
**KAUNO TECHNOLOGIJOS UNIVERSITETAS**
**INFORMATIKOS FAKULTETAS**

**Aurimas Beršky**s

# PATALPŲ APSAUGOS SISTEMOS TINKLO MODELIO SUDARYMAS IR TYRIMAS

Baigiamasis magistro darbas

**Vadovas**
Lekt. dr. Dangis Rimkus

**KAUNAS, 2015**

**KAUNO TECHNOLOGIJOS UNIVERSITETAS**
**INFORMATIKOS FAKULTETAS**
**KOMPIUTERIŲ KATEDRA**

TVIRTINU
Katedros vedėjas
(parašas) Prof. dr. Algimantas Venčkauskas
(data)

# PATALPŲ APSAUGOS SISTEMOS TINKLO MODELIO SUDARYMAS IR TYRIMAS

Baigiamasis magistro darbas
**Informacijos ir informacinių technologijų sauga (kodas 621E10003)**

**Vadovas**
(parašas) Lekt. dr. Dangis Rimkus
(data)

**Recenzentas**
(parašas) Doc. dr. Jonas Čeponis
(data)

**Projektą atliko**
(parašas) Aurimas Berškys
(data)

**KAUNAS, 2015**

KAUNO TECHNOLOGIJOS UNIVERSITETAS

(Fakultetas)

(Studento vardas, pavardė)

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „Pavadinimas“

**AKADEMINIO SĄŽININGUMO DEKLARACIJA**

20 ___ m. _____ ____ d.

Kaunas

Patvirtinu, kad mano **Aurimo Berškio** baigiamasis projektas tema „.....“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

_____ _____

*(vardą ir pavardę įrašyti ranka)* *(parašas)*

Berškys, A. Patalpų apsaugos sistemos tinklo modelio sudarymas ir tyrimas. Magistro baigiamasis projektas / vadovas lekt. dr. Dangis Rimkus; Kauno technologijos universitetas, informatikos fakultetas, kompiuterių katedra.

Kaunas, 2015. 48 psl.

## SANTRAUKA

Tobulėjant išmaniosioms technologijoms, jos vis sparčiau atkeliauja į kiekvieno asmens namus. Šios sistemos turi galimybę būti valdomos naudojant išmanųjį telefoną ar planšetę. Darbe naudojama patalpų apsaugos sistema taip pat turi tokį funkcionalumą, kuris vartotojui suteikia galimybę gauti pranešimus apie įvykius ar valdyti apsaugos sistemą nebūnant patalpose, kuriose ši įrengta. Tačiau šios apsaugos sistemos darbas nėra ištirtas, kuomet į tinklą įsibrovęs asmuo inicijuoja DoS ataką.

Šiame darbe yra tiriama kokį poveikį sistemos pasiekiamumui sudaro tinkle inicijuojama DoS ataka. Tyrimui vykdyti yra sukuriamas tyrimo metodas, aprašant tyrimo kriterijus ir nustatant kas yra laikoma DoS ataka. Taip pat, darbo metu yra sukuriami dviejų tipų patalpų apsaugos sistemos tinklo modeliai, kurių vienas yra vietinio tinklo modelis su viena patalpų apsaugos sistema, o kitas – tarpmiestinis tinko modelis, kuriame veikia tūkstantis sistemų.

Modelių tyrimas atliekamas naudojant „Riverbed Modeler“ tinklų modeliavimo įrankį. Tyrimo metu nustatomas vidutinis tinklo modelių tinklo srauto dydis ir vidutinis užklausos atsako vėlavimo laikas tinklui veikiant įprastu režimu, bei kuomet tinkle yra vykdoma DoS ataka.

Atlikus tyrimą ir nustačius atakos poveikį apsaugos sistemos pasiekiamumui, tinklo modeliuose diegiami saugumo sprendimai, užtikrinantys patalpų apsaugos sistemos pasiekiamumą atakos metu. Modifikuoti tinklo modeliai su įdiegtais saugumo sprendimais tiriami dar kartą, siekiant nustatyti, koks įdiegtų saugumo sprendimų efektyvumas, kuomet tinklas yra atakuojamas DoS ataka.

Berškys, A. Development and research of premisses security systems network model. Masters thesis / supervisor lect. dr. Dangis Rimkus; Department of Computer Science, Faculty of Informatics, Kaunas University of Technology.

Kaunas, 2015. 48 psl.

## SUMMARY

As smart technologies advance, they arrive to every persons home. These systems have a possibility to control them by using smartphone or tablet. In this work smart premises security system is used, which also has an option to be controlled using smartphone or table and gives an opportunity for a user to get notifications about events or control system status even when user is not near security system. However, premises security system has not been investigated when network in which it is working is accessed by a hacker and DoS attack is initiated.

In this work, a research is done to know what impact is done to premises security systems for accessing the system when DoS attack is initiated. To conduct a research, research method is made by describing research criteria and defining what is a DoS attack in this research. Also, during this work two network models are created. One of them is when security system works in a local network and other model is made when there is a thousand of security systems in the network.

Models research is done by using network modelling software “Riverbed Modeler”. During models testing average received traffic size and request delay time is determined in both models when network is working in its usual state and when DoS attack is initiated.

After tests and simulations and after finding effect of the attack to premises security systems accessibility, security upgrades are installed to each model in order to ensure systems accessibility when DoS attack is affecting the network. Updated network models with security upgrades are tested again in order to find out how effective these security upgrades are when DoS attack is active in the network.

**TURINYS**

**LENTELIŲ SĄRAŠAS**

**PAVEIKSLŲ SĄRAŠAS**

## TERMINŲ IR SANTRUMPŲ ŽODYNAS

DoS ataka – (angl. *Denial of Service*) ataka, nukreipta prieš kompiuterinę sistemą, dėl kurios sistema tampa nepasiekiama vartotojams.

ICMP – (angl. *Internet Control Messages Protocol*) interneto kontrolės žinučių protokolas, skirtas perduoti klaidos informaciją duomenų siuntėjui. ICMP naudojamas *ping* ir *traceroute* programose.

TCP – (angl. *Transmission Control Protocol*) perdavimo kontrolės protokolas. Vienas iš pagrindinių internetinių protokolų, kuris priklauso transportavimo lygmeniui.

UDP – (angl. *User Datagram Protocol*) vartotojo duomenų protokolas. Šis protokolas yra TCP protokolo alternatyva.

IP – (angl. *Internet Protocol*) pagrindinis interneto komunikacijų protokolas, kurio užduotis yra perduoti tinklo paketus iš siuntėjo gavėjui.

MPLS – (angl. *Multiprotocol Label Switching*) inkapsuliuojantis protokolas, žymintis srautus MPLS tinklo įėjimo taškuose ir naikinantis žymę MPLS tinklo išėjimo taške.

OSPF – (angl. *Open Shortest Path First*) atviras pirmo trumpiausio kelio nustatymo protokolas. Jis užtikrina informacijos apie maršrutizavimo galimybes sklaidą tarp maršrutizatorių, priklausančių tai pačiai autonominei sistemai.

VoIP – (angl. *Voice over IP*) tai yra balso ryšys perduodamas interneto tinklais.

Mbps – tinklo greitis. Megabitai per sekundę.

Kbps – tinklo greitis. Kilobitai per sekundę.

# ĮVADAS

Šiuolaikinėms technologijoms sparčiai žengiant į priekį, kiekviename būste galima rasti ne vieną technologinį įrenginį. Šiais laikais daugelis įrenginių yra taip vadinami išmanieji – atliekantys daugiau funkcijų nei jiems priklauso. Siekiant apsaugoti savo turtą nuo įsilaužėlių, vartotojai savo namuose vis sparčiau diegia patalpų apsaugos sistemas. Tačiau šiame „išmaniajame“ amžiuje net ir paprastos apsaugos sistemos spėjo ištobulėti. Nuo šiol gali ne tik perduoti pavojaus signalą į apsaugos įmonės sistemos pultą, kad apsaugos darbuotojai galėtų greit sureaguoti į pavojaus iškvietimą, bet ir informuoti būsto savininką pačiais įvairiausiais būdais – trumpąja žinute, skambučiu, ar netgi naudojant išmaniojo telefono ar planšetinio kompiuterio taikomąją programą, net jeigu savininkas yra išvykęs labai toli nuo savo namų.

Šis darbas skirtas atlikti tokių išmaniųjų patalpų apsaugos sistemų sujungtų į bendrą interneto tinklą modeliavimui ir tinklo bei apsaugos sistemų veiksmų stebėjimui atakos metu, panaudojant gytas žinias apie internetines atakas, bei apsisaugojimą nuo jų.

**Šio darbo tikslas –** išsiaiškinti kiek saugu yra diegti sukurtą apsaugos sistemą vartotojų namuose ir nustatyti kokios pasekmės gali laukti vartotojų internetinės atakos metu.

Siekiant įgyvendinti šį tikslą, keliami tokie uždaviniai:

1. Išanalizuoti internetinių atakų tipus, bei sukurtos patalpų apsaugos sistemos veikimą.
2. Pasirinkti internetinės atakos metodą ir panaudoti jį tyrimui.
3. Sukurti patalpų apsaugos sistemų tinklo modelį, kuris būtų panašus į realybėje galimo sukurti apsaugos sistemų tinklo modelį.
4. Nustatyti, kaip yra paveikiamas apsaugos sistemos darbas ir atsakas į siunčiamas komandas, kuomet tinkle vykdoma ataka.
5. Rasti saugos sprendimą, padėsiantį vartotojui neprarasti ryšio su apsaugos sistema, net jeigu bus vykdoma ataka.

Darbą sudaro keturi skyriai, kurių pirmasis – „Atakų internetu metodai ir sistemos analizė“. Šiame skyriuje yra analizuojamos visos galimos internetinių atakų rūšys, ir apžvelgiama pati apsaugos sistema, siekiant suprasti jos veikimą. Antrasis skyrius – „Apsaugos sistemos, esančios tinkle atakos metodo sudarymas“ aprašo patį apsaugos sistemų tinklo modelį, iš ko jis sudarytas ir kodėl yra pasirinktas būtent šis testavimo metodas. Trečiajame skyriuje aprašomas sukurto modelio testavimas ir rezultatai atakos metu. Paskutiniame skyriuje aprašomas pagerintas tinklo modelis, nurodomi tinklo pagerinimai ir pakeitimai, padedantys neprarasti apsaugos sistemos pasiekiamumo tinklo atakos metu.

# 1. ATAKŲ INTERNETU METODAI IR SISTEMOS ANALIZĖ

## 1.1. Darbe nagrinėjama problema ir jos apžvalga

Išmaniosioms sistemoms vis labiau žengiant į mūsų kasdienybę, vartotojų namuose atsiranda vis daugiau išmaniųjų įrenginių – nuo išmaniųjų dušų, kavinukų ar užuolaidų, iki išmaniųjų šildymo, vėdinimo ar apšvietimo sistemų. Visos išmaniosios sistemos turi galimybę valdyti jas naudojantis internetu. Pavyzdžiui, esant darbe, prieš baigiant darbą galima išmaniuoju telefonu ar interneto naršykle prisijungti prie išmaniojo šildymo sistemos ir įjungti šildymą, kad grįžus namo, pasitiktų optimali patalpų temperatūra. Taip pat, į gyventojų namus vis labiau skverbiasi ir išmaniosios patalpų apsaugos sistemos, kurios leidžia įjungti ar išjungti apsaugos sistemą, valdyti apsaugos zonas, peržiūrėti įvykius, ar gavus pranešimą apie apsaugos sistemos suveikimą imtis atitinkamų veiksmų, net būnant kitame pasaulio krašte.

Tam, kad apsaugos sistema būtų pasiekiama iš bet kur, ji turi turėti prieigą ne tik lokaliame interneto tinkle, tačiau ir globaliame. Apsaugos sistemos pajungimas į globalų tinklą iškart sukuria papildomas grėsmes saugumui, kadangi interneto įsilaužėliai gali bandyti pakenkti apsaugos sistemai.

Panaudojus internetines atakas, priklausomai nuo atakos mąsto, vartotojas ar visi vartotojai prie gali nepasiekti informacijos apie savo apsaugos sistemos būseną ir įvykus fiziniam įsilaužimui, nebūti informuoti apie tai.

Internetinės atakos yra aktuali problema siekiant namus aprūpinti išmaniosiomis apsaugos sistemomis, kurios būtų sujungtos į bendrą interneto tinklą, todėl šiame darbe vykdomas tyrimas yra skirtas nustatyti kokio mąsto grėsmė kiltų vykdant internetinę ataką į tinklą, kuriame yra prijungta (ar prijungtos) apsaugos sistemos, bei kokių reikėtų imtis veiksmų, kad net ir vykdant internetines atakas, vartotojams būtų pasiekiama jų patalpų apsaugos sistema.

## 1.2. Tyrimų objekto detalizavimas, siūlomos tyrimo metodikos apibūdinimas

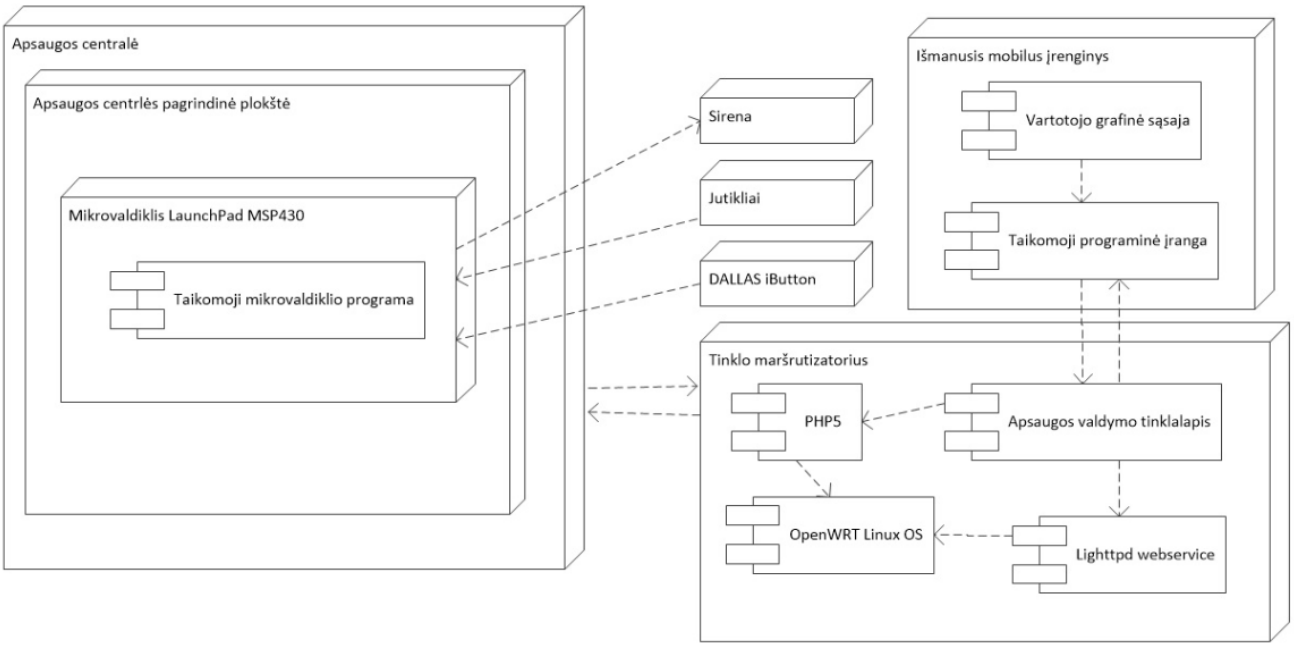
Šio darbo tyrimo objektas yra internetinis tinklas, kuriame prijungta išmanioji patalpų apsaugos sistema. Tyrimo metu siekiama nustatyti, kaip paveikiamas internetinis tinklas vykdant internetinę DoS (*angl. Denial of Service*) ataką, kuomet ataka vykdoma lokaliame interneto tinkle, kuriame pajungta tik viena apsaugos sistema, bei kuomet ataka yra vykdoma tinkle, kuriame yra prijungta daugiau nei viena apsaugos sistema. Išsiaiškinus atakos poveikį tinklui, priimamas sprendimas, kaip reikėtų perorganizuoti interneto tinklą, kad apsaugos sistemos (sistemų) darbas tinkle nebūtų sutrikdytas.

## 1.3. Trumpa naudojamos išmaniosios patalpų apsaugos sistemos analizė

Tyrime naudojama išmanioji patalpų apsaugos sistema yra pagaminta tai, kad ją galima būtų įjungti arba išjungti naudojantis internetu, arba panaudojant magnetinį raktą DALLAS iButton. Interneto pagalba, šią sistemą galima valdyti naudojant interneto naršyklę, arba sukurtą išmaniojo telefono programėlę, naudojant interneto ryšį. Atsižvelgiant į tai, kaip apsaugos sistema yra prijungta prie tinklo – lokaliai, ar su galimybe būti pasiekiamai iš globalaus interneto tinklo, vartotojas ją gali valdyti tik būdamas prie savo patalpų (kuomet išmanusis telefonas ar kompiuteris yra tame pačiame vietiniame tinkle), arba kuomet vartotojo išmanusis telefonas ar kompiuteris yra prisijungęs prie interneto tinklo bet kurioje pasaulio vietoje. Apsaugos sistema yra sudaryta iš sistemos centrinio valdymo bloko, kurio paskirtis yra prijungtų jutiklių informacijos priėmimas ir jutiklių (durų, langų ir kt.) valdymas. Apsaugos sistemos centrinis valdymo blokas yra prijungtas prie interneto tinklo maršrutizatoriaus, kuris suteikia galimybę sistemos būseną stebėti ir valdyti, bei gauti informaciją apie sistemos būsenos pasikeitimus nuotoliniu būdu interneto ryšiu. Tinklo maršrutizatorius, prie kurio prijungtas centrinis sistemos valdymo blokas, taip pat veikia kaip apsaugos sistemos serveris, kuriame yra patalpintas internetinis sistemos valdymo tinklapis, saugoma įvykių istorija, prisijungimo vardas ir slaptažodis ir kita informacija. Į savo išmanųjį telefoną įdiegus specialią taikomąją programą,

vartotojas gali sistemą valdyti nenaudodamas internetinio tinklalapio. Visus veiksmus atlikti gali naudodamas įdiegtą taikomąją programą.

Principinė apsaugos sistemos komponentų diagrama yra pavaizduota 1.1 pav.

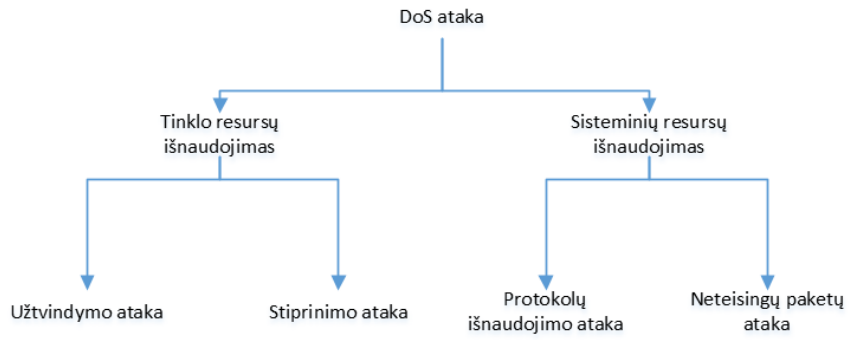



**1.1 pav. Išmaniosios patalpų apsaugos sistemos komponentų diagrama**

## 1.4. Atsisakymo aptarnauti atakos (DoS atakos)

Atsisakymo aptarnauti ataka (*angl. Denial of Service)*, kitaip vadinama DoS ataka, yra ataka, kurios metu sutrikdomas interneto tinklo veikimas, bei kai kurios ar visos interneto paslaugos tampa nebeprieinamos. Šios atakos yra įvairių tipų ir gali būti nutaikytos prieš atskirus vartotojus, vartotojų grupes ar ištisas kompiuterines sistemas. DoS atakos dažniausiai yra skirstomos į tris lygius, pagal atakos žalą ir atakos rimtumą. Paprasčiausia DoS ataka išnaudoja programinės įrangos klaidas, kurios gali būti paliktos ir nepastebėtos programiniame išeities kode. Antrojo lygio DoS ataka naudojama žinant konkrečią informaciją apie sistemą, stengiantis išnaudoti naudojamus interneto protokolus, limituotą talpyklos vietą, siekiant sukelti tinklo srauto perdavimo vėlavimą, taip apribojant sistemos pasiekiamumą ir galimybę naudotis sistema. Trečioji, daugiausiai žalos atnešanti ataka, naudoja ypatingas tinklo protokolų charakteristikas, siekiant atakuoti tinklą. Šios atakos yra sukurtos taip, kad tinkle nebūtų pastebėta jokių anomalijų, o pati ataka būtų užmaskuota taip, lyg tai būtų įprastinis tinklo srautas. [1]

DoS ataka gali būti įprastinė, arba paskirstytoji. Įprastinė DoS ataka yra vykdoma panaudojant vieną atakuojančią sistemą (kompiuterį), kuomet paskirstytajai DoS (*angl. Distributed Denial of Service*) yra naudojami keli, keliasdešimt ar net keli šimtai sistemų, kuriomis siunčiamas atakos tinklo srautas.



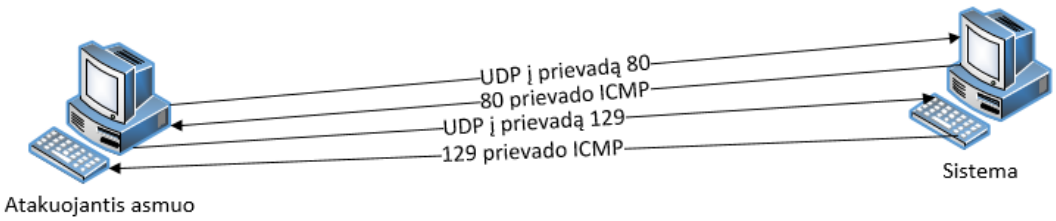

**1.2 pav. DoS atakų klasifikacija**

Taip pat, 1.2. paveiksle pateikiama DoS atakų klasifikacija, kurioje vaizduojama į kokius atakų tipus yra skirstomos įprastinės ir paskirstytosios DoS atakos.

DoS atakos yra skirstomos į dvi pagrindines grupes, pagal tai kas yra išnaudojama atakos metu. Atakos yra skirstomos į atakas, išnaudojančias tinklo resursus ir atakas, išnaudojančias sisteminius resursus. Pirmoji atakų grupė naudojasi tinklo pralaidumu siekiant padaryti sistemą ar paslaugas neprieinamas vartotojams, kuomet siunčiami dideli paketų kiekiai, su kuriais serveris nesugeba susidoroti. Išnaudojant sisteminių resursų spragas, ataka yra nutaikyta tiesiai į techninę įrangą, siekiant sukelti sistemos nepasiekiamumą, išnaudojant visą įrenginio procesoriaus, operatyviosios atminties ar kitos įrangos darbą, taip sukeliant tinklo vėlavimus ir neatsakymą į užklausas. Šios grupės atakos taip pat išnaudoja ir buferio ar steko perpildymus naudojant neteisingus paketus. [3]

## 1.5. UDP paketų užtvindymas

UDP užtvindymo ataka vykdoma tuomet, kai atakuojantis asmuo generuoja milžiniškus paketų kiekius į atsitiktinius aukos sistemos tinklo prievadus. [2] Jeigu tinklo prievadas yra uždarytas , aukos sistema privalo atsakyti į paketo užklausą siųsdama atgal ICMP paketą su informacija, kad prievadas yra uždarytas ir neprieinamas. Kadangi į prievadus siunčiamas milžiniškas kiekis paketų su užklausomis, atsakymų kiekis taip pat yra milžiniškas. Dėl to sistema dažniausiai tampa nepajėgi laiku atsakyti į visas užklausas, kas reiškia, kad sistemos darbas nuosekliai lėtėja, kol visiškai yra sutrikdomas ir sistema tampa nebeprieinama.



