Activity Report 2024

Team INZU

Opportunistic computing and networking for secure and dependable applications

D2 – NETWORKS, TELECOMMUNICATION AND SERVICES

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, Univ. Bretagne Sud, since Sep. 2024
Pascale Launay, Assistant professor, Univ. Bretagne Sud
Nicolas Le Sommer, Assistant professor, Univ. Bretagne Sud
Edward Staddon, Univ. Bretagne Sud, since Sep. 2024
Lionel Touseau, Assistant professor, Académie Militaire de Saint-Cyr Coëtquidan

Postdoctoral Fellows

Edward Staddon, Project RECSANet (AID RAPID), until Aug. 2024

Research engineers, technical staff

Abderrazaq Lahoua, Engineer, Project RECSANet (AID RAPID), since Sep. 2024

PhD students

Huy Dat Nguyen
Andrea Ndreveloarisoa, since Oct. 2024
Madické Diadji Mbodj, since Nov. 2024

Administrative assistants

Anne Le Tohic, Martine Milcent.

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 the security. Indeed the security mechanisms developed for traditional networks, that most often assume a permanent access to a trust authority, 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 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.

2.3 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.

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

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).

Team INZU has initiated the development of several CRDT-based demonstrators in order to show that distributed applications based on CRDTs can perform effectively in OppNets, despite the very low connectivity observed in such networks. QuillOpp and CartOpp are two CRDT-based collaborative editors we developed. They can be used by several users to edit and share text and augmented maps respectively.

Experiments based on QuillOpp have been reported in [r3]. This paper confirms that collaborative editing can be achieved in an OppNet, using a CRDT-based application for document editing among a small group of contributors. However, in a larger OppNet, involving possibly hundreds or thousands of nodes, there is no reason to presume that all the nodes should necessarily run the same distributed application, hosting replicas of the same CRDT. In a large OppNet it is actually likely that, for each CRDT instance, only a fraction of the network's population would be interested in this particular CRDT, and would thus host a replica of this 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.

Based on these observations, 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 protocols for replica-replica synchronization, replica-relay synchronization, and relay-relay synchronization. These protocols have been designed so as to minimize the amount of data transferred during each synchronization transaction, as well as the amount of data stored on a relay. Besides, the states exchanged during synchronizations can be encrypted and signed by the issuer replicas, so the relays can neither read nor modify these states, although they are helping in their propagation. Experiments 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.

Team INZU investigates the possibility of using LoRa (one of the main technology for Low-Power Wide Area Networks (LPWANs) in the design of a distributed system dedicated to the observation of the environment, and relying on opportunisting 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 network in a simple star topology, in which nodes and gateways must be in the radio range of each other to communicate. We proposed an alternative solution, called LoRaOpp [r5], 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 a opportunity appears. LoRaOpp is designed to run resource-constrained devices (e.g. ESP32 or STM32 mico-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 instead 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, thus avoiding to reboot devices when it is not needed.

Recently, we worked on the usage of 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. More generally, LoRa could provide a long-range communication support for team coordination, for both civilian or military purposes. LoRaOpp is consequently being redesigned in order to support these more intensive-paced communications on channels with limited throughput.

3.3 Mobility Tracking in 5G Cellular Networks

Participants: Mawloud Omar, Siham Bouchelaghem.

We proposed in [1] an LSTM-based next-cell prediction framework to address mobility challenges in 5G mission-critical IoT (mc-IoT) applications, which require ultra-reliable and low-latency communication (URLLC). The framework predicts the next serving cell for users based on their historical mobility traces, allowing for proactive resource allocation and seamless handover management in dynamic and high-mobility scenarios such as vehicular networks.

The proposed solution leverages the capabilities of LSTM (Long Short-Term Memory) neural networks to handle sequential data and capture long-term dependencies in user mobility patterns. By incorporating real-world vehicular mobility traces from a SUMO simulation, we validated the framework's effectiveness in predicting short- and long-term mobility. The results demonstrated that longer history datasets improve prediction accuracy, with the LSTM model outperforming traditional machine learning techniques such as KNN and SVM. This framework represents a significant advancement in 5G network slicing for critical IoT applications. It enables dynamic slices to adapt in near real-time, ensuring minimal latency, reduced resource wastage, and uninterrupted connectivity.

3.4 Attribute Capability-Based Access Control Model for IoT

Participants: Mawloud Omar.

