Kauno technologijos universitetas

Informatikos fakultetas

DoS/DDoS atakos požymiais pagrįstas atakos paviršiaus charakterizavimo modelis

Baigiamasis magistro studijų projektas

Džiugas Petrikas

Projekto autorius

dr. Rasa Brūzgienė

Vadovė

Kaunas, 2026

Kauno technologijos universitetas

Informatikos fakultetas

DoS/DDoS atakos požymiais pagrįstas atakos paviršiaus charakterizavimo modelis

Baigiamasis magistro studijų projektas

Informacijos ir informacinių technologijų sauga (6211BX008)

Džiugas Petrikas

Projekto autorius

dr. Rasa Brūzgienė

Vadovė

prof. Agnius Liutkevičius

Recenzentas

Kaunas, 2026

Kauno technologijos universitetas

Informatikos fakultetas

Džiugas Petrikas

DoS/DDoS atakos požymiais pagrįstas atakos paviršiaus charakterizavimo modelis

Akademinio sąžiningumo deklaracija

Patvirtinu, kad:

1. baigiamąjį projektą parengiau savarankiškai ir sąžiningai, nepažeisdama(s) kitų asmenų autoriaus ar kitų teisių, laikydamasi(s) Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo nuostatų, Kauno technologijos universiteto (toliau – Universitetas) intelektinės nuosavybės valdymo ir perdavimo nuostatų bei Universiteto akademinės etikos kodekse nustatytų etikos reikalavimų;

2. baigiamajame projekte visi pateikti duomenys ir tyrimų rezultatai yra teisingi ir gauti teisėtai, nei viena šio projekto dalis nėra plagijuota nuo jokių spausdintinių ar elektroninių šaltinių, visos baigiamojo projekto tekste pateiktos citatos ir nuorodos yra nurodytos literatūros sąraše;

3. įstatymų nenumatytų piniginių sumų už baigiamąjį projektą ar jo dalis niekam nesu mokėjęs (-usi);

4. suprantu, kad išaiškėjus nesąžiningumo ar kitų asmenų teisių pažeidimo faktui, man bus taikomos akademinės nuobaudos pagal Universitete galiojančią tvarką ir būsiu pašalinta(s) iš Universiteto, o baigiamasis projektas gali būti pateiktas Akademinės etikos ir procedūrų kontrolieriaus tarnybai nagrinėjant galimą akademinės etikos pažeidimą.

Džiugas Petrikas

Patvirtinta elektroniniu būdu

Petrikas, Džiugas. DoS/DDoS atakos požymiais pagrįstas atakos paviršiaus charakterizavimo modelis. Magistro baigiamasis projektas vadovė dr. Rasa Brūzgienė; Kauno technologijos universitetas, Informatikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Informacijos ir informacinių technologijų sauga (6211BX008)

Reikšminiai žodžiai: DoS, DDoS, IT, OT, Paviršius, Charakterizavimas, Kibernetika.

Kaunas, 2026. 74 p.

Santrauka

Paskirstytos ir paprastos paslaugos atsisakymo atakos darosi vis labiau sumanesnės, kadangi kibernetinių nusikaltėlių arsenale yra atsiradę daugybė skirtingų šios atakos variacijų. Šios atakos nebeapsiriboja senu principu sudaryti kuo didesnį srautą į sistemą, kadangi toks srauto šuolis greitai aptinkamas ir užblokuojamas. Atakos šiuo metu gali siųsti paketus labai lėtai, kad būtų trikdoma paslauga. Be to, skirtingų atakos tipų atsiradimas suteikia galimybę nusikaltėliams naudoti ir multivektorines atakas prieš įmonių sistemas, tokiu būdu atakuojant kelis įrenginius sistemoje vienu metu.

Akivaizdu, kad visiškai apsisaugoti nuo šių atakų nepavyks, tačiau vos tik įvykus atakai sistemoje, tinkamas jos ištyrimas gali ženkliai padėti išvengti tos pačios atakos pasikartojimo ateityje. Norint suprasti ataką, reikia suprasti kaip tiksliai ši ataka veikė sistemoje ir kokius įrenginius atakavo. Šiuo metu tai atliekama naudojant keletą skirtingų įrankių rankiniu būdu. Tai yra ilgai trunkantis procesas ir reikalaujantis atitinkamo personalo pasirengimo. Turint įrankį, gebantį greitai ir išsamiai išanalizuoti atakos paviršių, būtų galima greičiau organizuoti apsaugos priemones sistemoje, pasidalinti patirtimi su kitomis įmonėmis ir taip greičiau prisitaikyti prie nuolat kintančių paslaugos atsisakymo atakų.

Petrikas, Džiugas. Model for Characterizing the DoS/DDoS Attack Surface. Master's Final Degree Project supervisor dr, Rasa Brūzgienė; Faculty of Informatics, Kaunas University of Technology.

Study field and area (study field group): Security of Information and Information Technology (6211BX008)

Keywords: DoS, DDoS, IT, OT, Surface, Charaterization, Cybersecurity.

Kaunas, 2026. 74.

Summary

Distributed denial-of-service attacks are becoming increasingly sophisticated, as cybercriminals have a wide range of different attacks in their arsenal. These attacks are no longer limited to the old principle of creating as much traffic as possible into the system, since such a surge in traffic is quickly detected and blocked. Attacks can now send packets very slowly to disrupt the service. In addition, the emergence of various attack types allows criminals to use multi-vector attacks against corporate systems, thus attacking multiple devices at once.

It is obvious that it will not be possible to completely protect against these attacks, but once an attack has occurred, proper investigation can significantly help prevent the same attack from recurring in the future. To understand an attack, it is necessary to understand how exactly this attack worked and at what devices it attacked. Currently, this is done using several tools, manually. This is a time-consuming process and requires appropriate personnel training. Having a tool capable of quickly and comprehensively analyzing the attack surface would allow for organizing security measures, sharing experiences with other companies, and thus adapting to ongoing service denials.

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Įvadas

Paslaugos atsisakymo (*angl. Denial of Service – DoS*) ir paskirstyta paslaugos atsisakymo (*angl. Distributed Denial of Service – DDoS*) atakos kelia vis didesnius iššūkius kibernetinėje erdvėje taip trukdydamos įprastą internetinę veiklą įvairioms organizacijoms ir valstybės institucijoms. Šios atakos naudojamos ne tik prieš įmonių IT (*angl. information technology*) sistemas, tačiau, vis labiau vystantis ketvirtajai pramonės revoliucijai, šios atakos intensyviai pradedamos naudoti ir prieš OT *(angl. operational technology)* sistemas, esančias pramonės sektoriuje ir kritinėse infrastruktūrose [1]. Norint efektyviai apsiginti nuo DoS/DDoS atakų reikia gero šių atakų suvokimo, o šiam tikslui yra sudaromi įvairūs klasifikavimo ir charakterizavimo modeliai, kurie padeda šias atakas geriau suprasti kibernetinio saugumo specialistams.

Viešuosiuose šaltiniuose galima rasti daugybę informacijos apie skirtingų DoS ir DDoS atakų tipų, gynybos mechanizmų, atakos įrankių klasifikavimą [2], [3], yra nemažai informacijos apie įvairius požymius, pagal kuriuos galima aptikti šias atakas [4]. Daugybė straipsnių taip pat analizuoja įvarius mašininio mokymo metodus, norint mokyti dirbtinį intelektą realiu laiku aptikti ir užkardyti šias kibernetines atakas [5]. Tačiau nepaisant to, šios atakos vis tiek išlieka vienos iš dažniausiai pasitaikančių kibernetinių atakų. Taip yra dėl to, nes didėjant skaitmenizavimui ir vystantis naujausioms technologijoms, sparčiai didėja atakos paviršius organizacijų sistemose, o tai suteikia galimybę atsirasti naujiems atakos tipams ir veikimo metodikoms. Pagal 2024 metais CISA (*Cybersecurity and Infrastructure Security Agency*) organizacijos išleistą publikaciją [6], svarbu ne tik šių atakų kuo greitesnis užfiksavimas ir sustabdymas realiu metu, tačiau būtinas ir pasiruošimas atlikti išsamius įvykusių incidentų tyrimus. Kad būtų galima atlikti įvykusių DoS arba DDoS atakų tyrimus, yra poreikis įrankiams, kurie detaliai išanalizuotų ir pateiktų išsamią informaciją apie ataką ir atakuojamą sistemą. Šiuo metu, norint atlikti išsamią įvykusių atakų analizę, dažniausiai naudojamas skirtingų įrankių derinys [7], [8], [9]. Tai padaro analizę sudėtingesnę ir ilgesnę, taip pat reikalauja aukštų personalo kompetencijų. Dedikuoti, įvykusių DoS/DDoS atakų analizių, modeliai padėtų automatizuoti tyrimo procesą ir sumažintų priklausomybę nuo skirtingų įrankių naudojimo.

Vienas iš pagrindinių šaltinių, teikiantis informaciją apie įvykusią ataką, yra tinklo srautas, o pagal CISA, viena iš pagrindinių, įvykusios atakos, tyrimo užduočių yra pažeistų įrenginių ir sistemų identifikavimas. Įvertinant tai daroma prielaida, jog išgryninus DoS ir DDoS atakų savybes tinklo lygmeniu, yra galimybė sudaryti tinklo požymiais pagrįstą, atakos paviršiaus charakterizavimo modelį. Pagal tai realizuota programa galėtų automatiškai, iš tinklo srauto, identifikuoti puolamus įrenginius sistemoje, analizuoti atakos veikimą laike, stebėti jos judėjimą tarp įrenginių bei pamatyti kitus, su ataka susijusius, veiksmus. Nors šis modelis būtų orientuotas į jau įvykusių atakų analizę, visgi jis padėtų greičiau atlikti DoS ir DDoS incidentų analizes, o tai padėtų kibernetinio saugumo specialistams greičiau pamatyti savo administruojamų sistemų silpnąsias vietas ir jas atitinkamai sustiprinti.

Darbo tikslas – sudaryti DoS ir DDoS atakos požymiais grįstą atakos paviršiaus charakterizavimo modelį.

Darbo uždaviniai:

- išanalizuoti esamus atakos paviršiaus charakterizavimo modelius, nustatant būdus ir principus, kurie šiuo metu yra taikomi charakterizuojant atakos paviršių;

- apžvelgti atakų tipus, kad būtų galima identifikuoti atakuojamus taškus sistemoje ir sudaryti atakos paviršiaus klasifikavimą;
- sudaryti vertikalią atakos plitimo kreivę atakuojamoje sistemoje pagal *Purdue* modelį, kuris padėtų suprasti atakos plitimą sistemoje pagal gylį;
- sudaryti atakos požymiais grįstą atakos paviršiaus charakterizavimo modelį, pagal kurį būtų galima realizuoti vykdomąją programą;
- sukurti prototipą pagal sudarytą modelį, siekiant patikrinti naujojo modelio veiksmingumą;
- eksperimentiškai ištirti ir įvertinti pasiūlyto sprendimo kiekybines ir kokybines charakteristikas.

Analizės dalyje apžvelgiama atakos paviršiaus sąvoka ir paaiškinamas jos naudojimas šiame darbe. Toliau pateikiama informacija apie esamus DoS/DDoS atakos paviršiaus charakterizavimo modelius ir kitus susijusius tyrimus, apžvelgiami įvairūs atviro kodo ir komerciniai įrankiai. Vėliau atliekama atakos tipų IT ir OT sistemose analizė, jas suklasifikuojant pagal OSI (*angl. Open System Interconnection*) modelio lygmenis. Pagal atakos tipus sudaromas atakos paviršiaus klasifikavimas, kuris išskaidomas pagal *Purdue* modelio [10] lygmenis.

Projektavimo dalyje yra aprašomas siūlomas naujasis modelis ir pateikiama jo koncepcija. Vėliau sudaroma panaudos atvejų diagrama, išsikeliami funkciniai ir nefunkciniai reikalavimai. Aprašomas dinaminis sprendimo modelis sudarant UML (*angl. Unified Modeling Language*) veiklos diagramas išsikeltiems funkciniams reikalavimams.

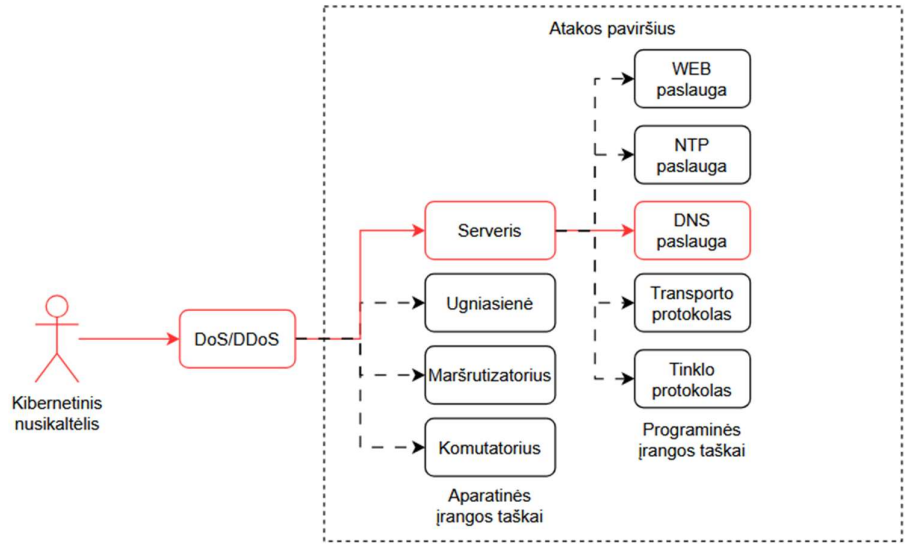
Realizavimo dalyje aprašomi realizavimui pasirenkami įrankiai, realizuojama vietinė *Purdue* lygmenų – prievadų duomenų bazė, kuri naudojama paslaugų ir sistemų išskaidymui į lygmenis pagal *Purdue* modelį, aprašoma naudotojo grafinė sąsaja, realizuojami funkciniai ir nefunkciniai reikalavimai, pateikiama diegimo diagrama.

Eksperimento dalyje pateikiamas siūlymas modelio veiksmingumui įvertinti ir iškeliami tyrimo tikslai. Aprašoma tyrimo metu naudojama aparatinė ir programinė įrangos, atliekami kiekybiniai ir kokybiniai tyrimai.

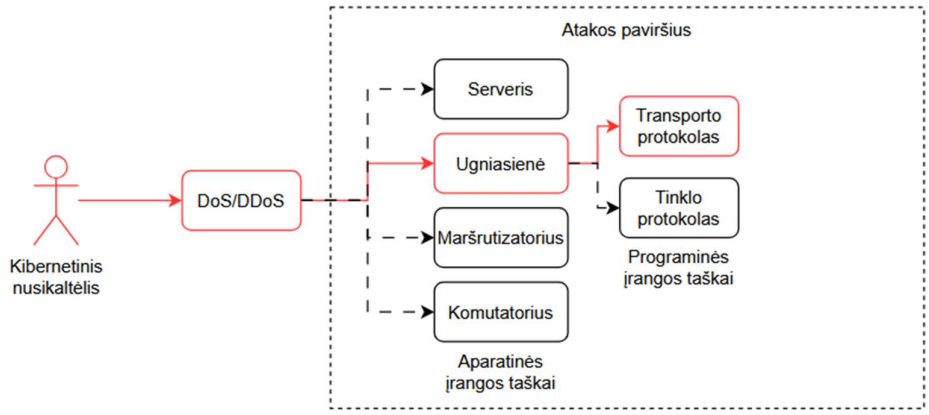
1. DoS/DDoS atakos paviršiaus charakterizavimo analizė

Pagrindinė šio magistrinio darbo užduotis yra sudaryti DoS/DDoS atakos požymiais pagrįstą atakos paviršiaus charakterizavimo modelį, pagal kurį realizavus atitinkamą programą būtų galima identifikuoti atakos paviršių atakuojamoje sistemoje vien tik iš tinklo srauto failų. Šiame darbe atliktas charakterizavimas apima ne tik įprastą atakos paviršiaus charakterizavimą, bet ir jo išskaidymą vertikaliai, kuriuo metu identifikuojami atakuojami įrenginiai ir paslaugos yra išdėstyti į gylį, pagal *Purdue* modelio siūlomą gynyba gilyn (*angl. defence in depth*) tinklo segmentavimo principą. Šis darbas atlieka analizę apie atakos paviršiaus nustatymą jau po įvykusios atakos, tad šiame darbe nėra analizuojamas DoS/DDoS atakų aptikimas ir užkardymas realiu metu.

Atakos paviršius (*angl. attack surface*) skirtingoje literatūroje suprantamas skirtingai, dėl to yra sudėtinga suprasti tyrėjų pateiktas ataskaitas arba straipsnius. Apie šią problemą rašoma mokslininkų C. Theisen'as ir kt [11], kurie atliko tyrimą išanalizavę 644 šaltinius, kuriuose buvo naudojama frazė „atakos paviršius". Šiame tyrime jie nustatė, kad didžioji dalis tyrėjų vis dar skirtingai interpretuoja ir neturi susiformavusios vienodos nuomonės dėl „atakos paviršiaus" sąvokos, taip kaip yra su kitomis sąvokomis, pavyzdžiui, „saugos pažeidžiamumas" (*angl. security vulnerability*). Šie mokslininkai pateikė keletą pavyzdžių, kada turėtų būti vartojama „atakos paviršiaus" sąvoka ir taip pat pabrėžė, kad šis terminas vis tiek turėtų būti papildomai tikslinamas kiekviename naujame darbe. Taigi, laikantis rekomendacijos paaiškinama, kad šiame darbe sąvoka „atakos paviršius" reiškia visus aparatinius ir programinius taškus, prijungtus prie tinklo, į kuriuos gali būti pasikėsinta naudojant skirtingus atakos vektorius pagal tai, kaip šie terminai vartojami kompanijos „Fortinet" [12]. Atakos vektorius – tai vienas konkretus metodas, kuris yra naudojamas kibernetinių nusikaltėlių atliekant kibernetinį nusikaltimą. Taigi DoS ir DDoS yra atakos vektoriai ir jie turi tik sau aktualų atakos paviršių atakuojamoje sistemoje. Šių atakos vektorių atakos paviršiaus pavyzdys pateikiamas 1.1 ir 1.2 paveikslėliuose.



1.1 pav. Supaprastintas atakos paviršius nurodant serverį ir DNS paslaugą kaip atakuojamus taškus



1.2 pav. Supaprastintas atakos paviršius nurodant ugniasienę ir transporto protokolą kaip atakuojamus taškus

1.1. Esamų atakos paviršiaus charakterizavimo tyrimų analizė

Toliau analizuojama literatūra nebūtinai susijusi su DoS ir DDoS atakomis. Tai daroma norint surinkti kuo daugiau informacijos apie šiuo metu esančius tyrimus apie atakos paviršiaus charakterizavimą.

Tyrėjų H. S. Obaid'o ir E. H. Abeed'o 2020 metais išleistoje publikacijoje yra rašoma apie DoS ir DDoS atakos tipus skirtinguose OSI modelio lygmenyse [13]. Nors šiame straipsnyje nėra rašoma tiesiogiai apie atakos paviršių ir išvis ši sąvoka šiame straipsnyje net nevartojama, visgi šiame straipsnyje galima įžvelgti atakos tipų klasifikavimą pagal programinių taškų grupes – OSI lygmenis. Šiame straipsnyje nėra informacijos apie aparatinius taškus.

OWASP yra tarptautinė ne pelno siekianti organizacija, skirta gerinti žiniatinklio paslaugos apsaugą [14]. Ji savo pateikiamose užrašinėse (*angl. cheatsheets*) DDoS atakos paviršių suskirsto į tris pagrindines kategorijas: paslaugų (*angl. application*), protokolo (*angl. protocol*) ir talpumo (*angl. volumetric*) [15]. Atitinkamai šios kategorijos vėliau yra papildomai detalizuojamos atakos tipais. Tačiau toks klasifikavimas nepadeda aiškiai suprasti kuriuos įrenginius atakuojamose sistemoje ši ataka gali atakuoti, kadangi šis būdas labiau primena įprastą atakos tipų klasifikavimą į atskiras grupes.

2021 metais mokslininkai N. Tripathi ir kt. [16] parašė straipsnį apie taikomojo lygmens DDoS atakas ir gynybos mechanizmus. Šiame straipsnyje jie šiek tiek užsimena apie atakos paviršių skirtinguose taikomojo lygmens protokoluose. Taip pat jie aprašo kaip konkrečiuose HTTP/1.1 ir HTTP/2 protokoluose galima papildomai įžvelgti platesnį atakos paviršių, nes protokolų vystytojai vis dar mažiau atsižvelgia į saugumą negu į funkcionalumą. Visgi šis straipsnis pateikia tik dalinį DDoS atakos paviršių paslaugų lygmenyje.

Mokslininkai iš Pensilvanijos valstijos universiteto 2020 metais parašė straipsnį apie kibernetinių atakų paviršiaus identifikavimą daiktų interneto tinkluose [17]. Šiame darbe jie nekalbėjo apie DoS ir DDoS atakos paviršiaus nustatymą, tačiau šis straipsnis pateikia įžvalgų kaip yra klasifikuojamas aparatinės įrangos atakos paviršius pagal atskirus sektorius (namų ūkio, sveikatos, transporto, finansų, pramonės įstaigų), atitinkamai analizuojant tik tam sektoriui būdingus IoT (*angl. Internet of Things*) įrenginius. Šis straipsnis puikiai suteikia galimybę suprasti, kad skirtinuose sektoriuose, atakos paviršius yra skirtingas dėl joje naudojamų specifinių įrenginių.

Apie atakų paviršiaus nustatymą buvo rašoma ir 2022 metais mokslininkų T. Ashley ir kt. [18], kurie bandė charakterizuoti atakos paviršių OT ir ICS (*angl. industrial control systems*) tinkluose. Šiame straipsnyje jie charakterizavo atakuojamą ICS įrangą pagal jų naudojamus protokolus ir prievadus. Nors šiame straipsnyje taip pat nerašoma konkrečiai apie DoS arba DDoS atakas, tačiau suteikiama naudingų įžvalgų, kurios padeda geriau suprasti kaip identifikuojami programiniai taškai įrenginyje.

Atlikus literatūros apžvalgą, nustatyti būdai ir principai pagal kuriuos šiuo metu yra charakterizuojamas atakos paviršius sistemoje. Tai apima įrenginių klasifikaciją pagal skirtingus sektorius ir jų identifikavimą pagal prievadus ir protokolus. Visgi atliekant analizę pastebėtas DoS/DDoS atakos paviršiaus charakterizavimo modelių trūkumas viešajame internete.

1.2. Esamų įrankių atakos paviršiui identifikuoti apžvalga

Dėl viešajame internete pastebėto informacijos trūkumo susijusio su DoS ir DDoS atakų paviršiaus charakterizavimu, toliau pateikiama apžvalga apie esamus įrankius, kurie kartu arba atskirai yra naudojami įvykusių kibernetinių incidentų analizei ir atakos paviršiaus identifikavimui.

1.2.1. Esami atakos paviršiaus identifikavimo įrankiai

„Wireshark“ – atviro kodo tinklo srauto analizavimo programa [19], kuri yra naudojama atliekant detalią tinklo srauto analizę. Ši programa, padedant jos integruota statistikos generavimo savybe, geba analizuoti PCAP tinklo srauto faile [20] užfiksuotų protokolų, IP (*angl. Internet Protocol*) ir MAC (*angl. Media Access Control*) adresų, prievadų pasiskirstymą, tokiu būdu suteikiant galimybę pastebėti tinkle veikiančius įrenginius ir jų naudojamus protokolus. Ši programa reikalauja atitinkamos patirties turinčio eksperto, kadangi pateiktos informacijos kiekis yra ypač didelis.

Atviro kodo **„Zeek“** programa yra naudojama pasyviam tinklo srauto stebėjimui ir analizavimui [21]. „Zeek“ užfiksuoja visus tinklo įvykius ir surašo juos į žurnalinius failus (*angl. logs*). Ši programa pasižymi tuo, kad atskiruose žurnaliniuose failuose surašo ne tik prisijungimus tarp įrenginių, bet ir komunikacijas vykstančias tarp skirtingų aplikacijų, kurios veikia septintame OSI modelio lygmenyje ir naudoja aukšto lygmens protokolus, tokius kaip HTTP (*angl. HyperText Transfer Protocol*), DNS (*angl. Domain Name System*) ir t.t. „Zeek“ pateikiami failai yra JSON formato [22], o tai suteikia galimybę šiuos failus panaudoti kitose, trečiųjų šalių, sistemose.

Saugumo informacijos ir įvykių valdymo (*angl. Security Information and Event Management – SIEM*) sistemos [23]. Šios sistemos surenka dubliuojamą tinklo srautą, išskaido jį žurnaliniais failais ir pateikia vartotojams apibendrintą informaciją ataskaitų skydelyje (*angl. dashboard*). Išskaidyti failai laikomi ilgą laiką, suteikiant galimybę juos vėliau detaliai peržiūrėti. *SIEM* sistemos įprastai skirtos grėsmių aptikimui ir incidentų valdymui realiu metu, jos yra didelės apimties, kompleksiškos ir reikalaujančios didelės darbuotojų kompetencijos.

Toliau peržiūrimi kiti įrankiai, kurie nėra skirti tiesiogiai tirti DoS ir DDoS atakoms, tačiau šie įrankiai yra artimi šiame darbe projektuojamam modeliui.

„NetworkMiner“ – kriminalistikoje naudojamas įrankis [24], kuris geba iš PCAP tinklo srauto failo ištraukti informaciją apie įrenginius ir komunikacijas vykstančias tarp jų. Programa automatiškai inventorizuoja aptiktą įrangą pateikdamas duomenis apie įrenginio operacinę sistemą, NIC tinklo plokštę, išsiųstų, bei gautų paketų skaičių ir kitus ypatumus. Ši programa taip pat iš pačios

komunikacijos gali ištraukti failus kurie buvo siunčiami tinkle, slaptažodžius ir kitą konfidencialią informaciją.

EmberOT kompanijos sukurtas ir nemokamai dalinamas **„OT PCAP analizatorius“** (*angl. OT PCAP analyzer*) [25] yra skirtas OT įrenginių ir protokolų analizei, iš pateikto PCAP failo, atlikti. Šis įrankis aptinka ir pateikia informaciją ne tik apie OT, bet ir apie IT įrenginius. Ši programa vartotojui pateikia surinktą informaciją ataskaitų skydelyje dviejuose languose: Bendrinė apžvalga (*angl. overview*), kurioje pateikia statistinius duomenis apie užfiksuotus protokolus ir turto suvestinė (*angl. asset summary*), kurioje pateikiama informacija apie užfiksuotus įrenginius. Šis įrankis gan paprastai ir suprantamai pateikia surinktą informaciją apie skirtingas sistemas ir protokolus. Įrankis dalinai pateikia statistinę įrenginių pasiskirstymo vizualizaciją ir skaido įrenginius į skirtingus sektorius pagal IT ir OT sistemas.

1.2.2. Esamų įrankių apžvalgos apibendrinimas

Peržiūrėti pagrindiniai įrankiai ir programos skirtos įvykusiems kibernetiniams incidentams atlikti. Kiekviena programa turi savo stiprybių ir silpnybių, visgi norint išsamiai išanalizuoti DoS/DDoS atakos paviršių reikėtų naudoti kelis įrankius, kadangi šiuo metu nėra vieno universalaus įrankio, kuris galėtų tai atlikti savarankiškai. Apibendrinta išanalizuotų įrankių informacija pateikta 1.1 lentelėje.

1.1 lentelė. Esamų kibernetinių atakų atakos paviršiaus analizavimo įrankių palyginimas

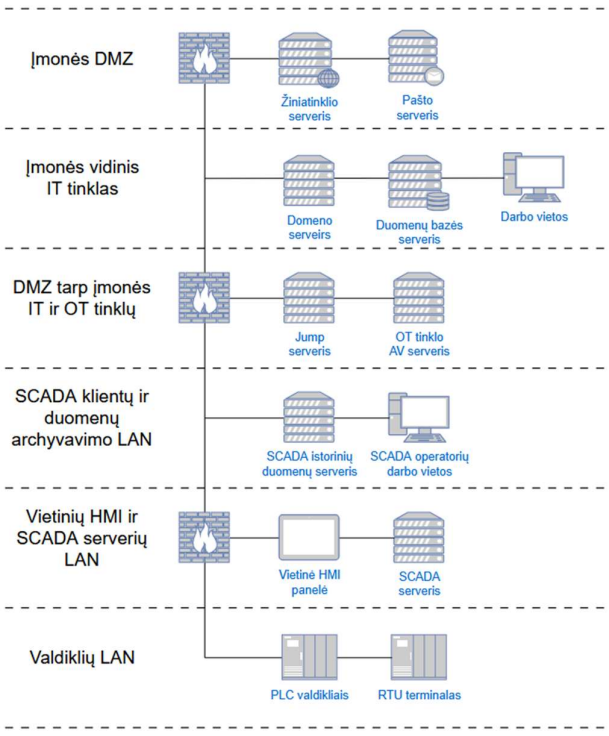
Savybė	**„Wireshark“**	**„Zeek“**	**„SIEM“**	**„NetworkMiner“**	**„EmberOT“**
Grafinė sąsaja	Taip	Ne	Taip	Taip	Taip
Naudojimo lygis	Sudėtingas	Sudėtingas	Sudėtingas	Vidutinis	Lengvas
Reikalaujamos techninės žinios	Labai aukštos	Aukštos	Labai aukštos	Vidutinės	Vidutinės
Identifikuojamas atakos paviršius	Taip	Taip	Taip	Dalinai	Dalinai
Sudaroma galimybė perduoti informaciją trečiajai šaliai	Taip	Taip	Taip	Taip	Ne
Vizualizacijos sudarymas	Ne	Ne	Dalinai	Ne	Dalinai
Skirta OT sistemoms analizuoti	Taip	Ne	Taip	Ne	Taip
Išskaidytas atakos paviršius pagal IT ir OT sektorius	Ne	Ne	Ne	Ne	Taip

1.3. *Purdue* modelis ir jo reikšmė OT sistemai

Kuriamas naujas modelis išskaido atakos paviršių į sektorius pagal IT ir OT sistemas. Šis skaidymas yra atliekamas panaudojant *Purdue* modelį, kuris yra aprašomas toliau skyriuje.

