KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ TINKLŲ KATEDRA

Artūras Aputis

DDoS (DISTRIBUTED DENIAL OF SERVICE) ATAKŲ ATRĖMIMO ALGORITMŲ TYRIMAS IR MODELIAVIMAS

Magistro darbas

Darbo vadovas
lekt. dr. Dangis Rimkus

Kaunas, 2012

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ TINKLŲ KATEDRA

Artūras Aputis

DDoS (DISTRIBUTED DENIAL OF SERVICE) ATAKŲ ATRĖMIMO ALGORITMŲ TYRIMAS IR MODELIAVIMAS

Magistro darbas

Recenzentas

doc.dr. Rimantas Kavaliūnas
2012-05-

Vadovas

lekt. dr. Dangis Rimkus
2012-05-

Atliko
IFN-0/3 gr.stud.
Artūras Aputis
2012-05-

Kaunas, 2012

TURINYS

DDoS (DISTRIBUTED DENIAL OF SERVICE) ATAKŲ ATRĖMIMO ALGORITMŲ TYRIMAS IR MODELIAVIMAS

SANTRAUKA

Šiuo metu yra sukurta nemažai priemonių aptikti įvairiausias DDoS atakas, tačiau siekiant sustabdyti arba bent sušvelninti DDoS atakų poveikį yra nuveikta labai nedaug. Yra labai sunku pasirinkti tinkamą DDoS atakos atrėmimo metodą. DDoS atakų atrėmimo metodų analizė galėtų padėti pasirinkti tinkamiausią metodą.

„*BGP DDoS Diversion“* atakų atrėmimo metodas yra vienas efektyviausių ir mažiausiai kaštų reikalaujantis metodas. Šis metodas įgyvendinamas panaudojant BGP protokolą. Ataka yra atremiama kuomet BGP protokolo pagalba yra paskelbiama tik dalis tinklo. DDoS atakos duomenų srautas tokiu atveju yra nukreipiamas į paskelbtą tinklo dalį, o kita tinklo dalis lieka nepažeista atakos. Interneto paslaugų teikėjai naudodami „*BGP DDoS Diversion“* atrėmimo metodą gali apsaugoti savo tinklą nuo visiško nepasiekiamumo.

Šiame tyrime buvo išnagrinėti DDoS atakų atrėmimo metodai. Išsamiai analizei buvo pasirinktas „*BGP DDoS Diversion“* atrėmimo metodas. Metodo analizei buvo pasirinkta virtuali terpė. Sudaryti virtualią terpę buvo pasirinkta OPNET tinklų modeliavimo programa. Panaudojant OPNET modeliavimo įrangą, buvo sukurtas virtualus tinklas, veikiantis Interneto tinklo pagrindu. Sukurtame tinkle buvo įgyvendintas „*BGP DDoS Diversion“* atakų atrėmimo metodas. Šiame darbe yra pateikta minėto atrėmimo metodo veikimo charakteristikų analizė

Raktažodžiai: DDoS ataka, atrėmimo metodas, OPNET, BGP.

ANALYSIS AND MODELING OF DDoS ATTACK MITIGATION ALGHORITHMS

SUMMARY

Nowadays there are lot of ways how to detect various types of DDoS attacks, but in order to stop, or at least to mitigate the impact of such DDoS attacks not enough work is done. It is very difficult to choose the right DDoS mitigation method. The research of DDoS attacks mitigation can provide a good manual how to choose the most appropriate method.

„*BGP DDoS Diversion"* method is one of the most effective and least cost to deliver DDoS mitigation method. This method is implemented using BGP protocol. BGP diversion mechanism is used to announce a specific part of the provider‘s network to (a part of) the Internet. Announcing a specific part of this network will divert the DDoS traffic and thereby prevent other parts of the provider‘s network becoming unreachable. This gives the provider the ability to continue providing services of the rest of his custumers.

This research was based on analyzing the DDoS mitigation methods. For the better analyzes the „*BGP DDoS Diversion"* method was chosen. To analyze this method the virtual environment was the best way to accomplish this task. OPNET modeler software was chosen to create the virtual environment. Using OPNET the virtual network was created. Virtual network was based on Internet network standards. „*BGP DDoS Diversion"* method was implemented and tested in the virtual network. This research provides the detail analyzes of „*BGP DDoS Diversion"* method.

Key words: DDoS attack, mitigation method, OPNET, BGP

ĮVADAS

Šis darbas buvo pradėtas vadovaujantis ankstesniame tyrime gautais rezultatais. Ankstesniame tyrime buvo atliktas tyrimas kokią galimą įtaką kibernetinės atakos gali padaryti Interneto tinklo infrastruktūrai. Imitavus kibernetines atakas buvo nustatyta tokių kibernetinių atakų įtaką, bei nustatyti pažeidžiamiausi mazgai Interneto tinklo topologijoje [1].

Atlikto tyrimo gauti rezultatai paskatino priimti sprendimą išanalizuoti galimus kibernetinių atakų atrėmimo metodus, bei virtualiai įgyvendinti vieną iš atrėmimo metodų ir atlikti atrėmimo metodo analizę. Šiam tikslui įgyvendinti buvo pasirinkta programinė įrangą OPNET Modeler.

Šiame darbe yra tiriamos DDoS[1] atakos ir tokių atakų atrėmimo algoritmai. Darbe yra apžvelgiamos DDoS atakos ir jų pasireiškimo tipai, taip pat supažindinama su DDoS atakų aptikimo priemonėmis, bei pateikiami išanalizuoti keli apsaugos būdai, kurie skirti tokių atakų atrėmimui kompiuteriniuose tinkluose.

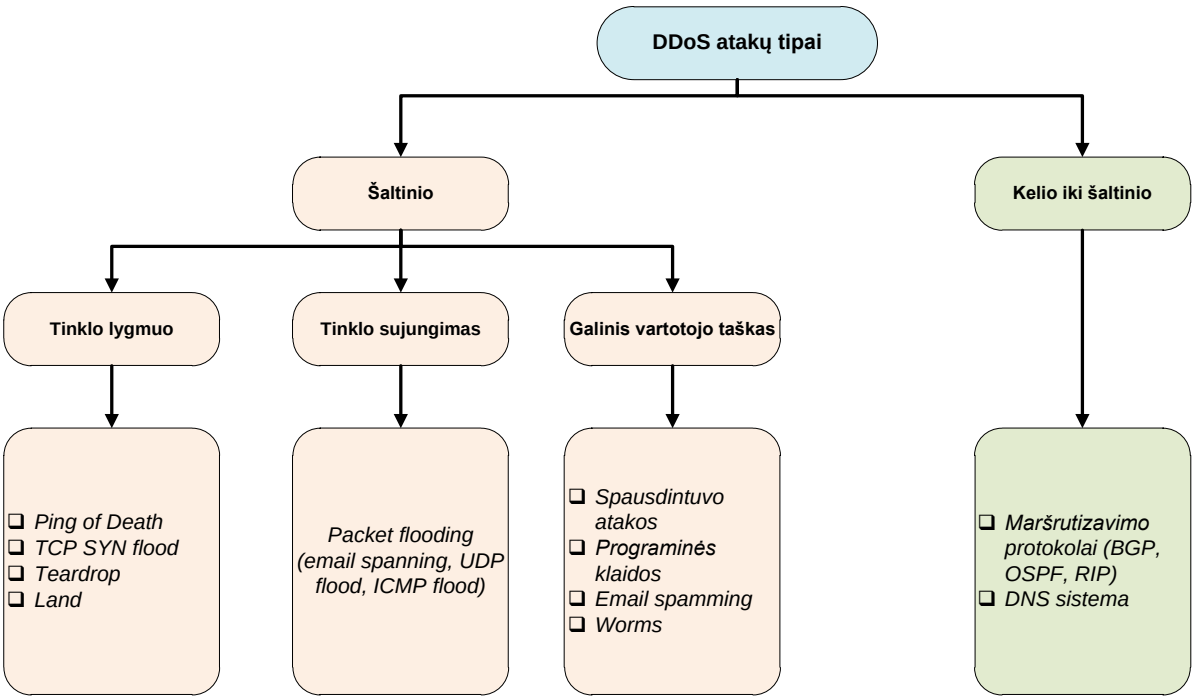
Šiuo metu yra sukurta nemažai priemonių aptikti įvairiausias DDoS atakų rūšis, tačiau siekiant sustabdyti arba bent sušvelninti DDoS atakų poveikį yra nuveikta labai nedaug. Kompiuterio tinklo vartotojas nežino, ką turėtų daryti ir kaip, kad sušvelnintu DDoS atakų poveiki. Dėl to turėtų būti aiškiau išanalizuotos, palygintos pačios atakos ir metodai kovojant su tokiomis atakomis. Galima pastebėti, kad vis dar nėra sukurtų metodų siekiant atremti tam tikrus DDoS atakų tipus. Dar viena svarbi priežastis, kodėl sunku kovoti prieš DDoS yra ta, kad nėra sukurtos jokios instrukcijos, kaip reikėtų pasirinkti tinkamą metodą atremti DDoS atakas. Kai kurie sukurti atakų atrėmimo mechanizmai nepastebi tam tikros rizikos, nes buvo modeliuojami priimant tam tikras idealias sąlygas [4].

Šio darbo tikslas yra išnagrinėti šiuo metu esančius DDoS atakų atrėmimo algoritmus. Atlikus esančių DDoS atakų atrėmimo algoritmų analizę yra pasirenkamas vienas iš atrėmimo metodų ir perkeliamas į virtualią erdvę. Šiame darbe yra pasirenkamas srauto nukreipimo metodas su „*BGP DDoS Diversion“* įgyvendinimu. Projektui įgyvendinti bus pasitelkta modeliavimo ir tyrimo programa OPNET Modeler. OPNET Modeler programa leidžia detaliai ištirti sukurto atrėmimo algoritmo veiksnumą ir naudingumą esančiame tinkle. Rezultatai bus išanalizuoti ir pateikti grafiniame pavidale.

[1] DDoS (Destributed denial of service) - paskirstyta atkirtimo nuo paslaugos ataka. Atakos tikslas - paveikti kompiuterinę sistemą arba tinklą taip, kad kompiuterinės paslaugos taptų neprieinamos vartotojams.

1. DDoS ATAKŲ TIPAI

Norint atlikti tinkamą DDoS atakų atrėmimo algoritmų analizę yra būtina susipažinti su pačiomis DDoS atakomis, jų tipais bei pasireiškimo būdais. DDoS atakų yra įvairiausių tipų todėl tikslinga yra tas atakas suskirstyti į šaltinio ir kelio iki šaltinio atakas.



1.1. pav. *DDoS atakų suskirstymo schema*

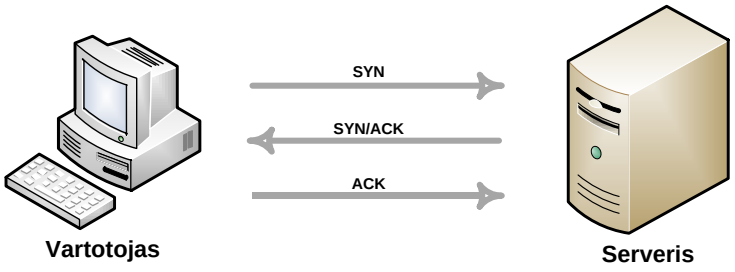
Šaltinio atakos apibrėžia tokias DDoS atakas kurios yra nukreiptos tiesiogiai į auką, o kelio iki šaltinio atakos apibrėžia tokias atakas, kurios paveikia patį kelią iki aukos, nukreipdama arba blokuodama keliaujantį srautą. Šaltinio lygmenyje yra trys papildomos skiltys, tai tinklo lygmuo, kuriame atakos rengiamos išnaudojant tam tikrus protokolus. Tinklo sujungimo lygmeniui priklauso atakos kurios išnaudoja aukos sujungimo pralaidumą. Galinio vartotojo taško lygmeniui priklauso atakos, kurios išnaudoja aukos sistemos resursus tokius kaip procesoriaus resursai, taip pat priklauso atakos, kurios išnaudoja operacinių sistemų, ar kitos programinės įrangos programines klaidas [5].

Analizuojant šaltinio lygmens DDoS atakas galima būti išskirti kelias pagrindines atakas:

Ping of Death: tai toks atakos būdas, kuomet atakuotojas siunčia aukai daug didesni IP paketą negu leistinas didžiausias paketas 0-65534 baitų. Paketai kurie yra didesni negu

didžiausias MTU[2] yra suskaidomi į mažesnius paketus. Paketai kurie viršija leistina dydi yra atmetami automatiškai. Tačiau auka negali priimti viso paketo tol, kol negaus visų suskaidytų dalių. Visai tai gali sukelti sistemos persipildymą ir priversti sistemą nutraukti darbą ir išsijungti [4].

TCP-SYN ataka: SYN ataka, tai ataka, kuri panaudodama trijų rankų paspaudimo metodą, sutrikdo normalų serverio darbą 1.2 pav. Atakos scenarijus yra vykdomas taip: kuomet serveris gauna SYN prašymą iš vartotojo, jis turi palaikyti dalinai atvira kanalą ir būti „klausytis eilėje“ *(angl. „listen queue“)* būsenoje tam tikra laiko tarpą. Tai leidžia sėkmingai sudaryti sujungimus, net ir su dideliu vėlinimu. Problema yra, kad daugelis sistemų gali palaikyti labai mažą kiekį tokių sujungimų. Atakos rengėjai gali pasinaudoti mažu „listen queue“ ir siųsti labai daug SYN užklausų, bet niekada neatsakyti į serverio išsiunčiama SYN/ACK. Tuo metu serveris privalės laukti iš kliento patvirtinimo. Tai įtakos serverio „listen queue“ greitą užsipildymą ir serveris negalės aptarnauti jokių naujų paraiškų, kol neaptarnaus esančių, arba kol nesibaigs jų aptarnavimui skirtas laikas. Šiuo būdu atakuotojas gali nutraukti serverio darbą ir atitraukti vartotojus nuo norimų paslaugų [4].



1.2. pav. *Trijų rankų paspaudimo metodas*

Packet flooding: tai toks atako būdas kuomet atakuotojas arba daug atakuotojų siunčia aukai labai daug paketų, tokių kaip UDP arba ICMP. Tokios atakos tikslas yra sumažinti aukos ryšio linijos pralaidumą ir tokiu būdu sutrukdyti sujungimo funkcionavimą [4].

Analizuojant kelio iki šaltinio lygmens DDoS atakas galima būti išskirti kelias tokias pagrindines atakas:

Atakos prieš RIP protokolą: pats maršruto parinkimo protokolas RIP nėra saugus. Atakuotojui nėra sunku sukurti klaidingus RIP paketus ir pasiųsti juos į tinklą, tam kad sutrikdyti duomenų kelią iki pasirinktos aukos. Jeigu atakuotojas yra arčiau aukos negu

[2] Maximu transmission unit- didžiausias perdavimo vienetas apibrėžtas baitais, kuris gali būti perduotas tam tikroje tinklo topologijoje

duomenų šaltinis, atakuotojas gali nukreipti duomenų srautą į savo pusę ir tokiu būdų perimti ir galbūt nuskaityti aukos duomenis. RIP protokolo antra versija suteikia autentifikavimo galimybę, tokių būdu yra apsaugomi maršruto parinktuvai nuo RIP paketų iš nežinomų sistemų [4].

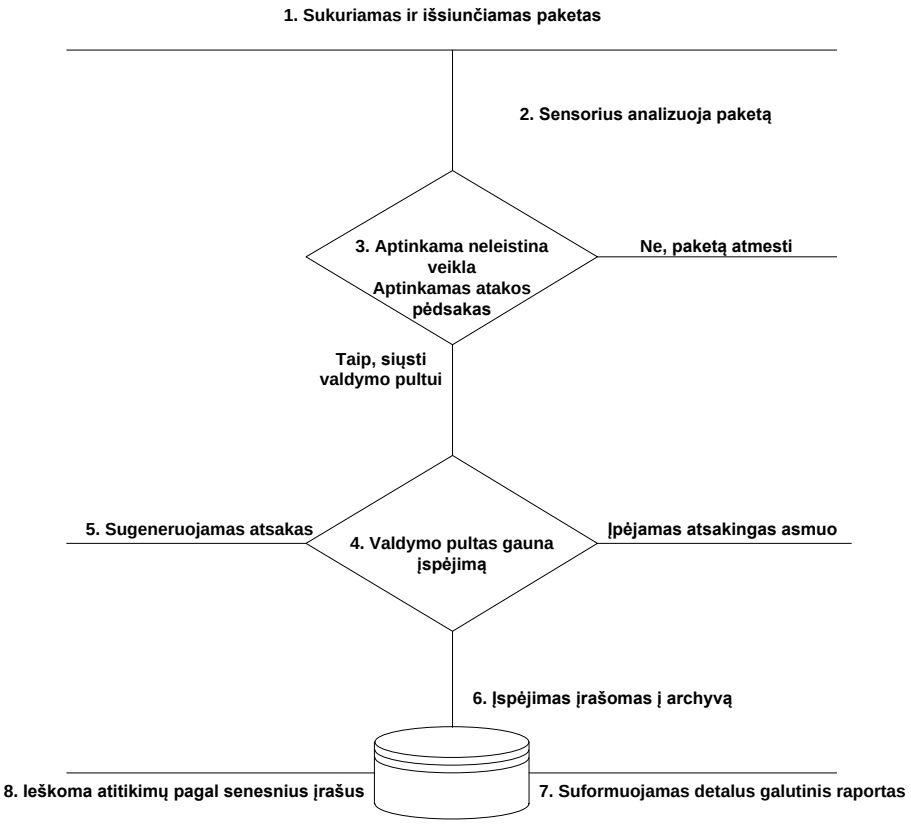
Atakos prieš BGP protokolą: BGP protokolas yra skirtas keistis maršruto parinkimo informacija tarp autonominių sistemų. Autonominė sistema tai grupė tinklų kurie yra kontroliuojami pagal vieną nustatyta tvarką. BGP protokolo architektūra leidžia autonominiai sistemai spręsti, kuriuos maršruto parinkimo kelius priimti, pakeisti ar atmesti. Būtent minėtu BGP protokolo bruožu ir naudojasi atakuotojai, kurie sutrikdo BGP protokolo veikimą, taip užblokuodami arba nukreipdami duomenų srautą iš autoniminių sistemų. Kadangi ryšio seansui BGP naudoja TCP protokolą atakuotojai užgrobia BGP sesija pasinaudodami TCP protokolo architektūros spragomis [4].

