

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Подобност теме и кандидата **Ђорђа Јовановића**, мастер инжењера електротехнике и рачунарства, за израду докторске дисертације **„Рано откривање уређаја заражених ботнет малвером коришћењем метода детекције аномалија мрежних токова”** (на енглеском **„Early discovery of the devices infected with botnet malware using network flow anomaly detection”**)

Одлуком бр. 5001/18-01 од 26.10.2021. године, именовани смо за чланове Комисије за оцену подобности теме и кандидата Ђорђа Јовановића за израду докторске дисертације и научне заснованости теме **„Рано откривање уређаја заражених ботнет малвером коришћењем метода детекције аномалија мрежних токова”** (на енглеском **„Early discovery of the devices infected with botnet malware using network flow anomaly detection”**)

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

ИЗВЕШТАЈ

1. Подаци о кандидату

1.1. Биографски подаци

Ђорђе Јовановић је рођен 7. августа 1994. године у Београду, Република Србија, где је са одличним успехом завршио Основну школу „Стеван Дукић“ и Прву београдску гимназију. У септембру 2017. године дипломирао је на Електротехничком факултету у Београду на смеру за Рачунарску технику и информатику са просечном оценом 9,17 и оценом 10 на дипломском испиту са темом „Виртуелне мреже реализоване у СДН технологији“. У септембру 2018. године завршио је мастер студије на Електротехничком факултету у Београду на смеру за Рачунарску технику и информатику са просечном оценом 10,00 и оценом 10 на дипломском испиту са темом „Имплементација лабораторијског окружења за софтверски дефинисане мреже помоћу класе Zodiac FX свичева“.

Докторске 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. У оквиру научноистраживачког рада, бавио се применом метахеуристика, блокчејн технологијама, машинским учењем и софтверски дефинисаним мрежама. Објавио је 16 радова у домаћим часописима и конференцијама, од којих 7 као првоименовани аутор.

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

1.2. Стечено научноистраживачко искуство

Кандидат је докторске академске студије на изборном подручију Електротехника и рачунарство на ЕТФ-у уписао 2018/2019. школске године. Од тренутка уписа до тренутка подношења Захтева за одобрење докторске дисертације положио је све испите (са просечном оценом 10,0) и обавио све обавезе предвиђене докторским академским студијама на изборном подручију Електротехника и рачунарство. Списак положених испита и обављених обавеза је дат у следећој табели:

бр.	Назив испита / обавезе	Оцена	ЕСПБ	Датум
1	Стохастички модели	10	9	28.09.2020.
2	Локалне рачунарске мреже	10	9	10.07.2020.
3	Моделовање и мерење рачунарских перформанси	10	9	14.07.2020.
4	Неуралне мреже	10	9	07.02.2020.
5	Енглески језик	10	6	03.02.2020.
6	Медицинска информатика	10	9	17.09.2019.
7	Виртуелна стварност	10	9	10.07.2019.
8	ТЦП/ИП архитектура	10	9	10.07.2019.
9	Мултимедијални системи - одабрана поглавља	10	9	13.02.2019.
10	Софтверски дефинисане мреже	10	9	13.02.2019.
11	Студијски истраживачки рад II		15	30.09.2020.
12	Научно стручни рад		3	30.09.2020.
13	Студијски истраживачки рад I		15	30.09.2019.

Ђорђе Јовановић се у оквиру научноистраживачког рада на Математичком институту САНУ и на Електротехничком факултету Универзитета у Београду бави детекцијом напада на информациону безбедност, посебно анализом ботнета и њихових карактеристичних образаца понашања, применом метахеуристика, блокчејн технологијама, машинским учењем и софтверски дефинисаним мрежама. Циљ истраживања кандидата у оквиру научног рада на изради докторске тезе је проналажење механизма за детекцију командне и контролне комуникације уређаја заражених ботнет малвером (ботова) коришћењем посебних статистичких одлика мрежних токова. Како би се добили посебни статистички параметри мрежних токова (тзв. intra-flow статистика) кандидат Ђорђе Јовановић је развио и предложио механизам за екстракцију ових параметара коришћењем софтверски дефинисаних мрежа одабирањем параметара мрежних токова док су још увек активни. Таквим приступом, у случају добијања адекватне тачности препознавања ботнет комуникације би се омогућила рана детекција ботнет мрежа уз коришћење за више редова величине мањих рачунарских ресурса (простора за складиштење, оперативне меморије и процесорског оптерећења за обраду).

