

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Подобност теме и кандидата мр Жума Ибрахим (*Juma Ibrahim*) за израду докторске дисертације

Одлуком бр. 5051/14-1 од 23.5.2019. године, именовани смо за чланове Комисије за оцену подобности теме и кандидата мр Жуме Ибрахима (*Juma Ibrahim*) за израду докторске дисертације и научне заснованости теме:

**„Архитектура система за препознавање неправилности у мрежном саобраћају
засновано на анализи ентропије“**

(енг. „*An architecture for network traffic anomaly detection system based on entropy analysis*“).

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

ИЗВЕШТАЈ

1. Подаци о кандидату

1.1. Биографски подаци

Кандидат је рођен 8. децембра 1965. године у Либији, у граду Алријајинах (*Alriyayinah*). Основне студије је завршио на Универзитету у Триполију, Природно математички факултет, на катедри за рачунарске науке.

Магистарске академске студије за уписао на Универзитету у Београду - Електротехничком факултету, а спроведено истраживање се односило на могућност примене оперативних система у реалном времену као део информационо-комуникационе инфраструктуре у научно-истраживачким центрима. Магистарски рад под називом „*Real-time operating system*“ је одбранио 15.10.1997,

Од маја 1989. до марта 2006. године је био запослен у научно-истраживачком центру у Триполију на радном месту програмера, где је радио на пословима имплементације софтверских система, инсталацији и одржавању софтвера и рачунара, као и обукама за различите врсте корисничких апликација (MS Windows, MS Office, Unix) и појединих програмских језика.

Периоду од јуна 2006. до новембра 2013. године запослен је на Колеџу за рачунарске технологије Триполи (ССТТ), у Либији као асистент у настави. У том периоду је био директор канцеларије за научне академске послове Колеџу за рачунарске технологије Триполи. Такође је држао предавања из различитих рачунарских области и био CCNA инструктор у оквиру Cisco мрежне академије Триполи (*Cisco Network Academy Tripoli*) и Cisco мрежне академије Инџела (*Cisco Network Academy Injella*) у Либији.

Током докторских студија спроводи истраживачки рад у широј области технологија рачунарских мрежа, истражујући и софтверски дефинисане мреже (SDN), да би се убрзо фокусирао на област безбедности рачунарских мрежа. Истраживање у овој области је усмерено на системе за детекцију напада (*Intrusion Detection Systems*) на бази ентропије и машинског учења, из чега је аутор или коаутор у три научна рада објављена и презентована на међународним стручним конференцијама.

Стипендиста је Министарства просвете Републике Либије на докторским академским студијама.

1.2. Стечено научноистраживачко искуство

У оквиру магистарских академских студија кандидат је спровео истраживање из области оперативних система у реалном времену, са посебним акцентом на њихову примену као део информационо-комуникационе инфраструктуре у научно-истраживачким центрима. Магистарски рад под називом „*Real-time operating system*“ је одбранио 15.10.1997, под менторством проф. др Душана Велашевића.

Докторске академске студије је уписао 2014. године на Универзитету у Београду – Електротехничком факултету, на морулу Рачунарска техника и информатика. Током студија је успешно и на време положио све предвиђене испите са просечном оценом 9.8, и то:

1. Одабрана поглавља из архитектуре рачунарских система, оцена 10 (9 ЕДП бодова)
2. Бежичне информационе мреже, оцена 10 (9 ЕДП бодова)
3. Интернет програмирање, оцена 10 (9 ЕДП бодова)
4. Локалне рачунарске мреже, оцена 10 (9 ЕДП бодова)
5. ТЦП/ИП архитектура, оцена 10 (9 ЕДП бодова)
6. Савремене радио-технологије, оцена 10 (9 ЕДП бодова)
7. Софтверски дефинисане мреже, оцена 10 (9 ЕДП бодова)
8. Енглески језик, оцена 8 (6 ЕДП бодова)
9. Сензорске мреже, оцена 10 (9 ЕДП бодова)
10. Сигурност и заштита рачунарских система, оцена 10 (9 ЕДП бодова),

Кандидат је остварио укупно 120 ЕСП бодова, укључујући и бодове остварене кроз спроведени истраживачки рад, чији су резултати презентовани на међународним конференцијама.

