KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Tomas Narbutaitis

Saugaus maršrutizavimo Ad Hoc tinkluose tyrimas

Magistro darbas

Vadovas
prof. dr. R. Plėštys

KAUNAS, 2011

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Saugaus maršrutizavimo Ad Hoc tinkluose tyrimas

Magistro darbas

Vadovas
prof. dr. R. Plėštys

Atliko:
IFN9/3 gr. studentas
Tomas Narbutaitis

Recenzentas:

KAUNAS, 2011

TURINYS

Lentelių sąrašas

Paveikslėlių sąrašas

Summary

Mobile Ad-Hoc networks are very useful in certain situations, but raise many challenges and one of the biggest is security. Specially designed routing protocols are required and they are quite well developed except for security area. In this thesis I concentrate on various active attacks on ad-hoc network during routing process, compromising network availability, data integrity and confidentiality and analyze some security aware protocols, that can be used to avoid these risks. New concept routing protocol is proposed, for coping with a specific scenario of really high level of malicious nodes on the network and insecure network model is created, which is used to simulate, get and compare performance metrics of some security aware routing protocols.

ĮVADAS

Bevieliai tinklai pasaulyje užima vis svarbesnį vaidmenį ir sparčiai keičia laidinius tinklus. Tačiau absoliučiai didžioji dauguma šių tinklų yra centralizuotos architektūros (infrastructure tipo). Taškas-taškas ad-hoc tinklai tarp dviejų mazgų taip pat gana dažnai naudojami. Na, o mobilieji daugelio mazgų (multihop) ad-hoc bevieliai tinklai taip pat nėra nauja idėja, tačiau vis dar nėra plačiai naudojami, nors turi tikrai naudingų ir unikalių pritaikymo sričių.

Pagrindinės ad-hoc tinklų panaudojimo sritys:

- Laikiniems tikslams, kai reikia greitai ir be papildomų įrenginių, t.y. pigiai turėti tarpusavio ryšį.
- Tarpusavio ryšio palaikymui mobilių karo, policijos, gelbėjimo operacijų metu.
- Internetinio ryšio pasiekiamumui nuošaliose vietovėse, kur kurti stacionarią belaidę ar laidinę infrastruktūrą finansiškai neapsimoka.
- Kaip alternatyvi komunikacijos priemonė stichinių nelaimių atveju, kai visa kita ryšio infrastruktūra yra išvesta iš rikiuotės.

Yra keletas priežasčių, kodėl ad-hoc tinklai mažiau paplitę, nei kitos komunikacijos rūšys. Iš dalies tai lemia gan specifinė panaudojimo sritis, tačiau svarbiausia priežastis – vis dar pilnai nerealizuotos esminės efektyviam tinklo veikimui svarbios funkcijos, o viena iš silpniausiai ištirtų ir daugiausiai problemų kelianti, tai saugumas.

Informacijos perdavimo tinklu saugumas yra kompleksinis uždavinys, skirtingai sprendžiamas skirtinguose lygiuose (pagal OSI modelį), tačiau ad-hoc tinkluose viena iš labiausiai paplitusių grėsmių – DoS (Denial of Service) atakos tinklo lygmenyje, besiremiančios nesankcionuotu maršruto parinkimo pranešimų modifikavimu.

Magistriniame darbe bus tiriama kaip galima apsisaugoti nuo DoS ir kitokių atakų tinklo lygmenyje, sukurto nesaugaus ad-hoc tinklo modelio aplinkoje bus tiriamos ir lyginamos jau egzistuojančių tradicinio maršruto parinkimo protokolų ir saugaus maršruto parinkimo protokolų savybės, bandoma pasiūlyti ir realizuoti naujų šios srities idėjų, jas taip pat palyginti su jau egzistuojančiais sprendimais, nusakyti tinkamiausius scenarijus jų panaudojimui.

Darbo tikslai ir uždaviniai

Darbo tikslas – sukurti modeliavimo aplinką, skirtą tirti nesaugaus maršrutizavimo protokolus, kurių metu modifikuojami maršruto užklausų ir atsakymų paketai. Darbo tikslui pasiekti reikia spręsti šiuos uždavinius:

- Sukurti savo nesaugaus ad-hoc bevielio tinklo modelį.
- Modeliavimo aplinkoje ištirti saugaus maršrutizavimo protokolo įtaką priešiškoje aplinkoje veikiančio tinklo veikimui.
- Papildyti priešiškų mazgų išvengimo strategija besiremiantį protokolą priešiškų mazgų toleravimo strategijos elementais ir modeliuojant palyginti jo savybes su originaliu algoritmu prieš modifikavimą.
- Parinkti optimalų saugaus maršruto parinkimo protokolą ar jų derinį, geriausiai tinkantį sudarytam mobilaus ad-hoc tinklo modeliui, nustatyti kitų ad-hoc maršrutizavimo protokolų tinkamiausią panaudojimo scenarijų.

1. SAUGAUS MARŠRUTIZAVIMO AD-HOC TINKLUOSE ANALIZĖ

Ad-hoc tinklams negalima tiesiogiai panaudoti tų pačių techninių sprendimų, kurie tinka laidiniams ir centralizuotos architektūros belaidžiams tinklams, nes ad-hoc tinklai yra išskirtiniai daugeliu atžvilgių. Pirmiausia jie neturi fiksuotos ryšio ir saugumo infrastruktūros, t.y. bazinių stočių, maršruto parinkimo įrenginių, RADIUS serverių ir panašiai. Informacija perduodama tiesiogiai tarp tinklo mazgų, o tuomet, kai atstumas tarp siuntėjo ir gavėjo mazgų yra per didelis dėl radijo ryšio aprėpties ribotumo, tenka informacijos perdavimą organizuoti per tarpinius mazgus. Taip pat tinkle mazgų išsidėstymas ir kiekis yra dinamiškas ir nuolat kinta.

Iš daugelio tokiomis sąlygomis kylančių iššūkių, keletas vis dar išlieka atviri, be visuotinai pripažintų pilnai problemą sprendžiančių sprendimų:

- Plečiamumas (Scalability)

Tai savybė, parodanti ar tinklas gali teikti priimtinos kokybės paslaugas dideliam mazgų skaičiui. Visi įrenginiai dalijasi tą pačią ryšio aplinką, todėl spartos dalis tenkanti vienam mazgui proporcingai mažėja plečiantis tinklui. Taip pat didėjant mazgų skaičiui tinkle sparčiai auga maršrutizavimui skirtos informacijos mainų kiekis, saugumo protokolų raktų apsikeitimų skaičius ir kitos tarnybinės informacijos kiekiai.[8]

- Paslaugos kokybė (Quality of Service)

Nepriklausomai nuo besikeičiančių radijo ryšio parametrų, turi būti galimybė užtikrinti tam tikros kokybės, kuri apibrėžiama tokiais parametrais kaip duomenų perdavimo pralaidumas, perdavimo vėlinimas, paketų praradimo koeficientas, maršruto suradimo laikas, palaikymą. Tam pasiekti labai svarbus ad-hoc tinklo maršrutizavimo algoritmų efektyvumas ir specialių paslaugos kokybės (QoS) maršrutizavimo protokolų naudojimas, leidžiantis formuoti skirtingo tipo srautus, juos prioritetizuoti, parinkti maršrutus pagal pageidaujamus kokybės reikalavimus.[1][8]

- Energetinis efektyvumas

Ad-hoc tinkluose paprastai naudojami įvairūs mobilūs įrenginiai, tokie kaip kompiuteriai, delninukai, specializuoti moduliai transporto priemonėse ir panašiai, kurių skaičiavimo galimybės yra labai ribotos, be to jas pilnai apkraunant nukenčia autonomiškumas – greičiau išsinaudoja baterijų energija. Kiekvienas įrenginys ne tik pats keičiasi informacija su kitais įrenginiais, tačiau kartu veikia ir kaip maršrutizatorius kitų įrenginių tarpusavio komunikacijai, todėl procesoriaus skaičiavimų kiekis, reikalingas užmegzti ir palaikyti ryšiui, t.y. maršrutų skaičiavimui, saugumo algoritmų raktų generavimui,

yra labai svarbus parametras, taip pat reikalingi ir kuriami ir kiti, fizinio lygmens sprendimai, tokie kaip bevielio tinklo plokštės galios reguliavimas, užmigdymas nenaudojant ir panašiai.[8]

- Saugumas

Tai kritinė ad-hoc tinklo problema, kadangi tinklas veikia viešoje radijo ryšio terpėje, nėra galimybės centralizuotų sertifikatų ir kriptografinių raktų naudojimui, dažnai dėl savo paskirties veikia padidintos rizikos erdvėje. O be tinkamo saugumo užtikrinimo ši kaip ir bet kokia kita technologija šiais laikais negali būti realiai panaudojama.[1][2]

Dėl naudojamos ryšio technologijos fiziniame lygyje saugumo technologijos neegzistuoja, o taikymo lygmenyje jau galima naudoti įvairias saugumo priemones. Šios priemonės gali apsaugoti nuo konfidencialios informacijos atskleidimo, klastojimo, apsimetimo atakų, tačiau turi būti sukurti specifiniai kriptografinių raktų ad-hoc tinkle apsikeitimo mechanizmai, atsižvelgta ir į saugumo priemonių įtaką paties tinklo veikimui. Pavyzdžiui dėl raktų apsikeitimo paprastumo, labai perspektyviai atrodo asimetrinė viešojo - privataus rakto infrastruktūra, tačiau ji gali sukelti plečiamumo ir energinio efektyvumo problemų, kadangi naudojant šią sistemą reikia daugiau skaičiavimo ir pralaidumo resursų, taip pat pilnam jos veikimui reikalingas centrinis patikimas sertifikatų centras, kurio vaidmenį galima priskirti kuriam nors mazgui, tačiau dėl to jis taps pažeidėjų taikiniu.

Taikymo lygmenyje veikiančios saugumo priemonės nuo dalies grėsmių gali apsaugoti, tačiau negali padėti nuo atakų siekiančių išvesti tinklą iš rikiuotės, blokuoti susijungimus, t.y. DoS (Denial of Service) ir panašių atakų veikiančių tinklo lygmenyje. Tam reikalingi saugūs maršrutizavimo (Security aware routing) protokolai. Ir būtent čia ad-hoc tinklų centrinės infrastruktūros, t.y. vienos silpnos grandies neturėjimas yra didelis privalumas, nes pakenkus vienam taškui, visa sistema nėra išvedama iš rikiuotės. Taip pat kadangi ad-hoc tinkle dažnai tarp siuntėjo ir gavėjo egzistuoja daugiau negu vienas maršrutas, siunčiama informacija gali būti išskaidoma į keletą, siunčiama skirtingais kanalais ir vėl surenkama į vieną vietą tik pasiekusi gavėją, o pakeliui perėmęs tik informacijos fragmentą piktavalis, negalės atskleisti viso pranešimo.[1]

Maršrutizavimas yra bene didžiausia tyrinėjimų sritis mobiliuose ad-hoc tinkluose. Kaip ir įprastuose laidiniuose tinkluose, čia naudojami maršrutizavimo protokolai optimalių maršrutų suradimui. Dažniausias optimalumo matas - šuolių (hop) skaičius. Tinklo mazgai gali laisvai judėti, todėl tinklo topologija gali nuolat keistis. Ad-hoc tinklams sukurti maršrutizavimo protokolai, kurie skirstomi į dvi pagrindines grupes:

- Statiniai paremti lentelėmis (table driven proactive)
- Dinaminiai inicijuojami šaltinio (source initiated reactive)

Statiniai maršrutizavimo protokolai pastoviai laiko informaciją apie visą tinklo topologiją, o jai atnaujinti periodiškai siunčia atnaujinimo paketus. Tokia veiksena yra panaši į dabartinių laidinių tinklų protokolų OSPF (Open Short Path First), RIP (Routing Information Protocol) veikimą. Statiniai protokolai maršruto suradimo greičiu lenkia dinaminius ir yra gana efektyvūs, jei ad-hoc tinklo mazgai beveik nejuda, tinklo topologija ypatingai nesikeičia, tačiau esant dideliam įrenginių mobilumui turima maršrutų informacija sunkiai spėjama atnaujinti pagal situaciją, o atnaujinimo paketai sunaudoja labai didelę dalį tinklo pralaidumo.[11]

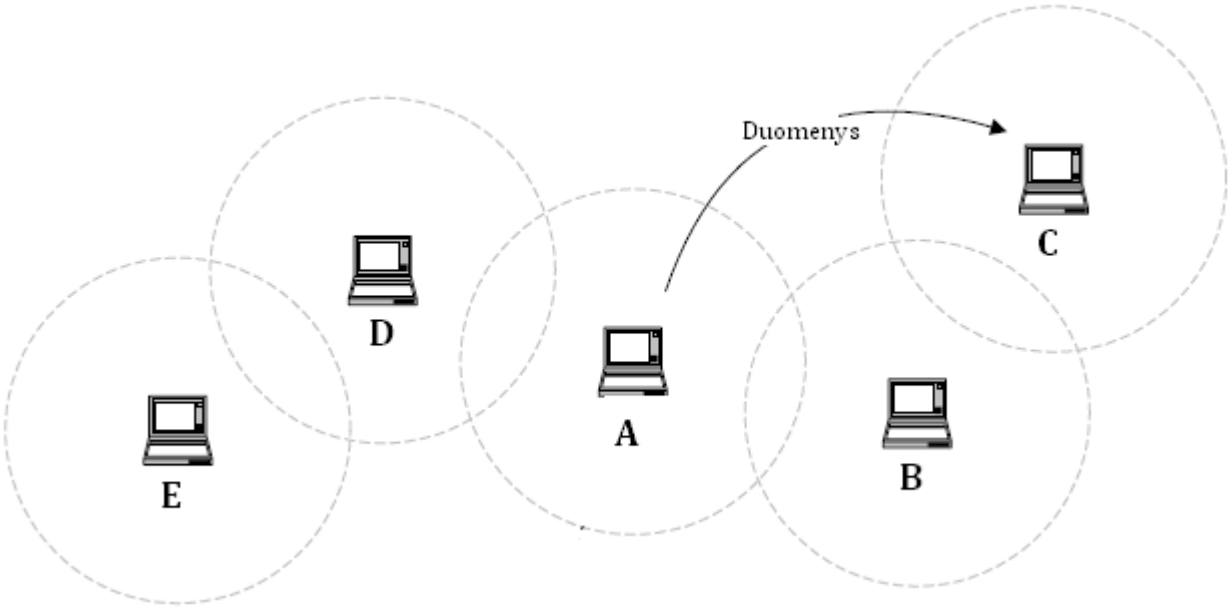
Dinaminiuose maršruto parinkimo protokoluose maršrutas sudaromas tik esant poreikiui persiųsti duomenis. Kai vienas mazgas nori persiųsti duomenis kitam mazgui, jis inicijuoja kelio suradimo procesą, o tarpiniai mazgai savo maršrutų lentelėse informaciją apie surastą kelią saugo tik tol, kol tas kelias naudojamas. Dinaminiuose maršruto parinkimo protokoluose kelio suradimas užtrunka ilgiau nei statiniuose, tačiau jie daug geriau susitvarko su tinklo topologijos pasikeitimais. Dėl šios priežasties pagrindiniai šiuo metu vystomi ir nagrinėjami maršrutizavimo protokolai mobiliems ad-hoc tinklams yra dinaminiai.[11]

1.1. Standartinis ad-hoc maršruto parinkimo protokolas AODV (Ad hoc On Demand Distance Vector)

Iš dinaminių maršruto parinkimo protokolų labiausiai žinomi AODV[6] ir DSR[17], tai vienas iš dviejų populiariausių maršruto parinkimo protokolų. Jis priklauso dinaminių atstumo-vektoriaus protokolų grupei, tai reiškia, kad maršrutas yra sudaromas tik tada, kai reikia siųsti duomenis ir tai, jog sudarius maršrutą siuntėjas neturi visų maršrutą sudarančių mazgų sąrašo, o tik atstumą arba šuolių skaičių iki gavėjo ir sekančio šuolio (next hop) mazgą.

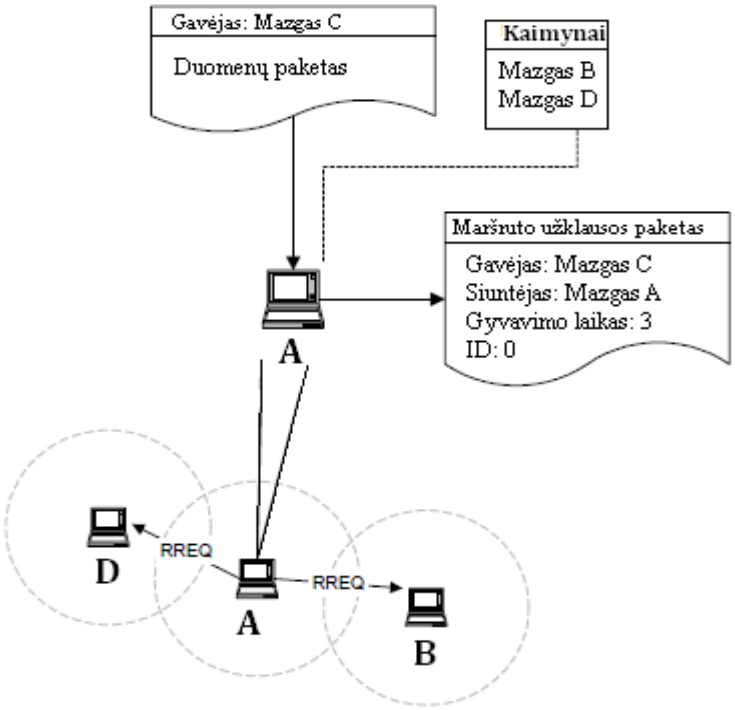
1.1.1. Maršruto sudarymo algoritmas

Mazgui A prireikus perduoti informaciją mazgui C, tikrinama ar laikinoje maršrutų lentelėje yra pakankamai naujas maršrutas iki mazgo C, jei ne – sudaromas naujas maršrutas: [6]



1. pav. AODV veikimas[16]

Transliacijos (broadcast) būdu suformuojamas ir siunčiamas užklausos paketas RREQ visiems kaimyniniams (aprėpties zonoje esantiems) mazgams (2 pav.)