Atakos prie DNS sistemą: DNS yra hierarchinė įvardijimo sistema skirta kompiuteriams, ar kitoms sistemoms prijungtoms prie Interneto, ar privataus tinklo. Svarbiausia DNS funkcija, tai paversti žmonėms lengvai suprantamus domenų vardus į skaitmeninį atitikmenį, kuris susijęs su tinklo įrangą. Atakos rengėjai atakuoja DNS sistemos serverius, siekdami sutrikdyti jų funkcionavimą ir taip atitraukti vartotojus nuo paslaugų teikimo.

Šiame skyriuje paanalizavome keletas pagrindinių DDoS atakų tipų. Galima pastebėti, kad šiuo metu vyrauja didelis skaičius įvairiausių DDoS atakų. Kiekvienai tokiai atakai reikia rasti skirtingą atrėmimo mechanizmą. Sekančiame skyriuje panagrinėsime keletas iš galimų atrėmimo mechanizmų.

2. ĮSILAUŽIMUS APTINKANČIOS SISTEMOS (IDS)

Norint atremti DDoS ataką visų pirma ją reikia aptikti ir identifikuoti jos tipą, bei pavojaus lygį. Šiuo metu yra sukurta nemažai atakas aptinkančių sistemų. Atakas aptinkančios sistemos veikia rinkdamos visus arba pasirinktus srauto paketus. Surinktus paketus IDS analizuoja juos pagal tam tikrus nustatytus metodus ir ieško atakų požymių. Aptikus atakas sistemoje, IDS skelbia aliarmą ir įspėja sistemą apie pavojų. 2.1 paveiksle yra pavaizduotas IDS veikimo principas [6].



2.1. pav. *IDS proceso principas*

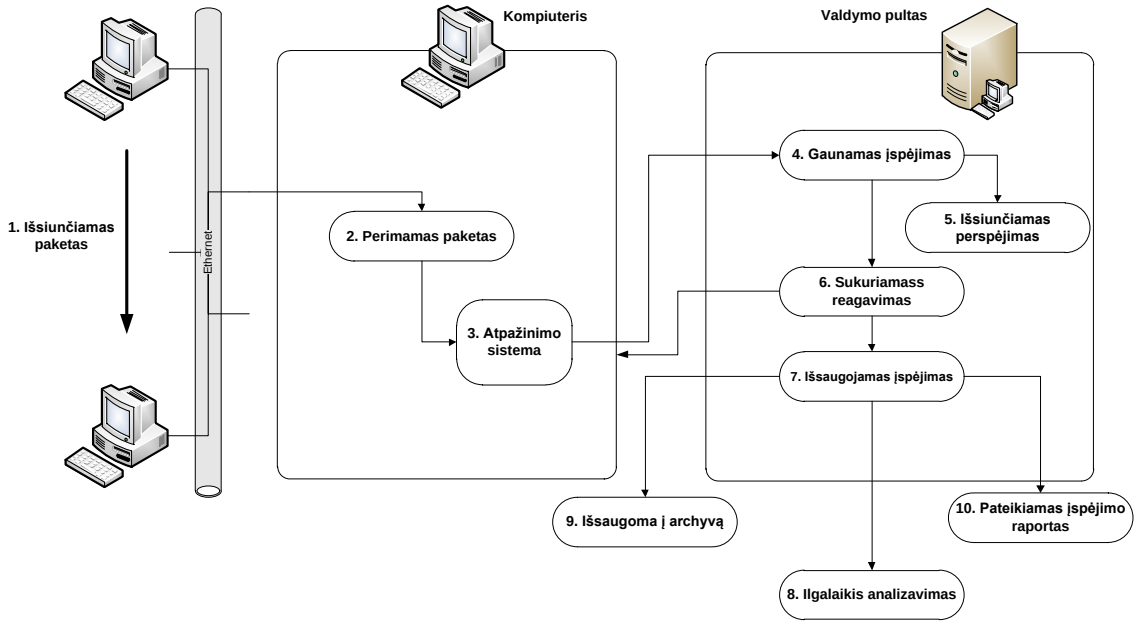
Keletas IDS tipų egzistuoja, kurie yra naudojami apsisaugant nuo atakų. Kiekvienas iš tų tipų turi savo trūkumus ir privalumus atsižvelgiant į IDS konfigūravimo sudėtingumą, atakų aptikimą ir kainą. Galima būtų išskirti du pagrindinius IDS tipus, tai programinė *(angl. „software“)* IDS ir IDS kaip visas įtaisas *(angl. „appliance“).* Programinę IDS sudaro vien pati IDS programinė įranga, kuri yra įdiegimą į kompiuterį arba serverį. Galima būtų paminėti šiuo metu populiariausias programines IDS, tai Snort, Aide, Bro, Samhain. Įtaiso IDS sudaro

visiškai atskiras įrenginys su savo programinę įranga, bei tinklo plokštėmis. Žinomiausi įtaiso IDS tai, Cisco ASA, Fortigate, Checkpoint.

IDS yra klasifikuojamos pagal tai ką jos saugo. HIDS tai tokios IDS kurios saugo atskirą kompiuterį. Tokios IDS veikia atskirame kompiuteryje ir užtikrina jo apsaugą. HIDS yra skirtos įvykiams, susijusiems su atskiru kompiuteriu aptikti (pvz., aptikti failų sistemos pakeitimus, neautorizuotus prisijungimus). HIDS disponuoja informacija surinkta ir atskiro kompiuterio. Gali būti įvertinti operacinės sistemos registrai, failų būklė, operacinės sistemos audito įvykių žurnalas *(angl. „log")*, bandymai prisijungti, į pagrindinį kompiuterį ateinantys srautai. HIDS tiria į atskira kompiuterį patenkančius paketus (ypač neautorizuotus susijungimo bandymus su TCP ar UDP prievadais) ir gali nustatyti būsimus prievadų skenavimus. Yra HIDS tyrinėjančių failų sistemos vientisumą. Jos gali nustatyti failų pasikeitimus, kurie operaciniai sistemai gali būti kritiniai. HIDS sistemos yra geros tuo, kad stebi įvykius, vykstančius konkrečiame kompiuteryje, nustato, ar ataka sėkminga, gali tirti šifruotą srautą, taip pat fiksuoja vartotojo prisijungimus, priėjimą prie failo, failų sistemos vientisumą. Tačiau HIDS turi ir nemažai minusų savo veikime. HIDS tenka įdiegti kiekviename kompiuteryje. Jos negali aptikti tinklo skenavimo, ar kitų pažeidimų, kurie aktualūs visam tinklui. Įsilaužus į kompiuterį visa surinkta informacija gali būti sugadinta. Taip pat HIDS naudoja išteklius, skirtus informacijai saugoti ir mažina kompiuterio operacijų vykdymo spartą. Kitą IDS rūšis yra NIDS, tai tinklinės IDS. Tinklines IDS verta paanalizuoti plačiau, nes būtent šiame darbe planuojama naudoti NIDS tinklo skanavimui ir atakų aptikimui tinkle [6].

NIDS stebi tinklo srautus, nagrinėja jo charakteristikas ir praneša apie įtartinus įvykius tinkle. Jeigu yra reikalinga stebėti TCP/IP srautus tinklo IDS yra geriausias sprendimas. NIDS analizuoja paketus keliaujančius laidais, taip pat tinklo įrenginiai, kaip komutatoriai arba maršruto parinktuvai gali būti suprogramuoti siųsti srautus į norima IDS. NIDS diegimas sudėtingas, kai tinkle yra daug perjungiklių, arba kai tinklas labai apkrautas. Tada iškyla paketų analizės problema, išauga įvykių žurnalų *(angl „log")* failai, pasilieka neužfiksuotų įsilaužimų, būna daug klaidingų aliarmo pranešimų. NIDS stebi tinklo srautus, nagrinėja jo charakteristikas ir praneša apie įtartinus įvykius tinkle. Atakos atpažįstamos tinklo saute ieškant žinomų atakų pavyzdžių arba naudojant statistinius, ar algoritminius anomalijos aptikimo metodus. IDS galimybė atpažinti ataką remiasi tuo, kad IDS davikliai gali perimti visą tinklo srautą iš prižiūrimo tinklo ir palyginti kiekvieną paketą su žinomais pavyzdžiais. Šis būdas reikalauja išdėstyti NIDS tokiuose tinklo taškuose, kuriuose visas tinklo srautas gali būti perimamas. Ieškodama sutapimo su atakų pavydžiais, NIDS gali išardyti paketus,

peržiūrėti jų antraštes. NIDS susiduria su sunkumais, kai srautas apsaugomas IPSec, SSL SSH protokolais. Įdiegus NIDS daugelyje tinklo vietų, galima tiksliau atpažinti anomalijas. NIDS reikia nedaug tinklo išteklių. Įsilaužėlis jas sunkiai randa, o jos gali aptikti prievadų skenavimą, tikrinti, ar nekenksmingi paketai, patenkantys į žinomas prievadus (pvz., http 80 prievadą), taip pat identifikuoti įvairias adresų pakeitimo atakas. NIDS nesusijusios su operacinėmis sistemomis. Įprastos konstrukcijos NIDS naudoja tinkle sensorius. Sensorius dažniausiai yra tinklinis įrenginys, kuriame yra įdiegta IDS programinė įranga, dažnu atveju tai būna visiškai atskiras tinklo įrenginys. Minėtas tinklo įrenginys (sensorius) turi atskiras tinklo plokštes, bei įdiegta programinę įrangą, kuri gali būti naudojama perimti paketus. Tinklinės NIDS veikimo principą geriausiai galima paaiškinti tradicinių NIDS veikimo pavydžiu 2.2 pav. [6].

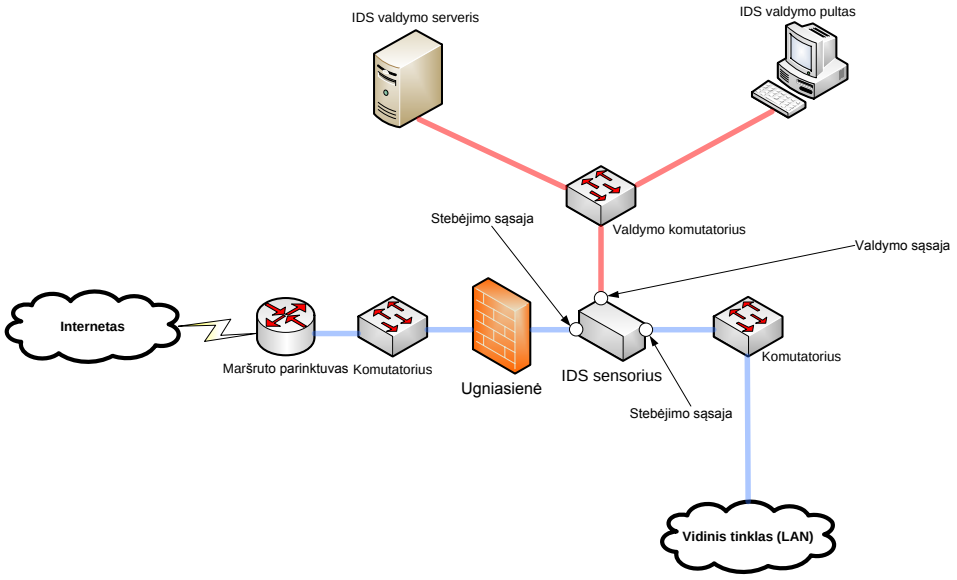


2.2. pav. *NIDS veikimo principas*

1. Duomenų paketas tinkle yra išsiunčiamas iš vieno kompiuterio į kitą (tai gali būti atėjęs paketas iš Interneto ir patekęs į ugniasienę).
2. Paketas realiu laiku sensoriaus pagalba yra perimamas iš komunikuojančių pusių.
3. Paketas yra persiunčiamas į atpažinimo sistemą ir yra analizuojamas pagal žinomus atakos požymius.
4. Jeigu yra atpažįstama ataka yra sukuriamas įspėjimas ir nusiunčiamas į valdymo pultą.
5. Specialistas atsakingas už tinklo saugumą yra informuojamas apie pasireiškusią ataką.
6. Yra sukuriamas atsakas į ataką. Veiksmas atremti ataką yra sukurtas saugumo specialistų komandos ir išsaugotas valdymo pulte.

7. Įspėjimas yra išsaugomas tolimesniam analizavimui.

8. Ilgalaikis analizavimas yra skirtas išsiaiškinti, ar ši ataka nėra dalis didesnės atakos.



2.3. pav. *Tipinis NIDS jungimas tinkle*

Visos įsilaužimo aptikimo sistemos naudoja du pagrindinius atakų atpažinimo metodus. Pirmasis metodas, tai atakų aptikimas pagal žinomus atakų požymius *(angl. „Signature-Based Detection“)*. IDS remiasi audito įrašais, kuriuos generuoja operacinė sistema, maršruto parinktuvų programinė įranga, ugniasienės, ar taikomosios programos. Toks būdas yra labai efektyvus naudojant žinomoms atakoms aptikti, tačiau gimus naujai atakai, tokia sistema jos negalėtų aptiki, tol kol nebus atnaujinta IDS atakų duomenų bazė. Antrasis metodas atakų aptikimo remiasi užfiksuojant norminius darbo profilius *(angl „Anomaly-Bases Detection“),* kurie atspindi tiek sistemos darbą, tiek vartotojo elgesį. Vartotojų profiliai nusako tipines užklausas, tipinius vartotojo veiksmus sistemoje, jų prisijungimą, sesijos trukmę. Sistemos profiliai apibrėžia mažiausius ir didžiausius apkrovimus, jos tipinę darbo charakteristiką (CPU apkrautumą, mainų intensyvumą, diskinės erdvės išnaudojimą). Anomalijos detektoriai nuolat seka elgsenos nukrypimus nuo normalaus profilio. Šie metodai leidžia aptikti naujas, nežinomas atakas ir panaudoti surinktą informaciją nusakant naujos atakos požymius [6].

Prieš sustiprinat saugumo lygį tinkle panaudojus IDS, būtina detaliai išanalizuoti savo sistemą, kurioje bus taikoma IDS. Išanalizavus sistemą būtina atsižvelgi į esančias IDS ir jos parametrus. Tik tais pasirinkus tinkamą IDS tipą ir jos parametrus galima pasiekti norimo tinklo saugumo lygį.

3. DDoS ATAKŲ ATRĖMIMO ALGORITMŲ ANALIZĖ

Kaip jau buvo minėta šiuo metu egzistuoja labai daug būdų kaip aptikti ataką, tačiau labai mažai yra padaryti siekiant atremti aptiktą ataką. Sprendžiant tokią bėda yra labai svarbu išanalizuoti esančius atakos atrėmimo metodus, rasti jų privalumus ir trūkumus, suskirstyti juos pagal atakas, pagal atakos atrėmimo būdus. Geras atakų atrėmimo algoritmų supratimas leidžia juos panaudoti efektyviau. Taip pat susipažinus su atakų atrėmimo algoritmų trūkumais galima sukurti naują idėją, kaip būtu galima patobulinti esamą atrėmimo metodą. Informacija apie tam tikrų DDoS atakų atmainų atrėmimo algoritmus egzistuoja, tačiau visai tai tik aprašyta popieriuje, neviskas yra išbandyta ir naudojama [5].

DDoS atakų atrėmimo algoritmus galima būtų išskirstyti į keletą tipų, pagal tai, kokias priemones ir būdus jie naudoja atremti tam tikrai DDoS atakai:

- Atsekimas
- Sulaikymas
- Perkonfigūravimas
- Nukreipimas
- Srauto apribojimas
- Duomenų kanalo pralaidumo padidinimas
- TCP/UDP blokavimas
- BGP maršrutų skelbimo sustabdymas

3.1. Atsekimas

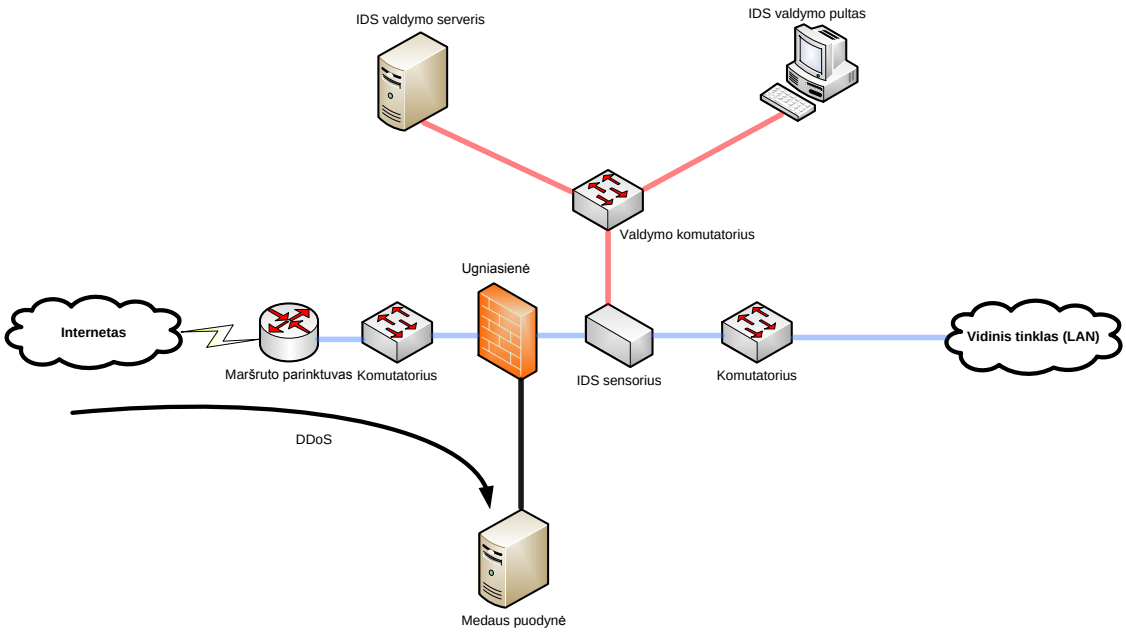
Kaip žinoma IP paketą sudaro šaltinio adresas ir gavėjo adresas. Gavėjo adresas yra reikalingas maršruto parinkimo sistemai pristatyti paketą. IP tinkluose siuntėjo adresas nėra autentifikuojamas IP paketuose, todėl tokioje IP sistemoje labai sunku identifikuoti siuntėjo adresą. Tokia spraga sistemoje būtent ir išnaudoja atakuotojai, surengdami DDoS ataką, suklastojus IP adresą. Pėdsakų ieškojimo mechanizmas buvo sukurtas siekiant atsekti tikrą atakos šaltinį. Taip pat šis metodas yra naudingas siekiant sustabdyti ataką, kuo arčiau jos židinio. Yra keletas atsekimo tipų. IP įrašų schema *(angl. „IP logging scheme“)* - kuomet tinkle esantys maršruto parinktuvai įrašinėja kiekvieną praėjusį IP paketą. IP žymėjimo (angl. „IP marking“) būdas pagrįstas tuo, kad tarpiniai maršruto parinktuvai pažymį IP paketus pridėdami papildomą informaciją, tokiu būdų auka gali pasinaudodama tokia informacija nustatyti atakos kelią ir ją sustabdyti. ICMP *(angl. „ICMP traceback“)* atsekimo mechanizme,

yra sukuriamas naujas ICMP žinutės tipas *(angl. „ICMP Traceback“)*. Ši žinutė palaiko informaciją apie IP paketo pasirinktus kelius. Pasinaudojus šios žinutės informacija yra sužinomas kelias iki atakos šaltinio [5].

