Neuro-inspired architecture of cognitive systems

Authors

Eliott Coyac
Vincent Gripon
Charlotte Langlais
Claude Berrou

Partners

European Research Council
Established by the European Commission

Neural clique networks

- Neural clique networks were introduced by Vincent Gripon and Claude Berrou in 2011 and are the focus of the ERC NEUCOD team.
- They are neuro-inspired associative memories: they can store, retrieve and test if data is present.
- They offer error-correcting abilities: a stored pattern can be retrieved from only pieces, and even errors in the structure of the network can be bypassed.
- They model *local* networks of the brain (e.g. networks connected to the Hippocampus).
- The goal of this PhD is to integrate neural clique networks in a larger intelligent architecture. We studied 1) how multiple networks can communicate through long distance and 2) how to aggregate multi-modal data with multiple local networks working together.

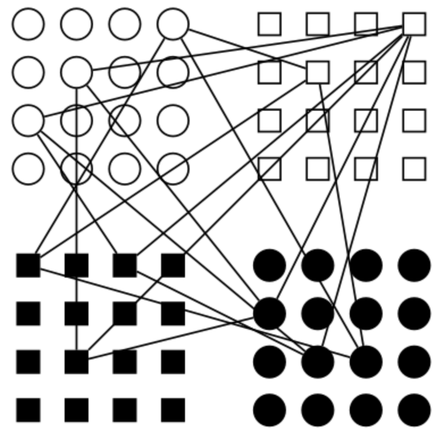


Figure: A small neural clique network with 4 clusters of 16 neurons each

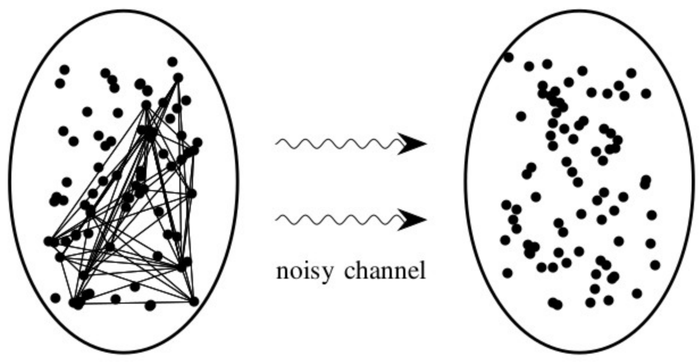


Figure: How to transmit Network A to Network B?

$$\begin{cases} \frac{dV}{dt} = -V + h(W \cdot V + I) \\ \frac{dW}{dt} = s(\epsilon \cdot VV^{\top} + W) - W \end{cases}$$

Figure: Recurrent equations of the network

1) Long distance communication

- We aim at transmitting data from a network to another network, mirroring long distance communication in the brain.
- The challenges lies in the fact that the environment is *noisy* (unreliable synapses, molecular factors, external interferences…).
- We introduced a unified model for learning and decoding. Using differential dynamics, we proved it robust to erasures and insertions.

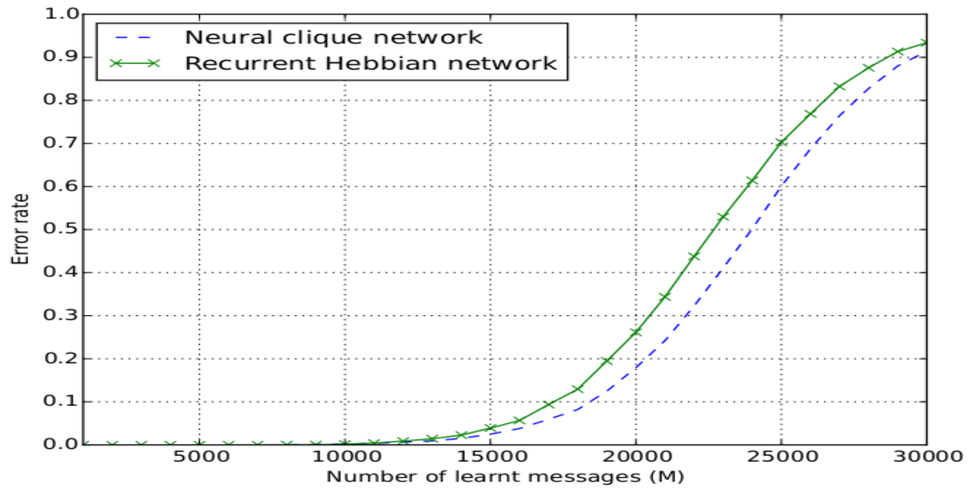


Figure: Error rate in Network B compared to Network A.

2) Hubs

- As long distance communication is possible, we build architectures comprising several neural clique networks: hubs.
- Hubs correlate information from different sources.
- These novel connectionist models open the way to aggregation of multi-modal data (for example audio and visual).
- The architecture can be further scaled to obtain “hubs of hubs”, which are commonly depicted in neuroscience articles.

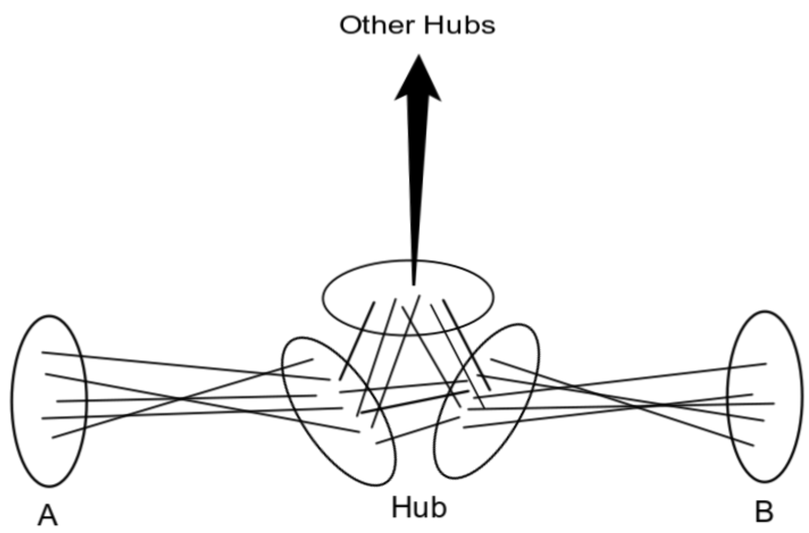


Figure: Architecture comprised of multiple neural clique networks, able to perform associations between elements of network A and B and communicate with other hubs.

Future work

- Combine local learning with global storing.
- Cross-reference multi-modal data to solve challenging cognitive tasks.
- Suggest new connectionist components for a novel model of computation.

