Vilniaus Universitetas
Duomenų mokslo ir skaitmeninių technologijų institutas
Kognityvinių skaičiavimų grupė

Ataskaitinė informatikos krypties doktorantų konferencija

Veiklos ataskaita už 2021-10 – 2022-03

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

2022-03-24, 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 – 2022 m. (III)

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.

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.

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
I (2019/2020)	1	1					
II (2020/2021)	2	2	1	0			
III (2021/2022)	**1**	**1**	**1 + 1 (skola iš II metų)**	**1 (skola)**	**1**		Rašoma publikacija
IV (2022/2023)					1		
Iš viso:	4	4	2	1	2		

ATASKAITINIŲ METŲ DARBO PLANAS IR JO ĮVYKDYMAS (1)

Egzaminai		
Planas	**Įvykdyta**	**Būklė**
Mašininis mokymasis	Egzaminas – Mašininis mokymasis, egzamino data 2022-02-21	Išlaikytas

ATASKAITINIŲ METŲ DARBO PLANAS IR JO ĮVYKDYMAS (2)

Dalyvavimas konferencijose		
Planas	**Įvykdyta**	**Konferencijos tipas**
10th World Conference on Information Systems and Technologies, 2022-04-12, Budva (Juodkalnija)	Autoriai: Žydrūnas Vaišnoras ir prof. dr. Olga Kurasova. Pranešimo pavadinimas – Techniques Involved in the Development of the New Dataset for Anomaly Detection in Computer Networks. Konferencijos pavadinimas – 10th World Conference on Information Systems and Technologies. Konferencijos data 2022-04-12/15. Konferencijos vieta – Budva (Juodkalnija) ir „online“. Straipsnis bus spausdinamas tarptautiniame moksliniame žurnale „Springer“.	Tarptautinė konferencija

ATASKAITINIŲ METŲ DARBO PLANAS IR JO ĮVYKDYMAS (3)

Dalyvavimas konferencijose			
Planas	**Įvykdyta**	**Būklė**	**Publikacijos tipas**
Proceedings of 10th World Conference on Information Systems and Technologies.	Vaišnoras Ž., Kurasova O. (2022). Techniques Involved in the Development of the New Dataset for Anomaly Detection in Computer Networks. Proceedings of 10th World Conference on Information Systems and Technologies. Lecture Notes in Networks and Systems. Springer.	Priimta	Konferencijų medžiaga

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)

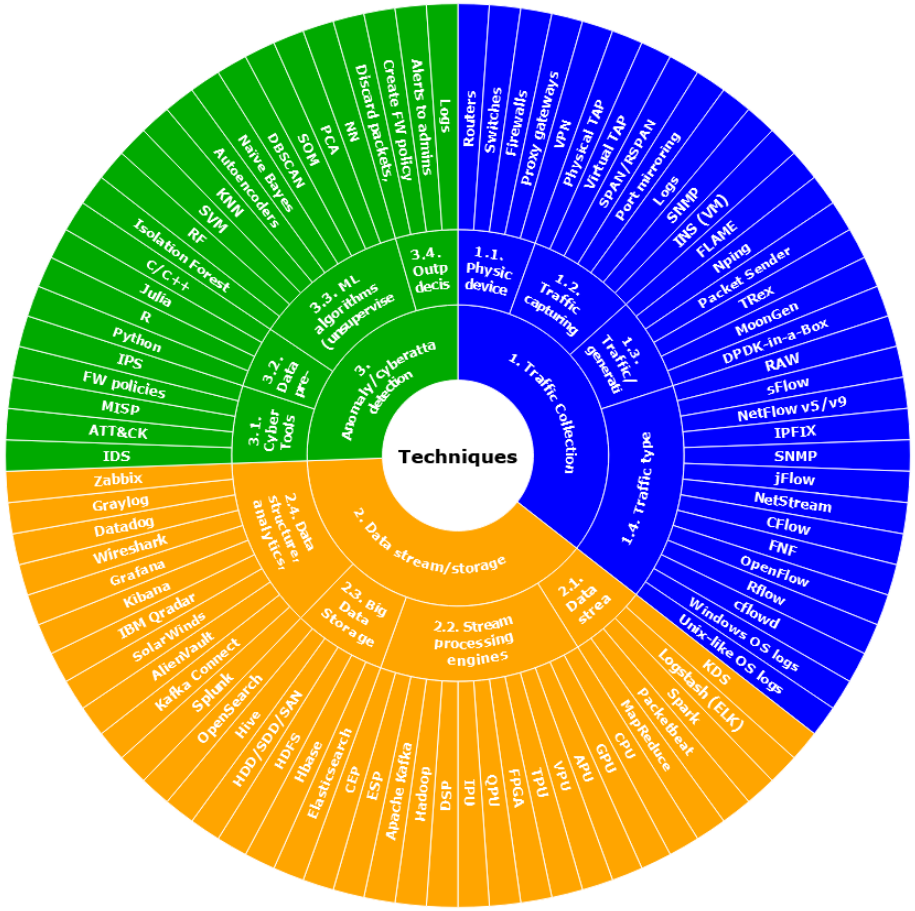
	Darbo pavadinimas	Atlikimo terminai	Pastabos
2.	Mokslinio tyrimo vykdymas: ---------- 2.1. Tyrimo metodikos sudarymas: 2.1.1. Tyrimo metodikos iškeltiems uždaviniams spręsti parinkimas; 2.1.2. Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką. ---------- 2.2. Teorinis tyrimas: 2.2.1. 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 teorinis tyrimas – sukurtas naujas metodas dideliems kompiuterių tinklo duomenims rinkti, kaupti apdoroti ir pritaikyti mašininio mokymosi algoritmams.**

