Универзитет у Београду
Електротехнички факултет

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Извештај о урађеној докторској дисертацији кандидата Ђорђа Јовановића, мастер инжењера електротехнике и рачунарства

Одлуком бр. 1575/36 од 10.9.2024. године, именовани смо за чланове Комисије за оцену дисертације кандидата Ђорђа Јовановића, мастер инжењера електротехнике и рачунарства под насловом

Рано откривање уређаја заражених ботнет малвером коришћењем метода детекције аномалија мрежних токова

(енг. *Early discovery of the devices infected with botnet malware using network flow anomaly detection*)

После прегледа достављене Дисертације и других пратећих материјала и разговора са Кандидатом, Комисија је сачинила следећи

И З В Е Ш Т А Ј

1. УВОД

1.1. Хронологија одобравања и израде дисертације

Докторске академске студије на Електротехничком факултету Универзитета у Београду, на модулу Рачунарска техника и информатика, кандидат Ђорђе Јовановић је уписао у октобру 2018. године. Кандидат је положио све испите са оценом 10 и остварио 120 ЕСПБ. Такође, испунио је све обавезе везане за студијски истраживачки рад које су предвиђене наставним планом и програмом докторских студија. У истраживачком раду усмерио се ка области софтверски дефинисаних мрежа, информационе безбедности и примене техника машинског учења на детекцију малициозног понашања у рачунарским мрежама.

Кандидат је пријавио тему за израду докторске дисертације под насловом „Рано откривање уређаја заражених ботнет малвером коришћењем метода детекције аномалија мрежних токова" Катедри за рачунарску технику и информатику на Електротехничком факултету Универзитета у Београду. Катедра за рачунарску технику и информатику, на својој седници одржаној дана 24.09.2021. године утврдила је да је надлежна за разматрање пријављене теме докторске дисертације, као и да су достављена пријава и њени прилози суштински и формално одговарајући и комплетни, чиме је прихватила да се пријава теме докторске дисертације проследи Комисији за студије трећег степена Електротехничког факултета Универзитета у Београду што је учињено 30.09.2021.

Комисија за студије трећег степена Електротехничког факултета Универзитета у Београду је на својој седници одржаној дана 06.10.2021. године разматрала пријаву теме за израду докторске дисертације и предлог састава Комисије за оцену научне заснованости теме докторске

дисертације и упутила их Наставно-научном већу Електротехничког факултета Универзитета у Београду на усвајање.

Наставно-научно веће Електротехничког факултета Универзитета у Београду је, на својој 865. седници одржаној дана 12.10.2021. године, донело одлуку бр. 5001/18-1 од 26.10.2021. о именовању Комисије за оцену научне заснованости теме докторске дисертације у саставу:

- др Жарко Станисављевић, ванредни професор, Универзитет у Београду - Електротехнички факултет
- др Татјана Давидовић, научни саветник, Математички институт САНУ
- др Горан Квашчев, ванредни професор, Универзитет у Београду - Електротехнички факултет

За ментора је предложен др Павле Вулетић, ванредни професор, Универзитет у Београду, Електротехнички факултет.

Јавна усмена одбрана теме докторске дисертације је одржана дана 03.11.2021. године. Комисија за оцену научне заснованости теме докторске дисертације оценила је усмену одбрану као успешну (оцена „задовољио"). Комисија за студије трећег степена Електротехничког факултета Универзитета у Београду је на својој седници која је одржана дана 07.12.2021. године разматрала записник Комисије за оцену научне заснованости теме докторске дисертације са јавне усмене одбране и упутила га је Наставно-научном већу Електротехничког факултета Универзитета у Београду на усвајање. Наставно-научно веће Електротехничког факултета Универзитета у Београду је, на својој 868. седници одржаној дана 14.12.2021. године, усвојило извештај Комисије за оцену научне заснованости теме докторске дисертације кандидата, а за ментора је именован др Павле Вулетић, ванредни професор Електротехничког факултета Универзитета у Београду. Веће научних области техничких наука Универзитета у Београду је, на својој седници одржаној дана 19.01.2022. године, дало сагласност на предложену тему докторске дисертације и именовање ментора (бр. одлуке 61206-5359/2-21).

