tiek per bazinę stotį padidintų patikimumą, mažintų tinklų kainą bei keltų prieinamumą prie tinklo resursų.

Lentelė 3. Populiariausių belaidžio tinklo technologijų palyginimas su ad hoc tinklais

	GSM	**Wi-Fi**	**WiMax**	**Ad hoc**
Ryšio operatorius	Būtinas	Ne	Būtinas	Nebūtinas
Įrangos kaina	Brangi	Pigi	Brangi	Pigi
Iš anksto įdiegta infrastruktūra	Būtina	Būtina (išskyrus ad-hoc režimą)	Būtina	Ne
Sparta	Santykinai maža	Didelė	Didelė	Vidutiniška
Reikalingi licensijuoti dažniai	Taip	Ne	Ne	Ne
Dabartinis paplitimas	Platus	Platus	Mažas	Nepaplitęs
Balso perdavimas	Taip	Taip	Taip	Taip
Vaizdo transliacija	Žema kokybė, nuo 3G kartos	Taip	Taip	Taip
Naudojama daugiašuolė technologija	Ne	Ne	Ne	Taip
Imlumas išoriniams trikdžiams	Žemas	Taip	Taip	Taip
Mobilumas	Aukštas	Vidutinišas	Aukštas	Aukštas

Iš anksto įdiegtos infrastruktūros poreikis lėtina šių tinklų diegimą bei kelia jų kainą. Kitų savybių palygimas su dabartiniais standartais bei šiuo metu vis dar koncepciniais ad hoc tinklais pateiktas Lentelė 3. Iš jos galime matyti, kad dar yra nemažai trūkumų, kuriuos

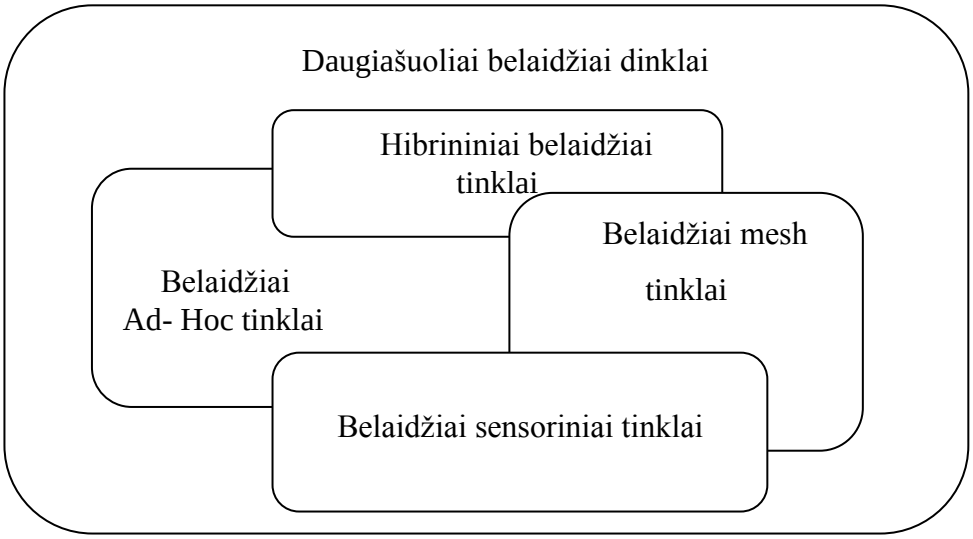
bandoma išspręsti, kuriant kitais principais veikiančius tinklus, galinčius geriau išnaudoti turimus resursus bei gerinti teikiamas paslaugas. Galima WiMax technologijos vystymo kryptis gali sutapti su Wi-Fi tinklų standartų vystymusi. Dabartinis įdirbis mobilios belaidės tinklo prieigos kūrime gali suteikti galimybes WiMax panaudoti labai aukšto mobilumo ir mažo tankio tinkluose, kur turi būti įveikiami dideli atstumai.

2. Naujos kartos tinklai

Daugelyje šių dienų belaidžių tinklų technologijų naudojama P-MP (angl. point to Multipoint - taškas - daug taškų) architektūra, kurios metu tik paskutiniame žingsnyje vartotojui ryšio paslauga pateikiama belaide terpe, naudojant centrinį prieigos maršrutizatorių ar bazinę stotį. Atitinkama įranga (Wi-Fi maršrutizatoriai, GSM radio stotys, ir t.t.) savo turimus tinklo resursus, kurie dažniausiai yra laidiniai, paskirsto vartotojams naudojant belaidę prieigą. Šis, dažnai neoptimalus dažninių resursų išnaudojimas verčia ieškoti naujų sprendimų.

Šiek tiek kitokia koncepcija yra pasiūlyta iš daugiašuolių (angl. multihop) belaidžių tinklų kūrėjų. Šiuo atveju netgi keleto tinklo mazgų prieiga prie kitų tinklų (interneto) yra prieinama visiems tinklo vartotojams. Šie vartotojai nebūtinai turi turėti tiesioginį ryšį su tinklo resursus turinčiais mazgais, bet gali tiesiogiai komunikuoti tarpusavyje. Komunikacija tarp tinklo paslaugas tiekiančio mazgo gali būti vykdoma ir tarpininkų pagalba. Ši architektūra labai teigiamai veikia tinklo patikimumą - priešingai nei GSM tinkluose, nustojus veikti vienai bazinei stočiai, tinklas nenustoja veikti . Visi vartotojai gali ir toliau gauti paslaugas. Į pasikeitimus reaguojantys maršrutizavimo algoritmai randa naujus maršrutus, kuriais toliau tęsiama komunikacija. Prijungus prie tinklo kitą mazgą ar pataisius senąjį, be žmogaus įsikišimo šis mazgas prisijungia prie tinklo, ir, esant reikalui, beveik iš karto gali tarpininkauti komunikacijoje.

Suaktyvėjus tyrimams šioje srityje, buvo pasiūlytas ne vienas daugiašuolių tinklų architektūrinis sprendimas. Šiuo metu dauguma šių sprendimų yra grupuojami pagal skirtingas pritaikymo sritis ar veikimo skirtumus (Pav. 5)[8].



Pav. 5. Daugiašuolių belaidžių tinklų klasifikacija[8]

Nors šis skirstymas neturi griežtų ribų, bet galima išskirti keturias pagrindines sritis, į kurias orientuojasi tyrėjai. Šios ribos gana dažnai peržengiamos ir kelių technologijų pritaikymas duoda gerų rezultatų bandant sukurti specifinei užduočiai atlikti reikalingus algoritmus.

Šiame skyriuje pateikti detalesni šių daugiašuolių belaidžių tinklų grupių aprašymai bei galimi algoritmai. Supažindinama su pagrindinėmis tyrimo kryptimis bei galiojančiais standartais.

Belaidžiai Ad-Hoc tinklai

Tai pagrindinė ir geriausiai atspindinti daugiašuolių tinklų problematiką, grupė [2, 3, 4, 5, 6, 9, 12, 14, 15]. Pats pavadinimas iš lotynų kalbos verčiamas kaip "laikinas" ar "šiam tikslui". Toks pavadinimas parinktas dėl šių tinklų esminės paskirties - šie tinklai turi susiorganizuoti automatiškai, tik atsiradus poreikiui. Išsiardyti taip pat be didesnių problemų ar pasekmių. Į šio tinklo veikimo aplinkybes įtraukiamas labai aukštas mazgų mobilumas bei nepastovus egzistavimas tinkle (dažnas įsijungimas bei atsijungimas, tarpusavio pozicijos keitimas).

Priešingai nei Wi-Fi šeimos standartuose naudojamame ad hoc režime, šio tipo tinklų koncepcijoje be tiesioginio bendravimo dar naudojama tarpininkavimo strategija, kai tinklo vartotojai perduoda reikiamus kaimyninių mazgų paketus link kitų mazgų ar link prieigos maršrutizatoriaus.

Tinklo dinamiškumas pasireiškia tuo, kad tinklas gali būti kuriamas tada, kada reikia, ir prie jo bet kuriuo metu gali prisijungti bei atsijungti pageidaujantys (leidimus turintys) įrenginiai. Vienas realus pavyzdys būtų studentų grupės tinklas. Bet kurioje auditorijoje

atvykę studentai su savo nešiojamaisiais kompiuteriais gali susijungti į bendrą tinklą ir dalintis medžiaga. Po paskaitos, visiems išjungus kompiuterius, tinklas išnyksta. Jis gali būti atkurtas kitoje auditorijoje, kitos paskaitos metu, ar neatkurtas niekada.

Šio tipo tinklai akcentuojami JAV gynybos ministerijos tyrimų centro DARPA veiklos planuose, kaip labai svarbus įrankis kovos lauke [18]. Susibūrus bet kokio tipo technikai ar atitinkama įranga apsirūpinusiems kariškiams tarp jų automatiškai turi atsirasti galimybė keistis reikiamais duomenimis. Komunikacija tarp būrių turėtų vykti decentralizuotu būdu, kad būtų kuo sunkiau sunaikinti tarpusavio ryšį - kas yra gyvybiškai svarbu mūšio lauke. Taigi, bet kuriems autorizuotiems vartotojams, susibūrus į teritoriją, kurioje visi gali komunikuoti bent su vienu kaimynu, galima visų vartotojų tarpusavio komunikacija. Kažkurioms grupėms nutolus vienai nuo kitos, komunikacija taip pat susiskaldo į atskiras grupes. Tarp būrių ryšį galima palaikyti kitos technologijos pagalba, kuri yra tik keliuose iš būrio įrenginių. Pavyzdžiui: tik tankai gali komunikuoti dideliu atstumu. Bet netoliese esantis pėstininkas gali pasinaudoti tanko ryšiu, ir naudotis visais (jam prieinamais) tinklo resursais.

Apibendrinant Ad hoc tinklų savybes, tai šie tinklai pasižymi:

- Mobilumu
- Infrastruktūros nebuvimu
- Taupumu
- Bendradarbiavimu
- Sparčiu prisijungimu prie tinklo (bei atsijungimu)
- Automatine reorganizacija

Ad hoc tinklai dar smulkiau skirstomi į mažesnes pritaikymo sritis. Dauguma šių sričių pasižymi skirtingais mobilumo modeliais ar perduodamų duomenų pobūdžiu. Toliau pateikiama MANET, VANET bei NANET pogrupių aprašymai.

MANET [3]

Vienas iš Adhoc tinklo pogrupių - mobilūs Ad hoc tinklai (angl. MANET - Mobile Ad-hoc NETwork). Iš anksčiau analizuotų dviejų pavyzdžių kovos laukas būtų tinkamas šio tipo tinklų pavyzdys - kai tinklas užmezgamas tarp judančių bei statinių įrenginių, kurie keičia tarpusavio pozicijas, nutola bei priartėja vienas prie kito. Taip pat gali būti įjungiami ir išjungiami be išankstinio perspėjimo.

Modeliavimo aplinkose, kaip ir realiuose eksperimentuose, dažniausiai naudojamas atsitiktinio judėjimo modelis. Kai kiekvienas tinklo mazgas juda nepriklausomai vienas nuo

kito dvimatėje ar netgi trimatėje erdvėje. Galimas komunikacijai trukdančių kliūčių atsiradimas ar netgi šių kliūčių judėjimas.

VANET [19]

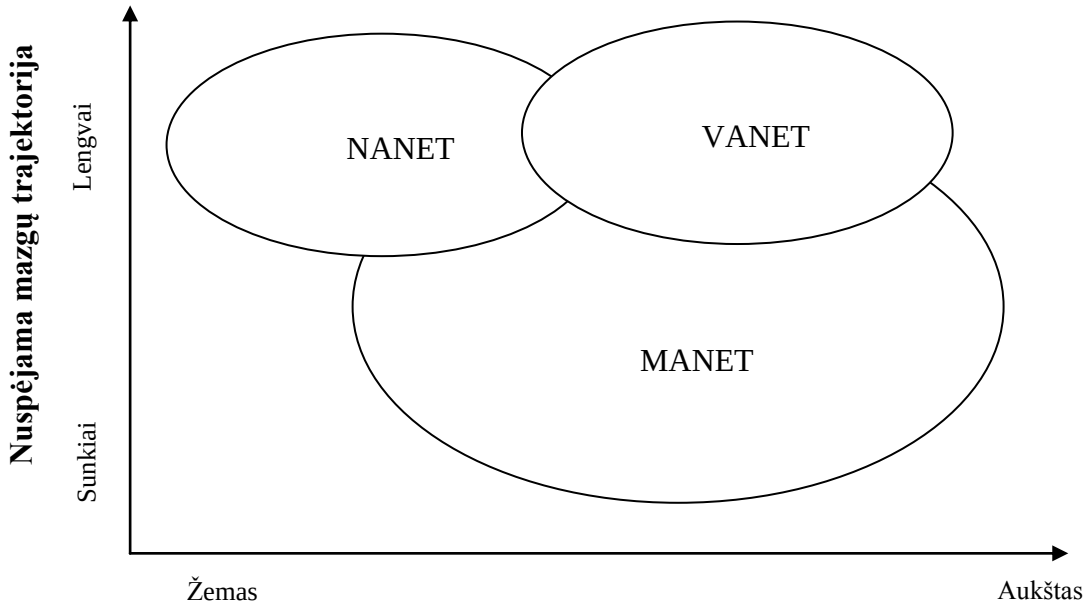
Specifinis MANET pritaikymo pavyzdys - VANET (angl. vehicular ad hoc network - transporto priemonių ad hoc tinklas). Išskirtinė savybė - transporto priemonės dažniausiai juda siaurais ruožais (keliais) bei ta pačia kryptimi. Taigi, vienu keliu važiuojantys automobiliai tarpusavio pozicijos nekeičia. Viena kryptimi bei panašiu greičiu judančios transporto priemones gana ilgam laikui gali užmegzti pastovų ryšį, taip neapsunkindamos tinklo santykiniu nestabilumu.

Šio tinklo taikymo sritis – auto karavanų tarpusavio komunikacija. Grupė automobilių, vykstančių tam tikra kryptimi, gali susijungti į auto karavaną. Šio auto karavano vairavimu rūpinsis tik pirmasis automobilis. Tuo tarpu kiti automobiliai ad hoc tinklo pagalba realiu laiku keičiasi informacija apie vairavimo sprendimus tarpusavyje ir vairuotojai gali ilsėtis.

NANET [12]

Pastaraisiais metais buvo pradėta nagrinėti ad hoc tinklų pritaikymo jūrų laivyboje galimybės. Šiuo metu jūriniai laivai naudoja labai žemo dažnio ryšio kanalus tarpusavio komunikacijai bei identifikacijai perduoti. Laivuose naudojama AIS (angl. automatic identification system) laivų vietos bei kurso informacijai perduoti tarpusavyje. Didesniems duomenų srautams šis komunikacijos metodas visiškai netinkamas. Interneto ryšys laivuose pasiekiamas tik palydovinio ryšio pagalba, kuris yra ganėtinai brangus.

Atsiradus WiMax technologijai suteikiama galimybė turėti plačiajuostį ryšį pakankamai dideliais atstumais. Šios technologijos pagrindu laivuose įrengtas ad hoc tinkas gali suteikti plačiajuosčio tinklo prieigą visam laivui esant gana dideliu atstumu nuo uosto, taip sumažinant palydovinio ryšio poreikį. Išskirtinės šios grupės tinklų savybės - mobilumas yra ganėtinai apibrėžtuose ruožuose, kadangi laivai juda tik jūrlapiuose pažymėtais keliais. Santykinis laivų greitis nėra labai aukštas, todėl šie tinklai nepasižymi labai didele dinamika bei poreikiu taupyti energiją, kaip yra MANET atveju.



Pav. 6. Ad hoc tinklų klasifikacija

Esminiai skirtumai tarp ad hoc tinklų pogrupių yra jų judėjimo greitis bei trajektorija. Paveikslėlyje Pav. 6 atvaizduojamos sritys, kurias padengia skirtingi pogrupiai. VANET pasižymi dideliu mazgų greičiu, bet ir labai nuspėjama judėjimo trajektorija. Tuo tarpu bendresnis MANET pogrupis įtraukia tiek aukšto tiek žemo mobilumo tinklus, kurių trajektorija gali kisti pagal labai įvairius dėsnius.

Duomenų perdavimas ad hoc tinklais kelia daug sudėtingų klausimų. Poreikis išnaudoti tą patį dažninį kanalą visiems mazgams labai apriboja perdavimo spartą, kelia problemų suvaldant tolygų mazgų perduodamų duomenų kiekį. Dinamiškumas kelia problemas surandant optimalius maršrutus. Kitų mazgų dalyvavimas, perduodant duomenis, kelia naujų saugumo problemų, kurias aktyviai sprendžia mokslininkų bendruomenė.

Belaidžiai sensoriniai tinklai

Automatizuojant daugumą procesų, šiuo metu priklausančių nuo žmogaus sprendimų reikalinga aktuali savalaikė informacija, padedanti kompiuterinėms sistemoms priimti reikiamus sprendimus. Šiam tikslui naudojami įvairūs sensoriai, matuojantys įvairius aplinkos ar kitų sistemų rodiklius. Kai kuriose sistemose naudojamas didžiulis kiekis labai plačiai pasklidusių sensorių, kurių tikslas kuo greičiau ir pigiau raportuoti centrinei stočiai apie savo būseną.

Labai geras pavyzdys - priešgaisrinė sistema miškams [17]. Šiuo metu daugumoje miškų sausros periodu budi sargai, kurie stebi aplinką ir tik pamatę gaisro požymius informuoja priešgaisrinę tarnybą. Šį nesudėtingą bet labai atsakingą darbą nėra lengva perduoti

automatinei mašinai - vaizdo apdorojimas kol kas nėra tiek pažengęs, kad galėtų iš kameros siunčiamų vaizdų identifikuoti gaisro požymių. Šios problemos sprendimui siūloma visame miške pažerti temperatūros sensorių. Centrinis kompiuteris, analizuojantis šių sensorių parodymus, gali identifikuoti anomalią temperatūrą ir daryti išvadas, kad atitinkamoje vietoje ką tik įsiplieskė gaisras.

Šiame pavyzdyje naudojamų sensorių paskirtis - matuoti temperatūrą ir siųsti parodymus į centrinę stotį. Sensoriaus užduotis nėra sudėtinga, tik jai keliamas reikalavimas: sensorius be išorinio maitinimo turi atlikti savo darbą gana ilgai. Taigi didelio ploto miške lėktuvo pagalba išberti sensoriai turi veikti keletą metų. Tiesioginė komunikacija tokiomis sąlygomis yra per brangi bei suvartojanti per daug energijos. Reikalingas sprendimas, kad visi šie sensoriai dibtų viename ad hoc tinkle, kuriuo duomenys nustatytais laiko intervalais pasiektų centrinę stotį. Tam pasitelkiami tarpiniai sensoriai, kurie ne tik siunčia, bet kartu ir persiunčia kaimynių sensorių duomenis.

Šio tinklo mobilumo modelis dauguma atvejų yra statinis. Tinklo įdiegimo pradžioje sensoriai turi susidėlioti maršrutus, kuriais ir bus siunčiami duomenys. Laikui bėgant, kai kurie sensoriai išseks ir taps nebepanaudojami, dėl to kuriant šio tipo tinklus reikėtų atsižvelgti į išnykstančius tarpinius mazgus ir lėtą tinklo degradaciją. Tinklo papildymas naujais sensoriais taip pat turi būti toleruojamas.

Pagrindinė problema - energijos suvartojimas. Įtaisai turi dirbti tik tuomet kai yra būtina. Budėjimo režimu nenaudoti nereikalingos energijos. Kadangi paketų persiuntimas yra energijos reikalaujantis procesas, taigi maršrutizavimas turi būti maksimaliai taupus, nešvaistantis įrenginių energijos bereikalingais tinklo palaikymo paketais bei maršrutų palaikymo ar atnaujinimo procesais.

Belaidžiai mesh tinklai

Pagrindinė mesh tinklų paskirtis - nebrangi bei paprastai diegiama plačiajuosčio belaidžio interneto prieiga vartotojams. Tai gana didelį kiekį statinės infrastruktūros naudojanti ad hoc tinklo versija. Taip pat mesh tinklai gali pasižymėti hierarchine architektūra, bei mazgai gali turėti daugiau nei po vieną radijo ryšio įrenginį.

Anglų kalboje žodis mesh reiškia tinklą. Tai daugiau su žvejybiniu tinklu susijęs terminas, parodantis dažniausią šio tinklo topologiją - kai mazgai tarpusavyje jungiasi panaudodami kelias turimas jungtis į bendrą mazgų tinklą, kuris teikia tinklo prieigos paslaugas žemesnio hierarchinio lygio įrenginiams.

Yra kelios mesh tipo atmainos pagal naudojamų belaidžio tinklo interfeisų kiekį: vieno ir kelių interfeisų įrenginiai. Vieno interfeiso įrenginiai naudoja tą patį kanalą tiek ryšio

palaikymui su išoriniu tinklu, tiek su mesh mazgo vartotojais. Pastebėjus, kad duomenis abejomis kryptimis siunčiant vienu kanalu labai krenta tinklo pralaidumas, buvo įdiegti kelis interfeisus turintys įrenginai. Vienas ar daugiau interfeisų yra skiriami tranzitinio tinklo palaikymui - ryšiui tarp to paties lygmens mesh mazgų palaikyti ar perduoti kitų mazgų srautams. Viena ar kelios sąsajos skirtos žemesnio lygmes vartotojų sąsajai. Šiuo būdu vartotojų srautas mažiau įtakoja viso tinklo aprūpinimą internetu bei galima geriau valdyti tinklo apkrovą.

