Vilniaus universitetas
Duomenų mokslo ir skaitmeninių technologijų institutas
L I E T U V A

INFORMATIKA (N009)

METODŲ, SKIRTŲ KIBERNETINĖS SAUGOS INCIDENTAMS TINKLO DUOMENYSE NUSTATYTI, ANALIZĖ

Viktoras Bulavas

2019 m. spalis

Mokslinė ataskaita DMSTI-DS-N009-19-11

VU Duomenų mokslo ir skaitmeninių technologijų institutas, Akademijos g. 4,
Vilnius LT-08412
www.mii.lt

Santrauka

Šiame studijų etape atliktų teorinių ir empirinių tyrimų tikslas – įgyti žinių ir praktinės patirties vertinant ankstyvojo kibernetinių atakų atpažinimo metodus ir atakų požymius.

Ši ataskaita sudaryta iš šių dalių: ankstyvojo kibernetinių atakų aptikimo problematikos aptarimo (1), panaudotų duomenų šaltinių pristatymo (2), kibernetinio įsibrovimo incidentų aptikimo metodų aptarimo (3), tinklo duomenų atributų svarbos analizės (4) ir rezultatų bei išvadų (5).

Pirmiausia tyrimo metu realizuotas duomenų nuskaitymas iš specializuoto kibernetinio tinklo duomenų formato (PCAP) į Python duomenų masyvus (Numpy). Pasirinktas vienas naujausių atviros prieigos kibernetinės saugos duomenų rinkinys CSE-CIC-IDS2018 (Sharafaldin, Lashkari and Ghorbani, 2018), kuriame yra dokumentuoti skirtingi kibernetinio įsibrovimo incidentai. Antrame tyrimo etape tinklo duomenų tyrimo tikslais įgyvendinti S. Kim, A. Reddy, ir M. Vannucci (Kim, Reddy and Vannucci, 2004) apžvalginiame straipsnyje ir S.Kim (Kim, 2005) disertacijoje MIT aprašyti DOS atakų atpažinimo algoritmai. Šie algoritmai išbandyti su tinklo įrašais, autoriaus surinktais Vilniaus universiteto kompiuterių tinkle ir, mokslinių tyrimų palyginamumui, su minėtu viešai skelbiamu duomenų rinkiniu.

Greta klasikinių statistinių metodų kibernetinės atakos atpažinimui buvo išbandytas T. Higuchi fraktalinės dimensijos skaičiavimo Boxcount metodas (Higuchi, 1988). Šio metodo taikymą tinklo srauto vertinimui pirmieji aprašė Xia, Lu ir Li (Xia, Lu and Li, 2012). Šiame darbe remiantis tinklo srauto fraktalinės dimensijos kaitos laike skaičiavimais buvo gauti gerai faktinius duomenis atitinkantys rezultatai.

Shapo verčių metodu (Lundberg and Lee, 2017) buvo atliekamas pasirinktais mašinų mokymo metodais (SVM, Random Forest, KNN) paskaičiuotų duomenų požymių svarbos nustatymas, parodęs, kad nėra vienareikšmiai dominuojančių dimensijų, o ženklus dimensijų sumažinimas sumažina prognozių kokybę, kas buvo patvirtinta ir ankstesniais autoriaus pirminių komponenčių dimensijų redukavimo tyrimais (Bulavas, 2018). Shapo verčių metodu gauti duomenų požymių svarbos įverčiai palyginti su Random Forest metodu gautais požymių svarbos įverčiais.

Reikšminiai žodžiai: kibernetinė sauga; incidentų atpažinimo metodai; Higuchi Box-Count metodas; Shapo verčių metodas.

Turinys

1 Ankstyvojo kibernetinio įsibrovimo aptikimo uždaviniai

1.1 Uždavinio aktualumo aptarimas

Ankstyvas įsibrovimo į tinklą, informacines sistemas ar darbo vietas atpažinimas, bei susijęs kenksmingos programinės įrangos operacijų ar nesankcionuotos individų veiklos aptikimas yra aktualūs kibernetinio saugumo srities uždaviniai. Kibernetinių atakų tyrimai reikalauja vis daugiau specialistų ir jų laiko visą parą, nes dėl kompiuterinio raštingumo augimo ir didėjančio kompiuterinės technikos prieinamumo auga pasaulinis kibernetinio nusikalstamumo lygis.

Gynyba kibernetinio saugumo specialistams užima vis daugiau laiko. Reaguodamos į problemą NATO valstybės įteisino kibernetinio saugumo pajėgas kaip reguliarios kariuomenės rūšį (Lewis, 2015), nes patys piliečiai, dėl specializuotų žinių, reikalingos brangios programinės įrangos ir laiko stokos, patys nebeapsigina. Tai patvirtina labai reikalingą mokslinių tyrimų sritį, kurios tikslas - padidinti grėsmės aptikimo tikslumą (sumažinti klaidingo aptikimo procentą) ir tinklo gynybos įrenginių (įsiskverbimo aptikimo sistemų IDS) mokymosi greitį. Šie uždaviniai sprendžiami optimizuojant duomenų nuskaitymo ir tvarkymo algoritmus, ieškant greitesnio kibernetinio įsilaužimo faktinių prielaidų patvirtinimo.

1.2 Kibernetinių atakų aptikimo metodų aptarimas

Literatūroje išskirti ir dažniausiai nagrinėjami trys pagrindiniai kibernetinių atakų aptikimo metodai: a) žinomų taisyklių (angl. rule, signature based) netinkamos veiklos aptikimo metodas, b) anomalios elgsenos (nuokrypio nuo įprastinės veiklos tinkle ir panaudojant informacines sistemas) aptikimo metodas, ir c) hibridinis metodas, kuriame taikomi abiejų metodų elementai.

Šiame darbe bus aptariami žinomų taisyklių ir anomalios elgsenos aptikimo mašininio mokymosi pagalba metodų algoritmai bei jų sudėtingumas.

1.3 Žinomų taisyklių mašinos

Netinkamos veiklos aptikimo sistemos naudoja parašus (taisyklių rinkinius), kurie apibūdina jau žinomus išpuolius. Pagrindinis taisyklių mašinų trūkumas yra tai, kad toks įvykis turi būti jau ištirtas, tokioms sistemoms reikia reguliariai atnaujinti taisykles, be to nedidelis

nuokrypis nuo taisyklės lemia kibernetinio užpuoliko nepastebimumą ir nebaudžiamumą. Aptikimo taisyklių atnaujinimas dažniausiai įgyjamas iš tiekėjo, užtikrinančio nuolatinį didelio skaičiaus kvalifikuotų ir brangių specialistų darbą. Informacija teikiama panaudojant debesų kompiuterijos sprendimus, kurie savaime yra didžiausi DOS atakų taikiniai, dėl ko trikdant kanalus sudaromos prielaidos plisti naujoms atakoms. Net augant kibernetinės saugos tiekėjų pasiūlai, dažnai užsakovas turi vieną pasirinktą sprendimą, o tiekėjai nespėja atnaujinti taisyklių, nes tarpusavyje nenoriai dalinasi atakoms atremti būtinų taisyklių rinkiniais. Ne visi gali įsigyti komercinius produktus, todėl naudojamos ir atviros kibernetinių įsilaužimų bazės, tačiau jos dar rečiau ir lėčiau atnaujinamos. Atviros taisyklių bazės atsilieka nuo komercinių produktų ir yra panaudojamos reaktyviai. Tik sąlyginis subjekto nepatrauklumas pirmam puolikui gelbėja, nes kol bazė neatnaujinta, pirmieji puolikai gali pasirinkti bet kurią auką, bet renkasi tą, kurios informacija brangesnė, nes puolikų laikas irgi ribotas. Jomis negali pasitikėti subjektai, valdantys brangią intelektinę nuosavybę, asmens duomenis ar paslaptis, todėl tai nėra perspektyvi kryptis gynyboje. Atsiradus besimokančioms gynybos sistemoms, atsirado ir besimokančios puolimo sistemos (Brundage *et al.*, 2018), dėl ko žinomų taisyklių mašinos gelbėja tik nuo pradedančių įsilaužėlių, o ne nuo profesionalų, panaudojančių besimokančias puolimo mašinas.

1.4 Anomalijų aptikimo mašinos

Šiai kategorijai priskirtini įvairūs statistiniai kibernetinių incidentų aptikimo metodai. Kita vertus, anomalijų aptikimo sistemos kuriamos aptikti nuokrypį nuo įprastinės elgsenos, tuo būdu statistiniai metodai leidžia lyginti gaunamus duomenis su patvirtintu įprastiniu objektų elgesiu. Tačiau tam svarbu nuolat kaupti ir nuolat apdoroti didelius kiekius duomenų, nuolat bendrauti su naudotojais ir stebėti informacinių sistemų stebėjimo įrašus (angl. system log). Anomalijų aptikimo metodą pasiūlė Andersonas (Anderson, 1980) o kibernetinių problemų sprendimui pirmieji pritaikė Denning (Denning, 1986). Pagrindinis anomalijų aptikimo algoritmų privalumas yra tas, kad šie algoritmai geba nustatyti naujas atakų formas, nes šie išpuoliai dažniausiai nukrypsta nuo žinomo (leistino, įprastinio) organizacijos sistemų ir naudotojų elgesio (Denning, 1986). Tačiau ir mašinų mokymu pagrįstas anomalijos nustatymas, kaip ir taisyklių mašinų atveju, reikalauja priežiūros ir nuolatinio specialistų stebėjimo, nes šiuo metu vis dar yra didelis klaidingas teigiamas ankstesnių, bet normalaus sistemos elgesio nustatymo rodiklis.

