RESEARCH CENTRE

Inria Paris Center

2022 ACTIVITY REPORT

Project-Team AIO

Dependable Networking, Low-Power Wireless and Micro-Robotics

DOMAIN

Networks, Systems and Services, Distributed Computing

THEME

Networks and Telecommunications

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, Researcher]

PhD Students

- Razane Abu-Aisheh [NOKIA, CIFRE]
- Said Alvarado-Marin [Inria, from Apr 2022]
- Sara Faour [Inria, from Oct 2022]
- Haouda Ghamni [University of Gabes, Tunisia, from Sep 2022]
- Abdelhak Hidouri [University of Gabes, Tunisia, from Sep 2022]
- Iman Hmedoush [Inria, until May 2022]
- Tayssir Ismail [University of Gabes, Tunisia]
- Felix Marcoccia [Thales, CIFRE, from Apr 2022]
- Trifun Savic [WATTSON ELEMENTS]

Technical Staff

- Said Alvarado Marin [INRIA, Engineer, until Mar 2022]
- Romain Facq [Inria, Engineer, from Oct 2022]
- Felix Marcoccia [THALES, Engineer, until Feb 2022]

Interns and Apprentices

- Theo Akbas [ENSEA, Intern, from May 2022 until Aug 2022]
- Kaouther Benguessoum [ENSI, Intern, from Mar 2022 until Jul 2022]
- Cristobal Huidobro-Marin [Universidad Técnica Federico Santa María, Intern, from Jun 2022]
- Charles Thonier [ENSTA Paris, Intern, from Mar 2022 until Jul 2022]

Administrative Assistant

- Anne Mathurin [INRIA]

Visiting Scientists

- Soumya Banerjee [U. College Cork, from Nov 2022]
- Miguel Gutiérrez Gaitán [U. Porto, Portugal, from Apr 2023 until Jul 2022]
- Leila Saidane [ENSI Tunisia, from Nov 2022]

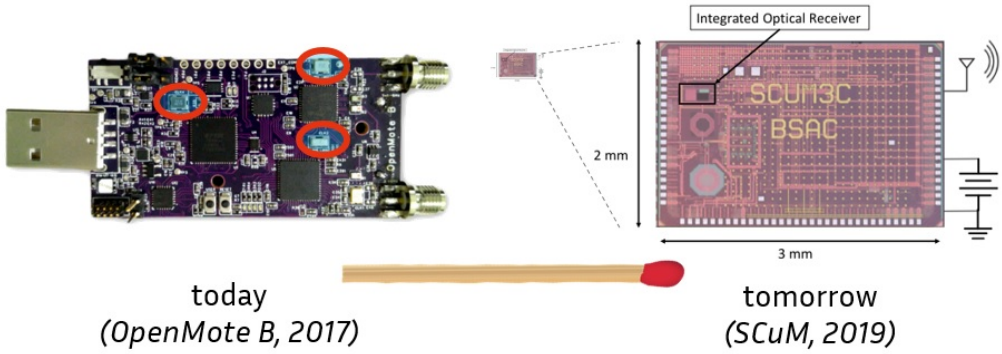


Figure 1: SCuM ("Single Chip Micro Mote") is the world's first crystal-free micro-mote which implements a full IEEE802.15.4 and BLE radio

External Collaborators

- Leila Azouz Saidane [ENSI TUNIS, from Mar 2022 until Mar 2022]
- Martina Maria Balbi Antunes [IMT ATLANTIQUE]
- Soumya Banerjee [UCC CORK]
- Selma Boumerdassi [CNAM]
- Samia Bouzefrane [CNAM]
- Mohamed Elhadad [SYSTEMX]
- Éric Renault [ESIEE]
- Leila Saidane [ENSI]

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 will lead 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.

[A1.1] Fast Calibration and Standardization

The behavior of the oscillators within the SCuM chip is not fully understood. We have shown in [77] 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 [65] 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 [77]. 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 [62] 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 [62], 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 [39], 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 [78] 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 [42], 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 [40] 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" [81], 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 [36], 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 [73] 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.* [60] 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 [41]. 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 [67, 44]. 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 [79].

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 [76]. One cornerstone component of such a solution is the LAKE protocol [75]. 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 [29].

Software update mechanisms are being standardized by the IETF [61]. 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 [83] 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 [74]?*

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 [54], 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 [66]) 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 [37]. 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

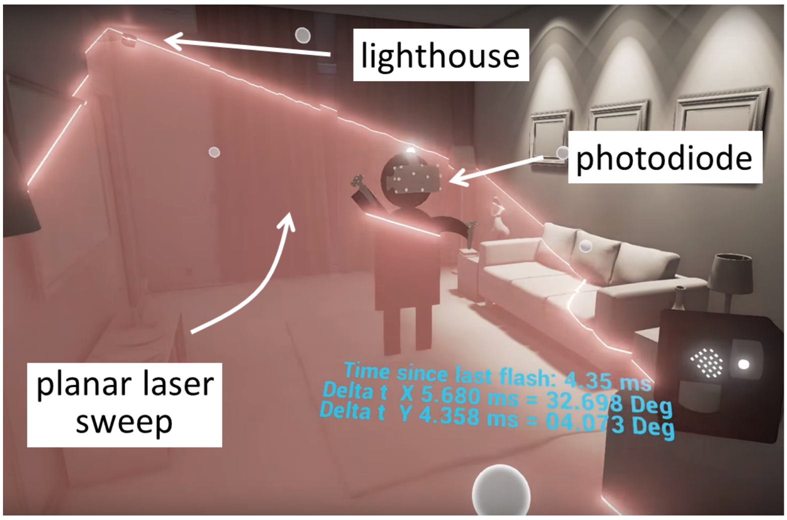


Figure 2: The principle of lighthouse localization.

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.* [82] 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 [50]. 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 [63, 43].

- 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 [64, 63, 43], 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

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 [31, 25]. 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 [30]. 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 [47, 48]. 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 [49]. These studies have been carried during Mohamed Hadded thesis [46]. We are currently working to improve these approaches. The idea is to use active signaling techniques in combination with TDMA approaches [33]. 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 [35, 32, 34]. 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) [53], 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 [57, 80].

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 [55] 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 [69, 68, 72]. 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 [71]. 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 [51, 58]. 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 [26].

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 [28, 27]. 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 [70]. 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.

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 networds 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 plats 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 2022, we started 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

6.1 What a Year!

This is the first year of the AIO team. While AIO inherits a lot from the previous EVA team, its research program takes up a new dimension by embracing much more hardware and electronics, and using swarm robotics around which a lot of the research is build: hardware, localization, networking, security. This year was somewhat of a test to see whether we hadn't bitten off too much. Clearly, that was not the case and 2022 was a spectacular year in many aspects.

We started the year with our spin-off startup company, Falco, receiving the IoT Award of the Embedded Trophy run by the French Ministry of Economy. This was a good indication the technology the team has been generating (and which is licensed by Falco) is appretiate by the embedded community, including the big industrial players.

One of the investement with the longest returns in the team leading the Horizon Europe OpenSwarm proposal, and getting it accepted. The 40-month project starts 1-Jan-2023, and brings together the ideal set of partners to push a research agenda which matches pretty much perfectly the research program of the team. Getting OpenSwarm accepted is also, for our team, some sort of validation of the proposed research. We are convinced that OpenSwarm, mainly through the fantastic consortium it brings together, will serve as a fantastic accelerator for our research n 2023 and beyond.

6.2 Awards

- Thomas Watteyne crossed 10,000 citations of his papers, according to Google Scholar
- Thomas Watteyne in the top 2% researcher across all fields, top 0.6% in the "Networking & Telecommunications" field per Stanford's Prof. Ioannidis work "A Standardized Citation Metrics Author Database Annotated for Scientific Field".
- Wattson Elements recipient of the IoT Award of the Embedded Trophy ("Trophés de l'Embarqué, catégorie "IoT Grand Public") on 14-Jan-2022, an annual innovation competition organized in partnership with the French Ministry of Economy, for their Falco product and the innovation roadmap driven by Thomas Watteyne.

7 New software and platforms

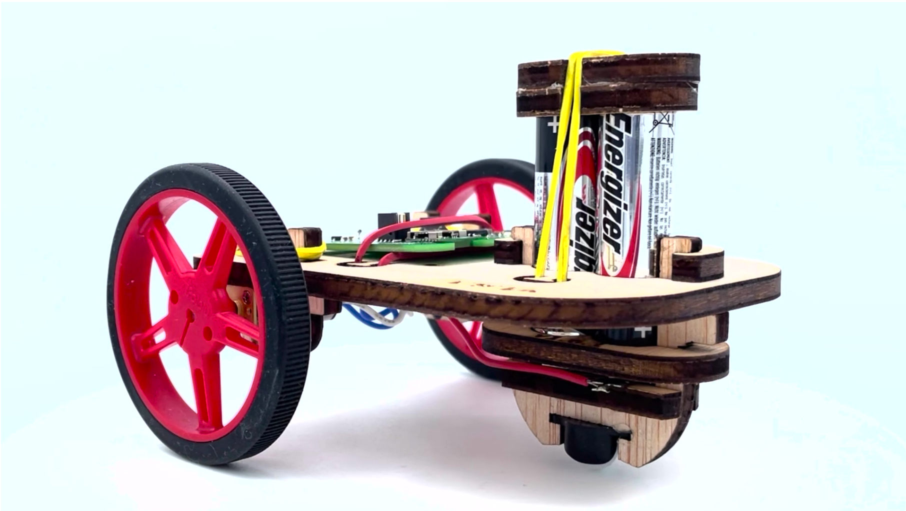
7.1 New software

7.1.1 edhoc-rs

Name: EDHOC Implementation in Rust / hacspec

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 / hacspec implementation of the protocol, adapted for use on microcontrollers.



