# Annuation for industry Research Report 2012

Dere

0

# Systems and Solutions Integration

 $\bigcirc$ 



Power elect

<sub>ron</sub>ic systems

0

Ó



**CEA** is a French government-funded technological research organization. Drawing on its excellence in fundamental research, its activities cover three main areas: Energy, Information and Health Technologies, and Defense and Security. As a prominent player in the European Research Area, with an internationally acknowledged level of expertise in its core competencies, CEA is involved in setting up collaborative projects with many partners around the world.

Within **CEA Technological Research Division**, three institutes lead researches in order to increase the industrial competitiveness through technological innovation and transfers: the CEA-LETI, focused on microelectronics, information & healthcare technologies, the CEA-LIST dedicated to technologies for digital systems, and the CEA-LITEN devoted to new energy technologies.

The **CEA-LETI** is focused on micro and nanotechnologies and their applications, from wireless devices and systems, to biology and healthcare or photonics. Nanoelectronics and Microsystems (MEMS) are at the core of its silicon activities. As a major player in the MINATEC innovation campus, CEA-LETI operates 8,000-m<sup>2</sup> state-of-the-art clean rooms, on 24/7 mode, on 200mm and 300mm wafer platforms. With 1,700 employees, CEA-LETI trains more than 240 Ph.D. students and hosts 200 assignees from partner companies. Strongly committed to the creation of value for the industry, CEA-LETI puts a strong emphasis on intellectual property and owns more than 1,880 patent families. For more information, visit http://www.leti.fr.

**Systems and Solutions Integration** research activity is mainly devoted to Telecommunications, Internet of Things and Power Management areas. This activity includes architecture design of fixed or nomadic devices with embedded power management, sensors, data and information processing, RF communications and security functions. The R&D works are performed with academic or industrial partners with the strategic objective to improve the next generation of industrial products thanks to the integration of emerging nanotechnology techniques. Industrial partners range from SME to large international companies. Typical internal equipments are available to partnership R&D works such as RF Anechoic Chamber, Information Technology Security Evaluation Facility, Magnetometers Test Facility, Multidisciplinary Creative Team, Students Platform for Industrial Innovation and Technological Showroom.



Annual Research Report > 2012

Page 5
 Roland Blanpain
 Interview
 Head of Systems and Solutions
 Integration Division

Page 7 Key Figures

Systems and Solutions

leti

Page 9 Scientific Activity

Page 11 Cellular Communications

Page 17 Cognitive Radio Page 23
 Wireless Short-Range
 Communications

Page 43 Secure Communications and Circuits

Page 55 Sensors

Contents

Page 71 Energy

Page 79 PhD Degree Awards





Interview with Roland Blanpain, Head of Systems and Solutions Integration Division



## Dear reader,

Two years ago, CEA-LETI decided to focus drastically on SMI/SME support for innovation and technological transfer. The objective was, when relevant, to enrich or to upgrade future industrial products with advanced electronic functions to boost industry. DSIS Division was created at CEA-LETI to coordinate this action in the field of Technologies for Information and Communication and Energy Management.

Based on MINATEC Campus in the Laboratory for Electronics & Information Technology (CEA-LETI), the Systems and Solutions Integration Division is today offering a large spectrum of technological solutions to foster the industry competitiveness. To propose such innovative capabilities, relevant research projects have to be raised and achieved. This document will introduce you on basic technological bricks investigated in the DSIS Division, sometimes in collaboration with other Leti or CEA laboratories or with external partnership.

Of course, a large part of research in Information and Communication technologies is devoted to new wireless transmission techniques. These works cover a large spectrum of our future daily life such as cellular networks, indoor communications, short range high data rate radio links but also contactless systems and more recently new relevant and efficient use of the old analog TV frequency bands.

A second key point is to provide technologies for miniaturized, efficient and smart sensors. This domain includes both conceptual physical approach and smart integrated interface chips in order to deliver solutions close to industrial requirements.

Finally, the most emerging and promising works are dedicated to energy management, including improvement of global efficiency and environmental preserving aspects. Beyond the mandatory energy management for both the future electrical vehicle and the smart grid, this strategic area unveils new energy harvesting solutions for nomadic devices.

Now, it is time to shift to the core of the different technologies developed inside the DSIS division and to hope that a large part of them will be integrated in our future daily applications.

**Roland Blanpain** 



Annual Research Report > 2012



7





© CFA-Leti

Systems and Solutions

leti

3 technical facilities: Anechoic chambers, Magnetometer test ground, Information Technology Security **Evaluation Facility (ITSEF).** 



© CEA-Leti-DSIS

46 granted patents 46 papers, journals & books 119 conferences & workshops

113 Permanent researchers, 32 PhDs and Post-docs



© Laurence Godart-CEA

© DR/CEA P.Avavian

27 M€ budget 85% funding from contracts







# **Publications**

167 publications in 2012, including journals and Top conferences like IEEE IMS, EuMW, CROWNCOM, NEWCAS, VTC, ESSCIRC, PIMRC, and DAC.

# **Prize and Awards**

IEEE French chapter young scientist award granted to Antonio Clemente at ANTEM 2012.

Best student paper award granted to Ramona Rosini at LAPC 2012.

Best Paper Award granted to Dominique Noguet and Vincent Berg at SDR-WinnComm-Europe 2012.

# **Experts**

21 CEA experts.

6 researchers with habilitation qualification (to independently supervise doctoral candidates).

# **Scientific Committees**

Participation to Technical Programs and Steering Committees in major conferences and international bodies: SDR-WinnComm-Europe, ICC, Globecom, CROWNCOM, PIMRC, IEEE RFID, COST IC1004, MEMSWAVE.

## **Conferences and Workshops organizations**

DCIS 2012, Cryptarchi 2012, EUROMICRO DSD 2012, QMCC 2012, EUCAP 2012, BODYNETS 2012.

## **International Collaborations**

I<sup>2</sup>R-A\*STAR (Singapore), Univ. La Sapienza (Italy), Univ. Di Bologna (Italy), Univ. Catholique de Louvain (Belgium), VTT (Finland), IISB Fraunhofer (Germany), CSEM (Switzerland), SupCom Tunis (Tunisia).









wireless services. Femtocell networks have recently been proposed as a cost-effective solution to improve indoor coverage, provide higher data rate services, and increase battery life of the devices. However, massive roll out of additional Base Stations may drastically increase the network energy consumption and rise cochannel interference. Here, we present a novel cell selection scheme for Open Access femtocells that maximizes macrocell offloading and adapt the network activity to the user deployment improving system energy efficiency and reducing co-channel interference.

Femtocells (HeNBs) are low-power Base Stations (BSs) that offer radio coverage through a given technology while a broadband wired link connects them to the backhaul of a cellular operator. Such a technical solution presents several benefits both to operators and users (UE).

Here, we show that macrocell offloading has an important impact on improving the cellular network energy efficiency. Moreover, we propose a novel cell selection scheme for Open Access femtocells that adapts the capacity of the network to the load while guaranteeing rate constraints.

Advanced Open Access limits the number of simultaneously active femtos to reduce the system power consumption [1].

Considering a macrocell region overlaid by a set of femtos deployed in a block of apartments, femtos operate in the same bandwidth as the macro and offer service to indoor UEs located in their coverage area. The Macro BS serves outdoor UEs and indoor UEs that cannot be served by active femtos. To optimize the aggregate power consumption, we aim at finding the subset of femtocells of minimum size able to serve the indoor UEs located in its coverage area.

Therefore, femtos that do not have users to serve can be dynamically switched off. Hence, by limiting the number of simultaneously activated BSs, our approach can reduce interference and energy consumption.



Figure 1: Classic approach vs proposed Advanced Open Access

Here, we assess the effectiveness of the proposed Advanced Open Access scheme by comparing its performance with the reference approaches (Closed Access and Open Access). The main differences between these schemes are the following:

1) In the Closed Access, a UE can be served by a femto only if the BS is placed in the user apartment.

2) In the Open Access, UEs can be in the coverage area of several femtos. Hence, each UE selects the available femto associated with the best received signal.

In Figure 2, we show the Energy Consumption Gain of the investigated approaches with respect to the femto deployment ratio. This gain accounts for both the macro and femto energy consumption and is computed considering the Closed Access scheme as the reference approach.

Both Open Access and Closed Access schemes save energy via the macrocell offloading. However, the former scheme further increases the offloading and reduces the power consumption. Simulation results show that Open Access achieves up to 10% of gain with respect to the Closed Access. Nevertheless, when the number of active femtos increases (i.e.,  $\rho_d \geq 0.4$ ), the aggregate capacity of Open Access femtos exceeds the service request and the energy saving decreases. The system performance can be further enhanced switching off those femtos that are not serving active UEs.

In our simulations, up to 4% of the gain can be achieved by switching off idle cells. Finally, the proposed Advanced Open Access gains up to 10% and 14% with respect to the classic strategies with and without cell switching off.



Figure 2: Aggregated energy consumption with respect to the femtocell deployment ratio.

**References** :

<sup>[1]</sup> A. De Domenico, E. Calvanese Strinati, and A. Duda, "An energy efficient cell selection scheme for Open Access femtocell networks," 23rd IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2012), 9-12 Sept. 2012, Sydney, Australia, pp.436-441.



Distributed Node-B architecture is the new paradigm in base stations architecture that breaks down the base station into a Base Unit (BU), which is a digital unit that implements the PHY/MAC functionality, and the Remote Radio Head (RRH) that sends the actual transmission. Figure 1a shows the standalone architecture of RRH. The further extension of the concept of standalone RRH results in Cloud RAN (CRAN) is shown in Figure 1b. In this novel concept, operators can now place numerous BUs in a single geographical point while distributing the RRHs according to the coverage plan. By centralizing all the active electronics of multiple cell sites, at one location, it is envisioned that energy, real-estate and security costs are minimized.





Energy efficiency is becoming a core investigation axis for future sustainable wireless communication networks. One solution is to temporarily switch off base stations during inactive period also called DTX. Another important technique is to utilize MIMO techniques that provide additional degrees of freedom which facilitate multiplexing and diversity gains. The main focus of our study is to analyze the impact of jointly utilizing MIMO and DTX on the energy efficiency of CRAN and propose solutions for buffering and traffic shaping.

The traditional DTX allows energy savings in BS for very lowload. However, with the enhanced DTX [1], the BS adaptively buffers the data and transmits it in a short burst, depending on the requested Quality of Service (QoS). By introducing MIMO, we can further increase the BS sleep duration; however, each activated period using MIMO consumes more power as shown in power model given in [2].

The impact of MIMO and DTX on the input system power for cloud RAN deployment is illustrated in Figure 2 as it is ultimately system power that needs to be reduced to effectively save energy consumption of BSs. The BS input power increases with traffic for all the scenarios. The scenario 1 represents the power model in which there is no consolidation of BU resources, and in this case Enhanced-DTX MIMO performs poorly in terms of EE compared to Enhanced-DTX SISO even though there is reduction in both transmit power and BS activity. The reason being that for the case of MIMO, the BU power doubles for the case of using 2 antennas, and this increase is much higher than the reduction achieved through the reduction of transmit power and BS activity reduction. The scenario 3 represents another extreme case, in which there is perfect consolidation of BU hardware components to an extent that BU power consumption is indifferent to the number of antennas. In this case, we can see that there is significant gain compared to Enhanced SISO (dotted-blue line). In fact, the EE gain increases at high traffic load scenarios, as MIMO becomes more efficient in buffering and offloading traffic in small bursts. The maximum gain in EE achievable for scenario 3 can be as much as 20% especially at high traffic loads, when utilizing 2 transmit antennas at the RRH.



Figure 2: RRH input power (per TTI).

One of the biggest challenges in enabling the proposed DTX approaches in current standard is the absence of control signaling during the period when the base station is in sleep mode. We envision that this problem will be solved either by the neighboring cells assisting the sleeping base station to provide control signaling during sleep cycle or modifying the future releases of the LTE standard to enable longer sleep modes at the base-station without the presence of control signaling during the sleep duration.

#### References:

R. Gupta and E. Calvanese Strinati, "Base station duty-cycling and traffic buffering as a means to achieve green communications," IEEE Vehicular Techn. Conf., Québec City, Canada, 3-6 Sep 2012.
 R. Gupta, E. Calvanese Strinati and D. Kténas, "Energy Efficient joint DTX and MIMO to achieve Green Communications in Cloud Radio Access," IEEE CloudNet, Paris, France, 28-30 Nov. 2012.



M. Gorgoglione, V. Savin, D. Declercq (ENSEA, France)

ABSTRACT: We analyze the performance of several bit-interleaving strategies applied to non-binary LDPC codes over the Rayleigh fading channel. We demonstrate the importance of the bit-interleaving design, and propose an optimized design inspired from the Progressive Edge Growth algorithm. This optimization algorithm depends on the topological structure of the LDPC code and can be applied to any degree distribution and code realization. We show that the use of bit-interleaving used over fading channel introduces an additional diversity in the nonbinary LDPC decoder, providing important gains in terms of frame error probability and error detection.

Over the last 15 years, spectacular advances in the analysis and design of graph-based codes and iterative decoding techniques paved the way for the development of error correction systems operating very close to the theoretical Shannon limit. A prominent role has been played by the class of Low Density Parity Check (LDPC) codes, introduced in the early 60's by Gallager's and described later in terms of sparse bipartite graphs. Nowadays, LDPC codes are known to be capacity-approaching codes for a wide range of channel models, which motivated the increased interest of the scientific community and supported the rapid transfer of this technology to the industrial sector.

Over the past few years there has been an increased interest in non-binary LDPC codes due to their enhanced correction capacity. They have been proven to provide better performance than their binary counterparts when the blocklength is small to moderate, or when the symbols sent through channel are not binary, which is the case for highorder modulations or for multiple-antennas channels.

The case of codes for which the underlying bipartite graph is ultra-sparse, in the sense that each symbol-node is connected to exactly  $d_v = 2$  linear constraint-nodes, is of particular interest. Practically, for NB-LDPC codes defined over Galois fields GF(q) with  $q \ge 64$ , best codes, both asymptotically and at finite lengths, are ultra-sparse codes. Despite those advantages, the ultra-sparse LDPC codes in GF(q) suffer from a serious drawback, as their minimum distance grows at best logarithmically with the coded-block length, which may cause a performance degradation in the error floor region.





In this work [1], we investigated the non-binary LDPC codes transmitted over a Rayleigh (fast) fading channel, in which different modulated symbols are affected by different fading factors. In case of one-to-one correspondence between modulated and coded symbols, deep fading can make some coded symbols totally unrecoverable, leading to a poor system performance. In order to avoid this phenomenon, binary diversity can be exploited by using a bit-interleaver module placed between the encoder and the modulator. We propose an optimized interleaving algorithm, inspired from the Progressive Edge-Growth (PEG) method, which ensures maximum girth of the global graph that extends the bipartite Tanner graph of the code with a new ensemble of nodes representing the modulated symbols (Fig. 1).

Figure 2 shows the frame error rate (FER) performance of NB-LDPC codes over GF(64) and coded-block length N = 102 symbols (or equivalently 612 bits). We consider codes with (symbol, constraint)-node degree pairs (2, 6) and (2, 12), corresponding respectively to coding rates r = 2/3 and r = 5/6. It can be observed that bit-interleaved NB-LDPC codes have better performance in the error-floor region. Indeed, bit-interleaving on a Rayleigh channel helps the decoder to avoid convergence to low-weight code-words, therefore improving at the same time the FER performance and the probability of error detection (not shown in the figure). Moreover, the optimized PEG-like interleaver shows a gain with respect to the random interleaver, as far as performance and error detection rates are concerned.





#### References:

[1] M. Gorgoglione, V. Savin, and D. Declercq, "Binary Diversity for Non-Binary LDPC Codes over the Rayleigh Channel", 2012 IEEE Wireless Communications and Networking Conference (WCNC), 1-4 April 2012, Paris, France, pp. 158–162.

• Annual Research Report > 2012 • Multi-Research Report > 2012 • Multi-Research Report > 2012

Multi-Relay Cooperative NB-LDPC coding with Non-Binary Repetition Codes over Block Fading Channels

#### Research topics: cooperative communications, non-binary LDPC codes

V. Savin, D. Declercq (ENSEA), S. Pfletschinger (CTTC)

ABSTRACT: In this work, we propose a cooperative coding scheme to communicate efficiently over multiplerelay fading channels. Our approach relies on NB-LDPC codes at the source, coupled with NB-repetition codes at the relays. A simple joint decoding strategy is used at the receiver end, so that the decoding complexity is not increased compared to a system without relays, while preserving the coding gain brought by re-encoding the signal at the relays. The proposed scheme allows maintaining a constant gap to the outage probability of the cooperative system, irrespective of the number of relays.

Cooperative diversity techniques over wireless relay channels allow exploiting the broadcast nature and the inherent spatial diversity of wireless communications. A relay channel is a multi-terminal network consisting of a source, a destination, and a collection of relays that might be of different nature. The source broadcasts a message to both relays and destination, while the relays forward the message or modified versions of it to the destination. Subsequently, different cooperation protocols have been proposed, which can be classified into three major categories, namely the amplifyand-forward (AF), the compress-and-forward (CF), and finally the decode-and-forward (DF) protocol.

The DF protocol allows each relay to decode the received signal, re-encode it, and forward it to the destination. The forwarded message can either be identical to, or part of the initial transmission (repetition coding), or it can be obtained by using a dedicated coding scheme at the relays. The destination uses the global knowledge of the cooperative coding scheme to jointly decode the received signals both from the source and the relays.

In this work [1], we propose a new approach to the problem of cooperative coding in the case of multiple relays. The approach is based on non-binary LDPC (NB-LDPC) codes and the recently introduced technique of multiplicative non-binary coding, also referred to as non-binary repetition coding. As illustrated in Figure 1, the source broadcasts a NB-LDPC codeword to the destination and the relays. When the relays successfully decode the received word, extra parity symbols are computed at the relays through optimized non-binary repetition codes, which are then sent to the destination.



Figure 1: Cooperative coding using non-binary repetition coding.

The receiver first collects the word received from the source and the non-binary extra symbols received from the relays, then combines them before the iterative decoding. Precisely, using the received values from source and relays it computes a joint-probability vector that merges the sufficient statistics of all active links, and which is fed to the decoder. As a consequence, the iterative decoding complexity is the same in the presence or the absence of relays, while combining the codeword and the additional non-binary repetition symbols brings an effective coding gain. We also proposed a strategy to jointly optimize the NB-LDPC code broadcasted by the source and the non-binary multiplicative coefficients used at the relays, in order to further increase the coding gain brought by the joint decoding approach.

Figure 2 shows the frame error rate (FER) performance of the proposed cooperative coding scheme in case that 1, 2 or 4 relays are activated. For each case, we plotted the corresponding outage probability (dotted curves, asterisk markers) and the FER of the proposed cooperative coding scheme with optimized non-binary repetition coefficients (solid curves, full markers). For comparison purposes, we have also plotted the FER of the proposed cooperative coding scheme with classical repetition coding (dotted curves, empty markers). It can be seen that the proposed coding scheme achieves full-diversity in every case, hence fully exploiting the spatial diversity brought by the existence of relays. When no relay is activated, the gap between the FER of the NB-LDPC code used at the source and the outage probability is about 1 dB. More important, the non-binary repetition coding proves to be strong enough to maintain the same gap to the outage probability, irrespective of the number of activated relays.