1.5 Hibridiniai metodai

Hibridiniai metodai yra neišvengiamas abiejų anksčiau apibūdintų metodų derinys. Tik sujungiant metodų privalumus įmanomas operatyvus ir efektyvus veiklai keliamų uždavinių, tokių kaip teisiniai reikalavimai (Elektroninių ryšių, Informacinių išteklių, Kibernetinio saugumo, Asmens duomenų teisinės apsaugos įstatymai ir poįstatyminiai aktai) išsaugoti kibernetinių nusikaltimų įkalčius (duomenis, kurie patvirtina kenksmingą veiklą), kai reikia įgyvendinti ilgalaikį didelių duomenų kiekio išrankos saugojimą, ir greitasis reagavimas bei bendradarbiavimas su gynybos ir vidaus reikalų sistemos organizacijomis, tiriančiomis ir užkardančiomis kompiuterių tinklo ir sistemų darbą trikdančią veiklą, sprendimas. Tokiam bendradarbiavimui reikalingos faktinių išpuolių tinklo ir sisteminių ryšių išrankos, kada svarbu iš didžiulio srauto įprastinių duomenų atpažinti ir sukaupti kenkėjiškos veiklos įrodymus.

1.6 Kibernetinių atakų klasės

Informacijos saugos analitikų renkami tinklo srauto duomenys skirstomi į keletą bendrų tipų. S. Hettich ir S. D. Bay (Hettich and Bay, 1999) DARPA[1] šaltinio (Laboratory, 1998) analizėje apibrėžė šias atakų klases:

- Paslaugų trikdymas (DoS), - bandymai sutrikdyti tikslinių naudotojų informacinius ar tinklo išteklius,

- teisių užvaldymas (U2R), - suteikiantis užpuolikui prieigą prie informacinių išteklių privilegijuotomis teisėmis,

- Nuotolinė prieiga (R2L), suteikianti užpuolikui prieigą į vietinį tinklą,

- skanavimas (Probing, Scan), - suteikiantis užpuolikui nuotoliniu būdu informaciją apie informacinių sistemų ir tinklo išteklių konfigūraciją.

1.7 Kibernetinių įvykių duomenų atributai

Kibernetinių įvykių duomenų šaltinių atributai gali būti suskirstyti į keturias skirtingų požymių klases, kaip pasiūlyta (Bouzida and Cuppens, 2004) ir aprašyta toliau:

1) baziniai požymiai: atributai, kurie gali būti išgauti iš TCP / IP ryšio (įėjimo sąsaja, šaltinio IP adresas, paskirties IP adresas, IP protokolas, šaltinio prievadas, paskirties prievadas ir IP paslaugos tipas).

[1] Sutrumpinimas nuo angl. Defense Advanced Research Projects Agency

2) prieglobos požymiai: stebimi srautai į tą patį paskirties serverį, ir kas nustatytas intervalas (NSL - KDD - 2 sekundės) apskaičiuojama statistika, susijusi su tuo pačiu fiziniu ištekliu (sąsaja, MAC adresas), naudojamu protokolu ar prievadu ir pan.

Pirmasis ir antrasis požymių tipai yra chronologiniai, jiems būdingas reguliarumas.

3) Paslaugos požymiai: nustatytu intervalu (NSL - KDD – 2 sekundės) stebimi srautai, kurie naudoja tą pačią paslaugą, kaip ir pasirinktasis srautas, ir apskaičiuojama statistika.

Atkreiptinas dėmesys, kad 2 sekundžių laikotarpis nebeatspindi esamos situacijos, nes išpopuliarėjo lėtai skanuojančios atakos, kurios nuskaito įrenginius naudodamos pavyzdžiui botneto valdymo centro nustatytą laiko intervalą (pavyzdžiui kas 2 ar neretai ir daugiau nei 5 minutės).

4) Turinio požymiai: skirtingai nei dauguma „DoS“ ir „Probing“ atakų, R2L ir U2R atakos neturi reguliarumo. R2L ir U2R atakos yra įtrauktos į paketų duomenų dalis ir paprastai yra tik vienas ryšio seansas. Norint aptikti tokius išpuolius, IDS duomenų dalyje turi turėti požymių, kuriuos būtų galima atpažinti kaip anomaliją, pvz., nepavykusių prisijungimo bandymų skaičius.

NSL-KDD duomenų rinkinio problema yra ribotas atakų tipų skaičius. Naujesni, bet dar mažai panaudoti ir aprašyti duomenų rinkiniai, pavyzdžiui CIC IDS 2017 (Sharafaldin, Lashkari and Ghorbani, 2018) įveda papildomų rūšių atakų, pvz., „DDoS“, „Brute Force XSS“, „SQL Inject“, infiltracijos ir „Botnet“. Duomenų rinkinys yra paženklintas (įrašai priskirti atakoms), surinkti ar apskaičiuoti 79 atributai.

Pastebėtina tendencija, kad duomenų rinkiniuose kaupiama vis daugiau atributų, nes siekiama surasti tuos, kurie padėtų mažinant klaidingo atpažinimo procentą (FAR).

Pagrindiniai atakų tipai, įvykę kibernetinėje erdvėje, mokslininkų ir praktikų jau išbandyti su įvairių tipų mašinų mokymosi algoritmų ansambliais, siekiant sumažinti klaidą, kuri svyruoja nuo 0,5 iki 5%, priklausomai nuo naudojamo metodo ir atakos tipo. Tuo tarpu naujos grėsmės vis dažniau naudoja daugiasluoksnius atakų vektorius, o žvalgyba vykdoma įvairiu nenuspėjamu metu ištisą parą be savaitgalių, todėl reikia naujų elgsenos nustatymo priemonių. Pažeidimo metu anomalija nepastebima ir dažnai aptinkama jau po įvykio arba visai neaptinkama. Naujos grėsmės nėra pažymėtos, kol neištirtas incidentas, todėl nusikaltėliams sukuriant naujus atakų būdus, etiketės dar nebūna prieinamos mašinų mokymui.

2 Tyrime naudotų duomenų formatai ir šaltiniai

2.1 Kibernetinių įvykių duomenų formatai

Tinklo srautų formatas nuolat keičiasi. Nors dominuoja tinklo įrangos gamintojų rinkos lyderių formatai, su naujais įrangos modeliais ir iššūkiais, tokiais, kaip duomenų šifravimas, kyla poreikis generuoti naujus, susijusius su naujais kibernetiniais pavojais ir technologijomis požymius. Tokių požymių duomenys, deja, dar nepatenka į moksliniams tyrimams skirtus rinkinius. Tiekėjai teikia panašią, bet nevienodą tinklo srautų stebėjimo technologiją, nes technologijos yra patentų objektas. Todėl mokymas turi būti pritaikytas konkretiems srautų įrašų tipui. Mokslinėse duomenų bazėse kalbama apie Netflow, kam pritaikyti dabartiniai atviro kodo sprendimai, tačiau jau plinta naujesnis tinklo srauto formatas IPFIX. Todėl įsibrovimo aptikimo sistemos turės būti pritaikytos arba pakeistos.

Šiame darbe naudojami 3 rūšių tinklo duomenų formatai:

a) PCAP - pilnos srauto įrenginių nuskaitymo būdu sukauptos tinklo veiklos srauto kopijos išranka, lentelės 1 ir 2;
b) NetFlows – agreguoti tinklo veiklos paketai (išranka stebėtų incidentų laikotarpiu);
c) CIC-FlowMeter – agreguoti, sodrinti ir žymėti tinklo veiklos įrašai – lentelė 3.

PCAP duomenys panaudoti iš CIC-IDS-2018 duomenų bazės ir autoriaus atliktų Vilniaus universiteto tinklo stebėjimų, NetFlows duomenys autoriaus generuoti iš CIC- FlowMeter CIC-IDS-2018 duomenų bazės.

Susidurta su viešai skelbiamų šio formato duomenų įkėlimo į duomenų masyvus paprogramių paviršutiniškumu, lemiančiu nepagrįstai ilgą duomenų įkėlimo į tinkamas analizei lenteles trukmę. Duomenų nuskaitymas ir perkėlimas į lentelių pavidalą buvo pagrindinis trukdis tolimesniam atakų atpažinimui ir klasifikavimui realiame laike. Pavyko rasti nesusijusių su algoritmų optimizavimu, bet ženkliai greitesnių, nei kitų autorių publikacijose viešai skelbiamų naudotos kalbos mechanizmų, leidžiančių geriau išnaudoti turimus kompiuterinius resursus, nuskaitant DOS atakų aptikimui pakankamus duomenis iš Vilniaus universiteto tinklo ir atviros prieigos kibernetinės saugos duomenų bazės CSE-CIC-IDS2018. Siekiant greitesnio nuskaitymo, lambda funkcijomis realizuoti ciklai ir sąlygų tikrinimai skaitymo metu, duomenų skaitymas perkeltas į kompiliuotą kodą vykdančias funkcijas, sumažintas kompiuterinės atminties, reikalingos analizei, panaudojimas.