Lentelė 4. Ad hoc, Mesh bei sensorinių tinklų palyginimas

Savybė	**Ad hoc tinklai**	**Mesh tinklai**	**Sensoriniai tinklai**
Topologija	Labai dinamiška	Santykinai statiška	Santykinai statiška
Paslaugas teikiančių mazgų mobilumas	Aukštas	Žemas	Žemas
Apribojimai energijos suvartojimui	Aukštas	Žemas	Labai aukštas
Pritaikymo charakteristika	Laikinas	Santykinai pastovus (semiperminent)	Pastovus
Reikalavimai infrastruktūrai	Jokios infrastruktūros	Dalinai arba pilnai išvystyta infrastruktūra	Beveik nėra
Tarpininkavimas komunikacijoje	Tarpininkauja mobilūs mazgai	Tarpininkavimas per statiškus mazgus	Tarpininkavimas taupant energiją
Maršutizavimas	Visiškai paskirstytas, tik esant poreikiui	Visikai paskirstytas arba dalinai paskirstytas. Hierarchinis arba statinių lentelių pagalba	Visiškai paskirstytas
Įdiegimas	Lengva įdiegti	Reikalingas bent dalinis planavimas	Lengva įdiegti
Srautų charakteristikos	Tik vartotojų srautai	Vartotojų ar sensorių srautai	Tik sensorių srautai
Populiarus	Komunikacija tarp	Didelių plotų	Priešgaisrinė

panaudojimo scenarijus	atsitiktinių automobilių automagistralėje	padengimas belaide plačiajuoste prieiga (prekybos centrai, miestai)	sistema miškams

Lentelė 4 pateikiamas pagrindinių minėtųjų tinklų grupių savybių palyginimas. Matoma, kaip aiškiai atsiskiria savybės, kurios yra reikalingos realizuojant kiekvieno tipo paslaugas. Jeigu mesh tipo tinklams reikalingas gana didelis kiekis infrastruktūros, tai ad hoc tinklams šios infrastruktūros poreikis visiškai minimalus.

Galimi hibridiniai tinklai, kai taikomos dvejų ar visų trijų sričių stipriosios savybės pritaikant atitinkamiems sprendimams. Kaip, tarkim, labai didelio ploto miškų priešgaisrinei apsaugai vien tik sensorinis tinklas gali nepalaikyti didelių srautų. Šiems sensoriams aptarnauti įdiegiamas mesh tipo tinklas, kuris surenka iš atitinkamų grupių sensorių informaciją ir kitais dažniais siunčia informaciją į centrą. Taip taupoma sensorių suvartojama energija, bei sutrumpinamas laikas, per kurį informacija pasiekia centrą. Išvengiama kai kurių sensorių perteklinio išnaudojimo bei perteklinių duomenų srautų, einančių per sensorius, esančius arti duomenų surinkimo centro.

3. Ad hoc tinklo saugumas

Mobilumas, atvira prieiga, tarpininkavimas - pagrindinės gerosios ad hoc tinklų savybės taip pat kelia dideles grėsmes šių tinklų vartotojų saugumui [8]. Kai kurios kyla iš naudojamų technologijų, kai kurias atneša naujos panaudojimo galimybės, kaip tarpininkavimas.

Pagrindinės ad hoc tinklo grėsmės:

- Tinklo užliejimo atakos - visas tinklo srautas užliejamas nereikalinga informacija;
- Trukdymo atakos - dalis tinklo, ar keli mazgai, užliejami nereikalinga informacija, kuri trukdo reikalingam srautui kirsti ar pasiekti atitinkamus tinklo segmentus;
- "miego trūkumo" ataka - pasirenkamas vienas mazgas, kuriuo naudojamas visam srautui maršrutizuoti, su tikslu išnaudoti visą turimą įrenginio energiją (bateriją);
- Paketų atmetimo ataka - piktybiškai atmesti paketus, kuriuos privalo persiųsti;
- Slaptas pasiklausymas - kaimynų pasiklausymo metu išgauta svarbi informacija;
- "Smegduobė" - įrenginys pasiskelbia turįs artimiausią kelią iki atakuojamo įrenginio. Tuomet srautas skirtas atakuojamam įrenginiui gali būti atmetamas (juodoji skylė) ar perduodama tik dalis srauto (pilkoji skylė). Taip pat srautas gali būti modifikuojamas (man in the middle);

- Maršrutų lentelių perpildymas - inicijuojama daugybės neegzistuojančių maršrutų įtraukimu į atakuojamus maršrutizatorius su tikslu užpildyti maršrutų lenteles, neleidžiant kurti naujų maršrutų ar panaudoti kitas silpnąsias protokolo savybes;
- Skubinimo ataka - aplenkiamas tikrasis maršrutizavimo algoritmas, ir grąžinamas neteisingas maršrutas;
- Lokacijos atskleidimas - gaunama informacija apie mazgų lokaciją ar tinklo topologiją.

Fundamentalios tinklo savybės, leidžiančios apsiginti nuo daugumos atakų:

- Konfidencialumas - Duomenys prieinami tik tikslinei grupei;
- Vientisumas - Duomenų modifikavimas visuomet aptinkamas;
- Autentifikacija - esybei priklauso būtent tas identitetas, kuriuo ji prisistato;
- Prieigos valdymas - užtikrina tik leistinų veiksmų vykdymą;
- Atsisakymo kontrolė - apsauga nuo tinklo vartotojų, atsisakančių teikti privalomas paslaugas;
- Prieinamumas - užtikrina tik leistinų veiksmų realų įgyvendinimą.

Yra pasiūlyta daugybė technologijų, leidžiančių realizuoti aukščiau paminėtas savybes ad hoc tinkluose. Deja, dar nėra visiškai nusistovėjusių standartinių sprendimų, kurie visiškai išpildytų užsibrėžtas gaires.

Neatsekamo elektroninio pašto principo taikymas ad hoc tinkluose

Šiuo metu siūloma daugybė įvairių tinklo saugumo, bei įsiveržimo aptikimo metodikų. Ad hoc, kaip ir kiti daugiašuoliai tinklai, gali būti jautrūs ne tik visiems plačiai žinomoms spragoms, bet ir kelti naujų problemų. Šiame skyriuje pateikiama anksčiau tokio didelio pavojaus nekėlusi problema - komunikuojančių šalių atskleidimas.

Dėl aiškios tinklo architektūros, kai naudojamasi tik patikimais įrenginiais, prižiūrimais patikimų administratorių, nekildavo tokio masto klausimas, kad komunikuojančių šalių atskleidimas yra lengvai prieinamas. Per bendrą maršrutizatorių keliaujančių srautų atsekimas būdavo žymiai sudėtingesnis. Daugiašuoliuose tinkluose beveik bet kas gali perduoti vartotojų duomenis, bei analizuoti jų turinį. Komunikuojančių šalių užslaptinimas padidina vartotojų saugumą.

Daugumoje saugumo užtikrinimo metodų taikomi įvairūs kriptografiniai sprendimai. Kriptografija - slaptos komunikacijos mokslas. Kriptografijos technologijos suteikia galimybę išsaugoti perduodamos informacijos slaptumą tūkstančiams metų. Šiuo metu naudojamos technologijos taip pat leidžia pakankamai slaptai perduoti ir naudojamus raktus, kurių pagalba

užšifruoti duomenys gali būti panaudojami tik jų adresatų. Taip duomenys apsaugomi nuo neteisėto jų perėmimo ar pakeitimo. Šis metodas buvo pasiūlytas elektroninio pašto laiškams perduoti, kuris papildomai leidžia neatskleisti komunikuojančių šalių [16]. Kai kuriais atvejais, užtikrinant duomenų vientisumą, konfidencialumą bei šalių autentifikaciją galima taikyti ir ad hoc tinklų duomenų perdavimui.

Optimaliam šio metodo panaudojimui pravartu iš anksto turėti nustatytą maršrutą, kuriuo gali būti siunčiami duomenys. Parinkus kelis tarpinius mazgus, padedančius užslėpti komunikuojančias puses galimas tiek optimalus, tiek slaptas maršrutas. Iš anksto nenustačius maršruto komunikuojančių šalių slaptumui užtikrinti parenkami keli atsitiktiniai mazgai. Patartina pasirinkti stabilesnius mazgus, kurie mažiau linkę keisti savo poziciją kaimynių mazgų atžvilgiu bei turi didesnę tikimybę veikti visą komunikacijos laiką. Šios savybės reikalingos norint užtikrinti geresnes ryšio laikines charakteristikas.

Viena labai populiari viešo-privataus rakto kriptografija leidžia duomenis M užšifravus vienu raktu K, duomenis iššifruoti naudojantis kitu raktu K^{-1}, bei atvirkščiai.

$$K^{-1}(K(M)) = K(K^{-1}(M)) = M$$

Šios technologijos pagalba galima garantuoti ne tik duomenų slaptumą, bet ir šių duomenų originalumą (garantija, kad šie duomenys yra išsiųsti iš patikimo siuntėjo).

Jeigu žinutės turinys M yra viena galima reikšmė iš baigtinės reikšmių aibės θ , tuomet atakuotojas (asmuo, norintis perimti žinutėje esančią informaciją, arba asmuo, norintis įsiterpti į komunikacijos procesą) gali spėjimo būdu tikrinti kuris žinutės turinys $Y \in \theta$ tenkina lygybę K(Y) = K(M), ir taip išsiaiškinti kokia informacija yra siunčiama. Šios atakos apsaugai prie žinutės turinio pridedama atsitiktinių skaičių seka R, taip apsauganti nuo šio tipo atakos. Tuomet siunčiama žinutė atrodytų taip: K(M,R).

Kiekvienas duomenų mainų dalyvis susigeneruoja po dvi poras raktų: viešąjį K bei privatųjį K^{-1}. Viešasis raktas išdalinamas visiems suinteresuotiems dalyviams, tuo tarpu privatusis raktas (K^{-1}) išlieka žinomas tik šios raktų poros kūrėjui.

Duomenų siuntėjas gali užkoduoti žinutę M savo privačiu raktu K_s^{-1}, bei gavėjo viešuoju raktu K_g:

$$K_s^{-1}\,(K_g\,(M, R))$$

Taip gaunamas užkoduotas pranešimas M, kurį iškoduojant reikalingas gavėjo privatus raktas K_g^{-1} (žinutės turinio apsaugojimas) bei siuntėjo viešasis raktas K_s (duomenų originalumo apsauga). Šiuo atveju atsitiktinė skaičių seka R pasitarnauja paslepiant vienodų žinučių srautą. Kiekvieną kartą siunčiant nors ir tokią pačią žinutę, tinkle šis pranešimas

visuomet bus skirtingas, todėl atakuotojui visos žinutės išliks skirtingos, apribojant galimybes aptikti pasikartojančią informaciją.

Dar vienas svarbi problema, kurios neišsprendžia dabartinės TCP/IP komunikacijos sistemos - tai komunikuojančių sistemų anonimiškumas. Nors ir komunikacijos turinys išlieka slaptas, bet dažniausiai galima atsekti duomenų srautų šaltinius. Kai kuriais atvejais šių duomenų anonimiškumas yra būtina sąlyga norint apsaugoti vykstančių procesų saugumą. Paprasčiausias galimas pavyzdys – elektroninio balsavimo biuletenių slaptumo užtikrinimas.

Naudojant viešo-privataus rakto koncepsiją yra pasiūlytas metodas kaip paslėpti komunikuojančių adresatų anonimiškumą. Tai galima įgyvendinti žinant bent dalį galimų tarpininkų (jų adresus $\{A_{t1}, A_{t2},...,A_{tn}\} \in A_t$) kurie gali dalyvauti žinutės perdavime iki gavėjo A_g. Taip pat reikalingi šių tarpininkų viešieji raktai $K_{t1}, K_{t2},..., K_{tn}$, kurių pagalba užkoduojami ir kitų perdavėjų adresai.

Paprasčiausiu atveju galime naudoti vieną tarpininką, kuris panaikina situaciją, kai siuntėjo ir gavėjo adresai vienu metu gali egzistuoti vienoje žinutėje. Naudojant vieną tarpininką A_{t1} (kurio viešasis raktas K_{t1}), siunčiamo pranešimo turinys gaunamas taip:

$$K_{t1}(R_1, K_s(R_0, M), A_g)$$

Šis užkoduotas pranešimas paslepia galutinio adresato adresą kol pasiekia tarpininką. Tarpininkas A_{t1} iškodavęs gautą pranešimą savo privačiu raktu:

$$K_{t1}^{-1}(K_{t1}(R_1, K_s(R_0, M), A_g)) \rightarrow R_1, K_s(R_0, M), A_g$$

sužino gavėjo adresą, bet žinutės turinys jam išlieka paslaptyje. Čia žymėjimas „->“ vaizduoja dekodavimo procesą.

Naudojant tik vieną tarpininką yra pavojus, kad atakuotojas stebėdamas įeinančius ir išeinančius srautus gali aptikti tiek siuntėjo, tiek gavėjo adresus. Pasitelkus didesnį kiekį tarpininkų, bei keičiant jų eiliškumą, galime kokybiškiau paslėpti komunikuojančias puses. Tokiu pačiu būdu, kaip ir vieno tarpininko atveju, pranešimą galima siųsti panaudojant didesnį kiekį tarpininkų. Vienos žinutės užkodavimo schema atrodytų taip:

$$K_{t1}(R_1, K_{t2}(R_2,... K_{tn}(R_n, K_s(R_0, M), A_g)... A_{n-1})A_{t3})A_{t2})A_{t1}$$

Kiekvienas tarpininkas naudodamasis savo privačiu raktu K_{ti} sužino kito tarpininko adresą, kuriuo reikia išsiųsti žinutę gaudamas informaciją, tik apie praėjusio tarpininko adresą. Vidiniai tarpininkai ($A_2...A_{n-1}$) neturi galimybės atskleisti siuntėjo ir gavėjo adresų. Žinutės turinys visiems tarpininkams A_t taip pat lieka nežinomas.

Iš pateiktos metodikos matome, kad nėra svarbu kad visiškai visi tarpiniai žinutę persiunčiantys mazgai dalyvautų žinutės kodavimo/dekodavimo procese. Užkoduota žinutė tarp tarpininkų A_i irA_{i+1} gali keliauti ir per kodavimo/dekodavimo nepalaikančius mazgus kurie tik padeda pasiekti tarpininką A_{i+1} tarpininką.

Ad hoc tinkluose ryšiai tarp vienos komunikuojančių mazgų poros yra labai nestabilūs, ir dažnai kintantys. Kiekvienas mazgas gali laisvai prisijungti ir atsijungti nuo tinklo. Nors ir dauguma pranešimų gali keliauti skirtingais keliais, vis tiek tarpiniams mazgams kiekvieno paketo siuntėjas ir gavėjas(-ai) išlieka žinomi. Aukščiau aprašyta strategija, kai paketų antraštėse yra talpinami tik tarpininkų adresai, gali padėti visiškai paslėpti komunikuojančių mazgų tapatybę. Deja, ši strategija, taikoma ad hoc tinklams gali sukelti keletą problemų:

- Padidėjęs tarpinių įrenginių procesoriaus apkrovimas;
- Padažnėjęs poreikis pakartoti siunčiamus duomenis;
- Išaugęs pranešimų perdavimo laikas;
- Išnaudojamos pastoviosios atminties kiekis viešųjų raktų saugojimui;
- Papildoma tinklo apkrova raktų apsikeitimui.

Padidėjęs tarpinių įrenginių procesoriaus apkrovimas

Kiekvienas tarpinis mazgas, kuris dalyvauja anonimiškų duomenų perdavime turi dekoduoti žinutę, kurioje yra užkoduotas kito mazgo adresas. Tai reiškia ne tik papildomą darbą dekoduojant pranešimą, bet ir naujų paketo antraščių kūrimas, naujo adresato paieška, bei maršrutų lentelių atnaujinimas.

Padažnėjęs poreikis pakartoti siunčiamus duomenis

Kadangi kiekvienas tarpinis mazgas ad hoc tinkle gali bet kada atsijungti nuo tinklo, ir nustoti perdavinėti duomenis, todėl galimas atvejis kad keliaujančios žinutės niekas nebegalės iškoduoti. Jegiu išsiunčiama žinutė, kuriai numatytas kelias per tarpininkus A_{t1}, A_{t2},...,A_{ti},...,A_{tn}, kurių viešieji raktai yra K_{t1}, K_{t2},...,K_{ti},...,K_{tn}, tai bent vienam tarpininkui A_{ti} atsijungus nuo tinklo prarandamas žinutės turinys, kadangi be jo privačiojo rakto K_{ti}^{-1} žinutės turinys bus neprieinamas kitiems tinklo nariams. Ši žinutė turėtų būti per naują persiunčiama.

Išaugęs pranešimų perdavimo laikas

Pranešimų laikas išauga ne tik dėl to, kad ilgiau užtrunka kodavimas bei dekodavimas. Taip pat žinutės siuntimo laiką gali prailginti ir neoptimalus kelio parinkimas. Kelias (tarpiniai mazgai) parenkami dar prieš siunčiant žinutę. Ad hoc tinkluose, kai labai sparčiai kinta tinklo mazgų išsidėstymas, labai dažnai keičiasi optimalūs maršrutai tarp dvejų mazgų. Kelių sekundžių bėgyje optimalus kelias gali tapti visiškai neveiksniu, ar gali atsirasti naujas maršrutas, kuris gali žymiai sparčiau perduoti duomenis.

Išnaudojamos pastoviosios atminties kiekis viešųjų raktų saugojimui

Viešųjų raktų panaudojimas koduojant pranešimus reikalauja kiekvieno tarpininko viešąjį raktą A_{ti} saugoti tam tikrą laiko tarpą. Sensorinių tinklų atveju, kai bandoma taupyti tiek aparatūrinės dalies kanos, tiek suvartojamos energijos atžvilgiu, ši metodika yra labai sunkiai pritaikoma. Visiškai kitaip yra mesh tipo tinkluose, kur pastovūs energijos šaltiniai nėra problema.

Papildoma tinklo apkrova raktų apsikeitimui

Kiekvienas tinklo narys, norintis dalyvauti kelio anonimiškumo užtikrinimo procese turi paviešinti savo viešąjį raktą. Tokiu būdu visi tinklo vartotojai galės pasinaudoti šiuo tinklo įrenginiu kaip tarpininku, ar autorizuoti šio įrenginio siunčiamus duomenis.

Viešojo rakto paviešinimas gali vykti dviem būdais. Vienas iš būdų - tik įrenginiui prisijungus prie tinklo išsiunčiant šį raktą visiems tinklo dalyviams (angl. broadcast). Kiekvienas tinklo įrenginys, dalyvaujantis anonimiškumo užtikrinime užregistruoja naują galimą tarpininką, bei išsaugo jo viešąjį raktą. Taip pat visi šie įrenginiai turėtų nusiųsti savo viešuosius raktus, norėdami užsiregistruoti pas naująjį narį. Šio būdo panaudojimas gali per daug apkrauti didesnį tinklą, kuriame pastoviai atsiranda ir išnyksta vartotojai – visuomet atsiradus vartotojui generuojamas gana didelis srauto kiekis.

Antrasis metodas – raktų apsikeitimas vyksta tik esant reikalui. Įrenginio viešasis raktas siunčiamas tik esant užklausimui tiesiogiai užklausėjui. Tokiu būdu naujo maršruto konstravimas bus žymiai ilgesnis nei pirmuoju atveju, bet bus sutaupoma didelis kiekis tinklo resursų.

Kaip matome, ši metodika neužtikrina visų galimų grėsmių išvengimo. Būtinos kitos metodikos papildančios apsaugą nuo kitų kenkėjiškų veiksmų tinkle.

Apibendrinimas

Dabartinės belaidžių tinklų technologijos paremtos centrinio prieitos taško principu - komunikacija tarp bet kurių dvejų tinklo mazgų gali vykti tik per tinklo centre esantį prieigos tašką. Tokia architektūra ne visuomet optimaliai išnaudoja fizinius (radijo bangų eterio) resursus. Naujos kartos belaidžiuose tinkluose naudojamas daugiašuolis paketų perdavimo principas, kai kiekvienas mazgas atlieka ir prieigos taško vaidmenį persiųsdamas kitų mazgų paketus. Ši technologija geriau išnaudoja belaidės terpės resursus, sumažina tinklų diegimo ir priežiūros kaštus. Su teigiamomis naujovėmis atkeliauja ir naujos grėsmes, kurioms panaudojami nauji ar adaptuoti sprendimai.

II. Maršrutizavimas

Labai didelė egzistuojanti problema siekiant panaudoti didelio masto belaidžius tinklus - nėra nusistovėjusių maršrutizavimo standartų, kurie užtikrintų visus šiems tinklams keliamus reikalavimus. Vieningi sprendimai nėra priimtini visiškai skirtingas pritaikymo sritis turintiems tinklams, todėl tuo pačiu metu skritingomis kryptimis vystomi ir maršrutizavimo algoritmai, galintys kaip įmanoma geriau išnaudoti specifines šių tinklų savybes.

Pagrindinės dvi problemos, sprendžiamos kuriant maršrutizavimo algoritmus yra vieno centrinio prieigos taško panaikinimas, kuris valdo visą maršrutizavimo procesą. Mazgų mobilumas, verčiantis pastoviai adaptuotis prie pastoviai kintančių maršrutų dar labiau apsunkina šį procesą. Kadangi nėra centrinio už maršrutizavimą atsakingo įrenginio, kiekvienas mazgas turi pats atlikti šią funkciją. Panaudodamas paskirstytus algoritmus mazgas privalo surinkti informaciją iš aplinkinių įrenginių ir rasti optimalų maršrutą iki reikiamo mazgo lokaliame tinkle, ar artimiausią išėjimą į globalų tinklą. Kelio paieškos algoritmai plačiau aprašomi šiame skyriuje, tuo tarpu apie vartų į globalų tinklą paieška plačiau analizuojama IV skyriuje.

Anksčiau aprašytos trys daugiašuolių tinklų rūšys – ad hoc, mesh bei sensoriniai tinklai taikomi skirtingomis aplinkybėmis, kuriose mazgai juda skirtingai. Modeliavimo metu svarbu atsižvelgti į tai, kad mazgų judėjimas būtų kuo artimesnis judėjimui realybėje. Panaudojant šiuos modelius geriau įvertinami specifiniai algoritmai, pritaikyti maršrutizavimo uždaviniui spręsti.

Šiame skyriuje apžvelgus pagrindinius mobilumo modelius, pristatomi pagrindiniai sprendimai taikomi mobiliesiems daugiašuoliams tinklams.

1. Tinklų mobilumo modeliai

Daugeliu atvejų belaidžio tinklo mobilumas labai stipriai apsprendžia jo poreikius maršrutizavimui. Nors ir energijos taupumo aspektas kai kuriais atvejais yra labai svarbus, bet patikimos paslaugos pristatymui dažniausiai mobilumas daro didžiausią įtaką, bei leidžia daryti prielaidas, kada galimas energijos taupymas.