#### References:

[1] V. Savin, D. Declercq, and S. Pfletschinger, "Multi-Relay Cooperative NB-LDPC Coding with Non-Binary Repetition Codes Over Block-Fading Channels", 20th European Signal Processing Conference (EUSIPCO), 27-31 August, 2012, Bucharest, Romania, pp. 1354–1358.



ABSTRACT: A miniature wideband switchable notch antenna was designed and demonstrated for wireless multistandard handheld terminals. The antenna, a quarter-wavelength notch antenna, integrates at its open end a PIN-diode switched capacitor to create two selectable bands at 880-960 MHz (GSM-900) and 1710-3200 MHz (DCS-1800, IMT-2000, LTE, WiFi-802.11b/g/n). It features a small size of  $\lambda$ /14 at the lowest frequency (880 MHz) and covers both bands with a VSWR < 3:1 and an efficiency between 50% and 85%.

Compact and efficient multi-band antennas are required for future wireless handsets, which must be compatible with a large set of communication standards. Multi-band antennas may be designed using wideband radiating elements [1] or arrays of multiple radiating elements, which are able to provide wideband responses at the expense of large dimensions (large electrical size, additional front-end circuits such as diplexer and matching circuits). Another solution consists in using monopole-type radiating elements with several folded branches in order to generate multiple resonances, but these designs lead to complex 3D geometries which may be difficult to optimize and manufacture. Another approach based on active devices (variable capacitors or switches) enable frequency-agile radiating elements with noticeable size reductions.

A miniature wideband antenna was developed, integrating an active switch in order to achieve a good mix between wideband antenna techniques to cover adjacent standard bands (e.g. cellular and WLAN standards in the 1.7-3 GHz band), and frequency-switching techniques to reach far-off standard bands (e.g. GSM-900 band at 880-960 MHz).

The proposed antenna, a quarter-wavelength ( $\lambda$ /4) slot antenna, is loaded at its open end by a switched discrete capacitance. Depending on both states (ON, OFF) of the PIN diode switch, a resonant band is selected covering either the 880-960 MHz band (GSM-900) or the 1710-3300 MHz band (DCS-1800, IMT-2000, LTE, WiFi-802.11b/g/n).

The antenna is 6 mm wide and 24 mm long, which corresponds to  $\lambda/14$  at the lowest frequency (880 MHz). The antenna miniaturization is obtained thanks to the capacitive loading of the slot. The slot is etched in the ground plane and the microstrip elements are printed on the back-side of a 0.8 mm-thick FR4 substrate (Fig. 1). The ground plane size is  $110 \times 50$  mm<sup>2</sup>, typically a smartphone size.

The antenna was fabricated and experimentally characterized in terms of reflection coefficient, impedance, total efficiency and radiation patterns. A good impedance matching level (VSWR < 3:1) is obtained for both states (ON, OFF) over the frequency bands 880-960MHz (capacitive-loading mode, ON state) and 1710-3200MHz (dual-resonance mode, OFF state) (Fig. 2). In the ON state, the measured relative bandwidth is 27% covering the GSM band (880-960MHz) while in the OFF state, the measured relative bandwidth is 58% and the following standards are covered: DCS-1800 (1710-1880MHz), IMT-2000 (1885-2025MHz and 2010-2070MHz), Wi-Fi-802.11 b/g/n (2400-2483MHz), and LTE (25002690MHz). Future developments may permit to reach an upper frequency of 3.6 GHz to include the WiMax (3400-3600 MHz) standard.

The efficiency was measured using the ultra-wideband Wheeler cap method and varies from 50% to 85% over the GSM-900 band and from DCS-1800 to LTE.

The gain patterns (total realized gain) of the antenna were measured in an anechoic chamber at 920 MHz and 2240MHz using a fiber-optic link connected to the antenna under test in order to limit the impact of a coaxial feed cable. A good agreement with the simulations was obtained [2].



Figure 1: Photograph of the switchable miniature notch antenna.





#### **References** :

M.A.C. Niamien, L. Dussopt, C. Delaveaud, "A compact dual-band notch antenna for wireless multi-standard terminals," IEEE Antennas and Wireless Propagation Letters, vol. 11, pp. 877-890.
 C. Niamien, L. Dussopt, C. Delaveaud, "Miniature switchable wideband notch antenna for multistandard wireless terminals," 6th European

<sup>[2]</sup> C. Niamien, L. Dussopt, C. Delaveaud, "Miniature switchable wideband notch antenna for multistandard wireless terminals," 6th European Conference on Antennas and Propagation, Prague Czech Republic, 26-30 March 2012.



High-gain electronically-reconfigurable antennas are required in several applications for military and civil space telecommunication systems. Electronically-reconfigurable transmit-array antennas are excellent candidates for these applications requiring a wide bandwidth as well as beam-

have been demonstrated.

steering and/or beam-forming capabilities. An X-band linearly-polarized electronically-reconfigurable transmit-array antenna was designed and demonstrated based on 1-bit unit-cells [1]. The unit-cells are fabricated on a three-layer stack of low-loss laminate substrates with four metal layers. Patch antennas are printed on each face of the stack, and connected through a metallic via. The inner metal layers are used for the ground plane and the biasing lines. One of the patch antennas include two PIN diodes controlled in opposite states in order to shift the phase of the transmitted signal by 180°. Each unit-cell is controlled with a single bias line. The unit-cell size is  $\lambda_0/2 \times \lambda_0/2$  at 10 GHz (15×15 mm<sup>2</sup>) in order to prevent the occurrence of grating lobes when steering the beam of the array. This unit-cell was characterized experimentally and showed less than 2.1 dB of insertion losses as well as a 3-dB bandwidth of 1.49 GHz (14.9%).



Figure 1:  $20 \times 20$  unit-cells electronically-reconfigurable transmit-array prototype with the steering-logic boards.

The size of the  $20 \times 20$  unit-cells antenna array is  $30 \times 30$  cm<sup>2</sup>. All the unit-cells are controlled through a total of 400 bias lines grouped on two opposite edges of the array. Steering-logic boards, controlled by a computer, are connected to the array and generate the appropriate biasing currents for each unit-cell (Fig. 1).

The array is fed through a 10-dBi horn antenna as a focal source. Simulated and experimental performances demonstrated a maximum gain of 22.7 dBi, a 3-dB fractional bandwidth of 15.8% (Fig. 2a), and pencil-beam scanning

over a  $140 \times 80$ -degree window (Fig. 2b) [2,3]. Good beam shaping capabilities have been demonstrated as well (flat-top beam).

To our best knowledge, this prototype is one of the largest reconfigurable transmit-array presented in the open literature, and its radiation efficiency is among the highest reported so far (52.9%).

The main author of this work received the IEEE (France Chapter) Young Scientist First Prize at ANTEM 2012 conference [2].



Figure 2: Simulated and measured broadside gain as a function of the frequency (a), measured H-plane radiation pattern for several scan angles ( $\theta_0 = \pm 70^\circ$ ) (b).

#### **References** :

A. Clemente, L. Dussopt, R. Sauleau, P. Potier, and P. Pouliguen, "1-bit reconfigurable unit-cell based on PIN diodes for transmit-array application in X-band," IEEE Trans. Antennas Propag., vol. 60, no. 5, pp. 2260-2269, May 2012.
 A. Clemente, L. Dussopt, R. Sauleau, P. Potier, and P. Pouliguen, "Design of a reconfigurable transmit-array at X-band frequencies," 15th Intern. Symp. on Antenna Tech. and Applied Electromagnetic, ANTEM 2012, 25-28 June 2012, Toulouse, France.
 A. Clemente, L. Dussopt, R. Sauleau, P. Potier, P. Pouliguen, "Electronically Reconfigurable Transmit-Array Antenna in X-Band," ESA Workshop on Large Deployable Antennas, 2 - 3 Oct. 2012, ESA/ESTEC, Noordwijk, The Netherlands.







Matthieu Gautier, Vincent Berg, Dominique Noguet

ABSTRACT: This work addresses wireless microphone sensing in the TV white space and efficient detection of narrowband FM modulation signals. To this end, a wideband frequency domain analysis is proposed. The required Fast-Fourier Transform for this operation may be shared between sensing analysis and modulation functions. A particular decision metric is then studied for the analysis of wireless microphone signals based on the Teager-Kaiser energy operator. Simulation results show that 6 dB of detection gain could be achieved when using a frequency-domain analysis compared to time-domain methods. The Teager-Kaiser detection leads to a further improvement of 1.5 dB. This performance could be reached at no extra cost in term of complexity.

The performance of sensing algorithms is fundamental to establish the opportunistic communication of a cognitive radio (CR) system. In the UHF band where the CR system could operate, the primary users are TV transmitters and wireless microphones. If the detection of TV signals has been addressed in the literature, solutions should be proposed for the detection of wireless microphones.

Wireless microphone signals are narrowband in comparison to their overall possible band of operation. This makes wireless microphone sensing difficult. The European TV band is composed of 48 channels of 8-MHz bandwidth and each band should be analyzed for microphone detection.

The analyzed TV channel is extremely wide compared to the frequency band occupied by the microphone signal (around 200 kHz). Thus, the detection of wireless microphones may be considered a narrowband signal detection problem.

Most of the references available in the literature use a blind detection for the specific case of wireless microphones.

The architecture proposed in [1] considers the narrowband property of the wireless microphone signal in the TVWS and proposes sharing a wideband Fast-Fourier Transform (FFT) operator that can be an element used by the cognitive device to simultaneously detect primary users and make the communication link.

The same FFT operation may also be used to perform the sensing step. This leads to a wideband sensing operation and a low complexity architecture with shared FFT operation.



#### Figure 1: Architecture of the wideband frequency domain detector.

A frequency domain metric is specifically proposed to detect wireless microphone signals. The Teager-Kaiser detector has already been proposed in the time domain and allows a better estimation of the energy of the wireless microphone signal. A frequency domain counterpart of this operator is introduced and analyzed and compared against different frequency analysis blocks.



Figure 2: Detection probability versus SNR.

Simulation results are provided in Figure 2. For a target probability of detection of 95%, the frequency-domain detectors enable the detection of signals with SNR of -14 dB and -15.5 dB for the energy and the Teager-Kaiser metrics respectively. In the time domain, the sensitivity levels are -7.5 dB for the energy detector, -9.5 dB for the Teager-Kaiser detector and -11.5 dB for the autocorrelation detector.

The simulation results show that, to the analyzed narrowband frequency-domain detection leads to a 6-dB improvement in comparison to the time domain energy detection. A further 1.5-dB gain is achieved using the Teager-Kaiser energy operator. Both frequency domain detectors outperform the autocorrelation detector with a gain of 4 dB for the Teager-Kaiser detector and a gain of 2.5 dB for the energy detector.

#### References:

[1] M. Gautier, V. Berg, D. Noguet, "Wideband frequency domain detection using Teager-Kaiser energy operator," 7th International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), 18-20 June 2012, Stockholm, Sweden, pp. 332-337.



CR systems are characterized by very strong requirements on flexibility. Particular scenarios are of interest: 'Cognitive femtocell' (e.g.: private wireless access of the same type as WiFi), 'cellular extension in the whitespace', and 'cognitive ad-hoc network'. The scenarios envisioned cover a wide range of QoS and Mobility and are foreseen to be tested on the unused TV spectrum, referred to as TV White Space (TVWS).

The identified cognitive scenarios have led notably to the study and development of advanced sensing mechanisms, context acquisition techniques and new flexible and spectrally-efficient multicarrier waveforms. These techniques will be combined to evaluate CR system solutions on a flexible hardware evaluation platform.

A set of requirements has been derived for the CR hardware platform. In order to test the mobility scenarios, the platform should be contained in size and battery powered. The radio link and the other stages of the cognitive radio, such as the reconfiguration of the radio, should also be available on the platform. An application will be run on top of the radio link to demonstrate QoS capability through advanced Medium Access Control (MAC) features.



Figure 1: Functional block diagram of the proposed CR hardware platform.

The CR hardware platform should include the following functionalities:

- Wide-band analog-to-digital and digital-to-analog converters should interface with an RF daughter board.
- Flexible hardware, i.e. Field Programmable Gate Array

(FPGA), should embed digital-signal-processing capabilities for the implementation of the digital physical layer multicarrier transmitter, receiver and spectrum sensing functionalities.

- An embedded microprocessor should complement the FPGA to control and configure the physical layer as well as execute the application and MAC.
- A fast data interface should link the platform to provide a network connection, and interface to a host display, and a Graphical User Interface (GUI).

An architecture based on a Xilinx Kintex 7 (xc7k325t) that is memory mapped to an ARM Cortex A8 core and digital signal processor TMS320C64x (Texas Instruments OMAP DM3730) forms the core of the design [1]. Ethernet PHY/MAC, WiFI and USB are provided for easy and high speed connectivity.

Particularly high performance converters have been chosen in order to relax the requirements on a flexible RF board.



Figure 2: Picture of the QoSMOS Flexible Hardware Platform.

A picture of the platform is presented in Fig. 2. The smartphone is given as size reference.

#### **References:**

[1] V. Berg, D. Noguet, X. Popon, "A Flexible Hardware Platform for Mobile Cognitive Radio Applications," 15th Euromicro Conference on Digital System Design (DSD), 5-8 Sept. 2012, Izmir, Turkey, pp. 459-462.

Heterogeneous Flexible Radio Platforms

#### Research topics: software-defined radio

P-H. Horrein, C. Hennebert, F. Petrot (INP-Grenoble)

ABSTRACT: Nowadays, many remote devices handle several communication standards. This raises new issues as the saturation of the radiofrequency domain and the energy consumption become major design issues with the increasing demand for mobility. Flexible radio is a promising solution to address these problems. In fact, a flexible radio device is able to process a given range of standards. The aim of FRK is to efficiently manage the platform reconfiguration for multi-mode, multi-standard operations, with several levels of abstraction.

Flexible radio encompasses any solution able to modify radio operations without changing the physical system. As an example, FPGA-based flexible radio platforms are statically reconfigurable. Dynamic reconfiguration of FPGA-based platform is very time consuming and not usable with the radio time constraints. Other solutions are only based on processors. In these solutions, called Software Defined Radio (SDR), all operations are performed thanks to software implementation.

The goal of FRK (Flexible Radio Kernel) is to provide an efficient and flexible framework for the management of flexible radio devices.

- It allows the management of multiple standards instances, from radio layer to Medium Access Control (MAC) layers, as well as abstraction for application developers
- It offers an independent application representation which can be deployed on any platform.
- It allows full use of the flexible platform presented in Figure 1, even if the developer has no knowledge of it.
- It provides a simple mean to integrate algorithms making use of flexibility.



Figure 1: Flexible radio reference.

FRK is built as a library. It offers an execution management through a runtime part and other services through an off-line part. The runtime part is based on software layers defined to provide control over the platform at all the development levels. The off-line part is integrated in the Radio Hardware Abstraction Layer (R-HAL) and is designed to translate a generic application called a waveform into an executable platform called a Configuration Instance (CI).

eti

The Protocol Layer (PL) acts as a networking standard scheduler in FRK. It stores all implemented MAC layers, and controls activation or inactivation of each MAC layers. The PL controller is responsible for managing the cooperation between the different MAC layers, as well as offering a standard selection service to upper layers.

FRK is based on the definition of targets in the platform. A target is a type of processing units for which the configuration method is similar. Each platform is made of a collection of targets. For example, a platform can be composed of a GPP target for software execution, a CUDA target for GPU execution and a RHW coprocessor target for hardware accelerator.

The integration of software operation is achieved using kernel tasks. A processor-like approach is introduced as a new way to handle hardware coprocessor, and configuration switch is used to manage concurrency.



Figure 2: Flexible Radio Kernel – Global architecture.

The flexible environment can be deployed on any platform, with no application adaptation, as long as the platform can provide the required processing power. The target view allows easy development of radio applications to build platform-dependent configurations.

#### **References:**

[1] P-H. Horrein, C. Hennebert, F. Pétrot, "An environment for (re)configuration and Execution Management of Heterogeneous Flexible radio Platforms", in Microprocessors and Microsystems, PII, Elsevier, June 2012.

• Annual Research Report > 2012 • Annual Research Report > 2012 • Annual Research Report > 2012

#### Research topics: software-defined radio

P-H. Horrein, C. Hennebert, F. Petrot (Grenoble – INP)

ABSTRACT: This work aims at taking benefit of the high computing resources offered by the new generation of Graphical Processor Units in the domain of radio signal processing. The operations achieved by a Software Defined Radio platform are not designed for GPU architecture. Two solutions, considering kernels of different sizes, are tested to realize this adaptation and the performance improvements are measured on typical radio operations.

The emergence of many communication standards handled into a single device raises new design strategies. Network devices that process the signal are traditionally implemented in hardware. But this implementation is not convenient to cope with flexibility underlying by the radio improvements in low-cost devices. Software Defined Radio (SDR) and General-Purpose computation on Graphics Processing Units (GPGPU) provide a possible solution.

Benefiting from GPU for radio processing is not a straightforward operation. As SDR environment is designed for General Purpose Processors (GPP), the platforms handle parallel tasks running simultaneously. In contrast, GPU architecture are Single Instruction Multiple Data (SIMD) architectures, designed to run simultaneously the same instruction on a large set of data. The adaptation of GPGPU to SDR should lead to high memory transfer overhead and centralized management, which may ruin the expected profit.

In order to use the GPU in a GNURadio application while keeping the benefit of the framework, operations on the GPU must be integrated in the environment, regardless of the selected approach.

The problem is handled carefully. Two models are considered in this study, a distributed model and a centralized one. The main idea behind the distributed integration is to keep the per-block approach of GNURadio. A GPU-executed block is similar to a classical CPU block. It provides the same interface, uses the same parameters and functions, and is based on the same FIFO channels. The only difference is the processing function. The scheduler for the GPU is thus distributed, with almost no information on the state of the other blocks. So, using distributed integration is the preferred option regarding GNURadio philosophy. But, using OpenCL environment also means using centralized control. In order to better fit the OpenCL approach, a centralized integration can be developed. The idea behind centralized integration is to use a single GNURadio block to implement a whole sequence of GPU operations. Using the centralized integration suppresses the need for FIFO between GPU operations. The centralized approach thus reduces the required memory on the GPU.

These two solutions can be seen as two levels of granularity for parallelization. The first one consists on a fine grain parallelism adapted to large computational complexity operations. The second one is more original and is based on a coarse grain approach allowing a better usage of the

**References** :

computing resources and more parallelism. Both solutions have been realized and analyzed on several radio operation types. Our study clearly highlights the interest of the coarse grain approach that provides performance improvements for the SDR.

As an example, the FFT operation implemented with a radix-2, requires  $log_2(N)$  iterations where N is the vector width. Each operation executes N/2 radix-2 butterflies. With the fine grain approach, the kernel for the operation is the radix-2 butterfly. In this solution, the small kernel leads to a high overhead to control the operation.

The coarse grain approach uses a bigger kernel to represent the entire operation - the FFT. While this approach may increase the latency and require more memory, it presents many advantages. The kernel implements the same algorithm than on a CPU, which avoids finding GPU-optimized version. Data dependent operations can be easily processed as long as there is no inter-vector dependency between the kernels. The latency induced by the approach can be decreased using a pipeline structure.



Figure 1: Comparison of FFT implementations on CPU and GPGPU.