2.2 Duomenų šaltiniai

Mokslo bendruomenė, tyrimų atkartojimo tikslais, naudoja apjungtus su sisteminiais ir nuasmenintus tinklo įvykių įrašų duomenų rinkinius. Paminėtini Linkolno universiteto surinkti DARPA 1998 (Laboratory, 1998) ir vėlesnių metų rinkiniai, KDD'99 (KDD, 1999), Kalifornijos universiteto, interneto srauto archyvas CAIDA (The Cooperative Association for Internet Data Analysis, 2010), taip pat Lawrence Berkeley National Laboratory, JAV archyvas LBNL (Lawrence Berkeley National Laboratory, 2010), „Shmoo Group“, JAV Defcon archyvas (The Shmoo Group, 2011), „Brunswick“ universiteto, Kanadoje archyvai ISCX IDS 2012 ir CIC IDS 2017, CSE-CIC-IDS2018 (Sharafaldin, Lashkari and Ghorbani, 2018), ir kiti.

Viena iš pirmųjų mokslinių tyrimų reikmėms panaudotų kibernetinių įvykių duomenų rinkinių yra įsilaužimo aptikimo duomenų rinkinys „KDD'99“, sukurtas 1999 m. KDD taurės konkursui. Jis buvo atnaujintas ir dabar pateikiamas atsisiųsti Brunswicko universitete, Kanadoje pavadinimu NSL – KDD. Šį rinkinį sudaro 41 matmuo (Bouzida and Cuppens, 2004).

Be išorinių šaltinių, atliekant šį tyrimą autorius rinko tinklo srautų įrašus Vilniaus universiteto tinkle. Šie pilno turinio duomenys transformuoti į formatą, leidžiantį juos toliau atvaizduoti N.Reddy et al. (MIT) disertacijoje aprašytais metodais.

Šiame darbe naudotas atviros prieigos kibernetinės saugos tinklo duomenų šaltinis CIC IDS 2018, kuriame sukaupti 80 tinklo parametrų. Rinkinyje pateikiami PCAP formato duomenys (lentelė 1 ir 2).

Lentelė 1: Duomenų išrankų rinkmenos

Name	Date modified	Type	Size
All 2018-02-23 between 14 and 17 UTC 172.31.69.20.pcap	2019-05-06 13:18	Wireshark capture...	66 679 KB
All 2018-02-23 between 14 and 17 UTC 172.31.69.21.pcap	2019-05-06 13:19	Wireshark capture...	310 KB
All 2018-02-23 between 14 and 17 UTC 172.31.69.22.pcap	2019-05-06 09:53	Wireshark capture...	497 KB
All 2018-02-23 between 14 and 17 UTC 172.31.69.23.pcap	2019-05-06 13:21	Wireshark capture...	52 545 KB
All 2018-02-23 between 14 and 17 UTC 172.31.69.24.pcap	2019-05-06 13:32	Wireshark capture...	63 900 KB
All 2018-02-23 between 14 and 17 UTC 172.31.69.25.pcap	2019-05-06 09:52	Wireshark capture...	350 KB
All 2018-02-23 between 14 and 17 UTC 172.31.69.26.pcap	2019-05-06 13:23	Wireshark capture...	26 427 KB
All 2018-02-23 between 14 and 17 UTC 172.31.69.28.pcap	2019-05-06 09:58	Wireshark capture...	10 956 KB
All 2018-02-23 between 14 and 17 UTC 172.31.69.29.pcap	2019-05-06 13:28	Wireshark capture...	56 472 KB
All 2018-02-23 between 14 and 17 UTC 172.31.69.30.pcap	2019-05-06 13:29	Wireshark capture...	60 343 KB

Lentelė 2: Pradiniai srauto (PCAP) duomenys

Ei. Nr.	IP	Dydis, KB	Išranka, KB	Pastabos
0	172.31.69.20	91’188	66’679	Normalus srautas
1	172.31.69.21	318	310	Normalus srautas
2	172.31.69.22	2’327	497	Normalus srautas
3	172.31.69.23	92’204	52’545	Normalus srautas

4	172.31.69.24	84’267	63’900	Normalus srautas
5	172.31.69.25	2’380	350	Normalus srautas, nepakanka duomenų
6	172.31.69.26	46’350	26’427	Normalus srautas
7	172.31.69.28	13’714	10’956	Normalus ir anomalus srautas, atrinktas tyrimo objektas su įsilaužimu
8	172.31.69.29	82’331	56’472	Normalus ir anomalus srautas, atrinktas tyrimo objektas su įsilaužimu
9	172.31.69.30	86’750	60’343	Normalus srautas

Tinklo srautų agregatų (NetFlow, CIC-FlowMeter) formatai yra išvestiniai, nuasmeninti, todėl dalis informacijos prarandama. Tačiau siekiant geriau suprasti duomenis, šiuose duomenų formatuose srautams pateikiama daug statistinių metrikų (Count, Min, Max, Mean, Std, Len). Tyrime panaudoti lentelėje 3 pateikti duomenys.

Lentelė 3: išvestiniai duomenys

Ei. Nr.	Duomenų šaltinis	Dydis, KB	Išranka, KB	Pastabos
1	CIC-IDS-2018 duomenų bazės IP 172.31.69.28 nuasmenintų duomenų rinkinys „Friday-23-02-2018_TrafficForML_CICFlowMeter.csv“	374’892	693	Tyrime naudota duomenų išranka – 1/1000 normalaus srauto, ir visas anomalus srautas

3 Kibernetininio įsibrovimo incidentų aptikimo metodų aptarimas

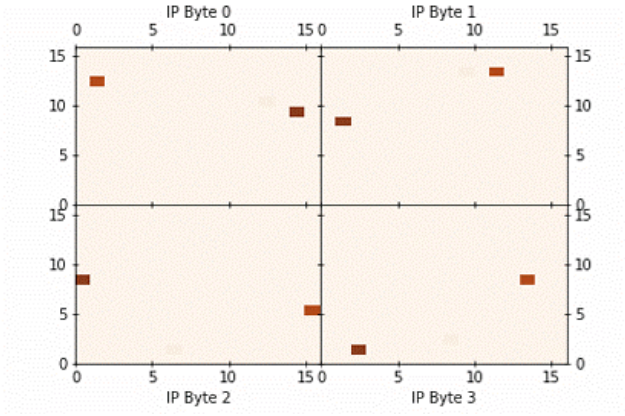
3.1 DOS ir DDOS atakų atpažinimas Kim metodu

Šiame skyriuje nagrinėjami statistiniai galimo įsibrovimo nustatymo algoritmai, padedantys atpažinti DOS (angl. Denial of service), DDOS (angl. distributed DOS), Brute Force ir SQL Injection atakas, aprašyti S.Kim (Kim, 2005) daktaro disertacijoje MIT, papildant naudotų algoritmų sudėtingumo analize.

DOS ir DDOS ataka atpažįstama iš bazinių požymių: IP adresų porų kiekio, srautų skaičiaus bei srautų pokyčio (dinamikos). Siekiant nustatyti galimą ataką, per nustatytą laiko vienetą (pavyzdžiui 30 sekundžių, 1, 2 ar 5 minutes) skaičiuojami sugeneruoti iš tam tikro šaltinio (nusakomo IP adresu) paketai į tikslo adresą. Sekančio periodo reikšmių masyvas lyginamas su ankstesniu. Nustačius reikšmingą (>3σ) nuokrypį nuo ankstesnės reikšmės, žinant įprastinių įeinančių srautų šaltinius (pavyzdžiui atmetus įrašus iš patikimų potinklių, ir įrašus, generuojamus atsakant į saugomo kompiuterio operacijas) galima išrinkti anomalius srautus ir daryti išvadą apie galimą kibernetinę ataką. Rašymo į lentelę metu, nuskaityto IP adreso lauko reikšmė lyginama su vidinio IP potinklio reikšme, tuomet tinkami įrašai įrašomi, o netinkami – praleidžiami. Perrinkus bloką, suskaičiuojama bloko įrašų, inicijuotų iš išorinių IP adresų, dažnių lentelė. Atliekama operacija yra panaši į rūšiavimą, atliekamą sumuojant skaitliukus, kurio sudėtingumo viršutinis asimptotinis vertinimas Θ(n log n). Tuomet labiau, nei leidžiamą skaičių nuo stebimų įrašų dažnių vidurkio nukrypusios reikšmės grafike matomos kaip anomalija (didelės stebimos reikšmės). Įvertinus nuokrypį gali būti priimamas automatinis sprendimas blokuoti tokį srautą ugniasienėje. Jei ženkliai nukrypusių nuo vidurkio įrašų nėra, taisyklė netaikoma. Nuskaitymas sudėtingėja, kai siekiama iš įrašo išrinkti tam tikrą požymį atitinkančius duomenis.