Access control is essential for securing IoT environments, yet traditional models like Access Control Lists (ACL) and Role-Based Access Control (RBAC) fail to scale or adapt to IoT's dynamic nature. To address these limitations, we proposed ACapBAC (Attribute Capability-Based Access Control) [2], which merges Attribute-Based Access Control (ABAC) with Capability-Based Access Control (CapBAC) to offer fine-grained, flexible access control and controlled delegation mechanisms.

ACapBAC embeds attributes into capability tokens, enabling granular, context-aware access decisions. A key feature is decentralized delegation, allowing entities (delegators) to transfer rights to others (delegatees) under strict conditions. On-demand revocation further ensures adaptability in dynamic IoT environments. The model employs Attribute-Based Signatures (ABS) to authenticate based on attributes, enhancing privacy and preventing risks like attribute collusion. By enabling distributed, secure authorization decisions at the device level, ACapBAC eliminates reliance on central entities, increasing scalability and fault tolerance.

Performance analysis highlights significant reductions in communication overhead and storage needs compared to traditional models. ACapBAC is optimized for IoT's large-scale, dynamic networks, addressing the growing demand for secure, flexible, and privacy-preserving access control systems.

4 Software development

4.1 Ligo

Participants: Frédéric Guidec, Yves Mahéo.

Ligo is a device (based on a Raspberry Pi) designed in team INZU that is meant to behave as a peripheral device of a smartphone, providing this smartphone with the opportunistic networking services it cannot implement natively [r2]. A Ligo unit hosts several software components that enable the communication in the opportunistic network and the interaction with the smartphone via Bluetooth.

Recent work has been done the robustness of the system startup, and its control from the smartphone. On one hand, the Android application that implements a bluetooth tunnel from the smartphone to the Ligo device has been revised. On the other hand, a web application has been developped in order to provide the user with a graphical tool to perform various administration tasks (wifi-configuration, Ligo naming, shutdown...).

4.2 DoDWAN

Participants: Frédéric Guidec, Yves Mahéo.

DoDWAN[2] is a flexible Java-based middleware platform that has been developed in team INZU in order to support content-based, disruption-tolerant communication in opportunistic networks. It is distributed under the GNU General Public License (GPL)[3].

Recent work concerning DoDWAN focused on the development of an easy-to-use demonstrator that can run on any Linux platform, including the Ligo device designed in the team. This demonstrator includes all the necessary software to establish an ad hoc network (typically using Wi-Fi), to launch DoDWAN, and to set a local web site from which one can run some demonstration in-browser applications. Three main applications are proposed : WebOpp (content-based publication/subscription system for exchanging small text messages and files), Quillopp (collaborative text editing) and Cartopp (collaborative editing of an augmented map). The two latter applications are based on the exploitation of CRDTs. An administration web console is also available, namely in order to configure the ad hoc network.

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 data gathering and sharing. The data considered in RECSANet can be provided by 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 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,

[2] DoDWAN stands for “Document Dissemination in Wireless Ad hoc Networks”

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

that is to say on nodes with limited energy, limited computing power and that must cope with low data rates over LoRa.

6 Dissemination

6.1 Promoting scientific activities

6.1.1 Scientific Events Organization

- M. Omar has organized the first edition of a scientific event titled "Safety, Security, Predictability, and Logistics in Intelligent Transport Systems" on December 6, 2024, at UBS, Vannes (https://split2024.github.io/split/). The event gathered experts, researchers, and students to exchange ideas, showcase innovations, and foster collaborations in intelligent transport systems.

6.1.2 Journal

Reviewer - Reviewing Activities

- Y. Mahéo: reviewer for Computer Networks (Elsevier)
- N. Le Sommer: reviewer for Applied System Innovation (MDPI), Sensors (MDPI), Drones (MDPI), Future Internet (MDPI)
- F. Guidec: reviewer for ACM Computing Surveys.

6.1.3 Scientific Expertise

- F. Guidec has served as an expert to evaluate PhD funding applications for ComUE Normandie Université.

6.1.4 Research Administration

- F. Guidec serves as the local representative of IRISA at Universié Bretagne Sud.
- F. Guidec is a member of the steering committee of the doctoral school (ED) MathSTIC - Bretagne Océane.
- M. Omar is a member of the evaluation committee of the doctoral school (ED) MathSTIC - Bretagne Océane.

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: Project management tool, 4h
  M2: Development of secure mobile applications, 40h

- L. Touseau
  ESM2 (M1): Project supervision, 30h, AMSCC
  ESM2 (M1): Databases, 30h, AMSCC
  Mastère Cyber: Opportunistic networks, 2h, AMSCC

- M. Omar
  ENSIBS (M2): AI and Cybersecurity, 30h
  CYBERUS (M1): Pentesting, 12h
  UFRSSI (M1): Project supervision, 40h
  ENSIBS (M2): Project supervision, 20h

- S. Bouchelaghem
  ENSIBS (M1): Messaging security, 33h
  ENSIBS (M1): Active Directory security, 32h
  CYBERUS (M1): Pentesting, 12h
  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).

