Compte rendu de la
Journée thématique GDR SoC^2 GDR RSD
Systèmes Embarqués et Objets Communicants

Date : 1er avril 2019
Lieu : Cnam, Paris

Organisateurs pour le GdR SOC2 :
- Sami Taktak (Cedric/Cnam)
- Franck Wajsburt (LIP6/SU)

Organisateurs pour le GdR RSD :
- Fabrice Theoleyre (ICube/CNRS)
- Stefano Secci (Cedric/Cnam)

84 Présents

Nom	Prénom	Affiliation
Achir	Nadjib	Université Paris 13
Aggour	Issam	Cnam (Master 2 SEMS)
Aguiraud	Guillaume	Cnam (Master 2 SEMS)
Bakowski	Przemyslaw	Univérsité de Nantes - LS2N
Barthel	Dominique	Orange
Bassi	Francesca	l2s
Beylot	André-Luc	IRIT - ENSEEIHT
Bissoli	Giulia	CNAM – CEDRIC
Bobin	Maxence	EDF R&D
Boe	Alexandre	IRCICA-IEMN
Bossuet	Lilian	Université Jean Monnet - Laboratoire Hubert Curien
Bou Tayeh	Gaby	FEMTO_ST
Boumerdassi	Selma	CNAM – CEDRIC
Braunstein	Cécile	LIP6
Bui	Dinh Thai	Nokia Bell Labs France
Chaouat	Nicole	CNAM – CEDRIC
Chetto	Maryline	Université de Nantes - Laboratoire LS2N
Chillet	Daniel	Université de Rennes 1 / Inria
Chotin	Roselyne	Sorbonne université/LIP6
Cirio	Laurent	Université Paris-Est
Da Silva Coelho	Wesley	Cnam
Delhomel	Romain	Cnam (Master 2 SEMS)
Diamanti	Alessio	Orange/Cnam
Djoudi	Aghiles	Paris-est
Dunglas	Thomas	Cnam (Master 2 SEMS)
Esseghir	Moez	UNIVERSITE DE TECHNOLOGIES DE TROYES
Fossati	Francesca	CNAM
Foubert	Brandon	Inria Lille
Fourmaux	Olivier	LIP6
Gal	Viviane	CNAM – CEDRIC
Gautier	Matthieu	Laboratoire IRISA
Gerzaguet	Robin	Univ Rennes, CNRS, IRISA, Granit
Gorce	Jean Marie	CITI-lab, INRIA, INSA Lyon
Guerin	David	Cnam (Master 2 SEMS)
Guiose	Semmy	Cnam (Master 2 SEMS)

Hadjadj-Aoul	Yassine	Université de Rennes 1
Herrera	Alan	Cnam (Master 2 SEMS)
Hoteit	Sahar	Université Paris Sud
Ibn Khedher	Hatem	Centrale Supelec
Ivan	Martinez	IETR - INSA de Rennes
Kecira	Rayan	Cnam (Master 2 SEMS)
Khawam	Kinda	UVSQ
Kifouche	Abdenour	ESIEE Paris
Louerat	Marie-Minerve	CNRS
Maaz	Bilal	ROC cnam
Mami	Amine	Université d'Oran
Maraninchi	Florence	Grenoble INP / Ensimag
Marchand	Cédric	École centrale de Lyon
Maudoux	Christophe	CNAM
Medina	Roberto	Inria Paris
Meziane	Farid	Cnam (Master 2 SEMS)
Montavont	Julien	ICube - Université de Strasbourg
Monteil	Thierry	LAAS-CNRS
Morin	Julien	Cnam (Master 2 SEMS)
Mroue	Hussein	Polytech Nantes
Natalizio	Enrico	LORIA
Nguyen	Mai Trang	LIP6 - Sorbonne Université
Noury	Ludovic	ESIEE Paris
Nouvel	Fabienne	INSA RENNES
Olejnik	Richard	CRIStAL UMR 9189
Oussakel	Imane	LAAS-CNRS
Parrein	Benoît	Université de Nantes / LS2N
Paul	Damien	Cnam (Master 2 SEMS)
Pétrot	Frédéric	Laboratoire TIMA, Univ. Grenoble Alpes
Pham	Congduc	Université de Pau
Phouratsamay	Kevin	Cnam (Master 2 SEMS)
Pirim	Patrick	Anotherbrain
Pujolle	Guy	Sorbonne Université
Quille	William	Cnam (Master 2 SEMS)
Rovedakis	Stephane	CEDRIC/Cnam
Ruben	Milocco	Université Comahue (Argentine)
Sailhan	Francoise	CNAM
Sampayo	Sebastián Lucas	University of Strasbourg
Secci	Stefano	Cnam
Song	Yeqiong	Université de Lorraine
Sorel	Yves	INRIA
Taktak	Sami	CNAM - CEDRIC
Tanguy	Philippe	Lab-sticc
Teles Hermeto	Rodrigo	Université de Strasbourg
Theoleyre	Fabrice	CNRS
Vantroys	Thomas	Université de Lille - CRIStAL / IRCICA
Vidal	Alan	Cnam (Master 2 SEMS)
Wajsbürt	Franck	LIP6
Zhou	Fen	ISEP

