UMR IRISA

Activity Report 2025

Team INZU

Opportunistic Networking and Computing for Secure and Dependable Applications

D2 – Networks, Telecommunications and Services

Université de Rennes | rennes | INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES | cnrs | Inria | Inserm | CentraleSupélec | IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom | Université Bretagne Sud ubs

1 Team composition

Researchers and faculty

Yves Mahéo, Assistant professor (HDR), Univ. Bretagne Sud, head of the team
Frédéric Guidec, Professor, Univ. Bretagne Sud
Mawloud Omar, Professor, Univ. Bretagne Sud
Siham Bouchelaghem, Assistant professor, Univ. Bretagne Sud
Pascale Launay, Assistant professor, Univ. Bretagne Sud
Nicolas Le Sommer, Assistant professor, Univ. Bretagne Sud
Edward Staddon, Assistant professor, Univ. Bretagne Sud
Lionel Touseau, Assistant professor, Académie Militaire de Saint-Cyr Coëtquidan

Associate members

Bournane Abbache, École Nationale Supérieure d'Ingénieurs de Bretagne-Sud

Research engineers, technical staff

Abderrazaq Lahoua, Engineer, Project RECSANet (AID RAPID)

PhD students

Huy Dat Nguyen
Andrea Ndreveloarisoa
Madické Diadji Mbodj
Alexandre Dohin, since Jan. 2025
Guillaume Bouzige, since Oct. 2025

Administrative assistants

Anne Le Tohic, Clotilde Bidon

2 Overall objectives

2.1 Overview

The research activity of team INZU aims at supporting communication and service provision in mobile networks that operate by exploiting transient radio contacts between mobile devices. Such networks are usually referred to as opportunistic networks in the literature [PPC06], although the terms delay-tolerant and disruption-tolerant networks (DTNs) are sometimes used instead.

In an opportunistic network, the topology of the network can be modeled as a dynamic graph. This graph is usually not connected, as a consequence of the sparse distribution of mobile nodes, and because radio transmissions between these nodes can only be performed at short range.

In such conditions, mobility can be considered as an advantage as it makes it possible for messages to propagate network-wide, using mobile nodes as carriers that can move between remote fragments of the network. Each mobile node can thus store each message for a while, carry messages while moving around, and use any radio contact as an opportunity to forward messages to another node. This store, carry and forward principle is the foundation of opportunistic networking.

Part of our activity in team INZU consists in studying routing protocols for opportunistic networks, namely by implementing these protocols in communication middleware so they can be tested in real conditions. We also investigate how distributed applications can be designed so as to perform satisfactorily in such networks. Indeed, designing distributed applications that require network-wide communication and coordination in an opportunistic network is quite a challenge, when communication and coordination depend on unpredicted pairwise contacts between neighbor nodes. The term Opportunistic Computing has been introduced in the literature in order to refer to a new computing paradigm that relies exclusively on such pairwise contacts [CGMP10]. Team INZU strives to contribute to the development of this computing paradigm by designing methods, models, and middleware tools that make it easier for programmers to tackle the challenges presented by opportunistic networks.

One of the challenges pertaining to opportunistic networking as well as to opportunistic computing is security. Indeed the security mechanisms developed for traditional networks are hardly applicable in the context of opportunistic networking. Team INZU has started to investigate this field of research, with the objective to propose practical solutions for selected application domains (IoT, tactic field, V2V).

[PPC06] L. PELUSI, A. PASSARELLA, M. CONTI, "Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad Hoc Networks", *IEEE Communications Magazine 44*, 11, 2006, p. 134–141.

[CGMP10] M. CONTI, S. GIORDANO, M. MAY, A. PASSARELLA, "From Opportunistic Networks to Opportunistic Computing", *IEEE Communications Magazine 48*, 9, 2010, p. 126–139.

2.2 Scientific foundations

2.2.1 Opportunistic Networking

In the early 2000s the IETF initiated the DTN Research Group, whose charter was to define an architecture for both Delay and Disruption Tolerant Networks. This group was concluded in April 2016. In the meantime it has defined the architecture requested by the IETF (in two versions), together with a bundling protocol (BP) specification, and several profile documents that contain descriptions of convergence layers intended to fit the needs of specialized networking environments (e.g., space, water, sensor networks).

