MFEs 2020-2021

OPERA – Wireless Communications Group

Ecole Polytechnique de Bruxelles

Distributed localisation of terminals in 5G wireless networks

Information: François Horlin, François Quitin, Evert Pocoma Copa
Students: ELEC, PHYS, INFO
Type: Theoretical

MOTIVATION

Geolocation services are of high importance in applications like surveillance, object or people tracking, crowd monitoring, etc. They have been studied for several years now, but the focus has only been on centralized localization: all the information about the signals observed at multiple base station antennas is collected and processed in a common place denoted Fusion Centre (FC) where localization algorithms are implemented. Such algorithms are based on properties of the observed signals such as: time-of-arrival (ToA) and/or angle-of-arrival (AoA). What is more, the collection of information in the FC requires a good signal representation to limit the degradation coming with the use of noisy control channels to exchange the information.

At the same time, the demand for high performance cellular networks is still increasing, on one hand due to the explosion of the number and variety of connected devices, and on the other hand to the ever-growing capacity requirements. To meet this demand, it is expected that the new 5G cellular networks will deploy a much higher number of base station antennas in the same area. This concept of dense cellular networks calls for the distributed implementation of the localisation algorithms: instead of implementing the localization centrally in the FC, it is implemented in a distributed fashion at the base stations located close to the wireless transmitter.

In that case, the localization happens closer and closer to the edge of the cellular network. All the base-stations (BS) involved in the distributed localization reach a consensus on the position of the transmitter, i.e., the user position is available at each BS. Such distributed localization involves several exchanges of "optimal-minimal" information between BS's, taking into account the network logical topology (one BS communicates only with a selected group of BS's, such as neighbouring BS's) and network physical geometry (e.g. all BS are located side by side in a straight line, as the lamppost in the streets).

The objective of this master thesis is to conceive and assess distributed localization algorithms for 5G networks. A special care will be taken to the design of efficient signal representations used to exchange information among the base stations involved in the distributed localization process.

OBJECTIVES

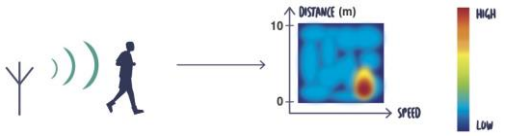
- Design distributed positioning algorithms for 5G networks
- Optimize the signal representation to support the distributed localisation
- Assess the positioning accuracy/precision as a function of the network logical topology
- Assess the positioning accuracy/precision as a function of the network physical geometry

CONTACT

François Horlin, fhorlin@ulb.ac.be, 02-650 6741
François Quitin, fquitin@ulb.ac.be, 02-650 2829
Solbosch campus, building U, level. 3, OPERA department

High Precision Passive Radars based on Wi-Fi signals for Indoor Monitoring

Information: François Horlin, Philippe De Doncker, Hasan Can Yildirim, Laurent Storrer
Students: ELEC, PHYS
Type: Theoretical and/or experimental



MOTIVATION

In order to detect and track objects in an indoor environment, one of the most widely used technology is radars. Radars usually transmit well designed signals, to build range-Doppler maps of the environment where each object is identified by its distance and speed from the radar. On the other hand, *passive radars* opportunistically capture existing communication signals to detect and track objects. Thereby they do not emit any additional signals. This reduces the complexity of the device and allows to avoid additional exposure to electromagnetic waves.

Wi-Fi, based on the IEEE 802.11 standard, is the most popular WLAN technology, i.e. a typical household consists of tens of Wi-Fi devices connected to one or more access points. The main Wi-Fi standards use the orthogonal frequency-division multiplexing (OFDM) modulation due to its ability to efficiently deal with multi-path channels which are typical for indoors wave propagation. From a passive radar point of view, Wi-Fi is an excellent opportunity for detecting/tracking objects due to its wide availability.

Until now, passive radars based on Wi-Fi signals have only been designed for the former versions of the standard (11a/g/n), which limits the range accuracy to approximately 10m. Recently, the OPERA department showed the interest of building passive radars, based on the new wide bandwidth 802.11ac/ax signals, to track objects and/or people indoors. Also, the classical methods to build range-Doppler maps are replaced by modern and novel channel estimation techniques that significantly improve the reliability and the precision of the radar.