Le programme était le suivant

- 9h00 -9h45 : Accueil, café
- 9h45 – 10:00 Présentation des 2 GDR
- 10:00 – 11:00 Keynote: Dominique Barthel, Orange, The elusive smart dust: the way ahead

- 11:00 – 11:20 LPWAN Networks, défis et opportunités, Fabienne Uzel-Nouvel, Jean Christophe Prevotet, Ivan Martinez, INSA Rennes
- 11:40 – 12:00 Framework for PHY-MAC layers Prototyping in Dense IoT Networks, O. Oubejja, JM. Gorce, D. Duchemin, LS. Cardoso, INSA Lyon
- 12:00 – 12:20 Retour d'expérience sur le déploiement ad-hoc de solutions LoRa pour des applications rurales, Phan Congduc, Université de Pau
- 12:20 – 12:40 Contribution à la conception des systèmes temps réel autonomes alimentés par l'énergie ambiante, Maryline Chetto, Université de Nantes
- 12:40 – 13:20 Pause déjeuner
- 13:20 – 14:10 Posters et démonstrations
- 14:10 – 15:10 Keynote: Florence Maraninchi, Univ. Grenoble, Infrastructures for Smart Cities: Towards Sharing Actuators
- 15:10 – 15:30 Spreading Factor and Channel Selection in LoRaWAN: A Learning Approach, Kinda Khawam, Université de versailles
- 15:30 – 15:50 A Domain-specific Language for Autonomic Managers in FPGA Reconfigurable Architectures, Eric Rutten, Inria, LIG
- 15:50 – 16:10 Pause café
- 16:10 – 16:30 Implémentation matérielle d'algorithmes de chiffrement authentifié sur FPGA, Roselyne Chotin, LIP6, Sorbonne Université
- 16:30 – 16:50 Support efficace de l'accès massif des dispositifs IoT dans les futurs réseaux sans fils, Yassine Hadjadj-Aoul, IRISA, Université de Rennes I
- 16:50 – 17:10 Sécurité dans l'Internet des Objets : de la communication aux capteurs, Cédric Marchand, Ecole Centrale de Lyon
- 17:10 – 18:00 Panel – discussions

Résumés des présentations

- **Keynote: Dominique Barthel, Orange, The elusive smart dust: the way ahead**
  - Résumé : Building smart devices as small as a grain of sand to be sprinkled on the ground or on walls to form a sensing fabric has been a dream for the last twenty years. We'll revisit the technical challenges in realising this dream and see how technology has advanced over the last two decades in this various areas. Some current projects will be described, highlighting their research thrust.
  - Bio : Dominique Barthel earned his engineering degrees at Ecole Polytechnique and SUPELEC in 1985 and 1987. In the first part of his career, he architected and designed microprocessors, CPUs for supercomputers and real-time video processors. He then moved to telecommunication and networking, and has been researching architecture and protocols for IoT devices since the early 2000's. He works for Orange Labs in Meylan and is a designated Orange Expert on Networks of the Future. He is the co-inventor of 15 international patents.

