Универзитет у Београду

Електротехнички факултет

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Извештај о прегледу и оцени докторске дисертације кандидата Mp. Yousefa Abuadlle, дипл. инж.

Наставно-научно веће Електротехничког факултета у Београду, на својој 776. Седници 8.7.2014. године, именовало нас је за чланове Комисије за преглед и оцену докторске дисертације кандидата Mp. Yousefa Abuadlle под насловом:

„Систем за детекцију упада заснован на токовима са две неуралне мреже"

"Flow-Based Intrusion Detection System With Two Neural Network Stages"

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

ИЗВЕШТАЈ

1. УВОД

1.1. Хронологија одобравања и израде дисертације

Кандидат Mp. Yousef Abuadlla уписао је докторске студије на Универзитету у Београду - Електротехничком факултету у Београду у школској 2008./2009. години. Пред лето 2013. године, кандидат је поднео предлог теме докторске дисертације. Наставно–научно веће именовало је Комисију за оцену услова и прихватање теме докторске дисертације на 765. седници одржаној 3.9.2013. Одлуком на 765. седници Изборног и наставно-научног већа Електротехничког факултета Универзитета у Београду одржане 03.09.2013. године именована је Комисија за оцену подобности теме и кандидата у саставу: др Зоран Јовановић, редовни професор, Универзитет у Београду - Електротехнички факултет, др Горан Квашчев, доцент, Универзитет у Београду - Електротехнички факултет, др Душан Старчевић, редовни професор, Универзитет у Београду – Факултет организационих наука, др Славко Гајин, доцент, Универзитет у Београду - Електротехнички факултет

Извештај Комисије за оцену услова и прихватање теме докторске дисертације Наставно–научно веће је прихватило на 771. седници одржаној 25.2.2014. godine, а Веће научних области техничких наука Универзитета у Београду дало је сагласност на тему на својој седници 31.3.2014. године.

Кандидат је предао докторску дисертацију и на 776. седници Наставно – научног већа одржаној 8.7.2014. године, именована је Комисија за преглед и оцену докторске дисертације Mp. Yousefa Abuadlle под насловом **"Flow-Based Intrusion Detection System With Two Neural Network Stages"**. За чланове комисије су именовани: др Зоран Јовановић, редовни професор, Универзитет у Београду - Електротехнички факултет (ментор), др Горан Квашчев, доцент, Универзитет у Београду - Електротехнички факултет, др Душан Старчевић, редовни професор, Универзитет у Београду – Факултет организационих наука, др Славко Гајин, доцент, Универзитет у Београду - Електротехнички факултет

1.2. Научна област дисертације

Научна област дисертације је Електротехника и рачунарство, а ужа научна област је Софтверско инжењерство. За ову ужу научну област Електротехнички факултет у Београду јесте матичан.

Дисертација је рађена под менторством професора др Зорана Јовановића. Ментор испуњава законске услове за ментора, бави се научним радом у ужој области Софтверског инжењерства, а професионално се бави заштитом података, рачунарским мрежама, паралелним рачунарима и конкурентним и дистрибуираним програмирањем

1.3. Биографски подаци о кандидату

Yousef Abuadlla рођен у месту Захра у Либији 1969. године. Након завршеног школовања до нивоа високе стручне спреме у Либији, наставља са успешном професионалном каријером. Влада Либије одлучује да стипендира његово даље школовање и 2001. године га шаље на магистарске студије на Универзитет у Београду, Електротехнички факултет. Ту завршава магистарске студије 06.10.2003. године. Наслов магистарске тезе је био:„Avoiding Mutual Exclusion of Shared Data in Real-Time Operating Systems", односно "Избегавање међусобног искључивања за дељене податке у оперативним системима за рад у реалном времену" Након додатне успешне професионалне каријере, добија стипендију Либије за докторске студије на Универзитету у Београду, Електротехнички факултет. Yousef је међу најталентованијим стипендистима Владе Либије. Пред лето 2013. године, поднео је предлог теме докторске дисертације, а одлуком на 765. седници Изборног и наставно-научног већа Електротехничког факултета Универзитета у Београду одржане. 03.09.2013. године именована је Комисија за оцену подобности теме и кандидата.

2. ОПИС ДИСЕРТАЦИЈЕ

2.1. Садржај дисертације

Докторска дисертација садржи насловну страну на српском и енглеском језику, резиме дисертације, кратак садржај, листу слика и табела, захвалнице, шест поглавља и преглед коришћене литературе, прилог, биографију кандидата и потписане изјаве. Поглавља су

насловљена на следећи начин: 1. Introduction, 2. Background, 3. Neural Networks, 4. Proposed intrusion detection systems, 5. Experimental results, 6. Conclusions and future work. Дисертација садржи 77 страна (не рачунајући изјаве и преглед коришћене литературе), 25 илустрација и 9 табела.

2.2. Кратак приказ појединачних поглавља

Прво поглавље, Introduction, састоји се из три дела. Први део овог поглавља описује проблем заштите рачунарских мрежа са посебним освртом на детекцију упада (напада). У другом делу увода је дата мотивација да се приступи изради дисертације са овом темом и на крају је дата структура и садржај дисертације.