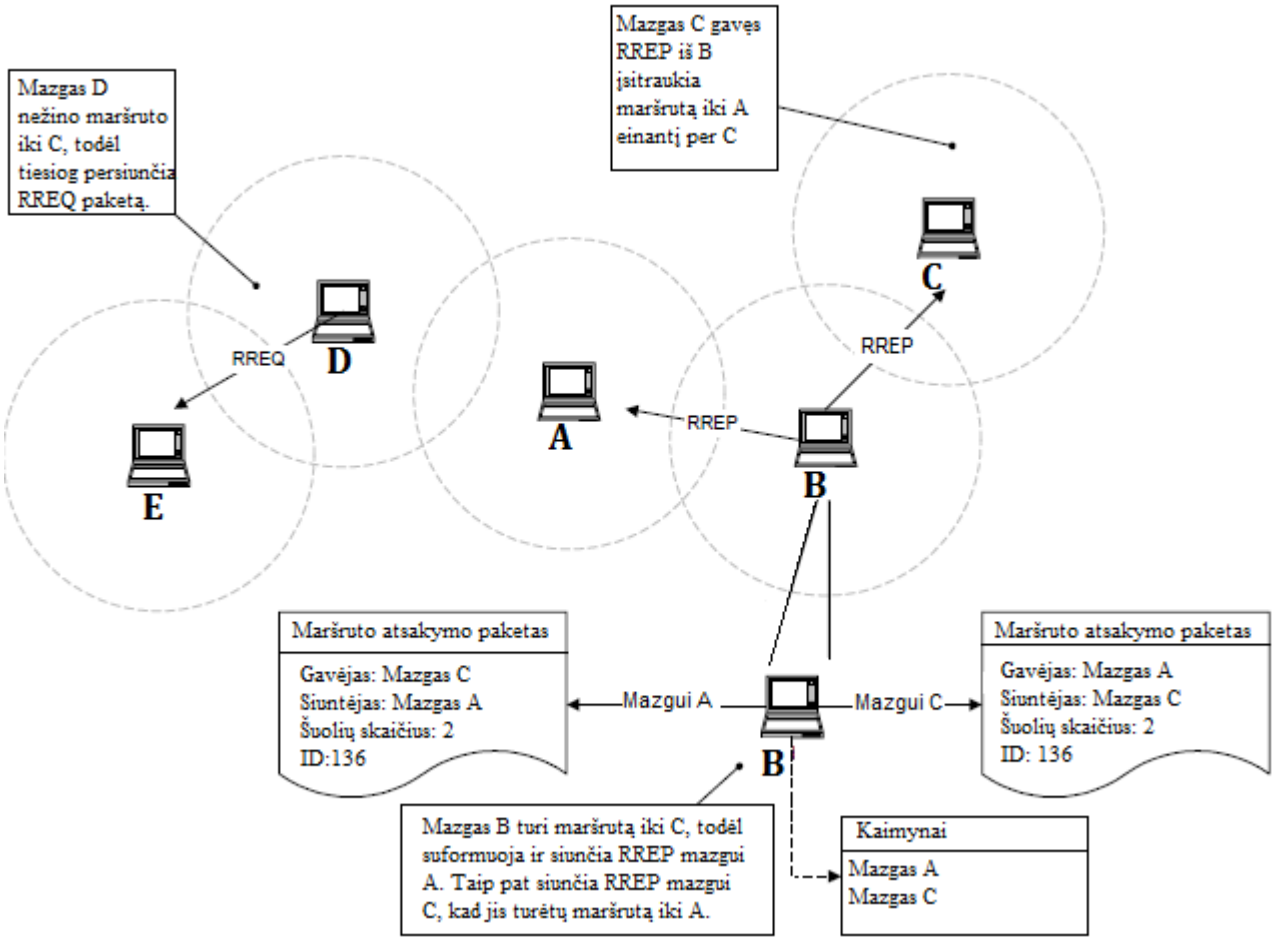


2. pav. AODV RREQ paketo sudarymas ir siuntimas[16]

1. Gavęs paketą RREQ kiekvienas mazgas ieško savo maršrutų lentelėje pakankamai naujo maršruto iki mazgo C, jei neranda – įsitraukia atgalinį maršrutą iki siuntėjo A, su nuoroda, kad

sekantis šuolis yra kaimyninis mazgas iš kurio gautas šis užklausos paketas ir persiunčia RREQ paketą visiems savo kaimyniniams mazgams.

2. Taip užklausa plinta tinklu, kol galiausiai pasiekiamas gavėjas – mazgas C, arba mazgas turintis maršrutą iki C. Tada formuojamas atsakymo pranešimas RREP ir siunčiamas atgal tuo pačiu keliu mazgui A (pagal keliaujant RREQ paketui įsitrauktus maršrutų įrašus), tarpiniai mazgai vėl į savo maršrutų lenteles įsitraukia maršrutą iki mazgo C, su gretimų mazgų adresus su nuoroda, kad sekantis šuolis yra kaimyninis mazgas iš kurio gautas šis užklausos paketas. Tokiu būdu užtikrinama, kad kiekvienas maršrute esantis mazgas galės persiųsti duomenis tarp A ir C mazgų abiem kryptimis. Mazgas C į tą patį užklausos paketą atsako tik vieną kartą, to paties paketo kopijos atkeliavusios per kitus mazgus atmetamos, nes laikoma, kad pirmasis atėjęs užklausos paketas tai padarė greičiausiu maršrutu.



3. pav. AODV veiksmai pasiekus gavėją[16]

3. Mazgas A, gavęs paketą RREP taip pat įsitraukia maršrutą į maršrutų lentelę ir pradeda siųsti juo duomenis.

Standartiškai pagal nutylėjimą visi mazgai laikomi patikimais. Parametrai apibrėžiantys maršruto gerumą yra mazgų maršrute kiekis ir maršruto naujumo skaitiklis. Papildomai yra įdiegtas maršruto nutrūkimo pastebėjimo mechanizmas – tarpinis mazgas pastebėjęs kaimyninio mazgo judėjimą iš ryšio zonos siunčia problemos pranešimą siuntėjui, tuomet siuntėjas pakartoja maršruto sudarymo procedūrą.

Šis protokolas efektyviai sprendžia tinklo topologijos kaitos problemą: jei tik maršrutas egzistuoja - jis visuomet randamas, papildomi skaičiavimai ir maršrutizavimo paketų dydžiai nėra dideli. Tačiau taip pat jis palieka daug galimybių kenkti ad-hoc tinklui maršrutizavimo lygmenyje.

1.1.2. Pagrindinės ad-hoc tinklų maršrutizavimo lygmens saugumo grėsmės

Ad-hoc tinkle kiekvienas tinklo mazgas privalo perduoti paketus gautus iš savo kaimyno kitam kaimyniniam mazgui, esančiam arčiau šaltinio. Tik kaimyninių mazgų bendradarbiavimas gali užtikrinti, kad informacija bus perduota iš siuntėjo gavėjui, todėl, jei atsiranda mazgas, kuris savo funkciją atlieka ne taip, kaip turėtų dėl techninių problemų ar dėl tyčinių suinteresuotų asmenų veiksmų, kyla įvairios grėsmės viso ad-hoc tinklo veikimui. Dėl šios priežasties saugaus maršrutų parinkimo protokolai tokie svarbūs.

Pagrindinės standartinių maršrutizavimo protokolų saugumo grėsmės (spragos) yra šios:

- Pasitikėjimas mazgais pagal nutylėjimą[2]

Dauguma dabartinių ad-hoc maršruto parinkimo protokolų pagal nutylėjimą visus mazgus laiko patikimais, vieninteliu maršruto gerumo įverčiu laikomas jo trumpumas, nėra galimybės identifikuoti mazgo patikimumo ir pagal tai parinkti atitinkamas saugos priemones, todėl piktavaliai mazgai nesunkiai pakliūna į duomenų perdavimo maršrutus ir turi galimybes perimti arba naikinti duomenis.

- Galimybė kenkiančiam mazgui apsimesti gavėju[1]

Kenkiantis mazgas gali neperduoti toliau maršruto parinkimo užklausos, o iš karto gražinti savo suklastotą maršruto parinkimo atsakymą, tarsi pats ir būtų gavėjas, tokiu būdu arba maršruto sudarymas tampa neįmanomu, arba gavėjui skirti duomenys siunčiami piktavaliui mazgui.

- Maršruto parinkimo įtakojimas keičiant maršrutizavimo pranešimų parametrus[2]

Kenkiantis mazgas gali neadekvačiai padidinti maršruto naujumo parametrą arba sumažinti mazgų maršrute skaičių, tokiu atveju per jį einantis maršrutas turės didžiausią prioritetą ir paketai eis per jį, o jis galės tuos paketus blokuoti, bandyti atskleisti ar modifikuoti jų turinį.

- Suklastotų pranešimų apie problemą siuntimas[2]

Kenkiantis mazgas gali pasinaudoti AODV algoritmo maršruto nutrūkimo pastebėjimo mechanizmu ir siųsti suklastotus pranešimus apie problemą aktyviame maršrute. Jei kenkiantis mazgas nuolat stebi

tinklą ir tik sukūrus naują maršrutą vėl siunčia pranešimus apie problemą jame, visiškai blokuojamas ryšys tarp dviejų mazgų.

1.2. Saugūs maršruto parinkimo protokolai

Šioje srityje aktyviai vyksta tyrimai ir mokslinėje literatūroje minima nemažai įvairių saugaus maršrutų parinkimo protokolų:

- Ariadne [14]
- TARP – Trust-aware Routing Protocol [18]
- SELRAN - A Secure and Efficient Link State Routing Protocol for Ad Hoc Networks [19]
- SAODV – Security Aware AODV) [12]
- SRP – Secure Routing Protocol [3]
- SAR – Security Aware Routing [1]

Paskutinius tris protokolus analizės dalyje nagrinėsime plačiau.

1.2.1. SAODV (Security-aware AODV) protokolas

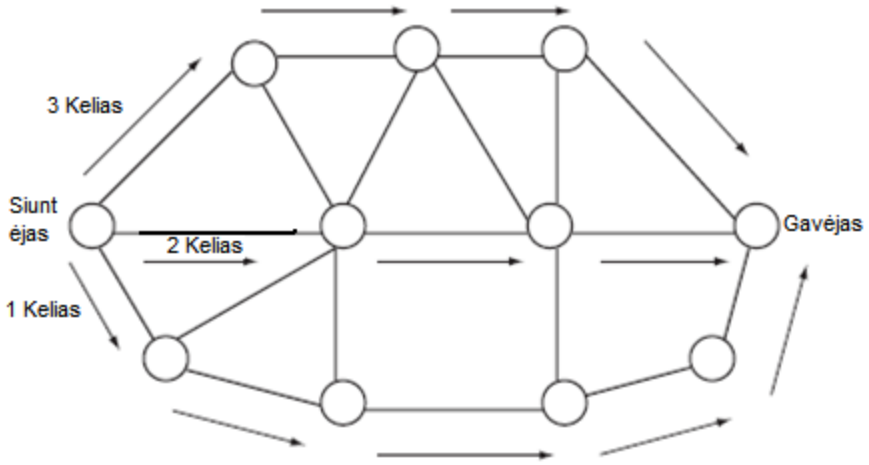
SAODV protokolas yra AODV protokolo išplėtimas, kuriame pasirūpinama maršrutizavimo paketų apsaugojimu, užtikrinant jų integralumą ir autentifikaciją. Siuntėjas, siųsdamas RREQ paketą, jį pasirašo savo privačiuoju raktu, o tarpiniai mazgai tik patikrinę parašo tikrumą, įsitraukia į maršrutų lenteles maršrutą iki siuntėjo mazgo, kuriame artimiausiu šuoliu nurodytas kaimyninis mazgas, iš kurio atėjo šis užklausos paketą ir persiunčia paketą toliau. Kai paketas pasiekia gavėją, gavėjas siunčia atgal RREP paketą jį taip pat pasirašęs savo privačiuoju raktu, o tarpiniai mazgai atlieka tuos pačius veiksmus, kaip ir su RREQ paketu.

1.2.2. SRP(Secure Routing Protocol) ir SMT(Secure Message Transmission) protokolai

Dauguma ad-hoc maršruto parinkimo protokolų gali būti padalinti į dvi dalis: maršruto radimą ir duomenų perdavimą rastuoju maršrutu. Abiems šioms dalims būtini papildomi saugumo sprendimai greta standartinio maršruto parinkimo protokolo, kuris kaip jau minėjome anksčiau, neturi beveik jokių saugumo užtikrinimo priemonių. Pirmoji dalis labiausiai jautri atakoms paremtoms apsimetimu gavėju, pasenusios ar piktybiškai modifikuotos maršruto parinkimo informacijos skleidimu. Antroji dalis atvira paketų naikinimo, modifikavimo, klaidingo nukreipimo atakoms. SRP(Secure Routing Protocol)[3] ir SMT(Secure Message Transmission)[4] protokolai buvo sukurti užtikrinti saugumą abiejose šiose dalyse.

1.2.2.1. Saugaus maršrutizavimo protokolas – SRP

Naudojant šį protokolą, ad-hoc tinklo darbas įmanomas net ir jame esant kenkiančių elementų. Protokolo funkcionavimui turi būti įkurta Saugumo Asociacija (SA), t.y. apsikeista slaptaisiais raktais tarp siuntėjo ir gavėjo mazgų. Iš kitos pusės nėra keliama jokių kriptografinių užduočių tarpiniams mazgams, todėl jie nėra papildomai apkraunami. SRP protokole prireikus sudaryti maršrutą siunčiamas užklausos paketas, kuris kaupia savyje visų mazgų IP adresus, kuriuos praeina, o kai pasiekia gavėją, tuo pačiu maršrutu atgal siunčiamas atsakymo paketas. Joks kitas mazgas negali apsimesti gavėju dėl įkurtos SA, nes neturi gavėjo saugumo raktų, taip pat negali modifikuoti grįžtančio paketo IP adresų sąrašo, nes jis apsaugotas santraukos (hash) funkcija paremta pranešimo autentifikacijos funkcija HMAC (Message Authentication Code)[5]. Tą patį paketą vienas mazgas persiunčia tik vieną kartą, jei ateina dar vienas paketas su tokiu pačiu ID, jis atmetamas. Dar vienas skirtumas nuo kitų maršruto parinkimo protokolų – siuntėjas išsaugo visus grįžusius atsakymo paketus, t.y. suformuojami visi įmanomi maršrutai į kuriuos kiekvienas tinklo mazgas įeina ne daugiau kaip vieną kartą.(2 pav.) Tai yra daroma dėl toliau sekančio SMT protokolo specifikos.



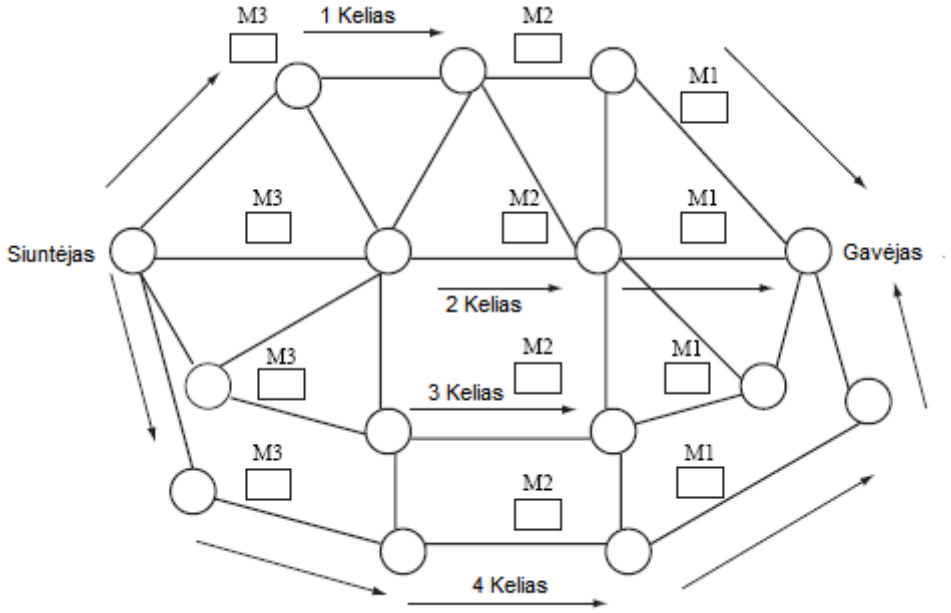
4. pav. 3 maršrutai nuo siuntėjo iki gavėjo[1]

1.2.2.2. Saugaus informacijos perdavimo protokolas – SMT

SRP protokolui suformavus maršrutus, informacijos perdavimo užduotis realizuojama SMT protokole. Tai jau nebe maršruto parinkimo protokolas, tačiau jis glaudžiai susijęs su prieš tai minėtu SRP maršruto parinkimo protokolu.

SMT protokole siuntėjo mazgas padalina siunčiamą pranešimą į kelias dalis panaudodamas IDA (Information Dispersal Algorithm) algoritmą[14], dalių skaičius priklauso nuo SRP protokolo sugeneruotų

maršrutų kiekio (Pav. 3). Padalinimui naudojamas perteklinis algoritmas, kuris užtikrina, kad pranešimą galima rekonstruoti netgi gavus ne visas dalis, kadangi kai kurios dalys gali būti prarastos dėl tinklo trikdžių ar kenkiančių mazgų. Kiekviena siunčiama dalis apsaugoma HMAC funkcija, todėl tarpiniai mazgai negali jų modifikuoti ar klastoti taip, kad to nepastebėtų gavėjas. Gavėjas, gavęs pranešimo fragmentus, grąžina patvirtinimus kiekvienam fragmentui, kuriuos irgi apsaugo HMAC funkcija. Siuntėjas tuo metu pagal gautus patvirtinimus keičia maršrutų reitingus, t.y. pakelia reitingą, jei perdavimas pavyksta ir smarkiai sumažina, jei dėl kažkokių priežasčių nepavyksta, tokiu būdu minimizuojamas informacijos srautas per kenkiančius mazgus.