The main objective of this master thesis is to design a passive radar based on the new 802.11ax WiFi signals to track the movements of objects (like robots) or people indoors.

OBJECTIVES

- Understanding the modulation and medium-access technologies integrated in the most recent Wi-Fi standards.
- Understanding/developing advanced parameter estimation methods to high precision range-Doppler maps.
- Gaining experience on the implementation and prototyping of radar receivers and Wi-Fi access points.

The methodology will/may include system level analysis, algorithm development, MATLAB simulations and experimental validation on hardware platforms such as USRPs.

CONTACT

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

Monitoring of crowd dynamics with passive radars

Information: François Horlin, Laurent Storrer, Hasan Can Yildirim
Students: ELEC, INFO
Type: Theoretical and/or experimental

MOTIVATION

There is a lot of interest in understanding and measuring the dynamics of crowds. A large number of applications can benefit from this information, such as the real-time management of people flow during large events, or the management of scenes of disaster.

Measuring crowd dynamics requires time-stamped position and speed information of the people. There are multiple ways to gather this information. One of them is the *passive radar* approach. Radars transmit specially designed signals, to build range-Doppler maps of the environment where each moving target is identified with a distance and speed. On the other hand, passive radars rather opportunistically capture existing communications signals to detect and track targets in the environment. Thereby they do not emit any additional signal.

Wi-Fi, based on the IEEE 802.11 standard, is the most popular WLAN technology, i.e. a typical household consists of tens of Wi-Fi devices connected to one or more access points. The main WiFi standards use the orthogonal frequency-division multiplexing (OFDM) modulation due to its ability to efficiently deal with multi-path channels. From a passive radar point of view, Wi-Fi is an excellent opportunity for detecting/tracking targets, along with estimating channel parameters for communication purposes.

The goal of this thesis is to leverage radar range-Doppler maps obtained with a Wi-Fi-based passive radar over time to monitor groups of people in a crowd, following three objectives. Firstly targets/people in the environment need to be clustered into groups based on their position and speed. For this, traditional **clustering algorithms** such as DBSCAN are currently used, but Neural Network-based clustering will be investigated. Secondly, methods to **estimate the number of people in each group** will be studied, involving Bayes classifiers, Support Vector Machines (SVM) and Neural Networks. Finally, advanced **tracking methods** such as Particle Filtering and Multiple Hypothesis Tracking (MHT) will be the explored to track the groups position and speed over time, and compared to traditional tracking methods. Those elements will first be implemented based on simulations, and then applied on measurements.

OBJECTIVES

- Develop a simulation environment to emulate crowd dynamics.
- Investigate machine learning-based clustering for radars.
- Study basic classifiers for people counting and compare their performance with more involved Neural Networks-related techniques.
- Explore advanced tracking techniques.

A strong background in mathematics (essentially in linear algebra and statistics) and in programming with mainstream high-level languages (e.g., Python and MATLAB) is desirable. Knowledge and experience with Neural Networks is a plus.

CONTACT

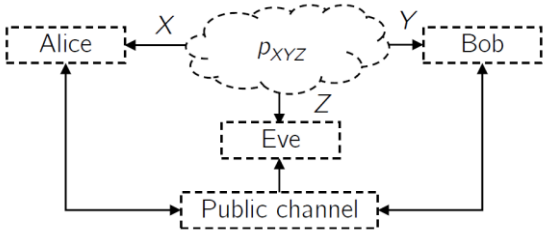
François Horlin, fhorlin@ulb.ac.be, 02-650 6741
Solbosch campus, building U, level. 3, OPERA department

Secret-key generation based on channel reciprocity

Information: Jean-Michel Dricot, Philippe De Doncker, François Rottenberg
Students: ELEC, PHYS
Type: Theoretical and/or experimental

MOTIVATION

The large majority of security techniques implemented in existing communication systems are mainly based on cryptographic primitives, which rely on mathematical problems conjectured (but not proven) to be hard to solve with limited complexity and time. However, there is currently no information-theoretic security implemented, *i.e.*, security with theoretical guarantees. This can be very limiting in view of the current technological trends (Internet of Things, quantum computing and environmental transition). This is why information-theoretic security has regained a lot of attention recently. In the source model (see, two legitimate parties (Alice and Bob) and one illegitimate party (Eve) observe the realizations of a discrete memoryless source. From their observations, Alice and Bob can generate an identical key that has to remain secret from Eve. It is possible to show that the source model is able to provide information-theoretic security, as opposed to conventional cryptographic primitives.