Visos šios paminėtos atsekimo sistemos reikalauja, didelio jų paplitimo Internete esančiuose maršruto parinktuvuose. Taip būtų sudarytos sąlygos bendradarbiavimui tarp maršruto parinktuvų, kurie yra administruojami skirtingų sistemų. Kol šis metodas nebus standartizuotas, užtruks nemažai laiko, kol bus pradėta naudoti tokia DDoS atrėmimo schema [5].

3.2. Sulaikymas

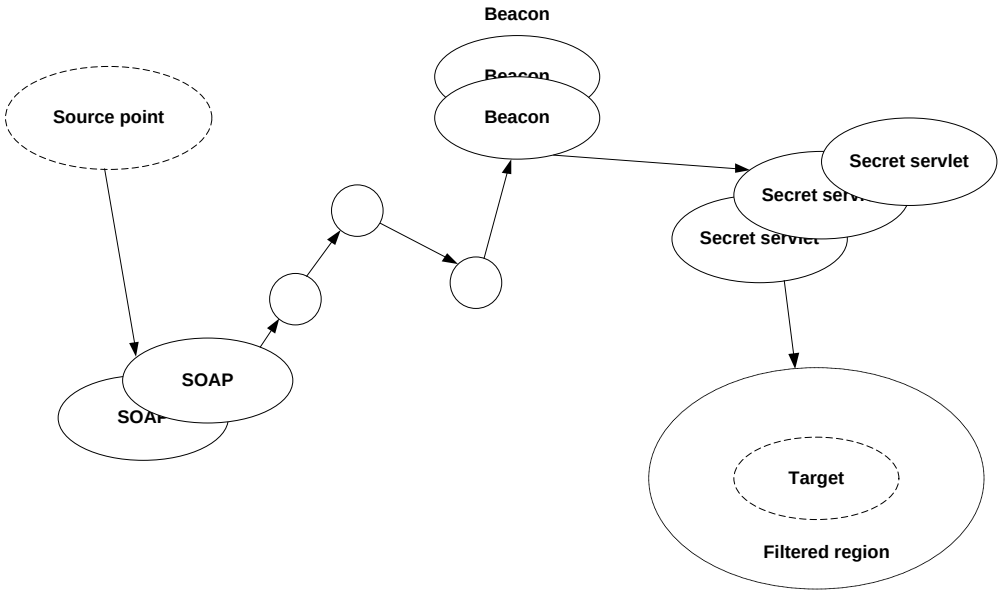
Medaus puodynės *(angl. „Honeypots“)* yra tokios sistemos, kuriuose yra paliktas labai mažas saugumo lygis, kad būtų galima sugundyti atakuotoją. Toks būdas nukreiptų atakuotoją kėsintis į medaus puodynę, o ne į pagrindinę sistemą ir tokiu būdų būtų sulaikyta ataka. Medaus puodynė yra naudojama ne tik kaip spąstai atakuotojui, tačiau ji yra panaudojama analizuoti atakoms, surinkti atakos naudojamus įrankius ir atakuotojo elgsenai. Medaus puodynės tikslas yra priversti atakuotoją įdiegti savo atakos kodą. Tokiu būdų galima išanalizuoti kodą ir rasti sprendimą, kaip užkirsti kelią tokiai atakai. Vienas iš būdų atremti DDoS ataką pagrįstas tuo, kad kuomet tinkle yra aptinkama ataka, ta ataka yra nukreipiama tiesiogiai į medaus puodynę, tokiu būdų yra sustabdomas atakos poveikis, o medaus puodynėje atėjęs srautas yra analizuojamas ir yra nusprendžiama kokių tolimesnių veiksmų reikia imtis [5].



3.1. pav. *Medaus puodynės jungimas tinkle*

3.3. Perkonfigūravimas

Perkonfigūravimo mechanizmas veikia pakeisdamas aukos arba tam tikro tinklo topologiją. Tokiu būdu DDoS atakos metu yra paslepiamas kelias iki aukos ir tam tikros sistemos. Vienas iš tokių atakos atrėmimo algoritmų yra SOS *(angl. „Secure Overlay Services")* 3.3 pav. Šis algoritmas yra naudojamas apsaugoti nurodytus taškus nuo DDoS atakų.



3.2. pav. *SOS algoritmas*

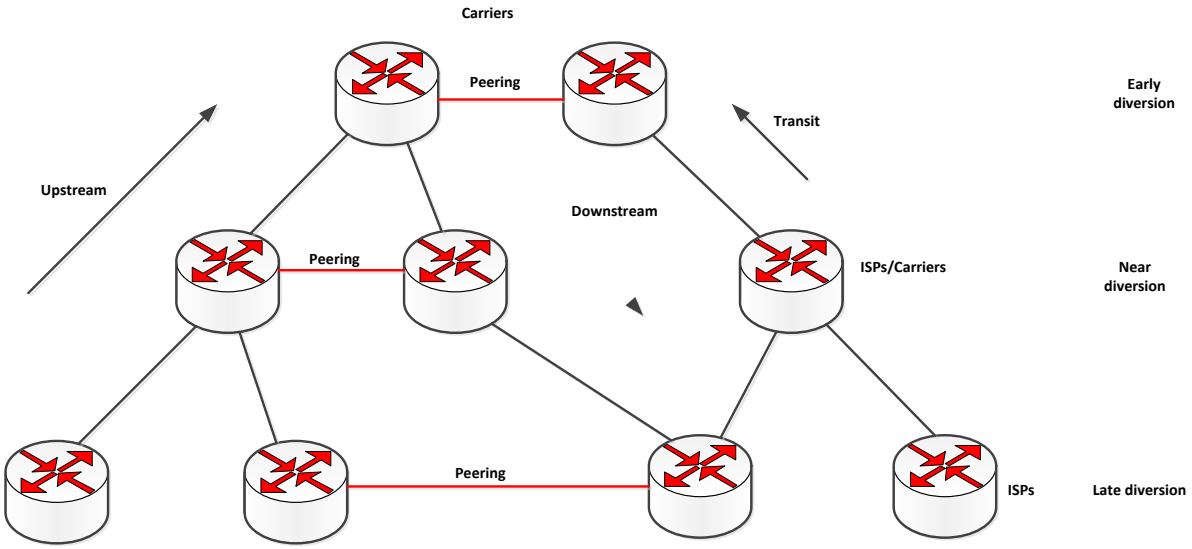
Perdengti patekimo į tinklą taškai SOAP atlieka autentifikacijos patikrinimą ir leidžia tik teisėtą patekimą į tinklą. SOAP apskaičiuoja ir įvertina į kurį Beacon persiųsti srautą. Toliau Beacon nusprendžia į kurį Secret servet nukreipti srautą. Beacon ir Secret servet tinkle yra laikomi slaptai nuo komunikuojančių pusių. Tinkle esanti auka, ar sistema yra apsaugota tam tikrais filtrais, kurie praleidžia srautą tik iš Secret servet [5].

Toks topologijos nepastovumas ir anonimiškumas yra pagrindinis šio algoritmo variklis. Visa tai padeda atremti DDoS ataką, sudarant sunkumus atakuotojui nustatyti kelią iki aukos. Kelių perteklius taip pat padeda paslėpti Beacon ir Secret servet buvimą. Tokį algoritmą yra sunku naudoti dėl to, kad reikia sukurti persidengiantį tinklą ir tam panaudoti sudėtingą Chord maršruto parinkimo algoritmą. Taip pat atakuotojų taikiniu gali patapti Beacon ir Secret servet, dėl to reikia turėti labai didelį skaičių Beacon ir Secret servet. Apkrautus taškus tokiu atveju bus galima pakeisti kitais [5].

3.4. Nukreipimas

Nukreipimas tai toks mechanizmas, kuomet aptikta ataka yra nukreipiama į kitą tam tikrą tašką. Interneto paslaugų tiekėjai dažnai naudoja vadinamąsias *„Juodąsias skyles“*[3]. Kuomet yra aptinkama ataka tai atakos srautas yra nukreipiamas į minėtas *„Juodąsias skyles“*. Atakos metu yra sukuriamas statinis kelio parinkimas į *„Juodąją skylę“* , tokiu būdų patekęs atakos srautas yra ten sustabdomas ir nutraukiamas. Toks atvejis nėra labai geras, nes paaiškėjus, kad ataka buvo netikra yra prarandamas duomenų perdavimas. Todėl geriau naudoti papildomas priemones, kad nukreiptas srautas nebūtų nutraukiamas iškart, bet galbūt persiunčiamas į kitą sistemą, kuri galėtų tą srautą išanalizuoti ir nuspręsti, ką su juo daryti toliau [5].

Vienas iš srauto nukreipimo metodų, kuris yra aktualus šiam darbui yra *„BGP DDoS Diversion“* metodas. Naudojant minėtą atrėmimo algoritmą Interneto paslaugų teikėjai gali apsaugoti savo tinklus nuo DDoS atakų poveikio. Metodo veikimas pagrįstas srauto nukreipimu į realiai neegzistuojantį tinklą. Galimi keli srauto nukreipimo lygiai:



3.3. pav. *Srauto nukreipimo lygiai*

Ankstyvasis nukreipimas *(angl. „Early diversion“)*- tai srauto nukreipimas aukščiausiame lygmenyje. Srauto nukreipimas šiame lygmenyje yra naudingas nes DDoS ataka yra sustabdoma arčiausiame kelyje ir į žemiau esančius lygmenys ji nepatenka

[3] Juodoji skylė- tai tinklo vieta, kurioje atėjęs duomenų srautas yra nutraukiamas, neįspėjant šaltinio apie duomenų nutraukimą į paskirties vietą.

Šalutinis nukreipimas *(angl. „Near diversion“)*- tai srauto nukreipimas vidutiniame lygmenyje. Tai reiškia, kad ataka pažeis viršutinius lygmenys, tačiau atakuojamas tinklas išliks nepažeistas, jei jis bus žemesniame lygmenyje

Vėlyvasis nukreipimas *(angl. „Late diversion“)*- tai nukreipimas pačiame žemiausiajame lygmenyje. Tokiu atveju visi aukštesni lygmenys yra pažeidžiami DDoS

Naudojant BGP maršruto parinkimo protokolą galima užtikrinti spartų ir optimalų maršruto parinkimą. Duomenų srautas keliauja tinkle pasikliaudamas BGP protokolo informacija. BGP paskelbia informacija apie galimus maršrutus savo kaimyninėms maršruto parinktuvams, kurie palaiko BGP protokolą. Tokiu būdų kiekvienas tinklas turi pasiekiamumą su kitais tinklais. Kiekvienas vidinis tinklas turi savo dydį, kurį apibudina to tinklo potinklio kaukė, kaip pavyzdžiui /8, /16, /24. Kuomet tinklas yra atakuojamas DDoS ataka, didelis paketų kiekis yra pasiunčiamas į tam tikrą taikinį. Didelis paketų srautas nukreiptas į tam tikrą autonominę sistemą gali ją padaryti nepasiekiama. DDoS ataka generuodama didelį duomenų srautą užpildo autonominės sistemos pagrindinį perdavimo kanalą tol ko autonominė sistema visiškai pranyksta iš Interneto tinklo. Tokios DDoS atakos Interneto paslaugų teikėjams kainuoja didelius pinigus, dėl to Interneto paslaugų teikėjai ieško būdų kaip atremti arba bent sušvelninti tokias DDoS atakas. Vienas iš metodų atremti arba sušvelninti DDoS atakas yras „*BGP DDoS Diversion“* metodas. Naudojant minėtą metodą galima DDoS sukeltą duomenų srautą nukreipti nuo atakuojamojo tinklo dalies. DDoS srautą galima nukreipti ten, kuris jis negali padaryti jokios žalos. BGP protokolo pagalba autonominės sistemos bendrauja tarpusavyje ir keičiasi informacija apie tinklus, kuriuos galima pasiekti per jas. BGP naudoja įvairius geriausio maršruto skaičiavimo algoritmus. Vienas iš svarbiausių veiksnių įtakojantis maršruto kelio pasirinkimą yra kuo tikslesnis duoto tinklo aprašymas. Maršruto parinktuvai visada pasirenka kuo tikslesnį kelią iki tikslo. „*BGP DDoS Diversion”* metodas yra paremtas šiuo principu. „*BGP DDoS Diversion”* metodas nukreipia atakos sukeltą duomenų srautą nuo taikinio paskelbiant labai tiksliai aprašyta tinklą, kuris turi potinklio kaukę su /32 prefiksu. Tokių būdų visas atakos srautas gali būti nukreiptas į vieną konkretų IP adresą [2].

3.5. Srauto apribojimas

Srauto apribojimo mechanizmas yra naudingas tada, kuomet norima sumažinti kenksmingo srauto patekimą į tinklą. Toks atvejis yra geriausiai panaudojamas tada, kuomet labai maža tikimybė, kad pasireiškusi ataka yra kenksminga. Visa tai apsaugo auką nuo visiškos perkrovimo, kurį gali sukelti DDoS. Srauto apribojimo mechanizmas, kuris apsaugo auką nuo DDoS kenksmingo srauto, apribojį tą srautą. Toks mechanizmas naudoja vietinę

atakos detektaciją ir kontroliuoja vietinio maršruto parinktuvo sąsajos srauto parametrus, apribojant ateinančius srautus. Taip mechanizmas pagrįstas bendradarbiavimu su kitais maršruto parinktuvais esančiais virš vietinio maršruto pariktuvo, kurie taip pat galėtų naudojant srauto ribojimo mechanizmą reguliuoti sąsajos srauto parametrus. Tokiu būdų yra apsisaugojama nuo DDoS atakos iki pat jos židinio, tačiau visa tai gali įtakoti ir bendrą srautą, kuris gali būti taip pat apribotas. Tokia schema tinkamiausiai naudoti tada, kuomet tinklas turi kelis duomenų perdavimo kelius. Nes apribojus vieną kelia, duomenų siuntimas gali būti nukreiptas per kitus kelius. Kitu atveju labai sudėtinga apsisaugoti jei ataka yra įgyvendinama iš skirtingų giografinių šaltinių [5].

3.6. Duomenų kanalo pralaidumo padidinimas

Vienas iš brangiausiu metodu apsisaugoti nuo DDoS atakų yra duomenų kanalo pralaidumo didinimas. Padidinant duomenų kanalo pralaidumą galima užsitikrinti, kad visuomet bus turima pakankamai pralaidumo kovojant su DDoS atakomis. Tokiu būdu DDoS atakos sukeltas didelis duomenų srautas turės mažai įtakos tinklo veikimui, nes nebus išnaudojamas visas galimas pralaidumas. Naudojant šį metodą, reikia nusistatyti, kad įprastomis tinklo veikimo sąlygomis pralaidumas neviršytų tam tikros ribos, tarkim 10%. Visas likęs pralaidumas yra panaudojamas kritiniams atvejams, kuomet pasireiškia DDoS ataka. Tokiu būdų galima užsitikrinti, kad DDoS atakos metu bus turima pakankamai pralaidumo, kad tinklas galėtų funkcionuoti įprastomis sąlygomis [5].

Žinoma toks metodas negali pilnai apsaugoti nuo DDoS atakų, nes tinkle esantys kiti įrenginiai lieka neapsaugoti nuo specialiai suformuotų paketų, kurie gali sutrikdyti tinklo įrenginių darbą.

3.7. TCP/UDP blokavimas

Norint sustabdyti DDoS atakas, galima pasitelkti paprasčiausią būdą, tai blokuoti tam tikrus IP adresus. Blokuoti DDoS ataką galima užblokuojant duomenų srautą iš tam tikrų IP adresų, kurių paskirties adresas yra DDoS taikinys. Toks metodas nėra pats efektyviausias nes, DDoS atakos metų duomenų srautas gali atkeliauti iš tūkstančiai skirtingų IP adresų, todėl juos blokuoti yra tikrai sudėtinga. Šių laikų ugniasienės gali atlikti IP adresų blokavimą pagal tai kokiai šaliai priklauso IP adresai, tai iš dalies palengvina DDoS atakos atrėmimą.

Kitas būdas atremti DDoS atakas, tai atlikti duomenų filtravimą pagal prievadus. Tačiau šis metodas nėra efektyvus, nes užblokavus prievadą, per kurį DDoS ataka keliauja, gali būti užblokuota paslauga, kuri taip pat veikia per minėtą prievadą [5].

3.8. BGP maršrutų skelbimo sustabdymas

BGP maršrutų skelbimo sustabdymas, kuomet yra nustojama skelbti tam tikra IP adresų sritis, gali būti naudingas kovojant prieš DDoS atakas. Kuomet Interneto paslaugų teikėjas nustoja skelbti kaimyninėms autonominėms sistemoms savo tinklo IP adresų sritį, globalus maršrutas į tą tinklą yra prarandamas. Yra keli būdai nustoti skelbti savo IP adresų sritį [5]:

Nustoti skelbti DDoS atakos pažeista adresų bloką (pvz. /24), darant prielaidą, kad tik dalis tinklo yra atakuojama.