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

Contact: Malisa Vucinic

7.2 New platforms

7.2.1 DotBot

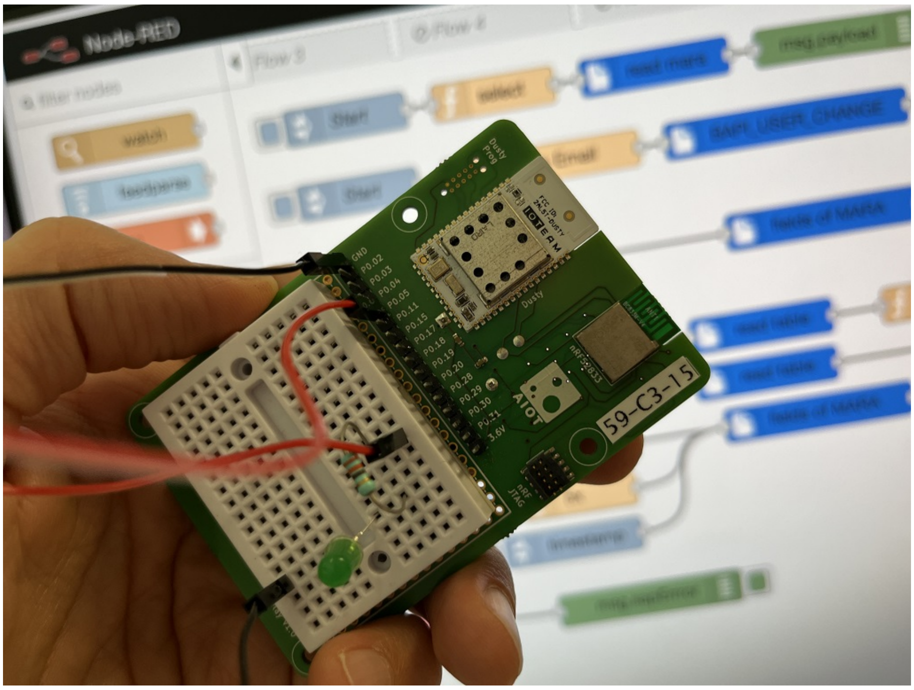
Large, coordinated "swarms" of small, resource constrained robots have the potential to complete complex tasks that single monolithic robots cannot. However, while there is ongoing research, little progress has been made in successfully deploying these swarms in the real world. To help further the field, we are building a research platform called DotBot, show in Fig. 7.2.1: 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.

We have been working hard on the DotBot in 2022. We started the year with a proof-of-concept design which could drive around, but could not self-localize. The work on hardware by Said Alvarado-Marin, on localization by Filip Maksimovic and on algorithms by Razanne Abu Aisheh has allows Alexandre Abadie to "put it all together". We now have small swarms of handful of DotBots moving around in the lab, self-locazing using the lighthouse. The DotBot features front and center in the Horizon Europe OpenSwarm project. This project, in particular through the very large partners it brings, will serve as a catalyst that will turn our small-scale testbed into a 1,000 DotBot in the next 18 months.

More information at www.dotbots.org.

7.2.2 AIOT Systems

AIOT Systems is a one-stop shop for learning embedded low-power wireless. The AIOT Play board, shown in Fig. 7.2.2, 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.

More information at www.aiotsystems.org.

8 New results

The team's research program, summarized in Section 3, is organized around five axes. We present the results of 2022 following the same organization.

8.1 Related to [A1] Smart Dust

We make some strong leaps in our “Smart Dust” research strand, thanks to very strong collaboration with the UC Berkeley team of Prof. Pister, a collboration which benefits hugely from the SWARM associate team which is in place. The SCuM chip we have been using is very interesting; it can “speak” both IEEE802.15.4 and Bluetooth without needing a crystal. That is, a device can be the size of a grain of rice, which opens up lots of potential applications. We have made a lot of progress in the calibration of the oscillators in that chip, to the point where we are now able to create small multi-hop mesh networks with SCuM chips.

8.1.1 A Temperature-Compensated BLE Beacon and 802.15.4-to-BLE Translator on a Crystal-Free Mote

Participants:

Titan Yuan(UC Berkeley)
, Filip Maksimovic
, Brad Wheeler(UC Berkeley)
, David Burnett(UC Berkeley)
, Lydia Lee(UC Berkeley)
, Thomas Watteyne
, Kris Pister(UC Berkeley).

Crystal-free radios have the potential to revolutionize the IoT: due to their single-chip nature, they are both very cheap (no external components required) and very small (the size of a grain of rice). The Single-Chip Micro Mote (SCμM) is a 2×3 mm^2 crystal-free chip that can communicate with off-the-shelf transceivers over Bluetooth Low Energy (BLE) or IEEE 802.15.4. Setting its communication frequency is challenging because the crystal-free chip can rely only on internal oscillating circuits, which are very susceptible to temperature. Without compensation, a SCμM chip can no longer communicate with an off-the-shelf BLE receiver if the temperature changes by more than 1.25 C. This paper introduces a two-step temperature compensation method, allowing SCμM to successfully send BLE frames over a 20 C temperature range. After performing initial calibration during optical bootloading, we use an open-loop linear model to estimate the ambient temperature and continuously tune the mote's local oscillator (LO) frequency as the temperature changes. We show how the mote can use the intermediate frequency of 802.15.4 frames it receives from nearby off-the-shelf transceivers as a frequency reference to adjust its LO frequency. This compensation method enables SCμM to operate as a tiny BLE beacon, a BLE temperature sensor (for retail or medical applications), or a 802.15.4-to-BLE translation device. This work was published as a conference paper [21].

8.1.2 Surviving the Hair Dryer: Continuous Calibration of a Crystal-Free Mote-on-Chip

Participants:

Tengfei Chang(Inria)
, Thomas Watteyne
, Brad Wheeler(UC Berkeley)
, Filip Maksimovic
, David Burnett(UC Berkeley)
, Kris Pister(UC Berkeley).

The Single Chip micro-Mote (SCμM) is a 2×3 mm^2 Single-Chip Crystal-Free mote-on-chip. SCμM implements the IEEE802.15.4 and BLE standards and can communicate which off-the-shelf radio compliant to those standards. SCμM exclusively uses on-chip oscillators, including a 2.4 GHz LC oscillator to synthesize the communication frequency, and a 2 MHz RC oscillator to clock the chip rate. The challenge is that the LC oscillator drifts at 2,100 ppm over a temperature range of 45°C, far from the 40 ppm maximum drift mandated by the the IEEE802.15.4 standard. While one-shot calibration is possible, any temperature change causes IEEE802.15.4 communication to fail. In this work, we introduce a continuous calibration approach for SCμM to adapt the tuning of its oscillators as the temperature changes. Experimental results show that it allows SCμM to keep communicating with an IEEE802.15.4 radio even under the extreme condition of using a hair dryer to heat up the chip at 3°C/min. Under these conditions, the drift of the LC oscillator stays within the ±40 ppm limit over 94% of the time. Similarly, the drift of the 2 MHz RC oscillator stays within ±1,000 ppm limit 99.98% of the time. This work was published as a journal article [7].

8.1.3 Compensation for Time and Frequency Error on Single-Chip Crystal-Free Motes in a Multi-Hop Time Synchronized Channel Hopping Wireless Network

Participants:
Filip Maksimovic
, Thomas Watteyne.

We have proposed and demonstrated a new protocol for a time synchronized channel hopping mesh network for wireless transceivers that use exclusively imprecise and inaccurate on-chip oscillators. This protocol is built on an IEEE 802.15.4 physical layer radio. The protocol includes a low-energy calibration scheme that enables interoperability with protocols such as 6TiSCH or personal area networks such as Thread. A calibration-bootstrapped multi-hop mesh network is demonstrated with a single crystal-enabled node acting as the root.

The synchronization and data-transfer protocol is designed to build a mesh network out of unreliable, noisy oscillators and compensate for drift in channel and time. These noisy oscillators are used because they can be integrated on the same chip as the radio and processor, greatly reducing the size and power consumption of each device. With a 4 s synchronization period, an experimental implementation of the network maintains, in the worst case, 1.8 ms 3σ absolute time synchronization and 820 μs 3σ 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 this synchronization with a supply variation of 2.5 mV/s, which is loosely equivalent to a temperature variation of 10 C/min with a packet rate of 0.5 Hz.

8.2 Related to [A2] Low-Power Wireless Networking

Directly inline with what had been done by the EVA team, the AIO team continues to work on networking. The team has demonstrate what we believe is the longest low-power wireless mesh network, 103 km, using long-range devices hanging from helium balloons floating 40 m in the air. The team also publishes some work on deploying their technology in environmental applications. Besides these demo/deployment activities, the team has continued to work on the 6TiSCH protocol stack, through several protocol-related work on scheduling and routing. An interesting domain the team has entered in real-time communication in these types of networks.

8.2.1 Distributed Sniffing in Large IoT Networks

Participants:
Mališa Vučinić
, Thomas Watteyne.

Context and goal. In coordination with the University of Montenegro, Inria-AIO has worked on the problem of distributed sniffing in large IoT networks. Due to the large space they occupy and radio propagation peculiarities, a single sniffer is not enough to capture the entire traffic exchanged in the network. The problem consists of finding the optimal number of sniffers and their placement.

Summary of activities. We derived two algorithms, one based on graph theory and the other based on probabilistic theory, whose inputs are the connectivity matrix of the network and the desired coverage level of the network, and the outputs are the number of sniffers and their positions in the network. We implemented the solution in the 6TiSCH simulator and tested it using network traces from the Inria-Paris OpenTestbed deployment. The work has resulted in two publications in 2022, see [8] and [16].

8.2.2 Building a 103 km Multi-Hop Network Replicating Claude Chappe's Telegraph

Figure 3: One of the 11 balloons used in a 103 km mesh network experiment [11]. If you look very closely, you can see the low-power wireless device hanging from the balloon.