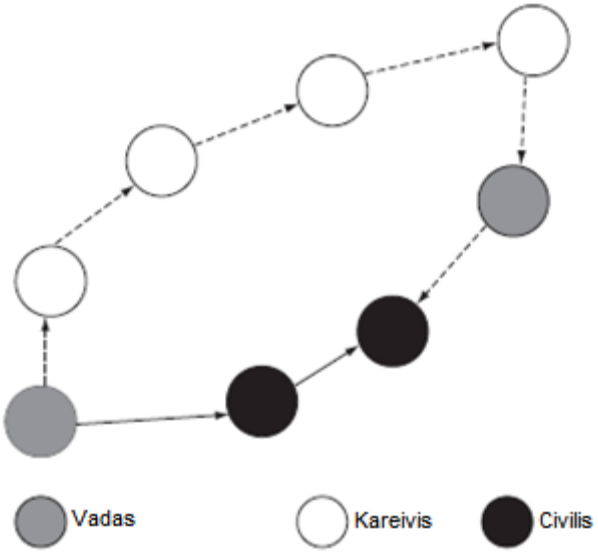


5. pav. Informacijos skaldymas į fragmentus[1]

1.2.3. Security aware routing – SAR protokolas

SAR protokolas gali papildyti įvairius dinaminius maršrutizavimo protokolus. Šiame protokole mazgai nebėra patikimi pagal nutylėjimą, jiems priskiriamas tam tikras patikimumo lygmens įvertis, kuris lemia maršruto pasirinkimą, kartu su standartiškai naudojamu maršruto ilgio įverčiu. Saugumo lygį apibrėžia iš anksto nustatyta vieta hierarchinėje struktūroje ir mazgo turimos saugumo užtikrinimo galimybės. Šis algoritmas prideda papildomus saugumo lygio laukus RREQ ir RREP paketams. Reikalingą saugumo lygį nustato siuntėjas, o to lygio negalintys patenkinti mazgai paketus atmeta. Suformavus maršrutą grįžtančiame RREP pakete įtraukiamas mažiausiai saugaus maršruto mazgo saugumo lygis kaip viso maršruto saugumo parametras.[7]. Praktinis vaizdas 6 pav. - balti, kareivių

mazgai turi aukštesnį saugumo lygį, negu juodi civilių mazgai, tad pasirenkamas nors ir ilgesnis, bet saugesnis maršrutas.



6. pav. SAR pavyzdys[1]

Tokia galimybė ne tik leidžia keisti reikalaujamą maršruto patikimumo lygį priklausomai nuo situacijos, pasirinkti atitinkamas taikymo lygio apsaugos priemones priklausomai nuo didžiausio įmanomo maršruto patikimumo lygio, bet ir užtikrinti maršrutizavimo paketų konfidencialumą. Dažnai pasitaiko atvejų, kad pats dviejų mazgų komunikavimo faktas kenkiančiam mazgui suteikia tam tikrą informaciją, pavyzdžiui karinio scenarijaus atveju, intensyvi komunikacija tarp būrių vadų galėtų signalizuoti apie rengiamą puolimą.[1]

Protokolo autoriai tiksliai apibrėžia maršrutizavimo paketų išplėtimus ir tarpinių mazgų elgesį priklausomai nuo patikimumo lygio atitikimo, tačiau neapibrėžiamos saugos priemonės skirtos užtikrinti korektišką mazgų elgesį, patikimumo lygio reikalavimo vientisumą ir jo laikymąsi.[7]

Tokių priemonių parinkimas būtinas tam, kad protokolas galėtų veikti realiuose mobiliuose ad-hoc tinkluose, vienas iš patikimumo lygio reikalavimo laikymosi galėtų būti vienam patikimumo lygiui priklausančių mazgų apsikeitimas slaptu raktu ir RREP paketų šifravimas simetriniu šifravimo algoritmu panaudojant bendrą slaptą raktą. Tokiu atveju mazgas, nesantis pakankamo patikimumo lygio, net nepamatytų RREP paketo turinio ir jį galėtų tik numesti, o patikimas mazgas dešifruotų, pakeistų reikiamus laukus ir vėl užšifravęs persiųstų paketą toliau.

1.2.4. Trūkumai

SAR protokolo pagrindinis trūkumas realiai veikiančiame ad-hoc tinkle yra tai, kad jis nėra visiškai išbaigtas sprendimas ir išsprendžia tik dalį saugumo problemų.

Naudojant SRP ir SMT protokolus kartu, gaunamas gan išbaigtas ir nuo beveik visų pagrindinių saugumo problemų apsaugantis sprendimas, tiesa ir jis turi silpnų vietų. Jo darbą gali sutrikdyti du kenkiantys ir kartu veikiantys mazgai, fiziškai esantys greta vienas kito, taip pat kenkiančiam mazgui gadinant maršrutizavimo paketo ID, tai pastebima tik gavėjo mazge, o kiti tarpiniai mazgai siuntinėja paketus kaip naujus ir padidina tinklo apkrovimą.

1.3. Skirtingų protokolų atsakas į pagrindines saugumo grėsmes

1. Lentelė. Protokolų atsakas į saugumo grėsmes

Grėsmė	**SAR**	**SRP**	**SMT**
Pasitikėjimas mazgais pagal nutylėjimą	Išsprendžiama įtraukiant reitingavimą pagal hierarchinę struktūrą ir mazgų technines saugumo galimybes.	Nesprendžiama, tačiau nepaliekama būdo kenkiantiems mazgams daryti didelę įtaką tinklo veikimui.	Išsprendžiama izoliuojant kenkiančius mazgus, jei jie elgiasi ne taip kaip iš jų tikimasi.
Galimybė kenkiančiam mazgui apsimesti gavėju	Išsprendžiama panaikinant galimybes paketui pasiekti kenkiantį mazgą, t.y. neleidžiant patekti jei kenkiančio mazgo saugumo lygis yra nepakankamas	Išsprendžiama įkuriant SA tarp siuntėjo ir gavėjo mazgų.	Nesprendžiama, tai išspręsta SRP protokole.
Maršruto parinkimo įtakojimas keičiant maršrutizavimo pranešimų parametrus	Išsprendžiama panaikinant galimybę paketui pasiekti kenkiantį mazgą, t.y. neleidžiant patekti jei kenkiančio mazgo saugumo lygis yra nepakankamas	Išsprendžiama apsaugant parametrus MAC hash funkcija, tokiu būdu bet koks jų pakeitimas būtų pastebėtas siuntėjo arba gavėjo ir būtų atmetamas.	Nesprendžiama, tai išspręsta SRP protokole.
Suklastotų pranešimų apie problemą siuntimas	Reikalinga modifikacija.	Nesprendžiama, tai išspręsta SMT protokole.	Naudojamos kitos tinklo priežiūros priemonės, siuntėjas pats stebi maršrutų gyvybingumą, be to

			dažniausiai yra daugiau negu vienas maršrutas.

1.4. Protokolų klasifikacija pagal sąveiką su kenkiančiais mazgais

Nors ad-hoc tinklai yra sąlyginai pradinėje vystymosi stadijoje ir kol kas komerciškai nėra labai plačiai taikomi, o jų sauga – dar mažiau ištirta sritis, tačiau mokslinė visuomenė labai intensyviai dirba kurdama naujus saugius protokolus, būdus saugiai komunikacijai ad-hoc tinkluose. Nors sprendimų daug, įvairių ir skirtingų, pagal sąveikos su kenkiančiais mazgais strategiją juos galima suskirstyti į dvi šakas: vengiančius kenkiančių mazgų ir toleruojančius kenkiančius mazgus. [3, 4]

1.4.1. Vengimo strategija

Vengimo strategijos besilaikančių maršrutizavimo protokolų pagrindinis tikslas dar pradinėje maršruto parinkimo stadijoje pastebėti bet kokią mazgų veiklą, nepatenkančią į protokolo veikimo taisykles ir šiuos mazgus eliminuoti iš savo maršrutų. Tai stipriai saugumą maršruto lygmenyje padidinanti strategija, tačiau ji kartu ir stipriai mažina tinkamų informacijos perdavimui maršrutų kiekį. Tai nesukelia problemų, kai tinkle yra nedaug kenkiančių mazgų, tačiau jei kenkiančių mazgų kiekis tinkle yra didelis, gana dažnai susidaro situacijos, kai išvis nelieka tinkamų maršrutų duomenų perdavimui ir informacija nepasiekia gavėjo, paketų praradimai tampa labai dažni. Iš kitos pusės, nors šios strategijos protokolai jau maršruto parinkimo lygyje labai stipriai sumažina tikimybę, kad informacija paklius kenkiančiam mazgui, tačiau visiškai tokios galimybės neeliminuoja, todėl nepašalina poreikio papildomai apsaugai aukštesniuose lygiuose, pvz. kaip duomenų paketų šifravimas. Vienas iš tokių scenarijų būtų atvejis, kai maršruto parinkimo fazėje kenkėjiškas mazgas neatlieka jokių nesankcionuotų veiksmų, kurie galėtų jį išduoti, tačiau pakliūna į informacijos perdavimo maršrutą atsitiktinai ar apgalvotai pasirinkęs palankią poziciją erdvėje.

Protokolai SAODV ir SAR priklauso kenkiančių mazgų vengimo strategijai.

1.4.2. Toleravimo strategija

Toleravimo strategijos pagrindimas remiasi prielaida, jog kenkiantiems mazgams duomenų perdavimo fazėje daug mažiau apsimoka trikdyti tinklo veiklą, naikinti per juos einančius duomenis, nei stengtis prisitaikyti prie tinklo veikimo ir bandyti periminėti, klastoti pro juos tekančią informaciją. Todėl parenkant maršrutą nesistengiama iš karto izoliuoti kenkiančius mazgus, tačiau jau parinkus maršrutą, labai atidžiai stebima informacijos perdavimo fazė, reikalaujant, kad gavėjas siųstų patvirtinimus kiekvienam išsiųstam paketui ir negavus kelių tokių patvirtinimų daroma išvada apie blokuojantį piktavalį

mazgą ir tokiu maršrutu daugiau nebesinaudojama. Taip pat vykdoma ir duomenų integralumo, autentiškumo kontrolė ir atitinkamai reaguojama į jos pažeidimus. Tačiau jei į maršrutą pakliuvęs piktavalis mazgas tvarkingai perduoda visus paketus, skirtingai nuo vengiančią strategiją naudojančių protokolų, toks maršrutas sėkmingai naudojamas. Žinoma čia labai atviras informacijos konfidencialumo klausimas, todėl papildomos saugos priemonės aukštesniuose lygiuose tampa absoliučiai neišvengiamos, jei norima konfidencialumą užtikrinti. Ši strategija dažniausiai užtikrina daug didesnį sėkmingai perduotų paketų procentą tinkluose kur kenkiančių mazgų kiekis yra didelis, tačiau kaip jau minėjau- daro šiokius tokius kompromisus saugos srityje.

Šią strategiją naudoja SRP protokolas.

2. Lentelė Sąveikos su kenkiančiais mazgais strategijų palyginimas

Kenkiančių mazgų vengimo strategija	**Kenkiančių mazgų toleravimo strategija**
Pastangos blokuoti, izoliuoti kenkiančius mazgus	Bandymas kooperuoti, imantis atitinkamų saugos priemonių
Svarbiausias prioritetas – informacijos integralumo ir konfidencialumo pažeidimo rizikos minimizavimas	Svarbiausias prioritetas – paslaugos pateikiamumas
Pagrindinės strategijai būdingos funkcijos realizuojamos maršruto parinkimo metu	Pagrindinės strategijai būdingos funkcijos realizuojamos duomenų perdavimo metu
Palyginus su standartiniu algoritmu, sumažina konfidencialumo pažeidimų riziką, tačiau jos neeliminuoja.	Maršruto parinkimo lygmens priemonėmis konfidencialumo pažeidimų rizika nėra sumažinama.

Abi strategijos turi tiek privalumų, tiek trūkumų, kiekviena turi savo specifinius pritaikymo scenarijus, na o šio darbo metu kuriamas ir tiriamas protokolas, apjungiantis abiejų strategijų kertines savybes, tuo pačiu pasižymintis abiejų protokolų privalumais.

2. SAUGIŲ AD-HOC MARŠRUTO PARINKIMO PROTOKOLŲ TYRIMO PROJEKTAS

2.1. Projekto perspektyva

Sukurtas mobilaus ad-hoc bevielio tinklo modelis leis modeliuoti ir tirti ad-hoc tinklo veikseną, saugumo, atsparumo, plečiamumo, greitaveikos, energetinio reiklumo savybes naudojant įvairius saugaus maršruto parinkimo protokolus. Tai aktualu, nes fizinis bandomojo pakankamo dydžio ad-hoc tinklo sukūrimas yra gan komplikuotas, o kiekvieno protokolo, kurį planuojama panaudoti realiai, veikimą ir savybes labai svarbu ištirti modeliuojant jo veiklą.

2.2. Sprendimo tikslai ir uždaviniai

- Sukurti savo ad-hoc bevielio tinklo modelį.
- Realizuoti modeliavimo aplinkoje ir modeliuojant ištirti populiaraus saugaus SAODV maršrutizavimo protokolo įtaką priešiškoje aplinkoje veikiančio tinklo veikimui.
- Papildyti priešiškų mazgų išvengimo strategija besiremiantį SAODV protokolą priešiškų mazgų toleravimo strategijos elementais ir modeliuojant palyginti jo savybes su originaliu algoritmu prieš modifikavimą.
- Parinkti optimalų saugaus maršruto parinkimo protokolą ar jų derinį, geriausiai tinkantį sudarytam mobilaus ad-hoc tinklo modeliui.

2.3. Sprendimo metodai ir priemonės

Ad-hoc bevielio tinklo modelis sukurtas C++ programavimo kalba, panaudojant modeliavimo įrankio NS-3 bibliotekas. Kadangi NS-3 įrankyje šiuo metu dar nėra realizuota saugių ad-hoc tinklų maršrutizavimo algoritmų NS-3 bibliotekos papildytos tyrimui reikalingomis saugos savybėmis. Artimo realioms sąlygoms dydžio bandomoji realizacija būtų perdaug sudėtingai įgyvendinama, būtent dėl to bus naudojamas programinis modelis.

2.4. Saugaus mobiliojo ad-hoc bevielio tinklo maršrutizavimo protokolo reikalavimų specifikacija

2.4.1. Funkciniai reikalavimai

- Protokole naudojamas adaptyvus maršruto parinkimo algoritmas.

Nors adaptyvūs algoritmai parinkimo proceso metu sukuria daugiau papildomų duomenų srautų, tačiau mobiliame, nuolat kintančiame ad-hoc tinkle efektyviai gali veikti tik adaptyvus maršruto parinkimo algoritmas.

- Užtikrinamas siuntėjo ir gavėjo autentifikavimas ir nėra galimybių tarpiniam mazgui apsimesti siuntėju arba gavėju.

Šis reikalavimas svarbus tuo, kad pavyktų apsisaugoti nuo apsimetimo gavėju ar siuntėju su tikslu perimti siunčiamus duomenis ar iškreipti tinklo darbą.

- Kontroliuojamas maršruto formavimo tarpinės informacijos integralumas.

Viena iš populiariausių ad-hoc tinklų atakų – maršruto užklausos ir atsakymo paketų parametrų modifikavimas, siekiant nukreipti kuo didesnę dalį duomenų srauto per kenkiantį mazgą, todėl maršruto lentelė privalo būti patikimai apsaugota, kad atsiradus bet kokiems nesisteminiams pakeitimams, tai matytų tiek gavėjas, tiek siuntėjas.

2.4.2. Nefunkciniai reikalavimai

- Maršrutizavimas sklandus ir nematomas vartotojui.

Maršruto parinkimo protokolas turi veikti sklandžiai, kad vartotojas nesusidurtų su nerastų, laiku neatnaujintų maršrutų problemomis, kitaip tinklas vartotojams nebus patrauklus ir greitai praras aktualumą.

- Maršruto parinkimas pakankamai spartus ir stipriai neįtakojantis viso tinklo spartos įvairaus dydžio ad-hoc tinkluose.

Maršruto parinkimui reikia nemažai papildomai persiunčiamos informacijos, tačiau informacijos neturėtų būti tiek, kad visas tinklas užsitvindytų ir taptų nepralaidus.

- Protokolo veikimas užtikrintas, t.y. jei maršrutas egzistuoja, jis visada randamas.

Neužtikrintai veikiant maršruto parinkimo algoritmui, tinklo paslaugos pateikiamumas bus labai prasto lygio ir tai atbaidys vartotojus.

- Aukštas paslaugos pateikiamumas esant dideliam kenkiančių mazgų kiekiui ir jų aktyvumui tinkle.

Net veikiant labai priešiškoje terpėje, turi būti užtikrintas maksimaliai sėkmingas informacijos perdavimas.

2.5. Ad-hoc tinklo modelio savybės

- Problemos sprendimui bus modeliuojamas fiksuoto mazgų kiekio ad-hoc tinklas.
- Ne didesniu nei signalo aprėpties atstumu vienas nuo kito nutolę mazgai visada galės tarpusavyje komunikuoti tiesiogiai, tarp mazgų nėra papildomų kliūčių.
- Aplinkos trukdžių fiziniame lygmenyje, t.y. pašalinių radijo signalų įtaka nebus modeliuojama.
- Tarp komunikuojančių mazgų egzistuoja iš anksto saugos asociacija, t.y. jie pasikeitę slaptaisiais raktais, SA įkūrimo procesas ir jo įtaka nemodeliuojami.
- Kintanti dalis mazgų tinkle yra kenkiantys, modeliuojamas įvairus nesankcionuotas veikimas ir stebimas protokolo atsparumas jam.
- Likusi mazgų dalis nekenkiantys, nesavanaudžiai, bet ir neturintys slaptų raktų mazgai.

2.6. Tiriamo maršrutizavimo protokolo aprašymas

Remiantis sudarytais reikalavimais protokolui, kaip bazinis protokolas pasirinktas ir tiriamas AODV protokolas [6]. Jis su tam tikrais pakeitimais išplėstas SAODV (Security-aware AODV) [12] saugumo savybėmis, o taip pat dalimi SRP/SMT [3, 4] protokolo funkcijų, realizuojančių kenkiančių mazgų toleravimo strategijos savybes.

SAODV protokole maršrutizavimo paketų integralumas, autentiškumas ir mazgų identifikacija užtikrinama naudojant paketų antraščių pasirašymą asimetriniais raktais, tačiau šiam tyrimui naudojama modifikacija, paremta simetriniais raktais ir HMAC antraščių santraukomis. Taip pat SAODV protokole į kriptografinius veiksmus, t.y. parašo tikrinimą įtraukiami visi tarpiniai mazgai, todėl yra poreikis, kad visi tinklo mazgai turėtų siuntėjo ir gavėjo viešuosius raktus, tokiu atveju reikalinga tam tikra infrastruktūra tinkle, skirta tų raktų dalijimuisi, o tai šiek tiek iškreipia ad-hoc tinklo idėją. Tiriamoje modifikacijoje tarpiniai mazgai jokių su saugumu susijusių veiksmų neatlieka. Nors šis protokolas ir nebus tiksli SAODV realizacija, tačiau paprastumo dėlei simuliacijos rezultatus žymėsime būtent šiuo vardu.