The DTN2 architecture and the associated bundle protocol (BP) are often believed to constitute an all-purpose solution for any kind of challenged network lacking end-to-end connectivity. Yet several authors have observed that although the Bundle Protocol is perfectly suited for inter-planetary networking, other kinds of networks (e.g., vehicular networks, pocket-switched networks, and mobile wireless sensor networks) may as well rely on alternative, lighter solutions [WHFE09,Voy12]. In [MCM+14] Mota et al. suggest that the term delay-tolerant network should be used only for networks that strictly adhere to the DTN2 architecture, and they propose that the term opportunistic network be used for any kind of challenged network that exploits transient radio contacts between mobile nodes

A plethora of routing protocol have been proposed for more than a decade [DKAGD21] but very few of them are implemented and used in effective opportunistic networks. It is now admitted that the research effort should also target the deployment of large-scale opportunistic networks [TKD+17], and scalability issues. The work of team INZU is conducted in this perspective, by focussing on the emulation of large opportunistic networks and the development of practical solutions for deploying opportunistic networks.

2.2.2 Opportunistic Computing

Opportunistic computing is a paradigm that builds on the results of several research areas (including autonomic computing and social networking), moving forward from simple communication to develop a framework to enable collaborative computing tasks in networking environments where long disconnections and network partitions are the rule [CGMP10].

[WHFE09] L. WOOD, P. HOLLIDAY, D. FLOREANI, W. M. EDDY, "Sharing the Dream: the Consensual Hallucination Offered by the Bundle Protocol", *in : International Congress on Ultra Modern Telecommunication (ICUMT'09)*, IEEE, p. 1–2, 2009.

[Voy12] A. G. VOYIATZIS, "A Survey of Delay- and Disruption-Tolerant Networking Applications", *Journal of Internet Engineering 5*, 1, 2012, p. 331–344.

[MCM+14] V. F. S. MOTA, F. D. CUNHA, D. F. MACEDO, J. M. S. NOGUEIRA, A. A. F. LOUREIRO, "Protocols, Mobility Models and Tools in Opportunistic Networks: A Survey", *Computer Communications 48*, 2014, p. 5–19.

[DKAGD21] R. DALAL, M. KHARI, J. P. ANZOLA, V. GARCÍA-DÍAZ, "Proliferation of Opportunistic Routing: A Systematic Review", *IEEE Access*, 2021.

[TKD+17] S. TRIFUNOVIC, S. T. KOUYOUMDJIEVA, B. DISTL, L. PAJEVIC, G. KARLSSON, B. PLATTNER, "A Decade of Research in Opportunistic Networks: Challenges, Relevance, and Future Directions", *IEEE Communications Magazine 55*, 1, 2017, p. 168–173.

[CGMP10] M. CONTI, S. GIORDANO, M. MAY, A. PASSARELLA, "From Opportunistic Networks to Opportunistic Computing", *IEEE Communications Magazine 48*, 9, 2010, p. 126–139.

The service-oriented paradigm has been the first to be well-suited for opportunistic networks as it fosters decoupling between applicative entities, and is able to accommodate intermittent connectivity constraints, and building applications by combining software services is now well mastered and supported by many techniques and tools, among which the most popular Web Services. In opportunistic networks, the absence of network-wide end-to-end connectivity, and the transmissions delays induced by the store, carry, and forward model require that specific solutions be devised in order to support both service discovery and service invocation.

Beside service-oriented computing, other computing paradigms have also long proved useful for designing distributed applications. Group communication, publish-subscribe systems, message queues, tuple spaces, or conflict-free replicated datatypes are thus abstractions or systems for which efficient implementations are available in software development kits. Yet most of these implementations have been realized for traditional, connected environments. They cannot operate satisfactorily in partially or intermittently connected environments, and must be completely revised in order to tolerate network partitions, transmission disruptions, or long transmission delays.

2.2.3 Security in Opportunistic Environments

Security in opportunistic environments raises a set of challenges that significantly differ from those encountered in traditional systems. They are characterized by intermittent connectivity, dynamic and unpredictable topologies, decentralized control, and interactions between mobile and resource-constrained devices. These properties invalidate many assumptions commonly made in classical security architectures, such as the availability of permanent communication paths, centralized trust authorities, or global system knowledge.

A key difficulty arises from the uncertain and evolving nature of system behavior. Connectivity disruptions, transient faults, mobility-induced variability, and delayed observations make it difficult to clearly separate normal operation from abnormal or malicious behavior. As a result, security mechanisms must operate in contexts where information is partial, outdated, or noisy, and where faults, attacks, or misconfigurations may have delayed or cascading effects across system components.

Another category of challenges concerns the monitoring and detection of abnormal behaviors in highly dynamic environments. Many existing approaches rely on centralized supervision, continuous data collection, or predefined models of expected behavior, which are poorly adapted to intermittently connected systems. Opportunistic environments instead require decentralized and adaptive mechanisms that can cope with sporadic observations, heterogeneous data sources, and strict limitations in computation, energy, and communication resources.

