Elektrotehnički Fakultet

UCG
Univerzitet Crne Gore

Faculty of Electrical Engineering (FEE) of the University of Montenegro (UoM) was established in 1961. It now employs 35 teachers (professors, associate professors, and assistant professors) and 25 teaching and research assistants. Approximately 70% of teaching staff has experience in teaching and research activities abroad, mainly in the EU countries and the USA. FEE has three departments: Department of Power Systems and Automatic Control; Department of Electronics, Communications and Computer Engineering; and Applied Computer Engineering. Within these departments, when research activities are concerned, the staff is organized in the total of 9 research centers and laboratories, most successful being Centre for Telecommunications, Laboratory for Digital Signal Processing, and Laboratory for Multimedia. The research output of the FEE in the last five years has been about 300 scientific papers, 100 in the leading world journals and 200 at the international conferences. Two full professors are associate editors in the world's leading IEEE journals while one is editor of the Elsevier journal. Additionally, our professors are authors of several books published by respective international publishers such as Springer, Kluwer, etc. They are also regular members of the editorial, technical and scientific committees of international conferences such as IEEE ICASSP, Eurasip, as well as regional events such as Telfor, Information Technologies: Present and the Future, etc.

Although the cybersecurity topic does not have a separate department at the FEE, research activities in this area are being conducted in the framework of the first CoE in Montenegro - **Centre of Excellence in Bioinformatics BIO-ICT** (www.bio-ict.ac.me).

Topics of our research in the area of security

FEE has not yet implemented projects in the cybersecurity area, but has included this topic in the ongoing research with regard to **Software-Defined Networking (SDN)**. FEE researchers have rich experience in development of SDN control applications for both wired and wireless networks. Respectable results have been accomplished in the area of traffic engineering applications which are able to meet diverse quality of service goals (e.g. bandwidth and delay requirements, failure recovery, etc.) Within the BIO-ICT project, which deals with implementation of Internet of Things (IoT) systems for smart agriculture and water/sea ecosystem monitoring, we have implemented **WSN (Wireless Sensor Network) testbed consisted of sensor nodes with SDN capability.** Our use-cases of interest for cybersecurity research are **IoT and DC networks**, which are i.a. fundamental and indispensable parts of BIO-ICT research infrastructure. In both use-cases, we take advantage of SDNs centralized control plane, and its global view of a given network, to mitigate the challenges and limitations associated with traditional cybersecurity models. The conventional systems are usually protected only from outside threads with IDS (Intrusion Detection System) devices, like security instrument at the Internet edge. However, IDSs are not sufficient for borderless networked systems, such as IoT environments, which are prone to "inside" attacks and therefore require extra threat protection. SDN can help IoT withstand many security attacks better, because SDN can provide visibility of all the traffic in the network, which makes it easier to detect any suspicious traffic. In addition, SDN controller can detect devices as they are added to the network, and can program the network to react differently depending on the nature of the device, its potential for maliciousness, and the traffic patterns. If a device becomes compromised with a malware, SDN controller can automatically begin security threat remediation process. Therefore, instead of having one firewall or IDS at the edge of the network, we can use SDN to perform network-wide anomaly detection and create series of virtual firewalls at different network locations in order to respond to various attacks.

An important aspect of our research focus is **Fog computing**. Using the Fog computing helps in analyzing and processing the data at the network edge, close to the IoT devices that generate and act on that data. This provides new opportunities to detect unusual behavior and spot malicious attacks in IoT environments. The 'fog' layer is of particular importance for initiatives such as "Industrie 4.0", where real-time data exchange and processing are required. Moreover, here, availability is a key concern, because any unnecessary delay in production results in loss of productivity and loss of revenues. This calls for increased protection against denial-of-service attacks.

Since IoT environments are increasingly taking a cloud-based approach, we consider **the security of DC networks** as well. In these high-speed environments, due to a large amount of transmitted data, the security model which involves accurate analysis of traffic (Deep Packet Inspection) is not possible. The requirement for flow-based analysis exposes SDN as a logical technology candidate for DC networks. Beside the classic security solutions, SDN controller offers a powerful monitoring mechanism for anomaly detection. The parameters and statistics, extracted from the fine-grained SDN/OpenFlow flow tables create tuples of features that could be used for traffic classification by using anomaly detection mechanisms. This allows identifying specific connections representing different network activities. Our researchers with experience in machine learning would be involved in the development of appropriate machine learning classification (neural networks, support vector machines) techniques, which will enable proper identification of particular types of malicious traffic. Based on the output of machine learning algorithms, security rules for SDN controller can be provided in order to identify unusual traffic on the network and shut down these connections as they occur, or to identify when the endpoint itself exhibits odd behavior. Because the fog is an extension of the cloud at the network edge, it would be possible to reuse developed detection systems in the fog platform. Development of new, advanced anomaly detection techniques is strongly required in **industrial IoT (manufacturing, energy, finance & insurance, agri-food), smart city and eHealth** sectors.

BIO-ICT DC stores a huge amount of data every day, coming either from diverse sensor nodes connected to **LiveGate cloud platform** (http://livegate.ac.me) or users of our commercial and research cloud services. In such systems, real-time anomaly detection, implementation of "warning" alerts and appropriate remediation policies are necessary. Selection of appropriate anomaly detection technique is an important issue and requires realistic testing environment. The LiveGate platform might serve for this purpose since it allows sensor nodes to connect via simple API. This API could be used to simulate virtual sensor nodes, generating a large amount of legitimate and/or corrupted data. However, in order to better understand network weaknesses, analyze cyber threats and make faster and accurate decision-making, it is often necessary to analyze relations between devices, events, location, IP addresses, users. Development of web solutions which can visualize the connections between different anomaly data (malware, vulnerabilities, etc.) and IP addresses, browser, country, etc., is also something essential in modern DC centers. Our researchers with experience in programming (PHP, Java, R, Python) and network administration could deal with the mentioned task.

Call-specific expertise

FEE is interested in joining a consortium for the H2020 call DS-07-2017 **"Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors" (Research and Innovation Action).** We can contribute with the expertise in the area of SDN, machine learning and software development. More specifically, we can develop SDN applications for flow-level anomaly detection based on the collected statistics regarding the normal network behavior. This would include work on: i) applications for network monitoring and clustering flow-level statistics based on the different packet header fields; ii) machine learning algorithms for predicting and identifying the threat of the malicious attack; iii) traffic control applications for directing the suspicious traffic towards the DPI (Deep Packet Inspection) devices; iv) feedback between the packet-level anomaly detection performed on DPI devices, and machine learning algorithm for flow-level anomaly detection on the SDN controller; v) visualization tools for different anomaly data. Also, for the purpose of creating a realistic testing environment, we are willing to put our LiveGate IoT platform and Data Center resources at the disposal of potential partners.

Projects implemented so far

As a project coordinator, the Faculty of Electrical Engineering participates/d in two projects presented below:

Project Title	Centre of Excellence in Bioinformatics BIO-ICT
Overview	BIO-ICT is established in 2014 with the aim of boosting the application and the use of latest ICT technologies in the areas of sustainable agriculture, monitoring of the crops, forest and water/sea ecosystem, development of techniques for controlling and reducing air pollution, analysis and standardization of food products, control of land quality, and improvement in the public health area.
Project Coordinator	Faculty of Electrical Engineering (FEE), Montenegro
Project Partners	Montenegrin research institutions: Biotechnical Faculty, Institute of Public Health, Institute of Marine Biology Montenegrin business community: Green House Jovović, COGImar EU Partner: Centre for TeleInFrastrukture, Denmark
Financing	HERIC project/World Bank loan
Website	www.bio-ict.ac.me

Project Title	ForeMont project
Overview	Fore-Mont aims at strengthening the UoM (FEE)'s excellence by improving its research infrastructure, human resources fostering and long-term partnerships. The project will create a strong synergy in research from the three current UoM (FEE) research groups working in the field of ICT. Through Fore-Mont, these groups will merge to provide a research centre dedicated to the innovative research in info-communication infrastructures and e-services engineering: Research Centre for Info-Communication Technologies.
Project Coordinator	Faculty of Electrical Engineering (FEE), Montenegro
Project Partners	Centre for TeleInFrastruktur, Denmark; Institut Jožef Stefan, Department of Communication Systems, Slovenia; iMinds, Belgium; Ericsson Nikola Tesla, Croatia; CEA-Laboratory for Electronics and Information Technology, France
Financing	European Union 7th Framework Programme (FP7 2007-2013)
Website	www.foremont.ac.me

As a project partner, the Faculty of Electrical Engineering participates/d in the projects listed below:

- VI-SEEM - Virtual Research Environment in Southeast Europe and the Eastern Mediterranean, funded under H2020, https://vi-seem.eu
- Low EMF Exposure Future Networks LEXNET, funded under European Union 7th Framework Programme (FP7 2007-2013), http://www.lexnet-project.eu
- eWall for Active Long Living, funded under European Union 7th Framework Programme (FP7 2007-2013), http://ewallproject.eu
- BalkanGEONet project, funded under European Union 7th Framework Programme (FP7 2007-2013), http://cordis.europa.eu/project/rcn/97148_en.html

Additionally, Center of Information System of the University of Montenegro and prof. Božo Krstajić are partners within the H2020 GÉANT Project (GN4-2), https://www.geant.org/Projects/GEANT_Project_GN4

Key persons who will be involved in the project

Prof. Igor Radusinović, PhD

Full Professor at the Faculty of Electrical Engineering, University of Montenegro. His research interests are mainly in telecommunications network protocols and systems design. His current research topics are future internet packet switch architectures, quality of service congestion control mechanisms in wired/wireless networks and in wireless networks. In these areas, he has published more than 100 referred publications in peer-review international journals and international proceedings. He is a member of several professional bodies and scientific boards and has wide experience related to international projects, including several FP7 projects. Professor Radusinović is a Director of BIO-ICT CoE.

Prof. Božo Krstajić, PhD

Full Professor at the Faculty of Electrical Engineering, University of Montenegro. His research interests are mainly in adaptive signal processing, internet technologies and distributed systems. In these areas, he has published more than 100 publications in international/national journals and international/national proceedings. He is a member of IEEE and chair of the biggest national ICT conference. Professor Krstajić has wide experience related to international projects, including several FP6, FP7 and H2020 projects, as well as TEMPUS and IPA projects and BIO-ICT CoE.

Assoc. Prof. Slobodan Đukanović, PhD

Associate Professor at the Faculty of Electrical Engineering, University of Montenegro who currently holds a position of Scientific Director at BIO-ICT Centre of Excellence. He was a team member of several FP7 projects. His research concerns time-frequency signal analysis, signal filtering, parameter estimation and pattern recognition. Full reference list can be found at www.tfsa.ac.me/slobodan_papers.html.

Assist. Prof. Žarko Zečević, PhD

Assistant Professor at the Faculty of Electrical Engineering, University of Montenegro, where he also received PhD degree. His research interests are mainly in adaptive control and adaptive signal processing, control systems and distributed algorithms. In these areas, he has published more than 30 publications in international/national journals and international/national proceedings. He is a member of IEEE. He has experience related to international projects (H2020, IPA). Professor Zečević is a team-member of BIO-ICT CoE.

Slavica Tomović, PhD student

Slavica Tomović received MSc degree in Telecommunications from Faculty of Electrical Engineering in Podgorica, University of Montenegro (2015). Currently, Slavica is a PhD student at the Faculty of Electrical Engineering, University of Montenegro and a Teaching Assistant at the same faculty. Her main research interests are in the areas of software-defined networking, quality of service (QoS) management and architectures, Internet of things (IoT) and 5G wireless network design. She was a team member of ForeMont FP7 project and is now engaged at BIO-ICT CoE.

Publications in the cybersecurity area with FEE authors:

1. Tomovic S., Pejanovic-Djurisic M., Radusinovic I., "SDN BASED MOBILE NETWORKS: CONCEPTS AND BENEFITS", Wireless Personal Communications 78(3), 2014, pp. 1629-1644.
2. Tomovic S., Prasad N., Radusinovic I., "SDN Control Framework for QoS Provisioning", Proc. of 22nd Telecommunication Forum TELFOR 2014, pp. 111-114, Belgrade, Serbia, November 2014.
3. Tomovic S., Radonjic M., Radusinovic I., "Bandwidth-Delay Constrained Routing Algorithms for Backbone SDN Networks", Proc. of TELSIKS 2015, pp. 227-230, Nis, Serbia, October 2015.
4. Tomovic S., Radusinovic I., "Fast and Efficient Bandwidth-delay Constrained Routing Algorithm for SDN Networks", IEEE NetSoft Conference, pp. 303-311, Seoul, South Korea, June 2016.
5. Tomovic S., Radusinovic I., "Energy Efficient Target Coverage in Partially Deployed Software Defined Wireless Sensor Network", Cognitive Radio Oriented Wireless Networks, Lecture Notes

of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 172, pp.729-740, June 2016.