This new method does not use GPU-specific optimization for the block implementation. It focuses on processing simultaneously several data blocks. It shows a significant gain compared to a classical CPU mapping approach (Fig. 1).

[1] P-H. Horrein, C. Hennebert, F. Petrot, "Integration of GPU Computing in a Software Radio Environment", Springer Journal of Signal Processing Systems (2012) 69:55-65.



# Research topics: tunable materials, miniature reconfigurable antennas

H. Nguyen, C. Delaveaud, R. Benzerga (IETR), A. Sharaiha (IETR), Y. Lu (IETR), C. Le Paven (IETR), L. Le Gendre (IETR), X. Castel (IETR)

ABSTRACT: A novel thin-film dielectric LaTiO<sub>x</sub>N<sub>y</sub> oxynitride (LTON) perovskite material is investigated for miniaturization and tunability of compact antennas. Its dielectric properties as well as its tunability were characterized at low and high frequencies using microstrip waveguide structures and Metal-Insulator-Metal capacitors. The design of miniature frequency-agile notch antennas based on tunable LTON capacitors was investigated.

The general trend towards miniaturization of wireless communicating electronic devices led to intensive researches on antenna miniaturization for systems operating in UHF frequency band. Due to the physical limitations associated with the miniaturization of antennas, the introduction of frequency agility techniques constitutes an interesting alternative to solve the problem of reduced bandwidth generally obtained in miniature antennas. Developments of the properties of a new type of material have been made in order to design a discrete tunable capacitor to reduce the size of an antenna and to control its operating frequency. The objective is to benefit from the high permittivity of the material, low-loss properties and variable permittivity under a limited voltage.

LaTiO<sub>x</sub>N<sub>y</sub> (LTON) is a newly developed dielectric material [1]-[2]. Thin films are deposited by reactive radio frequency magnetron sputtering on different substrates (Pt/MgO, Pt/Ti/SiO2/Si). Different compositions (oxide and oxynitride with low or high nitrogen content) and different thicknesses of LTON thin films have been tested (330 nm to 1200 nm). Properties of fabricated thin film materials have been studied over a wide frequency band (1 kHz-20 GHz) using different tests structures (Metal-Insulator-Metal capacitors, microstrip waveguide). The electrical properties of the material have been extracted from measurements for the different fabrication processes. Values of relative dielectric permittivity between 300 and 30 with low losses (tan $\delta$  = 0.005) can be obtained depending of the process and frequency. Agility of 30% for DC bias of only 1 V (or 50 kV/cm) at low frequencies (10 kHz) have been measured with low nitrogen film films. It was observed that the agility capability of the material decreases at high frequencies.

These material properties are used to investigate the miniaturization and tunability of a notch antenna based on the discrete loading of the slot open end by a static and variable capacitor made of LTON material [3]. A specific configuration of the variable capacitor is designed in agreement with the low capacitance value required by the antenna configuration. It is composed of three MIM capacitors based on LTON thin film. Capacitors are formed between the metal plates and the ground plane (Pt) (Fig. 1).

The integration of such a capacitor has been studied using a 3D electromagnetic simulation tool where equivalent models have been used to allow the simulation of thin material and

conductors in an antenna structure of a few centimetres.



Figure 1: Configuration of the thin film capacitor (left) and measured capacitance values for two different substrates (right).

The slot loading technique using a capacitor allows an antenna size reduction up to 54% for high capacitance values. The frequency agility of the antenna has been studied for the measured materials properties. In the example of performances reported in Fig. 2, the dielectric constant of the LTON thin film is varied from 40 and 60 (corresponding to an agility of roughly 30%). Consequently, the narrow operating frequency band of the antenna is shifted from 0.65 GHz to 0.71 GHz, resulting in a tuning range of 60 MHz, which corresponds to 8% of tunability.



Figure 2: Notch antenna structure loaded with a LTON varactor (left) and impact of the thin film's dielectric constant on antenna's reflection coefficient (right).

New investigations are in progress to improve the material agility at high frequencies and use it in different antenna structures.

#### **References** :

[1] Y. Lu, C. Le Paven-Thivet, L. Le Gendre, R. Benzerga, V. H. Nguyen, A. Sharaiha, F. Tessier, F. Chevire, C. Delaveaud, "Homogeneity of oxynitride LaTiOxNy thin film deposition by RF magnetron sputtering", 7th International Symposium on Nitrides - ISNT 2012, St-Malo, France, 3-6 june 2012.

[3] V.H. Nguyen, R. Benzerga, C. Delaveaud, A. Sharaiha, Y. Lu, C. Le Paven, L. Le Gendre, X. Castel, "New thin film varactor for frequency tunable slot antenna", Proc. of 6th European Conference on Antennas and Propagation (EUCAP), 26-30 March 2012, pp. 3595–3598.

<sup>[2]</sup> Y. Lu, C. Le Paven-Thivet, R. Benzerga, L. Le Gendre, V. H. Nguyen, A. Sharaiha, F. Tessier, F. Chevire, C Delaveaud, "Lanthanum titanium oxide and oxynitride thin films grown by water vapour and nitrogen reactive RF sputtering", 7th International Symposium on NiTrides - ISNT 2012, St-Malo, France, 3-6 june 2012.

# A Parasitic Technique for Miniature IFA Antenna Bandwidth Enhancement

#### **Research topics: miniature antennas**

O. Roncière, C. Delaveaud, R. Lionti

ABSTRACT: The design of an electrically-small antenna integrated into the helmet of a firefighter is presented. A miniature printed parasitic Inverted-F Antenna (IFA) has been developed in order to respect allotted volume and operating bandwidth. The antenna consists of two bended IFA with a single feed. The parasitic IFA is connected to the fed one by a metallic strip in order to enhance the impedance matching bandwidth. Good impedance matching and radiation properties have been measured and compatibility with fire fighter's equipment has been validated by experimental measurement campaigns.

The design of compact antennas integrated within wireless electronic devices is a research topic of growing interest for many consumer and industrial applications. Issues related to the size and performances (efficiency, bandwidth) of the antenna are critical for applications operating at sub-GHz frequencies where propagation properties are particularly attractive. This problem has been studied in a context of audio/video transmission for fire-fighters over a few kilometres with a minimal infrastructure (ANR Cockpit project). The device embedded in firefighter's equipment must fulfill sharp ergonomic constraint inside a very hostile environment.

Most particularly, the antenna must comply with the following specifications:  $\lambda_0/6 \times \lambda_0/23$  volume (including ground plane), matching impedance bandwidth 642-658 MHz (16 MHz) and an omnidirectional coverage with an average gain above -3 dBi. The absence of a ground plane with large dimensions compared to the wavelength is a major distinguishing feature compared to many developments made around IFA antennas. The small ground plane helps getting omnidirectional properties but contributes to reduce the antenna bandwidth quite significantly.

An IFA antenna was chosen as basic structure because it is a well known and flexible element, especially for miniaturization [1]. Due to size constraints, antenna miniaturization was firstly investigated. Among the numerous possible techniques, we have chosen a physical modification of the structure by bending the conducting strip (Fig. 1) in order to limit the bandwidth reduction.



Figure 1: Antenna location on the helmet (left) and antenna geometry with its parasitic element (right).

Nevertheless, a bandwidth enlargement technique has been investigated to cover the required frequency band. The

developed technique consists in duplicating the folded IFA structure and connecting the two antennas by a metallic strip, as described in Fig. 2. The presence of metal strip is necessary because of the difficulty to electromagnetically couple the folded resonators. Such antenna structure introduces two coupled resonances with two possible impedance-matched frequency bands. Based on a parametric study, the geometrical parameters settings associated with the two resonances have been optimized to enlarge the operating bandwidth of the antenna. As shown in Fig. 2, two contiguous bands are allowed to multiply by 4 (40 MHz) the antenna bandwidth compared to the single IFA configuration.



Figure 2: Comparison between measured and simulated reflection coefficient (left), measured gain pattern in horizontal cut plane (right).

The antenna position was optimized at the back of the fire fighter helmet as seen in Fig. 1. Radiation measurements of the final prototype, carried out using a human phantom equipped with the helmet, provide omnidirectional radiation properties (Fig. 2). The total absolute gain is superior to 0 dBi in all directions (horizontal plane) and the maximum gain is 2.2 dBi. An antenna efficiency of 85% was obtained despite its compact dimensions. It has been verified that shadow effect due to helmet (metallic) and user head is not significant at these wavelengths.

A miniature Inverted-F parasitic Antenna printed on thin dielectric substrate has been developed and designed over a compact ground plane. The parasitic technique provides a bandwidth widening of 4 times compared to the original structure. Radiation performances are correct with a total efficiency about 85%. This antenna structure has been optimized in its operating context (helmet + user head) and measurements have confirmed the good behavior in real operation situation.

#### **References:**

[1] O. Roncière, C. Delaveaud. and R. Lionti, "A parasitic technique for miniature IFA bandwidth enhancement", the 15<sup>th</sup> International Symposium on Antenna Technology and Applied Electromagnetics (ANTEM 2012), 25-28 June 2012, Toulouse, France.





#### Research topics: wireless body area networks, medium access control

G. Corbellini, C. Abgrall, E. Calvanese Strinati, A. Duda (CNRS Grenoble)

ABSTRACT: Energy consumption is one of the main challenge in wireless sensor networks to ensure a long battery life to devices that may be deployed in harsh environments once for all without human interaction. A simple probabilistic analysis of the energy consumption in preamble sampling MAC protocols is proposed and the analytical results are validated with simulations. We compare the classical MAC protocols (B-MAC and X-MAC) with the protocol LA-MAC. Our analysis highlights the energy savings achievable with LA-MAC with respect to B-MAC and X-MAC. It also shows that LA-MAC provides the best performance in the considered case of high density networks under traffic congestion.

Wireless sensor networks have recently evolved to support diverse applications in various and ubiquitous scenarios. Reducing energy consumption is one of the main design goals along with providing sufficient performance support for target applications. The overall energy budget is mainly due to the radio; Medium Access Control (MAC) methods play then a key role in saving energy because they schedule the different states of the radio of all devices. Thus, the main goal in designing an access method consists in reducing the effects of both idle listening during which a device consumes energy while waiting for a transmission and overhearing when it receives a frame intended to another device.

To save energy, devices aim at achieving low duty cycles: they alternate long sleeping periods (radio switched off) and short active ones (radio switched on). As a result, the challenge of MAC design is to synchronize the instants of the receiver wake-up with possible transmissions of some devices so that the network achieves a very low duty cycle. In the literature, two kinds of MAC methods are proposed. The first ones are synchronous methods where devices have a common sleep/wake-up schedule. These methods perform well but are not easily applicable and scalable because of the exchange of synchronization messages. Then, we prefer to consider preamble sampling methods with which each device transmits before each data frame a preamble long enough to ensure that intended receivers wake up to catch its frame.

In [1], we compared two preamble sampling methods from the literature, namely B-MAC and X-MAC, with LA-MAC presented in [2], in terms of energy consumption. These three methods define different sleep/wake-up schedules so that the radio of each device is switched on more or less longer. Overhearing may also be avoided or reduced by efficient radio schedules. We derive an analytical and statistical evaluation of the time spent by each device in all the different states of the radio, namely transmission, reception, polling (listening for any radio activity on the channel) and sleeping [3]. Each state is characterized by a different level of consumed energy. Energy consumption is derived according to the number B of buffered messages that must be sent by a group of devices. The higher the number of buffered messages, the higher the congestion is. Then collisions are more frequent, devices are switched on for longer periods, messages may be lost (reduced delivery ratio), latency increases, and energy is wasted.

Fig. 1 shows how LA-MAC permits to reduce the energy consumption of the network when B increases in comparison

to both X-MAC and B-MAC methods thanks to a more efficient schedule of sleep and wake-up periods that also minimizes overhearing. Analytical results are also validated by numerical simulations.



Figure 1: Energy analysis and numerical simulation vs. the buffer size.

Since devices are also constrained by latency requirements, we also numerically evaluated latency versus the number of buffered messages (Fig. 2). We note that LA-MAC allows delivering messages faster than B-MAC and X-MAC, even in case of congestion.



Figure 2: Average latency vs. the global message buffer.

Results highlight the energy savings achievable with LA-MAC with respect to B-MAC and X-MAC. It also shows that LA-MAC provides the best performance in high density networks under traffic congestion.

#### **References:**

 G. Corbellini, C. Abgrall, E. Calvanese Strinati, A. Duda, "Energy evaluation of preamble sampling MAC protocols for wireless sensor networks", IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communications (PIMRC), 9-12 Sept. 2012, Sydney, Australia, pp. 387-392.
 G. Corbellini, E. Calvanese Strinati, A. Duda, "LA-MAC: Low-latency asynchronous MAC for wireless sensor networks", IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communications (PIMRC), 9-12 Sept. 2012, Sydney, Australia, pp. 380-386.
 G. Corbellini, C. Abgrall, E. Calvanese Strinati, A. Duda, "Technical Report: Energy Evaluation of Preamble Sampling MAC Protocols for Wireless Sensor Networks," [Online] available at: http://hal.archives-ouvertes.fr/hal-00627873/. • Annual Research Report > 2012 • Annual Research Report > 2012 • Systems and Solutions • Systems Integration

# Dynamic Management of Cooperative Communications in Body Area Networks

#### Research topics: wireless body area networks, medium access control

M. Maman, A. Di Paolo (University of Bologna), R. Rosini, R. D'Errico

ABSTRACT: A well designed communication scheme managed by an efficient Medium Access Control (MAC) protocol can significantly prevent from the waste of energy in Body Area Networks (BAN). This design needs to know how the channels between the on-body nodes evolve during the human movement. In this study, the impact of cooperative mechanisms on MAC protocol is evaluated in terms of end-users Quality of Service (QoS) and energy consumption based on measured time-variant BAN channels at 2.45 GHz. A dynamic and efficient management of cooperative strategies based on beacon reception information is proposed.

BAN is a Radio-Frequency (RF) based networking technology that interconnects tiny nodes with sensing capabilities placed in or on the human body. The wireless nature of the network, the wide variety of sensors and their wide range of possible applications (medical, sport, entertainment, etc.), offer numerous new research challenges to improve Quality of Service (QoS). Radio front-end is a major source of power consumption of the sensors in a BAN. A well designed communication scheme managed by an efficient Medium Access Control (MAC) protocol can significantly prevent from the waste of energy in the network.

The goal of this study is to investigate innovative relaying and routing mechanisms for BANs under realistic radio channel and mobility conditions. A time-variant on-body channel measurement campaign was carried out at CEA-LETI to investigate the topology dynamics and the performance of relaying mechanisms in BANs [1].



Figure 1: Full-mesh body area network measurement campaign.

In this study, we considered the node 3 (left hip) as the coordinator. In a star topology, we can distinguish the most reliable links (e.g. hip-shoulder, hip-thigh or hip-wrist), from those under-performing (e.g. hip-ear and hip-back). Thus, we can consider nodes 1 (wrist), 2 (thigh) and 5 (shoulder) as relays to improve the performance of under-performing links. The aim of the cooperative approach is to satisfy the performance requirements for any link at any moment.

Concerning the MAC/Network protocols, we considered the BATMAC protocol, which is an IEEE 802.15.4 beacon-enabled

based TDMA MAC protocol. Dynamic relaying mechanisms based on beacon reception feedback are proposed to ensure energy efficiency, low latency and high data delivery ratio. Cooperative schemes counteract shadowing effects but generally need more energy than direct communication. The wisest strategy should use cooperative communication only when necessary keeping a good compromise between performances and energy consumption. Different cooperative approaches are used: Direct (DL), double hop (DH), combined (i.e. both DL and DH) and MIX (i.e. dynamic & smart selection of the previous approaches [2]). In MIX scheme, each node selects, thanks to a PER threshold, the most suitable strategy reinforcing the weakest links, respecting the QoS requirements and with the least amount of energy consumption. If a node receives a beacon directly from coordinator in good condition, it can send its data using the DL scheme. Otherwise, it elects the best relay and the cooperative scheme satisfying the QoS.

In order to evaluate the impact of the channel characteristics, we compared an ideal case in which the beacon and data packets experience the same channel conditions with a realistic case including time-variant fast fading variation.

In Fig. 2, we analyze the trade-off between the performance and the energy consumption for different strategies and as a function of different PER threshold when the MIX strategy with best relay is considered. We show that MIX strategy with best relay allows achieving a better compromise than that obtained using a simple static cooperative strategy.



Figure 2: Performance vs energy consumption in realistic cases for the hip-back link.

The innovation in our investigation is to implement an intelligent and dynamic selection, both for strategies (direct, double hop and combining) and relay, for each packet transmission, in order to have the best performance for heterogeneous body movements and scenarios.

#### References :

R. D'Errico, R. Rosini, M. Maman, "A Performance Evaluation of Cooperative Schemes for On-Body Area Networks Based on Measured Time-Variant Channels," IEEE International Conference on Communications (ICC), 5-9 June 2011, Kyoto, Japan, pp. 1–5.
 M. Maman, A Di Paolo, R. Rosini, R. D'Errico, "Dynamic Management of Cooperative Mechanisms in Body Area Networks", Future Network and Mobile Summit (FUNEMS), 4-6 July 2012, Berlin, Germany.

29



R. D'Errico, R. Rosini

ABSTRACT: Body Area Network channel models have been developed at CEA-LETI. Besides on-body channel models, which have been used to evaluate the system performance, new models for off-body and body-to-body communications are being investigated.

In the last years, CEA-LETI has been working in channel modeling for Body Area Networks. Real-time dynamic onbody channel measurements, performed using two sets of antennas with different polarization [1], were used as input values in a Medium Access Control simulator to describe the propagation channel in some reference scenarios. Network performance was given in terms of Packet Loss Rate (PLR), transmission average delay and node energy consumption, comparing different PHY and MAC protocol solutions. Results demonstrate that protocols should be designed as flexible as possible to fulfill the requirements. Depending on the application, the best solution could be selected in each particular situation and the simulation results presented in [2] could guide this choice. Analysis on the impact of antenna efficiency on the PLR (in or on-body) demonstrates the need to identify a proper trade-off between system performance and antenna dimensions. Some experiments performed using commercially available devices validated the simulation results obtained in terms of PLR and average packet transmission delay. Moreover, channel measurements have been employed for relay approach investigations [3] as well as for UWB-based on-body localization [4].



Figure 1: Off-body channel characterization.

BANs can be also extended to scenarios other than on-body communications. We refer to body-to-body channels when the communication takes place between at least two human subjects, wearing different BAN, free to move relatively to each other in the environment, whereas off-body communications occur when one of the end point of the channel is represented by an external fixed device e.g. a gateway or a router. Channel models for off-body and bodyto-body scenarios were extracted starting from indoor realtime measurements at 2.45 GHz recently performed at CEA-LETI (Fig.1), and the results were presented in [5] and [6].

The models are given as composed of a mean channel gain and a fading contribution. The body shadowing effect was also evaluated, considering the orientation of the human body (Fig.2). To account for the antenna impact on channel characteristics, all the acquisitions were repeated using two different sets of antennas. The presented results show that the mean channel gain is strictly related to the specific node emplacement (relative position of the transmitter and the receiver) and to the antenna type considered. In particular, normally-polarized antennas yield to higher channel gain in NLOS conditions, with respect to tangentially oriented antennas, because of the higher diffraction around the body characterizing the former antenna type. The fading contribution, which accounts for the body movement and the effect of the surrounding environment, was modeled by a Nakagami or Rice distribution.