The protection of data and services also raises specific issues. Opportunistic communication relies on the store-carry-and-forward paradigm, in which messages may be temporarily stored or relayed by intermediate nodes that cannot be assumed to be trusted. Ensuring confidentiality, integrity, and authenticity under these conditions requires limiting the trust placed in the communication infrastructure itself, while maintaining compatibility with long delays, disconnections, and constrained devices. This includes addressing access control in the absence of continuous coordination or online verification. In the absence of centralized infrastructures or global consensus mechanisms, trust relationships often rely on local interactions and contextual information. Designing mechanisms that support authentication, traceability, and

non-repudiation, while tolerating mobility, disconnections, and adversarial behavior, is a key challenge for systems operating in such environments.

2.3 Application domains

The research work carried out in team INZU is focused on the design and the implementation of middleware support for applications targeting challenged networking environments. We are particularly interested in providing support for mobility and continuity of service, even in the absence of any stable communication infrastructure. This applies to multiple environments where adaptive and cooperative applications are required, but where cost or technical constraints preclude the deployment of stable computing and communication resources. Possible application domains are:

- Collaborative computing in crisis operation fields (e.g., military operations, disaster relief situations);
- Sensor and actuator networking, as part of the Internet of Things (e.g., environment monitoring, crowd sensing, robot/drone control);
- Automotive computing (e.g., vehicle-to-vehicle and vehicle-to-roadside communication);
- Home automation (e.g., smart home applications);
- Nomadic computing (e.g., coordination and data sharing in rural or developing areas);
- Crowd-sensing (e.g., distributed content production and sharing);
- Personal communication systems (e.g., group communication, social interactions);
- Mobile health (e.g., ambulatory patient monitoring).

Most of the middleware systems developed in team INZU over the recent years can be considered as enablers for the above-mentioned application domains. Please refer to the team's Web site [1] for further information about these systems.

3 Scientific achievements

3.1 Conflict-free Replicated Data Types for opportunistic networks

Participants: Frédéric Guidec, Yves Mahéo.

Conflict-Free Replicated Data Types (CRDTs) are distributed data types that support optimistic replication: replicas can be updated locally, and updates propagate asynchronously among replicas, so consistency is eventually obtained. This ability to tolerate asynchronous communication makes them ideal candidates to serve as software building blocks in opportunistic networks (OppNets).

[1] https://www-inzu.irisa.fr/software

Team INZU has already developed several demonstrators, and run several small-scale experiments based on these demonstrators, in order to verify that distributed applications based on CRDTs can perform effectively in OppNets, despite the very low connectivity observed in such networks [r3, r2].

Whether CRDT-based applications can also perform effectively in large OppNets involving possibly hundreds or thousands of mobile nodes still needs to be demonstrated. In a large OppNet, there is no reason to presume that all the nodes should necessarily run the same distributed application, and maintain replicas of the same CRDT. The lower the density of nodes carrying replicas of a particular CRDT, the lower the chance for these nodes to get in radio contact, and thus to synchronize their replicas.

Team Inzu has started investigating the idea of enrolling nodes as relays to assist in the synchronization of replicas of state-based CRDTs. A Relay-Based Synchronization System (RBSS) has been designed, which implements specific synchronization protocols that have been designed so as to be frugal regarding the amount of data transferred between peer nodes, as well as the amount of data stored on each relay. Besides, these protocols do not require that the relays have any knowledge about the states they are carrying. These states can therefore be encrypted and signed by the issuer replicas, and the relays can neither read nor alter the information they are carrying. Simulations conducted with different scenarios confirm that using relays can significantly improve the synchronization of CRDT replicas in an OppNet.

3.2 Opportunistic Networking in Low-Power Wide Area Network

Participants: Nicolas Le Sommer, Lionel Touseau, Huy Dat Nguyen, Edward Staddon, Yves Mahéo, Guillaume Bouzige.

Team INZU investigates the possibility of using LoRa, which is one of the main technology for Low-Power Wide Area Networks (LPWANs), in the design of distributed systems dedicated to the observation of the environment or to tactical situations, and relying on opportunistic networking techniques. LoRa includes interesting features such as symmetric modulation for uplink and downlink, which allows nodes to establish device-to-device (D2D), and a potential radio range of several kilometers. However, the standard MAC layer associated with the LoRa physical layer (i.e., LoRaWAN) operates a gateway-centric star topology network, in which nodes and gateways must be in the radio range of each other to communicate. We proposed an alternative solution, called LoRaOpp [r4], that supports opportunistic multi-hop communications in LoRa-based networks. LoRaOpp allows (mobile) nodes to communicate together at several hops, and also allows nodes to send data to (mobile) gateways, also at several hops. LoRaOpp is designed so as to be configured dynamically in order to change for example the power transmission, the spreading factor, etc. With LoRaOpp, nodes and gateways can temporarily store messages in a local cache, and to retrieve them after a deep sleep phase in order to restransmit them when an opportunity appears. LoRaOpp is designed to run on resource-constrained devices (e.g. ESP32 or STM32 micro-controllers).

