Vilniaus Universitetas
Duomenų mokslo ir skaitmeninių technologijų institutas
Kognityvinių skaičiavimų grupė

Metinė ataskaitinė informatikos krypties doktorantų konferencija

Veiklos ataskaita už 2019–2020 m.

Doktorantas – Žydrūnas Vaišnoras (DMSTI-DS-N009-20-11)
Darbo vadovė – prof. dr. Olga Kurasova
Mokslo kryptis – 09 P Informatika
Doktorantūros laikotarpis – 2019-2023 m.

2020-10-22, Vilnius, Lietuva

Disertacijos tema, tyrimo objektas ir tikslai

Preliminari disertacijos tema:

- Mašininio mokymosi metodų vystymas įsilaužimams aptikti kompiuterių tinkluose.

Tyrimo objektas:

- Kompiuterių tinklo įrenginiais sukauptų realaus laiko duomenys;
- Mašininio mokymosi algoritmai įsilaužimams aptikti.

Tyrimo tikslas:

- Išvystyti našesnį mašininio mokymosi algoritmą kibernetiniams įsilaužimams atpažinti kompiuterių tinkluose pritaikant realaus laiko duomenis.

Tyrimo uždaviniai

- Atlikti skirtingų mašininio mokymosi metodų, naudojamų kompiuterių tinklo anomalijoms atpažinti, analizę ir tyrimą;
- Parinkti tyrimo metodiką iškeltiems uždaviniams spręsti;
- Sukurti našesnį mašininio mokymosi metodą anomalijoms atpažinti realaus laiko duomenims;
- Pritaikyti sukurtą mašininio mokymosi modelį realaus laiko duomenims ir atlikti gautų duomenų analizę, rezultatų apibendrinimą, išvadų parengimą.

Mokslinis naujumas

- Sukurtas našesnis mašininio mokymosi modelis įsilaužimams atpažinti realaus laiko duomenims;
- Sukurtas metodas, kuris naudos kuo įmanoma mažiau „nematytų“ kompiuterių tinklo duomenų paketų mašininio mokymosi modelio ap(si)mokymui – anomalijų atpažinimui;
- Mašininio mokymosi modelis bus pritaikomas darbui virtualioje aplinkoje, konteinerizavimo platformose.

2019–2020 m. darbo planas:

Studijų planas:

- Išlaikyti egzaminą „*Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika*“.

Mokslinių tyrimų ir disertacijos rengimo planas:

- Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):
    - Disertacijos tyrimo objekto detalizavimas;
    - Atlikti mašininio mokymosi metodų taikymo kompiuterių tinkluose analitinę apžvalgą;
    - Nustatyti (identifikuoti) mokslines problemas, kylančias uždaviniuose, susijusiuose su anomalijų aptikimu kompiuterių tinkluose taikant mašininio mokymosi metodus;
    - Tyrimo tikslo suformavimas.

Veiklos ataskaita už 2019–2020 m. (1)

2019–2020 m. išlaikyti egzaminai:

- Išlaikytas egzaminas „*Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika*“
  Vertinimo komisija: doc. dr. Audronė Lupeikienė (komisijos pirmininkas), prof. dr. Saulius Gudas ir dr. Virginijus Marcinkevičius.

2019–2020 m. dalyvavimas mokslinėse konferencijose:

- Dalyvauta mokslinėje konferencijoje: „*Data Analysis Methods for Software Systems 2019*“, vykusioje Druskininkuose, Lietuvoje. Konferencijos metu gilinau žinias mašininio mokymosi srityse.

Veiklos ataskaita už 2019–2020 m. (2)

2019–2020 m. dalyvavimas konferencijose:

- Sudalyvauta konferencijoje: „*Palo Alto Ignite Europe ’19*“, vykusioje Barselonoje, Ispanijoje. Konferencijos metu gilinau žinias apie anomalijų aptikimą naujos kartos ugniasienėse (angl.*next-generation firewall*, NGFW). Įgijau patirties konfigūruodamas laboratorijoje kompiuterių tinklų duomenų srauto apsaugos priemones;
- Dalyvauta konferencijoje: „*CISCO Live! ’20*“, vykusioje Barselonoje, Ispanijoje. Konferencijos metu gilinau žinias apie mašininio mokymosi metodų pritaikymą siekiant aptikti anomalijas kompiuterių tinkluose. Taip pat buvo susipažįstama su naujausių technologijų taikymu kompiuterių tinkluose – jų privalumai ir saugumo grėsmės.