- **LPWAN Networks, défis et opportunités, Fabienne Uzel-Nouvel, Jean Christophe Prevotet, Ivan Martinez, INSA Rennes**
  - Résumé : Les réseaux LPWAN sont présentés comme le nouveau paradigme de l'internet des objets. Ils permettent une communication sans fils, basse consommation, bas débit et longue portée. Lors de cette présentation vous allez découvrir en détail les sujets de recherche concernant LPWAN – LoRaWAN que nous abordons dans notre laboratoire (IETR-INSA). Nous avons deux axes de recherche: la mobilité et la cybersécurité au niveau physique et MAC. Pour le premier nous développons des techniques du type SCHC (plus spécifiquement LSCHC) avec des messages IPv6 légers permettant de gérer la mobilité des End-Devices lorsque l'ED est en itinérance entre différents opérateurs LoRaWAN. En ce qui concerne la cybersécurité notre objectif est de modéliser les attaques de brouillage à l'aide de modèles mathématiques (ALOHA) et de simulateurs d'événements (NS-3). En plus de cela, nous souhaitons développer un mécanisme de détection automatique des attaques de bas niveau.

- **Framework for PHY-MAC layers Prototyping in Dense IoT Networks, O. Oubejja, JM. Gorce, D. Duchemin, LS. Cardoso, INSA Lyon**
    - Résumé : In this work, an Internet-of-Things (IoT) network implementation, part of the project « Enhanced Physical Layer for Cellular IoT » (EPHYL), using FIT/CorteXlab radio testbed is presented. The aim of our work is to provide a customizable and open source SDR design for IoT networks prototyping in a massive multi-user, synchronized and reproducible environment thanks to the hardware and software capabilities of the testbed. The massive access feature is managed by emulating several sensors per radio nodes. Two categories of network components are used in our design: a base station unit and a multi-sensor emulator unit. The components are separately hosted in dedicated and remotely accessible radio nodes. Their design features can be illustrated through a live demo, which is also reproducible as it is available for any interested reader.

- **Retour d'expérience sur le déploiement ad-hoc de solutions LoRa pour des applications rurales, Phan Congduc, Université de Pau**
    - Résumé : Nous présenterons un retour d'expérience sur le déploiement adhoc de solutions LoRa pour des applications rurales. Ces études ont été effectués dans le cadre des projets EU H2020 WAZIUP et WAZIHUB pour déployer de l'IoT à bas-coût en Afrique. Nous présenterons le système LoRa générique développé et nous discuterons des difficultés et des limitations observées dans ces déploiements. Quelques solutions pour améliorer la connectivité et l'accès au support radio dans les réseaux LoRa seront ensuite présentés.

- **Contribution à la conception des systèmes temps réel autonomes alimentés par l'énergie ambiante, Maryline Chetto, Université de Nantes**
    - Résumé : Concevoir des systèmes embarqués, entièrement autonomes, nécessite la résolution d'un certain nombre de problèmes liés à la récolte de l'énergie ambiante (energy harvesting), son stockage et son utilisation, de façon à assurer une autonomie durable (d'une à une dizaine d'années) et ce, tout en maintenant un niveau de performance acceptable à la fois au système de traitement et au système de communication. S'agissant de systèmes temps réel, la performance s'exprime ici en termes de temps de réponse et plus particulièrement en termes de respect ou non d'échéances. Cet exposé a pour objectif de décrire les travaux menés sur cette thématique par le groupe STR du LS2N (Laboratoire des Sciences du Numérique de Nantes), spécifiquement au regard de l'ordonnancement et de la gestion dynamique d'activité des systèmes temps réel autonomes en architecture monoprocesseur. Nous effectuerons une synthèse des résultats de recherche les plus significatifs obtenus au cours de ces quatre dernières années.

