

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Подобност теме и кандидата мр Валентина Тимченко за израду докторске дисертације

Одлуком бр. 5046/16-1 од 30.9.2019. године, именовани смо за чланове Комисије за оцену подобности теме и кандидата мр Валентина Тимченко за израду докторске дисертације и научне заснованости теме:

„Детекција напада у рачунарским мрежама заснована на анализи структуре саобраћаја применом комбинованих алгоритама машинског учења“

(енг. „*Network attacks detection based on traffic flows analysis using hybrid machine learning algorithms*“).

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

ИЗВЕШТАЈ

1. Подаци о кандидату

1.1. Биографски подаци

Кандидаткиња је рођена 1978. године у Београду, где је завршила основну школу и гимназију. Студије на Електротехничком факултету у Београду започела је 1997. године, где је дипломирала 2004. године на Одсеку за Телекомуникације са темом „Оптичке WDM мреже“, под менторством проф. др Петра Матавуља са оценом дипломског рада 10. Просечна оцена у току студија била је 8,00. Постдипломске студије је уписала 2004. године, на Електротехничком факултету Универзитета у Београду, смер Телекомуникације, и положила све предмете предвиђене наставним планом, са просечном оценом 10.00. Магистрирала је 09.03.2010. године са темом „Принципи симулације мобилних ad hoc мрежа“ под менторством проф. др. Мирјане Стојановић.

Пред крај студија је била практикант у Енергопројект – ЕНТЕЛ, где се упознала са радом на обимним комерцијалним телекомуникационим пројектима, при чему је стекла основна знања о процесу писања тендера, развоју и управљању пројектима телекомуникационих система.

Запослена је у Институту Михајло Пупин у Београду од 2004. године, на пословима истраживања, развоја и пројектовања телекомуникационих мрежа и система. До сада је учествовала у неколико научно истраживачка пројекта, финансираних од стране Министарства просвете, науке и технолошког развоја Републике Србије. Учествовала је на међународном пројекту финансираном од стране Европске комисије, SEE TV-WEB, а такође је учествовала у пројектима и студијама телекомуникационих система Електропривреде Србије и Агенције за контролу летења.

Током магистарских студија интензивно се бавила радом у области примене знања из области телекомуникационих мрежа, при чему је завршила Cisco академију Рачунског центра Електротехничког факултета у Београду и сертифицивала се за неколико сертификата, од којих тренутно поседује следеће:

- CCNA - Cisco Certified Network Associate (640-802)
- CCNP ROUTE - Implementing Cisco IP Routing (ROUTE) (300-101)

У току је ресертификација за SWITCH - Implementing Cisco IP Switched Networks (642- 813) и TSHOOT - Routing and Switching (300-135).

Основно научно и стручно опредељење кандидаткиње обухвата истраживање, симулацију, дизајн и имплементацију решења из области телекомуникационих технологија и мрежа. Након завршених магистарских студија своје интересовање са области мобилних-*ad-hoc* мрежа је проширила истраживањима у области других мрежних технологија, при чему је главна окосница рада била истраживање аспеката сигурности података и безбедности мрежног окружења.

2016. године кандидаткиња је уписала докторске студије по новом програм, при чему је уз полагање одређеног броја испита разлике прешла са катедре за телекомуникације на катедру за рачунарску технику и информатику. Током рада на докторским студијама је наставила да се интензивно бави облашћу сигурности у рачунарским мрежама, са посебним фокусом на системе детекције, превенције и реакције на аномалије и нападе. Резултати њеног досадашњег истраживања су везани за области машинског учења и вештачке интелигенције и њихову примену у контексту савремених система за детекцију аномалија и напада. Из ове области је током досадашњег рада објавила неколико радова у часописима и на конференцијама од међународног значаја.

Кандидаткиња је вишегодишњи члан IEEE организације. Била је рецензент већег броја међународних конференција, међу којима су ICACCI-2015, IEEE WCNC 2015, ATC'14, а неколико година уназад је стални рецензент радова на међународним конференцијама TELFOR, MIC, ISDOC/OSDOC, INFOTEN. За конференције ISDOC/OSDOC је више пута била члан програмског одбора.

Била је коментор на више мастер радова одбрањених на Електротехничком факултету у Београду и на Високој школи електротехнике и рачунарства струковних студија у Београду.

Аутор је и коаутор 93 научна и стручна рада из области телекомуникација и рачунарских система, при чему је 30 радова на домаћим конференцијама, 56 на међународним конференцијама, 5 радова у међународним часописима, 2 у монографијама међународног значаја. Коаутор је већег броја техничких решења.

Кандидаткиња је током свог досадашњег стручног и научног ангажовања учествовала на неколико научно истраживачких пројеката финансираних од стране Министарства за науку и

технолошки развој Републике Србије (у периоду од 2005. до 2011.) и од Министарства просвете, науке и технолошког развоја Републике Србије (период од 2011. до 2019.). Осим тога, кандидаткиња је била ангажована на једном међународном пројекту Европске комисије, неколико идејних пројеката радио мрежа за системе за осматрање и обавештавање, изради студије за Агенцију за контролу летења и на изради студије финансираној од стране ЈП Електропривреда Србије.

[1] "Развој нових метода и алата за унапређење перформанси, мрежне и економске ефикасности телекомуникационих мрежа наредне генерације", пројекат технолошког развоја ТР32025, Министарство за науку и технолошки развој Републике Србије, 2011-2019.

[2] "Истраживање и развој робусних система за пренос података и њихова примена у корпоративним мрежама", пројекат технолошког развоја ТР32037, Министарство за науку и технолошки развој Републике Србије, 2011-2019.

[3] "Развој система за надзор и управљање мултисервисним телекомуникационим мрежама", Пројекат ТР-11002 из програма технолошког развоја, Министарство за науку и технолошки развој Републике Србије, 2008-2010.

[4] "Развој нове генерације комуникационих система у функционалним мрежама", Пројекат ТР-6105Б, из програма технолошког развоја, Министарство за науку и технолошки развој Републике Србије, 2005-2007.

[5] "SEE TV-WEB" међународни пројекат Европске комисије у оквиру програма South East Europe Terrestrial Cooperation Programme, 2013-2014.

[6] Студија развоја телекомуникационог система привредног друштва за дистрибуцију електричне енергије "Електродистрибуција Београд д.о.о.", ЈП Електропривреда Србије, 2011.

[7] Идејни пројекти радио мрежа за систем осматрања и обавештавања за:

- хидроелектране на Требишњици, ЈП Хидроелектране на Требишњици а.д. 2006.

- хидроелектране: Ђердап 1, Ђердап 2, Пирот, Власина, Врла 2 и Лисина, ПД ПХЕ „ХЕ Ђердап“, Кладово, 2007.

[8] IP телефонски систем Агенције за контролу летења Србије и Црне Горе, пројекат и реализација система, Агенција за контролу летења, 2007.

1.2. Стечено научноистраживачко искуство

У оквиру магистарских академских студија кандидаткиња је на Електротехничком факултету у Београду, смер Телекомуникације положила је све предмете предвиђене наставним планом са просечном оценом 10,00. Магистарску тезу под називом "*Принципи симулације мобилних ad hoc мрежа*" одбранила је 9. марта 2010. године (Комисија: др Мирјана Стојановић, ментор, проф. др Мирослав Дукић, проф. др Владанка Аћимовић-Распоповић, доц. др Миљко Ерић). Исте године је изабрана у звање истраживач-сарадник Института Михајло Пупин. Током магистарских студија а затим и након одбране магистарске тезе, кандидаткиња је наставила свој истраживачки рад у области мобилних *ad hoc* мрежа, а посебно на проблемима безбедности мобилних *ad hoc* мрежа. Резултате свог рада објавила је као аутор и коаутор у три рада у часописима са SCI листе. Свој даљи рад је усмерила на област сигурности у модерним мрежним окружењима обухватајући нове технологије, концептуалне трендове и информационо-комуникационе инфраструктуре (рачунарство у облаку, Интернет ствари).

Докторске академске студије је уписала 2016. године на Електротехничком факултету, Универзитета у Београду, на модулу Рачунарска техника и информатика. Том приликом је, у складу са правилником за докторске студије Електротехничког факултета и Универзитета у Београду, на основу магистратуре по старом програму стекла услов да упише трећу годину докторских студија по новом програму. С обзиром да је том приликом променила смер, дефинисани су испити разлике које је било потребно да положи. Дефинисана су два испита разлике: Организација система дискова и TCP/IP архитектура. Испите разлике је кандидаткиња успешно положила. Резултати који су остваривани истраживачким радом кандидаткиње представљени су у четири рада на међународним конференцијама.

Јавна усмена одбрана предложене теме докторске дисертације је спроведена 09.10.2019. године на Електротехничком факултету Универзитета у Београду. У трајању од 40 минута кандидаткиња је у најсажетијем облику изложила 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 кандидаткиња је успешно одговорила.

1.2.1. Објављени радови

Поглавље у монографији међународног значаја (M14)

- [1] Borislav Djordjevic, **Valentina Timcenko**, "Ext4 File System in Linux Environment: Features and Performance Analysis", International Journal of Computers, *Editor-in-Chief Prof. Metin Demiralp*, pp. 37-45, Issue 1, Volume 6, 2012, ISSN: 1998-4308.
- [2] **V. Timcenko**, M. Stojanović, S. Boštjančič Rakas, "A Simulation Study of MANET Routing Protocols Using Mobility Models," Computers and Simulation in Modern Science (Vol. III), *N. E. Mastorakis, M. Demiralp, V. Mladenov*, pp. 186–196, WSEAS Press, 2010, ISSN: 1792-6882, ISBN: 978-960-474-256-1.

Рад у међународном часопису (M23)

- [1] B. Djordjevic, N. Macek, **V. Timcenko**, "Performance Issues in Cloud Computing: KVM Hypervisor's Cache Modes Evaluation," Acta Polytechnica Hungarica, (2015), vol. 12 br. 4, pp. 147-165, DOI: 10.5755/j01.eee.20.7.8025.
- [2] B. Djordjevic, **V. Timcenko**, "LVM in the Linux environment: performance examination," Technical Gazzete - Tehnički vjesnik 22, 5(2015), pp. 1157-1164. doi: 10.17559/TV-20131113112940.
- [3] **V. Timcenko**, "An Approach for DDoS Attack Prevention in Mobile ad hoc Networks," Electronics and Electrical Engineering – Kaunas: Technologija Vol 20, No 6 (2014), ISSN: 1392-1215, pp:150-153, DOI: <http://dx.doi.org/10.5755/j01.eee.20.6.7289>.
- [4] N. Macek, B. Dordevic, **V. Timcenko**, M. Bojovic, M. Milosavljevic, "Improving Intrusion Detection with Adaptive Support Vector Machines," Electronics and Electrical Engineering – Kaunas: Technologija Vol 20, No 7 (2014), ISSN:1392-1215, pp. 57-60, DOI: <http://dx.doi.org/10.5755/j01.eee.20.7.8025>.
- [5] M. Stojanović, V. Aćimović-Raspopović, **V. Timcenko**, "The Impact of Mobility Patterns on MANET Vulnerability to DDoS Attacks," Electronics and Electrical Engineering – Kaunas: Technologija Vol 119, No 3 (2012), ISSN_1392-1215, pp. 29-34, DOI: <http://dx.doi.org/10.5755/j01.eee.119.3.1358>.

Предавање по позиву са међународног скупа штампано у целини (M31)

- [1] **V. Timcenko**, B. Djordjevic, N. Davidovic, "Stripped disk array organizations with distributed parity RAID-5: study and performance analysis", invited paper, ISDOC 2014, pp. 113 - 121, May, Lisboa, Portugal ISBN: 978-1-4503-2713-8.
- [2] **V. Timcenko**, B. Djordjevic, S. Bostjancic Rakas, N. Davidovic, "Performance examination of type-2 hypervisors: case of particular database application in a virtual environment", invited paper, ISDOC 2014, pp. 122 - 126, May, Lisboa, Portugal ISBN: 978-1-4503-2713-8.
- [3] **V. Timcenko**, B. Djordjevic, "The comprehensive performance analysis of striped disk array organizations - RAID-0", invited paper, *in proc. of Proceedings of the 2013 International Conference on Information Systems and Design of Communication*, Lisbon, Portugal, pp. 113-116, July 2013. ISBN: 978-1-4503-2299-7. doi:10.1145/2503859.2503877.
- [4] **V. Timčenko**, M. Stojanović, "Application of Forensic Analysis for Intrusion Detection against DDoS Attacks in Mobile Ad Hoc Networks", invited plenary lecture paper, *in Proc. of the 1st WSEAS Int. Conf. on Information Technology and Computer Networks (ITCN '12)*, Vienna, Austria, pp.301-310, November 2012, ISBN: 978-1-61804-134-0 (**Plenary lecture**).
- [5] **V. Timčenko**, S. Bostjančič Rakas, M. Stojanović, "The Role of Service Level Agreements in NGN Security Management Systems", invited paper, *in Proc. of the 1st WSEAS Int. Conf. on Information Technology and Computer Networks (ITCN '12)*, Vienna, Austria, pp.311-315, November 2012, ISBN: 978-1-61804-134-0.
- [6] B. Djordjević, **V. Timčenko**, "Ext4 File System on the Hardware RAID-1: Features and Performance Analysis", invited paper, *in Proc. of the 1st WSEAS Int. Conf. on Information Technology and Computer Networks (ITCN '12)*, Vienna, Austria, pp.316-321, November 2012, ISBN: 978-1-61804-134-0.
- [7] **V. Timcenko**, M. Stojanovic, A. Kostic-Ljubisavljevic, V. Radonjic, V. Dulovic, "The Impact of Pause Duration to Performance of AODV Protocol in the Urban Environment", invited paper, *in the Proceedings of OSDOC2012*, pp. 93 - 97, Lisabon, Portugal, June 2012.
- [8] **V. Timcenko**, B. Djordjevic, M. Stojanovic, "Porting GeoServer to Linux Environment and Applicability to Mobile Ad hoc Networks", invited paper, *in the Proceedings of OSDOC2012*, pp. 85 -91, Lisabon, Portugal, June 2012.
- [9] B. Đorđević, **V. Timčenko**, "Ext4 File System Performance Analysis in Linux Environment", invited paper, *In M. Lazard, A. Buikis, Y. S. Shmaliy, R. Revetria, N. E. Mastorakis, O. Martin, G. Bognar, S. H. Sohrab, D. N. Riahi, G. R. Gillich (eds), Recent Advances in Applied Informatics and Communications (AIC'11)*, Florence, Italy, pp. 288-293, August 2011, ISSN: 1790-5109, WSEAS Press. 2011, ISBN: 978-1-61804-028-2.
- [10] **V. Timčenko**, M. Stojanović, S. Boštjančič Rakas, "MANET Routing Protocols vs. Mobility Models: Performance Analysis and Comparison", invited paper, *In N. E. Mastorakis, M. Demiralp, V. Mladenov, Z. Bojković (eds), Recent Advances in Applied Informatics and Communications (AIC'09)*, Moscow, Russia, pp. 271-276, August 2009, ISSN: 1790-5109, WSEAS Press. 2009, ISBN: 978-960-474-107-6.

Предавање са међународног скупа штампано у целини (M33)

- [1] Nikola Davidovic, Borislav Đorđević, **Valentina Timcenko**, Slobodan Obradovic, Bojan Skoric, "RAID 0 on paired magnetic disk arrays", ICETAN 2019, Srebrno jezero, Serbia, RTI2.7.
- [2] **Valentina Timčenko**, Juma Ibrahim, and Slavko Gajin, "The Hybrid Machine Learning Support for Entropy Based Network Traffic Anomaly Detection", In: Konjović, Z., Zdravković, M., Trajanović, M. (Eds.) ICIST 2019 Proceedings Vol.1, pp.144-149, 2019.

- [3] Juma Ibrahim, **Valentina Timčenko**, and Slavko Gajin, "A comprehensive flow-based anomaly detection architecture using entropy calculation and machine learning classification", In: Konjović, Z., Zdravković, M., Trajanović, M. (Eds.) ICIST 2019 Proceedings Vol.1, pp.138-143, 2019.
- [4] Borislav S. Djordjevic, **Valentina V. Timcenko**, Nenad Kraljevic, Nikola Davidovic, "File system performance comparison in full hardware virtualization with ESXi and Xen hypervisors" (Proceedings Paper), 18th Int. Symposium INFOTEH-JAHORINA (INFOTEH), (2019), vol. br. , str. -. DOI: 10.1109/INFOTEH.2019.8717664, ISBN: 978-1-5386-7073-6
- [5] Nikola Davidović, Borislav Đorđević, **Valentina Timčenko**, Slobodan Obradović, Bojan Škorić, "Sistem za skladištenje podataka na uparenim nizovima magnetnih diskova - RAID 0", 18th Int. Symposium INFOTEH-JAHORINA (INFOTEH), (2019).
- [6] Anka V. Kabović, Milenko M. Kabović, Slavica V. Boštjančić Rakas, **Valentina V. Timčenko**, "Models for Short-Term Forecasting of Parameters Used for Calculation of the Overhead Line Ampacity", Telfor 2018, pp. 687 – 690, 2018. ISBN 978-1-5386-7170-2, IEEE catalogue number: CFP1898P-CDR.
- [7] Milan D. Simeunović, Borislav S. Đoršević, **Valentina V Timčenko**, Nevena D. Janković, "iSCSI and CIFS network disks for RAID0/RAID1 configurations", Telfor 2018, pp. 859 - 862. ISBN 978-1-5386-7170-2, IEEE catalogue number: CFP1898P-CDR.
- [8] Jadran Torbić, Ivan Stanković, Borislav Đorđević, **Valentina Timčenko**, "Hyper-V and ESXi hypervisors comparison in Windows Server 12 virtual environment" INFOTEH 2018, pp. 1-5. DOI: 10.1109/INFOTEH.2018.8345548.
- [9] Nikola Davidović, Slobodan Obradović, Borislav Đorđević, **Valentina Timčenko**, "XFS file system and occupancy impact space of a semiconductor disk", 2018, pp. 1-5, 10.1109/INFOTEH.2018.8345539.
- [10] **Valentina Timčenko**, Slavko Gajin, "Machine Learning based Network Anomaly Detection for IoT environments", ICIST 2018, pp. 196 – 201. ISBN 978-86-85525-22-3. Online: <http://www.eventiotic.com/eventiotic/files/Papers/URL/e5bb6a65-0030-4acf-815e-37c58cdc0bda.pdf>
- [11] **Valentina Timčenko**, Nikola Zogović, Borislav Đorđević, "Interoperability for the sustainability assessment framework in IoT like environments", ICIST 2018, pp. 21 – 27, ISBN 978-86-85525-22-3. Online: <http://www.eventiotic.com/eventiotic/files/Papers/URL/f34613c4-19a9-434c-8f6e-8ad92ca769e4.pdf>
- [12] **Valentina Timčenko**, Slavko Gajin, "Ensemble classifiers for supervised anomaly based network intrusion detection", IEEE ICCP2017, Cluj-Napoca, Rumunija, 07. - 09. septembar 2017, ISBN: 978-1-5386-3367-0, IEEE Catalog Number: CFP1709D-USB
- [13] Borislav Đorđević, **Valentina Timčenko**, "A performance comparison of Linux filesystems in hypervisor type 2 virtualized environment", INFOTEH, Jahorina BiH, INFOTEH-JAHORINA Vol. 16, 22-24.mart, 2017, pp. 630-634, ISBN 978-99976-710-0-4
- [14] Nikola Davidović, Slobodan Obradović, Borislav Đorđević, **Valentina Timčenko**, "Analiza performansi ext4, xfs i btrfs fajl sistema na poluprovodničkom disku (SSD)", INFOTEH, Jahorina BiH, INFOTEH-JAHORINA Vol. 16, 22-24.mart, 2017, pp. 407-411, ISBN 978-99976-710-0-4
- [15] **Timčenko, V.**, Zogović, N., Jevtić, M., Đorđević, B. "An IoT business environment for Multi Objective Cloud Computing Sustainability Assessment Framework", In: Zdravković, M., Konjović, Z., Trajanović, M. (Eds.) ICIST 2017 Proceedings Vol.1, pp.120-125, 2017 Kopaonik, Serbia, pp. 120-125, ISBN 978-86-85525-19-3

- [16] Pesic Djordje, Djordjevic Borislav, **Timcenko Valentina**, "Competition of Virtualized Ext4, Xfs and Btrfs Filesystems Under Type-2 Hypervisor", Telfor2016, pp.774-777, 22-23. november, 2016, Beograd, Srbija, ISBN: 978-1-5090-4085-8, Društvo za Telekomunikacije. M33
- [17] S. Boštjančič Rakas, **V. Timčenko**, M. Kabović, A. Kabović, "Cyber Security Issues in Conductor Temperature and Meteorological Measurement Based DLR System", 10th Mediterranean Conference on Power Generation, Transmission, Distribution, and Energy Conversion - Med Power 2016, Beograd, Srbija, 6 – 9 novembar, 2016. Paper 095, pp: 1-7. M33
- [18] B. Đorđević, **V. Timčenko**, S. Boštjančič Rakas, "SSHD: Modeling and Performance Analysis", in Proceedings of INFOTEH 2016 (CD), Jahorina, INFOTEH-JAHORINA Vol. 15, pp: 526-529, March 2016
- [19] S. Boštjančič Rakas, **V. Timčenko**, "A Survey on Quality of Service in MANET", in Proceedings of INFOTEH 2016 (CD), Jahorina, INFOTEH-JAHORINA Vol. 15, pp: 349-352, March 2016
- [20] **Valentina Timčenko**, Nikola Zogović, Miloš Jevtić and Borislav Đorđević, "Assessing Cloud Computing Sustainability", in Proceedings of ICIST 2016, pp. 40 - 45, March 2016.
- [21] Nikola Zogović, Miloš Jevtić, **Valentina Timčenko**, Borislav Đorđević, "A Multi-objective Assessment Framework for Cloud Computing", in *Proceedings of TELFOR 2015* (CD), Beograd, pp: 978 - 981, Novembar 2015, ISBN: 978-1-5090-0054-8.
- [22] S. Boštjančič Rakas, **V. Timčenko**, B. Đorđević, "Upravljanje kvalitetom servisa i zaštitom u bežičnim ad hoc mrežama", in Proceedings of INFOTEH 2015 (CD), Jahorina, INFOTEH-JAHORINA Vol. 14, pp. 295-300, March 2015.
- [23] N. Davidovic, S. Obradovic, P. Strbac, B. Djordjevic, **V. Timcenko**, "Komparativna analiza hibridnog diska sa hard diskom i poluprovodničkim diskom", in Proceedings of INFOTEH 2015 (CD), Jahorina, INFOTEH-JAHORINA Vol. 14, pp.731-734, March 2015.
- [24] B. Đorđević, **V. Timčenko**, S. Boštjančič Rakas, N. Maček, M. Kuprešanin, "Modelovanje i poređenje RAID performansi na hardverskom motherboard-RAID kontroleru", in Proceedings of INFOTEH 2015 (CD), Vol. 14, pp.776-781, Jahorina, BiH, March 2015.
- [25] Slavica Boštjančič Rakas, **V. Timčenko**, "Quality of service and security issues in MANET environment ", in *Proceedings of TELFOR 2014* (CD), Beograd, novembar 2014, pp. 419-422, ISBN: 978-1-4799-6190-0.
- [26] Borislav Đorđević, Slobodan Jovanović, **V. Timčenko**, "Cloud Computing in Amazon and Microsoft Azure platforms: performance and service comparison", in *Proceedings of TELFOR 2014* (CD), Beograd, novembar 2014, pp. 931-934, ISBN: 978-1-4799-6190-0.
- [27] B. Djordjevic, **V. Timcenko**, N. Macek, "Issues in Cloud Computing: Performance Evaluation of Type-1 Hypervisors", in Proceedings of 18th International Conference ELECTRONICS2014, Palanga, Lithuania, ISBN: 978-609-02-1065-9, pp.55-58, June 2014.
- [28] **Valentina Timčenko**, Slavica Boštjančič Rakas, "Policy Based Performance Management in Mobile Ad hoc Networks", 1st International Conference on Electrical, Electronic and Computing Engineering – IcETRAN 2014, pp. TE11.6.1-5, Vrnjačka Banja, Srbija, jun 2014.
- [29] **V. Timcenko**, B. Djordjevic, N. Davidovic, "Performance comparison of RAID-1, RAID-0 and single disk on operating system MS Windows 7", 1st Int. Conference on Electrical, Electronic and Computing Engineering – IcETRAN2014, pp. RT11.1.1-5, Vrnjačka Banja, Srbija, jun 2014.

- [30] Nikola Davidović, Dijana Kosmajac, Borislav Đorđević, **V. Timčenko**, "Komparativna analiza sekundarnih memorija –poređenje tvrdog diska sa poluprovodničkim diskom", in *Proceedings of INFOTEH 2014* (CD), Jahorina, INFOTEH-JAHORINA Vol. 13, pp. 769 - 773, March 2014.
- [31] **V. Timčenko**, Borislav Đorđević, Nemanja Maček, "NTFS fajl sistem u MS Windows i Linux okruženju", in *Proceedings of INFOTEH 2014* (CD), Jahorina, INFOTEH-JAHORINA Vol. 13, pp. 805 - 808, March 2014.
- [32] B. Đorđević, **V. Timčenko**, Verica M. Vasiljević, Branka N. Andrijašević, "Komparacija performansi softvera za virtuelizaciju na MS Windows 7", *Zbornik radova Telekomunikacionog foruma TELFOR 2013*, Beograd, novembar 2013, pp. 1019-1022, ISBN: 978-1-4799-1419-7.
- [33] Tijana Tomić, **V. Timčenko**, Goran Dimić, "HbbTV aplikacija za DVB-T2", *Zbornik radova Telekomunikacionog foruma TELFOR 2013* (CD), Beograd, novembar 2013, pp. 983-987, ISBN: 978-1-4799-1419-7.
- [34] B. Đorđević, **V. Timčenko**, S. Obradović, N. Čorni, "Uticaj disk keš bafera na performanse SSD diskova", *Zbornik radova INFOTEH 2013*, Vol.12. pp. 1002-1005, Jahorina, mart 2013.
- [35] Aleksandra Kostić-Ljubisavljević, Vesna Radonjić, Mirjana Stojanović, **Valentina Timčenko**, "Techno-Economic Issues in Optical Access Deployment", *Proceedings of the 21th International Electrotechnical and Computer Science Conference ERK 2012*, vol. 1, pp. 41 - 44, Portorož, Slovenia, Septembar 2012, ISSN: 1581-4572.
- [36] Aleksandra Kostić-Ljubisavljević, Vesna Radonjić, Mirjana Stojanović, **Valentina Timčenko**, "Charging Interconnection in NGN", *Proceedings of the 21th International Electrotechnical and Computer Science Conference ERK 2012*, vol. 1, pp. 61 - 64, Portorož, Slovenia, September 2012. ISSN: 1581-4572.
- [37] B. Đorđević, S. Obradović, **V. Timčenko**, "Ext4 sistem datoteka na RAID-0 konfiguracijama u Linux okruženju", *Zbornik radova INFOTEH 2012* (CD), Jahorina, INFOTEH-JAHORINA Vol. 11, Ref. RSS-1, pp. 635-638, Mart 2012, ISBN 978-99938-624-8-2., <http://infoteh.etf.unssa.rs.ba/zbornik/2012/radovi/RSS-3/RSS-3-1.pdf>
- [38] B. Đorđević, **V. Timčenko**, S. Obradović, "LVM in Linux Environment: Performance Examination", in *INFOTEH 2011 CD Proceedings*, Jahorina, March 2010, vol. 10, Ref. E-I-20, pp. 486-489, ISBN: 978-99938-624-6-8.
- [39] B. Đorđević, S. Obradović, **V. Timčenko**, T. Pavlov, "Poređenje performansi RAID-0 i RAID-5 u Linux okruženju pomoću Tiobench benchmarka", *Zbornik radova INFOTEH 2010* (CD), Jahorina, mart 2010, Vol. 9, Ref. E-II-11, pp. 542-544, ISSN: 99938-624-2-8.
- [40] B. Đorđević, **V. Timčenko**, "Examination of hardware RAID solutions under Linux: RAID-0 v RAID-1", *Proceedings of the International Conference on Advances in the Internet, Processes, Systems and Interdisciplinary Research - VIPSI 2009* (CD), Belgrade, April 2009, ISSN: 86-7466-117-3.
- [41] B. Đorđević, S. Obradović, **V. Timčenko**, T. Pavlov, "Poređenje performansi rada RAID-0 i RAID-5 rešenja u Linux okruženju", in *INFOTEH 2009 CD Proceedings*, Jahorina, March 2009, vol. 8, Ref. E-V-4, pp. 706-709, ISBN-99938-624-2-8.
- [42] S. Boštjančič, **V. Timčenko**, M. Stojanović, "A Common Framework for Inter-Provider IP Quality of Service Specification", in *Proceedings of the XLIII International Scientific Conference on Information, Communication and Energy Systems and Technologies – ICEST 2008*, Niš, June 2008, vol. 2, pp. 429-432, ISBN: 978-86-85195-61-7.

- [43] B. Đorđević, S. Obradović, N. Maček, **V. Timčenko**, D. Ilić, "Linux JFS sistem datoteka na kernelima 2.4 i 2", in *INFOTEH 2008 CD Proceedings*, Jahorina, March 2008, vol. 7, Ref. E-I-8, pp.403-406, ISBN: 99938-624-2-8.

Предавање по позиву са међународног скупа штампано у изводу (M32)

- [1] **V. Timčenko**, "An Approach for DDoS Attack Prevention in Mobile ad hoc Networks," International Conference ELECTRONICS2014, Palanga, Lithuania, June 2014. In paper format.

Предавање са међународног скупа штампано у изводу (M34)

- [1] Jevtić, M., **Timčenko, V.**, Zogović, N., Đorđević, B., "On The Use Of k-(Multi)Combination Decision Variables in Engineering Optimization Problems", In: Martić, M., Savić, G., Kuzmanović, M. (Eds.) Book of Abstracts of the XIII Balkan Conference on Operational Research BALCOR 2018, Belgrade, 25-28 May, 2018, ISBN: 978-86-80593-65-4, p.7.
- [2] N. Macek, B. Djordjevic, **V. Timčenko**, M. Bojovic, M. Milosavljevic, "Improving Intrusion Detection with Adaptive Support Vector Machines," International Conference ELECTRONICS2014, Palanga, Lithuania, June 2014. In paper format.

Предавање по позиву са скупа националног значаја штампано у целини (M61)

- [1] M. Stojanović, **V. Timčenko**, "Primena forenzičke analize u sistemima zaštite savremenih IP mreža", rad po pozivu, Zbornik radova XXX Simpozijuma o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – POSTEL 2012, Beograd, decembar 2012, pp. 295-306, ISBN: 978-86-7395-304-5.
- [2] M. Stojanović, **V. Timčenko**, S. Boštjančič Rakas, "Intrusion Detection against Denial of Service Attacks in MANET Environment", invited paper, in *Proceedings of XXIX Symposium on new technologies in the postal and telecommunications traffic – POSTEL 2011*, Belgrade, December 2011, pp. 201-212, ISBN: 978-86-7395-287-1.
- [3] M. Stojanović, **V. Timčenko**, S. Boštjančič Rakas, "Principi simulacije mobilnih ad hoc mreža", rad po pozivu, Zbornik radova XXVI Simpozijuma o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – POSTEL 2010, Beograd, decembar 2010, pp. 325-336, ISBN: 978-86-7395-274-1.
- [4] M. Stojanović, S. Boštjančič Rakas, **V. Timčenko**, "Experiences in Teaching and Researching Computer Networking using Simulation", rad po pozivu, in *Proceedings of XXVI Symposium on new technologies in the postal and telecommunications traffic – POSTEL 2008*, Belgrade, Decembar 2008, pp. 267-278, ISBN: 978-86-7295-252-9.

Предавање са скупа националног значаја штампано у целини (M63)

- [1] Slavica Boštjančič Rakas, **Valentina Timčenko**, Milenko Kabović, Anka Kabović, Mirjana Stojanović, "Savremena informaciono-komunikaciona podrška elektroenergetskom sektoru: arhitektura, karakteristike i problema zaštite", Cigre 2019, Vrnjačka Banja.
- [2] Slavica Boštjančič Rakas, **Valentina Timčenko**, Milenko Kabović, Anka Kabović, Mirjana Stojanović, "Mogućnosti implementacije DLR sistema u cloud okruženju", CIGRE 2018, Zlatibor, Zbornik radova 18. Simpozijuma CIGRE Srbija, R D2 03 (1-8), ISBN 978-86-80616-03-2.
- [3] Anka Kabović, Milenko Kabović, Jovanka Gajica, Slavica Boštjančič Rakas, **Valentina Timčenko**, "Modeli za kratkoročno predviđanje brzine i smera vetra azirani na neuralnim i mrežama sa neodređenom ("FUZZY") logikom", CIGRE 2018, Zlatibor, Zbornik radova 18. Simpozijuma CIGRE Srbija, R D2 09 (1-8). ISBN 978-86-80616-03-2.

- [4] Kabović Milenko, **Timčenko Valentina**, Boštjančič-Rakas Slavica, Kabović Anka, "Izbor metode za kratkoročno predviđanje maksimalnog dozvoljenog strujnog opterećenja dalekovoda", 33. savetovanje CIGRE Srbija, 5-8. jun 2017., Zlatibor, D2-4
- [5] B. Đorđević, **V. Timčenko**, Slobodan Obradović, Nikola Čorni, "Uticaj internog kontrolera na performanse SSD diskova", *Zbornik radova XVIII konferencije YU INFO 2013*, Kopaonik, mart 2013, pp. 433-436, ISBN: 978-86-85525-11-7. Online: <http://www.e-drustvo.org/proceedings/YuInfo2013/default.html>
- [6] B. Đorđević, **V. Timčenko**, "Portiranje GeoServer softvera u Linux okruženju", *Zbornik radova 57. konferencije ETRAN-a 2013*, Jun 2013, pp. RT6.6.1-4, ISBN 978-86-80509-68-6.
- [7] B. Đorđević, **V. Timčenko**, "Ext4 sistem datoteka na RAID-1 konfiguracijama u Linux okruženju", *Zbornik radova XVII konferencije YUINFO 2012 & ICIST*, Kopaonik, mart 2012, pp. 535/538, ISBN: 978-86-85525-04-9, <http://www.e-drustvo.org/yuinfo/yuinfo2012.html>
- [8] B. Đorđević, **V. Timčenko**, "Uticaj broja diskova na performanse striping RAID konfiguracija", *Zbornik radova Telekomunikacionog foruma TELFOR 2012*, Beograd, novembar 2012, pp. 1548-1551, ISSN: 978-1-4673-2982-8.
- [9] S. Boštjančič Rakas, **V. Timčenko**, J. Gajica, "Analiza razvoja elektroprivrednog telekomunikacionog sistema u uslovima deregulacije tržišta u Srbiji", *Zbornik radova 15. Simpozijuma CIGRE Srbija - "Upravljanje i telekomunikacije u elektroenergetskom sistemu"*, Donji Milanovac, Oktobar 2012, R D2 09 (1-8), ISBN: 978-86-82317-71-5.
- [10] **V. Timčenko**, V. Dulović, "Modelovanje mobilnosti u urbanom okruženju", *Zbornik radova Telekomunikacionog foruma TELFOR 2011*, Beograd, novembar 2011, pp. 206-209, ISSN: 978-1-4577-1500-6.
- [11] Đorđević Borislav, **Valentina Timčenko**, Randić Siniša, Pešović Uroš, Jovanović Željko, "Poređenje performansi SSD i magnetnih diskova u Linux okruženju", *Zbornik radova XVI konferencije YUINFO 2011*, Kopaonik, Mart 2011, CD Zbornik radova, pp. 634-637, ISBN: 978-86-85525-08-7.
- [12] **V. Timčenko**, B. Đorđević, S. Obradović, A. Dončev, "Analiza performansi ext4 sistema datoteka u Linux okruženju", *Zbornik radova 55. konferencije ETRAN-a*, pp. RT4.5, Teslić, BiH, jun 2011, ISBN 978-86-80509-65-5.
- [13] S. Boštjančič Rakas, M. Stojanović, **V. Timčenko**, "Sistemi za nadzor i upravljanje telekomunikacionim mrežama", *Zbornik radova 30. Simpozijuma CIGRE Srbija*, Zlatibor, maj/jun 2011, R D2 06 (1-8), ISBN: 978-86-82317-69-2
- [14] **V. Timčenko**, Mirjana Stojanović, "Analiza performansi reaktivnih protokola rutiranja u mobilnim ad hoc mrežama", *Zbornik radova 54. konferencije ETRAN-a*, TE2.2-1-4, Donji Milanovac, jun 2010, ISBN 978-86-80509-65-5.
- [15] B. Đorđević, **V. Timčenko**, "Poređenje performansi rada RAID-1 i RAID-5 rešenja u Linux okruženju pomoću Tiobench benchmarka", *Zbornik radova 54. konferencije ETRAN-a*, pp. RT2.2-1-3, Donji Milanovac, jun 2010, ISBN 978-86-80509-65-5.
- [16] **V. Timčenko**, B. Đorđević, "Modeli mobilnosti u simulaciji MANET mreža", *in the Proceedings of TELFOR 2009*, Belgrade, November 2009, pp. 1331-1334, ISSN: 978-86-7466-375-2.
- [17] B. Đorđević, **V. Timčenko**, "Poređenje performansi rada RAID-1 i pojedinačnog diska u LINUX okruženju", *in the Proceedings of TELFOR 2009*, Belgrade, November 2009, pp. 1280-1282, ISSN: 978-86-7466-375-2.

- [18] **V. Timčenko**, B. Đorđević, "Poređenje performansi rada RAID-1 i RAID-5 rešenja u Linux okruženju", in *the Proceedings of 53. ETRAN conference*, Vrnjačka Banja, June 2009, pp. RT3.8-(1-4), ISSN: 978-86-80509-64-8.
- [19] M. Miljković, M. Stojanović, **V. Timčenko**, "Primena MPLS tehnologije u telekomunikacionim mrežama Elektroprivrede", *Proceedings of 29th Conference CIGRE 2009*, Zlatibor, June 2009, pp. R D2 – 07-(1-8), ISSN: 978-86-82317-67-8.
- [20] B. Đorđević, **V. Timčenko**, "Poređenje performansi rada RAID-0 i RAID-1 rešenja u Linux okruženju", in *Proceedings of XV YU INFO Conference*, pp. 040 (1-5), Kopaonik, March 2009, ISBN: 978-86-85525-04-9.
- [21] **V. Timčenko**, S. Boštjančič Rakas, M. Stojanović, "Analiza karakteristika simulatora IP mreža NS2 u Linux i Windows okruženju", in *Proceedings of TELFOR 2008*, Belgrade, novembar 2008, pp. 146 – 149, ISBN: 978-86-7466-337-0.
- [22] B. Đorđević, **V. Timčenko**, "Komparacija 64-bitnih sistema datoteka na Linux kernelu 2.6", in *Proceedings of TELFOR 2008*, Belgrade, November 2008, pp. 739-742, ISBN: 978-86-7466-337-0.
- [23] **V. Timčenko**, B. Đorđević, "Evalvacija Linux sistema datoteka na kernelu 2.6", in *the Proceedings of 52. ETRAN Conference*, Palić, June 2008, pp. RT 1.2 (1-4), ISBN: 978-86-80509-63-1. **Awarded as the best work of young author in the RT section.**
- [24] **V. Timčenko**, B. Đorđević, "Komparacija Linux verzija kernela 2.4 i 2.6", in *the Proceedings of XIV YU INFO Conference*, pp. 008 (1-4), Kopaonik, March 2008, ISBN 978-86-85525-3-2.
- [25] **V. Timčenko**, G. Pernić, V. Vučurević, M. Dimitrijević, "Primena GSM/GPRS komunikacije u sistemima upravljanja i daljinskog nadzora", in *the Proceedings of TELFOR 2007*, Belgrade, November 2007, pp. 257-260, ISBN: 978-86-7466-301-1.
- [26] B. Đorđević, **V. Timčenko**, D. Ilić, "Komparacija sistema datoteka na Linux kernelu 2.6 ", in *the Proceedings of TELFOR 2007*, Belgrade, November 2007, pp. 573-576, ISBN: 978-86-7466-301-1.

1.3. Оцена подобности кандидата за рад на предложеној теми

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

2. Предмет и циљ истраживања

Савремени оквири развоја нових технологија условљени су диктатом снажног потрошачки-оријентисаног тржишта и тежњом за прилагођавањем потребама за сервисима, брзим протоцима информација, преносу великих количина података и њиховом чувању и обради. Такав приступ је довео до низа изазова, а приоритетно питање постало је обезбеђивање сигурности система и података. Упоредо са развојем технологија, развијају се и различити облици напада у циљу онемогућавања приступа ресурсима и сервисима, као и компромитовања информација и поверљивих/приватних података. Некада су биле довољне мрежне заштитне баријере (firewalls), које су уз примену базе познатих напада (Signature

based) успешно браниле мрежу од спољних нападача. Индустијска пракса и научна истраживања показују да се такве традиционалне методе заштите морају подржати софистицираним техникама које ће објединити интелигентно и ефикасно детектовање аномалија и напада.

Предмет истраживања овог рада је обезбеђивање технике за правовремено и прецизно препознавање напада у модерним рачунарским мрежама. Фокус је на развоју поузданијих и прецизнијих система за праћење и анализу структуре мрежног саобраћаја у циљу откривања аномалија (Network Anomaly Detection System, NADS) и детекцију различитих облика напада (Intrusion Detection System, IDS).

У овој области је објављен велики број радова, при чему је већина посвећена неком специфичном задатку детекције аномалија или напада у одређеним условима. Главни проблем представља испитивање услова под којима долази до напада, формирање основног профила понашања и праћење сваког одступања од тако дефинисаног регуларног понашања. Значајни допринос научне заједнице огледа се у развоју принципа детекције напада, при чему су се као основни издвојили системи засновани на (1) детекцији статистичких аномалија (statistical anomaly detection), и (2) детекцији заснованој на правилима (rule based detection). Статистички приступ обухвата примену детекције помоћу утврђених граничних вредности атрибута (threshold based), и методе детекције засноване на профилима (profile based). Детекција заснована на правилима подразумева детекцију аномалија (anomaly detection) при чему се детектују сва одступања од претходно утврђених шаблона понашања.

Оно што их све повезује је примена различитих метода машинског учења, а које подразумевају скуп корака којима се преузимају корисне информације из доступних података, обучавају алгоритми, а затим стечено знање примењује за потребе класификације нових података.

У литератури се могу наћи радови који се баве: обрадом и заштитом података везаних за безбедност система [1], дистрибуираним нападима ради ускраћивања сервиса [2], откривањем ботнета [3], нападима заснованим на скенирању портова [4], нападима заснованим на приступу исцрпљујуће претраге (Brute force [5]), итд. Иако је најквалитетнији приступ који би се заснивао на обради свих доступних података које преносе пакети (payload), све веће коришћење шифрованог саобраћаја, велике брзине протока и количине података које је потребно обрадити, условили су да се интензивирају истраживања метода обраде података и машинског учења на нивоу информација о комуникационим токовима (flow). Комуникациони токови дају информације о интернет адресама и портovima извора и одредишта, протоколу, броју пренетих бајтова и пакета и времену трајања комуникација. Иако обезбеђују мање детаља о мрежној активности крајњих уређаја, њихово је прикупљање лакше, а такав скуп атрибута је често довољан за анализу. Тиме се штеди на ресурсима, умањује се сложеност прорачуна, а анализом се могу добити одмах применљиви резултати и реаговати на нападе чак и у случају шифрованог саобраћаја. За сакупљање ових података се најчешће користи NetFlow протокол [6].

Први и највише анализиран скуп података за анализу напада је KDDCUP99. Ипак, велики број научних студија статистичке карактеристике овог скупа данас сматра дискутабилним, највише због застарелих инстанци, недостатка савремених напада и изразите небалансираности. Иако нема превише репрезентативних скупова података, на располагању је неколико савремених јавно доступних скупова (UNSW-NB15, CTU-13, CIDDS-001, CDX, CICIDS 2017 [7]). Већином су засновани на формату дефинисаном NetFlow протоколом, а проблем приватности је решен анонимизацијом приватног дела података.

Област машинског учења пружа могућност различитих приступа у анализи структурно разнородних података [8, 9]. Груба категоризација упућује на три групе алгоритама:

надгледано учење (Supervised), ненадгледано учење (Unsupervised), полунадгледано учење (Semi-supervised).

Основни циљеви истраживања су следећи:

- (1) Предлог принципа конструисања свеобухватног модела система детекције аномалија и напада на бази анализе ентропије различитих параметара комуникационих токова мрежног саобраћаја применом хибридних алгоритама машинског учења (Hybrid Machine Learning, HML).
- (2) Модификација скупова података, који ће бити обogaћени синтетички генерисаним инстанцама напада којима се симулирају напади новијег датума. На бази тога ће се генерисати нови скупови података применом софтверских алата за рачунање ентропије дистрибуција карактеристика података.
- (3) Обрада, имплементација и тестирање одабраних алгоритама машинског учења над модификованим и новим скуповима података.
- (4) Дефинисање карактеристика хибридног алгоритама машинског учења, који би на најефикаснији начин могао да одговори на потенцијалне потребе засноване на карактеристикама рада у реалним условима.

Значај планираног истраживања се огледа кроз дефинисање новог приступа и система који ће помоћи у обезбеђивању веће сигурности у условима реалног коришћења мрежних сервиса. Висок ниво сигурности је од посебног значаја нарочито у случајевима потребе за хитним интервенцијама и системима посебне намене. Тада је од највеће важности да се правовремено (скоро у реалном времену) и поуздано детектују малициозне активности и аномалије у коришћењу мреже које указују на сигурносне претње, како би се исте отклониле.

РЕЛЕВАНТНИ БИБЛИОГРАФСКИ ИЗВОРИ:

- [1] M. Ring et al, "A Toolset for Intrusion and Insider Threat Detection", Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications, Springer, 2017, pp. 3–31. doi:10.1007/978-3-319-59439-2_1.
- [2] C. Douligieris, A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", Computer Networks, 44.5 (2004): 643-666.
- [3] J. Wang, I. C. Paschalidis, "Botnet detection based on anomaly and community detection", IEEE Trans. on Control of Network Systems 4.2 (2016): 392-404.
- [4] M. Ring et al, "Detection of slow port scans in flowbased network traffic", PLOS ONE 13 (9) (2018), pp. 1–18. doi:10.1371/journal.pone.0204507.
- [5] A. Sperotto et al, "Hidden Markov Model modeling of SSH brute-force attacks", Int. Workshop on Distributed Systems: Operations and Management, Springer, 2009, pp. 164–176. doi:10.1007/978-3-642-04989-7_13.
- [6] B. Claise, "Cisco systems netflow services export version 9", No. RFC 3954. 2004.
- [7] Ring, Markus, et al, "A Survey of Network-based Intrusion Detection Data Sets", Computers & Security (2019).
- [8] TTT Nguyen, et al, "A survey of techniques for internet traffic classification using machine learning", IEEE Communications Surveys and Tutorials, 10.1-4, 2008, pp. 56-76.
- [9] A. L. Buczak, E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection", IEEE Communications Surveys & Tutorials 18.2 (2015), pp. 1153-1176.

- [10] H. Liu, M. Cocea, "Granular computing-based approach for classification towards reduction of bias in ensemble learning", doi 10.1007/s41066-016-0034-1.
- [11] M. Antonelli, et al, "Multi-objective evolutionary design of granular rule-based classifiers", Granular Computing 1.1 (2016), pp. 37-58.
- [12] M. A. Wani et al, "Advances in Deep Learning", vol. 57, Springer, 2020.

3. Полазне хипотезе

Основне хипотезе од које се полази у истраживању су следеће:

- Постоји могућност да се предложи нови метод за детекцију аномалија и напада којим би се омогућило обезбеђивање сигурности модерних мрежних окружења, а који ће бити ефикаснији и флексибилнији од постојећих приступа. Избор методе детекције напада и аномалија у великој мери зависи од карактеристика доступних података. Нове методе машинског учења се у великој мери ослањају на детаљније, грануларније препроцесирање улазних података, улажење дубље у структуру података и препознавање специфичних обриса профила саобраћаја, као и на упоређивање са основним карактеристикама нормалног саобраћаја. Том приликом се често комбинује више метода како обраде података тако и самог машинског учења, при чему се у том домену потенцирају комбиновани - хибридни приступи засновани на примени метода групног учења (Ensemble), груписања (Clustering), и полу-надгледаног учења.
- Предложени метод треба да обухвати могућност детекције познатих и непознатих напада и аномалија. Методе детекције напада на основу потписа из садржаја пакета (Signature Based IDS) су ефикасне само за познате нападе, док овакав приступ не може да се примени за детекцију нових напада тзв. напади нултог дана (Zero-Day attacks) као ни за нападе и аномалије чији је садржај шифрован (encryption empowered attacks). Потребно је стога применити софистициране и брзе методе детекције неправилности и неусаглашености са већ наученим особинама сличних напада, како би се они могли изоловати и тиме онемогућити њихово дејство.
- Модел треба да буде што мање завистан од типа напада, броја нападача, тренутка у којем долази до напада или аномалије, као и карактеристика генерисаног саобраћаја аномалије/нападача. Приликом развоја модела за детекцију напада и аномалија, потребно је узети у обзир потенцијалну примену у различитим мрежним окружењима, при чему је циљ обезбедити скалабилност модела у контексту: повећања броја учесника у комуникацији, промене профила тренутно испитиваног саобраћаја, повећања протока и количине информација које је потребно обрадити, као и активног испитивања и примену тренутно најповољнијег алгорита машинског учења.
- Постоји могућност дефинисања скупа хибридних алгоритама машинског учења којима ће бити могућ ефикасан рад у систему са структурално различитим улазним подацима. Истраживања у овој области указују на све већу тенденцију ка комбиновању више техника учења као и гранулацији процедура система за откривање напада и аномалија мрежног саобраћаја [10, 11]. Приступ комбинованог машинског учења у контексту ове тезе биће предвиђен кроз примену метода композитних класификатора (ensemble classifiers), груписања (clustering) које се може примењивати и у процесу предобраде података и касније при учењу, као и комбинованог надгледаног/ненадгледаног учења. Поштоваће се принцип заснован на примени концепта грануларног рачунарства, којим се омогућила примена машинског учење у

области обраде великих количина података (Big Data) и у области дубоког учења (Deep Learning) [12].

4. Научне методе истраживања

У обради предложене теме докторске дисертације, поред општих метода научног истраживања, биће примењене методе моделовања, функционалне анализе и симулације. Основни принцип је заснован на испуњавању три корака:

Моделовање: Примена метода машинског учења и оптимизација параметара како би одговарали најбољем моделу/конкретној примени.

Евалуација: Вредновање методе на основу прорачуна вредности одговарајућих метрика и њихова верификација у односу на мрежно окружење од интереса.

Имплементација: Генерисање оквира методе, односно примена модела који је на основу експерименталне анализе остварио најбоље перформансе.

Методологија истраживања и анализе ће бити примењена кроз следеће фазе:

Ф1. Утврђивање карактеристика скупа података одређеног за анализу и увођење модификација у складу са њиховим карактеристикама:

(а) Чишћење и обележавање претходно необележених аномалија које су уочљиве мануелним прегледом скупа података;

(б) Фрагментација континуалних токова саобраћаја у епохе од по један минут;

(в) Проширење скупа података синтетичким токовима зависним од анализираног модела саобраћаја;

(г) Допуна недостајућих података, усаглашавање типова атрибута којима се манипулише (номинални, категорички, итд.), по потреби да се обави нормализација или стандардизација улазних података.

Ф2. Препроцесирање са циљем добијања скупа оптималних података за даљу обраду. Иницијално препроцесирање је засновано на примени статистичких метода и прорачуна ентропије дистрибуција различитих параметара које је могуће прорачунати на основу података прикупљених NetFlow протоколом.

Ф3. Комбинована примена различитих метода машинског учења из различитих категорија (надгледано, ненадгледано, полунадгледано). Алгоритми машинског учења уче на основу задате хипотезе, модела система и одабраног класификатора. Ова фаза подразумева неколико подфаза:

(а) препознавање „регуларних“ догађаја и њихово издвајање из даље анализе;

(б) детекција аномалија и напада, лабелирање и издвајање из скупа преосталих „непознатих“ догађаја;

(в) испитивање „непознатих“ догађаја уз лабелирање и логовање за даљу анализу;

(г) редовно ажурирање скупа инстанци за обучавање алгоритма у циљу све бољег учења система и ефикасније детекције аномалија и напада.

Ф4. Експериментална анализа резултата заснована на примени модела хибридног машинског учења дефинисаног у оквиру предложеног система. Основна мера успешности алгоритма

класификације заснива се на прорачуну тачности класификације, прецизности (позитивне вредности предикције), осетљивости (вероватноћа детекције), специфичности, и мерама перформанси изведених из основних метрика (False Positive, False Negative, True Positive и True Negative) као што је ROC крива (Receiver Operating Characteristic).

5. Очекивани научни допринос

У оквиру предложене докторске дисертације очекују се следећи доприноси:

- Анализа, класификација и поређење постојећих концепата детекције аномалија и напада у модерним мрежним окружењима;
- Концепт оригиналног модела хибридног алгоритма машинског учења за примену у детекцији аномалија и напада у модерним мрежним окружењима.
- Свеобухватна анализа резултата добијених на основу извршавања скупа симулација над анализираним скуповима података.
- Естимација могућности примене предложеног модела у савременим мрежним окружењима (IoT, Cloud Computing);
- Предлог примене и интеграције решења IDS детекције у контексту интеракције са деловима система за превенцију и реакцију на нападе.

6. План истраживања и структура рада

Имајући у виду постављене циљеве, план истраживања је следећи:

- Анализа актуелних проблема истраживања у области система за детекцију аномалија/напада и анализа резултата објављених у стручној литератури;
- Преглед система за детекцију аномалија и напада и преглед алата за испитивање перформанси метода машинског учења и анализу резултата;
- Приказ принципа конструисања нове методе за детекцију различитих врста напада, дефинисање функционалног модела система, генеричка спецификација мрежног окружења које се разматра, типа напада и предлог алгоритма анализе перформанси модела за детекцију аномалија или напада;
- Избор алата за испитивање перформанси и извођење неопходних тестова над скуповима података.
- Извођење експеримената и анализа резултата узимајући у обзир варијације различитих параметара: димензије мреже, извори саобраћаја нападача, карактеристике елемената мреже, типови напада и аномалија;
- Предлог потенцијалне примене предложеног решења у контексту различитих услова рада и карактеристика мрежног саобраћаја.

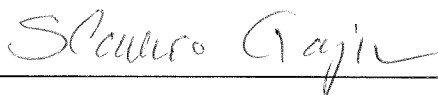
7. Закључак и предлог

Комисија је мишљења да је предложена тема докторске дисертације „Детекција напада у рачунарским мрежама заснована на анализи структуре саобраћаја применом комбинованих алгоритама машинског учења“ 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 кандидаткиње мр Валентине Тимченко, Комисија је донела одлуку да је она способна за научно-истраживачки рад и за реализацију предвиђених истраживања. Одлука је донета имајући у виду њене досадашње стручне резултате остварене током основних, магистарских и докторских студија, као и на основу њеног 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 „Детекција напада у рачунарским мрежама заснована на анализи структуре саобраћаја применом комбинованих алгоритама машинског учења“ и да кандидаткињи мр Валентини Тимченко омогући да приступи њеној изради.

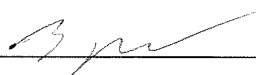
У Београду, 14.10.2019. године

ЧЛАНОВИ КОМИСИЈЕ



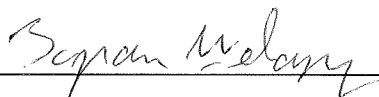
др Славко Гајин, ванредни професор,

Универзитет у Београду – Електротехнички факултет



др Зоран Јовановић, редовни професор у пензији

Универзитет у Београду – Електротехнички факултет



др Зоран Шеварац, ванредни професор,

Универзитет у Београду – Факултет организационих наука



др Зоран Чича, ванредни професор,

Универзитет у Београду – Електротехнички факултет