Source model for secret-key agreement

A practical source of common randomness at Alice and Bob consists of the wireless channel reciprocity, which implies that the propagation channel from Alice to Bob and from Bob to Alice is identical if both are measured within the same channel coherence time and at the same frequency. On the other hand, the channel at Eve is different given her different location. At each coherence time, Alice and Bob can repeatedly sample the channel by sending each other a pilot symbol to obtain a set of N highly correlated observations and finally start a key-distillation procedure.
The objective of this work is to assess and demonstrate the feasibility of secret-key generation based on channel wireless reciprocity for 5G communication systems.

OBJECTIVES

- Understand the core concepts of information-theoretic secret-key generation including quantitative security metrics (secret-key capacity, eavesdropper equivocation…).
- Study the impact of channel propagation properties on secret-key capacity and in particular, the impact of the three main dualities in channel modelling: space-angle, time-Doppler and frequency-delay.
- Design algorithms and coding schemes for closing the gap with secret-key capacity.
- Identification of key 5G scenarios for application and integration with the standards.
- Demonstration using new software defined radio (SDR) electronic platforms.

CONTACT

Jean-Michel Dricot jdricot@ulb.ac.be
Philippe De Doncker, pdedonck@ulb.ac.be
Solbosch campus, building U, level. 3, OPERA department

Secrecy-capacity optimization for 5G wireless communications

Information: François Horlin, Philippe De Doncker, François Rottenberg, Hien-Trung Nguyen
Students: ELEC, INFO, PHYS
Type: Theoretical and/or experimental

MOTIVATION

The large majority of security techniques implemented in existing communication systems are mainly based on cryptographic primitives, which rely on mathematical problems conjectured, but not proven, to be hard to solve with limited complexity and time. There is however today no information-theoretic security that would guarantee the security of the legitimate transmitter/receiver pair whatever how powerful an eavesdropper can be.

The absence of a stronger theoretical notion of security can be related to Shannon's pioneering work, which resulted in a somewhat pessimistic result regarding the practical application of information-theoretic security. Shannon showed that, to achieve the highest level of secrecy, the so-called perfect secrecy, the key used to encrypt the message and decrypt the cyphertext should be at least as long as the message itself, which leads to stringent constraints in terms of key generation, storage and exchange. This is mainly why the beautiful but rather impractical notion of information-theoretic secrecy has been discarded until now in favour of cryptographic primitives, that are much more practical but do not provide any information-theoretic guarantees.

One of the central assumptions of Shannon's model is that of an ideal channel. In practice however, all physical channels are far from ideal but subject to noise and uncertainty, which can be leveraged to circumvent Shannon's pessimistic result. The seminal work of Wyner has shown that a signal-to-noise (SNR) advantage at the legitimate receiver with respect to the eavesdropper is sufficient to guarantee a larger-than-zero secrecy capacity, implying that bits can be secretly transmitted in practice with information-theoretic guarantees.

The evolution in 5G towards the use very large bandwidths and massive numbers of antennas (massive MIMO technology) has the potential to revolutionize the domain of security. Indeed, since a multi-antenna base station forms a power beam in the direction of the intended user, it will result in an advantage in SNR with respect to a potential eavesdropper, located at a different place. Similarly, the frequency dimension can be used as well to provide an additional SNR advantage. The objective of this work is to study the secrecy performance and develop novel precoding/beamforming techniques taking advantages of the massive potentials of 5G communications.