Participants:

Mina Rady(INSA Lyon)

, Jonathan Mauricio Munoz Soto(Wattson Elements)

, Razanne Abu Aisheh

, Mališa Vučinić

, José Astorga Tobar(U. de Chile)

, Alfonso Cortes(U. Técnica Federico Santa María)

, Quentin Lampin(Orange Labs)

, Dominique Barthel(Orange Labs)

, Thomas Watteyne.

In 1794, French Engineer Claude Chappe coordinated the deployment of a network of dozens of optical semaphores. These formed "strings" that were hundreds of kilometers long, allowing for nationwide telegraphy. The Chappe telegraph inspired future developments of long-range telecommunications using electrical telegraphs and, later, digital telecommunication. Long-range wireless networks are used today for the Internet of Things (IoT), including industrial, agricultural, and urban applications. The long-range radio technology used today offers approximately 10 km of range. Long-range IoT solutions use "star" topology: all devices need to be within range of a gateway device. This limits the area covered by one such network to roughly a disk of a 10 km radius. In this work, we demonstrate a 103 km low-power wireless multi-hop network by combining long-range IoT radio technology with Claude Chappe's vision. We placed 11 battery-powered devices at the former locations of the Chappe telegraph towers, hanging under helium balloons, see Fig. 3. We ran a proprietary protocol stack on these devices so they formed a 10-hop multi-hop network: devices forwarded the frames from the "previous" device in the chain. This is, to our knowledge, the longest low power multi-hop wireless network built to date, demonstrating the potential of combining long-range radio technology with multi-hop technology. This work was published as a journal article [11].

8.2.3 Long-term Monitoring of the Sierra Nevada Snowpack Using Wireless Sensor Networks

Participants:

Ziran Zhang(UC Berkeley)

, Steven Glaser(UC Berkeley)

, Thomas Watteyne

, Sami Malek(UC Berkeley).

Historically, the study of mountain hydrology and the water cycle has been largely observational, with meteorological forcing and hydrological variables extrapolated from a few infrequent manual measurements. Recent developments in Internet of Things (IoT) technology are revolutionizing the field of mountain hydrology. Low-power wireless sensor networks can now generate denser data in real-time and for a fraction of the cost of labor-intensive manual measurement campaigns. The American River Hydrological Observatory (ARHO) project has deployed thirteen low-power wireless IoT networks throughout the American River basin to monitor California's snowpack. The networks feature a total of 945 environmental sensors, each reporting a reading every 15 minutes. The data reported is made available to the scientific community minutes after it is generated. This work was published as a journal article [15].

8.2.4 Bringing Life out of Diversity: Boosting Network Lifetime using Multi-PHY Routing in RPL

Participants:

Mina Rady(INSA Lyon)

, Quentin Lampin(Orange Labs)

, Dominique Barthel(Orange Labs)

, Thomas Watteyne.

In this work, we propose a routing mechanism based on the RPL protocol in a wireless network that is equipped with a mix of short-range and long-range radios. We introduce Life-OF, an objective function for RPL which uses a combination of metrics and the diverse physical layers to boost the network's lifetime. We evaluate the performance of Life-OF compared to the classical MRHOF objective function in simulations. Two key performance indicators (KPIs) are reported: network lifetime and network latency. Results demonstrate that MRHOF tends to converge to a pure long-range network, leading to short network lifetime. However, Life-OF improves network lifetime by continuously adapting the routing topology to favor routing over nodes with longest remaining lifetime. Life-OF combines diverse radios and balances power consumption in the network. This way, nodes switch between using their short-range radio to improve their own battery lifetime and using their long-range radio to avoid routers that are close to depletion. Results show that using Life-OF improves the lifetime of the network by up to 470% that of MRHOF, while maintaining similar latency. This work was published as a journal article [10].

8.2.5 YSF: A 6TiSCH Scheduling Function Minimizing Latency of Data Gathering in IIoT

Participants:

Yasuyuki Tanaka(Keio University)

, Pascale Minet(Inria)

, Mališa Vučinić

, Xavi Vilajosana(Universitat Oberta de Catalunya)

, Thomas Watteyne.

Data gathering systems in the Industrial IoT require an end-to-end latency as low as one second with coverage of a few hundred meters. The 6TiSCH standard is well suited for these types of applications. A

6TiSCH network is a multi-hop wireless IPv6 network which uses Time Slotted Channel Hopping (TSCH). TSCH is a medium access mode of IEEE802.15.4 which provides deterministic properties, and increases robustness against external interference and multipath fading. A key component of TSCH is its scheduling function that builds the communication schedule, which greatly impacts network performance. Although there are several proposed TSCH scheduling solutions in the literature, most of them are not directly applicable to 6TiSCH for realworld deployments because they fail to take into consideration the dynamics of a network. Some of them assume a fixed routing topology, which does not match 6TiSCH where the routing topology dynamically changes with the radio environment. In this work, we propose a full-featured 6TiSCH scheduling function called YSF, that autonomously takes into account all aspects of network dynamics, including network formation phase and parent switching. YSF aims at minimizing latency and maximizing reliability for data gathering applications. We evaluate YSF by simulation, and compare it to MSF, the state-of-art scheduling function being standardized by the IETF 6TiSCH working group. This work was published as a journal article [13].

8.2.6 Joint Scheduling, Routing and Gateway Designation in Real-Time TSCH Networks

Participants:

Miguel Gutiérrez Gaitán(CISTER [Porto])
, Luis Almeida(CISTER [Porto])
, Thomas Watteyne
, Pedro M. d'Orey(CISTER [Porto])
, Pedro M. Santos(Faculdade de Engenharia da Universidade do Porto, FEUP)
, Diego Dujovne(Universidad Diego Portales).

This research proposes a co-design framework for *scheduling*, *routing* and *gateway designation* to improve the real-time performance of low-power wireless mesh networks. We target time-synchronized channel hopping (TSCH) networks with centralized network management and a single gateway. The end goal is to exploit existing trade-offs between the three dimensions to enhance traffic schedulability at systems' design time. The framework we propose considers a global Earliest-Deadline-First (EDF) scheduler that operates in conjunction with the minimal-overlap (MO) shortest-path routing, after a *centrality-driven* gateway designation is concluded. Simulation results over varying settings suggest our approach can lead to optimal or near-optimal real-time network performance, with 3 times more schedulable flows than a naive real-time configuration. This work was published as a conference paper [17].

8.2.7 AIOT: the All-in-1 IoT Educational Tool You Need

Participants:

Charles Thonier
, Thomas Watteyne
, Francois Garde(ESIROI)
, Tahiry Razafindralambo(ESIROI)
, Bertrand Marcon(LaboMap).

We created 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. This work was published as a conference poster [24].

8.3 Related to [A3] Security in Constrained Systems

Security takes a bigger and bigger part in the team. The standardization activity in the LAKE working group, which the team co-chairs, is very strong, with three Internet-Drafts (draft standards) published in 2022. This standardization activity has been a catalyst for joint research with other entities, resulting in the constant implementation of the standards being developped. In parallel, AIO is working quite a bit with the PROSECCO team to formally validate those implementations, even for use on embedded platforms.

8.3.1 IETF LAKE Standardization

Participants:

Mališa Vučinić

, Thomas Watteyne.

Context and goal. The AIO team participates in the standardization activities of the Internet Engineering Task Force (IETF). The AIO team co-chairs the IETF LAKE working group through Mališa Vučinić and participates in the standardization in IETF ACE and IETF LWIG working groups.

Summary of activities. The LAKE working group, formed in November 2019, is actively working on standardizing a lightweight authenticated key exchange protocol for Internet-of-Things use cases [14]. LAKE working group has held a total of 5 meetings in 2022, 2 interim and 3 official IETF meetings.

In 2022, the LAKE's protocol, EDHOC, has undergone a thorough formal study by the community. Under the coordination of Inria-AIO, three independent teams have worked on analyzing the protocol's security properties, using both computational security and symbolic security models:

- Cottier and Pointcheval have worked on a computational analysis of the protocol, studying its properties when authenticated using static Diffie-Hellman keys [38].
- Günther and Ilunga have worked on a computational analysis of the protocol, studying its properties when authenticated using signatures [45]
- Jacomme *et al.* have worked on a symbolic model, covering all authentication methods of the EDHOC protocol [52].

During the formal analysis stage, the protocol, as specified in the IETF was "frozen" and no updates to the specification were made during the period November 2021 – May 2022. The reviews by the community fine-tuned and future-proofed the protocol but no major security vulnerabilities were found. Finally, following the results of the formal analysis stage and the internal working group discussions, the LAKE working group published 5 revisions of the protocol. The version -18 of the protocol was submitted for publication in December '22 and the working group is now expecting the reviews by the Internet Engineering Steering Group (IESG). The publication process shepherd of the protocol is Mališa Vučinić of Inria-AIO.

The working group has also organized in 2022 3 interoperability testing events , co-located with the IETF meetings. Inria-AIO team has participated to these events with the implementation of the EDHOC protocol in Rust / hacspec (see Section 8.3.2).

Other IETF Activities. In 2022, Inria-AIO published 2 versions of a draft standard on lightweight authorization for authenticated key exchange [56], complementing the EDHOC protocol with 3rd party authorization information. This document will be considered for adoption in IETF LAKE, once the working group recharters. We also published a version of a draft standard on comparison of security protocols [59].

8.3.2 Towards a Formally-verified Implementation of IETF LAKE for Microcontrollers

Participants:
Mališa Vučinić
, Thomas Watteyne.

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 / hacspec. Hacspec is an executable specification language for cryptographic primitives, led by Inria Prosecco. The language can be automatically translated into e.g. F* and so used for formally verifying the implementation.