Publications

Consolidated Hebbian learning and parsimonious energy consumption, resulting in large capacitive assocative memories Eliott Coyac, Vincent Gripon, Charlotte Langlais, Claude Berrou. *ICMNS 2015*

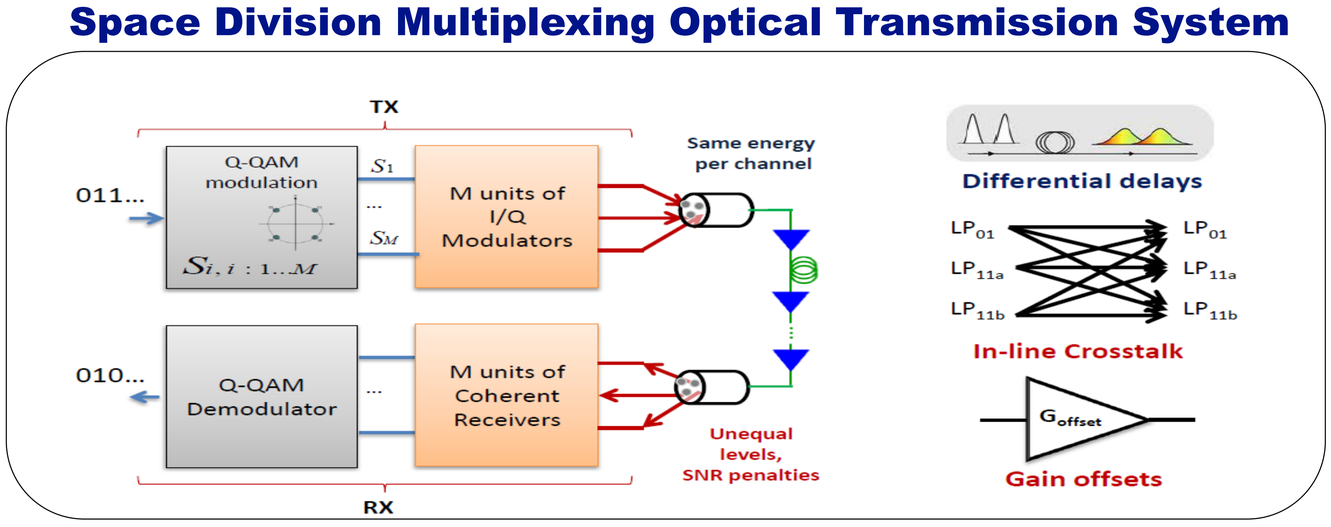
Impact du bruit synaptique sur les performances des réseaux de cliques neurales Eliott Coyac, Vincent Gripon, Charlotte Langlais, Claude Berrou. *Gretsi 2015*

Contact eliott.coyac@telecom-bretagne.eu

Futur & rupture
Janvier 2016

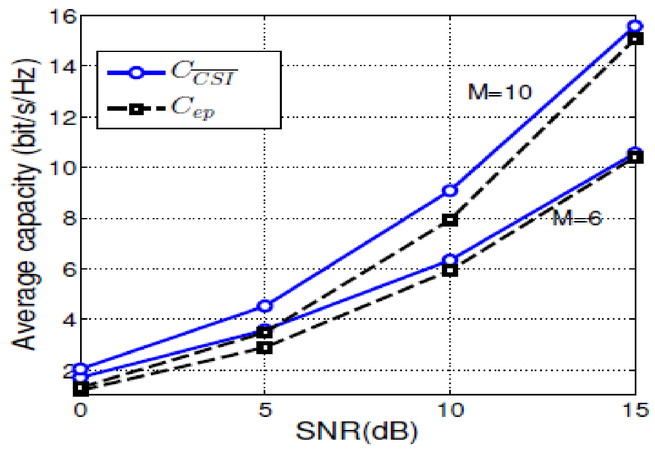
Coding Techniques for Few Mode Fibers

Space Division Multiplexing Optical Transmission System

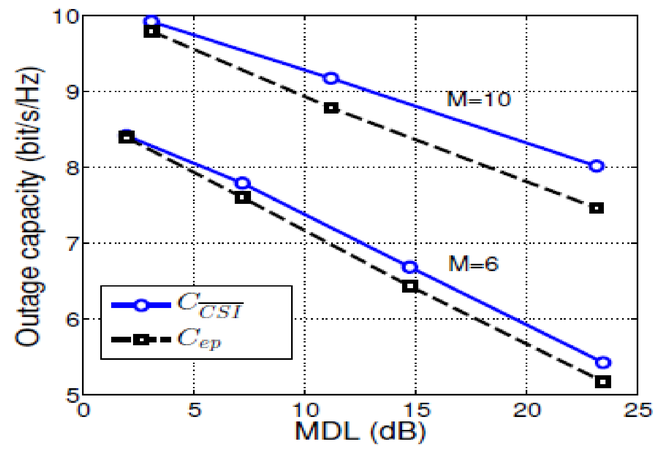


Capacity enhancement of SDM systems

- Perfect channel state information
  - ✓ Advantage: Improvement of channel capacity.
  - ❖ Drawback: needs instantaneous channel feedback.
- Proposed solution: Statistical channel state information:
  - ➢ Low digital signal processing complexity (low feedback).
  - ➢ Practical for real implementation.
  - ➢ Average and Outage capacity enhancement.



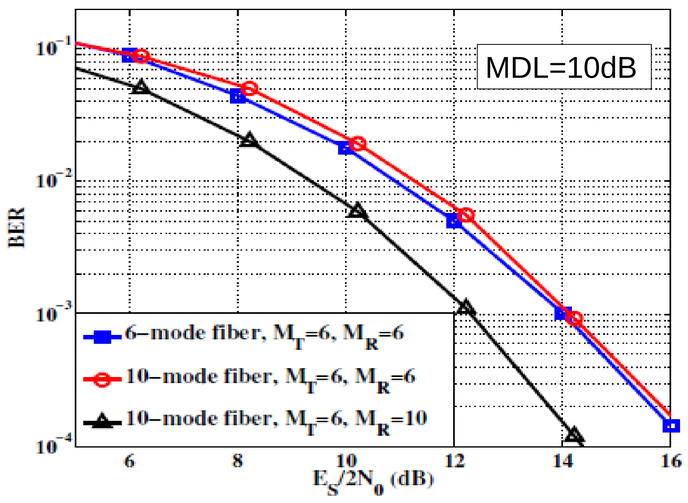
Average capacities VS SNR for M=6,10 modes, $\overline{CSI}$ and C_{ep} (equal power without CSI) for MDL=20dB

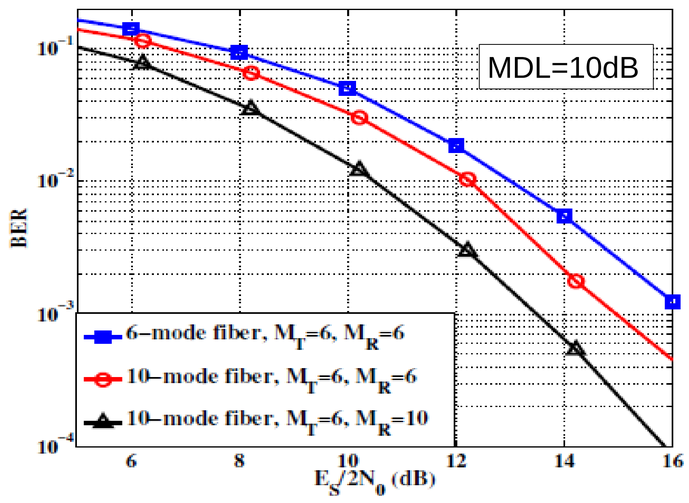


Outage capacities VS MDL for M=6 modes. $\overline{CSI}$ and C_{ep} (equal power without CSI) for SNR=10dB.