Друго поглавље, Background, уводи појам токова у рачунарским мрежама, поступке мерења и памћења токова у мрежним уређајима и поступак њихове екстракције, како би се пренели до сервера за детекцију упада, где се ради узорковање. Затим су детаљно приказане и класификоване методе детекције упада. Посебно су упоређене предности и мане система детекције упада заснованих на два принципа: детекције аномалија у саобраћају и детекције потписа напада. Затим су представљени системи за превенцију упада, са констатацијом да је проблем детекције упада кључна компонента система превенције. На крају овог поглавља је дат кратак преглед најважнијих класа упада.

Неуралне мреже, као компонента система за детекцију упада су предмет трећег поглавља. Дат је преглед архитектура и метода учења, посебно са аспекта примене у детекцији упада. Затим су посебно анализиране мреже са алгоритмима учења са простирањем уназад. На крају су дати преглед и анализа претходних метода детекције упада помоћу неуралних мрежа.

Четврто поглавље, Proposed Intrusion Detection System, приказује структуру предложеног система и описује улогу појединих компоненти у детекцији упада. Како је предложени систем заснован на детекцији токова, детаљније су приказани начини на који су претходно предложени системи других аутора користили токове у детекцији три најважније класе напада: онемогућавање сервиса, вируса и црва. Сваки од основних модула је детаљно описан: колектор токова, модул за припрему улаза неуралних мрежа, модул за детекцију аномалија, модул за детекцију и класификацију и на крају модул за креирање аларма. Затим су описана два скупа података са којима је обављено тренирање (учење) система.

Експериментални резултати су предмет петог поглавља. Прво је описано како су спровођени експерименти, а затим су посебно анализирани резултати експеримената за модул за детекцију аномалија и за модул за детекцију и класификацију. За сваки од њих су спровођени тестови са великим бројем напада и затим приказани табеларно резултати везани за вероватноће детекције напада, лажне аларме, погрешне класификације напада и сл. Добијени резултати су детаљно дискутовани, а затим су упоређени са резултатима других аутора.

У шестом поглављу, Conclusions and Future Work, изнети су основни закључци, као и будуће активности и правци развоја и истраживања. Након тога, дат је преглед коришћене литературе.

3. ОЦЕНА ДИСЕРТАЦИЈЕ

3.1. Савременост и оригиналност

Предмет истраживања у докторској дисертацији јесте проблем решавања детекције упада (напада) у рачунарским мрежама. Тај проблем је један од тренутно најактуелнијих проблема рачунарства, посебно зато што не постоји још увек добро решење које са високим процентом вероватноће детектује нападе, а истовремено не генерише велики број лажних аларма. Брзина мрежа и количина саобраћаја на њима условљава да посао детекције упада мора да ради софтвер као што је случај у овој дисертацији.

Постоје и други системи за детекцију упада засновани на неуралним мрежама, али је истраживање у овој дисертацији специфично по неколико аспеката. Пре свега, користе се токови за детекцију упада. Затим је направљена оригинална архитектура система са две неуралне мреже, којом се ради селекција узорака над којим се откривају упади помоћу прве неуралне мреже, а тек затим се над селектованим узорцима ради детаљна детекција и класификација упада. Осим тога, детаљно су испитане различите класе неуралних мрежа и испитивано је која класа највише одговара за одговарајуће компоненте архитектуре предложеног система.

3.2. Осврт на референтну и коришћену литературу

У дисертацији су наведене 142 библиографске референце на релевантне радове из области система за детекцију упада, скупова података за нападе на мреже, особина разноврсних напада на рачунарске мреже, неуралних мрежа и др. Литература садржи најновије радове релевантне за тему дисертације. У првом и другом поглављу је дат основни преглед области, али и у трећем и четвртом поглављу су дати краћи осврти, како би се боље објаснили елементи предложеног решења.

3.3. Опис и адекватност примењених научних метода

Истраживање у оквиру предложене докторске дисертације обухватило је следеће фазе:

1. систематично проучавање литературе из области дисертације,

2. идентификацију и евалуацију досадашњих метода детекције упада, посебно оних заснованих на токовима и/или неуралним мрежама.

3. развој и имплементацију напредне архитектуре за детекцију упада са две неуралне мреже

4. спровођење експеримената са евалуацијом резултата након тестирања различитих решења за неуралне мреже на оба места у наведеној архитектури

5. поређење добијених резултата са резултатима других аутора

Наведени поступци у основи припадају и теоријским и експерименталним истраживањима, и у потпуности одговарају проблему и циљу дисертације. Примењене експерименталне методе су адекватне и валидне.

3.4. Применљивост остварених резултата

Добијени резултати могу да се преточе у производ, ако би се направило окружење у коме би се систем подвргавао новим учењима када год се појави неки нови напад. Овакви системи могу да помогну да се детаљно анализирају напади и лакше изведе њихова превенција, што је један од кључних проблема рачунарских мрежа.

