MFÉs 2016-2017

OPERA – Wireless Communications
Ecole polytechnique de Bruxelles

Les thèmes proposés s’intègrent dans la palette des activités de recherche développées par le groupe Wireless Communications du Service OPERA.
User terminal positioning in 5G wireless networks

Information: François Horlin, Philippe De Doncker, Jean-Michel Dricot
Students: ELEC, PHYS
Type: Theoretical and/or experimental
Collaboration: Proximus, IMEC - can be combined with an internship

MOTIVATION

Cellular networks have continuously evolved to become one of the main blocks of our ICT all-pervasive world. The first 2G systems, like GSM, were dedicated to voice communications. Data communications with low-to-medium bit rates were included in 3G, while 4G now offers data rates similar to those experienced with Wi-Fi. But the demand for high performance cellular networks is still increasing, due on the one hand to the explosion of the number and variety of connected devices, and on the other hand to the ever-growing capacity requirements. 5G cellular networks are developed to meet this evolution. Especially new modulation formats characterized by a better spectrum confinement than the orthogonal frequency-division multiplexing (OFDM) modulation used today in 4G are considered to better cope with the multiple access issue critical in 5G networks.

In parallel, cellular networks have also evolved towards geo-located services. The user equipments (UE) can now be localized based on their communications with the cellular base stations. In 4G, a positioning reference signal (PRS) is included in the protocol to support the device positioning based on the estimation of the signal time-of-flight (ToF) to the base stations. To make 5G localization valuable, a high accuracy is required, even in more critical indoor or urban outdoor environments, where multipath propagation strongly degrades the performance of traditional ToF-based techniques.

The objective of this work is to develop a localization system that complements the 5G communications functionality and delivers a high position accuracy even in complex environments.

OBJECTIVES

- Understand the modulation formats foreseen for emerging 5G communications systems
- Design positioning algorithms for 5G networks, taking their specificities into account (new reference signals)
- Assess the positioning accuracy/precision as a function of main system parameters (bandwidth, base station positions...)
- Address complex urban or indoor multipath environments
- Demonstrate the system real-life by using new software defined radio (SDR) electronic platforms

A team of two students, one working on the functionality and the other working on the real-life demonstration, can ideally work on the project. It is organized in close collaboration with the IMEC research center (Leuven, Belgium), considered as a major actor in the fields micro-electronics and nano-technologies and with Proximus.

CONTACT

François Horlin (fhorlin@ulb.ac.be) 02-650 6741
Philippe De Doncker (pdedonck@ulb.ac.be) 02-650 3091
Jean-Michel Dricot (jdricot@ulb.ac.be) 02-650 3883
Solbosch campus, building U, level. 3, OPERA department
**Wireless positioning for the Internet-of-Things**

Information: Philippe De Doncker, François Horlin, Jean-Michel Dricot  
Students: ELEC, PHYS  
Type: Theoretical and/or experimental  
Collaboration: Proximus, Université Paris VI - can be combined with an internship

**MOTIVATION**

The Internet of Things (IoT) is currently being deployed by all major network providers, worldwide. In Belgium, for instance, Proximus is implementing the Lora IoT technology to complement its 4G network. The ultimate goal of the IoT is to connect billion of devices wirelessly. These devices must be located in the field in order to insure geolocated services. But their limited resources in terms of bandwidth and energy consumption is a major bottleneck that must be overcome for accurate positioning.

The objective of this work is to develop a localization system that complements the IoT communications functionality.

**OBJECTIVES**

- Understand the physical layer of IoT communications, e.g. Lora technology  
- Design positioning algorithms for IoT, taking their specificities into account: limited resources in terms of bandwidth and energy consumption  
- Develop polynomial-chaos based algorithms to assess the positioning accuracy/precision as a function of main system parameters (bandwidth, base station positions...)  
- Demonstrate the system real-life by using new software defined radio (SDR) electronic platforms

A team of two students, one working on the functionality and the other working on the real-life demonstration, can ideally work on the project. The Lora technology will be addressed with the help of Proximus. The work is organized in close collaboration with Université Paris VI where an internship can be done.

**CONTACT**

Philippe De Doncker (pdedonck@ulb.ac.be) 02-650 3091  
François Horlin (fhorlin@ulb.ac.be) 02-650 6741  
Jean-Michel Dricot (jdricot@ulb.ac.be) 02-650 3883  
Solbosch campus, building U, level. 3, OPERA department
Massive MIMO for 5G wireless networks

Information: François Horlin, Philippe De Doncker, Jean-Michel Dricot
Students: ELEC, PHYS
Type: Theoretical and/or experimental
Collaboration: IMEC - can be combined with an internship

MOTIVATION

*MIMO, Multiple-Input Multiple Output,* technology relies on multiple antennas to simultaneously transmit multiple streams of data in wireless communication systems. It has been successfully integrated in a series of well-established communication systems, such as the LTE-A fourth generation (4G) cellular system and IEEE 802.11n wireless LAN system. It is also considered as a promising key technology for future wireless systems of the fifth generation (5G). Unlike the traditional small-scale MIMO (e.g., at most 8 antennas in LTE-A), large-scale MIMO, which equips a very large number of antennas (e.g., 64 antennas or even more) at the base station (BS) to simultaneously serve multiple users, is proposed. It has been theoretically proved that large-scale MIMO can achieve orders of simultaneous increase in spectrum and energy efficiency.