Purdue modelis apibūdina kritinės infrastruktūros tinklą, nurodydamas kaip jis turėtų būti saugiai segmentuotas, atskiriant įmonės IT sistemas nuo OT sistemų. Tokiu būdu yra įgyvendinamas principas gynyba gilyn viduje. Pagal šį modelį sistema yra suskirstoma į šešis lygmenis. Aukščiausiame, penktame, lygmenyje yra organizacijos DMZ (*angl. Demilitarized Zone*) zona,

kurioje yra visi viešai prieinami serveriai ir aplikacijos. Ketvirtame lygmenyje yra vidiniai įmonės serveriai: domenas, duomenų bazės, darbo vietos. Įprastai šie įrenginiai nėra viešai prieinami iš išorės. Žemiau esančiame lygmenyje yra tarpinė riba tarp ketvirto ir trečio lygmenų – DMZ zoną tarp organizacijos vidinių IT ir OT tinklų. Šiame lygmenyje yra visi įrenginiai, kurie naudojami netiesioginiam duomenų perdavimui tarp įmonės intraneto ir jos OT tinklo. Trečiame lygmenyje turime OT tinklą, kuriame yra atskiras, gamybos sistemoms, skirtas domeno ir duomenų serveriai. Šiame lygmenyje taip pat yra SCADA (*angl. Supervisory Control and Data Acquisition*) istorijos serveriai, inžinerinės darbo vietos. Antrame lygmenyje yra SCADA serveriai, lokalios HMI (*angl. Human-Machine Interface*) panelės. Pirmame lygmenyje yra įvairūs PLC (*angl. Programmable Logic Controller*), RTU (*angl. Remote Terminal Unit*) ir kiti valdikliai. Nuliniame lygmenyje yra įvairūs sensoriai, matuokliai, pavaros. *Purdue* modelio topologija pavaizduota 1.3 paveiksle.



1.3 pav. *Purdue* modelis [10]

Atlikus analizę nustatyta, kad pagal tinklo sraute užfiksuotą prievadą yra nustatoma teikiama paslauga serveryje ir naudojamas protokolas, o pagal šią informaciją toliau yra galimybė įrenginiams priskirti atitinkamą lygmenį pagal *Purdue* modelį. Pritaikius šį modelį, pagal atakuojamą tinklo segmentą, yra įvertinamas atakos loginis gylis sistemoje.

1.4. DoS/DDoS atakos tipų IT ir OT sistemose apžvalga

Šiame skyriuje apžvelgiami DoS ir DDoS atakų tipai, kurie toliau yra naudojami atakos paviršiaus klasifikavimui sudaryti. Atakos tipai suskirstomi į tinklo pralaidumo ir įrenginių resursų išnaudojimo, bei specifines įrenginių sugadinimo atakos klases.

1.4.1. Tinklo pralaidumo išnaudojimo atakos

Tinklo pralaidumui pakenkti naudojamos atakos dažniausiai skirstomos į perpildymo (*angl. flooding*), pastiprinto perpildymo (*angl. amplification flooding*) ir nukreipto perpildymo (*angl.*

reflection flooding) atakas. Visų perpildymo atakų metu pagrindinis tikslas yra išeikvoti aukos tinklo pralaidumą siunčiant į jį didelį kiekį netikrų užklausų iš kitų įrenginių. Šioms atakoms yra naudojami didžiuliai užkrėstų kompiuterių tinklai, kurie naudodami kenkėjišką įrangą padeda sukurti ir išsiųsti netikras užklausas į aukos įrenginius. Nusikaltėlis, norėdamas pradėti ataką, nuotoliniu būdu, tiesiogiai arba per užkrėstus tarpininkus, išsiunčia nurodymą visiems užkrėstiems įrenginiams pradėti puolimą nurodytu IP adresu. Toliau peržiūrimos šios klasės atakos tipai [26], [27], [28].

Perpildymo atakos:

a) UDP (*angl. User Datagram Protocol*) perpildymas – atakos metu yra išnaudojamas UDP protokolas ir jo savybė nesudaryti patikimo prisijungimo tarp kliento ir serverio. Atakos metu nusikaltėlis siunčia didelį kiekį suklastotų UDP paketų į aukos serverio skirtingus prievadus. Tokiu būdu aukos tinklas yra perpildomas neteisėtu srautu ir todėl sumažėja bendras tinklo pralaidumas, suprastėja komunikavimas tarp tinklo įrenginių;

b) ICMP (*angl. Internet Control Message Protocol*) perpildymas – atakos metu yra išnaudojamas ICMP protokolas, kuris naudojamas tinklo įrenginių priežiūrai. Atakos metu nusikaltėlis siunčia didelį kiekį suklastotų ICMP paketų į aukos tinklo įrenginius. Aukos įrenginiai, naudodami savo resursus, bando atsakinėti į suklastotus paketus. Tokiu būdų aukos tinklas yra perpildomas neteisėtais paketais, sumažėja tinklo pralaidumas ir įrenginių komunikacija tarpusavyje.

Pastiprinto perpildymo atakos:

a) DNS pastiprintas perpildymas – atakos metu yra išnaudojami vieši DNS serveriai, kurie skirti išversti tinklapių žodinius adresus į kompiuteriui suprantamą IPv4 formos adresą. Atakos metu nusikaltėlis siunčia suklastotus paketus į viešus DNS serverius, kaip siuntėją nurodydamas aukos IP adresą. DNS serveriai generuoja atsakymus ir siunčia į aukos serverį. Tokiu būdų nusikaltėlis nukreipia srautą į aukos tinklą ir jį perpildo. Išskirtinė šios atakos savybė yra, jog gana nedidelis nusikaltėlio užklausų srautas gali virsti milžinišku;

b) NTP (*angl. Network Time Protocol*) pastiprintas perpildymas – atakos metu yra išnaudojami vieši NTP serveriai, kurie naudojami tinklo įrenginių laikui sinchronizuoti. Atakos metu, nusikaltėlis, išsiunčia suklastotas užklausas NTP serveriams nurodydamas aukos IP adresą kaip siuntėją. NTP serveriai generuoja atsakymus ir siunčia į aukos serverį sugeneruotą srautą. Pateikus tinkamą užklausą NTP serveriui, šis gali sugeneruoti daug didesnį atsakymą. Dėl šios priežasties ši ataka yra dirbtinai išpučiama ir aukos tinklas perpildomas neteisėtu srautu.

Nukreipto perpildymo atakos:

a) SSDP (*angl. Simple Service Discovery Protocol*) nukreiptas perpildymas – atakos metu yra išnaudojamas UPnP (*angl. Universal Plug and Play*) protokolas, kuris padeda automatiškai susijungti įrenginiams tarpusavyje. Nusikaltėlis siunčia suklastotą su aukos IP adresu paketą UPnP įrenginiui, prašydamas pateikti informaciją apie save ir savo turimas funkcijas. UPnP įrenginys generuoja atsakymą siuntėjui tokiu būdu perpildydamas aukos tinklą;

b) Chargen (*angl. Character Generator Protocol*) nukreiptas perpildymas – atakos metu išnaudojamas simbolių generavimo serveris, kuris įprastai naudojamas tinkle esančioms problemoms ieškoti. Atakos metu siunčiamas suklastotas paketas su aukos IP adresu UDP

protokolu, o ši paslauga generuoja atsakymą į aukos mašiną. Tokiu būdu aukos tinklas yra perpildomas neteisėtais paketais;

c) Portmap (*angl. Port Mapper*) nukreiptas perpildymas – atakos metu išnaudojama prievadų žemėlapio sudarymo paslauga. Nusikaltėlis siunčia padirbtą paketą su aukos IP adresu viešai pasiekiamam serveriui ir jame veikiančiai prievadų žemėlapio sudarymo paslaugai, o ši atsako į užklausą siųsdamas atsakymą aukos tinklo kryptimi;

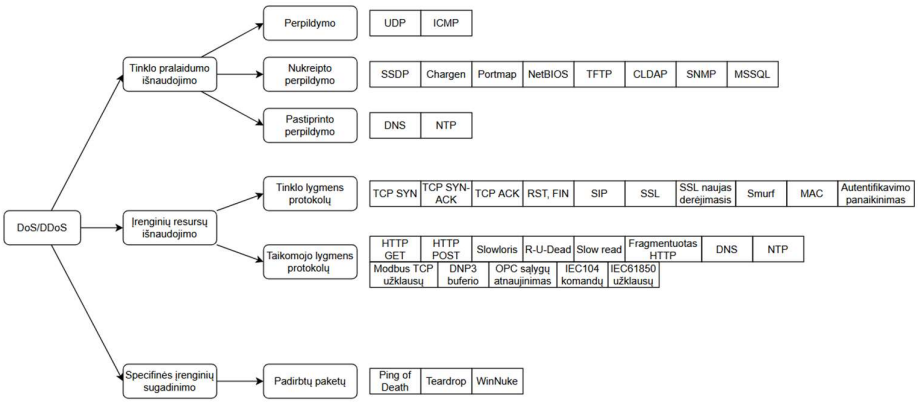
d) NetBIOS (*angl. Network Basic Input/Output System*) nukreiptas perpildymas – atakos metu išnaudojama tinklo įvesčių ir išvesčių paslauga. Nusikaltėlis siunčia suklastotą su aukos IP adresu užklausą serveriui su šia paslauga, o toliau servisas generuoja ir siunčia atsakymą į aukos tinklą;

e) TFTP (*angl. Trivial File Transfer Protocol*) nukreiptas perpildymas – Atakos metu yra sudaromas specialus paketas su nurodytu aukos IP adresu ir jis siunčiamas į nurodytą TFTP paslaugą teikiantį serverį. Paslauga gavus užklausą atitinkamai generuoja atsakymą aukos tinklo kryptimi;

f) CLDAP (*angl. Connectionless Lightweight Directory Access Protocol*) nukreiptas perpildymas – atakos metu išnaudojamas LDAP serveris kuris naudojamas vartotojų autentifikacijai. Nusikaltėlis siunčia užklausą LDAP serveriui su suklastotu aukos IP adresu o šis generuoja ir siunčia atsakymą siuntėjui;

g) SNMP (*angl. Simple Network Management Protocol*) nukreiptas perpildymas – atakos metu naudojamasi SNMP protokolu, kuris yra skirtas įvairių tinklo įrenginių valdymui ir jų būsenos stebėjimui. Atakos metu nusikaltėlis siunčia suklastotą su aukos IP adresu užklausą tinklo įrenginiams, o šie generuoja atsakymus siuntėjui. Tokiu būdu ataka yra nukreipiama į pasirinktą aukos įrenginį;

h) MSSQL (*angl. Microsoft Structured Query Language*) nukreiptas perpildymas – atakos metu yra išnaudojamas MC-SQLR (*angl. SQL Server Resolution*) protokolas, kuris naudojamas gauti informacijai apie duomenų bazę iš MS SQL serverio. Nusikaltėlis siunčia suklastotą su aukos IP adresu paketą MS SQL serveriui, o šis generuoja ir siunčia informaciją apie turimą duomenų bazę aukos kryptimi.



1.4 pav. DDoS atakos tipų klasifikavimas

1.4.2. Įrenginių resursų išnaudojimo atakos

Įrenginių resursų išnaudojimo atakos pasinaudoja įvairiuose protokoluose esančiais pažeidžiamumais. Pagrindinis šių atakų tikslas yra atakuoti aukos įrenginio resursus, užverčiant jį didžiuliu, netikrų paketų arba užklausų kiekiu. Tokiu būdu atakuojamoje sistemoje yra išnaudojamas didelis resursų kiekis, šių suklastotų paketų ir užklausų apdorojimui ir yra sutrikdomas kitų klientų aptarnavimas. Toliau peržiūrimi šios klasės atakos tipai [29], [30], [31], [32], [33], [34].

Protokolų atakos:

a) TCP (*angl. Transmission Control Protocol*) SYN perpildymas – atakos metu yra pasinaudojama TCP protokolo, trijų rankų paspaudimo savybė, kuri yra naudojama patikimam komunikacijos sudarymui tarp kliento ir serverio. Atakos metu nusikaltėlis siunčia didelį kiekį SYN paketų aukos tinklo įrenginiui ir ignoruoja aukos serverio pateiktus SYN-ACK atsakymus. Tokiu būdu serveris rezervuoja dalį savo resursų susijungimo sudarymui, kuris niekada nebus užbaigtas, o prisipildžius atminčiai yra sutrikdomas teisėtų klientų prisijungimas.

b) TCP SYN-ACK perpildymas – atakos metu išnaudojami trijų rankų paspaudimo SYN-ACK paketai. Atakos metu nusikaltėlis išsiunčia didelį kiekį SYN-ACK paketų į aukos serverį. Serveris naudoja vidinius resursus ir šiuos paketus tikrina vidinėse lentelėse ir vertina ar prisijungimas turi būti tęsiamas. Tokiu būdų yra išnaudojami serverio resursai.

c) TCP ACK perpildymas – atakos metu išnaudojami TCP protokolo, trijų rankų paspaudimo, ACK paketai, kurie naudojami pilnai užbaigti susijungimą tarp dviejų įrenginių. Atakos metu nusikaltėlis išsiunčia didelį kiekį ACK paketų į aukos serverį. Serveris priima ACK paketus ir tikrina juos vidinėse lentelėse ir vertindamas ar prisijungimas turi būti užbaigiamas. Tokiu būdų yra išnaudojami serverio resursai neegzistuojančiam susijungimui patikrinti.

d) TCP RST, FIN perpildymas – atakos metu yra išnaudojami RST arba FIN paketai, kurie naudojami patvirtinti užbaigimą tarp dviejų įrenginių. Nusikaltėlis siunčia didelį kiekį RST arba FIN paketų į aukos serverį, o šis skiria dalį atminties šiems susijungimams patikrinti vidinėse lentelėse.

e) SIP (*angl. Session Initiation Protocol*) perpildymas – atakos metu yra išnaudojamas SIP protokolas, kuris naudojamas skambučiams internetu sudaryti. Atakos metu yra kuriami ir siunčiami dideli kiekiai padirbtų INVITE, REGISTER arba OPTIONS paketų VoIP (*angl. Voice over IP*) paslaugų teikėjams. Kadangi paslaugos teikėjai turi skirti resursų neteisėtoms užklausoms atsakyti, sutrinka VoIP teikimas teisėtiems vartotojams.

f) SSL (*angl. Secure Sockets Layer*) perpildymas – atakos metu išnaudojamas SSL protokolas, kuris naudojamas saugiai komunikacijai tinkle sudaryti. Atakos metu serveriui siunčiamas didelis kiekis prašymų pateikti informaciją apie savo turimus sertifikatus. Serveris skiria resursus atsakymo generavimui ir pateikia savo turimus sertifikatus, bei naudojamus šifrus.

g) SSL naujo derėjimosi perpildymas – atakos metu išnaudojamas SSL protokolas. Nusikaltėlis sudaro daugybę saugių komunikacijų tinkle su atakuojamu serveriu pilnai įvykdydamas SSL keturių rankų paspaudimą, tačiau iškart po to jis nusiunčia serveriui prašymą iš naujo derėtis dėl rakto. Serveris turi skirti didelius resursus kriptografinėms užduotim spręsti, perskaičiuojant naujus raktus.

h) „Smurf“ ataka – atakos metu išnaudojamas ICMP protokolas, kuris skirtas tinklo įrenginių priežiūrai. Nusikaltėlis siunčia padirbtą su aukos IP adresu aido paketą tinklo transliacijos adresu. Tokiu būdu aido užklausa yra paskirstoma visiems tinklo įrenginiams, kurie vienu metu generuoja atsakymą aukos įrenginio kryptimi. Tokiu būdu aukos įrenginys yra perpildomas ICMP paketais.

i) MAC perpildymas – atakos metu yra išnaudojama komutatorių savybė sudarinėti MAC adresų lenteles. Nusikaltėlis siunčia didelį kiekį padirbtų paketų, su skirtingais MAC adresais, į aukos komutatorių arba per jį į kitus įrenginius. Komutatorius sudarinėja MAC adresų lentelę priskirdamas naujus adresus atitinkamiems fiziniams prievadams. Tokiu būdu yra išnaudojami resursai lentelės sudarymui ir palaikymui.

j) Autentifikavimo panaikinimo ataka – atakos metu yra išnaudojama bevielės prieigos taško savybė sudaryti autentifikavimą ir asocijavimą su klientu. Prieš sudarant pilną prisijungimą prie bevielės prieigos taško, klientas su bevielio prieigos tašku apsikeičia autentifikavimo ir asocijavimo kadrais. Atakos metu nusikaltėlis, apsimesdamas klientu, siunčia į bevielį prieigos tašką autentifikavimo panaikinimo kadrą, o šis pilnai nutraukia susijungimą su tikru klientu. Tokiu būdu yra sutrikdomas bevielis prisijungimas.

Taikomojo lygmens atakos:

a) HTTP GET ir POST perpildymas – atakos metu yra naudojamasi HTTP protokolu, kuris naudojamas informacijai iš tinklapio gauti arba informaciją į tinklapį įrašyti. Atakos metu nusikaltėlis, siunčia didelį kiekį GET arba POST užklausų aukos tinklapio serveriui. HTTP GET metu serveris bando surinkti ir pateikti informaciją suklastotoms užklausoms, taip išnaudodamas savo turimus resursus. HTTP POST metu serveris apdoroja nusikaltėlių siunčiamą informaciją, įrašydamas ją į duomenų bazę arba atmesdamas.

b) Lėtas HTTP puolimas (Slowloris) – atakos metu yra išnaudojamas HTTP protokolas ir trukmė kiek yra laikoma aktyvi sesija tarp kliento ir serverio. Atakos metu nusikaltėlis iš skirtingų IP adresų sukuria daugybę naujų prisijungimų su aukos serveriu. Sudarytos sesijos yra dirbtinai laikomos aktyviomis kol aukos serveris, dėl neaktyvumo, šias sesijas nutraukia. Tokiu būdu, esant dideliam kiekiui tuščių sesijų, serverio ištekliai kurį laiką yra rezervuojami ir užlaikomi, taip dirbtinai serverį apkraunant.

c) Lėtas HTTP POST puolimas (R-U-Dead) – atakai įvykdyti nusikaltėlis turi surasti tinklapyje formos laukelį. Radus formą nusikaltėlis pradeda siųsti didelį kiekį HTTP POST užklausų imituodamas legalų srautą ir serveriui pranešdamas, kad bus siunčiama didelis duomenų kiekis. Po to pradedamas formos pildymas kiek įmanoma lėčiau, kad būtų išlaikyta esama komunikacija ir užimamai serverio resursai.

d) Lėtas HTTP GET puolimas (Slow read) – atakos metu nusikaltėlis siunčia daugybę HTTP GET užklausų serveriui, tačiau atsakymą iš serverio skaito kiek įmanoma lėčiau mažindamas segmento langa dydį ir tokiu būdu užlaikydamas komunikaciją. Tokiu būdu išnaudojami resursai esamoms komunikacijoms išlaikyti.

e) Fragmentuotas HTTP užtvindymas – atakos metu yra išnaudojamas HTTP protokolo fragmentavimo galimybė. Nusikaltėlis sudarydamas susijungimą su tinklapiu išskaido HTTP

paketus į mažesnius, atskirus, paketus ir siunčia juos serverius kiek įmanoma lėčiau. Tokiu būdu tinklapis bando skirti resursus ir išlaikyti aktyvų neteisėtą prisijungimą.

f) DNS perpildymas – atakos metu išnaudojamas DNS serveris, kuris naudojamas išversti žodinį adresą į IP. Šios atakos metu siunčiamas didelis kiekis netikrų DNS užklausų iš įvairių įrenginių tokiu būdu serverį perpildant.

g) NTP perpildymas – atakos metu yra sutrikdoma laiko sinchronizavimo paslaugos ir pačio serverio, kuriame ji veikia veikimas. NTP perpildymo tikslas yra siųsti didelį kiekį netikrų užklausų su prašymu patikslinti laiką.

h) ModbusTCP (*Modbus protokolas veikiantis TCP/IP tinkluose*) užklausų perpildymas – atakos metu nusikaltėlis siunčia didelį kiekį suklastotų paketų į valdiklį su atitinkamu funkciniu kodu taip jį perpildant. Tikslas nebūtinai yra sutrikdyti įrenginį, tačiau siunčiant šiek tiek didesnį srautą negu teisėti valdikliai, kontroliuoti klaidingą duomenų srautą operatoriui arba draudžiant operatoriui siųsti komandas į valdiklį.

i) DNP3 (*angl. Distributed Network Protocol 3*) buferio perpildymas – atakos metu yra išnaudojamas DNP3 protokolo pažeidžiamumas, kurio metu iš atakuojančio įrenginio siunčiant didelį kiekį suklastotų neprašomų atsakymų (*angl. unsolicated response*) į kontroliuojančią stotį. Perpildant buferį įrenginys ignoruoja kitus gaunamus neprašomus atsakymus iš teisėtų įrenginių.

j) OPC UA (*angl. Open Platform Communications Unified Architecture*) sąlygų atnaujinimo perpildymas – atakos metu yra išnaudojamas OPC UA pažeidžiamumas, kada serveris yra įtraukiamas į nuolatinį prisijungimo sąlygų atnaujinimą (*angl. unlimited condition refresh*) kenkėjiškam klientui. Tokiu būdu serveris bando išlaikyti prisijungimą nė neįtariant, jog klientas tai daro tyčia norėdamas užimti serverio resursus ir sutrikdyti prisijungimą teisėtiems klientams.

k) IEC 104 (*IEC 60870-5-104 standarto protokolas*) komandų perpildymas – atakos metu nusikaltėlis siunčia didelį kiekį suklastotų komandų į valdiklį tokiu būdu priverčiant jį išnaudoti resursus, įvertinant šias gautas komandas. Valdiklis negebėdamas apdoroti šias komandas gali sutrikti.

l) GOOSE (*angl. Generic Object-Oriented Substation Event, IEC 61850 standarto protokolas*) užklausų perpildymas – atakos metu yra siunčiama didelis kiekis GOOSE pranešimų į IED (*angl. intelligent electronic device*) įrenginį. Dėl šios priežasties sutrinka įrenginio normalus veikimas.

1.4.3. Specifinės įrenginių sugadinimo atakos

Specifinės įrenginių sugadinimo atakos pasižymi tuo, jog tikslas yra sustabdyti arba išjungti konkretų įrenginį ir sistemą panaudojant vos keletą paketų. Dažnu atveju tai DoS specifinės atakos ir jos yra siejamos su konkrečiomis operacinėmis sistemomis, protokolų įgyvendinimais ir dar neatrastais jų pažeidžiamumais (*angl. zero-day attack*). Toliau peržiūrimos šios klasės atakos.

Padirbtų paketų atakos:

a) Mirties aidas (*angl. Ping Of Death*) – atakos metu yra išnaudojamas tinklo valdymui skirtas „aido“ įrankis (*angl. Ping*). Nusikaltėlis siunčia padirbtą, didesnį negu yra galima, aido užklausą aukos serveriui. Serveris gavęs didesnį aido užklausą gali nepajėgti jo apdoroti, perpildyti savo

buferį ir išsijungti arba užstrigti. Šio tipo atakos buvo ypač pavojingos senesnėms operacinėms sistemoms.

b) „Teardrop“ – atakos metu yra išnaudojama fragmentavimo galimybė, kuri leidžia tinklu siųsti didesnius paketus negu įprastai. Nusikaltėlis siunčia padirbtą fragmentuotą paketą nurodydamas klaidingus slenksčius, tam kad aukos serveris nesugebėtų tinkamai suprasti šio paketo. Tokiu atveju serveris gali išsijungti arba užstrigti dėl nesugebėjimo apdoroti fragmentuoto paketo.

c) „WinNuke“ – atakos metu yra siunčiamas specialiai suformuotas TCP paketas su aktyvia „URG“ vėliavėle į atakuojamo įrenginio (Windows mašinos) 139 prievadą. Mašina nesugebėdama tinkamai apdoroti paketo išsijungia rodydamos BSOD (*angl. Blue screen of death*).

1.4.4. Atakos tipų klasifikavimas pagal OSI lygmenis

Antrame OSI lygmenyje yra MAC perpildymo ir autentifikavimo panaikinimo atakos. Šios atakos vyksta kanaliniame lygyje ir jos yra gana specifinės konkrečiam įrenginiui t.y komutatoriams ir bevielės prieigos taškams.

Trečiame lygmenyje yra atakos, kurios gali būti nukreiptos į daugumą tinklo įrenginių ir mašinų, kadangi šiame lygyje yra naudojamas paketų maršrutizavimai tarp skirtingų tinklų. Atakos gali būti nukreiptos ne tik į maršrutizatorius, bet ir į kitus aukštesnio lygio įrenginius tokius kaip ugniasienės ir serveriai. Populiariausios atakos ICMP perpildymas ir „Smurf“. Egzistuoja taip pat ir Mirties aido ir „Teardrop“ atakos, tačiau jos yra veiksmingos tik prieš senesnius įrenginius.

Atakos ketvirtame lygmenyje yra nukreiptos prieš įrenginių išteklius, kadangi yra atakuojami jų prievadai. Pažeidžiami visi ketvirtame lygyje galintys dirbti įrenginiai t.y ugniasienės ir serveriai. Dažniausiai pasitaikančios atakos yra įvairios TCP perpildymų variacijos: SYN, SYN-ACK, ACK, RST, FIN. UDP perpildymas vyksta ketvirtame lygmenyje, tačiau jis naudojamas tinklo resursams išnaudoti.

Atakos šeštame lygmenyje yra specifinės ir naudojamos prieš serverius kurie palaiko saugaus komunikavimo metodus. Pasitaikančios atakos SSL ir SSL naujo derėjimosi perpildymai.

Didžioji dalis atakų vyksta septintame OSI lygmenyje, kuris dar žinomas kaip taikomasis lygmuo. Šiame lygmenyje atakos atakuoja įvairias paslaugas, taip pat šiame lygmenyje atakos yra keliančios daugiausiai nerimo, kadangi jas sudėtingiausia atpažinti dėl panašumų su teisėtu srautu. Šios atakos naudoja tinkamai sudarytus TCP susijungimus ir šioms atakoms sėkmingai įvykti reikia mažesnio užklausų kiekio ir resursų. Apibendrinta atakos tipų pagal OSI lygmenis informacija pateikta 1.2 lentelėje.

1.2 lentelė. DDoS atakos tipai pagal OSI modelį

OSI modelio lygmuo	**DDoS atakos tipai**
7 lygmuo	DNS, NTP, HTTP GET ir POST, SIP perpildymai, SSDP, Chargen, Portmap, NetBIOS, TFTP, CLDAP, SNMP, MSSQL, DNS, NTP nukreipti perpildymai, Lėtas HTTP, HTTP POST, HTTP GET puolimas, fragmentuotas HTTP perpildymas, ModbusTCP užklausų perpildymas, DNP3 buferio perpildymas, OPC sąlygų atnaujinimo perpildymas, IEC 104 komandų perpildymas
6 lygmuo	SSL perpildymas, SSL naujo derėjimosi perpildymas
4 lygmuo	UDP perpildymas, TCP SYN, SYN-ACK, ACK, RST, FIN perpildymas, „WinNuke“

OSI modelio lygmuo	DDoS atakos tipai
3 lygmuo	ICMP perpildymas, „Smurf“ ataka, Mirties aidas, „Teardrop“
2 lygmuo	MAC perpildymas, autentifikavimo panaikinimo ataka, GOOSE užklausų perpildymas
1 lygmuo	Blokavimas (*angl. jamming*)

1.5. DoS/DDoS atakos paviršius pagal atakos tipus

Išanalizavus atakos tipus, pradedama atakos paviršiaus klasifikacija, kuri kaip buvo apibrėžta praeituose skyriuose, susideda iš visų pažeidžiamų aparatinių ir programinių taškų.

1.5.1. Aparatiniai taškai

Toliau aprašoma aparatinė įranga, kuri pagal atliktą atakos tipų analizę yra atakuojama skirtingais DoS ir DDoS atakos tipais. Peržiūrima įranga priklausanti ne tik IT sistemose, tačiau ir įranga, kuri aptinkama OT sistemose. Įvertinamos ir IoT, bei IIoT (*angl. Industrial Internet of Things*) sistemos, virtualios mašinos.

1) **Tinklo įrenginiai:**

   a) **Bevielės prieigos taškas** yra tinklo įrenginys, kuris leidžia sujungti kelis įrenginius tarpusavyje į vietinį tinklą bevieliu būdu, naudojant Wi-Fi technologiją. Šis įrenginys dirba pirmame ir antrame OSI lygmenyse, todėl jis gali būti atakuojamas pirmo ir antro OSI lygmens atakomis, tokiomis kaip ryšio blokavimas ir autentifikavimo panaikinimo ataka.

   b) **Komutatorius** yra įrenginys, kuris naudojant internetinį kabelį, fiziškai sujungia keletą įrenginių tarpusavyje į bendrą vietinį tinklą. Šis įrenginys duomenų perdavimui naudoja MAC lenteles, tokiu būdu žinodamas, kuriam galiniam įrenginiui, kuri informacija priklauso. Šis įrenginys dirba antrame OSI lygmenyje, todėl jis gali būti pažeidžiamas antro OSI lygmens ataka MAC užtvindymu.

   c) **Maršrutizatorius** yra tinklo įrenginys, kuris naudojamas norint tarpusavyje sujungti du skirtingus tinklus. Šis įrenginys yra atsakingas už tinkamą paketų maršrutų sudarymą tarp skirtingų tinklų. Maršrutizatorius dirba trečiame OSI lygmenyje, o tai reiškia jog šis įrenginys yra pažeidžiamas trečio OSI lygmens atakomis. Pagrindinė trečio lygmens ataka yra ICMP užtvindymas, kuriuo metu į įrenginį yra siunčiama daugybę ICMP užklausų.

   d) **Ugniasienė** yra viena iš svarbiausių įrenginių apsauganti nuo kibernetinių atakų iš išorės ir jo veikimas jau siekia ketvirtą OSI lygmenį. Visgi šis įrenginys yra pažeidžiamas dėl savo elementarios funkcijos – komunikacijos būsenų sekimo. TCP ir UDP užtvindymo atakos metu ugniasienė išsaugo visas būsenas vidinėje lentelėje ir laiko jas iki kol prisijungimas yra nutraukiamas. Pilnai užpildžius šią būsenų lentelę ugniasienė gali nebepriimti naujų prisijungimų.

