

# 2025 Activity Report

RESEARCH CENTRE: Inria Centre at the University of Lille

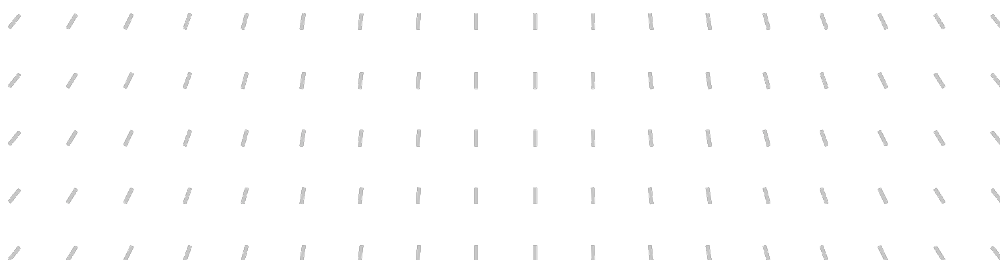
---

Team

# FUN

self-organizing Future Ubiquitous Network

---



## **Team FUN**

*Creation of the Team: 2013 July 01*

Each year, Inria research teams publish an Activity Report presenting their work and results over the reporting period. These reports follow a common structure, with some optional sections depending on the specific team. They typically begin by outlining the overall objectives and research programme, including the main research themes, goals, and methodological approaches. They also describe the application domains targeted by the team, highlighting the scientific or societal contexts in which their work is situated. The reports then present the highlights of the year, covering major scientific achievements, software developments, or teaching contributions. When relevant, they include sections on software, platforms, and open data, detailing the tools developed and how they are shared. A substantial part is dedicated to new results, where scientific contributions are described in detail, often with subsections specifying participants and associated keywords. Finally, the Activity Report addresses funding, contracts, partnerships, and collaborations at various levels, from industrial agreements to international cooperations. It also covers dissemination and teaching activities, such as participation in scientific events, outreach, and supervision. The document concludes with a presentation of scientific production, including major publications and those produced during the year.

## Keywords

### Computer sciences and digital sciences

A1.2.3. – Routing

A1.2.6. – Sensor networks

A1.2.8. – Network security

A1.3.6. – Fog, Edge

A1.6. – Green Computing

A5.10.6. – Swarm robotics

### Other research topics and application domains

B3.4.3. – Pollution

B3.5. – Agronomy

B5.1. – Factory of the future

B5.9. – Industrial maintenance

B6.4. – Internet of things

B8.1.2. – Sensor networks for smart buildings

B8.2. – Connected city

## Contents

<b>Team FUN</b>	<b>1</b>
<b>1 Team members, visitors, external collaborators</b>	<b>5</b>
<b>2 Overall objectives</b>	<b>6</b>
<b>3 Research program</b>	<b>6</b>
3.1 Research axes	7
3.1.1 Frugality and opportunism	7
3.1.2 Security	8
3.1.3 Interconnectivity	8
<b>4 Application domains</b>	<b>8</b>
<b>5 Social and environmental responsibility</b>	<b>9</b>
<b>6 Highlights of the year</b>	<b>9</b>
6.1 Awards	9
<b>7 Latest software developments, platforms, open data</b>	<b>9</b>
7.1 Open Access Software	9
7.2 Latest software developments	10
7.2.1 PILOT Dataset	10
7.2.2 my_ble	10
7.2.3 LoRa WuR	11
7.2.4 Wireless Sensor Network Planner & Controller Graphical User Interface	11
7.2.5 Wireless Sensor Network Planner & Controller REST API	12
7.2.6 ESP-IDF Img	12
7.3 New platforms	13
7.4 Open data	13
<b>8 New results</b>	<b>14</b>
8.1 Wireless Network Security	14
8.1.1 Anomaly detection	14
8.1.2 Drones detection	15
8.1.3 Jamming detection and Eavesdropping mitigation in heterogeneous wireless networks	15
8.1.4 Denial of service Vulnerabilities	16
8.2 Network servicing	16
8.3 Network deployment and exploration	17
8.4 V2X communications	18
8.5 Routing in wireless networks	18
8.6 Cell-Free MIMO in Vehicular Networks: Resources Allocation and Security Vulnerabilities	19
8.7 Localisation and fingerprinting approaches	19
<b>9 Partnerships and cooperations</b>	<b>20</b>
9.1 International initiatives	20
9.1.1 Associate Teams in the framework of an Inria International Lab or in the framework of an Inria International Program	20
9.2 International research visitors	20
9.2.1 Visits of international scientists	20
9.3 European initiatives	21
9.3.1 Horizon Europe	21
9.3.2 Other european programs/initiatives	26
9.4 National initiatives	26

9.5	PEPR	28
9.6	Regional Initiatives	29
9.7	Public policy support	30
<b>10</b>	<b>Dissemination</b>	<b>30</b>
10.1	Promoting scientific activities	31
10.1.1	Scientific events: organisation	31
10.1.2	Scientific events: selection	31
10.1.3	Journal	31
10.1.4	Invited talks	32
10.1.5	Scientific expertise	32
10.2	Teaching - Supervision - Juries - Educational and pedagogical outreach	32
10.2.1	Teaching	32
10.2.2	Supervision	32
10.2.3	Juries	33
10.3	Popularization	34
10.3.1	Specific official responsibilities in science outreach structures	34
10.3.2	Productions (articles, videos, podcasts, serious games, ...)	34
<b>11</b>	<b>Scientific production</b>	<b>34</b>
11.1	Major publications	34
11.2	Publications of the year	35
11.3	Cited publications	37

# 1 Team members, visitors, external collaborators

## Research Scientists

- Nathalie Mitton [Team leader, Inria, Senior Researcher, HDR]
- Valeria Loscri [Inria, Senior Researcher, HDR]

## Faculty Member

- Damien Charabidze [UNIV LILLE, Professor Delegation, from Sep 2025, HDR]

## Post-Doctoral Fellows

- Carol Habib [Inria]
- Kawtar Lasri [Inria, Post-Doctoral Fellow]
- Amira Mourad [Inria, Post-Doctoral Fellow]
- Christian Salim [Inria, from Nov 2025]
- Shrikant Tangade [Inria, from Dec 2025]
- Selma Yahia [Inria, Post-Doctoral Fellow, until Sep 2025]

## PhD Students

- Tatiana Al Jamous [UNIV. ANTONINE]
- Ildi Alla [Inria, until Sep 2025]
- Saif Aziz Baig [UNIV. LILLE, from Nov 2025]
- Aymen Salah Eddine Bouferroum [Inria]
- Hazem Chaabi [Inria, until Nov 2025]
- Selina Cheggour [UNIV LILLE, until Sep 2025]
- Roxane Degas [Inria, from Oct 2025]
- Lucien Dikla Ngueleo [Inria]
- Emi Dreckmeyr [Inria]
- Emile Egreteau-Druet [Inria]
- Mo Ringbe Saynbe [Inria]
- Marwa Slimene [Inria]
- Jiali Xu [Inria]

## Technical Staff

- Khalil Ben Kalboussi [Inria, Engineer]
- Lucille Colin [Inria, Technician, Project manager]
- Solenne Fortun [Inria, Engineer, Project Manager]
- Etienne Profit [Inria, Engineer]
- Prakriti Saxena [Inria, Engineer, from May 2025 until Oct 2025]
- Alexandre Veremme [Inria, Engineer]

## Interns and Apprentices

- Chady Abi Fadel [UNIV. ANTONINE, Inria, Intern, from Oct 2025]
- Amer Alzein [UNIV. ANTONINE, Inria, Intern, until Feb 2025]
- Adam Bounkhila [UNIV LILLE, Intern, from Nov 2025]
- Pablo Morais [LYCEE EIC TOURCOING - BTS, Intern, from May 2025 until May 2025]

## Administrative Assistant

- Anne Rejl [Inria]

## Visiting Scientists

- Paul Dayang [UNIV. NGAOUNDERE, CAMEROUN, from Dec 2025]
- Samuel Kotva Goudougou [UNIV. NGAOUNDERE, CAMEROUN, from Sep 2025]
- Megan Le Roux [UNIV. STELLENBOSCH, SOUTH AFRICA, until Mar 2025]

## 2 Overall objectives

With the foreseen increase of communicating devices around the world, many challenges will arise. Among them, the most predominant ones are certainly the scarcity of the medium, the energy consumption, the lack of interoperability and the security of these devices and their data.

Our objectives are to address these different challenges for the self-organization of these Future Ubiquitous Networks. Our focus will be set on wireless heterogeneous communicating objects that feature different limitations and constraints such as hardware limitations (low computing and memory storage capacities), limited energy, potentially high mobility or hostile environment. By wireless, we mean any communication with no wire. Objects could thus communicate through traditional RF transmissions or any alternative way such as visible light communication (VLC) or molecular technologies. They can be heterogeneous in terms of hardware processing, mobility patterns (mobility can be undergone or controlled, unknown or predictable), communication technologies, etc. For all these families of devices, we will design holistic communication protocols to allow them to efficiently function and cooperate in a harmonious energy- and data-priority aware fashion. These protocols will focus on low communication layers (PHY, MAC and NET) and combine opportunistically heterogeneous device features to make a global efficient behavior emerge.

*The goal of the FUN project team is to leverage the heterogeneity of the new communicating devices to override major rising issues. Heterogeneity and mobility will be seen as opportunities and strengths rather than flaws and exploited. Our protocols will foster the cooperation between devices in a secure, energy efficient and frugal way.*

## 3 Research program

### Objectives and methodology

To achieve our main objectives, we will mainly apply the methodology depicted in Figure 1 combining both theoretical analysis and experimental validation. Mathematical tools will allow us to properly dimension a problem, formally define its limitations and needs to provide suitable protocols in response. Then, they will allow us to qualify the outcome solutions before we validate and stress them in real scenarios with regards to applications requirements. For this, we will realize proofs-of-concept with real scenarios and real devices. Differences between results and expectations will be analyzed in return in order to well understand them and integrate them by design for a better protocol self-adaptation capability.

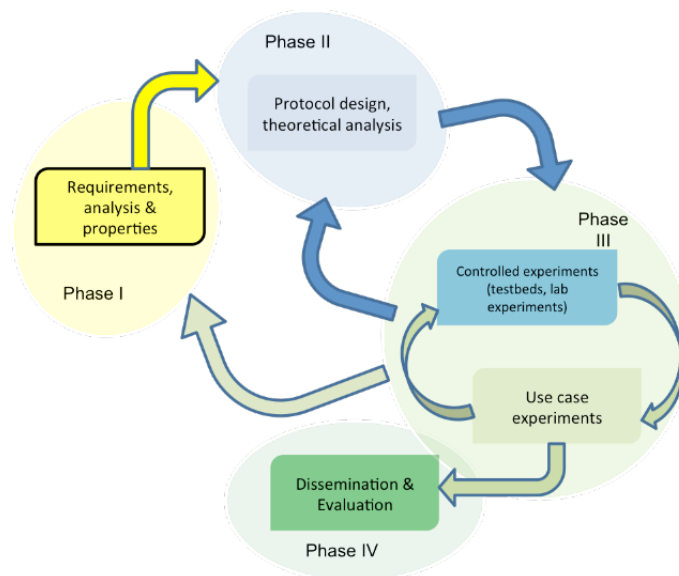


Figure 1: Methodology to be applied in FUN.

### 3.1 Research axes

To reach this overall objective, we will develop our research around the three following axes: *i)* Frugality and opportunism, *ii)* Security and *iii)* Interconnectivity. Note that these axes are not completely independent nor hermetic. A transversal axis will be the deployment and set up of experimental testbeds.

#### 3.1.1 Frugality and opportunism

As the objects we consider are resource-limited and that they use a rare resource to communicate (wireless medium), all our solutions must be frugal and use as little resources as possible. A way to alleviate the energy consumption and the medium utilization is to reduce the data to send and/or to smartly decide when to send it, by what mean and to whom without jeopardizing the accuracy and completeness of the data. When to send a piece of data can indeed impact the resource utilization since in a dynamic environment, some interference could appear at different times; in a mobile environment, a piece of data could be carried rather than transmitted; in an energy-harvesting network, the amount of available energy could grow. We thus intend to closely analyse and understand interference impacts on different environments and contexts on one hand (as the research initiated in LumiCar, EthiCam, AgriNET projects) and to exploit them in the design of our protocols.

Deciding what data to send allows for a data reduction and resource savings. To do so, we will use machine learning techniques (e.g. Thompson sampling, Bayesian approaches, linear approaches, ARMA, Pearson sampling etc) that we will adapt to fit the specific context of the applications. The idea is to propose predictive algorithms to "guess" a data rather than transmitting it. This is among others what we are investigating in the AgriNET project.