Veiklos ataskaita už 2019–2020 m. (3)

2019–2020 m. gauti moksliniai rezultatai:

- Nustatyti tyrimo tikslai, objektas, uždaviniai;
- Nustatytos papildomos mokslinės problemos, kylančios uždaviniuose, susijusiuose su anomalijų aptikimais kompiuterių tinkluose taikant mašininio mokymosi metodus;
- Atlikta mašininio mokymosi metodų taikymo kompiuterių tinkluose apžvalga;
- Publikacijų, susijusių su anomalijų, jų aptikimais lokaliuose ir globaliuose kompiuterių tinkluose, tyrimas, jo detalizavimas;
- Sukurtas pirminis prototipas duomenų kompiuterių tinkluose kaupimui, saugojimui, atvaizdavimui. Pritaikytas mašininio mokymosi algoritmas apsimokymui.

2020–2021 m. darbo planas (1):

Studijų planas:

- Išlaikyti egzaminus:
  - „*Fundamentalieji informatikos ir informatikos inžinerijos metodai* “;
  - „*Gilieji neuroniniai tinklai* “.

Rezultatų pristatymo planas:

- Pristatyti mokslinio darbo rezultatus:
  - „*International Science Conference on Computer Networks CN2021*“, vyksiančioje Gdanske, Lenkijoje, birželio mėn. Pranešimas: „Application of Machine Learning Methods for Intrusion Detection in Computer Networks“.

2020–2021 m. darbo planas (2):

Mokslinių tyrimų planas:

Tyrimo metodikos sudarymas:

- Tyrimo metodikos iškeltiems uždaviniams spręsti parinkimas;
- Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką.

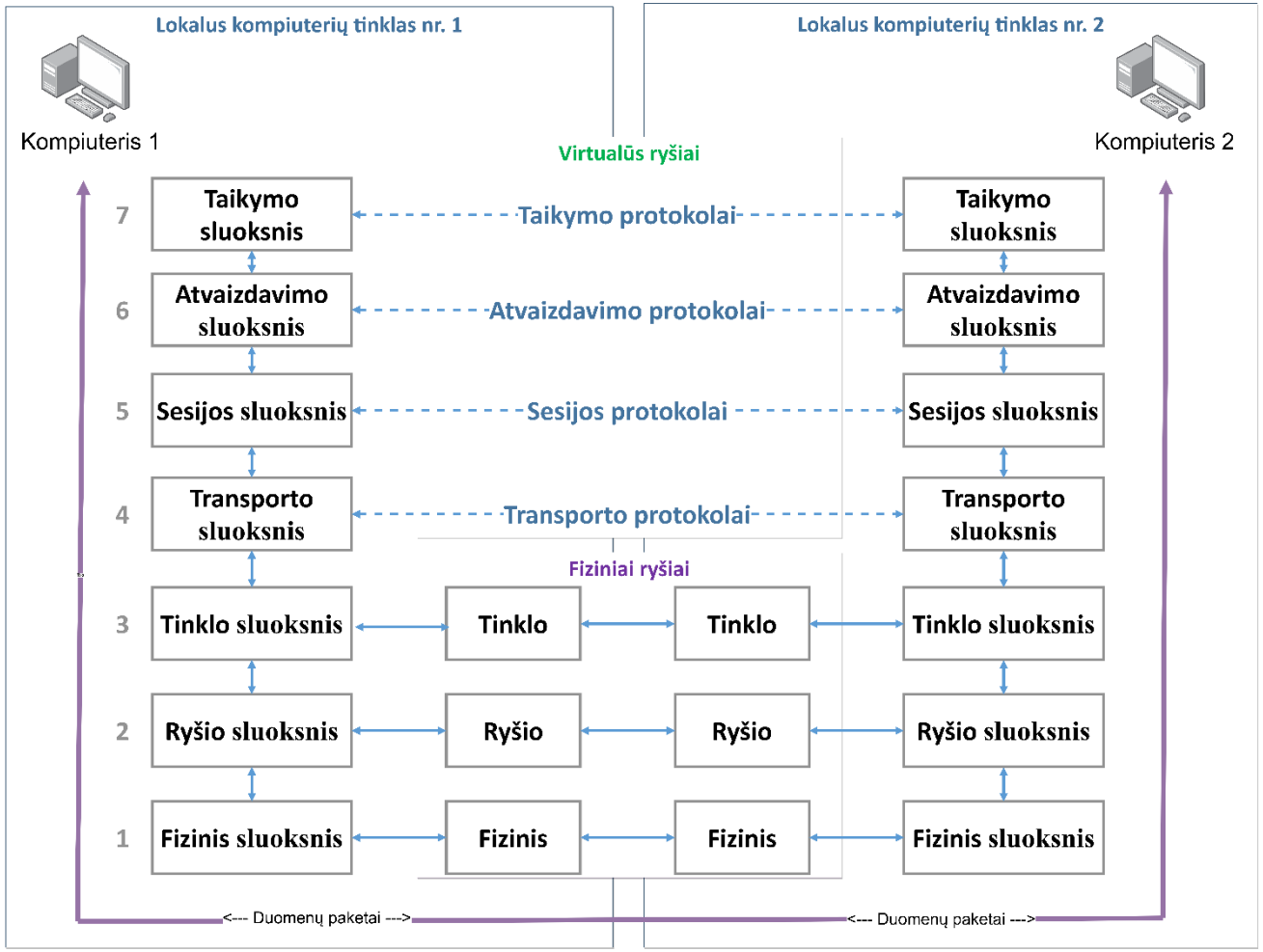
Teorinis tyrimas:

- Mašininio mokymosi metodų, naudojamų kompiuterių tinkluose anomalijoms aptikti, tyrimas;
- Anomalijų atpažinimo mašininio mokymosi metodo sukūrimas ir/ar testavimas.

Pedagoginis darbas 2019–2020 m.

- „*Kompiuterių tinklai*“ paskaitų dėstymas Vilniaus universiteto (VU) informacinių sistemų inžinerijos (ISI) bakalauro studentams.

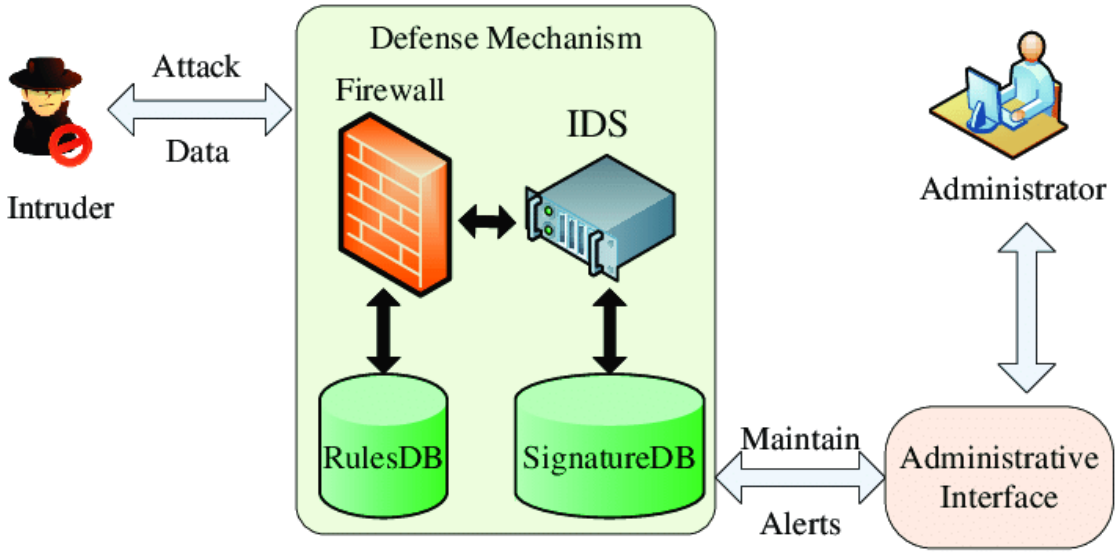
OSI modelis


Lokalus kompiuterių tinklas nr. 1
Lokalus kompiuterių tinklas nr. 2
Kompiuteris 1
Kompiuteris 2
Virtualūs ryšiai
7
Taikymo sluoksnis
Taikymo protokolai
Taikymo sluoksnis
6
Atvaizdavimo sluoksnis
Atvaizdavimo protokolai
Atvaizdavimo sluoksnis
5
Sesijos sluoksnis
Sesijos protokolai
Sesijos sluoksnis
4
Transporto sluoksnis
Transporto protokolai
Transporto sluoksnis
Fiziniai ryšiai
3
Tinklo sluoksnis
Tinklo
Tinklo
Tinklo sluoksnis
2
Ryšio sluoksnis
Ryšio
Ryšio
Ryšio sluoksnis