Summary of activities. Hacspec is executable on general purpose platforms but to date, no implementation has been attempted for constrained microcontrollers. The challenge when using hacspec on microcontrollers is that the standard library cannot be used due to the limited memory. We have designed and implemented the hacspec version of LAKE-EDHOC in a manner that uses only the features from the core Rust library, making it executable on constrained platforms, see 7.1.1. We tested the implementation on the following microcontrollers: nRF52840 from Nordic and CC2538 from Texas Instruments. It successfully completes the security handshake. At the time of the writing, we are benchmarking the implementation with regard the processing time and memory usage. We are coordinating with Inria Prosecco on proving the formal properties on the code such as panic freedom and injectivity of the transcripts. A publication on the subject is expected in 2023.

8.4 Related to [A4] Swarm Robotics

Maybe the biggest leap the team has taken in 2022 is jumping in the deep end of swarm robotics. The DotBot, which was a proof-of-concept platform at the end of 2021, has now turned into a true swarm robotics platform. We now have DotBots running around the lab, being controlled by a central orchestrator, using lighthouse as a cm-level localization solution.

8.4.1 Constrained Localization: a Survey

Participants:
Trifun Savic
, Xavi Vilajosana(Universitat Oberta de Catalunya)
, Thomas Watteyne.

Indoor localization techniques have been extensively studied in the last decade. The well established technologies enable the development of Real-Time Location Systems (RTLS). A good body of publications emerged, with several survey papers that provide a deep analysis of the research advances. Existing survey papers focus on either a specific technique and technology or on a general overview of indoor localization research. However, there is a need for a use case-driven survey on both recent academic research and commercial trends, as well as a hands-on evaluation of commercial solutions. This work aims at helping researchers select the appropriate technology and technique suitable for developing low-cost, low-power localization system, capable of providing centimeter level accuracy. The article is both a survey on recent academic research and a hands-on evaluation of commercial solutions. We introduce a specific use case as a guiding application throughout this article: localizing low-cost low-power miniature wireless swarm robots. We define a taxonomy and classify academic research according to five criteria: Line of Sight (LoS) requirement, accuracy, update rate, battery life, cost. We discuss localization fundamentals, the different technologies and techniques, as well as recent commercial developments and trends. Besides the traditional taxonomy and survey, this article also presents a hands-on evaluation of popular commercial localization solutions based on Bluetooth Angle of Arrival (AoA) and Ultra-Wideband (UWB). We conclude this article by discussing the five most important open research challenges: lightweight

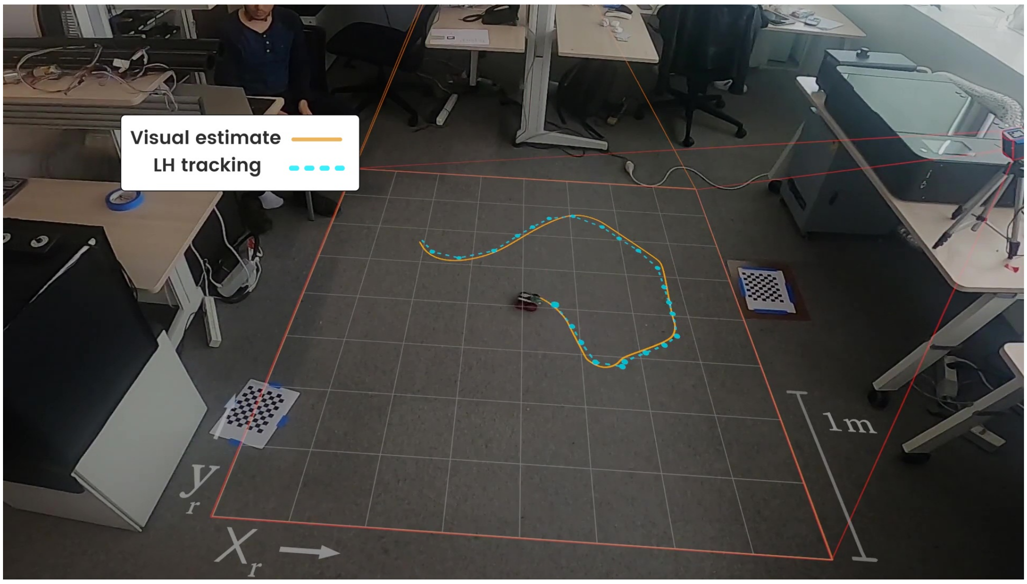


Figure 4: Demonstration of the indoor localization accuracy using lighthouse.

filtering algorithms, zero infrastructure dependency, low-power operation, security, and standardization. This work was published as a journal article [12].

8.4.2 Indoor Localization of Multiple Miniature Robots

Participants:

Filip Maksimovic

, Said Alvarado-Marin

, Alexandre Abadie

, Trifun Savic

, Thomas Watteyne.

In order to localize large numbers of small robots, we apply lighthouse localization technology originally design for virtual reality applications. To investigate the feasibility of the positioning system for microrobotic swarms, we implement lighthouse decoding and tracking on a low-power wireless microcontroller in a cm-scale form factor. One-time scene solving is performed on a computer after aggregating multiple individual robot measurements. After the scene solving is performed, the necessary pre-computed matrices are sent to the robots, and if all further computation is performed on the on-board 64 MHz Cortex-M4, the localization rate is nearly 10 Hz for planar robots. If, instead, no computation is performed on the robot and all localization is done by an off-board computer, the update rate is 50 Hz. The accuracy of the technique is 1.08 cm RMS for planar robots when compared to a “ground truth” single-camera motion-capture approach, see Fig. 4. Scene solving and localization with the lighthouses is performed both with a single robot in motion and with three robots simultaneously as a small-scale demonstration of multi-robot localization.

8.4.3 RRDV: Robots Rendez-Vous Detection Using Time-Synchronized Ultrasonic Sensors

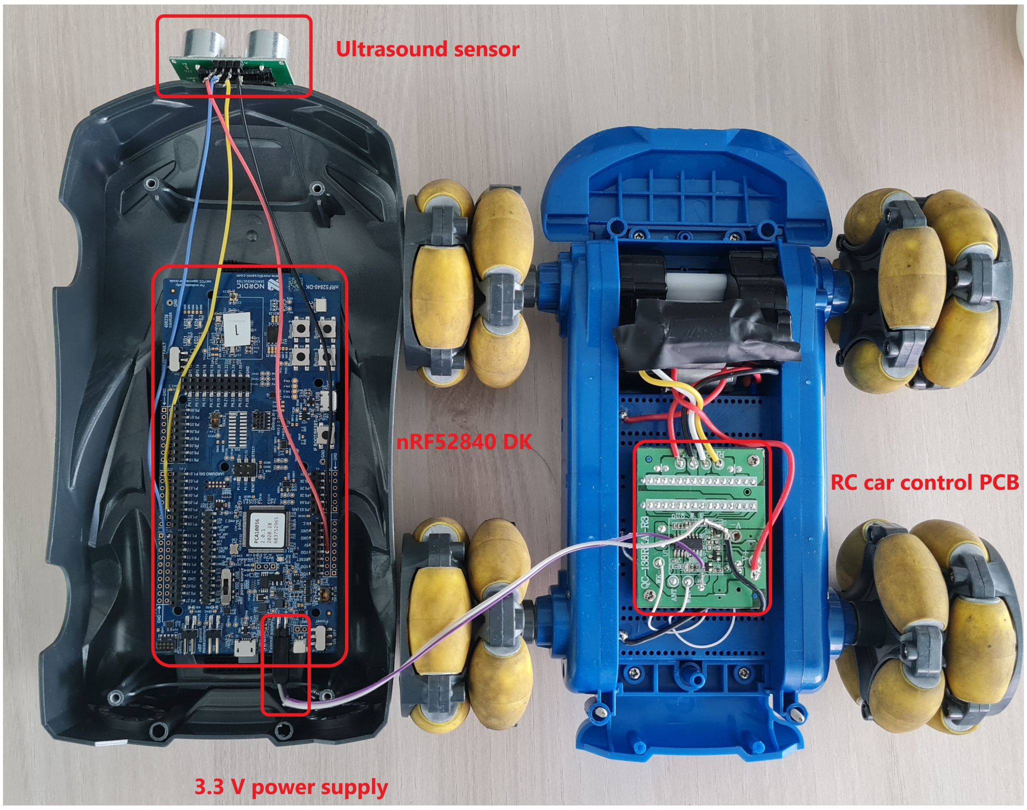


Figure 5: For the experimental validation of RRDV [19], we modified a toy by equipping it with an RF transceiver and an ultrasound sensor.

Participants:

Trifun Savic

, Said Alvarado-Marin

, Filip Maksimovic

, Thomas Watteyne.

In order to assist in the localization of constrained robotic systems, we proposed and implemented a Robot Rendez-Vous Detection (RRDV), a system for robot-to-robot encounter detection. We use a low-cost ultrasound sensor and time-synchronized mobile robots to detect when two robots are facing one another. Ultrasound ranging is triggered by the control application on a computer. The application sends a ranging command to the gateway, which broadcasts it to the mobile robots over the radio. Robots synchronize their ultrasound trigger pin with the start of frame event and send back the notifications with measured distances using Time-Division Multiple Access (TDMA). The system then finds the encounters by searching for timestamps where the difference in distance reported by two robots is less then 1 cm. In the current implementation, the system achieves a 20 Hz distance measurement update rate. RRDV is validated experimentally using 5 mobile robots which are controlled by the users and moved randomly, see Fig. 5. We implemented a Computer Vision (CV) algorithm for tracking mobile robots as they move and detect when they are facing one another. The CV algorithm is used as the ground truth for the experimental evaluation. The results show 96.7% successfully detected robot encounters, when the duration of the encounter is more than 5 s. This work was published as a conference paper [19].