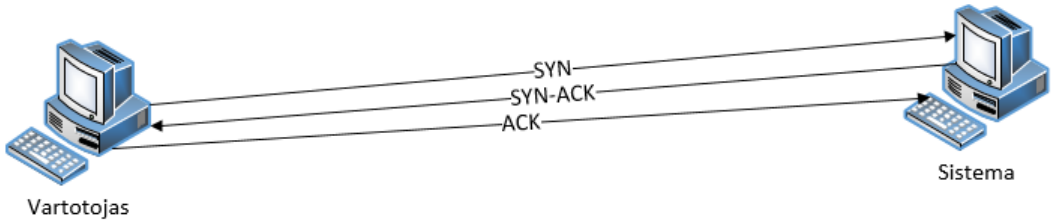

**1.3 pav. UDP paketų užtvindymas**

1.3. pav. yra vaizduojama tinklo užtvindymo UDP paketais schema, kuomet atakuojantis asmuo į pasirinktus ar atsitiktinius prievadus siunčia UD paketus, kurių kiekiai būna milžiniški.

## 1.6. TCP SYN paketų užtvindymas

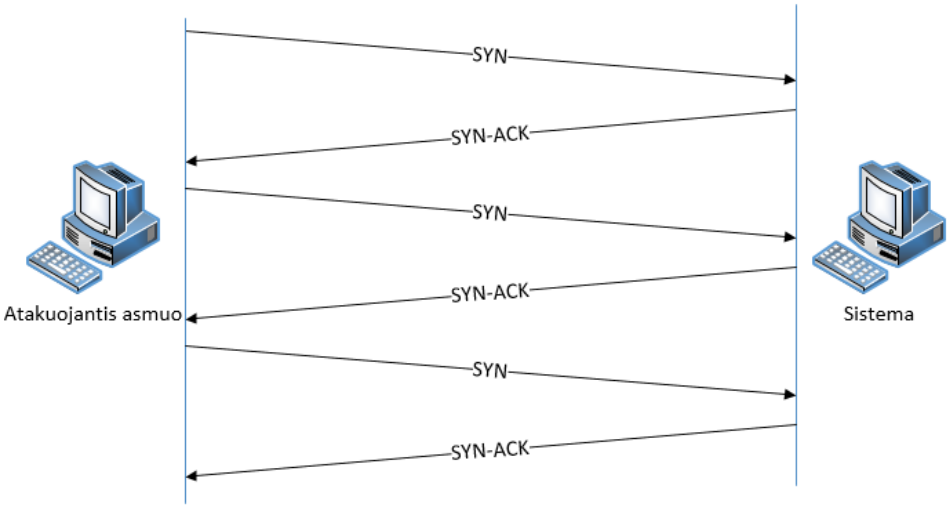
Kita užtvindymo atakų rūšis yra TCP SYN paketų užtvindymo ataka. DoS atakos dažnai išnaudoja įvairius tinklo komunikacijos pažeidimus, kadangi protokolai reikalingi komunikacijai, naudoja resursus palaikyti tinklo būsenai. [4] TCP SYN paketų užtvindymo DoS ataka gali turėti įvairaus dydžio poveikį sistemai. Kuomet prie tinklo prisijungęs vartotojas bando užmegzti TCP ryšį, pirmiausiai iš kliento į sistemą yra siunčiamas SYN tipo paketas. Kuomet tinklas yra pasiekiamas ir

sujungimas yra leidžiamas, sistema vartotojui siunčia SYN-ACK tipo paketą atgal kaip atsakymą (*angl. Acknowledged*). Vartotojo kompiuteris prisijungimą baigia siųsdamas į sistemą ACK tipo paketą. Sistema, gavusi vartotojo SYN paketą, turi išskirti atmintį, kurioje bus laikoma pusiau atidarytos jungties informacija. Ši atmintis nėra atlaisvinama iki sistema gauna iš vartotojo atsakantįjį ACK tipo paketą, arba kol sujungimas nustoja galioti. TCP ryšio užmezgimo eiga vaizduojama 1. 4. Pav.




**1.4 pav. TCP jungties užmezgimas**

Vykdant TCP SYN paketų užtvindymo ataką, atakuojantis asmuo siunčia pirmąjį TCP SYN paketą, tačiau gavęs iš sistemos atsakymą – SYN-ACK tipo paketą, neišsiunčia paskutiniojo ACK paketo atgal į sistemą. Tokiu atveju jungtis lieka pusiau atvira, jai yra išskirta atmintis, kuri nėra atlaisvinama. Tuo pačiu atakuojantis asmuo siunčia daugiau tokio pat tipo užklausų į sistemą, taip naudodamas vis daugiau sistemos atminties resursų, kol galiausiai sistema tampa nebepajėgi atsakyti į užklausas. TCP SYN paketų užtvindymo ataka pavaizduota 1.5. pav.




**1.5 pav. TCP SYN paketų užtvindymo ataka**

Kaip galima pastebėti, ši schema nuo įprastinės skiriasi tuo, kad nebeatsakoma į sistemos atsiųstą SYN-ACK paketą ir iškart siunčiamas naujas SYN paketas, dar vienos jungties užmezgimui.

### 1.7. „Mirties Ping“

„Mirties Ping“, tai dar viena DoS atakos rūšis, kurios metu sistema tampa nepasiekiama, kaip ir kitų atakų tipų metu, tačiau ši ataka yra apgalvota ir ją sunkiau numatyti.

Ping – tai įrankis, naudojamas siekiant nustatyti, ar tam tikras IP adresas, ar serveris, ar sistema yra pasiekiama interneto (ar lokaliame) tinkle, ir apskaičiuoja kiek laiko užtrunka, kol siunčiamas paketas pasiekia gavimo adresą. Standartinis ping yra vienas paketas be jokios perduodamos informacijos, dėl to yra visiškai nesukeliantis žalos. [5]

Naudojant „Mirties ping“ ataką, atakuojantis asmuo į sistemą siunčia ping paketą, kurio dydis yra didesnis nei 65535 baitų, kuriuos sistema gali priimti. Ši žinutė yra išskaidoma į fragmentus, kurie į sistemą siunčiami kaip atskiri IP paketai, o sistema gavusi juos sujungia į bendrą visumą, tam kad galėtų perskaityti paketo turinį. Kuomet visas ping paketo turinys sujungiamas į vientisą paketą, sistemos buferio dydis dažniausiai yra ne toks didelis, kad galėtų apdoroti gautą paketą (kadangi

paketas yra netinkamo dydžio), kas iššaukia sistemos buferio perpildymą ir sukelia sistemos nepasiekiamumą, nes dažniausiai sistema nesugebanti apdoroti buferyje esančios informacijos persikrauna, išsijungia arba pradeda keistai elgtis.

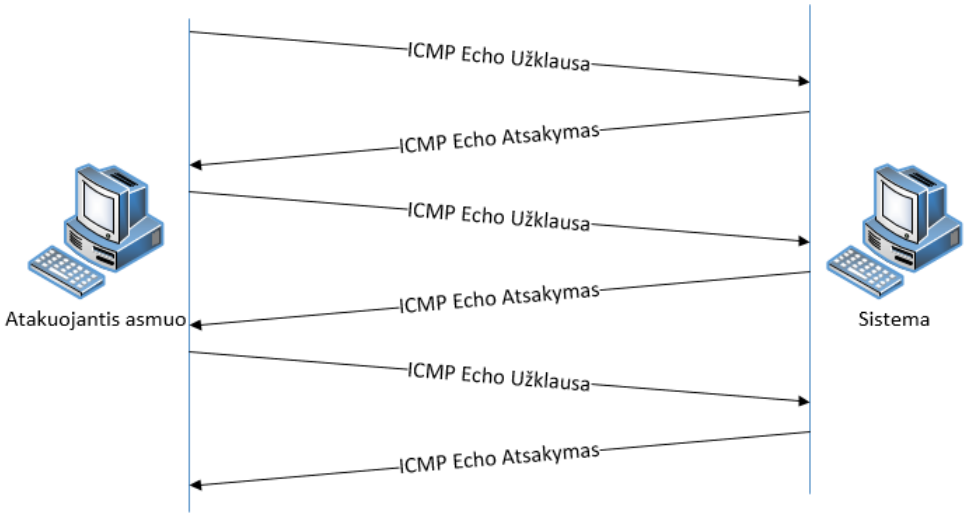
### 1.8. ICMP Ping paketų užtvindymas

ICMP tipo paketų protokolas valdo klaidų ir valdymo pranešimus. Kitaip tariant, ICMP paketai yra siunčiami maršrutizatorių ar sistemų tam, kad pranešti apie klaidas, ar iškilusias problemas sistemai, kuri kreipėsi. Kuomet pranešimas yra sugeneruojamas ir įvyksta klaida, originali paketo IP antraštė yra apgobiama atitinkamu ICMP pranešimu ir šie du pranešimai yra apgaubiami nauja IP paketo antrašte, kuri kartu su paketu grąžinama paketo siuntėjui. [6]

Geriausiai žinomas ICMP pranešimo panaudojimo pavyzdys praktikoje yra ping įrankis. Ping įrankiai naudoja ICMP pranešimus siekiant nustatyti nutolusio tinklo ar sistemos pasiekiamumą ir atsakomumą, bei nustatyti kiek laiko truko atsakymo gavimas iš nutolusio tinklo ar sistemos. Galima teigti, kad ICMP pranešimai yra labai naudingi, ypač kuomet tinkle yra įvykusi klaida ir tinklas nėra pasiekiamas.

Deja, tačiau blogai nusiteikę asmenys, siekiantys sukelti žalą sistemoms, ar tiesiog sutrikdyti tinklo veikimą, sugalvojo šį gerą tinklo įrankį panaudoti blogiems tikslams.

ICMP Ping paketų užtvindymas – tai ataka, kurios metu yra siunčiamas milžiniškas ping paketų kiekis, dažniausiai naudojant Unix šeimos sistemą kaip atakuojančiąją pusę. Vykdant šią ataką, atakuojama sistema nebesugeba greitai ir efektyviai atsakinėti į atsiradusį teisėtą tinklo srautą, dėl ko atsiranda tinklo srauto vėlavimas ir vėliau tinklas tampa visiškai nebepasiekiamas. Paveiksle 1.6. yra pavaizduotas ICMP Ping paketų siuntimo pavyzdys.

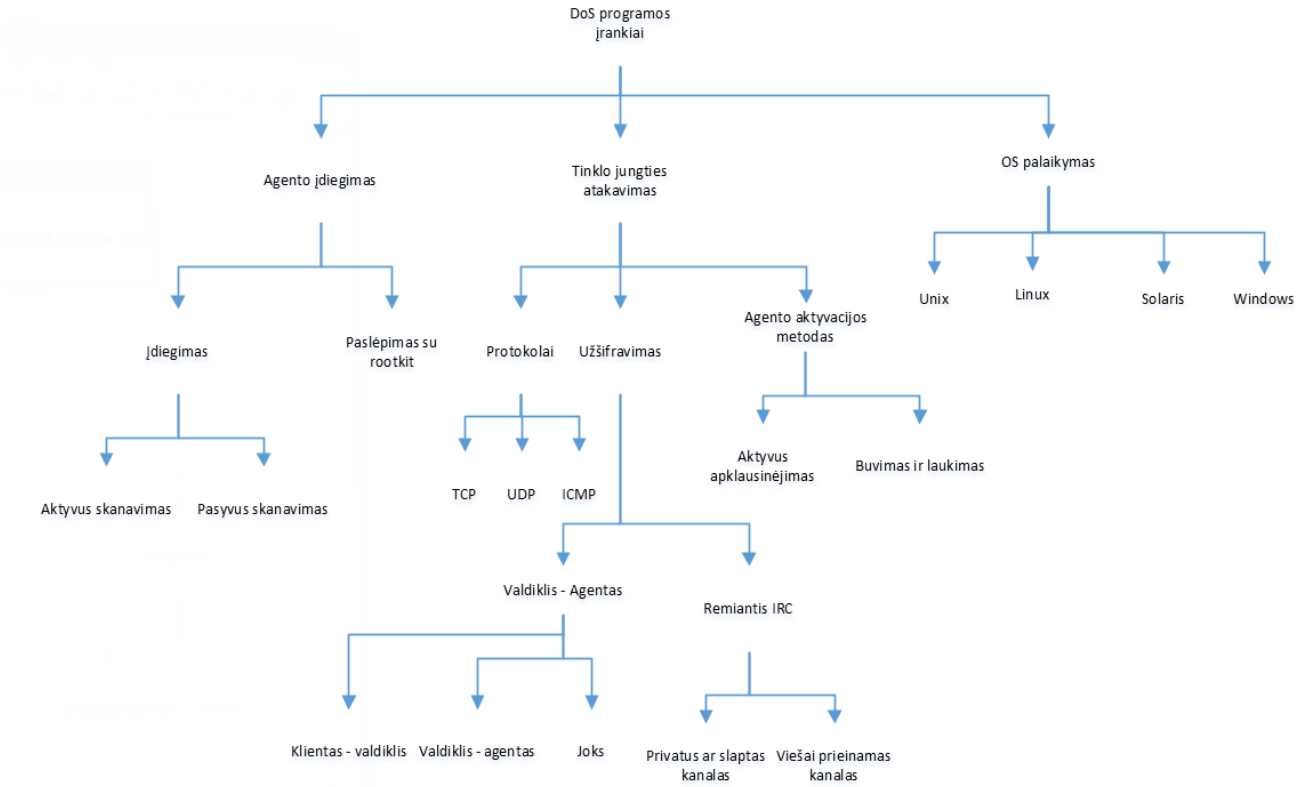



**1.6 pav. ICMP Ping paketų siuntimas**

Tokiu būdu taip pat yra vykdoma ir ICMP Ping paketų užtvindymo ataka, tik atakos metu per vieną sekundę yra siunčiamas ne vienas ar keli paketai, bet tūkstančiai, ar net šimtai tūkstančių paketų.

### 1.9. Įrankiai, naudojami DoS atakoms vykdyti

Įsilaužėliai, norintys sutrikdyti sistemos darbą, padaryti ją nepasiekiamą, naudoja tam skirtus įrankius. Dažniausiai tai būna įvairios specializuotos taikomosios programos, kurios yra skirtos inicijuoti ir vykdyti DoS atakas. Tačiau neretai tokia neteisėta veikla užsiimantys asmenys turi ir įrankius ar programas, kurios gali pasigirti didele įrankių gausa, skirta vykdyti internetines atakas, ar kitaip kenkti nutolusioms sistemoms. DoS atakoms vykdyti naudojamą programinę įrangą galima klasifikuoti ir skirstyti pagal įrankių veikimo charakteristikas.[7] Klasifikacijos schema yra pavaizduota 1.7. pav.




**1.7 pav. DoS atakų įrankių klasifikacija**

Kaip galima matyti iš paveikslėlio, įrankių klasifikacija yra labai didelė, pagal įvairius kriterijus. Stambiausios yra trys įrankių grupės – įdiegiami agentai, kurie skanuoja atakuojamą sistemą, siekiant nustatyti ir sužinoti kuo daugiau sistemos savybių, tinklo jungties atakos – kuomet sistema atakuojama per jos tinklą, siekiant sutrikdyti sistemos pasiekiamumą, bei įrankiai, nukreipti prieš operacines sistemas, panaudojant sistemų klaidas ir pažeidžiamumus. Visos trys grupės toliau skaidomos į mažesnes klasifikacijos grupes, kaip pavyzdžiui, tinklo jungties atakų įrankiai klasifikuojami į skirtus protokolų atakoms, užšifravimo atakoms, agento aktyvacijos metodų atakoms.

## 1.10. Išvados

Išsiaiškinus išmaniosios patalpų apsaugos koncepciją, iš ko ji sudaryta ir kaip veikia, nustatyta, kaip atakos metu galima būtų sutrikdyti sistemos darbą. Tam, kad sistemos darbas būtų sutrikdytas ir ji taptų neprieinama, reikalinga panaudoti DoS ataką, naudojant tinklo užtvindymo atakas. Taip pat buvo išanalizuoti tinklo užtvindymo atakų tipai, kuriais galima padaryti sistemą neprieinamą. Užtvindymo atakos veikia, panaudojant įvairius paketų tipus, tokius kaip TCP SYN, ICMP ping, ar UDP paketus. Atakuojančiam asmeniui siekiant sutrikdyti apsaugos sistemos prieinamumą, reikia panaudoti tam skirtą įrankį, kurių klasifikacija taip pat buvo išanalizuota. Atlikus pilną analizę, nustatyta, kad pagal DoS atakų įrankių klasifikaciją, įrankiai turėtų priklausyti tinklo jungties atakavimo grupės įrankių, protokolų porūšiui.

# 2. PATALPŲ APSAUGOS SISTEMOS TINKLO MODELIO SUDARYMO METODAS IR PRIEMONĖS

## 2.1. Modelio sudarymo priemonės

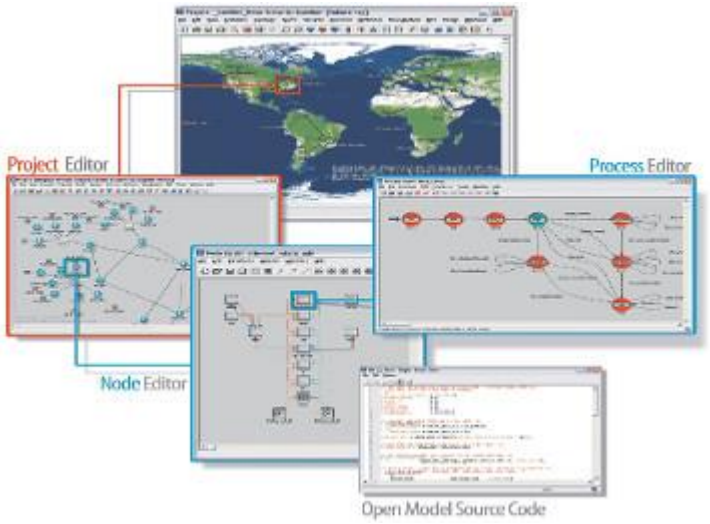
Atliekant tyrimą, pagrindinis įrankis, kuris yra naudojamas – „Riverbed Modeler“ tinklo modeliavimo programa.

„Riverbed Modeler“ – yra atnaujintas įrankis, anksčiau vadinęsis „OPNET“. Naująją „OPNET“ įrankio versiją sukūrė kompanija „Riverbed“, įsigijusi visas senosios programos teises. Naujoji kompanija ištaisė senosios programos klaidas, bei patobulino ir atnaujino programoje naudojamus įrankius.

„Riverbed Modeler“ leidžia modeliuoti bet kokio tipo ir topologijos tinklą, bei stebėti procesus ir tinkle esančių įrenginių elgseną atliekant tinklo veikimo simuliaciją vienu ar kitu atveju.

Norint išsiaiškinti, koks poveikis atakuojant tinklą, yra apsaugos sistemai, ir kiek reikšmės turi DoS ataka, reikia sukurti metodą, kuriuo remiantis bus atliekamas tyrimas. Dirbant su „Riverbed Modeler“ suteikiama galimybė geriau suprasti ir analizuoti tinklo veikimo principus, bei atrasti tai, kas gali būti nepastebima tiesiog kuriant realų tinklą ir jį testuojant realybėje. Tai sumažina testavimo ir tinklo kūrimo kaštus. [8]

Tyrimo metu, „Riverbed Modeler“ leidžia sukurti reikalingą tinklo modelį, kuris galėtų būti naudojamas realybėje jungiant išmaniąją apsaugos sistemą (ar daugiau nei vieną sistemą) į visuotinį interneto tinklą, stebėti sistemos pasiekiamumą, elgseną atakos metu, bei nustatyti, kokie atakos pažeidžiamumai yra matomi tinkle ir kokių saugos priemonių būtų galima imtis, tam kad užtikrinti apsaugos sistemos nepertraukiamą veikimą ir pasiekiamumą.




**2.1 pav. „Riverbed Modeler“ įrankio darbiniai langai**

Tinklo modeliavimo įrankis palaiko nemažai modeliavimo aplinkų, skirtų įvairiems modeliavimo procesams kurti ir stebėti. Keletas iš galimų modeliuoti aplinkų yra:

- MPLS
- IP
- VOIP
- OSPF
- TCP

Tinklo modelis gali būti modeliuojamas tiek kuriant tinko topologiją – dėliojant tinkle esančius komponentus, skirstant IP adresus, bei kuriant maršrutizavimo lenteles, tiek atliekant gilesnių modeliavimo lygių pakeitimus, tokius kaip:

- Tinkle esančio komponento programinio kodo pakeitimus – kuomet keičiamas pačio tinkle esančio komponento programinis kodas, keičiant komponento veikimo elgseną gaunant, ar siunčiant paketus.
- Tinkle esančio komponento procesų redagavimas – tinkle esančio komponento procesų redagavimas leidžia nustatyti, kaip komponentas elgiasi vienu ar kitu atveju, kokia logika yra naudojama jam atliekant vienokius, ar kitokius veiksmus, kurie atliekami vykdant komponento programinį kodą (pvz. mesti klaidos pranešimą gavus neteisingą paketą).
- Pakeitimai vieno komponento lygyje – tai yra labiau techninis komponento redagavimas, kurio metu galima pridėti ar pakeisti komponento viduje esančių elementų išsidėstymą ir ryšius. Pavyzdžiui, redaguojant komponentą vieno komponento lygyje, galima pridėti daugiau interneto jungčių, jų sumažinti, sudėlioti taip, kad maršrutizatorius (pavyzdinis komponentas) turėtų daugiau nei vieną MAC adresą ir t.t.

## 2.2. Modelio sudarymo metodas

Tyrimo metodas naudoja du skirtingus modelius, kuriuose tiriamas atakos poveikis. Tačiau skirtinguose modeliuose, atakos poveikis gali būti skirtingas, todėl yra sudaromi du skirtingi tinklo modeliai – pirmasis, kuomet patalpų apsaugos sistema nėra prieinama iš išorės, bei pasiekiama tik esant tame pačiame lokaliame tinkle, kuriame yra tik viena patalpų apsaugos sistema, o antrasis – kuomet patalpų apsaugos sistemų yra daugiau nei viena ir visos sistemos yra sujungtos į vieną bendrą tinklą. Šis tinklas yra dalis visuotinio išorinio interneto tinklo, todėl patalpų apsaugos sistema gali būti pasiekiama iš bet kur.