2) **Galiniai įrenginiai:**

   a) **Serveriai** tai tinkliniai įrenginiai, kurie teikia įvairias paslaugas kitiems įrenginiams, vietiniame tinkle arba internete. Kadangi šie įrenginiai dirba septintame OSI lygmenyje, jie yra pažeidžiami septinto lygmens atakomis. Šie įrenginiai gali teikti vieną arba daugiau paslaugų tuo pačiu metu, o tai reiškia jie gali būti atakuojami skirtingais atakos tipais. Verta

paminėti, kad serveriai gali būti atakuojami ne tik septinto lygmens atakomis, tačiau ir ketvirto (TCP, UDP užtvindymai) bei trečio (ICMP užtvindymas) lygmens atakomis.

b) **HMI panelės** reikalingi įvairių procesų valdymui ir duomenų stebėjimui konkrečioje, gamybinėje, vietoje. Šie įrenginiai, kaip ir serveriai, veikia septintame OSI lygmenyje, gali būti atakuojami trečio, ketvirto ir septinto lygmens atakomis.

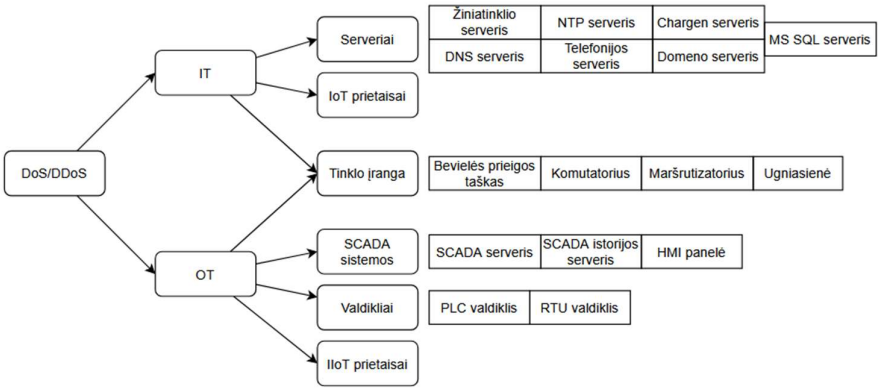
c) **PLC arba RTU valdikliai** yra skirti konkrečios sistemos automatizavimui. Šie įrenginiai autonomiškai surenka informaciją iš įvairių jutiklių ir pagal tam tikrą logiką siunčia komandas į įvairias pavaras arba perduoda šią informaciją toliau į duomenų surinkimo centrus. Šie įrenginiai veikia septintame OSI lygmenyje, o atakuojamas gali būti trečio, ketvirto ir septinto lygmens atakomis.

d) **IoT prietaisai** tai visi smulkūs įrenginiai, atliekantys konkrečias, dažniausiai nesudėtingas užduotis. Tai gali būti įvairi įranga išmaniuose namuose: išmanios lemputės, termostatai, užraktai, kameros ir t.t. Nors IoT įrenginiai gali būti atakuojami DoS ir DDoS atakomis, visgi šie įrenginiai įprastai nusikaltėlius domina dėl kitos priežasties – zombių tinklo (*angl. botnet*) sudarymo [35]. Būtent dėl to toliau nėra atskirai analizuojami šie įrenginiai, kadangi IoT įrenginiai yra įprastai atakuojami kitais atakos vektoriais, stengiantis juos užkrėsti ir užvaldyti, tokiu būdu priverčiant būti DDoS atakos šaltiniais.

e) **IIoT prietaisai** tai įvairūs pramonėje naudojami išmanūs sensoriai, matuokliai ir kiti panašūs prietaisai, kurie atlikdami specifinę užduotį, siunčia surinktus duomenis į aukščiau jų esančius įrenginius, tokius kaip PLC, RTU arba HMI. Šie įrenginiai taip pat gali būti atakuojamos DoS ir DDoS atakomis, kad būtų sutrikdytas šis duomenų perdavimas.

3) Virtuali įranga:

Kaip ir prieš fizinę įrangą, lygiai tokiu pat principu ir prieš virtualią, gali būti naudojamos DoS, bei DDoS atakos. Verta paminėti, kad atakos atveju prieš virtualizuotą įrangą, yra išnaudojami ne tik virtualaus įrenginio, bet ir kartu pačio hipervizoriaus resursai, o tai suteikia dar daugiau galimybių nusikaltėliams, kadangi įmonės kurios naudojasi debesijos paslaugomis ir moka paslaugų tiekėjams už išnaudojamą resursų faktą, susiduria su nauja DDoS atakos forma [36]. Vienas iš būdų yra atakuojant mažesniu atakos srauto dydžiu, tačiau periodiškai padidinant ir sumažinant šį srautą, taip sudarant periodinį pulsavimą. Dėl šios priežasties hipervizorius periodiškai padidina ir sumažina virtualios įrangos resursus, o dėl tokio resursų naudojimo įmonės vėliau turi atsiskaitinėti savo debesijos paslaugų tiekėjams. Tokio tipo ataka vadinama ekonominė tvarumo atsisakymo ataka (*angl. Economic Denial of Sustainability – EDoS*). Visgi šis būdas nepadidina atakos paviršiaus, tai yra atakos tikslo prisitaikymas prie debesijos paslaugų.



1.5 pav. DoS/DDoS atakų aparatinių taškų klasifikavimas

1.5.2. Programiniai taškai

Išanalizavus aparatinius taškus, pradedama programinių taškų analizė. Kad būtų paprasčiau suprasti, kokie programiniai taškai priklauso kuriems aparatiniams taškams, yra naudojama klasifikacija pagal OSI modelio lygmenis. Programiniai taškai susideda iš visų įrenginyje naudojamų pažeidžiamų protokolų, funkcijų arba teikiamų paslaugų.

1) **Kanalo lygmuo (antras OSI lygmuo):**

   a) **MAC adresų saugojimo funkcija** yra specifinė, komutatoriuose naudojama, funkcija, kuri naudojama norint tinkamai informacijos komutacijai tarp įrenginių bendrame vietiniame tinkle. Visgi ši funkcija yra pažeidžiama MAC užtvindymo atakos.

   b) **IEEE 802.11 protokolas (Wi-Fi)** yra taisyklių rinkinys, kuris aprašo kaip tiksliai turėtų būti sudaromas bevielis ryšys tarp dviejų įrenginių, tokiu būdu sudarant vietinį tinklą. Būtent šis protokolas ir turi pažeidžiamumą, kurio metu yra atliekama autentifikavimo panaikinimo ataka.

2) **Tinklo lygmuo (trečias OSI lygmuo):**

   a) **ICMP protokolas** naudojamas įvairių, bendrame tinkle prijungtų, įrenginių diagnostikos atlikimui. Šis protokolas turi pažeidžiamumų, kurių metu yra atliekamas ICMP užtvindymas ir „Smurf“ ataka.

   b) **ARP protokolas** naudojamas nuolat besikeičiančioje tinklo aplinkoje susieti įrenginių IP adresus su jiems priklausiančiais MAC adresais. Šis protokolas gali būti išnaudojamas norint atlikti ARP užtvindymo ataką.

   c) **IPv4 protokolas** yra taisyklių rinkinys, kuris aprašo kaip turėtų būti komunikuojama tarp skirtingų įrenginių bendrame tinkle. Visgi šis protokolas turi pažeidžiamumą, kuriuo metu yra atliekami fragmentavimo užtvindymas ir „Teardrop“ ataka.

3) **Transporto lygmuo (ketvirtas OSI lygmuo):**

   a) **TCP protokolas** vienas iš pagrindinių protokolų, kuris naudojamas norint sudaryti patikimą komunikaciją tarp skirtingų, įrenginiuose naudojamų, paslaugų. Šis protokolas pasižymi

patikimos komunikacijos užtikrinimu, tačiau tai yra išnaudojama įvairių tipų TCP užtvindymo atakų (SYN, ACK, RST ir t.t). Šis protokolas taip pat išnaudojamas ir „WinNuke“ atakai.

b) **UDP protokolas** taip pat svarbus komunikacijos protokolas, kuris naudojamas greitam duomenų perdavimui, nesudarant patikimo ryšio tarp įrenginyje veikiančių paslaugų. Tačiau dėl šios savybės šis protokolas yra išnaudojamas atliekant UDP užtvindymo atakas.

4) Atvaizdavimo lygmuo (Šeštas OSI lygmuo):

a) **SSL/TLS protokolas** yra naudojamas šifruotai ir saugiai komunikacijai sudaryti tarp įrenginiuose naudojamų paslaugų. Ši savybė yra išnaudojama SSL užtvindymo ir SSL naujo derėjimuisi atakoms atlikti.

5) Taikomasis lygmuo (Septintas OSI lygmuo):

a) **Žiniatinklio paslauga ir HTTP protokolas** naudojamas norint sukurti internetinius puslapius, kurie vartotojams galėtų pateikti tam tikrus dokumentus ir informaciją iš saityno (*angl. World Wide Web*). Tai viena iš svarbiausių paslaugų, kurią naudoja didžioji dalis tiek didelių, tiek mažų įmonių ir organizacijų. Atakos nukreiptos prieš žiniatinklio paslaugas ir HTTP protokolą gali būti skirtingos. Gali būti naudojamos HTTP užklausų užtvindymo, esamų HTTP sesijų, kiek įmanoma ilgiau išlaikymo, specialios HTTP užklausos, kurios tinklapio prašo pateikti didelį kiekį informacijos arba specialaus lėto komunikavimo, sudarius HTTP sesiją atakos.

b) **Vardų tarnybos paslauga ir DNS protokolas** naudojamas norint išversti lengvai įsimenamą žodinį vardą arba domeną į sudėtingiau žmogui įsimenamą IP adresą. Atakos tipas naudojamas prieš vardų tarnybos paslaugą vadinamas DNS užtvindymu. Vardų tarnybos paslauga gali būti išnaudojama ir kaip nukreiptos atakos dalis. Nusikaltėliai gali išnaudoti šią paslaugą ir padidintą keliasdešimt kartų srautą nukreipti į kitą subjektą tinkle. Toks atakos tipas vadinamas DNS pastiprinto užtvindymo ataka.

c) Laiko sinchronizavimo paslauga ir NTP protokolas naudojamas laikui sinchronizuoti tarp visų įrenginių tinkle. NTP užtvindymas yra vienas iš atakos tipų, kurio metu yra sutrikdoma laiko sinchronizavimo paslaugos ir pačio serverio, kuriame ji veikia veikimas. Laiko sinchronizavimo paslauga gali būti ne tik atakuojama, bet ir išnaudojama atakai nukreipti. NTP pastiprinto užtvindymo metu nusikaltėliai gali specialiai išnaudoti laiko sinchronizavimo veikimą ir keliasdešimt kartų padidintą srautą nukreipti į kitus subjektus tinkle.

d) Telefonijos paslauga ir SIP protokolas naudojamas interneto telefonijoje ryšiui sudaryti ir perdavinėti balsą, vaizdą arba kitus duomenis per kompiuterių tinklą. Ši paslauga naudojama įmonėse komunikavimui viduje ir su išore, tad tai yra svarbi verslo palaikymo dalis. Ataka nukreipta prieš interneto telefonijos paslauga yra SIP užtvindymas.

e) Simbolių generavimo paslauga ir Chargen protokolas naudojamas testavimo, klaidų ieškojimo arba tinklo srauto matavimo tikslais. Ši paslauga gali būti naudojama ir su TCP, ir su UDP protokolu, tačiau atakoje naudojamas būtent UDP protokolas. Simbolių generavimo paslauga yra išnaudojama nukreipto užtvindymo atakos metu.

f) **Katalogų prieigos paslauga ir CLDAP protokolas** naudojamas kaupti ir dalintis informacija organizacijos vidiniame tinkle. Ši paslauga gali laikyti informaciją apie organizacijos vartotojus, mašinas, tinklo įrenginius, sistemas, tinklus, servisus ir t.t. Tinkamai neapsaugota paslauga gali būti išnaudojama CLDAP nukreipto užtvindymo atakai.

g) **Prievadų žemėlapio sudarymo paslauga ir Portmap protokolas** naudojamas susieti nuotolinių procedūrų iškvietimo (RPC – *Remote Procedure Call*) programas su atitinkamais protokolais ir prievadais toje pačioje mašinoje, tokiu būdu sudarant galimybę RPC programomis naudotis kitoms mašinoms tinkle. Atakos tipas išnaudojantis šią paslaugą vadinamas Portmap nukreiptu užtvindymu.

h) **Tinklo bazinių įvesčių ir išvesčių paslauga ir NetBIOS protokolas** naudojamas komunikacijos sudarymui ir išteklių dalinimuisi tarp skirtingų kompiuterių taikomųjų programų lokaliame tinkle. Ši paslauga taip pat naudojama norint surasti tinkamus kompiuterius lokaliame tinkle. Konkrečiai NetBIOS vardų paslauga yra išnaudojama atakoje kaip nukreiptas užtvindymas.

i) **Microsoft SQL paslauga** yra reliacinė duomenų bazių valdymo sistema, kuri yra sukurta ir patentuota Microsoft kompanijos. Atakos tipas, kuris išnaudoja šią paslaugą yra MS SQL nukreiptas užtvindymas. Šios atakos metu yra pasinaudojama Microsoft SQL paslaugos leidimų servisu, kuris yra naudojamas klientui nuotoliu bandant prisijungti prie šios paslaugos.

j) **Industriniai komunikacijos protokolai** naudojami tarp įvairių PLC, RTU, IIoT įrenginių, HMI panelių ir SCADA sistemų. Visgi šie protokolai turi tam tikrų pažeidžiamumų, kurie gali būti išnaudojami specifinėms atakoms atlikti.

   i) **ModbusTCP protokolas** yra atviras industrinis protokolas veikiantis pagal TCP/IP modelį. Šis protokolas turi pažeidžiamumą, kuriuo metu yra atliekamas įvairių ModbusTCP užklausų ir komandų užtvindymas.

   ii) **DNP3 protokolas** atviro standarto industrinis protokolas naudojantis taškais pagrįstą (*angl. point-based*) adresų sistemą. Jis yra pažeidžiamas specifine DNP3 buferio užtvindymo ataka.

   iii) **OPC UA paslauga** naudojama duomenų surinkimui ir perdavimui tarp skirtingų gamintojų sistemų ir jų naudojamų industrinių protokolų. Ši paslauga gali būti išnaudojama OPC UA sąlygų atnaujinimo užtvindymo ataka.

   iv) **IEC 104 protokolas** yra IEC 60870-5-104 standartu pagrįstas protokolas, kuris naudojamas su TCP/IP modeliu. Šis protokolas yra pažeidžiamas IEC104 komandų užtvindymo ataka.

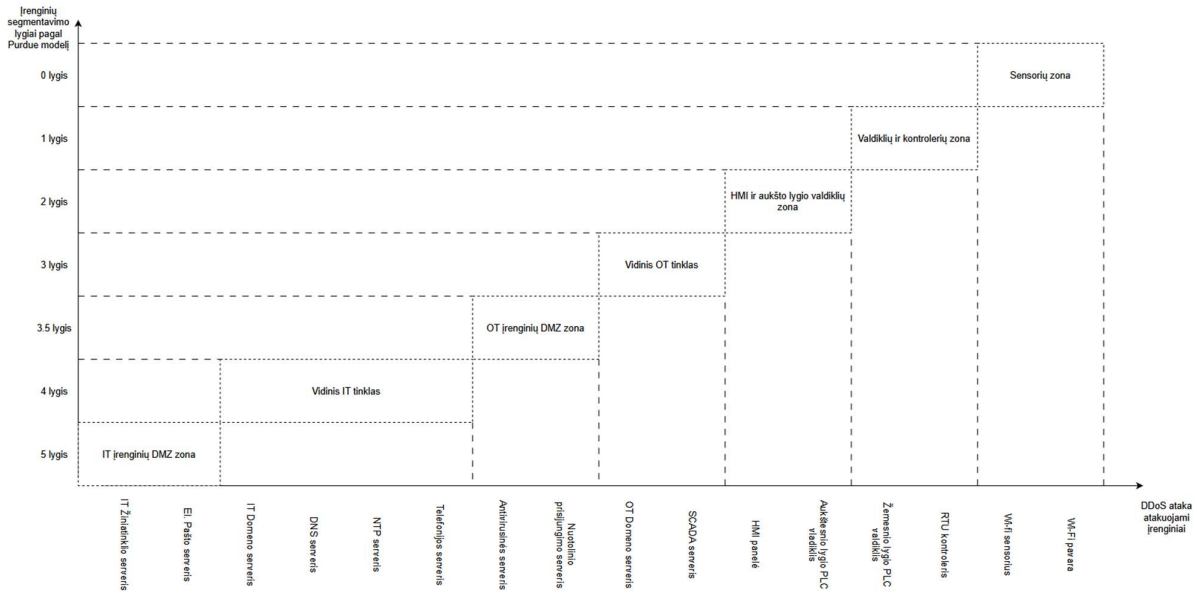
   v) **GOOSE protokolas** IEC 61850 standartu paremtas protokolas, naudojamas skirstyklų relinių apsaugų automatikoje. Jis pažeidžiamas GOOSE užklausų užtvindymo ataka.

1.5.3. Atakos paviršius pagal *Purdue* modelio lygmenis

Išanalizuotam atakos paviršiui yra pritaikomas *Purdue* modelis, kuris nurodo kaip gamybinėje įmonėje turėtų būti segmentuotas tinklas. Tai yra daroma, kadangi įrenginių išskaidymas pagal šį

modelį padeda geriau įvertinti įvykusios atakos gylį sistemoje, o tai geriau padeda įvertinti atakos pavojingumą ir galimus nuostolius. Įprastai IT tinkluose įvykusios atakos įmonėms atneša finansinių ir(arba) reputacinių nuostolių. Atakos prieš OT sistemas papildomai sukelia grėsmę sudėtingiems įrenginių procesams ir žmonių gyvybėms.

Kad būtų galima geriau suprasti atakos gylį sistemoje, atakos paviršius sujungiamas su *Purdue* modeliu ir sudaroma horizontali – vertikali atakos kreivė, kuri parodo kaip giliai DoS ir DDoS atakos atakuoja sistemą. Šioje kreivėje atakos gylis yra suskaidomas į šešis lygmenis, atakos plotas kiekviename lygmenyje yra skirtingas. Kiekvienas lygmuo turi aparatinius taškus, kurie susideda iš fizinių arba virtualių informacinių sistemų ir tinklo įrenginių. Kiekvienas įrenginys gali turėti vieną arba keletą pažeidžiamų programinių taškų. 1.6 paveiksle pateikiama horizontali – vertikali atakos kreivė.



1.6 pav. DoS/DDoS atakos gylis pagal *Purdue* modelį

1.3 lentelėje aprašomas tinklo įrenginių atakos paviršius, kuris yra aktualus visiems lygiams, kadangi visuose lygiuose įrenginiai yra tarpusavyje sujungti per tinklo įrenginius.

1.3 lentelė. Atakos paviršius tinklo įrenginiams

1-5 lygmenys	**Atakuojami aparatiniai taškai**	**Atakuojami programiniai taškai**	**Atakos tipai**
Tinklo įrenginiai	Bevielės prieigos taškas	IEEE 802.11 protokolas	Autentifikavimo panaikinimo ataka
	Komutatorius	MAC adresų saugojimo funkcija	MAC užtvindymas
	Maršrutizatorius	ICMP, IPv4 protokolai	ICMP užtvindymas
	Ugniasienė	ICMP, IPv4, TCP, UDP protokolai	ICMP užtvindymas, TCP, UDP užtvindymai

Toliau pateikiamos lentelės (1.4 – 1.9), kuriuose surašyti galimi aparatiniai ir programiniai taškai kiekviename lygyje, pradedant nuo penkto ir baigiant pirmu. Nulinis lygmuo yra neanalizuojamas, kadangi įprastai šiame lygmenyje nėra įrenginių veikiančių TCP/IP tinkluose.

1.4 lentelė. Atakos paviršius penktame *Purdue* modelio lygmenyje

Lygmuo	**Atakuojami aparatiniai taškai**	**Atakuojami programiniai taškai**	**Atakos tipai**
5 Lygmuo – Organizacijos DMZ zona	Viešas žiniatinklio serveris	HTTP protokolas, ICMP, IPv4, TCP, UDP protokolai	HTTP GET ir POST užtvindymai, Slowloris, R-U-Dead atakos, ICMP užtvindymas, TCP, UDP užtvindymai
	Viešas DNS serveris	DNS protokolas, ICMP, IPv4, TCP, UDP protokolai	DNS užtvindymas, DNS nukreiptas užtvindymas, ICMP užtvindymas, TCP, UDP užtvindymai

1.5 lentelė. Atakos paviršius ketvirtame *Purdue* modelio lygmenyje

Lygmuo	**Atakuojami aparatiniai taškai**	**Atakuojami programiniai taškai**	**Atakos tipai**
4 Lygmuo – Vidinio organizacijos tinklo zona	IT Domeno serveris	CLDAP, Portmap, NetBIOS protokolai, ICMP, IPv4, TCP, UDP protokolai	CLDAP, Portmap, NetBIOS nukreiptas užtvindymas, ICMP užtvindymas, TCP, UDP užtvindymai
	Vidinis DNS serveris	DNS protokolas, ICMP, IPv4, TCP, UDP protokolai	DNS užtvindymas, DNS nukreiptas užtvindymas, ICMP užtvindymas, TCP, UDP užtvindymai
	NTP serveris	NTP protokolas, ICMP, IPv4, TCP, UDP protokolai	NTP užtvindymas, NTP nukreiptas užtvindymas, ICMP užtvindymas, TCP, UDP užtvindymai
	Telefonijos serveris	SIP protokolas, ICMP, IPv4, TCP, UDP protokolai	SIP užtvindymas, ICMP užtvindymas, TCP, UDP užtvindymai

1.6 lentelė. Atakos paviršius tarp ketvirto – trečio *Purdue* modelio lygmenyje

Lygmuo	**Atakuojami aparatiniai taškai**	**Atakuojami programiniai taškai**	**Atakos tipai**
3,5 Lygmuo – DMZ tarp organizacijos OT ir IT tinklų	Antivirusinės serveris	ICMP, IPv4, TCP, UDP protokolai	ICMP užtvindymas, TCP, UDP užtvindymai
	Nuotolinio prisijungimo serveris	ICMP, IPv4, TCP, UDP protokolai	ICMP užtvindymas, TCP, UDP užtvindymai

1.7 lentelė. Atakos paviršius trečiame *Purdue* modelio lygmenyje

Lygmuo	**Atakuojami aparatiniai taškai**	**Atakuojami programiniai taškai**	**Atakos tipai**
3 Lygmuo – SCADA istorinių duomenų ir technologinio tinklo zona	OT Domeno serveris	CLDAP, Portmap, NetBIOS protokolai, ICMP, IPv4, TCP, UDP protokolai	CLDAP, Portmap, NetBIOS nukreiptas užtvindymas, ICMP užtvindymas, TCP, UDP užtvindymai
	SCADA istorijos kaupimo serveris	ICMP, IPv4, TCP, UDP protokolai	ICMP užtvindymas, TCP, UDP užtvindymai

1.8 lentelė. Atakos paviršius antrame *Purdue* modelio lygmenyje

Lygmuo	**Atakuojami aparatiniai taškai**	**Atakuojami programiniai taškai**	**Atakos tipai**
2 Lygmuo – SCADA serverių ir HMI panelių zona	HMI panelė	ICMP, IPv4, TCP, UDP protokolai	ICMP užtvindymas, TCP, UDP užtvindymai
	SCADA serveris		

1.9 lentelė. Atakos paviršius pirmame *Purdue* modelio lygmenyje

Lygmuo	**Atakuojami aparatiniai taškai**	**Atakuojami programiniai taškai**	**Atakos tipai**
1 Lygmuo – Nuotolinių ir lokalių valdiklių zona	PLC valdiklis	ICMP, IPv4, TCP, UDP protokolai, ModbusTCP, DNP3, IEC104, GOOSE protokolai	ICMP užtvindymas, TCP, UDP užtvindymai, ModbusTCP užklausų užtvindymas, DNP3 buferio užtvindymas, IEC 104 komandų užtvindymas, GOOSE užklausų užtvindymas
	RTU kontroleris		

1.6. Analizės dalies išvados

1. Analizuojant esamus DoS/DDoS atakos paviršiaus charakterizavimo modelius pastebėtas literatūros trūkumas šia tema. Tai yra dėl to nes atakos paviršiaus sąvoka dar nėra visiems gerai suprantama ir tyrėjai savo tyrimuose ją naudoja skirtingai, ne visada ją patikslindami.

2. Analizuojami įvairūs straipsniai, tyrimai, publikacijos apie atakos paviršių tiesiogiai ir netiesiogiai rašantys apie DoS/DDoS atakas IT ir OT sistemose, padėjo nustatyti principus ir metodus kaip šiuo metu atakos paviršius yra charakterizuojamas.

3. Išanalizavus atakos tipus jie buvo grupuojami pagal OSI modelio lygmenis. Pastebėta, kad tokie įrenginiai kaip serveris, gali būti atakuojamas ypač plačiu atakos tipų spektru, tad svarbu tinkamai apsaugoti įmonės perimetrą nuo šių atakų grėsmės.

4. Suklasifikuotas atakos paviršius pagal *Purdue* modelio lygmenis padeda įvertinti atakos gylį sistemoje, o tai padeda įvertinti atakos pavojingumą ir galimas pasekmes.

2. DoS/DDoS atakos paviršiaus charakterizavimo modelio projektavimas

Šiame skyriuje yra projektuojamas DoS/DDoS atakos požymiais pagrįstas, atakos paviršiaus charakterizavimo modelis. Toliau skyriuose yra pateikta siūlomo modelio koncepcija, paruošiama panaudojimo atvejų diagrama, surašomi realizavimui keliami funkciniai ir nefunkciniai reikalavimai. Pateikiama siūlomo funkcinių reikalavimų veiklos diagramos, naudojant UML modeliavimo kalbą.

2.1. Siūlomo modelio tikslas

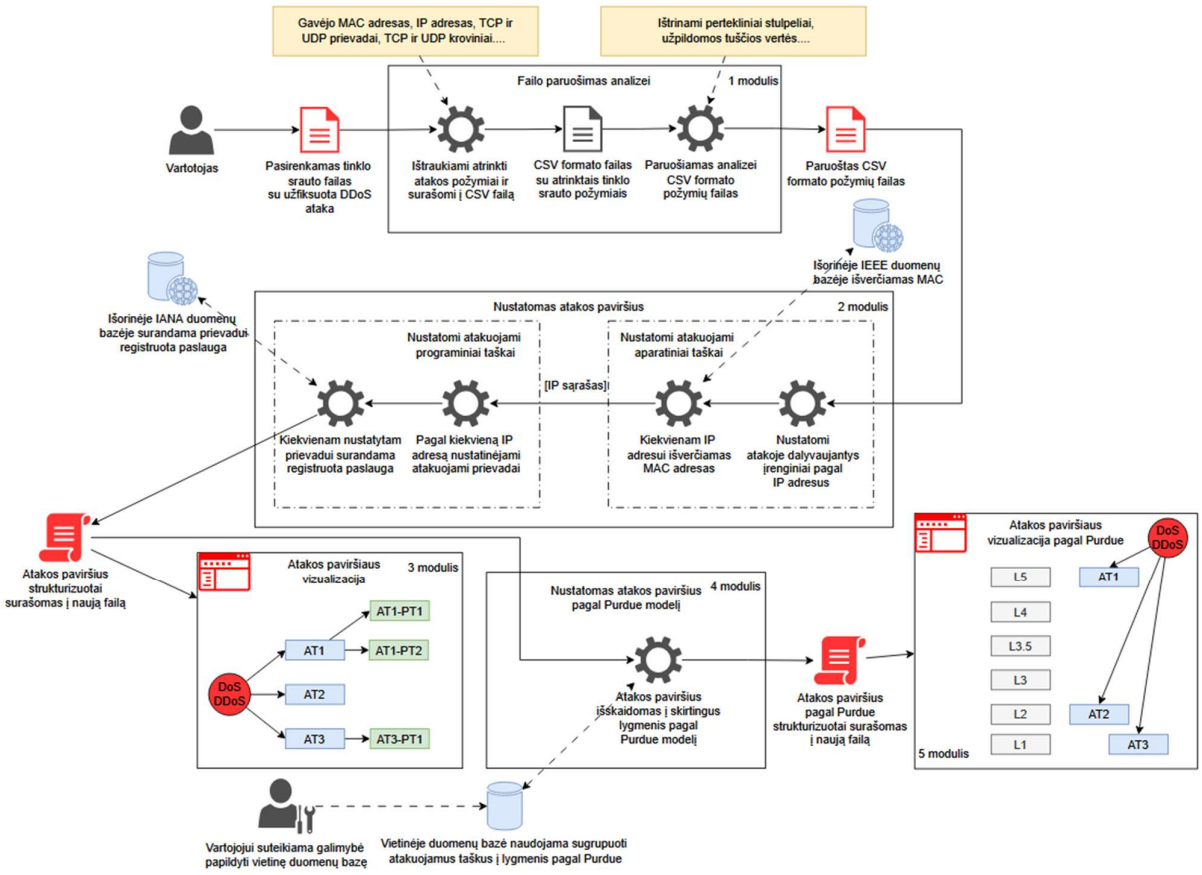
Tikslas šiame darbe yra sukurti modelį, kuris gebėtų iš tinklo srauto failo, kuriame yra užfiksuota DoS arba DDoS ataka, automatiškai identifikuoti atakuojamus įrenginius, kartu su jų pažeidžiamomis programinėmis funkcijomis arba paslaugomis. Siūlomas modelis padėtų, įvykusių atakų tyrimo metu, greičiau atlikti pažeidžiamų įrenginių identifikavimą. Taip pat šis modelis gebėtų nustatytą atakos paviršių išskaidyti pagal IT ir OT sistemas, tokiu būdu padedant tyrėjams greičiau įvertinti atakos pavojingumo lygį. Kuriamas modelis, yra skirtas sistemų administratoriams ir kibernetinio saugumo specialistams atliekantiems įvykusios atakos tyrimą.