Кандидат је предао докторску дисертацију на проверу оригиналности, преглед и оцену 27.08.2024. године. Комисија за студије трећег степена Електротехничког факултета Универзитета у Београду је, на седници одржаној дана 03.09.2024. године, потврдила испуњеност потребних услова за подношење предлога Наставно-научном већу Електротехничког факултета Универзитета у Београду за формирање Комисије за преглед, оцену и одбрану докторске дисертације. Наставно-научно веће Електротехничког факултета Универзитета у Београду је, на својој 900. седници одржаној дана 10.09.2024. године, именовало Комисију за преглед, оцену и одбрану докторске дисертације (бр. одлуке 1575/36) у саставу:

- др Жарко Станисављевић, ванредни професор, Универзитет у Београду - Електротехнички факултет
- др Татјана Давидовић, научни саветник, Математички институт САНУ
- др Горан Квашчев, редовни професор, Универзитет у Београду - Електротехнички факултет
- др Дражен Драшковић, ванредни професор, Универзитет у Београду - Електротехнички факултет
- др Марија Пунт, ванредни професор, Универзитет у Београду - Електротехнички факултет

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

1.2. Научна област дисертације

Дисертација припада научној области Електротехника и рачунарство, а ужа научна област дисертације је Рачунарска техника и информатика, док у оквиру уже научне области припада подобластима информационе безбедности и рачунарских мрежа. За ове области матичан је Електротехнички факултет. Ментор дисертације је др Павле Вулетић, ванредни професор Електротехничког факултета Универзитета у Београду, који има доприносе у наставном и научном раду у областима рачунарских мрежа, заштите података и информационе безбедности.

1.3. Биографски подаци о кандидату

Ђорђе Јовановић је рођен 7. августа 1994. године у Београду, Република Србија, где је са одличним успехом 5,00, као носилац Вукове дипломе, завршио основну школу „Стеван Дукић" и Прву београдску гимназију.

У септембру 2017. године дипломирао је на Електротехничком факултету у Београду на Модулу за рачунарску технику и информатику са просечном оценом 9,16 и оценом 10 на завршном раду на тему „Виртуелне мреже реализоване у *SDN* технологији".

У септембру 2018. године завршио је мастер студије на Електротехничком факултету у Београду на Модулу за рачунарску технику и информатику са просечном оценом 10,00 и оценом 10 на мастер раду на тему „Имплементација лабораторијског окружења за софтверски дефинисане мреже помоћу класе *Zodiac FX* свичева".

Докторске академске студије на Модулу за рачунарску технику и информатику је уписао 2018. године. Током докторских студија остварио је просечну оцену 10,00.

Од априла 2019. године ангажован је на Математичком институту САНУ као истраживач-приправник, а од априла 2022. године је ангажован као истраживач сарадник. У оквиру научноистраживачког рада, бавио се применом метахеуристика, блокчејн технологијама, машинским учењем и софтверски дефинисаним мрежама. Објавио је 30 радова у часописима и у зборницима националних и интернационалних конференција, од којих је на девет радова, потписан као првоименовани аутор.

Течно говори енглески језик, има напредни ниво знања из француског, средњи ниво знања из руског и кинеског, и служи се грчким, италијанским и тајландским језиком.