Mode Selection for SDM Systems

- Selection of only a small number of modes for multiplexing information symbols.
- Smaller MIMO systems: Low complexity decoding at the receiver side.
- Scalable technique for future MIMO SDM systems.





Performance of 6 and 10 mode fibers using M_T transmit modes and M_R receiver side modes. Spectral efficiency=12 bits/s

Perspectives and future work

- Investigate mode selection with inline distributed noise.
- Investigate the benefits of space time coding for SDM optical systems
  - ➢ numerical simulations and experimental validation
  - ➢ derivation of an upper bound for the error probability.

Publications

- E-M. Amhoud; E. Awwad; G. Rekaya Ben-Othman; Y. Jaouen. “Mode selection and larger set equalization for mode-multiplexed fiber transmission systems” OFC, March 2015.
- E-M. Amhoud; Y. Jaouen; G. Rekaya Ben-Othman. “Capacity Enhancement of Space-Division Multiplexed Systems by using Statistical Channel State Information” ACP, November 2015.

Partie prenante

Auteurs

- El Mehdi AMHOUD
- Ghaya REKAYA BEN-OTHMAN
- Yves Jaouen

Partenaires

26 Janvier 2016 Journée de restitution des travaux du Programme de recherche Futur & Ruptures

Contact el-mehdi.amhoud@telecom-paristech.fr Site web http://perso.telecom-paristech.fr/~amhoud

Wireless Node Cooperation:

The Nearest Neighbor Model.

Parties prenantes

Auteurs

Luis David Álvarez Corrales, INFRES, Télécom ParisTech.

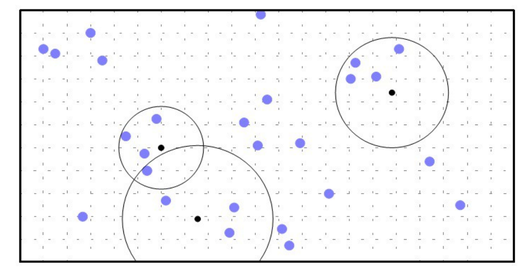
Advisors : CNRS Anastasios Giovanidis, Professor Philippe Martins, INFRES, Télécom ParisTech.

Partenaires

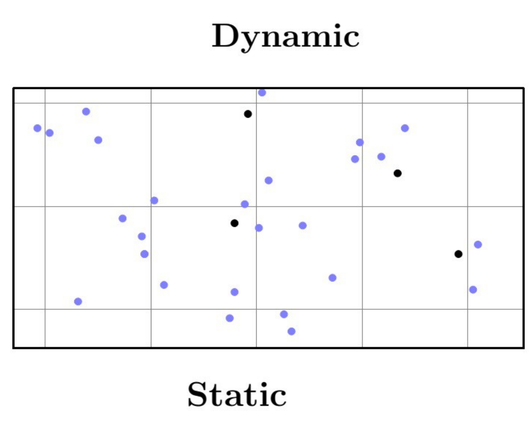
INTRODUCTION

Cooperating Base Stations. Why ?

Necessary due to densification through HetNets.
Coverage inprovement, Higher spectral efficency, Better service at cell edge.



Dynamic : Overburdens the backhaul, time-sharing between clusters.
Static : Reasonable information exchange, no resource-sharing, one controler per cluster.

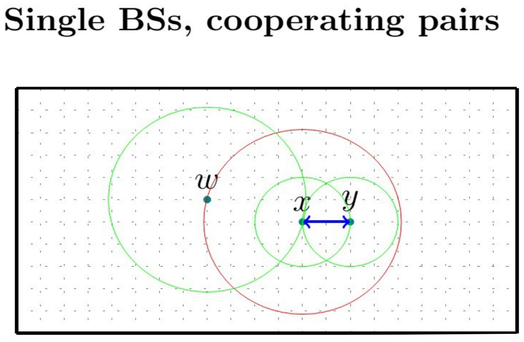


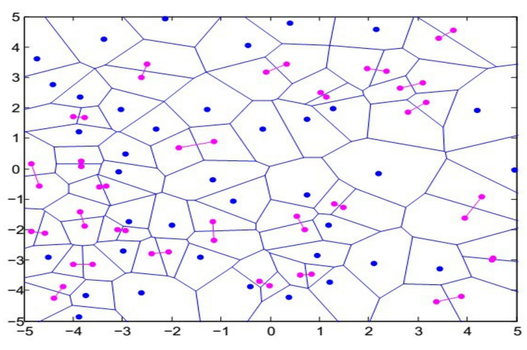
Our work.

Static groups by means of proximity : strong signal, weak interference, fast coordination, BSs share planar area of common interest.

The maximum group size is 2 : single BSs operating individually, pairs of BSs providing service cooperatively.

Single BSs, cooperating pairs





CONSTRUCTION AND SOME PROPERTIES

Given a stationary point process, we define the stationary point processes of (a) singles and (b) pairs from the Nearest Neighbour thinning.

Properties of the subprocesses originating from a Poisson

62% points are in pair and 38% are singles.
The two processes are not Poisson.
There is ***attraction*** between atoms in pair and ***repulsion*** between singles.

Expressions for the Palm measures of both processes resulted in the derivation of the distrubution of the distance between two cooperating BSs. This is a Rayleigh random variable, with scale parameter depending on the density of the original process.

INTERFERENCE

$$\mathcal{I}^{(1)} = \sum_{x \in \Phi^{(1)}} f(x), \qquad \mathcal{I}^{(2)} = \frac{1}{2} \sum_{y \in \Phi^{(2)}} \sum_{z \in \Phi^{(2)}} g(y,z) \mathbb{1}_{\{y \leftrightarrow z\}}$$

If v_x represents the random propagation effects from the BS x to the typical user,

$$f(x) = \frac{v_x}{\|x\|^\beta}, \qquad g(y,z) = \begin{cases} \frac{v_y}{\|y\|^\beta} + \frac{v_z}{\|z\|^\beta}, & [NC] \\ max\left(\frac{v_y}{\|y\|^\beta}, \frac{v_z}{\|z\|^\beta}\right), & [OF1] \\ \mathbb{1}_{on_y} \frac{v_y}{\|y\|^\beta} + (1 - \mathbb{1}_{on_z}) \frac{v_z}{\|z\|^\beta}, & [OF2] \\ \left| \sqrt{\frac{v_y}{\|y\|^\beta}} e^{i\theta_y} + \sqrt{\frac{v_z}{\|z\|^\beta}} e^{i\theta_z} \right|^2, & [PH] \end{cases}$$

Expressions for the expected value of interference, when the random fields f and g are independent of the process.