Nustoti skelbti visą adresų sritį ir pradėti skelbti tik mažas adresų sritis, kurios nėra pažeistos DDoS atakos

3.9. DDoS atakų atrėmimo algoritmų apibendrinimas. Išvados

Palyginimo lentelė suteikia vaizdą, kuriuo vadovaujantis galima pastebėti DDoS atakų atrėmimo metodų gerąsias, ar blogąsias savybes. Pateikti metodai gali būti naudojami atremti DDoS atakas tačiau nei vienas negali užtikrinti, kad bet kokiu atveju DDoS ataka bus atremta, be jokių papildomų nuostolių. Lentelėje pateikti atrėmimo metodai yra įvertinti dešimtbalėje sistemoje, 1 reiškia mažesnę vertę, o 10 didesnę vertę [2].

1 lentelė. *DDoS atakų atrėmimo algoritmų apibendrinimas*

	Kanalo pralaidumo padidinimas	**Sulaikymas**	**Perkonfigūravimas**	**Srauto ribojimas**	**Nukreipimas (BGP Diversion)**	**TCP/UDP blokavimas**	**BGP maršrutų skelbimo sustabdymas**
Įgyvendinimo kaštai	10	6	10	7	3	6	1
Efektyvumas	5	6	6	5	8	7	5
Patikimumas	6	5	7	6	7	6	7
Įgyvendinimo sudėtingumas	9	8	10	7	6	3	8
Lankstumas	3	5	3	3	7	4	8
Tinklo pasiekiamumas	8	5	7	4	9	7	1
Įrenginių pasiekiamumas	8	5	7	4	1	3	1
Bendras naudingumas	3	4	6	3	8	6	6
Veikimo metodas	Visada veikiantis	Rankinis/pagal poreikį	Rankinis/pagal poreikį	Rankinis	Pagal poreikį	Visada veikiantis/pagal poreikį	Pagal poreikį

4. PROBLEMOS SPRENDIMO TIKSLAI IR UŽDAVINIAI

Ankstesnėje darbo dalyje buvo aptarta atliekamo darbo problema. Nors yra nemažai metodų, kaip aptikti vienokią, ar kitokią atakos rūšį, tačiau mažai nuveikta atakos atrėmimo srityje. Šiame tyrime yra norima pademonstruoti ir aptarti atakų atrėmimo veikimo charakteristikas. Darbe išanalizavus DDoS atakų tipus, atakų aptikimo sistemas, bei keletą atrėmimo algoritmų buvo aiškiau suvokta sprendžiama problema. Šiai problemai spręsti buvo pasirinktas sprendimas sukurti virtualų kompiuterinio tinklo modelį OPNET modeliavimo programa su Interneto tinklo topologija. Esančioje topologijoje atlikti DDoS atakų eksperimentus. Kadangi šis tyrimas rėmesi ankstesniu tyrimu gautais rezulatais, buvo nuspręsta nagrynėti atakos atrėmimo metodus Interneto tinkle [1].

Tolimesnei analizei buvo pasirinktas „*BGP DDoS Diversion“* atakų atrėmimo metodas, kuris gali būti įgyvendintas Interneto tinkle. Šis metodas buvo pasirinktas todėl, kad yra vienas iš efektyviausių ir mažiausiai įgyvendinimo kaštų reikalaujantis metodas.

Pagrindinis šio tyrimo tikslas sukurti virtualią aplinką ir įgyvendinti DDoS atakų atrėmimo metodų analizę.

Problemos sprendimui yra iškelti pagrindiniai uždaviniai:

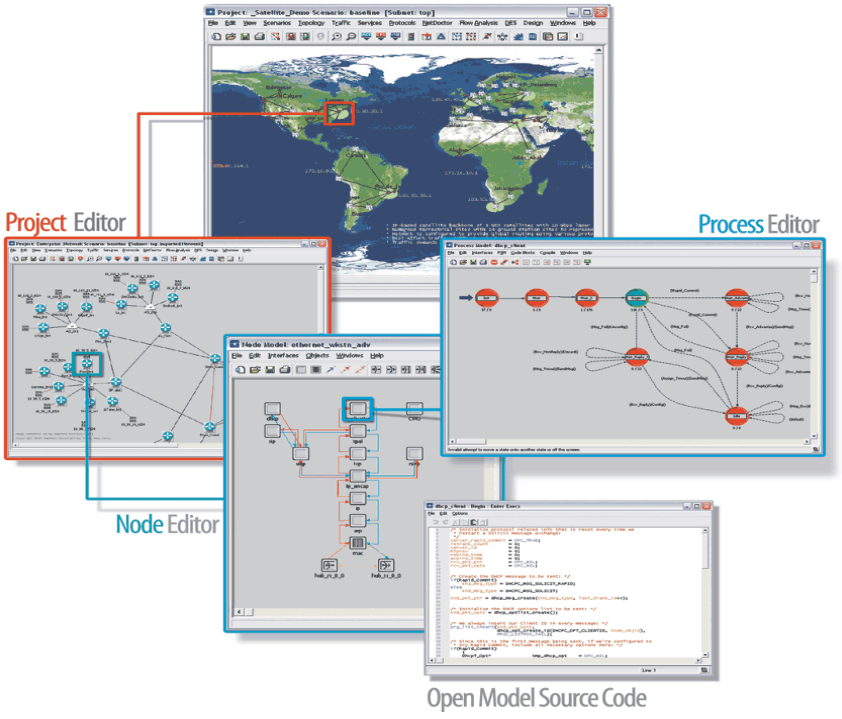
- Suprojektuoti Interneto tinklo topologiją
- Modelyje turi būti sudaryta galimybė imituoti DDoS atakas
- Sukurtame modelyje turi būti galimybė aptikti DDoS atakas
- Sukurtame modelyje turi būti galimybė atremti DDoS atakas
- Sukurtame modelyje būtų galima atlikti išsamią duomenų perdavimo analizę

Apibrėžti problemos sprendimo tikslai ir uždaviniai leis toliau suvokti, kokie galėtų būti sprendimo kūrimo metodai ir priemonės.

5. PROBLEMOS SPRENDIMO KŪRIMO METODAI IR PRIEMONĖS

Pagrindinė priemonė įgyvendinant projektą yra OPNET modeliavimo programa. OPNET modeliavimo įrankis palaiko R&D[4] procesus skirtus analizuoti ir kurti duomenų perdavimo tinklus, tam tikrus įrenginius, protokolus ir aplikacijas. Vartotojas gali analizuoti sukurtus tinklo modelius integruojant naujas technologijas ir stebėti, kaip tai įtakoja galutinius vartotojus. OPNET palaiko daug naujausių technologijų bei protokolų. Taip pat modeliavimo programa palaiko daug modeliavimo aplinkų, suteikiančiu modeliuoti tokias aplinkas kaip [9]:

- TCP
- IP
- VOIP
- OSPF
- MPLS



5.1. Pav. *Opnet modeliavimo įrankio grafinė sąsaja*

Opnet suteikia galimybę atlikti modeliavimą keliomis fazėmis:

- Project editor (galima atlikti pakeitimus viso modelio lygyje)

[4] R&D- tai procesas kuriuo metu yra sukuriami nauji produktai. Daugelis kompanijų naudoja šį procesą išreikšti naujas idėjas ir jas realizuoti, prieš paleidžiant gaminį į rinką.

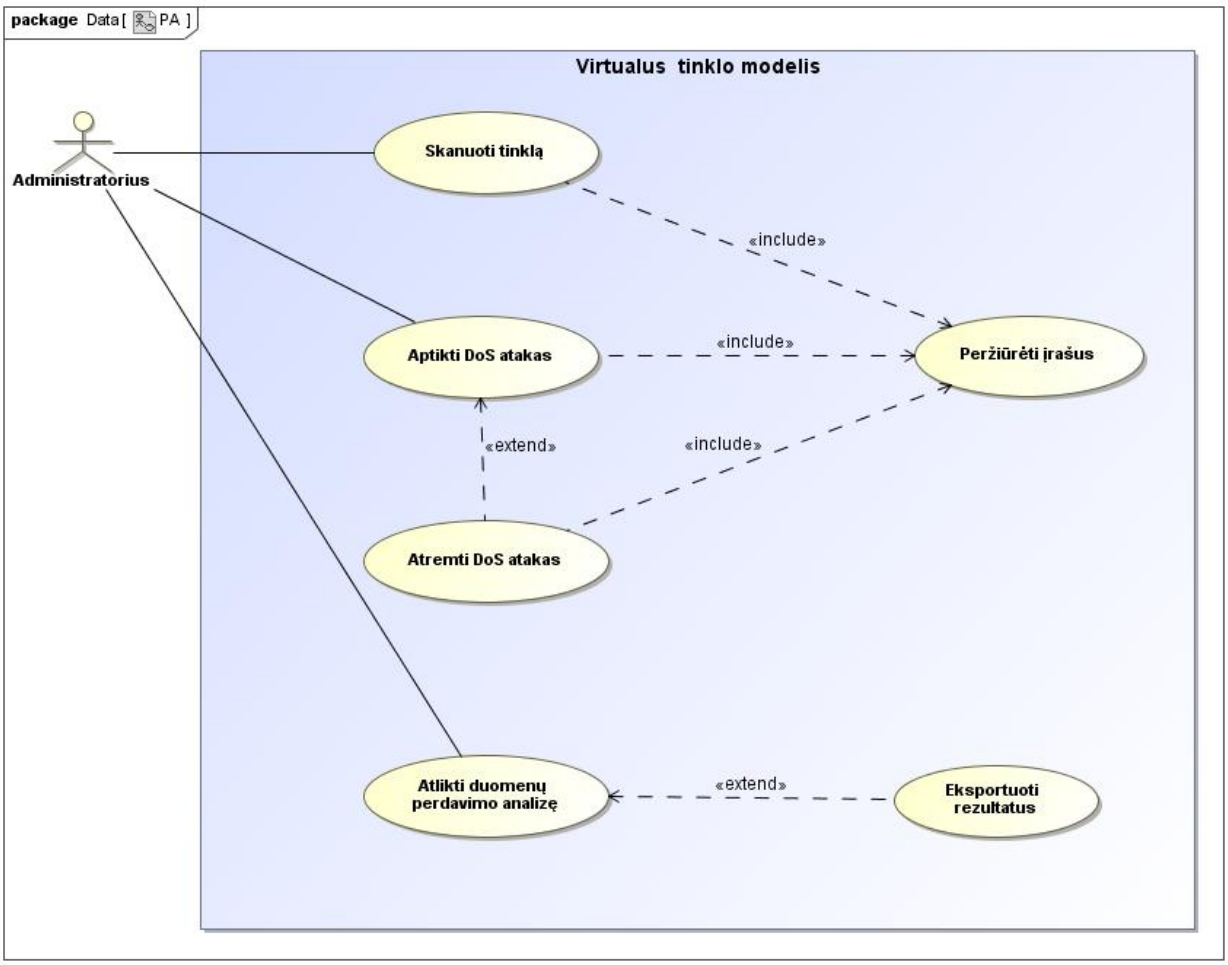
- Node editor (galima atlikti pakeitimus vieno elemento lygyje)
- Process editor (galima atlikti pakeitimus elemente vykstančiuose procesuose)
- Open Model Source Code (galima pakeisto elementų programinį kodą)

Šiame darbe kuriamas modelis bus atliekamas visomis anksčiau minėtomis fazėmis. Naudojant OPNET bus sukuriamas virtualus tinklo modelis. Virtualaus tinklo topologija buvo sudaryta vadovaujantis Interneto tinklo savybėmis. OPNET turi didelę tinklo įrangos duomenų bazę. Galima pasirinkti įvairių gamintojų (Cisco, Juniper, Checkpoint, HP) įrenginius. Kiekvienas įrenginys ir jų modelis turi savita charakteristiką. Projektuojant Interneto tinklo topologiją bus stengiamasi pasirinkti tinklo įrangą tokią, kokia šiuo metu realiai yra naudojama Interneto paslaugų tiekėjų tinkluose.

Sukūrus tinklo topologiją joje bus įgyvendindamas pasirinktas DDoS atrėmimo metodas. Taip pat tinklo topologijoje bus imituota DDoS atakos. OPNET programinis įrankis leidžia atlikti gilią duomenų srautų analizę. Pasitelkus OPNET bus galima surinkti reikalingus duomenų srautų rodiklius, tokius kaip paketų vėlinimas, paketų praradimas, srauto išnaudojimas. Gautus rodiklius OPNET leidžia pateikti grafiškai įvairiais pjūviais, taip pat atlikti palyginimus. Tokia gili analizė sudarys galimybę išsamiai ištirti naudojamą atrėmimo metodą.

6. PROBLEMOS SPRENDIMO FUNKCINIAI IR NEFUNKCINIAI REIKALAVIMAI

Norint tikslingai ir aiškiai apibrėžti problemos sprendimo būsimas funkcijas yra naudojami funkciniai reikalavimai. Daugelis šiuolaikinių sistemų analizės ir projektavimo metodų funkcinių reikalavimų specifikavimui naudoja panaudojimo atvejo modelį[5]. Panaudojimo atvejų modelis yra tapatinamas su panaudojimo atvejų diagrama [14].



***6.1. Pav**. Kuriamos sistemos panaudojimo atvejo diagrama*

Diagrama vaizduoja kokias funkcijos bus įgyvendintos projektuojamame modelyje. Sistema turės vieną vartotoją, šiuo atveju *„Administratorius“*. Vartotojas sistemoje galės atlikti tokius pagrindinius veiksmus:

- Atlikti tinklo duomenų skanavimą

[5] Panaudojimo atvejo modelis – tai sistemos vykdomų transakcijų visuma, kurios paskirtis yra pateikti veiklos dalyviui (angl. „Actor“) pageidaujamą konkretų rezultatą.

- Atlikti DDoS atakų identifikavimą
- Atlikti išsamią duomenų perdavimo analizę

Aptikus DDoS ataką suteikiama papildoma funkcija atremti ataka, taip pat funkcijoms *„Skanuoti tinklą“*, *„Aptikti DoS ataką“* ir *„Atremti DoS ataką“* yra priskiriama papildoma funkcija peržiūrėti įrašus. Funkcijai *„Atlikti duomenų perdavimo analizę“* yra pridėta papildoma funkcija. Leidžianti analizės metu gautus duomenis eksportuoti tolimesniam analizavimui.

Nefunkciniai reikalavimai specifikuoja numatomų sistemos funkcijų (išreikštų per funkcijos reikalavimus) savybes, t.y. apibrėžia kokybines funkcijų charakteristikas. Šiame darbe kuriamai sistemai yra keliami tokie nefunkciniai reikalavimai:

Patikimumui. Sistemos veikimo metu neturi būti prarandami duomenys. Sistema privalo išsaugoti surinktus duomenis. Sukurtas modelis turi veikti, taip kaip aprašytas specifikacijose.

Našumui. Turės būti įvertinta kokius duomenų perdavimo kiekius sistema sugebės apdoroti.

Kokybei. Kokybė supaprastintai reiškia, kad produktas atitinka specifikaciją, todėl sistema turėtų atitikti specifikaciją. Teisingas veikimas – vienas iš svarbiausių sistemos kokybės kriterijų. Sistema turėtų efektyviai ir teisingai veikti.

Panaudojamumui. Turėtų būti įvertinta kokias DDoS atakų rūšis sistema turėtų atpažinti ir atremti.

7. PROJEKTO MODELIO KŪRIMAS

7.1 Modelio sandara

Projekto modelis buvo kuriamas OPNET Modeler 14.5 paketu. Modelio vaizdas OPNET modeliavimo terpėje pavaizduotas 1 priede. Modelis buvo kuriamas vadovaujantis Interneto tinklo veikimo principais. Kadangi Interneto tinklo veikimas yra pagrįstas BGP protokolu, modelyje buvo realizuotas BGP protokolo veikimas. Modeliui sudaryti buvo pasirinkti tokie pagrindiniai elementai esantys OPNET elementų duomenų bazėje:

Autonominės sistemos- Autonominės sistemos modelyje atlieka Interneto paslaugų teikėjų vaidmenį. Autonominėse sistemose yra realizuotas BGP protokolo veikimas. Modelis yra sudarytas iš 7 autonominių sistemų (AS_1, AS_2, AS_3, AS_5, AS_6, AS_7, AS_8), veikiančių BGP protokolu. Autonominę sistemą modelyje atitinka vienas BGP protokolą palaikantys maršruto parinktuvas. Modelyje esančioms autonominėms sistemoms sudaryti buvo pasirinkti Cisco 7609 maršruto parinktuvai palaikantys BGP protokolą. Kiekviena autonominė sistema turi po savo vidinį tinklą.

Vidinis tinklas- Vidinis tinklas yra priklausomas autonominei sistemai. Vidiniame tinkle yra patalpinti įrenginiai kurie gali naudoti įvairius Internetinius resursus (HTTP, FTP, Database). Kiekvienas vidinis tinklas turi savo vartotojų skaičių, bei gali turėti darbines stotis teikiančias Internetines paslaugas (HTTP, FTP, Database). Vidiniai tinklai modelyje yra matomi pavadinimais susijusiais su priklausomybę autonominei sistemai (AS_1_network, AS_2_network, AS_3_network, AS_5_network, AS_6_network, AS_7_network, AS_8_network).

Interneto duomenų srautų apsikeitimo taškas- Modelyje pažymėtas kaip *"IXP"*. Tai vieta kurioje visos modelyje esančios autoniminės sistemos apsikeičia savo BGP maršruto lentelėmis. Kiekviena autonominė sistema prisijungdama prie IXP mato savo kaimynines autonomines sistemas ir gali apsikeisti BGP maršruto lentelėmis. Modelyje IXP funkcionalumui įgyvendinti buvo pasirinktas komutatorius dirbantis L2 lygmenyje.

