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

INFORMATIKOS INŽINERIJA (07 T)

DIRBTINIO INTELEKTO METODŲ TAIKYMAS ĮSISKVERBIMŲ Į KOMPIUTERIUS TINKLUS APTIKIMO SISTEMOSE

Doktorantas Liudas Ališauskas

2018 m. spalis

Mokslinė ataskaita MII-DS-07T-2018-1

VU Duomenų mokslo ir skaitmeninių technologijų institutas, Akademijos g. 4, Vilnius LT-08663

www.mii.lt

Santrauka

Ataskaitoje pateikiama kompiuterių tinklų duomenų srauto ir veiklą registruojančių įrašų analizės, įsiskverbimų į kompiuterių tinklus atakos vektorių analizės, dirbtinio intelekto metodų taikomų aptinkant įsiskverbimus į kompiuterių tinklus analizės rezultatai.

Ataskaitoje aprašomi srautiniai kompiuterių tinklo duomenys, motyvacija, kodėl tolimesnius tyrimus vykdysime tik su srautiniais duomenimis neanalizuojant kompiuterių tinklo paketų.

Pristatomas pasiruošimo tolimesniems tyrimams metodas ir įrankiai.

Reikšminiai žodžiai: Įsibrovimo į kompiuterių tinklus aptikimas, Dirbtinis intelektas, Neapmokomi metodai, anomalijos grafuose.

Turinys

1. Įvadas

Pastarųjų metų Valstybės saugumo departamento (VSD & AOTD, 2017), (VSD & AOTD, 2018) ir Krašto apsaugos ministerijos (NKSC, 2017), (NKSC, 2018) ataskaitose teigiama, kad šalies ypatingos svarbos infrastruktūra yra aktyviai stebima, skenuojama, nuolatos bandoma įsiskverbti, yra fiksuoti sėkmingi tokių įsilaužimų pavyzdžiai. Daugeliu atveju įsiskverbimų tikslas išlieka informacijos vagystė, tačiau įsiskverbus į industrinio valdymo sistemas sudaromos sąlygos fiziškai paveikti ypatingos svarbos infrastruktūrą, sustabdyti ar sutrikdyti ypatingai svarbios infrastruktūros veiklą ir taip pakenkti šalies veiklai ir vystymuisi.

Siekiant užkirsti kelia pažangiems įsilaužimams yra kuriamos įvairios apsaugos sistemos, analizuojančios tiek kompiuterių tinklo srauto duomenis, tiek tinklo įrenginių, darbo vietų (angl. end-point) veiklos duomenis. Didžioji dalis apsaugos sistemų veikia analizuojant sistemų veiklos duomenis ir lyginant rezultatus su turimais įsiskverbimo indikatoriais (angl. Indicator of Compromise). Šio tipo apsaugos sistemų veikimas yra pagrįstas sistemoje įdiegtais požymiais (angl. signature-based), jos geba greitai aptikti kibernetines atakas (angl. Cyber attack). Tačiau jei kibernetinė ataka dar nėra žinoma ir nėra žinomi jos požymiai – požymiais pagrįstos apsaugos sistemos nėra pajėgios aptikti kibernetinių atakų. Sistemos, kurios kibernetinių atakų aptikimui naudoja pažangesnius, dažnai anomalijų atpažinimo pagrįstus metodus (angl. anomaly-based), pasižymi gebėjimu aptikti dar neatpažįstamas kibernetines atakas, tačiau tokios sistemos dažnai būna lėtesnės ir turi nemažą klaidingo (angl. false positive) nustatymo procentą. Vertinant skirtingų apsaugos sistemų pranašumus ir trūkumus, dažnai kombinuojami tarpusavyje kibernetinių atakų aptikimo metodai siekiant efektyvaus apsaugos sistemų veikimo.

Nežinomų kibernetinių atakų aptikimui yra pasitelkiami dirbtinio intelekto metodai, ypatingas dėmesys yra skiriamas neapmokomiems (angl. Unsupervised) metodams, nepaisant jų didesnės paklaidos, kadangi su įvairių kibernetinių atakų požymiais sužymėtų duomenų rinkinių skirtų modelių formavimui nėra daug, o požymiai labai greitai kinta ir lieka nebeaktualūs.