2. ОПИС ДИСЕРТАЦИЈЕ

2.1. Садржај дисертације

Дисертација је написана на српском језику ћириличним писмом и има 142 стране, од чега је 127 нумерисано. Дисертација садржи 18 слика и 18 табела. Дисертација је организована у 6 поглавља:

1. Увод
2. Преглед развоја ботнет малвера
3. Анализа контролног канала савремених ботнета
4. Детекција ботнета коришћењем статистичих параметара унутар мрежних токова
5. Детекција новијих варијанти ботнет *CnC* комуникације (2022-2023)
6. Закључак

Такође, дисертација садржи и два додатка са историјским приказом развоја ботнет малвера и детаљнијим описом коришћених статистичких параметара временских низова, те насловне стране на српском и енглеском језику, страну са информацијама о ментору и члановима комисије за преглед и оцену, сажетак на српском и енглеском језику, садржај, списак слика, списак табела, списак литературе са 148 референци наведених по редоследу појављивања у

тексту, биографију аутора и потребне изјаве (о ауторству, о истоветности штампане и електронске верзије докторског рада и о коришћењу).

2.2. Кратак приказ појединачних поглавља

У уводном поглављу су приказани предмет, циљ и значај истраживања, као и основни појмови потребни за разумевање проблема који се решава. Описана је мотивација за истраживање која је пре свега последица све већих проблема које стварају велике ботнет мреже и непостојање квалитетних механизама који би предупредили нападе изведене њиховим путем. Истакнуте су основне идеје и хипотезе рада, а то је да постоје обрасци понашања ботнет малвера који су заједнички за више различитих класа у дужем временском периоду, да је могуће оптимизовати капацитете за складиштење података о малверима и процесорско оптерећење, без губитка тачности детекције, те да је предложеним приступом могућа детекција до тада недетектованих примерака малвера и то у реалном времену.

Друго поглавље уз први додатак садржи детаљан преглед историјата ботнета и ботнет малвера. Затим је дат опис архитектуре и животног циклуса ове врсте малициозног софтвера. Финални део поглавља је посвећен командном и контролном каналу ботнет малвера који администратори ботнет мреже користе како би држали на окупу све заражене уређаје, али и како би им слали команде којима се контролишу напади. Пошто је једна од основних идеја изложених у овом раду да детекција ботнета треба да почива на детекцији командног и контролног канала, посебна пажња је посвећена методама избегавања детекције и прикривања командног и контролног канала, које су уочене у досадашњим примерцима малвера.

Треће поглавље је посвећено истраживању командне и контролне комуникације ботнет вируса. Описана је методологија прикупљања узорака вируса и њихове динамичке и статичке анализе. Ови узорци, две велике класе малвера: *mirai* и *gafgyt*, су прикупљани у првој фази у периоду 2019-2021. године. Прикупљени узорци малвера су покретани на реалним уређајима, а не у изолованим или виртуелним окружењима, чиме је осигурано то да је забележено њихово аутентично понашање, чак и ако је малвер полиморфан. Приказани су карактеристични обрасци мрежне комуникације које прикупљени узорци поседују, а које одликују константно мали проток и периодичност. Управо ове карактеристике су мотивисале даљи дизајн система за детекцију ботнета, који је изложен у наредном поглављу.

У четвртом поглављу је представљен предлог система за детекцију ботнета. Прво је представљена темељна анализа релевантне научне литературе, која је показала два основна правца досадашњег начина рада детектора ботнета: детекција напада коришћењем података из мрежних токова или детекција командне и контролне комуникације коришћењем снимака комплетног саобраћаја на одређеном линку. Након тога је описан предложени систем за детекцију ботнета *PI-BODE* (енг. *Programmable Intraflow-based IoT Botnet Detection*) који поседује неколико оригиналних особина. Овај систем не почива ни на анализи комплетних мрежних токова ни на анализи свих пакета, већ на оригиналној методи узорковања броја бајтова и пакета за сваки мрежни ток на неком линку коришћењем механизама *OpenFlow* протокола и софтверски дефинисаних мрежа. Тиме се као основа за детекцију добијају временски низови из чијих је статистичких одлика методама машинског учења могуће детектовати командни и контролни канал. Показан је комплетан радни процес машинског учења који је коришћен, као и скуп података над којим је вршена анализа који укључује како снимљене примерке малвера, тако и неке од стандардно коришћених јавно доступних скупова података са Чешког техничког универзитета (*IoT-23* скуп података). Приказани су и резултати евалуације класификације који су показали да је предложеном методом могуће детектовати ботнет комуникацју са већом или једнаком прецизношћу као у случају анализе комплетним снимцима саобраћаја. Оно што је такође показано су резултати анализе количине података које користи метода *PI-BODE*. Ови резултати указују на то да је предложеном методом могуће добити квалитетну детекцију ботнета уз коришћење до два реда величине мање података.