Maršruto sudarymo algoritmas:

1. Siuntėjas nori siųsti duomenis, jis sukuria SAODV RREQ paketą, kurį sudaro tokie laukai:

- Siuntėjo adresas (source_addr)
- Siuntėjo skaitiklio reikšmė (source_sequence_#)
- Užklausos identifikatorius (rrequest_id)
- Gavėjo adresas (dest_addr)
- Gavėjo skaitiklio reikšmė (destination_sequence_#)
- Šuolių kiekis (hop_cnt)
- Antraštės nekintančių laukų HMAC santrauka(digest)

2. Prieš siųsdamas RREQ paketą, siuntėjas panaudodamas slaptą raktą sugeneruoja jo antraštės nekintančių laukų santrauką, ją prideda į paketo antraštę ir siunčia visiems aplinkiniams mazgams.

Laikoma, kad raktais pasidalinta iš anksto arba jau esant mobiliame ad-hoc tinkle, tai gali būti padaryta pasinaudojant kokiu nors (pvz. Diffie-Hellman, IKE ar panašiu) saugiu raktų apsikeitimo algoritmu arba tiesioginio apsikeitimo būdu dar prieš pradedant darbą priešiškame ad-hoc tinkle.

3. Tarpiniai mazgai, persiųsdami paketą keičia tik šuolių kiekio lauką, kuris nėra apsaugotas santrauka.
4. Kai RREQ paketas pasiekia gavėją, jis panaudodamas tą patį slaptą raktą taip pat suformuoja santrauką ir patikrina, ar apsaugoti antraštės laukai nebuvo pakeliui modifikuoti. Tuomet formuojamas RREP paketas, kurio antraštė taip pat apsaugoma HMAC santrauka ir siunčiamas atgal siuntėjui. Gavėjas atsako tik į pirmą gautą korektišką RREQ paketą, kitus paketus atmeta.
5. Pakeliui tarpiniai mazgai taip pat įsitraukia į maršrutų lenteles grąžinančius gretimus mazgus.
6. RREP paketui pasiekus siuntėjo mazgą, maršrutas įtraukiamas į maršrutų lentelę ir pradedami siųsti duomenys. Jei kažkuris maršruto mazgas tampa nepasiekiamas, kaimyniniai mazgai generuoja problemos pranešimą ir jį gavęs siuntėjas kartoja maršruto sudarymo procedūrą iš naujo.

Papildžius protokolą SRP/SMT protokolo savybėmis, algoritmas iki 4 punkto elgiasi taip pat, o toliau veiksena šiek tiek keičiasi:

4. RREP paketas papildomas nauju lauku IsMalicious, jame pažymima, jei buvo pastebėtas neatitikimas tarp RREQ antraštės ir jo santraukos, tačiau paketas neatmetamas. Taip pat atsakoma ne tik į pirmąjį atėjusį RREQ paketą, bet ir į visus kitus.
5. Pakeliui tarpiniai mazgai įsitraukia į maršrutų lenteles grąžinančius tarpinius mazgus, išskyrus atvejus, kai jau egzistuoja maršrutas, kurio siuntėjas, gavėjas ir sekantis šuolis sutampa.

6. RREP paketui pasiekus siuntėjo mazgą, maršrutas įtraukiamas į maršrutų lentelę, jei nėra jau egzistuojančio maršruto su tuo pačiu siuntėju, gavėju ir sekančiu šuoliu, taip pat į maršrutų lentelę įtraukiama lauko IsMalicious reikšmė. Kol yra nors vienas maršrutas nenurodytas kaip turintis kenkiantį mazgą, duomenys siunčiami juo, tačiau išsiųstas paketas iš eilės pašalinamas tik tada, kai gaunamas patvirtinimas, jog paketas gautas. Jei patvirtinimas neateina per nustatytą laiko tarpą, maršruto reitingas mažinamas ir kartojamas paketo siuntimas kitu maršrutu, kurio reitingas didesnis. Jei visų maršrutų reitingas pasiekia 0, o paketas vis tiek nenueina gavėjui, iš naujo kartojama maršruto parinkimo procedūra.

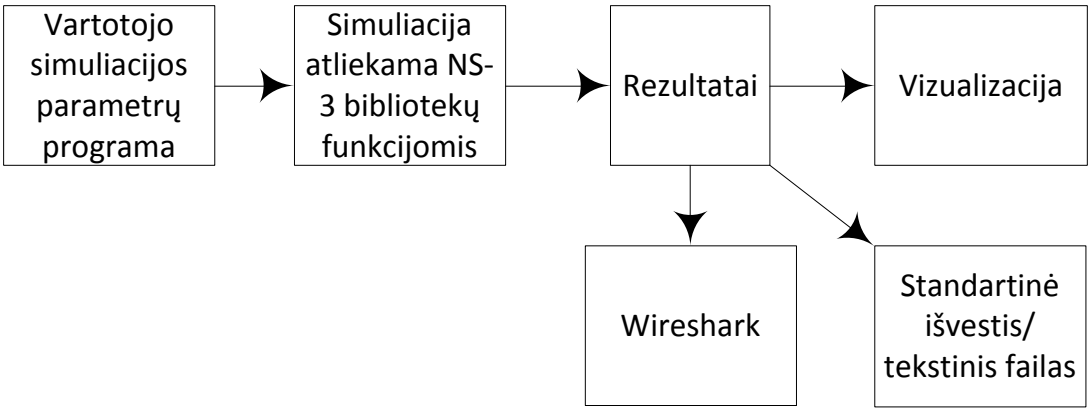
Protokolo su tokiu veikimo algoritmu moksliniuose šaltiniuose man nepavyko rasti, todėl paprastumo dėlei simuliacijos rezultatuose jį žymėsiu vardu SAODV+.

3. MODELIAVIMO APLINKA

Tinklo veikimo ir saugos simuliavimui buvo naudojamas Network Simulator 3 (ns-3) [9] programinis paketas.

3.1. Network Simulator

Network Simulator 3 (toliau ns-3) paketas vystomas Vašingtono universitete. Jis leidžia simuliuoti įvairius laidinius ir bevielius tinklo protokolus, įskaitant ir ad-hoc tinklus. Simuliatorius parašytas C++ programavimo kalba taip pat kai kurioms funkcijoms panaudojama Python programavimo kalba. C++ kalbos programėlėmis vartotojas aprašo tinklo parametrus (mazgų kiekį, ryšius tarp jų), duomenų srautus (siuntėjai, gavėjai, srauto tipas) ir naudojamus protokolus. Tuomet pagal šį scenarijų simuliuojamas tinklo veikimas. Pabaigus simuliaciją gaunamas tekstinis arba .pcap formato failas, kurio duomenis galima toliau analizuoti Wireshark ar tcpdump programomis. Taip pat pagal tinklo simuliaciją galima ir vizualizuoti.



7. pav. Network Simulator veikimo schema

3.2. NS-3 moduliai dalyvaujantys ad-hoc tinklų modeliavime

NS-3 modeliavimo aplinkoje modeliuojant bet kokio tinklo veiklą, modeliuojamas visų tinklo lygių veikimas. AODV protokolo atveju duomenų paketo kelias tarp siuntėjo ir gavėjo eitų per šiuos NS-3 modulius (pav. 5, 6), pavyzdyje paketas siunčiamas tarp kaimyninių mazgų, todėl jo persiuntimui užtenka tik po kartą patekti į kiekvieną iš šakų.

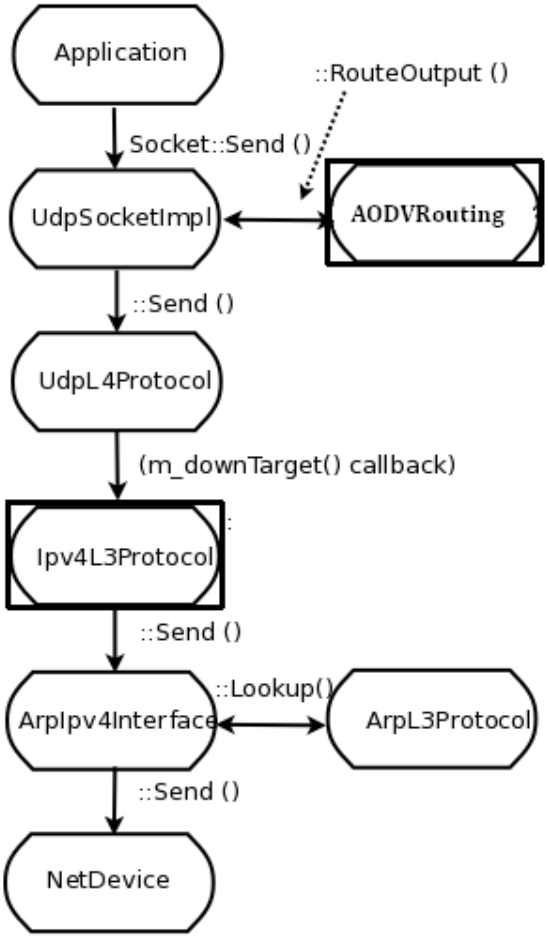
Mano darbo aprėpties sritis – tinklo lygmuo, tad visos modifikacijos buvo atliekamos už tinklo lygmenį atsakinguose moduliuose Ipv4L3Protocol ir AODVRouting (schemoje pažymėti stačiakampiais).

3.2.1. Siunčiamo duomenų paketo kelias

Programos siunčiamas duomenų paketas iki fizinio lygio praeina tokius žingsnius(5 pav.):[9]

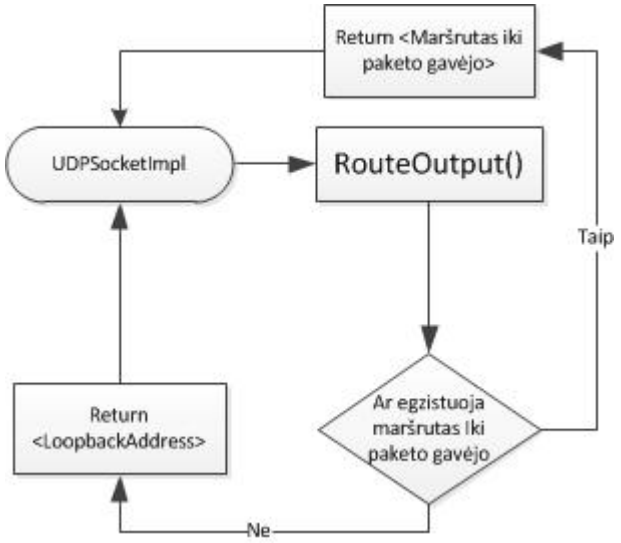
1. Programa, kuri nori siųsti duomenis prieš tai susikuria UDP soketą, tuomet iškviečia Socket::Send() metodą ir jam perduoda siunčiamus duomenis iš duomenų buferio.
2. Socket::Send() perduoda duomenis UdpSocketImpl::DoSend() ir po to UdpSocketImpl::DoSendTo(), atlieka soketų operacijas bind() ir connect(), nustato siuntėjo ir gavėjo adresus ir iškviečia UdpL4Protocol::Send() metodą. Tam, kad galėtų nustatyti gavėjo adresą (tai dar paprastai nebus galutinis gavėjas, o tik sekantis šuolis maršrute) šie metodai kreipiasi į AODVRouting::RouteOutput(), kuris grąžina arba sekančio šuolio adresą, jei tai ne pirmas siunčiamas paketas ir maršrutas jau egzistuoja maršrutų lentelėje, arba localhost adresą, tam, kad dar kartą būtų į jį kreipiamasi paketo gavimo šakoje ir tuomet būtų surastas maršrutas iki gavėjo.
3. UdpL4Protocol modulyje įgyvendinama nuo soketų nepriklausoma UDP protokolo logika. Send() metodas prideda UDP antraštę, suskaičiuoja ir nustato kontrolinę sumą (checksum) ir persiunčia suformuotą datagramą Ipv4 lygiui, šiuo atveju Ipv4L3Protocol moduliui.
4. Ipv4L3Protocol modulis prideda IP antraštę ir priklausomai nuo iš UDP lygio gauto maršruto (ar gavėjo adresas localhost, ar tinklo IP adresas), perduoda suformuotą paketą vienam iš Ipv4Instance modulių, atitinkamai Ipv4LoopbackInterface arba ArpIpv4Interface. Šiame pavyzdyje naudojamas antrasis variantas.

5. ArpIpv4Interface patikrina ar turi gavėjo MAC adresą laikinoje atmintinėje ir iškart perduoda paketą NetDevice moduliui, o jei ne tuomet prieš tai inicijuoja Arp užklausą ir sulaukia atsakymo.



8. pav. Siunčiamo paketo kelias[9]

3.2.2. Siunčiamo paketo kelias AODVRouting modulio viduje

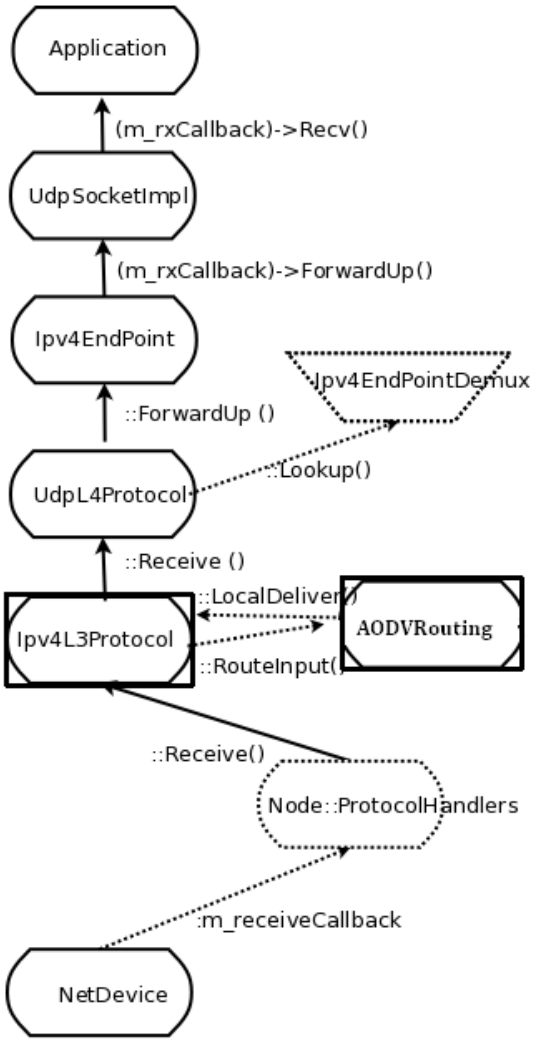


9. pav. Siunčiamo paketo kelias AODV modulyje

3.2.3. Gauto duomenų paketo kelias

Iš tinklo gautas duomenų paketas praeina tokius žingsnius, kol pasiekia priimančią programą(6 pav.):[9]

1. NetDevice modulis iškviečia Node::ReceiveFromDevice() metodą.
2. Node::ReceiveFromDevice perduoda paketą Ip4L3Protocol::Receive() metodui.
3. Ipv4L3Protocol modulis pašalina IP antraštę ir perduoda paketą AODVRouting::RouteInput() metodui, kurio pagalba aktyvuojama visa AODV logika, jei reikia parenkamas maršrutas ir Ipv4L3Protocol gražinamas sekančio šuolio adresas, kuriuo reikia toliau siųsti paketą, tuomet paketas keliauja vėl žemyn link NetDevice modulio. Šiame pavyzdyje AODVRouting modulis nustato, kad paketas jau pasiekė galutinį gavėją ir skirtas jam, o ne persiuntimui, todėl iškviečia Ip4L3Protocol::LocalDeliver() metodą ir jam perduoda paketą.
4. Ipv4L3Protocol::LocalDeliver() pagal datagramos antraštę nustato, kad reikalingas UDP protokolas, ir iškviečia UdpL4Protocol::Receive().
5. UdpL4Protocol modulis nuima UDP antraštę ir kreipiasi i demultipleksavimo modulį Ipv4EndPointDemux, kuris jam gražina Ipv4EndPoint objektą, susietą su konkrečiu soketu. Tuomet iškviečiamas Ipv4EndPoint::ForwardUp(), metodas, kuris savo ruožtu iškviečia UdpSocketImpl::ForwardUp().
6. UdpSocketImpl modulis perduoda programos sukurto soketo Recv() metodui.



10. pav. Gaunamo paketo kelias[9]

3.3. Network Simulator modelio modifikavimas

Ns-3 tinklų simuliacijos pakete realizuotas standartinis AODV protokolas[6]. Tam, kad būtų galima tirti jo atsparumą kenkiančių mazgų veiklai, jis buvo modifikuotas modeliuoti dviejų rūšių nesankcionuotą veikseną:

1. Maršrutizavimo paketų RREQ ir RREP antraščių (žr.priedą) modifikavimas.

Kenkiantis mazgas, gavęs RREQ paketą, pakeičia jo lauką RREQ ID. Lauko reikšmė pakeičiama į bet kokią kitą reikšmę, nei gautoji, kad gavėjo mazgas neatmestų paketo, kaip besidubliuojančio pagal RREQ ID ir siuntėjo IP adresą ir būtų gautas RREP paketas iš gavėjo mazgo. Gavus RREP paketą kuo labiau padidinamas gavėjo krypties naujumo parametras, tam kad maršrutas einantis per kenkiantį mazgą būtų kuo aukštesnio prioriteto ir siuntėjo mazge būtų priimtas kaip optimalus maršrutas. Tokio maršruto

iškreipimo tikslai dažniausiai būna duomenų perėmimas, žmogaus viduryje atakos to nepastebint nei siuntėjui, nei gavėjui arba tiesiog duomenų persiuntimo blokavimas, nuo to priklauso ar mazgas tvarkingai persiunčia duomenis pakeistuoju maršrutu, ar tiesiog naikina ateinančius duomenų paketus. Mano modifikacijoje naudojamos abi veiksenos, konkreti veiksena atsitiktinai parenkama priskiriant tinklo mazgui kenkiančio mazgo vaidmenį.

2. Apsimetimas gavėju, fiktyvaus RREP paketo sukūrimas ir grąžinimas siuntėjui.

Kenkiantis mazgas, gavęs RREQ paketą iš jo antraštės duomenų sukuria naują RREP paketą, į gavėjo adreso lauką taip pat įtraukia ne savo adresą, o adresą iš RREQ paketo. Vienintelis keičiamas laukas – tai gavėjo krypties naujumo parametras, kuris kuo labiau padidinamas, kad šis maršrutas būtų prioritetinis tuo atveju, jei jau bus spėjęs grįžti RREP paketas iš tikrojo gavėjo. Fiktyvus atsakymo paketas grąžinamas atgal siuntėjui, t.y. siunčiamas kaimynui iš kurio buvo gautas užklausos paketas. Toliau kenkiantis mazgas galėtų klastoti savo IP adresą, kad priimtų paketus skirtus gavėjui, tačiau mano modelyje jis nieko nedaro, duomenys fiktyviu maršrutu nepasiekia gavėjo, todėl kartojamas maršruto parinkimo procesas su ta pačia baigtimi, tad visas tinklas išvedamas iš rikiuotės, nes niekaip nepavyksta sudaryti veikiančių maršrutų.