Sudarant tinklo modelį, naudojamos 10 megabitų per sekundę (Mbps) tinklo srauto pralaidumo interneto jungtys. Žinant, kad toks tinklo pralaidumas galimas tik idealiomis sąlygomis, nuspręsta tyrimą atlikti, kuomet realus tinklo jungčių pralaidumas yra 8 Mbps. DoS atakos metu yra siunčiamas didelis paketų kiekis, o paketų dydis taip pat yra itin didelis. Kadangi DoS ataka yra laikomas tinklo srauto padidėjimas per trumpą laiko tarpą, stengiantis išnaudoti visą galimą tinklo pralaidumą, tam kad galima būtų teigti, jog tinkle yra vykdoma DoS ataka, gaunamas tinklo srauto dydis turėtų būti nemažesnis, nei 90% maksimalaus galimo tinklo jungčių pralaidumo dydžio. Teigiant, kad sukurto tinklo modeliu realus tinklo pralaidumas yra 8 Mbps, tuomet DoS ataka galima laikyti tinklo srauto dydį, ne mažesnį nei 7,2 megabitai.

### 2.2.1. Vietinio tinklo modelis

Patalpų apsaugos sistemos tinklo modelis yra sudaromas modeliuojant virtualų tinklą. Visų pirma, yra sudaromas modelis, kuomet tinklas yra vietinis (lokalus), ir jame egzistuoja ne daugiau nei viena patalpų apsaugos sistema.


**2.2 pav. Vietinio tinklo modelis**

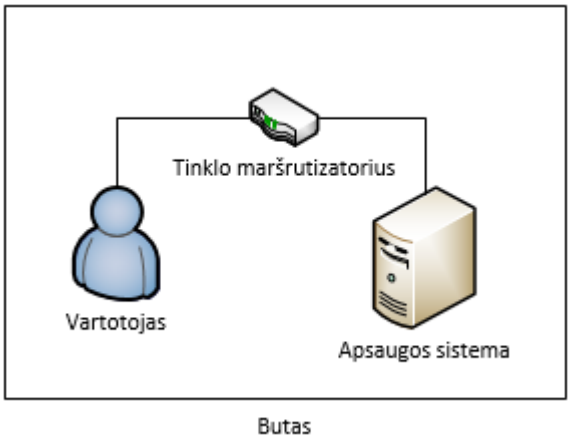
Vietinio tinklo modelyje egzistuoja tik viena apsaugos sistema ir namuose esantis tinklo maršrutizatorius, prie kurio prijungta patalpų apsaugos sistema. Patalpų apsaugos sistema nėra prijungta prie išorinio interneto tinklo ir yra pasiekiama, tik kuomet vartotojas yra prisijungęs prie to paties vietinio tinklo.

### 2.2.2. Apjungto bendro tinklo modelis

Norint ištirti, kaip elgsis viena sistema, ar visas sistemų tinklas, yra modeliuojamas ir imituojamas didelis tarpmiestinis tinklas, kuriame yra daugiau nei viena apsaugos sistema, bei visos apsaugos sistemos yra sujungtos bendrame interneto tinkle.

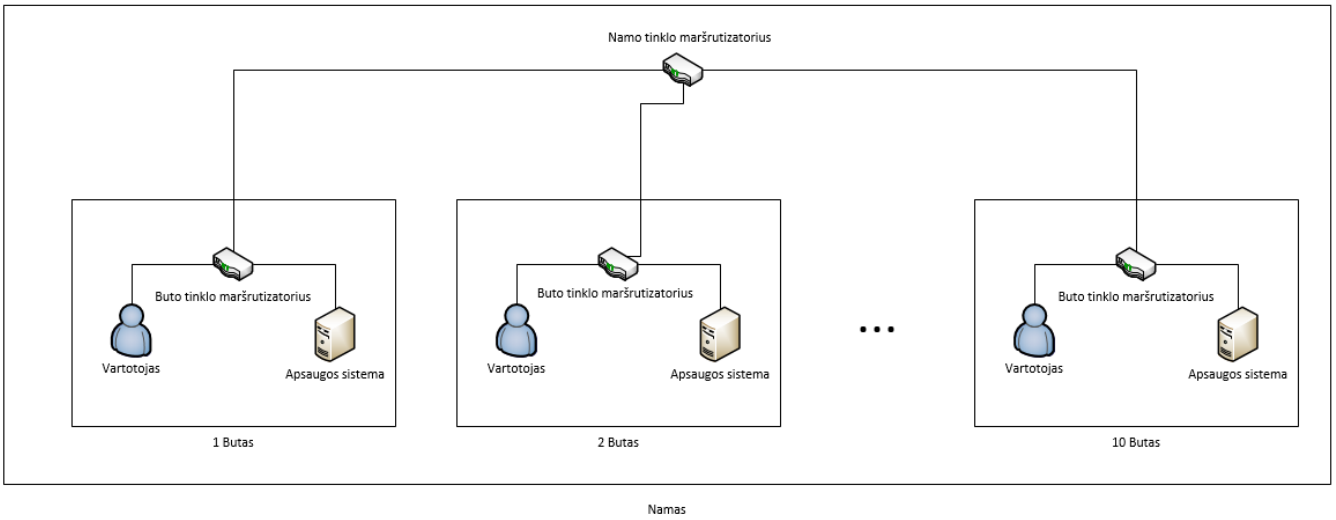
Tokiu būdu, yra modeliuojamas patalpų apsaugos sistemų tinklas, kuriame yra gyvenamieji namai, gyvenamųjų namų rajonai ir miestai. Modeliui tirti, buvo sugalvotas dviejų miestų tinklas, kuriame kiekviename mieste yra penki rajonai, kuriuose yra po 10 gyvenamųjų namų. Kiekviename gyvenamajame name yra po dešimt apsaugos sistemų. Visos sistemos, panaudojant tinklo maršrutizatorius yra sujungtos į vientisą tinklą ir bet kurią apsaugos sistemą galima pasiekti iš bet kur.

Name esančiame bute patalpų apsaugos sistema yra pajungta tokiu pat principu, kaip ir vietinio tinklo modelyje. Žemiau pateikiamame paveikslėlyje yra pavaizduota principinė bute esančios patalpų apsaugos sistemos schema.



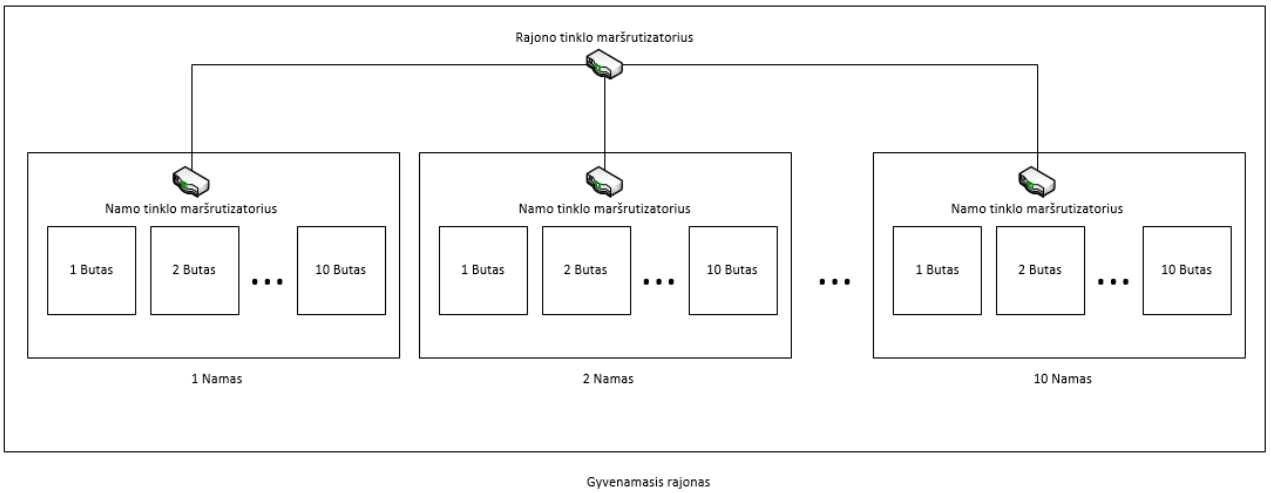

**2.3 pav. Tarpmiestinio tinklo modelio bute esančios patalpų apsaugos sistemos tinklo schema**

Tokių butų, kuriuose yra įrengtos patalpos apsaugos sistemos yra dešimt. Visų patalpų apsaugos sistemų tinklo maršrutizatoriai yra prijungti prie išorinio tinklo maršrutizatoriaus, kuris sudaro bendrą namo patalpų apsaugos sistemų tinklą. Šio tinklo schema yra vaizduojama žemiau.



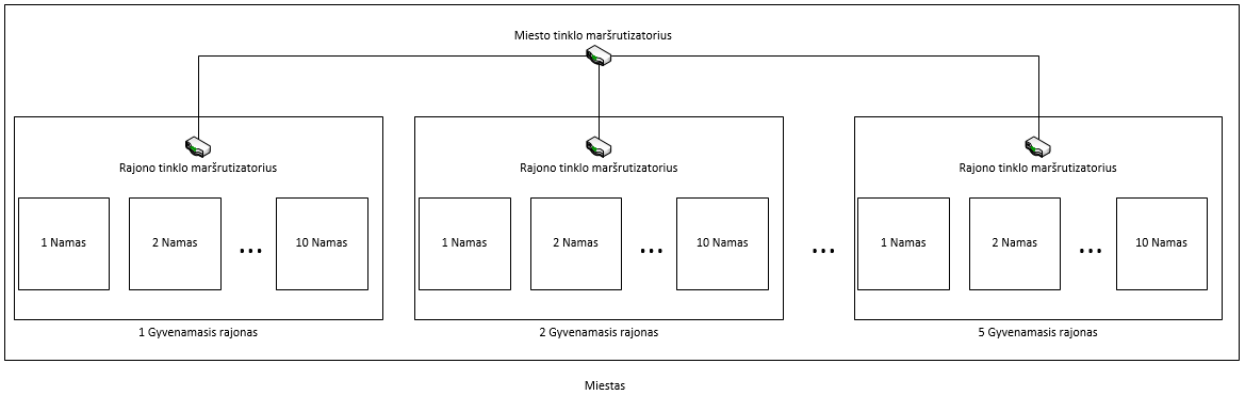

**2.4 pav. Bendrojo namo patalpų apsaugos sistemų tinklo schema**

Kadangi kiekviename rajone yra dešimt namų, su įrengtomis patalpų apsaugos sistemomis, kiekvieno namo tinklo maršrutizatorius yra jungiamas į mesto rajono tinklo maršrutizatorių. Tokiu būdu visos patalpų apsaugos sistemos yra apjungiamos į didesnį bendrą – rajono tinklą.



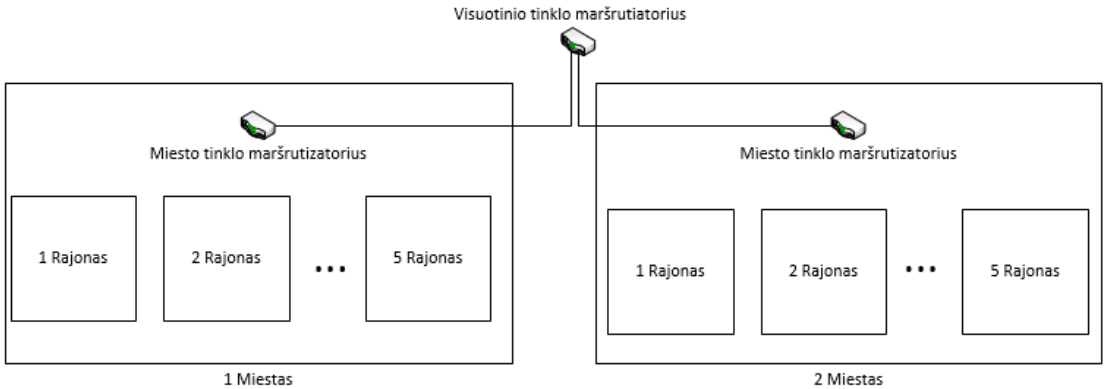

**2.5 pav. Tarpmiestinio tinklo modelio rajono tinklo schema**

Kadangi mieste yra daugiau nei vienas rajonas, tiksliau mieste yra penki rajonai, tai kiekvieno rajono tinklo maršrutizatorius yra sujungtas vienas su kitu, kad sukurti bendrą miesto interneto tinklą, kuriame yra sujungtos visos mieste įdiegtos patalpų apsaugos sistemos ir jų vartotojai galėtų jomis naudotis.




**2.6 pav. Tarpmiestinio tinklo modelio miesto tinklo schema**

Apjungtas bendrasis tinklas yra sudarytas iš dviejų miestų, kuriuose yra po penkis rajonus, todėl aukščiausio lygio tinklo modelio schema atrodo taip, kaip pavaizduota žemiau esančiame paveikslėlyje.




**2.7 pav. Bendroji tarpmiestinio tinklo modelio schema**

Miestai yra prijungti prie visuotinio tinklo maršrutizatoriaus, kuris leidžia vartotojui savo apsaugos sistemą valdyti, stebėti ir pasiekti iš bet kurio pasaulio kampelio turint interneto prieigą.

# 3. PATALPŲ APSAUGOS SISTEMOS TINKLO MODELIO SUDARYMAS IR TYRIMAS

## 3.1. Modelio struktūra

Tyrimo modelis sudarinėjamas panaudojant „Riverbed Modeler“ programinės įrangos 17.5 versiją. 1 priede yra vaizduojama patalpų apsaugos sistemos, esančios ir atakuojamos vietiniame tinkle, sumodeliuota struktūra, remiantis 2 skyriuje sudarytu modeliavimo metodu, kuomet tiek patalpų apsaugos sistema, tiek jos vartotojas, tiek atakuojantis asmuo yra tame pačiame tinkle. 2 Priede yra vaizduojama aukščiausio patalpų apsaugos sistemos tinklo lygmens modelio schema, kuomet atakuojama sistema yra bendrajame tarpmiestiniame tinkle, kuriame taip pat veikia ir kitos patalpos apsaugos sistemos. Kuriant šiuos modelius, visi elementai, kurie buvo panaudoti modelyje, yra „Riverbed Modeler“ duomenų bazėje. Modeliams kurti panaudoti elementai:

*Profiliai ir programos* – siekiant sukurti kuo tikroviškesnį tinklo naudojimo modelį yra panaudoti įvairūs profiliai ir programos. Programų modelyje yra aprašomi tinklo panaudojimai – kokio tipo tinklo srautas yra naudojamas. Nustatymuose galima pasirinkti vieną iš šių tinklo panaudojimo tipų – FTP, HTTP, VoIP, Database ir Email. Atitinkamas tipas įtakoja kokio dydžio tinklo srautas bus naudojamas, bei kaip tai apkraus visą tinklą.

*Vidiniai tinklai* – vidiniai tinklai yra naudojami tarpmiestinio tinklo modelyje. Vidiniai tinklai turi patalpintus įrenginius, bei tinklo vartotojus, kurie naudojasi interneto ryšiu, kad galėtų valdyti savo patalpų apsaugos sistemą. 2 priede esančioje sumodeliuotoje sistemoje vidiniai miesto tinklai yra pažymėti „Miestas_1“ ir „Miestas_2“

*IP paketų nustatymai* – IP paketų nustatymai yra skirti paketų, kurie bus siunčiami atliekant atakas nustatymų pakeitimui. Šiame elemente galima nustatyti elemento dydį, laiko tarpą tarp sėkmingo paketų išsiuntimo, bei laiko tarpą, po kiek laiko paketas yra pripažįstamas kaip pamestas, jeigu nesulaukiama atsakymo.

## 3.2. Patalpų apsaugos sistemos vietinio tinklo modelio tyrimas

Žemiau esančioje lentelėje yra surašyti visi elementai, naudojami sukurti vietinį patalpų apsaugos sistemos modelį, elementų skaičius modelyje, bei elemento pavadinimas „Riverbed Modeler“.

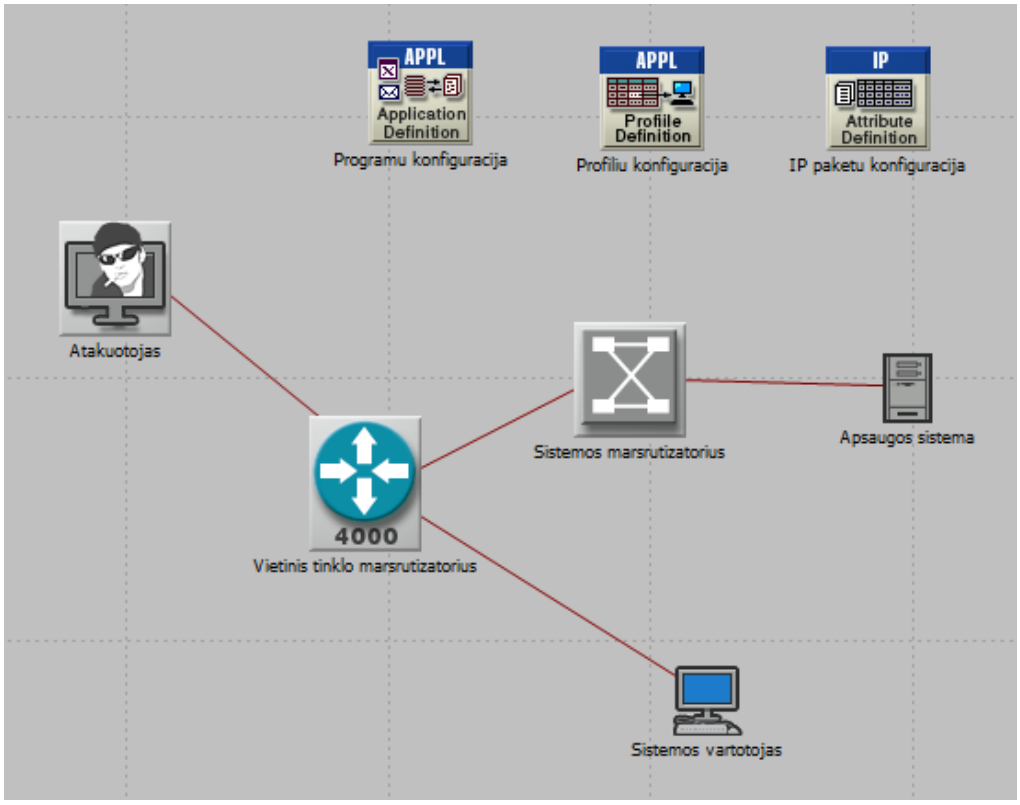
**1 lentelė. Patalpų apsaugos sistemos vietinio tinklo modelyje esantys elementai**

| **Elemento tipas** | **Elementų kiekis modelyje** | **Elemento pavadinimas** |
|---|---|---|
| Tinklo maršrutizatorius | 1 | CS_4000_3s_e6_fr2_sl2_tr2 |
| Apsaugos sistemos tinklo maršrutizatorius | 1 | Ethernet16_switch |
| Vartotojas | 1 | Ethernet_wkstn |
| Atakuotojas | 1 | Ethernet_server |
| Apsaugos sistema | 1 | Ethernet_server |
| Programų modelis | 1 | Application configuration |
| Profilių modelis | 1 | Profile configuration |
| IP paketų modelis | 1 | IP configuration |
| Jungtys | 4 | 10BaseT |

Modelis sudaromas pasinaudojant interneto tinklo veikimo principais. Sumodeliuotas tinklas, turi sudaryti galimybę tinkamai ištirti DoS atakos poveikį patalpų apsaugos sistemos pasiekiamumui, bei padėti priimti tinkamus sprendimus, siūlant saugos sprendimą apsaugoti sistemą nuo šio tipo atakų.

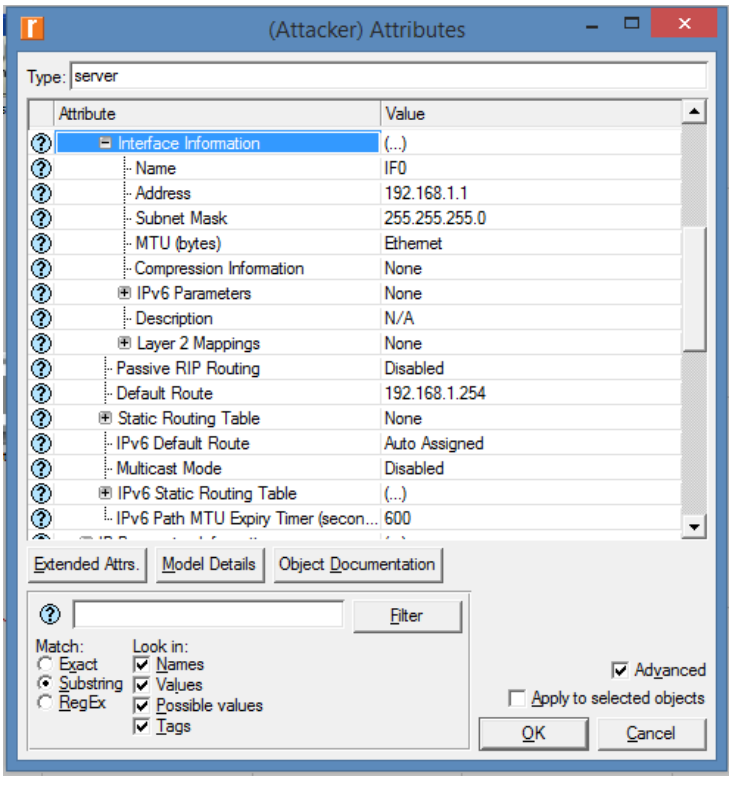
Realizuojant tinklo modelį „Riverbed Modeler“ programoje, panaudota IPv4 tipo adresacija, bei sukurtas tinklas, kuriame kiekvienas elementas turi statinius IP adresus.

Pirmasis žingsnis modeliuojant vietinį tinklą, kuriame veikia patalpų apsaugos sistema – modelio elementų išdėstymas ir sujungimas interneto jungtimis.




**3.1 pav. Patalpų apsaugos sistemos vietinio tinklo modelis su atakuojančiu asmenimis**

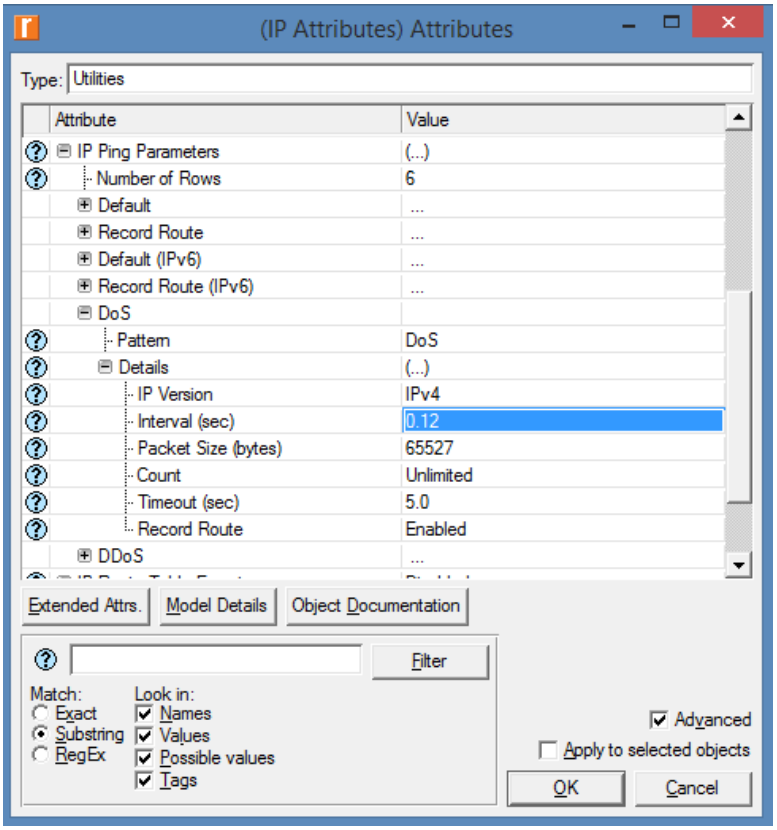
Sujungus tinkle esančius elementus, priskiriami IP adresai kiekvienam elementui, bei sukuriami maršrutizavimo maršrutai, kad paketai ir tinklo srautas veiktų tinkamai. Kad tai pasiekti, atakuojančio asmens, sistemos vartotojo, bei apsaugos sistemos elementams priskirti statiniai IP adresai, bei artimiausio elemento IP adresai. Vieno iš elementų IP adreso ir jam artimiausio elemento IP adreso nustatymai yra vaizduojami žemiau esančiame pav.