MOKSLINIŲ TYRIMŲ IR DISERTACIJOS RENGIMO ETAPAI (3)

Darbo pavadinimas		Atlikimo terminai	Pastabos
3.	Atskirų daktaro disertacijos dalių (tyrimo metodikos, rezultatų, ginamų teiginių, išvadų, ir kt.) parengimas: 3.1. Tikslų, uždavinių, tyrimo metodikos, ginamųjų teiginių patikslinimas; 3.2. Analitinės disertacijos dalies parengimas; 3.3. Teorinės disertacijos dalies parengimas; 3.4. Eksperimentinės disertacijos dalies parengimas; 3.5. Bendrųjų išvadų formulavimas	2022 m. spalio mėn. – 2023 m. gegužės mėn.	
4.	Daktaro disertacijos parengimas ir svarstymas padalinyje	2023 m. birželio mėn.	
5.	Daktaro disertacijos gynimas	2023 m. rugsėjo mėn.	

Per pusmetį gautų mokslinių darbų rezultatai (1)

- Parašytas, pateiktas ir priimtas spausdinimui (full paper) mokslinė publikacija konferencijų medžiagai:
  Vaišnoras Ž., Kurasova O. (2022). Techniques Involved in the Development of the New Dataset for Anomaly Detection in Computer Networks. Proceedings of 10th World Conference on Information Systems and Technologies. Lecture Notes in Networks and Systems. Springer;



Per pusmetį gautų mokslinių darbų rezultatai (2)

- Buvo analizuota literatūra apie kompiuterių tinklo įprastų ir kenkėjiškų duomenų srautų pagrindinių požymių skirtumus, jų klasifikavimo problematikas. Nustatyta, kad įprastame TCP/IP steko kompiuterių tinkle nėra aiškaus ir konkretaus skirtumo, kuris leistų lengvai atskirti kompiuterių tinklų „geruosius“ paketus, nuo „blogųjų“ (anomalijos);
- Taip pat buvo stengiamasi atlikti empirinį tyrimą remiantis atliktu teoriniu tyrimu – sukurti naują metodą dideliems kompiuterių tinklo duomenims rinkti, kaupti, apdoroti ir pritaikyti šį metodą mašininio mokymosi algoritmams. Praktinis tyrimas nepavyko – rezultatų nėra, nes nepavyko pritaikyti turimas žinias ir technologijas;

Per pusmetį gautų mokslinių darbų rezultatai (3)

- Buvo analizuojama mokslinė literatūra ir technologijų gamintojų tinklalapiai apie duomenų konteinerizavimo ir mikrosegementavimo procesus, duomenų srautų judėjimą juose ir jų saugumą. Šios technologijos yra naujos ir įgalinančios atlikti greitesnius duomenų saugojimo ir apdorojimo darbus.

Mokslinių darbai kitam pusmečiui (1)

- Bus gilinimąsi ir siekiama susisteminti kompiuterių tinklo įprastų ir kenkėjiškų duomenų srautų pagrindinių požymių skirtumus, jų klasifikavimo problematikas;
- Bus analizuojama mokslinė literatūra apie duomenų konteinerizavimo ir mikrosegementavimo procesus, duomenų srauto judėjimą juose ir jų saugumą;
- Bus siekiama išvystyti našesnį mašininio mokymosi algoritmą pritaikant teorinio tyrimo metu sukurtą metodą, kuris gebėtų išsaugoti didžiulius generuojamus srautus, apdoroti/paruošti sukauptus duomenis ir pritaikyti juos mašininio mokymosi algoritmams siekiant nustatyti nematytas (angl. *zero day*) kibernetines atakas kompiuterių tinkluose.

Mokslinių darbai kitam pusmečiui (2)

Studijų metai	Egzaminai	Dalyvavimas konferencijose	Publikacijos
III, 2022 m.		**2**	**1**

- Dalyvauti tarptautinėje konferencijoje „10th World Conference on Information Systems and Technologies“ (WorldCIST‘22), kurioje pristatysiu mano priimtą darbą;
- Pabaigti kurti, pateikti medžiagą (angl. *Proceeding*) konferencijai „12th International Conference on Advanced Computer Information Technologies“ ir pristatyti joje savo pateiktą medžiagą;
- Mokslinio straipsnio rašymas ir ruošimas jį pateikti į žurnalą su cituojamumo rodikliu.

Akademiniai darbai kitam pusmečiui (1)

- Vadovavimas bakalauro baigiamojo darbui Vilniaus universiteto (VU) informacinių sistemų inžinerijos (ISI) bakalauro studentui;
- Išnagrinėti, įsisavinti ir pritaikyti Vilniaus universiteto (VU) Matematikos ir Informatikos (MIF) fakulteto įsigytą Kibernetinio Saugumo Mobilųjį Modulį (KSMM) savo disertacijos uždaviniui išspręsti, įgyti patirties vykdant kibernetinės gynybos pratybos scenarijus. Taip pat pritaikyti/panaudoti/paruošti KSMM‘ą sekančių mokslo metų dėstomo dalyko pratyboms.

Vilnius University

Ačiū