1
Fizinis sluoksnis
Fizinis
Fizinis
Fizinis sluoksnis
<--- Duomenų paketai --->
<--- Duomenų paketai --->

Žymėmis paremtas IDS

Žymėmis paremtoje įsilaužimų aptikimo sistemoje (angl. *Signatrue-based IDS*) yra stebimi kompiuterių tinklo paketai, kurie yra lyginami su duomenų bazėje turimomis žymėmis ir/ar parašais, kurie yra nustatyti kaip kenkėjiškos grėsmės. Sutapimas tarp paketų antraščių (angl. *headers*) gali būti tikrinamas naudojant klasifikavimo techniką.

Kai kuriuose literatūros šaltiniuose šis IDS vadinamas netinkamu naudojimusi (angl. *misuse*) įsilaužimų aptikimo sistema.



https://www.researchgate.net/publication/328037690_Performance_Analysis_of_Honeypot_with_Petri_Nets

Informacijos saugumas (CIA)

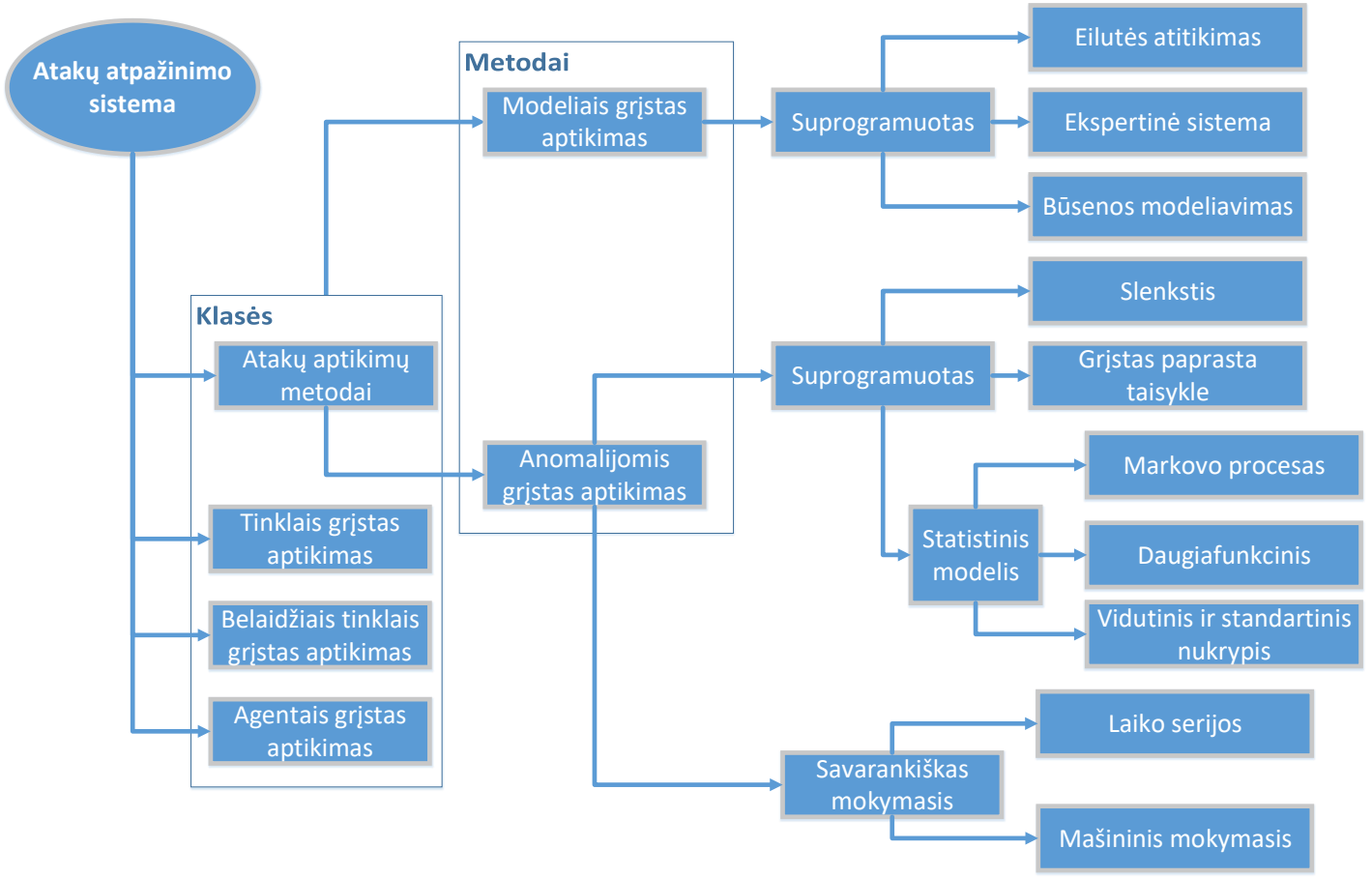
Kompiuterių tinklų saugumas, įskaitant anomalijų aptikimą, padeda palaikyti informacijos saugumą.