Projektuojamame modelyje, šiuo metu nenumatomas gebėjimas automatiškai aptikti DoS arba DDoS atakas. Taip pat modelis nenumato automatinio atskyrimo tarp atakos šaltinių ir atakos taikinių. Dėl to prieš naudojant modelį, tinklo srautas turėtų būti išfiltruojamas pagal atakuojančius įrenginius (Tinklo srauto faile, visuose paketuose esantis šaltinio IP (*angl. source IP*) adresas turėtų priklausyti atakuojantiems įrenginiams).

2.2. Siūlomo modelio koncepcija

Siūlomo modelio koncepcija bendrai sudaryta iš penkių modulių (2.1 pav.). Projektuojami trys pagrindiniai moduliai, kurie atliks požymių ištraukimo iš tinklo srauto failo, atakos paviršiaus identifikavimą ir atakos paviršiaus išskaidymą į IT ir OT sistemas pagal *Purdue* modelį. Šie moduliai yra pagrindinis projektuojamo modelio variklis dirbantis. Papildomai numatomi du moduliai, kurie naudojami topologijoms sudaryti. Atakos paviršiaus topologija projektuojama hierarchinėje formoje pradedant atakos tašku, toliau nurodant atakuojamus aparatinius taškus ir su jais susietus programinius taškus. Išskaidytoje atakos paviršiaus topologijoje numatoma aparatinių taškų sugrupavimas pagal *Purdue* modelio lygmenis. Kiekvienas modulis, atlikęs darbą, sukuria naują failą, kuriame surašyta, modulio veikimo metu, atrinkta svarbi informacija ir kuris yra panaudojamas kaip tarpinis įvesties failas sekančiame modulyje. Tokiu būdu yra užtikrinama integravimo galimybė, panaudoti tarpinius failus trečiųjų šalių sistemose.

Tinklo srauto failas, kuris naudojamas kaip pradinis įvesties failas, turėtų būti standartizuotos struktūros, tokiu būdu užtikrinant galimybę realizuotai programai veikti platesniu spektru. Rekomenduojamas failas yra PCAP (*angl. Packet Capture*), kadangi tai yra standartizuotas ir plačiai paplitęs tinklo srauto formatas [20], tačiau tai gali būti ir kito formato failas, jeigu jis geba pateikti požymius nurodytus 2.1 lentelėje. Analizuojant tinklo srauto failą, iš jo ištraukiami atrinkti požymiai, kurie surašomi į naujai sukurtą CSV (*angl. Comma-Separated Values*) formato failą. CSV formato failas pasirenkamas dėl to, nes šis formatas plačiai paplitęs [37] ir jo analizei galima rasti daugiau geresnių ir greitesnių įrankių, negu tiesiogiai analizuojant tinklo srauto failą. Pagrindiniai ištraukiami požymiai: naudojami protokolai, gavėjo MAC, siuntėjo ir gavėjo IP adresai, gavėjo TCP ir UDP prievadai. Pilnas ištraukiamų požymių sąrašas pateikiamas 2.1 lentelėje, paaiškinant kokiu tikslu šie požymiai ištraukiami.



2.1 pav. Siūlomo sprendimo koncepcija

Toliau sudarytas CSV formato failas apdorojamas ir paruošiamas analizei, kadangi požymių ištraukimo metu, gali susidaryti daugybė tuščių verčių arba stulpelių. Apdorojant CSV failą panaikinami pertekliniai arba tušti stulpeliai, užpildomi tušti langeliai, keičiami verčių tipai (iš skaičiaus į žodį ir atvirkščiai) ir kitaip paruošiama surinkta informacija.

2.1 lentelė. Ištraukiami atrinkti požymiai ir jų panaudojimo tikslas

Požymis	**Požymio panaudojimo aprašymas**
Gavėjo MAC adresas	Naudojama nustatyti atakuojamo įrenginio gamintoją
Naudojamas ETH protokolas	Naudojama nustatyti atakos gylį pagal OSI lygmenis, įvertinti aukštesnį trečio OSI lygmens atakos tipą ir nustatyti atakuojamo ETH protokolo dydį kadrais
Gavėjo IP adresas	Naudojama nustatyti puolamų įrenginių kiekį (aparatiniai taškai) ir nustatyti atakuojamo IP protokolo dydį paketais
Naudojamas IP protokolas	Naudojama nustatyti atakos gylį pagal OSI lygmenis arba įvertinti aukštesnį, ketvirto OSI lygmens atakos tipą
Gavėjo TCP prievadas	Naudojama nustatyti puolamų TCP paslaugų konkrečiame įrenginyje kiekį (programiniai taškai) ir nustatyti atakuojamo TCP protokolo dydį segmentais
Gavėjo UDP prievadas	Naudojama nustatyti puolamų UDP paslaugų konkrečiame įrenginyje kiekį (programiniai taškai) ir nustatyti atakuojamo UDP protokolo dydį datagramomis
Gavėjo TCP krovinio dydis	Naudojama nustatyti atakos gylį pagal OSI lygmenis, įvertinti aukštesnį septinto OSI lygmens atakos tipą ir nustatyti atakuojamos TCP paslaugos dydį užklausomis
Gavėjo UDP krovinio dydis	Naudojama nustatyti atakos gylį pagal OSI lygmenis, įvertinti aukštesnį septinto OSI lygmens atakos tipą ir nustatyti atakuojamos UDP paslaugos dydį užklausomis

Paruošus CSV formato failą su atrinktais požymiais, pradedamas atakos paviršiaus charakterizavimas. Visų pirma, pagal IP adresus, identifikuojami atakos paviršiaus aparatiniai taškai. IP adresų identifikavimas kaip aparatinių taškų pasirenkamas, kadangi šis požymis išskirtinai identifikuoja galinį tašką (*angl. endpoint*) tinkle [38]. Vėliau surandamas IP adresui priklausiantis MAC adresas ir pagal jo tris pirmus baitus išverčiamas tinklo plokštės gamintojas, tokiu būdu dalinai įvertinant atakuojamą įrenginį (tinklo įrenginys, virtualizuota sistema, valdiklis ir t.t). MAC adresui išversti kreipiamasi į išorinę IEEE (*angl. Institute of Electrical and Electronics Engineers*) duomenų bazę [39], kuriame yra MAC adresų registras. Toliau nustatinėjami kiekvieno aparatinio taško, atakuojami programiniai taškai. Programiniai taškai nustatinėjami pagal užfiksuotus antraščių protokolus arba gavėjo prievadus. Pagal protokolo laukelį nustatomi IP, ICMP, TCP, UDP protokolai, pagal prievadą ir jam perduodamą krovinį vertinami paslaugų protokolai: HTTP, DNS, NTP ir t.t. Paslaugos identifikuojamos iš prievado, kuriam išversti naudojama išorinė IANA (*angl. Internet Assigned Numbers Authority*) duomenų bazė [40] ir kurioje yra pateiktas prievadų – paslaugų registras. Visa surinkta informacija, apie atakos paviršių, struktūrizuota forma surašoma į naują failą, kuris toliau naudojamas atakos paviršiaus vizualizacijai sudaryti, bei identifikuotų įrenginių išskaidymui į *Purdue* modelio lygmenis atlikimui.

Pagal atakos paviršiaus nustatymo metu sudarytą failą, yra atliekamas paviršiaus išskaidymas į lygmenis pagal *Purdue* modelį. Skaidymas į lygmenis atliekamas pagal atakos paviršiaus metu identifikuotus TCP ir UDP prievadus. Šie prievadai lyginami su įvairių paslaugų, protokolų ir gamintojų vystomų sistemų numatytais prievadais (2.2 lentelė), kurie pagal lygmenis bus išskaidyti ir laikomi vietinėje duomenų bazėje. Vietinė duomenų bazė aprašoma ir ruošiama realizavimo dalyje. Kadangi IT ir OT infrastruktūra kiekvienoje įmonėje yra skirtinga, o jos tiksliai žinoti nėra galimybės dėl konfidencialumo, pateikiamą pradinį *Purdue* lygmenų – prievadų šabloną sistemos administratoriai galės patys, savo nuožiūra modifikuoti. Informacija, apie išskaidytą atakos paviršių, taip pat struktūrizuota forma surašyta į naują failą ir yra panaudojama, išskaidyto atakos paviršiaus, vizualizacijai sudaryti.

2.2 lentelė. Paslaugos, protokolai ir gamintojų vystomos sistemos išskaidytos pagal *Purdue* lygmenis

***Purdue* lygmuo**	**Šaltiniai iš kurių identifikuojami numatyti prievadai**
5 (DMZ)	Viešai internete naudojami protokolai ir paslaugos (Žiniatinklis, DNS)
4 (Vidinio intraneto zona)	Vidiniuose intranetuose naudojami protokolai ir paslaugos (Domenas, duomenų bazės)
3.5 (DMZ tarp IT ir OT)	Netiesioginiams duomenų mainams tarp IT ir OT sistemų naudojamos paslaugos
3 (operavimo zona)	SCADA programiniai paketai (SCADA istorijos kaupimas, SCADA klientai)
2 (SCADA zona)	SCADA programiniai paketai (SCADA serveriai)
1 (Valdiklių zona)	Industriniai duomenų perdavimo ir surinkimo protokolai

Planuojama atakos paviršiaus topologiją sudaryti hierarchine forma, kurio pradžia yra atakos šaltinis, toliau visi aparatiniai taškai ir visi, aparatiniams taškams priklausiantys, programiniai taškai, pagal tai kaip buvo atakos paviršiaus apibrėžtas analizės metu. Išskaidyto atakos paviršiaus vizualizacija sudaroma paruošiant *Purdue* modelio lygmenų vizualizaciją ir įrenginius sugrupuojant prie atitinkamo lygmens. Numatoma topologijas išsaugoti paveikslo forma vietiniame kompiuteryje, kad būtų galima jas peržiūrėti pakartotinai, neatliekant analizės iš naujo.

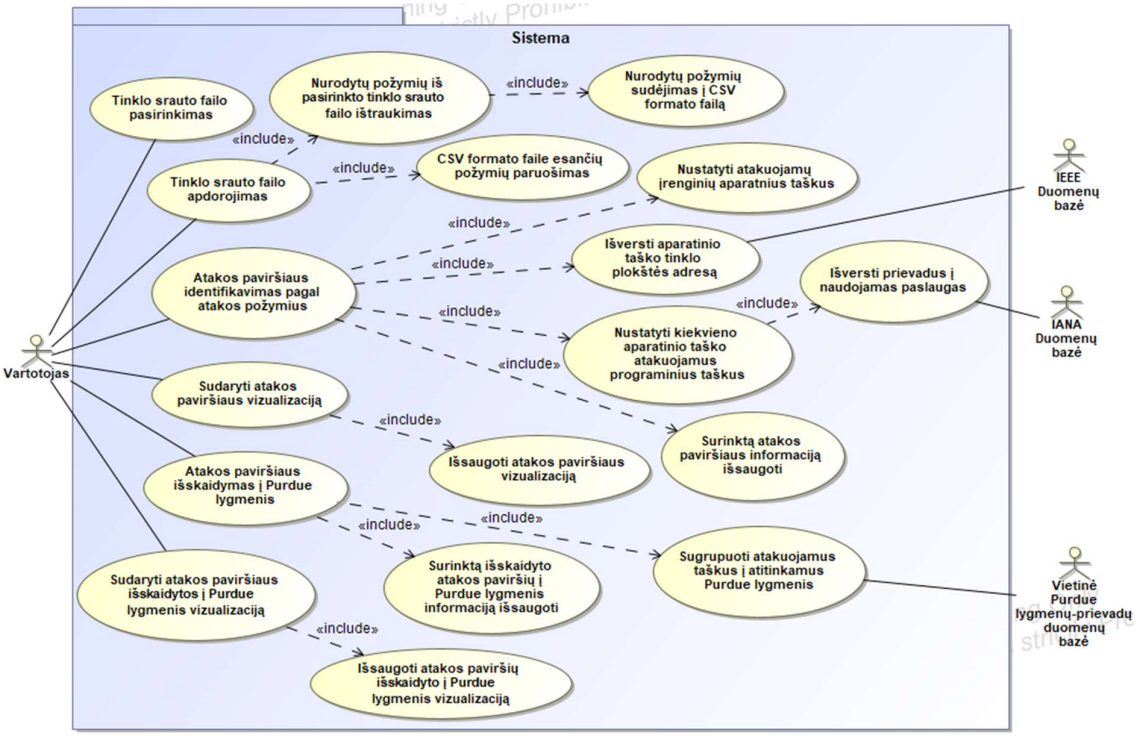
2.3. Realizavimui keliami reikalavimai

Toliau pateikiama siūlomo sprendinio panaudojimo atvejų diagrama, iškeliami realizavimui būtini funkciniai ir nefunkciniai reikalavimai.

2.3.1. Panaudojimo atvejų diagrama

Pateikiama DoS/DDoS atakos požymiais pagrįsto, atakos paviršiaus charakterizavimo panaudojimo atvejų diagrama (2.2 pav.). Pagrindiniai panaudojimo atvejai yra: tinklo srauto failo pasirinkimas, tinklo srauto failo apdorojimas, atakos paviršiaus identifikavimas, atakos paviršiaus vizualizacijos sudarymas, atakos paviršiaus išskaidymas į lygmenis pagal *Purdue* modelį ir išskaidyto į lygmenis atakos paviršiaus vizualizacijos sudarymas.

Tinklo srauto failo apdorojimo PA (panaudos atvejis) metu atliekamas atrinktų požymių, iš tinklo srauto failo ištraukimas, šių požymių sudėjimas į CSV formato failą ir naujo CSV formato failo apdorojimas. Atakos paviršiaus identifikavimo, pagal atakos požymius, PA metu atliekamas aparatinių taškų identifikavimas, MAC adresų vertimas, naudojant išorinę IEEE duomenų bazę, programinių taškų identifikavimas, prievadų vertimas iš išorinės IANA duomenų bazės ir visos surinktos informacijos išsaugojimas vėlesniam naudojimui. Atakos paviršiaus išskaidymo į *Purdue* lygmenis PA metu sugrupuojami atakuojami taškai pagal *Purdue* lygmenis, panaudojant vietinę *Purdue* lygmenų – prievadų duomenų bazę. Atakos paviršiaus, kartu su šio paviršiaus išskaidymo į *Purdue* lygmenis, vizualizacijų sudarymo PA metu sudaromos topologijų vizualizacijos, kurios išsaugomos vaizdine forma į vietinį kompiuterį, kad būtų galima peržiūrėti juos vėliau.



2.2 pav. Siūlomo sprendinio panaudojimo atvejų diagrama

2.3.2. Funkciniai reikalavimai

Pagal panaudojimo atvejų diagramą, matomi pagrindiniai funkciniai reikalavimai, kurie yra keliami realizavimo programai. Šie reikalavimai išvardinti žemiau pateikiamoje 2.3 lentelėje.

2.3 lentelė. Funkciniai reikalavimai

Funkcinio reikalavimo Nr.	**Funkcinio reikalavimo aprašymas**
FR01	Vartotojas pasirenka norimą analizuoti tinklo srauto failą
FR02	Vartotojas inicijuoja tinklo srauto failo apdorojimą
FR02.1	Nurodytų požymių iš pasirinkto tinklo srauto failo ištraukimas
FR02.1.1	Nurodytų požymių sudėjimas į CSV formato failą
FR02.2	CSV formato faile esančių požymių paruošimas
FR03	Vartotojas inicijuoja atakos paviršiaus identifikavimą pagal atakos požymius
FR03.1	Nustatyti atakuojamų įrenginių aparatinius taškus
FR03.2	Išversti aparatinio taško tinklo plokštės adresą
FR03.3	Nustatyti kiekvieno aparatinio taško atakuojamus programinius taškus
FR03.3.1	Išversti prievadus į naudojamas paslaugas
FR03.4	Surinktą atakos paviršiaus informaciją išsaugoti
FR04	Vartotojas inicijuoja atakos paviršiaus vizualizacijos sudarymą
FR04.1	Išsaugoti atakos paviršiaus vizualizaciją
FR05	Vartotojas inicijuoja atakos paviršiaus išskaidymą į *Purdue* lygmenis
FR05.1	Sugrupuoti atakuojamus taškus į atitinkamus *Purdue* lygmenis
FR05.2	Surinktą išskaidytos atakos paviršiaus į *Purdue* lygmenis informaciją išsaugoti
FR06	Vartotojas inicijuoja išskaidytos į *Purdue* lygmenis atakos paviršiaus vizualizacijos sudarymą
FR06.1	Išsaugoti išskaidytos į *Purdue* lygmenis atakos paviršiaus vizualizaciją

2.3.3. Nefunkciniai reikalavimai

Taip pat pateikiami pagrindiniai nefunkciniai reikalavimai, keliami realizavimo programai, kurie yra išvardinti žemiau pateiktoje 2.4 lentelėje.

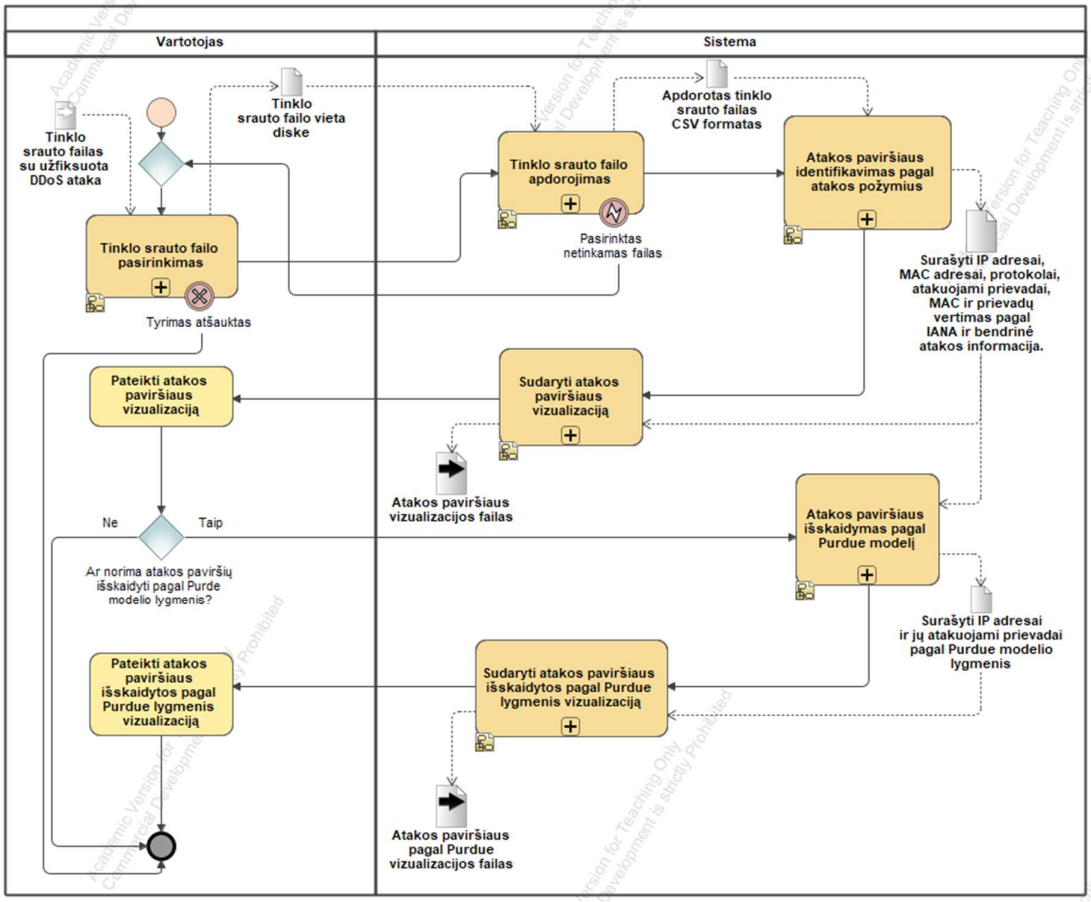
2.4 lentelė. Nefunkciniai reikalavimai

Nefunkcinio reikalavimo Nr.	**Nefunkcinio reikalavimo aprašymas**
NFR01	Visi programos naudojami komponentai turi būti atviro kodo ir nemokami.
NFR02	Programa turėtų veikti *Windows*, *Linux* ir *MacOS* operacinėse sistemose.
NFR03	Grafinė vartotojo sąsaja, pateikiama lietuvių kalba.
NFR04	Vartotojui turėtų būti teikiamas grįžtamasis ryšys apie atliekamų funkcijų sėkmingą arba nesėkmingą atlikimą.
NFR05	Galimybė vartotojui modifikuoti vietinę *Purdue* lygmenų – prievadų duomenų bazę.

2.4. Dinaminis sprendimo modelis

Siūlomo sprendinio pagrindinis veiklos procesas (2.3 pav.) susidaro iš iškeltų pagrindinių funkcinių reikalavimų FR01, FR02, FR03, FR04, FR05 ir FR06. Šioje veiklos diagramoje parodoma kaip

sąveikauja funkciniai reikalavimai vienas su kitu. Toliau pateikiami ir paaiškinami šių funkcinių reikalavimų detalizuoti subprocesai.



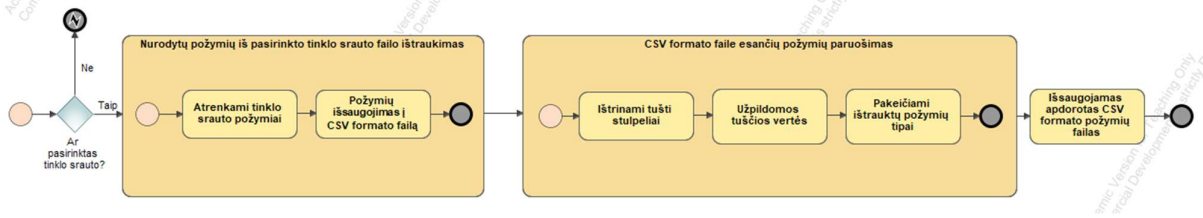
2.3 pav. Siūlomo sprendinio pagrindinis veiklos procesas

FR01 Tinklo srauto failo pasirinkimas

Projektuojama, kad failo pasirinkimui būtų iškviečiamas standartinis naudojamos operacinės sistemos langas failui pasirinkti, kad būtų taupomi resursai programa į kintamąją atmintį įrašys pasirinkto failo nuorodą vietiniame kompiuteryje, kuris toliau perduodamas sekančiai funkcijai.

FR02 Tinklo srauto failo apdorojimas

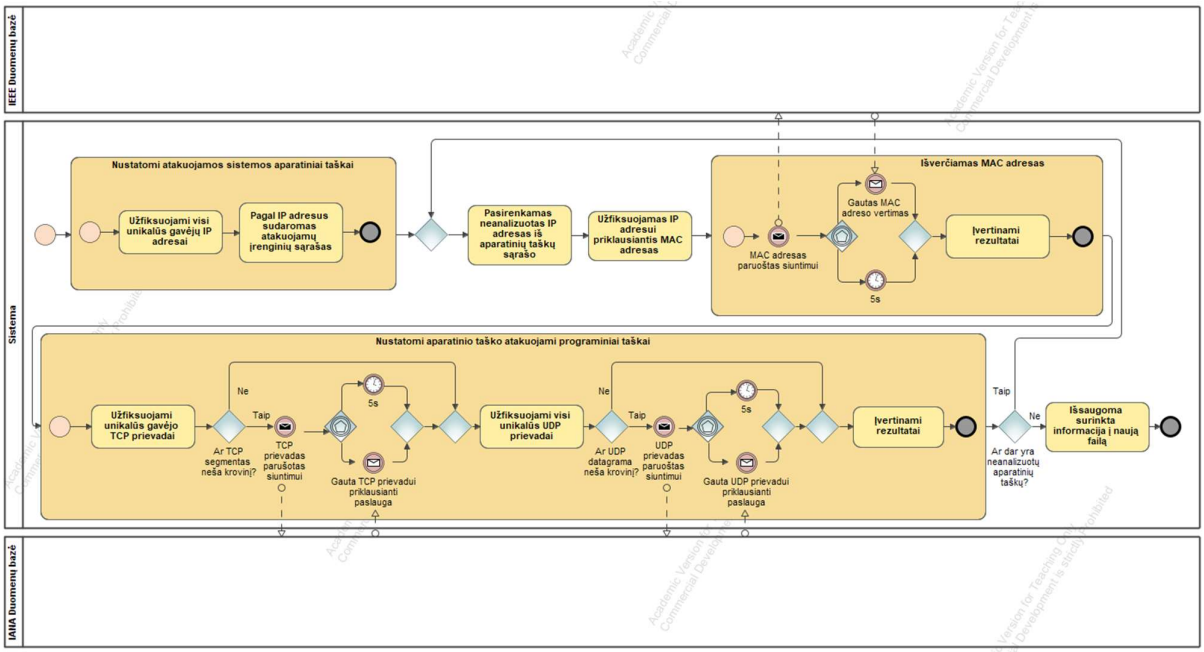
Pasirinktas tinklo srauto failą, toliau jis turi būti tinkamai apdorojamas. Projektuojama, kad iš tinklo srauto požymio failo, turėtų būti ištraukiami paketo gavėjo MAC adresas, gavėjo ir siuntėjo IP adresai, gavėjo TCP ir UDP prievadai, naudojami protokolai, TCP ir UDP krovinių dydžiai. Pilnas sąrašas pateiktas 2.1 lentelėje su nurodytais jų panaudojimo tikslais. Žemiau pateikiamas tinklo srauto failo apdorojimo subprocesas (2.4 pav.), kuriame matomi iškelti realizavimui reikalingi funkciniai FR02.1, FR2.1.1 ir FR02.2 reikalavimai.



2.4 pav. PCAP failo apdorojimo subprocesas

FR03 Atakos paviršiaus identifikavimas pagal atakos požymius

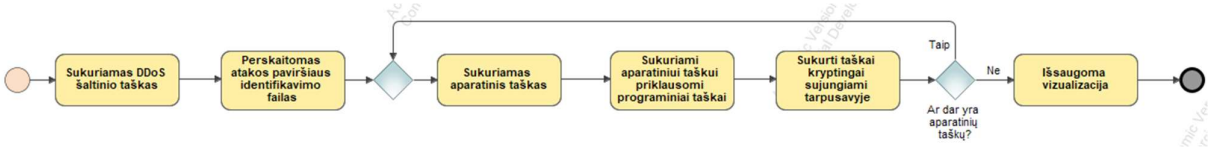
Pateikiamas subprocesas (2.5 pav.), kuriame vaizduojama, kokiu principu nustatinėjamas atakos paviršius atakuojamoje sistemoje. Šioje diagramoje matomi iškelti funkciniai FR03.1, FR03.2, FR03.3, FR03.3.1 ir FR03.4 reikalavimai. Darant prielaidą, kad tinklo srauto faile yra užfiksuota DoS arba DDoS ataka ir kad tinklo srauto failas yra išfiltruotas tik pagal atakos srautą, atakos paviršiaus aparatiniai taškai nustatomi pagal visus užfiksuotus unikalius gavėjo IP adresus, kurie surašomi į atskirą sąrašą. Prieš pradedant programinių taškų analizę yra patikrinamas kiekvienam užfiksuotam IP adresui priklausiantis MAC adresas ir surandamas jo gamintojas. Toliau eilės tvarka, pagal aparatinius taškus, yra analizuojami atakuojami programiniai taškai. Tai atliekama pagrindinį požymių failą išfiltruojant pagal pasirinktą IP adresą ir sudarant laikiną požymių failą tik su šiam IP adresui priklausiančiai paketais. Analizuojant programinius taškus, visų pirma yra užfiksuojami visi unikalūs gavėjo TCP ir UDP prievadai, kurie taip pat atitinkamai surašomi sąrašus. Toliau pagal šiuos sąrašus tikrinama, kurie TCP segmentai ir UDP datagramos neša krovinį. Aptikus krovinį laikoma, kad atakuojamas aukštesnio lygmens protokolas ir dėl to yra bandoma išversti prievadą nustatant jo paslaugą. Visa ši informacija surenkama ir išsaugoma į naują failą, kuris toliau bus naudojamas vizualizacijai sudaryti ir paviršiaus išskaidymui pagal *Purdue* lygmenis.