У петом поглављу је најпре дат опис новијих узорака ботнета, прикупљених током периода 2022-2023. године. Указано је на модификације понашања малвера које су уочене у поређењу са првом групом описаном у поглављу 3. Даље је приказан нови скуп статистичких параметара које је могуће извући из временских низова, а који могу да се користе као одлике у систему машинског учења. Потом је дат опис методологије даљег истраживања чији су циљеви постизање већег нивоа прецизности детекције коришћењем савремених техника обраде података, које укључују технике које се користе у случајевима небалансираности скупа података и анализа непроменљивих особина ботнета, које би се могле искористити за детекцију до тада непознатих примерака малвера, односно тзв. нападе нултог дана (енг. *zero day attack*) који су најтежи за детекцију. Проблем дисбаланса класа у узорцима за обучавање је веома чест у области информационе безбедности где малициозно понашање најчешће представља веома мали део укупне масе артефаката (пакета или других статистичких особина). Дат је детаљан опис различитих метода за решавање овог проблема попут метода за синтетичко генерисање примерака мањинске класе који су анализирани, као и преглед механизама за избор одлика које су значајне за детекцију, начин подешавања хиперпараметара модела и модерних детектора који су се показали посебно погодним за табеларне податке. Након приказа радних процеса, изложени су резултати експеримената који показују која методологија може да пружи адекватан квалитет детекције. У свим случајевима је остварено унапређење у односу на прве експерименте изложене у поглављу 4. Даљи експерименти су анализирали могућност детекције нових примерака малвера на класификатору обученом над старим примерцима. Различитим партиционисањем скупа за обучавање показано је да се укључивањем нових примерака малвера у скуп за обучавање остварују бољи резултати. Поред тога, показано је и да када је систем обучен старим примерцима малвера (из 2019-2021.) може са великом прецизношћу (преко 0.9) да препозна нове примерке малвера (из 2022–2023.) чиме су потврђене полазне хипотезе са једне стране, али је и показано да предложена методологија решавања дисбаланса не врши претренирање модела. Додатно, приказана је анализа минималног броја одбирака временских низова који је довољан да се оствари поуздана детекција како би се видело који су то временски оквири у којима је могуће детектовати ботнет малвер и анализирала могућност детекције у реалном времену.

Последње, шесто поглавље, је закључак докторске дисертације. Дат је кратак преглед спроведеног истраживања и сваке његове фазе, са освртом на полазне хипотезе и сажето представљеним резултатима и доприносима истраживања. Изложени су и нови изазови који се очекују у будућности у оквиру ботнет детекције и предложени даљи правци истраживања.

3. ОЦЕНА ДИСЕРТАЦИЈЕ

3.1. Савременост и оригиналност

Област информационе безбедности, са све већим упливом информационих технологија у различите аспекте људског живота, континуирано привлачи све већу пажњу истраживача, јер врсте и утицаји напада на инфраструктуру и услуге бивају све разорнији. Ботнети су једна од најчешће коришћених платформи за пласирање различитих напада и њихов број се не смањује. Према подацима *urlhaus* базе података свакодневно се пријављује између 1500 и 2000 примерака различитих локација на интернету на којима постоји малвер и то најчешће онај малвер чијим се покретањем уређај укључује у различите ботнет структуре. Такође, у последње време су уређаји који су све чешће део ботнета постали они које не користе људи, већ различити уређаји који аутономно обављају неку функцију, а повезани су на интернет (нпр. камере, међуумрежени уређаји (енг. *Internet of Things*, скр. *IoT*) и слично). У том смислу је тема истраживања ове дисертације савремена, актуелна и потребна, што је и потврђено великим бројем референци у дисертацији које су настале у последњих неколико година и које се и даље појављују.