Јавна усмена одбрана предложене теме докторске дисертације је спроведена 19.6.2019. године на Електротехничком факултет Универзитета у Београду. У трајању од 40 минута кандидат је у најсажетијем облику изложио област и предмет истраживања, актуелност истраживања, постојећа решења са критичким освртом, као и своје полазне хипотезе, планирану методологију рада, очекиване, као и већ остварене резултате, укључујући и остварени научни допринос. На усменој одбрани су били присутни сви чланови Комисије, а на сва њихова питања кандидат је успешно одговорио.

1.2.1. Објављени радови

М33-Саопштење са међународног скупа штампано у целини

1. Ibrahim J., Timčenko V., Gajin S.: *"A comprehensive flow-based anomaly detection architecture using entropy calculation and machine learning classification"*, ICIST 2019, 9th International Conference on Information Society and Technology, Kopaonik, Serbia on Mar 10-13, 2019, pp. 138-143.
2. Timčenko V., Ibrahim J., Gajin S.: *"The Hybrid Machine Learning Support for Entropy Based Network Traffic Anomaly Detection"*, ICIST 2019, 9th International Conference on Information Society and Technology, Kopaonik, Serbia on Mar 10-13, 2019, pp. 144-149.
3. Ibrahim J., Gajin S.: *"SDN-Based Intrusion Detection System Literature review"*, 16th International Symposium INFOTEH-JAHORINA, Vol. 16, March 2017, pp. 621-624
4. Ibrahim J.: *"The role of open source software in the success of the e-government"*, The First International Conference on Electronic Management, 1-4 June 2010, Tripoli, Libya, pp. 110-113.
5. Ibrahim J., Darweel H.: *"The digital gap in Arab world and its impact in e-learning"*, The first International Conference on E-Learning For ALL (ELFA2010), 3-5 June 2010, Hammamet, Tunisia.

М63-Саопштење са скупа националног значаја штампано у целини

1. Al-ahrash M., Abuajella M., Ibrahim J.: *"Information technology and computer science"*, Aljabal Algharbi University, Faculty of science 25-27 April 2009, Gharyan, Libya.
2. Ibrahim J.: *"Digital gap in the Arab world"*, The Islamic organization for education, culture and science, 5-7 October 2009, Kairouan, Tunisia.
3. Ibrahim J., Shfelow M.: *"Security requirements for the electronic archive"*, The general company of electricity, 19-20 December 2009, Tripoli, Libya.

1.3. Оцена подобности кандидата за рад на предложеној теми

Комисија је размотрила све претходно наведене резултате досадашњег рада и стечена искуства кандидата. На основу тога Комисија је стекла увид у способности кандидата за научно-истраживачки рад и његове могућности да током израде докторске дисертације оствари резултате који ће бити приказани и оцењени од стране међународне научне заједнице. Став Комисије је да мр Жума Ибрахим испуњава потребне услове да приступи изради докторске дисертације под наведеном темом.

2. Предмет и циљ истраживања

Огроман развој информационих технологија и Интернета, као и све већа употреба ове технологије у свим областима живота, довели су до појаве различитих врста сигурносних претњи и напада. Традиционални сигурности алати у рачунарским мрежама, као што су мрежне баријере (*firewall*) и анализа пакета на бази потписа (*Signature-based Deep Packet Inspection*), више не представљају довољну заштиту у рачунарским мрежама, јер нису у стању да детектује нове облике напада (тзв. *Zero-day attack*), чак и ако они представљају незнатну модификацију познатих напада. Такође, методе детекције засноване на потпису су немоћне у откривању напада које се спроводе шифрованим саобраћајем.