**3.2 pav. IP adresų priskyrimo konfigūracijos langas**

Siekiant turėti kuo tikroviškesnį tinklo apkrovimą atakos metu, yra sukuriamas profilis, bei programos nustatymai patalpų apsaugos sistemos vartotojui. Kadangi vartotojas naudojasi šiame tinkle esančia patalpų apsaugos sistema – valdo būsenas, peržiūri istoriją, keičia saugos zonas ir pan., jo darbas su sistema vyksta HTTP protokolais. Todėl, profilio ir programos nustatymai yra sumodeliuojami taip, kad tinklo apkrova būtų tokio at dydžio, kaip naršant internete.

Paskutinis žingsnis prieš atliekant tyrimą - IP paketų konfigūracijos nustatymas panaudojant IP paketų nustatymo elementą. IP paketų konfigūracijos duomenys yra matomi žemiau esančiame paveiksle.

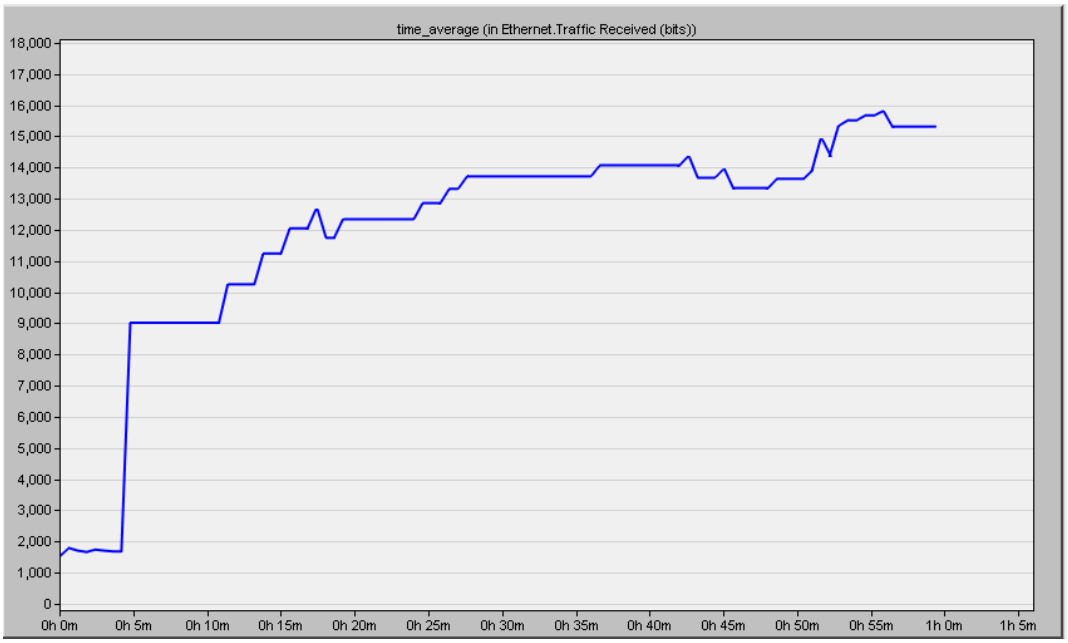



**3.3 pav. IP paketų DoS atakoms konfigūracija**

Šiame modelio elemente yra nustatoma, kad atakuojančio asmens leidžiami paketai būtų itin didelio dydžio (maksimalus leidžiamas dydis – 65527 baitai), bei laikas tarp paketų siuntimo yra itin mažas. Modelyje panaudoti 65527 baitų paketai yra leidžiami kas 0,12s, kas prognozuojant turėtų sudaryti apie 7,8 megabitų srauto dydį.

### 3.2.1. Patalpų apsaugos sistemos vietinio tinklo modelio rezultatai

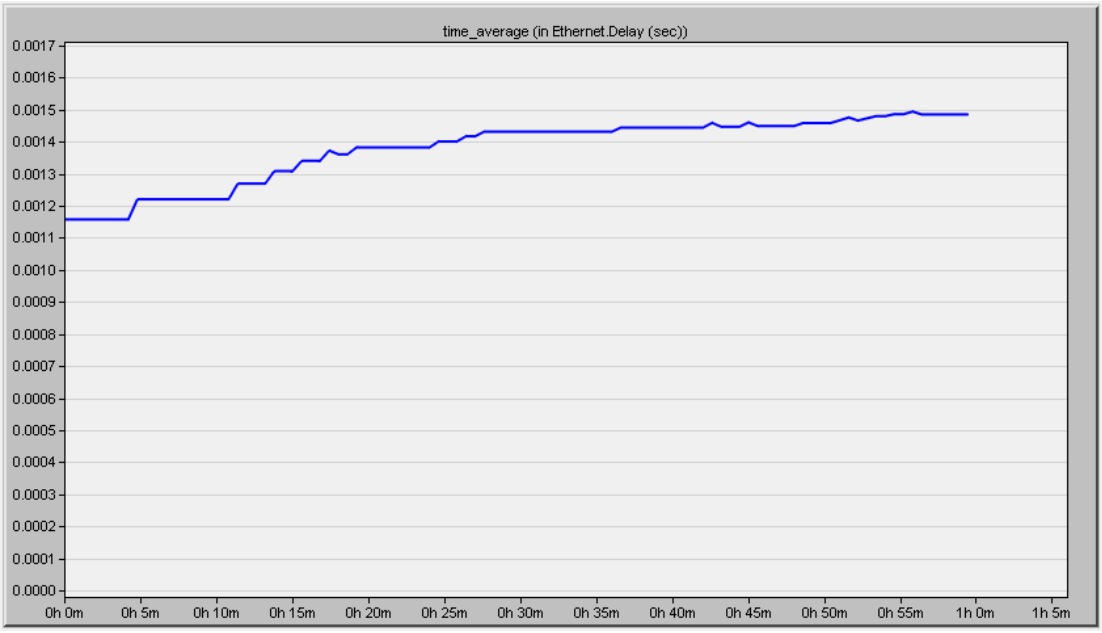
Norint ištirti, kaip DoS ataka veikia patalpų apsaugos sistemos pasiekiamumą vietiniame tinkle, reikia atlikti du tyrimus. Pirmasis tyrimas atliekamas, kuomet sistema veikia įprastu režimu. Šiame tyrime atakuojančio asmens nėra, o sistemos vartotojas valdo sistemą kaip įprastai. Tiriant yra nustatomas vidutinis sistemos atsako laikas, bei vidutinis sistemos gaunamo tinklo srauto dydis. Tyrimo trukmė yra 1 valanda.




**3.4 pav. Vidutinis sistemos tinklo srauto dydis vietiniame tinkle nevykstant atakai**

Atlikus tyrimą, kuomet patalpų apsaugos sistema yra vietiniame tinkle, bei kuomet vartotojas tiesiog naudojasi ir valdo apsaugos sistemą, buvo nustatytas vidutinis per modelio simuliacijos rezultatams gauti duotą laiką sistemos gautas tinklo srauto dydis. Pirmosios 5 minutės buvo nustatytos kaip apšilimo fazė, kuomet nevykdomi jokie veiksmai tinkle – tai apšilimo fazė, kuomet visa sistema yra ramybės būsenoje ir tinklo srautas susideda tik iš tarnybiniais protokolais keliaujančių paketų, skirtų užmegzti jungtims tarp sistemos komponentų – vartotojo kompiuterio, apsaugos sistemos, bei tinklo maršrutizatoriaus. Toliau, praėjus penkioms tyrimo minutėms, vartotojas pradeda naudotis apsaugos sistema - t. y., atlieka įvairius veiksmus, tokius kaip sistemos zonų perskirstymas, įvykių istorijos peržiūra, prisijungimas, atsijungimas nuo sistemos ir kiti veiksmai. Kiekvienas kreipimasis į patalpų apsaugos sistemą, kuria tinklo paketus, bei kuria tinklo srautą. Kaip matyti iš 3.3 paveikslo, tinklo srautas yra suminis ir nuolat pamažu didėja, kadangi vartotojas vis naudojasi sistemos funkcijomis. Kai vartotojas nesiunčia informacijos į sistemą (pavyzdžiui skaito įvykių istoriją, kuri interneto naršyklėje yra užkrauta ir statinė informacija), tuo momentu vidutinis tinklo srauto dydis sumažėja. Iš šio paveikslo taip pat galima spręsti, jog tinklas neturi neįprasto apkrovimo, kadangi vidutinis tinklo srauto dydis, kurį gauna sistema, didėja nedideliais kiekiais ir tolygiai.

3.5 paveiksle yra vaizduojamas vidutinis atsako vėlavimo iš patalpų apsaugos sistemos laikas.

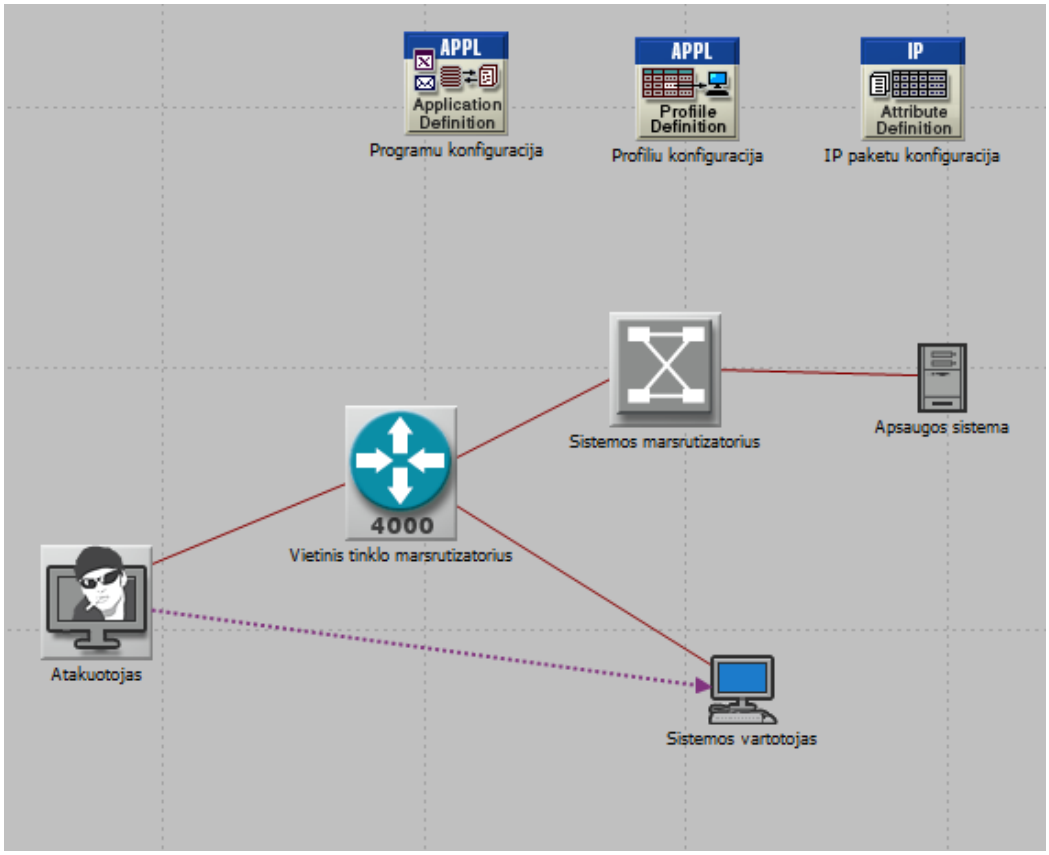



**3.5 pav. Vidutinis patalpų apsaugos sistemos užklausos atsako vėlavimo laikas, kai nevykdoma ataka**

Analizuojant vidutinį tinklo atsako vėlavimo grafiką, kuomet patalpų apsaugos sistema nėra atakuojama ir veikia tik vietiniame tinkle, yra pastebimas nežymus vėlavimo padidėjimas bėgant laikui, tačiau jis padidėja dėl to, jog vartotojas pradeda naudotis patalpų apsaugos sistema. Atsako vėlavimo laikas yra toks nežymus, kad galima teigti, jog sistema į siunčiamus užklausų paketus, bei valdymo komandas atsako iškart.

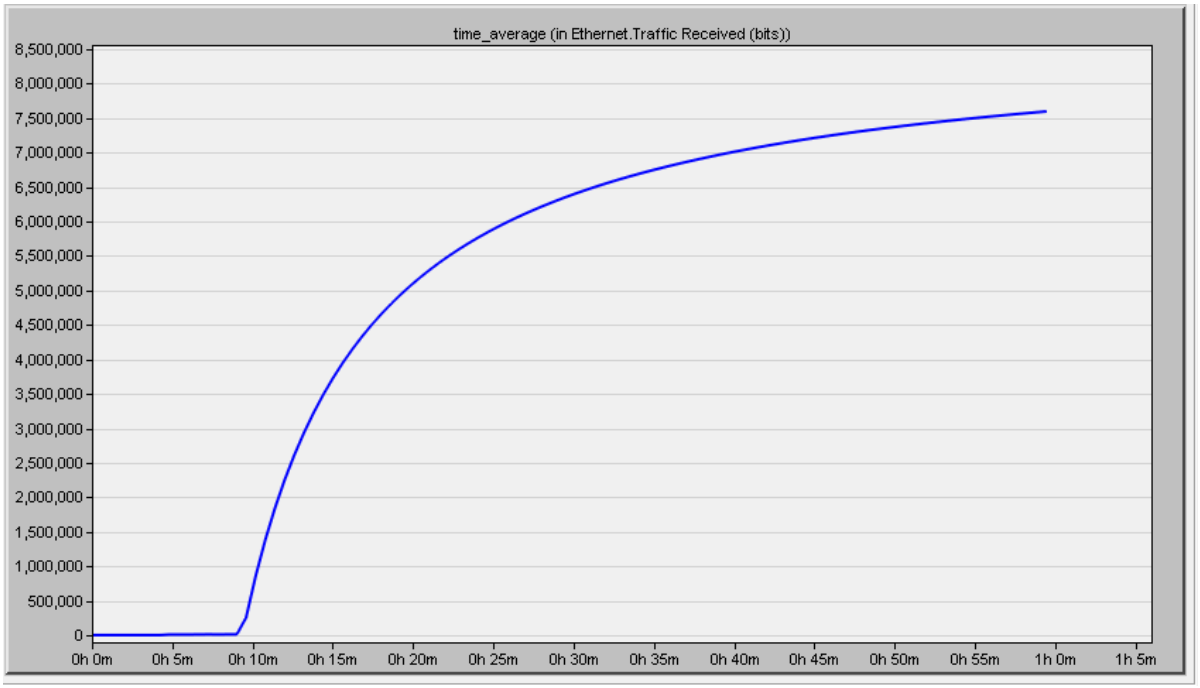
Atlikus tinklo tyrimą vadinamojoje ramybės būsenoje, į patalpų apsaugos sistemos vietinio tinklo modelį prijungiamas atakuojančio asmens kompiuteris, bei pasiruošiama antrajam patalpų apsaugos tinklo modelio, kuomet sistema yra pajungta vietiniame tinkle, tyrimui. Šio tyrimo metu siekiama nustatyti kaip paveikiamas patalpų apsaugos sistemos pasiekiamumas vartotojui, kuomet yra vykdoma DoS ataka.

Antrojo tyrimo metu, inicijuojama atakuojančio asmens ataka, nukreipta į patalpų apsaugos sistemą. Sistemai nuolat siunčiami dideli paketai, bei stebimas patalpų apsaugos sistemos vidutinis atsako vėlavimo laikas, bei vidutinis sistemos gaunamo tinklo srauto dydis. Tinklo paketų srautas, siunčiamas atakos metu yra vaizduojamas punktyrine rodykle, bei žemiau pateiktame paveiksle aiškiai nurodo iš kurio komponento į kurį DoS atakos paketų srautas keliauja.



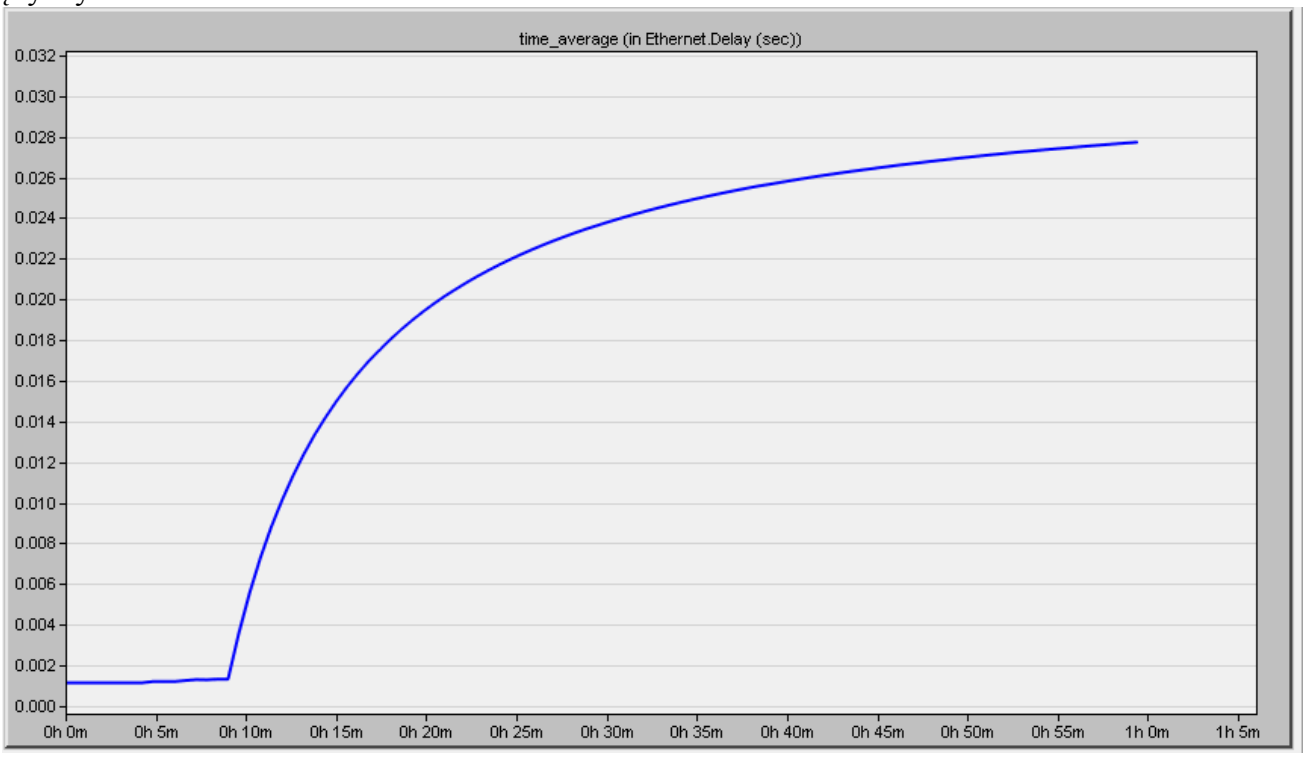

**3.6 pav. Patalpų apsaugos sistemos vietinio tinko modelis su inicijuota DoS ataka**

Kad tyrimo rezultatus būtų galima palyginti vienus su kitais, antrasis tyrimas taip pat yra vykdomas 1 valandą. Taip pat, siekiant tyrimą padaryti objektyvesniu, bei nustatyti kaip pasikeičia patalpų apsaugos sistemos pasiekiamumas, nuspręsta, kad DoS ataka bus pradėta vykdyti tik nuo dešimtos minutės. Kad aiškiau suprasti tinklo srauto kiekį, reikėtų prisiminti, kad pirmosios penkios minutės yra apšilimo fazė, kuomet nėra atliekami jokie veiksmai nei iš vartotojo nei iš atakuotojo pusės, o tinklo srautas susidaro tik iš tarnybinių protokolų siunčiamų ir gaunamų paketų tarp tinklo komponentų. Nuo penktosios minutės iki pat tyrimo pabaigos vartotojas naudojasi sistema. Kaip aprašyta aukščiau, tai sugeneruoja ne itin didelį tinklo srautą, kurio vidutinis dydis pasibaigus tyrimui yra apie 15500 bitų. Nuo dešimtosios minutės atakuojantis asmuo pradeda naudoti DoS ataką, nukreiptą prieš patalpų apsaugos sistemą, siekiant sutrikdyti jos darbą ir padaryti ją neprieinamą.




**3.7 pav. Vidutinis sistemos tinklo srauto dydis vietiniame tinkle vykdant DoS ataką**

Kaip matoma 3.7 paveiksle, pagal sumodeliuotą y ašies dydį, pirmosios penkios minutės (apšilimo fazė) yra beveik lygios nuliui bitų. Vartotojui pradėjus naudotis patalpų apsaugos sistema – atlikinėti įprastinius veiksmus, vidutinis tinklo srauto dydis, kurį gauna patalpų apsaugos sistema šiek tiek padidėja. Į tinklą įsilaužus atakuojančiam asmeniui, kuris siekia sutrikdyti apsaugos sistemos darbą, vidutinis tinklo srautas, kurį gauna apsaugos sistema, pradeda didėti dideliu tempu. Vidutinio tinklo srauto, kurį gavo patalpų apsaugos sistema, dydis viso tyrimo metu nuolat auga iki kol tampa didesnis nei 7,5 megabitų. Remiantis sukurtu metodu, kuomet tinklo srauto dydis, kurį gauna patalpų apsaugos sistema viršija nustatytą ribą – 7,2 megabitus, galima teigti, jog tinkle iš tikrųjų buvo įvykdyta DoS ataka.




**3.8 pav. Vidutinis patalpų apsaugos sistemos užklausos atsako vėlavimo laikas, vykdant DoS ataką**

Analizuojant patalpų apsaugos sistemos atsako vėlavimo, kuomet vykdoma DoS ataka, laiką, pastebėta, kad ši kreivė yra labai panaši į vidutinio tinklo srauto dydžio, kurį gavo patalpų apsaugos

sistema, grafiko kreivę. 3.8 paveiksle yra matoma, kad kaip ir 3.7 paveiksle, vėlavimo atsako laikas yra itin mažas, tačiau į tinklą patekus atakuojančiam asmeniui ir jam inicijavus DoS ataką panaudojant ICMP ping paketus, vėlavimo laikas pradeda drastiškai augti ir auga iki pat tyrimo pabaigos.

Antrojo tyrimo metu pastebėta, kad dėl tinkle įvykdytos atakos, užklausos atsako vėlinimo laikas padidėja beveik 20 kartų.