Massive-MIMO system exploits channel state information (CSI) in order to precode (in downlink) or decode (in uplink) the user data. The CSI is obtained from uplink pilots sent by the users. It has been shown that, for massive MIMO systems, low complexity linear precoding and detection can achieve performance very close to the channel capacity for the downlink and uplink respectively. When the signal is precoded or decoded with large number of antennas, energy is focused with extreme sharpness into small regions in space. The underlying physics is coherent superposition of wavefronts. By appropriately shaping the signals sent out by the antennas, the base station can make sure that all wave fronts collectively emitted by all antennas add up constructively at the locations of the intended terminals, but destructively (randomly) almost everywhere else.

The objective of this work is to assess and demonstrate the spatial focalization property obtained thanks to the massive MIMO technology.

OBJECTIVES

- Design massive-MIMO precoders/decoders compatible with 5G modulation formats
- Demonstrate the power focalisation property by using simplified channel models of the environment (ideal channel, ray tracing)
- Investigate the impact of system impairments (channel estimation error, hardware imperfections...)
- Design strategies to interpolate the precoder over the space and follow therefore the terminal trajectory
- Demonstrate a time-reversal implementation of the massive-MIMO technology real-life by using new software defined radio (SDR) electronic platforms

A team of two students, one working on the functionality and the other working on the real-life demonstration, can ideally work on the project. It is organized in close collaboration with the IMEC research center (Leuven, Belgium), considered as a major actor in the fields micro-electronics and nano-technologies.

CONTACT

François Horlin (fhorlin@ulb.ac.be) 02-650 6741
Philippe De Doncker (pdedonck@ulb.ac.be) 02-650 3091
Jean-Michel Dricot (jdricot@ulb.ac.be) 02-650 3883
Solbosch campus, building U, level. 3, OPERA department
5G Location-Enhanced Communications

Information: Philippe De Doncker, François Horlin, Jean-Michel Dricot
Students: ELEC, PHYS
Type: Experimental and Theoretical

MOTIVATION

5G networks are foreseen to allow very fine positioning of the users. This functionality is useful to offer geolocated services, but it will also pave the way to Location-Enhanced Communications: communication strategy will be optimized in real-time by knowing the user position, and so, his « radio environment » (in terms of channel characteristics). Information on the radio environment will be deduced from existing databases built on-line while the users are connected to the network.

The objective of this work is to develop radio environment databases by using geostatistics: the channel parameters are considered as geolocated random functions that can be modeled by techniques used in environmental sciences to model physical agents (pollution, weather parameters,..). A real-life implementation will be carried out on Software-Defined Radios.

OBJECTIVES

- Understand the physical layer foreseen for 5G communications
- Implement radio environment analysis codes on software-defined radios
- Analyze the radio environment parameters in terms of geostatistics
- Develop geostatistical algorithms to build radio environments databases.

A team of two students, one working on the functionality and the other working on the real-life demonstration, can ideally work on the project.

CONTACT

Philippe De Doncker (pdedonck@ulb.ac.be) 02-650 3091
François Horlin (fhorlin@ulb.ac.be) 02-650 6741
Jean-Michel Dricot (jdricot@ulb.ac.be) 02-650 3883
Solbosch campus, building U, level. 3, OPERA department
Networking protocols for 5G ultra-dense networks

Information: Jean-Michel Dricot, François Horlin, Philippe De Doncker,
Students: ELEC / INFO
Type: Theoretical and experimental

MOTIVATION

5G will provide an order of magnitude improvement in performance in the areas of more capacity, lower latency, more mobility, more accuracy of terminal location, increased reliability and availability. In order to meet the expected high throughput targets, small cells (a few tens of meters) will be pushed further leading to Ultra Dense Networks (UDN), hence triggering the need for an efficient and reliable core network.

It is anticipated that 5G will significantly be driven by software. Network functions are expected to run over a unified architecture, especially at the edge of the network for meeting performance targets. As a result, it will heavily rely on emerging technologies such as Software Defined Networking (SDN) to achieve the required performance, scalability and agility. SDN is a novel networking paradigm that reverses the classical, distributed networking paradigm by implementing a logical centralization of control functions (e.g., routing optimization, shortest route computations, QoS provisioning). These SDN controllers (i.e., the orchestrators of the network) are deployed in cloud technologies to scale out.