Paketų analizatoriai- Paketų analizatorius gali skanuoti ir gaudyti paketus, kurie keliauja tame segmente, kur yra įgyvendintas paketų analizatorius. Modelyje yra įgyvendinti du paketų analizatoriai (Packet_analyzer_Nr1, Packet_analyzer_Nr2). Paketų analizatorius (Packet_analyzer_Nr1) yra pajungtas prie IXP ir gali analizuoti visa duomenų srautą keliaujanti per IXP. Pagal surinktus duomenis paketus analizatorius gali paskelbti aliarmą apie esančius neatitikimus tinkle. Paketų analizatorius (Packet_analyzer_Nr2) yra pajungtas tinkle taip, kad galėtų analizuoti paketus, įgyvendinus DDoS atakų atrėmimo metodą.

Aplikacijos ir Profiliai- Aplikacijos ir profiliai modelyje yra reikalingi norint sukurti duomenų srautą tinkle. Aplikacijų modelyje yra aprašoma aplikacija (HTTP, FTP, Email, Database, VoIP). Aprašant aplikaciją galima pasirinkti įvarius šios aplikacijos parametrus. Profilių modelyje yra aprašomi vartotojai kurie naudos šias aplikacijas. Įgyvendinat duomenų srautą modelyje yra aprašomos kelios aplikacijos ir keletas vartotojų tipų.

Modelyje esantys elementai, jų skaičius ir tipas:

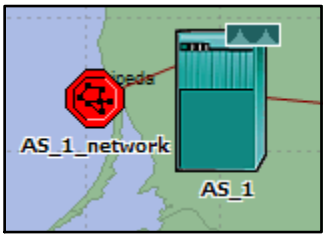
2 lentelė. *OPNET modelyje esantys elementai*

Elementai	Skaičius	Tipas
Maršruto parinktuvai	7	Cisco 7609
Komutatoriai	3	Ethernet
LAN Tinklai	8	LAN Nodes
Darbinės stotys	3	HTTP, FTP, Database
Paketų analizatoriai	2	Packet analyzer
Aplikacijų modelis	1	Application configuration
Profilių modelis	1	Profile configuration
Sujungimai	22	Ethernet (10Mbps, 100Mbps, 1Gbps)

7.2 Modelio konfigūracija

Modelio konfigūracija yra atliekama remiantis Interneto tinko veikimo principais. Modelio konfigūracija turi sudaryti galimybę atlikti analizuojamo DDoS atakų atrėmimo metodo „*BGP DDoS Diversion"* analizę. Tinklo modelyje yra pasirinkta IPv4 tipo adresacija. Modelyje esančių elementų adresacija yra pateikta antrajame priede. Konfigūracija yra pradedama nuo pagrindinių tinklo elementų. Atliekamas autonominių sistemų konfigūravimas.

Autonominės sistemos tinklo modelyje grafinis vaizdas pateiktas 7.1.pav



7.1 pav. *Autonominės sistemos vaizdas OPNET modelyje*

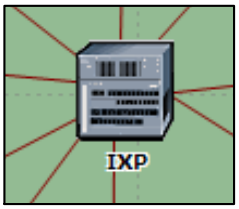
Autonominės sistemos konfigūravimas yra atliekamas pakeičiant jos atributus. Atributų konfigūravimą galima būtų suskirstyti į tokias dalis:

- BGP protokolo aktyvavimas
- Autonominės sistemos numerio priskyrimas
- Maršrutų paskirstymo iš vidinio tinklo į BGP protokolą konfigūravimas
- Kaimyninių autonominių sistemų konfigūravimas
- Sąsajų konfigūravimas

Detalus autonominių sistemų, bei visų kitų elementų konfigūravimas pateiktas trečiame priede.

Kitame žingsnyje yra pridedamas Interneto maršrutų apsikeitimo taškas IXP. IXP šiuo atveju yra L2 lygmens komutatorius. Komutatoriuje papildoma konfigūracija nebuvo atliekama. Kiekvienai autonominei sistemai buvo pridėtą sąsaja su IXP. Sąsajos buvo panaudotos 10BaseT, 100BaseT, 1000BaseX Ethernet technologijos su pralaidumais 10Mbps, 100Mbps, 1000Mbps.

IXP grafinis vaizdas tinklo modelyje 7.2 pav.



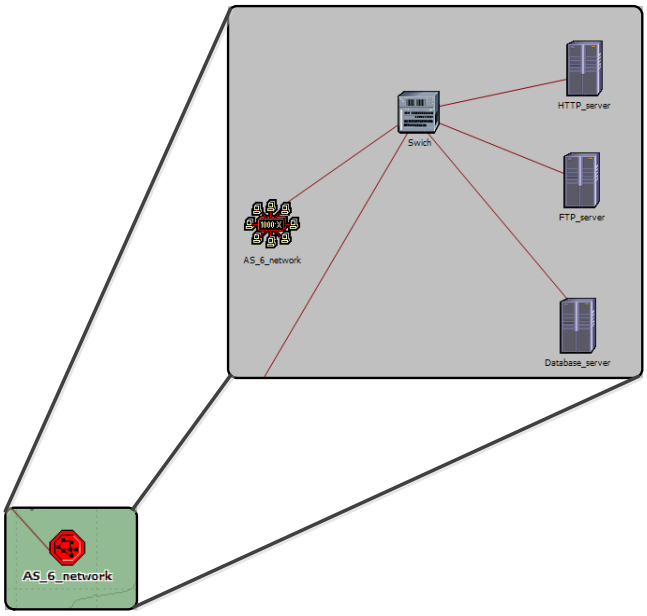
7.2 pav. *IXP vaizdas OPNET modelyje*

Toliau sukonfigūruojamas autonominių sistemų vidinis tinklas. Vidiniame tinkle yra patalpinti vartotojai bei darbinės stotys.

Konfigūravimo etapai:

- Sąsajos sudarymas su autonomine sistema
- IP adreso konfigūravimas sąsajai
- Pagal nutylėjimą maršruto konfigūravimas
- Vartotojų skaičiaus nustatymas

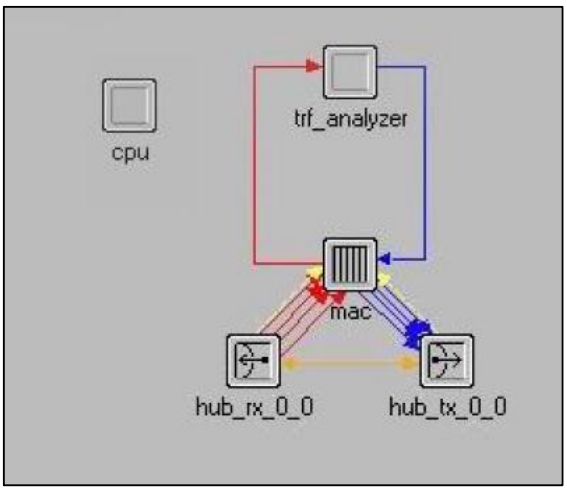
Detali vidinio tinklo konfigūracija pateikta trečiame priede. Vidinio tinklo grafinis vaizdas pateiktas 7.3 pav.



7.3 pav. *Vidinio tinklo vaizdas OPNET modelyje*

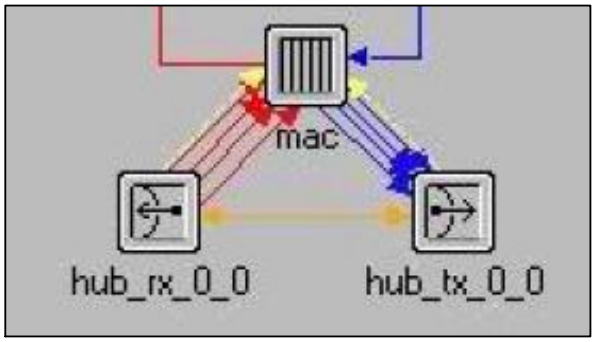
Paketų analizatorius tinklo modelyje veiks kaip atakų aptikimo mechanizmas. Paketų analizatorius yra sukonfigūruojamas, kad skanuotu ir gaudytu paketus. Paketų analizatorius aptikęs kelis kart didesnį paketų skaičių išsiunčia aliarmą autonominei sistemai, kuri bus atsakinga už nukreipimo įgyvendinimą.

Paketų analizatorius struktūra yra padalinta į du modulius. Pirmojo modulio paskirtis yra surinkti visą duomenų srautą keliaujanti tinkle. Antrasis modulis atlieka duomenų analizavimą. Abu šie moduliai pajungti taip, kad matytų duomenų srautą. Paketų analizatoriaus struktūra pavaizduota 7.4.pav. [10].



7.4 pav. *Paketų analizatoriaus struktūros vaizdas OPNET modelyje*

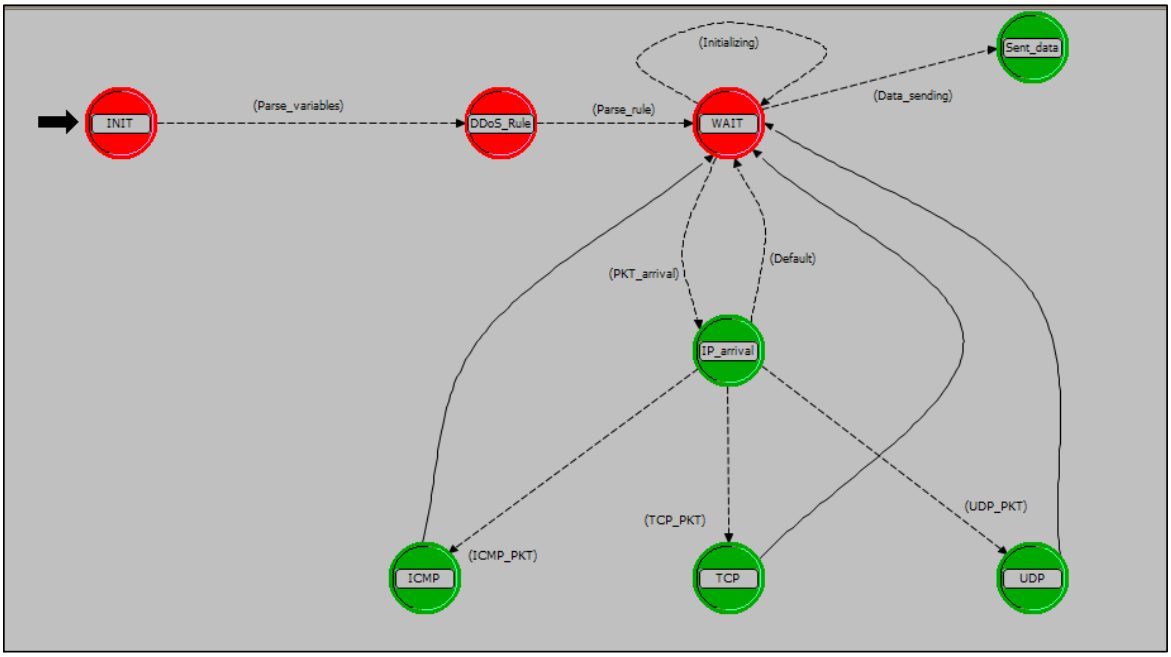
Srauto surinkimo modulis veikia „*Promiscouos mode*“[6] metodu. Jis surenka visa duomenų srautą keliaujanti tinklu, šiuo atveju duomenų srautą iš IXP. Srauto surinkimo modulis susideda iš trijų papildomų modulių: užklausų modulis, siuntimo modulis, gavimo modulis. Siuntimo ir gavimo modulis yra logiškai apjungtas. Minėti du moduliai komunikuoja su išoriniais sujungimais ir užklausų moduliu. Užklausų modulis atlieka surinktų duomenų kaupimą ir valdymą. Užklausų modulis iškviečia „*Ethernet_mac_v2*“ procesą, dėl to paketų analizatorius gali būti patalpintas bet kokiame TCP/IP tinkle. Srauto surinkimo modulis pavaizduotas 7.5 pav. [10].



7.5 pav. *Srauto surinkimo modulio vaizdas OPNET modelyje*

Srauto analizatorius yra atsakingas už DDoS atakų aptikimą. Srauto analizavimo komponentas analizuoja duomenų srautą ir priimą sprendimą apie aptiktą ataką. Šiame modulyje yra įdiegta taisyklė, kuri nusako, pagal kokiu požymius yra aptinkama ataka ir koks veiksmas turi būti atliekamas aptikus ataką. Šis modelis yra aprašomas procesų modelyje. Paketų analizatoriaus procesų modelis yra pavaizduotas 7.6 pav.[10].

[6] Promiscous mode- tai metodas, kuomet visas tinklo duomenų srautas yra nukreipiamas per CPU.



7.6 pav. *Paketų analizatoriaus procesų modelio vaizdas OPNET modelyje*

Šis procesų modelis susideda iš keletos būsenų. Pirminė būsena yra INIT būsena. INIT būsenoje yra vykdoma globalių kintamųjų initializacija. Sekanti būsena DDOS_Rule yra atsakinga už atakų aptikimo taisyklių užkrovimą. Kuomet visos kintamųjų reikšmės yra initializuotos, sistema gali pradėti paketų analizavimą. Pradedant paketų analizavimą sistema pereina į WAIT būseną. Sistema būna WAIT būsenoje tol kol neateina paketas. Atėjus paketui sistema pereina į IP_arrival būseną. IP_arrival būsenoje sistema tikrina ar atėjęs paketas atitinką IP taisyklę. Jeigu IP paketas transportuoja kitus protokolus, sistema pereiną į būsenas: ICMP, TCP, UDP. Sistema nustačiusi, kad paketas, ar paketai atitinka aprašytą taisyklę išsiunčia aliarmą nustatytam šaltiniui [10].

Paketų analizatorius yra sukonfigūruojamas taip, kad skanuotu tik paketus, kurių paskirties adresas nurodytas atakuojamas elementas. Atakos aptikimo taisyklė yra sudaroma tokiu principu:

Visų pirma yra sudaromas tinklo srautas įprastomis sąlygomis ir suskaičiuojamas paketų skaičius, kurių paskirties adresas atakuojamas šaltinis.

Užfiksavus paketų skaičių įprastomis sąlygomis yra aprašoma sąlyga, kuri nusako, kad kuomet paketų skaičius įprastomis sąlygomis yra viršijamas 5 kartus, traktuoti kaip DDoS ataką.

7.3 Modelio testavimas

Atliekant modelio testavimą yra siekiama nustatyti, ar modelio elementai veikia nustatyta tvarka, taip pat siekiama nustatyti tinklo veikimą įprastomis sąlygomis. Tinklo įprasto veikimo

sąlygos yra nustatomos tam, kad įgyvendinus DDoS ataką būtų galima įvertinti atakos poveikį. Tinklo veikimo įprastomis sąlygomis yra sukuriamas nedidelis duomenų srautas, bei išmatuojamos įvairios tinklo charakteristikos. Tinklo veikimo įprastomis sąlygomis metu yra surenkamos tokios tinklo charakteristikos:

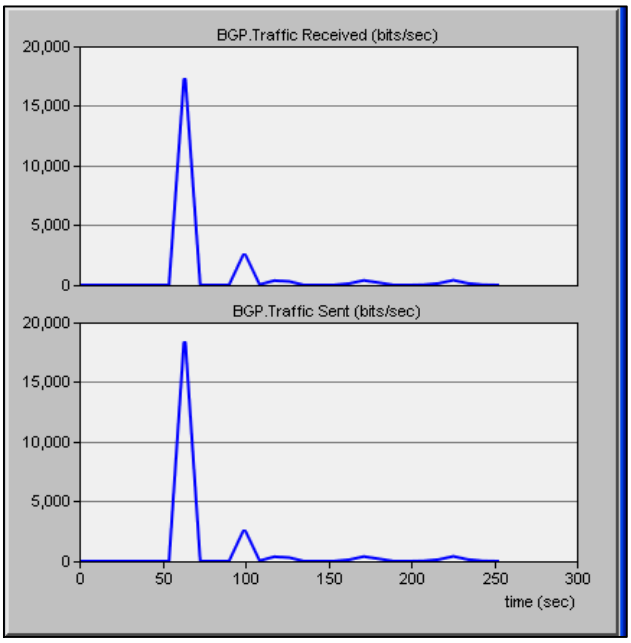
- BGP maršruto lentelės
- BGP duomenų srauto charakteristikos
- Sąsajų pralaidumo charakteristikos
- Paketų vėlinimo charakteristikos
- Paketų praradimo charakteristikos
- HTTP duomenų srauto charakteristikos
- FTP duomenų srauto charakteristikos
- Database duomenų charakteristikos
- TCP duomenų srauto charakteristikos

Surinkus išvardintas charakteristikas ir jas lyginat su charakteristikomis gautomis inicijuojant DDoS ataką, bus galima nuspręsti kokią įtaką daro DDoS ataka tinklo infrastruktūrai.

Tinklo veikimo testavimą galima suskirstyti į etapus:

1. BGP duomenų srauto tinkle matavimas.

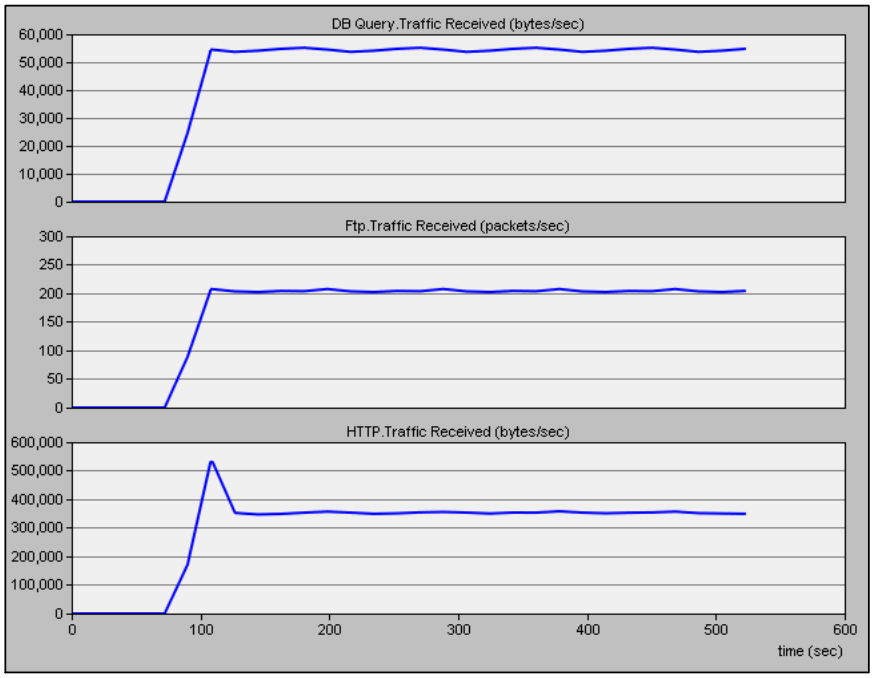
Tinkle yra 7 autonominės sistemos, kurios informacija apie savo vidinių tinklų pasiekiamumą keičiasi naudodamos BGP protokolą. Tinkle funkcionuojantį BGP protokolą nusako 7.7 pav. pateiktas grafikas. Grafike kreivė pirma staigiai šoką į viršų, kas simbolizuoja kad įvyko pirmasis BGP maršrutų apsikeitimas. Toliau kreivės dydis daug mažesnis, nes tinkle tėra perduodami BGP tarnybiniai duomenys.