### 3.3. Tarpmiestinio patalpų apsaugos sistemos tinklo modelio tyrimas

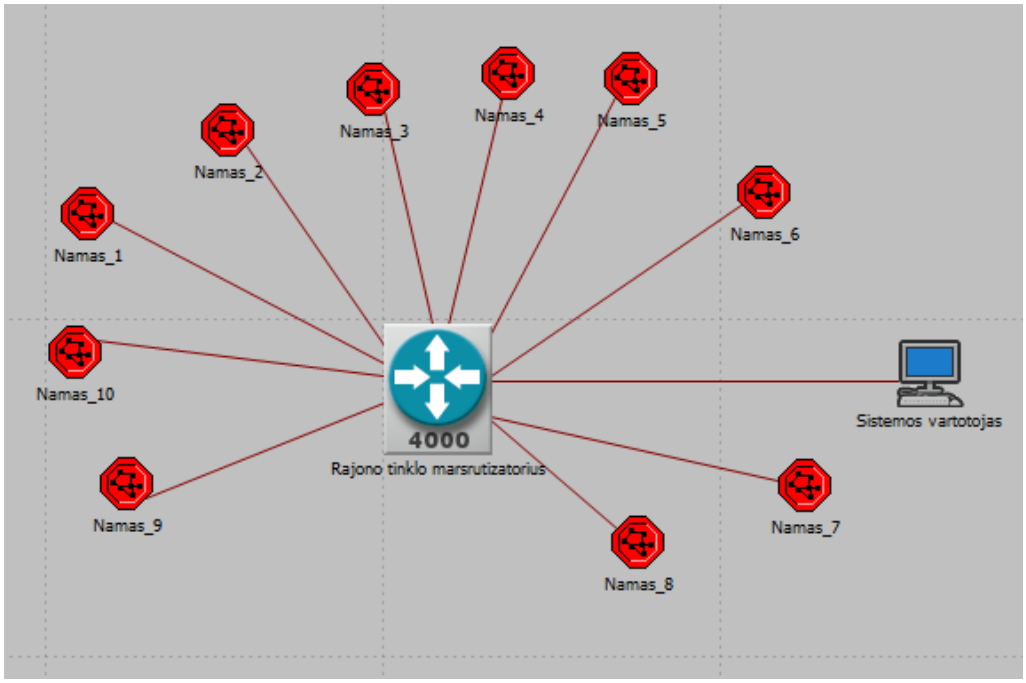
Sudarytoje lentelėje, kuri yra pateikta žemiau, yra surašyti visi komponentai, kurie panaudoti sudarant patalpų apsaugos sistemų tinklo modelį, kai yra modeliuojamas tarpmiestinis bendras patalpų apsaugos sistemų tinklas.

**2 lentelė. Patalpų apsaugos sistemos tarpmiestinio tinklo modelyje esantys elementai**

| **Elemento tipas** | **Elementų kiekis modelyje** | **Elemento pavadinimas** |
|---|---|---|
| Tinklo maršrutizatorius | 1112 | CS_4000_3s_e6_fr2_sl2_tr2 |
| Apsaugos sistemos tinklo maršrutizatorius | 1000 | Ethernet16_switch |
| Vartotojas | 10 | Ethernet_wkstn |
| Atakuotojas | 1 | Ethernet_server |
| Apsaugos sistema | 1000 | Ethernet_server |
| Programų modelis | 1 | Application configuration |
| Profilių modelis | 1 | Profile configuration |
| IP paketų modelis | 1 | IP configuration |
| Jungtys | 2111 | 10BaseT |
| Vidinis tinklas | 1100 | Subnet |

Sprendžiant iš elementų kiekio, tinklo modelis yra itin didelio masto. Kad atspindėti kuo realistiškesnį tinklo modelį ir tinklo srautus, nuspręsta tinkle prijungti dešimt įprastinių tinklo vartotojų, kurie naudojasi savo interneto sistemomis. 2 priede yra parodytas tik vienas tinklo vartotojas aukščiausiame tinklo modelio lygmenyje, tam kad būtų galima suprasti kaip tinklas atrodo šalies mastu. Kiti patalpų apsaugos sistemų vartotojai yra prisijungę prie tinklo žemesniuose lygmenyse ir statiškai prijungti prie jiems paskirtų patalpų apsaugos sistemų, kas realybėje atitiktų tai, jog kiekvienas vartotojas gali prisijungti tik prie savo patalpų apsaugos sistemos ir ją valdyti.

Patalpų apsaugos sistemų tarpmiestiniame tinkle esantys prisijungę vartotojai yra pavaizduoti skirtinguose lygmenyse, vaizduojant jų esamą vietą, kuomet naudojamasi savo patalpų apsaugos sistema. Pavyzdžiui, vartotojo komponentas pavaizduotas rajono lygmenyje, reiškia, kad vartotojas yra šiuo metu tam tikrame rajone – gatvėje, kavinėje ir pan. Aukščiausiame lygmenyje pavaizduotas vartotojas sistema naudojasi būdamas kitame mieste ar kitoje šalyje. Vaizdas, kaip atrodo miesto rajone esantis ir savo sistemą valdantis vartotojas, pateiktas 3.9 paveiksle.



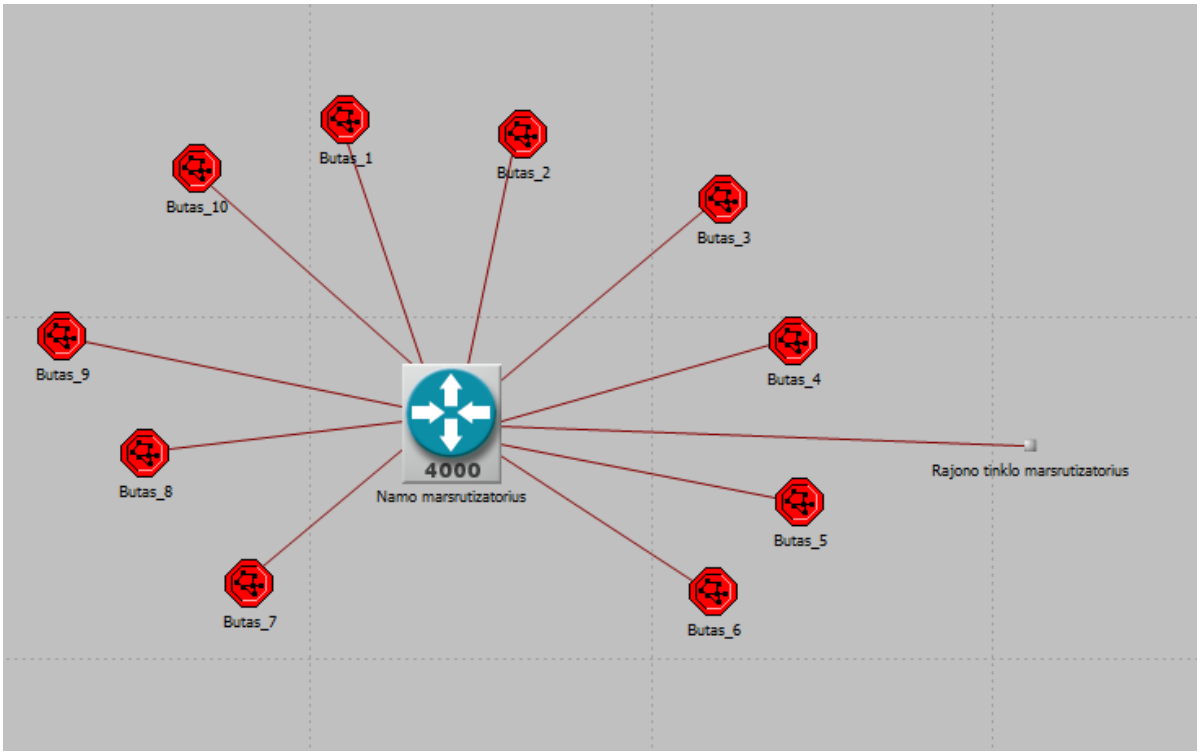

**3.9 pav. Tinklo vartotojo prisijungimas prie patalpų apsaugos sistemos esant mieste**

Žemiausias tinklo lygmuo savo struktūra yra panašus į pavaizduotą 1 priede (tik be atakuojančio asmens ir sistemos vartotojo. 3.10 paveiksle yra pavaizduota kaip tiksliai atrodo žemiausio patalpų apsaugos sistemos tarpmiestinio tinklo modelio lygmens struktūra.


**3.10 pav. Žemiausio lygmens tarpmiestinio patalpų apsaugos sistemos tinklo modelio struktūra**

Kaip matoma aukščiau pateiktame paveiksle, vietinis tinklo maršrutizatorius yra prijungtas prie namo maršrutizatoriaus, tam kad patalpų apsaugos sistema galėtų būti pasiekiama prisijungus prie aukštesniame lygyje esančio maršrutizatoriaus – esant bet namo bute.

Aukštesnysis tinklo topologijos lygis sukurtame tarpmiestinio tinklo modelyje – namo lygis. Šiame lygyje yra panaudota žvaigždės tipo tinklo topologija, kuomet kiekvieno buto vidinio tinklo maršrutizatoriai yra prijungti prie bendro tinklo maršrutizatoriaus. Šio lygio modelis pateiktas žemiau esančiame paveiksle.




**3.11 pav. Namo lygmens tarpmiestinio patalpų apsaugos sistemos tinklo modelio struktūra**

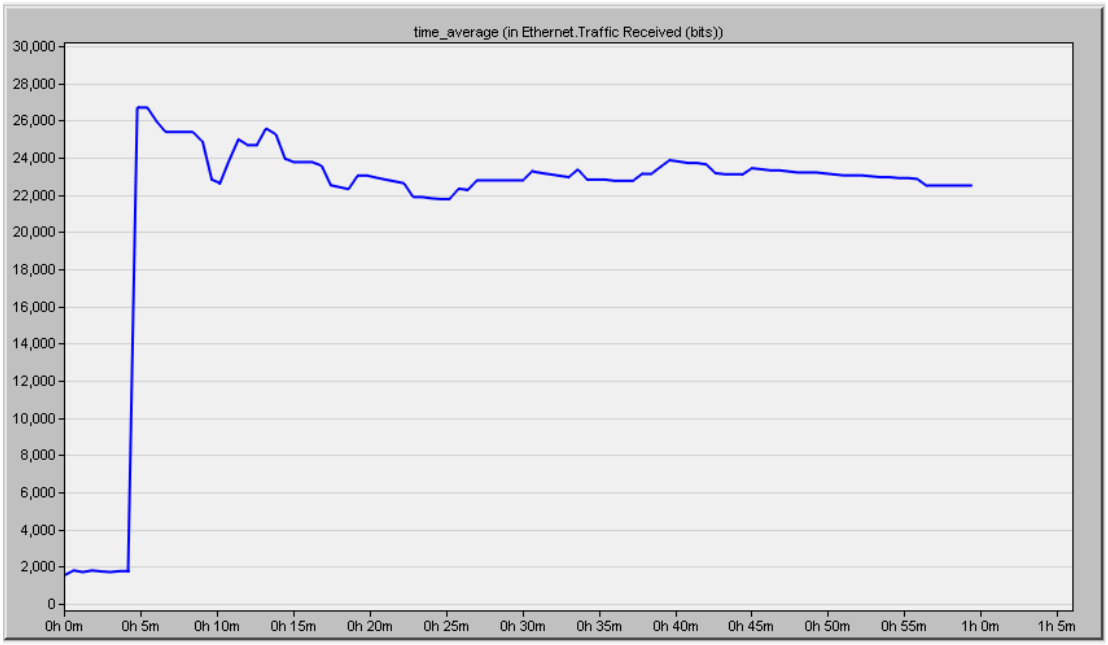
Kadangi tinklo modelyje yra daugiau nei vienas namas rajone, o vartotojas turi turėti galimybę pasinaudoti patalpų apsaugos sistema būnant bet kur, prisijungus prie šio tinklo, visi rajono namai yra sujungiami tokiu pačiu – žvaigždės tinklo topologijos principu į bendrą rajono patalpų apsaugos sistemų tinklą. Aukštesniajame – vieno rajono tinklo lygmenyje, modeliuojant tarpmiestinį apsaugos sistemų tinklą, visi namai yra prijungti prie vieno tinklo maršrutizatoriaus, o tinklo vaizdas yra identiškas namo tinklo lygmens vaizdui - t. y., dešimt namų prijungti prie bendro rajono tinklo maršrutizatoriaus. Kadangi mieste yra penki rajonai, visi rajonų tinklo maršrutizatoriai, aukštesniame – miesto lygmenyje, yra prijungiami prie bendro miesto tinklo maršrutizatoriaus. Tokiu modeliavimo principu yra sumodeliuojamas aukščiausias tarpmiestinio patalpų apsaugos sistemų tinklo modelio lygis, kuriame yra pavaizduoti du miestai, tarpusavyje sujungti panaudojant tinklo maršrutizatorių. Sukurtame tarpmiestinio patalpų apsaugos sistemų tinklo modelyje kiekvienam komponentui priskirtas statinis IP adresas, bei sudarytas statinis tinklo modelis, kurio dėka vartotojai gali prisijungti prie savo patalpų apsaugos sistemos būnant bet kurioje vietoje.

Tinkle naudojami tokie patys IP paketų, profilių, bei programų modeliai, kokie buvo naudojami atliekant tyrimą, esant vienai patalpų apsaugos sistemai, kuri prijungta prie vietinio tinklo.

### 3.3.1. Patalpų apsaugos sistemų tarpmiestinio tinklo modelio rezultatai

Kaip ir tiriant patalpų apsaugos sistemos pasiekiamumą, kai sistema veikia ir yra valdoma tik vietiniame tinkle, atliekami du tyrimai, kad būtų galima nustatyti ir išsiaiškinti kokį poveikį patalpų apsaugos sistemos pasiekiamumui turi inicijuojama DoS ataka.

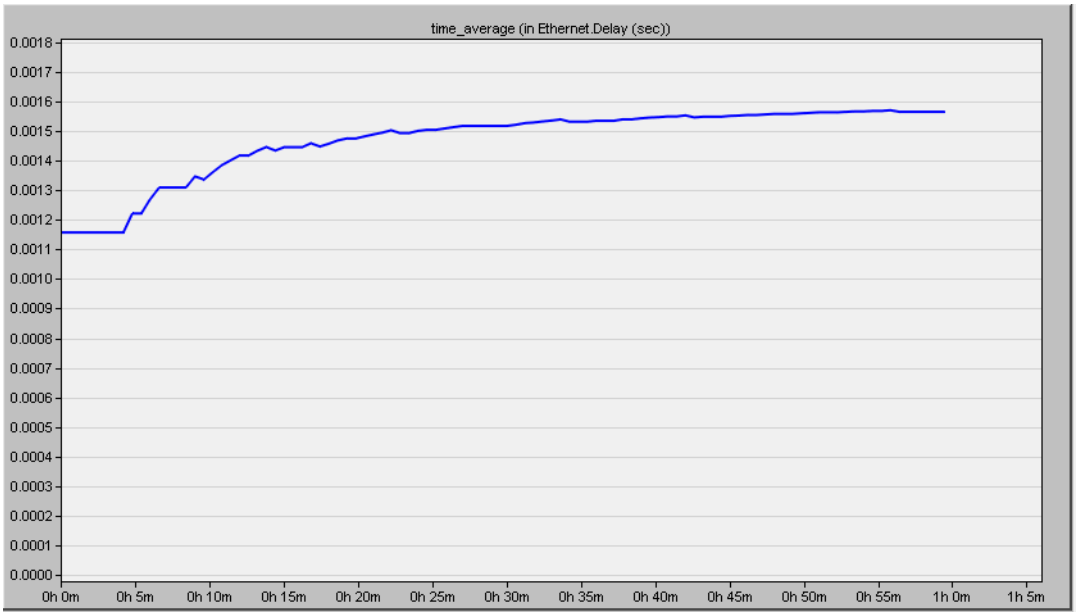
Primojo tyrimo metu, ataka nėra vykdoma. Tyrimas atliekamas siekiant nustatyti, koks yra atsako vėlavimo laikas, bei kokį tinklo srauto dydį priima apsaugos sistema, kuomet tinklu naudojasi daugiau nei vienas vartotojas, tačiau visi jie atlieka įprastines savo patalpų apsaugos sistemų valdymo užduotis. Tyrimo trukmė 1 valanda.




**3.12 pav. Patalpų apsaugos sistemos tarpmiestiniame tinkle vidutinis tinklo srauto dydis nevykstant atakai**

Atlikus tyrimą, kuomet tarpmiestiniame patalpų apsaugos sistemų tinkle vartotojai naudojasi savo patalpų apsaugos sistemomis, buvo stebimi vienos patalpų apsaugos sistemos duomenys. 3.12 paveikslas vaizduoja vidutinį, per modelio tyrimo laiką, patalpų apsaugos sistemos gautą tinklo srauto dydį. Kaip galima pastebėti, pirmosios penkios minutės yra nedidelis tinklo srautas, kadangi yra vykdoma apšilimo fazė, kuomet tinkle nevykdomi jokie veiksmai. Tinklo srauto dydis yra nedidelis, kadangi apsaugos sistema gauna tik tarnybinių protokolų siunčiamus paketus. Nuo penktosios minutės, visi vartotojai pradeda naudotis savo patalpų apsaugos sistemomis esančiomis tinkle. Nuo šio momento gaunamo tinklo srauto dydis padidėja, tačiau viso tyrimo metu kinta nežymiai, atsižvelgiant į tai kad vartotojas naudoja skirtingas funkcijas, vidutinis sistemos gaunamas tinklo srauto dydis yra stabilus. Tačiau, lyginant gautą rezultatą su rezultatu, atlikus identišką tyrimą, kuomet patalpų apsaugos sistema yra prijungta ir veikia tik vietiniame tinkle, galima pastebėti padidėjusį vidutinį tinklo srauto dydį. Tai lemia paketų dydžio pasikeitimas dėl sukurto tinklo modelio, kuriame yra daugiau nei vienas tinklo maršrutizatorius, bei yra nustatyti statiniai tinklo maršrutai. Kuo ilgesnis jungties kelias, apimantis daugiau tinklo maršrutizatorių, tuo didesnius tinklo paketus gauna patalpų apsaugos sistema iš sistemos vartotojo.

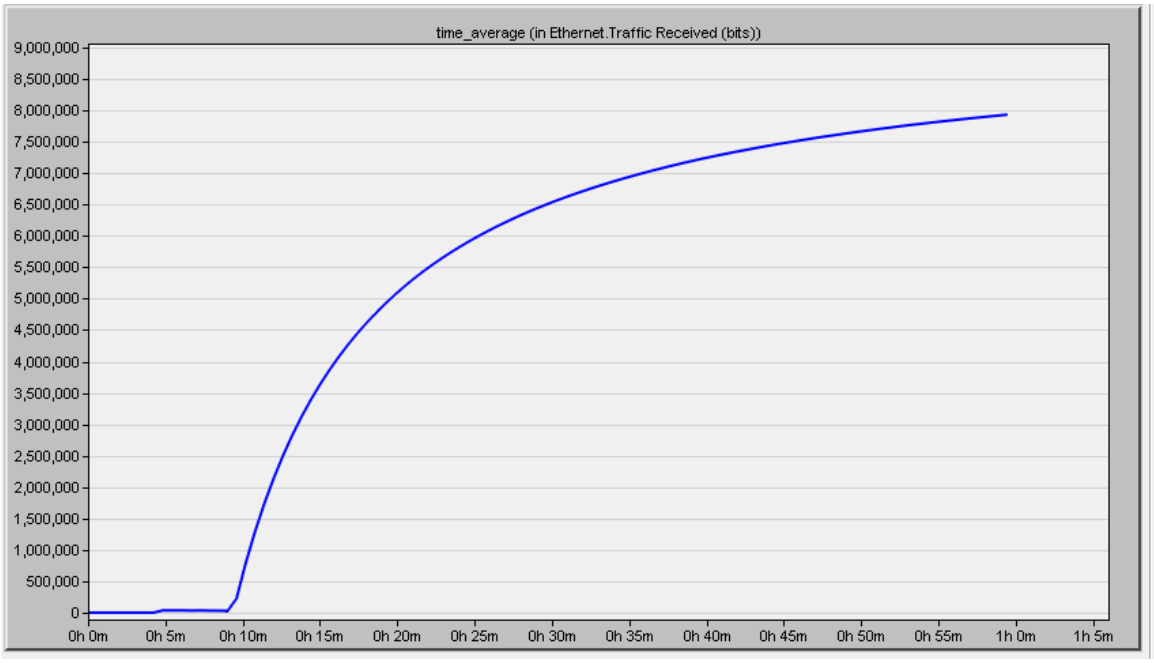
Taip pat šio tyrimo metu buvo nustatytas ir vidutinis patalpų sistemos atsako vėlavimo laikas, kurio grafikas pateiktas žemiau esančiame paveiksle.




**3.13 pav. Patalpų apsaugos sistemos tarpmiestiniame tinkle vidutinis atsako vėlavimo laikas nevykstant atakai**

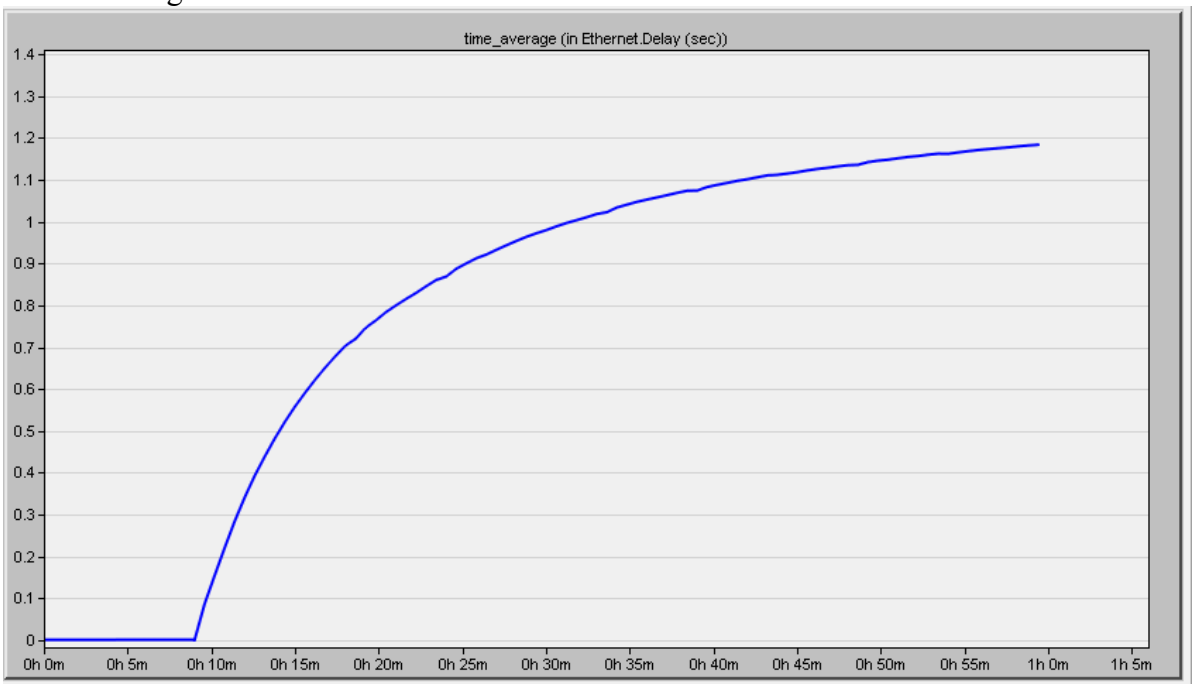
Lyginant vietiniame ir tarpmiestiniame tinklo modeliuose stebimas patalpų apsaugos sistemas, vidutinis tinklo atsako vėlavimo laikas yra labai panašus. Tačiau, patalpų apsaugos sistemų tarpmiestiniame tinklo modelyje stebima patalpų apsaugos sistema į užklausas vėluoja atsakyti šiek tiek ilgiau, ką galima paaiškinti tinklo topologijos išdėstymu, kitų vartotojų buvimu tinkle, bei naudojimusi savo patalpų apsaugos sistemomis. Lyginant pirmojo ir antrojo tinklo modelių patalpų apsaugos sistemų vidutinius atsako vėlavimo laikus, galima teigti, jog vartotojui sistema yra puikiai pasiekiama be jokių trikdžių, bei sistema į vartotojo siunčiamas užklausas atsako iškart.