Jokių saugaus maršruto parinkimo protokolų ad-hoc tinklams ns-3 simuliacijos pakete nėra realizuota, tad nesaugų standartinį AODV modelį saugumo funkcijomis teko papildyti pačiam.

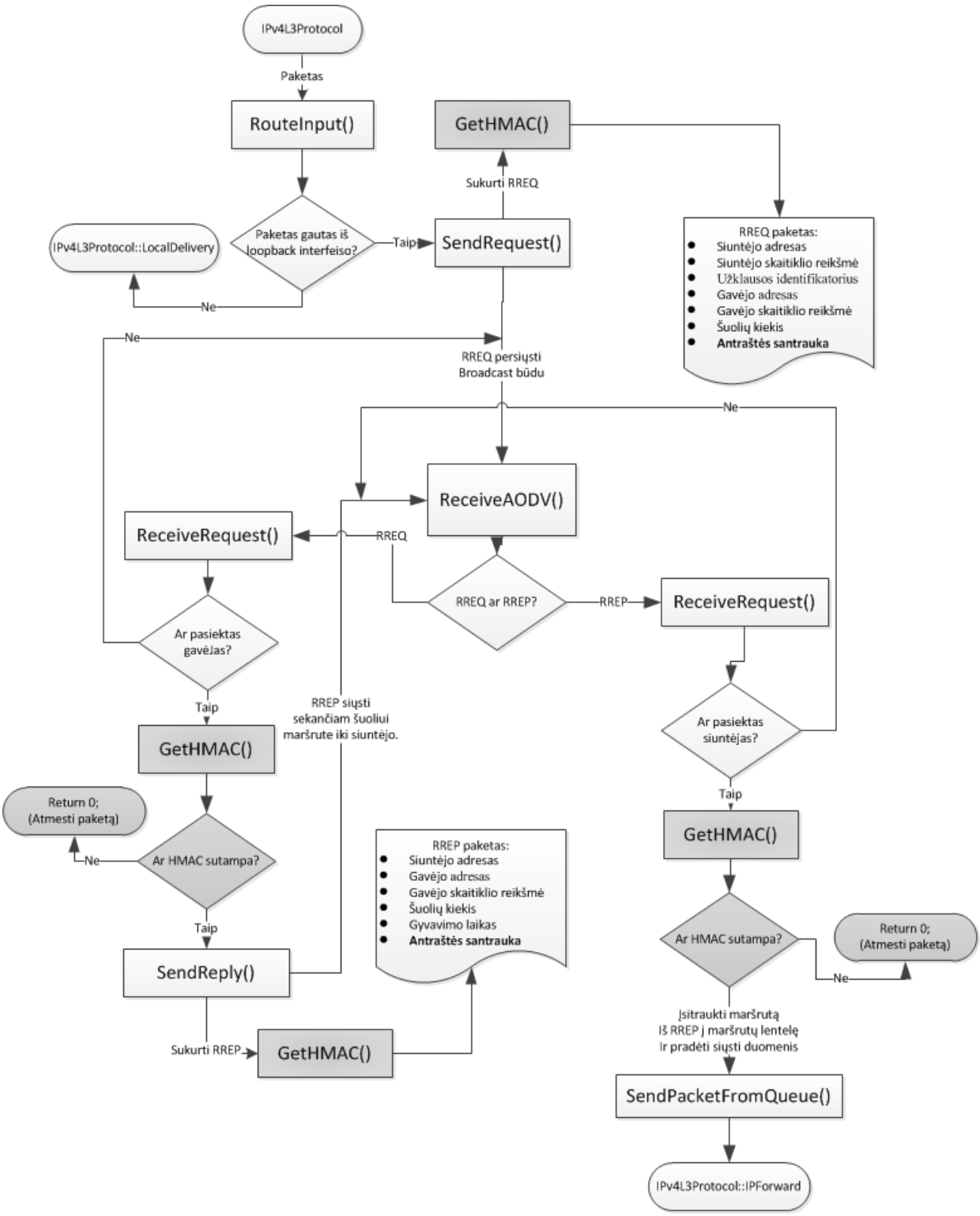
Pagrindinės modifikacijos:

Saugos priemonės vykdančios vengimo strategiją, remiantis SAODV aprašymu [12]

- RREQ ir RREP paketų antraštės išplėstos vienu papildomu 20 baitų lauku, skirtu HMAC santraukai, pagal naują antraštę perdaryti ir antrašte manipuliuojantys metodai.
- Parašytas metodas, realizuojantis HMAC_SHA1 algoritmą, sugeneruojantis santrauką iš duoto RREQ arba RREP paketo antraštės ir slapto rakto. RREQ paketo atveju santrauka generuojama iš slapto 20 baitų rakto ir eilutės sudarytos iš laukų RREQ ID, gavėjo IP adresas, gavėjo krypties naujumo parametras, siuntėjo IP adresas, siuntėjo krypties naujumo parametras. RREP paketo atveju santrauka generuojama iš slapto rakto bei eilutės sudarytos iš laukų gavėjo IP adresas, gavėjo krypties naujumo parametras, siuntėjo IP adresas.
- Modifikuoti metodai, atsakingi už RREQ ir RREP paketų išsiuntimą: prieš siunčiant paketus, sugeneruojama jų antraštės nekintančių laukų HMAC santrauka su slaptu raktu ir pridedama į antraštę.

- Modifikuoti metodai, apdorojantys gautus RREQ ir RREP paketus: jie taip pat sugeneruoja gauto paketo antraštės nekintančių laukų ir slapto rakto HMAC santrauką ir palygina ją su antraštėje pridėta santrauka, paketas toliau apdorojamas tik tuo atveju, jei santraukos sutampa, jei ne – paketas atmetamas.

12 pav. pateikta schema parodanti paketo apdorojimo logiką po AODV modifikacijos pagal SAODV protokolą, naujai pridėtos dalys – tamsesnės.



11. pav. Paketo kelias AODV modulyje su SAODV išplėtimais

Papildoma modifikacija saugos priemonėmis, būdingomis toleravimo strategijai, remiantis SRP/SMT aprašymu[3, 4]:

- RREP paketo antraštė papildyta dar vienu vieno bito lauku – vėliavėle(flag) IsMalicious.

- Gautą RREQ paketą apdorojantis metodas taip pat sugeneruoja jo antraštės HMAC santrauką ir lygina su gautąja, tačiau pastebėjus neatitikimą, paketas nėra iš karto atmetamas, o vis tiek formuojamas ir siunčiamas RREP paketas, tačiau IsMalicious reikšmė jame pakeičiama į 1. Taip pat iš gautą RREQ apdorojančio metodo pašalinta sąlyga, kad apdorojamas ir atsakomas tik pirmas gautas paketas, po šio pakeitimo metodas atsako į visus gautus RREQ paketus ir grąžina RREP atsakymus su atitinkamai nustatytu IsMalicious lauku į juos.
- Modifikuota maršrutų lentelės įrašus realizuojanti klasė, maršruto įrašas papildytas dviem papildomais laukais – vieno bito dydžio IsMalicious ir 4 baitų dydžio lauku Rating, atitinkamai pakeisti ir veiksmus su maršrutų lentelės įrašais atliekantys klasės metodai.
- Pakeistas metodas, priimantis RREP paketą – jis į maršrutų lentelę įtraukia naują maršrutą iš RREP paketo, jei dar nėra tokio maršruto, kurio siuntėjas, gavėjas ir sekantis šuolis būtų vienodi, o jei yra, gali jį perrašyti, pirmiausia remiantis IsMalicious lauku (prioritetas visada reikšmei 0), o jei lyginamų maršrutų IsMalicious lauko reikšmės lygios – pagal naujumo parametrą.
- Duomenų paketo antraštė papildyta 20 baitų lauku Digest, skirtu jo HMAC santraukai.
- Modifikuotas duomenis išsiunčiantis metodas: prieš siųsdamas sugeneruoja paketo HMAC santrauką ir ją įtraukia į paketo antraštės Digest lauką.
- Sukurtas naujas pranešimo paketas – ACK, kuris skirtas informuoti siuntėją apie sėkmingai perduotą paketą.
- Modifikuotas duomenis priimantis metodas: jame sutikrinama HMAC santrauka ir jai atitikus, duomenų paketas priimamas ir išsiunčiamas ACK pranešimas gavėjui.
- Sukurtas duomenų perdavimo kontrolės metodas, kuris tam tikrą laiką negavęs ACK patvirtinimo konkrečiam paketui, sumažina konkretaus maršruto reitingą ir kartoja paketo siuntimą kitu maršrutu.
- Modifikuotas maršruto pasirinkimo metodas iš keleto egzistuojančių maršrutų pasirenkantis pirmiausia pagal IsMalicious reikšmę, tada pagal reitingą.

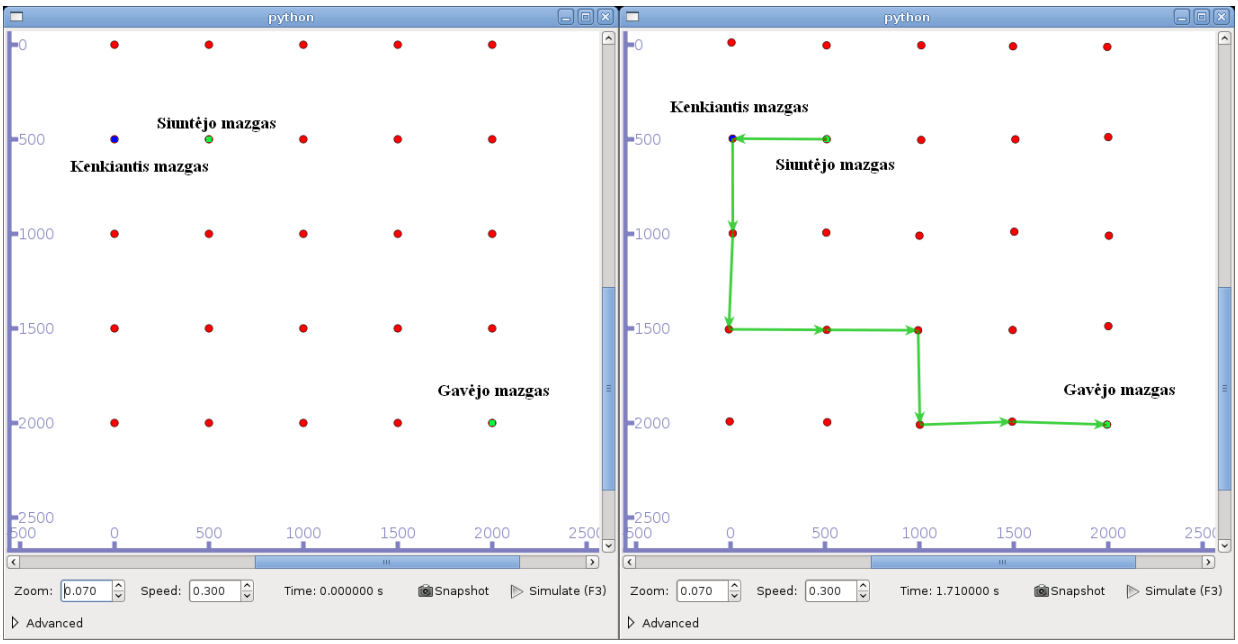
3.4. Modelio parametrai

Kaip simuliacinis modelis naudojamas 25 mazgų tinklas. Pradiniu simuliacijos laiko momentu tinklas išdėstytas tinklelio (5 x 5) forma. Pradiniai tinklo parametrai tokie:

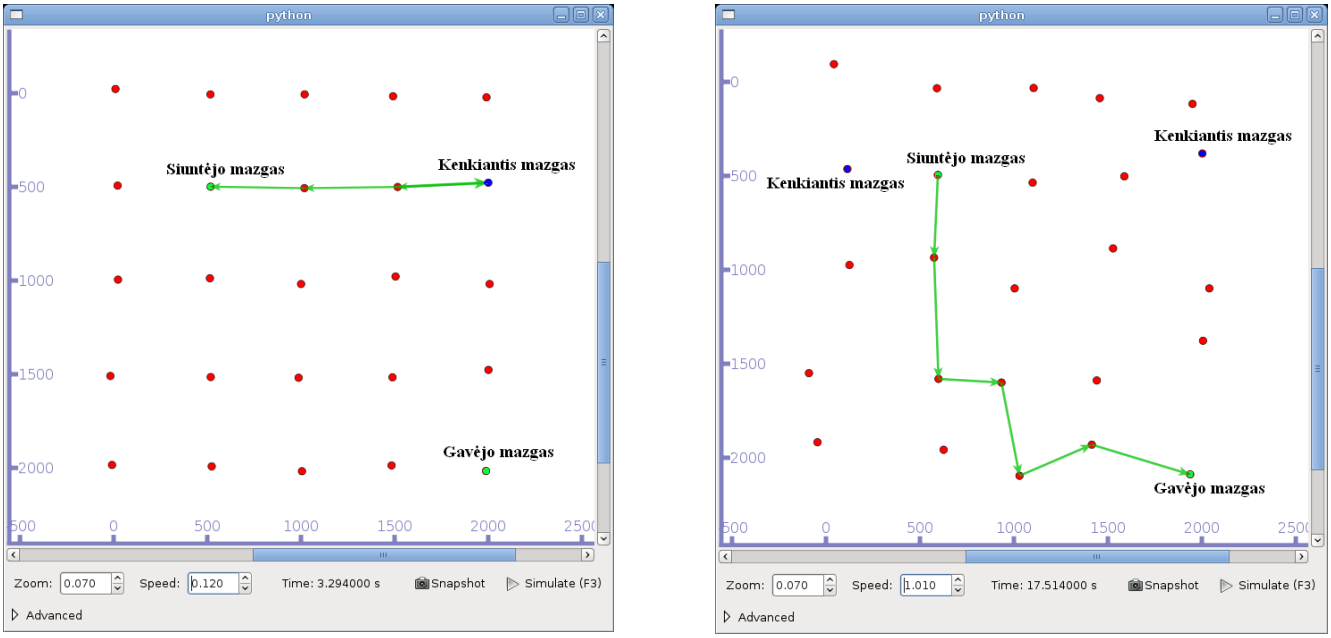
3. Lentelė. Tinklo modelio parametrai

Parametras	Reikšmė
Siųstuvo galia	500m
Atstumas tarp gretimų mazgų pradiniu laiko momentu	500m
Mazgų kiekis	25
Linijos pralaidumas	1 Mbit/s
Siunčiamų paketų kiekis	100
Paketų siuntimo dažnis	5 pak/s
Paketo dydis	1024 baitai
Teritorijos dydis	2000m x 2000m

Tinklo topologijos pavyzdžiai, vaizdžiai demonstruojantys kenkiančių mazgų įtaką AODV protokolui pateikti 5-8 pav.



12. pav. Vaizdas pradiniu laiko momentu; Maršruto pakeitimo ataka



13. pav. Apsimetimo gavėju ataka; Saugaus protokolo veikimas

- Pradiniu laiko momentu mazgai išdėstyti tinkleliu 5 x 5, iš kurių vienas mazgas kenkiantis (5 pav). Pradėjus simuliaciją, mazgai pradeda kontaktuoti tarpusavyje (Hello paketai[6] ir maršrutų užklausos, atsakymo, bei duomenų paketai) ir judėti atsitiktinėmis kryptimis. Judėjimo greitis taip pat atsitiktinis, tačiau neviršijantis dydžio, nustatyto vartotojo prieš vykdant simuliaciją. Taip pat veikia ir kenkiantis mazgas.
- Tinklo topologija kenkiančiam mazgui vykdant maršruto pakeitimo ataką: akivaizdžiai matomas sudarytas neoptimalus maršrutas (6 pav.)
- Tinklo topologija kenkiančiam mazgui vykdant apsimetimo gavėju ataką: akivaizdžiai matomas sudarytas maršrutas iki kenkiančio mazgo, o ne iki gavėjo(7 pav).
- Tinklo topologija veikiant saugiam maršrutizavimo protokolui: akivaizdžiai matoma, jog kenkiantys mazgai ignoruojami, duomenų perdavimas vyksta optimaliu maršrutu(8 pav).

4. MODELIAVIMO REZULTATAI

4.1. Tiriami parametrai

Tiriamame modelyje kenkiančių mazgų tikslas yra sutrikdyti ad-hoc tinklo veikimą ir neleisti sėkmingai perduoti informaciją. Pasirinkti du tinklo atsparumo ir vienas saugumo grėsmės parametrai:

- Sėkmingai perduotų tarp dviejų mazgų duomenų paketų kiekis, procentais nuo visų siųstų paketų.
- Paketų kiekis perduotas per kenkiančius mazgus, procentais nuo sėkmingai perduotų paketų.
- Paketų vėlinimas.

4.2. Simuliacijos parametrai

Pagrindinis simuliacijos parametras – kenkiančių mazgų kiekis, procentais nuo bendro tinkle esančių mazgų kiekio, prie skirtingų atakų ir skirtingų tinklo mobilumo scenarijų. Kenkiančių mazgų ir siuntėjo-gavėjo išsidėstymas tinklo topologijoje – atsitiktinis.

4.3. Simuliacijos eiga

Simuliacijoje protokolų tyrimui naudojami du skirtingi nesankcionuotos veiksenos maršruto parinkimo metu scenarijai: apsimetimas gavėju ir nesankcionuotas tarpinės maršruto parinkimo informacijos modifikavimas, maršruto iškreipimas. Kiekvieno iš šių scenarijų metu naudojama statinė ir dinaminė topologijos, tyrimas vyksta palaipsniui keičiant kenkiančių mazgų kiekį nuo 0 iki 15 (60%), stebima simuliacijos rodiklių priklausomybė nuo kenkiančių mazgų tinkle kiekio. Kiekvienam unikaliam atakos scenarijaus-rodiklio-topologijos-kenkiančių mazgų kiekio deriniui simuliacija vykdoma 10 kartų, kiekvieną kartą keičiant šiuos parametrus ir paimant gautų rezultatų vidurkį:

- Jei tiriama dinaminė topologija – parenkamas atsiiktinis mazgų atsitiktinio judėjimo modelis (RandomMobilityModel).
- Atsitiktinai parenkamos siuntėjo ir gavėjo pradinės pozicijos. Tam, kad siuntėjas ir gavėjas nebūtų greta vienas kito, jų pozicijos apribotos: siuntėjas gali būti bet kuris mazgas iš viršutinių dviejų tinklo pradinio išsidėstymo tinklelio eilučių, o gavėjas bet kuris mazgas iš dviejų apatinių eilučių.
- Atsitiktine tvarka tinklo pradinio išsidėstymo tinklelyje išdėstomi kenkiantys mazgai, visi mazgai homogeniški, vieno atakos tipo, priklausomai nuo to metu tiriamo atakos scenarijaus, tačiau jei tiriamas maršruto pakeitimo scenarijus, kiekvienam kenkiančiam mazgui atsitiktine tvarka priskiriama ne tik jo pozicija tinkle, bet ir veiksenos modelis, t.y. ar jis, perėmęs duomenų paketus, persiųs juos toliau, ar sunaikins.