Са друге стране, технике детекције напада базиране на анализи мрежног саобраћаја (*Network Behaviour Analysis*) и уочавање неправилности у односу на уобичајено понашање (*Anomaly Detection*) превазилазе горе наведена ограничења. Велики број научних радова у овој области обрађује различите методе детекције различитих врста напада на бази анализе аномалија у мрежном саобраћају. Анализа се односи на податке о мрежном саобраћају, у облику логова мрежних активности, које се прикупљају са крајњих уређаја или директно са рутера у мрежи. Иако први приступ може да пружи више података и детаља о мрежним активностима крајњих уређаја (нпр, величина ТЦП прозора, време пропагације пакета, цитер и други статистички подаци који се односе на појединачне мрежне токове), прикупљање ових података за већи број уређаја је веома отежано, чак и у експерименталне сврхе. Стога се последњих година истраживање у овој области претежно базира на подацима који су добијени са рутера посредством NetFlow протокола [1]. Ови подаци се односе на појединачне комуникационе токове у мрежи (*flow*), који су идентификовани преко ИП адреса, протокола и ТЦП/УДП портова учесника, а којима је придружен укупан број пренетих бајтова и пакета у овим комуникационим токовима.

Велики број радова у вези анализе мрежног саобраћаја односи се на примену различитих алгоритама машинског учења (*Machine Learning*). Документовано је да многи алгоритми надгледаног машинско учење (*Supervised Machine Learning*) дају задовољавајуће резултате у препознавању напада у мрежи. Ипак за њихово учење у фази тренирања неопходно је поседовање означеног сета података (*Labelled Dataset*), где је сваки податак о мрежној активности унапред означен као нормалан или као аномалија (напад одређене врсте). У литератури је такође изражен проблем недостатка кредибилних означених сетова података. Велики број радова се годинама базирао на првом сету података ове врсте, под називом КДД-99, који се већ одавно сматра застарелим и неадекватним за новије врсте напада. Тек последњих година у истраживачкој заједници су се појавили новији сетови означених података на бази NetFlow протокола (UNSW-NB15, CTU-13) [2]. Практична имплементација ових система у продукционим мрежама уводи још већи проблем, будући да стварне мреже имају различите карактеристике мрежних активности које нису познате унапред, а за њих не постоји означени сет података за потребе тестирања. Сличан приступ у литератури је заступљен и у случају коришћења неуронских мрежа (*Neural Network*).

Потребно је истаћи да технике машинског учења и неуронских мрежа по правилу захтевају интензивну обраду, што их чини захтевним по питању рачунарских ресурса и времена извршавања. Ово је посебно изражено код обраде веће количине података, а посебно за практичну примену у реалном времену. Стога све већу пажњу истраживача привлаче технике откривања аномалија базиране на рачунању ентропије дистрибуција вредности различитих параметара који се могу извести из података о мрежном саобраћају прикупљених преко NetFlow протокола [3][4][5]. Том приликом се подаци који се односе на дужи временски период деле у мање временске интервале, тзв. епохе, у којима се спроводи агрегација података по различитим критеријумима, на основу чега се рачуна ентропија [6]. Одступање вредности ентропије за поједине параметре у одређеним периодима указује на промену

структуре саобраћаја [7]. Иако овај приступ захтева далеко једноставније процесирање, отварају се нови проблеми, као што су:

- дефинисање критеријума за препознавање одступања ентропије које је резултата напада у односу на варијације које се јављају код нормалног саобраћаја,
- детекција напада се односи на интервале целих епоха, па је потребно издвојити стварне догађаје и учеснике у уоченим нападима
- различите врсте напада и њихове модификације изазивају промене вредности ентропија различитих параметара, па је потребно сагледавање и анализа већег броја ових вредности, како би се исправно препознали напади и остале аномалије.

Претходно истакнути недостаци и ограничења наведених приступа отварају простор за истраживање нових техника и методологије детекција аномалија у мрежном саобраћају у циљу откривања сигурносних претњи, што ће да представља основни предмет истраживања предложене теме докторске дисертација.