Šio tyrimo metu, mes fokusuojamės į neapmokamus dirbtinio intelekto metodų panaudojimo galimybes, šių metodų efektyvumą siekiant aptikti įsiskverbimo į kompiuterių tinklus (toliau – Įsiskverbimas) kibernetines atakas. Duomenys, kuriuose ieškoma Įsiskverbimų yra srautiniai kompiuterių tinklo duomenys gaunami ir saugomi NetFlow (CISCO, 2012) formate ar gimininguose srautu pagrįstuose (angl. flow-based) formatuose. Tolimesniam tyrimui šie duomenys yra pasirinkti dėl (1) paprastumo juos išgauti bet kuriame kompiuteriniame tinkle, (2) juose yra užregistruoti ne tik normalios kompiuterių tinklo įrenginių komunikacijos, bet ir komunikacijos, kurias iššaukia bandymai įsiskverbti, ar toliau vystyti kibernetines takas.

2. 2017 – 2018 metų tyrimas

2.1 Tyrimo objektas

Disertacijos tyrimo objektas: Dirbtinio intelekto metodai, jų rezultatų tikslumas ir efektyvumas aptinkant įsiskverbimus į kompiuterinius tinklus.

2.2 Tyrimo tikslas

Disertacijos tyrimo tikslas: Pagerinti dirbtinio intelekto metodų rezultatų tikslumą ir efektyvumą aptinkant įsiskverbimus į kompiuterinius tinklus.

Šioje ataskaitoje apžvelgiami šioje srityje jau atlikti tyrimai, vertinami tyrimų gauti rezultatai. Analizuojama duomenų reikalingų siekiant vykdyti įsiskverbimų aptikimą galimi šaltiniai, duomenų modelis. Palyginami dirbtinio intelekto metodai naudojami siekiant aptikti įsiskverbimus į kompiuterius tinklus.

2.3 Tyrimo uždaviniai

2017 - 2018 metams kelti uždaviniai:

- Atlikti teorinius ir praktinius tyrimus toliau sprendžiant dirbtinio intelekto metodų, taikymų įsiskverbimų į kompiuterinius tinklus aptikimo sistemose, tikslumo ir efektyvumo uždavinį;
- Tyrimo metodikos sudarymas:
    - Problemų kylančių iš tikslo suformulavimas būsimiems eksperimentiniams ir analitiniams tyrimams.
    - Uždavinių skirtų nustatytoms problemoms spręsti aprašymas.
    - Tinkamos tyrimo metodikos parinkimas iškeltiems uždaviniams spręsti.
    - Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką.

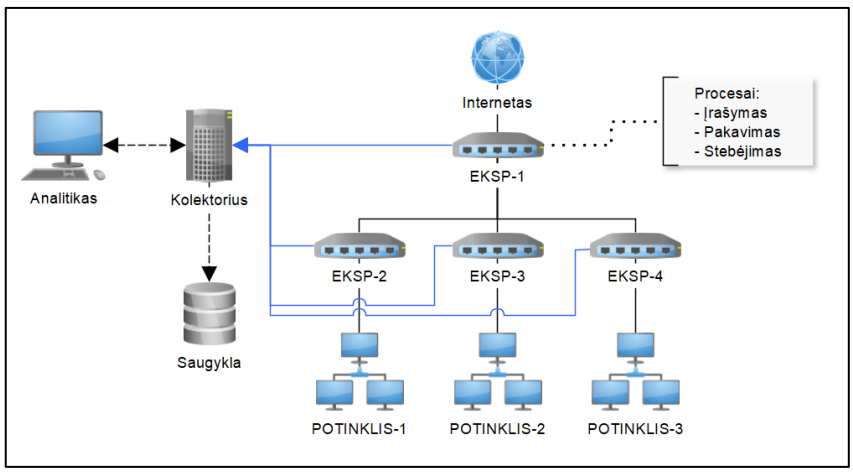
2.4 Tyrimo duomenys, jų gavyba

Informaciją apie tai kas vyksta kompiuterių tinkluose (angl. Computer network) gaunama analizuojant kompiuterių tinklo srautų (angl. Network flows, Network streams) duomenis. Kompiuterių tinklo duomenys gaunami iš kompiuterių tinklo įrenginių (angl. Network devices), tokių kaip maršrutizatorius (angl. Router), komutatorius (angl. Switch) pasinaudojant plačiai naudojamomis tinklo srautų duomenų išgavimo technologijomis, arba tiesiogiai nuskaitant kompiuterių tinkle perduodamus duomenų paketus (angl. Packet capturing).

Pasauliniai tinklo įrenginių gamintojai tinklo srautų duomenims gauti naudoja skirtingas technologijas. Plačiausiai paplitusios ir giminingos NetFlow (Cisco, 2012) technologijai yra JFlow (Juniper Networks, 2018), NetStream (HUAWEI, 2012), sFlow (sFlow.org, 2018) technologijos.