Keletas dažnai sutinkamų mobilumo modelių, naudojamų belaidžių tinklų tyrimuose (8):

- Statinis - visi tinklo mazgai nekeičia savo pozicijos;
- Atsitiktinis, vaikščiojimo modelis - atsitiktinės kryptys ir greičiai;
- Atsitiktinis, vaikščiojimo punktais modelis - įtraukiamos pauzės tarp krypties ar greičio pokyčių;
- Atsitiktinių krypčių modelis - kryptys keičiamos tik erdvės pakraščiuose;

- Beribis modelis - Dvimatė erdvė transformuojama į toro formos paviršių;
- Gauso-Markovo modelis - mobilumo atsitiktinumo dydis reguliuojamas vienu parametru;
- Tikimybinis atsitiktinio vaikščiojimo modelis - naudojami tikimybiniai skirstiniai apskaičiuojant sekančias mazgų pozicijas;
- Miesto mobilumo modelis - modeliuojamos miesto gatvės bei judėjimas jose.

Kiekvienas mobilumo modelis turi savo parametrų rinkinį, kuriuo tyrėjai adaptuoja tiriamajai sričiai: nustatomi atsitiktinių kintamųjų rėžiai, apskaičiavimo metodikos. Tarkim atsitiktinio vaikščiojimo modelio pagalba galima imituoti tiek judančių žmonių, tiek judančių transporto priemonių tinklą. Abejais atvejais priskiriami skirtingi greičių ruožai, kuriuos gali įgyti kiekvienas mazgas. Tikimybiniam modeliui galima parinkti reikiamas tikimybines funkcijas, kurios ribotų mazgų krypties keitimąsi, taip priartinant visiškai chaotišką judėjimą prie realiame gyvenime sutinkamo judėjimo.

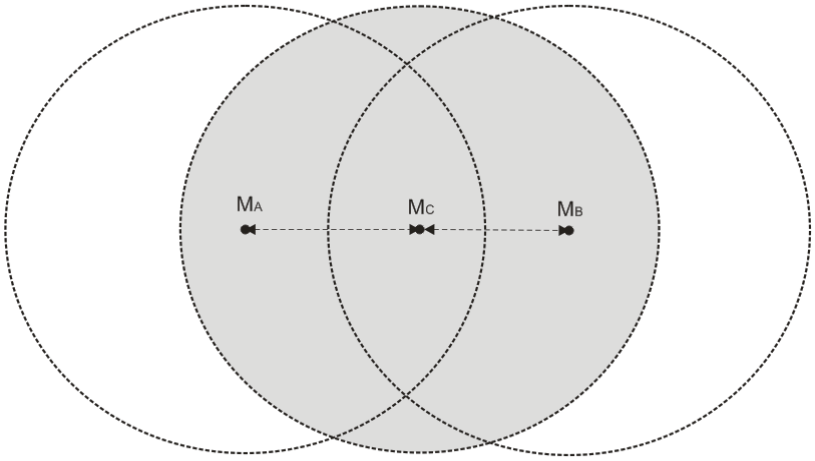
Mazgai mobiliuose dinamiškuose tinkluose gali prisijungti ir atsijungti nuo tinklo, nesutrikdydami viso likusio tinklo darbo. Tam reikalingas papildomas mazgų veikimo laiko modelis, parodantis veikimo ir prastovos laikotarpius. Tam naudojami tikimybiniai modeliai, kurie pagal pasirinktus skirstinius nustato kiekvieno mazgo veikimo trukmę modeliavimo metu.

Paminėti modeliai yra bendri judrumo ar veikimo laiko modeliai, labiausiai tinkami ad hoc tinklams, kurių pagalba galima konstruoti specifiniams tinklams reikiamus modelius. Pavyzdžiui mesh grupės tinklams, turintiems dalį stacionarios infrastruktūros vienu metu taikomi keli mobilumo modeliai. Vienai grupei mazgų taikomas statinis modelis, kuris reprezentuoja infrastruktūrinę tinklo dalį – paskirstymo tinklą. Šie mazgai pasižymi didele veikimo tikimybe, bet turi būti palikta ir prastovos tikimybė. Vartotojai, naudojantys infrastruktūrinę mesh tinklo dalį gali judėti pagal kitus modelius: atsitiktinius vaikščiojimo, miesto mobilumo ar kitus tikimybinius modelius, bei pasižymėti gana didele prastovos galimybe. Tuo tarpu sensoriniams tinklams gali būti taikomi visi judrumo modeliai, kadangi sensoriai gali būti įvairiuose tiek judančiuose tiek visiškai statiniuose objektuose. Prastovos tikimybė turi augti kartu su veikimo laiku, kadangi didėja išsikrovusios baterijos tikimybė. Taip kombinuojami modeliai priartinami prie realių aplinkybių.

2. Ad hoc tinklų maršrutizavimo algoritmai

Maršrutizavimo algoritmų pavyzdžių analizę, pradėsime nuo paprastų ad hoc tinklų analizės. Paketų srautų maršrutų sudarymas bei palaikymas yra viena didžiausių problemų, su kuriomis reikia susidoroti projektuojant šio tipo tinklus. Dinamiškoje aplinkoje bandoma

maksimizuoti pralaidumą taupant banginius bei energinius resursus. Optimalaus maršruto radimui su minimalios maršrutizavimo informacijos kiekiu problemos sprendimas pasiūlytas ne vienas. Pats paprasčiausias ad hoc tinko pavyzdys yra pateiktas iliustracijoje (Pav. 7).



Pav. 7. Bendravimas per tarpininką

Šioje iliustracijoje pavaizduoti trys lygiaverčiai įrenginiai. Nė vienas iš jų neveikia kaip prieigos taškas (angl. *access point*). Nors du įrenginiai M_A ir M_B negali užmegzti tiesioginio ryšio. Šiuo atveju abu įrenginiai gali užmegzti ryšį su tarp jų esančiu įrenginiu M_C. Jeigu tarpinis įrenginys M_C sutinka tarpininkauti M_A ir M_B įrenginių komunikacijoje, tai turime ad hoc bevielį tinklą kurio pagalba komunikuoja M_A ir M_B įrenginiai.

Įrenginys, inicijuojantis komunikacijos pradžią vadinamas siuntėju. Įrenginys su kuriuo siuntėjas nori užmegzti ryšį vadinamas gavėju. Procesas, kurio metu siuntėjas ieško kelio iki gavėjo yra kelio paieška. Siuntėjui išsiuntus kelio paieškos užklausą visiems kaimyniniams arba tik vienam įrenginiui pradedamas kelio paieškos procesas. Kaimyniniais įrenginiais vadinami visi įrenginiai, su kuriais analizuojamas įrenginys gali užmegzti tiesioginį ryšį (jie yra to įrenginio ryšio aprėpties zonoje). Pavyzdyje įrenginiui M_A kaimynas būtų tik įrenginys M_C. Tuo tarpu įrenginiui M_C kaimynai būtų M_A ir M_B.

Labai svarbi problema kuriant ad hoc tinklų maršrutizavimo protokolus yra kelio paieškos algoritmas. Tyrėjai ieško optimalių būdų kaip neperkraunant tinklo surasti kelią nuo siuntėjo iki gavėjo. Pateiktame pavyzdyje kelio paieška gana nesunkai išsprendžiama problema: siuntėjui M_A reikia sužinoti ar per vienintelį kaimyną M_C įmanoma rasti gavėją M_B. Šiuo atveju įrenginys M_A gali komunikuoti su įrenginiu M_B panaudodamas vienintelį tarpinį įrenginį. Dažniausiai realiuose tinkluose kyla sudėtingesnių problemų, nes įrenginiai gali keisti savo buvimo vietą, ar tiesiog atsijungti nuo tinklo. Tiriant tokio pobūdžio tinklus atstumai tarp įrenginių dažnai matuojami tarpinių mazgų skaičiumi (angl. hop count), kuris didesniuose tinkluose yra labai svarbus, bet ne vienintelis, rasto maršruto rodiklis.

Bet kurio automatinio maršrutų paieškos algoritmo tikslas - optimaliu maršrutu nugabenti paketus į tikslinį įrenginį. Labai svarbu vengti galimų kilpų maršrute, kai paketai ilgą laiką, ar be galo, keliauja tinklu bereikalingais mazgais. Atvejams, kai tinklo centre kyla susigrūdimo problemos, yra siūlomi sprendimai aplenkti labai apkrautas tinklo sritis [21]. Nors ir maršrutai kartais tampa ilgesni, bet bendras tinklo našumas kyla.

Daugiašuolių tinklų kelio paieškos algoritmus galima suskirstyti į dvi pagrindines grupes: pagal pareikalavimą (angl. on-demand) [6]arba pastovaus atnaujinimo [15]. Pirmieji maršrutus atnaujina tik tuomet kai jie yra reikalingi (paketai siunčiami naujam gavėjui, arba galėjo įvykti pasikeitimai tinklo topologijoje (dingo tarpininkas, atsirado geresnis maršrutas). Antrieji nepriklausomai nuo poreikio, pastoviai stebi tinklo pasikeitimus, ir bet kuriuo metu yra pasiruošę komunikuoti su bet kuriuo tinklo mazgu.

Pagal paketų persiuntimo krypties parinkimą, algoritmai gali būti skirstomi į šaltinio [15] ir krypties vektoriaus [6] algoritmus. Pirmuosiuose šaltinio mazgas nustato kuriuo maršrutu reikia siųsti paketą, ir šį maršrutą įveda į paketą. Kiekvienas tarpininkas analizuoja paketą, ir siunčia pagal po jo einančio mazgo adresą. Antrieji algoritmai remiasi laikinų (ar dalinai laikinų) lentelių saugojimu kiekviename tinklo mazge. Paketas siunčiamas artimiausiam kaimynui, o šis pagal savo atmintyje turimą informaciją sprendžia kur toliau paketas turi būti persiunčiamas, ar naujo maršruto paieška turi būti inicijuojama.

Kartais, ypatingai mesh tinkluose naudojami hierarchiniai maršrutizavimo algoritmai, kurie analizuodami paketą sprendžia, ar paketą perduoti kaimyniniams, to paties hierarchinio lygio mazgams, ar siųsti aukštesnio hierarchinio lygmens mazgui, kuris toliau maršrutizavimą vykdys savo lygmenyje.

Literatūroje [2, 5, 6, 8, 9, 14, 15] minimi du pagrindiniai kelio paieškos metodai: tinklo užliejimo (angl. flooding) bei vietos informacija paremti (angl. location aided) protokolai. Tinklo užliejimo algoritmų pagrindą sudaro kelio paieškos užklausos persiuntimas visiems savo kaimynams. Tokio tipo paieškose kiekviena naujo kelio paieška užlieja tinklą labai dideliu kiekiu duomenų, kurie reikalingi tik tinklo aptarnavimui. Metodai, kai maršruto paieškoje naudojama vietos informacija (pvz.: pagal GPS parodymus), padeda sumažinti tinklo aptarnavimui skirtų duomenų kiekį. Tai dažniausiai pasiekiama sumažinant įrenginių, reaguojančių į kelio paieškos užklausas.

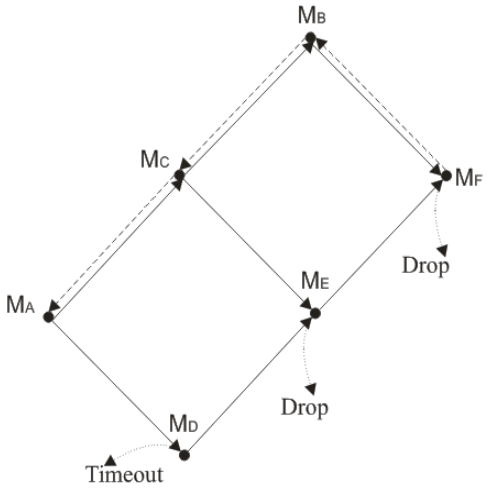
Kiekviena metodika turi savų trūkumų ir privalumų. Papildoma įranga, kaip GPS vartoja daugiau energijos, bei kelia įrenginio savikainą. Tai, galbūt, nėra pats tinkamiausias sensoriniam tinklui sprendimas, nors ad hoc tinklams neturėtų sudaryti jokių papildomų problemų. Mesh tinklai pasižymi daliniu stabilumu, kai aukštesnės hierarchijos mazgai

dažniausiai yra stabilūs. Šiuo atveju koordinačių kitimas daro mažesnę įtaką, ir daugiau stabilių maršrutų gali būti saugoma šiuose mazguose.

AODV

Ad hoc On Demand Distance Vector routing (AODV) algoritmas yra labai populiarus daugiašuolių tinklų maršrutizavimo protokoluose. Labai dažnai minimas literatūroje kaip atskaitos taškas lyginant skirtingus algoritmus bei yra įtraukiamas į naujai išleidžiamus standartus (kaip naujai išleistas IEEE 802.11s - wi-fi įrangos standartas mesh tinklams).

Šis algoritmas remiasi tinklo užliejimo [6] metodika. Priėmęs užklausos paketą (Rreq) gavėjas siunčia atgal siuntėjui atsakymo paketą (Rrep) tuo pačiu keliu, kokiu atkeliavo užklausos paketas. Šis kelias ir vadinamas maršrutu. Kad atsakymo paketas keliautų tuo pačiu maršrutu, AODV protokolą palaikantys įrenginiai turi specialią atmintinę, kurioje saugomi įrašai apie egzistuojančius maršrutus bei maršruto užklausas. Kad tarpinis įrenginys užtikrintų sėkmingą Rrep paketo grąžinimą, bei maršruto palaikymą, gavęs užklausos paketą Rreq į atmintinę įsirašo gavėjo IP adresą, įrenginio iš kurio atėjo paketas IP adresą, atgalinio maršruto galiojimo laiką, bei reikšmę *broadcast_id.* Pastaroji *broadcast_id* reikšmė skirta užtikrinti maršrutų naujumą, bei apsaugo nuo kilpų atsiradimo maršrute.



Pav. 8. Tinklo užliejimas

Pateiktame pavyzdyje įrenginys M_A nori užmegzti ryšį su įrenginiu M_F (Pav. 8). Tuomet įrenginys M_A siunčia užklausos paketą Rreq visiems kaimyniniams įrenginiams (M_C, M_D). Kiekvienas įrenginys gavęs užklausos paketą, patikrina ar jis nėra skirtas jam pačiam. Jeigu paketas skirtas ne M_C įrenginiui, tai jis vėlgi yra persiunčiamas visiems kaimyniniams įrenginiams (M_B, M_E). Jeigu įrenginys M_E visuomet persiuntinėtų tik gavęs Rreq paketus, tai tinklas niekuomet nenustotų persiuntinėti tų pačių užklausos paketų. Tam tikslui naudojama *broadcast_id* reikšmė. Siuntėjas siųsdamas naują užklausą vienetu padidina šią reikšmę ir ją

įdeda į Rreq paketą. Jeigu tarpinis įrenginys gauna daugiau nei vieną paketą su ta pačia *broadcast_id* ir gavėjo IP adreso reikšmėmis, tai apdoroja tik pirmąjį paketą, o visus kitus atmeta (angl. *drop*). Pateiktame pavyzdyje įrenginys M_E gauna Rreq paketus iš M_C ir M_D įrenginių, bet įrenginio M_D užklausa atmetama. Tas pats įvyksta ir įrenginyje M_F, kai šis atmeta M_E įrenginio užklausą. Abiem atvejais priimama prielaida, kad paketai iš M_C ir M_B įrenginių atėjo anksčiau. Kadangi įrenginio M_D persiųsta užklausa buvo atmesta, tai reiškia šis įrenginys nedalyvaus M_A ir M_F įrenginių bendravime ir jam nereikia saugoti jokios informacijos apie šį maršrutą. Šiam tikslui yra užklausų galiojimo laiko reikšmė, kuri nurodo kiek laiko laukti atsakymo paketo. Praėjus šiam laikui, visa informacija apie šiame įrenginyje buvusį Rreq paketą ištrinama.

Įrenginys M_F gavęs Rreq paketą patikrina ar jis yra gavėjas. Kadangi atsakymas yra teigiamas, tai šis generuoja ir siunčia atgal Rrep paketą tam pačiam įrenginiui iš kurio gavo Rreq paketą. Visi tarpiniai įrenginiai gavę RREP paketą ieško savo atmintyje įrašo su atitinkamu gavėjo bei *broadcast_id* įrašu, kad galėtų šį paketą persiųsti tam pačiam įrenginiui iš kurio buvo gautas Rreq. Persiuntę Rrep paketą tarpiniai įrenginiai papildo savo atmintį dar vienu įrašu apie egzistuojantį maršrutą ir jo galiojimo laiką.

Autorių teigimu [6] šis algoritmas sumažina bereikalingą informacijos dubliavimą, užtikrina apsaugą nuo kilpų susidarymo bei saugo tik reikšmingų maršrutų informaciją. Tai leidžia protokolą naudoti nemažos apimties tinkluose, bei taupyti įrenginių atmintį. Šis protokolas turi keletą praktinių realizacijų

3. Mesh tinklų maršrutizavimo algoritmai

Mesh tipo tinklų pagrindinė paskirtis - paskirstyta tinklo prieiga dideliam kiekiui vartotojų. Aukštus ryšio kokybės reikalavimus keliantys vartotojai, norintys naudotis tiek internetinės telefonijos, tiek vaizdo perdavimo paslaugomis kelia reikalavimus ne tik pralaidumui, bet ir ryšio stabilumui bei patikimumui.

Mesh tipo tinklai dažniausiai išnaudoja ne vieną, bet kelias belaides tinklo sąsajas. Taip paskirstymui naudojami mazgai galėti vienu metu išnaudoti kelis dažninius kanalus. Dažniausiai viena sąsaja skiriama vartotojų interneto prieigai, kitos sąsajos panaudojamos srautų paskirstymui tarp paskirstymo mazgų. Taip susijungę paskirstymo mazgai sudaro atskirą hierarchinį duomenų paskirstymo lygmenį, kuriame duomenys keliais skirtingais maršrutais gali pasiekti laidinę interneto prieigą.

Hierarchinis ryšio kanalų paskirstymas tinkle leidžia geriau išnaudoti tuos pačius dažninius kanalus. Vartotojų dažnis skiriasi nuo kitų hierarchinių tinklo lygmenų, taip netrukdomai perduodami duomenys tarp paskirstymo mazgų. Taip pat, vartotojai, esantys prie skirtingų

paskirstymo mazgų neužgožia vienas kito savo duomenimis, taip leisdami vienalaikį to pateies kanalo pakartotinį panaudojimą viename tinkle.

4. Sensorinių tinklų maršrutizavimo algoritmai

Esminis sensorinių tinklų išskirtinumas iš kitų rūšių daugiašuolių tinklų - tai į duomenis orientuoti tinklai. Pagrindinis tinklo tikslas yra surinkti sensoriaus užregistruotus ir sukauptus duomenis iš įvairių mobilių ar statinių taškų. Kadangi viso tinklo mazgai siunčia labai panašius duomenis, šie keliaudami tinklu gali būti agreguojami, tankinami ar kitaip apdirbami, kad pasiektų tinklui užbrėžtą pagrindinį tikslą - surinkti reikiamą informaciją.

Kadangi tai gali būti labai dideli tinklai, su labai dideliu kiekiu mazgų, įprasta mazgų adresacija praranda prasmę, dėl bereikalingai didelio atminties kiekio išnaudojamo šiam tikslui. Orientacija į duomenis leidžia mazgų adresaciją pakeisti duomenimis, kuriuos šie mazgai kaupia. Vienas iš galimų pavyzdžių, kad mazgo koordinatės, gali atstoti mazgo adresą. Gali būti netgi keli mazgai naudojantys tas pačias koordinates kaip savo adresą. Jeigu tinklo paskirtis yra kaupti duomenis apie temperatūrinius skirtumus iš didelio ploto, tai to paties taško temperatūrą gali matuoti ir keli mazgai, kas galutiniam rezultatui jokios įtakos neturi.

Dvi pagrindinės šių tinklų rūšys yra iniciatyvūs bei reaktyvūs. Pirmuoju atveju mazgai periodiškai persiunčia savo sukauptus duomenis, ar raportuoja savo būseną. Tai tinklai geriausiai tinkami pastoviam didelės sistemos stebėjimui. Antruoju atveju tinklo mazgai nedaro jokių veiksmų, kol nėra inicijuojami išorinių veiksnių, tokių kaip stebimos temperatūros iš anksto nustatytos slenkstinės reikšmės viršijimas. Šie tinklai tinkami įvairioms signalizacijoms ar apsaugos sistemoms.

Tinklo klasterizavimas labai padeda taupyti energiją. Kadangi dažniausiai sensoriniai tinklai yra sudaryti iš mazgų, naudojančių baterijas kaip vienintelį šaltinį. Aukščiau paminėti metodai leidžia sutaupyt nemažą kiekį energijos. Papildomai dar šių tinklų maršrutizavimo protokolai dažnai naudojasi klasterizavimo technika, kai visas tinklas automatiškai susiskirsto į atskirus klasterius. Kiekvienas klasteris turi vyriausiąjį mazgą, kuriam siunčiami duomenys. Šis duomenis agreguoja persiunčia duomenis į duomenų surinkimo mazgą. Gali būti ir kelių lygių hierarchija, kai klasterių vyriausieji mazgai susijungia į didesnius klasterius, kuriuose visi mazgai perduoda viso klasterio duomenis. Tokiu būdu duomenys yra apdorojami keliais lygiais, maksimaliai sumažindami siunčiamų duomenų kiekį.

Duomenų surinkimo mazgas dažniausiai turi pastovų energijos šaltinį, kurio pagalba gali naudoti daugiau energijos duomenų siuntimui. Taip jis gali tiesiogiai pasiekti visus tinklo mazgus. Tinklo mazgai taupydami energiją su surinkimo mazgu komunikuoja tik per klasterių

vyriausiuosius mazgus. Tai vadinama asimetrinė komunikacija, kurios pagalba taupomi tiek energiniai tiek dažniniai resursai.

Sensorinių tinklų traktavimas kaip duomenų surinkimo tinklas palengvina daugelį maršrutizavimo klausimų, leidžia panaudoti įvairias strategijas, tokias kaip duomenų agregavimas ar reaktyvus duomenų perdavimas. Šie metodai ne tik taupo energiją, bet ir mažina eterio taršą.