Циљ истраживања је развој нове методе за ефикасну детекцију аномалија у мрежном саобраћају на бази појединачних комуникационих токова у циљу правовременог уочавања неправилности у саобраћају као индикације сигурносних претњи рачунарским мрежама, са посебним акцентом на могућност практичне примене у продукционим рачунарским мрежама. Практична примена развијене методологије ће се огледати кроз предлог нове архитектуре система за детекцију аномалија у мрежном саобраћају, који на ефикасан и флексибилан начин комбинује различите методе детекције и анализе. Очекује се да се нова метода првенствено базира на рачунању ентропије, по потреби комбинујући друге технике детекције неправилности (машинско учење, неуронске мреже), анализе узрока (*Root Cause Analysis*) и метода одлучивања (*Fuzzy Logic*).

Главни изазови представљају одређивање методе за прецизно успостављање границе између нормалног и неправилног понашања у мрежи, како би се избегло лажно алармирање и постигао висок ниво откривање аномалија. Такође је битно да предложена архитектура и методологија буде применљива за различите врсте и интензитете мрежног саобраћаја, различите обрасце понашања учесника у мрежним комуникацијама, као и различите врсте напада и аномалија (нпр. DDoS, BOTNET, скенирање мреже и уређаја, погађање лозинки итд.).

Значај предложеног истраживања се огледа у чињеници да је неопходан константан развој и унапређење система детекције напада у рачунарским мрежама, како би се ефикасно одговорило на све присутније нове и софистициране нападе и остале сигурносне претње. Ова област је стога и даље веома актуелна и представља предмет великог броја истраживања и научних радова.

РЕЛЕВАНТНИ БИБЛИОГРАФСКИ ИЗВОРИ:

- [1] Claise, Benoit. Cisco systems netflow services export version 9. No. RFC 3954. 2004.
- [2] Sebastian Garcia, Martin Grill, Jan Stiborek and Alejandro Zunino, "An empirical comparison of botnet detection methods" Computers and Security Journal, Elsevier. 2014. Vol 45, pp 100-123. <http://dx.doi.org/10.1016/j.cose.2014.05.011>
- [3] Nychis, G.; Sekar, V.; Andersen, D.G.; Kim, H.; Zhang, H. An Empirical Evaluation of Entropy-based Traffic Anomaly Detection. In Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement (IMC '08), Vouliagmeni, Greece, 20–22 October 2008; pp. 151–156.
- [4] P. Bereziński, B. Jasiul, and M. Szpyrka, "An entropy-based network anomaly detection method," Entropy, vol. 17, no. 4, pp. 2367–2408, 2015.

- [5] T. Liu, Z. Wang, H. Wang, and K. Lu, "An entropy-based method for attack detection in large scale network," *Int. J. Comput. Commun. Control*, vol. 7, no. 3, pp. 509–517, 2012.
- [6] C. E. Shannon, "A mathematical theory of communication," *Bell system technical journal*, 27(3), pp. 379-423, 1948.
- [7] Winter, P., Lampesberger, H., Zeilinger, M., & Hermann, E. (2011, October). "On detecting abrupt changes in network entropy time series". In *IFIP International Conference on Communications and Multimedia Security* (pp. 194-205). Springer, Berlin, Heidelberg.

3. Полазне хипотезе

Основне хипотезе од којих се полази у истраживању су следеће:

- Различити напади у рачунарским мрежама узрокују различита одступања од уобичајеног понашања, који се могу препознати као обрасци промена у структури мрежног саобраћаја.
- Аномалије у структури мрежног саобраћаја узрокују промену ентропије одређених параметара, а за њихову ефикасну примену у детекције појединачних врста напада могуће је дефинисати одговарајућа правила која узимају у обзир одступања вредности ентропије од уобичајених вредности.
- Класификацијом улазног саобраћаја, односно поделом на мање класе саобраћаја по одређеним критеријумима, могуће је повећати прецизност у детекцији аномалија мањег интензитета, које су не приметне када се иста техника примењује на нивоу целокупног саобраћаја.
- Могуће је дефинисати модуларну архитектуру система за детекцију напада, која на флексибилан начин користи различите технике анализе и детекције, чиме се омогућава ефикасна детекција напада и аномалија у реалном времену у стварним рачунарским мрежама са различитим и унапред непознатим начинима коришћења мрежних сервиса и комуникација.

