2023
ACTIVITY REPORT

Project-Team

AIO

Dependable Networking, Low-Power Wireless and Micro-Robotics

DOMAIN

**Networks, Systems and Services,
Distributed Computing**

THEME

Networks and Telecommunications

Inria

Contents

Project-Team AIO

Creation of the Project-Team: 2022 March 01

Keywords

Computer sciences and digital sciences

A1.2.3. – Routing

A1.2.4. – QoS, performance evaluation

A1.2.5. – Internet of things

A1.2.6. – Sensor networks

A1.2.7. – Cyber-physical systems

A1.2.8. – Network security

A2.3. – Embedded and cyber-physical systems

A2.3.1. – Embedded systems

A2.3.2. – Cyber-physical systems

A2.3.3. – Real-time systems

A4.5. – Formal methods for security

A4.6. – Authentication

A4.7. – Access control

A5.10.1. – Design

A5.10.3. – Planning

A5.10.5. – Robot interaction (with the environment, humans, other robots)

A5.10.6. – Swarm robotics

A9.5. – Robotics

A9.9. – Distributed AI, Multi-agent

Other research topics and application domains

B3.3.1. – Earth and subsoil

B3.5. – Agronomy

B4.5.2. – Embedded sensors consumption

B5.1. – Factory of the future

B5.4. – Microelectronics

B5.6. – Robotic systems

B6.2.2. – Radio technology

B6.2.3. – Satellite technology

B6.4. – Internet of things

B6.6. – Embedded systems

B6.7. – Computer Industry (harware, equipments...)

B8.1. – Smart building/home

B8.1.2. – Sensor networks for smart buildings

B9.1.2. – Serious games

1   Team members, visitors, external collaborators

Research Scientists

- Thomas Watteyne [Team leader, INRIA, Senior Researcher, HDR]

- Filip Maksimovic [INRIA, Starting Research Position]

- Paul Mühlethaler [INRIA, Senior Researcher, HDR]

- Malisa Vucinic [INRIA, ISFP]

Faculty Member

- Branko Kerkez [University of Michigan, Professor, Inria International Chair]

PhD Students

- Razane Abu-Aisheh [INRIA, until Feb 2023]

- Said Alvarado Marin [INRIA]

- Martina Maria Balbi Antunes [ANALOG DEVICES, CIFRE]

- Kaouther Benguessoum [Gabes University - Tunisia]

- Sara Faour [INRIA]

- Fabian Graf [SIEMENS]

- Abdelhak Hidouri [Gabes University - Tunisia]

- Tayssir Ismail [Gabes University - Tunisia]

- Elsa Lopez Perez [INRIA, from Nov 2023]

- Felix Marcoccia [THALES]

- Trifun Savic [WATTSON ELEMENTS, until Sep 2023]

- Yuxuan Song [INRIA, from Oct 2023]

Technical Staff

- Alexandre Abadie [Inria, Engineer]

- Romain Facq [INRIA, Engineer]

- Geovane Fedrecheski [INRIA, from Apr 2023]

- Ichrak Kallala [INRIA, Engineer, from Apr 2023]

Interns and Apprentices

- Raul De La Fuente Armijo [INRIA, Intern, until Apr 2023]

- Marion Seychelles [INRIA, Intern, from May 2023 until Aug 2023]

- Fabrice Sivakumar [INRIA, Intern, from Jun 2023 until Jul 2023]

Administrative Assistants

- Anne Mathurin [INRIA]

- Clotilde Monnet [Inria, from Feb 2023, Project Manager, Horizon Europe OpenSwarm]

Visiting Scientists

- Ruben Milocco [UNIV NACIONAL DEL COMAHUE, from May 2023 until Jun 2023]

- Leila Saidane [National School of Computer Science (ENSI), until Nov 2023]

External Collaborators

- Soumya Banerjee [UCC CORK, until Dec 2023]

- Éric Renault [ESIEE]

- Trifun Savic [WATTSON ELEMENTS, from Oct 2023]

2 Overall objectives

The AIO team is a leading research team in low-power wireless communications. The team is designing Tomorrow's Internet of (Important) Things. It pushes the limits of low-power wireless mesh networking by applying them to critical applications such as robotics, industrial control loops, with harsh reliability, scalability, security and energy constraints. The AIO team co-chairs the IETF 6TiSCH and IETF LAKE standardization working group and co-leads Berkeley's OpenWSN project. It is heavily involved in real-world applications, and oversees over 1,000 sensors deployed on 3 continents for smart agriculture, smart city and environmental monitoring applications. The team's research program is organized around 5 pilars: Smart Dust, Low-Power Wireless Networking, Security in Constrained Systems, Swarm Robotics and Vehicle Area Networking. The team is associated with Prof. Pister's team at UC Berkeley, working on Smart Dust.

3 Research program

The team's research program is composed of five areas of research, which we number A1 through A5. Please note that the order of the areas does *not* represent any sort of order of importance, or dependence.

3.1 [A1] Smart Dust

SCuM ("Single Chip Micro Mote"), depicted in Fig. 1, is the world's first crystal-free micro-mote which implements a full IEEE802.15.4 and BLE radio. It uses oscillating circuits with a 16,000 ppm drift and which are very sensitive to temperature, instead of a traditional crystal oscillator (<40 ppm drift). This clock source is responsible for choosing communication frequency and modulation rate. This crystal-free approach reduces the size of the mote significantly, and will be widely adopted by the industry. While we conduct our research on SCuM, it is representative, and results carry over to other designs. We have shown anecdotally that we can manually calibrate the oscillators and have SCuM communicate with an off-the-shelf IEEE802.15.4-compliant mote. *Can we create an algorithm which continuously self-calibrates the clocks on SCuM so it keeps communicating even when the temperature changes?* The tools we have to answer that questions are Machine Learning and Control Theory. *Can we use Machine Learning to create a static model to tune the clocks? Can we then use Control Theory to augment this into a model that dynamically tracks the clock of a neighbor node, and keeps SCuM communicating even when temperature changes?* Answering these questions leads us to implementing these solutions onto SCuM and making sure two nearby SCuM motes can communicate.

This area of research is further divided into two strands.
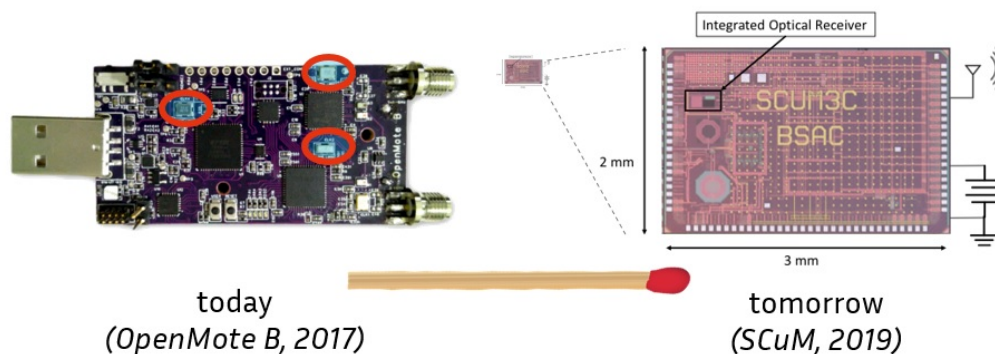
Figure 1: SCuM ("Single Chip Micro Mote") is the world's first crystal-free micro-mote which implements a full IEEE802.15.4 and BLE radio

[A1.1] Fast Calibration and Standardization

The behavior of the oscillators within the SCuM chip is not fully understood. We have shown in [69] that the oscillators drift by up to 16,000 ppm over temperature. This is much more than the maximum 40 ppm required by the IEEE 802.15.4 standards. The challenge is hence to turn an unstable 16,000 ppm oscillator into a stable 40 ppm oscillator so SCuM chips can reliably communicate with off-the-shelf IEEE 802.15.4 and BLE transceivers, and with other SCuM chips. This may be done in the following steps:

- The first question to answer is: *can we model the behavior of these oscillators?* Specifically, we want to know how much of the variation of these oscillators is a function of temperature, voltage or other parameters, and how much is due to thermal noise, i.e. a random variation which cannot be controlled. A secondary goal is to turn these lessons learnt into the simplest possible model (e.g. some form of a decision tree) so it can be implemented on individual SCuM chips. We know that simple curve fitting on 2-point of 3-point calibration over temperature is usually done for crystal-oscillators, but this will most likely not work here. We adopt the approach of Oroza [57] and use Machine Learning to answer both questions. Random Forest, LDA or PCA indicate the contribution of each feature to the overall model. One preliminary step is hence to gather a more complete and more annotated dataset as in [69]. We may reach out to the `scikit-learn` team, as well as Prof. Carlos Oroza from the University of Utah with whom we have been collaborating on ML approaches for wireless communication systems.

- There is a good possibility that the model from the study above is *not* able to fully characterize drift in all cases. *Do we need reinforcement learning to allow micro-motes to calibrate against regular motes?* In practice, we use motes from our OpenTestbed [54] as a "calibration box": they are programmed to listen on all frequencies, and acknowledge any calibration probe frames they receive. The goal is to create an algorithm by which a micro-mote transmits such probes as it sweeps through calibration settings until it receives an acknowledgement and thereby knows that setting is valid for a particular frequency. The challenge is that tuning the oscillators needs to happen continuously, as any temperature change will cause SCuM to lose connectivity to the calibration box. If reinforcement learning is needed, similar to our approach in [54], one option is to use game theory to model as a "Multi-Armed Bandit", and use an ϵ-greedy algorithm to balance using the tuning parameters that worked in the past, and exploring other parameters in case the temperature has changed. The target is for uncalibrated micro-motes to self-calibrate quickly, and stay calibrated as temperature changes.

- The study above results in a protocol between a micro-mote and the calibration box. We propose this as a candidate for standardization at the IETF, possibly in the 6TiSCH working group.

Results: From a scientific point of view, A1.1 generates the world's largest open and annotated dataset of micro-mote drift, and use Machine Learning to derive a model. In case that drift model does

not capture the drift fully and hence cannot ensure a micro-mote can always communicate, A1.1 also develops a dynamic fast calibration protocol against regular motes using game theory, and standardize that protocol. From a project point of view, A1.1 allows micro-motes to communicate, albeit with the help of regular motes, a necessary stepping stone for the remainder of the project.

[A1.2] The Network as a Time Source

A1.1 allows micro-motes to communicate, but does require having regular motes close to micro-motes, which puts a burden on the deployment strategy. The goal of this area is bold and ambitious: *can a micro-mote use the network as a relative time reference, instead of an absolute time reference such as a crystal oscillator?* This entails having a micro-mote calibrate against another micro-mote – which itself is drifting – and repeating this over a multi-hop network of micro-robots.

This goal translates into the following three studies:

- The challenge is that both neighbor nodes drift: if we were to use the approach from A1.1, neighbor nodes would lose connection. The question is: *can we develop a fast-tracking algorithm which allows micro-motes to calibrate against one another?* For that, we can use control theory: consider the time offset between two micro-motes as the variable, offset 0 as equilibrium, and tune the clock calibration. Similar to our approach in [35], we can use a PID controller to balance reactivity with resilience to short timing glitches. We can develop the controller in simulation by replaying its behavior against the datasets from A1.1, before implementing it on micro-motes and validating experimentally.

- In a scenario in which the micro-robots form a multi-hop mesh network, we want to avoid forming cliques of synchronized structures, given the important variation in drift between nodes. The question becomes: *can we have a micro-mote calibrate against multiple neighbors at the same time?* The complexity is that these neighbors can be far apart in time, so the micro-mote may need to "jump" in time depending on which neighbor it is communicating with, while implementing some averaging function that causes the network to eventually converge to a fully-synchronized state. We build upon the work published in [70] by integrating the datasets from A1.1 into the 6TiSCH simulator, and expand the controller from the study above to support multiple neighbors.

- All TSCH networks, including 6TiSCH, build a synchronization structure inside a multi-hop mesh network rooted at a single time master, which never changes. This does not match the micro-robot application, in which all micro-robots play a similar role. The question is hence: *can we build a TSCH network in which the role of time master changes from one micro-mote to another, without any disruption to the network?* A corollary question is: *can we imagine having multiple time masters, for example nodes equipped with crystals?* We will use our previous work on the flooding-based approach from [38], and standardize the behavioral/protocol changes through IETF 6TiSCH.

Results: From a scientific point of view, A1.2 results in deep changes to the base behavior of a TSCH protocol stack such as 6TiSCH, with a radically new way of tracking a time source neighbor, based on control theory, as well as the ability to track multiple neighbors, and have dynamic time masters. The protocol changes are standardized at the IETF. From a project point of view, A1.2 allows neighbor nodes to communicate: choose the communication frequency and the modulation/demodulation rate, and stay synchronized.

[A1.3] Wireless Enablers

Localization of individual robots in a swarm is critical for their coordination and control. Accurate localization, often implemented using visual markers and multiple cameras, is used as a ground truth to determine the accuracy of robotic control algorithms. To enable inexpensive and massive deployments of robots, we investigate lighthouse localization in conjunction with RF localization, both using angle-of-arrival techniques using antenna arrays, and ultra-wide band techniques.

The goal is summarized in the following studies:

- The first challenge involves the use of angle-of-arrival estimation using BLE transmission from the Single Chip Mote. A number of questions arise: *How does the time and frequency uncertainty of the Single Chip Mote affect the accuracy of angle-of-arrival estimate? Can inaccuracies and errors caused by multipath be mitigated by using frequency diversity, both with BLE standard channels and potentially with operation outside of the ISM band?*

- Lighthouse localization has already been established as a relatively accurate method to localize Single Chip Motes. However, with the addition of RF angle-of-arrival and RF localization techniques, can *sensor fusion* algorithms be applied to multiple measurements to both improve accuracy of the position estimate, and discard erroneous estimates caused by the mote's clock drift or unpredictable RF fading during robot movement?

- Millimeter wave (mm-wave) radios, operating at much higher frequencies than the 2.4 GHz ISM band, benefit from greater attenuation of environmental reflections, narrower beam widths when operating as phased arrays, and inherently higher spacial accuracy due to the smaller wavelength. These radios, both narrowband and wideband, have previously been used for automotive radar, range finding, and imaging. However, these solutions are rarely power constrained, unlike the devices and robots of interest to the research program. The question we contribute to address is: *can low-power mm-wave radios, duty-cycled to conserve energy, be used for robotic localization?* Two sub-questions arise: First, *to what degree will the performance limitations set by the time and frequency imprecision of crystal-free radios affect mm-wave localization accuracy, both using narrowband and UWB rangefinding*. Second, given that mm-wave radios typically burn more power when active, *how deeply would such devices need to be duty-cycled to minimize the effect on battery lifetime while still improving the location estimates of large numbers of robots?* The use of mm-wave radios on tiny, low-power robots also has implications for communication. Small antennas are significantly more efficient at higher frequencies. In the future, as micro-robot sizes become smaller than cm- or even mm-scales, maintaining optimal communication range will require the use of higher operating frequencies.

- Many of these studies could benefit from non-standards compliant and non-commercially available chips. To determine the effectiveness of custom RF localization solutions, we will use the Xilinx RFSoC software defined radios (SDRs) to rapidly prototype algorithms in both the 2.4 GHz and the mm-wave ISM bands. With external frequency conversion and amplification using off-the-shelf components, the same SDR can be used as a back-end for prototyping localization and communication algorithms with millimeter carriers.

Results: The results of A1.3 determine, both theoretically and practically, the performance limitations of low-power wireless devices in RF-based localization, both in the low (2.4 GHz, 5 GHz) ISM bands, and in the mm-wave ISM bands (24 GHz and 60 GHz). Furthermore, there are implications on the quality of low-power wireless networking in both power- and volume-constrained wireless devices. The extension of both localization and communication to millimeter wavelengths also generate results in small-scale ad-hoc mesh networking, which, combined with results from A2, have implications for the future of massive-scale communication for mobile wireless nodes.

3.2 [A2] Low-Power Wireless Networking

Our research has considered a large network of static motes. We see a swarm of mobile robots as a vehicle to push our networking protocols further, address all open challenges at once: mobility, latency guarantees and localization.

Let's hence assume a network of hundreds or thousands of short-range SCuM-based micro-robots moving through a cluttered building. *Can we empower these micro-robots with a communication protocol stack which allows them to communicate in a dependable fashion, even as all robots are continuously moving?* We define "dependable" as encompassing two things: the network guarantees end-to-end reliability (i.e. no data is lost), and timely delivery (i.e. end-to-end latency can be predicted). Time Synchronized Channel Hopping (TSCH), the low-power wireless approach used in the most demanding industrial applications today, is the ideal stepping stone because of its synchronized, scheduled, multi-hop and deterministic nature. That being said, the use case of mobile micro-robots is very different

from a factory floor, and the overall stack needs to be rethought. This includes the scheduling (which cannot rely on slow explicit signaling protocols), and the multi-hop routing protocol (as coordination between micro-robots requires efficient any-to-any communication). Our team has deep protocol development, implementation, experimentation and standardization expertise. We will use control theory to dynamically adapt the schedule, resulting in predictable latency. This work will result in a complete protocol stack implementation, allowing a swarm or micro-robots to efficiently communicate.

This area of research is further divided into two strands.

[A2.1] Swarm Behavior and Mobility

The network topology of a swarm of micro-robots is dynamic because the robots move and have a short communication range. This is in stark contrast to traditional TSCH networks, which are static and stable. The question we want to answer is hence: *can we use TSCH for networking a swarm of micro-robots where each node in the network is mobile?* Because the state-of-the-art is very limited, answering this question requires us to reinvent both the scheduling and routing approach in a TSCH-based networking stack to support mobility.

This leads to the following three studies:

- We introduced the concept of "autonomous cells" in [36] as a bootstrapping mechanism for a 6TiSCH network: each node has a "rendezvous" cell in the schedule, the position of which is computed by applying a hash function to its address. Neighbor nodes thereby know at what time and on which frequency it is listening. *Can we extend the concept of autonomous cells to support mobility?* Since no signaling is needed to set up this cell, nodes can move without communication overhead from re-scheduling. We can for example allow nodes to change the number of autonomous cells it has (adapting for changes in traffic), and communicate that number for example in Enhanced Beacons. We can evaluate this extension of the 6TiSCH standard on the 6TiSCH simulator, and answer the question: *what is the speed limit of the micro-robots at which point the network cannot adapt to the resulting topological changes?* That speed limit depends on the communication range. Furthermore, we need to look at the overhead associated with a robot losing connectivity to the swarm: *how long can it lose connectivity while staying synchronized? How long does it take for it to reconnect?*

- Micro-robots exchange data in a peer-to-peer fashion, rather than all sending data to a single collection point as in a sensor network. The first question we want to answer is: *does the peer-to-peer mode of an IoT routing protocols such as RPL apply to such a dynamic network?* Given our previous work on this protocol the answer is most likely "no", and we will need to take a new approach. We worked on the concept of "virtual coordinates" [73], some of which we have used to create RPL. The question is: *can we re-purpose the concept of virtual coordinates to support peer-to-peer communication in a micro-robotics context?* We will extend RPL to have multiple DODAGs: each potential destination is the root of a new DODAG, which it announces by sending RPL DIOs. We then use reinforcement-based learning to maintain only the DODAGs which are actively used.

- The IoT-lab testbed Inria manages includes robots. The Lille deployment contains 64 Turtlebot2 robots. These are large robots approximately 40 cm high, but are an ideal ready-to-use platform for experimentally evaluating the scheduling and routing approaches described above. We will equip these with micro-motes, and verify the performance of the micro-mote-based mesh network as we have the robots move on a hardcoded track. The question we want to answer is: *what are the mobility patterns which stress the mobile mesh network the most?* There is a trade-off between the mobility algorithm in the swarm which stretches the robots away from one another to progress fast, and the TSCH network which operates best when each robot has many neighbors.

Results: From a scientific point of view, a completely new approach to scheduling and routing in TSCH networks, which are evaluated both in simulation and experimentally on a testbed. These new scheduling and routing protocols are standardized in the 6TiSCH and ROLL IETF working groups. From a project point of view, A2.1 develops the networking stack which is the stepping stone for A3.1 (which adds localization) and the experimental validation.