In the context of IoT and LPWANs, we also studied the dynamic firmware updating of devices following an incremental and modular approach, considering both LoRaWAN networks and opportunistic communications over the LoRa physical layer using LoRaOpp (PhD of H.D. Nguyen). Such a modular approach aims at being able to perform partial updates in-

stead of replacing the whole firmware, thus allowing to reduce the network load and the power consumption. Moreover, in our approach, parts of the firmware can be replaced and loaded dynamically using the DROOPY dynamic runtime [12], thus avoiding to reboot devices when it is not needed. The firmware update process has been extended to perform both a multicast delivery of modules that must be updated, and a multi-hop transmission of these modules. Both multicast opportunistic delivery and multi-hop opportunistic delivery of modules have proven their effectiveness, for example by enabling 20 times faster updates in multi-hop process compared to standard LoRaWAN solution, and with much better energy efficiency.

Recently, we worked on extending LoRaOpp in the context of project RECSANet (see section 5.1.1), which mainly aims at studying and developing a self-adapting, resilient and energy efficient multi-technology communication middleware for resource-constrained devices with a focus on LoRa radio technology. Latest advances of project RECSANet made us reconsider LoRaOpp protocol. LoRaOpp was originally designed to support sparse communications like in LoRaWAN standard. Yet, LoRa technology provides some promising features that could address other use cases such as the deployment of emergency networks for disaster relief or to support Search And Rescue operations in challenging environments (PhD of G. Bouzige). By leveraging LoRa as the physical layer for long-range opportunistic communication, team coordination could be achieved, for both civilian or military purposes, where and when infrastructure networks are not available. LoRaOpp is consequently being redesigned as a multi-technology protocol tailored to the demanding requirements of LoRa constrainted technology, in order to support these more intensive-paced communications (e.g., text messaging, location sharing, ...) on channels with limited throughput.

3.3 Efficient Data Delivery in Delay-Tolerant Networks

Participants: Mawloud Omar.

Traditional routing protocols often struggle to handle intermittent connectivity, highlighting the need for a predictive and adaptive strategy in Delay-Tolerant Networks (DTNs). In this context, we proposed a Predictive Road Optimization Strategy (PROS) [2] that introduces a connectivity-aware routing mechanism selecting paths based on predicted link availability and connectivity duration. Unlike conventional DTN protocols, PROS estimates future connection and disconnection periods between nodes to determine the optimal transmission time. By dynamically evaluating link states, nodes can decide whether to forward or temporarily buffer messages, ensuring that each transmission occurs over a stable connection. By using predictive tables that record connectivity durations, disconnection times, and transmission intervals, PROS computes the shortest-time path for each message. This time-based optimization reduces overall delivery latency and limits redundant transmissions.

The simulation results show that PROS significantly reduces the average delivery time, energy consumption, and overhead ratio compared to established DTN protocols such as Epidemic, First Contact, MaxProp, and P-epidemic. PROS demonstrates strong performance in resource management, energy efficiency, and scalability across varying network densities, node speeds, and buffer sizes.

3.4 Intermittent Failure Dependencies in Dynamic Systems

Participants: Mawloud Omar, Siham Bouchelaghem, Bournane Abbache.

Our research in this area has primarily focused on the optimization of predictive maintenance and the anticipation of system failures. The main objective has been to improve system reliability, reduce unplanned downtime, and enhance operational efficiency by developing intelligent methods for early fault detection, diagnosis, and decision support.

