Activity Report 2022

Team CASA

Opportunistic Networking and Computing

D2 – Networks, Telecommunications 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, from September 2022
Pascale Launay, Assistant professor, Univ. Bretagne Sud
Nicolas Le Sommer, Assistant professor, Univ. Bretagne Sud
François Lesueur, Assistant professor, Univ. Bretagne Sud
Lionel Touseau, Assistant professor, Académie Militaire de Saint-Cyr Coëtquidan

Administrative assistants

Anne Le Tohic, Martine Milcent.

2 Overall objectives

2.1 Overview

The research activity of team CASA 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. According to Mota et al. [MCM+14], delay/disruption-tolerant networks should actually be considered as a subset of opportunistic networks..

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 CASA 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 CASA 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.

A new research orientation of the team CASA emerged recently as some of our work focus now on security in IoT and dynamic networks, with the objective to address security issues pertaining to opportunistic networking as well as to opportunistic computing.

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

[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*, July 2014, p. 5–19.

[CGMP10] M. Conti, S. Giordano, M. May, A. Passarella, "From Opportunistic Networks to Opportunistic Computing", *IEEE Communications Magazine 48*, 9, September 2010, p. 126–139.

2.2 Scientific foundations

2.2.1 Opportunistic Networking

In the early 2000s the IETF initiated the DTN Research Group (DTNRG), 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 [SB07], 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 CASA 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].

[SB07] K. Scott, S. Burleigh, "Bundle Protocol Specification", IETF RFC 5050, November 2007.

[WHFE09] L. Wood, P. Holliday, D. Floreani, W. M. Eddy, "Sharing the Dream: the Consensual Hallucination Offered by the Bundle Protocol", *in : Internation 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, June 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*, July 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, January 2017, p. 168–173.

[CGMP10] M. Conti, S. Giordano, M. May, A. Passarella, "From Opportunistic Networks to Opportunistic Computing", *IEEE Communications Magazine 48*, 9, September 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 CASA 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 CASA 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-casa.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 CASA has investigated the problem of implementing operation-based, state-based, and delta-state-based CRDTs in an OppNet, and proposed a specific synchronization algorithm for each variant (including an optional transitive mode for delta-state-based CRDTs) [1].

Experiments based on a variety of radio contact tracesets confirm that the use of CDRTs is indeed pertinent in Oppnets. The results show that all forms of synchronization (i.e., operation-based, state-based, and delta-state-based) ensure the convergence of replicas in about the same time frame, although the number of messages and the amount of data transfers required to reach convergence differ significantly depending on the synchronization method considered.

Delta-state-based synchronization globally outperforms operation-based and pure state-based synchronization. It compares with operation-based synchronization as far as the global amount of data transferred is concerned, while requiring much fewer messages. State-based synchronization yields significant transmission overhead, because it requires exchanging entire states whenever two mobile nodes get into radio contact. It should therefore only be used for CRDTs whose size is small and almost stable over time (i.e., non-container CRDTs).

Using transitive forwarding in delta-state-based synchronization was expected to speed up the convergence of replicas, but results show that it actually only brings very little benefit: the time to convergence of replicas is only reduced marginally, while the number of messages exchanged by neighbor nodes is increased significantly.

Besides running these experiments involving different kinds of synchronization models for CRDTs, team CASA has initiated the development of a CRDT-based demonstrator that is meant to support collaborative editing in OppNets. This demonstrator relies on Quill[2] (a web-based text editor), Yjs[3] (a Javascript library implementing several types of CRDTs), and our opportunistic communication middleware DoDWAN[4].

3.2 Opportunistic Networking in Low-Power Wide Area Network

Participants: Nicolas Le Sommer, Lionel Touseau.

Low-Power Wide Area Networks (LPWANs) have received in the last years a lot of attention from the research community and the industry for Internet of Things (IoT) applica-

[2]https://quilljs.com
[3]https://github.com/yjs
[4]https://casa-irisa.univ-ubs.fr/dodwan

tions.Team CASA investigates the possibility of using LoRa (one of the main technology for LPWANs) in the design of a distributed system dedicated to the observation of the environment, and relying on opportunisting networking techniques and participatory science. 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, but 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 propose an alternative solution, called LoRaOpp[6], 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).

3.3 Adaptative key management for IoT

Participants: Mawloud Omar,.