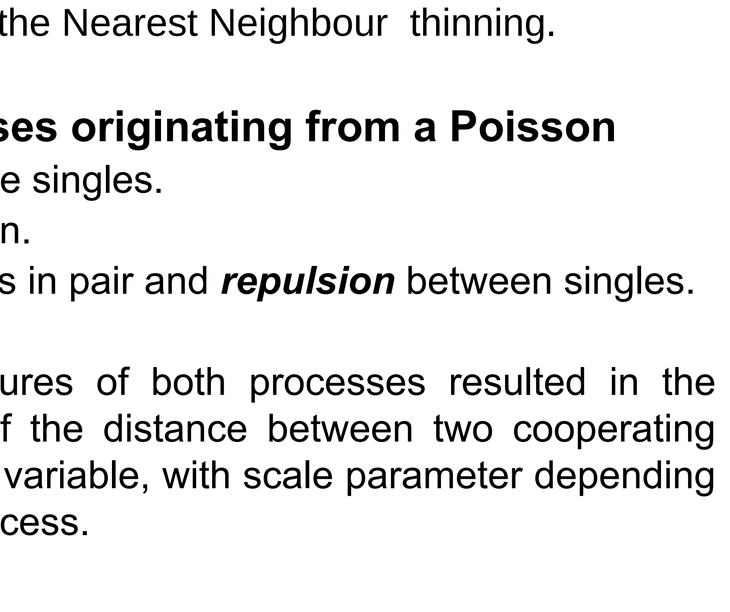
Approximation for the Laplace transform of the interference.

POISSON SUPERPOSITION MODEL

Given a density λ>0 for the BSs we define a Poisson process with parameter (0.3785)λ for the single atoms,
and a *marked* Poisson procees with parameter (0.6215)λ/2 for the pair parents.

Each mark $\mathbf{Z_r}$ represents the distance of the second cooperating BS (child) from the origin.

$\mathbf{Z_r}$ follows a Rice distribution, with parameter dependening on r and the density λ.



Contact luis.alvarez-corrales@telecom-paristech.fr

CItizen's Privacy in RFID & IoT contexts: An exploratory study about the socio-technical viability of the concept of *'silence of the chips'*

Parties prenantes

Auteurs

Crabu Stefano, PhD
Post Doc Researcher
stefano.crabu@unipd.it

Draetta Laura, PhD
Associate Prof.
laura.draetta@telecom-paristech.fr

Rizza Caroline, PhD
Associate Prof.
caroline.rizza@telecom-paristech.fr

Partenaires

THE STUDY

The concept of "Silence of the chips" (SoC)

- Elaborated while the use of RFID has been generalized (2005)
- Individuals should be able to disconnect their 'objects' from digital infrastructures at any time

Our research question

In a hyper-connected world characterized through the generalization of the IoT, does the concept of SoC relevant to protect consumers/citizens from the violation of their privacy?

The approach / methodology

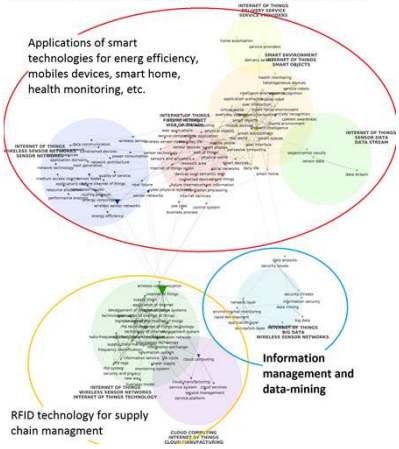
a) The emergence and genealogy of the IoT in relation to the RFID device:
   → Scientific literature review *(ISI Web of Science)* and documentary analysis

b) Opening the black box of the IoT by exploring the techno-scientific debate related to the issues of security and privacy in the field of the IoT
   → Bibliometric cartography of the scientific debate *(Cortext platform)*

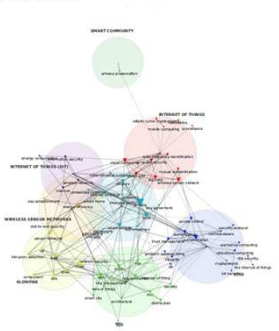
c) Collecting the voices of the policymakers & embracing the techno-scientific vision wrt the right to the SoC:
   → 6 in-depth interviews with 3 policymakers/advisors *(DG Connect – UE; CNIL; Institut de la Souveraineté Numérique)* and 3 researchers *(CNRFID and JRC)*

RESULTS: some key illustrations

Techno-scientific fields of the IoT:
Semantic network of the top 150 terms text-mined from the dataset



Security & Privacy in IoT context:
Semantic network of top 90 terms text-mined from the dataset



- **The concept of SoC is absent** of the techno-scientific literature & debate
- **Predominance of technical solutions to guarantee the security** of the infrastructures through which smart objects are connected anytime & anyplace
- Techno-scientific contributions do not strongly put into question issues related to the life cycle of information generated by smart objects (*i.e.* **few consideration about 'privacy'**)

- **From the interviews:**

The SoC: a 'concept' without 'real' technical solutions, a political construction to promote the idea of the necessity to control their own personal data in order to protect citizens/consumers' privacy.

RECOMMENDATIONS: Beyond this concept, which new strategy?

Main policy recommendations (ex.)

- Strengthening the autonomy of/ empowering the users in managing the entire lifecycle of their personal data in the IoT & IoEverything
- Activating a full right of access, modification, and deletion of personal data generated by users through IoT devices & in the IoEverything
- Supporting an European initiative supporting an institutional ethical brand in order to promote privacy & security as central assets for enterprises

Main industrial guidelines (ex.)