2.5 pav. Atakos paviršiaus pagal atakos požymius identifikavimo subprocesas

FR04 Atakos paviršiaus vizualizacijos sudarymas:

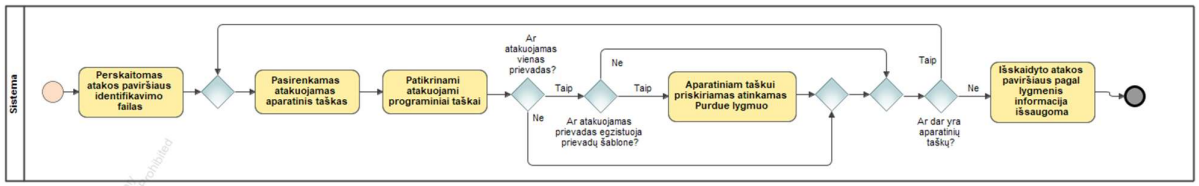
Sudarant atakos paviršiaus vizualizaciją, sudaromas hierarchinis grafikas vaizduojantis iš vieno DoS/DDoS šaltinio taško išeinantį srautą į visus užfiksuotus aparatinius taškus. Toliau aparatiniai taškai atitinkamai sujungiami su jiems priklausiančiais programiniai taškais. Vizualizacija pagal funkcinį reikalavimą FR04.1 išsaugoma, kad būtų galima ją peržiūrėti vėliau, nedarant atakos paviršiaus analizės pakartotinai.



2.6 pav. Atakos paviršiaus vizualizacijos subprocesas

FR05 Atakos paviršiaus išskaidymas į *Purdue* lygmenis

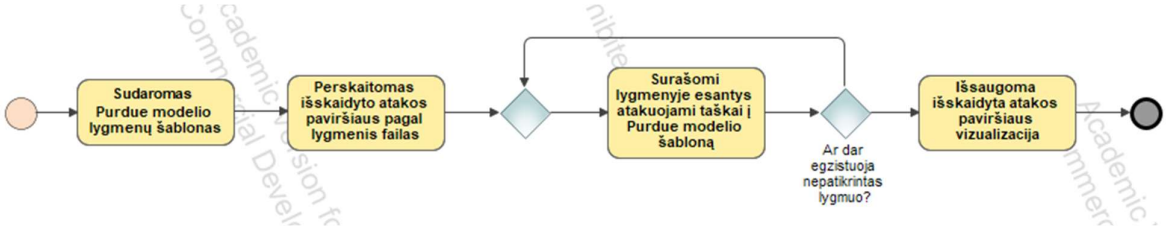
Atakos paviršiaus išskaidymo į *Purdue* modelio lygmenis metu yra perskaitomas atakos paviršiaus metu sudarytas failas. Vėliau eilės tvarka tikrinami aparatiniai taškai ir tikrinami jų atakuojami programiniai taškai. Aptikus, jog yra atakuojamas vienas prievadas, toliau patikrinamas šio prievado buvimas paruoštame *Purdue* lygmenų – prievadų šablone. Aptikus, jog prievadas egzistuoja šiame šablone, aparatiniam taškui yra priskiriamas lygmuo. Ciklas kartojasi tiek kiek yra aptiktų aparatinių taškų, atakos paviršiaus nustatymo metu. Atlikus išskaidymą surinkta informacija yra išsaugoma pagal FR05.2 reikalavimą.



2.7 pav. Atakos paviršiaus išskaidymo pagal *Purdue* modelį subprocesas

FR06 Atakos paviršiaus į *Purdue* lygmenis vizualizacijos sudarymas

Atakos paviršiaus išskaidymo pagal *Purdue* modelį metu, surinkta informacija yra naudojama vizualizacijai sudaryti. Tam tikslui vizualizacijoje yra sudaromas *Purdue* modelio lygmenų šablonas į kurį, lygmuo po lygmens, yra sudedami visi identifikuoti atakuojami taškai. Tokiu būdu vaizdžiai matomas atakos gylis sistemoje. Vizualizacija išsaugoma pagal FR06.1 reikalavimą.



2.8 pav. Atakos paviršiaus pagal *Purdue* modelį vizualizacijos subprocesas

2.5. Projektavimo dalies išvados

1. Projektavimo metu buvo aprašomos pagrindinės modelio savybės – automatizuotas atakos paviršiaus charakterizavimas ir jo išskaidymas pagal *Purdue* modelio lygmenis, tačiau numatomi

ir modelio ribojimai, tokie kaip būtinybė rankiniu būdu išfiltruoti tiriamą tinklo srauto failą nuo atsitiktinio srauto ir užtikrinimas, kad šiame faile yra užfiksuota DoS arba DDoS ataka.

2. Projektuojant modelį buvo nuspręsta šio modelio apimtyje sudaryti požymių ištraukimo ir surašymo į CSV formato failą funkciją, vietoje to kad būtų iš karto naudojami kitų tyrėjų paruošti CSV formato failai su tinklo srauto požymiais. Taip daroma dėl to, nes skirtingų tyrėjų, CSV failų turinys yra skirtingas, o tai sumažina realizuotos programos galimybę atlikti didesnį kiekį skirtingų tyrimų.

3. Atakos paviršiaus išskaidymo pagal *Purdue* modelį veikimui užtikrinti reikalinga duomenų bazė, kuri turėtų priskirtus prievadus ir paslaugas prie kiekvieno *Purdue* lygmenio. Kadangi tokia duomenų bazė nebuvo rasta viešai prieinamuose šaltiniuose nuspręsta prototipinį šabloną paruošti realizavimo metu su galimybę vartotojui modifikuoti šią duomenų bazę.

3. DoS/DDoS atakos paviršiaus charakterizavimo prototipo realizavimas

Suprojektavus DoS/DDoS atakos požymiais pagrįstą, atakos paviršiaus charakterizavimo modelį, toliau atliekamas demonstracinės programos realizavimas. Toliau skyriuje pateikti ir aprašyti prototipo kūrimui pasirinkti programiniai įrankiai. Vėliau sudaromas pradinis *Purdue* lygmenų – prievadų šablonas. Po to sudaroma prototipo grafinė sąsaja ir pradedamas funkcijų realizavimas. Galiausiai pateikiama ir aprašoma prototipo diegimo diagrama mašinoje.

3.1. Prototipo realizavimui pasirinkti pagrindiniai įrankiai

Pradinis įvesties failas, kuriame yra užfiksuotas DoS/DDoS atakos tinklo srautas ir kuris yra naudojamas realizavime, pasirenkamas PCAP formato. Šis formatas pasirenkamas, kadangi jame yra pilnai užfiksuoti duomenų paketai, kuriuose yra neapdorotos (*angl. raw*) visos antraštės ir kroviniai. Tai suteikia galimybę ištraukti arba išskaičiuoti visus modeliui būtinus tinklo srauto požymius, kartu leidžiant išgauti ir papildomos informacijos apie vykstančią ataką.

Pagrindinis įrankis, prototipo realizavimui, yra pasirinktas *Python* programinės kalbos paketas [41]. Ši programavimo kalba naudojama rašant pagrindinius ir kitus svarbius funkcinius scenarijus atakos paviršiaus charakterizavimui. Ji pasirinkta dėl jos paprastumo, lankstumo ir galimybės veikti operacinėse sistemose tokiuose kaip Windows ir Linux. Kartu su *Python* naudojamos įvairios *Python* bibliotekos ir moduliai. Kitas svarbus įrankis yra *Tshark* tinklo srauto analizatorius [42], kuris, *Python* scenarijuose, naudojamas greitam atakos požymių ištraukimui iš PCAP formato failo ir surašymui į CSV formato failą. *Tshark* taip pat gali būti įrašytas į įvairias operacines sistemas. Sąrašas visų naudojamų įrankių, *Python* modulių ir panaudojimo paaiškinimai pateikti 3.1 lentelėje.

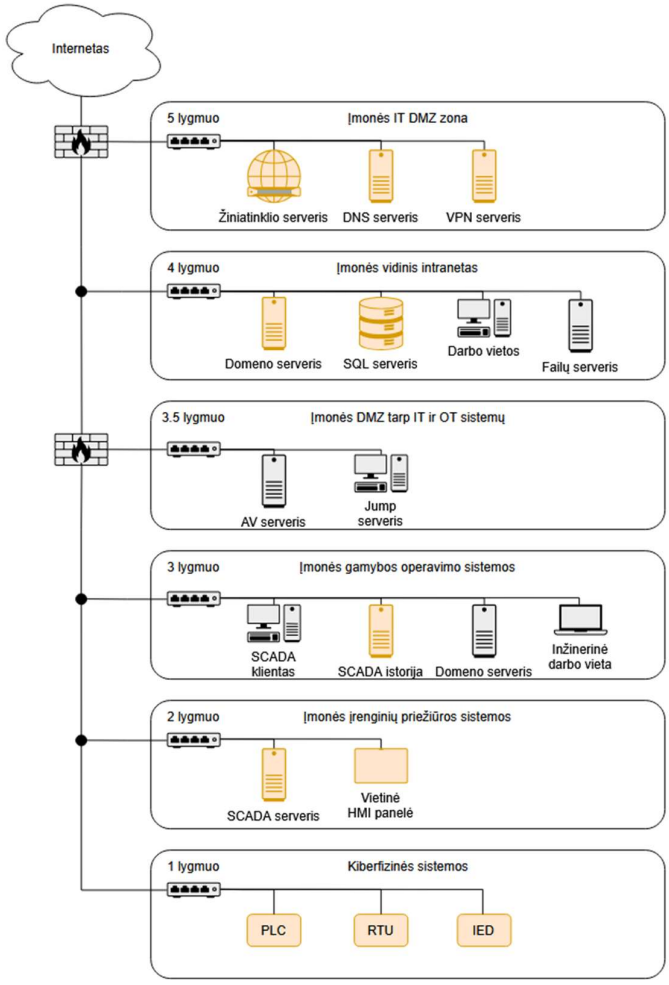
3.1 lentelė. Pagrindiniai realizavimui naudojami įrankiai

Įrankis	**Įrankio panaudojimo aprašymas**
Python programavimo kalba	Naudojamas pagrindiniam ir papildomiems scenarijams sukurti. Pasirinkta dėl paprastumo ir lankstumo, kadangi ši programavimo kalba siūlo daugybę modulių, kurie palengviną didelių duomenų masyvų analizę, o tai pat šia kalba parašyta programa gali veikti daugumoje operacinių sistemų aplinkose.
Tshark tinklo srauto analizatorius	Naudojamas PCAP failo požymių analizei, jų ištraukimui ir eksportavimui į CSV failą. Pasirinktas dėl to, nes tai vienas iš greičiausiai veikiančių tinklo srauto analizatorių, galintis eksportuoti duomenis iš PCAP į CSV. Taip pat veikiantis įvairiose OS.
Python „*Tkinter*“ modulis	Naudojamas vartotojo grafinei sąsajai sukurti. Šis modulis „*Python*“ aplinkoje yra numatytasis.
Python „*Pandas*“ modulis	Naudojamas CSV failų analizei. Pasirinktas dėl greičio ir paprasto naudojimo.
Python „*Networkx*“ modulis	Naudojamas paruošti atakos paviršiaus ir atakos paviršiaus išskaidyto į *Purdue* lygmenis topologijas. Pasirinktas dėl savo gebėjimo integruotis į kitus, „*Python*“ vizualizacijai sukurti skirtus, modulius.
Python „*Pyvis*“ modulis	Naudojamas atakos paviršiaus ir atakos paviršiaus išskaidyto pagal *Purdue* lygmenis vizualizacijai sudaryti. Pasirinktas dėl to, nes numatyta vizualizaciją daryti interaktyvią HTML pavidalu, kadangi didelės topologijos gali neinteraktyviam paveiksle būti labai suspaustos ir neįžiūrimos.
Python „Requests“ modulis	Naudojamas registruotų paslaugų prievadų tikrinimui iš išorinės IANA duomenų bazės.
Python „*Mac vendor lookup*“ modulis	Naudojamas MAC adresų vertimui atlikti iš išorinės IEEE duomenų bazės.

Prototipo realizavimo metu numatyta naudoti ir kitus struktūrizuotus duomenų failus, tokius kaip TXT (*angl. text*) ir JSON (*angl. JavaScript Object Notation*). TXT formato failas naudojamas kartu su *Python* „*Mac vendor lookup*“ moduliu, kuris parsiunčia naujausią informaciją iš IEEE išorinės duomenų bazės būtent šiuo formatu [43]. JSON formato failas naudojamas vietinėje sudarytoje *Purdue* lygmenų – prievadų duomenų bazėje, kurio paruošimas pateikiamas tolesniame skyriuje.

3.2. *Purdue* lygmenų – prievadų duomenų bazės šablono realizavimas

Tinklo architektūros, pagal *Purdue* modelį, įgyvendinimas skirtingose įmonėse yra skirtingas, todėl toliau pateikiama įprastinė gamybos įmonės tinklo architektūra (3.1 pav.). Ši architektūra paremta kitų tyrėjų atliktais darbais apie *Purdue* modelio panaudojimą tinklo architektūros projektavimui [44] ir kibernetinių priemonių panaudojimą skirtingose šio modelio lygmenyse [45].



3.1 pav. Įprastinė gamybos įmonės tinklo architektūra pritaikyta pagal *Purdue* modelį [44], [45]. Paryškinti įrenginiai, kurie gali būti identifikuojami pagal unikalų prievadą

Pagal 3.1 paveiksle pateiktą architektūrą yra kuriamas pradinis *Purdue* lygmenų – prievadų duomenų bazės šablonas, kuris bus laikomas vietiniame kompiuteryje. Ši duomenų bazė realizuojama JSON formatu, su galimybe tinklo administratoriams jį modifikuoti. JSON formatas pasirinktas dėl paprasto vardo – reikšmės struktūros. Pradinis *Purdue* lygmenų – prievadų duomenų bazės šablonas yra sudarytas iš šešių lygmenų. Kiekviename lygmenyje yra pateiktos dažniausiai aptinkamos sistemos, kurios yra atakuojamos DoS ir DDoS atakomis ir kurios yra surašytos pagal jų paslaugų

numatytuosius naudojamus prievadus iš IANA registro [40] arba iš programinės įrangos vystytojų, viešai pateikiamų kuriamų sistemų aprašymų. 3.2 lentelėje pateikiamas 5 *Purdue* lygmens išdėstymo pavyzdys su realiai tam lygmeniui būdingomis paslaugomis. Ruošiamoje duomenų bazėje prievadai turi būti priskirti vieną kartą ir jie neturi kartotis kituose lygmenyse.

3.2 lentelė. Purdue lygmenų – prievadų duomenų bazės, 5 lygmens išdėstymo pavyzdys

```
</> JSON failas
{
   "Level 5": {
         "TCP": {
            "80": "Web HTTP",
            "443": "Web HTTPS"
      },
         "UDP": {
            "500": "VPN IPsec VPN",
            "4500": "VPN IPsec VPN",
            "51820": "VPN WireGuard",
            "1194": "VPN OpenVPN",
            "53": "DNS"
      }
   },
}
```

***Purdue* lygmenų – prievadų šablono 5 lygmens paruošimas:**

Penktame lygmenyje yra įmonės IT sistemos, kurioms reikalinga prieiga iš viešo interneto. Pagal sudarytą įprastinę įmonės tinklo architektūrą, šiame lygmenyje įrašomi žiniatinklio paslaugos numatyti TCP protokolo 80 ir 443 prievadai. Kadangi VPN paslaugos taip pat yra vienas iš DDoS atakos taikinių [46], įrašomi ir numatyti, skirtingų VPN programų naudojami, UDP protokolo prievadai: 500, 4500 (*IPsec VPN*), 51820 (*WireGuard*), 1194 (*OpenVPN*).

***Purdue* lygmenų – prievadų šablono 4 lygmens paruošimas:**

Ketvirtame lygmenyje aptinkamos pagrindinės įmonės vidinės sistemos. Šiame lygmenyje surašomi domeno naudojamų paslaugų, numatyti prievadai: DHCP, kuris naudoja UDP protokolo 67 prievadą, LDAP, kuris naudoja UDP protokolo 389 ir TCP protokolo 389, bei 636 prievadus. Taip pat šiame lygmenyje įrašomi įvairių duomenų bazių naudojami TCP protokolo prievadai: 3306 (*MySQL*), 5432 (*PostgreSQL*), 1433 (*Microsoft SQL*), 1521 (*Oracle Database*).

***Purdue* lygmenų – prievadų šablono 3.5 lygmens paruošimas:**

OT DMZ zonoje įprastinėje architektūroje yra nuotolinio prisijungimo terminalai, OT tinklo antivirusinės, SCADA istorijos duomenis dubliuojantys serveriai. Šiame lygmenyje nerašoma jokių prievadų ir paslaugų, kadangi pagal standartinę analizuojamą infrastruktūrą šiame lygmenyje nėra unikaliai pagal prievadus identifikuojamų įrenginių. Šiame lygmenyje esantys įrenginiai gali būti aptinkami ir kitose lygmenyse.

***Purdue* lygmenų – prievadų šablono 3 lygmens paruošimas:**

Trečiame lygmenyje aptinkamos SCADA sistemų istorinių duomenų kaupimo serveriai, operatorių ir inžinierių darbo stotys, OT tinklo domenas. Unikaliai šis lygmuo yra identifikuojamas iš SCADA istorinių duomenų kaupimo serverių, kuriems skirtingi SCADA sistemų vystytojai naudoja unikalius prievadus: iFIX SCADA istorinių duomenų serveris naudoja 13000, 14000, 14001 ir 14003 TCP protokolo prievadus [47]. AVEVA System Platform naudoja TCP protokolo 32565, 32568, 32569 ir 32563 prievadus [48].

***Purdue* lygmenų – prievadų šablono 2 lygmens paruošimas:**

Antrame lygmenyje aptinkami SCADA sistemų serveriai ir HMI paneles. Šį lygmenį galima unikaliai atskirti iš SCADA serverių pagal nutylėjimą naudojamų prievadų. iFIX SCADA naudoja TCP protokolo 2010 ir 53014 prievadus [47], Ignition SCADA naudoja TCP protokolo 8043, 8060 ir 8088 prievadus [49], AVEVA System Platform SCADA naudoja TCP protokolo 808, 5026, 8090, 30000, 30001, 32568 prievadus [48], Citect SCADA naudoja 2084, 2080, 2085, 2082 ir 23104 TCP protokolo prievadus [50].

***Purdue* lygmenų – prievadų šablono 1 lygmens paruošimas:**

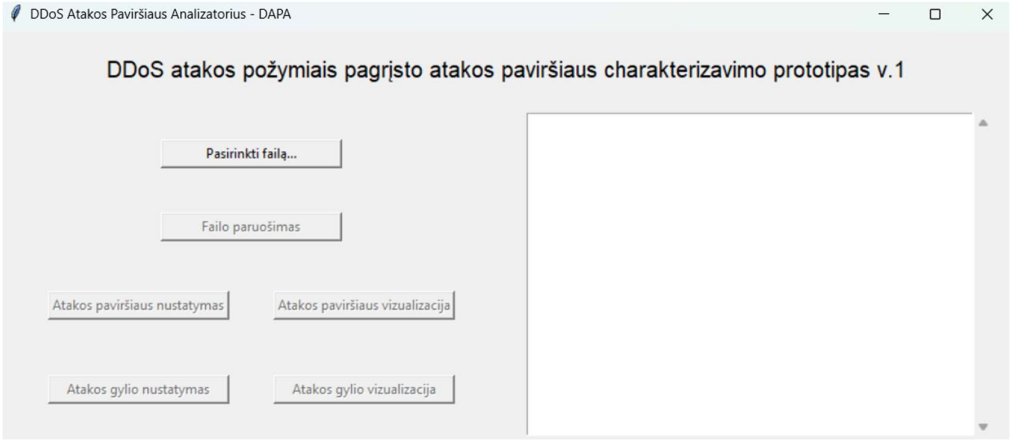
Pirmame lygmenyje yra naudojami valdikliai ir kontroleriai, todėl šiame lygmenyje įrašomi prievadai pagal populiariausius valdiklių naudojamus industrinius protokolus: 502 (*ModbusTCP*), 2024 (*IEC104*), 102 (*IEC61850*), 44818 (*Ethernet/IP*), 20000 (*DNP3*) [40].

Galutinai sudaryta, prototipinė *Purdue* lygmenų – prievadų duomenų bazė JSON formatu yra pateikta 1 priede.

3.3. Prototipo realizavimas

3.3.1. Naudotojo sąsajos prototipas

Prototipo realizavimui pasirinkti įrankiai yra atviro kodo, nemokami ir jie gali būti naudojami pagrindinėse operacinėse sistemose (Windows, Linux), todėl kuriamas prototipas atitiks išsikeltus **NFR01** ir **NFR02** nefunkcinius reikalavimus. Norint atitikti **NFR03** nefunkcinį reikalavimą programai reikia paruošti grafinę vartotojo sąsają lietuvių kalba. Tai atliekama naudojant *Python* „*Tkinter*“ modulį. Paruošta grafinė sąsaja pateikta 3.2 paveiksle.



3.2 pav. Programos grafinė vartotojo sąsaja

Šioje grafinėje sąsajoje matomi pagrindinių funkcinių reikalavimų FR01 – FR06 mygtukai, kurie yra naudojami pradedant jų vykdymą. Sėkmingai įvykdytas funkcinis reikalavimas atrakina sekantį mygtuką. Dešinėje pateiktas grįžtamoje ryšio langas, kuriame rašoma, ką programa sėkmingai atliko ir kas nepavyko (pagal **NFR04** nefunkcinį reikalavimą). Direktorijoje, kurioje programa paleista, yra pateiktas pradinis JSON formato failas apie paslaugas ir prievadus pagal *Purdue* lygmenis. Kad atakos paviršiaus išskaidymas būtų tikslesnis, jame vartotojas pats galės papildomai pridėti arba patikslinti informaciją apie įmonėje veikiančias paslaugas ir prievadus (Pagal **NFR05** nefunkcinį reikalavimą). Kadangi šis failas gali turėti konfidencialios informacijos jis laikomas tik vietiniame kompiuteryje.

3.3.2. Funkcinių reikalavimų realizavimas

FR01 PCAP formato failo pasirinkimo funkcijos realizavimas:

Failo pasirinkimui sukuriamas įprastas, naudojamos operacinės sistemos, failo pasirinkimo langas (*angl. file dialog*), kuriame suteikiama galimybė pasirinkti norimą failą. Pasirinkus failą, išsaugomas į kompiuterio atmintį yra kelias (*angl. path*) iki jo. Toliau išsaugotas kelias yra perduodamas failo apdorojimo funkcijai. Failo pasirinkimo funkcijai atlikti naudojamas *Python* „*Tkinter*“ modulis.

FR02 PCAP formato failo apdorojimo funkcijos realizavimas:

PCAP formato failo apdorojimui naudojami *Tshark* tinklo srauto analizavimo programa ir *Python* „*Pandas*“ modulis. PCAP failo absoliutus kelias yra perduodamas apdorojimo funkcijai, kuri paruošia *Tshark* komandą ir ją įvykdo nurodant pasirinkto failo adresą. *Tshark* komanda su argumentais ir failo keliu yra paruošiama *Python* sąrašo (*angl. list*) formoje (3.3 lentelė). Sujungus visas šias vertes į vieną sakinį gaunama komanda, kuri yra vykdoma naudojamos operacinės sistemos terminale (nematant vartotojui).

3.3 lentelė. *Python* sąrašo forma paruošta *Tshark* komanda PCAP failo požymių ištraukimui su argumentais ir pasirinkto failo adresu

['tshark', '-r', 'C:/Users/Gutle/Desktop/2025 Magistras/3. Realizavimas/DDoS atakos tyrimui/Filtered_IT_DoS_HTTP_GoldenEye_Attack.pcap', '-T', 'fields', '-e', 'frame.time_epoch', '-e', 'frame.len', '-e', 'eth.dst', '-e', 'eth.type', '-e', 'ip.src', '-e', 'ip.dst', '-e', 'ip.proto', '-e', 'ip.flags.mf', '-e', 'ip.frag_offset', '-e', 'tcp.dstport', '-e', 'tcp.flags', '-e', 'tcp.len', '-e', 'udp.dstport', '-e', 'udp.length', '-E', 'header=y', '-E', 'separator=,', '-E', 'quote=d', '-E', 'occurrence=f']

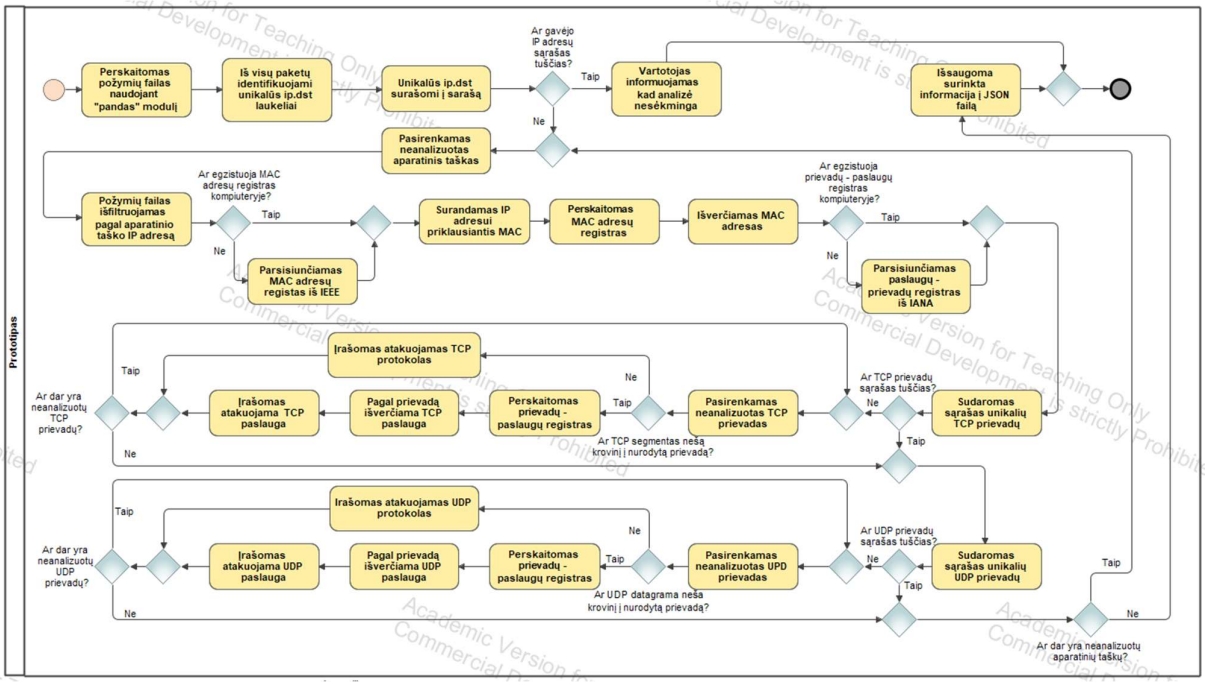
Vykdymo metu yra ištraukiami atrinkti požymiai iš PCAP formato failo ir ši informacija sudedama į naują CSV formato failą, kuris išsaugojamas toje pačioje direktorijoje, kurioje yra paleista programa. Ištrauktų požymių, CSV failo formatu, pavyzdys pateiktas 2 priede. Ištraukus požymius, naujai sukurtas CSV formato failas, yra apdorojamas naudojant *Python* „*Pandas*“ modulį. Apdorojimo metu yra užpildomos tuščios vertės, panaikinami tušti stulpeliai, keičiami verčių formatai (skaičius – žodis, žodis - skaičius). Failą apdorojus jis yra išsaugomas į tą pačią vietą, pakeičiant failo originalą. Dešinėje pusėje, grįžtamojo ryšio lange, yra pateikiama vartotojui informacija apie funkcijos vykdymo procesą.

FR03 Atakos paviršiaus identifikavimo pagal atakos požymius funkcijos realizavimas:

Atakos identifikavimo, pagal atakos požymius, metu yra naudojami *Python* „*Pandas*“, „*Mac Vendor Lookup*“ ir „*Requests*“ moduliai. PCAP failo apdorojimo metu, išsaugotas CSV formato failas yra

perskaitomas naudojant *Python* „*Pandas*“ modulį. Panaudojant šį modulį, pradedama ieškoti atakos paviršiaus aparatinius taškus, pagal gavėjo IP adresus, o tai atliekama išfiltruojant ir surašant į sąrašą unikalius gavėjo IP adresus pagal „*ip_dst*“ požymį. Toliau naudojant *Python* „*for*“ ciklą, iš eilės tikrinama informacija apie aparatinį tašką (IP adresą).

Pagal pasirinktą, neanalizuotą, aparatinio taško IP adresą, yra išfiltruojamas pagrindinis požymių failas naudojant „*Pandas*“ modulį ir toliau analizuojamas tik išfiltruotas požymių failas. Identifikuojamas IP adresui priklausiantis MAC adresas, jis yra išverčiamas, taip sužinant tinklo plokštės gamintoją. Prieš tai patikrinama ar kompiuteryje yra MAC adresų registras, o jo nepatikus, jis yra parsiunčiamas iš IEEE tinklapio, naudojant *Python* „*Mac Vendor Lookup*“ modulį. Surinkta informacija išsaugoma į nuolat pildoma *Python* žodyną.



3.3 pav. Realizuota atakos paviršiaus identifikavimo UML veiklos diagrama

Toliau pradedamas programinių taškų identifikavimas. Iš pradžių patikrinama ar kompiuteryje yra paslaugų – prievadų registras ir jo neradus jis parsiunčiamas iš IANA tinklapio. Toliau naudojant „*Pandas*“ modulį, surašomi į sąrašą unikalūs gavėjo TCP protokolo prievadai. Jeigu sudarytas sąrašas netuščias, pradedamas TCP prievadų analizės ciklas. Tikrinamas kiekvienas užfiksuotas prievadas, aptikus nešamą krovinį į analizuojamą prievadą, laikoma, kad yra atakuojama paslauga ir pagal šį prievadą yra surandama jam registruota paslauga iš IANA registro, kitu atveju laikoma, jog atakuojamas TCP protokolas. Baigus ciklą, pradedamas unikalių gavėjo UDP prievadų surašymas ir kartojamas ciklas kaip ir analizuojant TCP prievadus. Pabaigus programinių taškų analizę yra tikrinama ar dar yra neanalizuotų aparatinių taškų. Aptikus neanalizuotą aparatinį tašką visas ciklas pradedamas iš naujo. Išanalizavus visus įrenginius, visa surinkta informacija surašoma į JSON failą. Surinktos informacijos pavyzdys JSON faile pateiktas 3 priede.