7.7 pav. *BGP protokolo duomenų srautas tinkle*

BGP maršrutų lentelės pateiktos ketvirtame priede. Analizuojant BGP maršrutų lenteles bus galima nustatyti, ar tinkamai suveikė implementuotas BGP DDoS nukreipimo metodas.

Toliau tinkle patikrinam sukurtų (HTTP, FTP, Database) duomenų srautų charakteristikas.



7.8 pav. *HTTP, FTP, Database duomenų srautas tinkle*

Pagal pateiktame paveiksle 7.8 pav. esančias grafiko kreives galime spręsti apie egzistuojantį duomenų srautą tinkle.

Patikrinus paketų analizatoriaus veikimą, galima pastebėti, kad analizatorius geba stebėti tinkle esantį duomenų srautą. Paketų analizatoriaus ištrauka pateikiama penktajame priede.

7.4 Modelio tyrimas

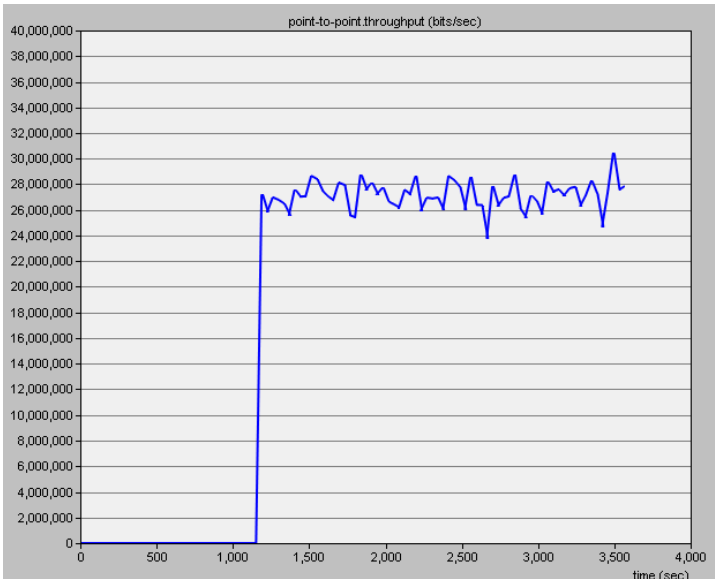
Tiriant suprojektuotą modelį pagrindinis tikslas yra išsiaiškinti, kaip modelyje veikia įgyvendintas DDoS atakų atrėmimo algoritmas. Tyrimo eigą aprašo tokie žingsniai:

- DDoS atakos sukūrimas
- DDoS atakos paleidimas
- Tinklo reakcija į DDoS ataką
- DDoS atakos atrėmimo metodo veikimas
- Tinklo reakcija į DDoS atakos atrėmimą
- Išvados

Norint sukurti DDoS ataką tinkle, reikia visų pirma sukurti didelį vartotojų skaičių ir nukreipti vartotojų užklausas į pasirinktą taikinį. Tinklo modelyje atakos taikiniu buvo pasirinkta darbinė stotis teikianti HTTP paslaugas. Darbinė stotis yra pajungta AS_6 autonominės sistemos vidiniame tinkle. Darbinės stoties pavadinimas yra HTTP_server. HTTP_server darbinės stoties IP adresas yra 192.168.6.2. DDoS atakų šaltiniais buvo pasirinkto keturios autonominės sistemos (AS_1, AS_2, AS_5, AS_8). Kiekviena iš šių autonominių sistemų turi vidinius tinklus, kuriuose yra po 500 kompiuterių. Aplikacijų konfigūravimo modulyje yra sukonfigūruojama HTTP paslauga kurią naudosis visi minėtų autonominių sistemų kompiuteriai. HTTP paslauga sukonfigūruojama tokias parametrais:

- Pavadinimas [DDoS_HTTP]
- Paslauga [HTTP 1.1]
- Laiko tarpas tarp puslapių užklausų [exponential 20s]
- Užklausos dydis [800kbit]
- DDoS atakos pradžia [1200 sekunde arba po 20 minučių nuo simuliacijos pradžios]

Kiekvienos autonominės sistemos tinklas atakos metu sugeneruoja 30Mbps duomenų srautą nukreiptą į HTTP_server darbinę stotį. Kadangi atakuojantys kompiuteriai išsidėstę per kelias autonominės sistemas duomenų srautas sumuojasi ir ataka įgauna DDoS atakos tipą. 7.9 pav. grafikas vaizduoja atakos duomenų srautą.



7.9 pav. *Atakos sukeltas duomenų srautas iš AS_1*

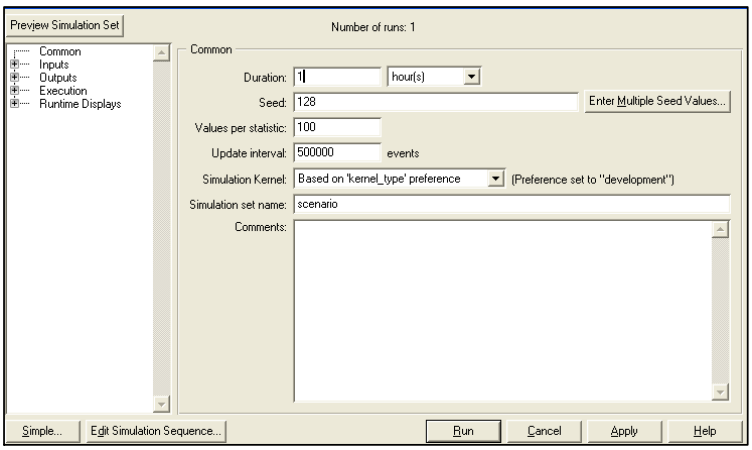
Pagal grafiko kreivę galima pastebėti, kad ataka prasideda 1200 sekundę ir atakos metu duomenų srautas vidutiniškai yra 30Mbps. Viso tinklo simuliacija yra vykdomą vieną valandą. Didesnės trukmės simuliaciją riboja kompiuterio kuriame įdiegta OPNET programa resursai.

Šiame tinklo modelyje yra įgyvendintas *„BGP DDoS Diversion“* atakų atrėmimo metodas. Šis atakų atrėmimo veikimo principas yra aprašytas ankstesniajame šio darbo skyriuje.

Šiame modelyje *„BGP DDoS Diversion“* metodas yra įgyvendintas taip, kad kuomet pasireiškia DDoS ataka, kuri yra nukreipta į HTTP_server darbinę stotį, būtų atliktas šios atakos nukreipimas į IP adresą, kuriame DDoS atakos poveikis nėra svarbus. Tyrimo scenarijų būtų galima aprašyti tokiais žingsniais:

- Sukuriama DDoS ataka kuri nukreipta į HTTP_server IP adresu 192.168.6.2
- Paketų analizatorius skanuoja paketus, kurių paskirties adresas 192.168.6.2
- Paketų analizatorius aptikęs 5 kartus didesnį paketų skaičių negu įprastai, išsiunčia aliarmą autonominei sistemai AS_7
- AS_7 gavusi pranešima paskelbia naują savo BGP maršruto lentelę su nauju įrašu, kad 192.168.6.2/32 tinklas yra pasiekimas per AS_7 su *„Next-hop-self“* parametru, kurio reikšmė 10.10.10.110.
- Atakos duomenų srautas nukreipiamas per 10.10.10.110 mazgą.
- Atlaisvinamas pagrindinis kanalas jungiantis AS_6.
- AS_6 tampa prieinama Interneto tinkle.

Modelio tyrimas prasideda paleidžiant tinklo simuliaciją vienos valandos trukmei 7.10 pav.

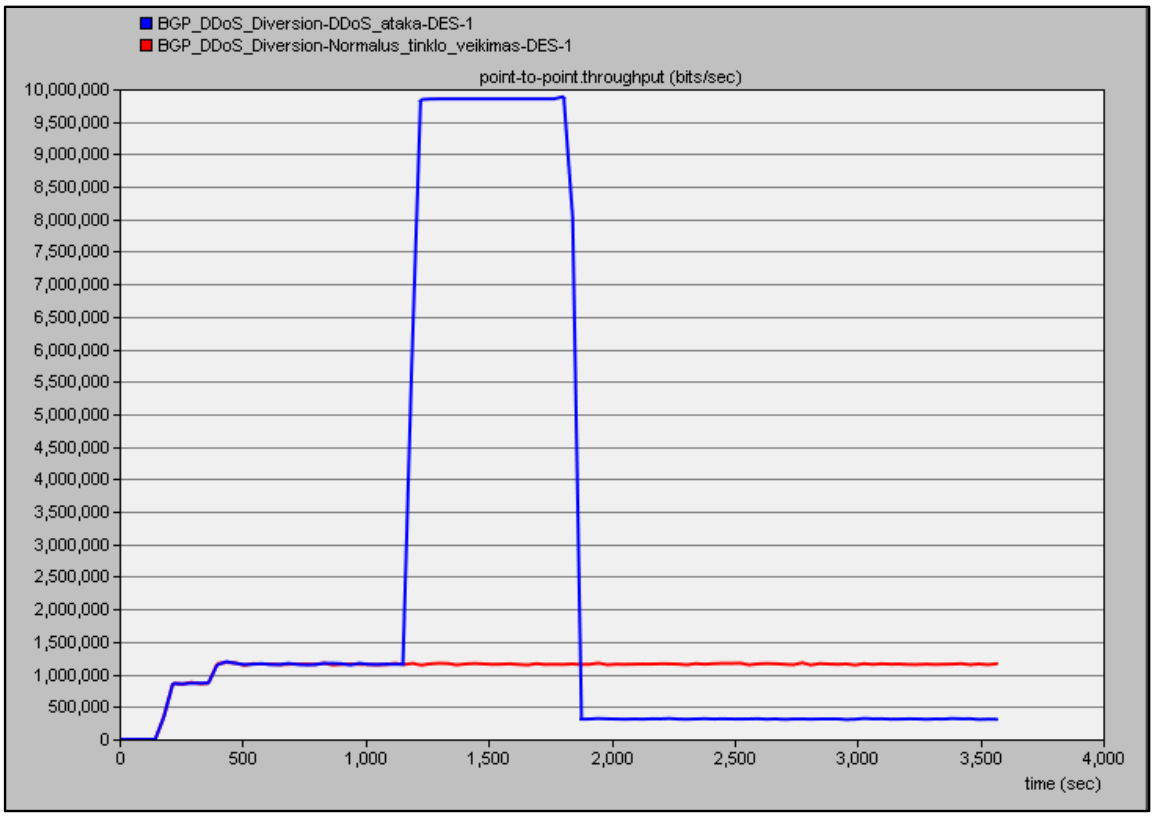


7.10 pav. *Simuliacijos konfigūravimo langas*

Simuliacijos metu bus paleista DDoS ataka ir įvykdomas jos atrėmimas. Simuliacijos metu sistema surinks visus prieš tai nustatytas statistikas. Simuliacijai pasibaigus bus galima peržiūrėti gautas statistikas ir padaryti atitinkamas analizes.

Kuomet simuliacija yra atlikta visų pirma yra peržiūrima sujungimo pralaidumo statistika, nes pagal sujungimo pralaidumo statistika yra galima nustatyti, ar modelyje pasireiškė DDoS ataka ir ar ataka buvo sėkmingai atremta.

DDoS atakos pasireiškimui ir atrėmimui nustatyti yra reikalinga paanalizuoti pagrindinį sujungimą jungianti AS_6 su IXP. AS_6 su IXP jungiantis sujungimas yra Ethernet 10BaseT tipo, tai reiškia sujungimo didžiausias pralaidumas yra 10Mbps . Autonominės sistemos, iš kurių yra kuriamos DDoS atakos, su IXP turi susijungimus Erhernet 100BaseT tipo. Sujungimų didžiausias galimas pralaidumas 100Mbps. 7.11 pav. pateiktas grafikas simbolizuoja AS_6 sujungimo su IXP pralaidumą.



7.11 pav. *AS_6 su IXP sujungimo pralaidumo grafikas*

Grafike pateikta raudona kreivė simbolizuoja duomenų srautą tinko veikimo įprastomis sąlygomis, o mėlyna kreivė simbolizuoja duomenų srautą DDoS atakos metu. Tinklo veikimo įprastomis sąlygomis duomenų srautas susideda iš HTTP, FTP ir Database duomenų srauto. HTTP, FTP ir Database paslaugas teikia AS_6 vidiniame tinkle esančios darbinės stotys, kurių IP atitinkamai yra 192.168.6.2, 192.168.6.20, 192.168.6.50. DDoS atakos metų yra sukuriamas papildomas HTTP duomenų srautas į 192.168.6.2 adresą. Pagal pateiktą grafiką galima pastebėti, kaip 1200 sekundę mėlyna kreivę staigiai šoką į viršų. Toks kreivės pokytis simbolizuoja sukurtos DDoS atakos pasireiškimą. Paketų analizatorius veikia, kaip DDoS aptikimo mechanizmas, kuris 10 minučių renka paketus kurie turi paskirties IP adresą 192.168.6.2. Kuomet paketų skaičius yra viršijamas 5 kartus negu nustatytomis sąlygomis, paketų analizatorius išsiunčia aliarmą autonominei sistemai AS_7 . AS_7 autonominė sistema atnaujina savo BGP maršrutų lentelę su įrašu, kad nuo šiol 192.168.6.2/32 tinklas yra pasiekiamas per AS_7 autonominę sistemą su „*Next-hop-self*“ parametru, kurio reikšmė 10.10.10.110. Toks metodas DDoS ataką nukreiptą į adresą 192.168.6.2, nukreipia į 10.10.10.110 tinklą. Analizuojant 7.11 pav. pateiktą grafiką galima pastebėti kaip 1800 sekundę mėlyna kreivė sumažėja. Toks reiškinys leidžia prieit prie išvados, kad DDoS ataka buvo sėkmingai nukreiptą. Lyginat raudoną ir mėlyną kreivę nuo 1800 sekundės, pastebima, kad

duomenų srautas yra skirtingas. Pagal tokį požymį galima teikti, kad HTTP duomenų srauto nebeliko, liko tiktais FTP ir Database duomenų srautas. Tokie rezultatai yra teisingi, nes HTTP duomenų srautas buvo nukreiptas į 10.10.10.110 tinklą. Išanalizavus grafiką galima būtų patvirtinti „*BGP DDoS Diversion*“ metodo veikimo charakteristikas.

Analizuojant „*BGP DDoS Diversion*“ atrėmimo metodą yra reikalinga paanalizuoti, kaip pasikeitė autonominių sistemų BGP maršruto lentelės atakos metu. Galima paanalizuoti dviejų autonominių sistemų AS_1 ir AS_8 BGP maršruto lenteles.

Category: Performance

Report: Routing Table - BGP at 3600 seconds

Table Properties

Line#	Destination	Source Protocol	Next Hop Address	Next Hop Node	Outgoing Interface	MED	Local Preference	Weight	AS Path
0	10.10.10.0/24	Direct	10.10.10.1	Network.AS_1	IF2	0	100	32768	
1	192.168.1.0/24	Direct	192.168.1.1	Network.AS_1	IF3	0	100	32768	
2	192.168.2.0/24	EBGP	10.10.10.2	Network.AS_2	IF2	0	100	0	2
3	192.168.3.0/24	EBGP	10.10.10.3	Network.AS_3	IF2	0	100	0	3
4	192.168.5.0/24	EBGP	10.10.10.5	Network.AS_5	IF2	0	100	0	5
5	192.168.6.2/32	EBGP	10.10.10.110	Network.AS_7	IF2	0	100	0	7
6	192.168.7.0/24	EBGP	10.10.10.7	Network.AS_7	IF2	0	100	0	7
7	192.168.8.0/24	EBGP	10.10.10.8	Network.AS_8	IF2	0	100	0	8
8	192.168.6.0/24	EBGP	10.10.10.6	Network.AS_6	IF2	0	100	0	6

7.12 pav. *AS_1 BGP maršruto lentelė*

Paveiksle 7.12 pav. Pateikta AS_1 autonominės sistemos BGP maršruto lentelė. Galima pastebėti, kad BGP maršrutu lentelėje atsirado papildomai vienas įrašas, lyginat su autonominės sistemos AS_1 BGP maršruto lentele pateikta 4 priede. Šioje lentelėje atsirado papildomas įrašas, kuris nusako, kad tinklas 192.168.6.2 su potinklio kauke /32 yra pasiekiamas per AS_7 su „*Next-hop-self*“ parametru 10.10.10.110. Galima daryt išvadas, kad šitas maršrutas atsirado, dėl tinkle įgyvendinto „*BGP DDoS Diversion*“ atrėmimo metodo. Nors BGP protokolo komunikacija vyksta su AS_7 autonomine sistema, tačiau visas kitas duomenų srautas su paskirties IP adresu 192.168.6.2 keliauja į tinklą 10.10.10.110, kuriame ataka jokios žalos nedaro. Gauta BGP maršruto lentelė iš AS_1 patvirtina 7.11 pav. pateikto grafiko rezultatus. Duomenis patvirtinti palyginame autonominės sistemos AS_8 BGP maršrutų lentelę. Lentelė pateikta 7.13 pav.