NetFlow ir JFlow technologijos savo realizavimu ir galimybėmis yra labai panašios. Abi technologijos analizuoja kiekvieną pro tinklo įrenginį praeinantį duomenų paketą, ištraukia iš duomenų paketo reikiamą informaciją pagal nustatytas taisykles, ją agreguoja ir transformavusios duomenis tinkamu formatu – perduoda į tinklo srauto duomenų surinkimo tašką. sFlow technologijos esminis skirtumas nuo NetFlow ir JFlow technologijų yra tai, kad čia yra analizuojamas yra tik 1 iš N per tinklo įrenginį praeinančių duomenų paketų. Tokiu būdu yra sumažinamas tinklo įrangos apkrovimas, atsiranda galimybė analizuoti didelius tinklo srautus, tačiau gaunami mažiau tikslūs tinklo duomenų srauto duomenys (Berk, 2018). Pastaruoju metu tinklo įrangos gamintojai tinklo srautų duomenų perdavimui stengiasi taikyti IPFIX (angl. IP Flow Information Export) tinklo srauto duomenų perdavimo standartą (Claise, 2008).

Principinė visų minėtų technologijų schema pateikiama 1 paveikslėlyje. Šioje schemoje juodomis linijomis pavaizduoti tinklo duomenų komunikacijos kanalas, o mėlynomis – duomenų srautų komunikacijos kanalai tarp tinklo įrenginių, kurie atlieka duomenų gavimo funkciją (angl. Exporter) ir tinklo srauto duomenų surinkimo funkciją (angl. Collector).



1 pav. Principinė tinklo srautų analizės technologijų schema.

Pasibaigus duomenų perdavimo sesijai, arba nutraukus sesijos agregavimą kopijuoja tam tikrų parametrų reikšmes iš duomenų paketų į tinklo srauto duomenų paketą, apskaičiuoja papildomas duomenų perdavimo sesijos reikšmės, gaunama NetFlow duomenų struktūra su šiais pagrindiniais laukais (neapsiribojant): (1) Sesijos pradžios ir pabaigos laikas, (2) Sesijos trukmė milisekundėmis, (3) Šaltinio IP adresas (angl. Source IP address), (4) šaltinio prievadas (angl. Source port), (5)

paskirties IP adresas (angl. Destination IP address), (6) paskirties prievadas (angl. Destination port), (7) IP protokolas (angl. IP protocol), (8) IP paslaugos tipas (angl. IP Type of Service), (9) perduotų paketų skaičius sesijos metu, (10) sesijos dydis baitais. Duomenų pavyzdys pateikiamas 1 lentelėje.

1 lentelė. NetFlow duomenų struktūros pavyzdys.

@timestamp	Dur	SrcIP	SrcPort	DstIP	DstPort	Proto	dTos	TotPkts	TotBytes
2011-08-10, 12:46:53.047	3550.18	212.50.71.179	39678	172.31.84.229	13363	udp	0	12	875B
2011-08-10, 12:46:53.048	0.00	84.13.246.132	28431	172.31.84.229	13363	udp	0	2	135B
2011-08-10, 12:46:53.049	0.00	217.163.21.35	80	172.31.86.194	2063	tcp	0	2	120B
2011-08-10, 12:46:53.053	0.06	83.3.77.74	32882	172.31.85.5	21857	tcp	0	3	180B
2011-08-10, 12:46:53.053	3427.77	74.89.223.204	21278	172.31.84.229	13363	udp	0	42	2.789KB
2011-08-10, 12:46:53.056	3086.55	66.169.184.207	49372	172.31.84.229	13363	tcp	0	591	44.854KB
2011-08-10, 12:46:53.058	3589.63	182.239.167.121	49649	172.31.84.229	13363	udp	0	12	1.459KB

Analizei NetFlow duomenys neturi savyje tiek informacijos kiek turi pilni tinklo srauto paketai (NETFORT, 2014), tačiau to paties laikotarpio duomenų dydžio skirtumas, bei užfiksuota informacija apie kompiuterių tinkle įvykusias komunikacijas įgalina kaupti ilgesnio laikotarpio duomenis, kurti ilgo laikotarpio normalios veiklos modelius.

2.5 Įsiskverbimai į kompiuterių tinklus

Remiantis NIST organizacijos apibrėžimu - kibernetine ataka yra laikoma ataka per kibernetinę erdvę, išnaudojant organizacijų kibernetinę erdvę su tikslu sutrikdyti, išjungti, sunaikinti ar neleistinai kontroliuoti aplinką ir infrastruktūrą; sugadinti organizacijos duomenis; pavogti organizacijos informaciją (Kissel, 2013). Kiekviena kibernetinė ataka (2 paveikslėlis) dažniausiai yra vykdoma nuosekliai šešiais etapais (Palo Alto, 2018):

1 etapas: **Žvalgyba** (angl. Reconnaissance) – Šio etapo metu nustatinėjami potencialūs atakos objektai, kuriuos išnaudojus būtų pasiekti išsikelti tikslai. Nustačius naudojamas apsaugos sistemas, susipažinus su infrastruktūra, parenkami atitinkamos atakos priemonės.