Apibendrinimas

Beveik visuose daugiašuoliuose tinkluose ir maršrutizavimo lygmenyje daromi sprendimai, kurie minimizuoja tinklo kaštus. Į šiuos kaštus įeina suvartojamos energijos taupymas, duomenų agregavimas bei dažninių kiekio optimizavimą. Srautų agregavimas, naudojamų tinklo sąsajų kiekio mažinimas bei jų optimalus panaudojimas bendrame šių tinklų kontekste atsiremia tiek į sutapytus fizinius resursus, tiek geriau išnaudotus išorinius resursus, kaip panaudotas radijo bangų diapazonas.

III. Modeliavimas

Dideli belaidžiai tinklai susiduria daugybe problemų trukdančių juos panaudoti praktikoje. Dabartiniuose GSM ar WiMax tinkluose dažnių paskirstymu rūpinasi ryšio operatorius. Į korius suskirstytose zonose gali būti skirtingi iš anksto parinkti dažniniai kanalai, tarp kurių nepasireiškia interferencijos reiškinys. Visiškai kitaip yra su daugiašuoliais tinklais - dabartinės technologijos leidžia naudoti tik vieną dažninį kanalą vienam tinklui. Dėl šios priežasties labai stipriai nukenčia bendras šios kartos tinklo pralaidumas.

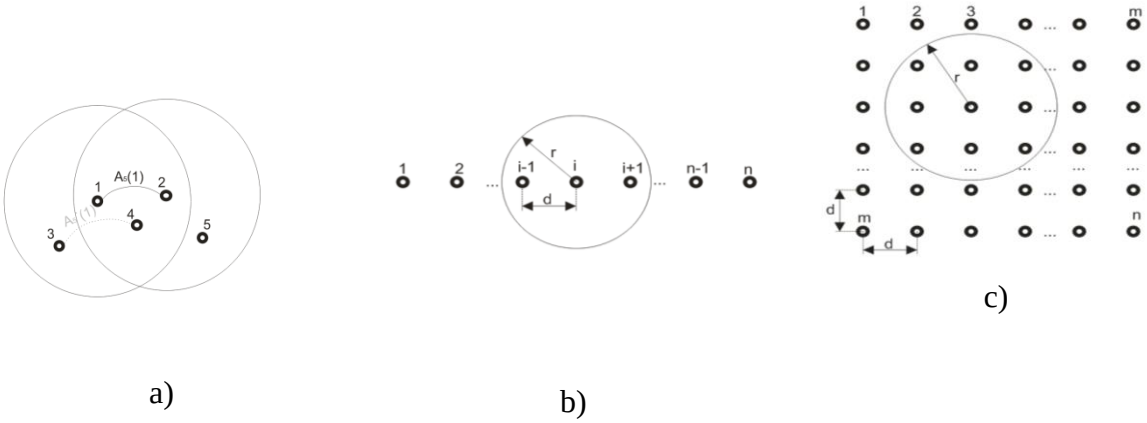
Jeigu visi tinklo mazgai yra labai arti, tai vienu metu gali siųsti informaciją tik vienas mazgas. Kai tinklo mazgai yra nutolę, keli tinklo mazgai vienu metu gali siųsti informaciją. Siuntimo laikų suderinimo algoritmas atitinka IEEE 802.11g standartą [13]. Tokių tinklų pralaidumo priklausomybės nuo mazgų skaičiaus tirtos P. Gupta ir P.R. Kumar darbe [7]. Tyrimai atlikti atsitiktinės topologijos tinkle ir nustatyta, kad pralaidumas į atsitiktinai pasirinktą tinklo įrenginį kinta pagal $\theta\left(\frac{W}{\sqrt{n \log n}}\right)$ dėsnį, naudojant neinterferuojant įprotokolą. Pateikiamo tyrimo tikslas yra nustatyti, kiek daugiausia gali būti tinklo mazgų porų *k*, kurios gali netrukdomai komunikuoti apibrėžtos topologijos tinkle.

1. Ad hoc tinklo mazgų interferencija

Gretimi tinklo mazgai gali tarpusavyje komunikuoti atstumu, kuris priklauso nuo siunčiamo signalo galios, moduliacijos rūšies ir mazgo imtuvo jautrumo. Ryšio nuotolis r gali kisti nuo 35m (patalpose) iki 95m (laisvoje erdvėje) [13]. Visi aplinkiniai įrenginiai, esantys atstumu $d<r$ nuo siunčiamo mazgo, gali priimti mazgo signalą.

Skirtingų mazgų porų interferencijos zonų pavyzdys, kai signalus siunčia mazgas 1 ir mazgas 2, parodytas Pav. 9a. Jeigu tinklo mazgai išsidėstę vienoje tiesėje (Pav. 9, b.), i-ojo mazgo signalai pasiekia i-1-ąjį ir i+1 -ąjį mazgus ir nepasiekia likusių mazgų. Jeigu tinklo mazgai išsidėstę vienodu *d* atstumu plokštumoje (Pav. 9c) į aprėpties zoną patenka 8 mazgai. Jei maksimalią linijinę perdavimo spartą pažymėsime *w*, tinklo mazgų kiekį - n, tai vienam tinklo mazgui vidutiniškai tenkantis srautas

$$\lambda = k\frac{w}{n} \qquad (1)$$



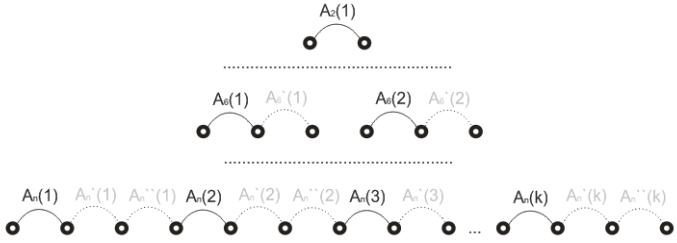
Pav. 9. interferencijos zonų išsidėstymas: a) Penkių mazgų tinkle, b) linijinės topologijos (1xn) tinkle, c) Plokštuminės topologijos (n=mxm) tinkle

2. *Neinterferuojančių mazgų porų suradimo metodika*

Tyrime analizuojami dvejų topologijų tinklai: linijinės bei gardelės. Linijinės topologijos tinklas - viena eile vienodais atstumais išdėstyti mazgai. Ši topologija primena VANET tinklų atvejus, kai automobiliai važiuoja ilgais keliais, nekintančiais atstumais tarp savęs. Gardelės topologijos tinklas - kvadrato formos tarpusavyje vienodais atstumais išdėstyti mazgai. Analizėje nenagrinėjami tarpusavyje padėtį keičiantys mazgai, todėl ši tinklo topologija artimiausia WSN tinklams - didelis kiekis tarpusavyje susijungusių, bei nejudančių įrenginių.

Linijinės topologijos tinklas

Linijinės topologijos tinklo atveju neinterferuojančių mazgų porų skaičiaus iliustracija, kai *d=r,* pateikta Pav. 10. Kai tinkle yra tik du mazgai, galima tik viena neinterferuojanti pora. Šešių mazgų atveju galimos tik dvi neinterferuojančios poros: $A_6(1)$ ir $A_6(2)$ arba $A`_6(1)$ ir $A`_6(2)$. Analogiškai pavaizduotos poros iš *n* tinklo



Pav. 10. Naujas srautas tiesėje

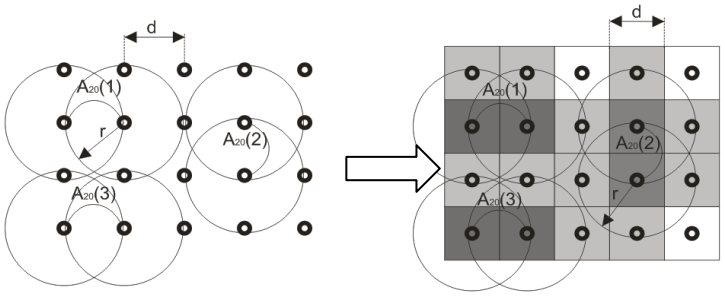
mazgų sudarytame tinkle. Jeigu tinklas proporcingai traukiasi mažėjant *d,* interferencija apima vis didesnį kiekį mazgų ir trukdo lygiagrečiai vykdyti siuntimą. Dėl to vis mažėja komunikuojančių porų skaičius kol gali sąveikauti tik viena pora. Porų skaičius *k* linijinės topologijos tinkle

$$k = \left\lfloor \frac{n}{\left\lfloor \frac{r}{d} \right\rfloor + 2} \right\rfloor \qquad (2)$$

Čia: $\lfloor X \rfloor$ reiškia sveikąją skaičiaus dalį.

Plokštuminės topologijos tinklas

Neinterferuojančių porų suradimui pasirinktas kvadratinės topologijos tinklas. Tinklo aprėpiamas plotas sudarytas iš elementarių kvadratų. Kiekvienas kvadratas gali turėti tris būsenas: siuntėjo, interferencijos ir laisvąją. Siuntėjo būsena pavaizduota tamsiai (Pav. 11) Kvadratai, kurių centrai yra užgožiami siuntėjų signalu, įgauna interferencijos būseną (Pav. 11). Nauji ryšiai gali būti sudaromi tik iš laisvųjų zonų, pažymėtų balta spalva (Pav. 11). Specialiai sudaryto algoritmo pagalba kvadratai išdėstomi taip, kad gauti didžiausią siuntėjų skaičius *k*.



Pav. 11. Neinterferuojančių porų paieška plokštuminiame tinkle

3. Neinterferuojančių porų paieškos algoritmas

Paieškos algoritmas paremtas tuo, kad atsitiktiniu būdu parenkame kiekviena porą ir apie ją nustatome interferencijos zoną. Atsitiktinai generuojant mazgų koordinates surandamos poros, kurios nepatenka į kitų porų interferencijos zonas. Algoritmas (Lentelė 5) kartojamas tiek kartų, kol surastas didžiausias porų skaičius toliau nekinta. Algoritme panaudoti tokie žymėjimai:

l- algoritmo kartojimo skaičius,

`kiekRysiu(tinklas)` –tinkle surastų neinterferuojančių porų skaičius,

`generuoti(dydis)` – atsitiktinių koordinačių reikšmės,

`dydis` – tinklo mazgų skaičius (n=mxm),

`apreptis` –

`maxRysiai` – tinkle surastų neinterferuojančių porų didžiausias skaičius,

`rysiu_kiekis(dydis, apreptis)`- funkcija, atsitiktinai sugeneruojanti ryšius tarp tinklo įrenginių,

`LAISVA` – kvadrato būsena,

Lentelė 5. Algoritmas

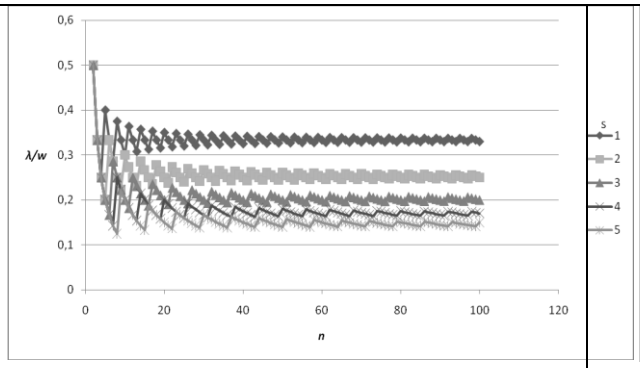
```
rysiuKiekisTikslus(dydis, apreptis)
  for i:=1,l {
    rysiai = rysiu_kiekis(dydis, apreptis);
    if (rysiai > maxRysiai)
      maxRysiai = rysiai;
  }
return maxRysiai

rysiu_kiekis(dydis, apreptis)
  rnd1:=generuoti(dydis);
  rnd2:=generuoti(dydis);
  for i:=1,dydis
    for j:=1,dydis
      if (tinklas[rnd1[i]][rnd2[j]] == LAISVA)
        naujasRysys(tinklas, rnd1[i], rnd2[j]);
return kiekRysiu(tinklas);
```

`generuoti(dydis)` – grąžina masyvą, kuriame saugomi atsitiktine tvarka išdėlioti skaičiai nuo 1 iki dydis. Taip generuojama atsitiktinė vieta, kurioje kuriamas naujas ryšys, bet tuo pačiu patikrinami visi tinklo mazgai, ar juose gali būti sukuriamas naujas ryšys.

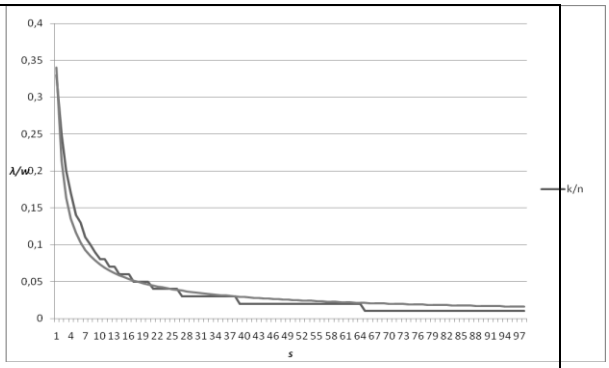
`naujasRysys(tinklas, i, j)` – atsitiktinai parenka laisvą kaimyninį langelį, langeliui i, j, su kuriuo gali būti užmezgamas ryšys. Šios funkcijos atsitiktinumo dėka, kiekvieną kartą gaunamas vis kitoks ryšių tinkle išdėstymas.

Tinklo dydžio ir mazgų tankio įtaka neinterferuojančių porų skaičiui

Linijinės topologijos tinklo neinterferuojančių porų skaičiaus priklausomybė nuo mazgų skaičiaus ir jų išsidėstymo tankio pavaizduota Pav. 12. Kiekviena linija atitinka skirtingą mazgų tankį. Galima padaryti išvadą, kad nuo mazgų skaičiaus n=20 toliau didėjant jų skaičiui, santykis λ/w išsidėsto apie pastovią reikšmę, būdingą atitinkamam tankiui. Pačiu geriausiu atveju, kaip aprėpties spindulys r yra lygus atstumui tarp gretimų mazgų d, tik kas trečias mazgas gali sudaryti mazgų porą (λ/w =0,33). Vienam tinklo mazgui tenkančios santykinės spartos λ/w priklausomybė nuo tinklo mazgų išsidėstymo tankio $s= r/d$ linijinės topologijos tinkle, sudarytame iš 100 mazgų, priklausomybė pateikta Pav. 13. Pradžioje pastebimas labai greitas neinterferuojančių mazgų porų skaičiaus kitimas. Kai visi mazgai patenka į vieną aprėpties zoną, tada neinterferuojančių mazgų porų skaičiaus k=1. Šis kitimas gali būti aproksimuotas priklausomybe



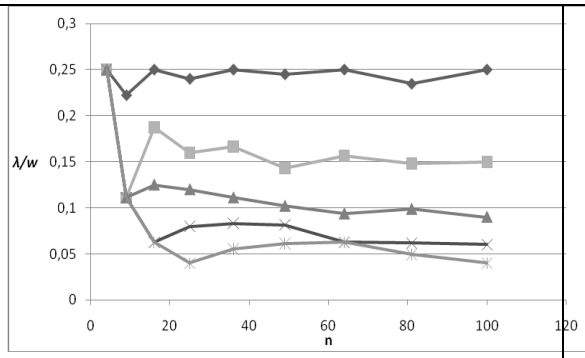
Pav. 12. Linijinio tinklo santykinio pralaidumo priklausomybė nuo mazgų skaičiaus ir jų išsidėstymo



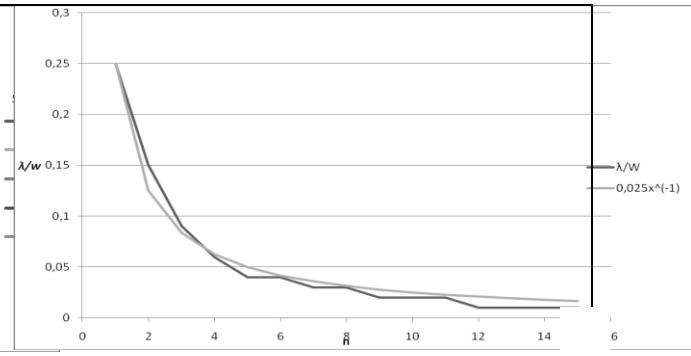
Pav. 13. 100 mazgų linijinio tinklo santykinio pralaidumo priklausomybė nuo mazgų

$$\frac{\lambda}{w}=\frac{k}{n}=\frac{0{,}34}{\sqrt[3]{s^2}},\ \text{kai}\ \frac{\lambda}{w}>\frac{1}{n}$$

Plokštuminės kvadratinės topologijos tinklo neinterferuojančių porų k priklausomybė nuo tinklo dydžio ir tinklo mazgų išsidėstymo tankio prie pastovios aprėpties zonos parodyta 7 pav. Prie minimalaus mazgų išsidėstymo tankio s=r/d=1, neinterferuojančių porų santykinis dydis lygus *λ/w = 0,25,* o didėjant tankiui vis mažėja (Pav. 14), kol pasiekia ribinę reikšmę *λ/w =0,01*. Neinterferuojančių porų santykio kitimas 100 mazgų dydžio tinkle pateiktas Pav. 15. Šis kitimas gali būti aproksimuotas priklausomybe



Pav. 14. Plokštuminio tinklo santykinio pralaidumo priklausomybė nuo mazgų skaičiaus ir jų išsidėstymo tankio



Pav. 15. 100 mazgų plokštuminio tinklo santykinio pralaidumo priklausomybė nuo mazgų išsidėstymo tankio

$$\frac{\lambda}{w}=0.25\frac{1}{s},\ \text{kai}\ \frac{\lambda}{w}>\frac{1}{n}$$

Lyginant linijinės ir plokštuminės topologijos tinklų pralaidumo priklausomybes, gauname, kad linijinės topologijos tinkle pralaidumas mažėja sparčiau.

4. Tinklų simuliacija ns3 tinklo modeliavimo įrankiu

Aprašytų tinklų modeliavimui buvo naudotas ns-3 [20]yra atviro kodo internetinių sistemų simuliatorius. Tai beveik visiškai atnaujinta jo populiariojo pirmtako ns-2 versija. Šie įrankiai pirmiausiai yra taikomi tyrimų bei mokymosi tikslais. Atviro kodo ideologija leidžia turėti visą programinį kodą savo kompiuteryje ir netrukdomai modifikuoti, norint sudaryti norimą tyrimų aplinką.

Tyrimui buvo parinktas tinklo statinis modelis. Vieno paketo siuntimo laikotarpiu (iki ~1ms) realių tinklų mazgo poslinkis yra labai mažas, ir neįtakoja persiuntimo kokybės. Mobilumo įtaka jaučiama tik stebint ilgesnius laiko tarpus, kai atsiranda poreikis keisti perdavimo spartą, ar dėl spartos neatitikimų sugadinami perduodami paketai. Tyrimu bandoma išsiaiškinti, ar pateiktuose skaičiavimuose padarytos prielaidos, apie maksimalią galimą santykinę tinklo pralaidumo reikšmę buvo padarytos teisingos. Statinis modelis leidžia sumažinti papildomų klaidų ar perdavimo trikdžių galimybes vienalyčiame tinkle, kadangi dėl šių priežasčių kylantys perdavimo trikdžiai nėra tyrimo objektas.

Tyrimai buvo atliekami naudojant IEEE 802.11g [13] belaidės įrangos standarto modelį. Šio standarto parinkimą lėmė jo populiarumas vartotojų, bei daugiašuolių tinklų tyrėjų tarpe. Populiarumo poreikis labai svarbus norint palyginti gaunamus rezultatus su kolegomis.

Spartos valdymo algoritmas

Kai kuriuose eksperimentuose naudojamas automatinis spartos parinkimo algoritmas. IEEE 802.11g standarte naudojama OFDM (angl. orthogonal frequency-division multiplexing) moduliacija. Nors standarto aprašyme dažniausiai pateikiama tik maksimali 54Mbps sparta, esant prastesnėms ryšio sąlygoms ar didesniems nuotoliams automatiškai parenkamos ir lėtesnės spartos moduliacija (galimi variantai: 6, 9, 12, 18, 24, 36, 48 ar 54 Mbps), kurios yra atsparesnės trikdžiams.

Tinklo įrenginio tvarkyklė pagal joje realizuotą algoritmą stebi reikiamus parametrus. Pagal šiuos parametrus parenkama sparta kuria bus vykdoma komunikacija tarp mazgų. Labiausiai paplitęs Linux OS tvarkyklių spartos parinkimo algoritmas yra Minstrel [10]. Tai euristiniais metodais paremtas algoritmas reaguojantis ne tik priimamo signalo stiprumo rodiklį. Pagal atliktus praktinius tyrimus, tai vienas geriausių algoritmų [10].

Tarp dvejų įrenginių siunčiamas paketas turi tam tikrą tikimybę būti sėkmingai pristatytas. Tikimybės funkcija turi keletą nežinomų kintamųjų: atstumas tarp įrenginių, atspindžių efektas, išorinė interferencija. Įrenginiai gali būti naudojami įvairiose aplinkose, kuriose šie

kintamieji išlieka nežinomi. Taip pat neaišku ir kuris kintamasis labiausiai įtakos sėkmingo persiuntimo tikimybę. Netgi nežinoma kokio tipo interferencija egzistuoja tarp įrenginių. Jeigu interferencija yra pulsuojanti, tuomet greitesni paketai (siunčiami didesne sparta) turi didesnę tikimybę būti sėkmingai perduoti. Turint tai omenyje buvo nuspręsta kad persiuntimo tikimybė naudojant vieną spartos reikšmę nėra priklausomas nuo kita sparta siunčiamų paketų persiuntimo tikimybės.

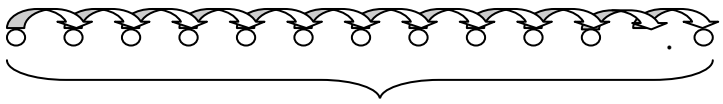
Atmintyje saugoma lentelė su įrašu kiekvienam įrenginiui, su kuriuo buvo komunikuojama bei išvestinė spartos reikšmė, kuri išvedama ilgainiui komunikuojant su atitinkamu įrenginiu. Komunikacijos metu, kas nustatytus laiko intervalus yra bandomos kitos spartos, kurių sėkmės tikimybė taip pat aukšta, ir persiuntimo rodikliai nenusileidžia dabartiniams. Taip, išbandomos kitos spartos reikšmės, kurios gali pagerinti perdavimo rezultatus. Pagerėjus rezultatams atnaujinamos reikšmės lentelėje, ir didžiąją dalį komunikacijai skirto laiko naudojama naujoji reikšmė.