OBJECTIVES

- Understand the core concepts of information-theoretic secure communications including quantitative security metrics (secrecy capacity, eavesdropper equivocation…).
- Design dedicated precoding techniques exploiting frequency and space variations of the channel to create an advantage at the legitimate receiver.
- Study the impact of the receiver design.
- Identify key 5G scenarios for application and integration with the standards.
- Demonstrate the concepts using new software defined radio (SDR) electronic platforms.

CONTACT

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

Stochastic geometry modelling of exposure to 5G base stations

Information: Philippe De Doncker
Students: ELEC, PHYS
Type: Theoretical and/or experimental

MOTIVATION

Exposure to Electro-Magnetic Fields (EMF) is a major public concern for years now. It triggers many debates among all relevant stakeholders (governments, public environmental agencies, network providers, non- governmental associations) every time a new network generation is emerging, as 5G nowadays.
5G brings an important evolution in terms of pervasive connectivity for people and objects, offering high data rates and low latencies. This evolution is possible e.g. thanks to network topology changes through deployment of small cells, and communication strategies improvements through the use of massive MIMO directive antennas at the Base Stations (BS). Clearly, these two technological approaches will significantly impact EMF exposure also. But theoretical and/or computational tools able to analyze the impact of such changes on EMF exposure in a generic way are lacking.

For some years now, stochastic geometry (SG) has proven to be a very powerful approach for generic network performance analysis at communication or network layers. But no application to EMF exposure exists, although SG seems able to fill in the gap in the existing exposure modeling tools.

OBJECTIVES

The goal of this Master Thesis is to develop, validate, and apply stochastic geometry models to the estimation of EMF exposure due to emerging cellular networks.

This goal will be achieved through

(i) New numerical and analytical models of EMF exposure within the stochastic geometry framework;
(ii) Experimental validation of the proposed models;
(iii) Comparison with real-world measurements during the early stage of 5G.

CONTACT

Philippe De Doncker, pdedonck@ulb.ac.be, 02-650 3091
Solbosch campus, building U, level. 3, OPERA department

Resource allocation and multiple access in multi-beam Spatial Data Focusing

Information: Philippe De Doncker, François Horlin, Guylian Molineaux
Students: ELEC, PHYS
Type: Theoretical and/or experimental

MOTIVATION

Location-based multicasting, or Geocasting, refers to the transmission of information that is retrievable only by users that are located in specific predetermined geographical areas and is inaccessible elsewhere. It is especially useful in the scope of future Internet-of-Things and Smart City environments, where large groups of mobile devices can benefit from location relevant and contextualized information. Geocasting is traditionally implemented using beamforming to focus power in a desired direction. The achievable accuracy is however limited. As an alternative to power focusing, Spatial Data Focusing (SDF) performs channel-based modulation that ensures symbol distortion in all but one direction, by directly exploiting the differences between the sub-channels in a Multiple-input Single-Output communication scheme. By omitting the array radiation pattern constraints, SDF is shown to provide great improvements over beamforming in terms of geocasting accuracy and flexibility.

OBJECTIVES

This Master thesis should investigate the possibilities to transmit separate datastreams simultaneously to multiple different geographical areas from a single SDF base station. Different datastreams should not interfere and hence resource allocation based on multiple access schemes should be employed, however its impact on system performance (datarate, spatial selectivity…) should be assessed and minimized. Additionally, user terminals require a means of distinguishing between relevant datastreams that are targeting their location and irrelevant datastreams that are targeting different locations and that can be ignored.

CONTACT

Philippe De Doncker, pdedonck@ulb.ac.be, 02-650 3091
François Horlin, fhorlin@ulb.ac.be, 02-650 6741
Solbosch campus, building U, level. 3, OPERA department

Optimization of a multi-sensor network of WiFi antenna arrays and radars for localization

Information: Philippe De Doncker, François Quitin, Jean-François Determe
Students: ELEC, PHYS
Type: Theoretical and/or experimental

MOTIVATION

Smart cities entail the real-time monitoring of traffic in urban environments. A promising approach for estimating the positions and speeds of targets (pedestrians, bikes, and cars) is the combination of different technologies. One of such technology is based on passive WiFi antenna arrays that opportunistically acquire WiFi signals transmitted by smartphones and process them to estimate user positions and speeds. Active radars are another complementary technology; they provide another set of position and speed estimates and their accuracy is different than that of passive WiFi arrays. Typically, several sensors endowed with WiFi and/or radar systems cooperate to identify targets. Thus, an interesting problem is to compute the placement of the sensors that optimizes localization accuracy.

