Универзитет у Београду
Електротехнички факултет

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Реферат о урађеној докторској дисертацији кандидата Жуме Ибрахима (Juma Ibrahim), магистра електротехничких наука.

Одлуком бр. 5051/14-3 од 23.06.2022. године именовани смо за чланове Комисије за преглед, оцену и одбрану докторске дисертације кандидата Жуме Ибрахима под насловом

АРХИТЕКТУРА СИСТЕМА ЗА ПРЕПОЗНАВАЊЕ НЕПРАВИЛНОСТИ У МРЕЖНОМ САОБРАЋАЈУ ЗАСНОВАНО НА АНАЛИЗИ ЕНТРОПИЈЕ

После прегледа достављене дисертације и других пратећих материјала, Комисија је сачинила следећи

Р Е Ф Е Р А Т

1. УВОД

1.1. Хронологија одобравања и израде дисертације

Жума Ибрахим је стекао академски назив магистра електротехничких наука за област Рачунарске технике и информатике на Електрохничком факултету у Београду. Магистарску тезу под насловом „Оперативни системи у реалном времену“ је одбранио 1997. године.

Жума Ибрахим је 2014. године уписао докторске академске студије на Електротехничком факултету Универзитета у Београду, на модулу Рачунарска техника и информатика.

Жума Ибрахим је 30.4.2019. године пријавио тему за израду докторске дисертације под називом „Архитектура система за препознавање неправилности у мрежном саобраћају засновано на анализи ентропије“ уз сву пратећу документацију (образложење теме, биографија, списак објављених радова, изјава да кандидат није пријављивао предложену тему на било којој другој високошколској установи у земљи или иностранству, уверење о положеним испитима).

Научно-наставно веће је на седници бр. 840 од 14.5.2019. донело одлуку о именовању Комисије за оцену научне заснованости теме докторске дисертације, у саставу др Зоран Јовановић, редовни професор, Универзитет у Београду – Електротехнички факултет, др Зоран Шеварац, ванредни професор, Универзитет у Београду – Факултет организационих наука, др Горан Квашчев, ванредни професор, Универзитет у Београду – Електротехнички факултет, док је за ментора докторске дисертације је предложен др Славко Гајин, ванредни професор, Универзитет у Београду - Електротехнички факултет (одлука бр.: 5051/14-1, датум: 23.5.2019).

Јавна усмена одбрана предложене теме докторске дисертације спроведена је 19.6.2019. године на Електротехничком факултету Универзитета у Београду. Кандидат је на јавној усменој одбрани предложене теме докторске дисертације добио оцену: задовољава, након

чега је 20.8.2019. године поднела позитиван извештај о подобности теме и дала предлог да се прихвати тема докторске дисертације и приступи њеној изради.

Наставно-научно веће Електротехничког факултета усвојило је извештај комисије за оцену услова и прихватање теме докторске дисертације (одлука бр. 5051/14-2 од 17.09.2019. год.), на основу чега је Веће научних области техничких наука Универзитета у Београду дало је сагласност на предлог теме докторске дисертације и одређивање проф. др Славка Гајина за ментора (одлуке бр. 61206-4338/2-19 од 28.10.2019. год.).

На основу члана 101. Статута Универзитета у Београду, члана 74. Статута Универзитета у Београду-Електротехничког факултета и захтева кандидата, одобрено је продужење рока за завршетак студија до истека троструког броја школских година потребних за реализацију уписаног студијског програма.

Кандидат Жума Ибрахим је предао докторску дисертацију на преглед и оцену 30.05.2022. године. На седници одржаној 7.6.2022. године, Комисија за студије трећег степена је потрврдила испуњеност потребних услова за подношење предлога Наставно-научном већу Електротехничког факултета за формирање комисије за преглед и оцену докторске дисертације.

Наставно-научно веће Електротехничког факултета је на седници одржаној дана 14.6.2022. године именовало Комисију за преглед и оцену дисертације (број одлуке 5051/14-3 од 23.6.2022. године) коју чине:

- др Славко Гајин, ванредни професор, Универзитет у Београду – Електротехнички факултет, ментор
- др Мило Томашевић, редовни професор, Универзитет у Београду – Електротехнички факултет
- др Мирослав Марић, редовни професор, Универзитет у Београду – Математички факултет.