Дана 03.11.2021. године одржана је јавна усмена одбрана теме докторске дисертације (докторски испит) пред Комисијом у саставу: др Жарко Станисављевић, ванредни професор са Електротехничког факултета; др Горан Квашчев, ванредни професор са Електротехничког факултета; др Татјана Давидовић, научни саветник из Математичког института САНУ. Оцена Комисије је да је кандидат Ђорђе Јовановић задовољио све критеријуме и одбранио предложену тему докторске дисертације.

У наставку је списак радова који показују резултате досадашњег рада и афинитета који су у складу са предложеном дисертацијом кандидата Ђорђа Јовановића.

(M33) Саопштења са међународних скупова штампана у целини

- [1] Ramljak, D., Davidović, T., Urošević, D., Jakšić-Krüger, T., Matijević, L., Todorović, M., **Jovanović, Đ.**, Combinatorial Optimization for Self Contained Blockchain: An Example of Useful Synergy, Proc. XLVIII Symposium on Operational Research, SYMOPIS 2021, Banja Koviljača, Serbia, Sept. 20-23, 2021, pp. 285-290.
- [2] Milenković, Branislav; **Jovanović, Đorđe**; Krstić, Mladen; Application of Particle Swarm Optimization for classical engineering problems; XX међународни симпозијум INFOTEH-JAHORINA 2021, 17 - 19. mart 2021, Jahorina, Istočno Sarajevo, Republika Srpska, Bosna i Hercegovina; 153-157
- [3] Milenković, Branislav; **Jovanović, Đorđe**; Application of Denavit-Hartenberg method to robot model KUKA IR 161/15.0; X International Scientific Conference Heavy Machinery HM2021, Faculty of Mechanical and Civil Engineering Kraljevo, Vrnjačka Banja, 23-25 June 2021; D.15-D.18
- [4] Krstić, Mladen; Milenković, Branislav; **Jovanović, Đorđe**; Numerical analysis of wagon leaf spring using Ansys software package; X International Scientific Conference Heavy Machinery HM2021, Faculty of Mechanical and Civil Engineering Kraljevo, Vrnjačka Banja, 23-25 June 2021; E.39-E.43
- [5] **Jovanović, Đorđe**; Milenković, Branislav; Krstić, Mladen; Application of grasshopper optimization algorithm in mechanical engineering; Young Researchers Conference, Belgrade, Serbia, September 28 2020; 1-6
- [6] **Jovanović, Đorđe**; Krstić, Mladen; Milenković, Branislav; Kinematic analysis of complex mechanism using SAM; Conference on Mechanical Engineering Technologies and Applications COMETA 2020, Faculty of Mechanical Engineering East Sarajevo, November 26-28. 2020
- [7] **Jovanović, Đorđe**, Scientific Calculation: Example of Graphic Representation for Main Fractional Order Modes of Fractional Type Forced Vibrations Using Convolutional Integral, *7th International Congress of Serbian Society of Mechanics*; 140-142, 2019
- [8] **Jovanović, Đorđe**; Vuletić, Pavle; Analysis and Characterization of IoT Malware Command and Control Communication; 27th Telecommunications Forum, TELFOR 2019, Belgrade, Serbia, Serbia 26-27 Nov. 2019; 1-4
- [9] Andjelka Hedrih, **Djordje Jovanovic**, Katica (Stevanovic) Hedrih; Theoretical Odeling of Forced Oscillations of Herbaceous Plant Inflorescence-influence of Branching Angle; XXV ICTAM 2020+1, August 22-27 2021. Milano, Italy

(M34) Саопштење са међународног скупа штампано у изводу

- [1] **Jovanović, Đorđe**; Milenković, Branislav; Determination of dynamic load factor for single element camshaft using various laws of follower motion; 8th International Congress of Serbian Society of Mechanics, Kragujevac, Serbia, June 28-30 2021; 52-53
- [2] Milenković, Branislav; **Jovanović, Đorđe**; Volume optimization of the worm gear using biologically inspired algorithm; 8th International Congress of Serbian Society of Mechanics, Kragujevac, Serbia, June 28-30 2021; 579-580
- [3] Hedrih, Andelka; Atanasovska, Ivana; **Jovanović, Đorđe**; Inflorescence Inspired Complex Oscillatory Systems; Symposium Nonlinear dynamics - Scientific work of Prof. Dr Katica (Stevanovic) Hedrih, September 04 - 06, 2019

