Vilniaus Universitetas
Duomenų mokslo ir skaitmeninių technologijų institutas
Kognityvinių skaičiavimų grupė

Ataskaitinė informatikos krypties doktorantų konferencija

Veiklos ataskaita už 2020-10 – 2021-03

Žydrūnas Vaišnoras (DMSTI-DS-N009-20-11)

2021-03-26, Vilnius, Lietuva

Doktorantūros studijos

- Disertacijos pavadinimas – Mašininio mokymosi metodų vystymas įsilaužimams aptikti kompiuterių tinkluose
- Doktorantas – Žydrūnas Vaišnoras (DMSTI-DS-N009-20-11)
- Darbo vadovė – prof. dr. Olga Kurasova
- Mokslo kryptis – 09 P Informatika
- Doktorantūros laikotarpis – 2019-2023 m.
- Studijų metai – 2021 m. (II)

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.

Planuojamas 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.

VISŲ STUDIJŲ PLANAS IR JO VYKDYMO SUVESTINĖ

Studijų metai	Egzaminai		Dalyvavimas konferencijose		Publikacijos		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta	Būklė [4]
I (2019/2020)	1	1					
II (2020/2021)	**2**	**1**	**1**				
III (2021/2022)	1		2		1		
IV (2022/2023)					1		

ATASKAITINIŲ METŲ DARBO PLANAS IR JO ĮVYKDYMAS

Egzaminai		Dalyvavimas konferencijose		Publikacijos	
Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta
Fundamentalieji informatikos ir informatikos inžinerijos metodai	Išlaikyta: Fundamentalieji informatikos ir informatikos inžinerijos metodai	Dalyvauti tarptautinėje mokslinėje konferencijoje „International Science Conference on Computer Networks CN2021“	Suplanuota konferencija atšaukta dėl COVID-19 pandemijos. Vietoje jos suplanuota dalyvauti ITMS’2021 konferencijoje 2021 m. spalio mėn.		

MOKSLINIŲ TYRIMŲ IR DISERTACIJOS RENGIMO ETAPAI (1)

	Darbo pavadinimas	Atlikimo terminai	Pastabos
1.	**Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):** 1.1. Disertacijos tyrimo objekto detalizavimas. 1.2. Atlikti mašininio mokymosi metodų taikymo kompiuterių tinkluose analitinę apžvalgą. 1.3. Nustatyti (identifikuoti) mokslines problemas, kylančias uždaviniuose, susijusiuose su anomalijų aptikimu kompiuterių tinkluose taikant mašininio mokymosi metodus. 1.4. Tyrimo tikslo suformavimas.	2019 m. spalio mėn. – 2020 m. rugsėjo mėn.	Atliktas disertacijos tyrimo objekto detalizavimas, nustatytos mokslinės problemos ir suformuotas tyrimo tikslas.

MOKSLINIŲ TYRIMŲ IR DISERTACIJOS RENGIMO ETAPAI (2)

	Darbo pavadinimas	Atlikimo terminai	Pastabos
2.	Mokslinio tyrimo vykdymas: ---------- **2.1. Tyrimo metodikos sudarymas:** 2.1.1. Tyrimo metodikos iškeltiems uždaviniams spręsti parinkimas; 2.1.2. Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką. ---------- **2.2. Teorinis tyrimas:** 2.2.1. Mašininio mokymosi metodų, naudojamų kompiuterių tinkluose anomalijoms aptikti, tyrimas. 2.2.2. Anomalijų atpažinimo mašininio mokymosi metodo sukūrimas ir/ar testavimas. ---------- **2.3. Empirinis tyrimas:** 2.3.1. Sudarytų metodų pritaikymas praktinių uždavinių sprendimui. 2.3.2. Gautų duomenų analizė, rezultatų apibendrinimas, išvadų parengimas.	2020 m. spalio mėn. 2020 m. lapkričio mėn. – 2021 m. rugsėjo mėn. 2021 m. spalio mėn. – 2022 m. gegužės mėn. 2022 m. birželio mėn. – 2022 m. rugsėjo mėn.	Atliktas disertacijos tyrimo objekto detalizavimas, nustatytos mokslinės problemos ir suformuotas tyrimo tikslas.

Disertacijos tema, tyrimo objektas ir tikslai

Disertacijos tema:

- Mašininio mokymosi metodų vystymas įsilaužimams aptikti kompiuterių tinkluose.

Tyrimo objektas:

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

Tyrimo tikslas:

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

Per pusmetį gautų mokslinių darbų rezultatai

- Atlikta gilesnė literatūros analizę apimant, bet neapsiribojant, naujesnius mašininio mokymosi metodus. Literatūros analizėje pateiktos teorinių tyrimų išvados ir jų taikymo galimybės geresniam mašininio mokymosi metodo vystymui.
- Buvo nagrinėjamos aktyvinės kompiuterių tinklo įrangos techninės specifikacijos siekiant sukurti našesnį prototipą fizinėje kompiuterių tinklo laboratorijoje.
- Buvo gilinamasi į kompiuterių tinklų paketų struktūrą, išsiaiškinta kaip paketų antraštės informacija, požymiai, turi būti tinkamai apdorojami (angl. *pre-processing*) pritaikant mašininio mokymosi metodams.

Mokslinių darbai kitam pusmečiui

- Įsibrovimų aptikimo indikatorių (angl. *Indicator of compromise*, IoC) duomenų bazių nagrinėjamas, jų apdorojimas ir panaudojimas siekiant eliminuoti kuo įmanoma daugiau įsilaužimo atakų.
- Toliau bus gilinamasi į fizinės kompiuterių tinklo ir virtualių mašinų laboratorijos sukūrimą ir taikymą disertacijos iškeltiems uždaviniams įvykdyti. Laboratorija bus naudojama siekiant taikyti ir plėtoti mašininio mokymosi metodą įsilaužimams kompiuterių tinkluose aptikti su realiais laiko duomenimis (įprasti paketai ir anomalijos).
- Bus pradėtas kurti anomalijų atpažinimo mašininio mokymosi metodas esamiems duomenų rinkiniams pritaikyti, kurį vėliau būtų galima taikyti realiems laiko duomenims.

Vilnius University

Ačiū