OBJECTIVES

This Master's thesis focuses on the optimal placement of sensors across streets, highways, etc. In particular, it shall study state-of-the-art theoretical tools for quantifying localization uncertainty (e.g., bounds from information theory such as the Cramer-Rao bound and dilution of precision). Leveraging these theoretical tools and a simulation environment, this thesis should propose and validate optimal designs for the placement of radar and WiFi sensors in realistic contexts. Finally, a partial experimental validation could be part of this thesis if time allows.

CONTACT

Philippe De Doncker, pdedonck@ulb.ac.be, 02-650 3091
François Quitin, fquitin@ulb.ac.be, 02-650 2829
Solbosch campus, building U, level. 3, OPERA department

Physical-layer security — IoT device authentication and ciphering using physical unclonable functions

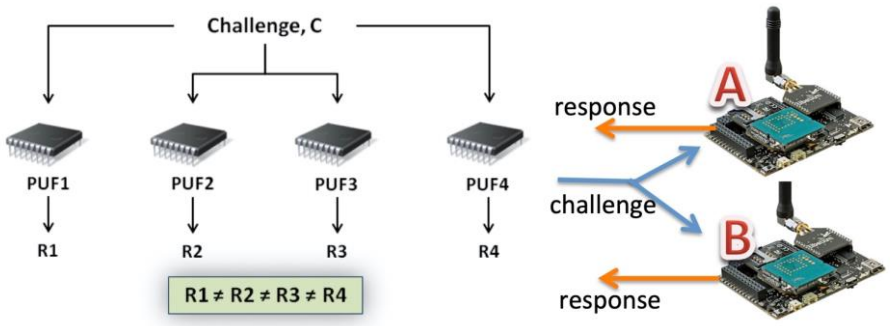
Information: Jean-Michel Dricot, Dragomir Milojevic, Olivier Markowitch
Students: Electronics / Computer Engineers, Cybersecurity scientists
Type: Theoretical and/or experimental

MOTIVATION

There are approximately 7 billion of IoT devices in the world today and their number grows aggressively over the years. With their large level of deployment comes the need of protecting these devices from malicious since IoT (in)security is a major problem and a rising threat (see for instance the Mirai botnet attack). In practice, there is a strong need to implement lightweight authentication and ciphering of the communication beyond classical crypto protocols, such as Diffie-Hellman key exchange or TLS that are out of the reach of embedded electronics.

A physical unclonable function (PUF) is a device that exploits inherent randomness introduced during CMOS manufacturing to give a physical entity a unique fingerprint of the device (similar to human biometrics). PUFs are most often based on unique physical variations which occur naturally during semiconductor manufacturing but can also be embodied in side electronics designed for that purpose. Examples include clock drifts, SRAM memory states at power-up, logical gates response, etc.

From a security perspective, any challenge presented to a device will lead to a different response, based on the unique characteristics of the electronics (see fig. below) and can be exploited to perform identification, signing, and key derivation.



Device fingerprinting at physical layer

OBJECTIVES

- Understand the core concepts of physical unclonable function and its application in the context of Internet of Things.
- Demonstrate using a FPGA-based implementation and analyse its sensitivity to the environment (e.g. power-up cycles, temperature) .
- Identify your device with its unique fingerprint and the corresponding fuzzer (a “correction” function to stabilize the input and output)

CONTACT

Jean-Michel Dricot jdricot@ulb.ac.be, D. Milojevic dmilojev@ulb.ac.be, and Olivier Markowitch

Physical-layer security — Physical unclonable functions from and for commodity hardware