FR04 Atakos paviršiaus vizualizacijos realizavimas:

Atakos paviršiaus vizualizacijos metu yra naudojamas naujai, atakos paviršiaus analizės metu, sukurtas JSON formato failas. Šis failas yra perskaitomas ir pagal jį yra ruošiama topologija dėliojant

taškus ir juos sujungiant tarpusavyje hierarchine forma iš kairės į dešinę. Visa tai atliekama naudojant *Python* „*Networkx*“ modulį.

Sudarius *networkx* topologiją, jos atvaizdavimui naudojamas *Python* „*Pyvis*“ modulis. Šis modulis leidžia perkelti paruoštą topologiją su taškais į interaktyvų HTML failą, kurį vėliau galima analizuoti vaizdą priartinant, slenkant taškus ir t.t. (3.4 lentelė). Tai suteikia galimybę pamatyti didelės apimties topologijas.

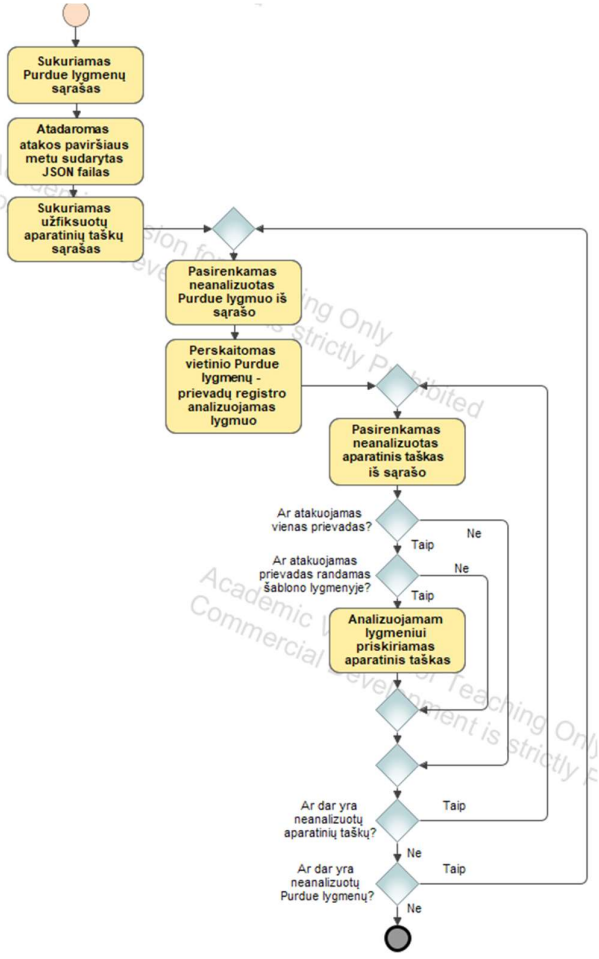
3.4 lentelė. Kodo dalie fragmentas sudaranti interaktyvią HTML topologiją iš networkx pateiktų duomenų

```
# Sudaromas interaktyvus HTML paveiksliuką naudojant PyVis
nt = Network(notebook=True, height="600px", width="100%", directed=True, layout=True)
nt.set_options(json.dumps(asv_options_attack_surface_pyvis))

# PyVis vizualizacijai panaudojamas DiGraph objektas su aprašytais taškais
nt.from_nx(attack_surface_nx_graph)

# Išsaugomas HTML formato failas
nt.save_graph(asv_filename_attack_surface_visualisation)
```

FR05 Atakos paviršiaus išskaidymo pagal *Purdue* lygmenis realizavimas:



3.4 pav. Realizuota atakos paviršiaus išskaidymo pagal *Purdue* lygmenis UML veiklos diagrama

Atakos paviršiaus išskaidymo, pagal *Purdue* lygmenis, metu programos atmintyje sudaromas tuščias *Python* sąrašas su visais *Purdue* lygmenis. Vėliau perskaitomas atakos paviršiaus metu sudarytas

JSON failas, pagal kurį yra sudaromas užfiksuotų aparatinių taškų sąrašas. Sudarius šiuos sąrašus pradedamas ciklas per *Purdue* lygmenis, o jų viduje kuriamas kitas ciklas, kuris tikrina visus užfiksuotus aparatinius taškus.

Purdue lygmenų analizės cikle yra perskaitomas vietinio *Purdue* lygmenų – prievadų šablono analizuojamas lygmuo ir jame surašyti prievadai. Toliau, tikrinant kiekvieną aparatinį tašką, yra tikrinama ar jame yra atakuojamas tik vienas prievadas. Aptikus jog atakuojamas vienas prievadas yra tikrinama ar šis prievadas egzistuoja analizuojamo lygmens šablone. Aptikus šį prievadą, aparatiniam taškui yra priskiriamas lygmuo, kuriame jis analizuojamas. Realizuota UML veiklos diagrama pateikta 3.4 paveiksle. Funkcijos pabaigoje sukuriamas ir išsaugojamas naujas JSON formato failas su surašyta informacija apie lygmenis.

FR06 Išskaidytos pagal *Purdue* modelį atakos paviršiaus vizualizacijos realizavimas:

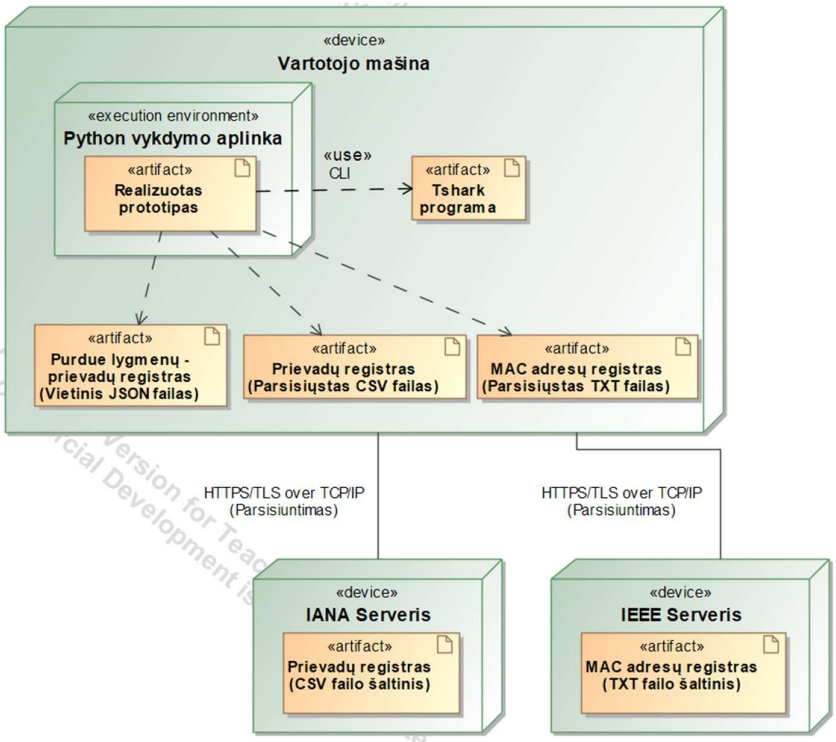
Išskaidytos, pagal *Purdue* lygmenis, atakos paviršiaus vizualizacija sudaroma naudojant tokius pat įrankius kaip ir sudarant atakos paviršiaus vizualizaciją. Naudojami *Python* „*Networkx*“ ir „*Pyvis*“ moduliai.

Pradžioje, naudojant *networkx,* sukuriama topologija su kiekvienu *Purdue* modelio lygmeniu. Vėliau perskaitomas JSON failas, kuris buvo sudarytas atakos paviršiaus išskaidymo į *Purdue* lygmenis metu ir naudojant ciklo funkciją tikrinamas kiekvienas lygmuo. Aptikus įrenginį, jo taškas įrašomas topologijoje atitinkamame lygmenyje. Atlikus taškų dėliojimą, naudojant *pyvis* sudaroma interaktyvi HTML topologija, kuri išsaugoma vietiniame kompiuteryje.

3.4. Prototipo diegimo diagrama

Pateikiama siūlomo prototipo diegimo diagrama (3.5 pav.). Realizuota programa parašyta *Python* programavimo kalba, dėl to jai reikalinga įrašyta *Python* vykdymo aplinka. Ši programa taip pat priklausoma nuo *Tshark* įrankio, kuris taip pat turėtų būti įrašytas naudojamoje mašinoje. Svarbu, kad *Tshark* įrankio vykdomojo failo direktorija, būtų įrašyta į kompiuterio aplinkos kintamųjų (*angl. environmental variables*) „*Path*“ kintamąjį. Tai reikalinga, kad *Python* aplinka, vykdydama prototipo parašytas funkcijas, gebėtų savarankiškai rasti ir pradėti vykdyti *Tshark* programą kompiuteryje.

Programa naudoja dvi išorines duomenų bazes, bei vieną, vietiniame kompiuteryje esančią iš anksto paruoštą, duomenų bazę. Viena, iš išorinių duomenų bazių, naudojama norint nustatyti tinklo plokštės gamintoją iš MAC adreso pirmų trijų baitų, kita, pagal prievadus nustatyti, jiems priklausiančias, registruotas paslaugas pagal IANA organizaciją. Kad būtų sumažinta priklausomybė nuo šių išorinių duomenų bazių, ši informacija yra parsisiaučiama ir laikoma vietiniame kompiuteryje. Visgi norint gauti naujausią informaciją apie vertimus reikalinga turėti interneto prieigą. Vietinėje duomenų bazėje naudojamas paruoštas, šabloninis duomenų bazės failas, kuris naudojamas išskaidyti atakos paviršių į lygmenis pagal *Purdue* modelį. Šis failas laikomas vietiniame kompiuteryje, kadangi gali turėti jautrios informacijos apie organizaciją IT ir OT sistemas.



3.5 pav. Siūlomo prototipo diegimo diagrama

3.5. Realizavimo dalies išvados

1. Realizuojant požymių ištraukimo iš PCAP failo funkciją buvo naudojami įvairūs, šiai užduočiai skirti *Python* moduliai. Tačiau dėl lėto jų veikimo buvo nuspręsta atskirai naudoti *Tshark* programą, kuris iššaukiamas per *Python* scenarijų operacinėje sistemoje ir jis veikia daug greičiau už *Python* siūlomus modulius.

2. Informacija apie MAC adresų vertimus ir registruotas, prievadams priklausiančias paslaugas yra galimybė parsisiųsti iš viešai prieinamų šaltinių, tačiau informacija apie prievadus, pagal *Purdue* lygmenis, nebuvo rasta. Dėl to nuspręsta sudaryti ir paruošti šį duomenų bazės failą, šio darbo apimtyje.

3. Sudarant *Purdue* lygmenų – prievadų registrą buvo nuspręsta neįtraukti jokių įrenginių į 3,5 *Purdue* lygmenį (DMZ zona tarp IT ir OT sistemų), kadangi šiame lygmenyje sudėtinga nustatyti unikalią, tik šiam lygmeniui būdingą paslaugą arba sistemą. Visgi paliekama galimybė sistemų administratoriams patiems pridėti įrenginius į šį lygmenį.

4. Nuspręsta atakos paviršiaus topologiją sudaryti interaktyvia HTML forma, kadangi didelis kiekis atakuojamų taškų padaro statinį vaizdą neįžiūrimą ir sunkiai analizuojamą. Realizuotame HTML formato faile planuojama galimybė taškus paslinkti ir vaizdą priartinti arba nutolinti, tokiu būdu sudarant analizę patogesnę.

4. DoS/DDoS atakos paviršiaus charakterizavimo prototipo eksperimentinis tyrimas

Pagal siūlomą modelį realizavus prototipą, pradedamas šios programos eksperimentinis tyrimas. Toliau skyriuje pateikiamas siūlomas eksperimentas prototipui įvertinti, eksperimento metu naudojama aparatinė įranga, aprašomi kiekybinis ir kokybinis prototipo tyrimai.

4.1. Tyrimo aprašymas ir tikslai

Tyrimo tikslas – įvertinti DoS/DDoS atakos požymiais pagrįsto, atakos paviršiaus charakterizavimo modelio prototipą ir nustatyti jo veikimo savybes, efektyvumą, tikslumą ir naudingumą.

Eksperimentui iškeliami tikslai:

1. Išmatuoti prototipo greitaveiką ir naudojamą RAM atmintį, analizuojant skirtingus PCAP failo dydžius;
2. Ištirti prototipo gebėjimą analizuoti skirtingus atakos tipus, įvertinant jo efektyvumą ir tikslumą;
3. Palyginti prototipą su esamais įrankiais, naudojamais įvykusių DoS/DDoS incidentų atakos paviršiaus ištyrimui.

4.2. Tyrimo metu naudojama aparatinė įranga

Prototipui ištirti yra naudojamas nešiojamas kompiuteris, kuriame paruošta prototipo programa, bei kuri naudoja *Python* ir *Tshark* programas. Šiame kompiuteryje taip pat yra įrašyta Wireshark programa, su kuria bus lyginamas siūlomas modelis. Visa tyrimo metu naudota įranga pateikta 4.1 lentelėje.

4.1 lentelė. Tyrimo metu naudojama aparatinė ir programinė įranga

Aparatinė / programinė įranga	**Techninės savybės**
Nešiojamas kompiuteris MSI	Operacinė sistema: Windows 11 Home
	Operacinės sistemos versija: 25H2
	Procesorius: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz (2.59 GHz)
	Sistemos tipas: x64 pagrindo procesorius
	Įdiegta atmintis: 16,0 GB
Python	Versija: 3.14.2 (64-bit)
Wireshark (Tshark)	Versija: 4.6.1 x64

4.3. Tyrimui reikalingi atakos srautai

Tinkamai atlikti tyrimui, reikia turėti įvairių tipų DoS arba DDoS atakų srautus PCAP formato faile, kurie būtų tinkamai paruošti. Paruošimas apima rankinį srauto išfiltravimą, nuo atsitiktinių paketų ir nuo atakuojamų įrenginių atsakymų, kadangi šiuo metu modelyje nėra suprojektuotas tokie funkcionalumai.

Viešuose šaltiniuose yra galimybė parsisiųsti įvairių tipų atakų, nukreiptų prieš IT sistemas. Visgi, viešai prieinamų atakų nukreiptų prieš OT sistemas, o ypač SCADA sistemas, yra ribotas pasirinkimas. Tyrime taip pat yra analizuojama multivektorinė ataka, tačiau vėlgi yra susiduriama su

ribotu, tokio tipo atakų, pasirinkimu. Dėl šių priežasčių, tyrimui atlikti yra naudojami, ir viešai prieinami, ir šio darbo apimtyje sugeneruoti, DoS arba DDoS atakos srautai.

4.3.1. Naudojami atakos tinklo srautai kiekybiniame tyrime

Kiekybiniam tyrimui reikalingos trijų, skirtingų atakos tipų, kurie būtų užfiksuoti penkiais skirtingais dydžiais, failai ir trylika, atsitiktinai pasirenkamų atakos tipų IT ir OT sistemose, kurių dydis nėra svarbus.

Pirmam kiekybiniam tyrimui, iš viešai prieinamų šaltinių, yra gaunamos UDP perpildymo [51], TCP SYN perpildymo [52] ir HTTP GET perpildymo [53] atakos. Kai kuriuose nurodytuose šaltiniuose, šios atakos yra kaip sudedamoji dalis didesnės atakos, dėl to, naudojant Wireshark, kiekviena ataka yra išfiltruojama ir padalinama į penkis skirtingo dydžio failus po 200000, 400000, 600000, 800000 ir 1000000 paketų. Galutinai gaunama UDP perpildymo ataka, kurios visos datagramos siunčia į atakuojamą sistemą nuo 300 iki 450 baitų krovinį, TCP SYN, kuri siunčia tik segmentus su pakelta SYN vėliavėle, be krovinio ir HTTP GET, kuri iš viso siunčia apie 10000, 20000, 30000, 40000 ir 50000 užklausų, priklausomai nuo failo. Pasirinktos atakos ir jų dydžiai nurodyti 4.2 lentelėje

4.2 lentelė. Pirmam kiekybiniam tyrimui pasirinkti trys atakos tipai, išskaidyti skirtingais dydžiais

Atakos tipas	**Atakos dydis, paketais**
UDP perpildymas / TCP SYN perpildymas / HTTP GET perpildymas	200000
	400000
	600000
	800000
	1000000

Antram kiekybiniam tyrimui, iš viešai prieinamos Mazebolt duomenų bazės [54], yra parsisiunčiama dešimt DoS arba DDoS atakų prieš IT sistemas. Prioritetas skiriamas atakoms, kurios veikia prieš skirtingus įrenginius ir skirtingus OSI lygmenis. Toliau, iš viešai prieinamo, duomenų bazių rinkinio [55] yra parsisiunčiamos trys atakos nukreiptos prieš valdiklius arba industrinius protokolus. Pasirinktos atakos ir jų aprašymai pateikti 4.3 lentelėje.

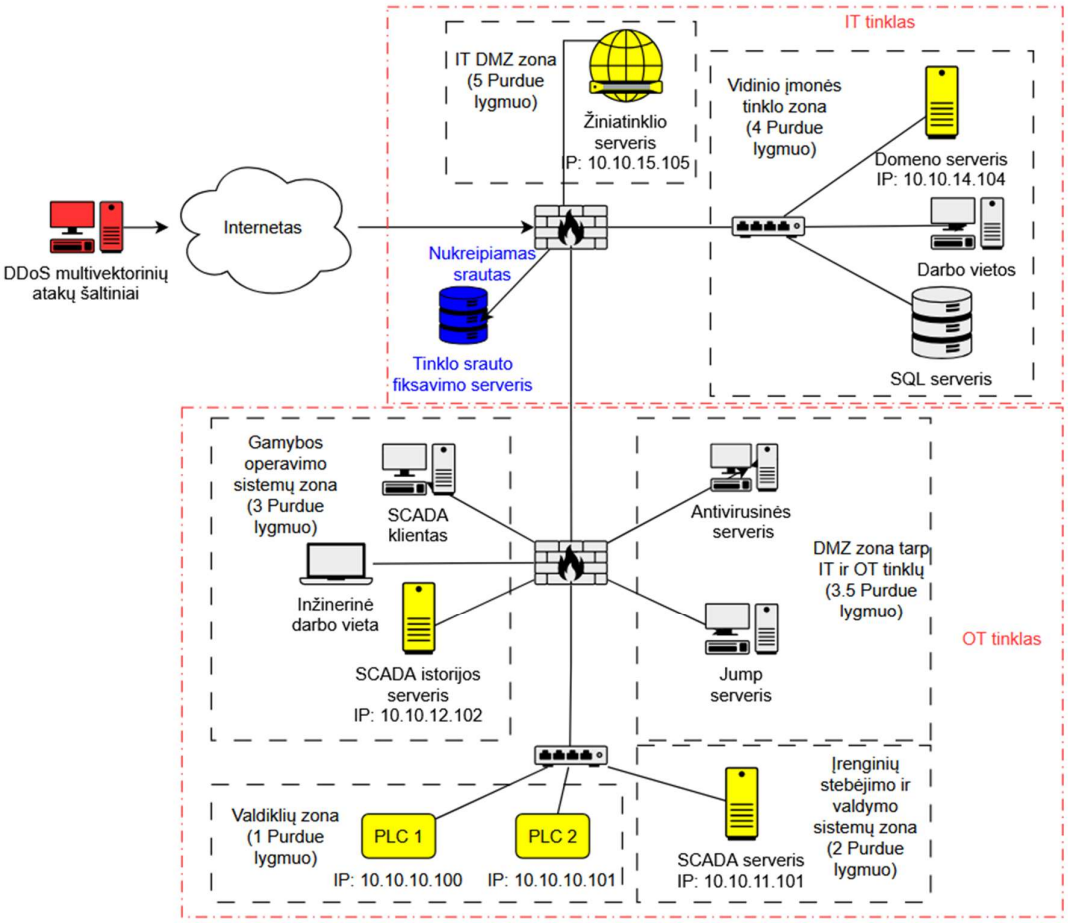
4.3 lentelė. Antram kiekybiniam tyrimui pasirinkta penkiolika skirtingų atakų ir jų aprašymai

Atakos numeris	**Atakos tipas**	**Atakuojami aparatiniai taškai**	**Atakuojami programiniai taškai**	**Atakuojama sistema (IT/OT)**	**Atakuojamas įrenginys**
IT1	DNS perpildymas	Vienas įrenginys	DNS protokolas	IT	Domeno vardų serveris
IT2	HTTP GET perpildymas	Vienas įrenginys	HTTP protokolas	IT	Žiniatinklio serveris
IT3	HTTPS perpildymas	Vienas įrenginys	HTTPS protokolas	IT	Žiniatinklio serveris
IT4	ICMP perpildymas	Vienas įrenginys	ICMP protokolas	IT	Žiniatinklio serveris
IT5	IPSEC IKE perpildymas	Vienas įrenginys	IPSEC IKE protokolas	IT	VPN šliuzo serveris
IT6	NTP nukreiptas perpildymas	Vienas įrenginys	UDP protokolas	IT	Žiniatinklio serveris
IT7	SYN perpildymas	Vienas įrenginys	TCP protokolas	IT	Žiniatinklio serveris
IT8	SIP perpildymas	Vienas įrenginys	SIP protokolas	IT	Telefonijos serveris
IT9	SMTP perpildymas	Vienas įrenginys	SMTP protokolas	IT	El. pašto šliuzo serveris

Atakos numeris	Atakos tipas	Atakuojami aparatiniai taškai	Atakuojami programiniai taškai	Atakuojama sistema (IT/OT)	Atakuojamas įrenginys
IT10	SSL raktų derėjimosi perpildymas	Vienas įrenginys	SSL protokolas	IT	Žiniatinklio serveris
OT11	IEC104 proceso perkrovimo komandų perpildymas	Trys įrenginiai	IEC104 protokolai	OT	Valdiklis
OT12	GOOSE perpildymas	Vienas įrenginys	GOOSE protokolas	OT	Valdiklis
OT13	ModbusTCP užklausų perpildymas	Vienas įrenginys	ModbusTCP protokolas	OT	Valdiklis

4.3.2. Naudojami atakos tinklo srautai kokybiniame tyrime

Išsamiam, kokybiniam tyrimui atlikti, yra reikalinga multivektorinė DoS arba DDoS ataka prieš įmonės IT ir OT sistemas. Šią ataką nusprendžiama sudaryti šio darbo apimtyje. Simuliuojama gamybos įmonė, kurioje yra IT ir OT sistemos, išskaidytos pagal *Purdue* modelį ir jo siūlomą tinklo segmentavimo principą. Šioje įmonėje imituojamas netinkamas tinklo įrenginių konfigūravimas, kuriuo metu dauguma įmonėje esančių įrenginių yra pasiekiami iš interneto. Simuliuojamos gamybos įmonės įrenginių tinklas pateiktas 4.1 paveiksle.



4.1 pav. Simuliuojamos gamybos įmonės įrenginių tinklo topologija. Geltona spalva paryškinti įrenginiai kurie atakuojami

Pirmu atakos simuliavimo etapu yra simuliuojama DDoS ataka prieš įmonės IT tinklo infrastruktūrą, žiniatinklio, bei įmonės domeno serverius. Simuliacijos metu yra naudojami UDP perpildymo, HTTP

GET ir LDAP užklausų perpildymo atakos tipai. Atakos tipams įvykdyti yra naudojami hping3 [56], ldapsearch [57] įrankiai ir *Python* scenarijus [58]. Visas srautas yra fiksuojamas tinklo srauto fiksavimo serverio naudojant Wireshark programą. Atakos pabaigoje PCAP formato failas yra rankiniu būdu išfiltruojamas, paliekant tik DDoS atakos srautą.

Antru atakos simuliavimo etapu yra simuliuojama DDoS ataka prieš įmonės OT tinklo infrastruktūrą, SCADA istorijos kaupimo ir SCADA serverius, bei du valdiklius, kurie naudoja skirtingus protokolus. Simuliacijos metu yra naudojami UDP ir TCP SYN perpildymai, ModbusTCP užklausų ir IEC104 komandų perpildymai. Atakos tipams susimuliuoti yra naudojami ankščiau minėti įrankiai kartu su ModbusTCP ir IEC104 perpildymams naudojamais *Python* scenarijais, kurie pateikti 5 priede. Srautas fiksuojamas serverio, kuris naudoja Wireshark programą. Atakos pabaigoje užfiksuotas PCAP failas yra rankiniu būdu išfiltruojamas ir išsaugojamas.

4.4. Kiekybinis prototipo tyrimas

Prototipo kiekybiniam tyrimui siūloma atlikti skirtingų DDoS atakos tipų, kurie būtų užfiksuoti skirtingais failo dydžiais, analizę, tokiu būdu įvertinant atlikimo trukmę ir programos naudojamą RAM atmintį. Taip pat siūloma atlikti skirtingų atakos tipų analizę, įvertinant modelio tikslumą ir gebėjimą šias atakas išanalizuoti ir pateikti reikiamą informaciją.

4.4.1. Tyrimas analizuojant skirtingo dydžio failus

Šiame tyrime pasirenkama po vieną atakos tipą iš pagrindinių atakos klasių. Kiekvienas pasirinktas atakos tipas išskaidomas į skirtingo dydžio, failus pagal paketų kiekį. Parinkti atakos tipai:

- UDP perpildymas (Tūrinės atakos);
- TCP SYN perpildymas (Protokolų atakos);
- HTTP GET perpildymas (Paslaugų atakos).

Analizės atlikimo laikas fiksuojamas rankiniu būdu naudojant chronometrą. Naudojama RAM atmintis fiksuojama naudojant „*Windows Resource Monitor*“ programos, „*Memory*“ langą. Šiame lange vertinamos dvi programos: *Python* programa (prototipas) ir jo iškviečiama *Tshark*.

Skirtingo dydžio failų, UDP perpildymo analizė:

Atliekamas UDP perpildymo atakos tyrimas, matuojant analizės atlikimo greitį sekundėmis ir iš viso panaudotą RAM atmintį megabaitais. Rezultatai pateikti 4.4 lentelėje.

4.4 lentelė. UDP perpildymo atakos analizės našumo įvertinimo rezultatai

Atakos tipas	Analizės nr.	Failo dydis, MB	Paketu kiekis	Analizės atlikimo laikas, s	Viso panaudota RAM atminties, MB
UDP perpildymas	UDP1	82,35	200000	10,84	656,34
	UDP2	164,74	400000	21,06	705,51
	UDP3	247,02	600000	29,88	763,04
	UDP4	329,16	800000	39,45	812,32
	UDP5	411,32	1000000	48,91	851,92

Skirtingo dydžio failų, TCP SYN perpildymo analizė:

Atliekamas TCP SYN perpildymo atakos tyrimas, matuojant analizės atlikimo greitį sekundėmis ir iš viso panaudotą RAM atmintį megabaitais. Rezultatai pateikti 4.5 lentelėje.

4.5 lentelė. TCP SYN perpildymo atakos analizės našumo įvertinimo rezultatai

Atakos tipas	**Analizės nr.**	**Failo dydis, MB**	**Paketų kiekis**	**Analizės atlikimo laikas, s**	**Viso panaudota RAM atminties, MB**
TCP SYN perpildymas	TCP1	13,67	200000	8,85	902,52
	TCP2	27,34	400000	17,57	1272,22
	TCP3	41,01	600000	25,64	1641,71
	TCP4	54,68	800000	34,10	1970,22
	TCP5	68,36	1000000	42,55	2339,77

Skirtingo dydžio failų, HTTP GET perpildymo analizė:

Atliekamas HTTP GET perpildymo atakos tyrimas, matuojant analizės atlikimo greitį sekundėmis ir iš viso panaudotą RAM atmintį megabaitais. Rezultatai pateikti 4.6 lentelėje.