- **Keynote Florence Maraninchi, Univ. Grenoble, Infrastructures for Smart Cities: Towards Sharing Actuators**
    - Résumé : Smart cities require the deployment of sensors and actuators, connected to a network infrastructure. A number of current solutions are vertical, in the sense that a set of sensors, actuators and even the network, are dedicated to one application (traffic control, light control, …). There is a trend towards horizontal solutions, in which sensors, actuators, and the network infrastructure, can be shared between actors and applications. Sharing sensors, typically between several monitoring applications, is technically much simpler than sharing actuators. In this talk, we will see what it means to share actuators, define a notion of conflicting commands, and see what type of access control protocol can be used to guarantee safety properties and atomicity in the presence of such conflicts. Since actuators influence the physical world, actions cannot be undone. This raises specific problems for the definition of a transaction-like mechanism.

- Bio: F. Maraninchi est professeure à Grenoble INP/Ensimag depuis 2000. Elle a été co-responsable de la filière « systèmes et logiciels embarqués' » de sa création en 2008 jusqu'à 2014. Elle enseigne actuellement les bases des architectures matérielles, les systèmes 'exploitation et la programmation concurrente, les systèmes temps-réel et la validation formelle des systèmes embarqués. Elle est directrice depuis 2016 du laboratoire Verimag, spécialisé dans la modélisation, l'analyse et l'implantation des systèmes cyberphysiques. Elle travaille actuellement sur deux thèmes : (1) les langages et méthodes pour l'implantation correcte par construction des systèmes temps-réel critiques sur des architectures multicoeurs ; (2) la modélisation fidèle et la simulation efficace de systèmes matériel/logiciel dans l'approche dite des « jumeaux numériques ». Elle a eu de nombreuses collaborations industrielles, en particulier avec STMicroelectronics, Orange, Airbus, Kalray, etc.

- **Spreading Factor and Channel Selection in LoRaWAN: A Learning Approach, Kinda Khawam, Université de versailles**
  - Résumé : For a seamless deployment of the Internet of Things (IoT), self-managing solutions are needed to overcome the challenges of IoT, including massive data processing and resource management in terms of calculation, memory and battery. One of the most promising solutions to these challenges is the use of artificial intelligence. This will enable IoT equipment to operate autonomously in a dynamic environment by using innovative and inherently distributed learning techniques, thus freeing IoT equipment from draining their limited energy by constantly communi- cating with a centralized controller. In particular, the work is applied to a specific context of the IoT, the LoRaWAN networks where the equipment communicates with the gateway (GW) via a distributed access with ALOHA type contention (without detection) and spread spectrum technology (CSS) by resorting to the Multi-armed bandit algorithm.

- **A Domain-specific Language for Autonomic Managers in FPGA Reconfigurable Architectures, Eric Rutten, Inria, LIG**
  - Présentation annulée

- **Implémentation matérielle d'algorithmes de chiffrement authentifié sur FPGA, Roselyne Chotin, LIP6, Sorbonne Université**
  - Résumé : Les systèmes communicants actuels ont besoin d'accéder, de stocker, de manipuler ou de communiquer des informations sensibles. Ils utilisent des primitives cryptographiques telles que les fonctions de hachage et de chiffrement par blocs pour assurer la confidentialité, l'intégrité et l'authenticité de ces informations. Des techniques existent pour combiner chiffrement et hachage en un seul algorithme appelé chiffrement authentifié (Authenticated Encryption ou AE en anglais). Ce type d'algorithme permet de meilleures performances puisque hachage et chiffrement peuvent ainsi partager une partie du calcul et une même clé. Nous verrons comment l'implantation dans les FPGAs du chiffrement authentifié est particulièrement intéressante dans les systèmes de communication à haut débit, mais aussi pour protéger la procédure de configuration du FPGA. Nous illustrerons cela par des implantations matérielles efficaces des algorithmes certifiés AES-CCM et AES-GCM. Nous présenterons également une implantation matérielle du nouvel algorithme AEGIS qui est un des 7 finalistes de la compétition CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) qui vise à proposer un portefeuille d'algorithmes de chiffrement authentifié avec leurs implantations matérielles et logicielles.