Figure 2: Body-to-body channel gain (left). Body shadowing in offbody communications (right).

These channel models are now being extended to take into account their space-time correlation properties.

#### **References** :

 R. Rosini, R. D'Errico, "Comparing On-Body Dynamic Channels for Two Antenna Designs", Loughborough Antennas and Propagation Conference (LAPC), 12-13 Nov. 2012, Loughborough, UK (BEST STUDENT PAPER).
 R. Rosini, F.Martelli, M.Maman, R. D'Errico, C. Buratti, R. Verdone, "On-Body Area Networks: from Channel Measurements to MAC Layer

 [2] R. Rosini, F.Martelli, M.Maman, R. D'Errico, C. Buratti, R. Verdone, "On-Body Area Networks: from Channel Measurements to MAC Layer Performance Evaluation", 18th European Wireless Conference, Poznan, Poland, 18-20 April 2012, pp. 1-7.
 [3] M. Maman, A. Di Paolo, R. Rosini, R. D'Errico, "Dynamic Management of Cooperative Communications in Body Area Networks", Future

 <sup>[3]</sup> M. Marian, A. Di Paolo, R. Rosini, R. D'Errico, "Dynamic Management of Cooperative Communications in Body Area Networks", Future Network & Mobile Summit (FUNEMS), 4-6 July 2012, Berlin, Germany.
 [4] J. Hamie, R. D'Errico, B. Denis, "Empirical Modeling of Intra-BAN Ranging Errors Based on IR-UWB TOA Estimation", 7th International

 <sup>[4]</sup> J. Harnie, R. D'Errico, B. Denis, "Empirical Modeling of Intra-BAN Ranging Errors Based on R-OWB TOA Estimation", 7th International Conference on Body Area Networks (Bodynets), 24-26 Sept. 2012, Oslo, Norway.
 [5] R. Rosini, R. D'Errico, "Off-Body Channel Modelling at 2.45 GHz for Two Different Antennas", 6th European Conference on Antennas and

Propagation (EUCAP), 26-30 March 2012, Prague, Czech Republic,, pp.3378-3382.

<sup>[6]</sup> R. Rosini, R. D'Errico, R. Verdone, "Body-to-Body Communications: a Measurement-based Channel Model at 2.45 GHz", IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Sydney, Australia, 9 - 12 September 2012.



#### Research topics: wireless body area networks, propagation channel, miniature antennas

R. D'Errico, R. Rosini, L. Huitema, C. Delaveaud

ABSTRACT: The propagation channel in Body Area Networks is strongly dependent on the antenna topology, which shows different behavior when placed on the body. Antenna-channel joint effects have been investigated for body-centric applications, resulting into a novel approach for radio channel modeling.

Recently, Body Area Networks (BANs) have been gaining a growing interest from both the academia and the industry, due to the huge number of possible applications in which they could be involved, from medical to entertainment.

For the development of such wireless networks, a deep knowledge of the propagation channel is needed for system performance evaluation and design, which is affected by the antenna characteristics on the body. On the other hand, the antenna development needs to take into account the propagation channel phenomena, to properly and efficiently design the radiating element. An antenna-channel joint modeling approach has been used for different applications in body-centric communication.

A miniature active dipole antenna for hearing-aid applications has been designed to study the radiofrequency link between ears [1]. Its good antenna polarization properties, in spite of its compact size, allowed an investigation of antenna polarization effect on the radio channel. Simulations with a SAM phantom and a dielectric sphere have shown that the orientation of electric field normal to head surface can improve the budget link by 10 dB, even when the antenna is positioned inside the ear. Given the low antenna efficiency due to miniaturization, the antenna location and orientation inside the ear plays an important role on the radio channel characteristics (Fig. 1).



Figure 1: Miniature antenna in the ear (left), channel gain for different antenna configurations (right).

The antenna-channel joint effect has been also investigated for dynamic on-body network (Fig. 2). Starting from realtime dynamic measurements at 2.45 GHz, the dynamic channel was modeled by considering two antenna designs: a Top-Loaded Monopole (TLM) and a Planar Monopole (PM) [2]. The former presents a normal polarization with respect to the body surface, while the latter is tangentially oriented. The channel was modeled as composed of three contributions: mean channel gain, shadowing and fast fading. The different behavior of the two antenna sets was analyzed for each channel component. Firstly, TLMs generally present larger mean channel gains with respect to PMs, due to their specific design that favors creeping waves propagation on the body. Moreover, the lack of a ground plane in PMs antenna layout, makes them more affected by the body characteristics than TLMs, with larger values of the mean channel gain standard deviation. The shadowing was modeled by a normal distribution with zero mean and a specific standard deviation, the latter accounting for the body movement. Results show that the specific node position plays an important role on the definition of the antenna behavior, but generally PMs appear to be more influenced by body motion than TLMs, resulting into a larger shadowing. Finally, the fast fading was described by a Rice distribution, with TLMs presenting smaller LCR values and larger K-factors as compared to PMs, because of the enhancement of the on-body creeping waves propagation characterizing normally-polarized antennas, as TLMs are.

These investigations represent a novel approach with respect to the classical channel modeling for BANs. The results have been presented at LAPC 2012 and obtained the Best Student Paper Award.



Figure 2: On-body channel measurements (left) and comparison of channel gain results for two different antenna designs (right).

#### **References** :

 L. Huitema, S. Sufyar, C. Delaveaud, R. D'Errico, "Miniature Antenna Effect on the Ear-to-Ear Radio Channel Characteristics", 6th European Conference on Antennas and Propagation (EUCAP), 26-30 March 2012, Prague, Czech Republic, pp.3402-3406.
 R. Rosini, R. D'Errico, "Comparing On-Body Dynamic Channels for Two Antenna Designs", Loughborough Antennas and Propagation Conference (LAPC), 12-13 Nov. 2012, Loughborough, UK (BEST STUDENT PAPER). Annual Research Report > 2012

# Links Selection Criteria for Enhanced Mobile Terminal Positioning in Cooperative Heterogeneous Networks

#### Research topics: cooperative heterogeneous networks, localization

S. Zirari, B. Denis

ABSTRACT: We consider different links selection criteria and mechanisms to assist the localization of multistandard mobile terminals in heterogeneous wireless networks. One goal is to enable parsimonious and opportunistic cooperation with other mobiles through peer-to-peer links under low power consumption, low latency and low complexity constraints. Specific quality indicators based on approximated theoretical bounds, which optionally integrate asynchronous velocity and location estimates from mobile neighbors, can reliably characterize the instantaneous localization errors along mobile trajectories with varying connectivity conditions.

In the near future, typical indoor environments should comprise heterogeneous wireless resources, such as WiFi Access Points, 3GPP-LTE Femto-Base Stations or even hundreds of wireless sensor nodes. They may be also densely populated by end-users equipped with multi-standard Mobile Terminals (MT) cooperating over short-range peer-to-peer links. In this context, the radiolocation capability has already been identified as a key enabling feature to improve the user's connectivity experience (e.g. through location-based vertical handover) or navigation capabilities.



Figure 1: Example of jointly cooperative and heterogeneous network

In such cooperative and heterogeneous location-enabled networks, one major stake is to exploit the existing infrastructure (i.e. to minimize new deployment costs), while benefitting from low energy consumption MT-to-MT cooperation under mobility. In particular, given a target level of location accuracy, selecting the best -i.e. sufficient- subset of neighbouring MTs in the localization process is absolutely critical.

Our initial proposal [1] was to rely on theoretical positioning performance indicators to make the selection decision, after assessing the actual instantaneous localization errors that could be achieved under partial connectivity. For instance, the Geometric Dilution Of Precision (GDOP) and the Cramer Rao Lower Bound (CRLB) can be approximated, based on location estimates transmitted from the 1-hop neighbours. One first step then consisted in verifying the level of correlation between those raw predictions and the actual errors under realistic connectivity and mobility conditions, in a WiFi/Zigbee heterogeneous scenario (Fig. 2). The resulting nominal selection algorithm, inspired by mono-objective genetic approaches, evaluates and compares the CRLB predictions associated with a limited set of random combinations of neighbors (among all the available ones), till an arbitrarily low localization accuracy threshold is reached and/or a finite number of comparisons has been performed,

hence alleviating the inherent combinatory complexity of exhaustive search procedures. For the sake of reducing even further complexity, the set of selected MTs is assumed valid for a certain timeout. In a more recent version of the algorithm, the asynchronism and the mobility of neighbouring MTs are also taken into account to refine CRLB predictions and dynamically adjust the validity timeout accordingly. Figure 3 provides a simulation-based illustration, still in a WiFi/Zigbee indoor context, showing that localization accuracy is not significantly degraded through links selection (with only three neighbouring MTs) in comparison with exhaustive cooperation.

eti

Systems and Solutions

Current investigations consider coupling this selection technique with adaptive Tx/Rx censorship and medium access schemes to reduce traffic, overhead and latency.









#### References:

[1] S. Zirari and B. Denis. "Comparison of Links Selection Criteria for Mobile Terminal Positioning in Cooperative Heterogeneous Networks". 20th Int. Conference on Software, Telecommunications and Computer Networks (Softcom), 11-13 Sept. 2012, Split, Croatia.



In the recent literature, most of the algorithms aiming at motion capture applications based on Wireless Body Area Networks i) estimate all the unknown nodes' locations simultaneously, after relaying inter-node measurements to a central coordinator, which is hardly compliant with real-time constraints under human mobility; ii) incorporate uniquely non-cooperative measurements with respect to fixed anchors, thus under-exploiting the available potential of mesh topologies; iii) require a priori parametric models incompatible with location-dependent and unpredictable mobility patterns experienced by on-body nodes under arbitrary deployment.

In this context, we have proposed a new Constrained Distributed Weighted Multi-Dimensional Scaling (CDWMDS) positioning algorithm with better suitability within the context of body sensor networks [1]. Accordingly, the nodes' locations are asynchronously updated with respect to their 1-hop neighbors in a body-strapped Local Coordinate System (Fig. 1), providing better immunity against the latency effects observed within classical centralized schemes and better adaptability to local nodes velocities (e.g. in terms of refreshment rate).



Figure 1: Typical scenario for the relative localization of on-body wireless nodes (grey circles) with respect to a body-strapped Local Coordinate System (LCS) (red circles).

Advantageously, this algorithm can be fed with cooperative peer-to-peer distance measurements in a mesh network topology, for instance based on Ultra Wide-Band (UWB) Time of Arrival estimation (TOA). Among all the available radio links, those that experience fixed lengths despite body mobility (e.g. between the hand's wrist and the elbow) can be set as self-learnt (or a priori) geometrical constraints, limiting the number of required on-line measurements and hence, reducing the amount of over-the-air traffic and power consumption. While updating the estimated locations of onbody nodes, we also take into account the latest estimates history as prior information to benefit from space-time correlations under body motion. Finally, new scheduling and censoring rules have been proposed [2] to prevent from error propagations among cooperative nodes. The idea is to limit the impact of the most penalizing nodes located at the body periphery, which experience the highest velocity/speeds and the poorest conditions in terms of geometric dilution of precision and neighborhood connectivity.

Assuming realistic UWB TOA-based ranging error magnitudes derived from [3] as well as realistic medium access constraints, the obtained average Root Mean Square Error affecting estimated nodes' locations show for instance (Fig. 2) i) benefits from fixed-length constraints in comparison with an unconstrained solution (blue bars), whatever the considered node, ii) no significant degradations after self-learning the fixed-length distances, e.g. during a pre-calibration phase (green bars) in comparison with a genius-aided introduction of exact fixed-length distances (red bars) iv) remaining limitations caused by the most demanding nodes (i.e. nodes #6 and 4), thus justifying the new approach in [2].

More recent investigations consider extending our CDWMDS algorithm within a global 2-step localization approach adapted to heterogeneous WBAN networks, incorporating also off-body links with respect to fixed infrastructure anchors. The idea is to enable absolute on-body nodes' positioning at the building scale with similar precision levels (i.e. reconciling motion capture and personal navigation).





References:

[1] J. Hamie, B. Denis, C. Richard, "Constrained Decentralized Algorithm for the Relative Localization of Wearable Wireless Sensor Nodes", IEEE Sensors Conference, 28-31 Oct. 2012, Taipei, Taiwan.

[2] J. Hamie, B. Denis, C. Richard, "Nodes Updates Censoring and Scheduling in Constrained Decentralized Positioning for Large-Scale Motion Capture based on Wireless Body Area Networks", 7<sup>th</sup> International Conference on Body Area Networks (BodyNets), 24-26 Sept. 2012, Oslo, Norway.

[3] J. Hamie, B. Denis, R. D'Errico, C. Richard, "Empirical Modeling of Intra-BAN Ranging Errors Based on IR-UWB TOA Estimation", 7<sup>th</sup> International Conference on Body Area Networks (BodyNets), 24-26 Sept. 2012, Oslo, Norway.



ABSTRACT: the current development of portable wireless devices leads to significant challenges on the design of miniature antennas. For the last sixty years, investigations on antenna miniaturization mainly focused on preserving a high radiation efficiency and bandwidth. A new research topic at CEA-Leti aims to design small antennas with specific radiation pattern requirements. The radiation of a small antenna can be distributed over multiple elementary electric and magnetic radiating sources. An example of multi-modal electrically-small antenna is demonstrated. New optimization opportunities of compact antenna radiation may be extrapolated.

In 1941, Stratton was the first to set basis functions for the expansion of electromagnetic field over planar, cylindrical and spherical scattering surfaces. Stratton's spherical expansion, known as the Spherical Wave Expansion (SWE), is a general formulation to describe a radiation pattern of an antenna by using a set of orthogonal functions over a spherical surface. Therefore, SWE is a powerful tool in antenna's investigation areas; a radiation pattern can be fully described with a set of coefficients applied to SWE. This approach has been used to analyze the radiation properties of compact antennas.



Figure 1: Electrically small antenna for 868-MHz ISM band (antenna size:  $1.5 \times 3$  cm<sup>2</sup>).

Fig. 1 presents an electrically small antenna [1]. This prototype has been designed at CEA-Leti for wireless sensor network application at ISM 868-MHz band (FP7 CHOSeN project).



Figure 2: Gain pattern (dBi); vertical (right) and horizontal (left) polarization.

The radiation pattern of the antenna has been measured in anechoic chamber using a specific non-intrusive method to confirm simulation results. The 3D gain pattern is presented in Fig. 2 for both vertical and horizontal polarization of the electric field. We can observe that the radiation properties are not a classical dipole-like pattern because of positive gain in z-axis direction and a significant part of the radiated power along the horizontal polarization.

Then the radiation properties are analyzed with SWE. A dedicated numerical tool has been developed to extract SWE decomposition. From this analysis, we have identified different spherical modes which are radiated by the electrically small antenna. The results are presented in Tab. 1.

Table I: SWE of the small antenna radiation (868 MHz).

Modes	Power	Phase	Equivalent source
<b>TM</b> <sub>10</sub>	-3 dB	8°	z-oriented electric dipole
$TE_{1\pm 1}$	-3.76 dB	-98°	x-oriented magnetic dipole
<b>TM</b> <sub>1±1</sub>	-11.5 dB	8°	y-oriented magnetic dipole

From the SWE, three main modes are radiated by the small antenna [1]. The excitation of each of these modes is assessed with amplitude and phase. These modes have some equivalent elementary radiating sources which are presented in Tab. 1. From the radiation point of view, the electrically small antenna can be modeled as an electric dipole with zaxis orientation and a magnetic loop orthogonal to x-axis; these two primary equivalent radiating sources are excited with almost balanced power and phase quadrature. The results of this analysis can be confirmed by an analysis of the geometric structure of the antenna and currents distribution.

SWE allows the analysis of the radiation properties and model of an antenna by means of equivalent elementary radiating sources. With this tool, we can observe multiple modes even from electrically small antennas. In future investigations, SWE will be used to carry out optimization of radiation properties with compact antenna geometry.

#### References:

[1] K. Belmkaddem, L. Rudant. and T.P. Vuong, "Electrically Small Antenna Analysis using Spherical Wave Expansion", 15<sup>th</sup> International Symposium on Antenna Technology and Applied Electromagnetics (ANTEM 2012), 25-28 June 2012, Toulouse, France.

Annual Research Report > 2012 Annual Research Report > 2012 Annual Research Report > 2012 Annual Research Report > 2012

# Integrated Antenna Array for Millimeter-Wave Short-Range Communications

#### Research topics: integrated antennas, millimeter-wave communications

L. Dussopt, H. Salti, Y. Lamy, C. Dehos, P. Vincent, S. Joblot (ST), J-F. Carpentier (ST)

ABSTRACT: A 60 GHz cavity-backed antenna array integrated on high-resistivity silicon was demonstrated. The antenna design makes use of Through-Silicon-Vias (TSV), silicon micromachining, and wafer-to-wafer bonding to meet the bandwidth and radiation gain requirements for short-range multi-Gbps communications. Simulated and experimental results show that the antenna element covers easily the 57-66 GHz standard band with good impedance matching and more than 5 dBi of gain. Several fixed-beam four-element antenna arrays demonstrate the capabilities for beam-steering across a range up to  $\pm 60^{\circ}$ .

The 57-66 GHz band is mainly dedicated to very high datarate applications, such as uncompressed video transmission, fast data downloading, or wireless local or personal area networks (WLAN, WPAN). At such high frequencies, transmission-line and interconnection losses require antennas to be integrated as close as possible to the RF transceiver front-end for an optimal budget link. Likewise, the limited output power of CMOS power amplifiers requires the use of directive antenna arrays and beamforming schemes to reach communication ranges of a few meters. To date, the integration of such antenna arrays at 60 GHz in a low cost System-on-Chip (SoC) or System-in-Package (SiP) remains a technical and economical challenge.





Figure 1: Photograph of a single antenna element (a) and a 1x4 antenna array (b).

SiP integration on silicon is an attractive option to benefit from the good thermal properties of this material (CTE, heat dissipation), the collective fabrication facilities for costeffective high-volume production, the fine design rules for a high integration density and very good reproducibility, and the perspective of embedded passive components. A folded-dipole antenna has been designed and demonstrated on a silicon interposer technology composed of a two-metallayers back-end, through-silicon vias (TSV), a one-metal redistribution layer, and a micromachined back-side cavity [1]. The antenna is fed through a CoPlanar Stripline (CPS) quarter-wavelength transformer associated to a CPSmicrostrip balun and a microstrip t-line (Fig. 1). The antenna is backed by a metallized cavity and is surrounded by a  $2.3 \times 2.2$  mm<sup>2</sup> metallic ring connected to the metallic backplane with TSVs.

The impedance and radiation characterizations of the antennas were performed on individual diced samples with a custom measurement set-up allowing RF-probe feeding of the antenna with minimum parasitic radiation scattering and installed in an anechoic chamber. The reflection coefficient of the antenna is lower than -10 dB from 56 to 67 GHz and its gain is 5.4-7.8 dBi at 57-66 GHz.

Four different  $1 \times 4$  antenna arrays, with 2.5 mm interelement spacing, were designed and fabricated in order to demonstrate experimentally the beam-steering capabilities of this antenna and integration technology. The experimental radiation patterns (Fig. 2) are in excellent agreement with the simulations in terms of gain, beamwidth and side lobe levels.

The future work will focus on the integration of a CMOS RF transceiver on the interposer, the packaging and the demonstration of a fully functional transceiver module.