Nors atsitiktinėms reikšmėms naudojami pseudo atsitiktinių skaičių generatoriai, tačiau naudojama tik 10 skirtingų pasėlių. Tai leidžia užtikrinti stabilius rezultatus kiekvieno simuliacijos vykdymo metu, bei lyginti rezultatus gautus stabiliomis sąlygomis, neiškreiptus skirtingų aplinkos parametrų.

4.4. Simuliacijos rezultatai

4.4.1. Apsimetimo gavėju ataka

Šiam simuliacijos scenarijui naudojami kenkiantys mazgai, kurie vykdo apsimetimo gavėju ataką.

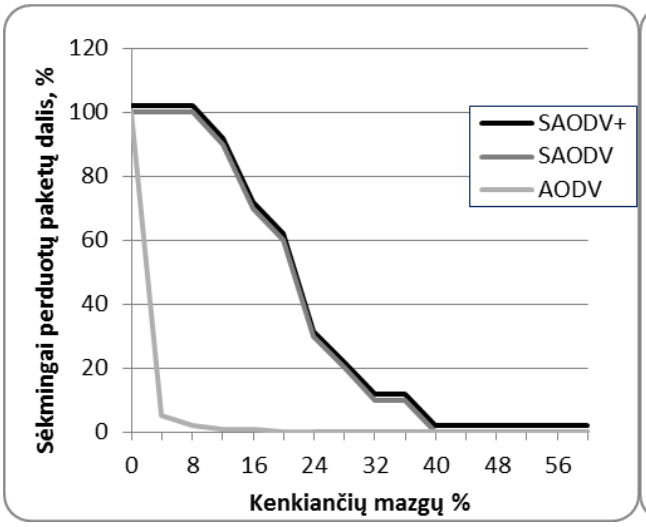
4.4.1.1. Sėkmingai perduotas paketų kiekis

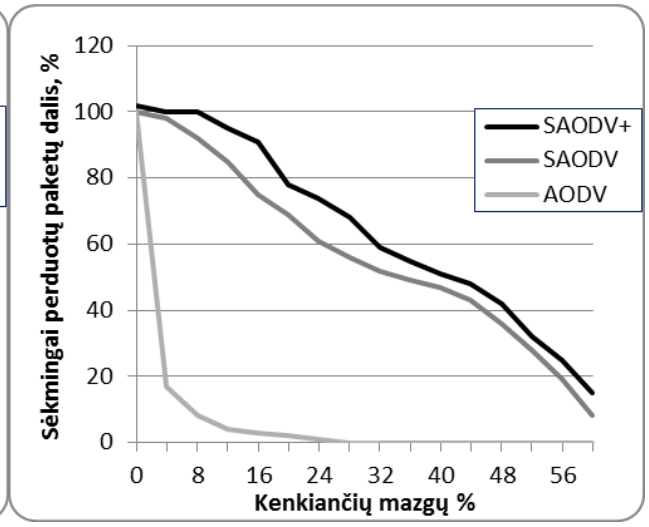
Šio tyrimo metu tiriamas sėkmingai gavėją pasiekusių siųstų paketų kiekis. Kuo jis didesnis didėjant kenkiančių mazgų kiekiui, tuo protokolas yra atsparesnis apsimetimo gavėju atakai ir tuo geriau užtikrina paslaugos pateikiamumą.

Tiek statinės, tiek dinaminės topologijos atveju (11, 12 pav) matome, kad AODV yra visiškai neatsparus šiai atakai, jau atsiradus pirmam kenkiančiam mazgui tinkle darbas sutrikdomas ir siunčiami duomenys nepasiekia gavėjo.

SAODV ir SAODV+ šios atakos metu demonstruoja identiškus rezultatus, todėl, kad apsimetimo gavėju atakos atveju kenkiantis mazgas niekada nepersiunčia informacijos, o ją tik naikina arba bando toliau kaip gavėjas komunikuoti su siuntėju, todėl SAODV+ gali ir panaudoja tik tas pačias saugos priemones kaip ir SAODV. O aplinka, kaip jau minėjau vienoda, nes simuliacijų atsitiktiniai elementai generuojami su ta pačia pasėlių aibe, tad ir rezultatai vienodi.

Abiejų protokolų demonstruojami rezultatai yra žymiai geresni, nei AODV protokolo, esant tik keletui kenkiančių mazgų, tinklo veikimas beveik nenukenčia, nes abu šie protokolai sėkmingai geba išvengti maršrutų su tokio tipo kenkiančiais mazgais. Vis tik atsirandant daugiau kenkiančių mazgų, susidaro tokie mazgų išsidėstymai, jog atmetus visus maršrutus su kenkiančiais mazgais tiesiog nebelieka maršruto nuo siuntėjo iki gavėjo. Tai ryškiausiai jaučiasi statinėje topologijoje, kur grafikas yra tolygus tik dėl vykdomų 10 simuliacijų su skirtingais išsidėstymais ir imamo vidurkio. Imant tik vieną simuliaciją grafikas būtų lygiagretus abscisės ašiai ties reikšme 100 tol, kol ties kažkuria mazgų kiekio reikšme, sėkmingai persiųstų paketų kiekis kristų iš kart iki 0. Dinaminėje topologijoje tai jaučiama mažiau, nes keičiantis mazgų išsidėstymui, atsiranda ir naujų maršrutų iki gavėjo, tik kuo kenkiančių mazgų daugiau, tuo tokio maršruto išsidėstymo tikimybė mažėja ir jo laukti tenka ilgiau, o dalis paketų šalinami iš buferio, dėl viršyto maksimalaus laiko. Taip pat dinaminėje topologijoje dalis paketų prarandama ir dėl pačio mobilumo, tiesiog pasitaiko momentų, kai nutrūkus ryšiui dar nepėja ateiti klaidos paketas, o vienas ar du duomenų paketai išsiunčiami ta kryptimi, o kadangi SAODV kaip ir AODV neturi jokios nusiųstų paketų kontrolės, tokie paketai prarandami. Tokia kontrole papildytas SAODV+ protokolas, todėl jis demonstruoja geresnius rezultatus dinaminės topologijos atveju.





14. pav. Statinė topologija Dinaminė topologija

4.4.1.2. Sėkmingai perduotų paketų dalis, perduota per kenkiančius mazgus

Šio rodiklio tyrimą praleidau, nes pagal šios atakos apibrėžimą, kenkiantys mazgai niekada neperduoda duomenų gavėjui, o juos tiesiog sunaikina.

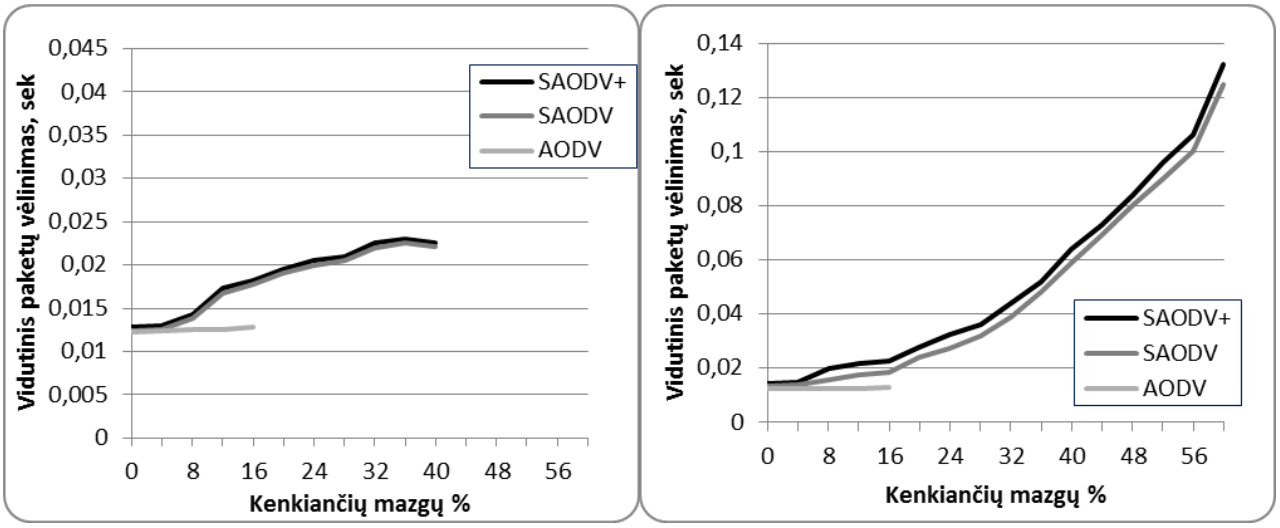
4.4.1.3. Vidutinis paketų vėlinimas

Tiriant vidutinį paketų vėlinimą, skaičiuojamas kiekvieno sėkmingai persiųsto paketo siuntimo pradžios momento ir jo gavimo gavėjo mazge momento laiko skirtumas ir išvedamas vidurkis. Paprastai didžiąją dalį sudaro maršruto parinkimas, tačiau daugėjant kenkiančių mazgų ir ilgėjant maršrutams skirtiems jų išvengti, šiek tiek didėja ir vėlinimas. Kuo vėlinimas mažesnis, tuo protokolas labiau tinkamas, kai svarbus greitis, t.y. realaus laiko sistemose ir panašiai.

Statinės topologijos atveju (13 pav.) vėl matome, kad SAODV ir SAODV+ protokolai turi identiškus vėlinimo rodiklius, to priežastys tos pačios kaip ir paketų perdavimo tyrimo atveju – abu protokolai statinėje topologijoje šios atakos atveju dirba vienodai. AODV protokolas abiejose topologijose turi geriausią rezultatą, bet tas rezultatas gautas iš tų keleto paketų, kurie spėja prasmukti iki gavėjo, kol ateina suklastoti paketai iš kenkiančio mazgo, o vėliau jokių vėlinimo rodiklių nebelieka, nes nebelieka sėkmingai persiųstų paketų.

Dinaminėje topologijoje (14 pav.) abiejų saugių protokolų vėlinimo rodikliai stipriai pakyla, tai natūralu, dėl to, kad judant mazgams maršrutai susidaro trumpam ir vėl išnyksta, maršruto parinkimo procesą reikia kartoti, o daugėjant kenkiančių mazgų ir mažėjant tinkančių maršrutų, tie tinkami

išsidėstymai retėja ir jų laukti tenka ilgiau. Taip pat dėl tų kelių paketų, kuriuos SAODV+ prasiunčia papildomai, palyginus su SAODV, pasinaudodamas persiuntimo patvirtinimo funkcionalumu, padidėja ir SAODV+ vėlinimo vidurkis, todėl, kad tuos keletą paketų nenuėjusių iš pirmo karto, tenka siųsti iš naujo, o tai stipriai pailgina vėlinimą ir padidina bendrą vidurkį.



15. pav. Statinė topologija Dinaminė topologija

4.4.2. Maršruto pakeitimo ataka

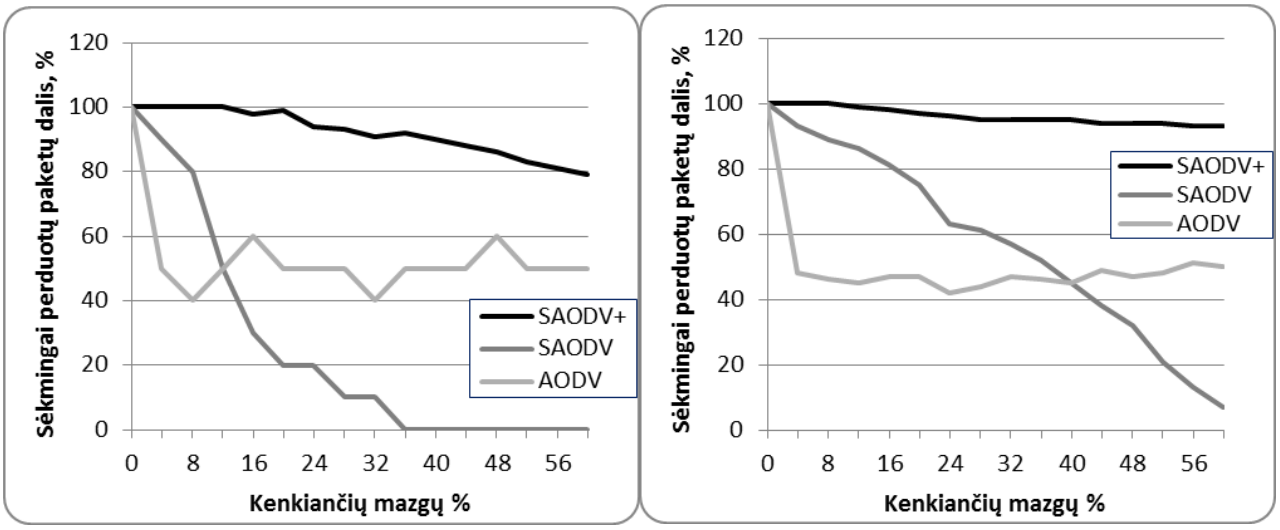
Šiam simuliacijos scenarijui tinkle naudojami kenkiantys mazgai, vykdantys maršruto nukreipimo ataką, kiekvienas iš jų gali arba blokuoti duomenis, su tikslu nutraukti ar paveikti tinklo veikimą, arba persiųsti juos toliau, su tikslu neišsiduoti ir perimti kuo daugiau duomenų.

4.4.2.1. Sėkmingai perduotų paketų kiekis

Šio tyrimu taip pat, kaip ir apsimetimo gavėju scenarijaus atveju, matuojamas sėkmingai perduotų duomenų paketų procentas nuo visų išsiųstų paketų.

Šios atakos atveju, skirtingai, nei praėjusios, abiejų topologijų atveju (15, 16 pav.) neblogus rezultatus demonstruoja ir AODV protokolas. Tai tiesiogiai priklauso nuo to, kad apytiksliai kas antras iš kenkiančių mazgų paketus vis tik perduoda gavėjui, todėl ir AODV protokolo sėkmingai perduodamų paketų kiekis svyruoja apie 50 procentų. Nors, palyginus su praeitu kenkiančių mazgų scenarijumi, tai atrodo gan neblogas rodiklis, ypač esant didesniems kenkiančių mazgų kiekiams, tačiau sekančiame tyrime pamatysime, kodėl taip iš tikrųjų nėra, jei rūpi perduodamų duomenų konfidencialumas ar integralumas. SAODV protokolo rezultatai tik prie nedidelių kenkiančių mazgų kiekių sėkmingai perduotų paketų kiekiu lenkia AODV protokolą, o prie didesnių kenkiančių mazgų kiekių lieka

paskutinėje vietoje. Iš tiesų, galima atkreipti dėmesį, kad SAODV protokolo rezultatai yra gan panašūs į praeito atakos scenarijaus metu gautus rezultatus, nes iš principo vengimo strategijos protokolams, koks yra SAODV, nėra skirtumo tarp šių dviejų atakų, nes jos abi modifikuoja maršruto parinkimo paketų antraštes ir dėl šios priežasties yra atmetamos. Geriausiais paketų perdavimo rezultatais pasižymi SAODV+ protokolas, todėl kad jis, nebeturėdamas tinkamu saugių maršrutų, pradeda naudotis per kenkiančius mazgus einančiais maršrutais, dėl šios priežasties jo rezultatas daug geresnis už SAODV protokolo. Iš kitos pusės jis stebi ar paketas nuėjo sėkmingai, todėl jei pataiko nusiųsti paketą į tokį maršrutą, kuriame yra blokuojantis kenkiantis mazgas ir negauna patvirtinimo apie paketo avimą, jis tiesiog pakartoja siuntimą tol kol pataiko į paketus persiunčiantį mazgą, taip žymiai aplenkdamas AODV protokolą. Iš esmės prarastus paketus lemia tik nepalankus kenkiančių mazgų išsidėstymas, kai arti siuntėjo atsiranda keli blokuojantys kenkiantys mazgai ir jį izoliuoja. Vis tik, šie geri rodikliai neapsieina be tam tikrų kompromisų saugos srityje, kaip matoma sekančiame tyrime.



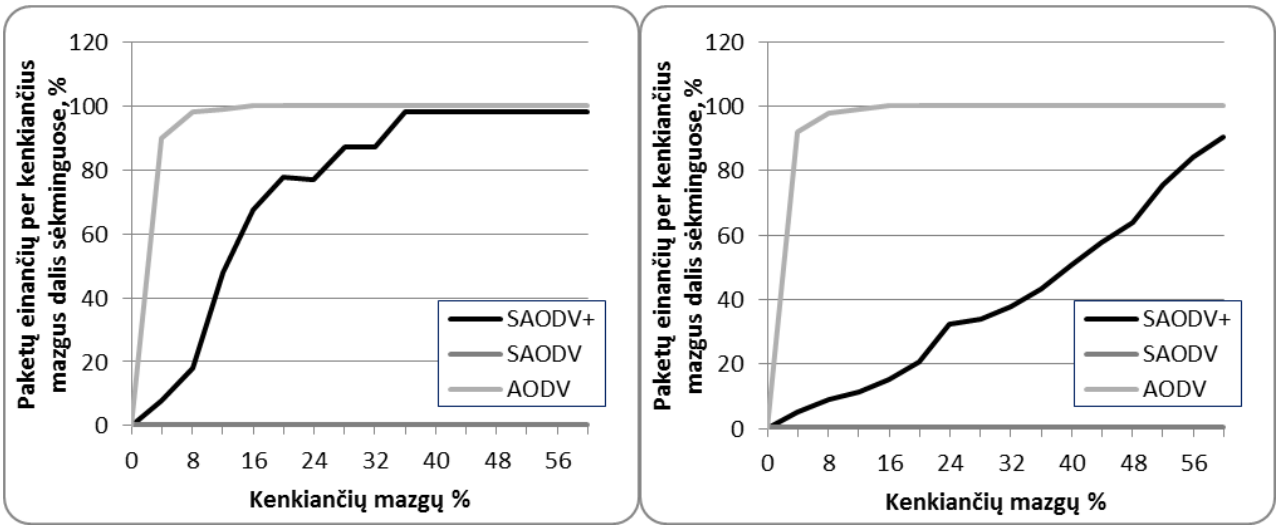
16. pav. Statinė topologija Dinaminė topologija

4.4.2.2. Sėkmingai perduotų paketų dalis, perduota per kenkiančius mazgus

Ši simuliacija parodo, kokia dalis iš sėkmingai perduotų gavėjui paketų buvo siunčiami per kenkiančius mazgus, t.y. kokia dalis komunikacijos duomenų susiduria su papildoma rizika konfidencialumo ir integralumo srityse.