Linijinės topologijos tinklas

Kintanti moduliacija

Modeliuojamas realus belaidis tinklas, su IEEE801.11g standarto įrenginiais. Pirmajame eksperimente 100 įrenginių išdėliojami eile vienodu atstumu vienas nuo kito. Atstumas keičiamas nuo 10 iki 300 ilgio vienetų (metrų) 10 metrų žingsniu.

Eksperimento įrenginiai naudojosi tik statiniais maršrutais, įdiegtais prieš matavimų pradžią. Paketai siunčiami tik artimiausiems kaimynams. Pirmasis įrenginys siunčia srautą į antrąjį, antrasis į trečiąjį ir t.t. (Pav. 16). Taip stengiamasi pasiekti maksimalų eterio išnaudojimą duomenų persiuntimui. Siunčiami 2000 bitų dydžio UDP paketai.

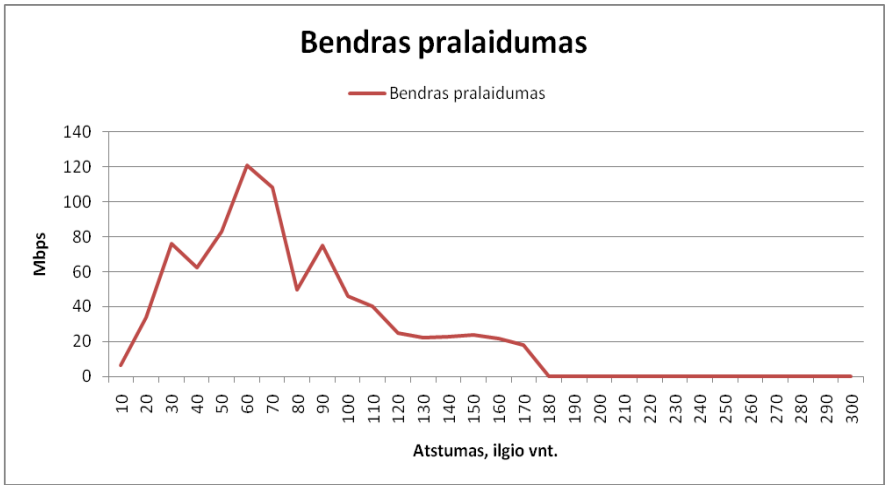


Pav. 16. Tinklo topologija. Srautai

Šio eksperimento metu įrenginių duomenų perdavimo sparta buvo automatiškai reguliuojama panaudojant Minstrel spartos parinkimo algoritmu.

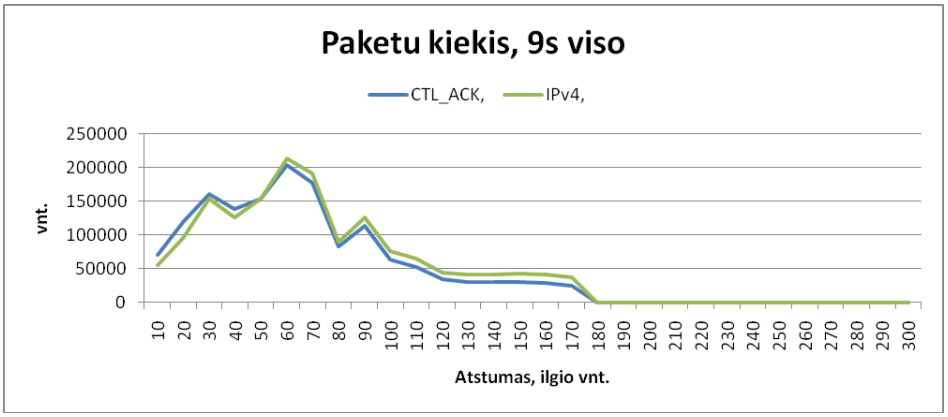
Bandymo trukmė 10 sekundžių. Pirmosios sekundės duomenys į statistiką neįtraukiami, nes startavus įrenginiams pirmąją sekundę įrenginiai elgiasi nestabiliai. Šis nestabilumas iškraipytų tyrimo statistiką.

Bendras pralaidumas - kiek duomenų visame tinkle buvo persiųsta per vieną sekundę. Jeigu per sekundę 5 įrenginiai persiuntė po 20 Mbit duomenų, tuomet bendras tinklo pralaidumas būtų 5*20=100 Mbit. X ašyje (Pav. 17) atidėta atstumas tarp gretimų mazgų. Grafike išsiskiria atitinkamas atstumas, kai visas tinklas dirba efektyviai. Pateikti skaičiai rodo viso tinklo siuntimo spartos sumą. Kadangi yra 100 įrenginių, tai padalijus šį skaičių iš 100 gautume vieno įrenginio išsiųstos informacijos kiekį.



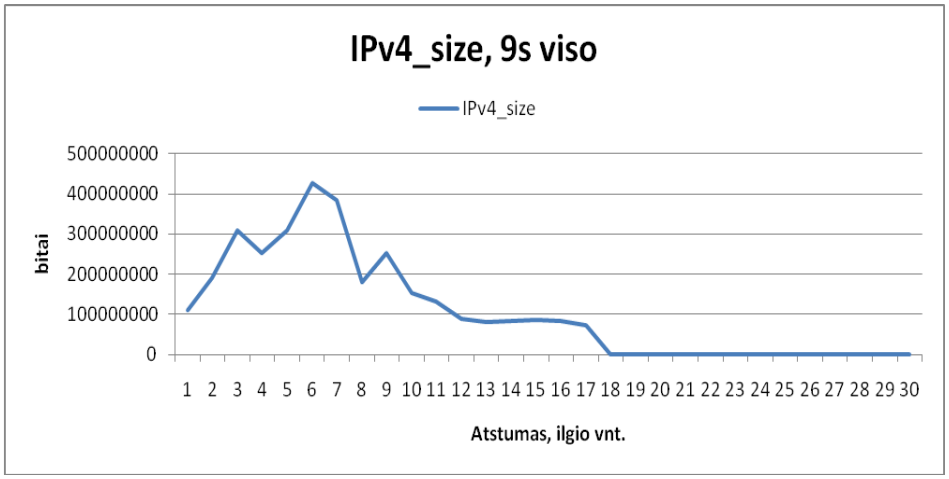
Pav. 17. Suminis linijinio tinklo pralaidumas

Taip pat buvo analizuotas persiunčiamų IP paketų, bei kontrolinių paketų (CTL_ACK) skaičius (Pav. 18). Kadangi naudojami pastovaus dydžio UDP paketai, taigi jų kiekis yra proporcingas vidutinei perdavimo spartai. Šie skaičiai labai panašūs (grafiko forma ta pati, tik skiriasi matavimo vienetai), tolimesniuose eksperimentuose šie rodikliai neanalizuojami.



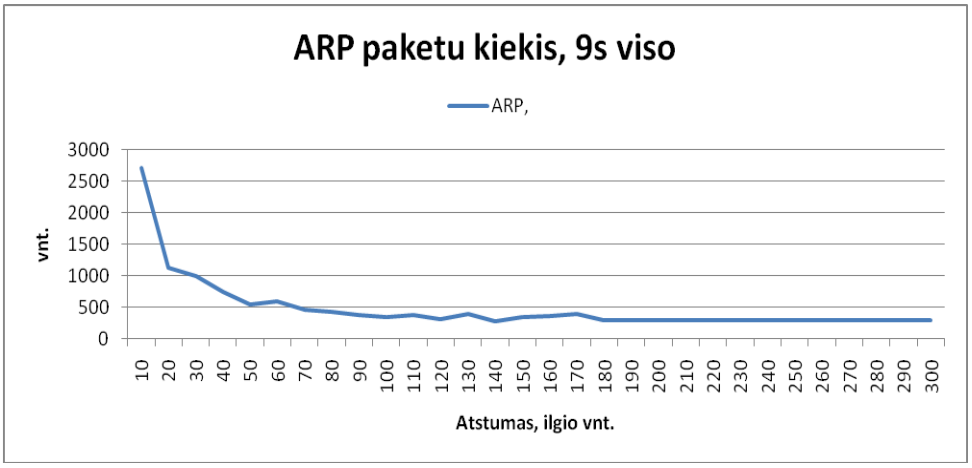
Pav. 18. Linijinio tinklo paketų analizė

IPv4_size dydis Pav. 19 atvaizduoja kiek per eksperimentą buvo persiųsta naudingos (angl. payload) informacijos. Vėlgi kreivės forma atitinka prieš tai buvusiąsias. Šie duomenys naujos informacijos nesuteikia - tolimesnėje tyrimo eigoje į juos bus neatsižvelgiama.



Pav. 19. Linijinio tinklo suminis paketų dydis.

Visiškai kitokia situacija su išsiųstų/priimtų ARP paketų kiekiu - šis ženkliai krenta didėjant atstumui tarp įrenginių (Pav. 20). Tai pasireiškia dėl to, kad kiekvieną ARP užklausą priima visi galintys įrenginiai. Taigi vieną išsiųstą paketą užregistruoja didelis kiekis mazgų. Didėjant atstumui šis skaičius sparčiai krenta žemyn - kol užklausas gali priimti tik gretimi mazgai.



Pav. 20. Linijinės topologijos tinklo ARP paketų kiekis

ARP paketų dydis visiškai neįtakojo bendro tinklo pralaidumo. ARP paketų kiekis dauguma atvejų neviršija 500 vnt per 10 sekundžių tyrimo. Tuo tarpu vis dar egzistuojant ryšiui tarp gretimų mazgų, bendras persiųstų paketų kiekis tinkle beveik siekdavo 5000 vienetų. ARP paketo vidutinis dydis yra apie 42 baitus, tuo tarpu šiame tinkle buvo siunčiami 2000 dydžio paketai. Pagal šiuos skaičius darėme išvadą, kad ARP paketai taip pat neįtakoja bendro tinklo pralaidumo rezultatų.

Linija išdėstytų mazgų vidutinio pralaidumo priklausomybė nuo tankio.

Pagal skyriaus pradžioje darytų skaičiavimų schemą buvo tirta realaus 100 mazgų tinklo santykinis pralaidumas. Santykinis pralaidumas - vienam mazgui tenkančio visame tinkle persiųstos informacijos kiekio dalis [4].

IEEE 802.11g standarte naudojama OFDM moduliacija. Galima parinkti vieną iš 8 spartos variantų: 6, 9, 12, 18, 24, 36, 48, bei 54 Mbps. Tyrimas buvo atliekamas su visomis šiomis moduliacijomis (atininkamai pavadinimai: ErpOfdmRate6Mbps, ErpOfdmRate9Mbps, ErpOfdmRate12Mbps, ErpOfdmRate18Mbps, ErpOfdmRate24Mbps, ErpOfdmRate36Mbps, ErpOfdmRate48Mbps, ErpOfdmRate54Mbps parinkimai ns3 simuliatoriuje).

Vienam įrenginiui tenkantis pralaidumas, w

Pirmiausia simuliatoriaus aplinkoje buvo ištirtas maksimalus mazgo pralaidumas. Tyrimo aplinka: Du įrenginiai pastatomi nedideliu (20 m) atstumu vienas nuo kito, siunčiamas maksimalus srautas (vienodo, 2000 baitų dydžio paketai). Tyrimo trukmė 10 s. Apskaičiuojamas vidutinis vienam mazgui tenkantis pralaidumas per sekundę (*w*).

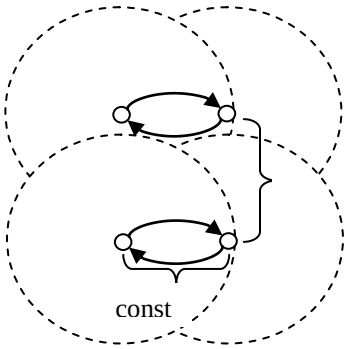
Tyrimo rezultatai pateikiami Lentelė 6. Stulpelyje "Bendras pralaidumas" pateikiama suminė abejų įrenginių perdavimo sparta per sekundę. Antrajame stulpelyje ši suma padalinama iš dvejų, kad galima būtų identifikuoti maksimalią siuntimo spartą tenkančią vienam įrenginiui *w*.

Lentelė 6. Maksimalus pralaidumas, 2 įrenginiai

Moduliacija	**Bendras pralaidumas**	**vienam įrenginiui, w**
ErpOfdmRate6Mbps	5,25	2,6261
ErpOfdmRate9Mbps	7,43	3,714745
ErpOfdmRate12Mbps	9,66	4,832405
ErpOfdmRate18Mbps	13,38	6,69155
ErpOfdmRate24Mbps	16,50	8,25065
ErpOfdmRate36Mbps	21,90	10,9478
ErpOfdmRate48Mbps	25,86	12,9298
ErpOfdmRate54Mbps	27,65	13,8239

Interferencijos atstumas, R

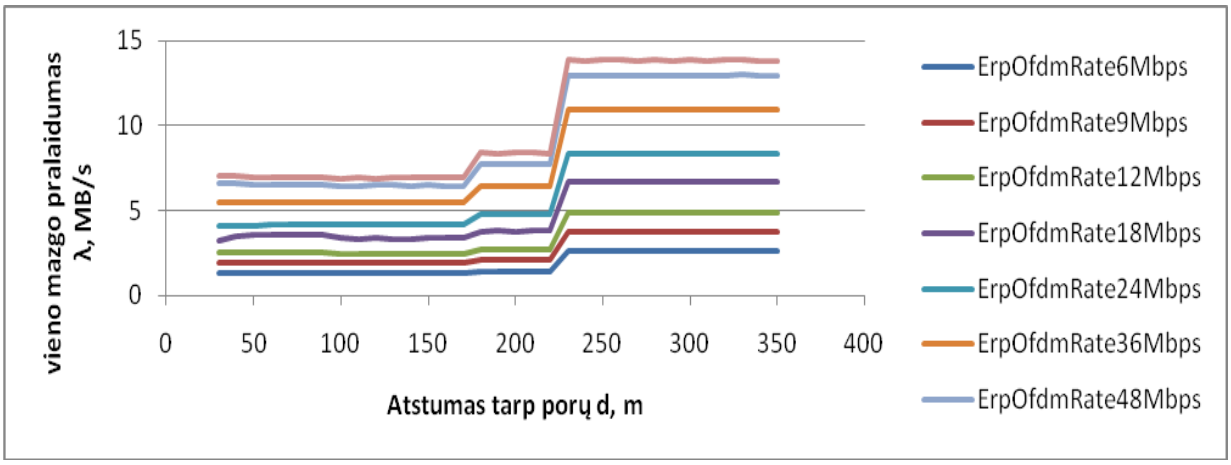
Remiantis anksčiau aprašytu modeliu, ns3 simuliatoriuje ieškomas interferencijos zonos dydis. Interferencijos zonos dydis, tai yra atstumas kuriuo nutolę mazgai visiškai neįtakoja vienas kito perduodamų srautų.



Pav. 21. Interferencijos tyrimas

Tyrimui atlikti buvo analizuojami dvejų mazgų porų srautai. Atstumas tarp porų buvo keičiamas, paliekant tą patį atstumą tarp poroje esančių mazgų. Schema pavaizduota paveiksle Pav. 21., kur d - kintantis atstumas, o „const“ pažymėtas atstumas nekinta.

Tyrimo rezultatai pateikiami grafike Pav. 22. X ašyje pažymėtas atstumas tarp porų d, Y ašyje pažymėtas pralaidumas, tenkantis vienam mazgui. Tyrimo tikslas - rasti minimalų atstumą, kuriuo nutolusios mazgų poros gali komunikuoti maksimalia sparta.



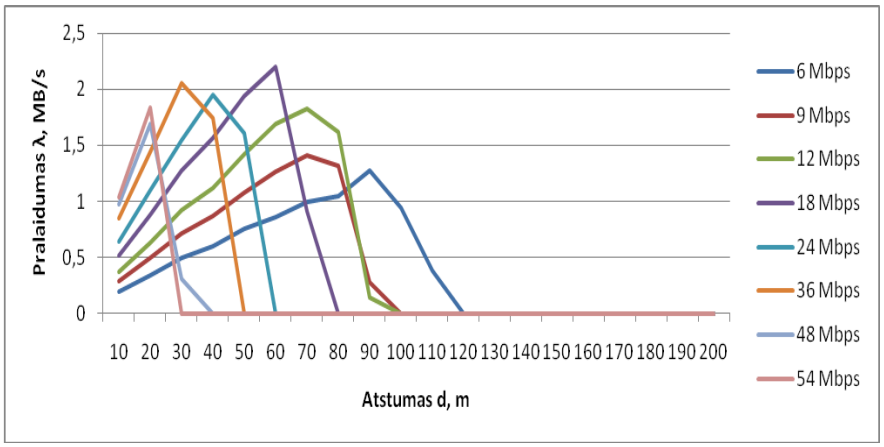
Pav. 22. Interferencijos zonos R tyrimas

Atlikus tyrimą buvo pastebėta, kad nepriklausomai nuo moduliacijos interferencijos zonos dydis R išlieka tas pats - R=230. Tai šiek tiek kelia abejonių ns-3 simuliatoriaus naudojamu interferencijos modeliu, kadangi dauguma įrenginių negali siųsti tuo pačiu galingumu naudodami skirtingas moduliacijas (kuo aukštesnė moduliacijos sparta, tuo sudėtingiau aukštu dažniu siųsti duomenis).

Pastovi moduliacija

Tyrimo schemoje apskaičiuoti viena linija išdėstytų 100 mazgų tankio ir vienam mazgui tenkančio pralaidumo sąryšis. Buvo prieita išvados, kad santykinis pralaidumas, tenkantis vienam mazgui yra atvirkščiai proporcingas mazgų tankiui. Santykinis pralaidumas skaičiuojamas pagal formulę $\frac{\lambda}{w}$, kur λ - vienam mazgui tenkantis pralaidumas, o w - maksimalus to mazgo pralaidumas. Šis santykis parodo kurią srauto dalį mazgas gali išnaudoti (vidutiniškai). Mazgų tankis taip pat santykinis dydis $s = \frac{R}{d}$, kur R - interferencijos zonos dydis, o d - atstumas tarp mazgų.

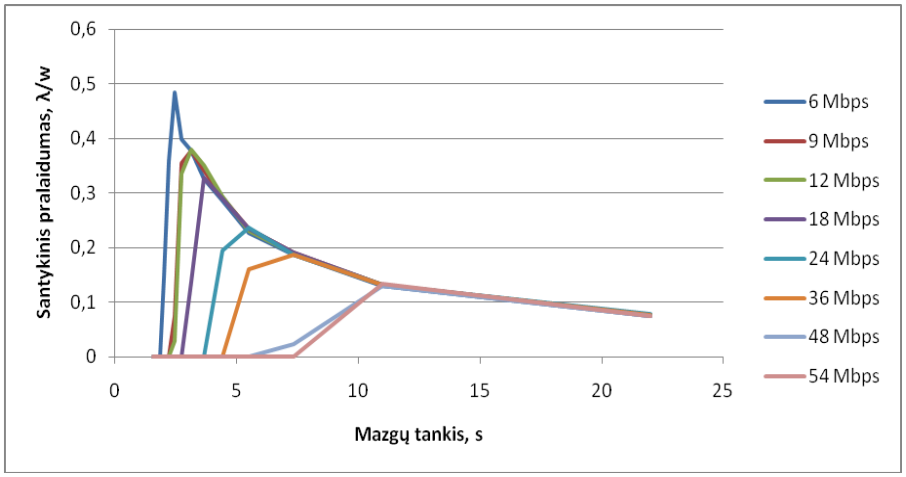
Atlikus eksperimentą su pastoviomis moduliacijomis buvo stebimi kaip keičiant moduliaciją bei atstumus tarp mazgų kinta pralaidumas, tenkantis vienam mazgui. Rezultatai pateikiami Pav. 23 grafike.



Pav. 23. Pralaidumas pagal atstumą d

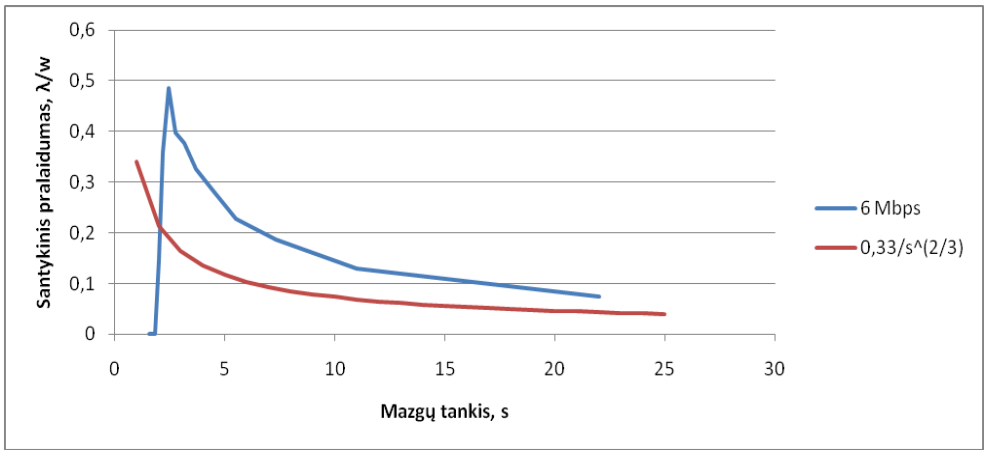
Rezultatų grafike matoma įdomi tendencija: didėjant atstumui tarp mazgų, kyla vienam mazgui tenkantis pralaidumas. Ši tendencija atsiranda dėl mazgų tankio mažėjimo: esant mažesniam tankiui, atsiranda galimybė pakartotinai išnaudoti tą patį dažnį. Mazgai, neesantys kitų mazgų komunikacijos sukeltoje interferencijos zonoje, gali netrukdomai komunikuoti.