Antrasis tyrimas atliekamas, kuomet aukščiausiame tinklo modelio lygmenyje yra prijungiamas atakuojantis asmuo, kuris inicijuoja DoS ataką, nukreiptą prieš pasirinktą patalpų apsaugos sistemą. Kaip galima matyti 2 priede, atakuojantis asmuo nėra šio tinklo vartotojas. Jam pavykus įsilaužti į tinklą, bandoma sutrikdyti pasirinktos tinklo apsaugos sistemos pasiekiamumą naudojant DoS ataką. Kad tyrimas būtų objektyvus, antrojo tyrimo trukmė taip pat yra 1 valanda.




**3.14 pav. Patalpų apsaugos sistemos tarpmiestiniame tinkle vidutinis tinklo srauto dydis vykdant DoS ataką**

Atlikus antrąjį tarpmiestinio patalpų apsaugos sistemų tinklo modelio tyrimą, kuomet atakuojantis asmuo atakuoja pasirinktą patalpų apsaugos sistemą panaudodamas DoS ataką, buvo ištirtas patalpų apsaugos sistemos vidutinis gaunamo tinklo srauto dydis. Kaip ir vietinio tinklo modelyje, tarpmiestinio tinklo modelyje yra kelios skirtingos fazės – apšilimo fazė, vartotojų fazė, bei atakos fazė. Pirmosios penkios tyrimo minutės yra apšilimo fazė, kurios metu grafiko kreivė yra itin mažame lygmenyje. Šios fazės metu gaunami tik tarnybinių protokolų paketai. Antroji fazė – nuo penktosios minutės yra vartotojo naudojimasis sistema. Trečioji fazė – DoS atakos inicijavimas ir nenutraukiamas naudojimas iki pat tyrimo pabaigos. Atlikus tyrimą, 3.14 paveiksle galima pastebėti, kad pirmosiomis dešimt tyrimo minučių lyginant su vėlesnėmis tyrimo minutėmis, vidutinis patalpų apsaugos sistemos gaunamas tinklo srauto dydis yra itin mažas. Prasidėjus DoS atakai, vidutinis gaunamas tinklo srauto dydis pradeda drastiškai augti ir tyrimo pabaigoje pasiekia itin didelę reikšmę. Taip pat, lyginant gautą tarpmiestinio patalpų apsaugos sistemų tinklo modelio vidutinio gaunamo tinklo srauto dydžio grafiką, kai yra vykdoma ataka, su vietinio patalpų apsaugos sistemos tinklo modelio vidutinio gaunamo tinklo srauto dydžio, kuomet yra vykdoma ataka grafiku, galima pastebėti, kad grafikų kreivės yra panašios, tačiau gaunamo tinklo srauto dydžiai skiriasi daugeliu kartų. Taip pat, remiantis tyrimo metodu, kuomet tinklo srauto pralaidumas yra 8 megabitai, galima pastebėti, kad patalpų apsaugos sistemų tarpmiestiniame tinklo modelyje vidutinis tinklo srauto dydis tyrimo pabaigoje pasiekia beveik maksimalų pralaidumo dydį, dėl ko galima teigti, kad DoS ataka yra vykdoma sėkmingai.




**3.15 pav. Patalpų apsaugos sistemos tarpmiestiniame tinkle vidutinis atsako vėlavimo laikas vykdant DoS ataką**

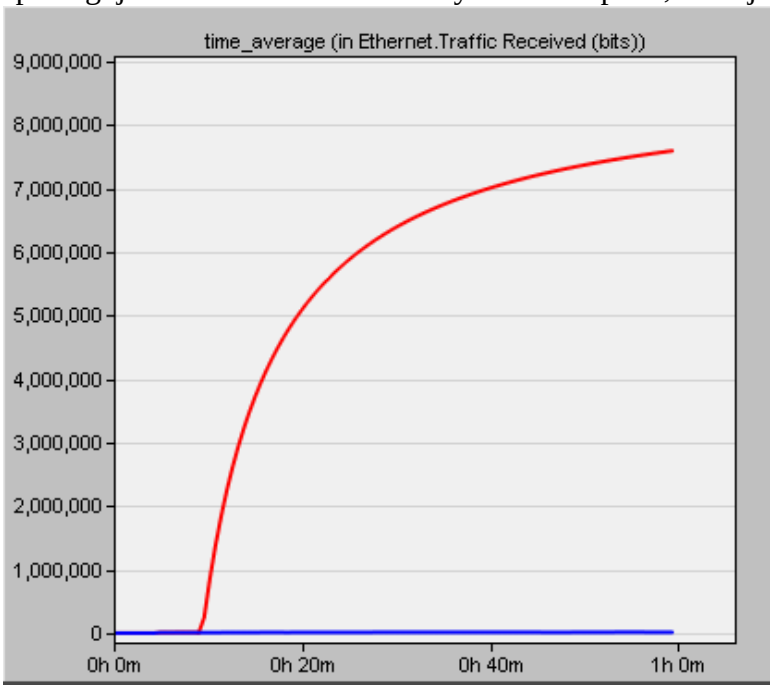
Antruoju tyrimu taip pat siekta nustatyti, kokį poveikį patalpų apsaugos sistemos, kuri veikia tarpmiestiniame tinkle, vidutiniam atsako vėlavimo laikui turi inicijuota DoS ataka. Kaip galima pastebėti 3.15 paveiksle, pirmosiomis dešimt tyrimo minučių, kurių metu vykdoma apšilimo fazė, bei pradedama tinklo naudojimosi fazė, patalpų apsaugos vidutinis sistemos užklausų atsako vėlavimo laikas yra toks mažas, kad grafike jis beveik yra lygus nuliui. Atakuojančiam asmeniui nusitaikius į pasirinktą patalpų apsaugos sistemą, bei inicijavus DoS ataką, vidutinis užklausų atsako vėlavimo laikas pradeda didėti. Patalpų apsaugos sistemos vidutinio užklausų atsako vėlavimo laiko kreivė yra panaši į vidutinę patalpų apsaugos sistemos gaunamo tinklo srauto dydžio kreivę, kas leidžia teigti, jog atakos metu didėjant gaunamam vidutiniam tinklo srauto dydžiui, tokiu pačiu greičiu didėja ir vidutinis užklausų atsako vėlavimo laikas. Lyginant šio tyrimo vidutinį užklausų atsako vėlavimo laiką su vidutiniu užklausų atsako vėlavimo laiku, gautu pirmojo tyrimo metu, kuomet inicijuojama ataka, galima pastebėti, kad atsako vėlavimo laikas yra daug didesnis.

### 3.4. Išvados

Šiame skyriuje aprašytas apsaugos sistemos tinklo modelio sudarymas, tyrimas, bei gauti rezultatai. Tyrimui atlikti buvo sukurti du skirtingų tipų modeliai. Vienas modelis, buvo sukurtas siekiant atlikti tyrimą, kai patalpų apsaugos sistema yra vietiniame tinkle, bei pasiekiama tik vartotojui esant tame pačiame tinkle. Kitas modelis sukurtas siekiant atlikti tyrimą, kai tinkle egzistuoja daugiau nei viena patalpų apsaugos sistema, pats tinklas yra didelis ir turi kelis tinklo topologijos lygmenis (buto, namo, rajono, miesto).

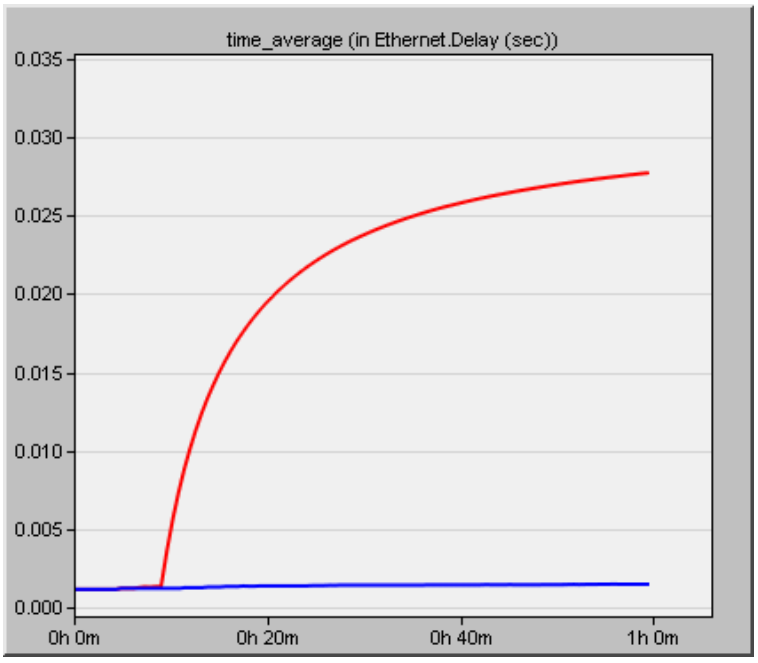
Kiekvienas modelis buvo tiriamas du kartus, siekiant nustatyti ir palyginti patalpų apsaugos sistemos gaunamą vidutinį tinklo srauto dydį, bei vidutinį patalpų apsaugos sistemos atsako į užklausas vėlavimo laiką. Pirmasis modelio tyrimas buvo vykdomas kuomet tinklas naudojamas tink patalų apsaugos sistemos(-ų) ir jų vartotojo(-ų), t. y., geruoju atveju, kuomet nevykdomos jokios atakos. Antrasis tyrimas buvo atliekamas siekiant nustatyti, koks poveikis yra patalpų apsaugos sistemos prieinamumui, kai tinkle vykdoma DoS ataka.

Pirmojo modelio atveju, nustatyta, kad patalpų apsaugos sistema atakos metu gauna daug kartų didesnį tinklo srauto dydį lyginant su tinklo srauto dydžiu, gaunamu kuomet tinklu naudojasi tik vartotojas. Tyrimo pabaigoje vidutinis tinklo srauto dydis be atakos siekė apie 16 tūkst. bitų, kuomet vykdant ataką tyrimo pabaigoje vidutinis tinklo srauto dydis buvo apie 7,8 milijonai bitų.




**3.16 pav. Vidutinio tinklo srauto dydžio vietiniame tinkle palyginimas vykdant ataką ir jai nevykstant**

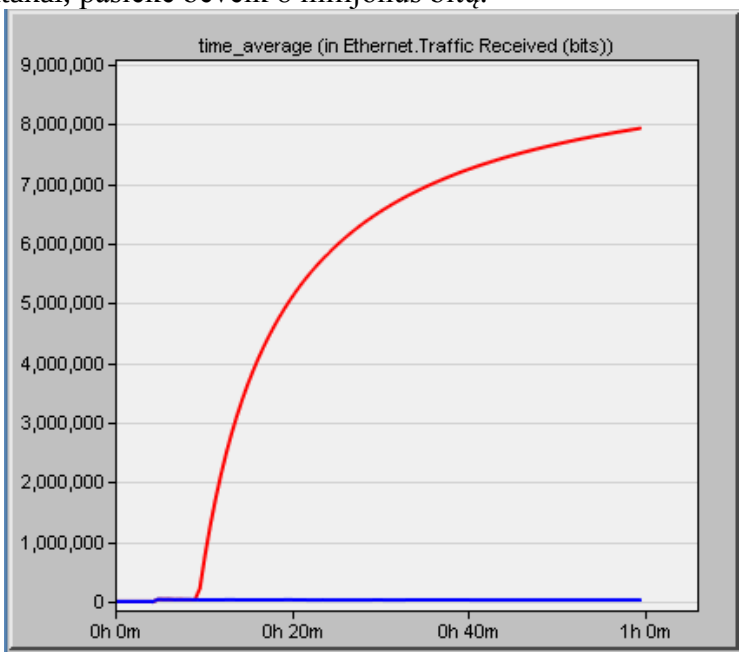
Dėl šios priežasties, patalpų apsaugos sistema bando susidoroti su visais gaunamais paketais ir atsakyti į gaunamas užklausas. Kadangi užklausų yra itin daug, užklausų atsako vėlavimo laikas atakos metu, lyginant su užklausų atsako vėlavimo laiku, kuomet tinkle nevykdoma jokia ataka, taip pat stipriai padidėja. Žvelgiant į bendrą palyginamąjį vidutinio atsako vėlavimo laiko paveikslą, galima matyti, kad nevykdant atakos, vidutinis atsako vėlavimo laikas neviršijo 0,002 s, o vykstant DoS atakai, tyrimo pabaigoje vidutinis atsako vėlavimo laikas buvo apie 0,028 s.




**3.17 pav. Vidutinio atsako vėlinimo laiko vietiniame tinkle palyginimas vykdant ataką ir jai nevykstant**

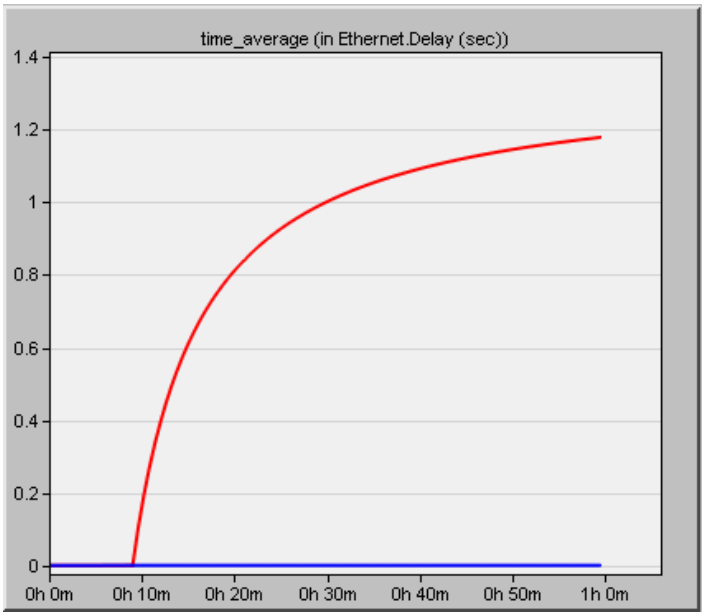
Kartojant tokį pat tinklo tyrimo metodą, buvo ištirtas atakos poveikis didelio masto tinkle, kuriame veikia daugiau nei viena patalpų apsaugos sistema. Gauti rezultatai buvo panašūs į gautuosius tiriant patalpų apsaugos sistemos vietiniame tinkle modelį, tačiau tiek vidutinis tinklo srauto dydis, tiek vidutinis užklausų atsako vėlavimo dydis buvo didesnis, nei modelyje, kuriame yra tik viena patalpų apsaugos sistema.

Vidutinis tinklo srauto dydis nevykstant atakai, šiame tinkle nebuvo didesnis už 28 tūkst. bitų, tačiau vykstant DoS atakai, pasiekė beveik 8 milijonus bitų.




**3.18 pav. Vidutinio tinklo srauto dydžio tarpmiestiniame tinkle palyginimas vykdant ataką ir jai nevykstant**

Vidutinis patalpų apsaugos sistemos atsako vėlavimo laikas lyginant abu tyrimo atvejus (kai nevykdoma ir kuomet vykdoma DoS ataka) taip pat stipriai skyrėsi. Nevykstant jokiai atakai, vidutinis atsako vėlavimo laikas neviršijo 0,016s. Tačiau pradėjus vykdyti ataką tinkle, atsako vėlavimo laikas išaugo iki 1,2s.




**3.19 pav. Vidutinio atsako vėlinimo laiko tarpmiestiniame tinkle palyginimas vykdant ataką ir jai nevykstant**

Atlikus šį tyrimą galima teigti, kad DoS atakos metu tiek tinklo srauto dydis tiek atsako vėlavimo laikas išauga kelis kartus, bei priklauso nuo tinklo dydžio ir tinklo topologijos. Tačiau, išanalizavus gautus duomenis, buvo nustatyta, kad vieno žmogaus inicijuojama DoS ataka nėra kritinė, bet atakuojančiam asmeniui inicijavus ataką turint daugiau resursų – kompiuterių, dideliame tinkle patalpų apsaugos sistemos darbas gali būti sutrikdytas, o pati sistema gali būti nepasiekiama vartotojui, kadangi didėjant atakuojančių kompiuterių skaičiui aritmetine progresija, atitinkamai aritmetine progresija didėja ir vidutinis gaunamas tinklo srauto dydis, ir vidutinis atsako vėlavimo laikas.

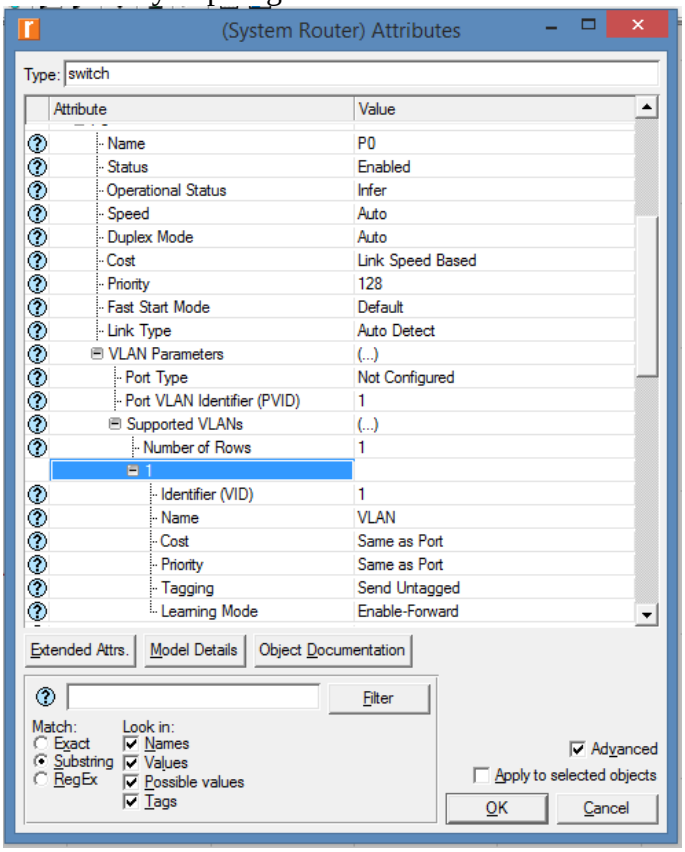
# 4. PATALPŲ APSAUGOS SISTEMOS TINKLO MODELIO SAGUMO SPRENDIMO PARINKIMAS IR EFEKTYVUMO TYRIMAS

Atlikus tiek patalpų sistemos, esančios vietiniame tinkle modelio, tiek patalpų apsaugos sistemų tarpmiestinio tinklo modelio tyrimus, buvo nustatytas DoS atakos poveikis patalpų apsaugos sistemos pasiekiamumui. Siekiant kaip įmanoma labiau sumažinti atakos grėsmę modeliuose, buvo nuspręsta įdiegti saugos sprendimus, kurie padėtų tai padaryti.

## 4.1. Patalpų apsaugos sistemos vietinio tinklo modelio saugumo sprendimo parinkimas ir efektyvumo tyrimas

Išanalizavus galimas atakos grėsmes, kai patalpos apsaugų sistema veikia vietiniame tinkle, buvo nustatyta, kad tokio tipo tinklo modelis gali dažniausiai būti naudojamas įmonėse, ar namuose, kurių vartotojams nereikalinga išorinė prieiga prie patalpų apsaugos sistemos valdymo. Todėl, nustatyta, kad šio tinklo modelyje inicijuota ataka gali būti vykdoma tik atakuojančiam asmeniui prisijungus prie to paties vidinio tinklo, kuriame veikia patalpų apsaugos sistema. Siekiant apsaugoti patalpų apsaugos sistemą, buvo nuspręsta panaudoti VLAN – virtualų vietinį tinklą, kuriam priklausytų tik patalpų apsaugos sistema, apsaugos sistemos naudojamas tinklo maršrutizatorius, bei patalpų apsaugos sistemos vartotojas. Prie šio virtualaus tinklo daugiau niekas negali prisijungti.

Tinklo modelio schema „Riverbed Modeler“ aplinkoje išliko tokia pati, tačiau prisidėjo papildomi nustatymai, kurie buvo nustatyti apsaugos sistemos tinklo maršrutizatoriuje.

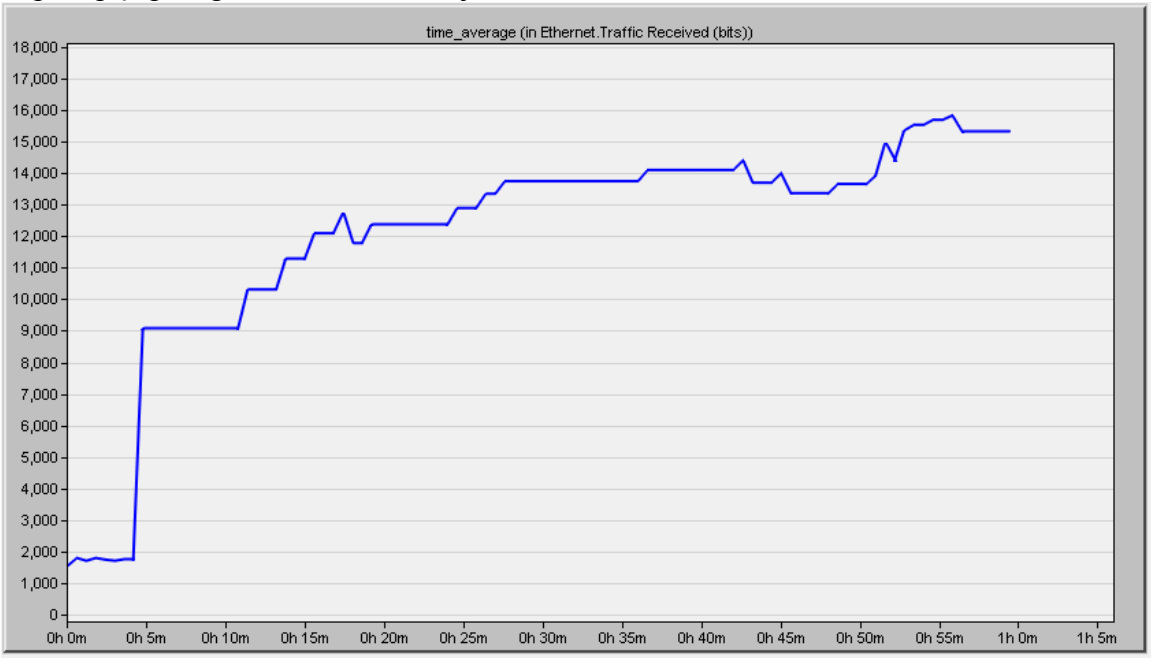



**4.1 pav. VLAN nustatymai tinklo maršrutizatoriuje**

Siekiant nustatyti šio saugos sprendimo diegimo efektyvumą, kuomet ataka vykdoma vietiniame tinkle, buvo atliktas tyrimas su modelyje įdiegtu virtualiu vietiniu tinklu. Vietinio tinklo modelio schema lyginant su schema, kuri buvo sumodeliuota trečiame skyriuje, nė kiek nepasikeitė.