3.5. Оцена достигнутих способности кандидата за самостални научни рад

Кандидат је у изради дисертације показао способност за самостални научни рад. Изградио је систематичну и критичку анализу постојећих решења, уз уочавање њихових недостатака. Развио је оригиналан систем за детекцију упада, који је упоредив или бољи од постојећих система за детекцију упада. Резултате својих истраживања објавио је у часописима од међународног значаја са значајним фактором утицаја.

4. ОСТВАРЕНИ НАУЧНИ ДОПРИНОС

4.1. Приказ остварених научних доприноса

Допринос изложене докторске дисертације је у домену развоја система за детекцију упада на мрежном нивоу. У оквиру дисертације су дати следећи научни доприноси:

- Нови оригинални двостепени систем за детекцију упада коришћењем мрежног приступа, а реализован са неуралним мрежама.
- Дефинисање најбољих неуралних мрежа за сваки од степена оригиналног система за детекцију напада.
- Висок степен класификације напада помоћу другог степена неуралне мреже у рангу најбољих до сада објављених резултата или боље.

4.2. Критичка анализа резултата истраживања

Увидом у дисертацију, полазне хипотезе и циљеве истраживања, Комисија констатује да је кандидат успешно одговорио на постављене изазове, и да резултати оправдавају почетна

очекивања. Предложен је оригиналан и темељан приступ развоју система за детекцију упада и наглашена важност унапређења у овом сегменту развоја софтвера. Оригинална архитектура и експериментално истраживање којим су дефинисане најбоље неуралне мреже чине га јединственим у односу на конкурентске приступе и употребљивим у великом броју реалних примена.

Дисертација се може сматрати важним кораком у приближавању тренутка када ће се системи за детекцију упада сматрати обавезним саставним елементом сваке рачунарске мреже. На крају, дисертација може да буде од користи будућим генерацијама студената докторских студија, инжењерима, практичарима и истраживачима које интересује ова област и који у њој желе да дају свој допринос.

4.3. Верификација научних доприноса

Кандидат је објавио следеће радове који су у непосредној вези са докторском

дисертацијом:

Међународни часописи:

1. Abuadlla Yousef, Goran Kvaščev, Slavko Gajin, Zoran Jovanovic: Flow-Based Anomaly Intrusion Detection System Using Two Stages Neural Network", Computer Science and Information Systems, ISSN: 1820-0214, Volume 11, Issue 2 (June 2014), pp 601-622, two-year impact factor (2012): 0.549. M23
2. Abuadlla Yousef, Zoran Jovanovic: International Journal of Information Technology & Computer Science (IJITCS) : Issue : July / August 2012 : Internet Computing , Informatics in E-Business and applied Computing , ISSN (Online) : 2091-1610, Volume 4/Issue 2, | Pages : 46 - 52 | Publication Date : July / August 2012. M53

Међународна конференција:

1. Abuadlla Yousef, Zoran Jovanovic: Flow-Based Anomaly Intrusion Detection System using Neural Network, International Conference on Internet Computing , Informatics in E-Business and applied Computing (ICIEACS 2012), Дубаи, 27-28 јул 2012., http://www.ijitcs.com/volume%204_No_2/Abuadlla+Yousef.pdf. M33

5. ЗАКЉУЧАК И ПРЕДЛОГ

Дисертација кандидата Мр. Yousefa Abuadlle, под насловом "Flow-Based Intrusion Detection System With Two Neural Network Stages" представља оригиналан, савремен и значајан научни допринос. Текст дисертације написан је јасно и разумљиво и добро је организован кроз поглавља и одељке. Циљеви дисертације су јасно формулисани и мотивисани, а резултати истраживања систематски изложени, тако да се научни доприноси могу недвосмислено утврдити. У спроведеним истраживањима предложена је нова архитектура за детекцију упада на основу скупљених токова са мрежних уређаја која садржи две неуралне мреже. За сваку од улога неуралних мрежа је дефинисана најбоља

врста неуралне мреже на основу експеримената. Затим је систем систематски испитан и упоређени су резултати са најбољим дотадашњим резултатима и добијени слични или бољи резултати. Објављивањем резултата својих истраживања у часопису међународног значаја са СЦИ листе, кандидат је показао способност за самосталан научни рад, а доприноси истраживања добили адекватну потврду ваљаности.

Комисија констатује да дисертација садржи оригиналне научне доприносе, испуњава све законске, формалне и суштинске услове, као и све критеријуме који се уобичајено примењују приликом вредновања докторских дисертација на Електротехничком факултету Универзитета у Београду. Комисија са задовољством предлаже Наставно-научном већу Електротехничког факултета Универзитета у Београду да се докторска дисертација под називом "Flow-Based Intrusion Detection System With Two Neural Network Stages"кандидата Мр. Yousefa Abuadlle прихвати, а кандидату одобри усмена одбрана.

У Београду, 5.9.2014.

ЧЛАНОВИ КОМИСИЈЕ

др Зоран Јовановић, редовни професор
Универзитет у Београду – Електротехнички факултет

др Горан Квашчев, доцент
Универзитет у Београду – Електротехнички факултет

др Душан Старчевић, редовни професор
Универзитет у Београду – Факултет организационих наука

Slavko Gajin

др Славко Гајин, доцент
Универзитет у Београду – Електротехнички факултет