The objective of this work is to develop the SDN-based 5G core network that will deliver highly-scalable, ultra-low delay, and ultra-fast handover.

OBJECTIVES

- Understand SDN paradigms and deploy a SDN controller in a lab environment
- Implement a data-filtering technique for static and dynamic localization that receives the estimated location and derives the location and speed of the terminals
- Implement the 5G networking interfaces and protocols used for updating the localization parameters (location, speed, target cell while moving) that are used in ultra-dense networks
- Design and implement SDN logic (i.e., a controller module) dealing with the handover of mobile terminals in small cells environments.
- Demonstrate the system real-life by using the SDN switches in the lab and assess the performance of your 5G ultra-dense network

CONTACT

Jean-Michel Dricot (jdricot@ulb.ac.be) 02-650 3883
François Horlin (fhorlin@ulb.ac.be) 02-650 6741
Philippe De Doncker (pdedonck@ulb.ac.be) 02-650 3091
Solbosch campus, building U, level. 3, OPERA department
Security of Real-Time Ethernet for automotive and avionics communications

Information: Jean-Michel Dricot
Students: ELEC / INFO
Type: Theoretical and experimental

MOTIVATION

Today, Ethernet is the worldwide standard in office communication. Not only is it used to network PCs and peripheral devices within the office, but also for communications between distributed servers or for the Internet and intranets. Annual growth for the use of Ethernet-compatible devices has been in double figures for years, and this trend is forecast to continue for years to come.

If one considers Ethernet as a network in which all devices and utilities can communicate with each other via the same medium, the idea of an industrial Ethernet seems completely natural. Over the last years, Real-Time Ethernet (or AFDX in avionics) was developed to provide a deterministic real-time Ethernet for the industrial environment. Older field buses like CAN (in automotive industry) are gradually being replaced by RTE. Direct integration of a security protocol for machinery safety purposes is equally essential. This security protocol is necessary for communicating information used to protect man, machine, and the environment from hazards.

However, some concerns have emerged regarding the securitization of cars and aircraft. Over the last year only, several car models have been remotely controlled and an aircraft Ethernet bus has been exploited.

The objective of this work is to investigate the security of Ethernet for real-time, critical industrial buses with respect to the broad range of existing attacks. Next, solutions will be presented. The real-time nature of the RTE bus will be considered as well.

OBJECTIVES

- Understand how RTE works in an industrial / automotive / avionics environment
- Investigate the possible attacks at the different layers (Ethernet, IP, car-to-phone communications)
- Demonstrate one attack in the laboratory and provide a solution

CONTACT

Jean-Michel Dricot (jdricot@ulb.ac.be) 02-650 3883
Solbosch campus, building U, level. 3, OPERA department
Design and Implementation of a GSM Network Security Lab Demonstrator

Information: Jean-Michel Dricot  
Students: ELEC/INFO  
Type: Theoretical and experimental

MOTIVATION

GSM is the largest mobile network technology worldwide. It was designed around the 90’s and several issues lies in the GSM architecture and ciphering algorithm. Due to leaking of the design of encryption in the past, it could be attacked, such as sniffing the voice in an established communication, performing IMSI catching (i.e., de-anonymization), and SIM card duplication.  
More recently, in the context of all-IP networks, GSM systems are often interfaced with the IP core network, mixing protocols such as the telephony SS7 with the new Voice over IP/SIP protocols (used in Skype-like apps). Today, it is possible to intercept and even decode in real-time GSM communications with no more that a home computer and a radio front-end.  
The objective of this work is to setup a lab environment for the academic learning and assessment of GSM security. The proposed architecture will then serve as a laboratory for the students following the networking classes. Several security flaws can be investigated, ranging from the physical layer (spectrum analysis), to GSM handover procedures, authentication protocols, call signaling, VoIP protocols, etc.  
To defend a system, you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. This is why this thesis offers you to perform security investigations and ethical self-learning in an academic environment. Acting lawfully and ethically is your responsibility.

OBJECTIVES

- Study the GSM architecture and the corresponding security mechanisms.  
- Propose a network architecture suitable for demonstrating the possible attacks on the GSM in an academic environment  
- Identify the relevant attacks at each level (spectrum, air interface, authentication, communication wiretapping, etc.)  
- Implement the vector of attacks and the monitoring tools that will be used to illustrate classes material and attack-in-progress.  
- Document and implement possible solutions to counteract the GSM flaws.

CONTACT

Jean-Michel Dricot (jdricot@ulb.ac.be) 02-650 3883  
Solbosch campus, building U, level. 3, OPERA department