Modelio tyrimas atliekamas tokiu pačiu principu, kaip ir trečiajame skyriuje – vykdomi du tyrimai, kuomet tinkle veikia tik vartotojas ir patalpų apsaugos sistema, bei tyrimas, kuomet prie tinklo prisijungia atakuojantis asmuo, bei inicijuojama DoS ataka.

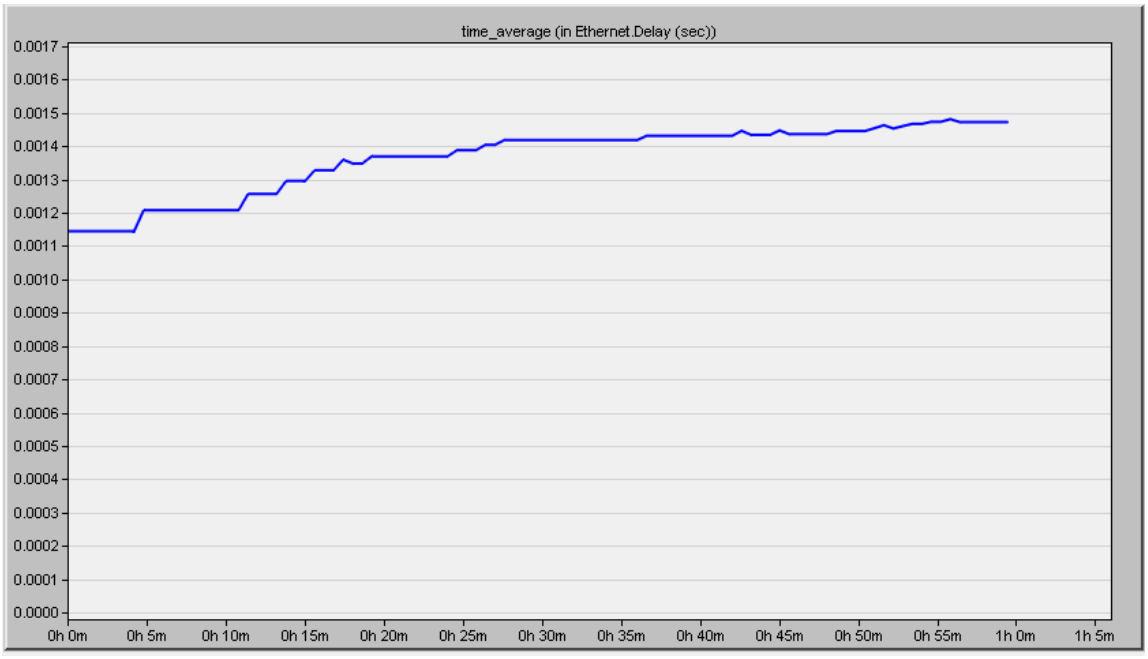
Tyrimų metu buvo tiriamas patalpų apsaugos sistemos vidutinis gaunamas tinklo srauto dydis, bei vidutinis patalpų apsaugos sistemos užklausų atsako vėlavimo laikas. Pirmasis tyrimas buvo atliktas, kuomet tinkle veikia tik patalpų apsaugos sistema ir sistemos vartotojas, kuris naudojasi įprastinėmis patalpų apsaugos sistemos funkcijomis.




**4.2 pav. Vidutinis sistemos tinklo srauto dydis vietiniame tinkle su VLAN nevykstant atakai**

Paveiksle 4.2 yra pateiktas patalpų apsaugos sistemos vietinio tinklo modelio su VLAN saugos sprendimu vidutinis tinklo srauto dydis, kurį gauna patalpų apsaugos sistema, kuomet tinkle nevykdoma jokia ataka. Kaip ir tyrimo metu, kuomet patalpų apsaugos sistemos vietiniame tinkle nebuvo įdiegtas joks saugumo sprendimas, vidutinis tinklo srautas, kurį gauna patalpų apsaugos sistema nėra didelis. Pirmosios penkios tyrimo minutės yra apšilimo fazė, kuomet vartotojas dar nesinaudoja patalpų apsaugos sistema. Nuo penktosios minutės, vartotojas pradeda naudotis patalpų apsaugos sistema, dėl ko pastebimas gaunamo tinklo srauto padidėjimas. Kadangi vartotojas naudojasi įvairiomis funkcijomis, vidutinis tinklo srauto dydis nuolat kinta, tačiau jo kitimas nėra drastiškas. Lyginant modelio, kuomet neįdiegtas saugumo sprendimas – VLAN, bei modelio, kuomet yra įdiegtas VLAN saugumo sprendimas, neatakuojamo tinklo srauto dydis yra identiškas.

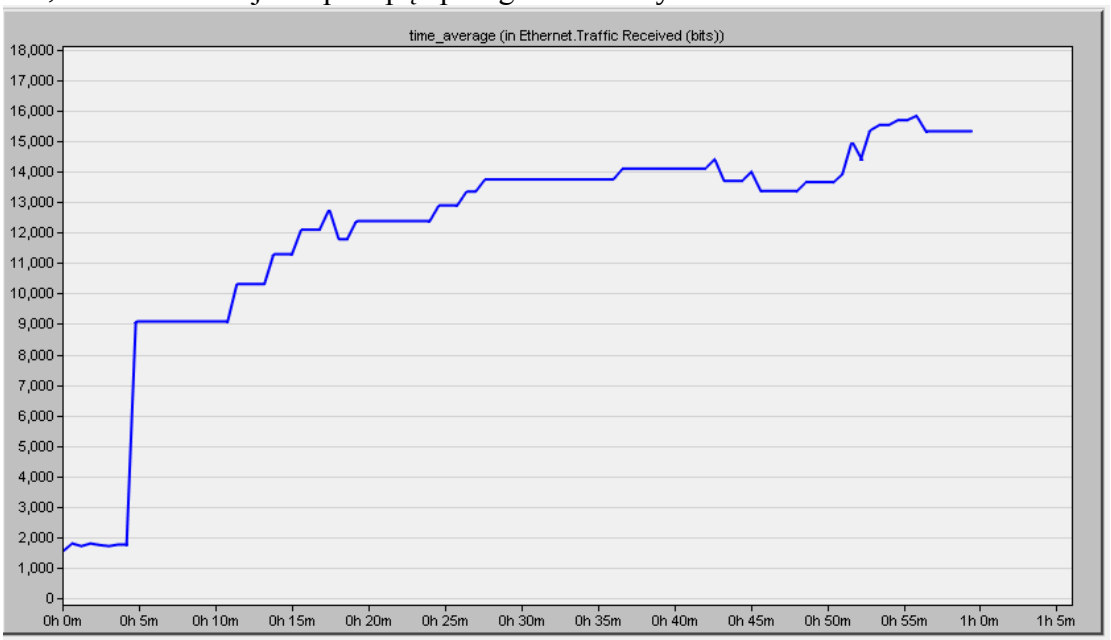
Žemiau pateiktame paveiksle, pateikiamas vidutinis užklausų atsako vėlavimo laikas.




**4.3 pav. Vidutinis užklausos atsako vėlavimo laikas vietiniame tinkle su VLAN nevykstant atakai**

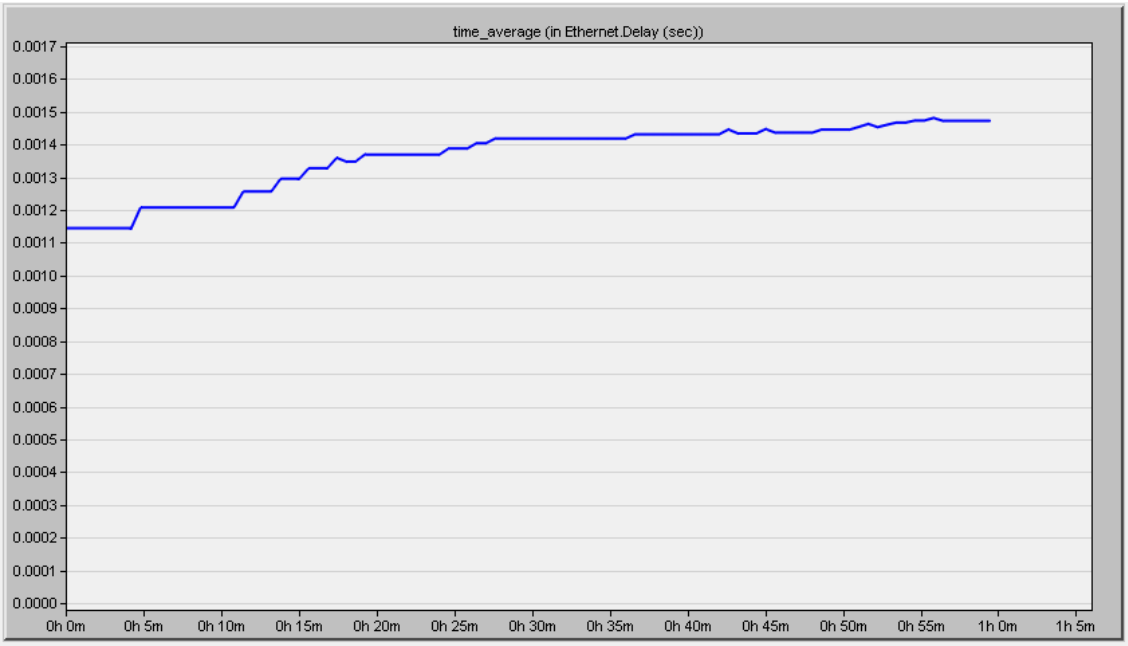
Lyginant modelio kuriame neįdiegtas saugumo sprendimas, bei modelio, kuriame įdiegtas saugumo sprendimas patalpų apsaugos sistemos vidutinio užklausos atsako vėlavimo laiko grafikus, galima pastebėti, kad jie taip pat yra identiški, kuomet tinkle nevykdoma DoS ataka.

Ištyrus patalpų apsaugos sistemos vietinio tinklo modelį su įdiegtu saugos sprendimu, kuomet tinkle nevykdoma DoS ataka, tinklo modelyje pridėtas papildomas tinklo modelio komponentas – atakuojantis asmuo, kuris inicijuoja DoS ataką siunčiant itin didelio dydžio ICMP ping paketus į patalpų apsaugos sistemą. Tokiu būdu atliekamas antrasis šio modelio tyrimas, siekiant nustatyti koks atakos poveikis, kuomet atakuojama patalpų apsaugos sistema yra sukurtame VLAN tinkle.




**4.4 pav. Vidutinis sistemos tinklo srauto dydis vietiniame tinkle su VLAN vykdant DoS ataką**

Atlikus tyrimą pastebėta, vidutinis tinklo srauto dydis, kurį gauna patalpų apsaugos sistema esanti VLAN tinkle, kartu su sistemos vartotoju, nė kiek nepakito. Žemiau pateikiamame paveiksle vaizduojamas vidutinis patalpų apsaugos sistemos užklausų atsako vėlavimo laikas.




**4.5 pav. Vidutinis užklausos atsako vėlavimo laikas vietiniame tinkle su VLAN vykdant DoS ataką**

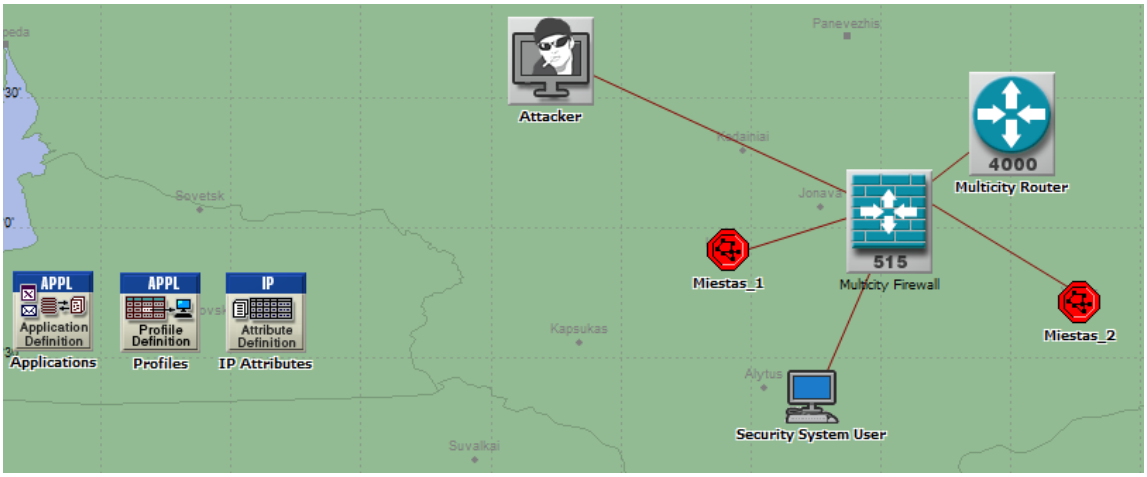
Išanalizavus patalpų apsaugos sistemos vidutinį užklausų atsako vėlavimo laiką taip pat pastebėta, kad dėl įdiegto VLAN tinklo, vidutinis atsako vėlavimo laikas yra identiškas vidutiniam užklausų atsako vėlavimo laikui, kuomet patalpų apsaugos sistemos vietiniame tinkle nevykdoma jokia ataka.

Taip yra todėl, kad VLAN tinklas izoliuoja prisijungimą prie patalpų apsaugos sistemos tinklo maršrutizatoriaus, todėl atakuojantis asmuo prisijungęs prie tinklo maršrutizatoriaus negali pasiekti patalpų apsaugos sistemos, bei siųsti jai DoS atakos ICMP paketų. Kadangi paprastas vartotojas taip pat yra prisijungęs prie VLAN tinklo, jo tinklo paketai pasiekia patalpų apsaugos sistemą lygiai taip pat, kaip ir prieš tai vykdytame tyrime.

## 4.2. Patalpų apsaugos sistemos tarpmiestinio tinklo modelio saugumo sprendimo parinkimas ir efektyvumo tyrimas

Atlikus tarpmiestinio patalpų apsaugos sistemų tinklo modelio tyrimą, tyrimo metu buvo nustatyta, kad didesniame tinkle patalpų apsaugos sistemos vidutinis atsakymo vėlavimo laikas, taip pat tampa didesnis, kuomet yra vykdoma DoS ataka. Norint panaikinti grėsmę, buvo sugalvota, jog reikalingas saugos sprendimas, kurį įdiegus DoS ataka taptų neveiksminga. Tarpmiestinis tinklo modelis gali būti pritaikytas, steigiant apsaugos įmonę, kurios tinklas bus panaudotas sukurti bendrą patalpų apsaugos sistemų tinklą vartotojų prisijungimui ir patalpų apsaugos sistemų valdymui iš bet kurios vietovės. Todėl sprendžiant saugos sistemos diegimo klausimą šiame tinkle buvo atsižvelgta į išlaidas, kurios turėtų būti kuo mažesnės.

Priimtas sprendimas, kurį reikėtų taikyti – ugniasienė, kuri būtų panaudota aukščiausiame tinklo lygmenyje, o visi tinklo vartotojai tiek iš tinklo vidaus, tiek iš tinklo išorės turėtų valdymo komandų paketus siųsti per ugniasienę, kuri prijungta prie išoriniame lygmenyje esančio tinklo maršrutizatoriaus. Patalpų apsaugos sistemos išorinio tinklo modelis buvo pakoreguotas, taip, kad atitiktų šiuos kriterijus. Tinklo maršrutai perkonfigūruoti taip, kad bet koks tinklo srautas visų pirma keliautų į aukščiausio lygmens tinklo maršrutizatorių, o tuomet keliautų į ta patalpų apsaugos sistemą, kuriai šis srautas yra skirtas. Taip pat, tinklo ugniasienė sukonfigūruota taip, kad filtruotų tinklo paketus, kurie atitinka DoS atakos kriterijus, t. y., kad filtruotų itin didelio dydžio ICMP ping paketus. Žemiau pateiktame paveiksle yra vaizduojama tinklo modelio struktūra su įdiegta tinklo ugniasiene aukščiausiame lygmenyje.

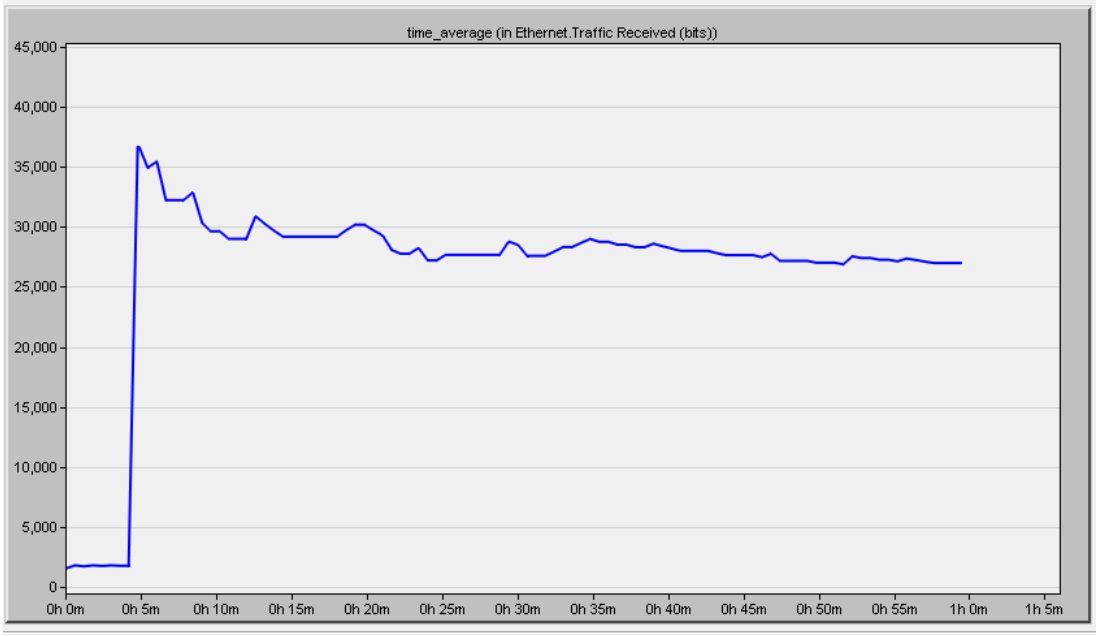



**4.6 pav. Tarpmiestinio tinklo modelio schema su įdiegta ugniasiene**

Visos išorinės jungtys į tinklą, bei miestų tinklai yra prijungti prie ugniasienės, o statiniai maršrutai visus tinklo paketus visų pirma nukreipia į tarpmiestinį tinklo maršrutizatorių, dėl ko visi siunčiami paketai keliauja pro ugniasienę, pasiekia tarpmiestinį tinklo maršrutizatorių, o tuomet keliauja į vieną ar kitą tinklą iki kol pasiekia reikiamą patalpų apsaugos sistemą.

Atlikus tinklo saugos sprendimo diegimą patalpų apsaugos sistemų tarpmiestinio tinklo modelyje, kartojamas identiškas tinklo modelio tyrimas. Tyrimas skaidomas į du tyrimus, iš kurių vienas tiria vidutinį tinklo srauto dydį tenkantį patalpų apsaugos sistemai, kuomet tinklu naudojasi tik tikrieji tinklo vartotojai – siunčia įvairias komandas savo patalpų apsaugos sistemoms.

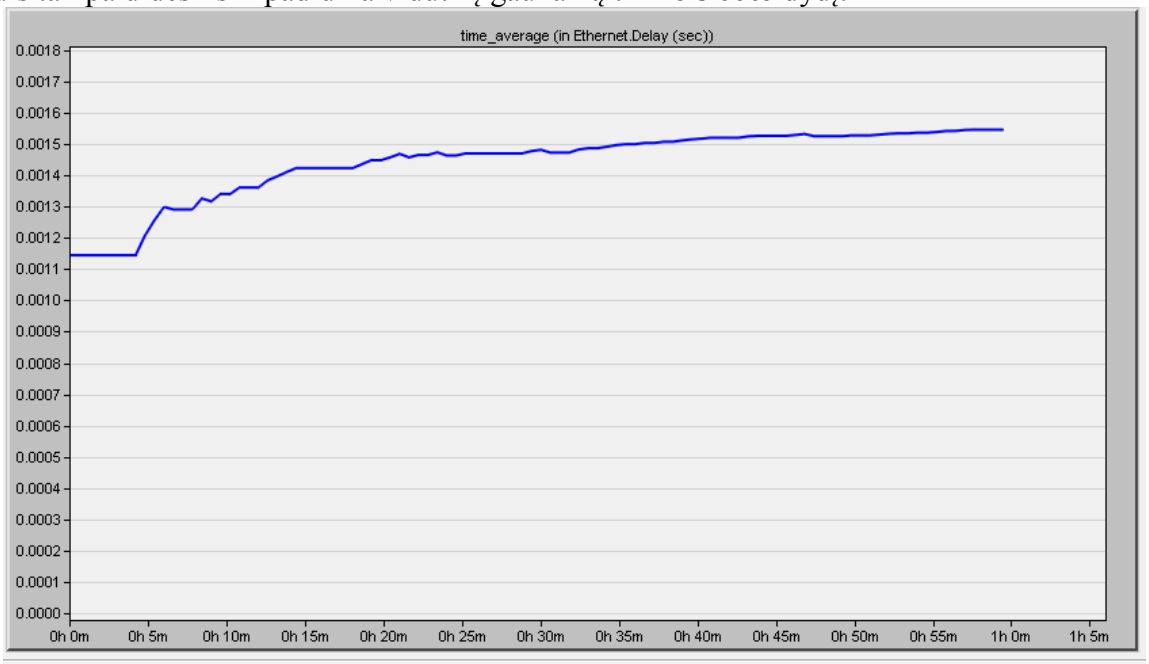
Pirmojo patalpų apsaugos sistemos tyrimas vykdomas, kuomet tinkle yra prisijungę tik patalpų apsaugos sistemų vartotojai, bei veikia patalpų apsaugos sistemos. Tyrimo metu gaunamas vidutinio tinklo srauto dydžio, tenkančio patalpų apsaugos sistemai grafikas, kuris yra pateiktas žemiau esančiame paveiksle.