Informacijos saugumo spektras skirstomas į tris pagrindinius aspektus, kuriuos :

- Informacijos **konfidencialumą** – informacijos apsaugą nuo nesankcionuoto atskleidimo;
- Informacijos **vientisumą** – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;
- Informacijos **prieinamumą** – užtikrinimą, kad informacija prieinama tada, kai ji yra reikalinga.

Šis informacijos saugumo modelis taip pat žinomas/vartojamas kaip CIA (Confidentiality, Integrity, Availability).

Atakų atpažinimo sistema (IDS)



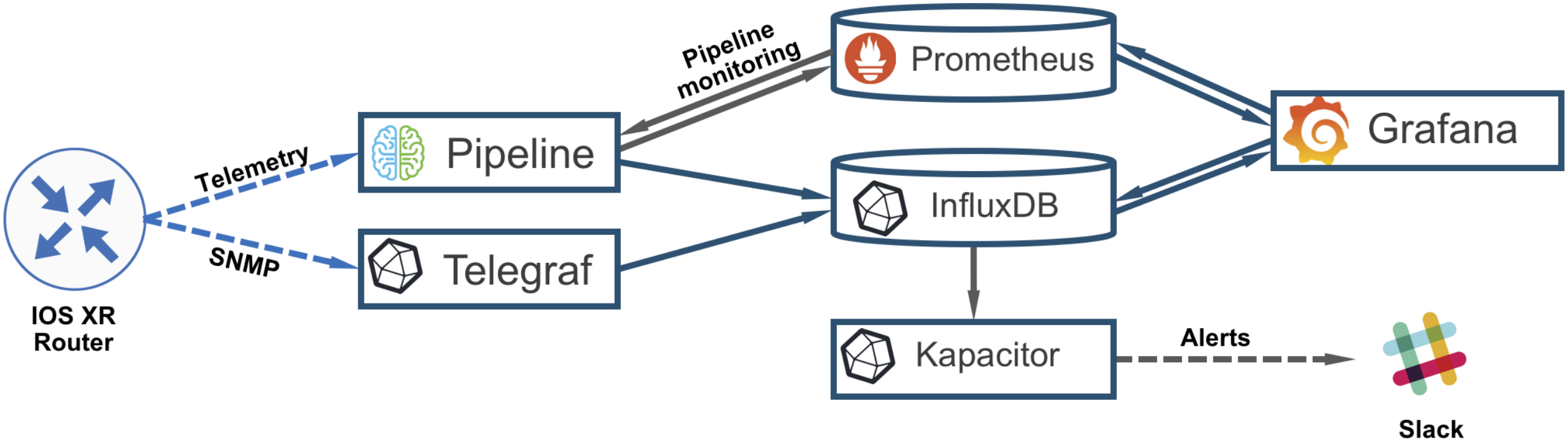
TICK stekas

TICK stekas (angl. *TICK stack*) – tai atviro kodo komponenčių platforma patogiam milžiniškiems laiko eilučių (metrikų, įvykių) duomenų kaupimui, saugojimui, atvaizdavimui ir stebėjimui.