[4] Vukšić Popović, Marija; **Jovanović, Đorđe**; Improvement of Train Dynamics Using Non-linear Modelling of Friction Draft Gear; Symposium Nonlinear dynamics - Scientific work of Prof. Dr Katica (Stevanovic) Hedrih, September 04 - 06, 2019

(M51) Рад у врхунском часопису националног значаја

[1] Milenković, Branislav; Krstić, Mladen; **Jovanović, Đorđe**; Primena algoritma sivog vuka za rešavanje inženjerskih optimizacionih problema; Tehnika 2021, vol. 76, br. 1, str. 50-57

(M52) Рад у истакнутом националном часопису

[1] Milenković, Branislav; **Jovanović, Đorđe**; Krstić, Mladen; Application of particle swarm optimization for classical engineering problems; International Journal of Electrical Engineering and Computing (IJECE); 42-49

(M53) Рад у националном часопису

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

(M63) Саопштење са скупа националног значаја штампано у изводу

[1] **Jovanović, Đorđe**; Milenković, Branislav; The use of FBG sensors in smart railway; 13th Student projects conference IEEEESTEC, November 2020, Niš; 35-38

1.3. Оцена подобности кандидата за рад на предложеној теми

Приликом писања овог Извештаја, Комисија је размотрила све претходно наведене чињенице и резултате у досадашњем раду Ђорђа Јовановића. Са посебном пажњом су размотрена искуства у истраживачком раду и узимајући све наведено, Комисија је стекла увид у његову способност за научно истраживачки рад и рад на предложеној теми докторске дисертације, која је, такође, препозната и вреднована и од стране научне заједнице.

2. Предмет и циљ истраживања

Предмет истраживања у оквиру предложене теме докторске дисертације је детекција ботнета анализом аномалија у статистичким параметрима мрежних токова карактеристичним за ботнете. Ботнети представљају скупове рачунара заражених вирусима који су путем рачунарских мрежа повезани у виртуелне инфраструктуре које се користе да би се извршиле различите врсте илегалних активности, попут ДДос (енг. *Distributed Denial of Service*) напада или дистрибуције малициозних садржаја [1]. Већина досадашњих истраживања у области детекције ботнета се оријентисала у правцу детекције ботнет напада након што се исти догодио [2]. Циљ оваквог приступа није превенција напада, што је лоше обзиром на штету коју овакви напади могу нанети, те самим тим проблем ране детекције ботнет саобраћаја постаје све важнији. Предмет истраживања у оквиру докторске дисертације је анализа карактеристичних облика понашања различитих ботнет малвера и њихових механизма комуникације (тзв. *Command and control* комуникација) са циљем предлагања оригиналног скупа одлика мрежног саобраћаја и методе за рану детекцију која ће бити у стању да сузбије ботнет мреже пре него што до било каквих напада дође, а која ће такође тежити да пронађе оптималан баланс између количине обрађених података и тачности детекције. Предложено истраживање је у складу са тренутно раширеним трендом коришћења алата и метода вештачке интелигенције за детекцију малициозних понашања.

Циљ истраживања је развој методологије и система за детекцију ботнет саобраћаја заснованог на технологији програмабилних мрежних уређаја и алгоритмима и техникама вештачке интелигенције. Постојеће методе детекције ботнета су усмерене у више праваца: ка детекцији карактеристичних DNS упита [3][4] због механизма које користе неки ботнети (тзв. DGA – *Domain Generation Algorithm*), инспекцији заглавља мрежних пакета [5][6], и инспекцији целих мрежних пакета [7][8]. Користе се методе машинског учења [9][10], дубоког учења [11][12], и хибридних метахеуристика [13][14][15]. Мана методе инспекције заглавља мрежних пакета јесте та што не постоји увид у врсту или величину порука између два уређаја, док инспекција целих мрежних пакета представља, са једне стране, велики захтев за безбедносни систем у погледу меморијског и складишног простора, као и касније потребних капацитета за процесирање, а са друге стране није оправдана јер је данас већина садржаја пакета енкриптована. У досадашњим истраживањима су се за детекцију напада, али не и детекцију ботнет комуникације пре напада, као ресурсно економична метода, често користили параметри мрежних токова (енг. *network flow*), који садрже мању количину података него у случају параметара прикупљених из мрежних заглавља те самим тим имају ограничену могућност детекције малициозног понашања. Циљ истраживања је разматрање могућности и развој методе извлачења и коришћења богатијих статистичких параметара мрежних токова добијених коришћењем програмабилних мрежних уређаја, који до сада нису анализирани (статистике параметара унутар појединачних мрежних токова).