Приступ који је примењен у оквиру ове дисертације за детекцију ботнета, кроз формирање временских низова за сваки од мрежних токова из којих ће се касније извлачити потребне одлике за детекцију машинским учењем је потпуно нов и оригиналан. Досадашња методологија је укључивала или анализу сумарних статистика мрежних токова којом су могли да се открију само волуметријски напади након што се десе, или анализу свих пакета на неком линку, што са данашњим капацитетима линкова и количином саобраћаја ствара озбиљне изазове у обради података. Квалитет предложеног приступа је доказан кроз експерименталне резултате који су показали да се коришћењем овог приступа добијају једнако добри или чак и бољи резултати детекције него када се користе снимци комплетног саобраћаја, али уз значајно мање скупове података, а тиме и мање хардверске захтеве који се постављају пред систем за детекцију.

3.2. Осврт на референтну и коришћену литературу

У дисертацији је приказан детаљан преглед релевантне литературе из области карактеризације понашања ботнета и малвера, детекције ботнета и малвера, софтверски дефинисаних мрежа, методологије детекције алгоритмима машинског учења и обраде података. У истраживање су укључени и најновији радови у релевантним областима, што потврђује значај, релевантност и савременост теме. Списак литературе садржи 147 референци наведених по реду цитирања у тексту.

3.3. Опис и адекватност примењених научних метода

Истраживање је започело детаљном и исцрпном анализом до сада познатих ботнета и бот малвера, а посебно начинима комуникације ботова са централном тачком/нападачем кроз командни и контролни канал комуникације и еволуцијом метода за сакривање командног и контролног канала. Даље је детаљно истражена научна литература која описује врсте скупова података из којих се вршила детекција, као и коришћене механизме детекције, данас најчешће методама машинског учења.

У следећој фази истраживања извршено је прикупљање већег броја примерака малвера чија су мета *IoT* уређаји. Малвер најчешћих група ботнета (*mirai* и *gafgyt*) је прикупљан преко јавно доступних линкова из база које пријављују ову врсту активности (база *URLhaus Database*, доступна на: *http://urlhaus.abuse.ch*), а сваки примерак малвера који је преузет је у контролисаним условима одмах и покретан на скупу *raspberryPi* уређаја повезаних на интернет, како би се осигурало да може да се повеже у ботнет, који је у том тренутку активан. За сваки примерак малвера је урађена статичка анализа кода, анализа у *cuckoo* изолованом окружењу и динамичка анализа понашања, кроз снимање комплетне командне и контролне комуникације, а у неким случајевима снимљен је и почетак напада. Како би се осигурало праћење промена понашања ботнет малвера, примерци су прикупљани у различитим интервалима током временског периода од 4 године, што ово истраживање чини ретким у поређењу са другим истраживањима у истој области која, како је показано у дисертацији, су се најчешће фокусирала на кратке временске периоде и тиме анализирале понашање и детекцију малвера који се у тим тренуцима појављивао. Из прикупљених података је формиран скуп података који је учињен јавно доступним, како би се обезбедила проверљивост добијених резултата, а додатно је коришћен још један актуелан скуп података који је формирао Чешки технички универзитет коришћењем различитих *IoT* уређаја (*IoT-23*). Овако формиран скуп података над којим је спроведено даље истраживање осигурава реалистичност и релевантност добијених резултата.

Након тога је дизајниран систем заснован на софтверски дефинисаним мрежама и *OpenFlow* протоколу који периодичним узорковањем података са мрежних уређаја из мрежног саобраћаја извлачи временске низове броја бајтова и пакета за сваки ток понаособ. Систем је имплементиран и његов рад верификован на савременом софтверском *OpenvSwitch* свичу.