[A2.2] Wireless Control Loops and Latency Predictability

As we have shown in [33], implementations of TSCH networks such as Analog Devices' SmartMesh IP guarantee delivery. That is, a TSCH network guarantees that data reaches the destination. The catch is that it does not guarantee *when*. Given the unreliable nature of wireless, this makes sense: if my neighbor did not get my frame, I retransmit until it does. One can even argue that, given an infinite amount of time and a connected network, only an implementation bug can justify not having 100% reliability. The next question is: *can a TSCH network guarantee latency?* The answer to that is "no", since there is always a non-zero probability of an infinite amount of retries to happen on a link that has a packet delivery ratio strictly below 100%. The bold and ambitious question this work package aims to answer is: *can TSCH network offer predicable latency and be used to run control loops?* We have anecdotally shown in [65] that the control loop of an inverted pendulum can run through a TSCH network, but without rigorous proof.

This objective leads to the following 3 studies:

- For the latency of a network to be predictable, the easiest is that it does not depend on the amount of traffic in the network. In a TSCH context, this means that the schedule is collision-free. While collision-free schedule is straightforward when using a centralized scheduler, the question is: *can we achieve collision free scheduling in a distributed setting such as a swarm of micro-robots?* One way of answering is to solve the following mathematical challenge: find a whitening function which turns a small number into a set of cells in a schedule, in such a way that any two different numbers result in disjoint sets of cells. If we can solve this, we can assign a unique number to each node in the network (possibly during secure join), which the whitening function turns in a collision-free schedule.

- Minet *et al.* [52] have shown on very simple topologies that it is possible to turn a connectivity graph and a schedule into a distribution of latencies, for stable topologies and convergecast traffic. This is similar to the repetition strategy used by 3GPP in the NB-IoT protocol. *Can we extend that work to take into account a changing topology, changing schedules and any-to-any traffic?* While the approach involves probabilistic analysis, it most likely results in a computational approach. This tool can then be used to explore trade-offs between throughput and power consumption on the one hand, and average latency and latency distribution on the other.

- The two studies above are a necessary mathematical foundation, but *can we turn that mathematical foundation into working scheduling approach?* Consistency cannot be guaranteed in a practical setting, i.e. nodes do not all have the same information at the same time, which we need to take into account using protocol engineering. To evaluate this protocol, we can define a control loop on the IoT-lab robots, for example a maximum round-trip time between two mobile nodes, and verify that our scheduling approach successfully closes that loop, while we control the movement of the robots.

Results: From a scientific point of view, a whitening function that serves as the cornerstone for a collision-free scheduling algorithm with a predictable latency distribution. This whitening function is formally proven, while the overall scheduling approach is implemented and exercised on different scenarios on the IoT-lab robots. From a project point of view, A2.2 develops the scheduling aspect of the protocol stack which allows micro-robots to communicate with predictable latency.

[A2.3] Agile Networking

Today's low-power wireless devices typically consist of a micro-controller and a radio. The most commonly used radios are IEEE802.15.4 2.4 GHz, IEEE802.15.4g sub-GHz and LoRA (SemTech) compliant. Radios offer a different trade-off between range and data-rate, given some energy budget. To make things more complex, standards such IEEE802.15.4g include different modulations schemes (2-FSK, 4-FSK, O-QPSK, OFDM), further expanding the number of options.

"Agile Networking" is the concept we are developing which redefines a low-power wireless device as having multiple radios, which it can possibly use at the same time. That is, in a TSCH context, for each frame a node sends, it can change the radio it is using, and its setting. If the next hop is close, it sends the

frame at a fast data rate, thereby reducing the radio on-time and the energy consumption. If the next hop is far, it uses a slower data rate.

The first challenge was hardware support. With our input, the OpenMote company designed the OpenMote B, which contains both a CC2538 IEEE802.15.4 radio, and an AT86RF215 IEEE802.15.4g radio, offering communication on both 2.4 GHz and sub-GHz frequency bands, 4 modulation schemes, and data rates from 50 kbps to 800 kbps.

The second challenge is to redesign the protocol stack in a standards-compliant way. We are working on a 6TiSCH design in which neighbor discovery happens independently on each radio, and the same neighbor node can appear as many times in the neighbor table as it has radios. The goal is to standardize an "Agile 6TiSCH" profile, without having to touch the core specifications. Jonathan Munoz has co-authored an Internet Draft which details the impact agile networking has on the IETF 6TiSCH protocol stack. This is being implemented in OpenWSN by Mina Rady. The next step is to evaluate the performance of the solution.

3.3 [A3] Security in Constrained Systems

Securing the traditional Internet has been a bumpy ride for the last 30 years, but recently we have witnessed progress, notably with major standardization bodies advocating against pervasive monitoring [37]. On the IoT side, however, popular magazines are full of stories of hacked devices (e.g. drone attack on Philips Hue), IoT botnets (e.g. Mirai), and inherent insecurity. A saying in the IETF, the standardization body behind the technical solutions of the Internet, goes: *"The S in IoT stands for security."*

Why has the IoT industry failed in adopting the available computer security techniques and best practices? Our experience in the research community, industry, and the standards bodies has shown that the main challenges are:

1. The circumvention of the available technical solutions due to their inefficiency.

2. The lack of a user interface for configuring the product in the field resulting in default parameters being (re)used.

3. Poorly tested and unverified software, often lacking or providing an insecure software upgrade mechanisms.

Our research goal is to contribute to a more secure IoT, by studying and proposing technical solutions to these challenges for low-end IoT devices, with immediate industrial applicability and transfer potential.

[A3.1] Lightweight Protocols and System-level Integration

The last couple of years have witnessed a significant progress in secure communication protocols for the IoT. The IETF has taken steps in standardizing new solutions for protecting the communication channel (e.g. OSCORE, TLS 1.3) and 3-party authorization protocols (e.g. ACE framework). These new solutions have been demonstrated as much more efficient than their predecessors (e.g. TLS 1.2, OAuth 2 as used in the Web), and are expected to be deployed with the next generation of IoT products [59, 40]. There are a couple of remaining pieces to complete the IoT puzzle. One of those pieces is the LAKE protocol – to be standardized by the group we co-chair in the IETF – a lightweight authenticated key exchange protocol for IoT. As an important building block, the LAKE protocol is expected to enable key exchange in the most constrained Internet-of-Things use cases [71].

A common assumption for these communication security solutions is that the trust relationship between the different entities involved in the communication has already been established through for example common keying material, root trust certificates. At manufacturing time, the trust relationship is typically established between the IoT device and the manufacturer. However, the domain where the IoT device will be installed is not known at manufacturing time, and before the IoT device can join a given domain, it needs to be provisioned with domain-specific credentials. Bootstrapping this trust relationship between the IoT device and the domain owner is typically considered out-of-scope for the standards bodies, yet it is a non trivial task as IoT devices lack a user interface. Companies typically resort to out-of-band channels (e.g. NFC, ad-hoc wireless network, pre-shared keys printed on the back of a device,

serial port) or proximity-based authentication, requiring the user to go through a cumbersome process of installing a new IoT device. This opens up various vulnerabilities as the "bootstrapping" protocol ends up being designed in-house, without a thorough review of the community and security experts.

One challenge is to enable a solution that allows an IoT device to join (mutually authenticate, authorize, be provisioned with parameters) a network in a new administrative domain, with zero pre-configuration of the IoT device required by the user [68]. One cornerstone component of such a solution is the LAKE protocol [67]. The open research questions include the provisioning of network bandwidth for initial bootstrapping in a zero-touch manner, efficient but flexible transport of public-key certificates.

With LAKE standardization under way, expectations are high in that the working group will provide an efficient key exchange solution for IoT that has been missing. This opens up questions on how the LAKE protocol compares to TLS 1.3 in terms of security and performance, which we plan on answering. Also, in collaboration with the Inria PROSECCO team, we work on a formally verified implementation of the LAKE protocol in the OpenWSN environment, similarly to what has been done during the standardization of TLS 1.3 [26].

Software update mechanisms are being standardized by the IETF [53]. Their use to patch vulnerabilities is primordial in constrained environments to improve the reputation IoT products have in terms of security. We plan to study these mechanisms [75] in the context of 6TiSCH networks to improve their performance and make it approachable to product designers.

Results: From a scientific point of view, we plan on delivering a turn-key, open-source solution for network access of constrained devices, which does not require user input at deployment time. We plan on publishing a comparative study focusing on performance in constrained environments between the LAKE protocol and TLS 1.3. We also plan on implementing the software update mechanism in 6TiSCH networks and improving it to support software updates of large networks. The envisioned work includes both the derivation of new algorithms and protocols, as well as the optimization of existing solutions.

[A3.2] Microrobot Swarm Security

We plan on exploring the applicability of security mechanisms developed and standardized as part of A3.1 with the swarms of constrained micro-robots. There are several challenges that we envision on such a path.

Highly dynamic logical topologies: Considering the structure such as a swarm of micro-robots moving through space, the wireless links between them are expected to have time-variant quality. As a consequence, we can expect highly dynamic logical topologies between nodes in the network. In such conditions, where a node constantly discovers and communicates with new neighbors, *how do we ensure that adequate pairwise cryptographic keys are in place?* This problem is similar to what is encountered in Mobile Ad-hoc Networks (MANETs), but the constraints of SCuM nodes are much higher. *Can we use the protocol(s) standardized by the LAKE standardization working group, or channel-anonymity-based solutions [66]?*

Securing Localization: Being able to localize nodes within a swarm is an essential feature from the application standpoint. To that end, as outlined in A4.2, we plan on using an approach with mobile lighthouses [48], each equipped with lasers that periodically sweep the surrounding space. *How to protect such a system from (accidental) Denial of Service attacks where the attacker randomly points a laser towards the network? Can we use the fact that mobile lighthouses are equipped with radio transceivers and can communicate with the SCuM nodes?* We plan on studying whether lighthouses can use the radio channel to authenticate their broadcasts (e.g. using TESLA-like solutions [58]) and exchange the supplementary information in order to pseudo-randomly change the sweep pattern, such that the presence of the attacker does not disturb the network's localization feature.

Absence of a stable clock source on SCuM: The fact that SCuM has no external components means that it also has no crystal oscillator to use as a stable clock source. This changes the very basics of how wireless networking is done [34]. The work laid out in in A1.2 aims at using the network of micro-robots to provide a relatively stable clock source to each individual SCuM. Instead of trusting its local clock, the nodes in the IoT network must now additionally use the network-provided information. However, this opens up an attack vector where the attacker can disturb the network by simply heating up some of the nodes and changing their clock drift. We plan on exploring the use of machine learning techniques on network drift patterns in order to design an Intrusion Detection System (IDS) to detect nodes under
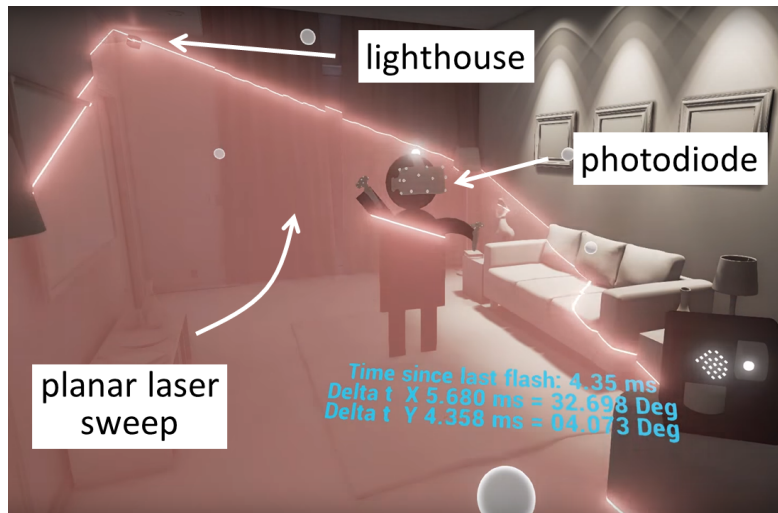
Figure 2: The principle of lighthouse localization.

attack.

Results: This research axis plans on closely following the team developments on micro-robot swarms and ensuring that the appropriate mechanisms are secure-by-design. To that end, the challenges presented serve as an example of the scientific studies we plan on pursuing.

3.4   [A4] Swarm Robotics

Micro-robots need to know where they are. The constrained nature of these devices, and the lack of any infrastructure makes this a unique problem, to which motion capture systems, or solutions based on resource-heavy sensors do not apply. *Can we augment these micro-robots with minimal sensors and smart algorithms which allows them to self-localize using only local measurements?* There is very little related work on lighthouse and ultrasonic localization on micro-robots. As shown in Fig. 2, each lighthouse is equipped with lasers that periodically sweep the surrounding space. "All" the mobile device needs to have is a lightsensor to precisely time when laser sweep passes it to find it's location is polar coordinates relative to that lighthouse. We can exploit the fact that the network is synchronized, and we can equip some of the robots with a combination of ultra-sonic transducers, planer lasers and photodiodes. To take the limited accuracy of relative bearing and distance measurements into account, the mathematical tools we have at our disposal include state estimation and sensor fusion, for example through Extended Kalman Filters (EKF). This work will result in a solution for micro-robots to cooperate and discover each robot's location, in real-time, possibly by having a heterogeneous set of specialized robots.

This area of research is further divided into two strands.

[A4.1] Mathematical Framework for Constrained Localization

Localization is key to any robotic application, and many solutions have been developed. Out of those, lighthouse bearing measurement and ultrasonic range measurements are simple enough sensors that they can be integrated in a subset of micro-robots relatively easily. Wheeler *et al.* [74] have shown that SCuM can detect the laser from a commercial lighthouse. In parallel to a more experimental work, this research area looks at the mathematical framework for constrained localization.

In this work, we assume all robots can be equipped with a lighthouse and/or an ultra-sonic transducer, which allows them to measure relative bearings and distance. The goal is to localize each robot, possibly in a coordinate system which is relative to the swarm. *Yet, what is the mathematical framework for turning local bearing and distance measurements into localization, and what is the resulting localization accuracy?* We combine mathematical modeling and simulation to answer:

- Assuming all nodes are equipped with a lighthouse, they can measure the relative bearing to one-another. It is well understood that having all relative bearing measurements is enough information to localize all nodes to one another [45]. The challenge is that, in any practical scenario, each bearing measurement comes with some error, and not all measurements happen at the same time. We first consider a simple case where all micro-robots are within lighthouse range of one another: *given the exact position of two "global anchor" micro-robots, how accurate can we get the location of all other robots, and how does that change with having more measurements?* This study involves state estimation. We formulate the state estimation model using an Extended Kalman Filter (EKF) to answer the following questions: *How many bearing measurements do I need to have a localization measurement better than X mm? How does the inaccuracy of the bearing measurement impact the location?* We introduce this mathematical model in a simulation with robots far enough from each other than they form a "multi-hop" topology rooted in these two global anchors.

- We add local distance measurements from ultrasonic transducers to our model, and use our EKF for sensor fusion. This allows us to answer the following question: *how much more accurate is the localization if we combine bearing with distance measurements, compared to bearing alone, or distance alone?* This helps us navigate the cost/accuracy trade-off, and compare our EKF-based methodology with well-established literature on localization using ultra-sonic measurements [55, 39].

- Robots move, which limits the number of bearing measurements for each location. By introducing movement in the simulator, we can answer the following questions: *what is the mobility pattern (maximum velocity, pause period, etc.) which yields an appropriate trade-off between speed of progression of the swarm and localization accuracy?*

- It is unnecessary to equip each robot with a lighthouse (the laser transmitter); a heterogeneous swarm is possible, in which a portion of robots are equipped with a laser transmitter, the others with only a photodiode. The question becomes: *what is the trade-off between the portion of laser-equipped robots and localization accuracy?*

Results: From a scientific point of view, A4.1 creates the mathematical framework for a localization solution which combines lighthouse and ultrasonic range measurements, in an infrastructure-free, distributed and mobile context. A state estimation and sensor fusion approach allows us to explore trade-offs between accuracy and cost, and understand the impact of robot movement, and of the portion of lighthouse robots on localization accuracy. From a project point of view, A4.1 allows us to decide what hardware to build for experimentation. The model we develop in A4.1 is used as-is in A4.2.

[A4.2] Localization and Network Stack Co-Design

The goal of A4.2 is to co-design the localization solution (the model is built in A4.1) and the networking stack. There are two aspects to this. On the one hand, the network puts constraints on the localization system, in particular on the amount of data that can be exchanged per period of time, and the associated latency. On the other hand, the synchronized and scheduled nature of the networking stack presents a tremendous opportunity for the localization solution: coordinating when the different sensors are on, yielding a better coexistence and power savings. Similar system-level studies can be found [56, 55, 39], yet none to be best of our knowledge focuses on extremely constrained micro-robots. The system-level questions we want to answer is: *What is the overhead of localization on the network? How scalable is a lighthouse and ultrasound-based localization? How low-power can a mote participating in the network and the localization be?* We use simulation and modeling.

- For a lighthouse, using the laser consumes power, and makes it harder for another lighthouse to also have its laser on. The same holds for the ultra-sonic transducers. *Can we use the synchronized nature of the network to schedule when each lasers and ultrasonic transducers are on, in such a way that only one pair of close nodes measures their relative bearing and distance at any given time?* The scheduled nature of these measurements has two immediate advantages. First, the swarm scales to more robots, as a collision-free localization schedule can be injected. Second, the robots

switch their lighthouse and ultrasound only exactly when they know they will be ranging, resulting in ultra-low power operation, key for immobile robots that want to extend their battery lifetime.

- Each node knows a relative bearing and distance to each or its neighbors. *Can this information be shared in such a way that all nodes can compute their location?* This location can be computed in a coordinate system that is local to the swarm. The goal of this task is to extend the 6TiSCH protocols with a mechanism to share local measurements, and a distributed localization algorithm.

- The protocol resulting from the previous task necessarily comes with some latency, which results in inconsistency between the view of that information. *What is the impact of this inconsistency on location accuracy?*

Each of these studies results in a new algorithm or protocol, which is first analyzed then evaluated through simulation.

Results: From a scientific point of view, this research has the potential of deeply changing indoor localization as it develops a full RTLS using micro-robots with extreme constraints, in particular in a heterogeneous setup. The result is a method by which a swarm of micro-robots localizes as it progresses through some space. From a project point of view, A4.2 is the last building block to realize the exploration and mapping expedition, including experimentally.

[A4.3] Coordination & Control of a Robotic Swarm

Two important considerations when programming large numbers of tiny cyber-physical agents is: *what is the easiest way to program them, either individually, or en masse, and, perhaps more importantly, how can a programmer debug them?* When the platforms themselves are on the mm or cm scale, the mass and volume requirements to make physical contact are prohibitive. The fact that the robots could move during live programming or debugging.

Four different approaches to contact-free programming will be compared for various swarm robotic applications. The first two are optical: both focused optical communication, and large-scale optical communication. The second two are electromagnetic: near-field communication (NFC) and far-field communication over a wireless data link. All of these have been used in the past to program cyber-physical systems, but we propose to perform a comprehensive survey on their reliability (effectively, program error rate). Furthermore, there is little effort on how these communication systems can be used for debugging, along the lines of a wireless JTAG interface. And, most importantly, we propose to study how these communication interfaces scale in performance with severe volume limitations. As an example, received optical power scales linearly with diode area, assuming uniform illumination.

For contact-free debugging, the problem is less constrained, as it is difficult to quantify how "easy" a system is to work with. Because physical access is impossible, not all on-board voltages and logic levels are accessible. But, it is feasible to create a back-and-forth communication between the robot's on-board processor and the programmer where certain logic levels and registers can be observed remotely, aiming for a wireless JTAG. This may not be realistic in the en-masse optical programming, although these robots could use diagnostic LEDs that can be read by the user (at low data-rate). The point-to-point laser programmer can also receive data from an on-board LED. The far-field RF communication presumably has a link already established, so debugging can be performed over any communication standard that the robot normally uses (earlier examples of Bluetooth or IEEE 802.15.4 are both valid). The near-field programming could be modified to incorporate an RFID style backscattering to send data from the device to the programmer.

Metrics, like power consumption, programming time, reliability (program error rate) and debug latency will all be concretely measured and compared. User safety, particularly in the case of IR programming for point-to-point optical, or heating due to the potentially low efficiency of near-field capacitive or inductive programming, will also be considered. A more holistic survey of experienced embedded systems engineers will also be performed to determine which programming strategy is most desirable, from the user's perspective, in various applications (single robot, two robot, and many robot, with either a uniform code-base, or a diverse and heterogeneous code-base).

3.5   [A5] Vehicle Area Networking - FANETs - Network Models

Vehicle Area Networking (VANETs) have been a research focus of the team, in particular broadcasting and opportunistic routing schemes. The AIO team continues working on these subjects, while extending them to medium access schemes. We also consider higher level transmission scenarios. For instance, the team plans to study how safety messages can be used to assist the driver, possibly by performing automatic maneuvers in VANETs.