In case of the availability of multiple communication technologies, the choice of this technology will impact the global system since all technologies do not provide the same QoS performances (delays, throughputs, etc) with different energy consumptions and do not face interferences the same way depending on the environment. We will thus analyse and understand all these specificities to combine them to get the best performances.

In all above mentioned cases, we will try to provide time and space depend protocols as frugal as possible but still meeting the application requirements and expectations. This will be done by opportunistically leveraging network particularities (multiple technologies, mobility, energy-harvesting, etc) based on experimental-driven behavioral analysis, as initiated with the collaboration with Sencrop.

### 3.1.2 Security

Security of wireless transmissions is a rising issue that gains importance with the increase of wireless devices. Our team has just started research work in security but we will pursue our efforts. Our goal will be to secure the wireless communications in different ways. Indeed, traditional security techniques (cryptography, firewalls, etc) cannot be applied in FUN because of their pervasive feature and limited resources. In terms of Security, we will focus on the lowest layers of the communication stack in order to first identify attacks that may appear at these levels and proposes *i*) recovering and healing solutions and *ii*) new solutions that are robust by design.

At the MAC layer, we will for instance investigate denial of sleep-like attacks that aim to make nodes deplete their energy quickly. At NET layer, we will investigate different routing protocols that are able to detect an abnormal behavior of a neighbor node to then exclude it from any network operation. This has obviously to be done locally and in a distributed way. In all cases, the same methodology will be applied: observe, understand and model, to then identify the threat or the malicious entity and finally heal. In some cases, we can leverage the characteristics of the communication technology to reinforce the security aspect, such as VLC that may allow Line-of-Sight (LOS) communications and for which certain types of attacks that can be effective for "traditional" wireless systems (i.e., jamming attacks) cannot be easily applied. The works initiated in the framework of the H2020 CyberSANE project, in the DGA grant and in DEPOSIA project, fall within this perspective.

### 3.1.3 Interconnectivity

Another challenge faced by FUN is their interconnectivity to traditional networks such as Internet and the data offloading. Because of their limited capacity, FUN devices may need to call for remote services. These latter are usually hosted in the cloud. But being served by the cloud implies sometimes long latency and uselessly congestion of the wired network. We will thus investigate how to get these services closer to the FUN devices to alleviate the energy consumption, reduce latency and network congestion. This will go from edge and mobile edge deployments to service distribution over more powerful heterogeneous devices. Our research will analyse devices needs and estimate in time and space the services to be deployed. When the service is expected to be temporary, mobile edge services could be deployed and so our investigations will include the self-deployment techniques. When some already deployed wireless devices feature more capacity, we can leverage this node heterogeneity to distribute the services over these nodes. The research conducted towards this third objective will call for adaptation of machine learning techniques to predict needs, to mobility modeling and cross-layer communication protocols. This has been initiated in the DRUID-NET project.

## 4 Application domains

The FUN research can be applied in various applications. We only cite here the ones on which we currently focus.

- **Smart Agriculture:** Wireless sensors are more and more deployed in remote fields and livestock for an accurate monitoring. This generates new challenges in terms of reliability, energy consumption and range as investigated in the D4SC and Agrinet projects.
- **Vehicular networks:** vehicles become smarter and smarter, providing new useful services. But communications between vehicles on the one hand and between vehicles and road infrastructures on the other hand raise a lot of challenges as investigated in the CORTESE project, by considering security aspects of the different communication technologies enabling the connected vehicles or with the *:dot.dot* company. Moreover, alternative technologies and interactions of traditional and unconventional communication technologies are considered in LumiCAR.
- **Smart infrastructures:** FUN research can also apply to different urban and civil infrastructure like road monitoring (as in the DEFI with CEREMA or SIRCAPASS project) or Smart Grids. In the project MLSysOps a full AI-based framework is implemented for autonomic end-to-end system management across the full cloud-edge continuum, that can be applied to different infrastructures.

- **Logistic and traceability:** RFID and IoT are the key technologies to enable large scale traceability. They are for instance investigated in the GoodFlow and AUtonomous Pack projects. Traceability is also investigated by the means of advanced technologies, that are the focus of ETHICAM project.
- **Post disaster recovery:** New services of different kinds (communications, processing, context analysis) need to be deployed quickly and efficiently after a disaster in order to support rescue operations. This requires adaptable and flexible resource deployment such as investigated in NEPHELE project.

## 5 Social and environmental responsibility

All protocols and algorithms designed and developed in the team are energy-efficient by design. Going further, especially in Research focus 1, we target applications that are environment-friendly and which aim to reduce a more global environmental footprint such as reducing the use of extra intrans in agriculture (such as water or fertiliser), enabling the reuse of packaging or less pollutant road and structures maintenance or with social concerns. This is reflected by the main topic of most of our collaborative projects and of the support from ADEME.

In the last few years, several solutions developed in the context of different projects in the team, are based on the integration of security aspects by design. In particular, the constrained and resource limitations of the IoT paradigm, that is at the core of the reasearch activities of the team, imposes a consideration of cyber-security solutions that explicitly account for these limitations. Advanced cyber-security approaches based on physical layer and cross-layer approaches have been recently developed in the context of European, National and Regional initiatives, accounting the social and environmental aspects by design.

## 6 Highlights of the year

Valeria Loscri has been appointed Deputy Scientific Director of Inria in charge of Networks and Distributed Systems in October 2025.

### 6.1 Awards

Nathalie Mitton has been selected as 2025 ComCom Best Associate Editor Award.

## 7 Latest software developments, platforms, open data

### 7.1 Open Access Software

In the context of the European Project MLSysOps, several open access software have been developed. In particular:

- An ML model was developed to detect jamming attacks within a 5G network by leveraging relevant features extracted from traces and logs generated by UE and the gNB. Concerning this contribution, two frameworks have been developed: SHIELD and GanSec;
- SHIELD, implements supervised learning models for detecting wireless jamming from native Android logs, GitHub repository. Available at: The code and data are available [here](#).
- Synchronized UE-gNB log & trace collector, Gitlab repository is available [here](#).
- SHIELD on-device detection, extension on industrial device (Teltonika RUTX50), Github repository is Available [here](#). Network simulation environment for MLSysOps project, GitHub repository is available [here](#).

- GANSec is a framework to generate reliable and robust synthetic data. GAN-based data augmentation training and evaluation framework are available as open access in a Github repository [here](#).

Moreover, a framework to geo-localise target devices has been developed.

- Sec5GLoc is a geolocation framework based on a new approach that integrates security and privacy features by design. Our approach incorporates a formal threat model and introduces architectural features to defend against spoofing and adversarial manipulation. Specifically, we leverage the known geometry of anchors and timing information as built-in consistency checks, and we use a multi-head attention fusion mechanism to dynamically mitigate the impact of suspicious signals. We also consider the system's deployment model to enhance privacy (e.g. enabling on-device localization to keep CSI data local). The overall code is available [here](#).

## 7.2 Latest software developments

### 7.2.1 PILOT Dataset

**Name:** Privacy-preserving data collectIon of wireLess cOmmunication Technologies.

**Keywords:** Wireless network, Human mobility, Sensors

**Scientific Description:** "PILOT dataset" is a privacy-preserving collection of wireless communication data from three technologies: WiFi, BLE (Bluetooth Low Energy), and LoRa (Long Range Radio), alongside sensor data (acceleration, roll, pitch). It is collected over 90 hours in various mobility scenarios, including static and mobile contexts, using Pycom FiPy devices. The dataset, which preserves privacy by masking sensitive information, is available on GitHub for use in human mobility studies and machine learning applications.

**Functional Description:** PILOT dataset provides a new generation of collected data that would help in providing keys for studying human mobility or other applications. It is characterized by mainly two novel approaches for collecting data, at the level of Model type and Parameters recorded, as follows: 1) Collecting different types of data from sensors and wireless communication technologies at a time: WiFi probe-response, BLE beacons, LoRa packets, and from the sensors: Acceleration, Roll and Pitch information. 2) The data is collected in different mobility scenarios and mainly classified into two categories: Static vs Mobile. The overall collected data till now spans about 90 hours in total in different mobility scenarios collected using a Micropython enabled microcontroller called FiPy device. The dataset is released as a collection of text files and comma-separated values (CSV) files with mainly the timestamp, a unique identifier of the emitting device, RSSI (Received Signal Strength), and other information dedicated to each wireless technology. This dataset is privacy-preserving since it fully meets the GDPR specification, where the mac addresses and the device names are masked.

**Contact:** Jana Koteich

### 7.2.2 my\_ble

**Name:** ESP-IDF my\_ble component

**Keyword:** Bluetooth

**Scientific Description:** The my\_ble library is an advanced software module designed to integrate the Apache MyNewt NimBLE host within the ESP-IDF v5.3.1 framework. It enhances Bluetooth Low Energy (BLE) management on ESP32 microcontrollers by providing a high-level functional abstraction while maintaining full control over low-level operations, such as task management, multiprocessor synchronization, and semaphore-based coordination under FreeRTOS.

**Functional Description:** This is a component compatible with ESP IDF V5.3.1 providing an API to use Apache MyNewt NimBLE host on ESP32 MCUs exposing simple to use predefined functions, yet giving full control over core functionalities like task handling, multiprocessing and semaphore enabled BLE scan checking.

**News of the Year:** Development and integration of the my\_ble library (ESP-IDF 5.3.1) for advanced Bluetooth Low Energy management using the NimBLE host on the ESP32 microcontroller.

**Contact:** Khalil Ben Kalboussi

**Participant:** Khalil Ben Kalboussi

### 7.2.3 LoRa WuR

**Name:** librairie ESP-IDF pour module LoRa sx1261

**Keywords:** Sx1261, LoRa, ESP32, ESP-IDF

**Scientific Description:** The LoRa SX1261 library enables advanced integration of the Semtech SX1261 transceiver on ESP32(S3) with ESP-IDF v5.3.1, simplifying SPI bus management, FreeRTOS tasks, and low-power RxDutyCycle operation. It supports GFSK packet transmission, reception, and detection, with two modes: automatic or advanced, providing full control over SPI and task scheduling.

**Functional Description:** This is a library (in the form of a component) compatible with ESP-IDF V5.3.1 that enables the use of the SEMTECH SX1261 LoRa module with the ESP32(S3). The component is based on the low-level hardware driver provided by SEMTECH, which operates over the SPI bus, modified to include functions for sending, receiving, and packet detection in sleep mode (RxDutyCycle) in GFSK mode. The library provides functions for use in a normal mode, where it automatically handles tasks and SPI bus management internally, or in an advanced mode that offers full control over SPI bus management and process scheduling.

**News of the Year:** Development and Integration of the LoRa SX1261 Library for ESP32(S3) The Fun Team designed an ESP-IDF v5.3.1 component enabling: advanced management of the Semtech SX1261 transceiver over the SPI bus, support for GFSK packet transmission, reception, and detection, implementation of RxDutyCycle low-power mode, two operational modes: automatic, with internal management of tasks and SPI, and advanced, providing full control over SPI transactions and FreeRTOS process scheduling.

**URL:** [https://gitlab.inria.fr/fun-team/lora\\_wur\\_v2/-/tree/lora\\_wur](https://gitlab.inria.fr/fun-team/lora_wur_v2/-/tree/lora_wur)

**Contact:** Khalil Ben Kalboussi

**Participants:** Nathalie Mitton, Carol Habib

### 7.2.4 Wireless Sensor Network Planner & Controller Graphical User Interface

**Name:** Wireless Sensor Network Planner & Controller GUI

**Keywords:** Sensors network, Wireless Sensor Networks, GUI (Graphical User Interface), User Interfaces, Front-end application, Web Application

**Scientific Description:** This web application allows users to define, configure, initialize, and start Wireless Sensor Networks (WSNs) in just a few steps. Using a map associated with an experiment (acquired and provided in PGM format, for example, data collected by a robot operating with ROS), the user can specify GPS coordinates of the sensors, which can then be deployed manually or by a robot.

Once the experiment is initiated and the sensors are deployed in the field, the application provides real-time visualizations of the measurements collected by the sensors. The application also enables continuous monitoring of the acquired data and the real-time detection and display of alerts related to the quality and consistency of the measurements produced by the network's sensors. These alerts are generated by a dynamic rules engine, which can be modified in real time by the application, and propagated across the networks to the sensors.

**Functional Description:** In this web application, a user can define experiment types to quickly initialize and launch WSN experiments in just a few clicks. Once an experiment map is provided or retrieved in PGM format, the user can set the GPS coordinates of the sensors (which can then be positioned either by a ROS robot or manually by the experimenter). Once an experiment has started and the sensors are deployed, time-based monitoring graphs become available, allowing users to view real-time alerts regarding the quality of the data provided by the network's sensors.