Apibendrinant šių tyrimų rezultatus gauti duomenys buvo suvesti į vieną grafiką: linijinio tinklo santykinės spartos priklausomybė nuo tankio s. Rezultatai pateikiami grafike Pav. 24. Aiškiai matoma labai panaši tendencija į numatytąją.



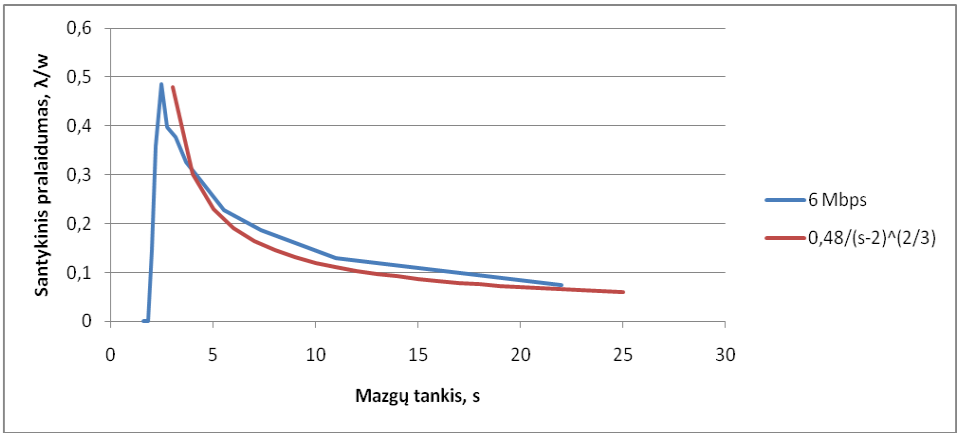
Pav. 24. Santykinio pralaidumo priklausomybė nuo tankio. Visos moduliacijos

Kadangi visos gautos kreivės Pav. 24 įgauna tą pačią formą, tik skirtingu metu, tikslinga analizuoti tik vieną. Tam tikslui buvo parinkta 6 Mbps kreivė, turinti didžiausią kiekį taškų, ir padengianti visas kitas moduliacijas.



Pav. 25. Teorinės kreivės palyginimas su 6Mbps gautais rezultatais

Įdomu pastebėti tai, kad gauti rezultatai geresni už teoriškai numatytuosius skyriaus pradžioje. Kreivė pasiekia maksimumą iki 0,48, kai teoriniais skaičiavimais buvo išskaičiuota 0,33 .



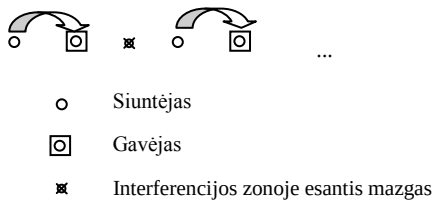
Pav. 26. Į rezultatus atsižvelgus patobulinta kreivė

Panašesni rezultatai gaunasi panaudojant formulę $\frac{\lambda}{w} = \frac{0.48}{(s-2)^{\frac{2}{3}}}$, kuri pakankamai gerai aproksimuoja gautuosius rezultatus.

Prielaidų bei rezultatų nesutapimas

Buvo bandoma apskaičiuoti maksimalų vidutinį pralaidumą, tenkantį vienam tinklo mazgui. Padaryta prielaida, kad radus maksimalų kiekį galinčių komunikuoti porų kiekį k, padalinus iš visų mazgų kiekio n, galime gauti santykinį pralaidumą, tenkantį vienam mazgui (kurią kanalo dalį išnaudoja vienas mazgas, būdamas atitinkamame tinkle).

Klaidinga prielaida buvo padaryta skaičiuojant galinčių komunikuoti mazgų porų kiekį k. Iliustracijoje Pav. 27 pavaizduota kai mazgai yra išdėstyti atstumu d lygi jų komunikavimo atstumui r (maksimalus atstumas, kuriuo mazgai gali komunikuoti pilna sparta). Buvo įsivaizduojama kad mazgai siunčia srautą tik viena kryptimi iš kairės į dešinę. Tuomet, kiekvienai komunikuojančiai porai dar būdavo priskiriamas dar vienas mazgas, kuris negali būti siuntėju, nes trukdytų komunikuoti pirmajai porai.

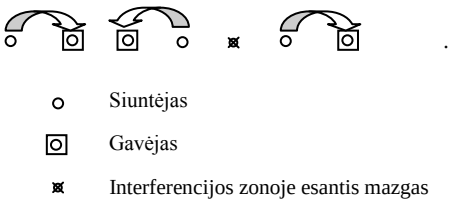


Pav. 27. Parametro K skaičiavimo prielaidos

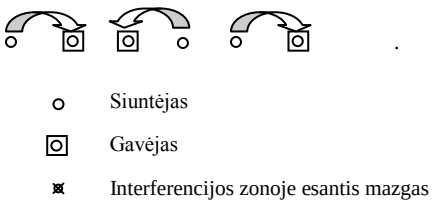
Dėl šios prielaidos buvo gauti rezultatai, kad linijinės topologijos tinkle maksimalus santykinis pralaidumas gali pasiekti tik apie 0,33 (iki 33% galimo maksimalaus pralaidumo vienam mazgui). Didinant tankį (mažinant atstumą d tarp mazgų) šis skaičius dar mažėja, vis didėjant interferencijos zonoje esančių mazgų kiekiui.

Kadangi eksperimento rezultatai parodė santykinio pralaidumo reikšmę netolimą 50%, dar kartą buvo peržiūrėtos teorinio skaičiavimo prielaidos.

Pastebėta, kad tiriant dvikryptę komunikaciją (srautas gali tekėti tiek į kairę, tiek į dešinę pusę), galimas kraštutinis variantas (išdėsčius atstumu d=R, kai tik vienas iš penkių mazgų negali dalyvauti komunikacijoje. T.y.: komunikuojančių porų skaičiaus k artėja prie pusės visų mazgų kiekio n ir galima artima 0,4 santykinio pralaidumo reikšmė. Tuomet kiekvieniem 5 mazgams tenka 2 poros (ne 6, kaip buvo manyta anksčiau). Šiuo būdu gaunamas maksimalus galimas santykinis pralaidumas lygus 0,4.



Pav. 28. Patikslintas k skaičiavimo



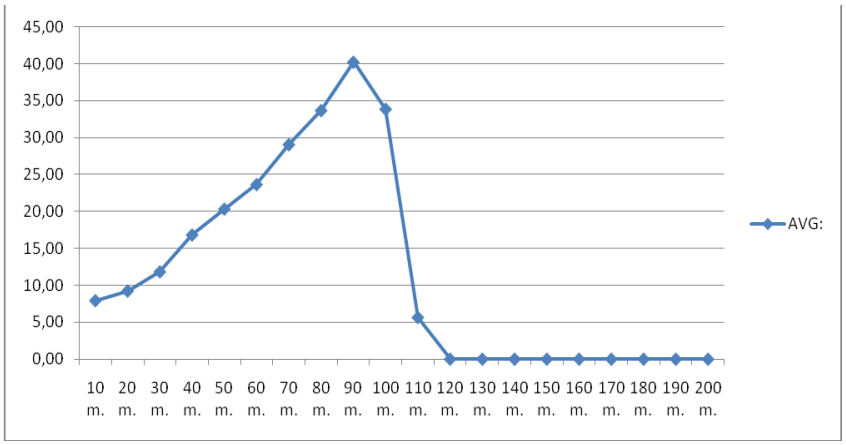
Pav. 29. Ns-3 interferencijos metodas

Ns-3 simuliatoriuje pastebėtas dar vienas įdomus reiškinys: siuntimo metu greta esantys siuntėjai nėra įtakojami vienas kito skleidžiamų bangų. Greta esantys siuntėjai, siunčiantys skirtingomis kryptimis gali išsiųsti paketus, kuriuos priima gavėjai, nesantys kito siuntėjo interferencijos zonoje (Pav. 29). Kadangi gavėjai nenukenčia nuo siuntėjų interferencijos, tai esant labai mažam tankiui visiškai visi mazgai gali dalyvauti komunikacijoje. Šiuo atveju gauname santykinius pralaidumus, lygius 0,5 reikšmei, esant mažam tankiui, kuris užtikrina tik kaimynių mazgų komunikaciją.

5. Gardelės tipo tinklo topologijos tyrimas

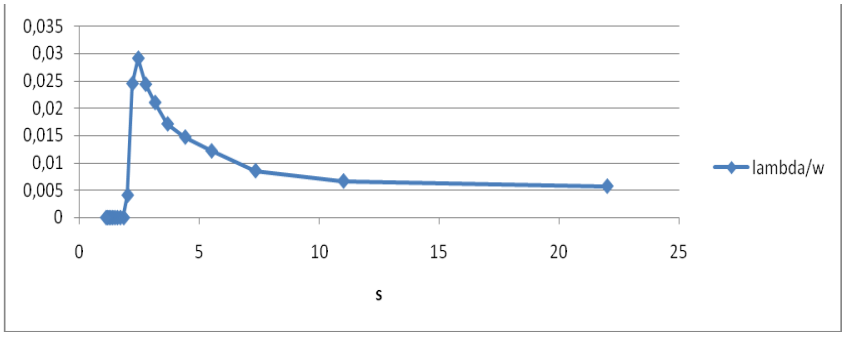
Kintanti moduliacija

Šios topologijos tinklo tyrimui buvo parinktos labai artimos sąlygos kaip ir tiesės topologijos tinklo. Tinklo dydis: 10x10= 100 mazgų. Tiriama vidutinis bendras pralaidumas per 1 s (10s laikotarpyje). Naudojamas Minstrel spartos valdymo algoritmas (automatinis spartos parinkimas tarp 6 ir 54Mbps). Rezultatai matomi Pav. 30.



Pav. 30. Bendras pralaidumas. Naudojant Minstrel spartos valdymo algoritmą

Rezultatai analizei perskaičiuojami į santykinę spartą bei tankį, naudojant prielaidose išvestas formules (Pav. 31).

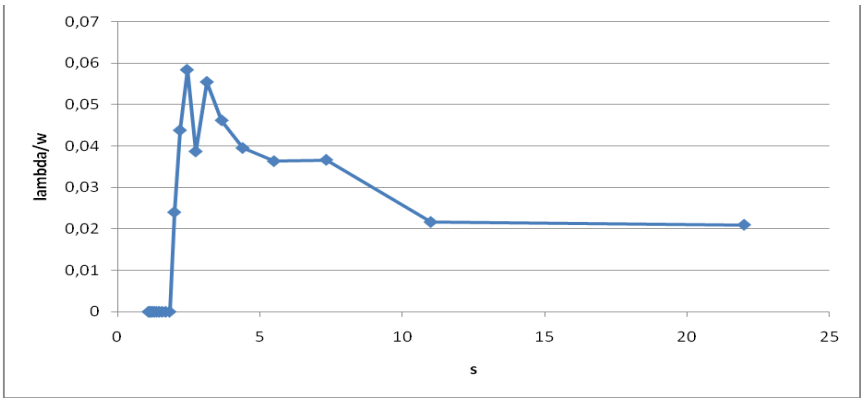


Pav. 31. Gardelės su Minstrel pralaidumo valdymo algoritmu

Vėlgi, kaip ir linijinės topologijos rezultatuose matoma ta pati tendencija: kanalo resursai maksimaliai išnaudojami esant mažam įrenginių tankiui.

Pastovi moduliacija

Gardelės formos tinklo analizė, naudojant pastovią 6Mbps moduliaciją. Visi kiti parametrai naudojami lygiai tokie patys, kaip ir ankstesniuose tyrimuose.



Pav. 32. Gardelės su OFDM 6Mbps moduliacija santykinio pralaidumo reikšmė pagal mazgų tankį

Išlieka tos pačios tendencijos kaip ir ankstesniuose tyrimo rezultatuose - sparta eksponentiškai krenta kylant tinklo tankiui. Žinoma, automatinis pralaidumo reguliavimas naudojant Minstrel algoritmą rezultatus padaro tolygesnius, bet išlieka aiškios tendencijos apie tai, kad nekintančiam signalo stiprumui egzistuoja atitinkamas mazgų tankis, kuriame yra geriausios sąlygos komunikacijai.

Gardelės tipo tinklo matematinio modelio patobulinimai

Darant matematines prielaidas gardelės atveju taip pat nebuvo atsižvelgta, kad du gavėjai gali būti greta vienas kito, jeigu siuntėjų interferencijos zonos nesikerta. Pavyzdys Pav. 33. Kadangi turime k=3 komunikuojančias poras, kai viso mazgų kiekis n=9, gauname iki 0,3 galimą santykinį pralaidumą, o ne 0,25, kaip buvo paskaičiuota prielaidose.

Pav. 33. Optimali gardelės konfigūracija

Apibendrinimas

Ištirtos linijinės bei gardelės topologijos tinkle matomas aiškus momentinis duomenų perdavimo vienam mazgui pikas, esantis ties ribine tankio riba. Toliau mažinant mazgų tankį duomenų perdavimas nutrūksta. Gautos pikinės momentinio pralaidumo reikšmės linijiniame bei gardelės topologijos tinkle yra atitinkamai $\lambda/w=0,5$ bei $\lambda/w=0,33$. Didėjant mazgų tankiui ši momentinis pralaidumas krenta iki ribinės $\lambda/w=1/n$ reikšmės (kur n yra tinkle esančių mazgų kiekis), parodo daugiašuolių tinklų našumo atvirkštinį sąryšį su mazgų kiekiu.

IV. Daugiašuolių belaidžių tinklų išvystymas

1. Modeliavimo rezultatų reikšmė

Siekiant diegti tinklus, kuriems nebūtų būtina centrinė bazinė stotis, norint komunikuoti tarpusavyje, reikalinga visiems prieinama komunikacijos terpė. Radijo bangomis komunikuojantys mazgai, kurie naudojasi tuo pačiu kanalu gali susijungti į vieningą bendrą tinklą, kuriuo netrukdomai gali komunikuoti.

Kadangi bandoma apeiti centrinio prieigos taško poreikį, tinkle nėra galimybės centralizuotai suvaldyti įrenginiams skiriamo laiko, kuriuo jie gali vykdyti komunikaciją. Bazinės stotys naudoja įvairias metodikas, tokias kaip TDMA moduliacija GSM standarte, ar prieigos taško išduodami leidimai siuntimui (Wi-Fi). Šiam tikslui daugiašuoliuose tinkluose pasitelkiami paskirstyti algoritmai, kurie dirba atskirai kiekviename įrenginyje.

Darbe modeliuoti dideli belaidžiai tinklai. Analizuotas šių tinklų našumas - vieno iš daugelio mazgų vidutinė galima sparta. Rezultatai parodo, kad tinklai turi būdingą savybę - optimalųjį tankį. Ši tinklo savybė gali parodyti koks maksimalus naudingas našumas gali būti pasiekiamas naudojant belaidę vieno dažninio kanalo komunikacijos įrangą.

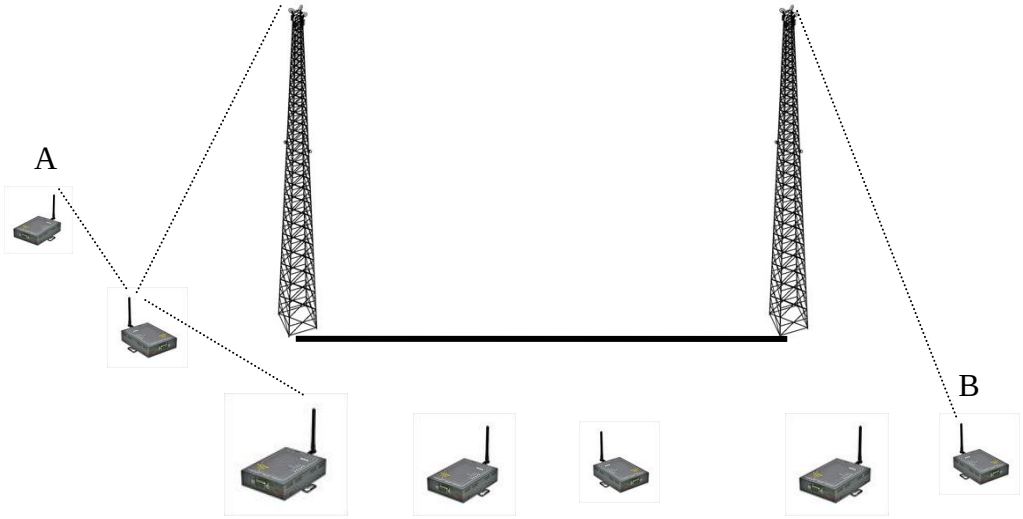
Kuriant, bei naudojant, įvairaus tipo daugiašuolius tinklus, verta atsižvelgti į šio tinklo optimalųjį tankį. Šis rodiklis parodo būtinų, bei perteklinių mazgų kiekį atitinkamame plote. Jeigu įrenginiai įdiegiami per daug dideliu tankumu, galimi tinklo veikimo sutrikimai ar pralaidumo degradacija. Pritaikius šią metriką galima tiek atpiginti kai kurių tinklų diegimo kaštus, tiek pagerinti tinklo charakteristikas.

Analizuojant rezultatus kyla klausimas apie šios tinklo savybės valdymą. Sugebėjus identifikuoti tinklo parametrus, galinčius įtakoti optimalų tinklo tankį, galima optimizuoti tinklą, derinant jo įrenginius. Taip pat, papildomų algoritmų realizavimas papildant galiojančius maršrutizavimo algoritmus, galėtų pagerinti tinklo veikimą. Mazgai, identifikuojantys esamą tinklo tankį, parinktų reikiamus parametrus maksimizuojančius šio tinklo bendrą našumą. Mobilių tinklų atveju tinklas, gebantis prisitaikyti prie kintančio mazgų tankio, optimaliai išnaudotų dažninius radijo bangų resursus.

Dėmesį vertėtų atkreipti į tai, kad buvo analizuotas vieno šuolio perdavimas – komunikacija vyko tik tarp kaimynių mazgų. Analizuojant srauto perdavimą tarp atsitiktinių mazgų, panaudojus tarpininkus, naudingų duomenų pralaidumas degraduoja priklausomai nuo tinkle esančių mazgų kiekio [7]. Optimalaus tankio metrika gali būti panaudojama ir daugiašuoliuose tinkluose, kur pagerinus komunikaciją tarp kaimynių mazgų, galime tikėtis geresnių bendro tinklo veikimo rezultatų.

Paskirstyto valdymo tinklų, kurių valdymas nėra paremtas centrinio prieigos taško nustatymais, reikalauja gerai išdirbtų paskirstytų algoritmų. Šių algoritmų pakankamas ištobulinimas gerina bendrus tinklo veikimo kokybės rodiklius. Sugebėjimas tinkle suvaldyti optimalaus tankio reikšmę stipriai prisidėtų prie geresnių tinklo veikimo rezultatų.

Vien tik optimizuojant daugiašuolių tinklų veikimą, nepanašu kad gali būti pasiekti tenkinantys rezultatai. Tinklo našumo degradacija pagal egzistuojančių mazgų kiekį neleidžia diegti labai didelio dydžio optimalių daugiašuolių tinklų. Reikalinga juos integruoti į kitus tinklus, kurie naudoja ir kitas technologijas. Maršrutizuojant turi būti automatiškai parenkama kuriuo keliu - per kaimynius mazgus, ar per greta esančią bazinę stotį verta kreipti srautus. Ši situacija pateikta iliustracijoje Pav. 34. Aplink ryšio bokštus esantys mazgai tarpusavyje komunikuoja tiesiogiai. Neesant ryšiui su bokštu, mazgai gali pasinaudoti kaimyniais mazgais, kad pasiektų šių bokštų turimus tinklo resursus. Kuomet mazgui A yra poreikis komunikuoti su B, šis galėtų pasinaudoti tiek bokšto, tiek kitų mazgų sąryšiais, kad užmegztų komunikaciją. Kadangi bokštai sujungti laidine linija, kurios sparta bei kokybė viršija belaidžio daugiašuolio tinklo spartą, maršrutizavimo algoritmai parenka sparčiausią kelią iki B.



Pav. 34. Daugiašuolių tinklų integracija

Iliustruotame pavyzdyje galima pademonstruoti ir patikimumo aspektą. Sugedus vienam iš bokštų šiuolaikiniuose tinkluose ryšys dingtų pusėje tinklo. Naudojant daugiašuolę technologiją, ryšio palaikymas būtų įmanomas per tarpinius mazgus visame tinkle. Žinoma, ryšio kokybė nukentėtų.

Šios schemos palaikymui atsiranda globalios marštutizacijos poreikis, kadangi tinklai

2. Ad Hoc – IP integracija

Visuose ankstesniuose skyriuose buvo kalbama tik apie vidinę komunikaciją belaidžiame tinkle. Iš vartotojų kylantis poreikis visuomet būti prisijungus prie pasaulinio Interneto tinklo kelia reikalavimą ne tik bendravimui tarpusavyje vidiniame tinkle, bet ir gauti prieigą prie pasaulinio tinklo. Integravimas į IP tinklus palengvina maršrutizavimo problemos sprendimą tarp kelių skirtingų daugiašuolių tinklų, ar netgi vieno didelio tinklo našumo optimizavimui (kaip pateikta ankstesnio skyriaus pavyzdyje).

Integravimas į IP tinklus yra šių tinklų prijungimas prie išorinių tinklų bei globalaus Interneto tinklo. Šiuo metu paplitusiuose tinkluose už prieigą prie interneto, maršrutizavimą bei adresų suteikimą yra atsakingi prieigos maršrutizatoriai. Vartotojai prie šių maršrutizatorių jungiasi tiesiogiai. Ši centralizuot architektūra leidžia maršrutizatoriui stebėti bei valdyti aktyvias jungtis, adresų sritį bei maršrutų lenteles. Daugiašuolių tinklų prijungimas prie išorinių tinklų kelia papildomus reikalavimus.

Daugiašuoliams, ypatingai ad hoc tinklams būtini tinklo elementai, vadinami interneto vartais (ang. internet gateways). Dažniausiai interneto vartais gali tapti kiekvienas ad-hoc tinklo narys, turintis išėjimą į pasaulinį tinklą. Galimi kiti variantai, kur įrengiami stabilūs infrastruktūriniai sprendimai, turintys pastovų internetinį ryšį, bei sąsają su ad-hoc tinklu.