Šios simuliacijos rezultatai iš ties atskleidžia, jog AODV protokolo palyginus neblogas rezultatas paketų perdavimo tyrime nublanksta prieš faktą, kad visi tie paketai eina per kenkiančius mazgus, todėl jei ir aukštesniuose lygiuose nebūtų jokių saugos mechanizmų, visa komunikacija būtų kaip ant delno piktavaliui. SAODV+ protokolo puikūs rezultatai taip pat turi savo kainą, tačiau tik prie gana didelio

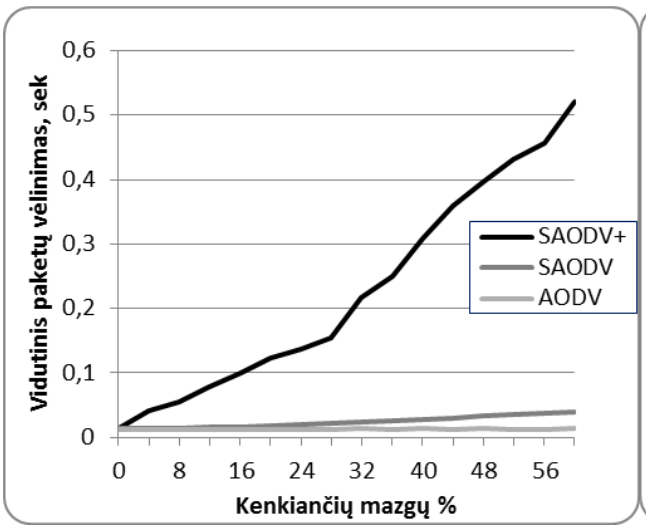
kenkiančių mazgų kiekio jis nemažai paketų perduoda per kenkiančius mazgus. Vis tik tai nėra taip pavojinga ir nekontroliuojama kaip AODV protokolo atveju, kadangi šis protokolas taip elgiasi sąmoningai, todėl jis prieš pradėdamas siųsti duomenis nesaugiu kanalu gali informuoti aukštesnio lygio protokolą, kad čia būtinas šifravimas ar kažkas panašaus, taip pat priklausomai nuo aplikacijos saugos ar atvirkščiai perdavimo patikimumo lygio reikalavimo, gali pasirinkti naudotis ar nesinaudoti kenkiančių mazgų paslaugomis. Na, o SAODV protokolas, nepaisant prastokų rezultatų paketų perdavimo simuliacijoje, kaip jam ir priklauso pagal apibrėžimą sėkmingai išvengia visų kenkėjiškų mazgų ir per juos neperduoda nė vieno paketo.



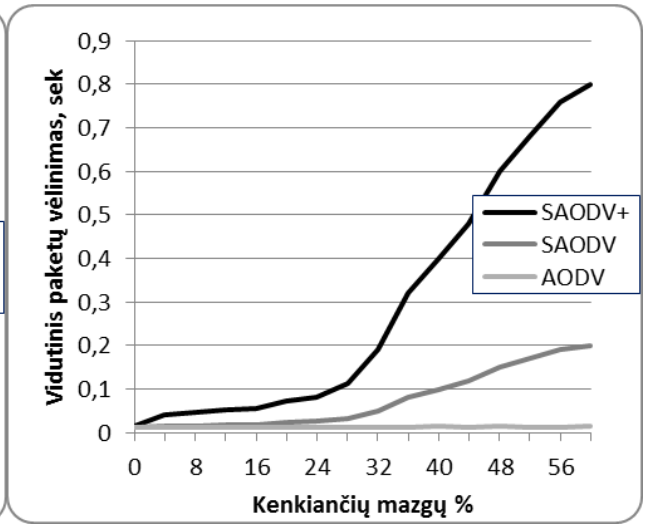
17. pav. Statinė topologija Dinaminė topologija

4.4.2.3. Vidutinis paketų vėlinimas

Maršruto pakeitimo atakos scenarijaus atveju ryškiau, nei apsimetimo gavėju atakos atveju ryškiau išsiskiria visų protokolų rezultatai. AODV protokolas pasižymi nedideliu vėlinimu, kadangi jis neatlieka jokių papildomų veiksmų atsparumo padidinimui, todėl paketai arba nueina greitai arba visai nenueina. SAODV protokolo rezultatas gan panašus į praeitos atakos tyrimo, jį gana stipriai įtakoja topologijos dinamiškumas, na o didžiausią vėlinimo vidurkį demonstruoja SAODV+ protokolas, o jį sukelia visi tie papildomi veiksmai, bandymai bet kokia kaina perduoti paketą sėkmingai.



18. pav. Statinė topologija



Dinaminė topologija

4.4.3. Simuliacijos apibendrinimas

Nors šioje simuliacijoje modeliuoti gana specifiniai ir siauri scenarijai, ne visos galimos atakų, protokolų variacijos, tačiau pavyksta pamatyti, kad kaip ir daugelyje sričių, kol kas nėra universalaus protokolo, kuris visuose tikruose rodikliuose būtų geriausias. Naudojant kiekvieną iš šių protokolų reikia turėti omenyje jų stipriąsias ir silpnąsias puses ir labiausiai tinkamą pritaikymo sritį.

4. Lentelė. Ištirtų protokolų savybių palyginimas

Protokolo sutartinė žymė	Stipriosios pusės	Silpnosios pusės	Pritaikymo scenarijai
AODV	Maži vėlinimo rezultatai	Neveikiantis tinklas esant nors vienam blokuojančiam mazgui. Visi tinkle bandomi siųsti duomenys patenka pas kenkiančius mazgus.	Aplinkos be kenkiančių mazgų.
SAODV	Visada išvengiama maršrutų parinkimo paketus modifikuojančių kenkiančių mazgų.	Stipriai sumažėjantis duomenų perdavimo efektyvumas, didėjant kenkiančių mazgų	Mažo kenkiančių mazgų kiekio aplinkos.

		kiekiui tinkle.	
SAODV+	Labai maži kiekiai prarastų paketų, jei ne visi mazgai tinkle blokuojantys, prie mažo kenkiančių mazgų kiekio duomenys nuo kenkiančių mazgų apsaugomi taip pat gerai, kaip ir SAODV protokole.	Dideli vėlinimai, prie didelių kenkiančių mazgų kiekio – pasirinkimas tarp paslaugos pateikiamumo ir paketų konfidencialumo, bei integralumo užtikrinimo.	Didelio kenkiančių mazgų kiekio aplinkos, kuriose ne visi kenkiantys mazgai blokuojantys, jei paketų perdavimo patikimumas yra svarbesnis už paketų vėlinimus.

5. IŠVADOS

Šiame magistriniame darbe pavyko išanalizuoti ad-hoc tinklų specifiką, kertines savybes, specifinę tarpusavio komunikavimo ir maršruto parinkimo veikseną. Taip pat įsigilinta į skirtingas maršruto parinkimo algoritmų savybes, ypatingai algoritmus, užtikrinančius maršruto parinkimo proceso saugą. Išanalizuoti keli populiarūs saugūs maršruto parinkimo protokolai, atskleisti esminiai jų skirtumai, privalumai ir trūkumai. Sudarytas specifinis ad-hoc tinklo scenarijus ir sukurtas jo modelis. Šio modelio pagalba pasirinkti tirti du skirtingų savybių maršruto parinkimo protokolai, taip pat sudarytas naujo protokolo, apjungiančio dalį pirmųjų dviejų protokolų savybių, modelis. Du iš trijų tirtų protokolų darbo metu realizuoti programinėmis priemonėmis, trečiasis panaudotas iš jau esančio simuliacijos paketo. Įvykdžius simuliacinį tyrimą gauti rezultatai išanalizuoti ir palyginti. Darbo metu atliekant visas šias užduotis buvo padarytos šios išvados:

- Nėra universaliai geriausio ad-hoc saugaus maršruto parinkimo protokolo, jų tinkamumas priklauso nuo naudojimo scenarijaus ir to kurioms rizikoms teikiamas didesnis prioritetas.
- Standartiniai ad-hoc maršruto parinkimo protokolai puikiai atlieka savo darbą saugioje aplinkoje tiek statiškuose, tiek mobiliuose tinkluose, tačiau yra visiškai bejėgiai net prieš paprastas ad-hoc tinklo atakas.
- Saugūs maršruto parinkimo protokolai pasižymi skirtingomis atsparumo skirtingoms grėsmėms, greitaveikos savybėmis.

- Esant nedideliems kenkiančių mazgų kiekiams, sėkmingai ir sparčiai veikia, užtikrina paslaugos pateikiamumą ir pagerina informacijos integralumo bei konfidencialumo savybes vengiantys kenkiančių mazgų protokolai, tokie kaip SAODV.
- Esant dideliems kenkiančių mazgų kiekiams tinkle, geresnes paslaugos pateikiamumo charakteristikas demonstruoja toleruojantys kenkiančius mazgus protokolai, tokie kaip SRP, tačiau jie visiškai neužtikrina duomenų konfidencialumo, tuo tenka rūpintis aukštesnių lygių protokolams.
- Mano pasiūlytas vengiančių ir toleruojančių protokolų junginys demonstruoja geras paslaugos pateikiamumo savybes esant dideliam kenkiančių mazgų kiekiui tinkle iš kurių dalis nėra blokuojantys, taip pat sugeba identifikuoti konfidencialumo ir integralumo pažeidimų riziką konkrečiame sudarytame maršrute ir padėti aukštesnio lygio protokolams parinkti atitinkamas saugos priemones, tačiau yra lėčiausias, t.y. demonstruojantis didžiausius paketų vėlinimus iš tirtų protokolų, todėl realaus laiko pagrindu veikiančiose sistemose.

Siūlau visada naudojant ad-hoc tinklus, prieš tai pasirūpinti jų saugumu, saugos priemones pasirinkti priklausomai nuo situacijos, aplinkos. Taip pat reikia turėti omenyje, jog pilnam saugumui vien tinklo lygmens saugos nepakanka, turi būti taikomos kompleksinės ad-hoc tinklams pritaikytos priemonės.

LITERATŪRA

[1] **A. Mishra,** "Security and Quality of Service in Ad Hoc wireless networks", *Johns Hopkins University*, 2008.

[2] **A K Bayya, S Gupte, Y Kshukla, A Garikapati**, "Security in Ad-hoc Networks", *Computer Science Department, University of Kentucky*

[3] **P. Papadimitratos and Z. J. Haas**, ''Secure routing for mobile ad hoc networks'',SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, Jan. 27–31, 2002.

[4] **P. Papadimitratos and Z. J. Haas,** ''Secure Message Transmission in Mobile Ad Hoc Networks,'' in Handbook of Wireless Ad Hoc Networks, (M. Ilyas, Editor), CRC Press, 2003.

[5] **H. Krawczyk, M. Bellare, and R. Canetti,** „HMAC: Keyed-Hashing for Message Authentication", www.rfc-ref.org/RFC-TEXTS/2104/, Feb. 1997.

[6] **C. E. Perkins and E. M. Royer, "**Ad Hoc On-Demand Distance Vector Routing Protocol".

[7] **S. Yi, P. Naldurg, and R. Kravets**, "Security-Aware Ad-Hoc Routing for Wireless Networks", UIUCDCS-R-2001-2241 Technical Report, Aug. 2001.

[8] **K.Taneja, R.B.Patel** „An Overview of Wireless Ad Hoc Networks: Challenges and Future."

[9] NS-3 dokumentacija – prieiga per internetą: **http://www.nsnam.org/docs/release/manual/singlehtml/index.html**

[10] **T. Larsson and N. Hedman,** „Routing Protocols in Wireless Ad-Hoc Networks – A Simulation Study", Lulea Tekniska Universitet, 1998.

[11] **G. Jayakumar, and G. Gopinath**, Ad Hoc Wireless Networks Routing Protocols – A Review, *Journal of Computer Science 3 (8):* 2007, psl. 574-582

[12] **M. Guerrero Zapata**, Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, Technical University of Catalonia, 2006

[13] **M.O.Rabin,** Efficient dispersal of information for security, load balancing and fault tolerance, psl. 335-348, 1989

[14] **Y.C. Hu, A. Perrig, and D. B. Johnson**, "Ariadne： a secure on-demand routing protocol for ad hoc networks, "

[15] **Luke Klein-Berndt**, A Quick Guide to AODV Routing, Wireless Communications Technologies Group, NIST

[17] **David B. Johnson David A. Maltz Josh Broch,** DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks

[18] **L. Abusalah, A. Khokhar, M. Guizani**, Trust Aware Routing in Mobile Ad Hoc Networks

[19] **Lin Chen, Jean Leneutre, Jean-Jacques Puig,** A Secure and Efficient Link State Routing Protocol for Ad Hoc Networks

Santrumpų ir terminų žodynas

AODV – Ad-hoc On demand Distance Vector maršruto parinkimo protokolas

SAODV – Security aware AODV maršruto parinkimo protokolas

SRP – Secure Routing Protocol maršruto parinkimo protokolas

SMT – Secure Message Transfer duomenų perdavimo protokolas

NS-3, NS3 – Network Simulator 3 tinklo simuliatorius

HMAC – Hash based Message Authentication Code autentifikavimo funkcija

RREQ – Route REQuest paketas

RREP – Route REPly paketas

SA – Saugi Asociacija

Priedai

5.1. AODV maršrutizavimo paketų antraštės

5.1.1. RREQ paketas

Tipas[8]	J	R	G	D	U	Rezervas[11]	Šuolių skaičius[8]
RREQ ID[32]							
Gavėjo IP adresas[32]							
Gavėjo krypties naujumo parametras[32]							
RREQ siuntėjo IP adresas[32]							
Siuntėjo krypties naujumo parametras[32]							

5.1.2. RREP paketas

Tipas[8]	L	Rezervas[15]	Šuolių skaičius[8]
Gavėjo IP adresas[32]			
Gavėjo krypties naujumo parametras[32]			
RREQ siuntėjo IP adresas[32]			
Gyvavimo laikas[32]			

Straipsnis

Straipsnis pristatytas ir publikuotas mokslinėje konferencijoje: „Technologijos Mokslo Darbai Vakarų Lietuvoje“, 2010 gegužės 14d.

SAUGUS MARŠRUTIZAVIMAS MOBILIUOSE AD-HOC TINKLUOSE

T.Narbutaitis, R.Plėštys

KTU, Informatikos fakultetas, Studentų g. 50, Kaunas, Lietuva

ANOTACIJA

Mobilieji Ad-Hoc tinklai iškelia vienus didžiausių iššūkių saugumo srityje. Šalia standartinės bevielių tinklų saugumo problemos – nesaugaus informacijos nešėjo, prisideda ir bendra Ad-Hoc tinklo maršrutų sudarymo specifika, aparatinių resursų skurdumas. Dėl šios priežasties saugumo sprendimai, tinkami stacionariesiems tinklams, nėra pakankami saugiam ir efektyviam Ad-Hoc tinklo veikimui. Darbe analizuojami saugaus maršruto parinkimo metodai Ad-Hoc tinkluose.

PAGRINDINIAI ŽODŽIAI: Ad-Hoc, saugumas, maršrutizavimas, maršruto parinkimas, AODV, SAODV, SRP, SMT

ABSTRACT

Mobile Ad-Hoc networks raise some major challenges in the security field. In addition to unsafety of wireless media, Ad-Hoc networks add void of any centralized security infrastructure, scarceness of technical resources. Security solutions from infrastructure wireless networks are not sufficient for secure and effective Ad-Hoc network operation. In this paper security-aware Ad-Hoc routing methods are analyzed.

KEY WORDS: Ad-Hoc, security, routing, AODV, SAODV, SRP, SMT

Įvadas

Belaidžiai tinklai pasaulyje užima vis svarbesnį vaidmenį ir sparčiai keičia laidinius tinklus. Tačiau didžioji dauguma šių tinklų yra centralizuotos architektūros (infrastructure tipo). Taškas-taškas Ad-Hoc tinklai tarp dviejų mazgų naudojami ten, kur būtina išvengti operatorių paslaugų. Mobilieji daugelio šuolių Ad-Hoc turi tikrai naudingų ir unikalių pritaikymo sričių.

Pagrindinės Ad-Hoc tinklų panaudojimo sritys:

1. Laikiniems tikslams, kai reikia greitai ir be išorinių operatorių, t.y. pigiai turėti tarpusavio ryšį.
2. Tarpusavio ryšio palaikymui mobilių karo, policijos, gelbėjimo operacijų metu.
3. Interneto pasiekiamumui nuošaliose vietovėse, kur kurti stacionarią belaidę ar laidinę infrastruktūrą finansiškai neapsimoka.
4. Kaip alternatyvi komunikacijos priemonė stichinių nelaimių atveju, kai visa kita ryšio infrastruktūra yra išvesta iš rikiuotės.

Yra keletas priežasčių, kodėl Ad-Hoc tinklai mažiau paplitę, nei kitos komunikacijos rūšys. Iš dalies tai lemia gan specifinė panaudojimo sritis, tačiau svarbiausia priežastis – vis dar pilnai nerealizuotos esminės efektyviam

tinklo veikimui svarbios funkcijos. Ad-Hoc tinklams negalima tiesiogiai panaudoti tų pačių sprendimų, kurie tinka laidiniams ir centralizuotos infrastruktūros belaidžiams tinklams, nes Ad-Hoc tinklai yra išskirtiniai daugeliu atžvilgių. Pirmiausia jie neturi fiksuotos ryšio ir saugumo infrastruktūros, t.y. bazinių stočių, atskirų maršruto parinkimo įrenginių, RADIUS serverių ir panašiai. Informacija perduodama tiesiogiai tarp tinklo vartotojų įrenginių, vadinamų tinklo mazgais. Kai atstumas tarp siuntėjo ir gavėjo mazgų yra per didelis dėl radijo ryšio aprėpties ribotumo, tenka informacijos perdavimą organizuoti per tarpinius mazgus. Taip pat tinkle mazgų išsidėstymas ir kiekis yra nuolat kintantys.[1]

Tarp daugelio tokiomis sąlygomis kylančių iššūkių, keletas vis dar išlieka neišspręsti, be visuotinai pripažinto pilnai problemą sprendžiančių sprendimų:

1. Plečiamumas (Scalability)[8],
2. Paslaugos kokybė (Quality of Service)[1][8],
3. Energetinis efektyvumas[8],
4. Saugumas.