In [4], we proposed a deep learning-based anomaly detection framework for autonomous vehicle systems. This approach leverages sensor fusion and multi-channel signal analysis to identify early signs of malfunction within the vehicle's control and communication networks. We experimentally validated the proposed model on the MT-CAN-LIN-BSI platform through a comprehensive testbed replicating the communication architecture of an autonomous vehicle. The results demonstrated the ability of our model to detect subtle deviations in system behavior, achieving high precision in anomaly identification while maintaining low false-positive rates. Later on, in [10], we introduced a fault graph-based modeling approach. By representing system components and their inter-dependencies, we were able to analyze the structural vulnerability of the system. Using the concept of dominating sets in graph theory, we developed a novel algorithm to identify the most critical components whose failures would have the greatest impact on overall system reliability. Finally, in [3], we extended our proposal to the railway domain by modeling the functional dependencies of the ERTMS/ETCS (European Rail Traffic Management System/European Train Control System) using a temporal fault graph. This model captures not only structural dependencies but also the temporal evolution of failures, enabling a dynamic understanding of fault propagation over time. By formulating and solving optimization problems related to graph traversal and dependency resolution, we demonstrated that our approach could effectively retrace error propagation paths, providing actionable insights to maintenance teams and enhancing the reliability of safety-critical railway operations.

3.5 Cybersecurity and Safety in Cyber-Physical Systems

Participants: Mawloud Omar, Siham Bouchelaghem, Alexandre Dohin.

Artificial Intelligence (AI) plays a central role in reinforcing both cybersecurity and safety in cyber-physical systems, where cyber threats and physical failures are tightly intertwined.

Cyberattacks targeting cyber-physical systems infrastructures may directly propagate to the physical layer, leading to service disruptions, unsafe operating conditions, or even catastrophic failures. To address this challenge, we proposed AI-driven cybersecurity mechanisms capable of detecting malicious behaviors at an early stage, before they impact system safety. In smart grids, we proposed, in [9], a deep learning-based energy auditing approach using convolutional neural networks to distinguish cyberattacks from natural faults and normal operations solely from electrical measurements, thereby enabling network-agnostic and resilient threat detection. In the context of IoT-based cyber-physical systems, we proposed, in [7], a lightweight anomaly detection framework based on Gaussian Mixture Models to identify Mirai botnet attacks while meeting the strict latency and computational constraints of resource-limited devices.

Building on this cybersecurity foundation, AI also serves as a key enabler for enhancing

the safety and resilience of cyber-physical system operating under uncertainty and dynamic conditions. In autonomous vehicular systems, failures may originate not only from malicious actions but also from sensor degradation, noise, or inconsistent data, all of which can compromise decision-making and endanger safety. To mitigate these risks, we proposed, in [5], a machine learning-based failure detection approach that accounts for sensing uncertainty by filtering unreliable data and quantifying anomaly levels, thus supporting predictive maintenance and improving system robustness. Furthermore, extending anomaly detection to the driving control level, we proposed, in [8], an AI-empowered, safety-centric approach that integrates deep learning with multimodal sensor fusion to identify hazardous driving behaviors in real time.

3.6 Fine-Grained Security for Fog-IoT Architectures

Participants: Mawloud Omar.

Traditional CP-ABE (Ciphertext-Policy Attribute-Based Encryption) schemes offer expressive and fine-grained access control but suffer from high computational costs, making them impractical for lightweight IoT and fog nodes. To overcome this, we proposed MABE (Meta-Attributes Based Encryption) [1]. MABE introduces a meta-attribute concept, where correlated attributes that frequently appear together are clustered into a single meta-attribute through vector space modeling and k-means classification. This reduces the size of access policies while maintaining their semantics and security guarantees. MABE integrates a primitive, which transforms the original access tree into a minimized version by replacing attribute subsets with their corresponding meta-attributes. This reduction leads to substantial performance improvements without relying on proxy re-encryption or outsourced decryption, thus avoiding additional security risks. Experimental evaluation within a fog-based monitoring system demonstrates that MABE reduces encryption time by up to 75% and decryption time by around 35% compared to traditional CP-ABE. Furthermore, it achieves significant reductions in ciphertext size and communication overhead while maintaining resistance to collusion attacks and scalability across multi-layer fog environments.

3.7 Cybersecurity for Trust and Traceability in Community-Based Systems

Participants: Andrea Ndreveloarisoa, Frédéric Guidec, Mawloud Omar.

In recent years, many digital systems aimed at supporting exchanges of goods and services have relied on centralized platforms or blockchain-based infrastructures to establish trust and traceability. While effective at large scale, these approaches often prove excessive for local economies and community-driven contexts, where exchanges are limited, trust relationships are situated, and sustainability is a key concern. In this context, we adressed the question of how to digitally support such local exchanges without introducing unnecessary technical, environmental, or organizational overhead.

The central problem that we investigated in [11] is the reliable tracking of the custody and transfer history of physical objects shared or exchanged within a community, in the absence of a trusted central authority. Existing solutions frequently assume constant connectivity and

global consensus, which are misaligned with local use cases. To address this, we proposed a lightweight, decentralized approach based on peer-to-peer interactions. Object transfers are recorded through locally stored, chained records, each signed by the previous and new custodians, ensuring integrity, authenticity, and non-repudiation. Trust is maintained through mutual verification and digital identities rather than through blockchain mining or third-party intermediaries. We proposed the underlying data structures and the interaction workflows, illustrating how object histories can be verified and updated locally.