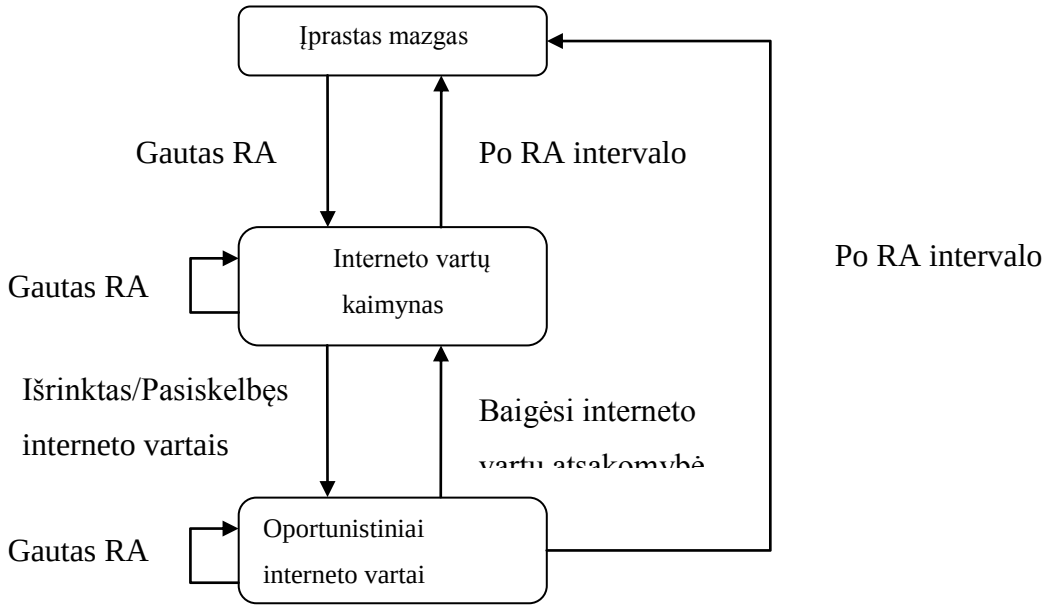
Viena iš svarbiausių interneto vartų užduočių – tinklo adresacija, kai tinklo mazgai aprūpinami unikaliais išoriniais adresais. Interneto vartai gali atlikti tiek DHCP (Dynamic Host Configuration Protocol) persiuntimo tiek pačio serverio funkciją.

Interneto vartai gali būti dvejopi: dedikuotieji bei oportunistiniai. Pirmieji tinklo administratorių iš anksto sukonfigūruojami, suteikiami reikiami parametrai, adresų sritys, kuriuos šis dedikuotasis serveris valdo. Oportunistiniai – be jokio išankstinio ar centralizuoto valdymo sprendimo automatiškai, pagal paskirstytus algoritmus veikiantys serveriai. Paskirstyti algoritmai padeda išrinkti naujus oportunistinius interneto vartus, automatiškai perleidžiant dalį valdomos adresų srities, bei reikalingus tinklo parametrus.

Automatiniam adresų erdvės valdymui gali būti parinkti dvejopi algoritmai: saugantys adresų būseną (angl. stateful) bei nesaugantys adresų būsenos (angl. stateless). Norint išsaugoti adresų būsenas pirmuoju atveju, dedikuotas serveris (serverio paslauga) turi prižiūrėti, kurie adresai yra suteikti iš turimos adresų srities. Kiekvienas mazgas, norėdamas gauti konfigūracijos parametrus, turi siųsti užklausą į dedikuotąjį serverį, bei gauti jo patvirtinimą su galimomis adresų reikšmėmis (taip pat kaip yra realizuotas DHCP protokolas). Būsenos nesaugantys algoritmai remiasi tuo, kad interneto vartų mazgai

perduoda tik tinklo priešdėlio (angl. prefix) reikšmę, kurios pagalba mazgas gali susigeneruoti unikalų IP adresą.

Būsenos nesaugančių algoritmų veikimas remiasi paskirstytu algoritmu, kai interneto vartų vaidmenį gali prisiimti kiti tinklo mazgai, esantys šalia interneto vartų. Tam naudojama RA (angl. Route Advertisement – maršrutų skelbimo) paketai. Šie paketai gali gyvuoti tik vieną šuolį – juos gauna tik interneto vartų kaimynai, ir toliau šie paketai nepersiunčiami. Taip gretimi mazgai identifikuoja greta esančius interneto vartus. Gavęs RA paketą, mazgas pakeičia savo būseną į „Interneto vartų kaimyno“ (Pav. 35). Po nustatyto laiko intervalo negavęs RA pranešimo mazgas vėl grįžta į įprasto mazgo būseną, arba toliau išlieka interneto vartų kaimyno būsenoje, kol gauna RA pranešimus. Šioje būsenoje esant reikalui mazgas gali pasiskelbti interneto vartais, arba inicijuojami interneto vartų rinkimai. Nugalėjęs mazgas tampa oportunistiniais interneto vartais. Tuomet, kol gauna RA pranešimus dažniau nei RA intervalas, šis mazgas taip pat gali siųsti RA pranešimus. Taip tinkle vienu metu veikia keletas interneto vartų. Dėl šios savybės ad hoc tinklai toleruoja tinklo pasidalijimą į atskiras dalis, susijungimus bei pakantumas tinklo topologijos dinamikai.



Pav. 35. Oportunistinių interneto vartų išrinkimo procesas

Automatinis išorinio IP adreso, bei kitų parametrų (kaip interneto vartų adreso) nustatymas vadinamas autokonfigūracija. Šiame procese dažniausiai gali dalyvauti šie pranešimai:

- RA (angl. Route Advertisement) – Maršruto pranešimas
- MPA (angl. Multicast prefix advertisement) – Multicast būdu siunčiamas tinklo priešdėlio pranešimas;

- PAS (angl. Prefix advertisement solicitation) – Tinklo priešdėlio pranešimo užklausa;
- UPA (angl. Unicast Prefix Advertisement) – tiesiogiai siunčiamas tinkle priešdėlio pranešimas.

Naudojant kai kuriuos maršrutizavimo algoritmus, šie pranešimai įterpiami į maršruto užklausas bei atsakymus. Tarkim AODV (1) algoritme pakeičiama interneto vartų vėliavėlės reikšmė į 1, tuomet ši užklausa nurodo, kad ieškomi artimiausi interneto vartai – veikia kaip PAS pranešimas, dar vadinamas RREQ_I. Tuomet siunčiamas atgal pranešimas RREP_I (ta pati interneto vartų vėliavėlės reikšmė kaip ir RREQ_I), kurio reikšmė tolygi UPA – tiesiogiai užklausos siuntėjui keliaujantis tinkle priešdėlio pranešimas, su reikiama informacija paketo viduje.

Interneto vartų paieškos procesas gali vykti iniciatyviai bei reaktyviai:

- Iniciatyvus procesas – interneto vartai pastoviai, kas T_{MPA} sekundžių siunčia MPA pranešimus visam tinklui;
- Reaktyvus procesas – interneto vartai siunčia UPA pranešimą tik tuomet, kai gauna PAS užklausą iš naujai prisijungusio mazgo;
- Hibridinis procesas – Naudojamos abejų procesų savybės.

Iniciatyvus paspartina mazgų įsiliejimo į tinklą trukmę, bet užlieja tinklą bereikalingu srautu. Dėl šios priežasties buvo pasiūlytas hibridinis procesas: iniciatyvaus proceso metu siunčiamų MPA pranešimų gyvavimo laikas (TTL) yra trumpas, ir parenkamas pagal tinklo diametrą. Naujas mazgas, per trumpą laiko tarpą negavęs MPA pranešimo, reaktyviu būdu siunčia PAS pranešimą, norėdamas prisjungti prie tinklo.

Daug problemų kelianti autokonfigūracijos proceso dalis – suteikiamų adresų unikalumas (tiek vietinio, tiek globalaus interneto tinklo prasme). Yra keletas scenarijų, kurių sprendimai kol kas galutinai nenusistovėję:

- Mazgo adresas sutampa su jau esančiu – Aptikimas bei reakcija.
- Dalis mobilaus tinko atsijungia nuo bendro tinklo – koks tolimesnis adresacijos procesas?
- Atsijungęs tinklas po kurio laiko prisijungia su naujais vartotojais – adresų konfliktas
- Dvejų nepriklausomų MANET tinklų apjungimas – adresų konfliktas

Dvi pagrindinės sprendimų rūšys, bandančios apeiti šias problemas:

- Konfliktų aptikimo schema – naudojamas besikartojančių adresų aptikimo algoritmas DAD (angl. duplicate address detection). Aptikus dublikatą, keičiamas adresas, ir vėl kartojamas DAD.
- Bekonfliktė paskirstymo schema – adresai parenkami tokiu būdu, kad niekuomet nekiltų konfliktai.

Pirmuoju atveju DAD pagalba aptinkamas dublikatas. Jei per atitinkamą laiką nėra dublikato ženklų, mazgas gali pradėti naudotis suteiktu IP adresu, kitu atveju kartojamas IP adreso užklausimo procesas (arba automatinio generavimo, Ipv6 atveju). Deja, šio proceso metu generuojamas nemažas srautas paketų, kuris trukdo normaliam tinklo darbui. Ypatingai tais atvejais, kai susijungia du tinklai. Šio proceso optimizavimui siūloma, kad interneto vartai kauptų informaciją apie tinkle naudojamus IP adresus, ir sparčiai raportuotų apie dublikatus.

Adresų paskirstymas išvengiant konfliktų yra žymiai sudėtingesnis uždavinys. Yra siūloma daugybė galimų schemų. Naudojant IPv6 protokolą, kiekvienas įrenginys naudodamas gautą tinklo priešdėlį ir savo MAC adresą gali sujungęs gauti nesikartojantį IP adresą. Deja, ši schema nėra tinkama GSM tinklo atveju, kai įrenginiai naudoja IMEI identifikatorių vietoje MAC adreso. Yra siūlomi IMEI perskaičiavimo algoritmai, bet šie negarantuoja kad rezultate bus gautas unikalus MAC adresas. Taip pat MAC adresai kartais gali sutapti (Aplaidus gamintojas, vartotojo galimybė pasikeisti šio adreso reikšmę. Dėl šios priežasties vistiek neapsieinama be DAD algoritmo.

Pastovios reikšmės (pvz. Įrenginio MAC) naudojimas IP adrese gali būti laikoma saugumo spraga: pažeidžiamas vartotojo anonimiškumas, kadangi bet kuriame tinkle, atmetus tinklo priešdėlį visuomet gaunama ta pati reikšmė. Tai gali kelti privatumo pavojus.

Kita adresų paskirstymo schema – kiekvienas mazgas, pereidamas į oportunistinių interneto vartų režimą, perima sritį adresų iš kaimynių interneto vartų, už kurią jis tampa atsakingu. Ši schema nesunkiai išsprendžia tinklo išsiskyrimo ir sujungimo atgal problemą. Deja, konfliktų gali iškilti sujungiant du atskirus tinklus. Vėlgi siūloma naudoti DAD algoritmą.

Daugiašuolių tinklų našumo degradacija priklausomai nuo tinklo dydžio kelia poreikį šiuos tinklus integruoti į didesnius laidinius, ar kitomis technologijomis paremtus tinklus. Pateikta daugiašuolių belaidžių tinklų, ypač ad hoc tipo tinklų integracija į dabartinius IP tinklus kelia daugybę vis dar neišspręstų klausimų. Literatūroje [11] minimi atviri klausimai, tokie kaip interneto vartų parinkimas iš kelių galimų, optimalus laikinių parametrų parinkimas, autokonfigūracijos saugumas, ad hoc ir mesh tinklų integracija, aukšto mobilumo palaikymas.

V. Išvados

Išanalizavus dabartinį didelio masto belaidžių tinklų veikimą bei juos palyginus su naujos kartos daugiašuoliais tinklais, matomas didelis kiekis pranašumų bei naujų panaudojimo sričių. Belaidžių tinklų decentralizavimas didina ryšio patikimumą, kai mazgų ryšys nėra priklausomas nuo vienintelio centrinio mazgo. Šie bei kiti nauji sprendimai padeda mažinti vartotojų komunikavimo kaštus bei išnaudoti belaidę prieigą naujoms paslaugoms.

Tinklo architektūros sprendimas, pašalinant privalomą komunikaciją su centriniu prieigos tašku geriau išnaudoja radijo bangų resursus, bei padidina to paties dažninio kanalo pakartotinio panaudojimo galimybę toje pačioje teritorijoje. Ad hoc tinklų panaudojimas padidintų dabartinių infrastruktūrinių tinklų našumą.

Ištirta momentinė tinklo našumo priklausomybė nuo mazgų tankio. Rastos ribinės linijinės bei gardelės topologijos belaidžių tinklų santykinės pralaidumo reikšmės. Linijinės topologijos tinkle maksimali santykinio pralaidumo reikšmė gali siekti $\lambda/w=0,5$, o gardelės topologijos tinkle ši santykinė reikšmė gali pakilti iki $\lambda/w=0,33$. Abejose topologijose, didėjant tankiui, ši reikšmė artėja prie ribinės $\lambda/w=1/n$ santykinio pralaidumo reikšmės, parodančios tinklo našumo priklausomybę nuo mazgų kiekio.

Vientisas didelis ad hoc tinklas nėra įmanomas dėl našumo degradacijos, atvirkščiai proporcingos tinkle veikiančių mazgų kiekiui. Būtina integracija su didesnės spartos stuburiniais tinklais. Tam turi būti iki galo išspręstos globalios adresacijos bei autokonfigūracijos problemos.

Atlikus tyrimą, buvo pastebėta tinklo savybė – optimalus belaidžio tinklo tankis, parodantis kokiu tankiu išsidėstę mazgai maksimizuoja persiunčiamų duomenų kiekį. Ši savybė matuojama santykiu tarp mazgų atstumų bei jų inteferencijos zonos dydžio. Santykinis tankis gali kisti priklausomai nuo aplinkos, bei patį tinklą sudarančių mazgų savybių. Tinklo diegimo metu, galima atsižvelgti į mazgų išdėstymo tankį, norint optimaliai išnaudoti tinklo dažninius resursus duomenų perdavimui bei maksimizuoti našumą.

Analizuojant rezultatus kyla naujas klausimas, kuriam reikalingas tolimesnis tyrimas: veiksniai, įtakojantys optimalųjį tankį. Sugebėjimas valdyti šiuos parametrus gali padėti optimizuoti tinklų veikimą ne tik jų diegimo metu, bei tinklams dinamiškai reaguojant į aplinkybių pasikeitimą.

VI. Naudota literatūra

[1] **WiMAX Forum.** *Recommendations and Requirements for WiMAX*.: WiMAX Forum, 2011 m.

[2] **Watanabe M., Higaki H.** *No-Beacon GEDIR: Location-Based Ad Hoc Routing with Less Communication Overhead*.: Fourth International Conference on Information Technology, 2007 m. 48-55 p..

[3] **Tracy Camp, Jeff Boleng, Vanessa Davies.** *A Survey of Mobility Models for Ad Hoc Network Research.* Golden : 2002 m., T. Wireless Communication & Mobile Computing (WCMC).

[4] **Plėštys R., Dagilis V.,** *Vartotojų tankio įtakos Ad-Hoc tinklo pralaidumui įvertinimas.* Klaipėda : Klaipėdos Universiteto Leidykla, 2010 m.

[5] **Plestys R., Zakarevicius R.,***Variable Response Zone Routing for Ad-Hoc Networks.* Kaunas : 2009 m., Information Technologies. 158-164 p.

[6] **Perkins C. E., Royer E. M.,** *Ad-hoc on-demand distance vector routing.*: WMCSA '99, 1999 m., Mobile Computing Systems and Applications.

[7] **P. Gupta, P. R. Kumar.,** *The Capacity of Wireless Networks.* : IEEE, 2000 m., IEEE Transactions on Information Theory.

[8] **Misra S., Misra S. C., Woungang I.** *Guide to Wireless Mesh Networks.* London : Springer, 2009.

[9] **Young Bae Ko, Nitin H. Vaidya.,** *Location-Aided Routing (LAR) in Mobile Ad Hoc routing with Less Communication Overhead.*: ITNG '07, 2007 m., Fourth International Conference on Information Technology. 48-55 p..

[10] **Wei Yin ir kiti.** *Evaluations of MadWifi MAC layer rate control mechanisms.* Beijing : IEEE, 2010 m. 978-1-4244-5987-2/1548-615X.

[11] **Yan Zhang, Jijun Luo, Honglin Hu.** *Wireless mesh networking : architectures, protocols and standards.* Boca Raton : Auerbach Publications, 2007. ISBN 9780849373992.

[12] **Y. Kim, J.. Kim, Y. Wag, K. Chang, J. Park Y. Lim.,** *Application Scenarios of Nautical Ad-Hoc Network for Maritime Communications.*: MTS, 2009 m.

[13] **IEEE.** *IEEE stdtandard 802.16.* s.l. : IEEE, 2011.

[14] **F. Anwar, Md. S. Azad, A. Rahman, M. M. Uddin.,** *Performance Analysis of Ad hoc Routing Protocols in Mobile WiMAX environment.*: IAENG International Journal of Computer Science, 2008 m., T. 35:3.

[15] **David B. Johnson, David A. Maltz.,** *Dynamic Source Routing in Ad Hoc Wireless Networks.* : Springer, 1996 m., Mobile Computing. 153-181 p.

[16] **Chaum, David L.,** *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.* 1981 m., Communications of the ACM, vol. 24 No. 2.

[17] **Chien-Liang Fok, Gruia-Catalin Roman, Chenyang Lu.,** *Rapid Development and Flexible Deployment of Adaptive Wireless.* Distributed Computing Systems, ICDCS 2005, Columbus : 2005 m. 0-7695-2331-5 .

[18] **Defence Advanced Research Projects Agency.** *Strategic Plan.* 2009.

[19] **J Yin, T ElBatt, G Yeung, B Ryu, S Habermas.,** *Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks.*: VANET '04, 2004.

[20] Network simulator 3. www.nsnam.org

[21] **Dragos Niculescu, Badri Nath**., Trajectory Based Forwarding and Its Applications. MobiCom '03, 2003, ISBN:1-58113-753-2

Analysis of high density wireless networks trhoughput

Summary

During last year there was high emphasis on mobile networking and access to the internet everywhere and any time. This was achieved by using wireless networks, like GSM or Wi-Fi family. New standards are emerging, like WiMax. This is centralized architecture networks, where central base station or access point is the essential part of the network. During down-time of this network part, whole network remains down. Other drawback this architecture – closely positioned users cannot communicate directly. Their communication is routed by some base station which is located at greater distance. This affects not optimal usage of wireless resources.

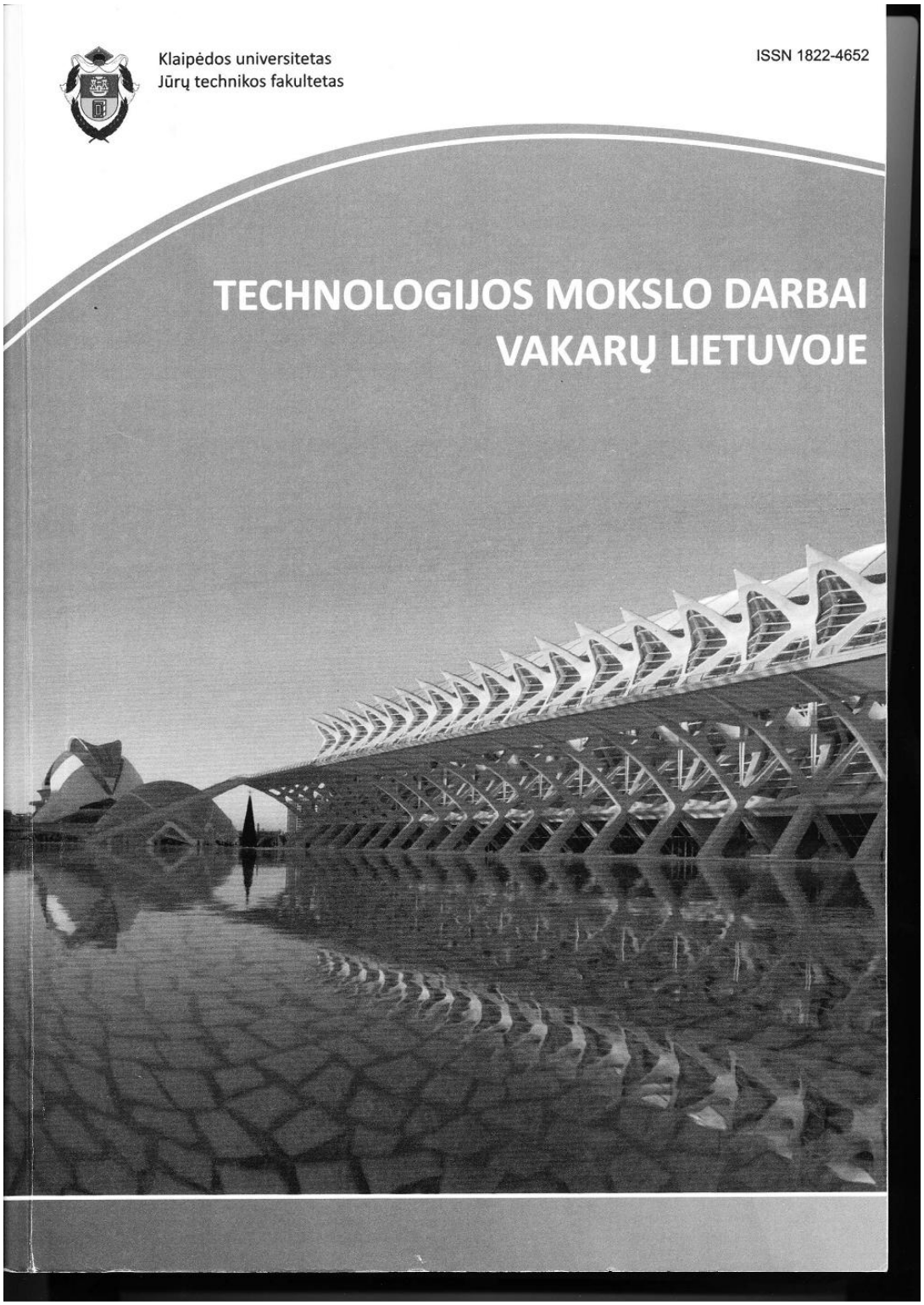
New generation of wireless networks uses multihop architecture. This architecture does not include central base station in it. Users can directly communicate with each other. This affects smaller area where radio resources are used. It can lead to higher channel reuse.