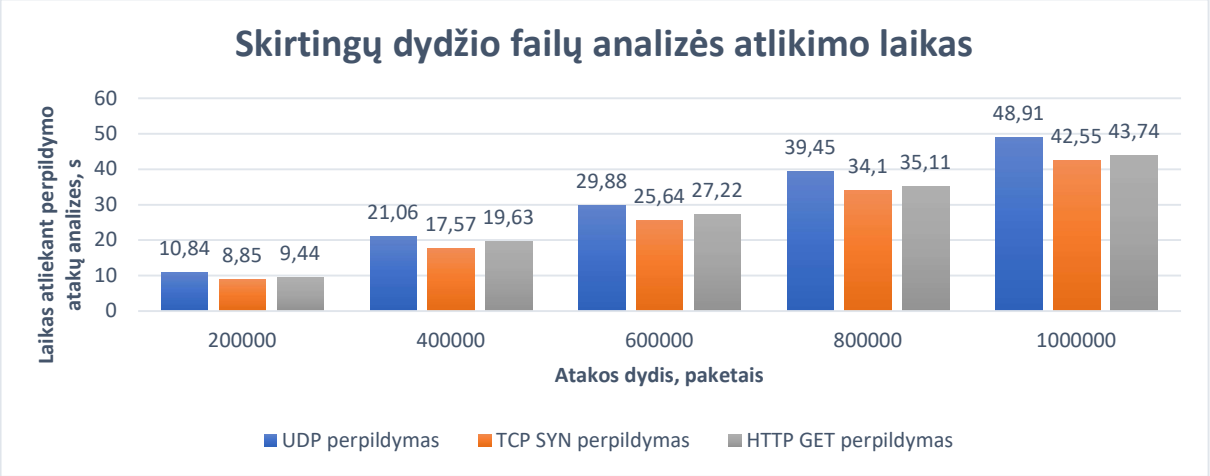
4.6 lentelė. HTTP GET perpildymo atakos analizės našumo įvertinimo rezultatai

Atakos tipas	**Analizės nr.**	**Failo dydis, MB**	**Paketų (užklausų) kiekis**	**Analizės atlikimo laikas, s**	**Viso panaudota RAM atminties, MB**
HTTP GET perpildymas	HTTP1	25,21	200000	9,44	738,35
	HTTP2	50,09	400000	19,63	845,18
	HTTP3	75,16	600000	27,22	968,31
	HTTP4	100,77	800000	35,11	1091,52
	HTTP5	126,22	1000000	43,74	1222,88

Skirtingo dydžio failų analizės išvados:

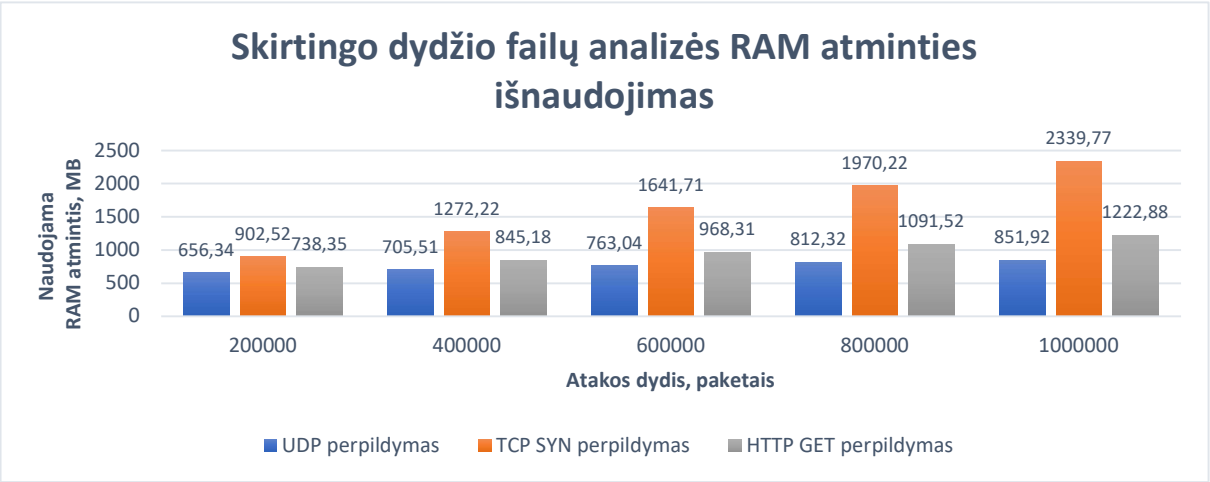
Iš atlikto pirmo kiekybinio tyrimo rezultatų sudaromi grafikai, kuriuose matomas laiko trukmės ir RAM atminties naudojimo priklausomybės nuo analizuojamo PCAP failo dydžio, skirtingais atakos tipais (4.2 ir 4.3 pav.).

Iš laiko trukmės, pagal failo dydį, grafiko matoma, kad faile esant didesniam skaičiui paketų, analizė tampa ilgesnė. 1000000 paketų failą, skirtinguose atakos tipuose, išanalizuoti vidutiniškai užtrunka apie 45 sekundes, nepaisant to, kad UDP perpildymo atakos, failo dydis megabaitais buvo gerokai didesnis už kitų atakos tipų. Taip yra dėl to, nes prototipas šiuo metu analizuoja informaciją tik iki ketvirto OSI lygmens, apie septintą OSI lygmenį spręsdamas pagal prievadus ir siunčiamo krovinio dydį. Failų dydžiai megabaitais skiriasi, nes UDP perpildymo atakos metu, kiekvienas paketas nešė 350 - 400 baitų krovinį, TCP SYN perpildymo ataka buvo siunčiami tik SYN paketai, be krovinio, o HTTP GET perpildymo atakos atveju, apie 400 baitų krovinys buvo siunčiamas tik kas devynioliktą paketą.



4.2 pav. Skirtingo dydžio failų, pagal atakos tipus, analizės trukmės rezultatai

Iš RAM atminties naudojimo, pagal failo dydį, nustatoma, kad analizė reikalauja daugiau RAM atminties, esant didesniems failams. Paleista programa savaime naudoja apie 522MB RAM ir atliekant paviršiaus analizę, atsiranda momentiniai šuoliai iki 1000MB priklausomai nuo aparatinių ir programinių taškų skaičiaus. Tačiau daugiausiai RAM atminties naudoja *Tshark* programa, kuri naudojama požymiams iš PCAP failo ištraukti. Vidutiniškai, 1000000 paketų failo, skirtinguose atakos tipuose, analizavimas reikalauja 1471,52 MB RAM atminties. Pastebima, kad TCP SYN perpildymo atakos analizė reikalauja daugiau atminties negu kitų atakos tipų analizės. Taip yra dėl to nes *Tshark* programa iš UDP protokolo antraštės ištraukia mažesnį kiekį požymių, negu iš TCP protokolo antraštės. O atminties naudojimo skirtumas tarp TCP SYN ir HTTP GET paaiškinamas tuo, jog TCP SYN perpildymo atveju visi paketai buvo siunčiami iš atsitiktinių prievadų.



4.3 pav. Skirtingo dydžio failų, pagal atakos tipus, analizės atminties panaudojimo rezultatai

4.4.2. Tyrimas analizuojant skirtingo tipo atakas

Šiame tyrime analizuojami pasirinkti atakos tipai, kurie yra nurodyti 4.3 lentelėje. Iš viso pasirinkta dešimt atakos tipų prieš IT sistemas ir trys prieš OT sistemas.

Tyrimo metu vertinamas prototipo gebėjimas pateikti informaciją pagal kriterijus, kurie išsikelti pagal siūlomo modelio numatytas funkcijas:

- Atakuojamų aparatinių taškų identifikavimas (unikalių IP adresų);
- Atakuojamų programinių taškų identifikavimas (unikalios paslaugos arba protokolai);
- Taškų priskyrimas IT arba OT sistemoms;
- Atakuojamo įrenginio identifikavimas.

Tinkamas aparatinių taškų identifikavimas laikomas gebėjimas išskirti ir pateikti visus atakuojamus IP adresus. Programinių taškų tinkamas identifikavimas laikomas, kada yra teisingai nurodomas atakuojamas protokolas arba paslauga. Tinkamas priskyrimas prie IT ir OT laikoma, kada prototipas nurodė atakuojamo taško lygmenį pagal *Purdue* modelį. Atakuojamo įrenginio identifikavimas laikomas tinkamu, kada gavus visą informaciją yra galimybė nustatyti įrenginio tipą ir jo paskirtį sistemoje. Galutiniai rezultatai pateikti 4.7 lentelėje.

4.7 lentelė. Skirtingų atakos tipų analizės rezultatai

Atakos numeris	**Analizuojamas atakos tipas**	**Nustatomi aparatiniai taškai**	**Nustatomi programiniai taškai**	**Priskyrimas IT arba OT sistemai**	**Nustatomas atakuojamo įrenginio tipas**
IT1	DNS perpildymas	Taip	Taip	Taip	Taip
IT2	HTTP GET perpildymas	Taip	Taip	Taip	Taip
IT3	HTTPS perpildymas	Taip	Taip	Taip	Taip
IT4	ICMP perpildymas	Taip	Taip	Ne	Ne
IT5	IPSEC IKE perpildymas	Taip	Taip	Taip	Taip
IT6	NTP nukreiptas perpildymas	Taip	Taip, tačiau klaidingai	Ne	Ne
IT7	SYN perpildymas	Taip	Taip	Taip	Taip
IT8	SIP perpildymas	Taip	Taip	Ne	Taip
IT9	SMTP perpildymas	Taip	Taip	Ne	Taip
IT10	SSL raktų derėjimosi perpildymas	Taip	Taip, tačiau klaidingai	Taip	Taip
OT11	IEC104 proceso perkrovimo komandų perpildymas	Taip	Taip	Taip	Taip
OT12	GOOSE perpildymas	Ne	Ne	Ne	Ne
OT13	ModbusTCP užklausų perpildymas	Taip	Taip	Taip	Taip

Skirtingų atakos tipų analizės išvados:

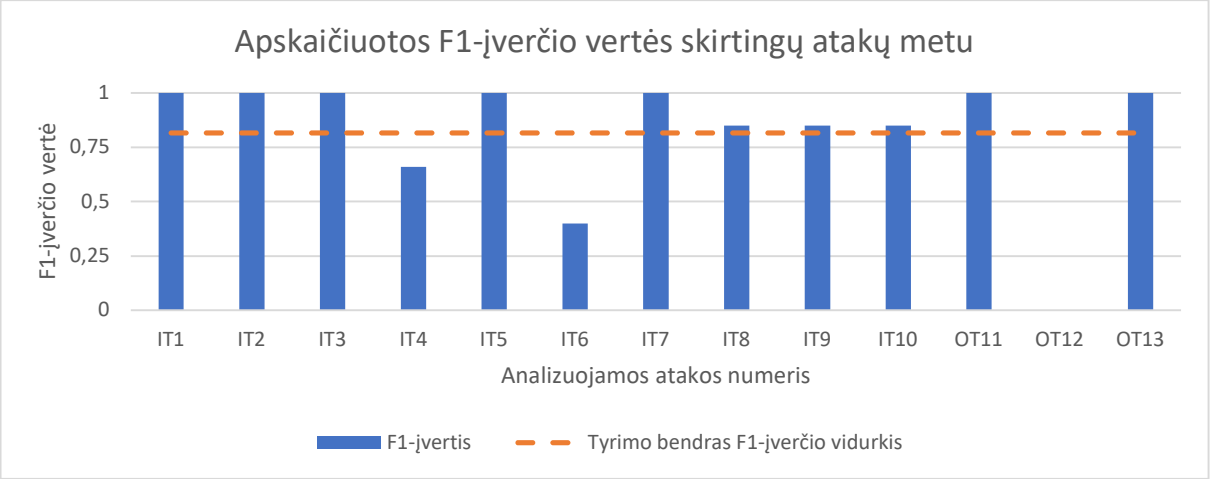
Iš atlikto antro kiekybinio tyrimo rezultatų (4.7 lentelė) galima teigti, kad prototipas sugebėjo pateikti atakos paviršių, pagal išsikeltus kriterijus, daugiau negu pusei analizuojamų atakų (IT1, IT2, IT3, IT5, IT7, OT11, OT13). Keturis atakos tipus (IT4, IT8, IT9, IT10) prototipas dalinai išanalizavo ir dvi atakos laikomos prastai išanalizuotomis arba visai neišanalizuotomis (IT6, OT12).

Tikslumui įvertinti, pagal gautus rezultatus, apskaičiuojamos metrikos: Jautrumas (*angl. recall*), tikslumas (*angl. precision*) ir F1-įvertis (*angl. F1-score*) [59]. Kriterijai, į kuriuos atsakyta „Taip“ laikomi teigiami (*angl. true positive*), į kuriuos atsakyta „Taip, tačiau klaidingai“ – klaidingai teigiami (*angl. false positive*) ir į kuriuos atsakyta „Ne“ – klaidingai neigiami (*angl. false negavite*). Metrikų apskaičiavimui naudojama internetinė skaičiuoklė [60]. Rezultatai pateikiami 4.8 lentelėje.

4.8 lentelė. Apskaičiuotos „Recall“, „Precision“ ir „F1-score“ metrikos

Atakos numeris	**Analizuojamos atakos tipas**	**Jautrumas (*recall*)**	**Tikslumas (*precision*)**	**F1-įvertis (*F1-score*)**
IT1	DNS perpildymas	1	1	1
IT2	HTTP GET perpildymas	1	1	1
IT3	HTTPS perpildymas	1	1	1
IT4	ICMP perpildymas	0,5	1	0,66
IT5	IPSEC IKE perpildymas	1	1	1
IT6	NTP nukreiptas perpildymas	0,33	0,5	0,4
IT7	SYN perpildymas	1	1	1
IT8	SIP perpildymas	0,75	1	0,85
IT9	SMTP perpildymas	0,75	1	0,85
IT10	SSL raktų derėjimosi perpildymas	1	0,75	0,85
OT11	IEC104 proceso perkrovimo komandų perpildymas	1	1	1
OT12	GOOSE perpildymas	0	0	0
OT13	ModbusTCP užklausų perpildymas	1	1	1

Atskirai vertinant jautrumo arba tikslumo metrikas galima susidaryti klaidingą išvadą apie tyrimą. Todėl galutinis vertinimas atliekamas pagal F1-įvertį, kuris įvertina pastarąsias dvi metrikas pateikdamas realų, atlikto tyrimo, balansą. Visos apskaičiuotos F1-įverčio vertės pateiktos 4.4 paveiksle.



4.4 pav. Skirtingų atakų analizės metu apskaičiuota F1-score vertė

Remiantis F1-įverčiu, skirtingų atakos tipų analizės metu (4.4 pav.), daroma išvada, jog prototipas gebėjo, tinkamai ištirti atakos paviršių daugumoje testų. Apibendrintas šio tyrimo metu gautas F1-įvertis yra 0,81.

Skirtingų atakos tipų analizės, klaidingų rezultatų priežastys:

Priežastys, dėl kurių buvo netinkamai atliekamos analizės, yra specifinio tipo atakos, kuriuos nebuvo įvertintos siūlomame modelyje. Vienas iš pavyzdžių yra ataka prieš GOOSE protokolą (OT12 testas), kuris atakuoja valdiklyje veikiančią paslaugą, tačiau tinklo lygmenyje, paketai sudaromi tik iki antro OSI lygmens. Modelis šiuo metu atliekant analizę priklauso nuo trečio OSI lygmens ir jo neradus analizės visai nepradeda. Dar vienas nesėkmingas testas yra IT6, kuriame buvo analizuojama NTP nukreipto užtvindymo ataka. Šio atakos metu yra gaunami NTP serverio atsakymai į atakuojamą sistemą fragmentuotais paketais. Modelis šiuo metu nevertina paketų fragmentavimo ir susidūręs su jais, juos ignoruoja arba apdoroja klaidingai. Testas IT10 atakuoja SSL protokolą, kuris veikia

šeštame OSI lygmenyje. Modelis šio lygmens taip pat neanalizuoja, kadangi šiame lygmenyje veikia nedaug atakų ir jos taip pat yra specifinės. Toliau, dalinai išanalizuotos atakos (IT4, IT8 ir IT9), priklausė nuo tinkamo *Purdue* lygmenų – prievadų šablono, kuriame šiuo metu nėra įtrauktos visos paslaugos su prievadais. Dėl šios priežasties prototipas negalėjo tinkamai parinkti lygmens pagal *Purdue* modelį.

4.5. Kokybinis prototipo tyrimas

Prototipo kokybiniam tyrimui siūloma atlikti DDoS multivektorinės atakos, prieš IT ir OT sistemas, analizę. Tyrimai atliekami naudojant Wireshark ir siūlomo modelio programas. Šių programų pateiktos analizės lyginamos tarpusavyje. Tyrimo metu yra analizuojami du skirtingi PCAP failai, vienas, kuriame yra atakuojamas IT tinklas ir kitas, kuriame atakuojamas OT tinklas.

4.5.1. Multivektorinių atakų analizė naudojant Wireshark

Analizė, naudojant Wireshark programą atliekama pagal siūlomą scenarijų [61]. Naudojant statistikos sudarymo funkcijas, yra patikrinami galiniai taškai, protokolų hierarchija, rankiniu būdu naudojami įvairūs filtrai. Kadangi analizuojama ataka yra DDoS, statistinių duomenų sudarymo metu reikalinga įvertinti, kad yra pateikiami visi atakoje dalyvaujantys IP adresai. Visgi yra žinoma, kad PCAP failuose esantis tinklo srautas išfiltruotas, todėl pagal „ip.dst“ filtrą galime nustatyti atakuojamus IP adresus. Protokolų hierarchijos statistikoje taip pat reikia įvertinti, kad UDP ataka atakuoja atsitiktinius prievadus. Wireshark visus žinomus prievadus verčia į aukštesnio lygmens protokolus. Visgi TCP prievadai ir atakuojami protokolai identifikuojami teisingai.

Atliekama analizė, abiem atvejais – IT ir OT sistemose, nėra niekaip išskiriama, tai turi atlikti tyrėjas savarankiškai, pagal gautą informaciją ir savo asmeninę patirtį. Be to, naudojant Wireshark programą, dalinai analizė atliekama rankiniu būdu filtruojant ir analizuojant gautą informaciją, taip ne tik prailgina analizės laiką, tačiau ir reikalauja atitinkamų programai reikalingų žinių.

Atlikus analizę gaunamos pagrindinės išvados:

- Analizė atliekama rankiniu būdu;
- Naudojant filtravimo metodą randami atakuojami aparatiniai taškai;
- Naudojant protokolų hierarchijos statistikos sudarymo funkciją dalinai aptinkami atakuojami programiniai taškai;
- Naudojant filtravimo metodus galima išsiaiškinti atakos pradžią ir pabaigą;
- Išverčiami MAC adresai;
- Išverčiami protokolai pagal prievadus.

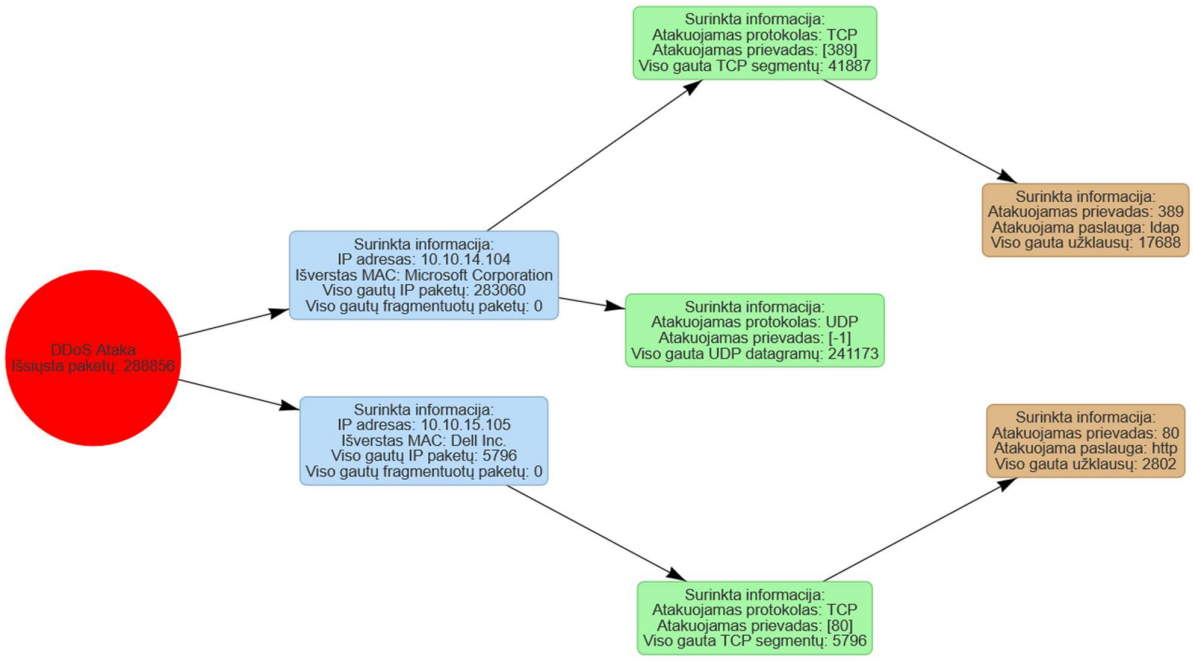
4.5.2. Multivektorinių atakų analizė naudojant siūlomo modelio programą

Analizė atliekama pagal siūlomo modelio prototipą yra automatizuota. Programa paleidžiama, pasirenkamas pirmas PCAP failas ir pradedama analizė, vėliau kartojama procedūra su antru PCAP failu. Abiejų analizių metu identifikuojami atakuojami aparatiniai ir programiniai taškai. Taip pat analizės pabaigoje gaunama po dvi topologijas kiekvienam PCAP failui: atakos paviršiaus ir atakos

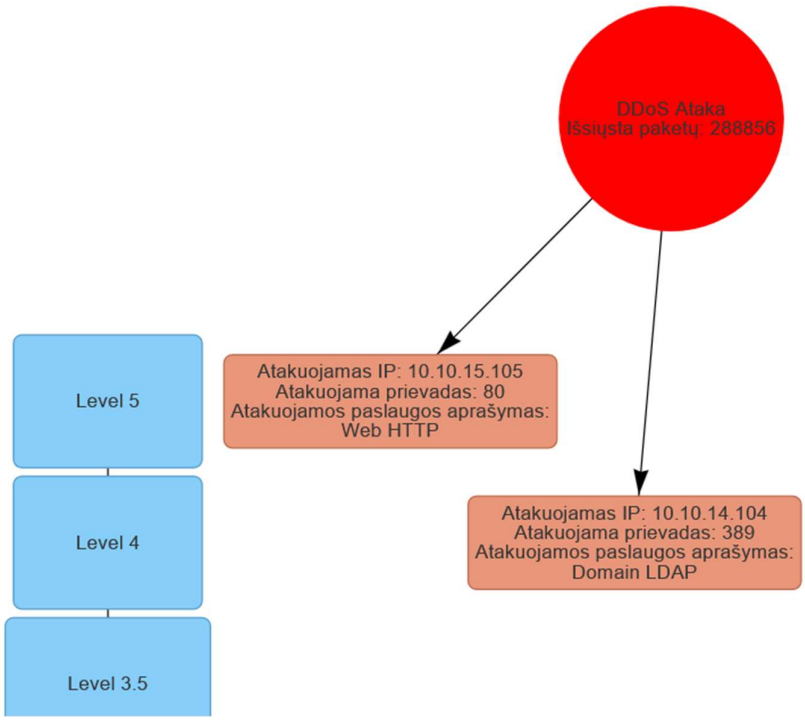
paviršiaus išskaidyto pagal *Purdue* modelį. Pagal šias topologijas vizualiai matomas skirtumas tarp analizuojamų atakų, kadangi viena ataka orientuota į IT sistemą, kita į OT sistemą. Šios vizualizacijos pateiktos žemiau esančiuose paveiksluose (4.5 – 4.8 pav.). Papildomai programa, automatiškai, surenka informaciją apie atakos pradžią ir pabaigą kiekvienam aparatiniam taškui, pateikiamas atakos srauto dydis baitais per sekundę.

Atlikus analizę gaunamos pagrindinės išvados:

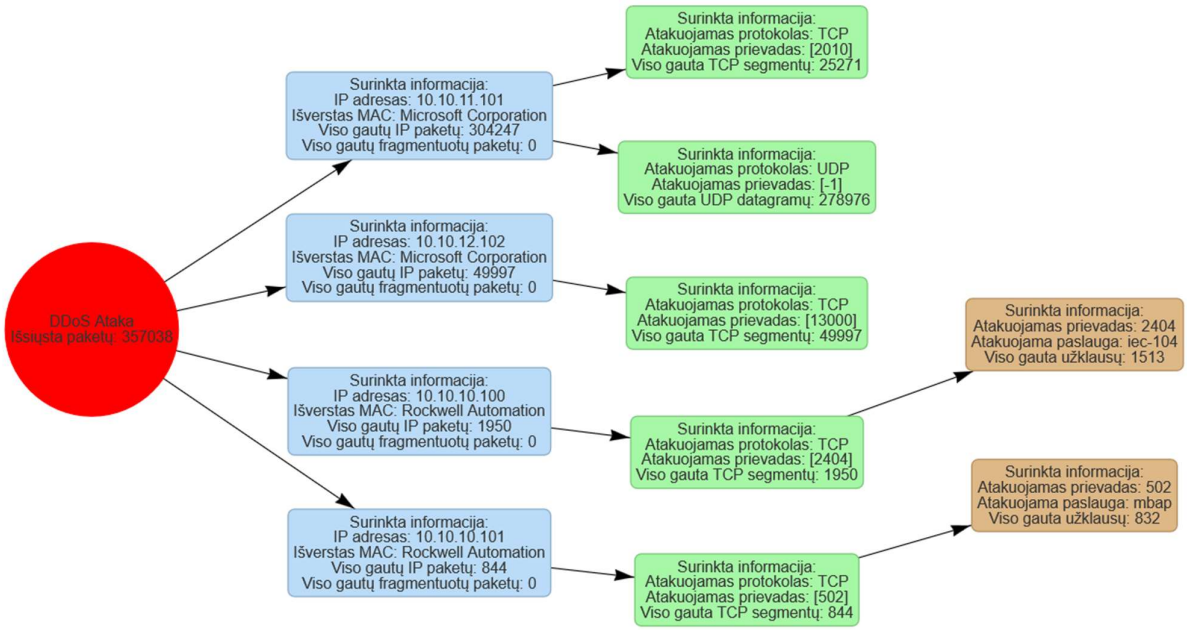
- Analizė veikia automatizuotai;
- Automatiškai identifikuojami aparatiniai taškai (gavėjo IP adresai);
- Automatiškai identifikuojami programiniai taškai (protokolai, prievadai, paslaugos);
- Analizė geba atskirti atakas IT ir OT tinkluose;
- Analizė pateikia topologijas;
- Automatiškai randami atakos pradžios ir pabaigos laikai;
- Automatiškai pateikiama atakos srauto dydis;
- Išverčiami MAC adresai;
- Išverčiami protokolai ir(arba) paslaugos pagal prievadus.



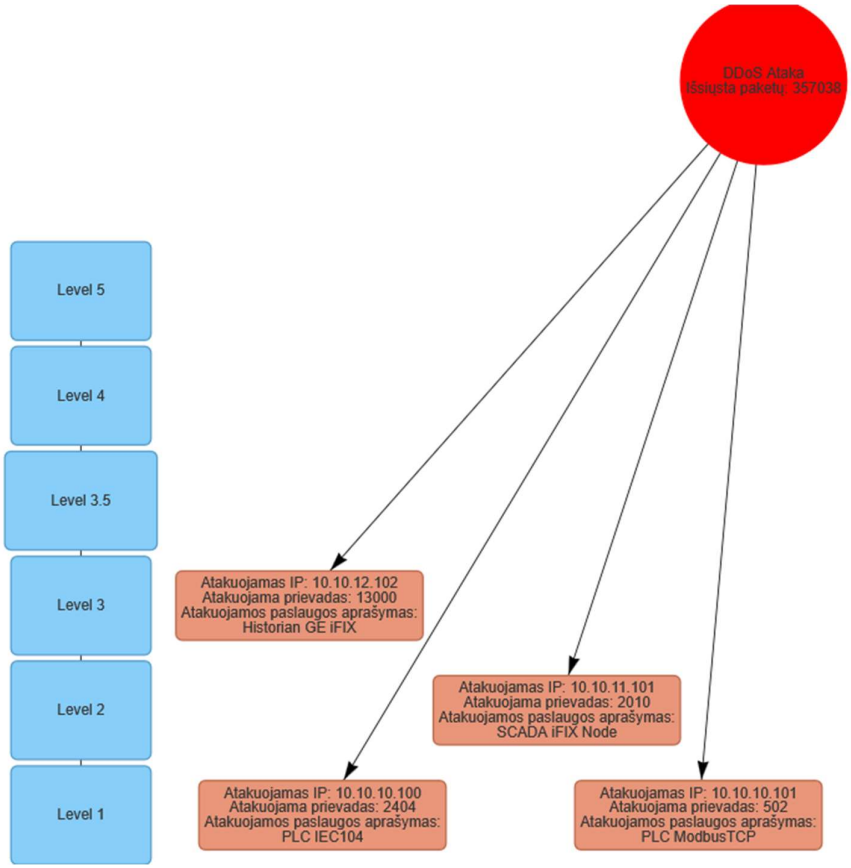
4.5 pav. Multivektorinės atakos IT tinkle atakos paviršiaus topologija



4.6 pav. Multivektorinės atakos IT tinkle atakos paviršiaus išskaidytos pagal *Purdue* lygmenis topologija



4.7 pav. Multivektorinės atakos OT tinkle atakos paviršiaus topologija



4.8 pav. Multivektorinės atakos OT tinkle atakos paviršiaus išskaidytos pagal *Purdue* lygmenis topologija

4.5.3. Kokybinio tyrimo rezultatai

Apibendrinti tyrimo rezultatai, analizuojant atakas prieš IT ir OT sistemas, pateikti 4.9 lentelėje. Atakos paviršiaus analizės srityje matomas siūlomo modelio pranašumas, kadangi analizė buvo atliekama automatiškai, bei įrenginiai buvo suklasifikuojami į skirtingas sistemas.

4.9 lentelė. Kokybinio tyrimo metu gauti pagrindiniai rezultatai

Kriterijus	**Įvertinimas analizei naudojant Wireshark**	**Įvertinimas analizei naudojant siūlomą modelį**
Analizės automatizavimas	Ne	Taip
Aparatinių taškų identifikavimas (atakuojami IP adresai)	Taip, filtruojant paketus	Taip, automatiškai
Programinių taškų identifikavimas (atakuojamos paslaugos, protokolai)	Dalinai, filtruojant paketus	Taip, automatiškai
Atakos IT ir OT sistemose išskyrimas	Ne	Taip,
Vizualizacijos pateikimas	Ne	Taip, dvi topologijos

Nors modelis šiuo metu ir pateikia atakos paviršiaus analizę paprasčiau ir greičiau negu kitos programos, visgi kiti svarbūs DoS arba DDoS aspektai nėra analizuojami šio modelio. Dėl tos priežasties yra sudėtinga lygiavertiškai atlikti įrankių palyginimą, kadangi kiti įrankiai geba analizuoti ne tik atakos paviršių. Taip pat siūlomas modelis šiuo metu yra stipriai priklausomas nuo tokių programų kaip Wireshark, kad prieš analizę būtų rankiniu būdu išfiltruojamas atsitiktinių įrenginių tinklo srautas ir identifikuojama ataka.

4.6. Eksperimento dalies išvados

1. Atliekant tyrimą nuspręsta naudoti, ir iš viešų šaltinių parsisiųstas, ir šio darbo apimtyje susimuliuotas, atakas. Priežastis – mažesnis DoS arba DDoS multivektorinių atakos tipų ir šių atakų į OT sistemas pasirinkimas viešuose šaltiniuose.