8.4.4 CARA: Connectivity-Aware Relay Algorithm for Multi-Robot Expeditions

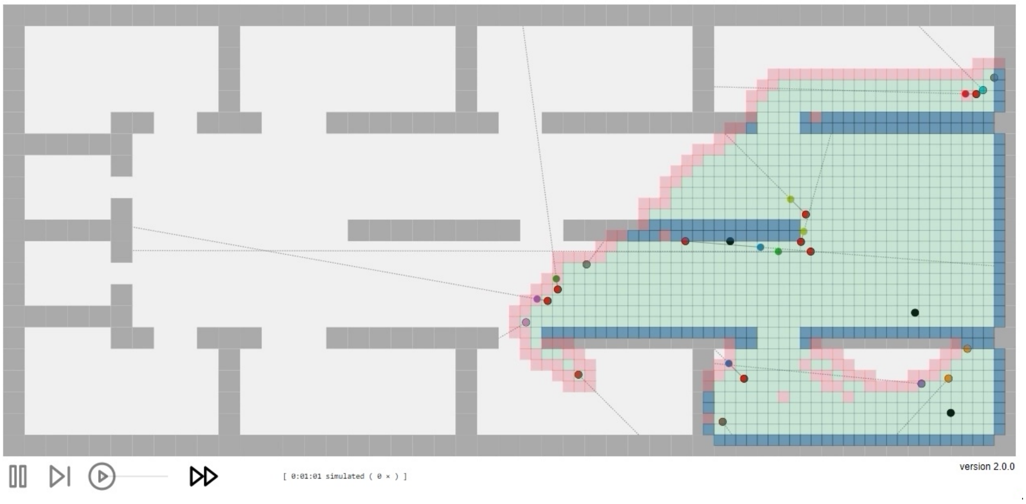


Figure 6: Interface of the Atlas simulator used to evaluate CARA [6].

Participants:

Razanne Abu Aisheh

, Francesco Bronzino(ENS Lyon)

, Lou Salaün(Nokia Bell Labs)

, Thomas Watteyne.

Exploration of unknown environments is an essential application of multi-robot systems, 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. One of the main ways to expand coverage is placing relays. Existing relay placement algorithms tend to either require prior knowledge of the environment, or rely on maintaining specific distances between the relays and the rest of the robots. These approaches lack flexibility and adaptability to the environment. This work introduces the “Connectivity Aware Relay Algorithm” (CARA), a dynamic context-aware relay placement algorithm that does not require any prior knowledge of the environment. We compare CARA against a state-of-the-art distance based relay placement algorithm using the Atlas simulator, see Fig. 6. Results demonstrate that CARA outperforms the state-of-the-art algorithm in terms of time to completion by a factor of 10 as it places, on average, half the number of relays. This work was published as a journal article [6].

8.5 Related to [A5] Vehicle Area Networking

The domains of Mobile Ad-Hoc Networks (MANET) and Vehicle Area Networks (VANET) are fascinating in the vision they offer in terms of user experience and satefy in the future of mobility. The team has explored them by applying Artificial Intelligence, Blockchain, Game Theoretic and Deep Reinforcement Learning approaching to the communication aspects of these times of networks.

8.5.1 Study Of MANET solutions for Radio Communication System based On Artificial Intelligence Algorihtms

Participants:

Cedric Adjih(Inria TRiBE)

, Felix Marcoccia

, Paul Mühlethaler.

Context and goal. The uprising of fifth generation fighters and unmanned combat aircrafts, designed to reach a high level of stealth and to follow a highly collaborative concept of operation, presents new challenges for military radio communication systems to meet expectations in terms of low probability of detection and interception while offering high throughput and low latency networking capabilities. To face this challenge, new communications solutions have been envisioned to operate in high spectrum bands (>10 GHz) where large bandwidth can be used despite constraints on spectrum allocated to military purposes. Such bands, particularly susceptible to signal degradation, impose the use of directive antennas to meet range and throughput requirements. The current challenge is to design an efficient ad-hoc networking system based on individual point-to-point communication links. During the last few years, military aeronautical communications have already evolved to support not only voice and tactical data, but also a growing part of machine-to-machine communications (e.g. sensor collaboration), making use of MANET principles at the routing protocol level. Applying such principles in the context of directive antenna has to be performed not only at routing level, but also at a network configuration level, where each point-to-point link has to be chosen, set up, maintained or disrupted to continuously adapt the network to fit with propagation, topology and technological constraints as well as operational connectivity needs. The optimization of such wireless networks with a high level of possible configurability poses new scientific challenges. It induces the need for simultaneous cross-layer considerations in order to optimize the network. Unlike traditional MANETs with a clearer separation of layers (physical and MAC layer, routing layer, application), here the question is how to best configure the system, to satisfy several objectives: establishing the connectivity of the network itself at the link level, but also at the multi-hop routing level, and satisfying the quality of service and requirements of active applications, and finally managing the dynamicity of the changes. Thus algorithmic solutions can no longer be simple solutions as simple 3-way link establishment, Dijkstra route computations, etc.: they result in more complex global optimization problems, and require new approaches that are heuristic by nature. Good candidates of methods come from machine learning approaches.

With the collaboration between Thales and Inria, the outcomes of this project are expected in multiple areas: first of all, the objective is to solve immediate scientific and technological issues for actual military networks (and upcoming next-generation products); second, addressing those, will provide applicable solutions and methods for more general classes of wireless networks (e.g. cellular, or IoT networks); in particular the application and the development of machine learning methods applied to network problems.

Summary of activities. The project has performed the following tasks:

- a formalization of the problem is in progress
- the state-of-the-art concerning of machine learning algorithms applied to the representation and the study of graphs is in progress
- the scaling laws of the global through in a multi-hop has been studied both with omnidirectional and directional antennas

8.5.2 Architecture for Sharing and Storing Data in a Cloud Computing Environment based on Blockchain Technology

Participants:
Houaida Ghanmi(FSG-Tunisie)
, Haifa Touati(FSG-Tunisie)
, Paul Mühlethaler
, Nasreddine Hajlaoui(FSG-Tunisie)
, Mohamed Elhadad(IRT SystemX).

Context and goal. Cloud computing is a model for providing convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage devices, applications, and services). It allows companies to reduce total costs by outsourcing their required services. The rapid development of this technology in recent years makes it more critical. Indeed, it introduces new security challenges in the management and control of secure services, the protection of privacy, the confidentiality of data, the protection of data integrity in distributed databases, the backup of data, synchronization and the procedures necessary for their processing. As a result, cloud security becomes a competitive challenge among cloud providers. The traditional cloud security trust model typically adopts a centralized architecture, resulting in significant management overhead, network congestion, and even a single point of failure. Additionally, due to a lack of transparency and traceability, the results of the trust assessment may not be fully recognized by all participants. Nowadays, the use of blockchain in cloud computing is one of the most common innovations that can solve the security problems of cloud computing due to its underlying characteristics such as transparency, traceability, decentralization, security, immutability and automation. Blockchain is a decentralized data management technology that can be leveraged to address the challenges of ensuring data security, anonymity, and integrity without any third party. The main objective of this thesis is to propose a secure, distributed and decentralized trust architecture for cloud computing environments based on blockchain technology. The proposed solution must meet security needs in terms of trust, authentication, confidentiality and integrity. Integrating blockchain into cloud outsourcing services will eliminate third parties and this combination will help manage trust assessment and security issues.

Summary of activities. The effort is put on the state-of-the-art of cloud computing using the blockchain technology. We study the way in which the blockchain is applied to provide security services in cloud computing models, we analyze the research trends of related techniques to integrate blockchain into current cloud computing models, we summarize the possible architectures and models and we analyze the main challenges.

8.5.3 Attack Detection Mechanisms and their Limitations in Named Data Networking (NDN)

Participants:
Abdelhak Hidouri(FSG-Tunisie)
, Haifa Touati(FSG-Tunisie)
, Paul Mühlethaler
, Nasreddine Hajlaoui(FSG-Tunisie)
, Mohamed Elhadad(IRT SystemX).

Proposals for Information Centric Networking (ICN) have recently emerged to rethink the foundations of the Internet and design a native data-oriented network architecture. Among the current ICN projects, Named Data Networking (NDN) is a promising architecture supported by the National Science Foundation (NSF). The NDN communication model is based on the Publish/Subscribe paradigm and focuses on broadcasting and finding content and introduces caching in intermediate routers. Data packets are sent in response to a prior request called an Interest packet and the data are cached along the way to the original requester. Content caching is an essential component of NDN in order to reduce bandwidth consumption and improve data delivery speed, however, this feature allows malicious nodes to perform attacks that are relatively simple to implement but very effective. For that reason, the goal of this work is to study and classify the types of attacks that can target the NDN architecture (Cache Pollution Attack (CPA), Cache Poisoning Attack, Cache Privacy Attack, Interest Flooding Attack (IFA), etc.) according to their consequences in terms of reducing the performance of the network. Moreover, we give an overview about the proposed detection mechanisms and their limitations, see [20] .

8.5.4 A Detection Mechanism for Cache Pollution Attack in Named Data Network Architecture

Participants:

Abdelhak Hidouri(FSG-Tunisie)
, Haifa Touati(FSG-Tunisie)
, Paul Mühlethaler
, Nasreddine Hajlaoui(FSG-Tunisie)
, Mohamed Elhadad(IRT SystemX).

Basic Named Data Networks (NDN) security mechanisms, rely on two main key features. The first one is the caching mechanism where it manages to minimize both the bandwidth usage and the data retrieval delay all along with congestion avoidance by storing, in the intermediate routers, the contents recently demanded to quickly serve future consumers' requests. The second key feature is the NDN security which stands on its foundation by signing each Data as soon as it released by the Producer and gets verified by each requesting consumer so that it makes it resilient to most attacks that affect the integrity of such content and the privacy of its end points. However, the availability of the Data in the cache of the CS allows the malicious consumers to perform several attacks such as Cache Pollution Attack (CPA) which is easy to implement and extremely effective. As a result, it makes the data on the cache unavailable for legitimate consumers and increases its retrieval delay. In this work, we propose a new detection mechanism of CPA called ICAN (Intrusion detection system for CPA attack in NDN architecture) based on several metrics such as Average Cache Hit Ratio, Average Interest Inter-Arrival Time, Hop Count and Prefix variation. We assess by simulation, using the NDNSim framework, the efficiency of our mechanism and the choice of the used parameters. Finally, we elaborate a qualitative comparison between our proposed solution and the state-of-the-art mechanisms, see [18].