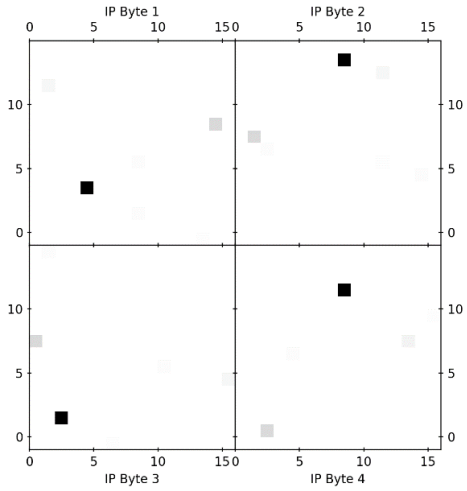
Duomenys iš 2019 m vasario 18 d. surinkto PCAP failo tiesiai iš tinklo įrenginio (Vilniaus universiteto tinklo srauto atveju) nuskaityti Python pritaikyta atviro kodo biblioteka Scapy. Šie duomenys transformuoti į Numpy masyvus ir sugrupuoti į 30s paketus. Paskaičiuotas srautų iš šaltinio į tikslą kiekis kiekvienai grupei, kurių skirstiniai atvaizduojami vizualizacija, realizuota Python Matplotlib priemonėmis. Principiniai vizualizavimo ir DOS atakų atpažinimo statistiniais metodais algoritmai pasiūlyti Kim, A. Reddy, ir M. Vannucci (Kim, Reddy and Vannucci, 2004) apžvalginiame straipsnyje bei S.Kim (Kim, 2005) disertacijoje (MIT), autoriaus pagal algoritmų aprašymus realizuoti Python aplinkoje.

Autoriaus sukurta srauto animacija pav. 1, kurios vaizdo kaita išryškina srauto pokyčius laike. Animacijoje atvaizduojamas 30 kartų pagreitintas realaus srauto duomenų kitimas.

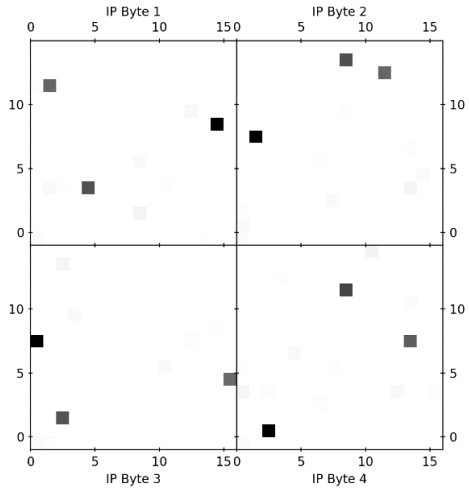


pav. 1 Srauto duomenų animacija

DOS ataka atpažįstama kaip ryškūs nauji taškai Pav. 2 b.

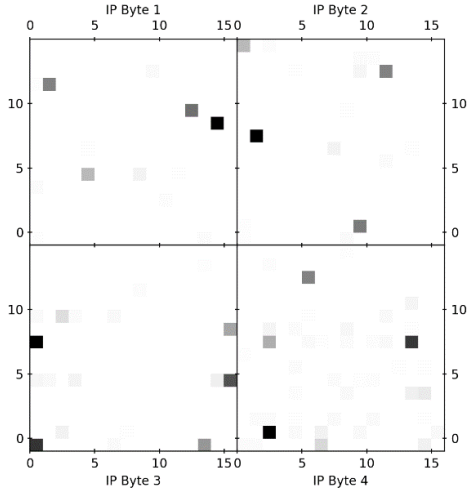


Pav. 2 a. Prieš DOS ataką

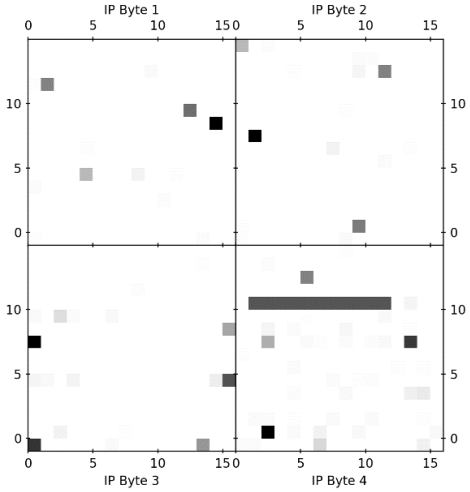


Pav. 2 b. Per DOS ataką

DDOS (angl. distributed DOS) ataka atpažįstama kaip nebūdinga įprastiniam tinklo srautui horizontali taškų grupė Pav. 3 b., reiškianti, kad didelis kiekis srautų tuo pačiu metu stebimas iš kelių užpuoliko valdomų kompiuterių. Užpuolikas valdo adresų ruožą, šaltinio IP adresai kinta IP adreso 4 okteto adresų atkarpoje.



Pav. 3 a. Prieš DDOS ataką



Pav. 3 b. Per DDOS ataką

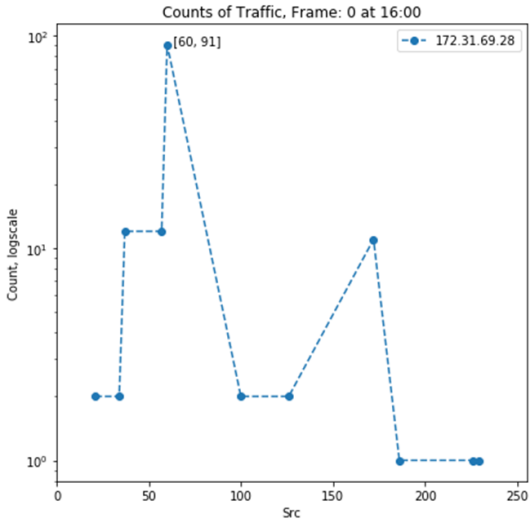
3.2 DOS statistinis atpažinimas

Duomenys iš PCAP failo (IDS 2018 atveju) ir tiesiai iš tinklo įrenginio (Vilniaus universiteto tinklo srauto atveju) nuskaityti Python pritaikyta atviro kodo biblioteka Scapy. Šie duomenys transformuojami į Panda masyvus ir grupuojami į 5 min duomenų blokus. Paskaičiuojami srautų iš šaltinio į tikslą kiekiai, standartinis nuokrypis ir Z-nuokrypis (lentelė 4).

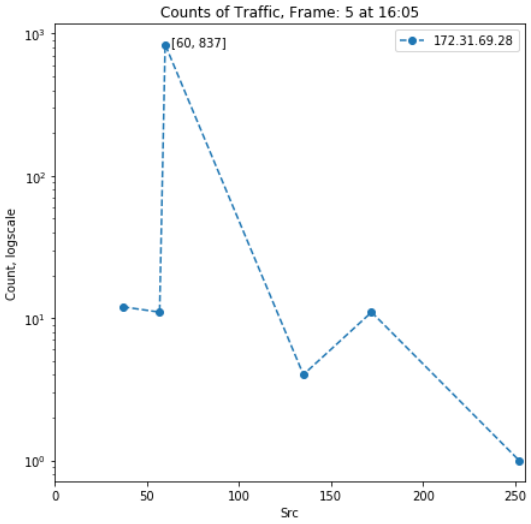
Lentelė 4. Agreguoti atakos pradžios duomenys.

Nr.	Šaltinio 4 oktetas	Srautų skaičius	Sigma (Z) nuokrypis	Normalizuota reikšmė
0	21	2	-0.414351	0.011111
1	34	2	-0.414351	0.011111
2	37	12	-0.018015	0.122222
3	57	12	-0.018015	0.122222
4	60	91	3.113033	1.000000
5	100	2	-0.414351	0.011111
6	126	2	-0.414351	0.011111
7	172	11	-0.057649	0.111111
8	186	1	-0.453984	0.000000
9	226	1	-0.453984	0.000000
10	229	1	-0.453984	0.000000

Šiame eksperimente reikšmės paskaičiuotos kas 5 minutes ir atvaizduojamos Python Matplotlib priemonėmis. DOS ataka atpažįstama iš didelio nuokrypio nuo ankstesnio stebėjimo reikšmės (Pav. 4 a. prasidedant atakai, Pav. 4 b. vykstant atakai). Faktinė atakos pradžia 16:04:30.

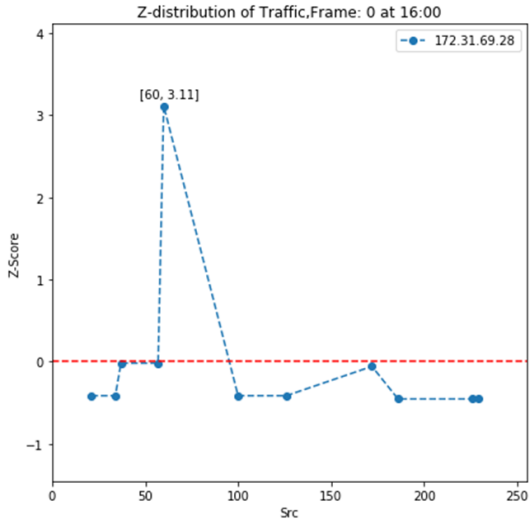


Pav. 4 a. Prieš DOS ataką (maksimumas-91 sesijos per 5 minutes iš puolančio adreso neženkliai išsiskiria iš kito srauto.)