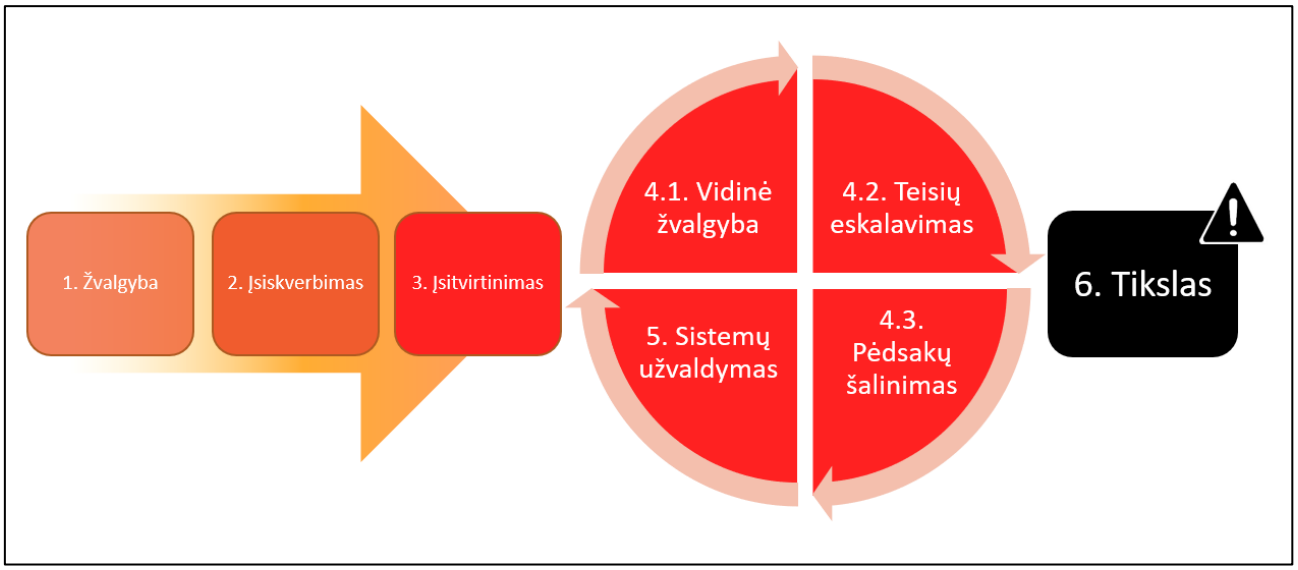
2 etapas: **Pirminis įsilaužimas** (angl. Initial compromise) – Šio etapo metu atakuojantys įveikia naudojamas apsaugos sistemas ir patenka į kompiuterio tinklo vidų per įsilaužtą įrenginį ar naudotojo paskyrą.

3 etapas: **Vadovavimas ir valdymas** (angl. Command & control) – kompromituotas įrenginys naudojamas kaip taškas, į kurį nusikaltėliai atsisiunčia papildomus įrankius (dažniausiai nuotolinės prieigos programas (angl. remote-access, Trojan).

4 etapas: **Horizontalus judėjimas** (angl. Lateral movement) – Sukūrus ne vieną prieigos kanalą nusikaltėliai siekia užvaldyti daugiau įrenginių. Kadangi nusikaltėliai veikia vidinių naudotojų vardu – jų veiklą yra sudėtinga aptikti.

5 etapas: **Taikinių užvaldymas** (angl. Target attainment) – Šiuo etapo metu nusikaltėliai jau tu užvaldę daug tinklo įrenginių, pilnai žino tinklo infrastruktūrą, gali užvaldyti didžiąją dalį įrenginių.

6 etapas: **Duomenų ištraukimas, sistemų sugadinimas ir sutrikdymas** (angl. Exfiltration, corruption, and disruption) – Tai paskutinis etapas, kurio metu žala įmonės veiklai didėja eksponentiškai ir priklauso nuo nusikaltėlių turėtų tikslų.



2 pav. Principinė kibernetinės atakos schema.

Žemiau 2 lentelėje pateikiamos susistemintos kibernetinių atakų grupės (Bhuyan, Bhattacharyya, & Kalita, 2014). Svarbu paminėti, kad visų šių kibernetinių atakų metu vykstančios komunikacijos tarp atakuojamos sistemos ir nusikaltėlio yra registruojamos tinklo srauto duomenyse (1 lentelė).