1.2. Научна област дисертације

Докторска дисертација кандидата Жуме Ибрахима под насловом „Архитектура система за препознавање неправилности у мрежном саобраћају засновано на анализи ентропије“ припада научној области *Техничких наука – Електротехника и рачунарство*, а ужа научна област је *Рачунарска техника и рачунарство*, за коју је Електротехнички факултет Универзитета у Београду матичан.

Именовани ментор докторске дисертације је проф. др Славко Гајин, ванредни професор на катедри за рачунарску технику и информатику на Електротехничком факултету Универзитета у Београду са 25% ангажовања, где се активно бави истраживањем из наведене научне области. Тренутно је ангажован у настави на предметима из области рачунарских мрежа на основним, мастер и докторским студијама, при чему је ангажован на предметима: „Рачунарске мреже 1“, „Пројектовање рачунарских мрежа“ и „TCP/IP архитектура“. Његов основни истраживачки рад усмерен је на управљање и мониторинг рачунарских мрежа, укључујући сигурносне аспекте рада рачунарских мрежа и сервиса. Учесник је већег броја међународних пројеката, укључујући и пројекат из програма ЕУРЕКА под називом „Систем за детекцију аномалија у мрежном саобраћају на бази анализе NetFlow података“, а који се непосредно односи на предмет дисертације. Објавио је преко 45 радова, од којих је 10 у међународним часописима са SCI листе. Објавио је уџбеник под називом „Принципи конфигурисања рачунарских мрежа“ из предмета „Пројектовање рачунарских мрежа“, који се користи у настави. Др Славко Гајин је са 75% ангажовања запослен на Универзитету у Београду на позицији директора Рачунарског центра Универзитета у Београду (РЦУБ).

1.3. Биографски подаци о кандидату

Јума Ибрахим је рођен 8. децембра 1965. године у Либији, у граду Алријахина. Основне студије завршио је на Природно-математичком факултету Универзитета у Триполију, смер рачунарство.

Завршио је магистарске студије на Универзитету у Београду – Електротехничком факултету, где је 1997. године одбранио магистарски рад под називом „Оперативни системи у реалном времену“, са тежиштем на њиховој примени у научно-истраживачким институцијама.

Од маја 1989. до марта 2006. године био је запослен у Истраживачком центру у Триполију на радном месту програмера, где је радио на имплементацији софтверског система, инсталацији и одржавању софтвера и рачунара, као и обуци за различите врсте корисничких апликација и програмских језика.

У периоду од јуна 2006. до новембра 2013. године био је запослен на Високој школи рачунарске технологије Триполи у Либији као асистент у настави. У том периоду био је директор канцеларије за научно-наставне послове на Високој школи рачунарске технологије у Триполију. Такође је држао предавања из различитих рачунарских области и био CCNA инструктор у оквиру Цисцо мрежне академије Триполи (Cisco Network Academy Tripoli) и Циско мрежне академије Иљела (Cisco Network Academy Injella) у Либији.

Академске докторске студије уписао је 2014. године на Универзитету у Београду – Електротехничком факултету, на модулу Рачунарска техника и информатика. Током студија успешно је положио све прописане испите са оценом 9,8, од чега 9 стручних предмета са оценом 10, и постигао 120 ЕСПБ бодова. Током докторских студија спроводи истраживачки рад на широком спектру технологија рачунарских мрежа, истражујући софтверски дефинисане мреже (SDN) да би се након тога фокусирао на област безбедности рачунарских мрежа. Истраживања у овој области су усмерена на системе за детекцију напада заснованих на ентропији и машинском учењу, из којих је аутор једног научног рада објављеног у стручном часопису из предметне области са SCI листе, као и аутор или коаутор у шест научних радова објављен и представљен на међународним стручним конференцијама.