У литератури постоји више познатих скупова података за детекцију малициозног понашања на мрежи, при чему не постоји конзистентна методологија прикупљања, бележења и анализе података. Један од проблема досадашњег истраживања у овој области је то што се у радовима често нису користили конзистентни скорови као ни адекватне методологије у ситуацијама неуравнотежених величина скупова бенигних и малициозних података који су у случају проблема у области информационе безбедности чести (увек је много више нормалног од малициозног понашања). Такође, постоје недостаци скупова података који се користе. Већина скупова података је прикупљена у кратком временском интервалу, те се нису могле посматрати потенцијалне промене у понашању одређене класе малициозног ботнет софтвера које су у реалним условима честе. Други недостатак јесте тај што већина скупова података садржи само једну класу малвера, те ће постојати проблеми са детектовањем малвера других класа. Такође постоји проблем што су чак и неки скорашњи радови урађени на скуповима података снимљеним пре чак 20 година [16][17], што представља проблем будући да су се у међувремену појавиле многе друге класе малвера и начини за избегавање механизма детекције. Стога је један од циљева истраживања и формирање квалитетног скупа података који је добијен динамичком анализом реалног злонамерног ботнет саобраћаја прикупљеног у лабораторијском окружењу током дужег временског периода и обухвата већи број класа малвера.

Значај истраживања је вишеструк. Најважнији допринос је предлог методологије и система за добијање унапређеног и проширеног скупа одлика мрежних токова (статистике параметара унутар појединачних мрежних токова) коришћењем програмабилних мрежних уређаја. Ова методологија ће омогућити брзу детекцију малициозног понашања већег броја класа малвера пре него што до било каквог напада дође, уз смањење потребних рачунарских ресурса. Нови скуп одлика мрежних токова се може користити у системима за детекцију злонамерног саобраћаја. Такође биће оформљен адекватан скуп података у лабораторијском

окружењу који ће обухватати више класа различитих малвера. За детекцију ће се користити методе детекције аномалија засноване на вештачкој интелигенцији. Примена статистика параметара унутар појединачних мрежних токова и метода вештачке интелигенције повећава шансу за рану детекцију будућих облика злонамерног понашања док су сами мрежни токови активни и пре него што напад почне. Актуелност и значај предложене теме потврђује и већи број научно-истраживачких радова из ове области публикованих у међународним часописима, међу којима су:

- [1] Gernot Vormayr, Tanja Zseby, and Joachim Fabini, Botnet Communication Patterns, "Communications Surveys & Tutorials", DOI 10.1109/COMST.2017.2749442
- [2] Kurniabudi et al., "CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection", IEEE Access, Volume 8, 2020, DOI: 10.1109/ACCESS.2020.3009843
- [3] Wang et al., "DBod: Clustering and detecting DGA-based botnets using DNS traffic analysis", Computers & Security 64 (2017) 1–15
- [4] Alieyan et al., "A survey of botnet detection based on DNS", Neural Comput & Applic DOI 10.1007/s00521-015-2128-0
- [5] Mathurb et al., "Botnet Detection via mining of network traffic flow", International Conference on Computational Intelligence and Data Science (ICCIDS 2018), Procedia Computer Science 132 (2018) 1668–1677
- [6] Blaise et al., „Detection of zero-day attacks: An unsupervised port-based approach“, Computer Networks journal DOI: <https://doi.org/10.1016/j.comnet.2020.107391>
- [7] Ali Zand, Giovanni Vigna, Xifeng Yan, Christopher Kruegel, "Extracting Probable Command and Control Signatures for Detecting Botnets", 2014
- [8] Guofei Gu, Junjie Zhang, and Wenke Lee, „BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic“, Computer Science and Engineering Faculty Publications
- [9] Imtiaz Ullah and Qusay H. Mahmoud, „A Two-Level Flow-Based Anomalous Activity Detection System for IoT Networks“, Electronics 2020, 9, 530; doi:10.3390/electronics9030530
- [10] Fadi Saloa, Ali Bou Nassifa,b, Aleksander Essex, „Dimensionality Reduction with IG-PCA and Ensemble Classifier for Network Intrusion Detection“, Computer Networks, DOI: <https://doi.org/10.1016/j.comnet.2018.11.010>
- [11] Popoolaa et al., „Stacked Recurrent Neural Network for Botnet Detection in Smart Homes“, Computers and Electrical Engineering, 2021.
- [12] Popoola, S.I.; Adebisi, B.; Ande, R.; Hammoudeh M.; Anoh, K.; Atayero, A.A. „SMOTE-DRNN: A Deep Learning Algorithm for Botnet Detection in the Internet-of-Things Networks“. Sensors 2021, 21, 2985. <https://doi.org/10.3390/s21092985>
- [13] Zhou et al., „Building an efficient intrusion detection system based on feature selection and ensemble classifier“, Computer Networks, DOI: <https://doi.org/10.1016/j.comnet.2020.107247>
- [14] Asadi, M., Jabraeil Jamali, M. A., Parsa, S., & Majidnezhad, V. (2020). Detecting botnet by using particle swarm optimization algorithm based on voting system. *Future Generation Computer Systems*, 107, 95–111. <https://doi.org/10.1016/j.future.2020.01.055>
- [15] Alharbi, A.; Alosaimi, W.; Alyami, H.; Rauf, H.T.; Damaševičius, R. Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things. *Electronics* 2021, 10, 1341. <https://doi.org/10.3390/electronics10111341>
- [16] Sarika Choudhary, Nishtha Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT," *Procedia Computer Science* Volume 167, 2020, Pages 1561-1573, <https://doi.org/10.1016/j.procs.2020.03.367>