4 Software development

4.1 DEMO-OPPNET

Participants: Yves Mahéo, Frédéric Guidec, Pascale Launay.

DEMO-OPPNET is a demonstrator running on Linux that allows a non-specialist user to create an opportunictic network and test some simple opportunistic applications. DEMO-OPPNET uses Wi-Fi (in ad hoc mode) for device-to-device transmissions. So it can be installed on any PC running Linux that is equipped with a Wi-Fi interface. Moreover, it is possible to externalize the user application on a smartphone or a tablet, provided that a Bluetooth interface is available. The proposed applications are webapps (running in a web browser): Quillop, a collaborative text editor; Cartopp, a collaborative map showing simple points of interest; Webopp, a text and file exchange system based on content-based publication-subscription. The two latter applications are based on the exploitation of CRDTs. In addition, DEMO-OPPNET allows the user to connect a usual mailer in order to take benefit from an opportunistic mailing system. An administration web console is also available, namely in order to configure the ad hoc network.

DEMO-OPPNET relies on the DoDWAN middleware plateform[2], developed by team INZU, to ensure communication in the opportunistic network. DoDWAN provides a network API (for publish/subscribe applications as well as CRDT-based applications) that is used by the applications proposed in the demo.

DEMO-OPPNET is distributed under the GNU General Public License (GPL)[3].

4.2 RECSANet

Participants: Nicolas Le Sommer, Edward Staddon, Abderrazaq Lahoua, Lionel Touseau.

RECSANet is a middleware platform targetting micro-controlers that aims at building resilient and self adaptive networks to support the execution of decentralized and delay-tolerant applications. RECSANet is an on-going joint development effort resulting from the collaboration of INZU with the IRISA/GRANIT team and CG-Wireless company. The middleware currently supports the STM32-based hardware architecture designed by CG-Wireless and implements the multi-technology opportunistic networking protocol described in Section 3.2. The REC-

[2]https://www-inzu.irisa.fr/dodwan
[3]https://www-inzu.irisa.fr/demo-oppnet

SANet software platform still requires in-depth testing, as well as an evaluation by the DGA sponsor, before being publicly released.

5 Contracts and collaborations

5.1 National Initiatives

5.1.1 Project RECSANet

Participants: Lionel Touseau, Nicolas Le Sommer, Edward Staddon, Abderrazaq Lahoua.

- Project type: AID RAPID
- Dates: 2023–2026
- Partners: CGWireless, IRISA/GRANIT

Project RECSANet addresses both military and civilian concerns: from battlefield digitalization to forest firefighting. It proposes to study and define a resilient hardware and software support for the creation of infrastructure-less and sovereign networks. Such networks should be able to tolerate the loss of communicating devices. RECSANet networks will have to support distributed applications for text-messaging, location sharing, and sensor data collection. The data considered in RECSANet can be provided by user terminals as well as fixed or mobile sensors that communicate through a self-adaptable opportunistic protocol, able to operate despite connectivity disruptions. The protocol will rely on a multi-technology and multi-band hardware layer built with low-cost off-the-shelf components.

In this context, the contribution of team INZU will consist in designing and implementing a multi-technology opportunistic protocol as well as a middleware (see 4.2) to support RECSANet distributed applications. The protocol will emphasize the use of LoRa as a radio technology to support opportunistic communications, particularly on the 2.4 GHz band. One of the challenges of this project will be to propose a lightweight solution that can run under heavy constraints, that is to say on nodes with limited energy, limited computing power and that must accomodate with LoRa low data rates.

6 Dissemination

6.1 Promoting scientific activities

6.1.1 Scientific Events Organization

- M. Omar organized, in partnership with UQO, a Winter School on the safety and security of cyber-physical systems from February 3 to February 13, 2025. This event offered an immersive academic experience alongside through an intensive ten-day program, including hands-on scenario-based exercises, applications of artificial intelligence to transport system safety, and strategies for protecting critical cyber-physical infrastructures.

6.1.2 Journal

Reviewer - Reviewing Activities

- N. Le Sommer: reviewer for Applied System Innovation (MDPI), Sensors (MDPI), Drones (MDPI), Future Internet (MDPI)
- S. Bouchelaghem: reviewer for IEEE Transactions on Intelligent Transportation Systems (T-ITS).
- M. Omar serves as an Associate Editor for the journal AI and Autonomous Systems. He also serves as a reviewer for many journals (IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Vehicular Technology, JNCA, etc.).