2. ОПИС ДИСЕРТАЦИЈЕ

2.1. Садржај дисертације

Докторска дисертација под насловом „Архитектура система за препознавање неправилности у мрежном саобраћају засновано на анализи ентропије“ је написана на укупно 90 страна текста на енглеском језику, са 30 слика, 9 табела и 17 нумеричких једначина. Дисертација по форми и структури потпуно одговара Упутству за обликовање докторске дисертације Универзитета у Београду.

Дисертација садржи насловну страну на енглеском и на српском језику, страну са информацијама о ментору и члановима комисије, захвалницу, посвету, апстракт рада на енглеском и на српском језику, списак скраћеница, списак слика, списак табела, садржај, 8 поглавља укључујући и литературу са 119 библиографских референци, уз приложену биографију кандидата, прилог којим је обухваћен списак радова везаних за истраживање и попуњене и потписане одговарајуће изјаве (Изјава о ауторству, Изјава о истоветности штампане и електронске верзије докторског рада и Изјава о коришћењу).

2.2. Кратак приказ појединачних поглавља

Прво поглавље обухвата уводна разматрања и осврт на основне идеје, мотивацију и циљеве који су иницирали истраживање представљено у овој дисертацији. Дефинисан је основни концепт система за детекцију напада и аномалија, дат је прегледни приказ основних категорија ових система, као и изазова који се пред њих постављају. Након тога, дат је кратак осврт на предмет истраживања, представљени су основни циљеви и значај истраживања, да би се затим представиле основне хипотезе на којима се заснива истраживање.

Поглавље 2 даје приказ проблема који се истражују у овој области, као и детаљан преглед научних радова који су обележили најзначајније приступе решавању проблема. Поглавље тематски полази од приказа референтне литературе која се односи на опште проблеме у области детекције напада дајући преглед решења заснованим на машинском учењу, а затим се фокус помера на решења која се заснивају на коришћењу ентропије као мере уједначености структуре мрежног саобраћаја, са посебном применом на подацима који се добијају путем NetFlow протокола.

У **поглављу 3** је изложен опис категорија и врста напада у савременим мрежним окружењима. При томе напади су представљени и описани према карактеристичним променама које остављају у структури мрежног саобраћаја, а што је предмет анализе, детекције и класификације аномалија које покрива ова дисертација.

У **поглављу 4** су представљени системи за препознавање напада у рачунарским мрежама (*Intrusion Detection System*). Најпре су описане метрике за анализу и представљање перформанси, као и изазови који се намећу пред овакве системе, да би се затим дао преглед основних техника детекције. Први приступ се заснова на тзв. потпису који се препознаје у садржају мрежних пакета (*signature-based*), док се други заснива на анализи аномалија у структури мрежног саобраћаја које настају као последица спровођења напада (*anomaly-based*). Описане су предности и мане оба приступа, уз указивање да се мотиви и циљеви дисертације више односе на методе засноване на анализи аномалија.

Поглавље 5 представља централно и највеће поглавље докторске дисертације јер описује реализовану методологију и пратеће архитектуру система за детекцију аномалија у мрежном саобраћају. Први део поглавља се односи на представљање теоријских концепата и анализу проблема, па се у поглављу најпре описује извор и структура коришћених података, а то су основне информације о комуникационим токовима који су прикупљени посредство *NetFlow* или неког сличног протокола. Основни механизам детекције напада се заснива на детекцији промене ентропије која се рачуна за различите комбинације атрибута, што се даље детаљно описује у поглављу користећи и формалне математичке једначине. Представљена је анализа карактеристика три најпознатије врсте ентропије – Шенонова (*Shannon*), Цалисаова (*Tsallis*) и Раниеова (*Rényi*) ентропија, које су посебно анализиране са аспекта могућности маскирања напада чиме се поништава промена ентропије. На основу тога је предложен оригинални метод детекције оваквог маскирања. Након тога се анализирају различити комуникациони модели претходно разматраних напада, да би се овај концепт генерализовао у види таксономије класа комуникационих модела који се третирају као карактеристични обрасци комуникационог понашања. Наредна целина у поглављу дефинише архитектуру предложеног система, уз опис основних елемената. У слоју прикупљања података су описани атрибути који се користе као кључеви агрегације, волуметријски атрибути и атрибути јединственог појављивања, тзв. атрибути понашања (*behaviour features*). Детаљно је описан процес агрегације уз формални опис алгоритма који то спроводи на оптималан начин.

