

УНИВЕРЗИТЕТ У БЕОГРАДУ

Факултет организационих наука

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Подобност теме и кандидата Људмиле Жарове (Lyudmila Zharova) за израду докторске дисертације

Одлуком 3/103-4 од 11.07.2018. године именовани смо за чланове Комисије за оцену теме и подобности кандидата **Људмиле Жарове** за израду докторске дисертације и научне заснованости теме „Развој безбедних IoT мрежа заснован на архитектури нултог поверења“.

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

РЕФЕРАТ

1. Подаци о кандидату

1.1. Биографски подаци

Људмила Жарова (Lyudmila Zharova) је рођена 1962 у Черкаску, Украјина где је завршила основну и средњу школу. Завршила је основне студије на два факултета. Државни Универзитет Харков у Украјини, Департман за филологију и романистику завршила је 1987. године са звањем Магистра француског и енглеског језика и књижевности. Завршила је и студије на АСА колеџу за Бизнис и рачунарске технологије у Бруклину, Њу Јорк, САД, 1999. године са дипломом у области програмирања и информационих технологија (ASA College, Computer Programing and Information Technology Associate of Occupational Studies Degree Program in New York). Мастер студије је завршила 2015. године на Њу Јоршком Институту за Технологију у Њу Јорку, САД, на Департману за безбедност информација, мрежа и рачунара (New York Institute of Technology, Master of Science in Information, Network, and Computer Security). Универзитет у Београду је 3.11.2016 донео Решење да се признаје високошколска исправу другог нивоа образовања број 06-61301-3762/2-16. Од 2016. године Људмила Жарова је студент докторских студија на Факултету организационих наука у Београду, студијски програм Информациони системи и квантитативни менаџмент, изборно подручје Електронско пословање. Тренутно је студент друге године докторских студија. Положила је све програмом предвиђене испите на докторским студијама са просечном оценом 10.

Од 1999. до 2007. године поред студирања, активно је радила као програмер и аналитичар у компанији Related Inc., у Њу Јорку. Као развојни инжењер радила је за компанију TBS Shipping Services, у Јонкерсу, САД. Као архитекта решења је радила за BGB у Њу Јорку, а као развојни инжењер ради за 3C компанију и компанију MRM Worldwide, у Њу Јорку 2009 – 2010. Године 2011. је радила као развојни инжењер архитекта Sharepoint решења за MF Global, у Њу Јорку. Од 2011. ради за компанију Stroz Friedberg LLC, у Њу Јорку као софтвер архитекта.

Људмила Жарова је завршила више програма стручног усавршавања и сертификације: Certification authority; Introduction to the Internet of Things and Embedded System; Microsoft Certified IT Professional; Microsoft Certified Technology Specialist; Microsoft Certified Professional Developer; SharePoint Administrator; SharePoint Configuration; SharePoint Developer; Web Developer.

Држала је предавања на више стручних скупова и учествовала у раду радних група стручних удружења, од којих се могу издвојити: 5th Annual Hartford Code Camp; NYC SharePoint Developers User Group; SharePoint Saturday Philly; SharePoint LA; SharePoint New York City; NYC Code Camp.

1.2. Стечено научноистраживачко искуство

У наставку ће бити приказане научноистраживачке активности кандидата. Оне обухватају радове објављене на конференцијама и у часописима, и преглед положених испита.

Током досадашњег рада Људмила Жарова је објавила више радова у земљи и иностранству и учествовала на више међународних и домаћих скупова и конференција.

Радови у зборницима научних скупова међународног значаја штампани у целини (M33):

1. V. Leggio, L. Zharova, R.A. Mihajlovic, A.R. Mihajlovic, (2017) "Structured Approach to IoT Protocol Security Analysis," BISEC2017, Proceedings of the Ninth International Conference on Business Information Security, Belgrade, 18th October 2017, pp.33-35.
2. V. Leggio, L. Zharova, A.R. Mihajlovic, S. Dontu, R.A. Mihajlovic, (2017) "Software Development Problems of the SDN Internals Engineering," BISEC2017, Proceedings of the Ninth International Conference on Business Information Security, Belgrade, 18th October 2017, pp.58-70.
3. L. Zharova, V. Leggio, A. Mihajlovic, S. Campbell, R. Mihajlovic. (2016). „Road Vehicle Embedded IoT Security“, BISEC2016, Belgrade, 15th October 2016, pp.18-26.
http://www.metropolitan.edu.rs/files/2016/10/BISEC2016_Conference-Proceedings.pdf
4. V. Leggio, L. Zharova, I. Stankovic, R. A. Mihajlovic, (2017) "On Some E-Commerce and Mobile Payment Security Issues," LEMIMA2017, Belgrade Serbia, 2017, Vol.II, pp.171-182.
5. R.A. Mihajlovic, L. Zharova, J.S. Mihajlovic, V. Leggio, (2017) "Systems Analysis of Political e-Marketing and Personal Branding in the USA Presidential Elections of 2016," LEMIMA2017, Belgrade Serbia, 2017, Vol.I, pp.57-72.

Радови у часописима националног значаја (M50)

1. L. Zharova, I. Stankovic, R. Mihajlovic, (2017) "Secure Activities Monitoring and Auditing in the Cloud," UDC 004.45, International Journal of Economics and Law, No.7, pp.143-151. ISSN: 2217-5504, M53, <http://media3.novi.economicsandlaw.org/2017/07/Zharova-16-IJEAL.pdf>

Радови у зборницима научних скупова националног значаја штампани у целини (M63):

1. R. Mihajlović, I. Stanković, V. Leggio, L. Zharova, (2017) "On Strategic Cyberwarfare Planning," *SPSSM 2017*, No.23, Beograd, Mart 13, 2017.
2. L. Zharova, V. Leggio, J.S. Mihajlovic, R.A. Mihajlovic, (2017) "Analysis of the strategic e-marketing planning of the last USA presidential elections," *SPSSM 2017*, No.24, Beograd, Mart 13, 2017.
3. L. Zharova, V. Leggio, J. Mihajlovic, R.A. Mihajlovic, (2018) "IoT Powered Modern Enterprise and Zero Trust Management," *IMCSM2018, XIV International May Conference on Strategic Management*, May 25-27, 2018. pp.14.
4. V. Leggio, L. Zharova, I. Stankovic, R.A. Mihajlovic, (2018) "Innovative Application of IoT and Cloud Computing to Management Information Systems," *IMCSM2018, XIV International May Conference on Strategic Management*, May 25-27, 2018. pp.34.

Мастер тезу је одбранила је 2015. године.

Кандидаткиња је дана 26.09.2018. године успешно одбранила приступни рад за израду дисертације под називом „Развој безбедних IoT мрежа заснован на архитектури нултог поверења“.

1.3. Оцена подобности кандидата за рад на предложеној теми

Узимајући у обзир:

- резултате остварене током досадашњег образовања;
- резултате истраживања у области интернета интелигентних уређаја и IoT сигурности, која су публикована на научно-стручним конференцијама и у часописима;
- радно искуство у области информационих технологија и развоја софтвера;

закључује се да је Људмила Жарова у потпуности квалификована и припремљена да тему докторске дисертације самостално истражује и пружи научно-стручне доприносе у тој области.

2. Предмет и циљ истраживања

Предмет истраживања докторске дисертације је развој безбедних IoT (енг. *Internet of Things*) мрежа пројектованих у складу са безбедносном архитектуром нултог поверења (енг. *Zero Trust Architecture*), у условима учесталих промена топологије IoT мреже и технолошких ограничења у могућностима одбране од малициозних напада, првенствено на нижим нивоима ISO-OSI референтног модела. Посебан фокус истраживања ће бити на ободу (енг. *edge*) IoT мреже, у коме функционишу IoT уређаји у условима наглашене промене топологије. Ове промене могу настати услед: престанка батеријског напајања IoT уређаја, физичког напада, крађе уређаја, недозвољеног упада у систем, као и угрожавања перформанси мреже са последицама блокирања сервиса (енг. *Denial of Service*).

Безбедне IoT мреже треба да: извршавају задате функционалности без обзира на промену у топологији мреже, одрже оптималне перформансе у односу на кориснике (људи или уређаји) и имају задовољавајућу робусност и безбедносну отпорност (енг. *Attack Resistance*) (Siddiqui et al. 2018). У области пројектовања безбедних IoT мрежа, у истраживачком и практичном раду је до сада мање пажње посвећивано безбедносној отпорности, а више развоју функционалних IoT уређаја једноставних за употребу (Al-Fuqaha et al. 2015)(Parmar & Desai, 2016)(Restuccia, 2018)(Smith, 2018).

Основа за пројектовање модела у овој дисертацији ће бити модел архитектуре безбедности нултог поверења (Kindervag, 2010)(Beck, 2014)(Kindervag, 2016). Овај модел се заснива на претпоставци да је сав саобраћај у мрежи несигуран и да се мора скенирати и ауторизовати. Ауторизација се врши на гејтвеју који представља централни део мреже и на коме се имплементирају сигурносне политике. Коришћење централизованог гејтвеја омогућава једноставну и ефикасну аквизицију мрежних података и њихову анализу у скоро реалном времену. За чување и анализу података користе се *big data* инфраструктура и сервиси (Anawar et al. 2018). Основне предности модела нултог поверења су независност од платформе, линеарна скалабилност, сигурна виртуелизација мреже и прилагођеност за примену у *cloud* инфраструктурама и рачунарским мрежама наредне генерације (енг. *next generation networks*) (DeCusatis et al. 2016)(Puthal, 2017) (Zhang, 2018).

За дефинисање методологије пројектовања архитектуре безбедних IoT мрежа у *cloud* окружењу размотриће се могућности и ограничења постојећих метода заснованих на апстракцији и виртуелизацији инфраструктуре (Pasquier et al. 2015)(Puthal, 2016) (Guo et al. 2017), уз употребу софтверски дефинисаних инфраструктурних елемената, као што су: софтверски дефинисано складиштење података (енг. *software defined storage*, SDS), софтверски дефинисане мреже (енг. *software defined networks*, SDN), софтверски дефинисани радио систем (енг. *software defined radio*, SDR), софтверски дефинисана безбедност (енг. *software defined security*, SDS) и виртуелизација протока података (енг. *data flow virtualization*, DFV)(Liu et al. 2015)(Vandana, 2016)(Kim et al. 2017)(Kim et al. 2018). Ограничења која приликом дефинисања методологије пројектовања посебно треба узети у обзир су: недостатак, несавршеност и честе промене постојећих стандарда, као и убрзани развој IoT хардвера, посебно за бежичне мрежне уређаје (Tayyaba et al. 2016) (Jayavel et al. 2017).

Модел архитектуре нултог поверења ће у овом раду бити проширен на цео организациони систем у коме IoT мрежа функционише. Модел ће обухватити људске ресурсе, IoT чворишта и остале рачунарске, софтверске и хардверске ресурсе који учествују у пословним процесима. У сваком од ових делова организационог система може постојати сигурносна претња која може довести до поремећаја функционисања IoT мреже и континуитета пословања организационе целине у којој мрежа функционише. Анализа ће се заснивати на резултатима актуелних истраживања објављених у релевантној литератури, која се односе на пројектовање безбедних архитектура, од спецификације захтева до процеса пројектовања конкретне мреже (Kim, 2015)(Puthal et al. 2017)(Abawajy et al. 2018)(Caminha, 2018)(Luo et al. 2018).

При дефинисању модела ће се узети у обзир:

- спецификација мреже,
- могућности отказа појединих хардверско-софтверских компоненти,
- очекиване промене у хардверу и софтверу на елементима мреже,
- променљива природа мрежног саобраћаја,
- променљиви захтеви безбедности,
- могуће промене понашања корисника,
- могући напади,
- финансијска ограничења.

Истраживачки рад ће бити усмерен ка испитивању могућности да се утврди корелација између структура мреже и компонената на физичком нивоу, са виртуелизованом контролом на нивоу управљања.

За IoT мреже, пројектовање система вођено архитектуром се показало као ефикасан начин пројектовања у односу на приступе вођене првенствено функционалним захтевима, документацијом или методологијом (Cavalcante, 2015)(Rodrigues et al. 2015). У овом

истраживању се архитектура IoT мреже посматра као подскуп архитектуре пословног система.

Примарни резултат истраживања у дисертацији треба да буде развој новог приступа пројектовању архитектуре комплексних IoT мрежа са фокусом на проблеме пројектовања безбедносне инфраструктуре у условима нултог поверења у односу на све кориснике. Применом концепата хијерархијске апстракције, паралелизације, виртуализације и софтверске контроле, биће дефинисан начин оптималног решавања проблема насталих услед губитака појединих делова IoT топологије на ободима система. Поступак пројектовања који се предлаже укључује и методе евалуације функционалности, перформанси и безбедносне робустности архитектуре у раним фазама пројектовања. Предложене методе ће бити засноване на симулацијама и мерењима која су често примењивана у току тестирања готовог пројекта али нису уобичајена за ране фазе пројектовања, што би омогућило идентификацију типичних грешака приликом израде спецификација, као и при пројектовању архитектуре.

Поред фокуса на унапређење архитектура са аспекта квалитета сервиса (енг. *quality of service*, QoS), пажња ће бити посвећена дефинисању скупа параметара који се односе на квалитет корисничког искуства (енг. *quality of experience*, QoE/QoX), тј. на субјективни доживљај при коришћењу имплементираних технологија.

Почетна листа библиографских извора која ће се користити приликом израде докторске дисертације:

- [1] J. Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", Forrester Research, 2010.
http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf
- [2] J Kindervag, "No more chewy centers: The Zero Trust Model Of Information Security", Forrester Research 2016. <http://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf>
- [3] E. Beck, How Zero-trust Network Security Can Enable Recovery From Cyberattacks, ISACA Journal, Vol 6. 2014. <https://www.isaca.org/Journal/archives/2014/Volume-6/Pages/How-Zero-trust-Network-Security-Can-Enable-Recovery-From-Cyberattacks.aspx>
- [4] D. Puthal, S. Nepal, R. Ranjan and J. Chen, "Threats to Networking Cloud and Edge Datacenters in the Internet of Things," in *IEEE Cloud Computing*, vol. 3, no. 3, pp. 64-71, May-June 2016.
doi: 10.1109/MCC.2016.63
- [5] F. Siddiqui, M. Hagan and S. Sezer, "Embedded policing and policy enforcement approach for future secure IoT technologies," *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, 2018, pp. 1-10. doi: 10.1049/cp.2018.0010
- [6] D. Banerjee, B. Dong, M. Taghizadeh and S. Biswas, "Privacy-Preserving Channel Access for Internet of Things," in *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 430-445, Oct. 2014.
doi: 10.1109/JIOT.2014.2346513
- [7] J. Guo, I. Chen, J.J.P. Tsai, "A survey of trust computation models for service management in internet of things systems", *Computer Communications*, Vol 97, 2017, pp 1-14, DOI: 10.1016/j.comcom.2016.10.012.
- [8] J. Abawajy, S. Huda, S. Sharmeen, M. Mehedi Hassan, A. Almogren, "Identifying cyber threats to mobile-IoT applications in edge computing paradigm," *Future Generation Computer Systems*, 2018, DOI: 10.1016/j.future.2018.06.053.

- [9] P. Zhang, M. Zhou, G. Fortino, "Security and trust issues in Fog computing: A survey," *Future Generation Computer Systems*, Vol 88, 2018, pp 16-27, DOI: doi.org/10.1016/j.future.2018.05.008.
- [10] D. Puthal, S. P. Mohanty, P. Nanda and U. Choppali, "Building Security Perimeters to Protect Network Systems Against Cyber Threats [Future Directions]," in *IEEE Consumer Electronics Magazine*, vol. 6, no. 4, pp. 24-27, Oct. 2017. doi: 10.1109/MCE.2017.2714744
- [11] E. Cavalcante, "On the Architecture-Driven Development of Software-Intensive Systems-of-Systems," 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering, Florence, 2015, pp. 899-902. doi: 10.1109/ICSE.2015.287
- [12] T. C. Rodrigues, T. Batista, F. C. Delicato and P. d. F. Pires, "Architecture-Driven Development Approach for WSN Applications," 2015 IEEE 13th International Conference on Embedded and Ubiquitous Computing, Porto, 2015, pp. 68-75. doi: 10.1109/EUC.2015.15
- [13] C. DeCusatis, P. Liengtiraphan, A. Sager and M. Pinelli, "Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication," 2016 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, 2016, pp. 5-10. doi: 10.1109/SmartCloud.2016.22
- [14] J. K. Parmar, A. Desai, "IoT: Networking Technologies and Research Challenges", *International Journal of Computer Applications*, Vol. 154 No. 7, pp. 1-6, November 2016.
- [15] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, J. Henry, "IoT Fundamentals : Networking Technologies, Protocols, and Use Cases for the Internet of Things", Published by: Cisco Press, 2017.
- [16] L. Zharova, et al, "Structured Approach To IoT Security Analysis", The 9 International Conference on Business Information Security the (BISEC-2017), 18 October 2017, Belgrade, Serbia.
- [17] F. Restuccia, "Securing the Internet of Things: New Perspectives and Research Challenges", *IEEE Internet of Things Journal*, vol. 1, no. 1, January 2018, 2018
- [18] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, M. Rossi, "Secure Communication for Smart IoT Objects: Protocol Stacks, Use Cases and Practical Examples", *IEEE*, 2012.
- [19] D. Altolini, V. Lakkundi, N. Bui, C. Tapparello, M. Rossi, "Low Power Link Layer Security for IoT: Implementation and Performance Analysis", *IEEE*, 2013.
- [20] V. Lakkundi, K. Singh, "Lightweight DTLS Implementation in CoAP-based Internet of Things", 20th Annual International Conference on Advanced Computing and Communications, ADCOM, 2014.
- [21] P. Kolios, G. Ellinas, C. Panayiotou, M. Polycarpou, "Energy Efficient Event-Based Networking for the Internet of Things", 2016 IEEE 3rd World Forum on Internet of Things, WF-IoT, 2016.
- [22] K. Das, S. Das, A. Mishra, A. Mohapatra, "Energy Efficient Data Prediction Model for the Sensor Cloud Environment", *IEEE International Conference on IoT and its Applications, ICIOT*, 2017.
- [23] S. G. T. Krishna, "A Systematic Study of Security Issues in Internet-of-Things (IoT)," *Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud)*, pp. 107–111, 2017.

- [24] E. R. Naru, H. Saini, M. Sharma, "A recent review on lightweight cryptography in IoT", Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC, 2017.
- [25] P. C. Ccori, L. C. Costa De Biase, M. K. Zuffo, F. S. Correa da Silva, "Device discovery strategies for the IoT", 2016 IEEE International Symposium on Consumer Electronics (a), 2016.
- [26] N. Bejar, O. Novo, J. Jimenez, J. Melen, "Gateway Selection in Capillary Networks Nicklas", 2015 5th International Conference on the Internet of Things (IoT) Gateway, 2015.
- [27] S. N. Swamy, "Security Threats in the Application layer in IOT Applications," pp. 477–480, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.
- [28] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015. doi: 10.1109/COMST.2015.2444095.
- [29] J.E. Luzuriaga, M.Perez, P. Boronat, J. C. Cano, C. Calafate, P. Manzoni, "A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks", 2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC, 2015
- [30] MicroThings: A Generic IoT Architecture for Flexible Data Aggregation and Scalable Service Cooperation, IEEE Communications Magazine, vol. 55, 2017.
- [31] P Kayal, H Perros, " A Comparison of IoT application layer protocols through a smart parking implementation", 20th Conference on Innovations in Clouds, Internet and Networks, ICIN 2017, pp. 331-336, 2017.
- [32] K. Jayavel, V. Nagarajan, K. Sornalakshmi, K. Navin, "Migration techniques of data centric networks to internet of Things with control plane based virtual sensor layer", IEEE International Conference on IoT and its Applications, ICIOT, 2017.
- [33] D. Mendez, I. Papapanagiotou, B. Yang, " IOT security Internet of Things: Survey on Security and Privacy", Information Security Journal: A Global Perspective, 2018.
- [34] K. W. Kim, S. G. Min and Y. H. Han, "A programmable data plane to support in-network data processing in software-defined IoT," 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2017, pp. 855-860. doi: 10.1109/ICTC.2017.8190798 7.
- [35] J. Liu, Y. Li, M. Chen, W. Dong and D. Jin, "Software-defined internet of things for smart urban sensing," in IEEE Communications Magazine, vol. 53, no. 9, pp. 55-63, September 2015. doi: 10.1109/MCOM.2015.7263373
- [36] Object Management Group, OMG, " DDS – The Proven Data Connectivity Standard for IoT",
- [37] T. Salman, R. Jain, "Networking protocols and standards for internet of things", <https://doi.org/10.1002/9781119173601.ch13>, 2016.
- [38] A. Dhumane, R. Prasad, J. Prasad, "Routing Issues in Internet of Things : A Survey", Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists, pp. 404-412, 2016.

- [39] O. Vermesan, P. Friess, "Internet of Things – From Research and Innovation to Market Deployment", River Publishers, 2014.
- [40] J. E. Luzuriaga, M. Perez, P. Boronat, J. Cano et al., "Improving MQTT Data Delivery in Mobile Scenarios: Results from a Realistic Testbed", Mobile Information Systems, 2016.
- [41] K. Yelamarthi, S. Aman, A. Abdelgawad, "An application-driven modular IoT architecture", Wireless Communications and Mobile Computing, Vol. 2017, <https://doi.org/10.1155/2017/1350929>, 2017.
- [42] M. Pasha, S. Muhammad W. Shah, "Framework for E-Health Systems in IoT-Based Environments", Wireless Communications and Mobile Computing Vol. 2018, <https://doi.org/10.1155/2018/6183732>, 2018.
- [43] J. S. Kumar, M. A. Zaveri, "Clustering Approaches for Pragmatic Two-Layer IoT Architecture", Wireless Communications and Mobile Computing Volume 2018, <https://doi.org/10.1155/2018/8739203>, 2018.
- [44] F. Liu, P. Li, D. Deng, "Device-Oriented Automatic Semantic Annotation in IoT," Journal of Sensors Volume 2017, <https://doi.org/10.1155/2017/9589064>, 2017.
- [45] M. De Donno, N. Dragoni, A. Giaretta, A. Spognardi, "DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation", Security and Communication Networks Volume 2018, <https://doi.org/10.1155/2018/7178164>, 2018.
- [46] Y. Kim, J. Seok, Y. Jung, O. Ha, "Light-Weight and Versatile Monitor for a Self-Adaptive Software Framework for IoT Systems", Journal of Sensors, Vol. 2016, <http://dx.doi.org/10.1155/2016/8085407>, 2016.
- [47] I. Sohn, "Small-World and Scale-Free Network Models for IoT Systems", Mobile Information Systems Vol. 2017, <https://doi.org/10.1155/2017/6752048>, 2017.
- [48] K. Lee, Y. Kim, C. Yoo, "The Impact of Container Virtualization on Network Performance of IoT Devices", Mobile Information Systems Vol. 2018, <https://doi.org/10.1155/2018/9570506>, 2018.
- [49] V. Sharma, K. Lee, S. Kwon et al., "A Consensus Framework for Reliability and Mitigation of Zero-Day Attacks in IoT", Security and Communication Networks Volume 2017, <https://doi.org/10.1155/2017/4749085>, 2017.
- [50] S. Ali, M. Golam Kibria, M. Aslam Jarwar et al., "A Model of Socially Connected Web Objects for IoT Applications", Wireless Communications and Mobile Computing Volume 2018, <https://doi.org/10.1155/2018/6309509>, 2018.
- [51] K. Kim, S. Min, Y. Han, "In-network Data Processing in Software-defined IoT with a Programmable Data Plane", Mobile Information Systems Volume 2018, <https://doi.org/10.1155/2018/8618267>, 2018.
- [52] M. R. Anawar, S. Wang, M. Azam Zia et al., "Fog Computing: An Overview of Big IoT Data Analytics", Wireless Communications and Mobile Computing Volume 2018, <https://doi.org/10.1155/2018/7157192>, 2018.
- [53] M.A. Ferrag, L.A. Maglaras, H. Janicke et al., "Authentication Protocols for Internet of Things: A Comprehensive Survey", Security and Communication Networks Volume 2017, <https://doi.org/10.1155/2017/6562953>, 2017.
- [54] M. Luo, Y. Luo, Y. Wan, Z. Wang, "Secure and Efficient Access Control Scheme for Wireless Sensor Networks in the Cross-Domain Context of the IoT", Security and Communication Networks Volume 2018, Article ID 6140978, <https://doi.org/10.1155/2018/6140978>, 2018.

- [55] A. Abdelgawad, K. Yelamarthi, "Internet of things (IoT) platform for structure health monitoring", *Wireless Communications and Mobile Computing* Volume 2017, <https://doi.org/10.1155/2017/6560797>, 2017.
- [56] H. Kim, S. Yun, H. Kim et al., "An Efficient SDN Multicast Architecture for Dynamic Industrial IoT Environments", *Mobile Information Systems* Volume 2018, <https://doi.org/10.1155/2018/8482467>, 2018.
- [57] X. Su, Z. Wang, X. Liu, C. Choi et al., "Study to Improve Security for IoT Smart Device Controller: Drawbacks and Countermeasures", *Security and Communication Networks* Volume 2018, <https://doi.org/10.1155/2018/4296934>, 2018.
- [58] S. Gokceli, N. Zhmurov, G. Karabulut Kurt et al., "IoT in Action: Design and Implementation of a Building Evacuation Service", *Journal of Computer Networks and Communications* Volume 2017, <https://doi.org/10.1155/2017/8595404>, 2017.
- [59] S. Kim, "Learning-based QoS control algorithms for next generation internet of things", *Mobile Information Systems* Volume 2015, <http://dx.doi.org/10.1155/2015/605357>, 2015.
- [60] J. Granjal, A. Pedroso, "An Intrusion Detection and Prevention Framework for Internet-Integrated CoAP WSN", *Security and Communication Networks* Volume 2018, <https://doi.org/10.1155/2018/1753897>, 2018.
- [61] P. Sethi, S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", *Journal of Electrical and Computer Engineering* Volume 2017, <https://doi.org/10.1155/2017/9324035>, 2017.
- [62] J. Caminha, A. Perkusich, M. Perkusich, "A Smart Middleware to Detect On-Off Trust Attacks in the Internet of Things", *Security and Communication Networks* Vol. 2018, <https://doi.org/10.1155/2018/6063456>, 2018.
- [63] A. Otebolaku, G. M. Lee, "A Framework for Exploiting Internet of Things for Context-Aware Trust-Based Personalized Services", *Mobile Information Systems* Vol. 2018, <https://doi.org/10.1155/2018/6138418>, 2018.
- [64] J.B. Bernabe, J. L. Hernandez-Ramos, A. F. Skarmeta Gomez, "Holistic Privacy-Preserving Identity Management System for the Internet of Things", *Mobile Information Systems* Vol. 2017, <https://doi.org/10.1155/2017/6384186>, 2017.
- [65] Z. Cai, R. N. Chang, S. Forsström et al., "Privacy in the Internet of Things", *Wireless Communications and Mobile Computing* Vol. 2018, <https://doi.org/10.1155/2018/8281379>, 2018.
- [66] J. Jarzombek, "IoT Supply Chain Management: Reducing Attack Vectors & Enabling Cybersecurity Assurance", *IEEE 4th World Forum on Internet of Things*, <http://wfiot2018.iot.ieee.org/program/track-presentations/>, 2018.
- [67] S. W. Smith, "Securing the IoT: Critical Research Challenges", *IEEE 4th World Forum on Internet of Things*, <http://wfiot2018.iot.ieee.org/program/track-presentations/>, 2018.
- [68] J. Guajardo, "Towards A More Secure Internet Of Everything", *IEEE 4th World Forum on Internet of Things*, <http://wfiot2018.iot.ieee.org/program/track-presentations/>, 2018.
- [69] C. Rodriguez, "DDoS Emerges as Primary Threat Vector for IoT", *Stratecast Perspectives & Insight for Executives (SPIE)* Volume 16, Number 41, 2016.
- [70] S. Vinoski, "Advanced Message Queuing Protocol," in *IEEE Internet Computing*, vol. 10, no. 6, pp. 87-89, Nov.-Dec. 2006. doi: 10.1109/MIC.2006.116.
- [71] O. Vermesanand, P. Friess, "Internet of Things – From Research and innovations to Market Deployment", *River Publishers Series in Communication*, 2014

- [72] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, “ Security, Privacy and Trust in Internet of Things : The road ahead”, Computer Networks, Vol. 76, 2015, pp. 146-164, DOI: 10.1016/j.comnet.2014.11.008.
- [73] M. J. Covington, R. Carskadden, “Threat Implications of the Internet of Things”, 5th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, 2013. https://ccdcoe.org/cycon/2013/proceedings/d1r1s6_covington.pdf.
- [74] Z. Zhang, M. Cheng, Y. Cho, C. Wang, “ IoT security: Ongoing challenges and research opportunities”, Proceedings - IEEE 7th International Conference on Service-Oriented Computing and Applications, SOCA 2014, pp. 230-234, 2014.
- [75] M. Ahlmeyer, A. M. Chirc, “Securing the Internet of Things : a Review’, Issues in Information Systems, http://www.iacis.org/iis/2016/4_iis_2016_21-28.pdf, 2015.
- [76] H. Suoa, J. Wan, C. Zoua et al., “Security in the Internet of Things: A Review”, 2012 International Conference on Computer Science and Electronics Engineering, DOI: 10.1109/ICCSEE.2012.373, 2012.
- [77] A. Gantait, J. Patra, A. Mukherjee , “Securing IoT devices and gateways”, IBM developerWorks, <https://www.ibm.com/developerworks/library/iot-trs-secure-iot-solutions1/iot-trs-secure-iot-solutions1-pdf.pdf>, 2016.
- [78] C.P. Vandana, “Security improvement in IoT based on Software Defined Networking (SDN)”, International Journal of Science, Engineering and Technology Research, <http://ijsetr.org/wp-content/uploads/2016/01/IJSETR-VOL-5-ISSUE-1-291-295.pdf>, 2016.
- [79] C. Li, Z. Qin, E. Novak, Q. Li, “Securing SDN Infrastructure of IoT-Fog Networks from MitM Attacks”, IEEE Internet of Things Journal, vol. 4, no. 5, 2017, pp.1156-1164
- [80] K. S. Sahoo, B. Sahoo, A. Panda, “ A secured SDN framework for IoT”, Proceedings - 2015 International Conference on Man and Machine Interfacing, MAMI 2015, DOI: 10.1109/MAMI.2015.7456584
- [81] I. Cvitić, M. Vujić, S. Husnjak, “Classification of Security Risks in the IoT Environment”, 26th DAAAM International Symposium, Viena, 2016, DOI: 10.2507/26th.daaam.proceedings.102
- [82] J. S., T. Pasquier, J. Bacon et al., “ Twenty security considerations for cloud-supported Internet of Things”, IEEE Internet of Things Journal, Vol. 3, No. 3, pp. 269-284, 2015.
- [83] S. K. Tayyaba, N.S.A. Khan, et al., “Software-Defined Networks (SDNs) and Internet of Things (IoTs): A Qualitative Prediction for 2020”, International Journal of Advanced Computer Science and Applications, Vol 7, No. 11, 2016. DOI: 10.14569/IJACSA.2016.071151
- [84] L. Zharova, V. Leggio, J. Mihajlovic, R. A. Mihajlovic, “IoT Powered Modern Enterprise and Zero Trust Management,” IMCSM2018, XIV International May Conference on Strategic Management, May 25-27, 2018. pp.14.
- [85] W. H. Chin, Z. Fan, R. Haines, ”Emerging technologies and research challenges for 5G wireless networks”, IEEE Wireless Communications, vol. 21, no. 2, Apr. 2014, pp.106-112.
- [86] Y. Liu, A. Y. Ding, S. Tarkoma, "Software-Defined Networking in Mobile Access Networks," Technical Report C-2013-1, University of Helsinki Department of Computer Science, Helsinki, September 19, 2013.
- [87] J. Stankovic, “Research Directions for the Internet of Things,”IEEE Internet of Things Journal, vol. 1, no. 1, Feb 2014, pp. 3-9.

- [88] M. Naohisa, T. Kenki, H. Sho, A. Hiroki, A. Aiko, "IoT Network Implemented with NFV," Special Issue on Telecom Carrier Solutions for New Value Creation, NEC Technical Journal, Vol.10 No.3, pp.35-40.
https://www.nec.com/en/global/techrep/journal/g15/n03/pdf/150308.pdf?fromPDF_E6803
- [89] J. Dizdarevic, F. Carpio, A. Jukan, X. Masip-Bruin, "A Survey of Communication Protocols for Internet-of-Things and Related Challenges of Fog and Cloud Computing Integration," ACM Computing Surveys, Vol. 1, No. 1, April 2018. pp.1-27.
- [90] Q. F. Hassan, A. Rehman Khan, S.A. Madani, "Internet of Things Challenges, Advances, and Applications," CRC Press, Taylor & Francis Group, LLC, 2018.

3. Полазне хипотезе

Главна хипотеза која ће бити тестирана у раду гласи:

Развојем и применом модела за пројектовање безбедних IoT мрежних система, заснованих на архитектури нултог поверења, унапређује се сигурност пројектоване архитектуре, повећава се степен искоришћења мреже и остварује већа флексибилност на промене у пословним процесима.

На основу дефинисаног предмета истраживања може се издвојити неколико посебних хипотеза:

- X01. Могуће је развити скуп патерна пројектовања адаптивних безбедних IoT мрежа у *cloud* окружењу заснованих на архитектури нултог поверења.
- X02. Архитектуру IoT мрежа је могуће контролисати софтвером у циљу прилагођавања променама током коришћења IoT система.
- X03. Пројектовање пословних процеса у предузећу је потребно извести интегрисано тј. у кохезији са пројектовањем IoT мреже.

Даљим прецизирањем наведених посебних хипотеза, формулишу се појединачне подхипотезе:

- X01.1. Адаптивност IoT мреже се може постићи софтверском аутоматизацијом виртуелизованих мрежних инстанци у складу са имплементацијом идентификованих патерна.
- X01.2. Адаптивну архитектуру засновану на прилагођавању променама физичких топологија на ободу, услед престанка рада или поновног активирања мрежних елемената, могуће је реализовати оптималном софтверском контролом.
- X02.1. Адаптивност контролисана софтвером је могућа у оквиру специфицираних карактеристика инстанци делова мрежа (енг. *network slice*) преко адаптације појединих инстанци виртуелних мрежа.
- X02.2. Адаптивност контролисана софтвером се може реализовати на хардверском нивоу.
- X02.3. Адаптивност контролисана софтвером је могућа на мрежно тополошком нивоу кроз флексибилни одабир и активирање резервних јединица на ободу.
- X02.4. Скуп идентификованих пројектних патерна се може интегрисати у јединствену методологију пројектовања комплексних IoT система.
- X03.1. Софтверска дефинисаност свих елемената инфраструктуре се може проширити, из домена ИКТ, у домен менаџмента и пословних процеса у оквиру архитектуре целокупног пословног система.

- X03.2. *Ad hoc* технике и методе системског инжењеринга архитектуре се могу интегрисати у скуп пројектних патерна за хибридно пројектовање архитектуре пословних система са гарантованим перформансама, безбедносном робусношћу и отвореношћу за скалирање и функционалне измене у току експлоатације система.

4. Научне методе истраживања

У сврху израде овог рада, од општих научних метода користиће се методе прикупљања и анализе постојећих научних резултата и достигнућа, моделирање, симулација, аналитичко-дедуктивна и статистичка метода. Моделирање се користи приликом израде модела архитектуре система комплексних интегрисаних мрежа. Формални дијаграми користиће се у анализи спецификација и домена проблема, као и на пројектовању архитектуре.

Поред основних системских и програмских алата користиће се и отворена софтверска решења и апликативни програмски интерфејси за повезивање контролне и физичке равни мреже засновани на *OpenFlow* протоколу у односу на мрежни контролер. На вишим нивоима архитектуре се разматра употреба протокола и пројекта отвореног кода за оркестрацију мрежних активности, као што су то *Cloudify* (за оркестрацију *cloud-a*) и *Tacker* (за оркестрацију виртуелизованих мрежних функција). Једна од метода у истраживању ће бити хибридне симулације, повезивањем виртуелизованих мрежа са више умрежених физичких IoT уређаја.

У вези са квантитативном анализом особина мрежних архитектура, оквир истраживања ће обухватити стандардне математичке апарате који се примењују у рачунарским мрежама: теорија графова, теорија скупова, вероватноћа, статистика са стохастичким процесима, теорија опслуживања редова чекања са анализом саобраћаја, теорија поузданости и робусности.

Истраживања која ће бити спроведена у докторској дисертацији су мултидисциплинарна и обухватају: организацију и архитектуру рачунарских мрежа, пројектовање софтвера и алгоритама, пројектовање хардвера и фирмвера, и пројектовање пословних процеса.

5. Очекивани научни допринос

Најзначајнији научни допринос дисертације ће бити развој модела безбедних IoT мрежа заснованих на концепту нултог поверења. Модел ће бити посебно прилагођен условима учесталих промена топологије IoT мреже и технолошким ограничењима у могућностима одбране од малициозних напада, првенствено на нижим нивоима ISO-OSI референтног модела. Финални резултат истраживања биће хибридни модел архитектуре адаптивних пословних система, са људима и IoT интелигентним уређајима као корисницима, где је адаптивност заснована на софтверској редифиницији целокупне информационо-комуникационе инфраструктуре.

Очекивани главни научни доприноси овог рада су:

- Формални опис приступа пројектовању архитектуре променљивих IoT система заснован на архитектури нултог поверења
- Идентификација патерни пројектовања безбедних IoT мрежа са променљивом топологијом.
- Унапређени модел архитектуре нултог поверења са могућношћу флексибилног сегментирања мреже.
- Модел за минимизирање безбедносног ризика од губитака мрежних елемената по ободу система услед напада и прилагођавање система функционалним захтевима после губитака.

- Хибридни модел архитектуре адаптивних пословних система, заснован на софтверској редифиницији информационо-комуникационе инфраструктуре.
- Анализа оправданост примене развијеног модела, узимајући у обзир техничке проблеме у интеграцији инфраструктуре, продуктивност, квалитет искуства корисника, капиталне инвестиције, цену одржавања и етичку димензију.

Рад на овој дисертацији резултоваће и низом стручних доприноса од којих су могу издвојити:

- Анализа динамике промене IoT мрежа.
- Преглед постојећих методологија развоја IoT мрежа.
- Компаративна анализа архитектура IoT мрежа коришћених у пракси са фокусом на безбедност.
- Идентификација софтвера и алгоритама за управљање променама у IoT мрежама.
- Преглед и анализа постојећих хардверских и софтверских решења за адаптацију архитектуре IoT мрежа.
- Симулација IoT мрежа заснована на новом алгоритму за реконфигурацију хибридних мрежа са могућношћу *ad hoc* умрежавања по ободу бежичне мреже.
- Дефиниција и тестирање алгоритма оптималне трансформације топологија мреже по ободу.

Са становишта друштвене корисности докторске дисертације, може се установити следеће:

- Од резултата истраживања се очекује да минимизирају и уклоне ограничења конективности. Један од циљева истраживања је приближавање идеје о мрежи као сервису и реалности имплементације као *cloud* сервиса (енг. *Network as a Service* или *NaaS*).
- Резултати истраживања треба да обезбеде континуално одржавање исплативости уложених средстава у IoT мреже и системе.
- Резултати истраживања ће допринети бољем и бржем развоју IoT мрежне инфраструктуре. Посредно ће довести до побољшања пословања и бржег прилагођавања предузећа захтевима корисника.
- Резултати истраживања допринеће оптимизацији коришћења хардверске инфраструктуре у предузећима, максимизирању безбедности система и приватности корисника.

6. План истраживања и структура рада

План истраживања докторске дисертације приказан је у следећој табели:

	ФАЗА	ЗАДАТАК	МЕТОДЕ, ТЕХНИКЕ, СТАНДАРДИ
1.	Анализа литературе и досадашњих резултата истраживања	- Прикупљање информација у циљу анализе постојећег стања и досадашњих резултата у реализацији адаптивних архитектура IoT применом <i>ad hoc</i> топологија.	- Претраживање база података - Претраживање научне и стручне литературе, и релевантних стандарда - Претраживање ресурса на вебу - Студије случаја примене трансформација IoT топологија.
2.	Предлог модела	- Систематизација и анализа постојећих метода и добрих пракси које дају решења за пројектовање адаптивних архитектура IoT рачунарских мрежа и система.	- Претраживање база података - Претраживање научне и стручне литературе - Претраживање Интернет ресурса - Посета стручним конференцијама на тему IoT безбедности.

		- Моделирање и идентификација патерна пројектовања који воде ка адаптивним решењима.	- Студије практичних случајева и решења које индустријски лидери нуде. - Интервју са стручњацима из релевантних области.
3.	Развој модела	- Анализа постојећих модела - Развој метода за пројектовање архитектуре на највишем нивоу апстракције - Идентификација кључних компоненти архитектуре која је потребно контролисати	- Анализа постојећих протокола и њихова употреба у слојевитим архитектурама модерних мрежних решења класификацијом безбедносних ризика и одбрамбених решења. - Примена системске анализе и пројектовања архитектуре комплексних система. - Симулације коришћењем пакета <i>PacketTracer</i>, <i>Mininet</i>, и <i>Emulab</i>. - Примена <i>big data</i> и предиктивне аналитике за адаптивно реконфигурање мрежа.
4.	Пројектовање решења	- Планирање - Идентификација дистрибуираних стања мреже - Идентификација основних елемената архитектуре - Проналажење алгорита за ефикасну идентификацију кључних стања - Пројектовање IoT система - Софтверска симулација основних елемената. - Имплементација - Унапређење	- Аналитичко-дедуктивна метода. - Комбинација симулационих метода са физичким прототипом и мерење перформанси. - Предиктивна анализа и обрада великих количина података. - Стандардне статистичке методе - Стандардне методе машинског учења - Апстракција и виртуализација - Анализа комплексности и хијерархијска редукција комплексности.
5.	Постављање хардверско софтверске инфраструктуре прототипа	- Дизајн структуре - Упрошћење модела архитектуре кроз апстрактно моделирање и виртуализацију - Апстракција спецификација - Апстракција прослеђивања саобраћаја - Апстракција топологије - Дистрибуција - Прослеђивање - Конфигурација	- Хардверске методе пројектовања мрежног слоја за управљање протоком података. - Методе конфигурације фирмвера и софтвера уређаја. - Методе софтверске контроле мрежа изван концепта конфигурације.
6.	Примена модела за пројектовање комплексних архитектура.	- Тестирање и имплементација развијене методологије и модела - Симулација решења са променљивим оптерећењима. - Имплементација прототипа и мерења на протипу. - Анализа резултата примене предложеног метода пројектовања и идентификација корективних мера.	- Методе анализе функционалних захтева и једноставности превода захтева у елементе архитектуре. - Методе анализе безбедносних захтева нултог поверења и њихова примена у дизајну архитектуре. - Математичке методе анализе карактеристика мрежног саобраћаја - Методе пројектовања апликационих интерфејса са опремом и контролним софтвером - Програмирање контролних функција - Верификација и валидација
7.	Закључак	- Анализа предложеног решења - Предлог будућег истраживања	- Анализа - Синтеза - Примери

ФАЗА	МЕСЕЦ											
	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
1												
2												
3												
4												
5												
6												
7												

Оквирно, структуру докторске дисертације сачињавала би следећа поглавља:

1. Увод

- Дефинисање предмета истраживања
- Циљеви истраживања
- Полазне хипотезе
- Методологија истраживања
- Структура и организација рада

2. IoT мреже

- IoT мрежне архитектуре
- IoT протоколи
- *Ad hoc* бежично умрежавање
- Софтверски дефинисане IoT мреже

3. Архитектура нултог поверења

- Класични прилаз комплексним архитектурама информационих система предузећа
- Преглед развоја актуелних ИКТ решења у рачунарским IoT мрежама са променљивим топологијама
- Безбедносни захтеви нултог поверења и карактеризација перформанси
- Архитектура нултог поверења и виртуелизација мрежних функција

4. Развој модела

- Анализа постојећих модела
- Функционални захтеви и дефиниција перформанси
- Пројектовање елемената архитектуре
- Развој алгоритама за оптимално тополошко реорганизовање IoT мреже
- Симулације елемената архитектуре
- Квантификација оптималне функционалности и безбедне робусности

5. Примена и евалуација развијеног система

- Пројектни захтеви
- Пројектовање и имплементација решења
- Тестирање и мерења на физичком прототипу
- Евалуација развијеног решења
- Анализа постигнутих резултата

6. Научни и стручни доприноси

7. Закључак и будућа истраживања

8. Прилози

9. Литература

7. Закључак и предлог

Из изложеног се може закључити да кандидат Људмила Жарова испуњава све услове предвиђене Законом о високом образовању за одобрење израде докторске дисертације под насловом „Развој безбедних IoT мрежа заснован на архитектури нултог поверења“.

Кандидаткиња поседује неопходна знања из интернет технологија, рачунарских мрежа и информатике за успешан рад на докторској дисертацији.

Тема припада ужој научној области Електронско пословање, мултидисциплинарна је и актуелна. Добијени резултати допринеће унапређењу постојећих пракси у области пројектовања бежичних IoT мрежа.

На основу свега наведеног, комисија предлаже Наставно-научном већу да прихвати предложену тему и одобри израду пријављене докторске дисертације. За ментора докторске дисертације предлаже се др Божидар Раденковић, редовни професор Факултета организационих наука, Универзитета у Београду.

ЧЛАНОВИ КОМИСИЈЕ:

Београд, 26.09.2018.

др Божидар Раденковић, редовни професор
Факултета организационих наука,
Универзитета у Београду

др Душан Савић, доцент
Факултета организационих наука,
Универзитета у Београду

др Ненад Стефановић, ванредни професор
Природно математичког факултета,
Универзитета у Крагујевцу