- **Support efficace de l'accès massif des dispositifs IoT dans les futurs réseaux sans fils, Yassine Hadjadj-Aoul, IRISA, Université de Rennes I**
  - Résumé : Le support efficace des terminaux IoT devrait être l'un des principaux moteurs du futur réseau 5G. L'augmentation significative du nombre de ces dispositifs pourrait

toutefois entraîner une augmentation considérable du trafic sur le réseau d'accès, ce qui pourrait entraîner une forte congestion et une dégradation du service, en particulier pour les applications les plus critiques. En effet, lorsque les arrivées du trafic IoT deviennent corrélées et synchrones, les performances du canal d'accès aléatoire (RACH) sont considérablement réduites, ce qui provoque des perturbations pour un grand nombre de dispositifs en raison de tentatives redondantes d'accès ratées. Il en résulte une augmentation de la consommation d'énergie et de très longs délais d'accès. Cette problématique et plusieurs solutions seront abordées dans cette présentation.

- **Sécurité dans l'Internet des Objets : de la communication aux capteurs, Cédric Marchand, Ecole Centrale de Lyon**
  - Résumé : L'Internet des Objets est aujourd'hui un écosystème bien connu dans lequel des objets plus ou moins intelligents communiquent au travers d'un réseau de communication. Le nombre d'objets connectés augmente depuis des années à une vitesse impressionnante passant d'environ 500 millions en 2016 à plus de 6.5 milliards en 2018. A ce rythme, il y aura 6 fois plus d'objets connectés que d'habitant sur terre en 2025. En conséquence, le nombre de données récoltées et transmises devient énorme et selon les applications, ces données peuvent être sensibles et nécessiter d'être protégées. Concernant ces aspects de sécurité, un certain effort a été effectué afin d'améliorer la sécurité des protocoles de communications. Il est également possible de trouver des solutions proposant d'ajouter un accélérateur matériel permettant d'ajouter un certain niveau de protection des données récoltées sur les nœuds de capteurs, avant qu'elles ne soient envoyées sur le réseau. Malheureusement, ce type de solutions augmente à la fois la surface et la consommation d'énergie des nœuds de capteurs. Dès lors, il est nécessaire de trouver de nouvelles solutions, permettant si possible d'amener la sécurité au plus proche des capteurs. Nous allons donc passer en revue l'ensemble des solutions actuellement proposées afin d'améliorer la sécurité de l'Internet des objets depuis la communication jusqu'au nœud de capteurs.

- **17h00 - 17h45 : Panel, Discussion**

  Participe au panel l'ensemble des orateurs de la journée. Les discussions se sont organisées autour de 3 questions :

  - Problème du développement durable quant à l'utilisation massive de petits objets. Dominique Barthel explique que la plupart des 28 milliards d'équipements correspondent à des tags passifs, donc sans batterie. Ainsi, les objets ne correspondent qu'à des circuits en silicium (du sable). Florence Maraninchi complète en terme d'objectif societal. Dans les villes intelligentes, se pose la question de l'utilisation des données. S'il s'agit d'informations non critiques, il s'agit d'applications « gadgets ». Inversement, des applications critiques requièrent un contrôle fin des ressources, et donc une extensibilité plus limitée.
  - La 5G remplacera-t-elle toutes les technologies actuelles ? La 5G est en réalité une collection de technologies hétérogènes (répondant à des caractéristiques différentes). Quant à l'extensibilité, LoRa permet de gérer des densités plus élevées en augmentant le nombre de passerelles (et donc le cout).
  - la sécurité des objets évolués. En réalité, les acteurs veulent aller vite, et la sécurité est souvent occultée. Par ailleurs, se pose également un problème de sûreté de fonctionnement, qui n'est bien souvent pas adressé.