2.6 Anomalijų aptikimas srautiniuose duomenyse

Dirbtinio intelekto metodai naudojami kompiuterių tinklo apsaugoje pasitelkiami tada kai nepakanka taisyklėmis paremtų saugos sprendimų siekiant aptikti naujas ir dar nežinomas kibernetines atakas. Kiekviena kibernetinės ataka gali būti aptinkama kaip pokytis nuo normalios sistemos veiklos. Pvz.: padaugėja užklausų iš vieno kompiuterio į kitą, nors iki šiol minėtas kompiuteris tokių užklausų negeneruodavo ir pan. Toks nuokrypis nuo normalios veiklos laikomas anomalija. Anomalijomis (angl. Anomaly) yra laikomos struktūros, šablonai duomenyse, kurie

neatitinka tiksliai apibrėžtų normalaus elgesio sąvokų (Chandola, Banerjee, & Kumar, 2009). Dažniausiai metodai veikia siekdami aptikti anomalijas tiek kompiuterių tinklų veikloje tiek ir stebint saugos problemas.

2 lentelė. Kibernetinių atakų klasės. Požymiai ir pavyzdžiai.

Attack name	*Characteristics*	*Example*
Virus	(i) A self replicating program that infects the system without any knowledge or permission from the user. (ii) Increases the infection rate of a network file system if the system is accessed by another computer.	Trivial.88.D, Polyboot.B, Tuareg
Worm	(i) A self replicating program that propagates through network services on computer systems without user intervention. (ii) Can highly harm network by consuming network bandwidth.	SQL Slammer, Mydoom, CodeRed Nimda
Trojan	(i) A malicious program that cannot replicate itself but can cause serious security problems in the computer system. (ii) Appears as a useful program but in reality it has a secret code that can create a backdoor to the system, allowing it to do anything on the system easily, and can be called as the hacker gets control on the system without user permission.	Example-Mail Bomb, phishing attack
Denial of service (DoS)	(i) Attempts to block access to system or network resources. (ii) The loss of service is the inability of a particular network or a host service, such as e-mail to function. (iii) It is implemented by either forcing the targeted computer(s) to reset, or consuming resources. (iv) Intended users can no longer communicate adequately due to non-availability of service or because of obstructed communication media.	Buffer overflow, ping of death(PoD), TCP SYN, smurf, teardrop
Network Attack	(i) Any process used to maliciously attempt to compromise the security of the network ranging from the data link layer to the application layer by various means such as manipulation of network protocols. (ii) Illegally using user accounts and privileges, performing actions to delete network resources and bandwidth, performing actions that prevent legitimate authorized users from accessing network services and resources.	Packet injection, SYN flood
Physical Attack	An attempt to damage the physical components of networks or computers.	Cold boot, evil maid
Password Attack	Aims to gain a password within a short period of time, and is usually indicated by a series of login failures.	Dictionary attack, SQL injection attack
Information Gathering Attack	Gathers information or finds known vulnerabilities by scanning or probing computers or networks.	SYS scan, FIN scan, XMAS scan
User to Root (U2R) attack	(i) It is able to exploit vulnerabilities to gain privileges of superuser of the system while starting as a normal user on the system. (ii) Vulnerabilities include sniffing passwords, dictionary attack, or social engineering.	Rootkit, loadmodule, perl
Remote to Local (R2L) attack	(i) Ability to send packets to a remote system over a network without having any account on that system, gain access either as a user or as a root to the system and do harmful operations. (ii) Performs attack against public services (such as HTTP and FTP) or during the connection of protected services (such as POP and IMAP).	Warezclient, warezmaster, imap, ftp_write, multihop, phf, spy
Probe	(i) Scans the networks to identify valid IP addresses and to collect information about host (e.g., what services they offer, operating system used). (ii) Provides information to an attacker with the list of potential vulnerabilities that can later be used to launch an attack against selected systems and services.	IPsweep, portsweep

Anomalijos klasifikuojamos į tris kategorijos (Goldstein & Uchida, 2016):

- Taško anomalijos (angl. Point anomalies), kaip vienas duomenų objektas laikomas anomalija lyginant su visais kitais objektais.
- Kontekstinės anomalijos (angl. Contextual anomalies), kada duomenys iš savęs yra normalūs, bet kontekste nebe.
- Kolektyvinė anomalija (angl. Collective anomaly). Kai susijusių duomenų egzempliorių rinkinys yra anomalus viso duomenų rinkinio atžvilgiu.

Mūsų tyrimo kontekste labiausiai tikėtinos yra kontekstinės ir kolektyvinės anomalijos, todėl numatomi papildomi pirminių duomenų transformavimas, agregavimas ir kitos procedūros siekiant kontekstines ir kolektyvines anomalijas transformuoti į taškine jų kokybiškesniam aptikimui.