[17] Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.

3. Полазне хипотезе

Докторска дисертација полази од четири хипотезе које су наведене и објашњене у наставку овог поглавља.

Хипотеза 1: Постоје обрасци понашања ботнет малвера који су заједнички за више различитих класа малвера, а који могу да се искористе за поуздану детекцију ботнета у дужем временском периоду.

Будући да се ботнет комуникација заснива на томе да ботмастер (уређај који контролише ботнет) мора да комуницира у неком временском интервалу са зараженим рачунарима (ботовима) [1], претпоставља се да постоје карактеристике мрежног саобраћаја између ботмастера и ботова које га издвајају од осталог мрежног саобраћаја, попут периодичности у слању порука и мале разлике у броју послатих података између смерова комуникације које могу да се искористе за детекцију.

Хипотеза 2: Могуће је оптимизовати капацитете за складиштење података о малверима и процесорско оптерећење, без губитка тачности детекције ботнет малвера.

Досадашњи приступи су се бавили најчешће анализом сумарних података о мрежним оковима или анализом целокупног садржаја пакета. Први приступ садржи недовољно података за детекцију ботнета пре него што се напад догоди, док је други приступ процесорски интензиван, и може спречити рад система. Ово истраживање ће се тицати проналажења већег скупа статистичких параметара мрежних токова, имајући у виду ефикасно коришћење меморије и процесорско оптерећење, у циљу ране детекције злонамерних ботнет мрежних токова.

Хипотеза 3: Могуће је детектовати нове варијанте ботнет малвера у систему обученом над старим малвером.

Полазећи од хипотезе Х1, због начина на који раде хакери који најчешће праве мале инкременталне промене у начину рада ботнет малвера, различите врсте ботнет малвера ће приказивати слично понашање за дати скуп карактеристика мрежног саобраћаја, те ће детекција нових варијанти малвера бити могућа у систему обученом над старим малвером.

Хипотеза 4: Могуће је реализовати детекцију ботнета у реалном времену, а не након завршетка мрежног тока или снимка пакета.

Досадашња истраживања у области ботнет детекције су се бавила детекцијом аномалија помоћу метода машинског учења, дубоког учења, и хибридних метахеуристика. То је подразумевало примену ових метода на већ формиране скупове података, то јест на унапред наснимљене мрежне токове. Такав приступ не представља ситуацију која се дешава у реалним сигурносним системима, где је потребно детектовати или спречити малвер комуникацију у реалном времену. Стога, претпоставља се да је могуће применити систем базиран на техникама вештачке интелигенције за детекцију малвер токова у реалном времену.

4. Научне методе истраживања

У предложеном истраживању ће бити заступљене теоријске, статистичке, експерименталне и методе вештачке интелигенције.