Подаци који су добијени узорковањем поменутих временских низова су даље статистички обрађени и из тих параметара су добијене одлике мрежних токова које су се користиле за класификацију методама машинског учења. Коришћен је комплетан радни процес машинског учења који укључује и методе којима се решава проблем дисбаланса класа, који је карактеристичан у области информационе безбедности, и методе оптимизације хиперпараметара и избора одлика које имају пресудни утицај на класификацију. Експерименти су понављани више пута са случајним узорковањем скупова за тренирање и верификацију. Методологија машинског учења је примењена коректно, а додатно је различитим партиционисањем извора података за скуп за обучавање и тестни скуп (из скупа старијих и новијих примерака малвера) показано да модели машинског учења нису претренирани на одређени узак скуп примерака и да је могућа детекција нових примерака на основу старих, што је посебно значајно у области информационе безбедности, јер ово значи могућност детекције до тада непријављених претњи.

3.4. Применљивост остварених резултата

Резултате овог истраживања је могуће у потпуности применити у реалном мрежном окружењу. Различити програмабилни мрежни уређаји (свичеви, мрежне картице) могу да се програмирају да извлаче временске низове мрежних токова у реалном времену, или директним коришћењем кода за *OpenvSwitch* развијеног у дисертацији или развијањем новог кода коришћењем неких новијих софтверских парадигми попут *P4* програмског језика. Тренд који је уочљив у последњих неколико година, прављења мрежних акцелератора који имају значајну процесорску снагу на самој мрежној картици и који су способни да значајан део обраде мрежних података изврше на картици, растерећујући централни процесор, додатно иду у прилог коришћењу оваквог приступа анализи мрежног саобраћаја и детекцији аномалија.

3.5. Оцена достигнутих способности кандидата за самостални научни рад

Ова докторска дисертација је резултат вишегодишњег истраживачког искуства у области информационе безбедности, рачунарских мрежа и детекције аномалија методама машинског учења. Искуство је формирано радом са реалним примерцима малвера, најсавременијим механизмима и алатима за рад са мрежним уређајима и методама машинског учења.

Кандидат је током израде пројекта, чији је циљ била дуготрајна анализа понашања ботнет малвера и детекција постојања ботова у некој инфраструктури пре него што ти ботови покрену нападе, захваљујући систематичном прегледу значајних радова у области, те посебно систематичном начину прикупљања примерака малвера и њиховој статичкој и динамичкој анализи, предложио оригиналну методологију и конструисао механизме којима је могуће остварити циљеве на далеко економичнији начин у односу на досадашње методе.

Научни доприноси верификовани су кроз објављени научни рад под називом „*PI-BODE: Programmable Intraflow-based IoT Botnet Detection system*" у којем су објављени главни резултати овог истраживања у часопису *Computer Science and Information Systems*. На основу доприноса и методологије истраживања, као и начина израде докторске дисертације, комисија закључује да је кандидат у потпуности способан за извођење самосталног научног рада.

4. ОСТВАРЕНИ НАУЧНИ ДОПРИНОС

4.1. Приказ остварених научних доприноса

Овај рад садржи више научних доприноса у једној веома активној научној области:

- Дат је опсежан преглед релевантних метода у домену детекције ботнета, понашања ботнет малвера и оптимизација метода машинског учења, посебно у ситуацијама

небалансираних скупова података, што је чест проблем у области информационе безбедности.