**Release Contributions:** First version

**URL:** [https://gitlab.eclipse.org/eclipse-research-labs/nephele-project/use-cases/use-case-1/uc1\\_inria\\_api](https://gitlab.eclipse.org/eclipse-research-labs/nephele-project/use-cases/use-case-1/uc1_inria_api)

**Contact:** Alexandre Veremme

**Participants:** Alexandre Veremme, Carol Habib, Nathalie Mitton, Amer Alzein

### 7.2.5 Wireless Sensor Network Planner & Controller REST API

**Name:** Wireless Sensor Network Planner & Controller API

**Keywords:** Web API, Sensors network, Wireless Sensor Networks, Control, Planning, Rule-based programming, Alerting Rule Engine

**Scientific Description:** This REST API manages all the entities needed to launch experiments based on Wireless Sensor Networks (WSNs). It allows users to define experiment templates and create experiments from their respective templates. A multitude of sensors can be associated with a single experiment. The API enables the configuration of sensor properties (in a completely generic way). From a map associated with an experiment (acquired and provided in PGM format, for example, by a robot operating under ROS), it is possible to specify the GPS coordinates of the sensors. A dynamic rule engine is implemented, enabling real-time alerts.

Once the experiment is initiated and the sensors are deployed in the field, the application provides endpoints to retrieve real-time measurement data, transmitted by the sensors. The application also allows for continuous monitoring of the acquired data and the real-time detection and display of alerts related to the quality and consistency of the measurements produced by the network's sensors. Alerts are generated by a dynamic rules engine that can be modified in real time, by the application, and propagated across networks to the sensors.

**Functional Description:** This API allows the manipulation (CRUD operations) of all entities involved in a WSN experiment: experiments, nodes, sensor types, geographic maps, node positions on the map, alerting rules, etc.

**Release Contributions:** First version

**URL:** [https://gitlab.eclipse.org/eclipse-research-labs/nephele-project/use-cases/use-case-1/uc1\\_inria\\_api](https://gitlab.eclipse.org/eclipse-research-labs/nephele-project/use-cases/use-case-1/uc1_inria_api)

**Contact:** Alexandre Veremme

**Participants:** Alexandre Veremme, Carol Habib, Nathalie Mitton

### 7.2.6 ESP-IDF Img

**Name:** ESP-IDF environment on Docker

**Keywords:** ESP-IDF, Docker

**Scientific Description:** The project involves the design and deployment of a Docker-encapsulated ESP-IDF development environment, aimed at standardizing and reproducing the compilation and flashing workflow for ESP32 microcontrollers in a multi-user context. The environment integrates all critical dependencies (Python, GCC, CMake, Ninja) and necessary system configurations, ensuring build reproducibility and version isolation. The solution leverages Docker volume sharing to synchronize code between the host and container, and exposes USB ports via `usbipd` or `esp_rfc2217_server` to allow direct hardware flashing from within the container. This architecture enhances collaborative development, reduces configuration-related errors on local machines, and supports continuous integration pipelines while maintaining cross-platform portability and source code security.

**Functional Description:** Deployment of an ESP-IDF environment on Docker, including all required dependencies (Python, GCC, CMake, Ninja) and system configurations. The container ensures version isolation, cross-platform portability, and build reproducibility, enabling collaborative development and continuous integration.

**News of the Year:** Development and integration of a Docker-encapsulated ESP-IDF 5.3.1 environment to standardize the compilation and flashing workflow for ESP32, with dependency management, version isolation, and support for multi-user collaborative development.

**Contact:** Khalil Ben Kalboussi

### 7.3 New platforms

#### SLICES

**Participants:** Nathalie Mitton, Solenne Fortun, Lucille Colin, Alexandre Veremme.

The FUN team is leading the deployment of the SLICES-FR research infrastructure, national node of the SLICES-RI ESFRI, also led by Inria and the FUN team. More details are available in [39]

### 7.4 Open data

We believe open software and open data collection or generation tools are mandatory in our research, to ensure reproducibility and repeatability. Therefore, we have built two main software tools. The first one relies on the SLICES/FIT IoT LAB open testbed and allows for the generation of network data. The second one allows for the collection of real communication traces. Both our tools are made available on open gitlab and the dataset either generated or collected are freely shared. A third dataset concerns the generation of data regarding hardware impairments in different reprogrammable devices, in order to develop RF fingerprinting on those devices and allowing the design of advanced authentication approaches. The software tools call to the enrichment of these datasets.

**Sisyphé.** The Sisyphé tool [40] relies on the SLICES/FIT IoT-Lab large scale testbed and state-of-the-art software engineering techniques to produce, collect and share artefacts and datasets in an automated way. This makes easy to track the impact of software updates or changes in the radio environment both on a small scale, e.g. during a single day, and on a large scale, e.g. during several weeks. By providing both the source code for the trace generation as well as the resulting datasets, we hope to reduce the learning curve to develop such applications and encourage reusability as well as pave the way for the replication of our results. While we focus in this work on IoT networks, we believe such an approach could be used in many other networking domains. All generated datasets and open software are available [here](#) and in [Zenodo](#). It has been then extended to include mobility in data generation. This extension is available [here](#).

**Participants:** Nathalie Mitton.

**PILOT.** Pilot dataset is a Privacy-preserving data collection tool of wireless communication technologies. The collected dataset is a collection of four jointly collected information in different mobility contexts. It includes three wireless communication technologies: WiFi probe-responses, BLE (Bluetooth Low Energy) beacons, and LoRa (Long Range Radio) packets, plus additional information: Acceleration, Roll, and Pitch, all collected at the same time. We provide the keys to reproduce such data collection and share the datasets already collected. The dataset is collected for approximately 90 hours, with a size of 200 MB using FiPy devices from Pycom and it is uploaded to GitHub. The dataset's utility is validated through the application of a classification machine learning model that determines the real-life situation of devices through the communication links monitored in different scenarios with an accuracy of 94%. Finally, we exploited this mobility status information to design an opportunistic routing protocol. Thus, we believe that such dataset is important for human mobility studies and applications of integrated sensing systems since it offers a new form of a classified collected data that does not exist in the already published datasets. All collected datasets and open software are available [here](#).

**Participants:** Nathalie Mitton.

**PLA.** We implemented a full stack to perform device authentication, independently of the wireless communication technology used. In fact, the authentication approach is based on the hardware impairment of the devices and how these impairments impact the signal generated by wireless. In particular, we induced a combination of three impairments, Carrier Frequency Offset (CFO), Direct Current Offset (DCO), and Phase Offset (PO). For that, we considered reprogrammable devices, in order to design more critical scenarios, with close signatures for devices, namely very similar impairments on the same models of devices. The general code as well as the data have been submitted for artefact evaluation in the context of the ACSAC 2024 conference, and the contribution received three badges, code available, code reviewed, and code reproducible [PLA-ACSAC](#).

**Participants:** Valeria Loscri, Ildi Alla.

## 8 New results

### 8.1 Wireless Network Security

**Participants:** Valeria Loscri, Selma Yahia, Ildi Alda, Jiali Xu, Aymen Bouferroum, Lucien Dikla Ngueleo.

As wireless ecosystems have grown more complex—with more IoT devices, remote work, and hybrid networks—security practices have also shifted toward stronger authentication, patching of firmware vulnerabilities, and deeper network monitoring, recognizing that even robust protocols need support from good operational security. Today's evolution reflects a move from basic encryption to more resilient, handshake-secure, and adaptive wireless security frameworks designed to meet modern threat landscapes. In this context, Physical Layer Security and cross-layer approaches combining PHY layer with protocols and upper layers is starting to gain momentum. The research contributions of the team related with wireless network security, are exactly developed at PHY and interactions among PHY and upper layer.

#### 8.1.1 Anomaly detection

Anomaly detection is a well studied problem since several years. However, it is still an important subject in modern wireless communication deployments, like 5G. In this context, to design solutions that are more

reliable, it is needed to leverage on reliable data. Data augmentation techniques show potential in various domains, yet their application to enhance robustness in wireless anomaly detection remains underexplored. Wireless datasets often suffer from anomaly scarcity and class imbalance, hindering the training of reliable detection models. This work introduces GANSec, a novel conditional Generative Adversarial Networks (GAN) framework specifically designed to augment wireless time-series data. We investigate different neural network architectures (MLP, LSTM, CNN) and two conditional training objectives (Embedded Conditional, Classification Oriented) within GANSec, evaluating the framework using real-world 5G measurements for jamming anomaly detection. For evaluation, we train the downstream anomaly detector exclusively on GANSec-generated data and test its performance in a cross-scenario setting. Our evaluation demonstrates that models trained this way significantly outperform those trained on original or baseline augmentation data when tested under unseen network conditions. Specifically, our approach achieved up to 92.13% accuracy on the unseen dataset (i.e., data collected from a different distribution reflecting network conditions distinct from the training set), compared to 78% for models trained on raw data and 83.33% for the best-performing baseline, exhibiting substantially enhanced robustness and generalization [33]

### 8.1.2 Drones detection

The increasing availability of drones and their potential for malicious activities pose significant privacy and security risks, necessitating fast and reliable detection in real-world environments. However, existing drone detection systems often struggle in real-world settings due to environmental noise and sensor limitations. This paper introduces TRIDENT, a tri-modal drone detection framework that integrates synchronized audio, visual, and RF data to enhance robustness and reduce dependence on individual sensors. TRIDENT introduces two fusion strategies—Late Fusion and GMU Fusion—to improve multi-modal integration while maintaining efficiency. The framework incorporates domain-specific feature extraction techniques alongside a specialized data augmentation pipeline that simulates real-world sensor degradation to improve generalization capabilities. A diverse multi-sensor dataset is collected in urban and non-urban environments under varying lighting conditions, ensuring comprehensive evaluation. Experimental results show that TRIDENT achieves 96.89% accuracy in real-world recordings and 83.26% in a more complex setting (augmented data), outperforming unimodal and dual-modal baselines. Moreover, TRIDENT operates in real-time, detecting drones in just 6.09 ms while consuming only 75.27 mJ per detection, making it highly efficient for resourceconstrained devices. The [dataset and code](#) have been released to ensure reproducibility [25, 9]

### 8.1.3 Jamming detection and Eavesdropping mitigation in heterogeneous wireless networks

Jamming remains a significant threat to the reliability and security of 5G networks, despite extensive investigation in the existing literature. This work addresses the scalability and robustness gaps found in previous approaches, introducing SHIELD—a scalable and holistic framework designed to evaluate jamming interference and support machine learning-based detection techniques without relying on costly external hardware. To validate our approach, we develop a realistic 5G testbed including a power-modulated jammer positioned between commercial off-the-shelf Android devices and an SDR-based radio access network. Our experimental results demonstrate that this jamming setup generates complex interference patterns that challenge detection methods proposed in prior work. We then propose a novel jamming detection methodology that, by synchronously collecting native logs from both the User Equipment (UE) and the Next-Generation Node B (gNB), captures a comprehensive view of network behavior in both normal and jammed states. SHIELD overcomes the shortcomings of existing detection methods—which typically fail under subtle, long-term interference—by employing a robust preprocessing pipeline that extracts multi-layer features through interpolation and sliding-window aggregation. We assess several lightweight yet accurate classifiers, including SVM, KNN, Gradient Boosting, and Random Forest, to determine detection performance across diverse real-world scenarios. Our evaluation shows that while current methods can achieve high accuracy—often exceeding 90%—in controlled scenarios, their performance can drop below 70% when exposed to varying conditions. In contrast, our proposed log-based framework maintains accuracy levels around 94% on unseen data, offering a scalable, cost-effective, and robust approach for large-scale 5G deployments [32, 31, 36].

The threat of power-modulated jammers to electronic systems has recently been reported in the literature. These are malicious devices that emit intentional electromagnetic interference whose power

changes rapidly over time. Such dynamic power emissions make it hard for traditional localization algorithms to track the jammer position in indoor environments, especially if the shadowing effects of the objects and people nearby the monitoring antennas are strong. In this work, we propose an indoor jammer localization strategy based on machine learning. The machine learning models are built from simulations based on the shooting-and-bouncing rays technique to quickly generate the required databases and provide a parametric study. The simulation model is validated by comparison with the measurement performed in a real room in the presence of a commercial jammer. Decision tree algorithms lead to predictions with an accuracy of tens of centimeters for a constant-power jammer and a power-modulated jammer. This result significantly outperforms conventional trilateration approaches. Furthermore, a new machine learning feature based on power ratios was introduced and provided good predictions even if the jamming power is unknown by the machine learning model. In addition, the main limitations are evaluated according to the uncertainties between measurement and simulations, the learning dataset size and changes in the considered environment. Finally, the proposed framework is validated using measurement as input of the machine learning models [11].