- Providers: Ensuring transparency, even for non-experts, about data collection, storage & possibility to edit/delete it.
- Consistently resorting to the *privacy-by-design* principles
- Supporting the design of technical functionalities, apps & objects allowing users to export / edit / delete in a friendly way their personal data (both in raw & aggregated format) & allowing the personalization of privacy management following the different types of users (e.g. Kids)

Programme Futurs & Ruptures
26 janvier 2016

Internet of Highly Mobile Things

MOBILITY MANAGEMENT CHALLENGES

On different layers of the communication stack

Transport: Keep session continuity

Network: Keep connectivity with routing topology

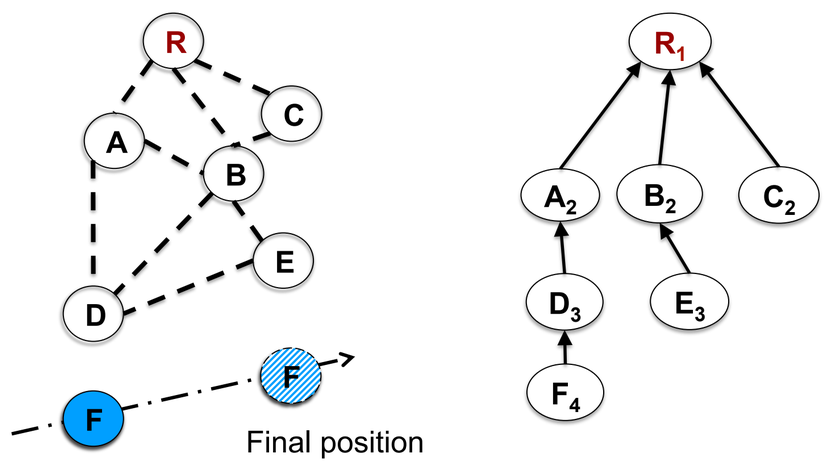
Data link (MAC): Integrate in transmissions

- **Focus on Network layer mobility:**
  Routing based solution using RPL

Image credit: http://www.3g.co.uk/PR/Feb2015/internet-of-things-everything-you-need-to-know.html

SCIENTIFIC CONTRIBUTION

Problem statement



Physical topology — Initial position

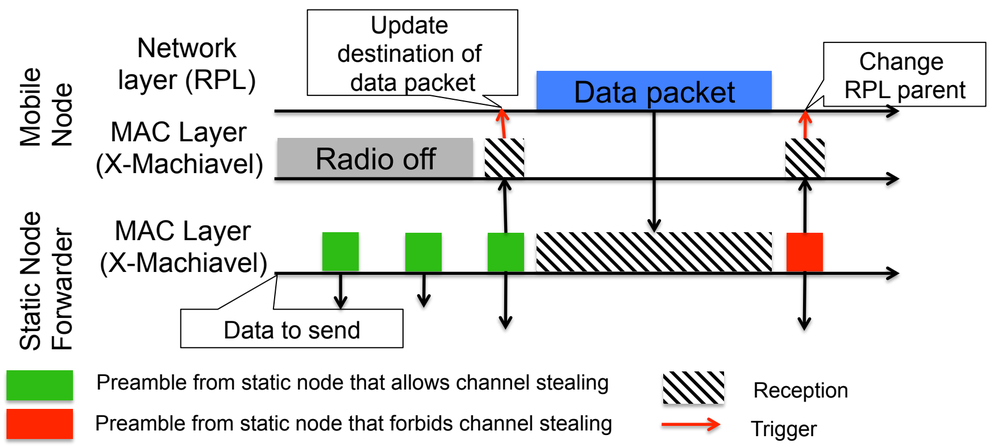
RPL DODAG Initial Position

RPL Message exchange

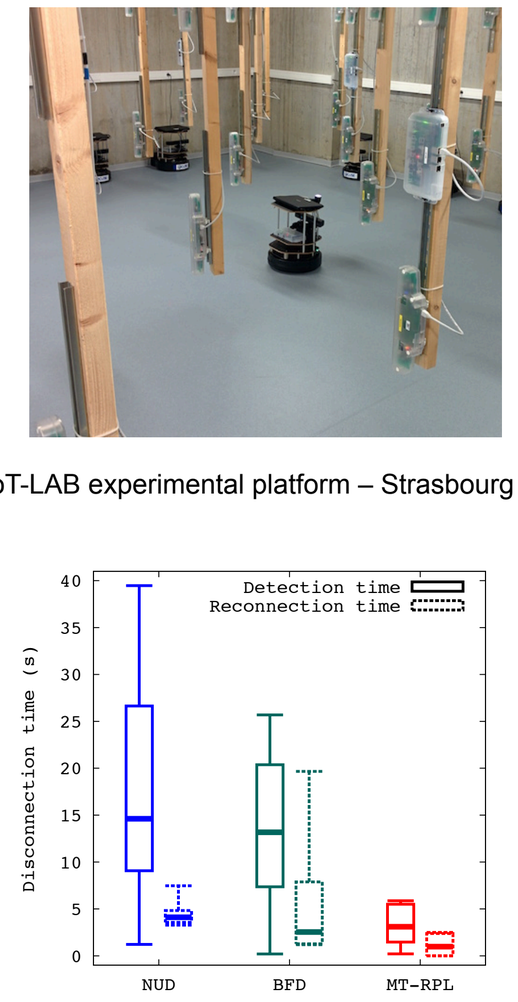
Radio link — X_Y Node id X, rank Y — Mobile Node Path

Metric - Hop count — Chosen parent — Mobile Node

Mobility-Triggered RPL



- Opportunistic forwarding through channel stealing



FIT IoT-LAB experimental platform – Strasbourg

Mobile node disconnection time – Strasbourg experiments

Conclusion

Enabling parent unreachability detection at mobile nodes

- reduces node disconnection time from the routing topology
- improves packet delivery ratio

Perspectives

- Enhance experiments with multiple mobile nodes
- Mobility between multiple DODAGs

Publications

[1] **C. Cobârzan**, J. Montavont and T. Noël, Integrating mobility in RPL, in proceedings of the 12th European Conference on Wireless Sensor Networks (**EWSN 2015**), Porto, Portugal, February 2015

[2] J. Montavont, **C. Cobârzan** and T. Noël, Theoretical Analysis of IPv6 Stateless Address Autoconfiguration in Low-power and Lossy Wireless Networks, in proceedings of the 11th IEEE-RIVF International Conference on Computing and Communication Technologies (**RIVF'15**), Cantho, Vietnam, January 2015

[3] **C. Cobârzan**, J. Montavont and T. Noël, Analysis and performance evaluation of RPL under mobility, in proceedings of the 19th IEEE Symposium on Computers and Communication (**ISCC'14**), Funchal, Portugal, June 2014