4. Научне методе истраживања

Методе које ће бити примењене у истраживању су следеће:

- Анализа различитих техника и приступа у детекцији напада на бази образаца у структури мрежног саобраћаја, а које су документоване у научној литератури.
- Анализа адекватних сетова означених података комуникационих токова мрежног саобраћаја, који су коришћени у научној литератури и другим истраживањима.
- Анализа актуелних напада и других сигурносних претњи које су присутне у стварним рачунарским мрежама.
- Моделовање структуре и интензитета појединачних напада, генерисање података који осликавају њихову манифестацију, као и генерисање нових означених сетова података.
- Рачунање ентропије по различитим параметрима означеног сета података применом одговарајућег софтвера, анализа резултата, корелација резултата у односу на врсте напада.
- Верификација полазних хипотеза на основу спроведених експеримената и анализе резултата.

5. Очекивани научни допринос

У оквиру предложене докторске дисертације очекују се следећи доприноси:

- Реализација оригиналног дизајна модуларне и флексибилне архитектуре система за детекцију напада и аномалија у продукционим рачунарским мрежама.
- Успостављање систематичног приступа рачунању ентропије различитих атрибута података мрежних токова.
- Допринос бољем разумевању образаца понашања појединачних врста напада.
- Доказивање ефикасности концепта предложене архитектуре система, како појединачних модула, тако и система у целини.

6. План истраживања и структура рада

Имајући у виду постављене циљеве, план истраживања је следећи:

- Анализа проблема и различитих приступа презентованих у научној литератури.
- Анализа постојећих сетова података и резултата примене ентропије
- Генерисање нових сетова података за различите моделе напада
- Рачунање ентропије за различите комбинације параметара над генерисаним сетовима података, анализа резултата за различите моделе напада
- Дефинисање правила за препознавање појединачних напада на основу промена ентропије
- Дефинисање архитектуре система за детекцију напада, уз доказивање концепта ефикасности и изводљивости практичне примене у продукционим рачунарским мрежама.

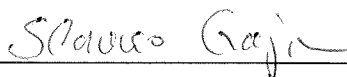
7. Закључак и предлог

Комисија је мишљења да је предложена тема докторске дисертације „Архитектура система за препознавање неправилности у мрежном саобраћају засновано на анализи ентропије“ адекватна у смислу наведених непосредних циљева рада, очекиваних резултата и научних доприноса, као и у контексту актуелности научних истраживања у предложеној области. Након увида у наведене резултате досадашњег рада кандидата мр Жуме Ибрахима, Комисија је донела одлуку да је он способан за научно-истраживачки рад и за реализацију предвиђених истраживања. Одлука је донета имајући у виду његове досадашње стручне резултате остварене током основних и докторских студија, као и на основу његовог досадашњег истраживачког ангажовања, напретка и остварених резултата. Такође, Комисија констатује да тема рада припада области Рачунарске технике и информатике, за коју је Електротехнички факултет Универзитета у Београду матичан и за ментора рада се предлаже др Славко Гајин, ванредни професор Електротехничког факултета Универзитета у Београду. Из тог разлога уз овај Извештај је приложен и списак радова проф. др Славка Гајина који га квалификују за ментора.

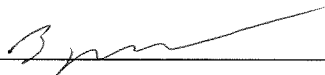
Имајући у виду чињенице наведене у овом извештају, Комисија предлаже Наставно-научном већу Електротехничког факултета у Београду да прихвати тему докторске дисертације „Архитектура система за препознавање неправилности у мрежном саобраћају засновано на анализи ентропије“ и да кандидату мр Жуми Ибрахиму омогући да приступи њеној изради.

У Београду, 20.8.2019. године

ЧЛАНОВИ КОМИСИЈЕ



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



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