8.5.5 A Game Theoretic Approach to Irregular Repetition Slotted Aloha

Participants:

Iman Hmedoush(Nokia)
, Cedric Adjih(Inria TRiBE)
, Kinda Khawam(Univ. Versailles)
, Paul Mühlethaler.

Many technological enhancements are being developed worldwide to enable the "Internet of Things" (IoT). IoT networks largely rely on distributed access of billions of devices, but are still lagging in terms of combined reliability and low latency. To mend that shortcoming, it is paramount to adapt existing random access methods for the IoT setting. In this article, we shed light on one of the modern candidates for random access protocols fitted for IoT: the "Irregular Repetition Slotted ALOHA" (IRSA). As self-managing solutions are needed to overcome the challenges of IoT, we study the IRSA random access scheme in a distributed setting where groups of users, with fixed traffic loads, are competing for ALOHA-type channel access. To that aim, we adopt a distributed game-theoretic approach where two classes of IoT devices learn autonomously their optimal IRSA protocol parameters to optimize selfishly their own effective throughput. Through extensive simulations, we assess the notable efficiency of the game based distributed approach. We also show that our IRSA game attains the Nash equilibrium (NE) via the "better reply" strategy, and we quantify the price of anarchy in comparison with a centralized approach. Our results imply that user competition does not fundamentally impact the performance of the IRSA protocol, see [9].

8.5.6 Deep Learning, Sensing-based IRSA (DS-IRSA): Learning a Sensing Protocol with Deep Reinforcement Learning

Participants:
Iman Hmedoush(Nokia)
, Cedric Adjih(Inria TRiBE)
, Paul Mühlethaler.

Irregular Repetition Slotted Aloha (IRSA) is one candidate member of a family of random access-based protocols to solve massive connectivity problem for Internet of Things (IoT) networks. The key features of this protocol is to allow users to repeat their packets multiple times in the same frame and use Successive Interference Cancellation (SIC) to decode collided packets at the receiver. Although, the plain IRSA scheme can asympotically reach the optimal 1 [packet/slot]. But there are still many obstacles to achieve this performance, specially when considering short frame length. In this report, we study two new variants of IRSA with short frame length, and we optimize their performance using a Deep Reinforcement Learning approach. In our first variant, Random Codeword Selection-IRSA (RC-IRSA), we consider an IRSA approach with random codeword selection, where each codeword represents the transmission strategy of a user on the slots. We apply a Deep Reinforcement Learning to optimize RC-IRSA: we train a Deep Neural Network model that choses the slots on which the user sends its packets. Our DRL approach for RC-IRSA is a new optimization method for IRSA using a DRL approach and it works as a base for our second proposed IRSA variant DS-IRSA. Our second variant is a sensing protocol based on IRSA and trained with machine learning to synchronize the nodes during the transmission and avoid collisions. For that aim, we proposed DS-IRSA, Deep Learning Sensing-based IRSA protocol which is composed of two phases: a sensing phase, where the nodes can sense the channel and send short jamming signals, followed by a classical IRSA transmission phase. We use a DRL algorithm to optimize its performance. Our proposed protocol has shown an excellent performance to achieve an optimal performance of almost 1 [decoded user/slot] for small frame sizes (≤ 5) slots and with enough sensing duration, see [23].

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”.
- 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 Research: Mališa Vučinić co-authors multiple IETF draft standards with Ericsson Research. We have also published together a paper [14] on LAKE standardization.
- Sony Research: Mališa Vučinić collaborates on 6TiSCH network design and security, including IETF standadization activities.

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") on 14-Jan-2022, an annual innovation competition organized in partnership with the French Ministry of Economy. The Falco solution is now deployed in 15 marinas; the Falco team is now 17 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 Inria Associate Team, part of Inria International Program

Participants:

Filip Maksimovic

, Sara Faour

, Thomas Watteyne

, Mališa Vučinić.

SWARM

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

Duration: 2021 -> 2023

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

Partners:

- UC Berkeley
- Inria AIO, France

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 STIC-AmSud project

Participants:

Mališa Vučinić

, Theo Akbas

, Trifun Savic

, Said Alvarado-Marin

, Thomas Watteyne.

Emistral

Title: Environmental Monitoring And Inspection Sailboat via Transfer, Reinforcement and Authonomous Learning

Duration: 2021 -> 2023

Coordinator: Luis Marti (lmarti@inria.cl)

Partners:

- Inria Chile, Chile
- Universidade Federal Fluminense, Brazil
- Universidade Federal Rio Grande do Norte, Brazil
- Inria SCOOL, France
- Inria AIO, France
- Universidad de la Republica, Uruguay

Inria contact: Mališa Vučinić

Summary: The current climate crisis calls for the use of all available technology to try to understand, model, predict and hopefully work towards its mitigation. Oceans play a key role in grasping the complex and intertwined processes that govern these phenomena. Oceans – and rivers – play a key role in regulating the planet's climate, weather and ecology. Recent advances in computer sciences and applied mathematics, such as machine learning, artificial intelligence, scientific computation, among others, have produced a revolution in our capacity for understanding the emergence of patterns and dynamics in complex systems while at the same time the complexity of these problems pose significant challenges to computer science itself. The key factor deciding about the success of failure of the application of these methods is having sufficient and adequate data. Oceanographic vessels have been extensively used to gather this data. However, they have been shown to be insufficient because their high operation cost, the risks involved and their limited availability. Autonomous sailboats present themselves as a viable alternative. In principle, by relying on wind energy they could operate for indefinite periods being only limited by the effects of fouling and the wear and tear of materials. Recent results in the area of machine learning are especially suited to fill this gap. In particular, reinforcement learning (RL), transfer learning (TL) and autonomous learning (AL). The combination of those methods could overcome the need of programming particular controller for every boat as it would be capable of replicating at some degree, the learning process of human skippers and sailors.

10.1.3 Others

- AIO and the Pister team at UC Berkeley awarded an award from the France-Berkeley-Fund for project "M3: Marvelous Micro-Motes" (2020-2022).
- Cristobal Huidobro-Marin came to AIO for an internship on "Low-Cost Human Motion Tracking" as part of an internship program coordinated by Inria Chile (1-Jun-2022 – 26-Aug-2022).

10.2 International research visitors

10.2.1 Visits of International Scientists

Neelakandan Rajamohan

Status: Professor

Institution of origin: IIT Goa

Country: India

Dates: 1-2 Dec-2022

Type of mobility: lecture

Soumya Banerjee

Institution of origin: University College Cork

Country: Ireland

Dates: 16-Nov-2022 to 7-Dec-2022

Type of mobility: research stay

Leila Saidane

Status: Professor

Institution of origin: ENSI

Country: Tunisia

Dates: 10-Nov-2022 to 16-Dec-2022

Type of mobility: research stay

Miguel Gutiérrez Gaitán

Status: PhD Student

Institution of origin: U. Porto

Country: Portugal

Dates: 01-Apr-2022 – 31-Jul-2022

Type of mobility: research stay

10.2.2 Visits to international teams (Research stays abroad)

Filip Maksimovic

Visited institution: UC Berkeley

Country: US

Dates: 21-Apr-2022 — 25-May-2022

Context of the visit: SWARM associate team

Type of mobility: research stay

Filip Maksimovic

Visited institution: Portland State University

Country: US

Dates: 28-Apr-2022 — 2-May-2022

Context of the visit: workshop organizer

Type of mobility: research stay

Filip Maksimovic

Visited institution: UC Berkeley

Country: US

Dates: 7-Dec-2022 — 13-Dec-2022

Context of the visit: SWARM associate team

Type of mobility: research stay

10.3 European Initiatives

10.3.1 Horizon Europe

Participants:
Thomas Watteyne
, Mališa Vučinić
, Filip Maksimovic.

The Inria team has coordinated a Horizon Europe proposal called "OpenSwarm" which was accepted. This is for out team a major milestone. The Horizon Europe OpenSwarm project starts on 1-Jan-2023, and has a duration of 40 months. The consortium is composed of 9 partners (Inria, IMEC, KU Leuven, University of Sheffield, Siemens Germany, Siemes Austria, Analog Devices, Ingeniarius, Wattson Elements). The project is coordinated by Inria, Thomas Watteyne is the scientific coordinator. The scientific project of OpenSwarm is closely related to the research program of AIO. We are tremendously excited as we see OpenSwarm as a true catalyst for our work.

10.3.2 Horizon 2020

Participants:
Mališa Vučinić.

H2020 SPARTA is a European excellence network in cybersecurity. The team's activities related to the standardization in IETF LAKE and IETF ACE are fed as inputs to SPARTA. The SPARTA project concluded on 31-Jan-2022.

10.4 National Initiatives

10.4.1 Exploratory Research Action - Inria Project Labs

- 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 platformis 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.

- IPL RIOT-fp, 2019-2022. RIOT-fp is an Inria Project Lab on cyber-security targeting low-end, microcontroller-based IoT devices, which run operating systems. Mališa Vučinić leads.

11 Dissemination

11.1 Scientific Citizenship

11.1.1 General Chair

- Paul Mühlethaler was honorary chair and co-organizer of the "Performance Evaluation and Modeling in Wired and wireless Networks" (PEMWN) conference, in 2022. The conference took place in Rome, Italy, 8-10 November 2022 Twelve international papers were presented. In addition, three keynote addresses and one tutorial were given:

  - "Demystifying 5G Electromagnetic Pollution with Traffic-based Measurements", by Luca Chiaraviglio, University of Rome - Tor Vergata, Italy.
  - "Semantic and Goal-Oriented Communications", by Sergio Barbarossa, Sapienza University, Rome, Italy.
  - "Frauds in the Cryptocurrency Ecosystem" by Alessandro Mei, Sapienza University, Rome, Italy.
  - "Data Dissemination in UAV Networks: Use Case Oriented Bio-inspired Routing Schemes" by Saadi Boudjit, Sorbonne University Paris Nord, France.