Securing resource-constrained communicating systems emerges as the current security methods fail to fit the requirements of such systems, which are hardly limited in computation power, transmission bandwidth, energy, and connectivity intermittence. These severe constraints require a new understanding of security by handling the trade-off between embeddability and robustness. In this context, CASA investigates the security of IoT, which is one of the most representative environments of such systems.

We addressed key management as it is among the most crucial functional module of any secure communicating system. We proposed a new key management protocol to secure communications before and after key establishment[2]. Our scheme uses hash and one-one functions to achieve security during the key establishment process. The symmetrical character of the invertible functions is exploited to conceal critical data and pairwise keys stored in the nodes' memories. Our proposal makes the key refresh period adjustable according to the attack intensity. Moreover, it incorporates a key revocation process that does not require any control message exchange between the network members, which relaxes the 1-affects-n phenomena and considerably reduces the overhead in terms of bandwidth consumption.

3.4 Characterization of Attackers

Participants: François Lesueur.

IT systems are regularly rocked by attacks. In recent years, it has become an important means of pressure on competing companies, governmental organizations, and individuals. But unfortunately, attacks can bring down a system and all the social structures behind it.

In [7], we presented a new and original methodology that increases the knowledge about IP addresses used by attackers by assigning organizational labels to these addresses. We introduced an algorithm collecting the following labels: the type of structure (e.g., IT companies, universities), the field of work (e.g., web service hosting) and the human size (e.g., number of employees). This algorithm uses RDAP and Wikidata as inputs and uses text-analysis to match the correct Wikidata item onto an RDAP result. Our approach aims to better characterize the socio-organizational characteristics of the attacking host rather than the attack to then establish the best security policies.

4 Software development

4.1 MUON

Participants: Pascale Launay, Frédéric Guidec, Nicolas Le Sommer.

Characterizing mobility and contact scenarios and measuring the performance of routing protocols is required to evaluate and compare the different approaches in the opportunistic networking community. The metrics typically used to evaluate the performances of network protocols do not always make sense in the context of opportunistic networks, and it is therefore important to define more appropriate data formats and metrics. Opportunistic networks can be modeled as dynamic graphs, and metrics related to dynamic graphs allow to capture the properties of mobility and contact scenarios and produce relevant measures to evaluate and compare the performances of protocols.

MUON[5] is a a platform composed of a suite of tools accessible through a Web front-end. The Web front-end makes it possible for a user to upload mobility, contacts and experiment log files, run conversion and analysis tools, and display and download results. Analysis tools allow to calculate and present metrics to characterize mobility and contact scenarios, and to evaluate the performance of algorithms. Conversion tools allow to transform, filter and sanitize datasets. The CASA team members use them to analyze the traces of field experiments and simulations carried out in their projects. The MUON Web front-end is functional, has been tested and made available for external users[6].

4.2 DoDWAN

Participants: Frédéric Guidec, Yves Mahéo.

DoDWAN[7] is a flexible Java-based middleware platform that has been developed in team CASA in order to support content-based, disruption-tolerant communication in opportunistic networks. It is distributed under the GNU General Public License (GPL)[8].

In content-based networking, information flows towards interested receivers rather than towards specifically set destinations. This approach notably fits the needs of applications and services dedicated to information sharing or event distribution.It can also be used for destination-driven message forwarding, though, considering that destination-driven forwarding is simply a

[5]MUON stands for “Miscellaneous Utilities for Opportunistic Networking”

[6]https://www-casa.irisa.fr/muon

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

[8]https://www-casa.irisa.fr/dodwan

particular case of content-driven forwarding where the only significant parameter for message processing is the identifier of the destination host (or user).

Recently, a set of functionalities have been added to DoDWAN, through its plugin mechanism, in order to support the synchronization of Yjs CRDTs[9]. We have build a so-called Yjs provider that is in charge of the communication underlying the synchronization of replicas. This provider allows the developpemnt of distributed applications that rely on the sharing of distributed data structures in an opportunistic network.

5 Dissemination

5.1 Promoting scientific activities

5.1.1 Journal

Reviewer - Reviewing Activities

- N. Le Sommer: reviewer for Ad Hoc Networks (Elsevier), Sensors (MDPI), Future Internet (MDPI), Applied Sciences (MDPI), Computers (MDPI).
- L. Touseau: reviewer for Remote Sensing (MDPI).

5.1.2 Scientific Expertise

- F. Guidec has served as an expert to evaluate PhD funding applications for ComUE Normandie Université.
- M. Omar has served as an expert for mid-term evaluation of a PhD student for University Gustave Eiffel.

5.1.3 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.

5.2 Teaching, supervision

5.2.1 Teaching

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

[9]https://github.com/yjs/yjs

- 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
- M. Omar
  CYBER3 (M2): Cloud Security, 34h
- L. Touseau
  ESM2 (M1): Project supervision, 30h, AMSCC
  ESM2 (M1): Databases, 30h, AMSCC
  ESM2 (M1): Object-oriented programming, 20h, AMSCC

5.2.2 Supervision

- Camille Moriot: "Analysis of Distributed Denial-of-Service (DDoS) attacks and their impact on the Internet architecture", PhD in progress at University Lyon, co-supervised by F. Valois (CITI, Agora), F. Lesueur (IRISA, CASA), and N. Stouls (CITI, Phenix).

5.2.3 Juries

- F. Guidec has served as a reviewer and jury member for the HdR defense of Yoann Pigné, Université Bretagne Loire, laboratoire LITIS, Le Havre, 12/12/2022.

- F. Guidec has served as a reviewer and jury member for the PhD defense of Safuriyawu Ahmed, INSA Lyon, laboratoire CITI, Lyon, 16/12/2022.

6 Bibliography

Major publications by the team in recent years

[r1] M. Bagot, *Plateforme adaptative pour le suivi de l'état de santé de patients mobiles*, PhD Thesis, Université Bretagne Sud / Université Bretagne Loire, July 2020.

[r2] F. Baklouti, *Service Composition in Opportunistic Networks*, PhD Thesis, Université Bretagne Sud / Université Bretagne Loire, March 2019.

[r3] F. Guidec, P. Launay, Y. Mahéo, "Causal and Δ-Causal Broadcast in Opportunistic Networks", *Future Generation Computer Systems 118*, May 2021, p. 142–156.

[r4] N. Le Sommer, Y. Mahéo, F. Baklouti, "Multi-Strategy Dynamic Service Composition in Opportunistic Networks", *Information 11*, 4, March 2020, p. 180.

[r5] 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.

[r6] L. Touseau, N. Le Sommer, "Contribution of the Web of Things and of the Opportunistic Computing to the Smart Agriculture: A Practical Experiment", *Future Internet 11*, 2, February 2019, p. 1–19.

Articles in referred journals and book chapters

[1] F. Guidec, Y. Mahéo, C. Noûs, "Supporting conflict-free replicated data types in opportunistic networks", *Peer-to-Peer Networking and Applications*, December 2022.

[2] M. Nafi, M.-L. Messai, S. Bouzefrane, M. Omar, "IFKMS: Inverse Function-based Key Management Scheme for IoT networks", *Journal of Information Security and Applications 71*, 2022, p. 103370.

[3] D. Zamouche, S. Aissani, M. Omar, M. Mohammedi, "Highly efficient approach for discordant BSMs detection in connected vehicles environment", *Wireless Networks 29*, 1, 2023, p. 189–207.

Publications in Conferences and Workshops

[4] N. Belloir, J. Buisson, L. Touseau, "Model-Driven Engineering as the Interface for Tactical Operation Order of Mixed Robot/Human Platoons", *in : Developments and Advances in Defense and Security, Proceedings of MICRADS 2021 Conference*, *Smart Innovation, Systems and Technologies*, *255*, Springer, p. 205–214, Cartagena da Índias, Colombia, 2022.

[5] S. Bouchelaghem, H. Boudjelaba, M. Omar, M. Amad, "User Mobility Dataset for 5G Networks Based on GPS Geolocation", *in : 27th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2022)*.

[6] 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.

[7] C. Moriot, F. Lesueur, N. Stouls, F. Valois, "How to build socio-organizational information from remote IP addresses to enrich security analysis?", *in : 47th Conference on Local Computer Networks (LCN)*, IEEE, p. 287–290, 2022.

[8] D. Zamouche, S. Aissani, M. Omar, N. Saad, "Safety-Oriented Train Control Systems Monitoring in Smart Railway Transportation: A Review", *in : 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS 2022)*, IEEE, p. 1–8, Oum El Bouaghi, Algeria, October 2022.

[9] D. Zamouche, S. Aissani, K. Zizi, L. Bourkeb, K. Hamouid, M. Omar, "A Behavioral Modeling-based Driver Authentication Approach for Smart Cars Self-Surveillance", *in : 27th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2022)*.