TICK steką sudaro komponentai:

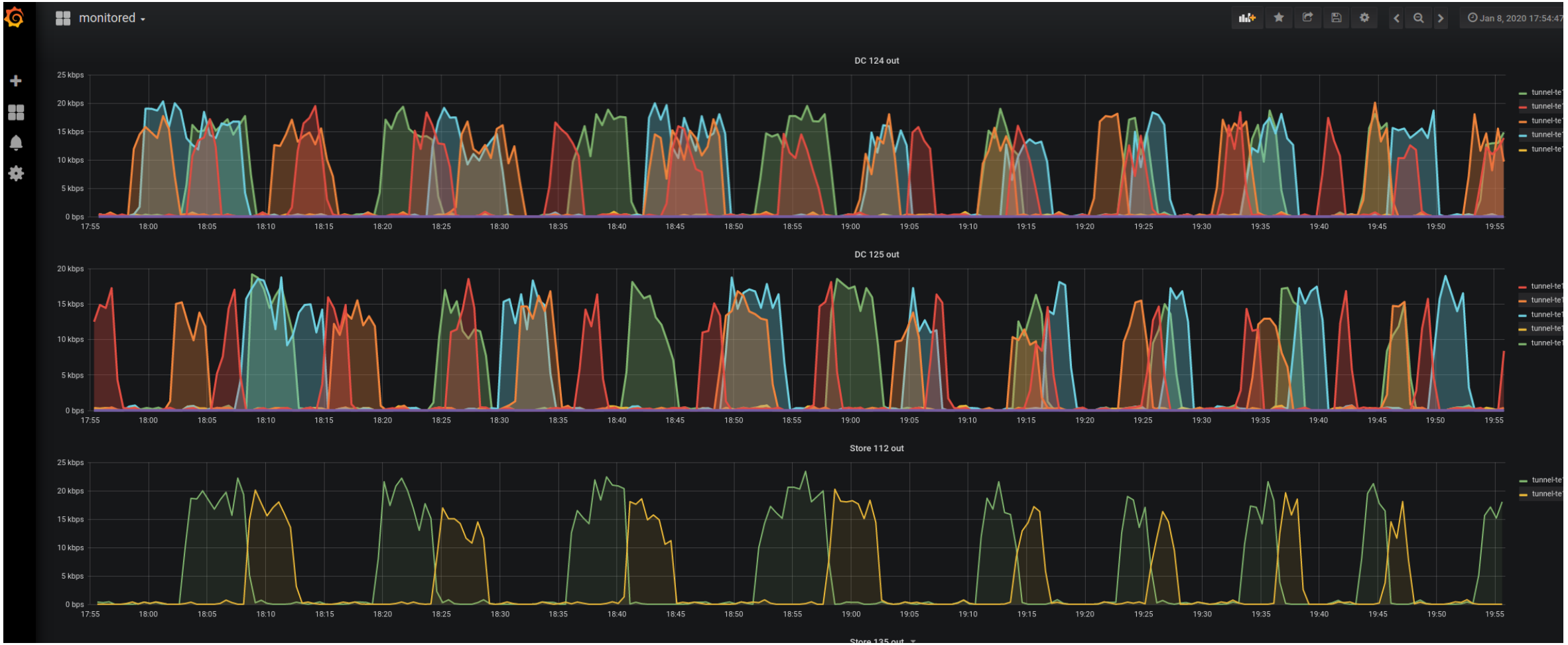
- **Telegraf** – serverio agentas skirtas metrikų rinkimui ir pateikimui;
- **InfluxDB** – didelio našumo laiko eilučių duomenų bazė;
- **Chronograf** – platformos vartoto sąsaja (duomenų atvaizdavimas);
- **Kapacitor** – duomenų apdorojimo sistema skirta srautinių ir paketinių duomenų apdorojimui iš „InfluxDB“.

Telemetrija



https://github.com/vosipchu/XR_TCS/blob/master/docs/topology.png

Duomenų rinkinio atvaizdavimas (Grafana)



Vilnius University

Ačiū