Figure 2: Experimental radiation patterns at 60 GHz of arrays with beams steered at 0°, 20°, 40° and 60°.

#### **References** :

[1] L. Dussopt, Y. Lamy, S. Joblot, J. Lantéri, H. Salti, P. Bar, H. Sibuet, B. Reig, J-F. Carpentier, C. Dehos, P. Vincent, "Silicon Interposer with Integrated Antenna Array for Millimeter-Wave Short-Range Communications," IEEE MTT-S Int. Microwave Symp., 17-22 jun. 2012, Montreal, Canada.

35



ABSTRACT: UWB semi-passive RFID systems are being developed by CEA-LETI in the framework of the European project SELECT. To design and evaluate the system performance, the UWB backscattering propagation channel has been characterized and modeled.

In recent years, a significant number of industrial realities have moved towards the so-called supply chain management

(SCM) approach, relying on the administration of the various logistics aspects of the company. One of the main requirements of the SCM approach is the visibility of the goods along the chain. More precisely, it is necessary to know what a given object is (the who question), and where it can be found (the where question) at a given instant in time (the when question).

In the framework of the FP7 European project SELECT, CEA-LETI is working on the development of passive or semipassive UWB-UHF RFID systems. The objectives of this project are: (a) to develop a new-generation Ultra-Wideband (UWB)-based, semi-passive, low-cost tag compatible with UHF-RFID standard; (b) to design an UWB real-time location system (RTLS) based on such tags, capable of offering submeter location accuracy.

The key technology of this system is the UWB backscattering modulation enabling localization features. In addition to UWB, an UHF signal is employed to ensure compatibility with RFID systems at 868 MHz, and to enable the tag wake-up for minimizing battery consumption and improve synchronization.

Extensive measurement campaigns have been carried out to characterize the antenna backscattering channel impulse response and the clutter impulse response [1]-[2] (Fig. 1). Two different wideband channel models have been proposed, based on a modified Saleh-Valenzuela model. In particular, the backscattering channel model proposes a distance dependent decay factor, and a saturation model for the mean value of the number of multi-path components. The path loss exponent, as well as the delay spread, is twice the typical values for the classical "one-way" channel. The characteristics of the backscattered channel strongly depend on the tag antennas employed, which have been considered in the model [3]. Moreover, the channel modeling requires the inclusion of the polarization distribution information, since the tag can be arbitrarily oriented [2].

The models (Fig. 2) have been implemented and employed to evaluate the localization and tracking performance in different scenarios [4]. Results take into account the hardware limitations, channel measured data, and interferences, showing that the system is able to provide

sub-meter accuracy in localization and tracking for different environments.

The overall system together with the reader and tag architectures are being developed in the scope of the SELECT European project.

In particular, the reader includes two UWB chips, one for the transmitter and the other for the receiver, to realize a quasimonostatic radar configuration, developed by CEA-LETI.

The tag architecture is based on three different chips connected to a UHF-UWB co-located antenna. The first one operates in the UHF band while the second one is connected to the UWB switch enabling passive backscattering schemes.

On-going works are focusing on the system integration, tests and proof of concept in real environments.









#### **References:**

<sup>[1]</sup> R. D'Errico "An Indoor Backscattering Channel Characterization for UWB Passive RFID Applications", 6th European Conference on Antennas and Propagation (EuCAP), 26-30 March 2012, Prague, Czech Republic, pp.1169-1173.

<sup>[2]</sup> R. D'Errico, J. Keignart, L. Rudant, "Characterization of UWB Backscattering Propagation for Passive Tags Identification and Localization", 7th European Conference on Antennas and Propagation (EuCAP), Gothenburg, Sweden, 8-12 april 2013.
 [3] A. Sibille, Z. Mhanna, M. Sacko, R. Contreras, R. D'Errico, "Channel Modeling for Backscattering Based UWB Tags in a RTLS System with

Multiple Readers", 7th European Conference on Antennas and Propagation (EuCAP), Gothenburg, Sweden, 8-12 april 2013. [4] R. D'Errico, M. Bottazzi, F. Natali, E. Savioli, S. Bartoletti, A. Conti, D. Dardari, N. Decarli, F. Guidi, F. Dehmas, L. Ouvry, U. Alvarado, N. Hadaschik, C. Franke, Z. Mhanna, M. Sacko, Y. Wei, A. Sibille, "An UWB-UHF Semi-Passive RFID System for Localization and Tracking Applications", IEEE RFID-TA Conference, Nice, France, 5-7 Nov. 2012.



Nowadays RFID use-cases, systems and applications, such as e-passports, medical cards, NFC, etc, require the transfer of very large amounts of data almost instantaneously. Data stored on biometric passports are about one hundred kilobytes in size. High resolution medical pictures need several megabytes and media files that could be transferred between two NFC phones may reach ten megabytes. Another example, for card suppliers, is the time to download the operating system into the card (personalization) which becomes today part of the critical path in the production process.

be achieved using a 15-states sequence detector.

For a couple of years, some research centers and major companies have been involved in the development of new technologies to improve the bit-rate of communications between contactless cards and readers [1]. These researches and development works are conducted for both UHF and HF systems.

This work focuses, more precisely, on the physical layer defined in ISO 14443 [2] and its very high bit-rate extension. This standard extension provides communication between a Proximity Coupling Device (PCD, reader) and a Passive Inductive Coupled Card (PICC, card) with bit-rate toward one megabit per second keeping a 13.56-MHz carrier frequency (Fc).

When we increase the data rate, the symbol duration decreases, and the Inter Symbol Interference (ISI) becomes more and more preponderant, making difficult to increase the bit rate. We have worked on advanced signal processing algorithm for VHBR to design robust detectors.

We have studied a MLSE (Maximum Likelihood Sequence Estimator) detector for PSK modulations over non linear channel in a VHBR context. By using a real time testbed (Fig. 1), we have characterized the channel seen by the baseband processor. The channel is no longer linear after the phase comparator making difficult to consider classical equalizer structure. Therefore, we have studied a MLSE detector for a ternary alphabet. It is possible to reduce the number of states of the trellis by taking into account the properties of the phase shift detector.



# Figure 1: Testbed illustration for a 13.56-Mbps VHBR contactless air interface.

Moreover, the case of non linear channel is treated by estimating for each transition state, the channel metrics. We have proposed a particular frame structure for the channel estimation process. Performance of the proposed algorithm using real-time front-end and matlab post-processing has been illustrated. The complexity of the proposed algorithm is discussed and compared to the state of art. Even if the complexity is widely increased compared to a threshold detection, the proposed algorithm seems to be attractive compared to FIR / RLS algorithm in terms of performance and complexity. Eventually, a 13.56-Mbps transmission has been demonstrated. The future work consists in implementing the Viterbi algorithm into the baseband processor to benchmark the real complexity and power consumption of the algorithm.

#### **References** :

[1] J-B. Dore, N. Touati, F. Pebay-Peyroula, "MLSE detector for beyond VHBR contactless air interface", 2012 IEEE Int. Conference on RFID-Technologies and Applications (RFID-TA), 5-7 Nov. 2012, Nice, France, pp. 222-227.



A radiofrequency identification (RFID) tag consists of a small chip with an antenna which is able to automatically identify objects or persons with a remote reader. In the framework of an ISO/IEC 15693 system often dedicated to the logistics of the supply chain from the manufacturer to the checkout of the supermarket, each RFID tag sends a unique identifier. This UID can then be considered as a pointer in a database where data related to the tag and therefore to the tagged item and its owner can be stored. Identification of items in databases and networking of different databases become the basis of the "Internet of things" (Fig. 1).



Figure 1: Internet of Things architecture.

A purpose of the Internet of Things is to track every item, so every tag. It brings privacy issues: if each tag is tracked, each owner may be tracked too. Indeed, the tags can be read by anybody from a 1.5 m distance without the knowledge and the consent of the owner, or the communication can be listened from 3.5–4 m. ISO/IEC 15693 standard does not provide anything to solve this privacy issue; that is why it cannot be used as it is in an "Internet of things" context. Moreover, existing techniques to preserve privacy remain not satisfying: they are heavy and not fully integrated in the standard. Furthermore, a process to transfer ownership securely has to be implemented (to preserve privacy when a customer buys an item, for instance).

Our method is based on two complementary levels of protection [1]: physical and protocol layers.

Concerning the first one, we developed a new device: the RFID noisy reader. Its goal is to prevent from the eavesdropping (unwanted listening) of the communication without modifying the tags but keeping the compatibility with the standards and transferring the load of security in the reader. Actually, it blurs the backward communication channel (tag  $\rightarrow$  reader) by adding some noise when the tag sends responses. Thus, an attacker listening to the communication would obtain a useless signal, while the

**References:** 

reader, knowing the noise characteristics can extract the tag's response (Fig. 2).



Figure 2: Noisy reader

Experiments using the noisy reader and a spying probe (stuck to the tag's antenna) show that with a certain gain on the noise, a window is opened where the reader is able to understand almost 100 % of the frames sent by the tag whereas the spying probe is ineffective (0% of decoded frames).

However, using this device, the forward channel stays unprotected. It means that anybody with a RFID reader could get a tag's UID. That is why we developed a challengeresponse protocol, fully integrated in the ISO/IEC 15693 standard, using random numbers and a lightweight cryptography algorithm (named PRESENT), which makes the tag able to authenticate the reader as secure. This protocol is based on the comparison between two keys: one coming from an owner, and the other contained in the tag. If they are the same, it means the tag's item belongs to the owner, and the UID is sent.



Figure 3: Challenge-response protocol.

We also developed an ownership transfer protocol, implementing the aforementioned one, which permits a secured sale between a customer and a seller. This protocol uses a temporary key, known by both parties, to process the item exchange. Thus, the owner of the tag remains always the only person able to read its UID.

[1] O. Savry, F. Achard, "A cross layer approach to preserve privacy in RFID ISO15693 systems", IEEE RFID-TA Conference, Nice, France, 5-7 Nov. 2012.







Annual Research Report > 2012

# On the Security of UWB Secret Key Generation Methods against Deterministic Channel Prediction Attacks

### Research topics: wireless sensor network, security

#### S. Tmar-Ben Hamida, J-B. Pierrot, B. Denis, C. Castelluccia (INRIA), B. Uguen (INSA)

ABSTRACT: Generating secret keys in mobile wireless networks is considered a challenging problem where a key management infrastructure is not always available. Recent security methods have shown that secret keys can be generated using Ultra Wide Band (UWB) channel properties such as reciprocity and spatial decorrelation. Accordingly, the radio channel responses can be used as common information to derive secret keys shared by legitimate parties. However, novel studies in the field of UWB channel prediction have demonstrated that channel profiles could be reliably inferred using for instance Ray-Tracing tools. This work explores this technique to perform attacks and to evaluate the security of UWB secret key generation methods.

Securing a wireless network is a challenging problem due to the shared broadcast medium that makes it easy to eavesdrop on communication, record and modify transmitted packets by adversaries. Conventional symmetric cryptography is required to establish communication confidentiality. Therefore, a trusted party must be developed to generate and share secret keys. However, such conditions are not usually available for dynamic wireless networks.

The concept for building secret keys from UWB channel responses exploits special properties of the wireless channel such as: the reciprocity and the spatial decorrelation. Electromagnetic theory indicates that in the absence of non-symmetric components, the radio channel responses between any two endpoints are reciprocal during the coherence time and decorrelate rapidly in space. As a consequence, the underlying channel responses can be used as common sources to generate secret keys [1].

These solutions rely on the reciprocity principle, which states that in the absence of interferences and non-symmetric components, both the emitter and the receiver experience the same channel response (CR). This shared information can be used to generate a secret key. In addition, the channel profile decorrelates rapidly in space in multipath radio environments. In fact, for a given emitter, waveforms travel differently from one receiver location to another. As a result, an eavesdropper cannot obtain the same CR and thereafter will be unable to extract the shared key, which guarantees its secrecy. However, in spite of favorable UWB properties, radio CRs can be inferred using existing simulation tools. In the field of radio propagation prediction, significant advances have indeed been achieved for the last past years, and more particularly regarding the site-specific deterministic Ray-Tracing methods. Recent results show that these simulators allow to generate realistic received multipath profiles, which are resulting from superposed 'rays'. The crucial information required for these tools are the transmitter and receiver positions, the waveform feeding the transmit antenna, the antenna angular radiation pattern and the description of the operating environment (e.g. electromagnetic characteristics of surrounding materials, building geometry, etc.). To the best of our knowledge, Ray-Tracing (RT) based attacks have not been considered previously to show the channel based encryption key strength. The aim of this work is to test the security of secret key generation method based on UWB

channel responses against channel prediction attacks. Two scenarios have been considered. First, the attacker tries to derive the emitter-receiver CRs assuming a known receiver location. The second scenario consists in performing a "brute force" attack to determine the most likely receiver location through cross-correlation. For the legitimate parties, we use real UWB channel measurements to generate secret keys. The resulting information is then compared to the attacker keys, which are obtained by simulation using the RT channel prediction tool.

eti

Systems and Solutions



Figure 1: Showroom layout for Ray-Tracing channel prediction showing the attacker, receiver and emitter locations (256 samples for the radio channel responses).

The studied attacks are very complex to perform since they require an important amount of information such as the emitted waveform, the emitter's antenna pattern, the environment layout, the transmitters' locations, etc. Our work demonstrates that the exhaustive UWB radio channel responses cannot be inferred by a third party (especially less significant paths) and, then it is impossible to recover the shared secret keys. The robustness of the novel key generation methods relies on the complexity to reproduce precisely the indoor environment and on the post processing phases (i.e. the quantization and key agreement). However, it is important to recognize that research on the UWB Ray-Tracing simulations are expanding greatly and that using the UWB channel as a mean to generate secret keys can be perilous, especially for narrower bandwidth applications.

#### References :

[1] S. Tmar-Ben Hamida, J.-B. Pierrot, B. Denis, C. Castelluccia, B. Uguen, "On the Security of UWB Secret Key Generation Methods against Deterministic Channel Prediction Attacks," 2012 IEEE Vehicular Technology Conference (VTC Fall), 3-6 Sept. 2012, Quebec city, Canada. Annual Research Report > 2012 Annual Research Report > 2012 Systems and Solutions Systems Integration

# A Unified Formalism for Side-Channel and Fault Attacks on Cryptographic Circuits

#### Research topics: hardware security, fault attacks

B. Robisson, H. Le Bouder, J-M. Dutertre (ENSMSE), A. Tria

ABSTRACT: Security is a very large research area involved in the whole information technology, related to both hardware and software. This work focuses on hardware security, and more specifically on hardware cryptanalysis whose aim is to extract confidential information (such as encryption keys) from cryptographic circuits. Many physical cryptanalysis techniques have been proposed in the last ten years but they always belong to one of those very distinct categories: fault or side channel attacks. In this work, a formal link between these two categories is proposed. To the best of our knowledge, this is the first time that a wide class of attacks is described in such a generic manner.

Since electronic devices with security primitives (such as components "smart cards") are key to secure communications, they are subjected to "attacks". A very important class of such attacks, called physical attacks, is due to vulnerabilities of the integrated circuits that implement these primitives. With the physical access to one of these integrated circuits, the attacker tries either to bypass hardware and software protections to get an unauthorized access to services such as pay-TV, web personal accounts, location, etc. He may also try to recover sensitive information such as cryptographic materials or hardware and software intellectual properties. All these threats share a set of experimental techniques. The first one, called side channel attacks, consists in observing some physical characteristics that are modified during the circuit's computation. The second technique, called fault attacks, consists in modifying the circuit's behavior (with a laser beam or intense electromagnetic fields for example). The third one consists in getting information about the chip design by direct inspection of its structure. This inspection may be performed by using any kind of imaging techniques or by using destructive means such as focused ion beam. Our work aims, first to enhance existing physical attacks or define new ones and second, to design and test the best protections. In this context, three evolutions of physical attacks have been proposed. Even if physical attacks seem very different at first sight, several works have been proposed to describe them with a common formalism. But these works only cover side channel attacks. This work proposes a common framework to both fault and side channel attacks.

In this framework, the first step of such physical attacks consists in collecting data such as power consumption, electromagnetic emissions, inputs (also called plaintexts), outputs (also called ciphertexts), etc. This set of values is called observable data, or observables. On the contrary, the running of a cryptographic algorithm involves data (such as cryptographic keys), that cannot be directly measured by the attacker. These data are called secret data. As they are computed by or emanate from the same circuit, secret data and observables are physically related to each other. Figure 1 represents the start and the end parts of the cryptographic algorithm AES (Advanced Encryption Standard). The observables are in red and small parts (1 byte) of secret keys are noted k0 and k10. The left part of the Figure represents the normal execution of the algorithm and the right part represents the end of the algorithm but modified by the attacker. Two relations used by the attacker to recover the

key are also represented. The first one, in blue, links the plaintext, the key k0 and the power consumption or the electromagnetic emission during the computation of the outputs of the SBoxes (noted "SB"). The second relation, in green, links the plaintext, the key k10 and the result of the faulty computation. Theses relations respectively involve a leakage function and an error function which have, in general no simple mathematical expression. More formally, p = R(f,k,o) denotes the relation that links an observable p (also called the reaction) and a set of other observables o according to the value k of (part of) the secret and some leakage or error functions f (also called physical functions).



Figure 1: Relations between observables and secrets.

The second step of the attack consists in choosing a set F' of models for the physical function f (for example, considering that the leakage function is an Hamming Weight or that the error function is a bit flip) and a set K' of hypotheses for k.

The last step consists in comparing the measured reactions p and the predicted ones p' = R(f',k',o) for all  $f' \in F$  and for all  $k' \in K$ . It appears that p and p' are similar only when the hypothesis k' is equal to the secret value k. By detecting such a similarity with ad-hoc statistical tools, the attacker is able to recover this secret value.

The different parameters of the formalism described above are presented for side channel attack (noted DPA), fault attack (noted DFA) and two combinations of these attacks (noted DBA and FSA). Note that more complex attacks may easily be formalized in the same way.

#### **References** :

[1] B. Robisson, H. Le Bouder, J-M. Dutertre, A. Tria, "A unified formalism for side-channel and fault attacks on cryptographic circuits", 27<sup>th</sup> Conference on Design of Circuits and Integrated Systems (DCIS), 28-30 Nov. 2012, Avignon, France.



#### Research topics: hardware security, fault attacks

R. Lashermes, G. Reymond, J-M. Dutertre (ENSMSE), J. Fournier, B. Robisson, A. Tria

ABSTRACT: Differential fault analysis (DFA) techniques aim at disrupting a cryptographic computation to recover the secret key. Most DFA techniques on the Advanced Encryption Standard (AES) either impose strong constraints on the fault injection process or require numerous faults in order to recover the secret key. This work presents a simple methodology based on information theory which allows to adapt the number of required faults for the analysis to the fault injection process. With this technique, the constraints on the fault model to recover the last round key are considerably lowered.

Since the electronic devices that implement cryptography (such as smart cards) are key components to secure communications, they are subjected to attacks. Among them, fault attacks are a major threat. They consist in disrupting the normal behavior of the algorithm to gain knowledge of the secret values manipulated during a cryptographic calculation. There are numerous ways to inject a fault in a device. Some are quite cheap such as clock or power glitches (i.e. short time underclocking or underpowering). The use of laser beams or electromagnetic pulses are more expensive but efficient to avoid localized countermeasures. Current fault attacks either impose strong constraints on the fault model (i.e. the allowed fault values) or require a large amount of faults. Each fault injected brings the risk to totally destroy the device which would make the attack fail. Attackers are thus interested in minimizing the number of faults needed to recover the secret.