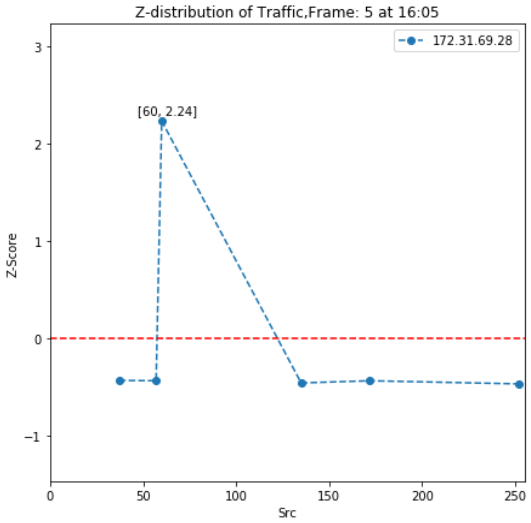


Pav. 4 b. Per DOS ataką (maksimumas – 837 sesijos per 5 minutes ženkliai išsiskiria iš kito srauto)

Pav. 5 a pavaizduota, kad sesijų iš puolančio adreso, kurio paskutinio okteto reikšmė 60, skaičius reikšmingai (>3σ) išsiskiria iš kitų tinklo šaltinių generuojamų srautų. Skaičiuojant sigma nuokrypius vėlesniuose laiko intervaluose Pav. 5 b, reikšmė mažėja dėl ankstesnio atpažinimo inercijos.

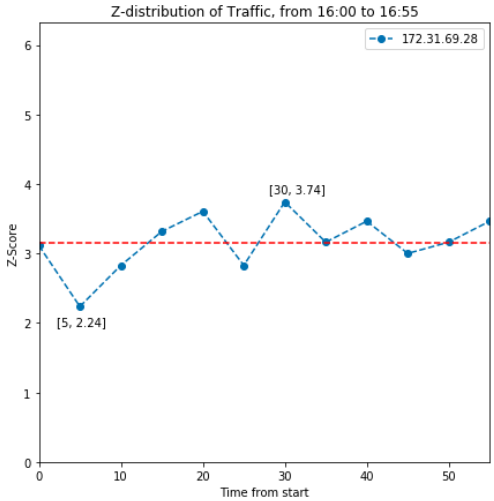


Pav. 5 a. Prieš DDOS ataką



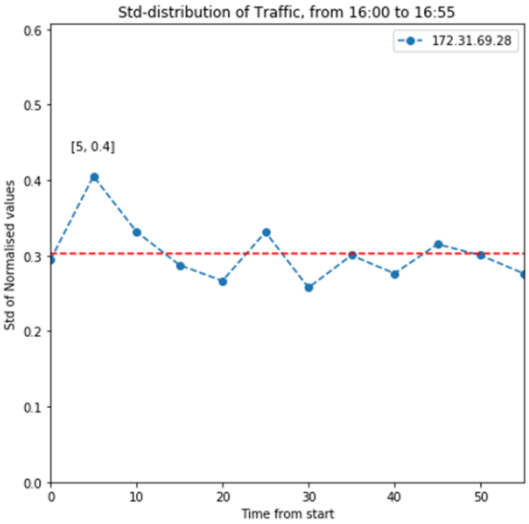
Pav. 5 b. Per DDOS ataką

Pav. 6 pavaizduota sigma nuokrypio kaita laike, kai reikšmė atakos pradžios momentu 16:05 pasiekia minimumą stebėjimo intervale ir maksimumą ties 16:30, kuomet ataka baigiasi.

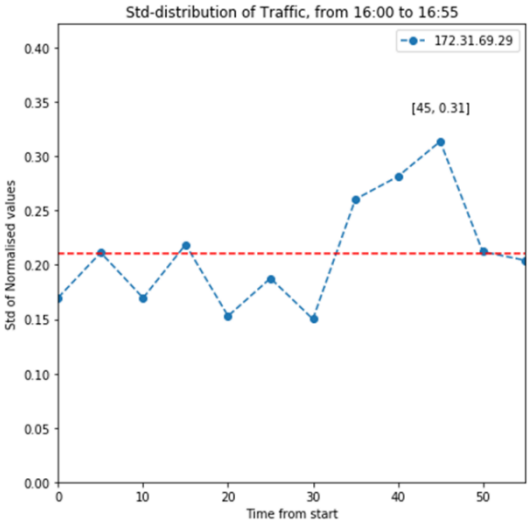


Pav. 6 Sigma-nuokrypio kaita laike

Skaičiuojant srautų kiekio pokytį laiko ašyje matomas didelis nuokrypis nuo vidurkio 16:05 ir 16:45. Pav. 7a ir Pav. 7b matomas šuolis, kuris atspindi atakos pradžią.



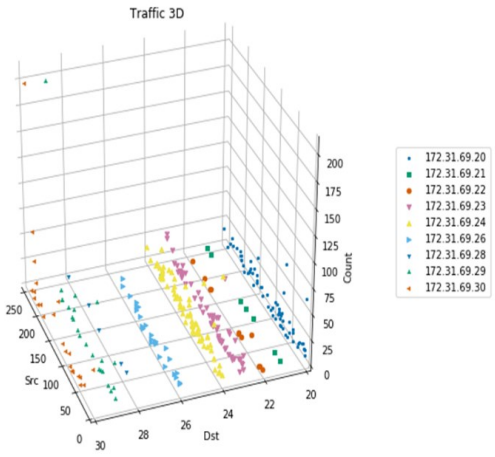
Pav. 7 a. Brute Force ataka adresu 172.31.69.28 16:00:16:05



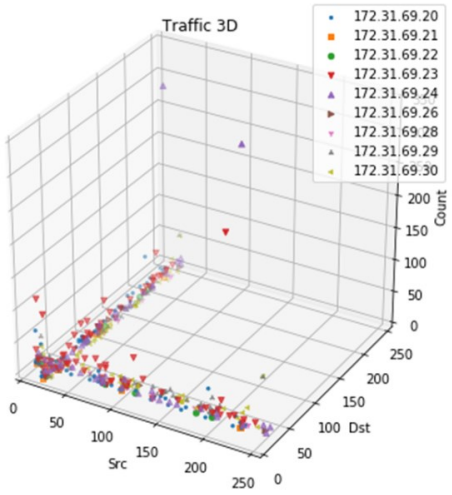
Pav. 7 b. Brute Force ataka adresu 172.31.69.29 16:35-16:45

3.3 DOS atakos atpažinimas 3D vizualizacija

Trimatėse vizualizacijose Pav. 8a ir Pav. 8b. pavaizduoti tyrimui atrinktų dešimties CIC-IDS-2018 duomenų bazės IP adresų duomenys 2018 vasario 23d. 16:05 val. laiku.



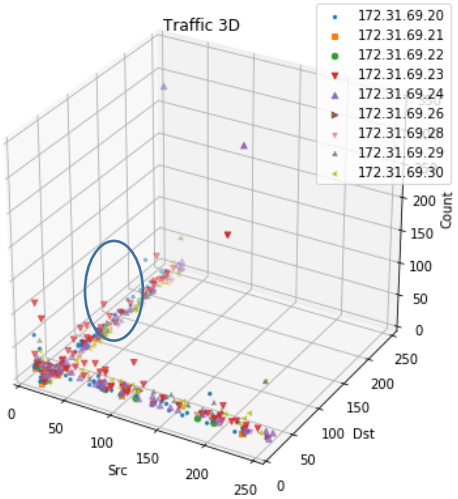
Pav. 8 a. Tiriamo kompiuterių tinklo įeinančių srautų intensyvumo vizualizacija.



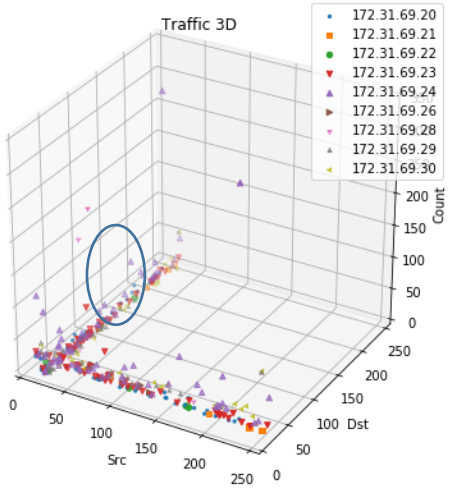
Pav. 8 b. Tiriamo kompiuterių tinklo abipusių srautų intensyvumo vizualizacija.

Atkreiptinas dėmesys į anomalijas kairiame viršutiniame Pav. 8 a. vizualizacijos kampe ir beveik simetrišką įeinančio ir išeinančio srauto vaizdą.