- Paul Mühlethaler was co-chair with Eric Renault of the "International Conference on Machine Learning for Networking" (MLN), in 2022. The conference took place at Inria Paris, 28-30 November 2022. Fourteen internaional papers were presented. In addition, three keynote addresses and one tutorial were given:

  - "Interpretable & Explainable Machine Learning (IML/XAI) in the Industrial IoT Domain: Are Bayesian Optimization and IML/XAI Far from Each Other?" by Soumya Banerjee, Research & Innovation Trasna Solutions Ltd., Europe.
  - "Reinforcement Learning for Irregular Slotted Aloha (IRSA) with Short Frames" by Iman Hmedoush, Nokia Bell Labs, France.
  - "Evolution of Network Architectures and Protocol Stacks" by Constantine Dovrotis, Georgia Institute of Technology, USA.
  - "Cloud Solution Architect – Artificial Intelligence & Machine Learning" by Franck Gaillard, Microsoft, France.

- Filip Maksimovic co-chaired the SCuM workshop organized at Portland State University on 28-Apr-2022 – 2-May-2022

11.1.2 Member of the Organizing Committees

- Thomas Watteyne was member of the organizing committee of the Inria Scientific Days in 2022.
- Paul Mühlethaler was member of the organizing committee of PEMWN 2022.
- Paul Mühlethaler and Thierry Plesse (DGA) organized a joint seminar on 5G Networks that took place at Inra Paris on 31-May-2022.

11.1.3 Journal Reviewer

- Filip Maksimovic, reviewer for IEEE Transactions on Microwave Theory and Techniques
- Filip Maksimovic, reviewer for IEEE International Conference on Robotics and Automation
- Filip Maksimovic, reviewer for IEEE Transactions on Circuits and Systems I: Regular Papers
- Paul Mühlethaler, reviewer for Ad Hoc Networks (Elsevier)
- Paul Mühlethaler, reviewer for Computer Communication (Elsevier)
- Paul Mühlethaler, reviewer for Vehicular Communications (Elsevier)
- Paul Mühlethaler, reviewer for IEEE Transactions on Intelligent Transportation Systems
- Mališa Vučinić, reviewer for IEEE Access
- Mališa Vučinić, reviewer for IETF Security directorate
- Mališa Vučinić, reviewer for IETF Internet of Things directorate

11.2 Scientific Leadership

11.2.1 Standardization Activities

- Mališa Vučinić is co-chair of the IETF LAKE working ground. 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 113 people, with a healthy mix of industrial and academia contributors. The WG met three times in 2022: in Vienna, Austria (IETF 113, 19-Mar-2022 – 25-Mar-2022), in Philadelphia, PA, USA (IETF 114, 23-Jul-2022 – 29-Jul-2022), in London, UK (IETF 115, 5-Nov-2022 – 11-Nov-2022). In 2022, the LAKE WG has produced three Internet-Drafts (which will become standards). Mališa Vučinić has been involved in all three; he is author of one and shepperd of another.

11.2.2 EU Working Groups

- Filip Maksimovic is a member 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 is member of the Inria-Paris “Commission de Développement Technologique” since 2018, where we ensure Inria project teams get sufficient engineering resources to change the world.
- Thomas Watteyne has the critical responsibilty of the Inria Paris guitar, which anyone can borrow for an hour, a day or a week-end free of charge.

11.2.4 Tutorials

- Thomas Watteyne gave a tutorial entitled “Dust Academy: Getting Your Hands Dirty!” at the 2022 IEEE-SPS / EURASIP Summer School on Data and Graph Driven Learning for Communications and Signal Processing, Banja Luka, Bosnia and Herzegovina, 5-9 September 2022.

11.2.5 Invited Talks

- Thomas Watteyne was invited to give a talk on “DotBot: cm-scale, easy-to-use micro-robot for Swarm Research”, Inria Scientific Days, Rocquencourt, France, 24-Nov-2022.
- Thomas Watteyne was invited to give a talk on “Les Technologies de l’Internet des Objets”, at ESIROI, Saint-Pierre, La Reunion, 2-Nov-2022.
- Thomas Watteyne was invited to give a talk on “Internet des Objets et Capteurs”, at the Cercle Entreprise et Sante, Paris, France, 19-Jan-2022.
- Mališa Vučinić was invited to give a talk on “IETF LAKE: Lightweight Authenticated Key Exchange for Internet-of-Things Use Cases” at the 2nd Future Network Security: Challenges and Opportunities Workshop.

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, 31-Oct-2022 – 4-Nov-2022.
- Thomas Watteyne taught course “Dust Academy: Getting Your Hands Dirty!”, at the 2022 IEEE-SPS / EURASIP Summer School on Data and Graph Driven Learning for Communications and Signal Processing, Banja Luka, Bosnia and Herzegovina, 5-9 September 2022.
- Thomas Watteyne taught a 1/2-day crash course on the Industrial IoT, Telecom ParisTech. Graduate level. 26-Sep-2022.
- Thomas Watteyne coordinated a 6-week hands-on course on IoT. Undergraduate level. ENSTA Paris. Together with Mališa Vučinić, Dominique Barthel (Orange Labs), Quentin Lampin (Orange Labs). April-May 2022.
- Mališa Vučinić taught the hands-on Internet of Things course at NGO Prona, Montenegro, from December 2022 to February 2023.
- Mališa Vučinić taught the laboratory part (travaux pratiques) of the Internet of Things course at ENSTA Paris in March-April 2022, with Thomas Watteyne.
- Mališa Vučinić taught a 1-day course on IoT security at ENSTA Paris in March 2022.

11.3.2 PhD Supervision

- Thomas Watteyne supervises the PhD studies of:
  - Trifun Savic
  - Razanne Abu Aisheh
  - Said Alvarado-Marin (co-supervisor only, the real work is done by Filip Maksimovic)
- Filip Maksimovic supervises the PhD study of:
  - Said Alvarado-Marin
- Paul Mühlethaler supervises the PhD studies of:

  - Haouda Ghamni
  - Iman Hmedoush (Nokia)
  - Abdelhak Hidouri (FSG-Tunisie)
  - Tayssir Ismael
  - Felix Marcoccia

- Mališa Vučinić supervises the PhD study of:
  - Sara Faour

11.3.3 PhD Juries

- Thomas Watteyne was member of the examination board of the 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.
- Thomas Watteyne was member of the examination board of the PhD thesis of Fabian Antonio Rincon Vija, as “rapporteur”. Doctoral work on “Enabling Robust Wireless Communication for Battery Management Systems in Electric Vehicles” done between IMT Atlantique and Renault, under the supervision of Georgios Z. Papadopoulos (IMT Atlantique), Nicolas Montavont (IMT Atlantique) and Samuel Cregut (Renault). Viva on 14-Dec-2022.
- Paul Mühlethaler was examiner for Iman Hmedoush’s PhD Thesis with Paris Sorbonne University entitled “Connectionless Transmission in Wireless Networks (IoT)” [22] and defended on 18-May-2022.
- Paul Mühlethaler was reviewer for Mamoudou Sangare’s PhD Thesis with Paris Sorbonne University entitled “Exploring Prediction Strategies in Vehicular Networks through Machine Learning Techniques and Hybrid Intelligence” and defended on 11-Jul-2022.
- Paul Mühlethaler was reviewer for Faiz Sanaullah’s PhD Thesis with Paris Sorbonne North University entitled “Increasing Vehicles Cooperative Preception through Enhanced CAM Service” and defended on 28-Sep-2022.
- Paul Mühlethaler was reviewer for Sehla Khabaz’s PhD Thesis with Paris Sorbonne University entitled “Resource Allocation in C-V2X From LTE-V2X to 5G-V2X” and defended on 30-Nov-2022.
- Paul Mühlethaler was reviewer for Hager Hafaiedh’s PhD Thesis with Gustave Eiffel University entitled “Dèploiement de la 5G dans un Contexte IoT” and defended on 12-Dec-2022.

11.4 Outreach

11.4.1 Within Inria

- Alexandre Abadie and Razanne Abu Aisheh gave a live demo of the DotBot testbed at the Inria Scientific Days on 24-Nov-2022.

11.4.2 Participation in Outreach Events

- Thomas Watteyne was invited to give a talk on “Les Technologies de l’Internet des Objets”, at ESIROI, Saint-Pierre, La Reunion, 2-Nov-2022.
- Thomas Watteyne was invited to give a talk on “Internet des Objets et Capteurs”, at the Cercle Entreprise et Sante, Paris, France, 19-Jan-2022.

11.4.3 In The News

- Thomas Watteyne contributed to the Whitepaper on wildfire detection and prevention published on Kineis in December 2022.
- Thomas Watteyne appeared in "Quelles stratégies pour combattre les feux de forêts ?", in "C'est deja demain", France 3 Rhone-Alpes (one of France's main national TV stations), 12-Oct-2022 [YouTube]
- Razanne Abu Aisheh contributed to "DotBot, a new affordable micro-robot for research purposes", Inria, 13-Jun-2022.
- Embedded Trophies 2021 : two Inria startups laureate, Inria.fr, 25-Jan-2022.
- Trophées de l'Embarqué 2021 : deux startups Inria lauréates, Inria.fr, 25-Jan-2022
- A closer look at a joint Inria-Berkeley project: M3 Marvelous Micro-Motes, Inria Silicon Valley, 21-Jan-2022.
- Estudiantes chilenos realizan sus pasantías de investigación en Francia, Inria Chile, 14-Jan-2022.
- Un écosystème numérique pour un port plus efficace, BoatIndustry, 5-Jan-2022

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] T. Chang, T. Watteyne, B. Wheeler, F. Maksimovic, D. C. Burnett and K. Pister. 'Surviving the Hair Dryer: Continuous Calibration of a Crystal-Free Mote-on-Chip'. In: *IEEE Internet of Things Journal* (15th Mar. 2022). URL: https://hal.inria.fr/hal-03538248.