Our goal was to develop a fault analysis method which accept all possible fault models and at the same time find the secret key with the minimum amount of faults. This method has been applied in [1] on an AES, the new standard of symmetric encryption, implemented on a FPGA. The secret data is thus the cryptographic key.

The principle of our method slightly reverse the way the fault analysis is generally performed i.e. it consists in trying to reconstruct the sequence of injected faults as a function of the secret key. Identifying the correct key is now transposed as identifying the sequence of faults that is really injected. For this identification, the non-linear properties of the AES are exploited so that the reconstructed sequence for a wrong key guess is pseudo-random. At the opposite, the correct sequence has an entropy exactly equal to the entropy of the injection means. The lower the injection entropy, the faster it is to identify the injection entropy from pseudo-random entropies (with sequences as short as containing only two elements). Figure 1 represents the entropy of the sequences obtained for different guesses of the key K10, computed on data sets of different sizes. We can see the slow separation of the injection entropy for the correct K10 guess with respect to random entropies. As a consequence, the lower the injection entropy, the less faults are needed to find the secret key. This relation can be seen on Figure 2 which displays the average minimum of faults needed to find the secret key according to the entropy of the injection means. As an example, a single-bit fault injection (entropy = 3)

requires in average 6.4 faults to recover the key.





Figure 2: Required number of faults vs injection entropy.

This work can be extended in different directions: applying the same methodology when the fault occurs at some other location in the AES algorithm, with other AES implementations, with other injections means (optical, EM, etc.). Finally the effects of existing masking schemes shall also be investigated.

**References** :

[1] R. Lashermes, G. Reymond, J-M. Dutertre, J. Fournier, B. Robisson, A. Tria, "A DFA on AES based on the entropy of error distributions.", Fault Diagnosis and Tolerance in Cryptography (FDTC), 9 Sept. 2012, Leuven, Belgium, pp. 34–43.



Surface reconstruction





#### Research topics: magnetic sensor, vehicle re-identification

A. Vassilev, A-C. Pitton, S. Charbonnier (GIPSA-Lab)

ABSTRACT: Vehicle re-identification enables the calculation of travel times and origin-destination matrices. These are key data for modeling and therefore optimizing the traffic flow. This paper compares the performances of different vehicle re-identification methods using the vehicle tridimensional magnetic signature recorded with a single three-axis magnetic sensor. The results obtained on a large data-base of signatures from 25 different vehicles show that the Dynamic Time Warping (DTW) method is able to correctly re-identify 70% of the vehicles with only 6% of false alarms.

One solution to reduce traffic congestion is to optimize the traffic flow. The implementation of dynamic traffic management solutions requires the urban traffic flow to be modeled on-line, which can be done by estimating specific traffic parameters in real time, for example, the Travel Time (TT). This parameter is easy to calculate, provided that it is possible to re-identify one vehicle at different locations.

A competitive solution is the use of magnetic sensors, which do not raise any privacy concern, are rather inexpensive and not sensitive to weather conditions. "Sensys Networks" company sells a system based on these sensors. The reidentification rate reaches 50% in straight line. The aim of our work is to develop novel methods to improve this rate [1].

A data-base of magnetic signatures from 25 different cars was collected in an empty parking lot (Fig. 1).

The signatures (Fig. 2) were measured at a sampling rate of 200 Hz with wireless three-axis magnetic sensors developed by CEA-Leti from AMR sensors of Honeywell.

The vehicles passed over the sensors with different orientations to the North.



Figure 1: Experimental setup



Different methods of vehicle re-identification using the vehicle three-dimensional magnetic signature measured with a single sensor were evaluated.

The best method is by far the Dynamic Time Warping (DTW) method, which measures the difference between the magnetic signatures in the three dimensional space. Links exist between the magnetic fields measured along the three axes, and these links must be taken into account by the similarity measure used.

The results obtained on pairs with the same orientation remain good with on average 84% of true detection (TD) with 3% of error (PE). When the vehicle changed its orientation, the results are slightly worse but remain acceptable with on average 69% of TD for 6% of PE.

It was also shown that the influence of the vehicle orientation to the North on the re-identification performances was limited.

Perspectives are to study the effect of lateral position of the vehicle and to fuse the signals of all the 10 sensors in order to improve the recognition rate.

#### **References** :

[1] S. Charbonnier, A-C. Pitton, A. Vassilev, "Vehicle re-identification with a single magnetic sensor", 2012 IEEE International Instrumentation and Measurement Technology Conference, I2MTC 2012, Graz, Austria, 13-16 May 2012.



# High-Resolution Acoustic Probing, Nano-Membranes Implementation

#### Research topics: nano-sensors, graphene

N. Sridi, J Azevedo (CEA-DSM), B. Charlet (CEA-LETI/DCOS), A. Ghis

ABSTRACT: For high-resolution acoustic probing purpose, we study the experimental implementation of suspended membranes with micrometric area and nanometric thickness. At these dimensions, the properties of the membranes have to be characterized using specific experiments because of the predominance of technological artifacts. We have settled a protocol allowing the prediction of the displacement profile of embedded membranes.

Acoustic probing using micrometric vibrating membranes is the technological challenge we rise up. The micrometric probes will open the way to high resolution ultrasound imaging, for medical or chemical application, and to porosity and pores statistics at the micron scale, for composites, polyphasic materials, cements, foams and yeasts morphological monitoring.

The technical challenges associated to ultrasonic probing with micrometric resolution first addresses the selection of an appropriate membrane material and the associated implementation technology.

The elementary probing device is a capacitively-actuated membrane with a typical size in the micron scale.

To obtain sufficient and detectable vibration of a suspended micrometric membrane, the key parameter is the thinness of the membrane as the amplitude of deflection linearly depends on the inverse of the cube of its thickness. To achieve nanometer range deflection, the suspended membrane is to be nanometer thick.

Once processed and integrated, the mechanical properties of thin films differ from those of bulk material. This may be caused by the fabrication process. Any drift of the mechanical properties affects the electromechanical system behavior through the motion and the resonance properties. In order to predict and compare the performances of the electromechanical system made out of different materials, we consider the bending rigidity D of the suspended membranes. The bending rigidity is an intrinsic property which includes the Young modulus, the Poisson's ratio and the thickness.



Figure 1: • Measurement of the stiffness constant k using an AFM in force mode to apply a punctual load. The bending rigidity of the membrane is deduced considering the membrane topology. • Measurement of the deflection profile under a capacitive electrostatic force, when a voltage is applied between the membrane and the bottom of the cavity. The deflection profile is measured point by point across the suspended area using an AFM in tapping mode.

We determine the bending rigidity of actual membranes using AFM measurements in force mode with a punctual load (Fig. 1). We developed an analytical model together with finite element calculation to link these measurements with the membrane behavior under an electrostatic load, as it is implemented in capacitive actuation. Experimental measurements of the deflection profile of the membrane under electrostatic force have been implemented to check for the validity of our approach and show a good agreement (Fig 2).



Figure 2: Comparison between the measured profile (blue dotted line) and the calculated profile (red line) using the bending rigidity value obtained with punctual load experiments. This profile corresponds to a 1.8 µm wide trench and a 9 V potential applied.

With these tools and models, we entered into technological realizations of suspended micrometric membranes of nanometer thickness using various materials (Fig. 3). Graphene appears as a most suitable 2D material because of its mechanical properties. We then made membranes using graphene through different technologies and multilayer stacking. We made as well silicon membranes as silicon takes benefit of a well controlled technology and integration facility into operational devices. A displacement of several ten nanometers can be achieved with less than ten Volts applied.

Knowing then the membrane behavior depending on the material, we can now design the driving and readout close electronic, and proceed to the fabrication and integration of the membrane into an operational device achieving high resolution acoustic probing at the micron scale.



Figure 3: Left: SEM picture of a graphene oxide suspended layer. The graphene oxide has been deposited using the BDM method developed at IRAMIS. Right: 10-nm thin silicon suspended membrane above a 1- $\mu$ m diameter cavity.

#### References

[1] N. Sridi, B. Lebental, E. Merliot, C.S. Cojocaru, J. Azevedo, J.J. Benattar, A. Nowodzinski, J-C.P. Gabriel, A. Ghis, "Mechanical properties of suspended few layers graphene sheets", Nanotechnology 2012: Advanced Materials, CNTs, Particles, Films and Composites, 18-21 June 2012, Santa Clara, CA.

45



Following our previous work on the reconstruction of surfaces from the Morphosense ribbons, we introduce geometric models of the surfaces so as to perform a more precise reconstruction depending on the type of surface we want to reconstruct. The more the underlying model is constrained, the less the sensor network we are using will need to be complex. In the case of a quasi-developable surface, we can reconstruct it with patches of any number of ribbons. In the even more constrained case of a developable surface (isometric to a plane), we introduced a method using only one ribbon for the reconstruction.

We reconstruct here patches with geodesic boundary curves for quasi-developable surfaces [1]. Methods for patches with n < 5 sides already exist, and we estimate the missing geodesic curves that will subdivide the patches so as to match this case.



Figure 1: Network of ribbons on a quasi-developable surface

The method is initialized by a flattening process approximating a developable surface and the degrees of freedom are then fixed by minimizing the Gaussian curvature of the surface.

In the case of a developable surface, we developed a method allowing the reconstruction of a portion of the surface with only one ribbon [2]. The geodesic ribbon allows the identification of the tangent plane at each point of the curve. Thanks to the envelope of tangent planes, one can identify what type of developable surface components the ribbon crosses (cone, cylinder, tangent developable), so as to segment and reconstruct each component. The method works with exact data but still needs to be adapted to the case of noisy data obtained from the physical Morphosense ribbon.



Figure 2: Reconstruction of a quasi-developable surface (simulation).



Figure 3: Ribbon lying on a developable surface.

#### **References** :

[1] M. Huard, N. Sprynski, L. Biard, N. Szafran, "Reconstruction of quasi developable surfaces from ribbon curves", Numerical Algorithms, Aug. 2012.

[2] M. Huard, N. Sprynski, L. Biard, "Rubans géodésiques pour la segmentation et la reconstruction de surfaces développables", Journées du Groupe de Travail en Modélisation Géométrique (GTMG), 21-22 March 2012, Strasbourg, France.







# Research topics: energy harvesting

B. Ahmed Seddik, G. Despesse, S. Boisseau, E. Defay (CEA-LETI/DCOS)

ABSTRACT: Vibration Energy Harvesting is a promising way to develop fully-autonomous Wireless Sensor Networks (WSN) powered by ambient vibrations. Based on mass-spring resonant architectures, Vibration Energy Harvesters (VEH) have a limited frequency bandwidth and therefore, they must be designed for the environment where they are installed; this greatly limits their adoption by industry. Here is presented a solution to develop wideband VEH using an innovative piezoelectric cantilever structure and its management electronic circuit, enabling the deployment of robust and simple to set up VEH-powered Wireless Sensor Networks.

Vibration Energy Harvesters (VEH) turn ambient vibrations into electricity, enabling the development of fullyautonomous Wireless Sensor Networks. Currently, VEH are based on resonant mass-spring structures and harvest power only if their resonant frequency is tuned to ambient vibrations frequency. As a consequence, VEH have three main drawbacks: (i) they must be designed for their environment; (ii) they can't harvest energy any longer if vibration frequencies change and, (iii) due to mechanical fatigue, VEH resonant frequency may change with time and may not fit ambient vibrations frequency anymore. Therefore, today's VEH are not generic, versatile, robust and simple to set up devices, which greatly limits their mass deployment by industry. Actually, developing generic VEH requires the design of mass-spring structures with a wide frequency bandwidth and/or able to adjust their resonant frequency to ambient vibrations.

The solution we developed [1-3] aims at enlarging the frequency bandwidth by tuning the VEH resonant frequency. Its objective is to change VEH resonant frequency by modifying the stiffness of its spring. One way to proceed consists in changing the electrical load on highly-coupled piezoelectric cantilever structures (Fig. 1a), which has a strong impact on the Young's Modulus of the piezoelectric material and then on the VEH global stiffness. Then, the VEH resonant frequency can be chosen by adapting the load; the higher the electromechanical coupling, the broader the frequency range.

Our solution relies on two innovative elements: (i) a new piezoelectric cantilever shape with an improved electromechanical coupling and (ii) a low-consumption active electronic circuit that maximizes the VEH output power by adapting the load (C1) according to the vibration frequency.



shape.

The standard cantilever piezoelectric energy harvester was improved by a triangular shape (Fig. 1b). Hence, we achieve a quasi-homogenous distribution of the mechanical stress in the piezoelectric layers, maximizing the global electromechanical coupling of the energy harvester. Furthermore, in order to get a higher electromechanical coupling, the piezoelectric material is cut in subparts and is oriented in the 33 mode. A prototype has been manufactured and has shown a resonant frequency change up to 40% (Fig. 2).



Figure 2: (a) Prototype and (b) resonant frequency of the energy harvester as a function of the capacitive load (C1).

The active electronic circuit, which adapts in real time the capacitive load placed at the output of the energy harvester, has also been manufactured; its power consumption is about 50  $\mu$ W. Thanks to this circuit, the energy harvester is able to provide an output power higher than 200  $\mu$ W on a wide frequency bandwidth (230-320 Hz). The net power balance is positive (Fig. 3) and the frequency bandwidth is increased (40 Hz in open loop vs 90 Hz in closed loop), definitely validating this concept.



Figure 3: Power balance – VEH output power as a function of the ambient vibration frequency.

These new energy harvesters and the associated low copresumption electronic circuits are a major advance towards robust and versatile VEH; the power balance is clearly positive and sufficient to power Wireless Sensor Networks.

#### References :

[1] B. Ahmed Seddik, G. Despesse, S. Boisseau, E. Defay, "Strategies for Wideband Mechanical Energy Harvesters", in Small-Scale Energy Harvesting, Intech, 2012.

[2] B. Ahmed Seddik, G. Despesse, E. Defay, "Wideband mechanical energy harvester based on piezoelectric longitudinal mode", 2012 IEEE New Circuits and systems Conf. (NEWCAS), Montreal, Canada, 17-20 june 2012, pp. 377-380.
[3] B. Ahmed Seddik, G. Despesse, E. Defay, "Autonomous wideband mechanical energy harvester", 2012 Int. Symp. on Industrial Electronics (ISIE), Hangzhou, China, 28-31 May 2012, pp. 1122-1127.



Many fields, such as transportation, industry and aeronautics, have a strong interest in developing and using Wireless Sensor Networks (WSN) to increase their productivity, reduce their cost or limit machine downtimes. A WSN node can be represented as a four-box system [1] with sensors, a microcontroller ( $\mu$ C), a RF system and a source of energy (Fig. 1a). Its power consumption depends on its operating modes. A typical example is depicted in Fig. 1b where the node consumes 5  $\mu$ W in standby mode, 1 mW in measurement mode ("on" state) and 50 mW in RF transmission mode.



Figure 1: (a) WSN as a four-box system and (b) power consumption.

Contrarily to batteries, energy harvesting (EH), aimed at converting ambient energy into electricity, can give WSN nodes a theoretical unlimited lifetime. Vibration Energy Harvesters (VEH) are part of EH solutions, aimed at turning ambient vibrations into electricity.

The VEH's basic architecture is a mass-spring system [2], damped by mechanical friction forces and resonating when submitted to ambient vibrations (Fig. 2a). Three main converters enable a mechanical-to-electrical transduction: piezoelectric, electromagnetic and electrostatic devices. Our work focuses on piezoelectric (based on piezoelectric materials [3]) and electrostatic (based on a capacitive architecture [4]) converters (Fig. 2b-2e). Output power levels up to 10  $\mu$ W per gram of mobile mass have been reached with both of these systems. Ambient vibrations (typically 0.1G at 50 Hz for standard vibration) have enabled us to harvest 100  $\mu$ W with small-scale energy harvesters.

Unfortunately, 100  $\mu$ W are not enough to make continuous measurements with WSN nodes (Fig. 1b). A common strategy is the principle of "energy buffering": by adopting an intermittent measurement strategy with a buffer, VEH can become a viable supply source (Fig. 3). The principle is straightforward: the energy harvester extracts power from its environment and stores it into a buffer (capacitor, battery) (Fig. 3a). During this time, the most energy-consuming

devices (µC, sensor and RF emitter) are in standby mode, consuming about 5  $\mu W.$ 



Figure 2: (a) Vibration Energy Harvesters, (b) piezoelectric converter (c) electret-based electrostatic converter, (d) piezoelectric VEH prototype and (e) electret-based VEH prototype.

Measurements (Fig. 3b) and RF emission (Fig. 3c) are performed when enough energy is stored in the buffer, emptying it and making the system return to its standby mode, waiting for a new measurement cycle (Fig. 3d). With such an energy-driven strategy, we demonstated a complete cycle (measurement, data processing, RF emission) with only 50  $\mu$ J. Then, only 10  $\mu$ W are sufficient to power a WSN node (as 5  $\mu$ W are consumed in standby mode), which is compatible with VEH output powers.



A complete WSN node has been designed and uses this energy-driven strategy. This demonstrator proves that only 50  $\mu$ J are required to make a complete measurement; intermittent measurement strategies are then the key to develop ultra-low power WSN, compatible with most of Energy Harvesting sources and in particular with VEH.

**References :** 

S. Boisseau, G. Despesse, "Energy harvesting, wireless sensor networks & opportunities for industrial applications", *EETimes*, 27 Feb. 2012.
 S. Boisseau, G. Despesse, "Vibration energy harvesting for wireless sensor networks: Assessments and perspectives", *EETimes*, 12 April 2012.

[4] S. Boisseau, G. Despesse, B. Ahmed Seddik, "Electrostatic Conversion for Vibration Energy Harvesting", in *Small-Scale Energy Harvesting*, *Intech*, 2012.

<sup>[3]</sup> B. Ahmed Seddik, G. Despesse, S. Boisseau, E. Defay, "Strategies for Wideband Mechanical Energy Harvester", in *Small-Scale Energy Harvesting, Intech*, 2012.



J.J. Chaillout, S. Boisseau, G. Despesse, J.S. Danel (CEA-LETI/DCOS)

ABSTRACT: MEMS open great opportunities for biomedical applications. Reducing size and power consumption, they pave the way to tiny and autonomous medical implants that could greatly improve patients' comfort. Power supply of medical implants is challenging: batteries have limited lifetimes and their replacement imply new surgeries. Energy Harvesting could be the solution to this challenge, enabling medical implants to be powered by the ambient energy provided by the human body itself. Here is presented the research on a new device able to scavenge the vibrations induced by heartbeats and aimed at powering the pacemakers of the future.

Heart diseases are a major and growing public health concern, affecting millions of people and costing tens of billions of dollars each year. Among them, arrhythmias are one of the most common heart disorders but can be quite easily treated with pacemakers. Since the first pacemaker back in 1958, many improvements have been performed making these devices safer and more comfortable. Yet, the pacemakers of the future, relying on Micro-Electro-Mechanical Systems (MEMS) technologies is still to come. Smaller and smarter, these devices will reduce costs and further improve patients' comfort and safety. In fact, size reduction thanks to MEMS devices makes it possible to imagine tiny pacemakers fixed directly on the heart wall (epicardium), limiting the quantity of energy given to the heart at each cycle, paving the way to leadless pacemakers powered by energy harvesting, and solving the problems of leads (which can be hard to place - Fig. 1a) and autonomy at the same time (Fig. 1b) [1].