Concerning other types of wireless networks, as for example optical wireless networks. Providing secure optical wireless communication is a crucial challenge also in underwater scenarios, even though it has not been extensively investigated in the literature yet. In this paper, we propose a novel physical layer optical jamming scheme for underwater communications that, by leveraging signal reflection by mirror surfaces integrated with the reference transmitter (Alice), allows a reliable signal detection for a legitimate node while denying the transmission interception to potential eavesdroppers. Preliminary results demonstrate the proposed solution to effectively deny a reliable signal detection for an eavesdropper, while preserving the legitimate link integrity [27]

#### 8.1.4 Denial of service Vulnerabilities

With the rapid evolution of communication technologies, 5G networks promise to deliver a wide range of services and higher speeds. However, as these networks integrate into critical infrastructure, ensuring their security against malicious attacks is paramount. This paper focuses on a specific security vulnerability within the Next Generation Application Protocol (NGAP), which facilitates communication between Next-Generation Node B (gNB) and Access and Mobility Management Function (AMF) in the 5G Core Network (5GCN). Through an experimental study that draws on an open source testbed based on the latest Third Generation Partnership Project (3GPP) specifications, we identify and validate a Denial-of-Service (DoS) attack. The attack exploits the absence of mandatory security measures, such as IPSec, allowing a fake gNB to impersonate a legitimated one and inject malicious NGAP messages, causing unintended user disconnections. Although the study is conducted on an open source implementation, we discuss its broader implications, emphasizing how similar vulnerabilities could raise in commercial deployments due to operator-specific configurations and optional security controls in 3GPP standards. Mitigation strategies are proposed to address these risks, including enforcing mandatory security controls and improving gNB authentication mechanisms. This work highlights the need for stricter enforcement of security measures to safeguard the reliability of 5G networks [26]

## 8.2 Network servicing

**Participants:** Nathalie Mitton, Carol Habib, Alexandre Veremme.

In the last decade, edge computing emerged as a paradigm allowing close-to-the-source processing. It brings multiple benefits for mission-critical applications especially that they cannot tolerate delays, downtime or failure. Particularly, in post-disaster management, where the network is scarce and access to the Internet might not be possible, edge servers can be embarked on the robots that are exploring the disaster area transforming them to edge-enhanced devices. When required, they run resource-intensive tasks and provide local decisionmaking to other constrained devices in the disaster area such as a Wireless Sensor Network (WSN). The robots are battery-powered and are used for a mission-critical application where sensitivity and low tolerance for delays are crucial. Therefore, these edge-enhanced devices must be properly managed

to meet the needs of the application. In [22], a Fuzzy Inference System (FIS)-based approach is proposed enabling robots to decide, whenever a resource-intensive task must be executed, whether they can stop exploring the disaster area and act as edge servers. Six parameters reflecting the status of the network and the application are used by the FIS for the decisionmaking. Preliminary simulation results show that, in the proposed approach, the energy consumption in the network is 1.7 times less than the baseline network. This has been showcased in a demon [29].

### 8.3 Network deployment and exploration

**Participants:** Nathalie Mitton, Hazem Chaabi.

The wireless sensor networks are widely studied in the scientific literature due to their practical importance. They are used for monitoring and surveillance of strategic areas, and tracking targets in several fields, such as military, battlefields, health care, agriculture, and industry. Challenges in wireless sensor networks are related to localization, routing, limited storage, and deployment of sensors. In [10], we focus on deployment issues. While the main aim is to use the smallest number of sensors, a wireless sensor network has to ensure full coverage of the area of interest, collect the proper data, and guarantee that such data are available at a sink node, that plays the role of the central base station. We consider the problem of deploying the minimum number of sensors that are able to fully cover the area of interest, ensuring the connectivity of each sensor with the sink node. We propose a new formulation, based on both the set covering problem and the shortest paths problem from a single source to all destinations. The proposed model has been compared with the state-of-the-art considering instances inspired by the scientific literature. The numerical results highlight the superiority of the proposed formulation in terms of both efficiency and effectiveness.

Multi-Robot Systems (MRS) have become essential for autonomous missions in unknown or hazardous environments, notably in critical scenarios like search and rescue, where efficient mapping and robust communication are crucial. However, effectively balancing rapid exploration with reliable network connectivity remains challenging, especially for decentralized systems operating under dynamic conditions without centralized control. In the PhD thesis of Hazem Chaabi [34], we introduce a novel distributed multi-robot exploration algorithm, Dynamic Role-Based Exploration with Connectivity Maintenance (DRBECM) [18], specifically designed to address these challenges. The proposed algorithm utilizes decentralized decision-making based on local information sharing, enabling autonomous role assignment among robots without relying on global information or centralized oversight. Robots dynamically adopt either "explorer" roles, focusing on maximizing information gain through frontier-based strategies, or "supporter" roles, employing flocking-inspired positioning to sustain robust communication links across the team. Neighbor selection and connectivity maintenance are efficiently managed using the Relative Neighborhood Graph (RNG). To further enhance exploration efficiency under realistic communication constraints, we extend DRBECM into a machine learning-enhanced framework, Multi-Robot Exploration via Flocking Coordination and Machine Learning-Driven Connectivity Assessment (DRBECM-ML). DRBECM-ML [17] integrates distributed flocking dynamics with lightweight machine learning models, trained using real-world signal propagation data from the FIT-IoT-Lab testbed, to accurately predict Received Signal Strength Indicator (RSSI) values in real-time. These predictions significantly improve autonomous decision-making related to role-switching and frontier selection, ensuring stable and resilient communication networks throughout exploration tasks. Comparative evaluations indicate that tree-based algorithms, including Decision Trees and Extreme Gradient Boosting (XGBoost), offer optimal balance between prediction accuracy and computational efficiency suitable for deployment on mobile robots. Furthermore, this thesis investigates alternative communication strategies by comparing the performance of K-Nearest Neighbors (KNN) against the RNG for inter-robot communication, utilizing data generated via the Network Simulator 3 (NS-3) to analyze their effectiveness under various configurations [16]. Our simulation results consistently show significant improvements in exploration time and reduction in redundant exploration compared to baseline approaches, while effectively maintaining network connectivity. Ultimately, this work aims to provide robust, adaptable, and decentralized multi-robot system solutions suitable for deployment in complex, dynamic, and infrastructure-limited real-world scenarios.

## 8.4 V2X communications

**Participants:** Nathalie Mitton, Amira Mourad, Marwa Slimene.

The rise of connected vehicles has transformed transportation by enhancing mobility, safety, and driving comfort. However, ensuring secure and trustworthy communications in vehicular networks remains a challenge due to the risks of malicious activities, privacy breaches, and unauthorized access.

[12] aims to address these challenges by evaluating and comparing existing authentication schemes used in vehicular communications. Specifically, the article focuses on analyzing their efficiency, security, and applicability for audit systems in Vehicle-to-Everything (V2X) communications. The main objectives of this study are to provide a clear taxonomy of authentication strategies, evaluate their ability to preserve anonymity and integrity while ensuring accountability, and identify protocols suitable for robust audit mechanisms. Through qualitative and quantitative analysis, this paper highlights the strengths and limitations of current solutions, emphasizing aspects like scalability, privacy preservation, and infrastructure dependency. Findings indicate that combining Public Key Infrastructure (PKI)-based methods with Blockchain technology can yield secure and transparent communication solutions. Nevertheless, significant hurdles remain in scenarios lacking infrastructure support. The key contribution of this work consists in identifying authentication protocols that successfully balance security, efficiency, and privacy—while still enabling effective audits—thereby laying the groundwork for designing reliable, trust-oriented audit systems in tomorrow’s vehicular networks, including outside the infrastructure coverage.

The approach in [28] aims to allow vehicles to perform V2V authentication using locally stored data, in order to ensure continuity of secure communications even when disconnected from the Infrastructure. We further analyze the probability of successful authentication under two scenarios, which are the first with up-to-date databases, and the second with outdated ones. The analytical results show that the authentication probability decreases to below 75% after 30 hours of disconnection with long-lived certificates, while updates keep it above 90% in highway scenarios, even with short-lived certificates. These findings demonstrate the feasibility of maintaining reliable V2V authentication outside the infrastructure coverage, and point out the necessary improvements for evolving towards secure and auditable V2V communications.

Reliable intra-platoon communication is critical for safety-related message delivery within a platoon of connected and automated vehicles. However, the intra-platoon communication is challenged by packet collisions due to hidden nodes and merging collisions due to vehicle mobility. To address these challenges, [13] proposes a packet collision avoidance resource selection (PCA-RS) scheme to enhance the standardized SPS scheme. The proposed PCA-RS scheme introduces three enhancement mechanisms, which aims to alleviate merging collisions and hidden-node collisions in intra-platoon message delivery. A resource partition mechanism is introduced to divide frequency-time resources in a selection window into two sets in order for vehicles (both platoon and non-platoon vehicles) moving in opposite directions to select different frequency-time resources and thus avoid potential merging collisions; an intra-platoon cooperative mechanism is introduced to enable the leader of a platoon to know the resource occupation status on the hidden nodes of the platoon according to the messages received from the last platoon member of the same platoon and thus avoid potential hidden-node collisions; and a merging collision detection mechanism is introduced to enable a non-platoon vehicle to detect the status of the frequency-time resources it currently occupies after the non-platoon vehicle changes a lane and thus avoids potential merging collisions among non-platoon vehicles due to lane-change maneuvers. Simulation results demonstrate that compared with the standardized SPS scheme, the proposed PCA-RS scheme can improve the reliability of intra-platoon message delivery in terms of the intra-platoon packet delivery ratio.

## 8.5 Routing in wireless networks

**Participants:** Nathalie Mitton, Amira Mourad.

The development of delay tolerant networks (DTNs) has been driven by the need to overcome communication barriers in situations where traditional network assumptions do not apply. DTNs are designed

to function effectively in situations where traditional networks fail due to limited connectivity, extended delays, and recurrent disruptions. They are characterised by their ability to store and forward data, adapt to changing network conditions, and maintain communication even in the face of disruptions. They are typically decentralized, self-organizing and fault tolerant.

In [23, 24], we propose 'Baton-relay', a mobility context-aware routing protocol in DTN. This protocol relies on low-cost communication and storage devices that can embed different communication technologies, resulting in a global privacy-preserving data-sharing system based on natural crowd mobility. First, we analyse crowd mobility patterns to assign a delivery probability for a message based on its mobility pattern. The device will estimate its real-life situation, then exploits this information to take a forwarding decision. We tested and validated the approach using the ONE simulator, which is designed for an opportunistic network environment. The idea of Baton-relay is simple, not based on extensive mathematical calculations, does not require a huge memory or buffer, yet is robust, guaranteeing a reasonable probability of delivery and it preserves privacy. Results show that Baton-relay achieves a significant improvement for the buffer time average, number of hops and copies overhead compared to other routing protocols.

## 8.6 Cell-Free MIMO in Vehicular Networks: Resources Allocation and Security Vulnerabilities

**Participants:** Valeria Loscri, Selina Cheggour.

As 6G networks aim to meet the increasing demand for high data capacity and ultra-reliable, low-latency communication, cell-free massive Multiple-Input Multiple-Output (CFm-MIMO) systems emerge as a key technology by eliminating traditional cell boundaries and ensuring seamless coverage. However, a critical challenge arises when considering the frequency dimension in the channel and system model, specifically the need to address frequency selectivity and bandwidth sharing. These factors complicate resource allocation, particularly in dynamic environments like vehicular networks, where maintaining Quality of Service (QoS) becomes increasingly difficult. This paper tackles these issues by proposing a novel multi-user allocation strategy within shared subbands, designed to optimize spectral efficiency (SE), ensure fairness, and minimize interference under realtime user mobility conditions. To ensure practical and realistic performance evaluations, we base our analysis on real-world mobility patterns and channel characteristics derived from empirical data. A Simulated Annealing (SA) algorithm is employed to solve the multi-objective optimization problem, with comparisons made to Genetic Algorithm (GA) and Ant Colony Optimization (ACO). Our results show that the SA-based approach significantly improves SE and achieves up to 40% savings in frequency resources, providing a scalable and robust solution for frequency management in CFmMIMO systems, particularly for dynamic vehicular communication scenarios [19, 20, 35]. Machine learning (ML) models integrated into physical-layer functions in wireless systems are increasingly vulnerable to adversarial attacks. Although prior research has investigated such threats in conventional massive MIMO architectures, the security risks in future 6G topologies, particularly user-centric cell-free massive MIMO (UC-CFmMIMO) deployed in vehicular environments, remain largely unexplored. These architectures depend heavily on frequency-domain channel gain estimation, which opens new attack surfaces. In this work, we present a black-box adversarial framework tailored to UC-CFmMIMO networks operating in dynamic vehicular environments. The attacker passively collects RF data to train a surrogate model and crafts perturbations using the FGSM attack. A local anomaly detector is integrated to assess stealth prior to uplink injection via pilot contamination. Our method significantly disrupts channel gain estimation and subband allocation, while requiring no access to the target model's internals. These results underscore emerging vulnerabilities in ML-enabled wireless systems and highlight the need for robust, context-aware defenses. [21]

## 8.7 Localisation and fingerprinting approaches

**Participants:** Valeria Loscri, Ildi Alla.

As the spectrum becomes increasingly crowded, quick and reliable authentication of wireless devices is critical to avoid harmful interference to incumbents of the spectrum. Radio fingerprinting achieves fast waveform-level authentication by distinguishing devices based on unique hardware imperfections in the radio circuitry. However, existing approaches can fingerprint only one signal in a specific band, making them inapplicable in real-world scenarios where multiple signals coexist in spectrum bands. This paper introduces Multi-band Multi-device Radio Fingerprinting (M2RF) to address this challenge. Specifically, we propose a learning-driven segmentation algorithm to directly process in-phase/quadrature (I/Q) samples coming from the receiver and assign each I/Q sample to a specific radio. In contrast to existing approaches, M2RF simultaneously identifies and locates in the spectrum multiple devices that emit overlapping signals and avoids the burden of processing data, making the overall approach with reduced overhead and faster. Our approach can be generalized to different channels and signal bandwidths without retraining, making it scalable. Experiments in three different spectrum scenarios under 2 transmission conditions and with 15 radio transmitters demonstrate the effectiveness of M2RF, achieving up to 99.56% of F1-score, and 92.44% detection rate of malicious users with only a 2.72% mean Miss Rate (MR). Dataset and code will be shared for reproducibility and a (demo video) is available [37, 14]. To improve the robustness of wireless networks, in [15] we propose a novel fingerprinting method by applying the controlled non-linearities of RF amplifiers in compression mode to generate robust signal signatures. By analyzing the distinct distortion patterns and harmonic content produced under compression, we define a signaling mechanism helping to generate a robust fingerprinting mechanism. Our approach presents an ability to generate confusion in eavesdroppers so ensuring high robustness and resilience against passive and active attacks. Numerical results demonstrate the consistency and robustness of the signal signatures. This method not only enhances security by integrating physical-layer properties, but may contribute to reduce the computational burden of traditional cryptographic techniques. Our findings indicate that using amplifier non-linearities for fingerprinting significantly improves the security and efficiency of wireless communication systems.

## 9 Partnerships and cooperations

### 9.1 International initiatives

#### 9.1.1 Associate Teams in the framework of an Inria International Lab or in the framework of an Inria International Program

**Title:** Development of Physical Layer Security Tools in Cyber Physical Systems (DePhaSe-CPS)

**Partner Institution(s):** • CISPA, Germany

**Date/Duration:** 2025-2029

### 9.2 International research visitors

#### 9.2.1 Visits of international scientists

**Participant:** Megan Leroux

**Status:** intern (master/eng)

**Institution of origin:** Univ. of Stellenbosch

**Country:** South Africa

**Dates:** 20/01/2025 - 14/03/2025

**Context of the visit:** Megan visited us in the context of the follow up of our associated team with university of Stellenbosch and our common work on smart agronomy and more specifically on wireless sensor based jackal attack monitoring.

**Mobility program/type of mobility:** research stay

**Participant:** Samuel Kotva Goudoungou

**Status** PhD student

**Institution of origin:** Univ. of Ngaoundéré

**Country:** Cameroun

**Dates:** 23/09/2025 - 19/12/2025

**Context of the visit:** Samuel visited us in the context of the follow up of our collaboration with University of Ngaoundéré and common work on opportunistic data forwarding in infrastructureless areas.

**Mobility program/type of mobility:** research stay

**Participant:** Paul Dayang

**Status** Professor

**Institution of origin:** Univ. of Ngaoundéré

**Country:** Cameroun

**Dates:** 01/12/2025 - 05/12/2025

**Context of the visit:** Paul visited us in the context of the follow up of our collaboration with University of Ngaoundéré and supervision of the work of Samuel Kotwa.

**Mobility program/type of mobility:** research stay

### 9.3 European initiatives

#### 9.3.1 Horizon Europe

##### NEPHELE

**Participants:** Nathalie Mitton, Carol Habib, Alexandre Veremme, Hazem Chaabi.

[NEPHELE project on cordis.europa.eu](https://cordis.europa.eu/project/NEPHELE)

**Title:** A LIGHTWEIGHT SOFTWARE STACK AND SYNERGETIC META-ORCHESTRATION FRAMEWORK FOR THE NEXT GENERATION COMPUTE CONTINUUM

**Duration:** From September 1, 2022 to September 30, 2025

**Partners:**

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- UNIVERSITY OF MACEDONIA, Greece

- ECLIPSE FOUNDATION EUROPE GMBH (ECL), Germany
- INTERNET INSTITUTE, COMMUNICATIONS SOLUTIONS AND CONSULTING LTD (INTERNET INSTITUTE LTD), Slovenia
- ESAOTE SPA, Italy
- WINGS ICT SOLUTIONS TECHNOLOGIES PLIROFORIKIS KAI EPIKOINONION ANONYMI ETAIREIA (WINGS ICT SOLUTIONS AE), Greece
- ODIN SOLUTIONS SOCIEDAD LIMITADA (OdinS), Spain
- ETHNICON METSOVION POLYTECHNION (NATIONAL TECHNICAL UNIVERSITY OF ATHENS - NTUA), Greece
- SMILE, France
- ALTER WAY, France
- IBM IRELAND LIMITED, Ireland
- FUNDINGBOX ACCELERATOR SP ZOO (FBA), Poland
- LUKA KOPER, PORT AND LOGISTIC SYSTEM, D.D., Slovenia
- FUNDINGBOX COMMUNITIES SL (FBC), Spain
- ATOS IT SOLUTIONS AND SERVICES IBERIA SL (ATOS IT), Spain
- GEIE ERCIM (ERCIM), France
- CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI (CNIT), Italy
- ZURCHER HOCHSCHULE FUR ANGEWANDTE WISSENSCHAFTEN (ZHAW), Switzerland
- SIEMENS AKTIENGESELLSCHAFT, Germany

**Inria contact:** Nathalie Mitton

**Coordinator:** Symeon Papavassiliou

**Summary:** The vision of NEPHELE is to enable the efficient, reliable and secure end-to-end orchestration of hyper-distributed applications over programmable infrastructure that is spanning across the compute continuum from Cloud-to-Edge-to-IoT, removing existing openness and interoperability barriers in the convergence of IoT technologies against cloud and edge computing orchestration platforms, and introducing automation and decentralized intelligence mechanisms powered by 5G and distributed AI technologies.

## SLICES-PP

**Participants:** Nathalie Mitton, Solenne Fortun, Alexandre Veremme, Lucille Colin.

[SLICES-PP project on cordis.europa.eu](https://cordis.europa.eu/project/SLICES-PP)

**Title:** Scientific Large-scale Infrastructure for Computing/Communication Experimental Studies - Preparatory Phase

**Duration:** From September 1, 2022 to December 31, 2025

### Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- KUNGLIGA TEKNISKA HOEGSKOLAN (KTH), Sweden
- OULUN YLIOPISTO (UOULU), Finland

- THE PROVOST, FELLOWS, FOUNDATION SCHOLARS & THE OTHER MEMBERS OF BOARD, OF THE COLLEGE OF THE HOLY & UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN (TRINITY COLLEGE DUBLIN), Ireland
- UNIVERSITE DE GENEVE (UNIGE), Switzerland
- TECHNISCHE UNIVERSITAET MUENCHEN (TUM), Germany
- INTERUNIVERSITAIR MICRO-ELECTRONICA CENTRUM (IMEC), Belgium
- UCLAN CYPRUS LIMITED (UCLan Cyprus), Cyprus
- SIMULA RESEARCH LABORATORY AS, Norway
- INSTYTUT CHEMII BIOORGANICZNEJ POLSKIEJ AKADEMII NAUK, Poland
- INSTITUT MINES-TELECOM, France
- UNIVERSITE DU LUXEMBOURG (uni.lu), Luxembourg
- MANDAT INTERNATIONAL ALIAS FONDATION POUR LA COOPERATION INTERNATIONALE (MI), Switzerland
- CONSIGLIO NAZIONALE DELLE RICERCHE (CNR), Italy
- HUN-REN SZAMITASTECHNIKAI ES AUTOMATIZALASI KUTATOINTEZET (HUN-REN SZTAKI), Hungary
- EBOS TECHNOLOGIES LIMITED (eBOS), Cyprus
- EURECOM GIE (EURECOM), France
- PANEPISTIMIO THESSALIAS (UNIVERSITY OF THESSALY - UTH), Greece
- IOT LAB ASSOCIATION, Switzerland
- CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI (CNIT), Italy
- CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE CNRS (CNRS), France
- UNIVERSIDAD DEL PAIS VASCO/ EUSKAL HERRIKO UNIBERTSITATEA (UPV/EHU), Spain
- UNIVERSIDAD CARLOS III DE MADRID (UC3M), Spain
- UNIVERSITEIT VAN AMSTERDAM (UvA), Netherlands
- SORBONNE UNIVERSITE, France
- CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI), Italy

**Inria contact:** Nathalie Mitton

**Coordinator:**

**Summary:** The digital infrastructures research community continues to face numerous new challenges towards the design of the Next Generation Internet. This is an extremely complex ecosystem encompassing communication, networking, data-management and data-intelligence issues, supported by established and emerging technologies such as IoT, 5/6G, cloud-to-edge computing. Coupled with the enormous amount of data generated and exchanged over the network, this calls for incremental as well as radically new design paradigms. Experimentally-driven research is becoming worldwide a de-facto standard, which has to be supported by large-scale research infrastructures to make results trusted, repeatable and accessible to the research communities.

SLICES-RI (Research Infrastructure), which was recently included in the 2021 ESFRI roadmap, aims to answer these problems by building a large infrastructure needed for the experimental research on various aspects of distributed computing, networking, IoT and 5/6G networks. It will provide the resources needed to continuously design, experiment, operate and automate the full lifecycle management of digital infrastructures, data, applications, and services.

## MLSysOps

**Participants:** Valeria Loscri, Jiali Xu, Ildi Alla.

[MLSysOps project on cordis.europa.eu](https://cordis.europa.eu)

**Title:** Machine Learning for Autonomic System Operation in the Heterogeneous Edge-Cloud Continuum

**Duration:** From January 1, 2023 to January 31, 2026

### Partners:

- Augmenta Agriculture Technologies Monoprosopi Idiotiki Kefalaiouchikietaireia, Greece
- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- UNIVERSITY COLLEGE DUBLIN, NATIONAL UNIVERSITY OF IRELAND, DUBLIN (NUID UCD), Ireland
- NTT DATA ITALIA SPA, Italy
- MELLANOX TECHNOLOGIES LTD - MLNX (MELLANOX), Israel
- NUBIS IDIOTIKI KEFALAIOUCHIKI ETAIRIA (NUBIS P.C.), Greece
- ASSOCIACAO FRAUNHOFER PORTUGAL RESEARCH (FRAUNHOFER), Portugal
- PANEPISTIMIO THESSALIAS (UNIVERSITY OF THESSALY - UTH), Greece
- CHOCOLATE CLOUD APS (CHOCOLATE CLOUD), Denmark
- UBIWHERE LDA (Ubiwhere), Portugal
- UNIVERSITA DELLA CALABRIA (UNICAL), Italy
- TECHNISCHE UNIVERSITEIT DELFT (TU Delft), Netherlands

**Inria contact:** Valeria Loscri

**Coordinator:** University of THESSALY

**Summary:** MLSysOps will achieve substantial research contributions in the realm of AI-based system adaptation across the cloud-edge continuum by introducing advanced methods and tools to enable optimal system management and application deployment. MLSysOps will design, implement and evaluate a complete framework for autonomic end-to-end system management across the full cloud-edge continuum. MLSysOps will employ a hierarchical agent-based AI architecture to interface with the underlying resource management and application deployment/orchestration mechanisms of the continuum. Adaptivity will be achieved through continual ML model learning in conjunction with intelligent retraining concurrently to application execution, while openness and extensibility will be supported through explainable ML methods and an API for pluggable ML models. Flexible/efficient application execution on heterogeneous infrastructures and nodes will be enabled through innovative portable container-based technology. Energy efficiency, performance, low latency, efficient, resilient and trusted tier-less storage, cross-layer orchestration including resource-constrained devices, resilience to imperfections of physical networks, trust and security, are key elements of MLSysOps addressed using ML models. The framework architecture disassociates management from control and seamlessly interfaces with popular control frameworks for different layers of the continuum. The framework will be evaluated using research testbeds as well as two real-world application-specific testbeds in the domain of smart cities and smart agriculture, which will also be used to collect the system-level data necessary to train and validate the ML models, while realistic system simulators will be used to conduct scale-out experiments. The MLSysOps consortium is a balanced blend of academic/research and industry/SME partners, bringing together the necessary scientific and technological skills to ensure successful implementation and impact.

## UniMaaS

**Participants:** Nathalie Mitton, Carol Habib, Mo Ringbe Saynbe.

[UniMaaS project on cordis.europa.eu](https://cordis.europa.eu)

**Title:** Unified Modeling and Automated Scheduling for Manufacturing as a Service

**Duration:** From January 1, 2025 to December 31, 2027

### Partners:

- Institut National de Recherche en Informatique et Automatique (INRIA), France
- Catone Logistica S.R.L., Italy
- Odin Solutions Sociedad Limitada (OdinS), Spain
- Adient LTD LTD & CO KG, Germany
- Ethnicon Metsovion Polytechnion (NTUA), Greece
- Netcompany SA (INTRASOFT), Belgium
- Université catholique de Louvain (UCLouvain), Belgium
- Technische Universität Berlin (TUB), Germany
- Aeroporia Aigaiou Aninymi aeroporiki etaireia, Greece
- Queen's University of Belfast, United Kingdom
- Four dot infinity information and teelcommunications solutions private company, Greece
- Ecole de technologie Supérieure (ETS), Canada
- Cyberethics Lab, Italy
- Siec Badawcza Lukasiewicz - Przemyslowy Instytut Automatyki I Pomiarow Piap (LUKASIEWICZ - INSTYTUT PIAP), Poland
- Universitat Politecnica de Valencia (UPV), Spain
- ANV Production, Poland
- Flanders Make, Belgium
- Netcompany S.A., Luxembourg

**Inria contact:** Nathalie Mitton

### Coordinator:

**Summary:** Manufacturing in Europe should urgently address the following challenges towards the adoption of the Manufacturing as a Service paradigm: product customisation, circularity and sustainability, minimal downtime, predictive maintenance, seamless communication, reliability and robustness to uncertainties in demand and variability of resources, and cost reduction and performance optimisation. Unified Modeling and Automated Scheduling for Manufacturing as a Service (UniMaaS) project will develop a platform with a set of advanced technologies for offering flexible and decentralized manufacturing resources and supply chains as a Service to European SMEs and Industries.

### 9.3.2 Other european programs/initiatives

#### BeingWise

**Participants:** Valeria Loscri, Ildi Alla.

**Title:** Behavioral Next Generation in Wireless Networks for Cyber Security

**Duration:** October 2023 - September 2027

**Action Chair and Scientific Holder** Valeria Loscri

**Summary:** The always-connected world we are living in, gives us an unprecedented plethora of new advanced services and automated applications requiring, more and more, less human intervention due to the increased integration of Machine Learning (ML), Artificial Intelligence (AI) approaches and sophisticated emerging wireless technologies.

On the other side, this connected world opens new breaches and creates new potential vulnerabilities for smart advanced cyber-attacks, namely attacks and offender relying on ML/AI and advanced wireless technology integration, to make their attack more effective and less detectable. If an increasing awareness by the users could help to contrast the security issues, it is not sufficient against the new generation of cyber-attacks. In this context, a drastic paradigm shift, putting human-being in the loop for the conception of novel and more effective cyber-security solutions, must be considered.

Human-beings have a double role in the cyber-connected world: as potential offender and potential victim. The focus of BEiNG-WISE will be on how these different human-being features can be combined with the advanced technological characteristics, in order to conceive non-conventional, responsible by design, cyber-security solutions accounting for both these factors. In this complex connected system, another fundamental aspect that needs to be accounted to, is the legal one, related to the conception of solutions that can be effectively employed in the real world. Also, legal aspects should be considered at the design stage. The Action relies on cross-domains expertise, ranging from cybersecurity, wireless communication technology, data science, sociology, psychology and law.

### 9.4 National initiatives

#### BPI AutonomousPack

**Participants:** Khalil Ben Kalboussi, Carol Habib, Nathalie Mitton.

**Title:** ADEME AutonomousPack Project

**Duration:** September 2023 - August 2026

**Coordinator:** GoodFlow

**Inria contact:** Nathalie Mitton

**Summary:** The goal of the AUTONOMOUS PACK project is to push forward the achievements of the GoodFlow project by design a very energy efficient node to manage reusable packaging in a more sustainable way by combining enhanced IA techniques, wake up radio and multi MAC layers.

#### ANR NeMIoT

**Participants:** Valeria Loscri, Lucien Dikla Ngueleo.

**Title:** Detection and geolocation of an illegitimate electromagnetic source with AI

**Duration:** Jan. 2024 - Dec. 2028

**Coordinator:** Univ. Lyon 1

**Inria contact:** Valeria Loscri

**Summary:** NEMIoT aims at (i) designing a solid framework to model, analyse and forecast the actual behaviour of IoT devices when placed in an actual IP network infrastructure as well as their impact on the hosting network infrastructure itself and (ii) developing original cross-layer solutions to finely and quickly detect and/or mitigate potential anomalies resulting from the introduction of IoT devices. To do that, NEMIoT will provide the necessary analytical methods and tools, establish a step-by-step methodology thought to be automated, and demonstrate their efficiency on testbeds with real-life IoT devices.

#### FRAME-xG

**Participant:** Valeria Loscri.

**Title:** Optical Wireless Security (OptiWISE)

**Duration:** Jan. 2025 - Sept. 2025

**Inria contact:** Valeria Loscri OptiWISE is to support the further prototype development of an end-to-end optical wireless communication system, encompassing heterogeneous wireless technologies. Targeted end-users are in the military domain and for civil applications. Just as an example, based on different discussions had with different companies, it has been clear that wired fibre based communication cannot meet all the user requirements, above all when these requirements are dynamic, as in the case of high rise of the demand related for example to specific events as Olympic Games. In this context, the proposed solution can meet these dynamic needs, with similar performance of the wired version and reduced costs in respect of other potential concurrent solutions.

#### ANR OCOD

**Participants:** Nathalie Mitton, Kawtar Lasri, Christian Salim.

**Title:** Optimization of Data Acquisition via Terrestrial Nodes and Air Means, in Constrained Environment, and Application in Agriculture

**Duration:** Jan. 2025 - Dec. 2027

**Coordinator:** INRAe

**Inria contact:** Nathalie Mitton

**Summary:** OCOD aims to invent a new generation of data collection, combining smart wireless sensors and aerial means, and to test this approach in agriculture. The main objective is to use unmanned aerial vehicles (UAVs, commonly known as drones) as data mules to collect data from connected objects on the ground in natural environments. This aerial solution will facilitate data collection in natural environments that are difficult to access and may also suffer from signal attenuation with traditional communication networks. In this context, drones offer a wide geographical coverage area and are easier to deploy than mobile ground vehicles (e.g., land vehicles).

**SIRCAPASS, BPI**

**Participants:** Nathalie Mitton, Emi Dreckmeyr.

**Title:** Monitoring road infrastructure using passive sensors

**Duration:** June 2024 - June 2028

**Coordinator:** SilMach

**Summary:** This project aims to provide an operational response to the challenges associated with the preventive monitoring of bridges and the planning of their maintenance. SIRCAPASS will propose an innovation that breaks with current practices and concepts, based on the use of energy-free sensors.

**ROAD-AI, common DEFI Inria and Cerema**

**Participants:** Nathalie Mitton, Emi Dreckmeyr.

**Title:** Routes et ouvrages d'art Diversiformes, Augmentés et intégrés

**Duration:** July 2021 - June 2025

**Coordinator:** Nathalie Mitton

**Summary:** Integrated management of infrastructure assets is an approach which aims at reconciling long-term issues with short-term constraints and operational logic. The main objective is to enjoy more sustainable, safer and more resilient transport infrastructure through effective, efficient and responsible management. To achieve this, CEREMA and Inria are joining forces in this Inria Challenge (DEFI) which main goals are to overcome scientific and technical barriers that lead to the asset management of tomorrow for the benefit of road operators: (i) build a “digital twin” of the road and its environment at the scale of a complete network; (ii) define “laws” of pavement behavior; (iii) instrument system-wide bridges and tunnels and use the data in real time; (iv) define methods for strategic planning of investments and maintenance.

**9.5 PEPR**

The FUN team is involved in PEPR Networks of the future (PC6 and PC7), PEPR Cloud (PC8) and PEPR MobiDec (PC 3).

**PEPR Network of the Future - Just Enough Network**

**Participants:** Nathalie Mitton, Emile Egreteau-Druet.

**Title:** PEPR NoF JEN

**Duration:** 2023 - 2028

**Inria contact:** Nathalie Mitton

**Summary:** Jointly with the Inria AVALON team and the AIVANCITY school, Inria FUN investigates the full life cycle of IoT-based 5G Solutions for Smart Agriculture in order to design holistic system for data collection in agriculture that take account of the full environmental footprint.

### PEPR Network of the Future - FITNESS

**Participants:** Nathalie Mitton, Valeria Loscri, Aymen Salah Eddine Bouferroum, Marwa Slimene, Amira Mourad.

**Title:** PEPR NoF FITNESS

**Duration:** 2023 - 2028

**Inria contact:** Nathalie Mitton and Valeria Loscri

**Summary:** FUN collaborates in WP2 and WP8 of this project. In WP2, Industry 4.0, we consider Industrial internet of Things (IIoT) and investigate the security aspects related to the co-existence and interaction of different wireless communication technologies. In WP2, we investigate a whole hierarchical architecture, managing in an effective, energy-aware way trust model between resource-constrained and heterogeneous nodes. In WP3, we design a Collaborative Security and Remote Audit of V2X Communications, namely SCAR2X, aiming at a global security solution. [38]

### PEPR MobiDec

**Participants:** Nathalie Mitton, Amira Mourad.

**Title:** PEPR Mobidec DataFactory

**Duration:** 2023 - 2026

**Inria contact:** Nathalie Mitton

**Summary:** In collaboration with Inria TRIBE and COATI teams, we build an open source easy-to-use software tool able to collect and generate data traffic over different wireless network technologies and to infer some mobility characteristics from it.

### PEPR Cloud

**Participants:** Nathalie Mitton, Solenne Fortun, Lucille Colin.

**Title:** PEPR Cloud PC SILECS

**Duration:** 2024 - 2031

**Inria contact:** Nathalie Mitton

**Summary:** This project aims to build the research infrastructure to allow reproducible research in the full cIoT/edge/cloud continuum and contributes to the set up and deployment of SLICES-RI.

## 9.6 Regional Initiatives

### CORTESE

**Participants:** Valeria Loscri, Selma Yahia.

**Title:** CORTESE

**Duration:** January 2023 - April 2026

**Summary:** This project led by the Inria Lille - Nord Europe center and in partnership with the Gustave Eiffel University (UGE), the LAMIH (Université Polytechnique Hauts de France (UPHF)) aims at the coexistence of different wireless communication technologies, in the vehicular context. The objective is to advance in the search for methods based on sustainable Artificial Intelligence (AI) which can automate the selection of the most relevant communication technology to improve performance in terms of latency (i.e., of the order of 1 ms), reliability (i.e., of the order of 99.99% of data delivered) in order to reduce the energy envelope of the communication system and guarantee increased robustness in the face of cyber attacks. Given the high dynamicity of the environment, the learning approaches developed must be capable of responding in real time. Particular attention will be paid to the sustainability and security aspects of wireless communication networks. This project is part of the field of embedded Artificial Intelligence and the new emerging sector of cyber security for critical systems such as the vehicular context. With a clear experimental footprint, this project will advance research in the Hauts-de-France region in 5G technology in a key sector such as Intelligent Transport.

## 9.7 Public policy support

### ASGARd

**Participants:** Nathalie Mitton, Etienne Profit.

**Title:** Automatisation de la Surveillance des GALeries souterraines par Réseaux sans fil (ASGARd)

**Duration:** July 2024 - June 2025

**Summary:** Upon request of the city of Lille, the objective of this project is to study the implementation of a sustainable monitoring system that would enable continuous rather than sporadic monitoring, including in tunnels that are difficult to access. The aim is not to replace existing monitoring and prevention measures, but to provide automated tools for better risk anticipation.

### CCASIS

**Participants:** Nathalie Mitton, Damien Charabize, Alexandre Veremme, Saif Aziz Baig.

**Title:** Capteurs Chimiques Autonomes pour le Suivi Interne des Sépultures

**Duration:** September 2025 - August 2026

**Summary:** The CCASIS research project aims to design and deploy embedded funeral sensors, making it possible for the first time to monitor physicochemical parameters inside graves. To achieve this result, the project brings together the humanities and social sciences, chemistry, and computer science, automation, and electronics. The unprecedented data obtained through this interdisciplinary collaboration will provide insight into how buried bodies decompose, thereby addressing important scientific, health, and operational issues. The project is funded by the French Ministry of Culture and Communication, the French Ministry of Health, and the French Ministry of the Interior.

## 10 Dissemination

**Participants:** Valeria Loscri, Nathalie Mitton, Carol Habib, Kawtar Lasri, Amira Mourad, Marwa Slimene.

## **10.1 Promoting scientific activities**

### **10.1.1 Scientific events: organisation**

#### **General chair, scientific chair**

- Valeria Loscri is/was General Chair of IEEE LANMAN 2025
- Valeria Loscri is/was Executive Chair of IEEE CNS 2025
- Nathalie Mitton is/was general chair of IThings 2026 and PhD Forum chair of MSWIM 2026.

#### **Member of the organizing committees**

- Valeria Loscri is/was Tutorial Chair of IEEE CAMAD 2025
- Valeria Loscri was Panel Organizer and Moderator of "The industrial perspective of security and Trust aspects in 6G" in IEEE CNS 2025
- Valeria Loscri was Panel Organizer and Moderator of "The Security Aspects in 6G" at EuCNC and 6G Summit 2025
- Valeria Loscri co-organized the 1st INSEPTION- Interdisciplinary Aspects of Cybersecurity in conjunction with IEEE CNS
- Valeria Loscri was co-organizer of IEEE CyWiNet6'2025 Workshop

### **10.1.2 Scientific events: selection**

#### **Chair of conference program committees**

- Valeria Loscri is/was TPC Track Chair - Track 6: IoV, IoT, M2M of IEEE VTC-Spring 2025
- Valeria Loscri was TPC chair of MedComNet 2025
- Nathalie Mitton is/was co-TPC chair of ICIN 2025.

#### **Member of the conference program committees**

- Valeria Loscri has been a TPC member of PerCom 2025, ESORICS 2025, MASCOTS 2025, SECRIPT 2025.
- Nathalie Mitton has been a TPC member of DCOSS 2025, Percom 2025, CORES 2026.
- Carol Habib has been a TPC member of ICIN 2025 and MenaComm 2025.

### **10.1.3 Journal**

#### **Member of the editorial boards**

- Valeria Loscri is Associate Editor of IEEE Transactions on Information Forensics and Security (since 2022), IEEE Communications Survey and Tutorials (COMST, since 2020), Elsevier ComCom (since 2021), Frontiers in Communications and Networks, ITU-FET Journal, IEEE Transactions on Nanobioscience journal since 2017.
- Nathalie Mitton is an editorial board member of COM\_COM since 2025, Adhoc Networks since 2012, of IET-WSS since 2013, of Wireless Communications and Mobile Computing since 2016, of Journal of Interconnection Networks since 2021.

#### 10.1.4 Invited talks

- Valeria Loscri was Panel Member at the Panel « Evaluating progress and shaping the future of 6G research in Europe » in EuCNC 2025
- Valeria Loscri was Panel Member at the Panel « Valorisation et construction d'un écosystème » in Rencontres Sécurité Informatique et Sciences Humaines et Sociales, january 2025
- Valeria Loscri was invited speaker at the IEEE WMNC 2025 Conference.
- Valeria Loscri gave an invited talk to a 1) joint LINC/Sorbonne (Paris) workshop, 2) Journée Screaming channel & RF fingerprinting of the GDR Security, 3) NSSR Tech Trends NOKIA.
- Nathalie Mitton gave an invited talk at joint COST Action CA20120 INTERACT and PEPR-NF workshop.

#### 10.1.5 Scientific expertise

- Valeria Loscri is Scientific Chair of FWO Fundamental Research Committee Selection
- Valeria Loscri has been appointed as Expert Evaluator for European Project in the context of SNS-JU Programs.
- Valeria Loscri has been appointed as scientific expert evaluator for iTrans, for ANR Projects, for Projects from Czechoslovakia.
- Nathalie Mitton has been appointed as scientific expert to evaluate projects submitted to ANR, South Africa's National Research Foundation (NRF), NSERC (Canada) and NSC (Poland) Bourses L'Oréal FRANCE, Polish National Science Centre and BPI.
- Nathalie Mitton is an external expert of scientific board for Inrae, IRIT lab and ESISAR.

### 10.2 Teaching - Supervision - Juries - Educational and pedagogical outreach

#### 10.2.1 Teaching

- Master: Kawtar Lasri, Wireless networks, 16h eqTD (Master TC), Université de Lille, France
- Master: Kawtar Lasri, Wireless sensor networks, 16h eqTD (Master IdO), Université de Lille, France
- Master: Carol Habib, Smart objects, 10h CM + 12h TP, Ecole Centrale de Lille, France
- Master: Carol Habib, Industrial Internet of Things, 10h CM, Ecole Centrale de Lille, France
- Master: Amira Mourad, Internet of Things, 10h CM, IMT Nord Europe, France
- Master: Marwa Slimene, Internet of Things, 20h TD, IMT Nord Europe, France

#### 10.2.2 Supervision

- PhD defended:
  - Selina Cheggour, Cell-free approaches in wireless networks, Université Lille 1, 2022-2025, Valeria Loscri
  - Jiali Xu, anomaly and attack detection in intelligent, deep systems with heterogeneous, reprogrammable nodes, Université Lille 1, 2023-2025, Valeria Loscri
  - Hazem Chaabi, Adaptive deployment of a distributed wireless monitoring network and edge services using a fleet of wireless robots, Université Lille 1, 2022-2025, Nathalie Mitton
  - Ildi Alla, Monitoring for detection and localisation of cyber attacks in wireless networks, Université Lille 1, 2022-2025, Valeria Loscri

- PhD in progress:
  - Aymen Bouferroum, vulnerability detection, trust and authentication methods applied to multi-technology communication in Industrial IoT (IIoT), Univ. Lille, 2023-2026, Valeria Loscri
  - Marwa Slimene, Blockchain-based security and audit for IoT and V2X communications, Université Lille 1, 2023-2026, Nathalie Mitton
  - Lucien Dikla Ngueleo, Attack and anomaly detection in IoT, Université Lille 1, 2024-2027, Valeria Loscri and Kevin Jiokleng
  - Emile Egreteau-Druet, Analyzing full life cycle of IoT based 5G solutions for smart agriculture Mitton Nathalie, ENS Lyon, 2024-2027, Nathalie Mitton and Laurent Lefevre, Inria AVALON
  - Tatiana Al Jamous, Smart Grid management for university campus, Univ. Lille, 2024-2027, Nathalie Mitton, Carol Habib and Jad Nassar (Antonine Univ., Lebanon)
  - Mo Ringbe Saynbe, Smart IoT networks for sustainable manufacturing in Industry 4.0, Univ. Lille, 2025-2027, Nathalie Mitton, Carol Habib.
  - Emi Dreckmeyr, Data capture and collection by energy-free sensors and very low-power transmission in harsh environments, Université de Côte d'Azur, 2025, 2027, Nathalie Mitton and Christelle Caillouet.
  - Roxane Degas, Signal and attack detection infrastructure based on heterogeneous antennas in wireless networks, Univ. Lille, 2025-2028, Valeria Loscri

### 10.2.3 Juries

- PhD committees:
  - Valeria Loscri is/was member of the following PhD thesis committees:
    - \* Denis Donadel, University of Padova, chair
    - \* Gabriele Orazi, University of Padova, chair
    - \* Jiaxin Li, University of Padova, chair,
    - \* Nicola Drago, University of Padova, chair
    - \* Fatemeh STODT, Université de Strasbourg, reviewer
    - \* Tianwei Lan, Université Paris Cité, examiner
    - \* Asma ARAB, Université de Technologie de Compiègne Laboratoire Heudiasyc, examiner
    - \* Gurtaj Singh, University Mediterranea of Reggio Calabria, reviewer
    - \* Marco Loaiza, University of Calabria, reviewer
  - Nathalie Mitton is/was member of the following PhD thesis committees:
    - \* Hamza Kchok, Université Paris Saclay, chair
    - \* Mamadou NGOM, IMT Nord Europe, chair
    - \* Théotime Balaguer INSA Lyon, chair
    - \* Said Alvarado Marin, Sorbonne University, chair
    - \* Louis Closson, UGA, reviewer
    - \* Meroua Moussaoui, IMT Sud Paris, reviewer
    - \* Mohamed Abderrahmane Madani, IMT Nord Europe, chair
- HDR committees:
  - Valeria Loscri was a member of the following HDR committees:
    - \* Omar Sami OUBBATI, Université Gustave Eiffel, Paris-Est Sup, reviewer
    - \* Malisa VUCINIC, Université ENS PSL, Université Paris, reviewer
  - Nathalie Mitton was a member of the following HDR committees:
    - \* Pedro Braconnot Velloso, CNAM, reviewer

\* Nicola Accetura, LAAS, reviewer

- Research selection committees :
  - Valeria Loscri is/was member of the following selection committees:
    - \* Associate Professor, IMT Nord Europe
  - Nathalie Mitton was member of the following selection committees:
    - \* Inria researcher: chair of the junior researcher committee (CR) for Inria Bordeaux and member of Inria Senior researcher committee (DR2)

## 10.3 Popularization

### 10.3.1 Specific official responsibilities in science outreach structures

Valeria Loscri was Mentor for undergraduate students in the context of ElleStime.

### 10.3.2 Productions (articles, videos, podcasts, serious games, ...)

- Nathalie Mitton was one of the speakers in the EDIH GreenPower webinar on digital traceability.
- Valeria Loscri gave a BPI webinar on "Etat de l'art Cyberattaques dans les réseaux sans fils : quel impact, quels enjeux ?" and contributed to the Inria article on "Cybersecurity: malicious connected objects betrayed by their radio frequencies"

## 11 Scientific production

### 11.1 Major publications

- [1] I. Alla, S. Yahia and V. Loscri. 'TRIDENT: Tri-modal Real-time Intrusion Detection Engine for New Targets'. In: *Computers & Security* (15th May 2025). URL: <https://hal.science/hal-05441894>.
- [2] I. Alla, S. Yahia, V. Loscri and H. Eldeeb. 'Robust Device Authentication in Multi-Node Networks: ML-Assisted Hybrid PLA Exploiting Hardware Impairments'. In: Annual Computer Security Applications Conference (ACSAC). Waikiki, Hawaii, USA, United States, 13th Dec. 2024. URL: <https://hal.science/hal-04727491>.
- [3] E. Bout, V. Loscri and A. Gallais. 'HARPAGON: An energy management framework for attacks in IoT networks'. In: *IEEE Internet of Things Journal* (2nd May 2022). DOI: [10.1109/jiot.2022.3172849](https://doi.org/10.1109/jiot.2022.3172849). URL: <https://hal.science/hal-03658197>. In press.
- [4] H. Chaabi and N. Mitton. 'Multi-Robot Exploration via Flocking Coordination and Machine Learning-Driven Connectivity Assessment'. In: 2025 23rd International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt). Linköping, Sweden, May 2025. URL: <https://hal.science/hal-05055785>.
- [5] A. Hameed, J. Violos, N. Santi, A. Leivadreas and N. Mitton. 'FeD-TST: Federated Temporal Sparse Transformers for QoS prediction in Dynamic IoT Networks'. In: *IEEE Transactions on Network and Service Management* (8th Nov. 2024). DOI: [10.1109/TNSM.2024.3493758](https://doi.org/10.1109/TNSM.2024.3493758). URL: <https://hal.science/hal-04774861>.
- [6] J. Koteich and N. Mitton. 'Machine Learning Approach for Mobility Context Classification using Radio Beacons'. In: *Proc of 31st International Symposium on the Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*. MASCOTS2023 IEEE. New York, United States, 16th Oct. 2023. URL: <https://hal.science/hal-04208815>.
- [7] N. Mitton, Y. Saleem, V. Loscri and C. Bureau. 'Adaptive HELLO Protocol for Vehicular Networks'. In: *ITU Journal on Future and Evolving Technologies* (2024). URL: <https://inria.hal.science/hal-04459157>.

- [8] B. Wang, J. Zheng and N. Mitton. ‘A Packet Collision Avoidance Resource Selection Scheme for Reliable Intra-Platoon Message Delivery in a C-V2X network’. In: *IEEE Transactions on Vehicular Technology* (2025). DOI: [10.1109/TVT.2025.3544826](https://doi.org/10.1109/TVT.2025.3544826). URL: <https://hal.science/hal-04904559>.

## 11.2 Publications of the year

### International journals

- [9] I. Alla, S. Yahia and V. Loscri. ‘TRIDENT: Tri-modal Real-time Intrusion Detection Engine for New Targets’. In: *Computers & Security* (15th May 2025). URL: <https://hal.science/hal-05441894> (cit. on p. 15).
- [10] L. Di Puglia Pugliese, F. Guerriero and N. Mitton. ‘Optimizing wireless sensor networks deployment with coverage and connectivity requirements’. In: *Annals of Operations Research* 346 (23rd Jan. 2025), pp. 1997–2008. DOI: [10.1007/s10479-025-06487-x](https://doi.org/10.1007/s10479-025-06487-x). URL: <https://hal.science/hal-05021385> (cit. on p. 17).
- [11] P. Monferran, A. Costanzo, A. N. d. S. José, V. Deniau, J. Villain, V. Loscri and C. Gransart. ‘Indoor 1D-Localization of Omnidirectional Power-Modulated Jammers: a Machine Learning Approach with Rapid Database Generation’. In: *IEEE Transactions on Electromagnetic Compatibility* (8th Dec. 2025). DOI: [10.1109/TEMC.2025.3637711](https://doi.org/10.1109/TEMC.2025.3637711). URL: <https://hal.science/hal-05408174> (cit. on p. 16).
- [12] M. Slimene, A. Chriki, N. Mitton, P. Sondi and A. Meddahi. ‘A Comparative Survey of Authentication Schemes Suitable for the Audit of V2X Communications’. In: *IEEE Transactions on Intelligent Transportation Systems* 26.11 (12th Nov. 2025), pp. 18304–18324. DOI: [10.1109/TITS.2025.3603250](https://doi.org/10.1109/TITS.2025.3603250). URL: <https://hal.science/hal-05247525> (cit. on p. 18).
- [13] B. Wang, J. Zheng and N. Mitton. ‘A Packet Collision Avoidance Resource Selection Scheme for Reliable Intra-Platoon Message Delivery in a C-V2X network’. In: *IEEE Transactions on Vehicular Technology* (2025). DOI: [10.1109/TVT.2025.3544826](https://doi.org/10.1109/TVT.2025.3544826). URL: <https://hal.science/hal-04904559> (cit. on p. 18).

### International peer-reviewed conferences

- [14] I. Alla and V. Loscri. ‘Sec5GLoc: Securing 5G Indoor Localization via Adversary-Resilient Deep Learning Architecture’. In: 13th IEEE Conference on Communications and Network Security - CNS 2025. Avignon, France, 8th Sept. 2025, pp. 1–9. DOI: [10.1109/cns66487.2025.11194175](https://doi.org/10.1109/cns66487.2025.11194175). URL: <https://hal.science/hal-05441877> (cit. on p. 20).
- [15] M. Biagi and V. Loscri. ‘A Robust Fingerprinting Mechanism based on Amplifier non Linearities’. In: European Conference on Networks and Communications (EUCNC) - 6G SUMMIT 2025. Poznan, Poland, 3rd June 2025. URL: <https://hal.science/hal-05045767> (cit. on p. 20).
- [16] H. Chaabi and N. Mitton. ‘Comparative Analysis of KNN, RNG and K-RNG for Inter-Robot Communication’. In: The 18th International Workshop on Selected Topics in Wireless and Mobile computing (STWiMob 2025). Marrakech (Maroc), Morocco, 2025. URL: <https://hal.science/hal-05239453> (cit. on p. 17).
- [17] H. Chaabi and N. Mitton. ‘Distributed Multi-Robot Exploration Approach With Connectivity Maintenance’. In: DCOSS-IoT 2025 - 21st Annual International Conference on Distributed Computing in Smart Systems and the Internet of Things. Lucca, Italy, 9th June 2025. URL: <https://hal.science/hal-05057323> (cit. on p. 17).
- [18] H. Chaabi and N. Mitton. ‘Multi-Robot Exploration via Flocking Coordination and Machine Learning-Driven Connectivity Assessment’. In: 2025 23rd International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt). Linköping, Sweden, May 2025. URL: <https://hal.science/hal-05055785> (cit. on p. 17).
- [19] S. Cheggour and V. Loscri. ‘Frequency Channel Selectivity in Vehicular CFmMIMO Systems: a Multi-Objective Optimization Approach’. In: VNC 2025 - IEEE Vehicular Networking Conference. Porto, Portugal, 2nd June 2025. URL: <https://hal.science/hal-05011230> (cit. on p. 19).

- [20] S. Cheggour, E. P. Simon and V. Loscri. ‘Advanced Resource Management in Cell-Free Massive MIMO Systems with WINNER II Channels’. In: LANMAN 2025 - IEEE International Symposium on Local and Metropolitan Area Networks. Lille, France, 7th July 2025. URL: <https://hal.science/hal-05062956> (cit. on p. 19).
- [21] M. Ghorbel, S. Cheggour, V. Loscri, Y. Imine, H. Ouarnoughi and S. Niar. ‘Machine Learning Vulnerabilities in 6G: Adversarial Attacks and Their Impact on Channel Gain Prediction and Resource Allocation in UC-CFmMIMO’. In: 30th European Symposium on Research in Computer Security (ESORICS) 2025. Toulouse, France, 22nd Sept. 2025. URL: <https://hal.science/hal-05127853> (cit. on p. 19).
- [22] C. Habib and N. Mitton. ‘A fuzzy based approach for managing smart edge-enhanced IoT devices in mission-critical applications’. In: 28th Conference on Innovation in Clouds, Internet and Networks. Paris, France, 11th Mar. 2025. URL: <https://hal.science/hal-04946021> (cit. on p. 17).
- [23] J. Koteich, N. Mitton and R. Wolhuter. ‘Mobility Context Aware Routing Protocol in DTN’. In: 39th International Conference on Information Networking (ICOIN). Chang Mai, Thailand, 15th Jan. 2025. URL: <https://inria.hal.science/hal-04817572> (cit. on p. 19).
- [24] J. Koteich, N. Mitton and R. Wolhuter. ‘Mobility Context Aware Routing Protocol in DTN’. In: CORES 2025 - 10èmes Rencontres Francophones sur la Conception de Protocoles, l’Evaluation de Performances et l’Expérimentation des Réseaux de Communication. CORES 2025 - 10èmes Rencontres Francophones sur la Conception de Protocoles, l’Evaluation de Performances et l’Expérimentation des Réseaux de Communication. Saint Valery-sur-Somme, France, 2nd June 2025. URL: <https://hal.science/hal-05001173> (cit. on p. 19).
- [25] N. Merabtine, V. Loscri, D. Djenouri and S. Latif. ‘A Novel Hybrid Framework for Realistic UAV Detection using a Mixed RF Signal Database’. In: IEEE Future Networks - FNWF. FNWF 2024 - IEEE Future Networks World Forum. Dubai, United Arab Emirates, Jan. 2025. URL: <https://hal.science/hal-04702908> (cit. on p. 15).
- [26] A. Moheddine and V. Loscri. ‘Identifying and Exploiting a Denial-of-Service Vulnerability in the NGAP Protocol in 5G Networks’. In: European Conference on Networks and Communications 2025 EuCNC & 6G Summit. Poznan, Poland, 2025. URL: <https://hal.science/hal-05018484> (cit. on p. 16).
- [27] A. Petroni, M. Shoaib, V. Loscri and M. Biagi. ‘A Mirror-based Jamming Scheme against Eavesdropping in Underwater Optical Communication’. In: OCEANS 2025 Conference and Exposition. Brest, France, 16th June 2025. URL: <https://hal.science/hal-05113095> (cit. on p. 16).
- [28] M. Slimene, N. Mitton, P. Sondi and A. Meddahi. ‘An enhanced authentication solution for infrastructureless vehicle environments’. In: WiMob 2025. Marrakech (Morocco), Morocco, 20th Oct. 2025. URL: <https://inria.hal.science/hal-05263522> (cit. on p. 18).
- [29] A. Veremme, C. Habib and N. Mitton. ‘Demo : Dynamic Management of Wireless Sensor Networks using Virtual Objects and a Rule Engine’. In: 28th Conference on Innovation in Clouds, Internet and Networks. Paris, France, 11th Mar. 2025. URL: <https://hal.science/hal-04946062> (cit. on p. 17).
- [30] S. Wang, A. Brighente, V. Loscri, J. Zhang and M. Conti. ‘Capodoglio: Tackling Multi-Armed Bandit Jamming Attacks’. In: IEEE Data S&P 2025 International Workshop on Data Security and Privacy. Guizhou, China, Nov. 2025. URL: <https://hal.science/hal-05457264>.
- [31] J. Xu and V. Loscri. ‘Leveraging UE-Level Collaborative Intelligence for Scalable Jamming Detection in 5G Networks’. In: IEEE DCOSS-IoT 2025 (Workshop on Distributed COLlective Intelligence). Lucca, Italy, 9th June 2025. URL: <https://hal.science/hal-05055815> (cit. on p. 15).
- [32] J. Xu, A. Moheddine, V. Loscri, A. Brighente and M. Conti. ‘SHIELD: Scalable and Holistic Evaluation Framework for ML-Based 5G Jamming Detection’. In: 20th International Conference on Availability, Reliability and Security (ARES). Ghent (BE), Belgium, 11th Aug. 2025. URL: <https://hal.science/hal-05055784> (cit. on p. 15).

- [33] J. Xu, S. Wang, V. Loscri, A. Brighente, M. Conti and R. Rouvoy. ‘GANSec: Enhancing Supervised Wireless Anomaly Detection Robustness through Tailored Conditional GAN Augmentation’. In: ESORICS 2025 - 30th European Symposium on Research in Computer Security. Toulouse, France, 22nd Sept. 2025. URL: <https://hal.science/hal-05137717> (cit. on p. 15).

#### Doctoral dissertations and habilitation theses

- [34] H. Chaabi. ‘Distributed Multi-Robot Exploration With Connectivity Maintenance Under QoS Constraints’. Université de Lille, 17th Nov. 2025. URL: <https://hal.science/tel-05379346> (cit. on p. 17).
- [35] S. Cheggour. ‘Energy-efficient and intelligent 5G massive MIMO solutions based on machine learning for vehicular communications’. Université de Lille 1 - Sciences et Technologies, 26th Sept. 2025. URL: <https://hal.science/tel-05424510> (cit. on p. 19).
- [36] J. Xu. ‘Characterisation of Anomalous Behaviour for Security in Deep-Edge Wireless Systems: Applied Machine Learning From On-Device Jamming Detection to Collaborative Intelligence’. Lille University; Inria Lille, 3rd Dec. 2025. URL: <https://hal.science/tel-05420774> (cit. on p. 15).

#### Reports & preprints

- [37] I. Alla, M. Zhang, J. Ashdown, V. Loscri and F. Restuccia. *Finding a Needle in a (Spectrum) Haystack: Multi-Band Multi-Device Radio Fingerprinting*. 14th Sept. 2025. URL: <https://hal.science/hal-05253332> (cit. on p. 20).

#### Other scientific publications

- [38] N. Cassiau, N. Achir, C. Adjih, G. Andrieux, W. Bechkit, S. Ben Hadj Said, O. Boissier, A. Bouferroum, R. Combes, F. Courrèges, H. Dakdouk, A. Dhaouadi, J.-F. Diouris, S. E. Elayoubi, J. Härrri, M. Kassi, X. Lagrange, Y. Liu, V. Loscri, V. Mannoni, S. Maudet, N. Mitton, A. Mokdad, E. Moulay, A. Nadar, R. Nahon, R. Négrier, v. T. Nguyen, A. Pelov, C. Perrine, M. Pierre, S. Pillement, A. Pottier, C. Poulliat, Y. Pousset, M. Rady, N. Sboui, P. Sondi and L. Toutain. *Overcoming the Technical Hurdles of IoT Adoption: the FITNESS Project Vision and Insights*. 15th Sept. 2025. DOI: [10.5281/zenodo.17119689](https://doi.org/10.5281/zenodo.17119689). URL: <https://hal.science/hal-05257163> (cit. on p. 29).

#### Scientific popularization

- [39] S. Fortun, N. Mitton and C. Pérez. ‘Experiment. Innovate. Transform. The future of digital infrastructure starts with SLICES.’ In: *Innovation Platform 24* (Dec. 2025), pp. 16–24. URL: <https://hal.science/hal-05409390> (cit. on p. 13).

### 11.3 Cited publications

- [40] N. Santi, R. Grünblatt, B. Foubert, A. Hameed, J. Violos, A. Leivadeas and N. Mitton. ‘Automated and Reproducible Application Traces Generation for IoT Applications’. In: *Q2SWinet 2021 - 17th ACM Symposium on QoS and Security for Wireless and Mobile Networks*. Alicante, Spain: ACM, Nov. 2021, pp. 1–8. DOI: [10.1145/3479242.3487321](https://doi.org/10.1145/3479242.3487321). URL: <https://hal.science/hal-03390693> (cit. on p. 13).