[A5.1] Improvement of communications protocols

The standard IEEE 802.11p protocol has been shown no to scale properly the density of vehicles rapidly varies. In EVA, we have proposed enhancement of the IEEE 802.11p access scheme by considering an adaptive carrier sense level [28, 22]. The idea is to create local communication and to allow the network traffic to scale with the density of the vehicle. Detailed proposals have been developed during Younes Bouchaala thesis [27]. Another approach is to use a TDMA approach. The main concept is to use the position of vehicles on the roads to control the slots allocations [42, 43]. This technique allows to drastically reduce packets collision. We can use a decentralized (possibly using cluster heads) or a centralized approach assisted by roadside units [44]. These studies have been carried during Mohamed Hadded thesis [41]. We are currently working to improve these approaches. The idea is to use active signaling techniques in combination with TDMA approaches [30]. The active signaling techniques work as an advanced CSMA scheme and thus bring to the protocol the advantage of random access scheme. We can thus benefit from the stability of the TDMA approaches whereas the active signaling scheme allows the protocol to reduce the collision and offer low latency access when required [32, 29, 31]. This present work will Fouzi's Boukhalfa thesis whose defense is scheduled in October 2021. We can probably even improve your protocol if we use another communication medium such as the visible light. We have started to propose a new architecture which uses simultaneously visible light and radio communication. The smart combination of these two media will be on the focus of our work during the next research period.

We have to study if the visible light communication is mature enough to be used in VANETs in replacement of radio links. The question of the performance and the stability of the visible link is not satisfactorily answered. According to the present state of the art vlc, there are significant problems with interference (natural light, car headlight) [47], and beam propagation due to vehicles trajectories and their movements. Thus vlc appears more to be a complementary technology to radio communication than a technology that can be used alone. So we do not know yet if the visible light links can be used reliably or if we can use them only as backup liaison to increase our protocols reliability .

The standard IEEE 802.11p protocol has slowly started its deployment in the real life leaving the door open to operator initiative. 5G has developed an approach for vehicles promising a very low latency access for vehicles. We need to better understand what are the 5G services for vehicular networks and what are their strength and limitations We plan a collaboration with the RITS team to deploy a 5G vehicular network in Rocquencourt. More specifically we plan to use 5G network to send Cooperative Awareness Messages CAMs and Decentralized Emergency Notification Messages and to develop a 5G assisted intersection crossing application. We will try to take benefit of this deployment to evaluate how 5G could scale on a real VANET network.

[A5.2] Towards Autonomous Cars

Autonomous driving is a target followed by many new companies such as Google, Uber, Telsa, and even by older players in the field such BMW, Mercedes, etc. Recent progress has been accomplished but it is still unclear whether whether full autonomous vehicles can be obtained in large amount of different cases or if we have to treat only special case such as driving in platoon. The exact role of communication in an autonomous car also remains to be further studied even the importance of the vehicular communication networks has been acknowledge [50, 72].

We wish to start by the study of platoons of vehicle and to design the suitable communication network to ensure a high degree of safety. The idea is to use the concepts of [49] and to adapt them to the protocol AS-DTMAC that we have recently designed. Given the nature and the probability of hazards and assumptions on packet transmission errors, we plan to compute the probability that our platoon

of vehicles communicating with our protocol, and according to strict rules, can safely progress. The use of VANETs can be studied in other simple situation such as keeping safe distance between vehicles, changing lanes or inserting in a lane at the entrance of an highway. We plan to combine the use of radio VANETs with other sensing technologies (RADAR, LIDAR, Video) or even with visible light communication to increase the reliability of the system. We believe that as any safety system, autonomous cars have to rely on many different and independent sensing systems to be able to ensure a high degree of reliability. We will have to

We also have to study if the visible light communication is mature enough to be used in VANETs. According to the present state of the art vlc, there are significant problems with interference (natural light, car headlight) and beam propagation due to vehicle trajectories and their movements. Thus vlc appears more to be a complementary technology to radio communication than a technology that can be used alone.

[A5.3] Machine learning and VANETs

Vehicular networks can generate a lot of data; the vehicles have positioning capabilities (e.g. GPS), they also have communication devices and computing power. We have shown that the power received from packets transmitted by road side units can be used by machine learning algorithms such as Random Forest (RF) , K Nearer Neighbors (KNN), Neural Networks (NN) to predict the position of the vehicle and performance of the wireless network (e.g. packet delivery ratio) see [61, 60, 64]. We have shown that these prediction can obtained even a significant portion of the measurements are lost and that the predictions still remain exploitable. We believe that these results remain to be improved, for instance the use communication data with input of other sensor appear to be very promising. These studies will depend on the availability of large amount of vehicle network data.

It is also possible to use machine learning to forecast accidents. Urban traffic forecasting models generally follow either a Gaussian Mixture Model (GMM) or a Support Vector Classifier (SVC) to estimate the features of potential road accidents. Although SVC can provide good performances with less data than GMM, it incurs a higher computational cost. We have proposed framework that combines the descriptive strength of the Gaussian Mixture Model with the high-performance classification capabilities of the Support Vector Classifier. A new approach is presented that uses the mean vectors obtained from the GMM model as input to the SVC. Experimental results show that the approach compares very favorably with baseline statistical methods, see [63]. Advances are possible in forecasting accidents, these progresses depend on the availability of data, in particular covering a wide variety of problems from simple incidents to accidents with injuries to fatalities. It is clear that such a system could be very interesting for a driver who could in dangerous conditions increase his attention and even activate driving aids.

The positioning of the AIO team in machine learning for VANETs consists of using and combining techniques already available and exploiting these techniques in open data sets. This positioning is different from that of the SIERRA team which seeks the design of a new algorithm preferably to solve fundamental problems in networks. For example in AIO we plan to use a customized Deep Learning mechanism-based congestion control identification approach that does not need any enriched domain knowledge other than training traffic of a congestion control variant. By only using packet arrival data, it is also directly applicable to encrypted (transport header) traffic. At the same time, during the customization phase, we will also use deep reinforcement learning to consolidate the congestion control. Trust Region Policy Optimization (TRPO) and proximal policy optimization will be adopted in the proposed customized approach as the measure of optimization.

[A5.4] Security and Privacy in VANETs

Security in VANETs has already been the subject of numerous studies [46, 51]. Attacks can be carried out in several places: on the air interface of the network, in the hardware or software of vehicle transmissions, in the vehicle sensors whose information is sent over the network, in the infrastructure of the VANET network. All types of security attacks can be found in vehicular networks and the dynamics of network links add further complexity to the problem. Faced with the difficulty of the problem, VANET networks still have an advantage, the vehicles and infrastructure elements have significant computing power and

energy resources. The classic security approach in VANETs is the deployment of a PKI. This approach has been standardized in Europe at ETSI and in the US. This approach does not solve all the issues and gives rise to problems in particular of Privacy. To remedy this, the technique of pseudonyms has been proposed [23].

The approach of the AIR project is not to study security in VANETs networks in general but to propose punctual improvements of the state-of-the-art on precise and well-defined security problems.

VLC links could be used between vehicles for communications. We plan to study how the use of such a link could advance security in VANETs. With the nature of VLC links, it is clear that capturing messages or sending of fraudulent packets is almost impossible in the context of point to point VLC links. On the privacy side, the use of VLC links can be very beneficial. We plan to quantify this benefit compared to existing solutions.

Another area we want to tackle is the security of routing protocols in VANETs. We have started to study security attacks on cross-layer routing and the benefit of trust against these attacks [25, 24]. Ismael Tayssir in her PhD plans to development of a new intelligent routing protocol which uses information from the MAC layer to find an optimized path between the transmitter and the receiver and which takes into account the specificities of the transmission medium while minimizing the time of transmission. In her PhD, detection of malicious behavior at the MAC and routing layer will be proposed to secure the routing protocol developed.

We also have started very preliminary studies to use blockchains in VANETs [62]. We will continue on this topic and will try to determine if there are cases of applications in VANETs where this technology can find its best application.

The RITS team works primarily on security issues in VANETs caused by the sending of fraudulent or erroneous data coming from vehicle sensors. Collaboration between our team and RITS in this area is possible.

[A5.5] FANETs

The field of FANETs (Flying Area NETworks) is experiencing significant growth in the academic community and also among manufacturers, particularly the arms manufacturers. This area poses many interesting problems such as maintaining connectivity, multiple access, satisfying quality of service, etc. The problems obtained are often very combinatorial in nature and the arrival of artificial intelligence opens a new horizon of research in this field. AIO has Cifre PhD with Thales

[A5.6] Advanced network protocols and models

4   Application domains

4.1   Industrial Process Automation

Wireless networks are ubiquitous and are an integral part of our daily lives. These networks are present in many application domains; the most important are detailed in this section.

Networks in industrial process automation typically perform monitoring and control tasks. Wired industrial communication networks, such as HART, have been around for decades and, being wired, are highly reliable. Network administrators tempted to "go wireless" expect the same reliability. Reliable process automation networks – especially when used for control – often impose stringent latency requirements. Deterministic wireless networks can be used in critical systems such as control loops, however, the unreliable nature of the wireless medium, coupled with their large scale and "ad-hoc" nature raise some of the most important challenges for low-power wireless research over the next 5-10 years.

Through the involvement of team members in standardization activities, protocols and techniques are proposed for the standardization process with a view to becoming the de-facto standard for wireless industrial process automation. Besides producing top-level research publications and standardization activities, this activity fosters further collaborations with industrial partners.

4.2 Environmental Monitoring

Today, outdoor IoT networks are used to monitor vast rural or semi-rural areas and may be used to detect fires. Another example is detecting fires in outdoor fuel depots, where the delivery of alarm messages to a monitoring station in an upper-bounded time is of prime importance. Other applications consist in monitoring the snow-melt process in mountains, tracking the quality of water in cities, registering the height of water in pipes to foresee flooding, etc. These applications lead to a vast number of technical issues: deployment strategies to ensure suitable coverage and good network connectivity, energy efficiency, reliability and latency, etc.

We work on such applications through associate team "SWARM" with the Pister team at UC Berkeley.

4.3 The Internet of Things

The Internet of Things (IoT) is composed of small, often battery-powered objects that measure and interact with the physical world, and encompasses smart home applications, wearables, smart city and smart plant applications.

It is essential to (1) clearly understand the limits and capabilities of the IoT, and (2) develop technologies which enable user expectation to be met.

The AIO team is dedicated to understanding and contributing to the IoT. In particular, the team maintains a good understanding of the different technologies at play (Bluetooth, IEEE 802.15.4, WiFi, cellular), and their trade-offs. Through scientific publications and other contributions, AIO helps establish which technology best fits which application.

4.4 Military, Energy and Aerospace

EVA has developed cutting-edge expertise in using wireless networks for military, energy and aerospace applications. Wireless networks are a key enabling technology in these application domains, as they allow physical processes to be instrumented (e.g. the structural health of an airplane) at a granularity not achievable by its wired counterpart. Using wireless technology in these domains does however raise many technical challenges, including end-to-end latency, energy-efficiency, reliability and Quality of Service (QoS). Mobility is often an additional constraint in energy and military applications. Achieving scalability is of paramount importance for tactical military networks, and, albeit to a lesser degree, for power plants. AIO works in this domain.

Smart cities share the constraint of mobility (both pedestrian and vehicular) with tactical military networks. Vehicular Ad-hoc NETworks (VANETs) will play an important role in the development of smarter cities.

The coexistence of different networks operating in the same radio spectrum can cause interference that should be avoided. Cognitive radio provides secondary users with the frequency channels that are temporarily unused (or unassigned) by primary users. Such opportunistic behavior can also be applied to urban wireless sensor networks. Smart cities raise the problem of transmitting, gathering, processing and storing big data. Another issue is to provide the right information at the place where it is most needed.

4.5 Emergency Applications

In an "emergency" application, heterogeneous nodes of a wireless network cooperate to recover from a disruptive event in a timely fashion, thereby possibly saving human lives. These wireless networks can be rapidly deployed and are useful to assess damage and take initial decisions. Their primary goal is to maintain connectivity with the humans or mobile robots (possibly in a hostile environment) in charge of network deployment. The deployment should ensure the coverage of particular points or areas of interest.

The wireless network has to cope with pedestrian mobility and robot/vehicle mobility. The environment, initially unknown, is progressively discovered and may contain numerous obstacles that should be avoided. The nodes of the wireless network are usually battery-powered. Since they are placed by a robot or a human, their weight is very limited. The protocols supported by these nodes should be energy-efficient to maximize network lifetime. In such a challenging environment, sensor nodes should

be replaced before their batteries are depleted. It is therefore important to be able to accurately determine the battery lifetime of these nodes, enabling predictive maintenance.

4.6   Types of Wireless Networks

The AIO team distinguishes between opportunistic communication (which takes advantage of a favorable state) and collaborative communication (several entities collaborate to reach a common objective). Furthermore, determinism can be required to schedule medium access and node activity, and to predict energy consumption.

In the AIO project, we propose self-adaptive wireless networks whose evolution is based on:

- optimization to minimize a single or multiple objective functions under some constraints (e.g. interference, or energy consumption in the routing process).

- machine learning to be able to predict a future state based on past states (e.g. link quality in a wireless sensor network) and to identify tendencies.

The types of wireless networks encountered in the application domains can be classified in the following categories.

4.7   Wireless Sensor and Mesh Networks

Standardization activities at the IETF have defined an "upper stack" allowing low-power mesh networks to seamlessly integrate into the Internet (6LoWPAN), form multi-hop topologies (RPL), and interact with other devices like regular web servers (CoAP).

Major research challenges in sensor networks are mostly related to (predictable) power conservation and efficient multi-hop routing. Applications such as monitoring of mobile targets, and the generalization of smart phone devices and wearables, have introduced the need for WSN communication protocols to cope with node mobility and intermittent connectivity.

Extending WSN technology to new application spaces (e.g. security, sports, hostile environments) could also assist communication by seamless exchanges of information between individuals, between individuals and machines, or between machines, leading to the Internet of Things.

4.8   Deterministic Low-Power Networks

Wired sensor networks have been used for decades to automate production processes in industrial applications, through standards such as HART. Because of the unreliable nature of the wireless medium, a wireless version of such industrial networks was long considered infeasible.

In 2016, the publication of the IEEE 802.15.4e standard triggered a revolutionary trend in low-power mesh networking: merging the performance of industrial networks, with the ease-of-integration of IP-enabled networks. This integration process was spearheaded by the IETF 6TiSCH working group, co-chaired by AIO. A 6TiSCH network implements the IEEE 802.15.4e TSCH protocol, as well as IETF standards such as 6LoWPAN, RPL and CoAP. A 6TiSCH network is synchronized, and a communication schedule orchestrates all communication in the network. Deployments of pre-6TiSCH networks have shown that they can achieve over 99.999% end-to-end reliability, and a decade of battery lifetime.

The communication schedule of a 6TiSCH network can be built and maintained using a centralized, distributed, or hybrid scheduling approach. While the mechanisms for managing that schedule are standardized by the IETF, which scheduling approach to use, and the associated limits in terms of reliability, throughput and power consumption remain entirely open research questions. Contributing to answering these questions is an important research direction for the AIO team.

4.9   MANETs and VANETs

In contrast to routing, other domains in Mobile Ad-hoc NETworks (MANETs) such as medium access, multi-carrier transmission, quality of service, and quality of experience have received less attention. The establishment of research contracts for AIO in the field of MANETs is expected to remain substantial.

MANETs will remain a key application domain for EVA with users such as the military, firefighters, emergency services and NGOs.

Vehicular Ad hoc Networks (VANETs) are arguably one of the most promising applications for MANETs. These networks primarily aim at improving road safety. Radio spectrum has been ring-fenced for VANETs worldwide, especially for safety applications. International standardization bodies are working on building efficient standards to govern vehicle-to-vehicle or vehicle-to-infrastructure communication.

4.10   Cellular and Device-to-Device Networks

We propose to initially focus this activity on spectrum sensing. For efficient spectrum sensing, the first step is to discover the links (sub-carriers) on which nodes may initiate communications. In Device-to-Device (D2D) networks, one difficulty is scalability.

For link sensing, we study and design new random access schemes for D2D networks, starting from active signaling. This assumes the availability of a control channel devoted to D2D neighbor discovery. It is therefore naturally coupled with cognitive radio algorithms (allocating such resources): coordination of link discovery through eNode-B information exchanges can yield further spectrum usage optimization.

5   Social and environmental responsibility

We are accutely aware of the role Inria and our team plays in society and on the environment. While we are of course primarily focused on our purely scientific duties, we are actively trying to stay connected to society and to be aware of the environment.

As researchers, we have a fantastic tool at our disposal to make a deep change into society: education. We teach classes and short courses mainly to the engineering student and believe that embedded systems are the perfect teaching tool. They offer infinite opportunities to let student "see for themselves". And adding connectivity to them (low-power wireless for example) allows the students to build very complex chains of information. In the most complete case, information goes from a physical sensor to a micro-controller, through a low-power wireless mesh network, to a gateway, to a single-board computer, to a cloud-based back-end system, to a database, and to the student's browser. Being able to build up this entire chain fast and with relatively simple components is both incredibly motivating for the students ("The dial is moving on my phone!", "I can control my fan remotely!"), and offers the instructor infinite possibilities to dig into any topic, from SPI buses to RTOS priority inversion, embedded protocols or web interaction. Given that perspective, our first guiding principle when teaching is to "build real things".

One of the things we see when interviewing people is that students are often not exposed to the technology being used in real-world applications. They have often some experience with open-source projects, development boards and DYI hardware. And while these tools are perfectly valid, they don't convey to the student a clear picture of what the state of the art is. Given that perspective, our second guiding principle when teaching is to use technology that's really out there.

In 2023, we continued developing two distinct platforms which can both he used for our research, as well as for education.

The first is the DotBot (www.dotbots.org), an open-source robotic platform. It consists of a printed circuit board and two motors installed on a laser-cut wooden chassis, also featuring an HTC VIVE lighthouse receiver for mm-accurate positions at 100 Hz. The DotBot's wireless System-on-Chip (SoC) allows different DotBots to communicate. We are building a 1,000 DotBot swarm for our research of swarm orchestration. As an open-source platform, DotBot is being designed for education and research well beyond the project. We envision educational and research kits targeting students at the primary school, high school and university levels, with a particular focus on female students. DotBot is a fantastic stepping stone for the community to embrace swarm communication, train the next generation of collaborative node experts and educate students, thereby training the next generation of smart system which incorporate decentralized orchestration, constrained AI and swarm programming.

The second is the AIOT Systems (www.aiotsystems.org), a one-stop shop for learning embedded low-power wireless. The AIOT Play board is a ready-to-learn-on platform, designed specifically to be both easy to learn with, and close to an production system. It features a prototyping area allowing a student to build little circuits directly on the board. They then write firmware directly on the fully programmable

micro-controller to interact with the circuit, and hand the data to the true mesh networking module. The source code consists of Python code that runs on a computer, and C code that runs on a micro-controller. The source code is developed under an open-source license so students can really see how things are working, and use it beyond learning. We crafted the AIOT Systems Academy so it is a completely self-contained set of course material. The AIOT Systems Academy is a collection of dozens of short labs. For instructors, the material is ready to present.

Of course, there is no way we can argue the core technology we develop is good for the environment. Any electronic circuit is build from materials and through fabrication method which are harmful. Yet, unlike a cell phones or a tablet, we look for applications in which our sensors are used to prevent events which would have a very negative effect on the environment, and for which the environment cost of the technology is much smaller than the environmental benefit they allow. This is the reason why a lot of our applications are related to the environment. We have deployed sensors to detect early stage of wildfires to be able to put them out before they destroy entire ecosystems (see France 3 interview). We have deployed sensors in marinas to detect fires on board ships, and prevent boats from overconsuming electricity (through our Falco startup). We are working with architects in tropical climates to monitor their buildings to be able to reduce the use of air conditioning (through our collaboration with ESIROI). Besides these projects, we have deployed sensors to detect frost events in vineyards or in peach orchards, combat the invasion of the Asian Hornet that is several impacting an already fragile bee population, or monitoring the snowmelt process in regions prone to draughts. Through this focus on environmental responsibility, we are convinced that the technology we develop has an overall positive impact on our planet.

6   Highlights of the year

What a year 2023 was for the AIO team!

First of all, 2023 was the very first year of our Horizon Europe project, OpenSwarm. This is a project that the team championed by coordinating the writing of the proposal in 2022, and which we were delighted was accepted. The project started on 1-Jan-2023, with Inria as scientific coordinator. With this started a very fun series of events, including the kick-off meeting, the hiring processes, the monthly executive committee meetings, an all-hands meeting in Belgium, events organized by the European Commission and our first review meeting. For Thomas Watteyne, this was all new as this is the first European project he coordinates, with input from all of the team. In particular, Clotilde Monnet has been a true driving force behind the project, and has coordinated all of the non-scientific activities.