Auteurs

Cosmin Cobârzan
Julien Montavont
Thomas Noël

Parties prenantes

Partenaires

Journée Futur & Ruptures 2016

Janvier 2016

Contact cobarzan@unistra.fr

Site web http://icube-reseaux.unistra.fr/

Cloud resource scheduling and pricing

Parties prenantes

EURECOM
Sophia Antipolis

Auteurs

Patrick Loiseau
Xiaohu Wu

Partenaires

FONDATION TELECOM

INSTITUT CARNOT Télécom & Société numérique

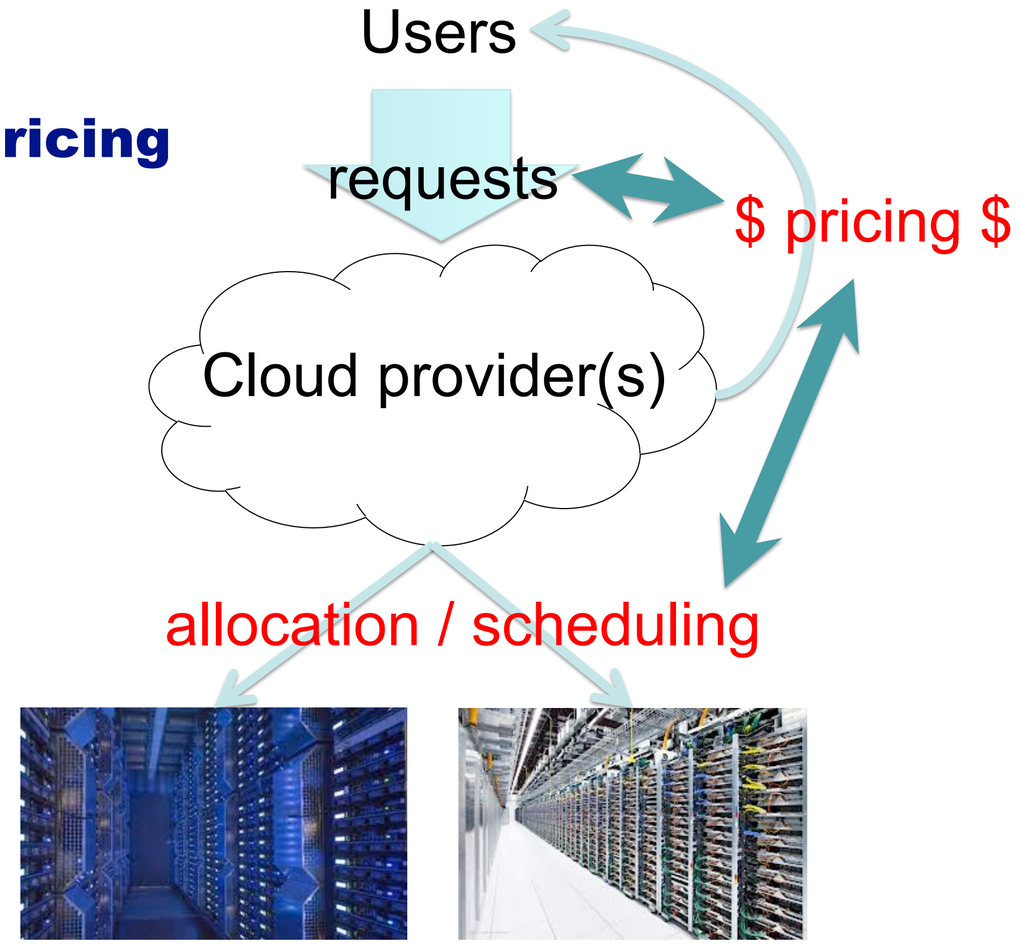
Cloud resource allocation and pricing

Context and challenges

- Gap between tenants needs and cloud providers offer
  - ➢ inefficiencies and potential loss of revenue

Main questions

- How to allocate resources in the data center?
  - ➢ Batch jobs: how to schedule parallel tasks with deadlines?
- How to price requests?
  - ➢ Objective: maximizing revenue/social welfare
  - ➢ Challenge: first understand how users will allocate resource between instances to minimize their cost



Scheduling work-preserving tasks (ex: Hadoop)

Model

- Cloud of capacity C, n tasks to schedule
- Tasks are defined by (1) value v_i (2) demand D_i (3) parallelism constraint k_i (4) deadline d_i
- Work preserving: demand remains constant if executed in parallel with p_i processors

Core results

- A boundary condition under which a set of tasks can be scheduled on C machines
- A scheduling algorithm that maximizes the resource utilization
  - Complexity $O(n^2)$
  - LDF (latest deadline first): allocate from deadline towards earlier slots, move previous allocation to fit a new job if necessary

➢ New framwork to design and analyze algorithms for various objectives with deadlines

Applications:

- Best possible greedy algorithm for social welfare optimization
- First exact dynamic programming algorithm for social welfare optimization
- First exact algorithm for machine minimization
- A (1, 1+eps)-approximation algorithm for the general minmax objective

Other scheduling problems

Scheduling monotonic tasks

- Monotonic tasks: allocating more processors increases demand
  - ➢ Captures inefficiencies introduced by parallelization
- Result: generic greedy approximation algorithm, 2/3-approximation under mild assumption

Learning framework to allocation instances

- Flexible scheduling between reserved, on-demand and spot
- Learning algorithm to allocation between spot and on-demand

Contact patrick.loiseau@eurecom.fr
xiaohu.wu@eurecom.fr

Site web www.eurecom.fr/~loiseau/

MFC: Memory-based Flexible Computing

Stakeholders

Authors

Postdoc F&R: Yeter Akgul

Télécom Bretagne/Lab-STICC:
Amer Baghdadi
Vincent Gripon

CNRS/Lab-STICC:
Jean-Philippe Diguet

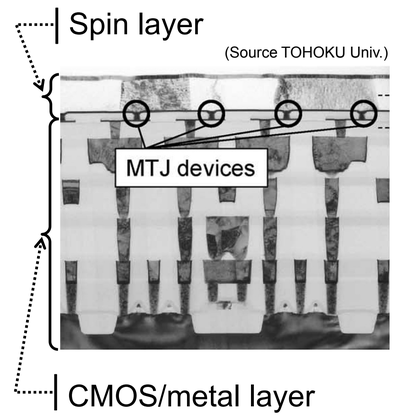
TOHOKU University:
Takahiro Hanyu
Naoya Onizawa

Partners

Context & Objective

Disruptive technology: Memristors

- Original features to overcome current barriers: low power, configuration backup, logic-in-memory, CMOS compatible, Back End Of Line integration.
- Several variants of emerging non-volatile memory technologies: Phase Change RAM, Magnetic RAM, Resistive RAM (Conductive-Bridge RAM and Metal oxide RAM)
  ➔ MTJ (Magnetic Tunnel Junction) RAM technology available at **TOHOKU University**



Proof-of-concept application: Sparse Clustered Network (SCN)

- Original neural network approach based on information theory proposed in Telecom Bretagne
- Search engine in large databases as target application

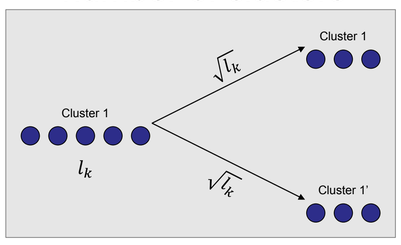
Objective: proposal of novel reconfigurable energy-efficient architecture models that take full advantage of emerging memristors technologies