6.1.3 Research Administration

- F. Guidec served as the local representative of IRISA at Université Bretagne Sud (2021-2025).
- F. Guidec served as a member of the steering committee of the doctoral school (ED) MathSTIC - Bretagne Océane (2021-2025).
- L. Touseau serves as the representative of the team MIRIAD from the CReC Saint-Cyr, composed of 12 researchers in computer science and mathematics.

6.2 Teaching, supervision

6.2.1 Teaching

- F. Guidec
  M1: Network administration, 52h
  M2: Wireless networking technologies, 52h
  M2: Innovative systems and networks, 15h
  M2: Internet of Things, 26h

- Y. Mahéo
  M1: Introduction to Distributed Systems, 26h
  M1: Network administration, 52h
  M2: Distributed middleware, 29h
  M2: Innovative systems and networks, 26h
  M2: Personal Project, 48h

- P. Launay
  M1: Introduction to Distributed Systems, 21h
  M1: Advanced Object Programming, 39h
  M2: Innovative systems and networks, 8h

- N. Le Sommer
  M1: research introduction project, 8h
  M2: Development of secure mobile applications, 42h

- L. Touseau
  ESM2 (M1): Project supervision, 80h, AMSCC
  ESM2 (M1): Databases, 24h, AMSCC
  Mastère Cyber: Opportunistic networks, 2h, AMSCC

- M. Omar
  ISEN - Brest (M2): Cloud Security, 30h
  ISEN - Brest (M2): AI and Cyberecurity, 22h
  UFRSSI (M1): Project supervision, 40h
  ENSIBS (M2): Project supervision, 20h

- S. Bouchelaghem
  ENSIBS (M1): Human Factors Seminar, 20h

- B. Abbache
  ENSIBS (M2): Android Security, 110h
  ENSIBS (M1): Cybersecurity Simulation Exercise, 10h
  ENSIBS (M1): Human Factors Seminar, 20h
  ENSIBS (M1): Project supervision, 10h
  ENSIBS (M2): Project supervision, 20h

6.2.2 Supervision

- Huy Dat Nguyen: "Opportunistic protocol for distributed update of an IoT-based environmental observation system relying on participatory science", PhD in progress at Université Bretagne Sud, supervised by Yves Mahéo (IRISA, INZU), Nicolas Le Sommer (IRISA, INZU) and Lionel Touseau (IRISA, INZU).

- Roumaissa Bekkouche: "Securing 5G Networks", PhD in progress at Université Gustave Eiffel, supervised by R. Langar (UGE) and M. Omar (IRISA, INZU).

- Alexandre Dohin: "Cyber Resilience and Predictive Maintenance in Supply Chains: Tackling Disruptions in Weak Institutional Environments", PhD in progress at Université Bretagne Sud, supervised by M. Omar (IRISA, INZU), K. Zkik (RBS), and A. Akilal (ENSIBS).

- Madické Diadji Mbodj: "Anomaly Detection with Uncertainty Management on Confidential Network Data: Application to Autonomous Transport Systems", PhD in progress at Université Bretagne Sud, supervised by M. Omar (IRISA, INZU), S. Bouchelaghem (IRISA, INZU), R. Yaich (SystemX), and A. Bekakria (SystemX).

- Andrea Ndreveloarisoa: "Security of a local exchange trading system based on device-to-device communication", PhD in progress at Université Bretagne Sud, supervised by

F. Guidec (IRISA, INZU) and M. Omar (IRISA, INZU).

- Guillaume Bouzige: "Auto-organized communication network for post-disaster citizen mutual aid", PhD in progress at Université Bretagne Sud, supervised by Y. Mahéo (IRISA, INZU) and Nicolas Le Sommer (IRISA, INZU).

6.2.3 Juries

- M. Omar: member of the PhD jury (reviewer) of Mohammad Beyrouti (University of Technology of Compiegne), "Risk identification and secure management for IoT systems", 2025/04/28.

7 Bibliography

Major publications by the team in recent years

[r1] A. BELHADJ, K. AKILAL, S. BOUCHELAGHEM, M. OMAR, S. AISSANI, "Next-cell prediction with LSTM based on vehicle mobility for 5G mc-IoT slices", *Telecommunication Systems 87(3)*, June 2024, p. 809–833.

[r2] F. GUIDEC, Y. MAHÉO, C. NOÛS, "CRDT-based Collaborative Editing in OppNets: a Practical Experiment", *in : 17th Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (Ubicomm 2023)*, IARIA, p. 13–21, Porto, Portugal, September 2023.