Saugumas yra kritinė Ad-Hoc tinklo problema, kadangi tinklas veikia viešoje radijo ryšio terpėje, nėra galimybės centralizuotų sertifikatų ir kriptografinių raktų naudojimui, dažnai dėl savo paskirties veikia padidintos rizikos erdvėje. O be tinkamo saugumo užtikrinimo ši technologija negali būti realiai panaudojama.[1,2]

Dėl naudojamos ryšio technologijos fiziniame lygyje saugumo technologijos neegzistuoja, o taikymo lygmenyje jau galima naudoti įvairias saugumo priemones. Šios priemonės gali apsaugoti nuo konfidencialios informacijos atskleidimo, klastojimo, apsimetimo atakų, tačiau turi būti sukurti specifiniai kriptografinių raktų Ad-Hoc tinkle apsikeitimo mechanizmai, atsižvelgta ir į saugumo priemonių įtaką paties tinklo veikimui. Pavyzdžiui dėl raktų apsikeitimo paprastumo, labai perspektyviai atrodo asimetrinė viešojo - privataus rakto infrastruktūra, tačiau ji gali sukelti plečiamumo ir energinio efektyvumo problemų, kadangi naudojant šią sistemą reikia daugiau skaičiavimo ir pralaidumo resursų.

Taikymo lygmenyje veikiančios saugumo priemonės nuo dalies grėsmių gali apsaugoti, tačiau negali padėti nuo atakų, siekiančių išvesti tinklą iš rikiuotės, blokuoti susijungimus. Paslaugų blokavimo ir panašios atakos veikia tinklo lygmenyje. Tam reikalingi saugūs maršrutizavimo (Security aware routing) protokolai. Ad-Hoc tinklų centrinės infrastruktūros, t.y. vienos silpnos grandies neturėjimas yra didelis privalumas, nes pakenkus vienam taškui, visa sistema nėra išvedama iš rikiuotės. Kadangi Ad-Hoc tinkle dažnai tarp siuntėjo ir gavėjo egzistuoja daugiau negu vienas maršrutas, siunčiama informacija gali būti išskaidoma į keletą dalių, siunčiama skirtingais kanalais ir vėl surenkama į vieną vietą tik pasiekusi gavėją. Pakeliui perėmęs tik informacijos fragmentą piktavalis, negalės atskleisti viso pranešimo.[1]

1. Ad-Hoc maršruto parinkimo protokolas AODV (Ad hoc On Demand Distance Vector)

Protokolas AODV (Ad Hoc On Demand Distance Vector) yra labiausiai paplitęs. Maršrutas sudaromas tokiu būdu.

Mazgui A prireikus perduoti informaciją mazgui B, tikrinama ar laikinoje maršrutų lentelėje yra pakankamai naujas maršrutas iki mazgo B, jei ne – sudaromas naujas maršrutas: [6]

1. Siunčiamas paketas RREQ visiems kaimyniniams mazgams.
2. Gavęs paketą RREQ kiekvienas mazgas ieško savo maršrutų lentelėje pakankamai naujo maršruto iki mazgo B, jei neranda – prideda savo adresą į pranešimą RREQ ir siunčia jį toliau visiems savo kaimyniniams mazgams.
3. Kai galiausiai randamas mazgas, turintis maršrutą iki mazgo B, formuojamas pranešimas RREP siunčiamas atgal tuo pačiu keliu mazgui A, tarpiniai mazgai į savo maršrutų lenteles įsitraukia gretimų mazgų adresus.
4. Mazgas A iš paketo pakete RREP gautuoju maršrutu pradeda siunti duomenis, taip pat įsitraukia maršrutą į savo laikiną maršrutų lentelę.
5. Jei vėliau gauna papildomų RREP paketų su geresniais parametrais, atnaujina savo maršrutų lentelę šiais maršrutais.

Standartiškai pagal nutylėjimą visi mazgai laikomi patikimais. Parametrai, apibrėžiantys maršruto gerumą, yra maršruto mazgų kiekis ir maršruto naujumo skaitiklis. Papildomai yra įdiegtas maršruto nutrūkimo pastebėjimo mechanizmas – tarpinis mazgas pastebėjęs kaimyninio mazgo judėjimą iš ryšio zonos siunčia problemos pranešimą siuntėjui, tuomet siuntėjas pakartoja maršruto sudarymo procedūrą.

Šis protokolas efektyviai sprendžia tinklo topologijos kaitos problemą, jei tik maršrutas egzistuoja, jis visuomet randamas, papildomi skaičiavimai ir maršrutizavimo paketų dydžiai nėra dideli. Tačiau taip pat jis palieka daug galimybių kenkti Ad-Hoc tinklui maršrutizavimo lygmenyje.[6]

2. Pagrindinės saugumo grėsmės

1. Pasitikėjimas mazgais pagal nutylėjimą[2].

Dauguma dabartinių Ad-Hoc maršruto parinkimo algoritmų pagal nutylėjimą visus mazgus laiko patikimais, todėl kenkiantys mazgai gali netrukdomi gauti maršruto parinkimo pranešimus, juos modifikuoti ir tokiu būdu įtakoti visą maršruto parinkimo procesą.

2. Galimybė kenkiančiam mazgui apsimesti gavėju[1].

Kenkiantis mazgas gali neperduoti toliau maršruto parinkimo užklausos, o iš karto gražinti savo suklastotą maršruto parinkimo atsakymą, tarsi pats ir būtų gavėjas.

3. Maršruto parinkimo įtakojimas keičiant maršrutizavimo pranešimų parametrus[2].

Kenkiantis mazgas gali neadekvačiai padidinti maršruto naujumo parametrą arba sumažinti mazgų maršrute skaičių, tokiu atveju per jį einantis maršrutas turės didžiausią prioritetą ir paketai eis per jį, o jis galės tuos paketus blokuoti, bandyti atskleisti ar modifikuoti jų turinį.

4. Suklastotų pranešimų apie problemą siuntimas[2].

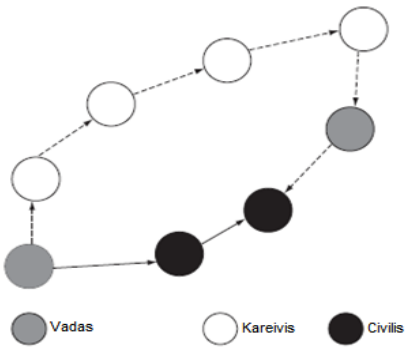
Kenkiantis mazgas gali pasinaudoti AODV algoritmo maršruto nutrūkimo pastebėjimo mechanizmu ir siųsti suklastotus pranešimus apie problemą aktyviame maršrute. Jei kenkiantis mazgas nuolat stebi tinklą ir tik sukūrus naują maršrutą vėl siunčia pranešimus apie problemą jame, visiškai blokuojamas ryšys tarp dviejų mazgų.

3. Saugūs maršruto parinkimo protokolai

Kiekvienas tinklo mazgas privalo perduoti paketus gautus iš savo kaimyno kitam kaimyniniam mazgui, esančiam arčiau šaltinio. Tik kaimyninių mazgų bendradarbiavimas gali užtikrinti, kad informacija bus perduota iš siuntėjo gavėjui, todėl, jei atsiranda mazgas, kuris savo funkciją atlieka ne taip, kaip turėtų dėl techninių problemų ar dėl tyčinių suinteresuotų asmenų veiksmų, kyla įvairios grėsmės viso Ad-Hoc tinklo veikimui. Dėl šios priežasties saugaus maršrutų parinkimo protokolai tokie svarbūs.

3.1. SAODV (security-aware AODV) protokolas

SAODV protokolas yra paremtas AODV protokolu, išskyrus kelis skirtumus.[7] Šiame protokole mazgai nebėra patikimi pagal nutylėjimą, o yra skirstomi pagal saugumo lygį. Saugumo lygį apibrėžia iš anksto nustatyta vieta hierarchinėje struktūroje ir mazgo turimos saugumo užtikrinimo galimybės. Šis algoritmas prideda papildomus saugumo lygio laukus RREQ ir RREP paketams. Reikalingą saugumo lygį nustato siuntėjas, o to lygio negalintys patenkinti mazgai paketus atmeta. Suformavus maršrutą grįžtančiame RREP pakete įtraukiamas mažiausiai saugaus maršruto mazgo saugumo lygis kaip viso maršruto saugumo parametras. Praktinis vaizdas 1 pav. - balti, kareivių mazgai turi aukštesnį saugumo lygį, negu juodi civilių mazgai, tad pasirenkamas nors ir ilgesnis, bet saugesnis maršrutas.



1 pav. SAODV pavyzdys[1]

3.2. SRP(Secure Routing Protocol) ir SMT(Secure Message Transmission) protokolai

Dauguma Ad-Hoc maršruto parinkimo protokolų gali būti padalinti į dvi dalis: maršruto radimą ir duomenų perdavimą rastuoju maršrutu. Abiems šioms dalims būtini papildomi saugumo sprendimai greta standartinio maršruto parinkimo protokolo, kuris kaip jau minėjome anksčiau, neturi beveik jokių saugumo užtikrinimo priemonių. Pirmoji dalis labiausiai jautri atakoms paremtoms apsimetimu gavėju, pasenusios ar piktybiškai modifikuotos maršruto parinkimo informacijos skleidimu. Antroji dalis atvira paketų naikinimo, modifikavimo, klaidingo nukreipimo atakoms. SRP(Secure Routing Protocol)[3] ir SMT(Secure Message Transmission)[4] protokolai buvo sukurti užtikrinti saugumą abiejose šiose dalyse atitinkamai.

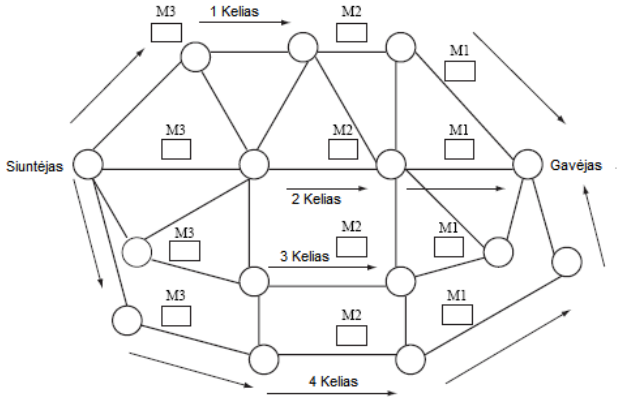
3.3. Saugaus maršrutizavimo protokolas – SRP

Naudojant šį protokolą, Ad-Hoc tinklo darbas įmanomas net ir jame esant kenkiančių elementų. Protokolo funkcionavimui turi būti įkurta Saugumo Asociacija (SA) tarp siuntėjo ir gavėjo mazgų. Iš kitos pusės nėra keliama jokių kriptografinių užduočių tarpiniams mazgams. SRP protokole prireikus sudaryti maršrutą siunčiamas užklausos paketas, kuris kaupia savyje visų mazgų IP adresus, kuriuos praeina, o kai pasiekia gavėją, tuo pačiu maršrutu atgal siunčiamas atsakymo paketas. Joks kitas mazgas negali apsimesti gavėju dėl įkurtos SA, nes neturi gavėjo saugumo raktų, taip pat negali modifikuoti grįžtančio paketo IP adresų sąrašo, nes jis apsaugotas hash funkcija MAC(Message Authentication Code)[1,5]. Tą patį paketą vienas mazgas persiunčia tik vieną kartą, jei ateina dar vienas paketas su tokiu pačiu ID, jis atmetamas. Dar vienas skirtumas nuo kitų maršruto parinkimo protokolų – siuntėjas išsaugo visus grįžusius atsakymo paketus, t.y. suformuojami visi įmanomi maršrutai į kuriuos kiekvienas tinklo mazgas įeina ne daugiau kaip vieną kartą.(2 pav.) Tai yra daroma dėl toliau sekančio SMT protokolo specifikos.

3.4. Saugaus informacijos perdavimo protokolas – SMT

SRP protokolui suformavus maršrutus, informacijos perdavimais jais yra SMT protokolo atsakomybė. Šis protokolas taip pat gali veikti netgi esant kenkiantiems elementams dalyje maršrutų.

SMT protokole siuntėjo mazgas padalina siunčiamą pranešimą į kelias dalis(Pav. 3), tam naudojamas perteklinis algoritmas, kuris užtikrina, kad pranešimą galima rekonstruoti netgi gavus ne visas dalis, kadangi kai kurios dalys gali būti prarastos dėl tinklo trikdžių ar kenkiančių mazgų. Kiekviena siunčiama dalis apsaugoma hash funkcija MAC, todėl tarpiniai mazgai negali jų modifikuoti ar klastoti taip, kad to nepastebėtų gavėjas. Gavėjas, gavęs pranešimo fragmentus, grąžina patvirtinimus taip pat MAC apsaugojimo ir sudalinimo į fragmentus metodu. Siuntėjas tuo metu pagal gautus patvirtinimus keičia maršrutų reitingus, t.y. pakelia reitingą, jei perdavimas pavyksta ir smarkiai sumažina, jei dėl kažkokių priežasčių nepavyksta, tokiu būdu minimizuojamas informacijos srautas per kenkiančius mazgus.



2 pav. Informacijos skaldymas į fragmentus[1]

4. Protokolų lyginamoji analizė

SAODV protokolo pagrindinis trūkumas, kad jis nėra visiškai išbaigtas sprendimas ir išsprendžia tik dalį saugumo problemų.

1 Lentelė. Skirtingų protokolų atsakas į pagrindines saugumo grėsmes

Grėsmė	**SAODV**	**SRP**	**SMT**
Pasitikėjimas mazgais pagal nutylėjimą	Išsprendžiama įtraukiant reitingavimą pagal hierarchinę struktūrą ir mazgų technines saugumo galimybes.	Nesprendžiama, tačiau nepaliekama būdo kenkiantiems mazgams daryti didelę įtaką tinklo veikimui.	Išsprendžiama izoliuojant kenkiančius mazgus, jei jie elgiasi ne taip kaip iš jų tikimasi.
Galimybė kenkiančiam mazgui apsimesti gavėju	Išsprendžiama tik iš dalies, sumažinant galimybes paketui pasiekti kenkiantį mazgą, t.y. neleidžiant patekti jei kenkiančio mazgo saugumo lygis yra nepakankamas	Išsprendžiama įkuriant SA tarp siuntėjo ir gavėjo mazgų.	Nesprendžiama, tai išspręsta SRP protokole.
Maršruto parinkimo įtakojimas keičiant maršrutizavimo pranešimų parametrus	Išsprendžiama tik iš dalies, sumažinant galimybes paketui pasiekti kenkiantį mazgą, t.y. neleidžiant patekti jei	Išsprendžiama apsaugant parametrus MAC hash funkcija, tokiu būdu bet koks jų pakeitimas būtų	Nesprendžiama, tai išspręsta SRP protokole.

	kenkiančio mazgo saugumo lygis yra nepakankamas	pastebėtas siuntėjo arba gavėjo ir būtų atmetamas.	
Suklastotų pranešimų apie problemą siuntimas	Neišsprendžiama.	Nesprendžiama, tai išspręsta SMT protokole.	Naudojamos kitos tinklo priežiūros priemonės, siuntėjas pats stebi maršrutų gyvybingumą, be to dažniausiai yra daugiau negu vienas maršrutas.

Naudojant SRP ir SMT protokolus kartu gaunasi gan išbaigtas ir nuo beveik visų pagrindinių saugumo problemų apsaugantis sprendimas, tiesa ir jis turi silpnų vietų. Jo darbą gali sutrikdyti du kenkiantys mazgai esantys greta vienas kito, taip pat kenkiančiam mazgui gadinant maršrutizavimo paketo ID, tai pastebima tik gavėjo mazge, o kiti tarpiniai mazgai siuntinėja paketus kaip naujus ir padidina tinklo apkrovimą.

Išvados

1. Nuo saugaus maršrutizavimo protokolo priklauso informacijos perdavimo paslaugos kokybė, perdavimo sparta, maršruto suradimo trukmė, paketų vėlinimas ir paketų praradimas.
2. Taikant vieną ar kitą protokolą svarbu nustatyti kaip jis veiks pakankamai didelės apimties Ad-Hoc tinkle, kaip kris tinklo pralaidumas augant mazgų skaičiui, kokią įtaką jis turės tinklo plečiamumui, kaip įtakos maitinimo energijos suvartojimą, kas besąlygiškai įtakos įrenginių autonominio veikimo trukmę.

Literatūra

1. A. Mishra, "Security and Quality of Service in Ad Hoc wireless networks", Johns Hopkins University, 2008, p. 1-5, 8-10,14-15, 129-146.
2. A K Bayya, S Gupte, Y Kshukla, A Garikapati, "Security in Ad-Hoc Networks", Computer Science Department, University of Kentucky, p. 6-7, 14-18
3. P. Papadimitratos and Z. J. Haas, „Secure routing for mobile ad hoc networks",SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, Jan. 27–31, 2002., p. 4-5
4. P. Papadimitratos and Z. J. Haas, „Secure Message Transmission in Mobile Ad Hoc Networks" in Handbook of Wireless Ad Hoc Networks, (M. Ilyas, Editor), CRC Press, 2003, p. 2-4.
5. H. Krawczyk, M. Bellare, and R. Canetti, „HMAC: Keyed-Hashing for Message Authentication", www.rfc-ref.org/RFC-TEXTS/2104/, Feb. 1997, p. 1.
6. C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing Protocol", p. 2-4.
7. S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad-Hoc Routing for Wireless Networks", UIUCDCS-R-2001-2241 Technical Report, Aug. 2001, p. 2-3.
8. K.Taneja, R.B.Patel „An Overview of Wireless Ad Hoc Networks: Challenges and Future.", p. 2-3

SECURITY-AWARE ROUTING IN MOBILE AD-HOC NETWORKS

T. Narbutaitis, R. Plėštys

S u m m a r y

Mobile Ad-Hoc networks are very useful, but raise many challenges and one of the biggest is security. Specially designed routing protocols are required and they are quite well developed except for security area. One of the most popular of the simple, not secure-aware protocols is AODV. It's security-aware extension SAODV offers some enhancements, such as hierarchy of nodes and ability to involve only trusted nodes in the route. Other two protocols try to provide security from a different angle – by splitting packets through more than one

route and reconstructing transmission at the end point. More research is needed not only to develop security features, but also to know how security-aware protocol will perform in large network, what will be its impact on throughput, scalability and energy consumption.