Истраживање ће се заснивати на анализи оптималног скупа одлика мрежног саобраћаја ботнета и проналажењу нових статистичких карактеристика које ће представљати улаз у модел вештачке интелигенције за учење и препознавање карактеристика ботнет саобраћаја. Подаци за истраживање ће бити прикупљени у реалном окружењу, у којем ће бити покретани реални малвери и у ком ће бити праћено понашање злонамерних ботнет апликација током дужег временског периода. Такође, користиће се неки од новијих скупова података који су јавно доступни (нпр. IoT23). На основу прикупљених података злонамерни мрежни токови ће бити анализирани, уочени и означени. На екстрахованим мрежним токовима биће примењене статистичке методе за њихову анализу и генерисање параметара модела за детекцију. Више различитих модела вештачке интелигенције биће коришћено и упоређено у погледу резултата, као и меморијског простора који је потребан за такав систем. Биће примењен адекватан скуп скорова, који показује меру стабилности метода. Сваки од модела ће бити оптимизован у погледу одабира параметара скупа података и хиперпараметара модела.

Модел вештачке интелигенције ће бити имплементиран у одговарајуће софтверско решење. Ово решење ће бити тестирано на подацима прикупљеним у лабораторијском окружењу, као и на неком од добро познатих скупова података из литературе.

5. Очекивани научни допринос

Значајан научни допринос се очекује у погледу анализе облика мрежног понашања који су заједнички за различите ботнет сојеве. Такође се допринос очекује и у екстракцији статистичких параметара мрежних токова, који ће повећати прецизност детекције, уз ефикасно коришћење рачунарских ресурса (простора за складиштење, оперативне меморије и процесорског оптерећења потребног за обраду). Најзначајнији допринос се очекује у погледу развијања система за динамичку детекцију ботнет саобраћаја, са циљем ране детекције злонамерних мрежних токова. Очекивани научни допринос ће бити изражен кроз имплементацију, оптимизацију и тестирање модела вештачке интелигенције на више различитих скупова података.

6. План истраживања и структура рада

Планирано је да се истраживање детекције ботнет саобраћаја коришћењем метода вештачке интелигенције одвија у следећим корацима:

1. Анализа доступне релевантне научно-стручне литературе и стандарда из дате области.
2. Прикупљање артефаката понашања малвера.
3. Анализа мрежних токова и проналажење аномалија у мрежном саобраћају.
4. Статистичка анализа мрежних токова и екстракција параметара тока
5. Формирање модела заснованом на вештачкој интелигенцији.
6. Имплементација и тестирање модела.
7. Симулација динамичке детекције мрежних токова користећи модел базиран на вештачкој интелигенцији.
8. Анализа свих добијених резултата. Приказ закључака и давање предлога за даља испитивања у области.

7. Закључак и предлог

Приликом писања извештаја, Комисија је размотрила релевантне чињенице о подобности теме и кандидата. Узимајући у обзир резултате досадашњег рада кандидата **Ђорђа Јовановића**, Комисија је закључила да кандидат јесте способан за научно истраживачки рад. Детаљном анализом предложене теме под називом „**Рано откривање уређаја заражених ботнет малвером коришћењем метода детекције аномалија мрежних токова**” (на енглеском „**Early discovery of the devices infected with botnet malware using network flow anomaly detection**”), Комисија је у потпуности сагласна да оваква тема задовољава све услове подобности за докторску дисертацију.

Комисија констатује да предложена тема припада ужој научној области **Рачунарска техника и информатика** и да је Универзитет у Београду - Електротехнички факултет (ЕТФ) матичан за ову научну област. За ментора докторске дисертације комисија предлаже др **Павла Вулетића, ванредног професора** са ЕТФ-а, и прилаже уз овај Извештај и списак радова др Павла Вулетића, који га квалификују за ментора докторске дисертације.

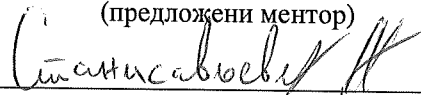
Имајући у виду све претходно наведено, Комисија има част и задовољство да Наставно-научном већу ЕТФ-а предложи да прихвати тему докторске дисертације „Рано откривање уређаја заражених ботнет малвером коришћењем метода детекције аномалија мрежних токова” (на енглеском „Early discovery of the devices infected with botnet malware using network flow anomaly detection”) и да кандидату Ђорђу Јовановићу омогући приступ њеној изради.

У Београду, 12.11.2021.

ЧЛАНОВИ КОМИСИЈЕ



др Павле Вулетић, ванредни професор
Универзитет у Београду – Електротехнички факултет
(предложени ментор)



др Жарко Станисављевић, ванредни професор
Универзитет у Београду – Електротехнички факултет
(председник комисије)



др Татјана Давидовић, научни саветник
Математички институт САНУ
(члан комисије који није запослен на ЕТФ)



др Горан Квашчев, ванредни професор
Универзитет у Београду – Електротехнички факултет
(члан комисије)