У **поглављу 6** изложене су експерименталне процедуре и резултати анализе и валидације предложеног решења уз опис коришћених скупова података. Најпре је презентована валидација предложене методе детекција маскирања промене ентропије, и то за све три разматране врсте ентропије. Након тога су представљени експериментални резултати

који на појединачним атрибутима демонстрирају успешност примењене методе детекције промене ентропије која указује на аномалију у структури мрежног саобраћаја. Представљени су свеобухватни резултати утицаја свих комуникационих модела на све атрибуте, и то најпре за волуметријске, а затим и за изведене атрибуте понашања. У оба случаја је демонстрирана карактеристична периодичност утицаја комуникационих модела на атрибуте, из чије су анализе произашла правила која се осим детекције могу користити за класификацију аномалија. Дефинисана правила су потврђена кроз презентоване резултате додатних експеримената. Коначно, представљени су и резултати поређења приступа на бази ентропије у односу на методе примене машинског учења, уз дискусију предности и мана оба приступа.

У **поглављу 7** су представљена закључна разматрања, указано је на оригиналност представљеног приступа и на најважније научне доприносе и резултате дисертације. Затим су назначене смернице потенцијалних праваца даљег истраживања.

У **поглављу 8** је дата преглед литературе кроз списак од 119 коришћених референци.

Додатно је приложена биографија кандидата која обухвата податке о датуму и месту рођења, школовању, напредовању у струци, радном искуству и додатним биографско-пословним подацима, као и Изјава о ауторству, Изјава о истоветности штампане и електронске верзије докторског рада и Изјава о коришћењу ове докторске дисертације.

3. ОЦЕНА ДИСЕРТАЦИЈЕ

3.1. Савременост и оригиналност

Докторска дисертација кандидата Жуме Ибрахима припада области сигурности рачунарских мрежа, а бави се детекцијом аномалија у мрежном саобраћају као индикације сигурносних претњи, засновано на промени вредности ентропије различитих атрибута. Савременост развијене методологије и предложене архитектуре система се огледа у могућности широке примене за потребе детектовања аномалија и класификације напада у савременим мрежним окружењима у скоро реалном времену, при чему је предложено решење модуларно, флексибилно и прошириво.

Оригиналност предложеног приступа се огледа кроз развој нове методе за детекцију маскирања промена ентропије, као и нове свеобухватне методологије за детекцију и класификацију аномалија као индикације напада. Кључни допринос дисертације представља генерализација додатних атрибута понашања, за које је кроз детаљну анализу експерименталних резултата показано да имају боље перформансе и ширу примену у односу на волуметријске атрибуте. На основу утицаја карактеристичних аномалија на ове атрибуте изведена су правила класификације аномалија, што представља додатни научни допринос.

3.2. Осврт на референтну и коришћену литературу

Литература која се наводи у оквиру дисертације садржи 119 референци, чиме је обухваћен широк опсег публикација, укључујући радове публиковане у реномираним међународним часописима и конференцијама, књиге, релевантне техничке извештаје и одређене изворе са интернета. Велики број радова је новијег датума, што указује на актуелност разматране проблематике. На основу изнетог може се закључити да је кандидат имао темељан увид у досадашње доприносе у овој области и да је научни допринос стављени у одговарајући контекст.

3.3. Опис и адекватност примењених научних метода

Дисертација се заснива на примени метода анализе, моделовања и имплементације предложеног решења, укључујући валидацију и компарацију добијених експерименталних резултата. Коришћене су различите инжењерске и научне технике анализе велике количине података који представљају логове о спроведеним мрежним комуникацијама, који су преузети из јавно доступних скупова података ове врсте. Основни софтверски алат који је коришћен за анализу података је клијентска апликација за агрегацију података и рачунање ентропије, која је претходно развијена у оквиру одвојеног мастер рада на Електротехничког факултету. Додатно је коришћен и Python програм за генерисање синтетичких података према дефинисаним комуникационим моделима, а који је добијен од аутора чији је рад референциран под бројем 44 у списку коришћене литературе. Ради оптимизације, из коришћених скупова података уклоњени су атрибути који нису били од интереса, а додати су нови изведени атрибути.