2. Pirmo kiekybinio tyrimo metu, tiriant skirtingus atakos tipus, skirtingais failo dydžiais, nustatyta, kad nepaisant atakos tipo, vidutiniškai 1000000 paketų failas yra analizuojamas apie 45 sekundes ir vidutiniškai analizavimas reikalauja 1471,52 MB RAM atminties.

3. Antro kiekybinio tyrimo metu, tiriant atakos paviršių, skirtingais atakos tipais, nustatytas F1-įvertis – 0,81. Tai parodo modelio aukštą tikslumą nustatinėjant atakos paviršių sistemoje. Visgi pastebėtas modelio trūkumas, kuriuo metu nėra tinkamai išanalizuojamos labiau specifinės DoS arba DDoS atakos.

4. Kokybinio tyrimo metu, naudojant prototipą pasimatė jo efektyvumas ir pranašumas prieš kitus įrankius, kadangi tik jis gebėjo atlikti analizę automatiškai ir suklasifikuoti atakuojamus įrenginius į IT ir OT sistemas.

5. Nors ir matomas prototipo kokybinis pranašumas, kokybinio tyrimo metu, visgi jis išlieka stipriai priklausomas nuo tų pačių programų su kuriais buvo atliekamas palyginimas. Prototipas savaime nesugeba išfiltruoti tinkamai tinklo srauto nuo atsitiktinių paketų, bei pats nesugeba aptikti DoS arba DDoS atakos.

Išvados

1. Analizuojant skirtingų atakos vektorių, atakos paviršiaus charakterizavimo modelius nustatyta, pagal kokius metodus ir tinklo srauto požymius šiuo metu atliekamas atakuojamų įrenginių ir jų funkcijų identifikavimas sistemoje.

2. Remiantis DoS/DDoS atakų tipų analize nustatyti ir aprašyti pagrindiniai aparatiniai ir programiniai atakos taškai, pagal kuriuos sudaryta atakos paviršiaus klasifikacija, papildomai ją susiejant su *Purdue* modelio lygmenimis. Toks klasifikavimas leidžia geriau suprasti atakos loginį gylį sistemoje ir įvertinti atakų keliamą pavojingumą.

3. Modelis projektuojamas tokiu principu, kad būtų galima sudaryti automatizuotus įrankius atakos paviršiaus analizei iš įvairių formatų tinklo srauto failų, visgi tinklo sraute privalo egzistuoti tam tikri požymiai, tokie kaip MAC adresai, IP adresai, prievadai ir kroviniai, be kurių ši analizė negalėtų būti atliekama.

4. Kadangi siūlomas prototipas kuriamas PCAP formato tinklo srauto analizei, kuriame yra užfiksuotos visų OSI modelio lygmenų antraštės, papildomai yra surenkama informacija apie atakos pradžios ir pabaigos laikus, bendrą išsiųstų baitų kiekį, išskaičiuojamą atakos srauto dydį, tokiu būdu parodant gebėjimą plėsti analizės programą.

5. Kiekybinio tyrimo metu nustatyta, jog analizuojant didesnį paketų skaičių analizės trukmė ir naudojama RAM atmintis tai pat didėja, o analizuojant skirtingus atakos tipus pasiektas F1-įvertis – 0,81, o tai gana aukštas tikslumas. Atliekant tikslumo nustatymo tyrimą pasimatė modelio silpnybė prieš specifines DoS arba DDoS atakas.

6. Kokybinio tyrimo metu nustatytas modelio pranašumas prieš kitus įrankius dėl atakos paviršiaus analizės automatizacijos ir gebėjimo priskirti įrenginius į IT ir OT sistemas pagal *Purdue* modelį, tačiau modelis turi trūkumų dėl kurių stipriai priklauso nuo tų pačių įrankių, su kuriais buvo atliekamas palyginimas.

Literatūros sąrašas

1. A. S. Mohammed, E. Anthi, O. Rana, N. Saxena, ir P. Burnap, „Detection and mitigation of field flooding attacks on oil and gas critical infrastructure communication“, *Computers & Security*, t. 124, p. 103007, saus. 2023, doi: 10.1016/j.cose.2022.103007.

2. M. Merkebaiuly, „Overview of Distributed Denial of Service (DDoS) attack types and mitigation methods“, *InterConf*+, nr. 43(193), p. 494–508, kovo 2024, doi: 10.51582/interconf.19-20.03.2024.048.

3. Sunny Behal ir Krishan Kumar, „Characterization and Comparison of DDoS Attack Tools and Traffic Generators - A Review“, *International Journal of Network Security*, t. 19, nr. 3, geg. 2017, doi: 10.6633/IJNS.201703.19(3).07.

4. I. Sharafaldin, A. H. Lashkari, S. Hakak, ir A. A. Ghorbani, „Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy“, *2019 International Carnahan Conference on Security Technology (ICCST)*, CHENNAI, India: IEEE, spal. 2019, p. 1–8. doi: 10.1109/CCST.2019.8888419.

5. O. Ussatova, A. Zhumabekova, Y. Begimbayeva, E. T. Matson, ir N. Ussatov, „Comprehensive DDoS Attack Classification Using Machine Learning Algorithms“, *Computers, Materials & Continua*, t. 73, nr. 1, p. 577–594, 2022, doi: 10.32604/cmc.2022.026552.

6. „Understanding and Responding to Distributed Denial-Of-Service Attacks | CISA“. Žiūrėta: 2026 m. balandžio 17 d. [Interaktyvus]. Adresas: https://www.cisa.gov/resources-tools/resources/understanding-and-responding-distributed-denial-service-attacks

7. Wazuh ir O. Soneye, „Network security monitoring with Wazuh and Zeek“, Wazuh. Žiūrėta: 2026 m. balandžio 17 d. [Interaktyvus]. Adresas: https://wazuh.com/blog/network-security-monitoring-with-wazuh-and-zeek/

8. R. Sharma, „Analyzing a DDOS Attack Using Wireshark“, Medium. Žiūrėta: 2026 m. balandžio 17 d. [Interaktyvus]. Adresas: https://medium.com/@ronak.d.sharma111/analyzing-a-ddos-attack-using-wireshark-8535274cd00e

9. „Incident Forensics with SIEM: A Comprehensive Guide - SearchInform“. Žiūrėta: 2026 m. balandžio 17 d. [Interaktyvus]. Adresas: https://searchinform.com/articles/cybersecurity/measures/siem/analytics/incident-forensics/

10. T. C. Team, „ICS Security: The Purdue Model“, Claroty. Žiūrėta: 2026 m. kovo 29 d. [Interaktyvus]. Adresas: https://claroty.com/blog/ics-security-the-purdue-model

11. C. Theisen, N. Munaiah, M. Al-Zyoud, J. C. Carver, A. Meneely, ir L. Williams, „Attack surface definitions: A systematic literature review“, *Information and Software Technology*, t. 104, p. 94–103, gruodž. 2018, doi: 10.1016/j.infsof.2018.07.008.

12. „What is an Attack Surface? Definition and How to Reduce It“, Fortinet. Žiūrėta: 2026 m. kovo 29 d. [Interaktyvus]. Adresas: https://www.fortinet.com/resources/cyberglossary/attack-surface

13. Hadeel S. Obaid ir Esamaddin H. Abeed, „DoS and DDoS Attacks at OSI Layers“, saus. 2020, doi: 10.5281/ZENODO.3610833.

14. „OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation“. Žiūrėta: 2026 m. kovo 29 d. [Interaktyvus]. Adresas: https://owasp.org/

15. „Denial of Service - OWASP Cheat Sheet Series“. Žiūrėta: 2026 m. kovo 29 d. [Interaktyvus]. Adresas: https://cheatsheetseries.owasp.org/cheatsheets/Denial_of_Service_Cheat_Sheet.html#analyzing-dos-attack-surfaces

16. N. Tripathi ir N. Hubballi, „Application Layer Denial-of-Service Attacks and Defense Mechanisms: A Survey“, *ACM Comput. Surv.*, t. 54, nr. 4, p. 1–33, geg. 2022, doi: 10.1145/3448291.

17. S. Rizvi, R. Orr, A. Cox, P. Ashokkumar, ir M. R. Rizvi, „Identifying the attack surface for IoT network“, *Internet of Things*, t. 9, p. 100162, kovo 2020, doi: 10.1016/j.iot.2020.100162.

18. T. Ashley, S. N. G. Gourisetti, N. Brown, ir C. Bonebrake, „Aggregate attack surface management for network discovery of operational technology“, *Computers & Security*, t. 123, p. 102939, gruodž. 2022, doi: 10.1016/j.cose.2022.102939.

19. „Wireshark • Go Deep“, Wireshark. Žiūrėta: 2026 m. balandžio 8 d. [Interaktyvus]. Adresas: https://www.wireshark.org/

20. G. Harris ir M. Richardson, „PCAP Capture File Format“, Internet Engineering Task Force, Internet Draft draft-gharris-opsawg-pcap-01, gruodž. 2020. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://datatracker.ietf.org/doc/draft-gharris-opsawg-pcap-01

21. „The Zeek Network Security Monitor“, Zeek. Žiūrėta: 2026 m. balandžio 12 d. [Interaktyvus]. Adresas: https://zeek.org/

22. „JSON“. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://www.json.org/json-en.html

23. „Kas yra SIEM? | ‚Microsoft‘ sauga“. Žiūrėta: 2026 m. balandžio 17 d. [Interaktyvus]. Adresas: https://www.microsoft.com/lt-lt/security/business/security-101/what-is-siem

24. „NetworkMiner - The NSM and Network Forensics Analysis Tool ⛏“, Netresec. Žiūrėta: 2026 m. balandžio 12 d. [Interaktyvus]. Adresas: https://www.netresec.com/?page=NetworkMiner

25. Josue, „EmberOT | OT PCAP Analyzer: A Free Tool for the Community“, EmberOT. Žiūrėta: 2026 m. balandžio 12 d. [Interaktyvus]. Adresas: https://www.emberot.com/ot-pcap-analyzer/

26. P. Kumari ir A. K. Jain, „A comprehensive study of DDoS attacks over IoT network and their countermeasures“, *Computers & Security*, t. 127, p. 103096, bal. 2023, doi: 10.1016/j.cose.2023.103096.

27. R. Uddin, S. A. P. Kumar, ir V. Chamola, „Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions“, *Ad Hoc Networks*, t. 152, p. 103322, saus. 2024, doi: 10.1016/j.adhoc.2023.103322.

28. I. Sharafaldin, A. H. Lashkari, S. Hakak, ir A. A. Ghorbani, „Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy“, *2019 International Carnahan Conference on Security Technology (ICCST)*, CHENNAI, India: IEEE, spal. 2019, p. 1–8. doi: 10.1109/CCST.2019.8888419.

29. V. D. M. Rios, P. R. M. Inacio, D. Magoni, ir M. M. Freire, „Detection and Mitigation of Low-Rate Denial-of-Service Attacks: A Survey“, *IEEE Access*, t. 10, p. 76648–76668, 2022, doi: 10.1109/ACCESS.2022.3191430.

30. R. L ir P. Satyanarayana, „Detecting Flooding Attacks in Communication Protocol of Industrial Control Systems“, *IJACSA*, t. 11, nr. 1, 2020, doi: 10.14569/IJACSA.2020.0110149.

31. Dong Jin, D. M. Nicol, ir Guanhua Yan, „An event buffer flooding attack in DNP3 controlled SCADA systems“, *Proceedings of the 2011 Winter Simulation Conference (WSC)*, Phoenix, AZ, USA: IEEE, gruodž. 2011, p. 2614–2626. doi: 10.1109/WSC.2011.6147969.

32. R. S. Silva *ir kt.*, „Evaluating OPC UA Security: Insights from DoS Attack Scenarios“, *2025 IEEE Latin Conference on IoT (LCIoT)*, Fortaleza, Brazil: IEEE, bal. 2025, p. 356–359. doi: 10.1109/LCIoT64881.2025.11118519.

33. P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, ir E. Panaousis, „Attacking IEC-60870-5-104 SCADA Systems“, *2019 IEEE World Congress on Services (SERVICES)*, Milan, Italy: IEEE, liep. 2019, p. 41–46. doi: 10.1109/SERVICES.2019.00022.

34. S. Ashraf, M. H. Shawon, H. M. Khalid, ir S. M. Muyeen, „Denial-of-Service Attack on IEC 61850-Based Substation Automation System: A Crucial Cyber Threat towards Smart Substation Pathways“, *Sensors*, t. 21, nr. 19, p. 6415, rugs. 2021, doi: 10.3390/s21196415.

35. R. Vishwakarma ir A. K. Jain, „A survey of DDoS attacking techniques and defence mechanisms in the IoT network“, *Telecommun Syst*, t. 73, nr. 1, p. 3–25, saus. 2020, doi: 10.1007/s11235-019-00599-z.

36. PG Scholar, Department of Computer Science and Engineering, NITTTR, Chandigarh, India., S. Nautiyal, C. R. Krishna, Department of Computer Science and Engineering, NITTTR, Chandigarh,

India., S. Wadhwa, ir Department of Computer Applications, Post Graduate Govt. College, Chandigarh, India, „Mitigating Economic Denial of Sustainability (EDoS) in Cloud Environment using Genetic Algorithm and Artificial Neural Network“, *IJITEE*, t. 8, nr. 10, p. 3415–3421, rugpj. 2019, doi: 10.35940/ijitee.J9680.0881019.

37. „Comma-separated values“, *Wikipedia*. 2026 m. kovo 10 d. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://en.wikipedia.org/w/index.php?title=Comma-separated_values&oldid=1342795644

38. „What is an IP Address? How it works? How to Locate it?“, Fortinet. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://www.fortinet.com/resources/cyberglossary/what-is-ip-address

39. „MAC Addresses“, IEEE Standards Association. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://standards.ieee.org/products-programs/regauth/mac/

40. „Service Name and Transport Protocol Port Number Registry“. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

41. „Welcome to Python.org“, Python.org. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://www.python.org/

42. „Tshark | tshark.dev“. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://tshark.dev/

43. *mac-vendor-lookup: Find the vendor for a given MAC address*. Python. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://github.com/bauerj/mac_vendor_lookup

44. M. Odejobi, „Cybersecurity Architecture for Telemetry Networks: Development of a Comprehensive Cybersecurity Framework for Industrial Control Systems (ICS) and SCADA Networks“, *International Telemetering Conference Proceedings*, spal. 2025, Žiūrėta: 2026 m. kovo 29 d. [Interaktyvus]. Adresas: https://repository.arizona.edu/handle/10150/679578

45. G. K. Mondal, B. Neogi, D. Singh, S. Roy, ir R. Bose, „Challenges in Security and Mitigation Measures at Different Purdue Model in Industrial Control Systems“, *Smart Systems and Wireless Communication*, R. Chaki, A. Cortesi, S. DasGupta, ir S. Saha, Sud., Singapore: Springer Nature, 2025, p. 455–464. doi: 10.1007/978-981-96-1348-9_34.

46. „Real danger: DDoS attacks on VPNs and their consequences“, Link11. Žiūrėta: 2026 m. gegužės 2 d. [Interaktyvus]. Adresas: https://www.link11.com/en/blog/threat-landscape/when-the-secure-tunnel-breaks-ddos-attacks-on-vpns-and-their-consequences/

47. „TCP/UDP ports used by GE Products - White Listing - AutomaTech Technical Support - AutomaTech Confluence“. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://automatechinc.atlassian.net/wiki/spaces/SUPPORT/pages/1491107845/TCP+UDP+ports+used+by+GE+Products+-+White+Listing

48. „Ports used by System Platform products“. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://docs.aveva.com/bundle/system-platform/page/686254.html

49. „Gateway Port Reference | Ignition User Manual“. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://www.docs.inductiveautomation.com/docs/8.1/appendix/reference-pages/gateway-port-reference

50. „Default port numbers“. Žiūrėta: 2026 m. balandžio 7 d. [Interaktyvus]. Adresas: https://product-help.schneider-electric.com/EcoStruxure-Power-Operation-2024/content/11_other_content/itrequs/firewallports.htm?TocPath=Cybersecurity%7CConfigure%7C_____5

51. „DDoS 2019 | Datasets | Research | Canadian Institute for Cybersecurity | UNB“. Žiūrėta: 2026 m. gegužės 5 d. [Interaktyvus]. Adresas: https://www.unb.ca/cic/datasets/ddos-2019.html

52. S. Kumar ir S. Gupta, „SDN-TCP-SYN ATTACK-DDOS DATASET“, t. 2, saus. 2022, doi: 10.17632/236bd4cjmk.2.

53. „DDoS-AT-2022“. Žiūrėta: 2026 m. gegužės 5 d. [Interaktyvus]. Adresas: https://www.kaggle.com/datasets/meenakshimittal/ddos-at-2022

54. „DDoS General | Knowledge Base | MazeBolt“. Žiūrėta: 2026 m. gegužės 4 d. [Interaktyvus]. Adresas: https://kb.mazebolt.com/kbe_taxonomy/ddos-general/

55. ITI, „ICS-Security-Tools/pcaps/README.md at master · ITI/ICS-Security-Tools“, GitHub. Žiūrėta: 2026 m. gegužės 5 d. [Interaktyvus]. Adresas: https://github.com/ITI/ICS-Security-Tools/blob/master/pcaps/README.md

56. „hping3 | Kali Linux Tools“, Kali Linux. Žiūrėta: 2026 m. balandžio 9 d. [Interaktyvus]. Adresas: https://www.kali.org/tools/hping3/

57. „The ldapsearch Command-Line Tool“. Žiūrėta: 2026 m. balandžio 9 d. [Interaktyvus]. Adresas: https://docs.ldap.com/ldap-sdk/docs/tool-usages/ldapsearch.html

58. R. Gadzhovski, *Gadzhovski/HTTPH4mm3r*. (2026 m. sausio 4 d.). Python. Žiūrėta: 2026 m. balandžio 26 d. [Interaktyvus]. Adresas: https://github.com/Gadzhovski/HTTPH4mm3r

59. P. Kashyap, „Understanding Precision, Recall, and F1 Score Metrics“, Medium. Žiūrėta: 2026 m. gegužės 6 d. [Interaktyvus]. Adresas: https://medium.com/@piyushkashyap045/understanding-precision-recall-and-f1-score-metrics-ea219b908093

60. „Confusion Matrix Calculator“, Omni Calculator. Žiūrėta: 2026 m. gegužės 6 d. [Interaktyvus]. Adresas: https://www.omnicalculator.com/statistics/confusion-matrix

61. R. Sharma, „Analyzing a DDOS Attack Using Wireshark“, Medium. Žiūrėta: 2026 m. balandžio 26 d. [Interaktyvus]. Adresas: https://medium.com/@ronak.d.sharma111/analyzing-a-ddos-attack-using-wireshark-8535274cd00e

1 Priedas. Purdue lygmenų – prievadų duomenų bazės šablonas.


```
{
   "Level 5": {
         "TCP": {
            "80": "Web HTTP",
            "443": "Web HTTPS"
      },
         "UDP": {
            "500": "VPN IPsec VPN",
            "4500": "VPN IPsec VPN",
            "51820": "VPN WireGuard",
            "1194": "VPN OpenVPN"
      }
   },
   "Level 4": {
         "TCP": {
            "88": "Domain Kerberos",
            "389": "Domain LDAP",
            "636": "Domain LDAPS",

            "3306": "SQL MySQL",
            "1433": "SQL Default",
            "1521": "SQL Oracle",
            "5432": "SQL PostgreSQL"
      },
         "UDP": {
            "88": "Domain Kerberos",
            "389": "Domain LDAP"
      }
   },
   "Level 3.5": {
         "TCP": {
      },
         "UDP": {
      }
   },
   "Level 3": {
         "TCP": {
            "13000": "Historian GE iFIX",
            "14000": "Historian GE iFIX",
            "14001": "Historian GE iFIX",
            "14003": "Historian GE iFIX",

            "32565": "Historian System Platform AVEVA",
```

```
            "32568": "Historian System Platform AVEVA",
            "32569": "Historian System Platform AVEVA",
            "32563": "Historian System Platform AVEVA"
        },
            "UDP": {
        }
    },
    "Level 2": {
            "TCP": {
            "2010": "SCADA iFIX Node",
            "53014": "SCADA iFIX Sync / Failover",

            "8043": "SCADA Ignition Gateway SSL",
            "8060": "SCADA Ignition Gateway SSL",
            "8088": "SCADA Ignition Gateway No SSL",

            "808": "SCADA System Platform Multi-Galaxy",
            "5026": "SCADA System Platform NMXSVC",
            "8090": "SCADA System Platform aaGR",
            "30000": "SCADA System Platform Redundancy",
            "30001": "SCADA System Platform Redundancy",
            "32568": "SCADA System Platform aaEngine.exe",

            "2084": "SCADA Citect Reports",
            "2080": "SCADA Citect Alarms",
            "2085": "SCADA Citect Trends",
            "2082": "SCADA Citect I/O",
            "23104": "SCADA Citect Events"
        },
            "UDP": {

        }
    },
    "Level 1": {
            "TCP": {
            "102": "PLC IEC61850 / SIMATICS7",
            "502": "PLC ModbusTCP",
            "2404": "PLC IEC104",
            "20000": "PLC DNP3",
            "44818": "PLC EtherNet/IP"
        },
            "UDP": {
            "20000": "PLC DNP3"
        }
    },
}
```

2 Priedas. Ištrauktų požymių CSV formatu failo pavyzdys.

frame_time_epoch,frame_len,eth_dst,eth_type,ip_src,ip_dst,ip_proto,ip_flags_mf,ip_frag_offset,tcp_dstport,tcp_flags,tcp_len,udp_dstport,udp_length
1776268639.544997,1442,00:15:5d:0f:69:01,0x0800,240.125.173.63,10.10.11.101,17,False,0,-1,,-1,1,1408
1776268639.545011,1442,00:15:5d:0f:69:01,0x0800,240.125.173.63,10.10.11.101,17,False,0,-1,,-1,1,1408
1776268639.545042,1442,00:15:5d:0f:69:01,0x0800,240.125.173.63,10.10.11.101,17,False,0,-1,,-1,1,1408
1776268639.54571,1442,00:15:5d:0f:69:01,0x0800,37.23.130.38,10.10.11.101,17,False,0,-1,,-1,2,1408
1776268639.545717,1442,00:15:5d:0f:69:01,0x0800,37.23.130.38,10.10.11.101,17,False,0,-1,,-1,2,1408
1776268639.545733,1442,00:15:5d:0f:69:01,0x0800,37.23.130.38,10.10.11.101,17,False,0,-1,,-1,2,1408
1776268639.546375,1442,00:15:5d:0f:69:01,0x0800,92.244.89.232,10.10.11.101,17,False,0,-1,,-1,3,1408
1776268639.546381,1442,00:15:5d:0f:69:01,0x0800,92.244.89.232,10.10.11.101,17,False,0,-1,,-1,3,1408
1776268639.546394,1442,00:15:5d:0f:69:01,0x0800,92.244.89.232,10.10.11.101,17,False,0,-1,,-1,3,1408
1776268639.547033,1442,00:15:5d:0f:69:01,0x0800,246.40.41.31,10.10.11.101,17,False,0,-1,,-1,4,1408
1776268639.547038,1442,00:15:5d:0f:69:01,0x0800,246.40.41.31,10.10.11.101,17,False,0,-1,,-1,4,1408
1776268639.547056,1442,00:15:5d:0f:69:01,0x0800,246.40.41.31,10.10.11.101,17,False,0,-1,,-1,4,1408
1776268639.547697,1442,00:15:5d:0f:69:01,0x0800,222.47.207.140,10.10.11.101,17,False,0,-1,,-1,5,1408
1776268639.547702,1442,00:15:5d:0f:69:01,0x0800,222.47.207.140,10.10.11.101,17,False,0,-1,,-1,5,1408
1776268639.547715,1442,00:15:5d:0f:69:01,0x0800,222.47.207.140,10.10.11.101,17,False,0,-1,,-1,5,1408
1776268639.548875,1442,00:15:5d:0f:69:01,0x0800,199.124.198.45,10.10.11.101,17,False,0,-1,,-1,6,1408
1776268639.548884,1442,00:15:5d:0f:69:01,0x0800,199.124.198.45,10.10.11.101,17,False,0,-1,,-1,6,1408
1776268639.548907,1442,00:15:5d:0f:69:01,0x0800,199.124.198.45,10.10.11.101,17,False,0,-1,,-1,6,1408
1776268639.550694,1442,00:15:5d:0f:69:01,0x0800,13.91.92.143,10.10.11.101,17,False,0,-1,,-1,7,1408

3 Priedas. Pavyzdinis atakos paviršiaus analizės metu sudarytas JSON formato failas.


```
"10.10.14.104": {
    "COMMON_INFO": {
      "FIRST_PACKET": "2026-04-15 16:05:20.608956+00:00",
      "LAST_PACKET": "2026-04-15 16:06:20.396751+00:00",
      "DURATION_IN_SECONDS": 59.79,
      "DURATION_IN_MINUTES": 1.0,
      "DURATION_IN_HOURS": 0.02,
      "TOTAL_RECEIVED_BYTES": 350994428,
      "TOTAL_RECEIVED_MEGABYTES": 350.99,
      "ATTACK_FLOW_BITS_PER_SECOND": 46963629.77,
      "ATTACK_FLOW_MEGABITS_PER_SECOND": 46.96
    },
    "OSI2": {
      "MAC_ADDRESS": "00:15:5d:0f:69:04",
      "TRANSLATED_MAC": "Microsoft Corporation",
      "ETH_FRAMES_COUNT": 283060
    },
    "OSI3": {
      "IS_FRAGMENTS": false,
      "IP_PACKETS_COUNT": 283060
    },
    "OSI4": {
      "TCP": {
        "ATTACKED_TCP_PORTS": [
          389
        ],
        "TCP_SEGMENTS_COUNT": {
          "389": 41887
        }
      },
      "UDP": {
        "ATTACKED_UDP_PORTS": [
          -1
        ],
        "UDP_DATAGRAMS_COUNT": {
          "-1": 241173
        }
      }
    },
    "OSI6": {},
    "OSI7": {
      "ATTACKED_HIGHER_LAYER_TCP_PROTOCOLS": {
        "389": [
          "ldap",
```

```
            "Lightweight Directory Access Protocol"
          ]
        },
        "TCP_SEGMENTS_WITH_DATA_COUNT": {
          "389": 17688
        },
        "ATTACKED_HIGHER_LAYER_UDP_PROTOCOLS": {},
        "UDP_DATAGRAMS_WITH_DATA_COUNT": {}
      }
    },
    "10.10.15.105": {
      "COMMON_INFO": {
        "FIRST_PACKET": "2026-04-15 16:05:30.885921+00:00",
        "LAST_PACKET": "2026-04-15 16:05:56.362014+00:00",
        "DURATION_IN_SECONDS": 25.48,
        "DURATION_IN_MINUTES": 0.42,
        "DURATION_IN_HOURS": 0.01,
        "TOTAL_RECEIVED_BYTES": 1333413,
        "TOTAL_RECEIVED_MEGABYTES": 1.33,
        "ATTACK_FLOW_BITS_PER_SECOND": 418654.0,
        "ATTACK_FLOW_MEGABITS_PER_SECOND": 0.42
      },
      "OSI2": {
        "MAC_ADDRESS": "e8:cf:83:9d:97:3f",
        "TRANSLATED_MAC": "Dell Inc.",
        "ETH_FRAMES_COUNT": 5796
      },
      "OSI3": {
        "IS_FRAGMENTS": false,
        "IP_PACKETS_COUNT": 5796
      },
      "OSI4": {
        "TCP": {
          "ATTACKED_TCP_PORTS": [
            80
          ],
          "TCP_SEGMENTS_COUNT": {
            "80": 5796
          }
        },
        "UDP": {
          "ATTACKED_UDP_PORTS": [],
          "UDP_DATAGRAMS_COUNT": {}
        }
      },
      "OSI6": {},
```

```
      "OSI7": {
        "ATTACKED_HIGHER_LAYER_TCP_PROTOCOLS": {
          "80": [
            "http",
            "World Wide Web HTTP"
          ]
        },
        "TCP_SEGMENTS_WITH_DATA_COUNT": {
          "80": 2802
        },
        "ATTACKED_HIGHER_LAYER_UDP_PROTOCOLS": {},
        "UDP_DATAGRAMS_WITH_DATA_COUNT": {}
      }
    }
}
```

4 Priedas. Pavyzdinis atakos paviršiaus išskaidytos pagal Purdue lygmenis analizės metu sudarytas JSON formato failas.


```
"Level 5": {
      "10.10.15.105": {
         "Attacked port": 80,
         "Attacked MAC": "Dell Inc.",
         "Attacked service": "Web HTTP"
      }
   },
   "Level 4": {
      "10.10.14.104": {
         "Attacked port": 389,
         "Attacked MAC": "Microsoft Corporation",
         "Attacked service": "Domain LDAP"
      }
   },
   "Level 3.5": {},
   "Level 3": {},
   "Level 2": {},
   "Level 1": {}
}
```

5 Priedas. Python scenarijai naudojami ModbusTCP ir IEC104 protokolų perpildymams.

ModbusTCP protokolo perpildymui:

```
import time
import threading
from pyModbusTCP.client import ModbusClient

c = ModbusClient(host='10.10.10.101', port=502, auto_open=True)
while True:
    coils_l = c.read_holding_registers(0, 99)
    if coils_l:
        print('coil ad #0 to 99: %s' % coils_l)
    else:
        print('unable to read coils')

    time.sleep(0.01)
```

IEC104 protokolo perpildymui:

```
import c104
import time

client = c104.Client()

connection = client.add_connection(ip="10.10.10.100", port=2404)
station = connection.add_station(common_address=1)

cmd = station.add_point(io_address=50, type=c104.Type.C_SC_NA_1)

client.start()

while True:
    cmd.transmit(cause=c104.Cot.SPONTANEOUS)
    time.sleep(0.01)
    cmd.transmit(cause=c104.Cot.SPONTANEOUS)
    time.sleep(0.01)
```