Vizualizacijose pav. 9a-pav. 9b, padarytose 2 minučių intervalu, atkreiptinas dėmesys į 172.31.69.28 adreso vizualizacijoje per šias 2 minutes iškylančias reikšmes ovalu pažymėtoje srityje.



pav. 9a Srautas 16:02



pav. 9 Srautas 16:04

3.4 DOS ir DDOS analizė fraktalinės dimensijos metodu

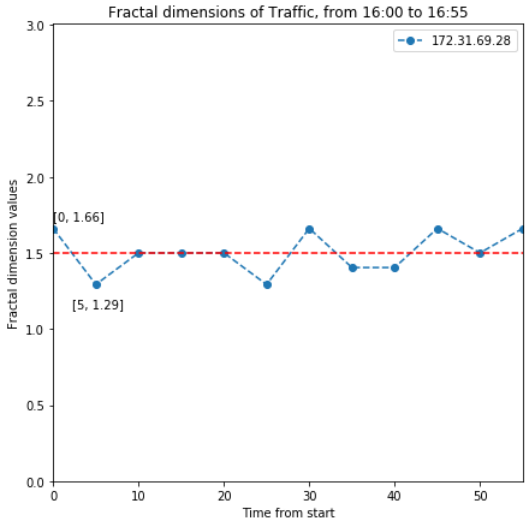
Šioje eksperimento dalyje galimam kibernetiniam išpuoliui nustatyti naudojamas T. Higuchi Boxcount algoritmas (Higuchi, 1988). Šis DOS ir DDOS atakų atpažinimo algoritmas pasiūlytas (Xia, Lu and Li, 2012) tinka ir Brute Force atakoms.

Tinklo srauto Hausdorfo[2] fraktalinė dimensija (Hausdorff, 1918) paskaičiuojama Higuchi metodu (Higuchi, 1988). Šiuo metodu aproksimuojamas Kim, Reddy ir Vannucci metodu parengto vaizdo, sudėtingumas. Fraktalinės dimensijos rodiklis toliau naudojamas kaip indikatorius aptinkant kibernetinį DOS incidentą. Algoritmas perrenka visus vienspalvio vaizdo Z taškus kurių yra N ($m*n = c*n^2$, kur m ir n vaizdo išmatavimai pikseliais, o c – skalės koeficientas, pvz. 4:3, 16:9), poromis (kiekvieną su kiekvienu), atlieka konstantos tikslumu panašų skaičių aritmetinių operacijų, todėl algoritmo sudėtingumas yra proporcingas taškų porų skaičiui. Tačiau, įvertinus taškų retumą, galimas algoritmo spartinimas, praleidžiant nulines reikšmes turinčias taškų poras, o tada griežtas asimptotinis sudėtingumo vertinimas būtų $\Theta(n^k)$ kur $k \in [\log_2 3, 2]$. Čia $O(n^{\log_2 3})$ yra daugybos Karatsuba algoritmu sudėtingumas, o $O(n^2)$ paprastos daugybos stulpeliu sudėtingumas.

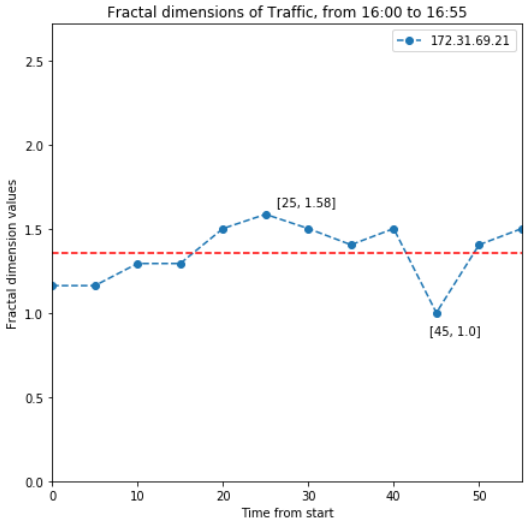
Tinklo duomenų srautas eksperimento metu buvo dalinamas į vienodos trukmės rinkmenas ir suskaičiuotos ryšio seansų poros tarp įvairių išorinių kompiuterių ir tiriamojo. Tuomet sugrupavus duomenis, paskaičiuotos srautų kiekių reikšmės laiko intervale ir Box-counting metodu suskaičiuota trečio IP adreso okteto duomenų, sugrupuotų į vaizdą 16x16, fraktalinė dimensija. Eksperimentas atliktas su 30s, 1, 2 ir 5 minučių intervalais, perrenkant 10 tiriamųjų IP adresų iš CIC-IDS-2018 duomenų bazės.

Fraktalinės dimensijos kaita pav. Pav. 10a ir Pav. 10b. parodo DOS ataką tais atvejais, kai dėl kompiuterio perkrovimo duomenų srautas nutrūksta. Tokia situacija Pav. 10b. stebima 16:45, kai fraktalinės dimensijos reikšmė krinta iki mažiausios galimos pagal Higuchi aproksimuojantį algoritmą d = 1. O kai vaizdo užpildymas didėja, dimensijos reikšmė galimai artėja link d = 2.

[2] Felix Hausdorff (1868 –1942), vokiečių matematikas



Pav. 10 a. Įprastinės veiklos fraktalinės dimensijos dinamika

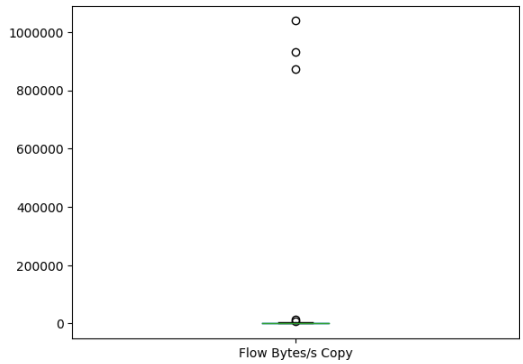


Pav. 10 b. Stebimas minimumas Per ataką 16:45

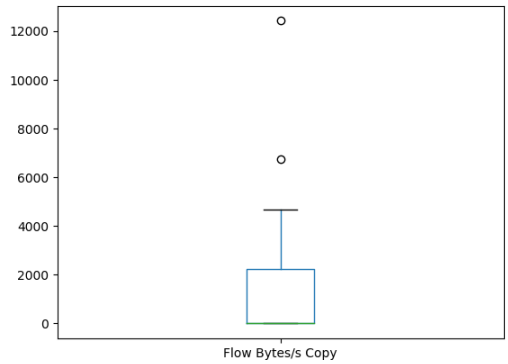
Padaryta prielaida, kad fraktalinės dimensijos pokytis indikuos ataką. Tyrimas parodė, kad nors duomenų statistinis pasiskirstymas turi įtakos fraktalinės dimensijos absoliutinei reikšmei, dimensijos reikšmės nuokrypis nuo vidurkio yra akivaizdus tuomet, kai užpuolikui laužiantis generuojami dideli neįprastų naujų įvykių srautai ir dimensijos reikšmė reikšmingai pakyla virš normalaus veiklos srauto fraktalinės dimensijos vidurkio (d=1.5). Tuo tarpu, įvykus įsilaužimui, fraktalinė dimensija dėl taškų porų skaičiaus sumažėjimo krenta ir rodo artimas d= 1 reikšmes, jei parinktas ilgesnis agregavimo periodas (2, 5 minutės). Tuo būdu, kai fraktalinės dimensijos reikšmė stebimu periodu statistiškai reikšmingai išauga virš ilgalaikio stebėjimo laikotarpio vidurkio (1 val.) ir išvestinis pokytis rodo reikšmingą skirtumą su ankstesniu periodu (30s, 1 min, 2 min, 5 min), galima prognozuoti įsilaužimą. Kai įsilaužimas (pagal faktinius duomenis) jau yra įvykęs, duomenų srautas ženkliai sumažėja, dėl ko tiek statistiniai tiek fraktalinės dimensijos skaičiavimo rezultatai indikuoja minimalias reikšmes (d = 1). Skaičiuojant 30 sekundžių intervale minimumas akivaizdus, tačiau skaičiavimai ir algoritmas darosi nestabilūs dėl reikšmių trūkumo. Šio trūkumo lengvai pavyksta išvengti papildant duomenis standartinio nuokrypio (Z-score) skaičiavimais, kurie yra pakankami ir veikia su mažesniu taškų skaičiumi.

3.5 Atakų atpažinimas histogramų metodu

Šio tyrimo metu buvo tikrinamos anomalijos iš CIC-FlowMeter duomenų. Žinant įprastinio srauto intensyvumą, buvo tirti srauto intensyvumą parodantys duomenys (Pav. 11a ir Pav. 11b.).



Pav. 11 a. Anomalijos virš 800 kB/s



Pav. 11 b. Anomalijos virš 6 kB/s

Lentelėje 4 pateikiami išrinkti anomalijų taškai.

Lentelė 4. Anomalijų Pav. 11a. ir b. taškų duomenys

Pav.	Laiko žymė	Prievadas	Protokolas	Atakos tipas	Srautas B/s
12a	2018-02-23 09:57:12	67	17	Brute Force –Web	1.037954e+06
12a	2018-02-23 10:21:59	67	17	Brute Force –Web	8.736111e+05
12a	2018-02-23 01:41:46	67	17	Brute Force –XSS	9.318519e+05
12b	2018-02-23 09:17:04	31808	6	Brute Force –Web	1.241361e+04
12b	2018-02-23 10:27:48	22	6	Brute Force –Web	6.736396e+03

Taškų histograminė analizė parodė, kad didžioji dauguma taškų reikšmių yra ruože iki 2kB/s.