[2] I. Hmedoush, C. Adjih, K. Khawam and P. Mühlethaler. 'A Game Theoretic Approach to Irregular Repetition Slotted Aloha'. In: *IEEE Access* 10 (5th Jan. 2022), pp. 4600–4614. DOI: 10.1109/ACCESS.2022.3140495. URL: https://hal.inria.fr/hal-03533559.

[3] Y. Tanaka, P. Minet, M. Vučinić, X. Vilajosana and T. Watteyne. 'YSF: a 6TiSCH Scheduling Function Minimizing Latency of Data Gathering in IIoT'. In: *IEEE Internet of Things Journal* (1st June 2022). DOI: 10.1109/JIOT.2021.3118017. URL: https://hal.inria.fr/hal-03538246.

[4] 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://hal.inria.fr/hal-03434293.

[5] Z. Zhang, S. D. Glaser, T. Watteyne and S. Malek. 'Long-term Monitoring of the Sierra Nevada Snowpack Using Wireless Sensor Networks'. In: *IEEE Internet of Things Journal* (15th Sept. 2022). URL: https://hal.inria.fr/hal-01388391.

12.2 Publications of the year

International journals

[6] R. Abu-Aisheh, F. Bronzino, L. Salaun and T. Watteyne. 'CARA: Connectivity-Aware Relay Algorithm for Multi-Robot Expeditions'. In: *Sensors* 22.23 (22nd Nov. 2022). URL: https://hal.inria.fr/hal-03943660.

[7] T. Chang, T. Watteyne, B. Wheeler, F. Maksimovic, D. C. Burnett and K. Pister. 'Surviving the Hair Dryer: Continuous Calibration of a Crystal-Free Mote-on-Chip'. In: *IEEE Internet of Things Journal* (15th Mar. 2022). URL: https://hal.inria.fr/hal-03538248.

[8] J. Crnogorac, J. Crnogorac, M. Vucinic, E. Kočan and T. Watteyne. 'Dense Multi-Channel Sniffing in Large IoT Networks'. In: *IEEE Access* (1st Oct. 2022). DOI: 10.1109/ACCESS.2022.3210966. URL: https://hal.inria.fr/hal-03783828.

[9] I. Hmedoush, C. Adjih, K. Khawam and P. Mühlethaler. 'A Game Theoretic Approach to Irregular Repetition Slotted Aloha'. In: *IEEE Access* 10 (5th Jan. 2022), pp. 4600–4614. DOI: 10.1109/ACCESS.2022.3140495. URL: https://hal.inria.fr/hal-03533559.

[10] M. Rady, Q. Lampin, D. Barthel and T. Watteyne. 'Bringing life out of diversity: Boosting network lifetime using multi-PHY routing in RPL'. In: *Transactions on emerging telecommunications technologies* (17th July 2022), e4592. DOI: 10.1002/ett.4592. URL: https://hal.inria.fr/hal-03726255.

[11] M. Rady, J. M. Munoz Soto, R. Abu-Aisheh, M. Vucinic, J. Astorga Tobar, A. Cortes, Q. Lampin, D. Barthel and T. Watteyne. 'A Historical Twist on Long-Range Wireless: Building a 103 km Multi-Hop Network Replicating Claude Chappe's Telegraph'. In: *Sensors* (6th Oct. 2022). DOI: 10.3390/s22197586. URL: https://hal.inria.fr/hal-03820397.

[12] T. Savić, X. Vilajosana and T. Watteyne. 'Constrained Localization: A Survey'. In: *IEEE Access* 10 (2nd May 2022), pp. 49297–49321. DOI: 10.1109/ACCESS.2022.3171859. URL: https://hal.inria.fr/hal-03668819.

[13] Y. Tanaka, P. Minet, M. Vučinić, X. Vilajosana and T. Watteyne. 'YSF: a 6TiSCH Scheduling Function Minimizing Latency of Data Gathering in IIoT'. In: *IEEE Internet of Things Journal* (1st June 2022). DOI: 10.1109/JIOT.2021.3118017. URL: https://hal.inria.fr/hal-03538246.

[14] 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://hal.inria.fr/hal-03434293.

[15] Z. Zhang, S. D. Glaser, T. Watteyne and S. Malek. 'Long-term Monitoring of the Sierra Nevada Snowpack Using Wireless Sensor Networks'. In: *IEEE Internet of Things Journal* (15th Sept. 2022). URL: https://hal.inria.fr/hal-01388391.

International peer-reviewed conferences

[16] J. Crnogorac, J. Crnogorac, E. Kocan and M. Vucinic. 'Experimental evaluation of distributed sniffer solution for wireless sensor networks'. In: IT 2022 - 26th International Conference on Information Technology. Zabljak, Montenegro: IEEE, 16th Feb. 2022, pp. 1–4. DOI: 10.1109/IT54280.2022.9743525. URL: https://hal.inria.fr/hal-03935652.

[17] M. Gutiérrez Gaitán, L. Almeida, T. Watteyne, P. M. d'Orey, P. M. Santos and D. Dujovne. 'Joint Scheduling, Routing and Gateway Designation in Real-Time TSCH Networks'. In: RTNS 2022 - 30th International Conference on Real-Time Networks and Systems. Paris, France, 7th June 2022. URL: https://hal.inria.fr/hal-03685331.

[18] A. Hidouri, H. Touati, M. Hadded, N. Hajlaoui and P. Muhlethaler. 'A Detection Mechanism for Cache Pollution Attack in Named Data Network Architecture'. In: *Advanced Information Networking and Applications - Proceedings of the 36th International Conference on Advanced Information Networking and Applications (AINA-2022)*. AINA 2022. - International Conference on Advanced Information Networking and Applications. Vol. 449. Lecture Notes in Networks and Systems. Sydney, Australia: Springer International Publishing, 31st Mar. 2022, pp. 435–446. DOI: 10.1007/978-3-030-99584-3_38. URL: https://hal.science/hal-03933549.

[19] T. Savić, S. Alvarado-Marin, F. Maksimovic and T. Watteyne. 'RRDV: Robots Rendez-Vous Detection Using Time-Synchronized Ultrasonic Sensors'. In: IEEE International Conference on Robotics, Automation and Artificial Intelligence (RAAI 2022). Singapore, Singapore, 9th Dec. 2022. URL: https://hal.inria.fr/hal-03936464.

Conferences without proceedings

[20] A. Hidouri, M. Hadded, H. Touati, N. Hajlaoui and P. Muhlethaler. 'Attacks, Detection Mechanisms and Their Limits in Named Data Networking (NDN)'. In: ICCSA 2023 - 23rd International Conference on Computational Science and Its Applications. Malaga, Spain, 3rd July 2022. URL: https://hal.science/hal-03933012.

[21] T. Yuan, F. Maksimovic, B. Wheeler, D. C. Burnett, L. Lee, T. Watteyne and K. S. J. Pister. 'A Temperature-Compensated BLE Beacon and 802.15.4-to-BLE Translator on a Crystal-Free Mote'. In: EuMW - European Microwave Week 2021. London, United Kingdom, 2nd Apr. 2022. URL: https://hal.inria.fr/hal-03538251.

Doctoral dissertations and habilitation theses

[22] I. Hmedoush. 'Connectionless Transmission in Wireless Networks (IoT)'. Sorbonne Université, 18th May 2022. URL: https://theses.hal.science/tel-03860953.

Reports & preprints

[23] I. Hmedoush, C. Adjih and P. Mühlethaler. *Deep Learning, Sensing-based IRSA (DS-IRSA): Learning a Sensing Protocol with Deep Reinforcement Learning*. RR-9479. INRIA-SACLAY, 2nd June 2022. URL: https://hal.inria.fr/hal-03744126.

Other scientific publications

[24] C. Thonier, T. Watteyne, F. Garde, T. Razafindralambo and B. Marcon. 'AIOT: the All-in-1 IoT Educational Tool You Need'. In: Future-IoT PhD school. Berlin, Germany, 29th Aug. 2022. URL: https://hal.inria.fr/hal-03820401.

12.3 Cited publications

[25] 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.

[26] 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.

[27] 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).

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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).

[36] 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).

[37] 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.

[38] B. Cottier and D. Pointcheval. 'Security Analysis of Improved EDHOC Protocol'. In: *International Symposium on Foundations & Practice of Security (FPS)*. 2022.

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

[40] 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.

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

[42] 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.

[43] 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).

[44] 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).

[45] F. Günther and M. I. T. Mukendi. *Careful with MAc-then-SIGn: A Computational Analysis of the EDHOC Lightweight Authenticated Key Exchange Protocol*. Tech. rep. 2022/1705. ETH Zurich, Trail of Bits, Dec. 2022.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

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

[51] 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.

[52] C. Jacomme, E. Klein, S. Kremer and M. Racouchot. 'A Comprehensive, Formal and Automated Analysis of the EDHOC Protocol'. In: *Usenix Security Symposium*. 2023.

[53] 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.

[54] 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.

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

[56] *Lightweight Authorization for EDHOC*. Tech. rep. draft-selander-lake-authz-00. Work-in-Progress. Internet Engineering Task Force (IETF), Oct. 2022.

[57] 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.

[58] 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.

[59] J. P. Mattsson, F. Palombini and M. Vučinić. *Comparison of CoAP Security Protocols*. Tech. rep. draft-ietf-lwig-security-protocol-comparison-06. Work-in-Progress. Internet Engineering Task Force (IETF), Dec. 2022.

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

[61] 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.

[62] 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.

[63] 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.

[64] 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.

[65] 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).

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

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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.

[73] 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.

[74] 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.

[75] 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.

[76] 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.

[77] 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.

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

[79] 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.

[80] 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.

[81] 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).

[82] 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.

[83] 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.