Anomalijų aptikimo metodai veikia trimis veiksenomis (Chandola ir kt., 2009):

1. Apmokamas anomalijos aptikimas (angl. Supervised Anomaly Detection). Metodas remiasi duomenų žymėmis, kai duomenys pateikiami kartu su normalios ir anomalios klasės žymėmis. Visi nežymėti duomenys yra lyginami su žinomomis klasės ir priskiriami vienai jų. Problemos: (1) anomalios klasės egzempliorių dažniausiai būna mažiau nei

normalios veiklos klasės; (2) Tikslių ir reprezentatyvių žymių gavyba yra sudėtinga, kartais tam naudojami dirbtiniai anomalijų generavimo metodai.

2. Pusiau apmokamas anomalijos aptikimas (angl. Semi supervised Anomaly Detection). Metodas remiasi tik vienos iš klasių pateikimu, dažniausiai normalios veiklos klase pažymėtus duomenis. Taip atpažinimo metodai vertina duomenis pagal normalios veiklos požymius. Šis metodas plačiau naudojamas, nei prižiūrimo aptikimo metodas.
3. Neapmokamas anomalijos aptikimas (angl. Unsupervised Anomaly Detection). Šiam metodui nereikia iš anksto sužymėtų mokymo duomenų. Šios kategorijos metodai paremti prielaida, kad didžioji duomenų dalis yra iš normalios veiklos ir tik keletas egzempliorių yra anomalūs. Esant skirtingai situacijai – šios kategorijos anomalijų atpažinimo metodai generuoja daug klaidingai teigiamų (angl. False positive) rezultatų.

Tolimesniame tyrime fokusuosimės į neprižiūrimus anomalijų aptikimo metodus. To priežastis – nėra daug viešai prieinamų sužymėtų duomenų rinkinių. Kibernetinės atakos labai greitai evoliucionuoja ir išmoksta likti nepastebimomis anomalijų pagrindu veikiančios saugos sistemoms.

Neprižiūrimų anomalijų aptikimo metodų rezultatai pateikiami 3 lentelėje (Goldstein & Uchida, 2016). Rezultatai rodo, kad skirtingi metodai gali būti taikomi skirtingiems uždaviniams spręsti. Siekiant aptikti kibernetines atakas svarbūs faktoriai yra metodų gebėjimas greitai dirbti su dideliais duomenų kiekiais.

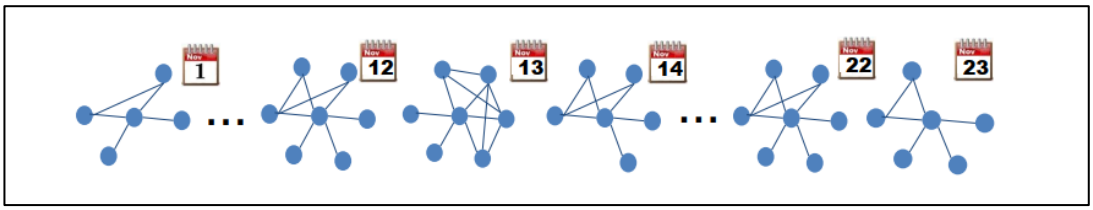
3 lentelė. Neapmokamų dirbtinio intelekto metodų rezultatai.

Alg.	accuracy	deterministic	sensitivity	speed	global detection
k-NN	++	++	+	o	++
LOF	++	++	+	o	– –
COF	–	++	+	o	– –
INFLO	o	++	+	o	– –
LoOP	++	++	+	o	– –
LOCI	o	++	++	– –	– –
aLOCI	–	– –	– –	o	–
CBLOF	– –	o	o	+	– –
uCBLOF	++	o	o	+	++
LDCOF	–	o	o	+	o
CMGOS-Red	o	o	o	+	–
CMGOS-Reg	o	o	o	+	+
CMGOS-MCD	–	–	–	– –	o
HBOS	+	++	o	++	++
rPCA	o	++	+	+	o
oc-SVM	o	+	+	– –	+
η-oc-SVM	o	+	+	– –	o

doi:10.1371/journal.pone.0152173.t006

2.7 Anomalijų aptikimas grafuose

Anksčiau minėti anomalijų aptikimo metodai taikomi tiesiogiai analizuojant srauto duomenis. Dažnai labai svarbūs ryčių tarp tinklo dalyvių parametrai (Šaltinio ir Tikslo IP adresai) nėra analizuojami, nes tai nėra lengvai normalizuojamos vertės, o normalizavus jie mažai atvaizduoja ryšius tarp tinklo elementų (2 paveikslėlis). Tolimesniame tyrime bandysime konvertuoti srautinius duomenis į grafus laiko intervaluose, bei panaudoti žinomus anomalijų aptikimo grafuose metodus (Akoglu, Tong, & Koutra, 2014).