Techninėje literatūroje nurodyta, kad 67 prievadas rezervuotas DHCP paslaugai, atliekančiai IP adreso pradinį suteikimą nutolusiems įrenginiams [RFC 951]. Normaliai veiklai (autorizuotam kompiuteriui užmegzti pradinį ryšį) užtenka vieno srauto, tuo tarpu čia stebimi tūkstančiai srautų. Toks elgesys pateisina atakos pavadinimą – brutalia jėga (Brute Force) trikdomas kompiuteris, nespėjant tenkinti užklausų išnaudojama visa atmintis, kol kompiuteris restartuoja, o tuo metu neveikia dalis sistemos apsaugų. Tokią ataką įvykdžius, užpuolikas iš išorės įgauna didesnes teises ir atlieka administracinius pakeitimus, arba įvykdo duomenų kopijavimo (SQL Inject) komandas, kurioms nebereikia didelių srautų (lentelė 5):

Lentelė 5. SQL Inject duomenys

Laiko žymė	Prievadas	Protokolas	Atakos tipas	Srautas B/s
2018-02-23 15:05:22	80	6	SQL Inject	438

4 Tinklo duomenų atributų svarbos analizė

Tolimesniame tyrime buvo siekiama išskirti svarbiausius atributus, lemiančius įrašų priskyrimą kibernetinės grėsmės klasei. Duomenų atributų analizei buvo nagrinėjami SVM, Random Forest ir KNN mašinų mokymosi metodų taikymai. Įvertinus mokymosi sudėtingumą ir trukmes, atsisakyta SVM ir KNN metodų.

Ruošiant duomenis statistinėmis priemonėmis buvo nustatyti ir eliminuoti duomenų stulpeliai, kurių dispersija mažesnė už 0,16 (standartinis nuokrypis <±0,4), arba kurių reikšmės su didesne nei 80% tikimybe artimos arba lygios konstantai (lentelė 6):

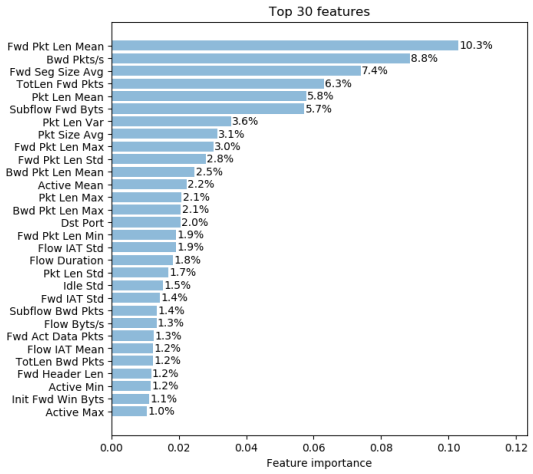
Lentelė 6: statistiniai eliminuojamų atributų duomenys

Nr.	Atributas	Vidurkis	std	min	25%	50%	75%	max
1	Fwd PSH Flags	0,04	0,19	0	0	0	0	1
2	Bwd PSH Flags	0,00	0,00	0	0	0	0	0
3	Fwd URG Flags	0,00	0,00	0	0	0	0	0
4	Bwd URG Flags	0,00	0,00	0	0	0	0	0
5	FIN Flag Cnt	0,01	0,07	0	0	0	0	1
6	SYN Flag Cnt	0,04	0,19	0	0	0	0	1
7	RST Flag Cnt	0,12	0,32	0	0	0	0	1
8	URG Flag Cnt	0,04	0,20	0	0	0	0	1
9	CWE Flag Count	0,00	0,00	0	0	0	0	0
10	ECE Flag Cnt	0,12	0,32	0	0	0	0	1
11	Fwd Byts/b Avg	0,00	0,00	0	0	0	0	0
12	Fwd Pkts/b Avg	0,00	0,00	0	0	0	0	0
13	Fwd Blk Rate Avg	0,00	0,00	0	0	0	0	0
14	Bwd Byts/b Avg	0,00	0,00	0	0	0	0	0
15	Bwd Pkts/b Avg	0,00	0,00	0	0	0	0	0
16	Bwd Blk Rate Avg	0,00	0,00	0	0	0	0	0

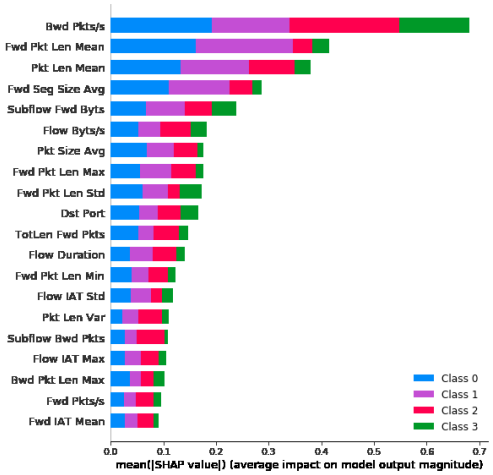
Remiantis duomenų aprašymu, išrinkti faktai intervale tarp 2018-02-23 15:00 iki 15:20, atitinkantys SQL Inject atakos laiką pagal iš CIC-IDS-2018.

Atlikus mokymą Random Forest metodu, buvo paskaičiuotos ir vizualizuotos duomenų požymių svarbos vertės (Pav. 12a). To paties mokymo duomenys buvo panaudoti duomenų požymių svarbos prognozei paskaičiuoti Shapo verčių metodu (Lundberg and Lee, 2017) (Pav. 12b). Palyginimas rodo, kad vertinimai nesutampa, duomenyse nėra vienareikšmiai dominuojančių atributų. Be to jie skirtingi tiriant skirtingas atakas. Ankstesniais autoriaus pirminių komponenčių dimensijų redukavimo tyrimais (Bulavas, 2018) buvo nustatyta, kad patikimesni prognozės rezultatai gaunami panaudojus 10 pirminių komponenčių. Tuo tarpu

atrinkus 10 svarbiausių atributų, teisingai prognozuojama tik apie 64% įrašų, kas yra nepakankamas tikslumas.

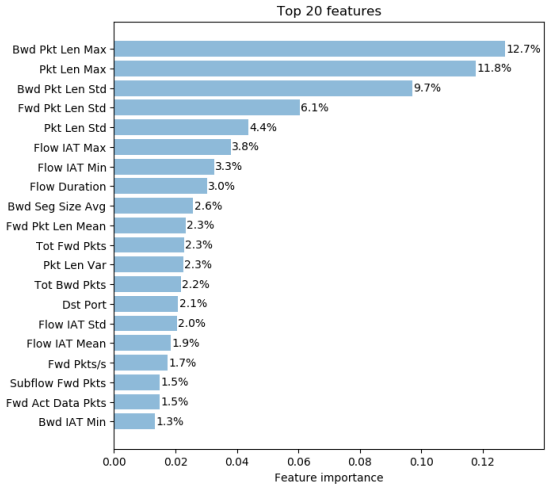


Pav. 12 a. Reikšmės paskaičiuotos iš 4 klasių duomenų Random Forest metodu

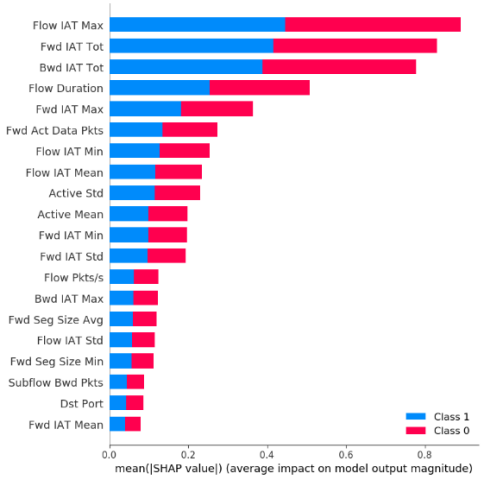


Pav. 12 b Reikšmės paskaičiuotos iš 4 klasių duomenų Random Forest metodu, interpretuotos Shap verčių metodu

Nustatyta, kad norint pasiekti 99% tikslumą reikia 45 atributų. Pav. 13 a. nustatytas svarbiausias atributas reiškia siunčiamų atsakymų paketų ilgio maksimumą. Jis yra SQL Inject paaiškinantis atributas, reiškiantis, kad vyksta didelių paketų užpuolikui siuntimas, kuris prasideda sėkmingai įsilaužus į duomenų bazę. Flow IAT[3] Max atributas, arba maksimalus laikas tarp užpuoliko siunčiamų paketų, Pav. 13 b. paaiškina pradinę užpuolimo fazę. Mažesnis laikas tarp siunčiamų paketų reiškia, kad jų siunčiama labai daug ir dažnai.



Pav. 13 a. Reikšmės paskaičiuotos iš 2 klasių duomenų Random Forest metodu



Pav. 13 b Reikšmės paskaičiuotos iš 2 klasių duomenų Random Forest metodu, interpretuotos shap verčių metodu

[3] IAT - angl. Flow Inter Arrival Time

5 Rezultatai ir išvados

Šiame tyrime buvo nagrinėjami bei grafiškai atvaizduoti lyginamajame Kanados kibernetinio saugumo instituto (CIC) rinkinyje CSE-CIC-IDS2018 (Sharafaldin, Lashkari and Ghorbani, 2018) surinktų DOS, DDOS, Brute Force –Web, Brute Force –XSS ir SQL Inject atakų ir ją sekusių įsilaužimų duomenys. Daugiamačiai kibernetinio saugumo duomenys redukuoti (Kim, Reddy and Vannucci, 2004), (Kim, 2005) pasiūlytais metodais, sukuriant dvimates vizualizacijas, kurių kaita laike teikia kibernetinio įsilaužimo indikacijas. Vykdant tyrimą susidurta su duomenų apdorojimo spartos problemomis Python kalboje, tačiau jos sėkmingai išspręstos. Pavyko pritaikyti Python kodo spartinimo rekomendacijas (Lambda functions, List comprehensions) kibernetinio saugumo duomenų formato PCAP įkėlimo į analizei tinkamus masyvus, leidusias geriau išnaudoti turimus kompiuterinius resursus keliant didelius duomenis ir juos toliau apdorojant realiu laiku.