Linear and plane topology multihop networks were analyzed. Instant network capacity can reach up to $\lambda/w=0.5$ with line topology and up to $\lambda/w=0.33$ with plane topology. This achieved with lowest possible density when nodes can still communicate. When network density increases there is exponential drop of capacity heading towards $\lambda/w=1/n$ value. It shows negative relation of network size and capacity.

Experiment shows that there is some density, when wireless network can operate at maximum capacity. We call it optimal density. This can be used as a recommendation for deploying wireless multihop networks. There are questions which arise after analysis of experiment results – what can influence optimal network density. By controlling the network density, there can be improvement of wireless multihop networks. Dynamic adjusted parameters by routing algorithms could help improve mobile network capacity.

VII. Priedai

1. Susiję straipsniai



Mokslinis komitetas

Pirmininkas: prof. habil. dr. A. Ramonas, Klaipėdos universiteto prorektorius
Pirmininko pavaduotojai: prof. dr. R. Didžiokas, Klaipėdos universiteto prorektorius
prof. habil. dr. V. Zabukas, Klaipėdos universitetas

nariai:
prof. dr. A. Andziulis, Klaipėdos universitetas
prof. habil. dr. J. Atkočiūnas, Vilniaus Gedimino technikos universitetas
prof. habil. dr. V. Barzdaitis, Kauno technologijos universitetas
prof. habil. dr. D. Eidukas, LMA akademijos akademikas
prof. habil. dr. V. Laurutis, Šiaulių universitetas
prof. habil. dr. S. Lebedevas, Klaipėdos universitetas
dr. R. Levinskas, Lietuvos energetikos instituto direktoriaus pavaduotojas
prof. dr. R. Plėštys, Kauno technologijos universitetas
prof. habil. dr. V. Smailys, Klaipėdos universitetas
doc. dr. A. Žukauskaitė, Klaipėdos universitetas

Recenzentai

prof. habil. dr. A. A. Bielskis
prof. habil. dr. V. Zabukas
prof. dr. D. Ambrazaitienė
prof. dr. A. Andziulis
prof. dr. M. Bogdevičius
prof. dr. R. Didžiokas
doc. dr. B. Andziulienė
doc. dr. K. Bagdonas
doc. dr. A. Brėskis
doc. dr. V. Bulbenkienė
doc. dr. V. Denisovas
doc. dr. J. Janutėnienė
doc. dr. A. Krutinis
doc. dr. V. Kvedaras
doc. dr. A. Lapinskienė
doc. dr. O. Ramašauskas
doc. dr. T. Paulauskienė
doc. dr. G. Skripkiūnas
doc. dr. A. Stankus
doc. dr. L. Vasiljeva
doc. dr. J. Vaupšas
doc. dr. A. Žukauskaitė
dr. P. Mažeika
lekt. dr. D. Narmontas
lekt. dr. I. Rupšienė
lekt. dr. A. Skaisgirienė
lekt. dr. A. Štuopys

Leidinyje pateikta konferencijos medžiaga, parengta laikantis Lietuvos Mokslo tarybos nustatytų reikalavimų, keliamų recenzuojamoms mokslinėms publikacijoms.
Mokslinė konferencija „Technologijos mokslo darbai Vakarų Lietuvoje" rengiama kas dveji metai ir yra jau 7-asis renginys. Konferencijos tikslas – suburti moksleivinkus ir gamybininkus plėtojant mokslinę ir technologinę integraciją.
Leidinyje pateikti mokslinių tyrimų rezultatai technologijos mokslų srityje, apimančioje informacines ir mechatronines sistemas, inžinerinius statinius bei medžiagas, technologijų plėtrą ir aplinkosaugą.

Autorių kalba netaisyta

Rėmėjai

ARMGATE nanoVITA VILDoma

ISSN 1822-4652

Klaipėdos universiteto leidykla

Technologijos mokslo darbai Vakarų Lietuvoje VII

Viršelio autorius Aleksandras Paulauskas

Klaipėda, 2010

SL 1335. 2010 05 04. Apimtis 54 sąl. sp. l. Tiražas 90 egz.
Klaipėdos universiteto leidykla, Herkaus Manto g. 84, LT-92294 Klaipėda
Tel. (8~46) 398 891, el. paštas: leidykla@ku.lt
Dauginta Klaipėdos universiteto leidykloje, Herkaus Manto g. 84, LT-92294 Klaipėda

TURINYS

VARTOTOJŲ TANKIO ĮTAKOS AD-HOC TINKLO PRALAIDUMUI ĮVERTINIMAS

V. Dagilis, R. Plėštys
Kauno technologijos universitetas

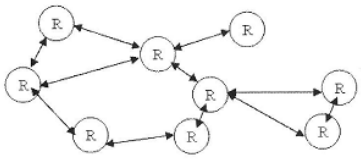
Anotacija
Analizuojama linijinės ir plokštuminės topologijos Ad-Hoc tinklo pralaidumo priklausomybės nuo tinklo dydžio. Nustatytos ribinės įvairaus dydžio tinklų pralaidumo reikšmės prie labai mažų ir labai didelių tinklo mazgų išsidėstymo tankių. Modeliavimo būdu gautos tinklo pralaidumo reikšmės prie tarpinių tinklo mazgų išsidėstymo tankių.
PAGRINDINIAI ŽODŽIAI: belaidės prieigos tinklai, Ad Hoc tinklai.

Abstract
Analysis of network size impact on capacity of linear and plane topology Ad-Hoc network. The capacity limits for large and dmall density networks are determined. Network capacity values for various density networks are modelled.
KEY WORDS: wireless access netwoks, Ad Hoc networks.

Įvadas

Mobiliojo ryšio Ad-Hoc tinklai paremti tinklo mazgų bendradarbiavimu su tikslu sukurti mišrią ir patikimą tinklo topologiją, užtikrinančią informacijos perdavimą kintant atstumams tarp tinklo mazgų. Mazgai tarpusavyje sujungti radijo linijomis, kurių ilgiai priklauso nuo tinklo mazgų siunčiamų signalų parametrų. Tokie tinklai dirba naudodami vieną bangų dažnį. Kai atstumai tiek padidėja, kad siunčiamą signalą nebegali patikimai priimti ryšyje dalyvaujantys tinklo mazgai, vyksta naujų maršrutų sudarymas [1, 2]. Ad Hoc tinklo mazgų (R) išdėstymo topologijos pavyzdys pateiktas 1 pav.

Jeigu visi tinklo mazgai yra labai arti, tai vienu metu gali siųsti informaciją tik vienas mazgas. Kai tinklo mazgai yra nutolę, keli tinklo mazgai vienu metu gali siųsti informaciją. Siuntimo laikų suderinimo algoritmas atitinka IEEE 802.11g standartą [3]. Tokių tinklų pralaidumo priklausomybės nuo mazgų skaičiaus tirtos P. Gupta ir P.R. Kumar darbe [5].



1 pav. Ad-Hoc tinklo topologija

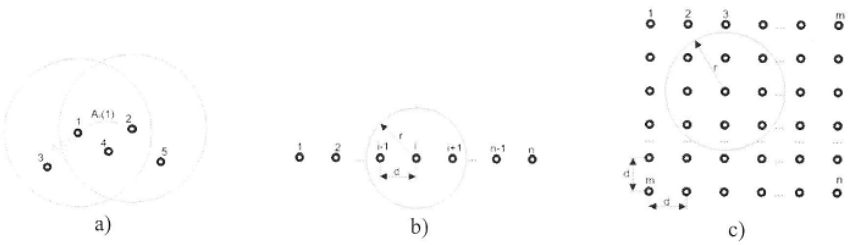
Tyrimai atlikti atsitiktinės topologijos tinkle ir nustatyta, kad pralaidumas į atsitiktinai pasirinktą tinklo įrenginį kinta pagal $\theta\left(\frac{W}{\sqrt{n\log n}}\right)$ dėsnį, naudojant neinterferuojant įprotokolą. Mūsų pateikiamo tyrimo tikslas yra nustatyti, kiek daugiausia gali būti tinklo mazgų porų k, kurios gali netrukdomai komunikuoti apibrėžtos topologijos tinkle.

Ad Hoc tinklo mazgų interferencija

Gretimi tinklo mazgai gali tarpusavyje komunikuoti atstumu, kuris priklauso nuo siunčiamo signalo galios, moduliacijos rūšies ir mazgo imtuvo jautrumo. Ryšio nuotolis r gali kisti nuo 35 m (patalpose) iki 95 m (laisvoje erdvėje) [3]. Visi aplinkiniai įrenginiai, esantys atstumu d<r nuo siunčiamo mazgo, gali priimti mazgo signalą.

Skirtingų mazgų porų interferencijos zonų pavyzdys, kai signalus siunčia mazgas 1 ir mazgas 2, parodytas 2 pav. Jeigu tinklo mazgai išsidėstę vienoje tiesėje (3 pav.), i-ojo mazgo signalai pasiekia i-1-ąjį ir i+1 -ąjį mazgus ir nepasiekia likusių mazgų. Jeigu tinklo mazgai išsidėstę vienodu d atstumu plokštumoje (4 pav.), į aprėpties zoną patenka 8 mazgai. Jei maksimalią linijinę perdavimo spartą pažymėsime w, tinklo mazgų kiekį – n, tai vienam tinklo mazgui vidutiniškai tenkantis srautas:

$$\lambda = k\frac{w}{n} \qquad (1)$$

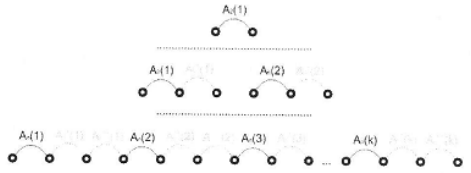


2 pav. Interferencijos zonų išsidėstymas: a) penkių mazgų tinkle, b) linijinės topologijos (1xn)tinkle , c) plokštuminės topologijos (n=mxm) tinkle

Neinterferuojančių mazgų porų suradimo metodika

Linijinės topologijos tinklas. Linijinės topologijos tinklo atveju neinterferuojančių mazgų porų skaičiaus iliustracija, kai d=r, pateikta 3 pav. Kai tinkle yra tik du mazgai, galima tik viena neinterferuojanti pora.

Šešių mazgų atveju galimos tik dvi neinterferuojančios poros: A6(1) ir A6(2) arba A'6(1) ir A'6(2). Analogiškai pavaizduotos poros iš n tinklo mazgų sudarytame tinkle. Jeigu tinklas proporcingai traukiasi mažėjant d, interferencija apima vis didesnį kiekį mazgų ir trukdo lygiagrečiai vykdyti siuntimą. Dėl to vis mažėja komunikuojančių porų skaičius kol gali sąveikauti tik viena pora.



3 pav. Naujas srautas tiesėje

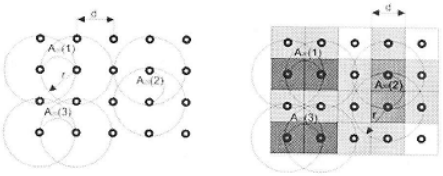
Porų skaičius k linijinės topologijos tinkle:

$$k = \left\lfloor \frac{n}{\left\lfloor \frac{r}{d} \right\rfloor + 2} \right\rfloor \qquad (2)$$

čia: $\lfloor X \rfloor$ reiškia sveikąją skaičiaus dalį.

Plokštuminės topologijos tinklas. Neinterferuojančių porų suradimui pasirinktas kvadratinės topologijos tinklas. Tinklo aprėpiamas plotas sudarytas iš elementarių kvadratų. Kiekvienas kvadratas gali turėti tris būsenas: siuntėjo, interferencijos ir laisvąją.

Siuntėjo būsena pavaizduota tamsiai (4 pav.) Kvadratai, kurių centrai yra užgožiami siuntėjų signalu, įgauna interferencijos būseną (4 pav.). Nauji ryšiai gali būti sudaromi tik iš laisvųjų zonų, pažymėtų balta spalva (4 pav.). Specialiai sudaryto algoritmo pagalba kvadratai išdėstomi taip, kad gauti didžiausią siuntėjų skaičius k.



4 pav. Neinterferuojančių porų paieška plokštuminiame tinkle

Neinterferuojančių porų paieškos algoritmas. Paieškos algoritmas paremtas tuo, kad atsitiktiniu būdu parenkame kiekviena porą ir apie ją nustatome interferencijos zoną. Atsitiktinai generuojant mazgų koordinates surandamos poros, kurios nepatenka į kitų porų interferencijos zonas. Algoritmas (1 lentelė) kartojamas tiek kartų, kol surastas didžiausias porų skaičius toliau nekinta. Algoritme panaudoti tokie žymėjimai: `l` – algoritmo kartojimo skaičius, `kiekRysiu(tinklas)` –tinkle surastų neinterferuojančių porų skaičius, `generuoti(dydis)` – atsitiktinių koordinačių reikšmės, `dydis` – tinklo mazgų skaičius (n=mxm), `apreptis` – maxRysiai – tinkle surastų neinterferuojančių porų didžiausias skaičius, `rysiu_kiekis(dydis, apreptis)` – funkcija, atsitiktinai sugeneruojanti ryšius tarp tinklo įrenginių, `LAISVA` – kvadrato būsena.

1 lentelė. Algoritmas

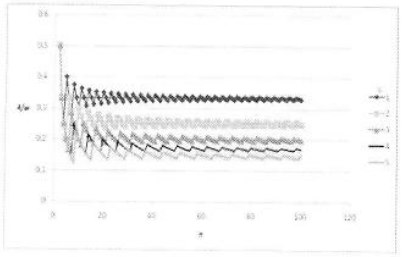
```
rysiuKiekisTikslus(dydis, apreptis)
  for i:=1,1 {
    rysiai = rysiu_kiekis(dydis, apreptis);
    if (rysiai > maxRysiai)
      maxRysiai = rysiai;
  }
return maxRysiai
rysiu_kiekis(dydis, apreptis)
  rnd1:=generuoti(dydis);
  rnd2:=generuoti(dydis);
  for i:=1,dydis
    for j:=1,dydis
      if (tinklas[rnd1[i]][rnd2[j]] == LAISVA)
        naujasRysys(tinklas, rnd1[i], rnd2[j]);
return kiekRysiu(tinklas);
```

`generuoti(dydis)` – grąžina masyvą, kuriame saugomi atsitiktine tvarka išdėlioti skaičiai nuo *1* iki *dydis*. Taip generuojama atsitiktinė vieta, kurioje kuriamas naujas ryšys, bet tuo pačiu patikrinami visi tinklo mazgai, ar juose gali būti sukuriamas naujas ryšys.

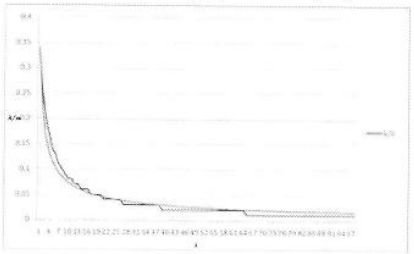
`naujasRysys(tinklas, i, j)` – atsitiktinai parenka laisvą kaimyninį langelį, langeliui i, j, su kuriuo gali būti užmezgamas ryšys. Šios funkcijos atsitiktinumo dėka, kiekvieną kartą gaunamas vis kitoks ryšių tinkle išdėstymas.

Tinklo dydžio ir mazgų tankio įtaka neinterferuojančių porų skaičiui

Linijinės topologijos tinklo neinterferuojančių porų skaičiaus priklausomybė nuo mazgų skaičiaus ir jų išsidėstymo tankio pavaizduota 5 pav. Kiekviena linija atitinka skirtingą mazgų tankį. Galima padaryti išvadą, kad nuo mazgų skaičiaus n=20 toliau didėjant jų skaičiui, santykis λ/w išsidėsto apie pastovią reikšmę, būdingą atitinkamam tankiui. Pačiu geriausiu atveju, kaip aprėpties spindulys r yra lygus atstumui tarp gretimų mazgų d, tik kas trečias mazgas gali sudaryti mazgų porą (λ/w =0,33). Vienam tinklo mazgui tenkančios santykinės spartos λ/w priklausomybė nuo tinklo mazgų išsidėstymo tankio s= r/d linijinės topologijos tinkle, sudarytame iš 100 mazgų, priklausomybė pateikta 6 pav.



5 pav. Linijinio tinklo santykinio pralaidumo priklausomybė nuo mazgų skaičiaus ir jų išsidėstymo tankio

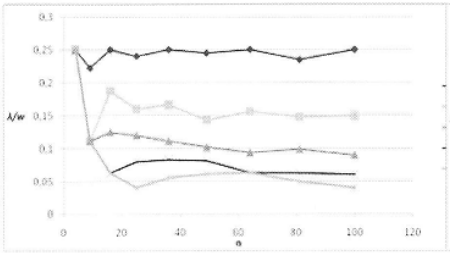


6 pav. 100 mazgų linijinio tinklo santykinio pralaidumo priklausomybė nuo mazgų išsidėstymo tankio

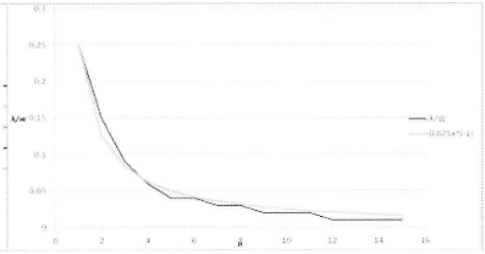
Pradžioje pastebimas labai greitas neinterferuojančių mazgų porų skaičiaus kitimas. Kai visi mazgai patenka į vieną aprėpties zoną, tada neinterferuojančių mazgų porų skaičiaus k=1. Šis kitimas gali būti aproksimuotas priklausomybe:

$$\frac{\lambda}{w}=\frac{k}{n}=\frac{0{,}34}{\sqrt[3]{s^2}},\ \text{kai}\ \frac{\lambda}{w}>\frac{1}{n} \qquad (3)$$

Plokštuminės kvadratinės topologijos tinklo neinterferuojančių porų k priklausomybė nuo tinklo dydžio ir tinklo mazgų išsidėstymo tankio prie pastovios aprėpties zonos parodyta 7 pav. Prie minimalaus mazgų išsidėstymo tankio s=r/d=1, neinterferuojančių porų santykinis dydis lygus λ/w = 0,25, o didėjant tankiui vis mažėja (7 pav.), kol pasiekia ribinę reikšmę λ/w =0,01. Neinterferuojančių porų santykio kitimas 100 mazgų dydžio tinkle pateiktas 8 pav.



7 pav. Plokštuminio tinklo santykinio pralaidumo priklausomybė nuo mazgų skaičiaus ir jų išsidėstymo tankio



8 pav. 100 mazgų plokštuminio tinklo santykinio pralaidumo priklausomybė nuo mazgų išsidėstymo tankio

Šis kitimas gali būti aproksimuotas priklausomybe: $\frac{\lambda}{w} = 0.25\frac{1}{s}$, kai $\frac{\lambda}{w} > \frac{1}{n}$ (4)

Lyginant linijinės ir plokštuminės topologijos tinklų pralaidumo priklausomybes, gauname, kad linijinės topologijos tinkle pralaidumas mažėja sparčiau.

Išvados

1. Linijinės topologijos Ad-Hoc tinklų neinterferuojančių porų skaičius yra atvirkščiai proporcingas kubinei šakniai iš tinklo mazgų tankio kvadrato. Plokštuminės topologijos Ad-Hoc tinklų neinterferuojančių porų skaičius yra atvirkščiai proporcingas tinklo mazgų tankiui.
2. Linijinės topologijos Ad-Hoc tinklo didžiausias santykinis pralaidumas lygus 0,34, o plokštuminės topologijos tinklo nuo 0,25, kai atstumas tarp mazgų lygus aprėpties zonai. Kai visi mazgai patenka į vieną aprėpties zoną, santykinis tinklo pralaidumas sumažėja iki dydžio 1/n.

Patvirtinimas

Šis straipsnis buvo parengtas su projekto MOBAS-2010 „Mobiliųjų ir bevielių paslaugų informacinės aplinkos sukūrimas“, vykdomam pagal Aukštųjų technologijų plėtros Lietuvoje 2007–2013 metais programą (Lietuvos mokslo tarybos Gamtos ir technikos mokslų komiteto, 2010-04-12 nutarimu Nr. 064-GTM-8) finansine pagalba.

Literatūra

1. Perkins C.E., Royer E. M., Ad-Hoc On-Demand Distance Vector Routing, Mobile Computing Systems and Applications, 1999, Proceedings. WMCSA '99. Second IEEE Workshop, Feb. 1999, p. 90–100.
2. Plestys R., Zakarevicius R., Variable Response Zone Routing for Ad-Hoc Networks, Information Technologies' 2009, Kaunas, Lithuania. p. 158-164.
3. Misra S., Misra S. C., Woungang I., Guide to Wireless Mesh Networks, Springer, 2009, London.
4. IEEE. IEEE Std. 802.11, Wireless LAN Medium Access Control (MAC) and Physical (PHY) specications: Amendment 6: Medium Access Control (MAC) Security Enhancements (Amendment to IEEE Std 802.11, 1999 Edition as amended by IEEE Std 802.11g-2003 and IEEE Std 802.11h-2003), 2004.
5. P. Gupta and P. R. Kumar, The Capacity of Wireless Networks. IEEE Transactions on Information Theory, 46(2):388–404, 2000.

USER DENSITY INFLUENCE ON AD-HOC NETWORK CAPACITY

V. Dagilis, R. Plėštys

Summary

Ad-Hoc network simulation was made. We are using relative measurement for network capacity λ/w, which shows part of maximum bandwidth utilized on average. Algorithm for network simulation was made. Aproximation of Simulation of the linear topology network capacity dependency on network density is $\frac{0,34}{\sqrt[3]{s^2}}$, whereas for plane topology it is $0.25\frac{1}{s}$.

Recenzentas – prof. dr. A. Andziulis