2 pav. Kompiuterių tinklo elementų ryšiai laiko intervaluose.

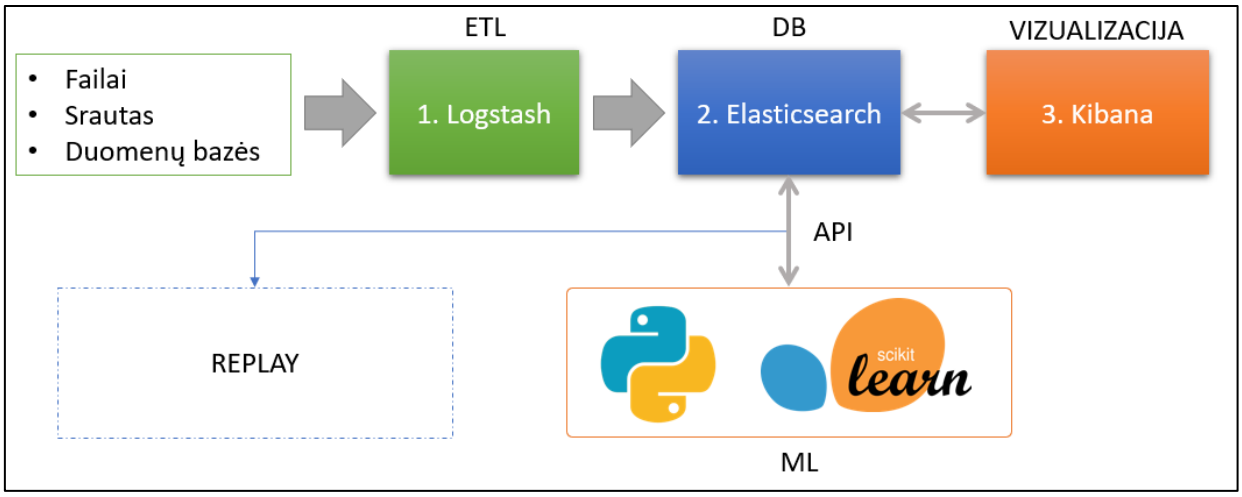
2.8 Duomenų rinkiniai

Tolimesniems tyrimams naudosime viešai prieinamus srauto duomenų rinkinius. CTU-13 (García, Grill, Stiborek, & Zunino, 2014) duomenų rinkinyje yra 13 Botnet kibernetinių takų pavyzdžių. Taip pat ketinama panaudoti UGR-16 (Maciá-Fernández, Camacho, Magán-Carrión, García-Teodoro, & Therón, 2018) duomenų rinkinį. Pastarajame yra keturių mėnesių kompiuterio tinklo srautiniai duomenys su įvairiomis kibernetinėmis atakomis. Taip pat planuojame metodų bandytus atlikti ir realiame didelės organizacijos (~4000 tinklo elementų) kompiuterių tinkle.

2.9 Tyrimų laboratorija

Tolimesniems tyrimams atlikti esame paruošę laboratoriją. Sukurta aplinka leidžia vienodomis sąlygomis išbandyti tyrimui pasirinktus dirbtinio intelekto metodus, ar jų kombinacijas su viešai prieinamais kompiuterių tinklo srautinių duomenų rinkiniais, bei kartoti tyrimus realiu laiku pasirinktuose kompiuterių tinkluose. Principinė laboratorijos schema pateikiama 3 paveikslėlyje.

Laboratorijai panaudota ELK Stack duomenų gavybos, transformavimo, saugojimo komponentės (ELK, 2018), bei scikit biblioteka (scikit-learn, 2018), skirta darbui su daugeliu žinomų dirbtinio intelekto metodų.



3 pav. Tyrimų laboratorijos principinė schema.

2.10 Tolimesnė tyrimo eiga

Tolimesni tyrimai bus vykdomi šia seka:

- Į laboratoriją bus sukelti kiek įmanoma daugiau tinklo srauto duomenų rinkinių.
- Bus bandomi atsirinkti neapmokomi dirbtinio intelekto metodai, matuojami jų tikslumas ir greitis.
- Bus transformuojami srauto duomenys į grafus ir bandomi anomalijų grafuose aptikimo metodai, arba grafų funkcijų rezultatais praturtinami srautiniai duomenys.
- Gautus tyrimų rezultatus publikuoti tarptautiniame recenzuojamame leidinyje.