[r3] F. GUIDEC, Y. MAHÉO, C. NOÛS, "Supporting conflict-free replicated data types in opportunistic networks", *Peer-to-Peer Networking and Applications 16*, January 2023, p. 395–419.

[r4] N. LE SOMMER, L. TOUSEAU, "LoRaOpp: A Protocol for Opportunistic Networking and Computing in LoRa Networks", *in : 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2022)*, IEEE, p. 308–313, Thessaloniki, Greece, 2022.

[r5] D. ZAMOUCHE, S. AISSANI, M. OMAR, M. MOHAMMEDI, "Highly efficient approach for discordant BSMs detection in connected vehicles environment", *Wireless Networks 29*, 1, January 2023, p. 189–207.

Articles in referred journals and book chapters

[1] A. KRINAH, Y. CHALLAL, M. OMAR, O. NOUALI, "Enhancing fine-grained access control in fog-based e-health applications", *Cluster Computing 28(9)*, June 2025, p. 605.

[2] D. TOUAZI, M. MOHAMMEDI, M. OMAR, A. BOUABDALLAH, "Predictive Road Optimization Strategy for Efficient Message Delivery in Delay-Tolerant Networks", *Wireless Personel Communication 144(3-4)*, June 2025, p. 337–375.

Publications in Conferences and Workshops

[3] B. ABBACHE, M. OMAR, S. BOUCHELAGHEM, "Graph Optimization for Failure Propagation in Intermittent Systems-of Systems: Railway Use Case", *in : 20th Annual System of Systems Engineering Conference (SOSE)*, p. 1–6, 2025.

[4] B. ABBACHE, M. OMAR, S. BOUCHELAGHEM, "Toward Optimized Predictive Maintenance for Vehicle Systems: Deep Learning-Based Anomaly Detection Using CAN Traffic", *in : 14th International Conference on Pattern Recognition Applications and Methods (ICPRAM)*, p. 418–425, 2025.

[5] S. AISSANI, M. OMAR, K. HAMOUID, "Failure Detection Under Sensing Uncertainty in Vehicular Systems", *in : 4th International Conference on Computer Technologies (ICCTech)*, p. 60–65, 2025.

[6] A. BELHADJ, M. OMAR, S. AISSANI, "Predictive Maintenance for QoS in 5G Communication: A State of the Art Review", *in : 10th International Conference on Information and Network Technologies (ICINT)*, 2025.

[7] B. BRAHIM, K. HAMOUID, M. OMAR, M. RAHOUTI, H. DRID, "Towards a Lightweight and Efficient Gaussian Mixture Model for Detecting Mirai Botnet Attacks in IoT Environments", *in : 11th International Conference on Control, Decision and Information Technologies (CoDIT)*, p. 101–106, 2025.

[8] T. CHENACHE, K. ZIZI, S. BOUCHELAGHEM, S. AISSANI, M. OMAR, "Driving Control in Autonomous Vehicles: An AI-Empowered Safety-Centric Approach", *in : 20th Annual System of Systems Engineering Conference (SOSE)*, p. 1–6, 2025.

[9] A. DOHIN, K. ZKIK, M. OMAR, A. AKILAL, "Deep Learning-Driven Energy Auditing for Smart Grid Cyberattack Detection", *in : 18th International Symposium on Foundations and Practice of Security (FPS)*, 2025.

[10] M. LALOU, M. OMAR, K. HAMOUID, "Optimizing Predictive Maintenance in Vehicular Systems via Positive Influence Dominating Sets", *in : 17th International Conference on Knowledge and Smart Technology (KST)*, p. 393–398, 2025.

[11] A. F. NDREVELOARISOA, F. GUIDEC, M. OMAR, "A Secure Lightweight System Based on Device-to-device Communication for Objects Sharing in Local Communities", *in : 18th International Symposium on Foundations and Practice of Security (FPS)*, 2025.

[12] H. D. NGUYEN, N. LE SOMMER, Y. MAHÉO, L. TOUSEAU, "Droopy: A Dynamic Runtime Platform for Micro-Controller Units supporting Partial and Incremental Updates of Modularized Firmware", *in : 3rd International Workshop on Long and Short Range Wireless Technologies Applied to IoT for Networks of Tomorrow (DCOSS-IoT/LS-NoT)*, IEEE, p. 866–873, Lucca, Italy, 2025.

[13] H. D. NGUYEN, N. LE SOMMER, Y. MAHÉO, "LoRaWAN-Based Multicast and Disruption-Tolerant Protocols for Firmware Update Over-the-Air", *in : 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, p. 251–255, 2025.