Contribution 1

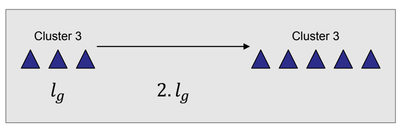
New SCN homogenization approach

- Trade-off area/error rate P_e for the SCN
  - Area ← max. number of interconnection
  - P_e ← number of fanals l_i in the cluster c_i and number of messages stored
- Homogenization of the Database

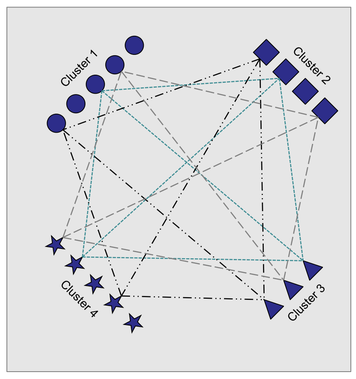
1. Cut the biggest clusters if $\max(l_k) \gg \max(l_g)$, with $k, g \in [1, N], N$ the number of clusters

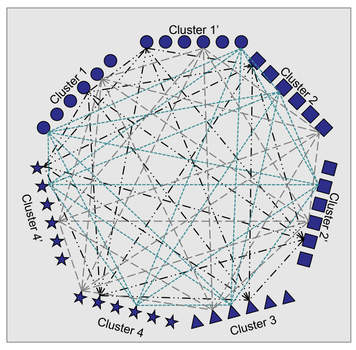


2. Duplicate the smallest clusters



3. Duplicate the cut clusters if necessary to homogenize the SCN



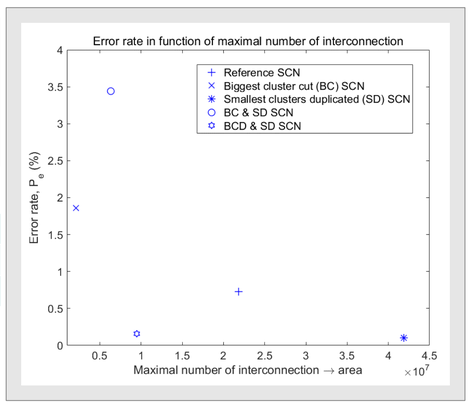


Results

- Reference SCN
  - [100; 200; 300; 400; 500; 256; 256; 1000]

100	200	300	400	500	256	256	10000
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	ceil($\sqrt{l_8}$) ceil($\sqrt{l_8}$)
5	3	2	1	1	2	2	1
5	3	2	1	1	2	2	ceil($\sqrt{l_9}$) ceil($\sqrt{l_8}$)
5	3	2	1	1	2	2	5.ceil($\sqrt{l_8}$) 5.ceil($\sqrt{l_8}$)

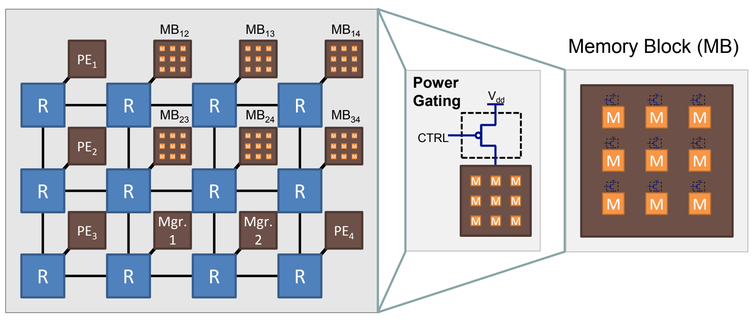
SCN	BC	SD	BC&SD	BCD&SD
P_e	×2.55	÷6.94	×4.71	÷4.52
Area	÷10.4	×1.92	÷3.43	÷2.30



Contribution 2

Flexible MTJ and NoC based design

- Trade-off area/performance/power consumption
  - Area ← size of the Network on Chip (NoC), number of memories and size of memories
  - Performance ← latency of the NoC, access time of MTJ
  - Power consumption ← power consumption of Memory Blocks (MB) and granularity of Power Gating (PG) technique



- Flexibility parameters
  - Size of the NoC
  - Size & number of Memory Blocks
  - NoC mapping
  - Memory mapping (**shared** MB or not)
- Ongoing work at **TOHOKU University**
  - Extract power consumption, access time and configuration time of MTJ Memory Blocks
  - Establish a model of power consumption
  - Extract the power consumption of the NoC
  - **Two publications** on SCN homogenization approach & MFC NoC-based implementation

Perspectives

- Power Management methods to advise trade-off values of the flexibility parameters
- Extension of the proposed memory-based flexible computing to other application domains

Journée Futur & Ruptures à l'Institut Mines-Télécom
January 26th, 2016

Contact amer.baghdadi@telecom-bretagne.eu **Web site** http://departements.telecom-bretagne.eu/elec/

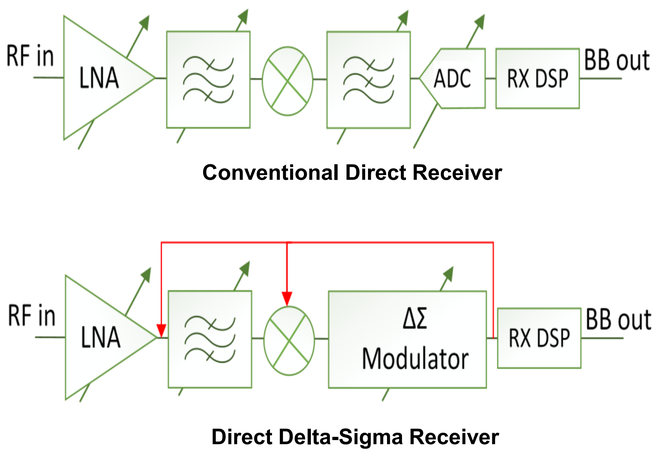
A Discrete-Time Direct Delta-Sigma Receiver for SDR

Challenges for Flexible Receivers

- High numbers of bands and standards ➡ **High Flexibility**
- Coexistence with strong blockers ➡ **High Dynamic Range**
- Handset applications ➡ **Low Power Consumption**

5 GSM bands
4 CDMA bands
5 HSDPA bands
1 EVDO band
2 TD-SCDMA bands
20 LTE bands
WLAN/Bluetooth/GPS/NFC

[http://www.gsmarena.com/]



Direct Delta-Sigma Receivers (DDSR)