Figure 1: (a) pacemakers with leads and battery, (b) future pacemaker using energy harvesting.

Yet, since the pacemaker is inserted into the heart, only energy coming from the human body is available. Four ambient sources can theoretically be exploited: radiant mechanical sources. thermal sources, sources and biochemical sources. However, only vibrations and biochemical products are available in the heart, as the body is opaque and thermo-regulated. Extracting energy thanks to biochemistry is generally complicated and especially in the harsh environment of the body, leading to packaging challenges, that are hard to solve (semi-permeable membranes' lifetimes, clogging). On the other hand, heartbeat's vibration energy harvesting offers a great opportunity to develop hermetic systems, not in contact with any human body fluids, and was then chosen by HBS consortium (Sorin Group, Tronics, Cedrat, Easii IC, CEA-LETI, TIMA) as a solution to power Sorin's future pacemakers.

Harvesting energy from vibrations consists in developing mass-spring resonant devices that turn vibrations into a relative movement between two elements (mechanical-tomechanical converter) which is then turned into electricity thanks to a mechanical-to-electrical converter (piezoelectric, electrostatic, electromagnetic devices) (Fig. 2a and 2b).



Figure 2: (a) two-step conversion for vibration energy harvesting and (b) equivalent model of vibration energy harvesters.

We focused our research on electrostatic converters (Fig. 3a) [2], based on a capacitive architecture polarized by an electret (Fig. 3b). The relative movement between the two plates generates a capacitance variation and then electric charges. They are collected by a power management circuit and stored into a capacitor, used as a buffer, powering the pacemaker.



Figure 3: (a) schematic of the energy harvester, (b) electret, (c) prototype and (d) pacemaker powered by energy harvesting.

A first MEMS electrostatic prototype (Fig. 3c) has been manufactured using cleanroom processes. The energy harvester has a total volume of 1 cm<sup>3</sup> and an output power of 10  $\mu$ W is expected to be reached as soon as the pacemaker is implanted into the heart (Fig. 3d).

This research was partially funded by Sorin through the Sorin-LETI joint laboratory.

#### References :

S. Boisseau, J.J. Chaillout, M. Deterre, R. Dal Molin, "Toward pacemakers powered by heartbeats", *EETimes*, 17 Oct. 2012.
 S. Boisseau, G. Despesse, B. Ahmed Seddik, "Electrostatic conversion for vibration energy harvesting", in *Small-Scale Energy Harvesting*, *Intech*, 2012.



# Innovative Devices for Thermal Energy Harvesting

51

#### Research topics: energy harvesting

S. Boisseau, G. Despesse, S. Monfray (ST), O. Puscasu (ST), T. Skotnicki (ST)

ABSTRACT: Thermal energy harvesting is a field of growing interest enabling the development of fully autonomous Wireless Sensor Networks powered by ambient thermal gradients. Here is presented a new concept of thermal harvester using a curved bimetallic strip coupled to an electret-based converter. A two-step conversion is carried out: the curved bimetallic strip converts the thermal gradient into a mechanical oscillation, which is then converted into electricity by an electret-based electrostatic converter. This concept enables low cost designs, semi-flexible concepts and paves the way to mass production over large areas of thermal energy harvesters.

Generally, thermal energy harvesters are based on bimetallic junctions generating a thermoelectric voltage (Seebeck effect) when submitted to a temperature gradient. This concept has long been known and some thermoelectric energy harvesters are already commercialized. Moreover, thermoelectric energy harvesters have quite good conversion efficiencies that may reach up to 10-15% of the Carnot cycle efficiency. Yet, they require quite expensive materials such as bismuth telluride, and developing flexible devices is rather complicated.

Here, an alternative to these standard thermoelectric devices is proposed, relying on a bimetallic strip and an electretbased converter. Actually, bimetals (Fig. 1a) and electretbased converters have long been known, but the idea of coupling them to harvest energy from thermal gradients is new.

Curved bimetallic strips are made of two metals with different coefficients of thermal expansion (CTE) and are used as thermal actuators able to turn temperature changes into a sudden mechanical movement (snapping), involving buckling effects (Fig. 1b).



Figure 1: (a) bimetallic strip and (b) curved bimetallic strip.

Curved bimetallic strips are then capable of switching between two mechanical states according to the temperature with a hysteretic cycle (snapping back and forth).

Therefore, a curved bimetallic strip inserted into a cavity whose lower plate is hot and whose upper plate is cold will turn the thermal gradient between these two plates into a mechanical oscillation (Fig. 2a and 2b).

As for electrets, they are electrically charged dielectrics that can keep their charges for years; they are generally used as a polarization source for electrostatic energy harvesters. Thanks to electrets, electrostatic converters directly turn a relative movement between their two plates into electricity due to conservation of charges and charge influence variation phenomena [1].

**References:** 



Figure 2: (a) heat engine – lower state, (b) heat engine – upper state, (c) electret-based converter and (d) bimetal-and-electret-based converter.

The bimetal-based heat engine is then coupled to the electret-based converter (Fig. 2c), involving a two-step conversion (Fig. 2d): the thermal energy from the thermal gradient is firstly turned into a mechanical oscillation (mechanical energy) by the curved bimetal, which is eventually converted into electricity with the electret-based converter.



Figure 3: (a) rigid prototype showing the different states of the bimetallic strip, (b) semi-flexible concept, (c) bimetallic strip – lower state and (d) bimetallic strip – upper state.

Rigid (Fig. 3a) and semi-flexible devices (Fig. 3b, 3c, and 3d) [2] have been manufactured from various bimetals and various dimensions to adapt the energy harvesters to several ambient thermal gradients.

Experiments showed that, as expected, when a device is placed on a hot source, its bimetal oscillates between the two plates and the electret-based converters turn this mechanical movement into electricity. The snapping frequency is about 1 Hz and the output power is in the  $10-\mu W$  range.

Finally, a power management circuit has been developed to harvest power from multiple devices in parallel; it has been proven that these devices are compatible with WSN powering [3].

 S. Boisseau, G. Despesse, B. Ahmed Seddik, "Electrostatic conversion for vibration energy harvesting", in *Small-scale Energy Harvesting*, Intech, 2012.
 S. Boisseau, G. Despesse, S. Monfray, O. Puscasu, T. Skotnicki, "Semi-flexible bimetal-based thermal energy harvesters", *Smart Materials and Structures*, 2013.

[3] S. Boisseau, G. Despesse, "Energy harvesting, wireless sensor networks & opportunities for industrial applications", EETimes, 27 Feb. 2012.



## Research topics: energy harvesting, power management

P. Gasnier, J. Willemin, C. Condemine, G. Despesse, S. Boisseau, J-J. Chaillout

ABSTRACT: Using ambient energy to supply Wireless Sensor Nodes (WSN) is possible thanks to Energy Harvesting transducers, providing an efficient conversion to an appropriate voltage level. This work presents a fully autonomous Integrated Circuit that efficiently converts the electromechanical transducers' energy into a 3-V supply source compatible with WSNs. The circuit operates with high output-voltage transducers (>60 V) and performs an inductive power conversion (10  $\mu$ w to 500  $\mu$ W) to a storage element (battery or capacitor). The innovative control of the inductive converter and the low power consumption (sub-micro-amp) of the integrated circuit can increase the harvested power (17% gain) or reduce the size of the magnetic component.

With the size reduction of embedded sensors, another challenge of the WSNs community is to develop fullyautonomous Wireless Sensor Nodes. For a few years, the interest in mechanical energy harvesting from ambient environments has increased; indeed, in dusty or dark environments submitted to shocks, stresses or vibrations, mechanical energy harvesting is a relevant candidate to power WSNs. Actually, many ways to convert mechanical energy into electricity exist; the most commonly used principles are piezoelectricity [1], electrostatic [2] and electromagnetism.

Here, we focus on the conditioning and the control stages that convert the energy from electrostatic and piezoelectric harvesters (High Voltage and AC) into an appropriate supply source (3 V DC).

This work performs the discharge of the harvester in coupled inductors when the harvestable energy reaches its maximum, i.e. when the output voltage of the energy harvester is maximal. A flyback topology is used, performing an efficient power conversion from high-output-voltage (> 60 V) transducers to low voltage (3 V) energy storage elements.

The innovative point of this work consists in discharging the electric energy by using multiple magnetic transfers (called "multi-shots"). This strategy enables to reduce the size of the magnetic circuit or to increase the efficiency of the power conversion [1]. Fig. 1 compares the synchronous discharge of a piezoelectric harvester using the one-shot and the multi-shots strategies: a gain between 15% and 20% is demonstrated with this technique.





A fully autonomous and self-starting integrated circuit was

designed in the standard voltage AMS0.35 CMOS technology and is currently being tested. The integrated circuit (called "EPHIC" : Electrostatic and Piezoelectric Harvesting Integrated Circuit) carries out two main functions:

- the energy transfer when the piezoelectric/electrostatic output voltage reaches a maximum through a maximum voltage detector. This function is implemented thanks to a derivation of the piezoelectric/electrostatic output voltage and with an ultra-low-power comparator.
- the control of the external power switches through an accurate and tunable pulse generator to implement the multi-shots strategy.

The architecture of the whole system (the Flyback, the ASIC and the storage elements) is depicted in Fig. 2a. The integrated circuit uses a non-optimized path to self-start and the Flyback path to efficiently extract electricity from the energy harvester.

Simulation results have shown a power consumption of the circuit below 2  $\mu$ A (@3V) which contributes to improve the power conversion efficiency. Fig. 2b shows a micrograph of the chip which implements both digital and analog functions.



Figure 2: (a) Power circuit architecture and (b) die of the chip.

An innovative multiple magnetic transfer strategy has been experimentally validated. A 15% increase of the energy transfer (compared to the classical single transfer strategy) has been measured. A low power integrated circuit has been designed and fabricated. This chip controls the Flyback topology and performs the novel multi-shots strategy. Moreover, this system is fully autonomous, self-starting and efficiently converts power (10  $\mu$ W to 500  $\mu$ W) from high-output-voltage harvesters to low voltage storage elements required to supply WSNs.

#### **References :**

 P. Gasnier, J. Willemin, J.-J. Chaillout, C. Condemine, G. Despesse, S. Boisseau, G. Gouvernet, and C. Barla, "Power conversion and integrated circuit architecture for high voltage piezoelectric energy harvesting," 2012 IEEE New Circuits and Systems Conference (NEWCAS), Montreal, Canada, 17-20 Jun. 2012, pp. 377 –380.
 S. Boisseau, G. Despesse, and B. Ahmed, "Electrostatic conversion for vibration energy harvesting," in Small-Scale Energy Harvesting, InTech, Oct. 2012.



ABSTRACT: a detection system of electric arcs generated by connector faults in a battery was developed. The principle is based on the detection of acoustic emissions from the arcs. The approach was firstly to identify the acoustic signature of an electric arc as well as disturbances in the environment of detection. Subsequently, we investigated the propagation of acoustic waves emitted by the arc in the confined environment of the battery. Finally, we proposed several detection methods whose performances were evaluated. A demonstrator has been realized and validated the performances of the detection.

The battery of an electric vehicle (EV) is made of several cells arranged in series and in parallel. The connections between these cells may be damaged or broken (because of aging, shocks or vibrations), which may result in maintained electric arcs because of DC current flowing into the battery. Thus, these arcs can cause overheating and even thermal runaway in the battery, which can lead to dangerous fires. Because of the transient signals present on the voltage and current measurements made on the battery, we chose to focus our work on the acoustic emission of electric arcs to detect them as soon as they start and prevent possible thermal runaway [1].

The physical process that starts an arc is a broken contact. When a connection between two cells is broken, an electric discharge begins in the space between electrodes. The majority of the power of the wave is released into the air and a negligible portion of the wave created at the arc feet will propagate into connectors and cells. As an example, Figure 1 presents a typical time acoustic signal produced by an arc and its frequency spectrum.



Figure 1: Time and frequency acoustic signals of a fuse arc measured with an Avisoft sensor.

The specificity of the acoustic arc signal is characterized by a transient signature with a decreasing envelope. Therefore, the sensors used for the detection must be microphones having an excellent coupling with the air and a large flat bandwidth.

We have then developed two methods to detect the time signature of an arc. The first one consists in a correlation between the time signal measured by the sensors and an ARMA (Auto-Regressive Moving Average) model of the arc. The second method is less specific to the arc signal and uses higher-order statistics to separate transient components from Gaussian noise. We evaluated the receiver operating characteristic (ROC) curves to compare the quality of these two detectors. Noise and disturbances specific from the environment of an EV (transient acoustic emission from motor, blinker, battery ...) were added to an arc signal. These disturbances can induce false alarms because most of there spectra overlap that of the arc. But the ROC results demonstrate that detection by correlation is very robust; indeed, in noisy condition, the probabilities of correct detection and false alarm are both excellent. However, the ARMA model is very sensitive to the properties of the sensor (in particular its resonances). Although less efficient, the second method is also robust to noise. An advantage is its simplicity of implementation, but all disturbances with transient shapes will generate false alarms.

A demonstrator (Fig. 2) has been realized based on a geometry consistent with those used in batteries developed at CEA. We have reproduced a typical assembly of cylindrical cells using plexiglas elements for safety reasons.



Figure 2: Demonstrator with arcing flash present on a fuse wire placed between cylindrical cells in Plexiglas and arc processing.

Perspectives of this work are to develop a localization process to improve the maintenance of the battery and to miniaturize the sensors to integrate the whole system inside the battery and reduce the cost. Technological developments are underway in CEA for this purpose.

#### **References:**

[1] V. Cattin, P. Périchon, J. Dahmani, "Detection of electric arcs in large batteries", Research and Innovation for Transport Systems of the Future Int. Symp. (RITF), 12-15 November 2012, Paris, France.



## Research topics: battery monitoring system

R. Al-Nazer, V. Cattin, M. Montaru (CEA-LITEN), P. Granjon (GIPSA-Lab)

ABSTRACT: In hybrid electrical vehicles (HEV) and electrical vehicles (EV), an accurate estimation of the battery states is required to optimize its operation. The battery electrical impedance is known to provide useful information on those states, and electrical impedance spectroscopy is one of the most informative investigation methods. However, it cannot be easily implemented in embedded system and broadband excitation signals, which are frequently used in system identification applications, are proposed to perform impedance measurements on a battery cell. Moreover, spectral coherence is an advanced parameter estimated in order to determine the frequency bands where the transfer function of the system is accurately identified.

A linear and time invariant (LTI) single-input single-output system is fully defined by its frequency response function (FRF)  $H(\lambda)$ .



Figure 1: Non-parametric identification of an LTI system.

Non-parametric identification estimates the FRF from input x[n] and noisy output measurements z[n] without the use of any model (Fig. 1). The unknown additive measurement noise is supposed uncorrelated with the input and therefore with the output. Under this last assumption and using the input auto-spectral and input-output cross-spectral power densities ( $\hat{s}$  and  $\hat{s}$ ), we can write:

$$\hat{H}(\lambda) = \frac{\hat{S}_{xx}(\lambda)}{\hat{S}_{xx}(\lambda)} \qquad \text{if } \hat{S}_{xx}(\lambda) \neq 0 \qquad (Eq \ 1)$$

Based on the computation of the spectral coherence (Eq 2), we can quantify the quality of the FRF estimation and calculate the upper and lower 95% confidence limits for the gain (Eq 3) or the phase.

$$\left|\hat{c}_{zx}(\lambda)\right|^{2} = \frac{\left|\hat{S}_{zx}(\lambda)\right|^{2}}{\hat{S}_{w}(\lambda)\hat{S}_{w}(\lambda)}$$
(Eq 2)

$$\log_{10} \{ \hat{G}(\lambda) \} \pm 1.96 \sqrt{\frac{(\log_{10}(e))^2}{2L} \frac{1 - |\hat{c}_{zx}(\lambda)|^2}{|\hat{c}_{zx}(\lambda)|^2}}$$
 (Eq 3)

Broadband identification is valid when the excitation signal shows an almost flat power spectral density in the frequency band of interest ([1-7] Hz is considered here). A Pseudo Random Binary Sequence (PRBS) and a swept square have been designed to estimate the battery impedance over this frequency band from a single set of measurements. Based on simulation data and using the previous equations, we plot the theoretical and the estimated gains of the FRF and the confidence limits on this estimation (Fig. 2).

Several studies reveal that the state of charge (SOC) distorts the battery electrical impedance at lowest frequencies. We perform an experimental broadband identification process on a graphite/LiFePO4 cell with a nominal capacity of 2.3 Ah at room temperature over three different theoretical SOCs (estimated by coulomb counting) (Fig. 3). We have shown that a broadband identification method is able to reflect the SOC effect on the battery electrical impedance. Next steps consist in electronic development and fine performances quantification.







Figure 3: Nyquist plots for experimental results with PRBS signal for several states of charge.

#### **References** :

R. Al Nazer, V. Cattin, P. Granjon and M. Montaru, "A new optimization algorithm for a li-ion battery equivalent electrical circuit identification", 9th international conference of modeling, optimization and simulation (MOSIM), Bordeaux, France, 6-8 June 2012.
 R. Al Nazer, V. Cattin, P. Granjon and M. Montaru, "Broadband identification of battery electrical impedance for HEV", Research and Innovation for Transport Systems of the Future Int. Symp. (RITF), 12-15 November 2012, Paris, France.



# State of Charge Estimation Based on Battery Mechanical Impedance Measurement

55

## Research topics: battery monitoring system

G. Despesse, E. Le Baron, S. Mailley (CEA-LITEN), S. Genies (CEA-LITEN), G. Bretin

ABSTRACT: The State of Charge (SoC) of first battery technologies (Pb, Ni-Mh...) could be infered from their voltage but this is no longer the case for all Li-ion technologies. To overcome these limitations, we propose to estimate the battery's SoC from a mechanical impedance measurement of the battery. In fact, during the charge and discharge phases, the displacement of Lithium ions changes the electrode material composition and therefore induces a change of the mass density (up to 2%), the strain/stress, the mechanical stiffness, the vibration propagation and the mechanical damping. Finally, from the battery mechanical impedance change, one can expect to deduce the SoC and potentially its State of Health (SoH).

By deforming a material and sense its pressure or applying a pressure in a material and sense its deformation at different frequencies, one can deduce its complex mechanical impedance. This deformation/pressure can be applied to the material or sensed simply by using a piezoelectric sensor inserted in the material to sense (Fig. 1). Finally the pressure/displacement relation can be translated in voltage/current relation in the electric domain thanks to the electromechanical coupling of the piezoelectric sensor in the material to characterize (i.e. the internal battery materials) will slightly change its global mechanical behavior but we focus here only on the mechanical impedance shift due to a battery State of Charge change and not to the absolute mechanical impedance value.



Figure 1: Example of a piezoelectric material integration in a multilayer Li-ion battery.

Two types of prototypes have been fabricated; a first type based on coin-shape battery cells quite easy to fabricate manually (Fig. 2), and a second one based on soft-packaging stacked Li-ion batteries more representatives of an industrial product (Fig. 3).