У скуп уједначених података, са одстрањеним постојећим нападима и другим уоченим нерегуларностима, додати су синтетички генерисани подаци о фиктивном саобраћају који карактерише понашање свих 16 уведених комуникационих модела. Резултати ентропија за укупно 103 атрибута унакрсно су анализирани у посебном окружењу за графички приказ вредности током времена, а које је развијено као Excel апликација, уз динамичко прорачунавање и приказ пратећих вредности на основу постављених параметара.

3.4. Применљивост остварених резултата

Један од дефинисаних циљева при изради ове докторске дисертација је био да предложено решење има практичну примену у реалном времену. Овај циљ је остварен тако што се предложена методологија и архитектура базира на подацима који се на једноставан начин могу прикупити са мрежних уређаја путем NetFlow или сличних протокола. Додатно је показано да се детекција аномалија може спровести коришћењем само основних атрибута (изворишне и одредишне ИП адресе и бројеви портова). Шта више, показано је да атрибути изведени из ових података остварују боље перформансе у односу на волуметријске атрибуте, чија примена доминира у научној литератури.

По питању комплексности алгоритма прорачуна ентропија, најзахтевнији је процес агрегације који директно зависи од број података за обраду у времену. Коришћена клијентска апликација за агрегацију и рачунање ентропије, реализована у програмском језику Јава, на радној станици остварује обраду више хиљада записа у секунди. У случају већег броја података, предложено је решење које се базира на случајном одабиру података (*sampling*) које се по потреби може применити.

3.5. Оцена достигнутих способности кандидата за самостални научни рад

На основу прегледане дисертације, Комисија процењује да је кандидат показао истраживачку зрелост и способност за самостални научни рад, почевши од систематског приступа дефинисању проблема, критичког осврта на постојећа решења из области, па до развоја оригиналног решења, његове имплементације и валидације. У прилог поменутом је и чињеница да је кандидат објавио више научних радова који су проистекли из дисертације, а у којима се појављује као први аутор.

4. ОСТВАРЕНИ НАУЧНИ ДОПРИНОС

4.1. Приказ остварених научних доприноса

Научни доприноси и резултати докторске дисертације кандидата Жуме Ибрахима су следећи.

- На бази спроведене анализе могућности маскирања вредности ентропије предложено је оригинално решење које ове покушаје може успешно детектовати.
- Систематизован је и генерализован приступ који се базира на коришћењу само атрибута понашања изведених из основних података о мрежним комуникацијама.
- Дефинисано је 16 карактеристичних комуникационих модела на бази образаца комуникационих активности и резултујућих записа који се бележе у логовима.
- Показано је да се мање аномалије, које су маскиране интензивним активностима регуларних комуникација, могу успешно детектовати поделом саобраћаја на различите подкласе.
- Утврђено је да различити комуникациони модели остварују различите утицаје на вредности ентропија посматраних атрибута, на основу чега су изведена правила препознавања појединачних комуникационих модела, а која се могу користити за класификацију аномалија.
- Предложена је модуларна и флексибилна архитектура система који имплементира развијену методологију и принципе детекције и класификације аномалија.

4.2. Критичка анализа резултата истраживања

Наведени научни доприноси представљају генерализацију и унапређење постојећих метода или предлог оригиналног решења за одређени проблем, као што следи.