- 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).

6.2.3 Juries

- M. Omar: member of the PhD jury (reviewer) of Ali Haj-Hassan (Polytechnic University of Hauts-de-France), "Securing the communication protocols for industrial Internet of things", 2024/01/09.

7 Bibliography

Major publications by the team in recent years

[r1] F. GUIDEC, P. LAUNAY, Y. MAHÉO, "Causal and Δ-Causal Broadcast in Opportunistic Networks", *Future Generation Computer Systems 118*, May 2021, p. 142–156.

[r2] F. GUIDEC, Y. MAHÉO, P. LAUNAY, L. TOUSEAU, C. NOÛS, "Bringing Opportunistic Networking to Smartphones: a Pragmatic Approach", *in : 45th Computers, Software, and Applications Conference (COMPSAC)*, IEEE, p. 574–579, Madrid, Spain, July 2021.

[r3] 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.

[r4] 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.

[r5] 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.

[r6] A. SÁNCHEZ-CARMONA, F. GUIDEC, P. LAUNAY, Y. MAHÉO, S. ROBLES, "Filling in the missing link between simulation and application in opportunistic networking", *Journal of Systems and Software 142*, August 2018, p. 57–72.

[r7] 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. BELHADJ, K. AKILAL, S. BOUCHELAGHEM, M. OMAR, S. AISSANI, "Next-cell prediction with LSTM based on vehicle mobility for 5G mc-IoT slices", *Telecommunications Systems 87*, September 2024, p. 809–833.

[2] S. Tegane, K. Hamouid, M. Omar, F. Semchedine, A. Boudries, "An extended Attribute-based access control with controlled delegation in IoT", *Journal of Information Security and Applications 82*, May 2024, p. 103747.

Publications in Conferences and Workshops

[3] S. Aissani, M. Omar, K. Hamouid, "A Comprehensive Review of Predictive Maintenance Technologies for Vehicle Reliability", *in: 11th Annual Conference on Computational Science and Computational Intelligence (CSSI'24)*, Las Vegas, NV, USA, December 2024.

[4] T. Chenache, K. Zizi, S. Aissani, M. Omar, "Improving Road Safety: Real-Time Detection of Dangerous Driving Behaviors with Random Forest Classification", *in: 2nd International Conference on Big Data, IoT, Web Intelligence, and Applications (BIWA'2024)*, Bejaia, Algeria, May 2024.

[5] K. Hamouid, M. Omar, S. Aissani, "Safe Vehicular Platooning Control: Mitigating Uncertainty and Enhancing Stability", *in: 8th International Conference on System Reliability and Safety (ICSRS 2024)*, Catania, Italy.

[6] A. Lahoua, M. Younes, L. Touseau, "Improving Energy-Efficiency In Lora Networks Thanks to a Holistic Transmission Model", *in: 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2024)*, p. 469–476, Paris, France, October 2024.

[7] E. Lemonnier, J. El Hachem, L. Touseau, J. Buisson, N. Belloir, J.-F. Wiorek, "Analyse des mécanismes de contrôle d'accès pour une approche dynamique et décentralisée du data-centric security (DCS)", *in: 31st Computer & Electronics Security Application Rendezvous (C&ESAR 2024)*, Rennes, France, November 2024.

[8] F. Nawshin, R. Arnal, D. Unal, P. Suganthan, L. Touseau, "Assessing the Effect of Model Poisoning Attacks on Federated Learning in Android Malware Detection", *in: 2nd Cognitive Models and Artificial Intelligence Conference (AICCONF 2024)*, SETSCI, p. 147–154, Istanbul, Türkiye, May 2024.

[9] H. D. Nguyen, N. Le Sommer, Y. Mahéo, "Over-the-Air Firmware Update in LoRaWAN Networks: A New Module-based Approach", *in: Procedia Computer Science, 21st Conference on Mobile Systems and Pervasive Computing (MobiSPC 2024), 241*, Elsevier, p. 154–161, Huntington, WV, USA, August 2024.

[10] M. Omar, S. Aissani, K. Hamouid, "A Review of Uncertainty Management in Vehicular Platooning: Safety and Efficiency in Opportunistic Transport Environments", *in: 8th International Conference on System Reliability and Safety (ICSRS 2024)*, Catania, Italy.