Category: Performance

Report: Routing Table - BGP at 3600 seconds

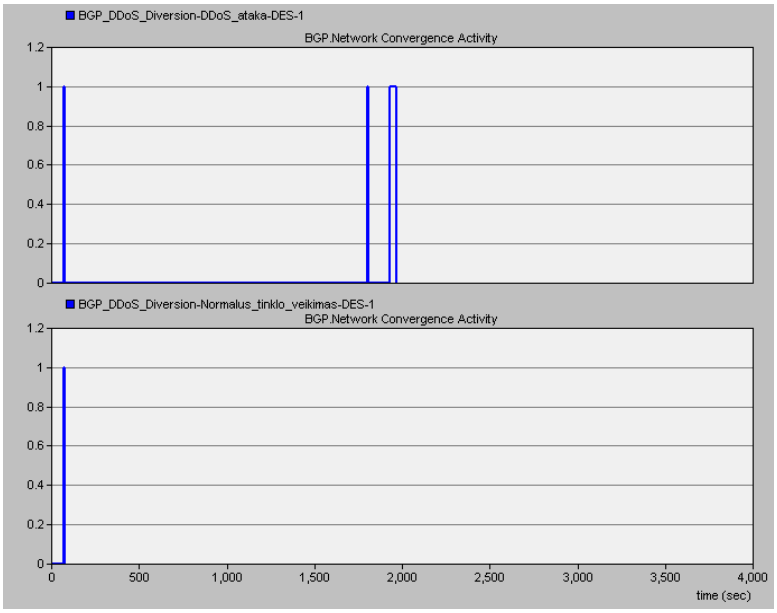
Table Properties

Line#	Destination	Source Protocol	Next Hop Address	Next Hop Node	Outgoing Interface	MED	Local Preference	Weight	AS Path
0	10.10.10.0/24	Direct	10.10.10.8	Network.AS_8	IF2	0	100	32768	
1	192.168.1.0/24	EBGP	10.10.10.1	Network.AS_1	IF2	0	100	0	1
2	192.168.2.0/24	EBGP	10.10.10.2	Network.AS_2	IF2	0	100	0	2
3	192.168.3.0/24	EBGP	10.10.10.3	Network.AS_3	IF2	0	100	0	3
4	192.168.5.0/24	EBGP	10.10.10.5	Network.AS_5	IF2	0	100	0	5
5	192.168.6.2/32	EBGP	10.10.10.110	Network.AS_7	IF2	0	100	0	7
6	192.168.7.0/24	EBGP	10.10.10.7	Network.AS_7	IF2	0	100	0	7
7	192.168.8.0/24	Direct	192.168.8.1	Network.AS_8	IF3	0	100	32768	
8	192.168.6.0/24	EBGP	10.10.10.6	Network.AS_6	IF2	0	100	0	6

7.13 pav. *AS_8 BGP maršruto lentelė*

Paanalizavus AS_8 autonominės sistemos BGP maršruto lentelę, galima pastebėti tas pačias tendencijas, kaip ir AS_1 autonominės sistemos BGP maršruto lentelėje.

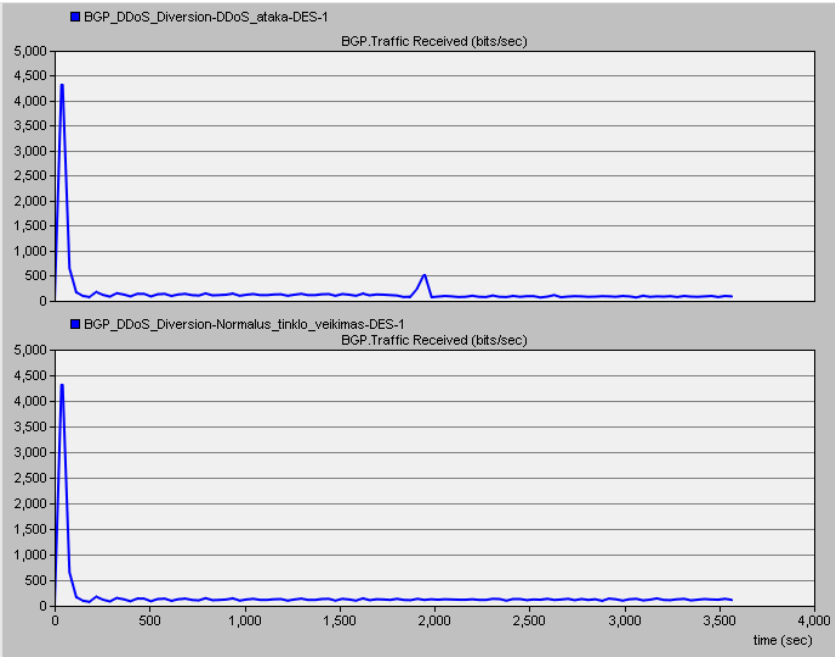
Nagrinėjant „*BGP DDoS Diversion*“ atrėmimo metodo charakteristikas vertėtų atkreipti dėmesį į BGP protokolo elgseną tinkle DDoS atako metu. Tokiai analizei pasitelksime BGP protokolo gautas statistikas.



7.14 pav. *BGP protokolo konvergencijos statistika*

7.14 pav. pateikta BGP protokolo konvergencijos statistika. Žemiau pateiktame grafike yra pateikta tinklo veikimo įprastomis sąlygomis BGP protokolo statistika. Grafike mėlyna kreivė simbolizuoja, kad tuo metu BGP maršruto parinktuvai pasikeitė BGP informacija. Įprastomis tinklo veikimo sąlygomis matome tik vieną tokią kreivę, nes pirmą karta paleidus

simuliacijai autonominės sistemos apsikeitė BGP informacija ir toliau jokių pokyčiu tinkle neįvyko. Pažvelgus į grafiką kuris simbolizuoja BGP statistika surinkta DDoS atakos metu, pastebime, kad egzistuoja trys kreivės. Pirmoji kreivė atsirado analogiškai, kaip prieš tai minėtame atvejyje. Tačiau stebint kitas atsiradusias kreives, kurios atsirado 1800 sekundę, galima daryt išvadas, kad tai įtakojo DDoS ataka ir įgyvendintas atrėmimo mechanizmas. Matome, kaip 1800 sekundę atsiranda kreivė. Šitą kreivė atsirado, nes tuo metu paketų analizatorius išsiuntė aliarmą AS_7 autonominiai sistemai, o ši savo ruoštu išsiuntė atnaujinta BGP informaciją. Autonominės sistemos gavusios šią informaciją atnaujino savo BGP lenteles, ką ir simbolizuoja grafike atsiradus trečioji kreivė.



7.15 pav. *BGP gauto srauto statistika*

Analizuojant BGP gauto srauto statistikas pateiktas 7.15 pav. galime pastebėti analogiškas tendencijas, kaip prieš tai aptartame grafike. Grafike matosi, kaip dėl DDoS atakos 1800 sekundę yra pasiunčiamas papildomas BGP duomenų srautas, kurio metu yra atnaujinamos BGP maršrutų lentelės.

7.5 Išvados

Modelio tyrimo metu, išanalizavome OPNET programa surinktas statistikas. Išvadas buvo formuluojamos lyginant gautas statistikas tinklo veikimą įprastomis sąlygomis su statistikomis tinklo veikimo DDoS atakos metu. Gautos statistikos leido išanalizuoti *„BGP DDoS Diversion“* atrėmimo metodo charakteristikas. Tinklo modelyje šis metodo veikimas buvo patvirtintas, kaip tinkamas metodas atremti DDoS ataką. Atlikus BGP protokolo elgsenos analizę

DDoS atakos metu, galima buvo suprasti, kad naudoti šį protokolą DDoS atakoms yra tinkama. Šiame tyrime DDoS atakos buvo kuriamos naudojant nedidelius duomenų srautus. Atlikti tyrimus naudojant didelius duomenų srautus yra reikalinga turėti didelius techninius resursus. Šiam atvejui duomenų srautai reikšmingos įtakos neturėjo, nes buvo analizuojamas pats veikimo principas. Turint galimybė atlikti tyrimus dideliais duomenų srautais, galima būti šį metodą taikyti analizuojant saugumo problemas realiais duomenų srautais, kurie pasitaiko Interneto paslaugų teikėjų tinkluose.

8. IŠVADOS

Šiuo metu egzistuoja nemažai būdų, kaip aptikti DDoS atakas, tačiau yra labai nedaug nuveikta, kad aptikus atakas būtų paleistas mechanizmas jas atremti. DDoS atakų atrėmimo mechanizmų yra sukurta, tačiau realiai jie nėra naudojami, tiktais aprašyti popieriuose. Todėl šiame darbe buvo nuspręsta išanalizuoti esamus DDoS atrėmimo algoritmus. DDoS atakų atrėmimo metodų analizės tyrimui pasirinkti turėjo įtakos, prieš tai atliktas tyrimas. Ankstesniajame tyrime buvo nustatyta kokią įtaką DDoS atakos gali turėti Interneto tinklo infrastruktūrai [1].

Šiam Darbui įgyvendinti buvo pasirinkta virtuali erdvė, tai suteikė didesnes analizavimo galimybes, nes atakų sukūrimas ir analizavimas realiuose tinkluose yra labai nesaugus ir atsiradusias problemas yra sunku suvaldyti. Tyrimo atlikimas virtualiuose aplinkose sumažiną riziką patirti neprognozuojamus veiksnius ir tuo pačiu išplečia tyrimo galimybes.

Darbo pradžioje buvo pristatytos pagrindinės DDoS atakos rūšys pagal jų pasireiškimo pobūdį, bei atakuojamas sistemas ir jos dalis. Taip pat buvo pristatytos atakų aptikimo priemonės ir jų rūšys. Buvo pateikti atakų aptikimo veikimo algoritmai. Atakų aptikimo sistemų veikimo ištyrimas buvo reikalingas, nes darbe buvo panaudoto atakų aptikimo sistema. Atlikta atakų atrėmimo algoritmų analizė padėjo susipažinti su esama situacija atrėmimo algoritmų sistemoje.

Tyrimui atlikti buvo pasirinktas *„BGP DDoS Diversion“* atrėmimo metodas, nes jis yra aktualiausias šiam tyrimui, kadangi tyrimas remiasi anksčiau atliktu tyrimu, kuriame buvo sprendžiamos DDoS atakos problemos susijusios su BGP protokolu [1].

Šiame darbe buvo iškelta problema, kad mažai yra nuveikta analizuojant atakų atrėmimo metodus ir yra labai sunku pasirinkti tinkama atrėmimo metodą. Problemai spręsti buvo sukurta virtuali kompiuterinio tinklo infrastruktūra. Tinklo modelis buvo sukurtas naudojant OPNET Modeler modeliavimo programą. Panaudojant OPNET programą buvo sukurtas virtualus tinklo modelis paremtas Interneto veikimo principu. Tinkle buvo įgyvendintas BGP protokolo veikimas. Panaudojant esantį tinklo elementą buvo sukurta atakų atpažinimo sistema, gebanti skanuoti tinkle keliaujančius paketus, bei išsiųsti aliarmą nustatytam šaltiniui. Atakos atrėmimo metodo tyrimas buvo atliekamas lyginat gautus rezultatus tinklo veikimo įprastomis sąlygomis su gautais rezultatais tinklo veikimo DDoS atakos metu. Tyrimo metu buvo surinkti tokie rezultatai:

- Sąsajų pralaidumo charakteristikos
- BGP protokolo charakteristikos
- BGP maršruto lentelės

Gauti rezultatai, leido nustatyti tyrinėjamo metodo veikimo charakteristikas. Išanalizavus rezultatus buvo nustatyta, kad naudojant „*BGP DDoS Diversion“* atrėmimo metodą, galima sumažinti DDoS atakų poveikį ir išvengti nereikalingo duomenų srauto savo tinkluose.

Atlikę tyrimą galima būtų išskirti tokias pagrindiniais neigiamas ir teigimas tyrinėjamo atrėmimo metodo savybes:

Neigiamos savybės

- Ne visi Interneto paslaugų teikėjai priimą BGP atnaujinimus su potinklio kaukę /32
- Norint sukurti visiškai nepriklausomą atrėmimo sistemą reikalinga turėti atskirą autonominės sistemos numerį
- Realiame tinkle reikalinga suderinti šią sistemą su kitais Interneto paslaugų teikėjais
- Nėra panaikinama DDoS ataka, o tiesiog sumažinami jos padariniai

Teigiamos savybės

- Nesudėtingas techninis įgyvendinimas
- Lengvas atrėmimo valdymas
- Užtikrintas nereikalingo duomenų srauto nukreipimas
- Nedideli įgyvendinimo kaštai realiame tinkle

Pažvelgus į kitus DDoS atrėmimo metodus „*BGP DDoS Diversion“* metodą galime laikyti vieną iš paprasčiausiai įgyvendinamu ir gan efektyviai veikiančiu. Žinoma, yra ir įvairių tinklo įrangos gamintojų siūlomu DDoS atrėmimo sistemų, tačiau tokios sistemos yra brangios ir ne kiekvienas Interneto paslaugų teikėjas gali įsigyti tokia įrangą.

Kad ir koks geras, bei lankstus būtų „*BGP DDoS Diversion“* atrėmimo metodas, jis neteikia visiškos apsaugos nuo DDoS atakos. Kaip tyrime buvo pastebėta, kad pats DDoS atakos nukreipimas yra įgyvendinamas, tačiau atakuojamas įrenginys tinkle jau nebėra matomas. Tokiu būdų tik yra sumažinama DDoS atakos žala, nes kiti tinklo įrenginiai esantys tinkle išlieka pasiekiami.

Kalbant apie tolimesnius darbus, kurie remtųsi gautais rezultatais šiame tyrime, būtų galima paanalizuoti galimybę tobulinti patį atakos aptikimo mechanizmą. Aptikimo mechanizmas galėtų turėti daugiau požymių, pagal kuriuos galima būtų nuspręsti, ar tai DDoS ataka. Norint, kad kuo daugiau būtų taikomas „BGP DDoS Diversion“ atrėmimo metodas, reikėtų panagrinėti kokių sąlygų reikėtų, kad šis sprendimas taptų standartų Interneto tinkluose, kovojant su DDoS atakomis.

LITERATŪRA

1. A. KAJACKAS, R. RAINYS, A. APUTIS. ELEKTRONIKA IR ELEKTROTECHNIKA. *Kibernetinių atakų įtakos interneto tinklui tyrimas*. Vilniaus Gedimino Technikos Universitetas. 2011. 92.p

2. W.BORREMANS. R.VALKE. *BGP DDoS Diversion.* 2009.

3. LAMMLE T. *CompTIA Network+*. Indiana: Willey Publishing, 2009. 892p.

4. DULANEY.E. *CompTIA Security+*. Indiana: Willey Publishing, 2009. 679p.

5. VRIZLYNN THING LING LING. *Adaptive Response System for Distributed Denial-of-Service Attacks.* Imperial College London Department of Computing. 2008. 204p.

6. PETERSON.W. *Tactical Perimeter Defense*. Security Cerified Program, 591p.

7. R. PLĖŠTYS, D.RIMKUS, R.KAVALIŪNAS, I.LAGZDINYTĖ, N.SRAFINIENĖ. *Kompiuterių tinklų sauga*. Kauno Technologijos Universitetas.2008. 186p.

8. T.J.MCNEVIN. *Mitigating Network-Based Denial-of-Service Attacks with Client Puzzles.* Virginia Polytechnic Institute. 2005. 90p.

9. J.PROKKOLA. *OPNET – Network Simulator.* VTT Technical Research Center. Finland. 2006. 56p.

10. G.CORRAL, A.ZABALLOS, J.ABELLA, C.MORALES. *Building an IDS using OPNET.* Universitat Ramon Llull, Spain. 2006. 21p.

11. S.RAZAK, M.ZHOU, SHEAU-DONG LANG. *Network Intrusion Simulation Using OPNET.* University of Central Florida, Orlando. 2005. 5p.

12. A.ZABALLOS, G.CORRAL, I.SERRA, J.ABELLA. *Testing Network Security Using OPNET.* Universitat Ramon Llull, Spain. 2006. 15p.

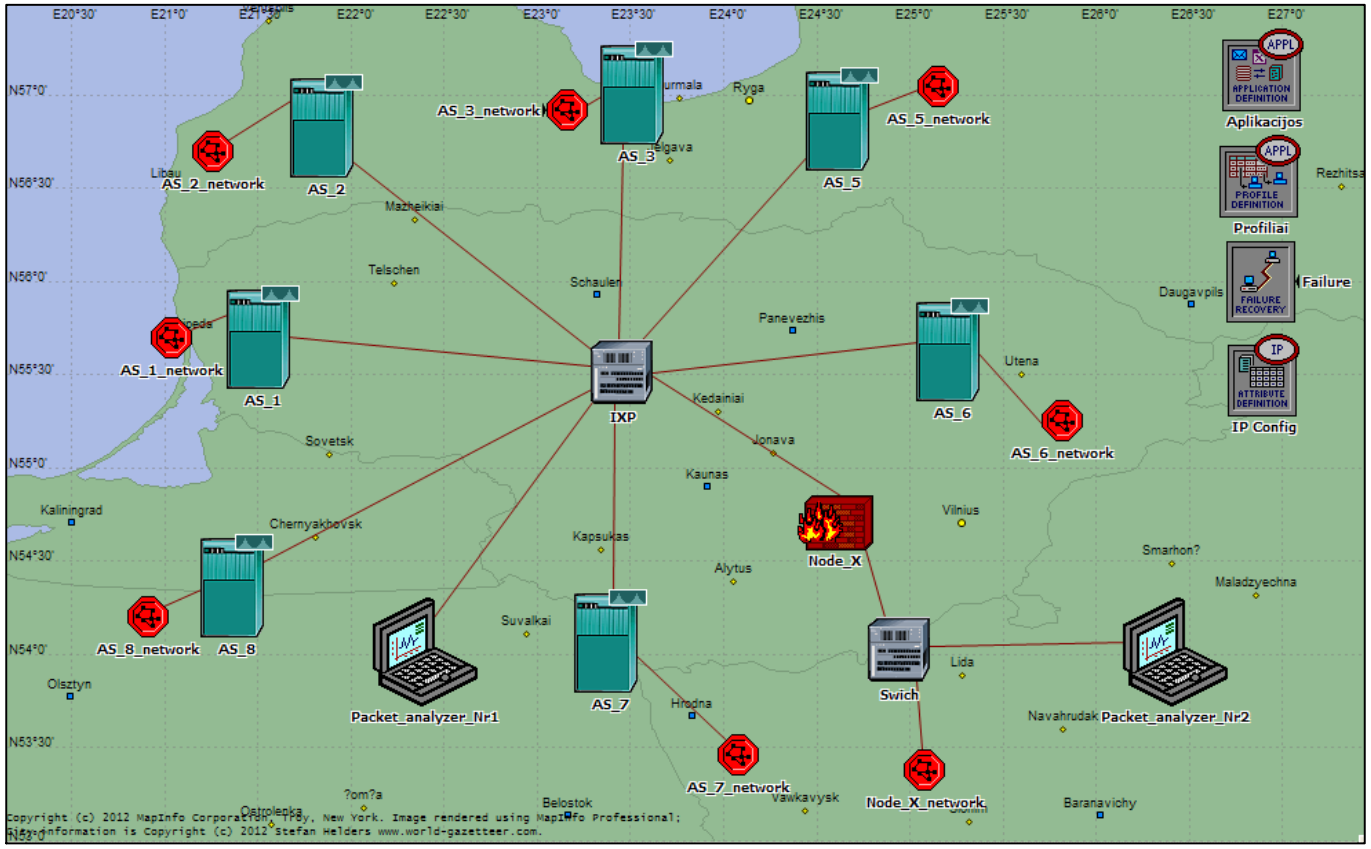
13. Cisco Safe System. Prieiga per Internetą http://www.cisco.com/en/US/netsol/ns954/index.html

14. H.GOMAA. *Designing Software Product Lines with UML: From Use Cases to Pattern-Based Software Architectures.* Addison Wesley Longman Publishing Co., Inc. Redwood City, CA, USA. 2004.