Figure 2: Piezoelectric sensor placed in a coin cell Li-ion battery

We do not know a priori in which frequency band the most relevant information is because an accurate mechanical model of a full battery would be too difficult to derive. To identify where the most relevant information is, we developed a software comparing at each frequency the current/voltage phase measurement to the SoC. The software then performs a linear interpolation of the measurement points. Finally, the software looks for the frequency measurement giving the lowest deviation compared to its interpolated straight line pondered by the straight line slope. Figure 4 shows the correlation obtained at that optimal frequency [1].



Figure 3: Sensor placed in a soft-packaging stacked Li-ion battery.



Figure 4: Current/voltage phase as a function of the State of Charge.

If some changes in term of best frequency to measure can occur between the various prototypes we made, there is always a frequency where there is a good correlation between the phase and the battery State of Charge. Finally, the mechanical impedance measurement could be a good candidate to estimate the SoC of future Li-ion batteries. Some other types of configurations, like differential frequency correlations or SoH correlations are under study.

#### References:

[1] G. Despesse, E. Le Baron, S. Mailley, S. Genies, G. Bretin, "State of Charge estimation based on battery mechanical impedance measurement", Research and Innovation for Transport Systems of the Future Int. Symp. (RITF), 12-15 November 2012, Paris, France.



G. Despesse, S. Lechat Sanjuan, S. Gery

ABSTRACT: In electric cars, the electrical chain is composed of a charger (AC/DC converter), a Battery Management System (BMS) to ensure the battery cell balancing and monitor their voltage, and an inverter to drive the electrical motor from the battery pack. We developed a novel architecture where all of these functions are ensured by dynamically switching the battery cells. This architecture consists in connecting or disconnecting in real time each cell placed in the serial arrangement. We demonstrate the feasibility to drive a three-phase electric motor with an efficiency up to 98.5% from few Hz to 400 Hz, while maintaining the cells balanced.

In standard battery architectures, a single cell failure may severely compromise the complete battery pack capabilities. One possible solution is to divide the battery pack into a few electrically switchable modules. If one cell fails, a single module of the battery pack is isolated, enabling the system to continue its operation. The current through the battery pack in electrical vehicles can exceed 100 A and the transistor cost increases as a function of the current level handled by the transistor. As a result, a two-switch-permodule configuration may not be the most suitable option. At constant price and constant losses, it is interesting to decrease the transistor size and increase their number, which in addition multiplies the thermal dissipating points and decreases the losses, making it easier to maintain the temperature of the system without costly and heavy radiators. Multiplying the number of transistors also ensures redundancy, which increases security and shortens electrical connections.

An optimum module voltage is around 20 V, since below this limit, the individual transistor cost is no longer proportional to the voltage and becomes constant. A level of 20 V is equivalent to 4 or 5 serial battery cells depending on their maximum voltage. This module voltage is close to the standard maximum MOSFET gate-source voltage  $V_{gs}$  and hence easily drivable. Furthermore, small voltage modules enable to significantly reduce the switching losses and the electromagnetic perturbations during transistor transitions.

With the optimal module size in terms of transistor cost sorted, the system now requires a BMS in each module (to ensure cell balancing inside each module), a charger and an inverter. The cell balancing circuit can be replaced by singleserial-cell modules, cell balancing thus proceeding by using more often the modules having higher States of Charge. With such modules, the output voltage can be adjusted by steps of a single battery cell voltage (3.2V/3.6V for Li-ion battery). By dynamically switching the modules, it becomes possible to produce a near-perfect sinusoidal waveform that can directly drive an electrical motor. As the output voltage step is lower than the resistive voltage drop in classical electric chains, one can also directly recharge the battery pack on the electrical network without any or with a very low size inductor. In conclusion, dynamic switching of the modules would enable to get rid of the costly inverter and its cooling system, the costly and heavy capacitor placed before the inverter to filter the current, the costly and heavy charger and the costly converter placed in the rapid charging stations. Furthermore, as the battery cell voltages tend to increase and the power transistor voltages tend to decrease with the transistors gate length reduction, there is a good chance that in the near future, optimal cost architectures will indeed tend towards modules of only one serial cell.



Figure 1: Detailed architecture (left), prototype (right)

The prototype we made is able to manage 18\*4=72 battery cells of 40 A.h, representing 9.5 kWh (considering 3.3-V battery cells) (Fig. 1). The chosen transistors allow a continuous current of 40 A per battery cell without any thermal radiator. Figure 2 shows the voltage and current provided by the prototype when supplying an asynchronous motor.



Figure 2: Experimentally generated voltage and current waveforms.

We have shown that it is possible to directly drive an electric motor by dynamically switching batteries with an efficiency up to 98.5%. Losses are very low and spatially distributed, which prevents the use of a cooling system. Although this solution requires numerous transistors, the latter operate in low voltage and hence are relatively cheap (less than 0,6\$ per transistor, less than 100\$ per 10 KWh to manage; these costs can be reduced by large scale production). This solution can also significantly increase the security by isolating a failing cell, cutting the current path in many points in case of vehicle crash, flood, short circuit or simply during maintenance. The main remaining challenge is to increase the data bus speed for driving more modules and for producing an output wave at more than 500 Hz (currently limited to 400 Hz).

**References:** 

[1] G. Despesse, S. Lechat Sanjuan, S. Gery, "Battery Monitoring System using switching battery cells", Research and Innovation for Transport Systems of the Future Int. Symp. (RITF), 12-15 November 2012, Paris, France. PhD Degrees Awarded

Mathilde Souccaros Bouhadjar Ahmed-Seddik François Poucheret Antonio Clemente Matteo Gorgoglione Antonio De Domenico Yan Fu Giorgio Corbellini Pierre-Henri Horrein

# Annual Research Report > 2012

Systems and Solutions

# PhD degrees awarded in 2012

# Mathilde Souccaros

## University: Université de Grenoble

#### Analysis of random numbers generators in abnormal use conditions

Random numbers have been used through the ages for games of chance, more recently for secret codes and today they are necessary to the execution of computer programs. Random number generators have now evolved from simple dices to electronic circuits and algorithms. Accordingly, the ability to distinguish between random and non-random numbers has become more difficult. Furthermore, whereas in the past dices were loaded in order to increase winning chances, it is now possible to influence the outcome of random number generators.

In consequence, this subject is still very much an issue and has recently made the headlines. Indeed, there were talks about the PS3 game console which generates constant random numbers and redundant distribution of secret keys on the internet.

This thesis presents a study of several generators as well as different means to perturb them. It shows the inherent defects of their conceptions and possible consequences of their failure when they are embedded inside security components. Moreover, this work highlights problems yet to be solved concerning the testing of random numbers and the post-processing eliminating bias in these numbers distribution.

# Bouhadjar Ahmed-Seddik

#### University: Université de Grenoble

### Wideband vibration energy harvesting systems

The first limit of vibration energy harvester's efficiency is the input mechanical energy. This energy is tightly related to the amplitude of the relative displacement obtained by the converter. In fact, harvesting vibrating energy requires converting the vibration into a relative displacement first before it can be translated into a useful electrical energy. This relative displacement is obtained by adding a seismic mass placed in suspension. The effect of the seismic mass becomes minimal especially for miniature structures.

Thus, the input mechanical energy and then the electrical recovered power are reduced. To overcome this limitation, the effect of seismic mass inertia is amplified by using the resonance phenomenon. However, using resonance means that the system should be excited at its resonance frequency which is not known in advance and might change over time. This is the objective of this thesis, allowing vibration energy harvesters to maintain an optimal operation at resonance even if the vibration frequency changes.

The work of this thesis is organized around three solutions: 1) Adjustment of the resonance frequency by applying an electric field in a piezoelectric material; 2) Adjustment of the resonance frequency by adapting the electrical load coupled with the harvester; 3) Amplification of the relative displacement at off resonance by actuating a synchronized rebound

In the present work, modelling and optimization of both the frequency range of operation and the mechanical-electrical conversion were carried out. Three structures have been developed, tested and used to validate the three approaches. Finally, a very low power electronic has been developed for controlling, in real time, the resonant frequency and the extracted electrical energy in order to maintain an optimum quality factor.



# PhD degrees awarded in 2012

# François Poucheret

University: Université de Montpellier II

Electromagnetic injections : development of tools and methods for faults attacks

Attacks based on fault injection consist in disturbing a cryptographic computation in order to extract critical information on the manipulated data. Fault attacks constitute a serious threat against applications, due to the expected effects: bypassing control and protection, granting access to some restricted operations... Nevertheless, almost of classical ways (T°,V,F) and optical attacks are limited on the newest integrated circuits, which embed several countermeasures as active shield, glitch detectors, sensors... In this context, potentials of Electromagnetic active attacks must undoubtedly be taken into account, because of their benefits (penetrating characteristics, contactless energy transmission, low cost power production...).

In this work, EM active attacks based on continuous mode are presented, with a particular attention to the development and optimization of injection probes, with a complete characterization of EM fields provided by each probe at the IC surface. Finally, some experiments are realized on internal clock generator or on true random numbers generators, and then evaluated to prove the efficiency of these techniques.

# Antonio Clemente

University: Université de Rennes I

Design of transmit-array antennas for beam-steering and beam-forming applications

This PhD thesis investigates the design and realisation of electronically reconfigurable transmit-array antennas. A transmit-array is composed of one or more focal sources illuminating a first antenna array operating in receive mode and connected, using phase-shift elements, to a second antenna array operating in transmission mode. The incident power received on the first array, as in the case of a lens, is transmitted in the free space and can be focused or collimated by tuning the transmission phase of the unit-cells in order to obtain a specific phase distribution across the array aperture. Beam-steering and beam-forming can be achieved using electronically tunable unit-cells.

A theoretical study of transmit-arrays performances has been carried out using an in-house CAD tool based on analytical formulas. The reduction of the focal distance using multiple feeds and the reduction of the spill-over losses using a beam-formed focal source have been investigated as well.

A linearly-polarized electronically reconfigurable transmit-array at X-band frequencies has been designed and demonstrated. This prototype is composed of  $20 \times 20$  unit-cells. 800 PIN diodes have been integrated on the array in order to control the transmission phase of each unit-cell. A maximum broadside gain of 22,7 dBi, a bandwidth of 1,56 GHz (15,6% at 10 GHz), a total efficiency of 52,9%, and a 2D beam-steering capability of  $\pm 70\%$  have been measured.

Finally, the use of RF-MEMS switches to reduce the unit-cell insertion losses and the transmit-array total power consumption has been investigated.

59

## Annual Research Report > 2012

eti

Systems and Solutions

# PhD degrees awarded in 2012

# Matteo Gorgoglione

## University: Université de Cergy-Pontoise

#### Analysis and construction of non-binary LDPC codes for fading channels

Low Density Parity Check (LDPC) codes are capacity approaching codes for a wide range of channel models. In particular, this thesis investigates the non-binary LDPC codes that demonstrated an enhanced correction capacity with respect to their binary counterparts (especially when the block-length is small to moderate, or when the symbols sent through channel are not binary) but they require more complex decoding architecture.

The main goal of the thesis is then to demonstrate that besides the gain in the decoding performance, the use of non-binary LDPC codes can bring two principal benefits that may offset the extra cost in decoding complexity: the "flexibility" – the capacity of a coding system to accommodate multiple coding rates through the use of a unique encoder/decoder pair – and the "diversity" – the coding system's capacity to fully exploit the communication channel's heterogeneity. Four main contributions have been presented in the dissertation: 1) The development of a Density Evolution method based on the Monte-Carlo simulation of an infinite code. 2) The analysis of flexible coding schemes through the use of puncturing, 3) The design of an optimized interleaver in order to exploit the binary diversity over the slow fading channel, 4) The conception of flexible coding scheme, which achieves full-diversity over the slow fading channel.

# Antonio De Domenico

## University: Université de Grenoble

## Energy efficient mechanisms for heterogeneous cellular networks

Wireless communications proliferate into nearly every aspects of the human society, driving to the exponential growth in the number of connected devices. Powerful smart-phones and tablets, ubiquitous wireless broadband access, and machine-to-machine communications generate volumes of data traffic that was unpredictable few years back. In this novel paradigm, the telecommunication industry has to simultaneously guarantee the economical sustainability of broadband wireless communications and users' quality of experience. Additionally, there is a strong social incentive to reduce the mobile communications carbon footprint, which has notably increased in the last decade.

In this context, the integration of femtocells in cellular networks is a low-power, low-cost solution to offer high data rates to indoor customers and simultaneously offload the macrocell network. However, the massive and unplanned deployment of femtocell access points and their uncoordinated operations may result in harmful co-channel interference. Moreover, a large number of lightly loaded cells increases the network energy consumption.

In this thesis, we investigate the effects of femtocells deployment on the cellular network energy efficiency. Moreover, we look into adaptive mechanisms for femtocell networks as a mean to pave the way towards agile and economically viable mobile communications. Our goal is to dynamically match the resource demand and offered capacity in order to limit the average power consumption and co-channel interference, while guaranteeing quality of service constraints. We take advantage of the unusual communication context of femtocells to propose resource allocation and network management schemes that coordinate the access point's activity, power consumption, and coverage. Simulation results show that our proposals improve system energy efficiency and users' performance in both networked and stand-alone femtocell deployment scenarios.

# PhD degrees awarded in 2012

61

# Yan Fu

Systems and Solutions

## University: Université de Grenoble

Annual Research Report > 2012

# Development of a test bench for characterization of integrated antennas at millimeter-wave frequencies

In this thesis, we designed and built a new 3D test bench, particularly for low-directivity integrated antennas at millimeter-wave frequencies. We proposed three feeding techniques for the antenna under test (AUT): a probe-fed technique, a flexible-transmission-line-fed technique and a radarcross-section (RCS) method. The probe-fed method was developed with a customized probe, which involves an elongated (50 mm) coaxial line between the probe tip and the probe body, wherein the probe body is reversed (relative to the conventional measurement configuration) so it lies below the plane of the AUT. This method reduces the range of angles that are masked from 80° (for a conventional probe setup) to 20°. The second method was developed using a flexible transmission line with a modified flip-chip connection to the AUT. This method completely eliminates the masked zone. The third method characterizes the radiation pattern using a radar cross-section (RCS) method. This method requires neither a probe system nor connectors. However the simulation results demonstrate that there is insufficient variation in the ratio of received power to incident power as the load on the AUT is varied in order to make precise measurement with conventional measurement equipment.

# **Giorgio Corbellini**

#### University: Université de Grenoble

#### Adaptive medium access control for heterogeneous wireless sensor networks

Heterogeneous Wireless Sensor Networks (WSN) are composed of different sensors generating readings with different characteristics. The initial deployment can be random resulting in heterogeneous distribution of nodes across the playground. Other factors such as node death because of energy resource exhaustion, mobility, or generic fault influence the heterogeneity of the distribution of nodes. Heterogeneity conditions may evolve during time and space and require adaptive mechanisms able to react to different characteristics. In this thesis, we investigate energy-efficient adaptive MAC methods for heterogeneous WSN able to take into account heterogeneity variations.

First, we study the problem of heterogeneous traffic. To cope with multiple traffics with different QoS, we propose an adaptive MAC protocol based on the asynchronous preamble sampling (PS) approach, a simple energy saving MAC technique. The proposed protocol (Low-Latency MAC, LA-MAC), ensures efficient message forwarding throughout a multi-hop network thanks to the transmission of bursts. We propose an analytic model for an accurate energy consumption evaluation of preamble sampling (PS) that depends on the instantaneous traffic load of localized regions so that it is independent of the network traffic patterns that can also be heterogeneous.

Second, we study dynamic WSNs with density of nodes varying across space and time. We address the case of dynamic networks in which nodes and/or radio links may appear and disappear over time due to battery exhaustion, node mobility, or network management operations. We show that it is possible to provide QoS support in dynamic networks using an adaptive Density Aware MAC (DA-MAC) method. The proposed protocol offers a configurable channel sensing phase during which nodes request transmission opportunity in a way that avoids collisions.

## Annual Research Report > 2012

eti

Systems and Solutions

# PhD degrees awarded in 2012

# **Pierre-Henri Horrein**

## University: Université de Grenoble

# Software architectures for flexible radio: integration of heterogeneous computation units

The development of flexible radios enables more efficient and smarter wireless networks. A flexible radio can be based on a software implementation of radio operations, a hardware implementation based on configurable hardware coprocessors, or an heterogeneous implementation. In this thesis, we focused on two different aspects of flexible radios.

First, the use of graphical processors, especially for software radios, is studied. These execution targets enable impressive performances, when studying raw attainable processing throughput, through the use of massively parallel architectures. The problem is that the data parallelism exhibited by these processors does not match the task parallelism of software radio applications. Different approaches to correct this mismatch are studied. The results show an improvement in the attainable software implementation, while letting the processor perform other tasks.

Second, an environment able to support multiple implementation choices for flexible radio is defined. This includes heterogeneous platforms support, as well as application management on these platforms. While this environment is still in early development stage, preliminary results demonstrate its adaptability, and ease of application development on different heterogeneous platforms.

## Sana Tmar

#### University: Université de Grenoble

## Signal-based security in wireless networks

Security in mobile wireless networks is considered a major impediment since these environments are a collection of low-cost devices, generally connected in ad-hoc manner without trusted third party. Therefore, conventional security methods are often inappropriate. Recent contributions propose to explore the radio communication interface and to turn the radio propagation problems into advantages by providing new alternatives to enhance security. In this thesis, we investigate the signal-based security concept and study its effectiveness through experiments.

The first part of this dissertation discusses the problem of key generation from Ultra Wide Band channels. To derive secret keys from channel measurements, three stages are required: channel estimation, quantization and key agreement. A measurement campaign has been performed to confirm the fundamental channel requirements for key generation (i.e. the reciprocity and the spatial correlation). Results show that the robustness of such techniques depends on the channel information used as source of randomness as well as on the underlying algorithms. Analysis on the impact of each stage (i.e. the quantization and the key agreement) on the security has been presented. An adaptive key extraction method is proposed, performances are evaluated and robustness against deterministic channel prediction attacks is presented.

The second part of the dissertation considers the problem of intrusion detection. First, we test a method based on electromagnetic radiation to discover the presence of an adversary in the receiver/emitter vicinity. Then, the problem of relay attack detection is investigated in RFID systems. A new solution based on the noise channel is proposed to detect this attack. Experimental and theoretical results are provided to test the effectiveness of this new proposition.



Editorial Committee

Laurent Dussopt François Vacherand Dominique Noguet Sébastien Dauvé Jean-Jacques Chaillout

**Coordination LETI** 

Hélène Vatouyas

Graphic Art

Majda Kholti Valérie Lassablière

0





Roland Blanpain Head of Systems & Solutions Integration Division roland.blanpain@cea.fr

François Vacherand Deputy manager Systems & Solutions Integration Division francois.vacherand@cea.fr

Céline Soubeyrat Program Manager céline.soubeyrat@cea.fr

Contacts

Jean-Michel Léger Program Manager jean-michel.leger@cea.fr

Dominique Noguet Head of Telecoms and security Lab. dominique.noguet@cea.fr

Sébastien Dauve Head of Sensors and Systems Lab. sebastien.dauve@cea.fr

Tiana Delhome Head of Innovation Lab. tiana.delhome@cea.fr



# Leti CEA - Leti - DSIS CEA Grenoble

17, rue des Martyrs F-38054 GRENOBLE Cedex 9 Tel. (+33) 4 38 78 48 20 www.leti.fr

© CEA 2012. All rights reserved, any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA.