University POLITEHNICA of Bucharest
Faculty of Automatic Control and Computers

Splaiul Independenței nr.313, sector 6, cod 060042,
Bucharest, ROMANIA

conf. Dragoș Ș. Niculescu
PhD coordination in “Computers and Information Technology”
Doctoral School of Automatic Control and Computers,
University POLITEHNICA of Bucharest

Contact:
University Politehnica of Bucharest
School of Control and Computers
Computer Science and Engineering Departament
Splaiul Independentei, 313, sala Precios 203, sector 6, 060042,
Bucharest Romania

E-mail: dragos.niculescu at upb.ro
Web: http://wi-fi.cs.pub.ro/~dniculescu
LinkedIn: https://ro.linkedin.com/in/niculescu

Research profile:

- computer networks, wireless networks, internet, 5G
- communication protocols
- wireless networks, ad hoc networks, sensor networks
- pervasive computing, internet of things

PhD coordinator since 2013 – Electrical Engineering (Electronică), 2015 – Computer Science

- 3 ongoing theses

Publications:

- 3 books, chapters
- 25 papers
- 5 US patent applications, 1 OSIM patent application

Research project

Year	**Acronym**	**Role**	**Title**	**Program**
2009-2011	RP4-2008	director	Algorithmic Methods for Interference Mitigation in 802.11 Networks	PN II
2008-2012	SMART-NET	consultant	SMART-antenna multimode wireless mesh Network	FP7
2010-2013	ALICANTE	consultant	Media Ecosystem Deployment Through Ubiquitous Content-Aware Network Environments	FP7
2011-2014	TRILOGY2	consultant	Building the Liquid Net	FP7
2012-2015	MOBIL4	consultant	ENABLING MOBILITY WITH MULTIPATH TCP	PNII
2015-2017	SUPER - FLUIDITY	consultant	Superfluidity: a super-fluid, cloud-native, converged edge system	H2020
2017-2018	4.5G	director	4.5G service based on MPTCP	PN III

Research proposals:

- **Air documents.** Virtual management of physical indoor space can be done without a positioning teechology (such aș GPS), but only with radio signatures. Associating documents with locations is a widespread technology outdoors, but finding exact location indoors is still a challenge. The aim of the project is to develop a system to associate documents not with actual position în the building, but with the rich wireless signature that is generated în todays saturated radio homes and offices.

- **Guaranted latency în 5G.** Part of migration towards 5G architectures targets virtualization of all support services în current 4G networks LTE, LTE-A. În 5G one of the requirements is guaranteeing a low RTT(round trip delay) as low as 1ms, to allow for implementatuion of a tactile Internet (remote use of hand driven machinery). These requirements need redesign of the entire technology stack that comprises a mobile network în order to minimize delay at all layers: from the operating system (with realtime features) to the protocols employed, which also need redesigning for high speed and low delay.

- **virtualization of MAC and PHY în 5G**. Part of migration towards 5G architectures targets virtualization of all support services în current 4G networks LTE, LTE-A. On the other hand, availability of SDR(Software Defined Radio) devices at the edge of the network allows for replacing of low level protocols. These trends (network virtualization and SDR) allow for virtualization of the entire communication system: from internal server hardware to the devices associated with the access network(base stations, enodeB, WiFi Aps), from the communication stack to the end to end protocols.

- **management of dense IoT networks**. Growing number of personal devices is already a problem, even before the imminent coming of IOT. A challenge both for domestic users and for institutions is the high cost of managing the large population of heterogenous devices. This cost is usually în highly specialized manpower needed for the interconnection, management and security of all networked devices – either wireless (Bluetooth, WiFi, NFC, Zigbee), or networked by other methods (PLC, SCADA, home automation, building sensors).

- **mobile application fingerprinting.** A typical home environment includes many personal devices permanent or temporary/visiting. They usually host an ecosystem of applications whose security is difficult to diagnose and monitor because of the sheer quantity, diversity, and continuous upgrading. The device owner is not usually the same aş the network administrator, and neither of them is specialized în the behavior of the Apple/Android mobile device, or the management of a local WiFi/Ethernet network. We wish to create a service to automatically identify applications present în a network so that to implement an application firewall that can be easily controlled by nonspecialized users. Applications are identified based on the traffic they generate: the Internet destinations contacted, patterns and conversation recognized, or some othetr local probing methods.