Second, the DotBot project has evolved dramatically over the past year. The DotBot is the swarm robot that the team is developing, with the eventual goal of building a massive swarm of 1,000 robots. This robotic platform is an integral part of the OpenSwarm project. Thanks in part to the incredible contributions of Alexandre Abadie, the team has added the ability to control the robot swarm from a remote server, and has designed a more robust version of the DotBot hardware that includes customizable shields for quickly adding new features. In addition, as part of Said Alvarado-Marin's PhD work, the team has developed a new approach for precise indoor localization using virtual reality lighthouse technology. This new approach is less expensive and much more portable than camera-based systems, and is an integral part of our goal to deploy DotBots as educational tools in classrooms.

Third, the work on "Smart Dust" continued, under the leadership of Filip Maksimovic. In particular, he demonstrated the first ever multi-hop mesh network of SCuM chips – the research platform developed in collaboration with UC Berkeley – as well a heterogeneous networks of crystal-free and crystal-enabled off-the-shelf devices. In her PhD work, Sara Faour has been working on the security on chip-scale systems, including using randomness in volatile memory as a Physically Unclonable Function (PUF). The work on Smart Dust culminated with the organization in September 2023 of the Invited Workshop on Crystal-Free Radios, Chip-Scale Wireless Systems and Swarms, see attendees in Fig. 3, with lots of help from Anne Mathurin. We invited the leaders in the small but growing crystal-free community and, for three days, shared both research advances in the field and defined a joint research roadmap for the next five years.

Fourth, under the leadership of Mališa Vučinić, the team continues to actively participate in standardization activities in the realm of security for low-power wireless networks. In particular, the IETF LAKE

Figure 3: Attendees of the Invited Workshop on Crystal-Free Radios, Chip-Scale Wireless Systems and Swarms.

working group met three times in 2023, at IETF 116 (Yokohama, Japan, March), IETF 117 (San Francisco, July) and IETF 118 (Prague, November). The team has contributed significantly to both standardization and implementation. The IETF LAKE working group finalized the standardization of the EDHOC protocol. In collaboration with Inria PROSECCO and Inria TRIBE, the AIO team demonstrated the only microcontroller-optimized, formally-verified implementation of the LAKE EDHOC under the leadership of Geovane Fedrecheski. This work was performed in the context of the RIOT-fp Inria Challenge.

Fifth, the development of the Wattson Elements/Falco startup, the first spin off of the AIO team, continues. In 2023, Falco grew to a team of 12 people, expanded to a total of 38 marinas and now monitors 15,000 moorings across the world. Its smartphone application now has 8,920 active accounts and has assisted in 1,867 marina contract renewals in 2023, an increase of 26% over 2022.

Sixth, as a result of this activity, the team is proud to have received the following recognitions in 2023:

- Inria was identified as "Key Innovator" by the European Commission's Innovation Radar for innovation "Developing the DotBot Platform for Teaching Swarm Robotics".

- Spin-off startup company Wattson Elements has deployed its solution in Vancouver, Canada, the 38th marina equipped.

- Falco was identified as "Key Innovator" by the European Commission's Innovation Radar for innovation "Smart Buoy and Embedded AI for Ocean Noise Pollution Monitoring".

- Mališa Vučinić was elevated to IEEE Senior Member.

Seventh, the team would like to congratulate its alumni who graduated in 2023: Razanne Abu Aisheh succesfully defended her PhD on "Context-Aware Information Gathering and Processing Towards Supporting Autonomous Systems in Industry 4.0 Scenarios" Trifun Savic succesfully defended his PhD on "Localization in Constrained Environments".

Eighth, the team welcomed many new members in 2023: Branko Kerkez (as Inria International Chair recipient), Clotilde Monnet (as Project Manager), Ichrak Kallala (as Research Engineer), Geovane Fedrecheski (as Research Engineer), Elsa Lopez-Perez (as PhD student), Yuxuan Song (as PhD student), Martina Balbi (as PhD student), Fabian Graf (as PhD student), Marion Seychelles (as MsC intern),
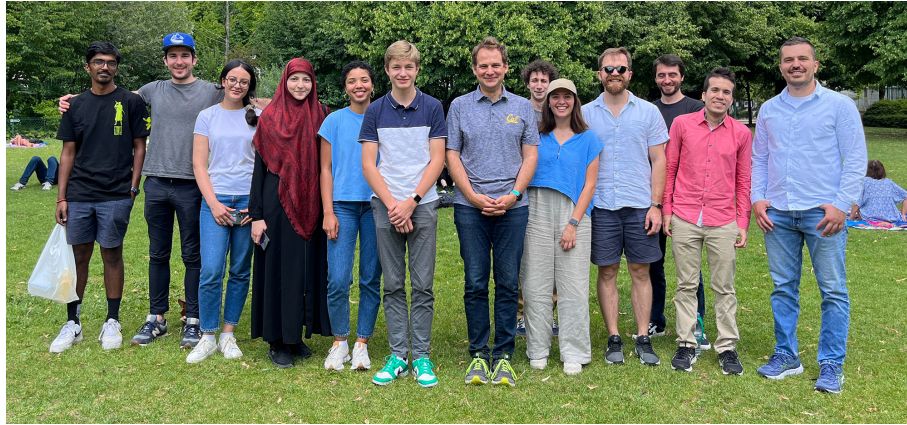
Figure 4: (almost all) members of the AIO team on 23-Jun-2023

Fabrice Sivakumar (as hMsC intern), Raul de la Fuente (as MsC intern), Eloi Joyeux (as high-school intern).

And finally, and perhaps most importantly, the AIO team is, and always will be, the enthusiastic, happy and welcoming team you can see in Fig. 4.

7 New software, platforms, open data

7.1 New software

7.1.1 lakers

Name: EDHOC Implementation in Rust

Keywords: Cybersecurity, Internet of things, EDHOC

Functional Description: EDHOC is a lightweight authenticated key exchange protocol targeting constrained environments and Internet of Things use cases. This is a Rust implementation of the protocol, adapted for use on microcontrollers.

URL: https://github.com/openwsn-berkeley/edhoc-rs

Contact: Malisa Vucinic

7.1.2 DotBot-hardware

Keywords: 3D printing, Electrical circuit, Robotics

Functional Description: PCB and Mechanical Parts for DotBots

URL: https://github.com/DotBots/DotBot-hardware

Contact: Thomas Watteyne

7.1.3 DotBot-firmware

Keywords: Robotics, Embedded, Microcontroller

Functional Description: Source code for firmwares usable with the DotBot hardware.

Release Contributions: https://github.com/DotBots/DotBot-firmware/releases/tag/REL-1.14

URL: https://dotbot-firmware.readthedocs.io/en/latest

Contact: Thomas Watteyne
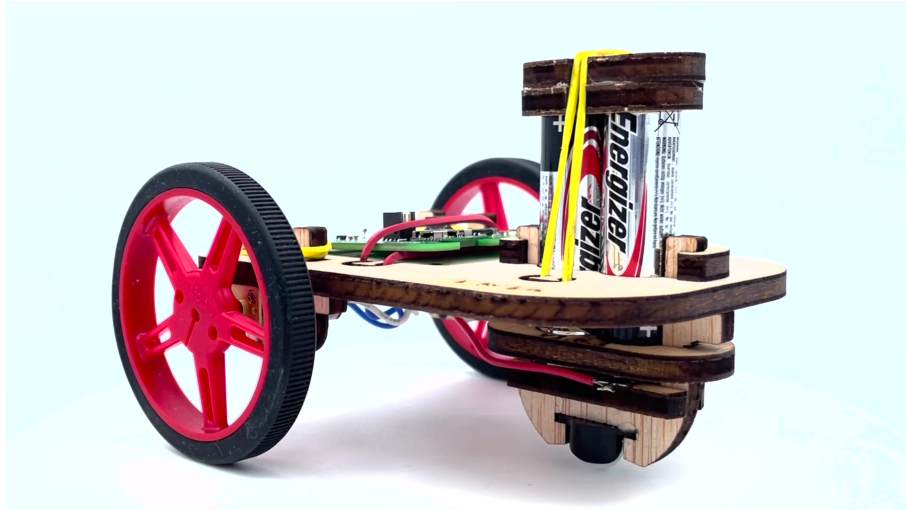
Figure 5: The DotBot swarm robot.

7.1.4 PyDotBot

Keywords: Robotics, Python, Web Application

Functional Description: A complete environment for controlling and visualizing DotBots.

URL: https://pydotbot.readthedocs.io/en/latest/

Contact: Thomas Watteyne

7.2 New platforms

7.2.1 DotBot

Large, coordinated "swarms" of small, resource-constrained robots have the potential to complete complex tasks that single monolithic robots cannot. However, while there is ongoing research, little progress has been made in successfully deploying these swarms in the real world. To help further the field, we are building a research platform called DotBot, shown in Fig. 5: a low-price, versatile laser cut robot that can inexpensively act as an agent in a swarm of robots. Each DotBot has two small motors for mobility, accurate localization using laser lighthouses, and can communicate using off-the-shelf radios in either time-synchronized channel-hopping mesh networks originally designed for reliable transmission in crowded IoT networks, or with BLE so that the robots can be programmed from a cell phone or other Bluetooth-enabled device. We see the DotBot platform as an ideal tool for introducing robotics and embedded programming in education. We target three levels. First, in primary school, DotBot serves as a basic introduction to robotics, using simple interaction and remote-control scenarios. In high school, DotBot is used as an introduction to embedded programming, with a focus on the interaction with the real world. Finally, in university, a DotBot swarm is used to introduce the concepts of distributed algorithms, task assignment as well as planning and scheduling.

More information at www.dotbots.org.

7.2.2 Lighthouse v2 mini-mote

The PhD works of Said Alvarado-Marin has allowed us to put together an experimental environment to work on mm-level indoor localization used a laser system known as "lighthouse". The enviornment consists of the lighthouse v2 mini-motes, their calibration board and Visually tracked Lighthouse v2 basestation. This experimental tooling is set up inside the AIO team's offices.

The mini-mote, shown in Fig. 6, is a miniaturized version of the localization hardware found in the DotBot. Its small size make it an ideal platform for motion tracking experiment with the lighthouse
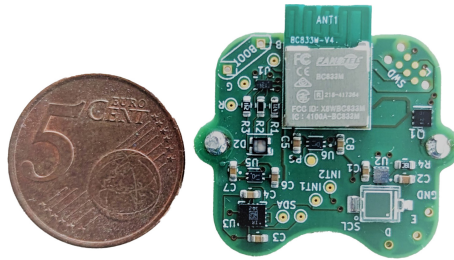
Figure 6: Lighthouse v2 mini-mote.
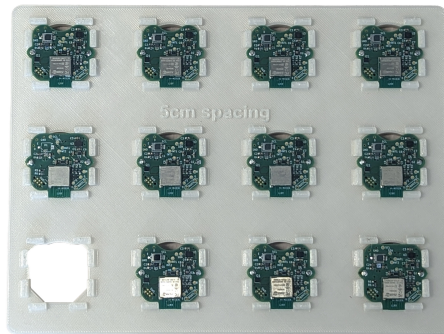
Figure 7: Lighthouse v2 mini-mote calibration board.

localization system. It can be attached to any object that needs to be tracked in 3D space (such as robot, or an elbow joint), and it will relay its location through an radio module embedded in the PCB.

The mini-mote calibration board, shown in Fig. 7, is a 3D printed calibration board allows the placement of up to twelve mini-mote in a 5 by 5 centimeter grid with high degree of precision. It can then serve as a reference to measure and correct any distortion or misalignment found in the lighthouse v2 basestation hardware.

The visually tracked lighthouse basestations, shown in Fig. 8, are specially prepared lighthouse basestation can be tracked in 3D space with a high accuracy optical motion capture system. This setup allows us to measure the accuracy of the lighthouse localization system.

7.2.3 AIOT Systems

AIOT Systems is a one-stop shop for learning embedded low-power wireless. The AIOT Play board, shown in Fig. 9, is a ready-to-learn-on platform, designed specifically to be both easy to learn with, and close to an production system. It features a prototyping area allowing a student to build little circuits directly

Figure 8: Visually tracked Lighthouse v2 basestation
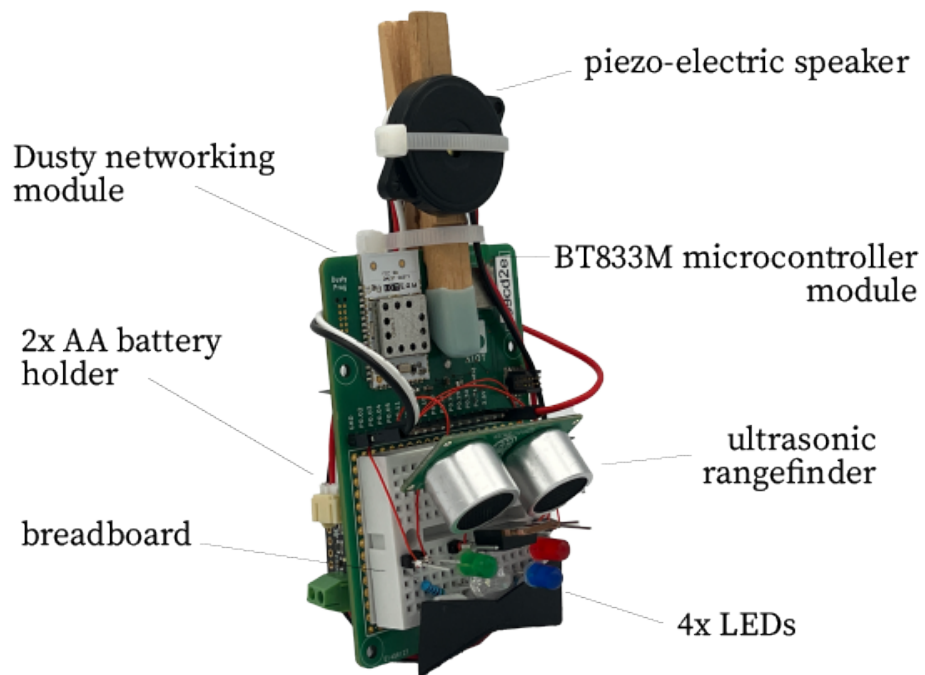
Figure 9: The AIOT Play board equipped with sensors and a speaker, ready to be deployed in the Inria Expo.
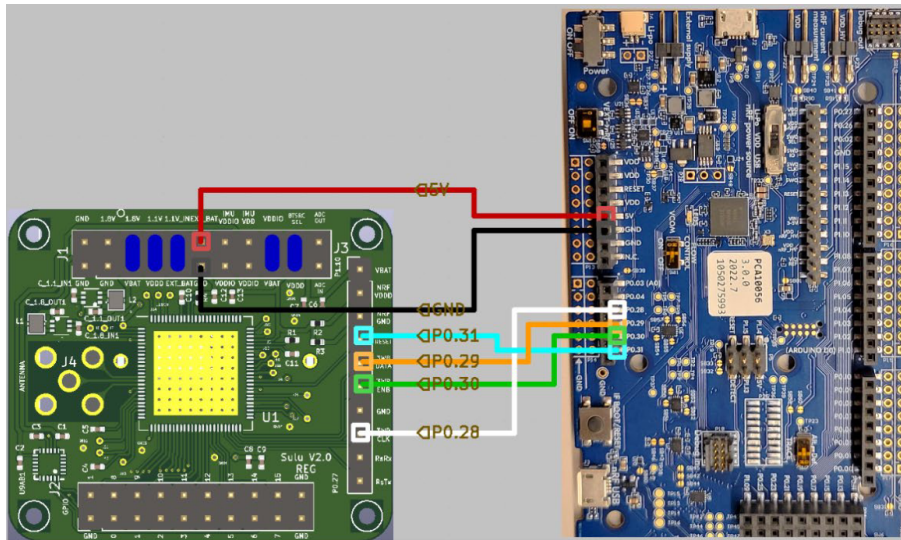
Figure 10: The Single Chip Mote test platform with external programming bootstrapping

on the board. They then write firmware directly on the fully programmable micro-controller to interact with the circuit, and hand the data to the true mesh networking module. The source code consists of Python code that runs on a computer, and C code that runs on a micro-controller. The source code is developed under an open-source license so students can really see how things are working, and use it beyond learning. We crafted the AIOT Systems Academy so it is a completely self-contained set of course material. The AIOT Systems Academy is a collection of dozens of short labs. For instructors, the material is ready to present.

In 2023, we have started working with the Inria Expo to use AIOT Play boards in its permanent exhibition. That is, 20 AIOT Play boards are being installed on the elements of the computer science exhibition, allowing visitors to understand the concept of mesh networking. In addition,

More information at www.aiotsystems.org.

7.2.4 Single Chip Mote Testbeds

A number of testbeds have been developed for experiments concerning crystal-free wireless communication. These include combinations of the mote chips themselves in conjunction with commercial off-the-shelf wireless and wired hardware that are used for programming, networking, and performance benchmarking.

These testbeds are used extensively in networking research as part of a number of projects including: an investigation of security vulnerabilities of single-chip wireless systems (part of the PhD work of Sara Faour), as part of the PEPR-5G project as a low-performance node vulnerable to high-power blockers in high-density high-throughput networks, as well as the SDMote project as the wireless front-end. The chip's digital transmitter inputs and sampled receiver outputs are exposed to an FPGA that can be reconfigured to handle arbitrary transmitted frequency modulations and even more arbitrary (albeit, heavily band-limited) received signal modulations.

7.2.5 SailBot

Autonomous sailing vessels are an attractive target for marine and environmental research: powered by wind, these boats can operate for long periods of time without any human intervention. While on a mission, they collect and analyze sensor data about the environment they are in. Making them autonomous is a technical challenge spanning the fields of (low-power) robotics and sensor networking.

The quality of sensor inputs plays a crucial role for the correct functionality of the system. Decisions such as whether to trim the sails or to adjust the route are all based on the provided sensor inputs: the current position, heading, tilt, wind direction.

Figure 11: The SailBot robotic platform.

Figure 12: Lac Daumesnil: SailBot test site. "Destination waypoint" and "Origin" refer to the locations used for in-situ tests of the SailBot platform in autonomous mode with the goal of crossing the lake.

The AIO team leads the design and testing of a mini autonomous vessel prototype called SailBot. SailBot is a 61 cm×114 cm commercial off-the-shelf replica of a real boat with custom electronics built by the AIO team. The boat is remotely controlled and features an autonomous sailing mode to reach the given waypoint. The project shares low-level implementation details with the DotBot platform, allowing for code reuse.

In 2023, we have tested the SailBot's autonomous sailing mode by doing in-situ tests on Lac Daumesnil in Paris, see Fig. 12. The first test consisted in performing simple radio-controlled manouvers, like keeping course and tacking. The second, more advanced test, consisted in programming the SailBot over its interface to autonomously reach a waypoint at the other side of the lake. Due to the absence of a wind sensor on board, the SailBot's sails were trimmed manually. The SailBot successfully reached the waypoint at the other side of the lake. We had several lessons learnt from the test and we continued the development of the platform. The ultimate goal is for the SailBot to autonomously circle the lake, sailing in all points of sale.

8 New results

The team's research program, summarized in Section 3, is organized around five axes. We present the results of 2023 following the same organization.

8.1 Related to [A1] Smart Dust

8.1.1 A Time Synchronized Multi-Hop Mesh Network with Crystal-Free Nodes

Participants: Filip Maksimovic , David Burnett *(UC Berkeley)* , Thomas Watteyne ,
Kris Pister *(UC Berkeley)*.

For the first time, we have demonstrated a standards-compatible multi-hop crystal-free network that exclusively uses CMOS oscillators. This multi-hop network is built using a time-synchronized channel-hopping protocol that is exclusively limited in performance by the time jitter of on-chip oscillators. The protocol itself is built on an IEEE 802.15.4 physical layer radio that enables simple interoperability with existing protocols academic and industrially supported protocols like 6TiSCH, Thread, and Matter. A calibration-bootstrapped network is demonstrated with a single crystal-enabled off-the-shelf node acting as the root and as the network's time reference.

The protocol is designed both to communicate data and transfer time in a multi-hop mesh while compensating for noisy and drifting oscillators and timers. With a 4 s synchronization period, an experimental implementation of the network maintains, in the absolute worst case, 1.8 ms 3 σ absolute time synchronization and 820 μs 3 σ hop-to-hop synchronization across four hops, under ambient environmental conditions. The resistance to environmental variation is tested by varying one node's supply voltage. With time and frequency feedback from received packets, the node maintains synchronization and connectivity with a supply variation of 2.5 mV/s, which is equivalent to a temperature variation of 10° /min with a beacon period of 2 s.