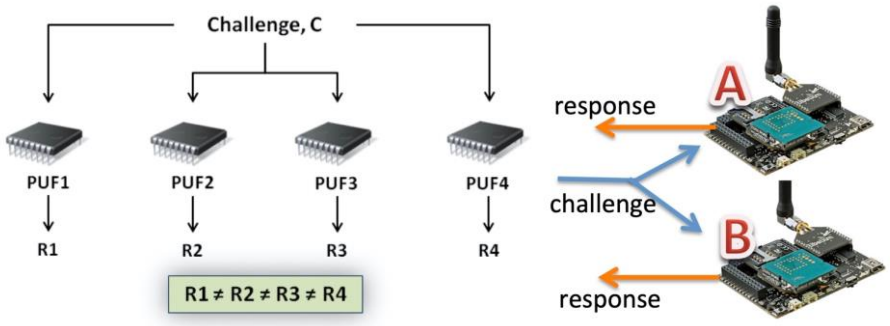
Information: Jean-Michel Dricot, Dragomir Milojevic
Students: Electronics / Computer Engineers, Cybersecurity scientists
Type: Theoretical and/or experimental

MOTIVATION

There are approximately 7 billion of IoT devices in the world today and their number grows aggressively over the years. With their large level of deployment comes the need of protecting these devices from malicious since IoT (in)security is a major problem and a rising threat (see for instance the Mirai botnet attack). In practice, there is a strong need to implement lightweight authentication and ciphering of the communication beyond classical crypto protocols, such as Diffie-Hellman key exchange or TLS that are out of the reach of embedded electronics.

A physical unclonable function (PUF) is a device that exploits inherent randomness introduced during CMOS manufacturing to give a physical entity a unique fingerprint of the device (similar to human biometrics). PUFs are most often based on unique physical variations which occur naturally during semiconductor manufacturing but can also be embodied in side electronics designed for that purpose. Examples include clock drifts, SRAM memory states at power-up, logical gates response, etc.

From a security perspective, any challenge presented to a device will lead to a different response, based on the unique characteristics of the electronics (see fig. below) and can be exploited to perform identification, signing, and key derivation.



Device fingerprinting at physical layer

OBJECTIVES

- Understand the core concepts of physical unclonable function and its application in the context of Internet of Things.
- Investigate how commodity hardware can be exploited / extended in order to embed PUF.
- Deliver an implementation on a RaspberryPi box.

CONTACT

Jean-Michel Dricot jdricot@ulb.ac.be and Dragomir Milojevic dmilojev@ulb.ac.be

Physical-layer security — WiFi security using wireless channel authentication

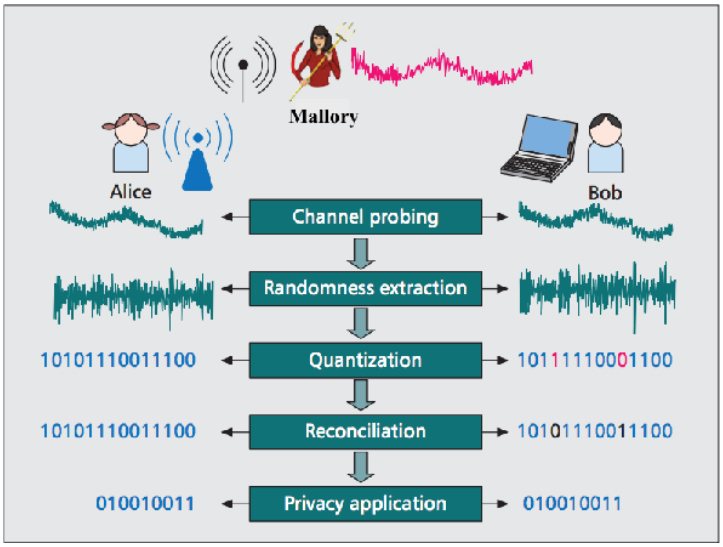
Information: Jean-Michel Dricot, François Rottenberg
Students: Electronics / Computer Engineers, Cybersecurity scientists
Type: Theoretical and/or experimental

MOTIVATION

In 2017 was discovered a weakness in WPA2, the protocol that secures all modern protected Wi-Fi networks. An attacker within the vicinity of a victim could intercept the key exchange phase and force a key re-installation, hence leading to insecure communication (possibly zeroing the key).

This attack makes use of a channel-based MitM attack, where the rogue access point is cloned on a different channel with the same MAC address as the targeted access point. A practical counter-measure to this is channel authentication, i.e., use the physical properties of the wireless channel (i.e., reciprocity) to determine if a relaying antenna has been inserted or not between the terminals.

A previous and successful master thesis conducted in our lab showed that a shared secret key can be silently computed by Alice and Bob (without any exchange of information). Then, this key can be used to authenticate the communication channel and/or bootstrap a key scheduling for crypto.



Wireless channel fingerprinting and key derivation

OBJECTIVES

- Understand the core properties of wireless physical transmission and its application to security
- Implement a permanent proof-of-concept for WiFi systems with a channel signature scheme or channel authentication scheme
- Demonstrate by implementing a CRACK-resistant variant of WPA2 protocol based on channel authentication

CONTACT

Jean-Michel Dricot jdricot@ulb.ac.be

Privacy-aware localization and tracking

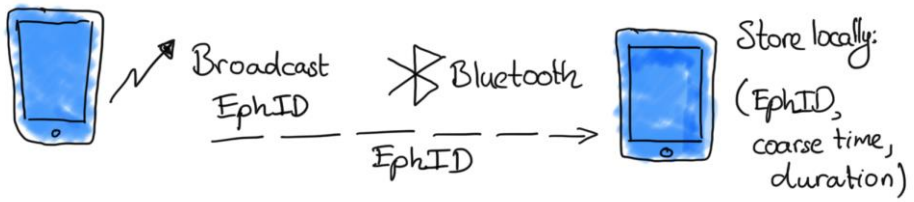
Information: Jean-Michel Dricot
Students: Computer Engineers, Cybersecurity scientists
Type: Theoretical and/or experimental

MOTIVATION

The COVID-19 crisis has increased the pressure to track and localized assets and people. Public authorities (from nation states) and companies (such as Google and Apple) have begun designing location-tracking strategies with various approaches in order to help authorities plan their COVID-19 containment strategies, and better ensure that they're addressing key areas of concern.

The data provided is anonymized and somewhat aggregated, so there are generally no personally identifying markers. Still, several questions arise since the original data are usually now anonymous by themselves. The temptation is high for authorities to ask some day for a (partial) de-anonymization of the inputs. On the other side, complete anonymous collection (i.e., on a voluntary basis) can be subject to fooling, DOS, and be seen as trustless sources.

Hence the question: *humanity vs. localization, is privacy always going to be the loser?*



More generally, privacy tracking is a long-term question in logistics, medicine, and safety, especially since the advent of the Internet of Things. Several technologies (low-range Bluetooth) and techniques physical unclonable functions[1]) are nowadays available in complement to large-scale networks (5G) and could be integrated to develop a whole privacy-aware system.

OBJECTIVES

- Understand the core requirements of privacy-aware tracking and the use of physical unclonable function in key schedule.
- Design a reliable, privacy preserving tracking protocol that inherently avoids de-anonymization while allowing to verify medical accuracy of the information.
- Implement in the form of an app in a smartphone.

CONTACT

Jean-Michel Dricot jdricot@ulb.ac.be

[1] A physical unclonable function (PUF) is a device that exploits inherent randomness introduced during electronics manufacturing to give a physical entity a unique fingerprint of the device (similar to human biometrics).

ULB as a future SmartCampus — blockchain-based data monitoring

Information: Jean-Michel Dricot, Jean Landercy
Students: Computer Engineers, Cybersecurity scientists
Type: Theoretical and/or experimental

MOTIVATION

The project SmartCampus started in 2018 as a long-term transformation of the university campus towards a 2.0, green-oriented campus thanks to the use of Internet of Things and open data. As of today, several steps have been achieved: LoraWAN deployment, data collection from energy flows, real-time usage of IT infrastructure. This information is made available to the academic community through an open data hub.

Blockchain will be a key element of SmartCampus in order to increase trust and integrity as well to bootstrap digital governance. SmartCampus follows the industry-standard GMP/GLP (Good Manufactoring or Laboratory Practice) that concerns the whole of the data life cycle, from when the data is acquired through to when it is archived, encompassing verification, processing, use and communication and covering both electronic and paper-based data.

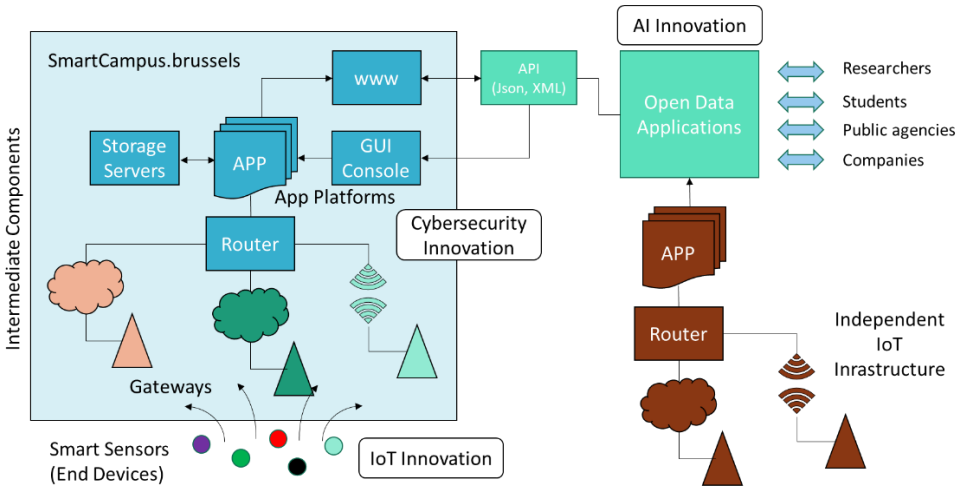


Figure 1 - Smart campus architecture

The objective of this (applied) master thesis is to deploy, develop, and implement a blockchain platform, based on Ethereum / Solidity for the SmartCampus project. It follows a preliminary work made by a student last year.

OBJECTIVES

- Understand the core concepts of Ethereum (and associated Solidity language) in order to fulfil the requirements of our University.
- Deploy semi-private Ethereum nodes and code the chain governance.

CONTACT

Jean-Michel Dricot jdricot@ulb.ac.be and Jean Landercy Jean.Landercy@ulb.be

High-performance blockchain signatures for e-payment

Information: Jean-Michel Dricot, Gaurav Sharma
Students: Computer Engineers, Cybersecurity scientists
Type: Theoretical and/or experimental

MOTIVATION

ULB and Worldline collaborate to build an innovative blockchain platform which can enhance the performance of blockchain systems comparable to centralized systems. The Worldline's smart payment engine (SPE) facilitating the payments between consumer and merchant banks, is planned to employ blockchain technology to its core architecture and hence decentralize the trust. One of the major challenges is to achieve the desired transaction throughput satisfying the merchants and banks privacy requirements.

The project is about the development of a high-performance permissioned blockchain architecture focusing on three types of transactions. A normal transaction is a public transaction without any privacy focus while private transactions conceal the participant parties as well as the transaction amount. Currently, some existing blockchain platforms facilitate these two types of transactions. However, our objective is to add a new type of transaction which is an outcome of a bidding process, keeping the privacy as the highest priority. The major challenge here is to choose the bidding winner in an extremely efficient way.

OBJECTIVES

- Produce a proof of concept for an auction/bidding system in a permissioned blockchain environment (Ethereum with Solidity language).
- Implement a protocol with the following properties:
    - Bid privacy. All bidders cannot know the bids submitted by the others before committing to their own
    - Posterior privacy. All committed bids are maintained private from the bidders and public bidders.
- The scientific contribution targeted for this internship is to achieve bidder's privacy but the *highest bidder (winner) is traceable*.

REFERENCES

[1].Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.

[2]. Galal, H. S., & Youssef, A. M. (2018, February). Verifiable sealed-bid auction on the ethereum blockchain. In *International Conference on Financial Cryptography and Data Security* (pp. 265-278). Springer, Berlin, Heidelberg.

CONTACT

Jean-Michel Dricot jdricot@ulb.ac.be and Gaurav Sharma Gaurav.Sharma@ulb.ac.be