Tyrimo metu nagrinėtas kibernetinio įsilaužimo nustatymo statistinio ir mašinų mokymosi algoritmų sudėtingumas. Įvertinus statistinių algoritmų sudėtingumą, galima apibendrinti, kad nagrinėti metodai yra taikytini realaus laiko uždavinyje nustatant DOS ir DDOS atakas, tačiau esant dideliems duomenų srautams, pasirinktas spartesnis $\mathcal{O}(n \log n)$ sudėtingumo algoritmas.

Įvertinta gautų taškinių vaizdų Hausdorfo fraktalinė dimensija (sudėtingumas) ir aproksimuojančio (Higuchi, 1988) Box-Counting algoritmo sudėtingumas $\mathcal{O}(n^2)$. Įvertinant dvimačio vaizdo retumą, galima teigti, kad griežtesni asimptotiniai Hausdorfo dimensijos skaičiavimo aproksimuojančiu Higuchi Box-Counting algoritmu vertinimai galimai būtų $\mathcal{O}(n^k)$, kur $k \geq \log_2 3$ ir $n \leq 2$, kadangi n nėra tokie dideli, kad būtų išlošiama skaičiuojant efektyvesniais prie didelių n, nei Karatsubos daugybos skaičiavimo algoritmais. Tačiau n log n auga lėčiau nei n^k, kai $n>3$ ir $k> 1$, todėl paprasta statistika veikia greičiau.

Shapo verčių metodu (Lundberg and Lee, 2017) buvo atliekamas pasirinktais mašinų mokymo metodais (SVM, Random Forest, KNN) paskaičiuotų duomenų požymių svarbos nustatymas, parodęs, kad nėra vienareikšmiai dominuojančių dimensijų, o ženklus dimensijų sumažinimas blogina prognozių kokybę, kas buvo patvirtinta ir ankstesniais autoriaus pirminių komponenčių dimensijų redukavimo tyrimais (Bulavas, 2018).

6 Literatūros sąrašas

[1.] Anderson, J. P. (1980) *Computer security threat monitoring and surveillance*, *Technical Report James P Anderson Co Fort Washington Pennsylvania, 1980*.

[2.] Augustine Chang (2019) *Computational Complexity Theory in ML modeling*, *Medium*. Available at: https://medium.com/@augustinechang/computational-complexity-theory-in-ml-modeling-66b5a5fa610f (Accessed: 14 October 2019).

[3.] Bouzida, Y. and Cuppens, F. (2004) 'Efficient intrusion detection using principal component analysis', *Proceedings of the*. Available at: http://yacine.bouzida.free.fr/Articles/2004SAR.pdf.

[4.] Brundage, M. *et al.* (2018) 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation', (February 2018). Available at: http://arxiv.org/abs/1802.07228.

[5.] Buczak, A. and Guven, E. (2015) 'A survey of data mining and machine learning methods for cyber security intrusion detection', *IEEE Communications Surveys & Tutorials*, PP(99), p. 1. doi: 10.1109/COMST.2015.2494502.

[6.] Bulavas, V. (2018) 'Investigation of network intrusion detection using data visualization methods', in *59th International Scientific Conference on Information Technology and Management Science of Riga Technical University, ITMS 2018 - Proceedings*. doi: 10.1109/ITMS.2018.8552977.

[7.] Burges C. J. C (1998) 'A Tutorial on support vector machines for pattern recognition', *Data mining and knowledge discovery*, 2(2), pp. 121–167.

[8.] Čiegis, R. (2007) *Duomenų struktūros, algoritmai ir jų analizė*, *Duomenų struktūros, algoritmai ir jų analizė*. Vilnius, Lithuania: Vilnius Gediminas Technical University. doi: 10.3846/922-S.

[9.] Dasgupta, S., Papadimitriou, C. and Vazirani, U. (2006) *Algorithms*. McGraw-Hill.

[10.] Denning, D. E. (1986) 'An Intrusion-Detection Model', in *1986 IEEE Symposium on Security and Privacy*. IEEE, pp. 118–118. doi: 10.1109/SP.1986.10010.

[11.] Garey, M. R. and Johnson, D. S. (1979) *Computers and intractability. A guide to the theory of NP-completeness.* San Francisco: W. H. Freeman and Company. Available at: https://katalog.ub.uni-heidelberg.de/cgi-bin/titel.cgi?katkey=65902109.

[12.] Hausdorff, F. (1918) 'Dimension and outer measure', *Mathematische Annalen*, 79(1–2), pp. 157–179. doi: 10.1007/BF01457179.

[13.] Hettich, S. and Bay, S. D. (1999) 'The UCI KDD Archive [http://kdd.ics.uci.edu]', *University of California, Department of Information and Computer Science*.

[14.] Higuchi, T. (1988) 'Approach to an irregular time series on the basis of the fractal theory', *Physica D: Nonlinear Phenomena*, 31(2), pp. 277–283. doi: 10.1016/0167-2789(88)90081-4.

[15.] Jim Dowling (2017) *Distributed ML and Linear Regression*, *ID2223 Lecture 2*. Available at: https://www.kth.se/social/files/5a040fe156be5be5f93667e9/ID2223-02-ml-pipelines-linear-regression.pdf (Accessed: 14 October 2019).

[16.] KDD (1999) *KDD Cup 1999 Data*, *KDD Cup 1999 Data*. Available at: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[17.] Kim, S. S. (2005) *REAL-TIME ANALYSIS OF AGGREGATE NETWORK TRAFFIC FOR ANOMALY DETECTION*.

[18.] Kim, S. S., Reddy, A. L. N. and Vannucci, M. (2004) 'Detecting traffic anomalies using discrete wavelet transform', *Information Networking*, (July), pp. 951–961. doi: 10.1007/978-3-540-25978-7.

[19.] Koch, R. (2011) 'Towards Next-Generation Intrusion Detection', in C. Czosseck, E. Tyugu, T. W. (Eds. . (ed.) *2011 3rd International Conference on Cyber Conflict*. Tallinn, Estonia: CCD COE Publications, pp. 151–168.

[20.] Krylovas, A. (2004) *Diskrečioji matematika*. Vilnius: Technika.
[21.] Laboratory, L. (1998) *Darpa intrusion detection data sets (1998)*, *http://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset*. Available at: http://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset.
[22.] Lawrence Berkeley National Laboratory (2010) *The Internet Traffic Archive*. Available at: http://ita.ee.lbl.gov/index.html.
[23.] Lewis, J. A. (2015) 'The Role of Offensive Cyber Operations in NATO's Collective Defence', *The Talliban Papers*, (8).
[24.] Lundberg, S. M. and Lee, S.-I. (2017) 'A Unified Approach to Interpreting Model Predictions', in *31st Conference on Neural Information Processing Systems (NIPS 2017)*. Long Beach, CA. Available at: https://github.com/slundberg/shap (Accessed: 21 June 2019).
[25.] Oliveto, P. S., He, J. and Yao, X. (2007) 'Time complexity of evolutionary algorithms for combinatorial optimization: A decade of results', *International Journal of Automation and Computing*, 4(3), pp. 281–293. doi: 10.1007/s11633-007-0281-3.
[26.] Quinlan, J. R. (1986) 'Induction Fo Decion Trees', *Machine Learning*, 1, pp. 81–106.
[27.] Sharafaldin, I., Lashkari, A. H. and Ghorbani, A. A. (2018) 'Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization', in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. SCITEPRESS - Science and Technology Publications, pp. 108–116. doi: 10.5220/0006639801080116.
[28.] Si Si *et al.* (2017) 'Gradient Boosted Decision Trees for High Dimensional Sparse Output', in *Proceedings of the 34 th International Conference on Machine Learning, Sydney, Australia*. Available at: http://www.stat.ucdavis.edu/~chohsieh/rf/icml_sparse_GBDT.pdf (Accessed: 14 October 2019).
[29.] The Cooperative Association for Internet Data Analysis (2010) 'CAIDA - The Cooperative Association for Internet Data Analysis', *CAIDA*. Available at: http://www.caida.org/home/.
[30.] The Shmoo Group (2011) *Defcon*.
[31.] Witten, I. H. *et al.* (2005) *Data Mining: Practical Machine Learning Tools and Techniques*. Second Edi, *Data Mining: Practical Machine Learning Tools and Techniques*. Second Edi. Edited by J. Gray. San Francisco: Morgan Kaufmann Publishers.
[32.] Xia, Z., Lu, S. and Li, J. (2012) 'DDoS flood attack detection based on fractal parameters', *2012 International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2012*. IEEE, (2), pp. 1–5. doi: 10.1109/WiCOM.2012.6478475.