15. STEPHEN A. WHITE. *Introduction to BPMN.* BPTrends July. 2004

PRIEDAI

1 priedas. Tinklo modelio vaizdas OPNET modeliavimo terpėje



2 priedas. Tinklo modelio elementų IPv4 adresacija

Node Name: Network.AS_6
Iface Name IP Address Subnet Mask Connected Link
---------- --------------- --------------- ----------------
IF2 10.10.10.6 255.255.255.0 Network.AS_6 <-> IXP
IF5 192.168.6.1 255.255.255.0 Network.AS_6 <-> AS_6_network 1
Node Name: Network.AS_1
Iface Name IP Address Subnet Mask Connected Link
---------- --------------- --------------- ----------------
IF2 10.10.10.1 255.255.255.0 Network.AS_1 <-> IXP
IF3 192.168.1.1 255.255.255.0 Network.AS_1 <-> AS_1_network
Node Name: Network.AS_5
Iface Name IP Address Subnet Mask Connected Link
---------- --------------- --------------- ----------------
IF2 10.10.10.5 255.255.255.0 Network.AS_5 <-> IXP
IF3 192.168.5.1 255.255.255.0 Network.AS_5_network <-> AS_5
Node Name: Network.AS_7
Iface Name IP Address Subnet Mask Connected Link
---------- --------------- --------------- ----------------
IF2 10.10.10.7 255.255.255.0 Network.AS_7 <-> IXP
IF3 192.168.7.1 255.255.255.0 Network.AS_7_network <-> AS_7
Node Name: Network.AS_2
Iface Name IP Address Subnet Mask Connected Link
---------- --------------- --------------- ----------------
IF2 10.10.10.2 255.255.255.0 Network.AS_2 <-> IXP
IF3 192.168.2.1 255.255.255.0 Network.AS_2 <-> AS_2_networ
Node Name: Network.AS_3
Iface Name IP Address Subnet Mask Connected Link
---------- --------------- --------------- ----------------
IF2 10.10.10.3 255.255.255.0 Network.AS_3 <-> IXP
IF3 192.168.3.1 255.255.255.0 Network.AS_3_network <-> AS_3
Node Name: Network.AS_8
Iface Name IP Address Subnet Mask Connected Link
---------- --------------- --------------- ----------------

IF2 10.10.10.8 255.255.255.0 Network.AS_8 <-> IXP

IF3 192.168.8.1 255.255.255.0 Network.AS_8 <-> AS_8_network

Node Name: Network.AS_4

Iface Name IP Address Subnet Mask Connected Link

---------- --------------- --------------- ----------------

IF2 10.10.10.4 255.255.255.0 Network.AS_4 <-> IXP

IF3 192.168.4.1 255.255.255.0 Network.AS_4 <-> AS_4_network

Node Name: Network.AS_6_network.AS_6_network

Iface Name IP Address Subnet Mask Connected Link

---------- --------------- --------------- ----------------

IF0 192.168.6.100 255.255.255.0 Network.AS_6_network.AS_6_network <-> Swich

Node Name: Network.AS_6_network.FTP_server

Iface Name IP Address Subnet Mask Connected Link

---------- --------------- --------------- ----------------

IF0 192.168.6.20 255.255.255.0 Network.AS_6_network.FTP_server <-> Swich

Node Name: Network.AS_6_network.HTTP_server

Iface Name IP Address Subnet Mask Connected Link

---------- --------------- --------------- ----------------

IF0 192.168.6.2 255.255.255.0 Network.AS_6_network.HTTP_server <-> Swich

Node Name: Network.AS_6_network.Database_server

Iface Name IP Address Subnet Mask Connected Link

---------- --------------- --------------- ----------------

IF0 192.168.6.50 255.255.255.0 Network.AS_6_network.Database_server <-> Swich

Node Name: Network.AS_5_network.AS_5_network

Iface Name IP Address Subnet Mask Connected Link

---------- --------------- --------------- ----------------

IF0 192.168.5.2 255.255.255.0 Network.AS_5_network <-> AS_5

Node Name: Network.AS_4_network.node_0

Iface Name IP Address Subnet Mask Connected Link

---------- --------------- --------------- ----------------

```
IF0                 192.0.0.1       255.255.255.0    Network.AS_4 <-> AS_4_network
# Node Name: Network.AS_3_network.AS_3_network
#  Iface Name          IP Address      Subnet Mask     Connected Link
#  ----------          --------------  --------------  ----------------
IF0                 192.168.3.2     255.255.255.0    Network.AS_3_network <-> AS_3
# Node Name: Network.AS_2_network.AS_2_network
#  Iface Name          IP Address      Subnet Mask     Connected Link
#  ----------          --------------  --------------  ----------------
IF0                 192.168.2.2     255.255.255.0    Network.AS_2 <-> AS_2_network
# Node Name: Network.AS_1_network.AS_1_network
#  Iface Name          IP Address      Subnet Mask     Connected Link
#  ----------          --------------  --------------  ----------------
IF0                 192.168.1.2     255.255.255.0    Network.AS_1 <-> AS_1_network
# Node Name: Network.AS_8_network.AS_8_network
#  Iface Name          IP Address      Subnet Mask     Connected Link
#  ----------          --------------  --------------  ----------------
IF0                 192.168.8.2     255.255.255.0    Network.AS_8 <-> AS_8_network
# Node Name: Network.AS_7_network.AS_7_network
#  Iface Name          IP Address      Subnet Mask     Connected Link
#  ----------          --------------  --------------  ----------------
IF0                 192.168.7.2     255.255.255.0    Network.AS_7_network <-> AS_7
# Node Name: Network.Packet_analyzer_Nr1
#  Iface Name          IP Address      Subnet Mask     Connected Link
#  ----------          --------------  --------------  ----------------
IF0                 10.10.10.100    255.255.255.0    Network.Packet_analyzer_Nr1 <-> IXP
# Node Name: Network.Packet_analyzer_Nr2
#  Iface Name          IP Address      Subnet Mask     Connected Link
#  ----------          --------------  --------------  ----------------
IF0                 10.10.10.200    255.255.255.0    Network.Node_X <-> Packet_analyzer_Nr2
# Node Name: Network.Node_X_network.Test_network
#  Iface Name          IP Address      Subnet Mask     Connected Link
#  ----------          --------------  --------------  ----------------
IF0                 10.10.10.110    255.255.255.0    Network.Node_X <-> Node_X_network
```

3 Priedas. Tinklo modelyje esančių elementų detali konfigūracija

Autonominės sistemos konfigūracija:

IP Routing Protocols

- BGP Parameters [Status Enabled]
- Address Family Parameters [IPv4, Any, None]
- Address Family Properties [Redistribution: Directly Connected “Redistribute w/Default”, Static “Redistribute w/Default”]
- Neighbors [IP address X.X.X.X, Remote AS X, Neighbor Properties]

Reports

- BGP Routing Table [Status Enable]

IP

- IP Routing Parameters
- Autonomous System Number [X]
- Interface Information [IF2: UP, Address X.X.X.X, Subnet Mask X.X.X.X, Routing Protocol None, MTU IP]

Vidinio tinklo konfigūracija:

Applications

- Application Supported Profiles [Profile Name XXXXX]
- Application Supported Services [Name XXXXX]

IP

- IP Host Parameters

- Interface Information [Name IF0, Address X.X.X.X, Subnet Mask X.X.X.X, Default Route X.X.X.X]

LAN

- Number of Workstations X

4 Priedas. BGP maršruto lentelės

AS_1 BGP maršruto lentelė

Category: Performance
Report: Routing Table - BGP at 268 seconds

Table Properties

Line#	Destination	Source Protocol	Next Hop Address	Next Hop Node	Outgoing Interface	MED	Local Preference	Weight	AS Path
0	10.10.10.0/24	Direct	10.10.10.1	Network.AS_1	IF2	0	100	32768	
1	192.168.1.0/24	Direct	192.168.1.1	Network.AS_1	IF3	0	100	32768	
2	192.168.2.0/24	EBGP	10.10.10.2	Network.AS_2	IF2	0	100	0	2
3	192.168.3.0/24	EBGP	10.10.10.3	Network.AS_3	IF2	0	100	0	3
4	192.168.5.0/24	EBGP	10.10.10.5	Network.AS_5	IF2	0	100	0	5
5	192.168.6.0/24	EBGP	10.10.10.6	Network.AS_6	IF2	0	100	0	6
6	192.168.7.0/24	EBGP	10.10.10.7	Network.AS_7	IF2	0	100	0	7
7	192.168.8.0/24	EBGP	10.10.10.8	Network.AS_8	IF2	0	100	0	8

AS_2 BGP maršruto lentelė

Category: Performance
Report: Routing Table - BGP at 268 seconds

Table Properties

Line#	Destination	Source Protocol	Next Hop Address	Next Hop Node	Outgoing Interface	MED	Local Preference	Weight	AS Path
0	10.10.10.0/24	Direct	10.10.10.2	Network.AS_2	IF2	0	100	32768	
1	192.168.1.0/24	EBGP	10.10.10.1	Network.AS_1	IF2	0	100	0	1
2	192.168.2.0/24	Direct	192.168.2.1	Network.AS_2	IF3	0	100	32768	
3	192.168.3.0/24	EBGP	10.10.10.3	Network.AS_3	IF2	0	100	0	3
4	192.168.5.0/24	EBGP	10.10.10.5	Network.AS_5	IF2	0	100	0	5
5	192.168.6.0/24	EBGP	10.10.10.6	Network.AS_6	IF2	0	100	0	6
6	192.168.7.0/24	EBGP	10.10.10.7	Network.AS_7	IF2	0	100	0	7
7	192.168.8.0/24	EBGP	10.10.10.8	Network.AS_8	IF2	0	100	0	8

AS_3 BGP maršruto lentelė

Category: Performance
Report: Routing Table - BGP at 268 seconds

Table Properties

Line#	Destination	Source Protocol	Next Hop Address	Next Hop Node	Outgoing Interface	MED	Local Preference	Weight	AS Path
0	10.10.10.0/24	Direct	10.10.10.3	Network.AS_3	IF2	0	100	32768	
1	192.168.1.0/24	EBGP	10.10.10.1	Network.AS_1	IF2	0	100	0	1
2	192.168.2.0/24	EBGP	10.10.10.2	Network.AS_2	IF2	0	100	0	2
3	192.168.3.0/24	Direct	192.168.3.1	Network.AS_3	IF3	0	100	32768	
4	192.168.5.0/24	EBGP	10.10.10.5	Network.AS_5	IF2	0	100	0	5
5	192.168.6.0/24	EBGP	10.10.10.6	Network.AS_6	IF2	0	100	0	6
6	192.168.7.0/24	EBGP	10.10.10.7	Network.AS_7	IF2	0	100	0	7
7	192.168.8.0/24	EBGP	10.10.10.8	Network.AS_8	IF2	0	100	0	8

AS_5 BGP maršruto lentelė

Category: Performance
Report: Routing Table - BGP at 268 seconds

Table Properties

Line#	Destination	Source Protocol	Next Hop Address	Next Hop Node	Outgoing Interface	MED	Local Preference	Weight	AS Path
0	10.10.10.0/24	Direct	10.10.10.5	Network.AS_5	IF2	0	100	32768	
1	192.168.1.0/24	EBGP	10.10.10.1	Network.AS_1	IF2	0	100	0	1
2	192.168.2.0/24	EBGP	10.10.10.2	Network.AS_2	IF2	0	100	0	2
3	192.168.3.0/24	EBGP	10.10.10.3	Network.AS_3	IF2	0	100	0	3
4	192.168.5.0/24	Direct	192.168.5.1	Network.AS_5	IF3	0	100	32768	
5	192.168.6.0/24	EBGP	10.10.10.6	Network.AS_6	IF2	0	100	0	6
6	192.168.7.0/24	EBGP	10.10.10.7	Network.AS_7	IF2	0	100	0	7
7	192.168.8.0/24	EBGP	10.10.10.8	Network.AS_8	IF2	0	100	0	8

AS_6 BGP maršruto lentelė

Category: Performance
Report: Routing Table - BGP at 268 seconds

Table Properties

Line#	Destination	Source Protocol	Next Hop Address	Next Hop Node	Outgoing Interface	MED	Local Preference	Weight	AS Path
0	10.10.10.0/24	Direct	10.10.10.6	Network.AS_6	IF2	0	100	32768	
1	192.168.1.0/24	EBGP	10.10.10.1	Network.AS_1	IF2	0	100	0	1
2	192.168.2.0/24	EBGP	10.10.10.2	Network.AS_2	IF2	0	100	0	2
3	192.168.3.0/24	EBGP	10.10.10.3	Network.AS_3	IF2	0	100	0	3
4	192.168.5.0/24	EBGP	10.10.10.5	Network.AS_5	IF2	0	100	0	5
5	192.168.6.0/24	Direct	192.168.6.1	Network.AS_6	IF5	0	100	32768	
6	192.168.7.0/24	EBGP	10.10.10.7	Network.AS_7	IF2	0	100	0	7
7	192.168.8.0/24	EBGP	10.10.10.8	Network.AS_8	IF2	0	100	0	8

AS_7 BGP maršruto lentelė

Category: Performance
Report: Routing Table - BGP at 268 seconds

Table Properties

Line#	Destination	Source Protocol	Next Hop Address	Next Hop Node	Outgoing Interface	MED	Local Preference	Weight	AS Path
0	10.10.10.0/24	Direct	10.10.10.7	Network.AS_7	IF2	0	100	32768	
1	192.168.1.0/24	EBGP	10.10.10.1	Network.AS_1	IF2	0	100	0	1
2	192.168.2.0/24	EBGP	10.10.10.2	Network.AS_2	IF2	0	100	0	2
3	192.168.3.0/24	EBGP	10.10.10.3	Network.AS_3	IF2	0	100	0	3
4	192.168.5.0/24	EBGP	10.10.10.5	Network.AS_5	IF2	0	100	0	5
5	192.168.6.0/24	EBGP	10.10.10.6	Network.AS_6	IF2	0	100	0	6
6	192.168.7.0/24	Direct	192.168.7.1	Network.AS_7	IF3	0	100	32768	
7	192.168.8.0/24	EBGP	10.10.10.8	Network.AS_8	IF2	0	100	0	8

AS_8 BGP maršruto lentelė

Category: Performance

Report: Routing Table - BGP at 268 seconds

Table Properties

Line#	Destination	Source Protocol	Next Hop Address	Next Hop Node	Outgoing Interface	MED	Local Preference	Weight	AS Path
0	10.10.10.0/24	Direct	10.10.10.8	Network.AS_8	IF2	0	100	32768	
1	192.168.1.0/24	EBGP	10.10.10.1	Network.AS_1	IF2	0	100	0	1
2	192.168.2.0/24	EBGP	10.10.10.2	Network.AS_2	IF2	0	100	0	2
3	192.168.3.0/24	EBGP	10.10.10.3	Network.AS_3	IF2	0	100	0	3
4	192.168.5.0/24	EBGP	10.10.10.5	Network.AS_5	IF2	0	100	0	5
5	192.168.6.0/24	EBGP	10.10.10.6	Network.AS_6	IF2	0	100	0	6
6	192.168.7.0/24	EBGP	10.10.10.7	Network.AS_7	IF2	0	100	0	7
7	192.168.8.0/24	Direct	192.168.8.1	Network.AS_8	IF3	0	100	32768	

5 Priedas. Paketų analizatoriaus skanuoti paketai

Flags	Frame	Delta Time	Destination	Source	Protocol	Summary
M	1	0	[AS_1]	[AS_6]	TCP	D=179 S=1024 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	2	0.000011	[AS_6]	[AS_1]	TCP	D=179 S=1024 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	3	0.000007	[AS_2]	[AS_1]	TCP	D=179 S=1025 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	4	0.000007	[AS_3]	[AS_1]	TCP	D=179 S=1026 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	5	0.000007	[AS_5]	[AS_1]	TCP	D=179 S=1027 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	6	0.000007	[AS_7]	[AS_1]	TCP	D=179 S=1028 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	7	0.000007	[AS_8]	[AS_1]	TCP	D=179 S=1029 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	8	0.000022	[AS_2]	[AS_6]	TCP	D=179 S=1025 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	9	0.000067	[AS_3]	[AS_6]	TCP	D=179 S=1026 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	10	0.000067	[AS_5]	[AS_6]	TCP	D=179 S=1027 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	11	0.000007	[AS_1]	[AS_7]	TCP	D=179 S=1024 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	12	0.000007	[AS_2]	[AS_7]	TCP	D=179 S=1025 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	13	0.000007	[AS_3]	[AS_7]	TCP	D=179 S=1026 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	14	0.000007	[AS_5]	[AS_7]	TCP	D=179 S=1027 SYN ACK=0 SEQ=17500000 LEN=0 WIN=8760
	15	0.000007	[AS_6]	[AS_7]	TCP	D=179 S=1028 SYN ACK=0 SEQ=17500000 LEN=0