- Проблем маскирања вредности ентропије није довољно третиран у научној литератури, па је изостало и адекватно решење. Ова празнина је попуњена наведеним доприносом који је остварeним овом дисертацијом.
- За атрибуте понашања је показано да остварују ширу примену уз боље перформансе детекције аномалија и предност што се могу генерисати коришћењем само основних података који су лако доступни за коришћење у реалном времену.
- Уведени систематизовани комуникациони модели доприносе бољем разумевању проблема и отварају могућност даљих истраживачких активности.
- Подела саобраћаја на мање подкласе представља једноставан али ефикасан метод чиме се унапређују способности детекције мањих аномалија, које често остају сакривене сличним обрасцем понашања регуларног саобраћаја.
- Предложена правила препознавања аномалија према уведеним комуникационим моделима представљају оригинални допринос у области класификације аномалија на бази ентропије, за шта у литератури постоје значајно мање радова него што је то случај коришћењем метода машинског учења.
- Предложена архитектура даје потврду изводљивости имплементације развијене методологије у реалном мрежном окружењу.

4.3. Верификација научних доприноса

Научни доприноси који су настали кроз истраживање у оквиру докторске дисертације кандидата Жуме Ибрахима публиковани су у међународном часопису са SCI листе и презентовани на међународним конференцијама и стручним скуповима. У наставку је дат списак радова који су у директној вези са израдом докторске дисертације, класификовани у складу са релевантним Правилником Министарства просвете, науке и технолошког развоја Србије.

Категорија М23:

[1] Ibrahim, Juma, and Slavko Gajin. "Entropy-based network traffic anomaly classification method resilient to deception." Computer Science and Information Systems 19(1):87–116, (2021), DOI: https://doi.org/10.2298/CSIS201229045I (IF: 1.167)

Категорија М33:

[3] J. Ibrahim, V. Timčenko, and S. Gajin, „A comprehensive flow-based anomaly detection architecture using entropy calculation and machine learning classification “, in 9th Int. Conf. Information Society and Technology – ICIST2019, pp. 138-143, 2019. Online: https://www.eventiotic.com/eventiotic/library/paper/466

[5] J. Ibrahim, S. Gajin: "SDN-Based Intrusion Detection System Literature Review", 16th International Symposium INFOTEH-JAHORINA 2017, 22-24 March 2017, Jahorina, Bosnia and Herzegovina.

[2] A. Elsadai, J. Ibrahim, F. Hajjaj, P. Jakić, “The Overview of Intrusion Detection System Methods and Techniques,” in Sinteza 2019 - International Scientific Conference on Information Technology and Data Related Research, Belgrade, Singidunum University, Serbia, 2019, pp. 155-161. doi:10.15308/Sinteza-2019-155-161

[4] V. Timčenko, J. Ibrahim, and S. Gajin, „The hybrid machine learning support for entropy based network traffic anomaly detection“, in 9th Int. Conf. Information Society and Technology – ICIST2019, pp. 144-149, 2019.

5. ЗАКЉУЧАК И ПРЕДЛОГ

На основу претходно наведеног, Комисија је закључила да докторска дисертација кандидата Жуме Ибрахима под насловом „Архитектура система за препознавање неправилности у мрежном саобраћају засновано на анализи ентропије“ испуњава све формалне и суштинске услове предвиђене Законом о високом образовању и прописима Универзитета у Београду и Електротехничког факултета.

Предлози и резултати садржани у овој докторској дисертацији су верификовани објављивањем једног рада у часопису са SCI листе. Демонстриран је оригинални научни допринос предложеног решења, чија је ефикасност и применљивост верификована на релевантним скуповима података. Додатно, предложеним решењем кандидат је испунио све постављене почетне циљеве свог научноистраживачког рада.

Комисија предлаже Наставно-научном већу Електротехничког факултета да се докторска дисертација под насловом „Архитектура система за препознавање неправилности у мрежном саобраћају засновано на анализи ентропије“ кандидата Жуме Ибрахима прихвати,

изложи на увид јавности и упути на коначно усвајање Већу научних области техничких наука Универзитета у Београду и давање одобрења кандидату да приступи усменој одбрани.

Београд, 24.6.2022.

ЧЛАНОВИ КОМИСИЈЕ

др Славко Гајин, ванредни професор
Универзитет у Београду – Електротехнички факултет

др Мило Томашевић, редовни професор
Универзитет у Београду – Електротехнички факултет

др Мирослав Марић, редовни професор
Универзитет у Београду – Математички факултет