These results are published in [14].

8.1.2   Implications of Physical Fault Injections on Single Chip Motes

Participants: Sara Faour , Mališa Vučinić , Filip Maksimovic , Thomas Watteyne.

Single-chip motes are wireless sensor nodes that integrate computation,communication, power and sensing on a single chip. We consider the security threats these novel devices are subject to when employed in safety-critical applications. Fault injection attacks are a prominent form of physical attacks that pose a threat to the normal and secure functioning of targeted devices, potentially compromising their intended behavior. These attacks have been studied mainly on commercial off-the-shelf devices which rely on external components such as crystal oscillators and passives. Such external components are absent from single-chip motes, resulting in a uniquely different attack surface compared to commercial systems. In this study, we first survey the features of the common fault injection methods, and then study and compare their implications on single-chip motes. This study has been published as a conference paper [9].

8.2   Related to [A2] Low-Power Wireless Networking

8.2.1   Application Performance Monitoring in the IIoT

Participants: Fabian Graf , Thomas Watteyne.

Application Performance Monitoring (APM) is key for ensuring computer systems perform well. While most APM tools target servers and networking infrastructure, here we focus on APM for devices with strict resource constraints: extremely limited in terms of power, memory and bandwidth. For this research topic, we have conducted an exhaustive literature survey on APM approaches for low-power wireless networks. We survey performance metrics characterizing the network health condition and show how to capture the health of a network universally. Furthermore, the active APM solution "Memfault" has been analyzed. Memfault offers a framework for monitoring these low-power wireless devices. In a proof of concept has been shown that this solution is also suited for networks based on SmartMesh IP. The APM topic will be pursued and extended in terms of Application Performance Management, which targets enhancing the system's performance, as well as reacting on critical trends and events.

8.2.2   Augmenting Low-Power Wireless Network Management through Embedded AI

Participants: Martina Balbi , Thomas Watteyne.

In the context of Time Synchronized Channel Hopping (TSCH) networks, the efficacy of communication lies in the orchestration of a communication schedule. This schedule dictates the actions of each node during specific timeslots, including decisions on transmission, reception, and sleep modes, as well as specifying the communication partner and frequency. The construction of this schedule then becomes determinant, influencing network throughput, battery longevity, and overall reliability. Historically, various approaches, ranging from centralized to distributed, have been employed and designed by networking experts. However, a recent shift has occurred with the availability of microcontrollers equipped with embedded Artificial Intelligence (AI) capabilities. These microcontrollers can autonomously execute AI models, like Convolutional Neural Networks (CNNs), directly at low-power devices, challenging the conventional cloud-centric approach. This integration of embedded AI not only redefines the potential of low-power wireless devices but also introduces new opportunities for optimizing communication schedules, ultimately enhancing the efficiency, adaptability, and reliability of TSCH networks. This research aims to investigate how we can use embedded AI for augmenting the management of TSCH networks, exploring how this transformative integration can reshape low-power wireless communication.

8.2.3   Header Compression in Low-Power Wide-Area Networks (LPWANs)

Participants: Ichrak Kallala , Thomas Watteyne.

The objective of the this work is to establish an automated methodology for the generation of SCHC rules. The resulting algorithms, which we call "CHIC", leverage machine learning methodologies and scrutinize recorded data packet traces to automatically produce SCHC rules for devices and gateways. To evaluate the overall header compression and decompression efficiency on IPv6/UDP headers, we conducted benchmark tests. We carried out a series of performance analyses to gauge the effectiveness of these processes. We also developed a C-based implementation of the compression and decompression routines, which we ported to the nRF5340 dual-core microcontroller. This code is extensively tested to ensure functionality and optimize performance. The automation of these tasks was facilitated by a self-hosted GitHub Actions runner on a Linux machine, that maintains continuous communication with the nRF5340-DK via SSH to expedite the workflow. In addition, we implemented dictionary-based compression and decompression routines, first in Python, then in C for execution on the microcontroller. Thorough testing has validated the success of our approach, with the compression algorithm proving capable of handling a dataset of PCap files. This initiative aimed to integrate with SCHC for payload compression, given SCHC's limitation to header compression exclusively.

8.2.4   Minimal-Overlap Centrality for Multi-Gateway Designation in Real-Time TSCH Networks

Participants: Miguel Gutiérrez Gaitán *(CISTER (Porto))* , Luis Almeida *(CISTER, Porto)* , Pedro M. d'Orey *(CISTER, Porto)* , Pedro M. Santos *(Faculdade de Engenharia da Universidade do Porto, FEUP)* , Thomas Watteyne.

The objective of the this work is to develop a novel centrality-driven gateway designation framework for the improved real-time performance of low-power wireless sensor networks (WSNs) at system design time. We target time-synchronized channel hopping (TSCH) WSNs with centralized network management and multiple gateways with the objective of enhancing traffic schedulability by design. To this aim, we propose a novel network centrality metric termed minimal-overlap centrality that characterizes the overall number of path overlaps between all the active flows in the network when a given node is selected as gateway. The metric is used as a gateway designation criterion to elect as a gateway the node leading

to the minimal number of overlaps. The method is then extended to multiple gateways with the aid of the unsupervised learning method of spectral clustering. Concretely, after a given number of clusters are identified, we use the new metric at each cluster to designate as cluster gateway the node with the least overall number of overlaps. Extensive simulations with random topologies under centralized earliest-deadline-first (EDF) scheduling and shortest-path routing suggest our approach is dominant over traditional centrality metrics from social network analysis, namely, eigenvector, closeness, betweenness, and degree. Notably, our approach reduces by up to 40% the worst-case end-to-end deadline misses achieved by classical centrality-driven gateway designation methods.

This work is published in [7].

8.2.5   Hands-on Evaluation of Kinéis Satellite IoT Technology

Participants: Raul de la Fuente , Thomas Watteyne.

Satellite technology offers exciting new opportunities for IoT applications. This poster shows the performance one may expect using Kinéis – a leading operator – as a representative example. We use an implementation we provide as open-source for repeatability, and measure an end-to-end latency of 45 min, a battery lifetime of 1,000 packet when using a pair of AA batteries, and an end-to-end reliability of 23%/54%/99% when using 1/10/18 repetitions.

This work was published in [12].

8.3   Related to [A3] Security in Constrained Systems

8.3.1   IETF LAKE Standardization

Participants: Mališa Vučinić , Geovane Fedrecheski , Yuxuan Song , Thomas Watteyne.

Context and goal. The Inria AIO team plays a crucial role in the standardization activity on *lightweight security for the Internet of Things* within the Internet Engineering Task Force (IETF). This is a cross-working-group effort, spanning different working groups of the IETF. In that context, we *co-chair* the IETF LAKE working group (Mališa Vučinić), and also participate in the standardization activities in the IETF ACE and IETF IOTOPS working groups.

Summary of activities. The past year has seen the wrap up of the major milestone related to our standardization activity. First, the base publication of the IETF LAKE working group, the EDHOC protocol, has been approved to be published as an RFC. Second, a draft standard we co-author on EDHOC traces [8], has also been wrapped up and approved for publication as an RFC. The publication of these two draft standards concluded the initial work items of the LAKE working group.

The IETF LAKE working group has rechartered in July 2023 to include new work items such as remote attestation and lightweight authorization. Following the new charter, the LAKE working group has formally adopted AIO's draft standard on lightweight authorization (zero-touch onboarding) of IoT devices) . In parallel, our draft standard on lightweight certificate enrollment has been adopted in the IETF ACE working group . Together with a draft standard in the IOTOPS group which compares different security protocols in terms of their overhead , this makes all AIO's documents formally adopted by the IETF and on the path to becoming Internet standards.

8.3.2   A Formally-verified Implementation of IETF LAKE for Microcontrollers

Participants: Geovane Fedrecheski , Mališa Vučinić.

Context and goal. In collaboration with Inria Prosecco and Inria TRIBE in the context of the RIOT-fp Inria Challenge, we have worked on an implementation of the LAKE-EDHOC protocol in Rust. By using Inria Prosecco's hax verification tool, our implementation in Rust can be automatically translated into e.g. F* and so used for formally verifying the implementation against different security properties.

Summary of activities. In 2023, together with external collaborators interested in the implementation, we have significantly reworked the code base and now use vanilla Rust instead of the hacspec language. By using the hax tool, we were able to automatically translate the implementation into F*. In collaboration with Inria Prosecco, we proved panic freedom on the core parts of the protocol, such as the parser and the encoding functions. In parallel, our implementation uses only the features from the core Rust library, making it executable on constrained platforms, see 7.1.1. This makes lakers, the only microcontroller-optimized, formally-verified implementation of LAKE-EDHOC available.

8.3.3 Performance Comparison of EDHOC and DTLS 1.3 in Internet-of-Things Environments

Participants: Geovane Fedrecheski , Mališa Vučinić , Thomas Watteyne.

Authenticated key exchange protocols play a crucial role in the communication security stack of an Internet-of-Things (IoT) device: they authenticate the communicating parties and establish a shared symmetric secret between them. Following a large debate in the community, the Internet Engineering Task Force (IETF) has recently standardized a new protocol called EDHOC for authenticated key exchange targeting IoT environments. The EDHOC protocol performs a compact Diffie-Hellman key exchange handshake, requiring several times less bytes-over-the-air than the de-facto solution used in the Internet, the (D)TLS protocol. In this work, we study how this reduction in message size correlates with the usage of other scarce resources in IoT environments: time, energy, and memory. We evaluate EDHOC and DTLS with different authentication configurations over two IoT radio technologies. First, we measure the EDHOC and DTLS handshakes on constrained hardware over an IEEE 802.15.4 radio. We observe that EDHOC achieves ×6 to ×14 reduction in packet sizes, ×1.44 improvement in handshake duration and ×2.79 reduction in energy consumed. Next, we simulate time on air on LoRaWAN networks and find that, in the most restrictive configuration (SF=12), DTLS uses at least ×7 more time on air than EDHOC. Finally, we measure flash memory and RAM usage, with the EDHOC implementation achieving a ×4 reduction in both. This study has been published as a conference paper [10].

8.3.4 Remote Attestation for Internet-of-Things Swarms

Participants: Yuxuan Song , Mališa Vučinić , Thomas Watteyne.

Remote attestation is a security process which verifies and confirms the integrity and trustworthiness of a remote device or system in the network. The objective of this work is to design, implement and validate techniques for remote attestation that are scalable to large Internet-of-Things swarms. The open challenge is to make the existing techniques scalable, yet practical and secure for Internet-of-Things swarms considered in the scope of the OpenSwarm project.

Since the start of Yuxuan Song thesis in October 2023, we have worked on the state-of-the-art survey about remote attestation techniques for Internet of Things in research and standardization domains. We have read and documented the papers of the existing techniques for remote attestation, and the relevent Internet standards and the drafts of the working groups (especially RATS and LAKE) within the IETF. Right now, we are working on a preliminary draft that specifies how to perform remote attestation via IETF LAKE, based on the Remote ATtestation procedureS (RATS) architecture.

8.3.5 Ensuring Availability of Internet-connected Constrained Wireless Networks

Participants: Elsa Lopez-Perez , Mališa Vučinić , Paul Mühlethaler.

With the global reachability enabled by the IP connectivity, IoT devices are easy Denial-of-Service (DoS) targets. Ensuring service availability has many challenges with battery-powered or energy-harvested IoT devices. Every packet forwarded into the constrained network has an impact on the resource consumption of network nodes. We will study techniques that will enable IoT gateways to filter out the undesired traffic before forwarding it into the IoT network and detect suspicious activity.

Since the start of Elsa Lopez-Perez's thesis in November 2023, the work has consisted in studying the state-of-the-art mitigation techniques against DDoS attacks using constrained Internet-connected devices. The literature shows that, in spite of the current defense mechanisms, DDoS attacks are still a threat and can have serious impact on targeted devices. The current goal is to document the information in a survey paper about IoT related DDoS attacks, including different types of attacks, their technical description, real-world examples of Denial of Service attacks and their impact, and different mitigation techniques that are currently being employed.

8.4   Related to [A4] Swarm Robotics

8.4.1   Lighthouse Localization of Miniature Wireless Robots

Participants: Said Alvarado-Marin , Alexandre Abadie , Filip Maksimovic.

In this work, we apply lighthouse localization, originally designed for virtual reality motion tracking, to positioning and localization of indoor robots. The first contribution is a lighthouse decoding and tracking algorithm on a low-power wireless microcontroller with hardware implemented in a centimeter-scale form factor. One-time scene solving is performed using a variety of standard computer vision techniques. Three different robotic localization scenarios are analyzed in this work. The first is a planar scene with a single lighthouse and four-point pre-calibration. The second is a planar scene with two lighthouses that self-calibrated with either multiple robots in the experimental scene or a single robot in motion. In the 2D case, the absolute accuracy was measured to be 7.25 mm RMS against a camera-based tracking system. In the 3D case, the accuracy was measured to be 5.77 mm RMS as determined by moving the tracking device with a high-accuracy stepper motor. This demonstrates the viability of lighthouse tracking both for smal-scale robotics and as an inexpensive and compact alternative to camera-based localization systems.

This work is currently under review in IEEE Robotics and Automation Letters.

8.4.2   New Version and Enhanced User Experience for the DotBot

Participants: Alexandre Abadie , Said Alvarado-Marin , Filip Maksimovic ,
                      Thomas Watteyne.

We have continued to work hard on the DotBot in 2023. The DotBot is now at the heart of the Horizon Europe OpenSwarm project. A new version of the hardware was released in 2023 and a lot of effort has been put into porting the embedded code base to this new, more powerful, dual-core family of microcontrolers. With the help of Said Alvarado-Marin and Filip Maksimovic, the lighthouse localization have been optimized and made user friendly: it's now incredibly easy to set up a swarm of DotBots in a lab. This allows more complex and more secure applications to be used on DotBots. Thanks to Alexandre Abadie, the code base of the whole infrastructure has gained a lot in maturity and is now fully published under open-source BSD 3-clauses license, from hardware design to the high level web based controls. This project, in particular through the very large partners it brings, serves as a catalyst that will turn our small-scale testbed into a 1,000 DotBot in the next 18 months.

8.4.3   FreeBot, a Battery-Free Swarm Robotics Platform

Participants:	Mengyao Liu *(DistriNet, KU Leuven)* , Fan Yang *(DistriNet, KU Leuven)* , Sam Michiels *(DistriNet, KU Leuven)* , Tom Van Eyck *(DistriNet, KU Leuven)* , Danny Hughes *(DistriNet, KU Leuven)* , Said Alvarado-Marin , Filip Maksimovic , Thomas Watteyne.

A growing range of networked embedded devices are moving away from batteries and towards super-capacitor charge storage. However, mobile robots remain largely dependent upon batteries with slow recharge cycles and limited lifetimes. In this work, we introduce a novel battery-free platform for swarm robotics which features: 24 min of operation running at its top speed of 1.24 km/h, a carrying capacity of over 2.5 kg, full recharge cycles of under 12 s and rapid peer-to-peer charge transfer in the field. This is supported by an nRF52840 Cortex-M4F equipped with BLE/ANT/802.15.4 transceiver. Notably, while the autonomy of FreeBots is limited compared to battery-powered robots, their operational vs charging duty-cycle is significantly higher at over 99%.

This work was published in [13].

8.4.4   Blip: Identifying Boats in a Smart Marina Environment

Participants:	Trifun Savic , Keoma Brun-Laguna *(Wattson Elements)* , Thomas Watteyne.

In this work, we developed Blip, a system for boat identification that uses the existing Internet of Things (IoT) network of sensors deployed inside a smart marina. Blip combines the data from two types of commercial low-power wireless sensors: Falco Presence and Falco Boat. The former is deployed on the pontoons, to detect boats that dock at the slips. The latter is installed inside the boats' cabins to monitor various parameters and trigger an alarm in case of: intrusion, fire, shock and tilt. To identify a boat, we fuse the boat presence events from the Falco Presence devices and the health reports from a Falco Boat. The health reports contain information about nearby Falco Presence devices and their received signal strength (known as Received Signal Strength Indicator or RSSI). When a boat enters the marina, Falco Boat joins the network and starts sending health reports. Initially, Blip estimates the slip location assigning the boat to the slip where a Falco Presence has the strongest RSSI. Then, Blip selects the closest slip to it, which changed to occupied in a given time window. We validate our system using a historical dataset from a marina over a period of 4 months. Every slip in the marina is equipped with a Falco Presence device, and 8 boats are equipped with a Falco Boat device. The results show that the Blip system identifies boats upon entering the marina with 100% accuracy. The main advantage of the Blip system is that it provides location-aware service to the marina without any additional cost or hardware deployments.

This work was published in [16].

8.4.5   WELOC: Localizing Equipment in Marinas using Ultrasound

Participants:	Trifun Savic , Keoma Brun-Laguna *(Wattson Elements)* , Thomas Watteyne.

In this work, we proposed WELOC, an ultrasoundbased localization system for localizing objects in a marina environment. WELOC uses the already installed infrastructure of commercial battery-powered IoT devices, with several years of autonomy, fixed at each slip on the pontoons, used for boat presence monitoring. These devices are equipped with an ultrasound sensor, have known GPS positions and form a wireless, time-synchronized (<15 us synchronization error), mesh network around the gateway. Without impacting the main function of the smart parking system for boats, we propose a scheme to schedule when each ultrasound sensor is triggered. We design a mobile device, from an off-the-shelf

ultrasound sensor, compatible with those already present in marinas. We synchronize the device with each ultrasound trigger in the marina, and collect the timestamped distance measurements. The location of the mobile device is then computed using trilateration. We test the ranging accuracy of the mobile device in the lab, where we achieve a 3.5 cm mean absolute error, with a maximum range of 10 m. We perform field testing for the ultrasound signal detection inside the marina, which is equipped with 471 presence sensors, one at each of its slips. We show that our mobile device successfully detects the ultrasound signal on the pontoons.

This work was published in [17].

8.4.6 Context-Aware Information Gathering and Processing Towards Supporting Autonomous Systems in Industry 4.0 Scenarios

Participants: Razanne Abu Aisheh , Thomas Watteyne.

Industry 4.0 environments are characterized by the coexistence of a diverse set of devices, including sensors, mixed-reality displays, robots, drones, and smart objects. These systems must be capable of autonomously taking critical in-time decisions necessary to perform complex tasks without human input. One essential application for Industry 4.0 is multi-robot exploration and mapping of unknown environments, especially in critical missions such as hazard detection and search and rescue. These missions share the need to reach full coverage of the explorable space in the shortest time possible. To minimize completion time, robots in the fleet must be able to exchange information about the environment reliably with one another. However, existing exploration and mapping algorithms suffer from inaccuracies and inefficiencies due to their lack of contextual awareness of their surroundings, especially in terms of communications, lacking flexibility and adaptability to the environment, and hence, adding unnecessary delay to the mission at hand.

In this work, we investigate the impact of communication awareness on the performance of multi-robot exploration and mapping expeditions, in terms of time to completion. We evaluate existing research in the field and demonstrate the impact of not considering communication impairments when designing such algorithms. From there, we propose Atlas, an exploration and mapping algorithm that natively takes packet loss into account, with a 100% completion ratio even with Packet Delivery Ratios (PDRs) as low as 0.1. However, Atlas on its own cannot handle scenarios where connectivity is completely lost. It also adds a significant delay to the completion of the mission, as lost packets keep getting re-transmitted periodically until they are received. One solution is relay placement. Most research on relay placement for multi-robot expeditions tend to fall into two categories. First, communication-aware relay placement based on initial Received Signal Strength Indicator (RSSI) is used. However, this requires running a full mission prior to the exploration to find the optimal position for the relays to be placed. Second, maintaining a distance (specified prior to the mission) between relays and exploration robots. These methods add to the time it takes to complete the mission. The research question becomes how can we place relays to maintain communication as reliable as possible, and also dynamically throughout the exploration mission without prior knowledge of the environment, in a way that reduces delay to the exploration and mapping time to completion. We solve this by proposing "Connectivity Aware Relay Algorithm" (CARA), a dynamic context-aware relay placement algorithm that does not require any prior knowledge of the environment. We developed an open-source simulator for multi-robot expeditions which we used to test both algorithms against state-of-the-art algorithms. Using both Atlas and CARA results in a dynamic context-aware multi-robot expedition that autonomously builds a map of a fully unknown environment, while dynamically placing relays when needed to maintain connectivity that outperforms state-of-the-art algorithms, in terms of time to completion, by a factor of 10.

This work was published in [19].

8.4.7   Localization in Constrained Environments

Participants: Trifun Savic , Thomas Watteyne.

This work focuses on low-power localization in constrained environments, without the need for localization infrastructure. We consider two target use cases: localizing boats in a marina, and localizing mobile robots in an indoor environment. We start by evaluating two RF-based Real-Time Localization Systems (RTLS), based on Bluetooth Angle-of-Arrival and Ultra-Wide Band ranging. Their main drawbacks are that they require the prior deployment of anchors and are not low power, making them poorly compatible with our target use cases. This work contributes to addressing these drawbacks by proposing two novel systems: WELOC and Blip. We further propose RRDV, a robot encounter detection solution for multi-robot systems. WELOC is an ultrasound-based localization system that re-purposes boat presence detection sensors already deployed in the marina. It features a scheduling scheme that triggers each presence sensors' ultrasonic transceiver at specific times. WELOC introduces a battery-powered mobile device capable of securely communicating with both ultrasound and radio signals, designed entirely from off-the-shelf components. Real-world tests in a real-life marina in the South of France show a mobile device can be localized with cm-level accuracy when it is up to 10 m away from presence sensors. Blip is a system for boat identification in a marina, which only requires a software update to existing smart marina sensor systems. It uses the information from already installed boat monitoring sensors (mounted in a boat's cabin), and combines that with the information from the fixed infrastructure of presence sensors to identify boats on slips. In our real-world tests, the system exhibits 100% boat identification accuracy. This work further proposes RRDV, a system for detecting robot-to-robot encounters in a multi-robot system. Many robots are already equipped with an ultrasound sensor for measuring the distance to objects in front of them. RRDV is a software update to those robots, allowing them to use those ultrasound sensors for detecting encounters with other robots. When testing RRDV on a real-world multi-robot system, it correctly detects 96.7% of the times two robots face one another for 5 s or more. The work contributes to the growing research field of localization and low-power wireless by proposing innovative solutions for low-power and accurate localization in constrained environments. While these solutions have countless applications well beyond the ones outlined in this work, we chose the use cases of localization of boats in marinas and localization of robots in an indoor environment to remain perfectly focused. The work demonstrates the effectiveness of ultrasound-based systems and highlights the potential of ubiquitous off-the-shelf hardware for the development of localization systems.

This work was published in [20].

8.5   Related to [A5] Vehicle Area Networking – FANETs – Network Models

8.5.1   Optimization of Security Messages in VANETS

Participants: Nadjib Achir *(Inria Saclay)* , Paul Mühlethaler.

Cooperative Awareness Messages (CAM) is an essential service in VANETs, allowing vehicles to transmit radio beacons containing their positions and velocities. These messages inform nearby vehicles about the traffic situation. This work focuses on Extended Cooperative Awareness Messages (ECAM), which include additional information about nearby vehicles. ECAM beacons consist of a vehicle's speed, position, and data on the positions and velocities of other vehicles in its vicinity. This comprehensive information enables nearby vehicles to understand the traffic situation and take appropriate actions to prevent potential collisions. Studies demonstrate that ECAM has the potential to significantly improve road safety by providing comprehensive and up-todate traffic information. This work uses stochastic geometry to evaluate different versions of ECAM services and compare the results with simple simulations. The evaluation assumes random vehicle placement using a homogeneous Poisson Point Process and models the ECAM service using the Matern Point Process.

VANETs are continuously progressing, bringing benefits that can improve road safety at multiple levels. CAMs are messages that carry the nodes' positions and speed and thus can be very useful to

increase safety in vehicular networks. But the amount of traffic in terms of the number of packets sent can rapidly be high, and optimizations are very useful. In an ECAM a vehicle sends in addition to its speed and position the positions and speeds of vehicles within its sensors' range. In this work, we discuss algorithms to select the vehicles which send these ECAMs. We have shown that the benefit of these algorithms is important. We have also proposed an analytical model based on the Matern process which evaluates the number of vehicles sending ECAMs in the random and greedy approach. Thus one can easily evaluate the gain obtained with ECAMs compared with when every vehicle sends classical CAMs. With reasonable figures, we show that the gain in bandwidth can be easily evaluated using a model derived from the Matern selection process. This gain remains large in normal conditions of utilization.

This work was published in [15]

8.5.2   A Deep Learning Approach to Topology Configuration in Multi-Hop Wireless Networks with Directional Antennas

Participants: Cedric Adjih *(Inria TRiBE)* , Felix Marcoccia , Paul Mühlethaler.

Multi-hop wireless networks can be optimized using directional antennas, as they allow for in-depth interference management and network topology optimization. This type of optimization involves ensuring high operational guarantees such as instantaneous connectivity, minimum SNRs and SINRs thresholds, and improved QoS. It simplifies tasks of future network layers and allows for more relaxed routing protocols and scheduling. However, attaining optimal performance via network configuration involves selecting an antenna orientation for each node to create a link with another node. This is challenging, especially when the process is carried out in real-time. To tackle this challenge, we present nodes2net, a Deep Neural Network (DNN) that is trained to imitate solved, ideal network instances. This approach uses nodes' positions as inputs and produces a set of links as output. By leveraging learning of patterns and theoretically driven properties, nodes2net can generate reliable network configuration solutions when dealing with new sets of node positions. It utilizes efficient neural network aggregation operators to facilitate and process information about the nodes, to finally produce the final solution as set of links. Our results demonstrate the competitive performance of this method.

With nodes2net ([18]), we provide an effective framework to allow for a constant time and flexible network creation, which can be really useful, especially in the here described field of wireless network topology optimization, where solving optimization problems on the go, or using online convergence algorithms, are not possible. Using Attention between nodes as a feature extractor suits our problem well and allows to efficiently capture features between nodes while respecting permutation invariance and without suffering from over smoothing of the input signal. We derived a variational inference formulation that overcomes the theoretical limit of supervised learning for a non-deterministic problem. The good inductive bias that our model seems to present are confirmed by our experiments. Future work will aim at improving even further the generalization capabilities and allowing to enforce strict respect of constraints. Future work will also consist in more applicative studies to jump from our Deep Learning method to a whole operational network solution and measure the performance and the QoS we can expect from it. We will also work on the integration of such a neural network on embedded devices. Given that the model is small and can be parallelized, and in view of the recent advances in network quantization and pruning, real time graph prediction seems realistic.

We continue the previous work in the same framework of FANETs and directional antennas. We tackle throughout this work the problem of inferring optimized network topologies in constant time with a Deep Neural Network with strong theoretical generalization properties that is trained to imitate a dataset following a given algorithm (a Integer Programming solver in our case). We cover the notion of Permutation invariance and how important it is when dealing with graphs. We then showed how Attention is a perfect feature aggregator for such graph problematics and proposed several versions of Attention-based models from a pure Attention model using attention scores as predictions to Graph Transformers. Some additional architecture elements to Graph Transformers, namely U-shaped skip connections and Registers have been implemented to help us tackling our problem. We obtain very satisfactory results that highlight the utility of the components of our models. We hence provide a flexible,

constant time model that provides trustable topologies of network links given the nodes' positions. It can greatly help instantaneously reaching some very important structural properties (connectedness...) and feature the desirable traits of the graphs that we train the model on. We highlighted the capacities of the different proposed architectures their contribution to the expressivity of the and the robustness of the predicted links. We hope our work has highlighted the interest of using Deep Learning methods to tackle combinatorial problems by turning them into monolithic global graph generation problems. Future steps will aim at improving the reliability of the inferred topologies, possibly by introducing some link pruning algorithms. While this work is purely focused on one-shot generation of graphs, we will also investigate more progressive methods such as Denoising Diffusion Probabilistic Models, which follow similar "global generation" baselines but in an Langevin-dynamic-ish formulation.

This work was presented at MLN 2023.

8.5.3   Q-learning based Cache Pollution Attack Mitigation Approach for Named Data Networking

Participants: Abdelhak Hidouri *(FSG-Tunisia)* , Haifa Touati *(FSG-Tunisia)* , Mohamed Elhadad *(Abu Dhabi University)* , Nasreddine Hajlaoui *(FSG-Tunisia)* , Paul Mühlethaler , Samia Bouzefrane *(CNAM Paris).*

The Cache Pollution Attack (CPA) is a recent threat that poses a significant risk to Named Data Networks (NDN). This attack can impact the caching process in various ways, such as causing increased cache misses for legitimate users, delays in data retrieval, and exhaustion of resources in NDN routers. Despite the numerous countermeasures suggested in the literature for CPA, many of them have detrimental effects on the NDN components. In this paper, we introduce Q-ICAN, a novel intelligent technique for detecting and mitigating cache pollution attacks in NDN. More specifically, Q-ICAN uses Q-Learning as an automated CPA prediction mechanism. Each NDN router integrates a reinforcement learning agent that utilizes impactful metrics such as the variation of the Cache Hit Ratio (CHR) and the interest inter-arrival time to learn how to differentiate between malicious and legitimate interests. We conducted several simulations using NDNSim to assess the effectiveness of our solution in terms of Cache Hit Ratio (CHR), Average Retrieval Delay (ARD) and multiple artificial intelligence evaluation metrics such as accuracy, precision, recall, etc. The obtained results confirm that Q-ICAN detects CPA attacks with a 95.09% accuracy rate, achieves a 94% CHR, and reduces ARD by 18%. Additionally, Q-ICAN adheres to the security policy of the NDN architecture and consumes fewer resources from NDN routers compared to existing state-of-the-art solutions.

NDN is susceptible to several vulnerabilities that can severely disrupt the functionality of its essential components. CPA is one of the most harmful attacks, with the highest impact on the availability of contents in the cache of the CS. Multiple mitigation mechanisms have been suggested by the researcher for such attack, but the question always remains: whether the attack is still effective under all these mitigation mechanisms and whether these mechanisms negatively affect the performance of the essential components of NDN. In this paper, we propose Q-ICAN, a lightweight detection and mitigation mechanism that relies on the Q-Learning algorithm to prevent CPA attacks. Through several simulations, Q-ICAN has demonstrated its beneficial effect on mitigating the cache of the CS, using a variety of metrics that directly relate to the CS and consumers within the same security path. Furthermore, our real-time detection and mitigation mechanism exhibits high accuracy in detecting the presence of the attack and defending the core of the CS. Moreover, it improves the cache process, leading to better performance even in the normal state where no attack is present.

Although Q-ICAN has proven to be an effective countermeasure implemented in each router of the NDN network to detect and mitigate CPA attacks. our future work entails designing a collaborative communication system among Q-ICAN agents to provide even greater protection. Specifically, we aim to create a global model of Q-ICAN that can communicate with the sub-model in each NDN router, facilitating the sharing of information about suspected attacks and enabling early-stage mitigation. Furthermore, we plan to investigate the use of Deep Reinforcement Learning (DRL) to optimize the performance of our agents. Our objective is to enhance the detection rate of malicious attacks through the application of advanced deep learning techniques.

8.5.4 A Deep Reinforcement Learning and Sensing Based Irregular Repetion Slotted Aloha (IRSA)

Participants: Iman Hmedoush *(Nokia)* , Pengwenlong Gu *(Inria TRiBE)* , Cedric Adjih *(Inria TRiBE)* , Paul Mühlethaler , Ahmed Serhouchni *(Telecom Paris)*.

One of the main difficulties to enable the future scaling of IoT networks is the issue of massive connectivity. Recently, Modern Random Access protocols have emerged as a promising solution to provide massive connections for IoT. One main protocol of this family is Irregular Repetition Slotted Aloha (IRSA), which can asymptotically reach the optimal throughput of 1 packet/slot. Despite this, the problem is not yet solved due to lower throughput in non-asymptotic cases with smaller frame sizes. In this study, we propose a new variant of IRSA protocol named Deep-Learning and Sensing-based IRSA (DS-IRSA) to optimise the performance of IRSA in short frame IoTs, where a sensing phase is added before the transmission phase and users' actions in both phases are managed by a deep reinforcement learning (DRL) method. Our goal is to learn to interact and ultimately to learn a sensing protocol entirely through Deep Learning. In this way, active users can coordinate well with each other and the throughput of the whole system can be well improved. Simulation results show that our proposed scheme convergence quickly towards the optimal performance of almost 1 packet/slot for small frame sizes and with enough minislots and can achieve higher throughput in almost all cases.

This work was published in [11]

8.5.5 A Decentralized Blockchain-based Platform for Secure Data Sharing in Cloud Storage Mode

Participants: Houaida Ghanmi *(FSG-Tunisia)* , Nasreddine Hajlaoui *(FSG-Tunisia)* , Haifa Touati *(FSG-Tunisia)* , Mohamed Elhadad *(Abu Dhabi University)* , Paul Mühlethaler , Saadi Boudjit *(L2TI - Paris 13)*.

In recent years, cloud-based storage systems have played a crucial role in facilitating secure user communication. These systems enable businesses to gain convenient, on-demand network access to a shared pool of configurable computing resources and effectively reduce overall costs by outsourcing the necessary services. However, it introduces new security challenges in management and control, specifically related to secure services and data sharing in distributed databases. In addition, until now there are still limits, especially in terms of security, access control, and centralization problems. In this study, we propose a secure distributed cloud file storage and sharing system based on the Ethereum blockchain and Interplane- tary File System (IPFS) to address these shortcomings. First, we encrypt data with the AES symmetric algorithm before storing it on IPFS, to resolve data leaks and tampering in centralized cloud storage. Second, we implement a distributed and reliable access control policy by sharing the list of authorized users on the blockchain network as a smart contract. We use the ECC algorithm to share encryption keys between data owners and users. Our solution is designed to ensure secure commu- nication, data storage reliability over IPFS, and data controllability without relying on a centralized cloud storage architecture. Finally, the proposed scheme was tested and evaluated on the Ethereum test network. Performance evaluation shows that our system provides a feasible and reliable environment and could effectively resist both isolated and collaborative attackers, as well as untrusted cloud servers.

8.5.6 Management of datacenter job queues

Participants: Ruben Milocco *(Neuquen University)* , Paul Mühlethaler , Eric Renault *(ESIEE)* , Selma Boumerdassi *(CNAM Paris)*.

Dynamic programming is often used to study a system with constraints such as the distribution of jobs in a data-center. This technique is accompanied by a drawback, namely it is highly difficult to obtain

an explicit control law. This article presents how to make the management of datacenter job queues optimal using the lifting approach. First, we demonstrate the efficiency of our proposal with the support of a mathematical model. Then, the application of our method applied on a data set provided by Google shows its effectiveness.

Both optimal and suboptimal strategies exhibit similar performance. This similarity is attributed to the potential improvement achieved with the optimal design being lost in the errors of the estimated variance of vk (prediction error) , which must be performed in real-time. On the other hand, the suboptimal strategy offers several advantages: (i) it does not require knowledge of the probability density function of vk; (ii) it has an explicit solution, hence eliminating the need for numerical minimization to obtain the optimal offer quantity; (iii) the unserved demand will always be constrained to its minimum possible value at any given time, regardless of the size of the considered dispatching period T.

We plan to propose this work to one of these conferences: OLA, ACM SIGMETRICS, AnNet 2024, DDINS.

8.5.7   A Markovian analysis of an IEEE-802.11 station with buffering

Participants: Guy Fayolle *(Dr Emerite)* , Paul Mühlethaler.

The purpose of this study ([21] is to analyze the so-called backoff technique of the IEEE 802.11 protocol with buffers. In contrast to existing models, packets arriving when a station (or node) is in backoff state are not discarded, but are stored in a buffer of infinite capacity. As in previous studies, the key point of our analysis hinges on the assumption that the time on the channel is viewed as a random succession of transmission slots (whose duration corresponds to the length of a packet) and mini-slots during which the backoff of the station is decremented. These events occur independently, with given probabilities and there is a Poisson external process. The state of a node is represented by a three-dimensional Markov chain in discrete-time, formed by the triple (backoff counter, number of packets at the station and the transmission attempt number). The stability (ergodicity) conditions are obtained for an arbitrary station and interpreted in terms of maximum throughput. Several approximations related to these models are also discussed.

9   Bilateral contracts and grants with industry

9.1   Bilateral contracts with industry

- Orange Labs: Thomas Watteyne and Paul Mühlethaler lead a joint project on "CHIC: Automated Rule Generation for SCHC".

- Analog Devices: Thomas Watteyne co-supervises the CIFRE PhD thesis of Martina Balbi.

- Siemens: Thomas Watteyne co-supervises the CIFRE PhD thesis of Fabian Graf on "Application Performance Management of Smart Field Devices for the Industrial Internet of Things".

- Wattson Elements: Thomas Watteyne co-supervises the CIFRE PhD thesis of Trifun Savic on "Localization in Constrained Environments".

- Nokia: Thomas Watteyne co-supervises the CIFRE PhD thesis of Razanne Abu Aisheh on "Context-Aware Information Gathering and Processing Towards Supporting Autonomous Systems in Industry 4.0 Scenarios".

- Thales: Paul Mühlethaler co-supervises the CIFRE PhD thesis of Felix Marcoccia on "Machine Learning Techniques for MANETs".

9.2   Collaboration with industry

- Ericsson: Mališa Vučinić co-authors multiple IETF draft standards with Ericsson. We are organizing together a Hackathon on "Lightweight Security for the Internet of Things" in May 2024 in Paris.

9.3   Spin-Off

The team spun off startup Falco (www.wefalco.fr) in 2019. The company continues to develop fast. After winning the Innovation Competition of the 2019 Paris Nautic Show, Falco was recipient of the i-Lab award, the largest Innovation competition for startup companies in France, in July 2020. Falco received the IoT Award of the Embedded Trophy ("Trophés de l'Embarqué, catégorie "IoT Grand Public") in 2022, an annual innovation competition organized in partnership with the French Ministry of Economy. The Falco solution is now deployed in 38 marinas; the Falco team is now 12 people. The relationship remains very tight with the AIO team, both formally – through the CIFRE of Trifun Savic, the contract of Romain Facq and the OpenSwarm – project, but also informally, as many Falco people are closely related to the research team.

10   Partnerships and cooperations

10.1   International initiatives

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

SWARM

Title: Robust Communication and Localization for Swarms of Mobile Miniaturized Wireless Motes

Duration: 2021 -> 2023

Coordinator: Kris Pister (pister@eecs.berkeley.edu)

Partners:

- University of California, Berkeley (USA)

Inria contact: Thomas Watteyne

Summary: Micro-motes are a breakthrough technology which offers communication and computation capabilities in a single-chip design the size of a grain of rice. Our long-term vision is to use micro-motes at the heart of micro-robots to form swarms of coordinated ant-sized micro-robots. These swarms can carry out missions in small and hard-to-reach places. One example is exploring and mapping the internal structure of a collapsed building after an earthquake. A micro-mote has no stable crystal oscillator, only an unstable internal oscillating circuit. This requires us to completely re-think time-keeping by using the network as a time source. This research changes the foundations of low-power wireless and opens up new research domains on micro-motes and micro-robots.

10.1.2   Others

The AIO team hosted Raul de la Fuente, Student at the Unversity of Chile, as part of an Inria Chile's internship program. This stay was very succesful, with the publication of a paper [12] as an outcome of his internship.

10.2   International research visitors

10.2.1   Visits of international scientists

Inria International Chair   Prof. Branko Kerkez, who is an Arthur F. Thurnau Associate Professor of Civil and Environmental Engineering and the University of Michigan, obtained a Inria International Chair position in the AIO team.

Other international visits to the team

- Prof. Ruben Milocco

  - status: Professor
  - Institution of origin: U. del Comahue
  - Country: Argentina
  - Dates: 1-May-2023 to 10-Jun-2023
  - Type of mobility: invited professor

- Prof. Leila Saidane

  - status: Professor
  - Institution of origin: National School of Computer Science (ENSI)
  - Country: Tunisia
  - Dates: 13-Feb-2023 to 13-Mar-2023
  - Type of mobility: invited professor

10.2.2   Visits to international teams

Filip Maksimovic visited Universidad Technica de Santa Maria in Valparaiso, Chile.
Filip Maksimovic visited the University of California in Berkeley, USA.

10.3   European initiatives

10.3.1   Horizon Europe

The Horizon Europe OpenSwarm Project (www.openswarm.eu) started in 2023. Inria is the coordinator the project with Thomas Watteyne serving as scientific coordinator and Clotilde Monnet as Project Manager.

Low-power wireless technology tends to be used today for simple monitoring applications, in which raw sensor data is reported periodically to a server for analysis. The ambition of the Horizon Europe OpenSwarm project is to trigger the next revolution in these data-driven systems by developing true collaborative and distributed smart nodes, through groundbreaking R&I in three technological pillars: efficient networking and management of smart nodes, collaborative energy-aware Artificial Intelligence (AI), and energy-aware swarm programming. Results are implemented in an open software package called "OpenSwarm", which is verified in our labs on two 1,000 node testbeds. OpenSwarm is then validated in five real-world proof-of-concept use cases, covering four application domains: Renewable Energy Community (Cities & Community), Supporting Human Workers in Harvesting (Environmental), Ocean Noise Pollution Monitoring (Environmental), Health and Safety in Industrial Production Sites (Industrial/Health), Moving Networks in Trains (Mobility). A comprehensive dissemination, exploitation, and communication plan (including a diverse range of activities related to standardization, educational and outreach, open science, and startup formations) amplifies the expected impacts of OpenSwarm, achieving a step change enabling novel, future energy-aware swarms of collaborative smart nodes with wide range benefits for the environment, industries, and society.

The project brings together nine partners: Inria (France, coordinator), Analog Devices (Ireland), IMEC (Belgium), Ingeniarius (Portugal), KU Leuven (Belgium), Siemens (Germany), Siemens (Austria), the University of Sheffield (United Kingdom) and Wattson Elements (France). It runs from January 2023 to April 2026.

10.3.2   Other european programs/initiatives

- Thomas Watteyne became a member of the DISCOVER-US Horizon Europe Coordination Action in December 2023

- Trifun Savic became a member of the Montenegrin Artificial Intelligence Association (MAIA) in July 2023

10.4 National initiatives

10.4.1 Inria Exploratory Research Action: AEx SDMote, 2021-2024

The goal of the SDMote project is to develop a software-reconfigurable wireless hardware platform, consisting of a low-power FPGA running a RISC-V soft core and a wide-band wireless transceiver. This entire battery-powered embedded platform is open-source. SDMote is the next-generation IoT hardware that empowers the research community to design custom digital peripherals and radio configurations, giving it the ultimate flexibility to address applications that cannot be addressed with today's off-the-shelf motes. Filip Maksimovic leads.

The current state of the project is primarily development in software. Customizable RISC-V soft cores have been synthesized and ported to FPGAs with both memory mapped and peripherally accessible interfaces to custom digital receiver hardware. At the moment, this still uses closed-source and proprietary synthesis tools, but work is progressing on an open-source flow. The wireless front-end that is used is a fairly limited custom integrated circuit. Work with a multi-application off-the-shelf transceiver is underway.

10.4.2 Inria Project Lab: IPL RIOT-fp, 2019-2023

IPL RIOT-fp

Title: A cybersecurity-focused distribution of RIOT

Duration: 2019 -> 2023

Coordinator: Emmanuel Baccelli (emmanuel.baccelli@inria.fr)

Partners:

- Inria AIO
- Inria EPICURE
- Inria GRACE
- Inria PROSECCO
- Inria TEA
- Inria TRiBE

Inria AIO contact: Mališa Vučinić

Summary: RIOT-fp is a research project on cyber-security targeting low-end, microcontroller-based IoT devices, on which run operating systems such as RIOT and a low-power network stack.

10.4.3 PEPR 5G - Small Connected Devices in Large Numbers

The goal of this subject is an investigation of both the limitations of extremely size-limited (millimeter-scale) wireless communication devices as well as their ability to maintain reliable communication in unfavorable and changing wireless environments. These tiny devices have short range due to low antenna gain, low transmit power, and low receive sesitivity. However, networks of these devices create new opportunities with applications in micro-robotics, high resolution sensing, and smart medicine.

Experiments will be performed both with an academic research platform and with off-the-shelf hardware designed for wireless mesh networking. A number of performance metrics will be evaluated on these experimental hardware platforms including individual and network-level energy consumption, packet delivery rate, and latency. Furthermore, the coexistence of crystal-free and crystal-enabled de17 vices will be investigated. A crystal-free network has the potential benefit of further miniaturization and reduced energy consumption, but requires overhead due to consistent requirement to maintain time and channel. Additional concerns that merit investigation in networks with large numbers of elements are the tradeoffs between reliability and latency and the effects of of receive and transmit linearity on packet delivery. There exists a fundamental tradeoff between network traffic and energy consumption.

For crystal-free devices, this tradeoff is exacerbated by requiring more keepalive packets if there is a faster change in their environment (like a rapid temperature change). Because of their limited resources, an investigation of the security vulnerabilities of both the devices and their networks is necessary, as proven by recent IoT BotNet denial-of-service attacks. The final portion of the project will be deployments of these large scale sensor networks for agricultural monitoring, early-warning wildfire detection with temperature sensing, and an evaluation of network performance and adaptation in a changing wireless channel by building a time synchronized mesh network on a swarm of robots.

The expected outcomes are: a simulated evaluation of energy optimization of crystal-free mesh networks with experimental validation, an evaluation of the security requirements for miniature wireless devices, and real-world deployments that stress the reliability of the network when latency is critical (by testing the control of a large number of connected swarm robots) and when packet delivery and minimal energy consumption are critical (in a smart-agriculture monitoring application).

10.4.4 PEPR 5G - NF-HISEC

Title: End-to-End Security for the Network of the Future

Duration: 2023 -> 2028

Coordinator: Hervé Debar (herve.debar@telecom-sudparis.eu)

Partners:

- Institute Mines-Télécom
- CEA-List
- CNRS
- Eurecom
- Inria AIO
- Inria RESIST

Inria AIO contact: Mališa Vučinić

Summary: The HiSec project focuses on cyber-security issues in future networks. These networks have played a key role in service delivery for digital infrastructures. These new networking technologies have also penetrated essential and critical services for our daily lives, such as energy, transportation or healthcare. The pervasive use of digital services and networks to control these critical infrastructures significantly increases the attack surface and the opportunities for attackers. We regularly observe attacks against these infrastructures, leading to successful compromise and very significant impacts. The objective of the NF-HiSec project is thus to handle cybersecurity issues in these environments, and propose new mechanisms to protect these networks and detect attacks, attacks against the networking infrastructure itself, or against the services hosted or the users of the network.

11 Dissemination

11.1 Scientific Citizenship

11.1.1 Organization

- Thomas Watteyne and Filip Maksimovic were general co-chairs of the Invited Workshop on Crystal-Free Radios, Chip-Scale Wireless Systems and Swarms, Paris, 12-14 September 2023.

- Filip Maksimovic was a chair of a session titled "Federated Learning" at IEEE GLOBECOM in December 2023.

- Paul Mühlethaler has been co-organizer with Thierry Plesse of the Inria-DGA seminar day. In 2023, the topic was 'Blockchain and Networks' and took place May 31 at Inria Paris. Nine presentations were given, four frome industrial companies and five from academic itenties.

11.1.2 General chair

- Paul Mühlethaler has been Honorary Chair and organizer of the 12th IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks, Berlin 27-29 September 2023. During this conference four keynotes were presented from hightly recognized presenters. Twelve international publications were presented during four sessions.

- Paul Mühlethaler has been Co-Chair and organizer of the 6th International Conference on Machine Learning for Networking (MLN 2023), 28-30 November 2023 Paris. During this conference four keynotes were presented from hightly recognized presenters. Twenty international publications were presented during five sessions.

11.1.3 Member of the organizing committees

- Paul Mühlethaler is member of organizing committees for the IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN) and for the International Conference on Machine Learning for Networking (MLN)

11.1.4 Journal Reviewer

- Paul Mühlethaler is reviewer for the Ad Hoc Networks journal, the Annals of Telecommunications journal, the IEEE Transactions on Industrial Informatics journal, the Internet of things journal, the JSAN journal (Journal of Sensor and Actuator networks), the Pervasive and Mobile Computing journal, the Vehicular Communications network .

- Mališa Vučinić is a reviewer for the IEEE Internet of Things journal.

- Filip Maksimovic is a reviewer for IEEE Transactions on Circuits and Systems, IEEE Journal on Microwave Theory and Techniques, and the IEEE International Conference on Robotics and Automation (ICRA)

- Trifun Savic reviewer for IEEE Access, Feb-2023.

11.2 Scientific Leadership

11.2.1 Standardization Activities

- Mališa Vučinić is co-chair of the IETF LAKE working group. This is a very significant scientific responsibility. The two co-chairs (the other is Stephen Farrell from Trinity College Dublin) steer and trigger the work of the working group (WG). The activity of the LAKE group is followed by 116 people, with a healthymix of industrial and academia contributors. In 2023, two of the LAKE documents were approved to be published as Internet standards, and Mališa Vučinić is involved on both of them; as the author of one and shepherd of another. The LAKE WG has rechartered in 2023 enlarging its scope and adopting another AIO document on lightweight authorization that is co-authored by Mališa Vučinić and Geovane Fedrecheski.

- IETF 116 - Yokohama, Japan - March 2023

    – Mališa Vučinić attended the meeting in person chairing the LAKE working group and presenting a document in the ACE working group. As a result of the meeting, the document in the ACE working group was adopted as an official IETF document.

- IETF 117 - San Francisco, CA, USA - July 2023

    – Mališa Vučinić and Geovane Fedrecheski attended the meeting remotely. Mališa Vučinić chaired the LAKE working group meeting and presented a document in the ACE working group.

- IETF 118 – Prague, Czech Republic – November 2023

- – Geovane Fedrecheski, Yuxuan Song, Ichrak Kallala and Mališa Vučinić attended the meeting in person.
- – Geovane Fedrecheski and Mališa Vučinić improved credential processing in the `lakers` library during the IETF 118 Hackathon.
- – Geovane Fedrecheski presented Implementer Feedback: Lightweight Authorization using EDHOC during the LAKE session and Mališa Vučinić chaired the meeting.
- – Ichrak Kallala and Yuxuan Song attended, allowing them to meet the leaders and experts in the Internet Engineering Task Force (IETF) community, triggering valuable feedback and meetings about their work on the SCHC standard and on remote attestation.

- Ichrak Kallala attended the Journées LPWAN, gathering valuable information about Low Power Wide Area Networks (LPWAN).

11.2.2 EU Working Groups

- Thomas Watteyne, as scientific coordinator of the Horizon Europe OpenSwarm project, is contributor to the DISCOVER-US Horizon Europe Coordination Action, which pioneers distributed computing and swarm intelligence, forging a smarter, more connected future.

- Filip Maksimovic attends meetings of the "Open Source Semiconductors for EU Sovereignty" Working Group. As part of this, he is a volunteer reviewer for Open-Source Integrated Circuit Projects.

11.2.3 Responsibilities within Inria

- Thomas Watteyne is member of the Inria-Paris "Bureau du Comite de Projets" (BCP) since March 2022, a committee part of the Inria Paris scientific leadership.

- Thomas Watteyne is member of the Inria-Paris "Commission des Usagers de la Rue Barrault" (CURB) since January 2022, to make sure we build ourselves the most enjoyable new Inria Paris building.

- Thomas Watteyne manages the Inria Paris guitar, which anyone can borrow for an hour, a day or a week-end free of charge.

11.2.4 Tutorials

- Filip Maksimovic gave a hands-on Single-Chip Mote proramming tutorial at the workshop in Paris.

- Alexandre Abadie gave a hands-on tutorial on "DotBot" at the 8th Robotics Craftsmanship International Academy (RobotCraft), Porto, July 2023

11.2.5 Invited Talks

- Thomas Watteyne gave a talk "Swarm Robotics are the next IoT Frontier" at the University of Porto on 6-Feb-2023.

- Mališa Vučinić gave a talk "IETF LAKE: Lightweight Authenticated Key Exchange for Internet-of-Things use cases" at the 2023 Future Network Security Workshop on 14-Mar-2023.

- Filip Maksimovic gave a talk on "Monolithic Wireless Transceiver Design" at the CANELOS symposium at the Universidad Technica de Santa Maria in Valparaiso, Chile.

- Sara Faour gave a talk on "Physical Attacks: Implications on Single Chip Motes" at the Invited Workshop on Crystal-Free Radios, Chip-Scale Wireless Systems and Swarms, Paris, September 2023.

- Said Alvarado-Marin gave a talk on "Miniature Robot Localization using HTC Vive Lighthouse 2.0 System" at the Invited Workshop on Crystal-Free Radios, Chip-Scale Wireless Systems and Swarms, Paris, September 2023.

- Said Alvarado-Marin gave a remote presentation on PCB component assembly for students at ESIROI, La Reunion, 23-Oct-2023.

11.3   Teaching - Supervision - Juries

11.3.1   Teaching

- Thomas Watteyne taught a 1-week intensive module entitled "AIOT Systems: Getting Your Hands Dirty!", at ESIROI, La Reunion, 30-Oct-2023 – 3-Nov-2023.

- Mališa Vučinić taught the 'Internet of Things Security" one-day class at ENSTA Paris on 15-March-2023.

- Mališa Vučinić taught the hands-on Internet of Things course at NGO Prona, Montenegro, in October 2023.

- Mališa Vučinić taught the hands-on Internet of Things course at NGO Prona, Montenegro, from December 2022 to February 2023.

- Alexandre Abadie taught course "Using LoRaWAN with RIOT", Option Internet of Things, at ENSEA (12h).

- Alexandre Abadie taught practical course "RIOT & LoRa", at Telecom Sud Paris (8h).

- Alexandre Abadie taught a course on Git at Inria Paris (6h).

11.3.2   PhD Supervision

- Thomas Watteyne supervises the PhD studies of:

  - Martina Balbi
  - Fabian Graf
  - Yuxuan Song (co-supervised with Mališa Vučinić),
  - Said Alvarado-Marin (co-supervised with Filip Maksimovic)

- Paul Mühlethaler co-supervises the PhD studies of:

  - Kaouther Benguessoum
  - Sara Faour
  - Abdelhak Hidouri
  - Tayssir Ismail
  - Elsa Lopez-Perez
  - Felix Marcoccia

- Mališa Vučinić supervises the PhD studies of:

  - Sara Faour (co-supervised with Paul Mühlethaler)
  - Yuxuan Song (co-supervised with Thomas Watteyne)
  - Elsa Lopez-Perez (co-supervised with Paul Mühlethaler)

- Filip Maksimovic supervises the PhD studies of:

  - Said Alvarado-Marin

11.3.3 PhD Juries

- Thomas Watteyne was member of the examination board PhD thesis of Quentin Bailleul, as "examinateur". Doctoral work on "Dimensionnement de la Synchronisation d'un Réseau TSN dans Différents Contextes Embarqué" done at Toulouse INP, under the supervision of Katia Jaffrès-Runser and Jean-Luc Scharbarg. Viva on 24 November 2023.

- Thomas Watteyne was member of the examination board PhD thesis of Samir Si-Mohammed, as "rapporteur". Doctoral work on "Multi-Criteria Selection and Configuration of IoT Network Technologies" done at ENS Lyon, under the supervision of Thomas Begin (Univ. Lyon 1), Isabelle Guérin Lassous (ENS Lyon) and Pascale Vicat-Blanc (Inria). Viva on 4 October 2023.

- Thomas Watteyne was member of the examination board PhD thesis of Miguel José Gutiérrez Gaitán. Doctoral work on "Real-Time Overwater Wireless Network Design" done at the University of Porto, Portugal, under the supervision of Prof. Dr. Luís Miguel Pinho de Almeida, Dr. Pedro Miguel Salgueiro dos Santos and Dr. Pedro Miranda de Andrade de Albuquerque d'Orey. Viva on 6 February 2023.

- Paul Mühlethaler has been reviewer for A. Boualhouache's candidature for the habilitation.

11.4 Outreach

11.4.1 Within Inria

- Filip Maksimovic gave a talk at the "Demi Heure de Science" about standards compliant wireless networking without crystal oscillators.

- Alexandre Abadie gave a demo of "DotBot" at the Journée de l'Europe du centre Inria Paris, May 2023.

- Alexandre Abadie gave talk "Working at AIO" and a demo of the DotBot platform at the séminaire SED-PRO, Lyon, September 2023.

11.4.2 Participation in Outreach Events

- Thomas Watteyne has been working with Remy Taillefer and his team since December 2023 on an installation around low-power wireless at the Expo Inria, which retraces the history of computing and presents the digital revolution in which Inria is a major player.

- Mališa Vučinić gave a demo of the SailBot platform at the 8th Robotics Craftsmanship International Academy, Porto, Portugal 2023 on 10-Jul-2023

- Mališa Vučinić gave a demo of the SailBot platform at the Invited Workshop on Crystal-Free Radios, Chip-Scale Wireless Systems and Swarms, Paris, September 2023

- Mališa Vučinić participated in the startup competition jury during 2023 Summer School for High School talents organized by NGO Prona in Ivanova korita, Montenegro, August 2023

- Filip Maksimovic volunteered as part of the IEEE Circuits and Systems "Chip-a-Thon" as an expert advisor to student designers.

- Romain Facq did scientific mediation for the general public at the following events :

  - Salon culture et jeux mathématiques, Saint Sulpice place, 27th and 28th May 2023
  - Launching event for "Chut! Explore" magazine, La Poste Museum, 30th September 2023
  - Fête de la science, ENS Ulm, 8th October 2023

- Romain Facq did "Chiche! 1 scientifique 1 classe" meetings with high-school classes on the following dates (same date and same hour means there where several classes in the same room) :

- Lycée général privé Notre Dame des Missions - 13-Nov-2023 13:20
- Lycée général privé Notre Dame des Missions - 13-Nov-2023 14:10
- Lycée général privé Notre Dame des Missions - 17-Nov-2023 13:20
- Lycée général privé Notre Dame des Missions - 30-Nov-2023 08:00
- Lycée général privé Notre Dame des Missions - 30-Nov-2023 08:00
- Lycée polyvalent Les Pierres Vives - 08-Dec-2023 14:30
- Lycée polyvalent Les Pierres Vives - 08-Dec-2023 15:30

- Alexandre Abadie gave a demo of the DotBot platform at the Invited Workshop on Crystal-Free Radios, Chip-Scale Wireless Systems and Swarms, Paris, September 2023

- Alexandre Abadie gave a demo of the DotBot platform at the Open-Source Experience and SIDO tradeshows, Paris, December 2023.

- Said Alvarado-Marin gave a demo on "DotBot Control using Lighthouse Localization" at the Invited Workshop on Crystal-Free Radios, Chip-Scale Wireless Systems and Swarms, Paris, September 2023

- Geovane Fedrecheski attended the Journées INRAE - Inria 2023 in Nancy, July 2023.

- Geovane Fedrecheski gave a presentation about the role of the IETF in the evolution of the Internet & the IoT at the Computing Updates Days, Universidade do Centro Oeste do Paraná, Brazil, August 2023 (remote).

11.4.3 In The News

- Thomas Watteyne was featured in OpenSwarm: a highly innovative project for the Internet of Things, inria.fr, 16-Mar-2023.

- Trifun Savic was interviewed for the University of Montenegro as a successful alumni, February 2023 (https://www.ucg.ac.me/objava/blog/1267/objava/156564-predstavljamo-uspjesne-alumniste-elektrotehnickog-fakulteta-ucg-trifun-savic)

11.4.4 Videos

The team published a lot of short videos showing the scientific progress. You can find them listed at https://aio.inria.fr/videos/.

12 Scientific production

12.1 Major publications

[1] F. Boukhalfa, M. Hadded, P. Mühlethaler and O. Shagdar. 'An Analytical Model for Performance Analysis of an Active Signaling-based TDMA MAC Protocol for Vehicular Networks'. In: VTC-FALL 2019 - IEEE Vehicular Technology Conference. Honolulu, Hawaii, United States, 22nd Sept. 2019. URL: https://hal.science/hal-02178355.

[2] I. Hmedoush, C. Adjih and P. Mühlethaler. 'A Regret Minimization Approach to Frameless Irregular Repetition Slotted Aloha: IRSA-RM'. In: MLN 2020 - International Conference on Machine Learning for Networking. MLN 2020 - International Conference on Machine Learning for Networking. Paris / Virtual, France, 24th Nov. 2020. URL: https://hal.science/hal-03043877.

[3] F. Maksimovic, B. Wheeler, D. Burnett, O. Khan, S. Mesri, I. Suciu, L. Lee, A. Moreno, A. Sundararajan, B. Zhou, R. Zoll, A. Ng, T. Chang, X. Vilajosana, T. Watteyne, A. Niknejad and K. S. J. Pister. 'A Crystal-Free Single-Chip Micro Mote with Integrated 802.15.4 Compatible Transceiver, sub-mW BLE Compatible Beacon Transmitter, and Cortex M0'. In: 2019 VLSI - IEEE Symposium on VLSI Technology & Circuits. Kyoto, Japan, 9th June 2019. DOI: 10.23919/VLSIC.2019.8777971. URL: https://inria.hal.science/hal-02420868.

[4]   X. Vilajosana, T. Watteyne, T. Chang, M. Vučinić, S. Duquennoy and P. Thubert. 'IETF 6TiSCH: A Tutorial'. In: *Communications Surveys and Tutorials, IEEE Communications Society* (4th Sept. 2019). URL: https://inria.hal.science/hal-02420974.

[5]   X. Vilajosana, T. Watteyne, M. Vucinic, T. Chang and K. Pister. '6TiSCH: Industrial Performance for IPv6 Internet of Things Networks'. In: *Proceedings of the IEEE* 107.6 (1st June 2019), pp. 1153–1165. DOI: 10.1109/JPROC.2019.2906404. URL: https://inria.hal.science/hal-02266569.

[6]   M. Vučinić, G. Selander, J. P. Mattsson and T. Watteyne. 'Lightweight Authenticated Key Exchange with EDHOC'. In: *Computer* (Apr. 2022). DOI: 10.1109/mc.2022.3144764. URL: https://inria.hal.science/hal-03434293.

12.2   Publications of the year

International journals

[7]   G. Miguel Gutiérrez, A. Luís, D. Pedro M., S. Pedro M. and T. Watteyne. 'Minimal-Overlap Centrality for Multi-Gateway Designation in Real-Time TSCH Networks'. In: *ACM Transactions on Embedded Computing Systems (TECS)* (1st July 2023). URL: https://inria.hal.science/hal-04170029.

[8]   G. Selander, J. P. Mattsson, M. Serafin, M. Tiloca and M. Vučinić. 'Traces of EDHOC'. In: *Internet Engineering Task Force RFC series* (2024). URL: https://inria.hal.science/hal-04395899.

International peer-reviewed conferences

[9]   S. Faour, M. Vučinić, F. Maksimovic, D. Burnett, P. Mühlethaler, T. Watteyne and K. Pister. 'Implications of Physical Fault Injections on Single Chip Motes'. In: IEEE World Forum on Internet of Things. Aveiro, Portugal, 12th Oct. 2023. URL: https://inria.hal.science/hal-04216977.

[10] G. Fedrecheski, M. Vučinić and T. Watteyne. 'Performance Comparison of EDHOC and DTLS 1.3 in Internet-of-Things Environments'. In: IEEE Wireless Communications and Networking Conference. Dubai, United Arab Emirates, 21st Apr. 2024. URL: https://hal.science/hal-04382397.

[11] I. Hmedoush, P. Gu, C. Adjih, P. Mühlethaler and A. Serhrouchni. 'DS-IRSA: A Deep Reinforcement Learning and Sensing Based IRSA'. In: GLOBECOM 2023 - IEEE Global Communications Conference. Kuala Lumpur, Malaysia, 4th Dec. 2023. URL: https://inria.hal.science/hal-04238023.

[12] R. de La Fuente and T. Watteyne. 'Poster Abstract: Hands-on Evaluation of Kinéis Satellite IoT Technology'. In: IPSN 2023 - ACM/IEEE International Conference on Information Processing in Sensor Networks. San Antonio, TX, United States, 9th May 2023. URL: https://inria.hal.science/hal-04048809.

[13] M. Liu, F. Yang, S. Michiels, T. Van Eyck, D. Hughes, S. Alvarado-Marin, F. Maksimovic and T. Watteyne. 'Demo Abstract: FreeBot, a Battery-Free Swarm Robotics Platform'. In: ACM Conference on Embedded Networked Sensor Systems (SenSys). Istanbul, Turkey, 13th Nov. 2023. DOI: 10.1145/3625687.3628401. URL: https://inria.hal.science/hal-04393880.

[14] F. Maksimovic, A. Patel, D. Burnett, T. Watteyne and K. S. J. Pister. 'A Time Synchronized Multi-Hop Mesh Network with Crystal-Free Nodes'. In: *Proceedings of IEEE GLOBECOM 2023*. GLOBECOM 2023. Kuala Lumpur, Malaysia, 4th Dec. 2023. URL: https://inria.hal.science/hal-04394968.

[15] P. Muhlethaler and N. Achir. 'Analyzing and Optimizing Extended-CAM Service Using Simple Stochastic Geometry Model'. In: PEMWN 2023 - 12th IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks. Berlin, Germany: IEEE, 27th Sept. 2023, pp. 1–6. DOI: 10.23919/PEMWN58813.2023.10304925. URL: https://hal.science/hal-04393587.

[16] T. Savić, K. Brun-Laguna and T. Watteyne. 'Blip: Identifying Boats in a Smart Marina Environment'. In: DCOSS 2023 - 19th International Conference on Distributed Computing in Sensor Systems. Paphos, Cyprus, 19th June 2023. URL: https://inria.hal.science/hal-04158385.

[17] T. Savić, K. Brun-Laguna and T. Watteyne. 'WELOC: Localizing Equipment in Marinas using Ultrasound'. In: IEEE World Forum on Internet of Things (WF-IoT). Aveiro, Portugal, 12th Oct. 2023. URL: https://inria.hal.science/hal-04248793.

Conferences without proceedings

[18] M. Félix, C. Adjih and P. Mühlethaler. 'A Deep Learning Approach to Topology Configuration in Multi-Hop Wireless Networks with Directional Antennas: nodes2net'. In: PEMWN 2023 - The 12th IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks. Berlin, Germany, 27th Sept. 2023. URL: https://hal.science/hal-04387755.

Doctoral dissertations and habilitation theses

[19] R. Abu-Aisheh. 'Context-Aware Information Gathering and Processing Towards Supporting Autonomous Systems in Industry 4.0 Scenarios'. Sorbonne Université, 27th Feb. 2023. URL: https://hal.science/tel-04017864.

[20] T. Savić. 'Localization in Constrained Environments'. Sorbonne Université, 22nd Sept. 2023. URL: https://theses.hal.science/tel-04223124.

Reports & preprints

[21] G. Fayolle and P. Muhlethaler. *A Markovian analysis of an IEEE-802.11 station with buffering.* 22nd Dec. 2023. URL: https://inria.hal.science/hal-04362437.

12.3 Cited publications

[22] N. Achir, Y. Bouchaala, P. Muhlethaler and O. Shagdar. 'Optimisation of spatial CSMA using a simple stochastic geometry model for 1D and 2D networks'. In: *IWCMC 2016 - 12th International Wireless Communications & Mobile Computing Conference.* Paphos, Cyprus, 2016, pp. 558–563.

[23] A. Adigun, B. A. Bensaber and I. Biskri. 'Protocol of Change Pseudonyms for VANETs'. In: *38th Annual IEEE Conference on Local Computer Networks - Workshops.* 2013, pp. 162–167.

[24] S. Baccari, M. Hadded, H. Touati and P. Muhlethaler. 'A Secure Trust-aware Cross-layer Routing Protocol for Vehicular Ad hoc Networks'. In: *Journal of Cyber Security and Mobility* (2020).

[25] S. Baccari, H. Touati, M. Hadded and P. Muhlethaler. 'Performance Impact Analysis of Security Attacks on Cross-Layer Routing Protocols in Vehicular Ad hoc Networks'. In: *SoftCom 2020 - International Conference on Software, Telecommunications and Computer Networks.* Hvar / Virtual, Croatia, Sept. 2020.

[26] K. Bhargavan, B. Blanchet and N. Kobeissi. 'Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate'. In: *2017 IEEE Symposium on Security and Privacy (SP).* IEEE. 2017, pp. 483–502.

[27] Y. Bouchaala. 'Gestion des Messages de Sécurité dans les Réseaux VANET'. Thèse de doctorat dirigée par Mühlethaler, Paul et Shagdar, Oyunchimeg Réseaux, information et communications Université Paris-Saclay (ComUE) 2017. PhD thesis. Université Paris-Saclay, 2017.

[28] Y. Bouchaala, O. Shagdar and P. Muhlethaler. 'Analysis of broadcast strategies and network parameters in IEEE 802.11p VANETs using simple analytical models'. In: *International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN).* Hammamet, Tunisia, Nov. 2015.

[29] F. Boukhalfa, C. Adjih, P. Muhlethaler, M. Hadded and O. Shagdar. 'Physical and MAC Layer Design for Active Signaling Schemes in Vehicular Networks'. In: *STWiMob 2020 - 16th International Workshop on Selected Topics in Wireless and Mobile computing.* Thessaloniki / Virtual, Greece, Oct. 2020.

[30]   F. Boukhalfa, M. Hadded, P. Muhlethaler and O. Shagdar. 'An Active Signaling Mechanism to Reduce Access Collisions in a Distributed TDMA based MAC Protocol for Vehicular Networks'. In: *AINA-2019 - Advanced Information Networking and Applications*. Matsue, Japan, Mar. 2019.

[31]   F. Boukhalfa, M. Hadded, P. Muhlethaler and O. Shagdar. 'Coexistence of IEEE 802.11p and the TDMA-based AS-DTMAC Protocol'. In: *SoftCOM 2020: International Conference on Software, Telecommunications and Computer Networks 2020*. Hvar / Virtual, Croatia, Sept. 2020.

[32]   F. Boukhalfa, M. Hadded, P. Muhlethaler and O. Shagdar. 'Performance Evaluation of an Active Signaling based Time-Slot Scheduling Scheme for connected vehicles'. In: *Annals of Telecommunications - annales des télécommunications* (2020).

[33]   K. Brun-Laguna, A. L. Diedrichs, D. Dujovne, C. Taffernaberry, R. Leone, X. Vilajosana and T. Watteyne. 'Using SmartMesh IP in Smart Agriculture and Smart Building Applications'. In: *Elsevier Computer Communications Journal* (2018).

[34]   T. Chang, T. Watteyne, B. Wheeler, F. Maksimovic, O. Khan, S. Mesri, L. Lee, I. Suciu, D. Burnett, X. Vilajosana et al. '6TiSCH on SCμM: Running a Synchronized Protocol Stack without Crystals'. In: *Sensors* 20.7 (2020), p. 1912.

[35]   M. Domingo-Prieto, T. Chang, X. Vilajosana and T. Watteyne. 'Distributed PID-based Scheduling for 6TiSCH Networks'. In: *IEEE Communications Letters* (2016).

[36]   S. Duquennoy, B. Al Nahas, O. Landsiedel and T. Watteyne. 'Orchestra: Robust Mesh Networks Through Autonomously Scheduled TSCH'. In: *ACM Conference on Embedded Networked Sensor Systems (Sensys)*. 2015.

[37]   S. Farrell and H. Tschofenig. *Pervasive Monitoring Is an Attack*. Tech. rep. RFC7258. Internet Engineering Task Force (IETF), May 2014.

[38]   P. H. Gomes, T. Watteyne, P. Gosh and B. Krishnamachari. 'Reliability through Time-Slotted Channel Hopping and Flooding-based Routing'. In: *International Conference on Embedded Wireless Systems and Networks (EWSN), Dependability Competition*. 2016.

[39]   R. Grabowski, L. E. Navarro-Serment, C. J. Paredis and P. K. Khosla. 'Heterogeneous Teams of Modular Robots for Mapping and Exploration'. In: *Springer Autonomous Robots* (2000).

[40]   M. Gunnarsson, J. Brorsson, F. Palombini, L. Seitz and M. Tiloca. 'Evaluating the Performance of the OSCORE Security Protocol in Constrained IoT Environments'. In: *Internet of Things* 13 (2021).

[41]   M. Hadded. 'Design and Optimization of Access Control Protocols in Vehicular Ad Hoc Networks (VANETs)'. Thèse de doctorat dirigée par Laouiti, Mohamed Anis Informatique Evry, Institut national des télécommunications 2016. PhD thesis. Informatique Evry, 2016.

[42]   M. Hadded, A. Laouiti, P. Muhlethaler and L. A. Saidane. 'An Infrastructure-Free Slot Assignment Algorithm for Reliable Broadcast of Periodic Messages in Vehicular Ad hoc Networks'. In: *VTC Fall 2016*. Proceedings of VTC Fall 2016. Montréal , Canada, Sept. 2016.

[43]   M. Hadded, P. Muhlethaler and A. Laouiti. 'TDMA scheduling strategies for vehicular ad hoc networks: from a distributed to a centralized approach'. In: *SoftCOM 2018 - 26th International Conference on Software, Telecommunications and Computer Networks*. Split, Croatia, Sept. 2018.

[44]   M. Hadded, P. Muhlethaler, A. Laouiti and L. A. Saidane. 'A Centralized TDMA based Scheduling Algorithm for Real-Time Communications in Vehicular Ad Hoc Networks'. In: *SoftCom 2016*. Proceedings of SoftCom 2016. Split , Croatia, Sept. 2016.

[45]   S. Hammel, P. Liu, E. Hilliard and K. Gong. 'Optimal Observer Motion for Localization with Bearing Measurements'. In: *Computers & Mathematics with Applications* (1989).

[46]   H. Hasrouny, A. E. Samhat, C. Bassil and A. Laouiti. 'VANET Security Challenges and Solutions: a Survey'. In: *Vehicular Communications* 7 (2017), pp. 7–20.

[47]   R. Khoder, R. Naja and S. Tohme. 'Impact of Interference on Visible Light Communication Performance in a Vehicular Platoon'. In: *2020 International Wireless Communications and Mobile Computing (IWCMC)*. 2020, pp. 1935–1939.

[48] B. G. Kilberg, F. M. R. Campos, F. Maksimovic, T. Watteyne and K. S. Pister. 'Accurate 3D Lighthouse Localization of a Low-Power Crystal-Free Single-Chip Mote'. In: *Journal of Microelectromechanical Systems* 29.5 (2020), pp. 818–824.

[49] G. Le Lann. *Cyberphysical Constructs and Concepts for Fully Automated Networked Vehicles.* Research Report RR-9297. INRIA Paris-Rocquencourt, Oct. 2019.

[50] Y. Maalej, S. Sorour, A. Abdel-Rahim and M. Guizani. 'Vanets Meet Autonomous Vehicles: Multimodal Surrounding Recognition Using Manifold Alignment'. In: *IEEE Access* 6 (2018), pp. 29026–29040.

[51] D. Manivannan, S. S. Moni and S. Zeadally. 'Secure Authentication and Privacy-Preserving Techniques in Vehicular Ad-hoc NETworks (VANETs)'. In: *Vehicular Communications* 25 (2020), p. 100247.

[52] P. Minet and Y. Tanaka. 'Optimal Number of Message Transmissions for Probabilistic Guarantee of Latency in the IoT'. In: *MDPI Sensors* (2019).

[53] B. Moran, H. Tschofenig, D. Brown and M. Meriac. *A Firmware Update Architecture for Internet of Things.* Internet-Draft draft-ietf-suit-architecture-16. Work in Progress. Internet Engineering Task Force, Jan. 2021. 28 pp.

[54] J. Munoz, F. Rincon, T. Chang, X. Vilajosana, B. Vermeulen, T. Walcarius, W. Van de Meerssche and T. Watteyne. 'OpenTestBed: Poor Man's IoT Testbed'. In: *IEEE INFOCOM, CNERT workshop.* 2019.

[55] L. E. Navarro-Serment, C. J. Paredis and P. K. Khosla. 'A Beacon System for the Localization of Distributed Robotic Teams'. In: *International Conference on Field and Service Robotics.* 1999.

[56] B. Nemsick, A. Buchan, A. Nagabandi, R. Fearing and A. Zakhor. 'Cooperative Inchworm Localization with a Low Cost Team'. In: *IEEE International Conference on Robotics and Automation (ICRA).* 2017.

[57] C. A. Oroza, Z. Zhang, T. Watteyne and S. D. Glaser. 'A Machine-Learning Based Connectivity Model for Complex Terrain Large-Scale Low-Power Wireless Deployments'. In: *IEEE Transactions on Cognitive Communications and Networking* (2017).

[58] A. Perrig, R. Canetti, J. D. Tygar and D. Song. 'The TESLA Broadcast Authentication Protocol'. In: *RSA Cryptobytes* 5.2 (2002), pp. 2–13.

[59] G. Restuccia, H. Tschofenig and E. Baccelli. 'Low-Power IoT Communication Security: On the Performance of DTLS and TLS 1.3'. In: *IFIP International Conference on Performance Evaluation and Modeling in Wireless Networks (PEMWN).* 2020.

[60] M. Sangare, S. Banerjee, P. Muhlethaler and S. Bouzefrane. 'Predicting transmission success with Machine-Learning and Support Vector Machine in VANETs'. In: *PEMWN 2018 - 7th IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks.* Toulouse, France, Sept. 2018.

[61] M. Sangare, S. Banerjee, P. Muhlethaler and S. Bouzefrane. 'Predicting Vehicles' Positions using Roadside Units: a Machine-Learning Approach'. In: *IEEE CSCN 2018- IEEE Conference on Standards for Communications and Networking.* Paris, France, Oct. 2018.

[62] M. Sangare, S. Banerjee, P. Muhlethaler and T. Le Vinh. 'Graph-Based Subjective Matching of Trusted Strings and Blockchain-Based Filtering for Connected Vehicles'. In: *MSPN 2020 - 6th International Conference on Mobile, Secure and Programmable Networking.* Paris / Virtual, France, Oct. 2020.

[63] M. Sangare, S. Gupta, S. Bouzefrane, S. Banerjee and P. Muhlethaler. 'Exploring the Forecasting Approach for Road Accidents: Analytical Measures with Hybrid Machine Learning'. In: *Expert Systems with Applications* (2020), p. 113855.

[64] M. Sangare, D.-V. N. Nguyen, S. Banerjee, P. Muhlethaler and S. Bouzefrane. 'Comparing different Machine-Learning techniques to predict Vehicles' Positions using the received Signal Strength of periodic messages'. In: *WMNC 2019. 12th IFIP Wireless and Mobile Networking Conference.* Paris, France, Sept. 2019.

[65] C. Schindler, T. Watteyne, X. Vilajosana and K. S. J. Pister. 'Implementation and Characterization of a Multi-hop 6TiSCH Network for Experimental Feedback Control of an Inverted Pendulum'. In: *IEEE International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*. 2017.

[66] S. Sciancalepore, G. Oligeri, G. Piro, G. Boggia and R. Di Pietro. 'EXCHANge: Securing IoT via Channel Anonymity'. In: *Computer Communications* 134 (2019), pp. 14–29.

[67] G. Selander, J. P. Mattsson and F. Palombini. *Ephemeral Diffie-Hellman Over COSE (EDHOC)*. Internet-Draft draft-ietf-lake-edhoc-04. Work in Progress. Internet Engineering Task Force, Jan. 2021. 84 pp.

[68] G. Selander, J. P. Mattsson, M. Vučinić, M. Richardson and A. Schellenbaum. *Lightweight Authorization for Authenticated Key Exchange*. Internet-Draft draft-selander-ace-ake-authz-02. Work in Progress. Internet Engineering Task Force, Nov. 2020. 20 pp.

[69] I. Suciu, F. Maksimovic, D. Burnett, O. Khan, B. Wheeler, A. Sundararajan, T. Watteyne, X. Vilajosana and K. S. J. Pister. 'Experimental Clock Calibration on a Crystal-Free Mote-on-a-Chip'. In: *IEEE INFOCOM, CNERT workshop*. 2019.

[70] Y. Tanaka, K. Brun-Laguna and T. Watteyne. 'Demo: Simulating a 6TiSCH Network using Connectivity Traces from Testbeds'. In: *IEEE INFOCOM, CNERT workshop*. 2019.

[71] M. Vučinić, G. Selander, J. P. Mattsson and D. Garcia-Carillo. *Requirements for a Lightweight AKE for OSCORE*. Internet-Draft draft-ietf-lake-reqs-04. Work in Progress. Internet Engineering Task Force, June 2020. 25 pp.

[72] M. Wadea, A. Mostafa, D. P. Agrawal and A. Hamad. 'Enhancing VANET Connectivity through Utilizing Autonomous Vehicles'. In: *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 2017, pp. 204–211.

[73] T. Watteyne, I. Auge-Blum, M. Dohler, S. Ubeda and D. Barthel. 'Centroid Virtual Coordinates – A Novel Near-Shortest Path Routing Paradigm'. In: *Elsevier International Journal of Computer and Telecommunications Networking* (2009).

[74] B. Wheeler, A. Ng, B. Kilberg, F. Maksimovic and K. S. J. Pister. 'Low-Power Optical Receiver for Contact-free Programming and 3D Localization of Autonomous Microsystems'. In: *IEEE Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. 2019.

[75] K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig and E. Baccelli. 'Secure Firmware Updates for Constrained IoT Devices using Open Standards: a Reality Check'. In: *IEEE Access* 7 (2019), pp. 71907–71920.