- Урађена је јединствена дуготрајна анализа динамичког понашања ботнет малвера у периоду од 4 године (2019-2023) која показује ритам промена начина рада малвера, али и неке инваријантне особине које омогућавају ефикасну детекцију чак и оних примерака малвера над којима систем није обучаван.
- Предложена је оригинална методологија за детекцију присуства ботова у некој инфраструктури кроз екстракцију методама софтверски дефинисаних мрежа и анализу унутартоковских статистичких параметара. У дисертацији је показано да је оваквим приступом могуће да се оствари једнака или већа прецизност детекције као у ситуацијама када се користи најдетаљнија могућа анализа – снимком свих пакета на неком линку, али за око два реда величине мањи захтевани простор за чување скупа података са једне стране, али и процесорске снаге захтеване за обраду са друге.
- Извршена је детаљна анализа различитих методологија за решавање проблема небалансираности класа у скупу података и показано које комбинације метода примењене на табеларне статистичке податке који су коришћени у овом случају дају највећу прецизност детекције, уз очување могућности откривања оних примерака малвера над којима систем није обучаван.
- Извршена је анализа оних одлика које пресудно утичу на класификацију и одлуку да ли је неки мрежни ток део ботнет командне и контролне комуникације или није. Овиме су се показале оне особине малвера које су инваријантне током целокупног временског периода анализе малвера и могу да се употребе за ефикасну детекцију.
- Додатно, извршена је анализа могућности детекције у реалном времену кроз анализу времена које је потребно временским низовима да се стабилизују њихови статистички параметри.

4.2. Критичка анализа резултата истраживања

Докторска дисертација под називом „Рано откривање уређаја заражених ботнет малвером коришћењем метода детекције аномалија мрежних токова“ пружа детаљан и обједињен преглед области архитектуре и механизама рада ботнета, а посебно врсте бот малвера чија су мета *IoT* уређаји, те механизама за њихову детекцију. Спроведено експериментално истраживање динамичког понашања малвера током четворогодишњег периода је јединствено у својој дуготрајности и темељној анализи мењања понашања малвера у времену унутар једне класе ботнет малвера.

Као исход овог истраживања пројектован је, имплементиран и експериментално верификован оригиналан систем заснован на софтверски дефинисаним мрежама и *OpenFlow* протоколу који периодичним узорковањем података са мрежних уређаја из мрежног саобраћаја формира временске низове броја бајтова и пакета за сваки ток понаособ. Временски низови добијени узорковањем поменутих променљивих мрежних уређаја су статистички обрађени коришћењем врло детаљне анализе са преко 70 статистичких параметара. Из тих параметара су добијене одлике мрежних токова које су се користиле за класификацију методама машинског учења. Детекција машинским учењем је показала и потврдила полазне хипотезе рада, да је могуће остварити најмање једнаку тачност детекције малвера, као у научним резултатима других истраживача у области, али уз значајно, до скоро 300 пута мањи, скуп података из којег се врши детекција, чиме се захтева и мања процесорска снага потребна за детекцију. Ниво уштеде зависи од периоде узорковања, али и статистичких карактеристика саобраћаја на посматраном линку. Решење је могуће имплементирати у реалним условима.

Такође, у овој дисертацији је дата детаљна анализа механизама за решавање проблема небалансирности скупа података који је врло карактеристичан за област информационе безбедности, којом се остварују и бољи резултати класификације мрежних токова. Овом анализом су пронађене комбинације метода које дају врло високу прецизност детекције. Оно што је у овом делу анализе најзначајније је то што је показано да је овако обучаван модел у стању да детектује нове примерке малвера, иако је обучаван на старим примерцима, са прецизношћу од око 0.9, што представља могућност квалитетне детекције тзв. напада нултог дана, а указано и је и на карактеристичне одлике које су у великој мери непроменљиве и у случају промена понашања малвера у времену.

4.3. Верификација научних доприноса

Резултати и научни доприноси ове дисертације су приказани и верификовани у три научна рада: научном раду у часопису са импакт фактором *Computer Science and Information Systems*, у којем је описана методологија детекције; научном раду на ТЕЛФОР конференцији и његовом проширењу у ТЕЛФОР часопису, у којима је описана динамичка анализа понашања малвера у првом периоду анализе (2019-2020). Информације о радовима приказане су у наставку:

Категорија М23:

1. **Đorđe D. Jovanović**, Pavle V. Vuletić, PI-BODE: Programmable Intraflow-based IoT Botnet Detection system, *Computer Science and Information Systems* 21(1):37–56, DOI: 10.2298/CSIS211116064J, (ISSN: 1820-0214) (IF 2023: 1,2)

Категорија М33:

1. **Đorđe D. Jovanović**, Pavle V. Vuletić, Analysis and Characterization of IoT Malware Command and Control Communication, *2019 27th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, 2019, pp. 1-4, DOI : 10.1109/TELFOR48224.2019.8971194.