6. Tomovic, S., Yoshigoe, K., Maljevic, I. & Radusinovic, I., "Software-Defined Fog Network Architecture for IoT", Wireless Personal Communications (2016), pp. 1-16, ISSN: 0929-6212, DOI:10.1007/s11277-016-3845-0.
7. Gardasevic, G., Veletic, M., Maletic, N., Vasiljevic, D., Radusinovic, I., Tomovic, S. & Radonjic, M., "The IoT Architectural Framework, Design Issues and Application Domains", Wireless Personal Communications, pp.1-22, Oct. 2016, ISSN: 0929-6212 (print version), ISSN: 1572-834X (Online). DOI: 10.1007/s11277-016-3842-3.
8. M. Bajčeta, P. Sekulić, S. Djukanović, T. Popović, and V. Popović-Bugarin, "Retinal blood vessels segmentation using ant colony optimization," 2016 13th Symposium on Neural Networks and Applications (NEUREL) , Belgrade, November 22-24, 2016.
9. M. Brajović, V. Popović-Bugarin, I. Djurović, and S. Djukanović, "Post-processing of Time-Frequency Representations in Instantaneous Frequency Estimation Based on Ant Colony Optimization," Signal Processing, Vol. 138, September 2017, pp. 195–210, http://dx.doi.org/10.1016/j.sigpro.2017.03.022.

Relevant infrastructure and laboratory equipment include SDN Testbed, SDN Wireless Sensor Network, and BIO-ICT Data Center.

Our OpenFlow testbed is composed of Pica8 and HP Procurve 6600 switches, six NetFPGA 1G and 10G boards, three NetFPGA cubes, four Workstations (2x Intel Xeon 6-core 2.5 GHz processor, 16 GB RAM each) and 12 PCs (Intel Core i7 processor at 3.5 GHz, 8GB RAM). To implement SDN data-plane we have used software and hardware solutions of OpenFlow switches. Software solutions, based on OpenvSwitch software, are installed on the workstations and PCs in the testbed. Hardware solutions of OpenFlow-enabled devices include NetFPGA boards (including those in the cubes), HP Procurve 6600 and Pica8 switches. NetFPGA boards are hardware platforms designed for networking research. Thus, their purpose in the testbed is dual - they could be used to develop advanced SDN devices, or they can serve as OpenFlow switches which are capable of running at line-rate. Pre-assembled NetFPGA computer systems, so-called cubes, are used to provide a greater level of network interconnectivity or generate traffic flows in the experiments. Important parts of the testbed are Pica8 and HP Procurve switches. These high-performance commercial network switches possess Layer 2 and Layer 3 switching capabilities and offer most complete OpenFlow standard support. With appropriate configuration, their ports could be grouped to virtually form multiple instances of OpenFlow switches. Thus, Pica8 and HP Procurve actually introduce a full network of OpenFlow switches to the testbed. HP Procurve has 24 1Gpbs interfaces and 4 SFP+ optical transceivers. Pica8 is equipped with 48 1Gbps ports and 4 SFP+ optical transceivers. The same optical transceivers are part of NetFPGA-10G programmable boards.

The Internet of Things testbed includes 10 Texas Instruments cc2530 boards and 10 OpenMote cc2538 board. Each OpenMote node integrates temperature/humidity sensor, light sensor, and 3-axis accelerometer.

BIO-ICT Data Center includes three servers, each with 2x6 CPUs (2.893 GHz) and 128 GB RAM, one server with 4x6 CPUs (2.6 GHz) and 120GB RAM, and 10TB of storage.

Montenegrin political context

Considering the EU's adherence towards encouraging international cooperation as stipulated under the Strategy for EU International Cooperation in Research and Innovation (COM(2012)497), broadening the geographical coverage of the project may prove favorable for ensuring its successful implementation. As the newest NATO member, Montenegro became a part of an organized system of collective defense and has pledged to improve its cyber incident prevention, resilience and response capabilities, as well as marked cybersecurity as the top priority issue. Montenegro ranked 70th among 165 countries in the Global Cybersecurity Index 2017 report by the UN International Telecommunication Union (ITU) and was grouped in the "maturing" stage. This group refers to 77 countries which have developed complex commitments and engage in cybersecurity programmes and initiatives.

Contact us:
Faculty of Electrical Engineering
Džordža Vašingtona Boulevard
81000 Podgorica
Montenegro
www.ucg.ac.me/etf
www.bio-ict.ac.me
bio-ict@ac.me