**4.7 pav. Vidutinis sistemos tinklo srauto dydis tarpmiestiniame tinkle su ugniasiene nevykstant atakai**

Išanalizavus gautą vidutinio tinklo srauto dydžio grafiką, gautą atlikus tarpmiestinio tinklo modelio su įdiegta ugniasiene, bei pertvarkytais tinklo maršrutais, galima pastebėti, kad lyginant su tarpmiestiniu tinklo modeliu, kuriame nebuvo įdiegtas saugos sprendimas, grafiko kreivės yra panašios. Tačiau dėl nustatytų statinių maršrutų, kuomet visi tinklo srautai bet kokiu atveju keliauja į aukščiausio tinklo modelio topologijos tinklo maršrutizatorių ir iš ten keliauja į reikalingą pasiekti patalpų apsaugos sistemą, pastebėta, jok tinklo srautas tapo šiek tiek didesnis. Tą paaiškinti galima remiantis tinklo maršrutais, kuomet dėl didesnio tinklo ir ilgesnio paketo kelio keliaujant pro daugiau

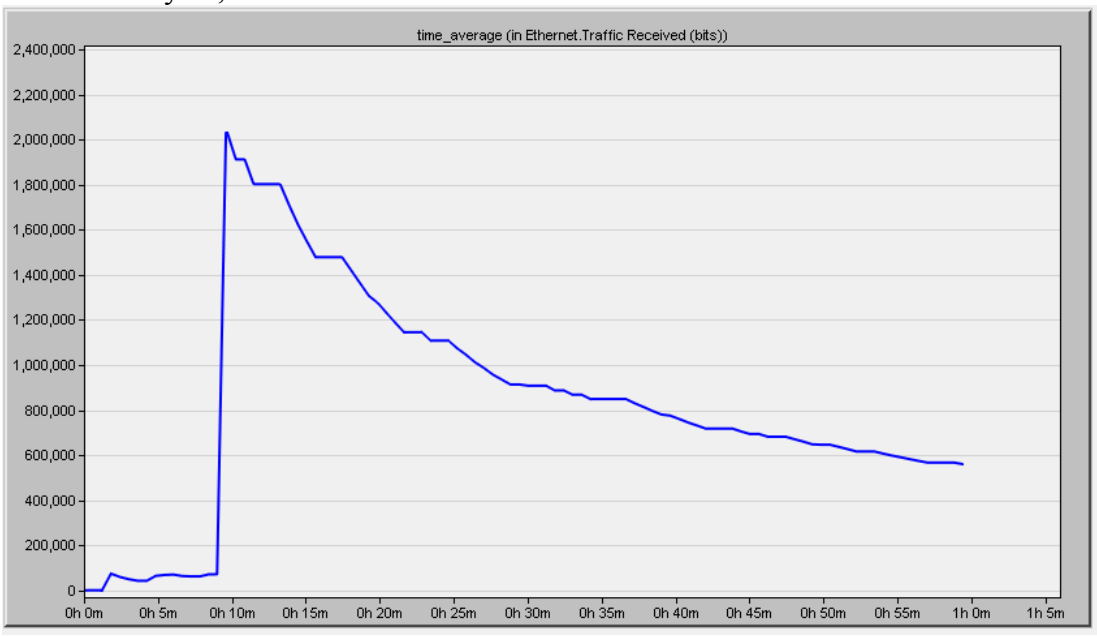
tinklo maršrutizatorių, prie paketo pridedama daugiau informacijos apie paketo kelią. To pasekoje, paketų dydis tampa didesnis ir padidina vidutinį gaunamą tinklo srauto dydį.




**4.8 pav. Vidutinis užklausos atsako vėlavimo laikas tarpmiestiniame tinkle su ugniasiene nevykstant atakai**

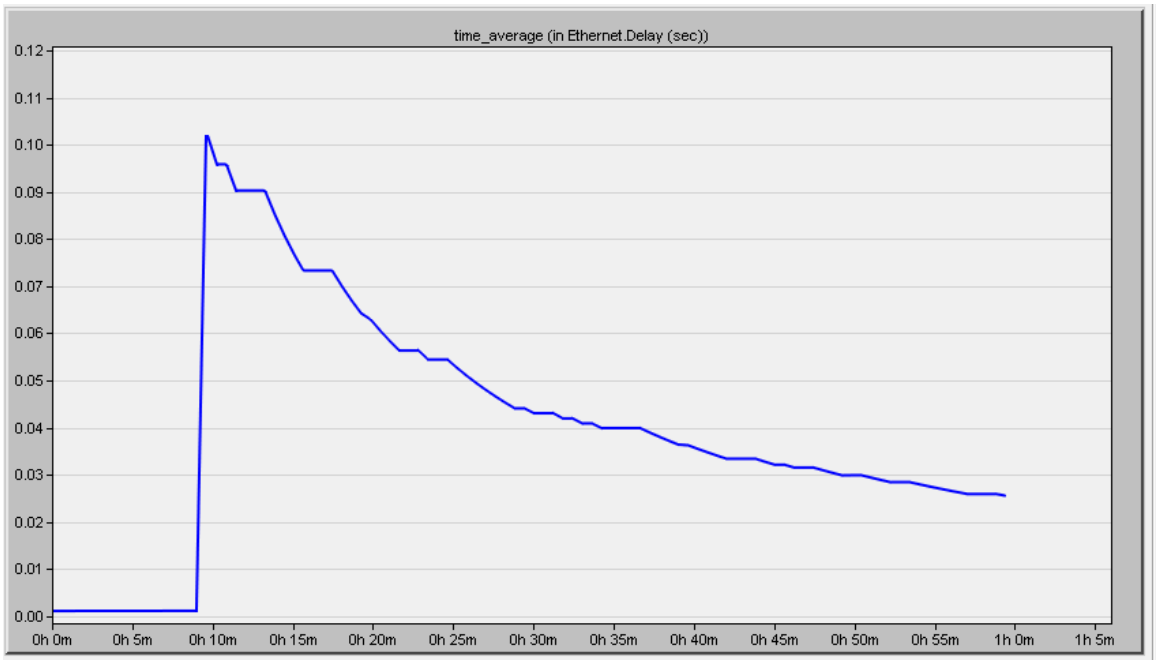
Patalpų apsaugos sistemų tarpmiestinio tinklo modelyje nevykstant DoS atakai, buvo išanalizuotas ir vidutinis patalpų apsaugos sistemos užklausų atsako vėlavimo laikas. Žvelgiant į gautą grafiką, esantį 4.8 paveiksle, galima pastebėti, kad patalpų apsaugos sistemos vidutinis užklausų atsako vėlavimo laikas beveik nepakinta, lyginant su identiško tyrimo grafiku, aprašytu trečiame skyriuje. Vidutinis užklausos atsako laikas yra nedidelis ir pakankamai tolygus, kas leidžia daryti prielaidą, kad tinkle nepastebėta jokių trikdžių, o nežymiai padidėjęs tinklo srautas, kurį gauna patalpų apsaugos sistema dėl pailgėjusio paketų maršruto, neįtakoja patalpų apsaugos sistemų atsako vėlavimo laiko.

Antrasis tyrimas vyksta, kuomet prie tinklo prisijungia atakuojantis asmuo, kuris inicijuoja DoS ataką, nukreiptą prieš pasirinktą vieną patalpų apsaugos sistemą. Tyrimas yra analogiškas aprašytam trečiajame skyriuje, kuomet atakos metu stebimas patalpų apsaugos sistemos vidutinis gaunamas tinklo srauto dydis, bei vidutinis užklausos atsako vėlavimo laikas.




**4.9 pav. Vidutinis sistemos tinklo srauto dydis tarpmiestiniame tinkle su ugniasiene vykdant DoS ataką**

Išanalizavus 4.9 paveiksle pavaizduotą vidutinį tinklo srauto dydį, tenkantį patalpų apsaugos sistemai, kuomet vykdoma ataka, galima pastebėta, kad nuo dešimtosios minutės, kuomet prie tinklo prisijungia atakuojantis asmuo ir pradeda vykdyti DoS ataką, vidutinis tinklo srauto dydis pakyla, tačiau lyginant su vidutinio tinklo srauto dydžio grafiku, kuomet tarpmiestiniame tinklo modelyje nėra įdiegta tinklo ugniasienė, bei yra vykdoma ataka, vidutinis srauto dydis nepadidėja tiek, kiek modelyje be ugniasienės. Taip pat, dėl ugniasienės konfigūracijos, tinklo srauto dydis iškart pradeda mažėti ir normalizuojasi, nes ugniasienė pradeda atmetinėti atakuojančio asmens siunčiamus ICMP ping paketus.




**4.10 pav. Vidutinis užklausos atsako vėlavimo laikas tarpmiestiniame tinkle su ugniasiene vykdant DoS ataką**

Analizuojant tyrimo metu gautą vidutinį patalpų apsaugos sistemos užklausų atsako vėlavimo laiką, pateiktą 4.10 paveiksle, pastebėta, jog vidutinis atsako vėlavimo laikas, taip pat staiga padidėja, kuomet pradedama vykdyti DoS ataka, nukreipta prieš apsaugos sistemą, tačiau pokytis nėra toks didelis, koks buvo pastebėtas tiriant tarpmiestinį tinklo modelė, kuriame nėra įdiegta tinklo ugniasienė. Taip pat, dėl tinklo ugniasienės įdiegimo ir konfigūracijos, vidutinis atsako vėlavimo laikas iškart po pakilimo pradeda mažėti, kol pasiekia įprastinį atsako vėlavimo laiką, kuomet tinkle nevykdoma jokia ataka.

## 5. IŠVADOS

Šiame darbe aprašyta išmanioji patalpų apsaugos sistema yra prototipo stadijoje, todėl buvo nuspręsta sudaryti tinklo, kuriame patalpų apsaugos sistema galėtų funkcionuoti, modelį, bei atlikti modelio tyrimą, siekiant išsiaiškinti kokį poveikį patalpų apsaugos sistemos pasiekiamumui gali turėti vykdomos DoS atakos.

Darbo pradžioje buvo trumpai išanalizuota išmaniosios patalpų apsaugos sistemos koncepcija ir sudėtis. Taip pat buvo išanalizuoti DoS atakų tipai, bei jų veikimo principai. Buvo pateikti trumpi atakų aprašymai, bei veikimo schemos. Iš išanalizuotų DoS atakų tipų, tyrimui buvo pasirinkta ICMP ping ataka.

Šiame darbe buvo sukurtas tyrimo metodas, kuriame numatyta, kad tinklo modelyje bus panaudotos 10Mbps tinklo pralaidumo jungtys. Atsižvelgiant į tai, kad realybėje tokio pralaidumo jungtys nepraleidžia maksimalaus skelbiamo tinklo srauto, numatyta, kad tikrasis tinklo pralaidomas bus 8Mbps. Taip pat, sudarinėjant metodą nustatyta, kad DoS ataka bus laikomas tinklo srauto dydis ne mažesnis nei 90% tikrojo tinklo srauto pralaidumo, kas yra ne mažiau nei 7,2 megabitai.

Darbo metu, panaudojant „Riverbed Modeler“ tinklo modeliavimo įrankį buvo sumodeliuoti du skirtingi tinklo modeliai, atsižvelgiant į tai, kad vieni patalpų apsaugos sistemos vartotojai gali naudotis patalpų apsaugos sistema savo reikmėms ir tik vietiniame tinkle, o antrasis modelis buvo sukurtas mąstant apie platesnį apsaugos sistemos panaudojamumą – apsaugos įmonės, kuri diegs šią apsaugos sistemą vartotojų namuose, bendrą tinklą, jungiantį visas įdiegtas patalpų apsaugos sistemas, sudarant galimybę vartotojams naudotis sistema ir gauti jos pranešimus būnant bet kur.

Sukūrus tinklo modelius, jie buvo panaudoti tiriant patalpų apsaugos sistemos pasiekiamumą DoS atakos metu. Pirmojo tyrimo metu, buvo išsiaiškintas DoS atakos veiksmingumas, vertinant vidutinį patalpų apsaugos sistemos gaunamą tinklo srauto dydį, bei vidutinį patalpų apsaugos sistemos užklausos atsako vėlavimo laiką. Atlikus tyrimą, nustatyta, kad vidutinis tinklo srauto dydis tarp neatakuojamo tinklo ir tinklo, kuriame inicijuojama DoS ataka, skiriasi – atitinkamai apie 16 tūkst. bitų ir 7,8 mln. Bitų. Nustatyta, kad tyrimo pabaigoje vidutinių tinklo srauto dydžių skirtumas yra daugiau nei 487 kartai. Taip pat ištirtas vidutinis užklausos atsako vėlavimo laikas, kuomet tinklas veikia įprastu režimu ir kuomet tinkle inicijuojama DoS ataka. Atlikus tyrimą nustatyta, kad skirtumas tarp gautų rezultatų yra apie 20 kartų.

Įvertinus tyrimo rezultatus, bei tokio tinklo panaudojimo galimybes, nuspręsta vietinio tinklo modelyje įdiegti VLAN. Pakartojus tyrimą vietinio tinklo modelyje su įdiegtu saugos sprendimu, pastebėta, kad DoS atakos inicijavimas visiškai neįtakoja tinklo veikimo, kadangi tiek tiriant neatakuojamą tinklą, tiek tiriant tinklą, kuriame vykdoma DoS ataka, vidutinis tinklo srauto dydis, bei vidutinis užklausos atsako vėlavimo laikas lieka nepakitęs.

Tiriant tarpmiestinį tinklo modelį, nustatyta, kad vidutinis tinklo srauto dydis, kuomet tinkle nevykdoma ataka, yra nedidelis ir priklausomai nuo tinklo vartotojų veiksmų daugiausiai yra šiek tiek virš 26 tūkst. bitų. Atakos metu, vidutinis tinklo srauto dydis pasiekia beveik 8 megabitus, kas leidžia suprasti, jog tinkle yra vykdoma DoS ataka.

Taip pat, ištyrus vidutinį patalpų apsaugos sistemos užklausų atsako vėlinimo laiką nevykstant jokiai atakai, bei vykdant DoS ataką tarpmiestiniame tinkle, nustatyta, kad skirtumas tarp šių laikų yra apie 75 kartai. Atsižvelgus į tinklo topologiją, tyrimo rezultatus ir šio tinklo modelio panaudojimą realybėje, nuspręsta prie tarp miestų esančio tinklo maršrutizatoriaus prijungti tinklo ugniasienę, bei nustatyti tinklo maršrutus taip, kad visas tinklo srautas pirmiausiai pasiektų ugniasienę ir tinklo maršrutizatorių esantį tarp miestų, o tik tuomet būtų nukreiptas į reikalingą tinklo tašką. Atlikus tarpmiestinio tinklo modelio pakeitimus, buvo pakartotas tyrimas. Ištyrus atnaujintą tinklo modelį su įdiegtu saugumo sprendimu, nustatyta, kad tinkle nevykdant jokių atakų, vidutinis tinklo srauto dydis, kurį gauna patalpų apsaugos sistema, šiek tiek išauga ir didžiausias tinklo srautas tyrimo metu neviršija 36 kilobitų. Tačiau išanalizavus tyrimo metu gautą vidutinį patalpų apsaugos sistemos užklausų atsako vėlinimo laiką nustatyta, kad jis išlieka beveik toks pats, kaip ir tinklo modelyje, kuriame nėra įdiegtas saugumo sprendimas.

Inicijavus DoS ataką patalpų apsaugos sistemų tarpmiestinio tinklo modelyje, nustatyta, kad tik pradėjus vykdyti ataką, vidutinis tinklo srauto dydis padidėja iki 2 megabitų ir iškart pradeda

mažėti. Lygiai toks pats pokytis buvo pastebėtas ir analizuojant vidutinį užklausų atsako vėlinimo laiką, vykstant atakai. Vidutinis atsako vėlinimo laikas tik inicijavus ataką padidėja iki 0,1 sekundės ir taip pat iškart pradeda mažėti. Nustatyta, jog šį mažėjimą lemia ugniasienės konfigūracija, dėl kurios tinklo srautas identifikuotas kaip DoS ataka, yra atmetamas.

Lyginant tinklo modelių tyrimų rezultatus prieš ir po saugos sprendimų įdiegimo, nustatyta, kad parinkti saugos sprendimai yra labai efektyvūs siekiant apsaugoti vietinį ar tarpmiestinį tinklą nuo DoS pobūdžio atakų.

Tolimesniuose darbuose būtų galima remtis šiuo tyrimu, siekiant patobulinti pačią patalpų apsaugos sistemą, ar suprojektuoti saugų tinklą, skirtą atremti didesnio mąsto DoS atakas, nukreiptas prieš vieną ar daugiau patalpų apsaugos sistemų esančių bendrame tinkle.

## 6. LITERATŪRA


[1] D. M. Gregg, W. J. Blackert, D. V. Heinbuch, D. Furnanage, „Assessing and quantifying denial of service attacks“ 2001. [Tinkle]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=985767 [Kreiptasi 20 03 2015].

[2] S. S. Kolahi, K. Treseangrat, B. Sarrafpour, „Analysis of UDP DDoS Flood Cyber Attack and Defense Mechanisms on Web Server with Linux Ubuntu 13“ 2015. [Tinkle]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7081286 [Kreiptasi 20 03 2015].

[3] C. Douligeris ir A. Mitrokotsa, „DDoS attacks and defense mechanisms: a classification“ 2001. [Tinkle]. Available: http://mediamatica.ewi.tudelft.nl/sites/default/files/ISSPIT03.pdf [Kreiptasi 20 03 2015].

[4] Q. Gu ir P. Liu, „Denial of Service Attacks“ 2001. [Tinkle]. Available: http://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf [Kreiptasi 20 03 2015].

[5] Kimberly Heu, „Vulnerability Exploits and Countermeasures: The Ping of Death“ 2001. [Tinkle]. Available: http://pearl.ics.hawaii.edu/~sugihara/courses/ics426f09/AssignmentReports/assign4_report2_PingOfDeath.pdf [Kreiptasi 20 03 2015].

[6] M. Bogdanoski, A. Risteski, „Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques, “International Journal of Communication Networks and Information Security, Vol. 3, No. 1, pp. 17-24, 2011 [Tinkle]. Available: http://eprints.ugd.edu.mk/6462/1/__ugd.edu.mk_private_UserFiles_biljana.kosturanova_Desktop_Mitko%20Bogdanoski%20-%20Trudovi%20za%20UGD%20Repozitorium_Telekomunikacii%20-%20Kompjuterski%20Nauki_8.%2065-254-1-PB.pdf [Kreiptasi 20 03 2015].

[7] S. M. Specht, R. B. Lee, „Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures“ 2004. [Tinkle]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.133.4566&rep=rep1&type=pdf [Kreiptasi 20 03 2015].

[8] „Introduction to Riverbed Modeler Academic Edition“. [Tinkle]. Available: http://faculty.winthrop.edu/domanm/csci566/Labs/IntroductiontoModeler.pdf [Kreiptasi 30 04 2015].

[9] Team Cymru, “DDoS Basics”, 2010. [Tinkle]. Available: http://www.team-cymru.com/ReadingRoom/Whitepapers/2010/ddos-basics.pdf [Kreiptasi 30 04 2015].

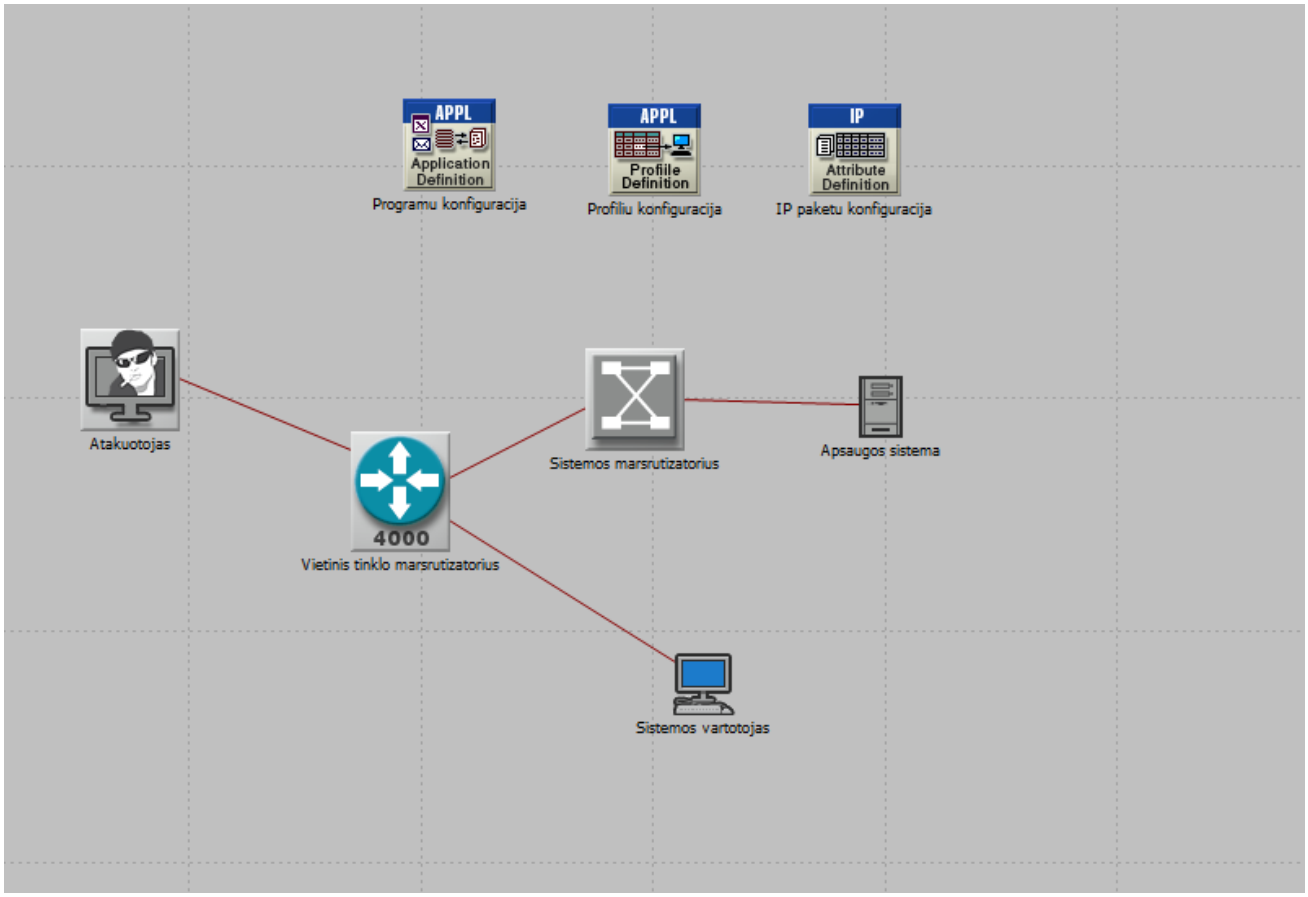
[10] B. Gupta, C. Joshi, and M. Misra. “Distributed Denial of Service Prevention Techniques” IJCEE, vol. 2, no. 3, 2010, pp. 268-276. [Tinkle] Available: http://arxiv.org/ftp/arxiv/papers/1208/1208.3557.pdf [Kreiptasi 01 05 2015].

[11] R. Subramani, "Denial of Service Attacks and Mitigation Techniques: Real Time with Detailed Analysis," 2011. [Tinkle]. Available: http://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764 [Kreiptasi 01 05 2015].

[12] F. Gont, “rfc5927: ICMP Attacks against TCP, July 2010. [Tinkle]. Available: https://tools.ietf.org/html/rfc5927 [Kreiptasi 05 05 2015].

**PRIEDAI**

# 1 priedas. Patalpų apsaugos sistemos vietiniame tinkle vaizdas, sumodeliuotas „Riverbed Modeler“ aplinkoje



**2 priedas. Patalpų apsaugos sistemos tarpmiestinio tinklo modelio vaizdas, sumodeliuotas „Riverbed Modeler“ aplinkoje**