Категорија М53:

1. **Đorđe D. Jovanović**; Pavle V. Vuletić ; Analysis and Characterization of IoT Malware Command and Control Communication ; *The TELFOR Journal*; 12(2); 80-85.

5. ЗАКЉУЧАК И ПРЕДЛОГ

Докторска дисертација под називом „Рано откривање уређаја заражених ботнет малвером коришћењем метода детекције аномалија мрежних токова“ кандидата Ђорђа Јовановића, мастер инжењера електротехнике и рачунарства, представља значајан научни допринос у области информационе безбедности и посебно детекције ботнета. Значај рада лежи у оригиналном приступу који омогућава ефикасну детекцију уз значајно мање захтеване хардверске ресурсе система за детекцију.

У оквиру дисертације кандидат се бавио истраживањем динамичког понашања ботнет малвера током четворогодишњег периода. На основу ове анализе, кандидат је предложио оригиналну методу за узорковање унутартоковских временских низова бројева бајтова и пакета, коришћењем софтверски дефинисаних мрежа. Затим су одређени статистички параметри ових временских низова који су послужили као одлике за модел машинског учења којим је вршена детекција аномалија, односно тога да ли неки од мрежних токова припада ботнет командној и контролној комуникацији. Поред овога, кандидат је извршио детаљну анализу и примену различитих метода које решавају проблем небалансираности скупова података који је врло чест у области информационе безбедности и дао је смернице и методологију како ово урадити. Показано је да предложена методологија може да детектује чак и оне примерке малвера над којима није обучаван модел машинског учења, што је од великог значаја у области информационе безбедности, јер се на овај начин детектују тзв. напади нултог дана. Додатно,

анализиране су оне особине временских низова малвера које су непроменљиве током дужег временског периода и које је могуће користити за ефикасну детекцију. Приказана метода детекције је у потпуности применљива у реалним условима било коришћењем већ реализованог софтвера било адаптацијом на неке новије платформе попут *P4*-програмабилних уређаја. Резултати, као и реализовани циљеви истраживања, су верификовани објављивањем научног рада у часопису са импакт фактором. Осим конкретних доприноса ефикасности детекције, која је потврђена бројним изведеним експериментима, резултат истраживања представљају и закључци, као и потенцијал за даља унапређења метода детекције.

На основу свега наведеног, Комисија констатује да је кандидат Ђорђе Јовановић испунио све формалне и суштинске услове предвиђене Законом о високом образовању, Статутом и Правилником о докторским студијама Електротехничког факултета Универзитета у Београду. Комисија има посебно задовољство да предложи Наставно-научном већу Електротехничког факултета Универзитета у Београду да се докторска дисертација под називом „Рано откривање уређаја заражених ботнет малвером коришћењем метода детекције аномалија мрежних токова" кандидата Ђорђа Јовановића, мастер инжењера електротехнике и рачунарства, прихвати, изложи на увид јавности и упути на коначно усвајање Већу научних области техничких наука Универзитета у Београду.

ЧЛАНОВИ КОМИСИЈЕ

др Жарко Станисављевић, ванредни професор
Универзитет у Београду – Електротехнички факултет

др Горан Квашчев, редовни професор
Универзитет у Београду – Електротехнички факултет

др Татјана Давидовић, научни саветник
Математички институт САНУ

др Дражен Драшковић, ванредни професор
Универзитет у Београду – Електротехнички факултет

др Марија Пунт, ванредни професор
Универзитет у Београду – Електротехнички факултет