3. Rezultatai ir išvados

- Nors srauto duomenyse nėra tiek informacijos kiek tinklo srauto paketuose, tolimesniam tyrimui pasirenkama tinklo srauto duomenų struktūra.
- Viešai publikuojami anomalijų kompiuterių tinkluose metodai dažnai neišnaudoja tinklo elementų ryšių informacijos, todėl ketiname išbandyti duomenų konvertavimą į grafus ir vykdyti tyrimus su grafų duomenimis.

4. Literatūra.

Akoglu, L., Tong, H., & Koutra, D. (2014). Graph-based Anomaly Detection and Description: A Survey. *ArXiv:1404.4679 [Cs]*. Gauta http://arxiv.org/abs/1404.4679

Berk, V. (2018). The NetFlow/sFlow®/CFlow/JFlow Flow Dilemma - FlowTraq. Gauta 2018 m. lapkričio 5 d., /resources/whitepapers

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network Anomaly Detection: Methods, Systems and Tools. *IEEE Communications Surveys & Tutorials*, *16*(1), 303–336. https://doi.org/10.1109/SURV.2013.052213.00046

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *41*(3), 1–58. https://doi.org/10.1145/1541880.1541882

CISCO. (2012). Introduction to Cisco IOS NetFlow - A Technical Overview. Gauta 2018 m. lapkričio 5 d., https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

Claise, B. (2008). Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information. Gauta 2018 m. lapkričio 5 d., https://tools.ietf.org/html/rfc5101

ELK. (2018). ELK. Gauta 2018 m. lapkričio 5 d., https://www.elastic.co/elk-stack

García, S., Grill, M., Stiborek, J., & Zunino, A. (2014). An empirical comparison of botnet detection methods. *Computers & Security*, *45*, 100–123. https://doi.org/10.1016/j.cose.2014.05.011

Goldstein, M., & Uchida, S. (2016). A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data. *PLOS ONE*, *11*(4), e0152173. https://doi.org/10.1371/journal.pone.0152173

HUAWEI. (2012). NetStream Configuration. Gauta 2018 m. lapkričio 5 d., http://support.huawei.com/enterprise/docinforeader!loadDocument1.action?contentId=DOC1000019448&partNo=10022#dc_fd_netstream_0002

Juniper Networks. (2018). Flow Monitoring Output Formats - TechLibrary - Juniper Networks. Gauta 2018 m. lapkričio 5 d., https://www.juniper.net/documentation/en_US/junos/topics/concept/flowmonitoring-output-formats-overview-solutions.html

Kissel, R. L. (2013). Glossary of Key Information Security Terms | NIST. *NIST Interagency/Internal Report (NISTIR) - 7298rev2*. http://dx.doi.org/10.1002/https://dx.doi.org/10.6028/NIST.IR.7298r2

Maciá-Fernández, G., Camacho, J., Magán-Carrión, R., García-Teodoro, P., & Therón, R. (2018). UGR‘16: A new dataset for the evaluation of cyclostationarity-based network IDSs. *Computers & Security*, *73*, 411–424. https://doi.org/10.1016/j.cose.2017.11.004

NETFORT. (2014). *Flow Analysis Versus Packet Analysis. What Should You Choose?*

NKSC. (2017). *2016 metų Nacionalinio kibernetinio saugumo būklės ataskaita.* (Metinė). NKSC. Gauta https://kam.lt/download/57062/nksc_metine_ataskaita_uz_2016.pdf

NKSC. (2018). *2017 metų Nacionalinio kibernetinio saugumo būklės ataskaita.* (Metinė). NKSC. Gauta https://kam.lt/download/61258/nksc%20ataskaita_final.pdf

Palo Alto. (2018). How to Break the Cyber Attack Lifecycle - Palo Alto Networks. Gauta 2018 m. lapkričio 5 d., https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

scikit-learn. (2018). scikit-learn: machine learning in Python — scikit-learn 0.20.0 documentation. Gauta 2018 m. lapkričio 5 d., http://scikit-learn.org/stable/

sFlow.org. (2018). About sFlow Overview @ sFlow.org. Gauta 2018 m. lapkričio 5 d., https://sflow.org/about/index.php

VSD, V., & AOTD, A. (2017). *Grėsmių nacionaliniam saugumui vertinimas 2017.* (Metinė). VSD. Gauta https://www.vsd.lt/wp-content/uploads/2017/03/2016-gr%C4%97smi%C5%B3-vertinimas.pdf

VSD, V., & AOTD, A. (2018). *Grėsmių nacionaliniam saugumui vertinimas 2018.* (Metinė). VSD. Gauta https://www.vsd.lt/wp-content/uploads/2018/03/LTU.pdf