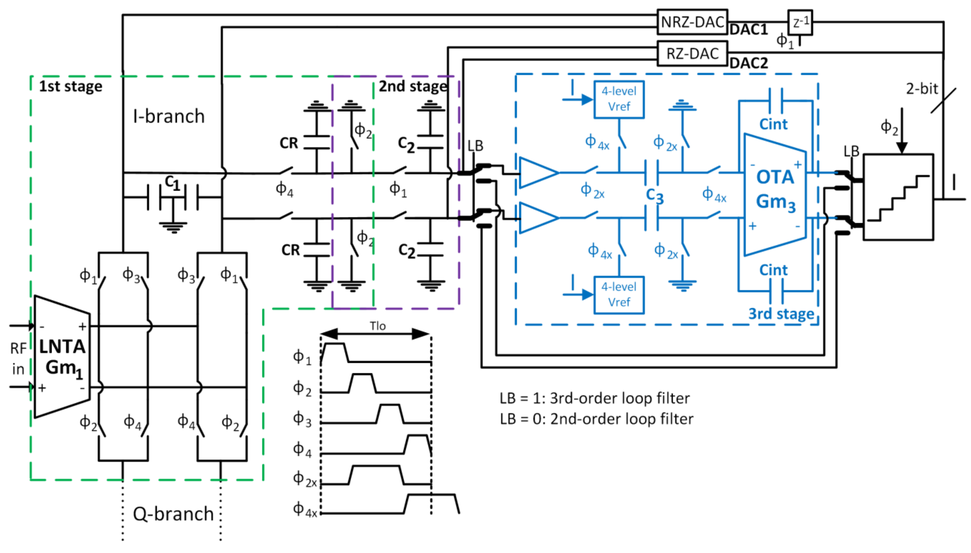
- Feedback from the baseband to the RF blocks

The whole receiver is an ADC

- The RF feedback loops :
  - Reduce the swing at RF ➡ Better linearity
  - Increase number of ADC stages ➡ Better resolution

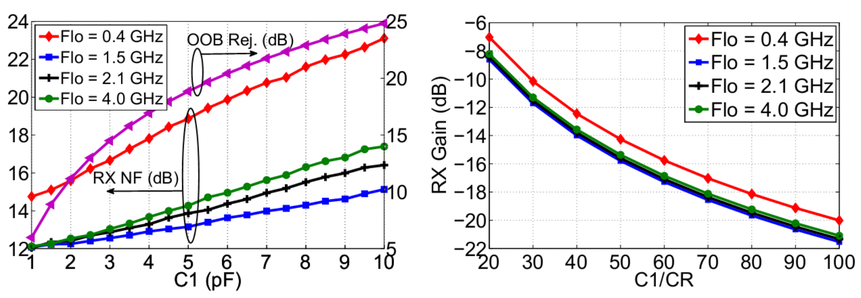
Proposed 2nd/3rd-order DT DDSR

- 1st stage: 25% duty-cycle passive mixer
- 2nd stage: passive integrator to save power
- 3rd stage: can be turned off/on in high/low bands to have good NF & power efficiency
- Quantizer: 2-bit for good trade-off between quantization noise and complexity
- RF DAC : NRZ for low jitter sensitivity



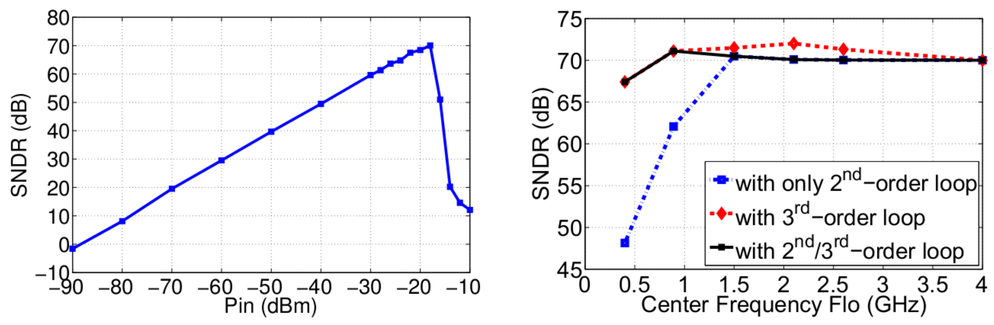
Receiver Design

- Target 0.4 GHz – 4.0 GHz bands, 10 MHz BW, 65 dB SNDR
- Design in a 1.2 V 65 nm CMOS technology from STM
- Size C1, C2 based on NF and OOB rejection
- Size C1/CR, C2/CR ratio based on receiver gain



Simulation results

- Obtained SDNR from 67.4 dB to 71.1 dB
- 3rd-order improves the SNDR by 19 dB at 0.4 GHz
- Obtained SDNR from 67.4 dB to 71.1 dB
- Achieved 10 dBm receiver IIP3



Conclusions

- Compared with [2], the resolution improvement in low bands is 1 to 3 bit at the cost of 10 % power consumption increase
- Compared with the DDSR in [1], the receiver features fewer RF stages and quantization noise folding free

References

[1] M. Englund *et al.*, “A Programmable 0.7-to-2.7 GHz Direct Receiver in 40 nm CMOS,” *IEEE J. Solid-State Circuits* , vol. 45, no. 99, pp. 1–12, 2015.
[2] C. Wu *et al.*, “A Wideband 400 MHz-to-4 GHz Direct RF-to-Digital Multimode Receiver,” *IEEE J. Solid-State Circuits* , vol. 49, no. 7, pp. 1639–1652, July 2014.
[3] M.T. Nguyen *et al.*,“A Flexible Receiver Using ΔΣ Modulation,” to be published in *ISCAS*, May 2016.

Parties prenantes

Auteurs

Minh Tien Nguyen
Chadi Jabbour
Van Tam Nguyen

Partenaires

Contact mnguyen@telecom-paristech.fr
Site web

Timed FSM strategy for optimizing web service compositions w.r.t. the quality and safety issues

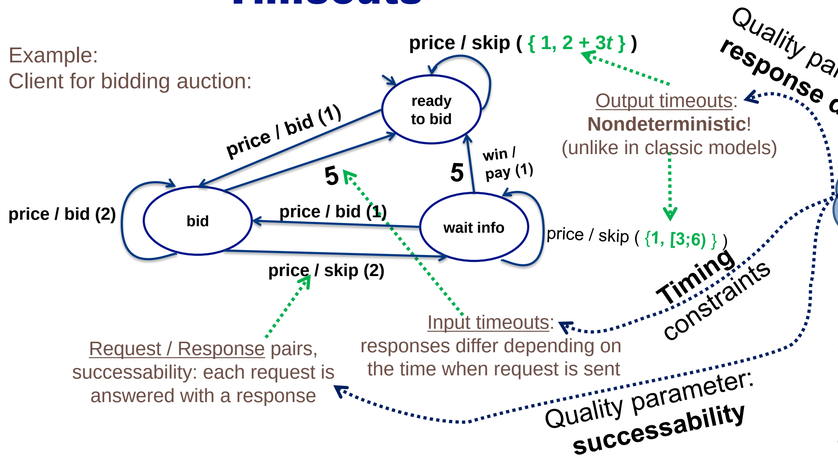
THESIS OVERVIEW

Started: 01.10.2012 **Defended: 03.12.2015** NNT : 2015SACLL004

Objectives:

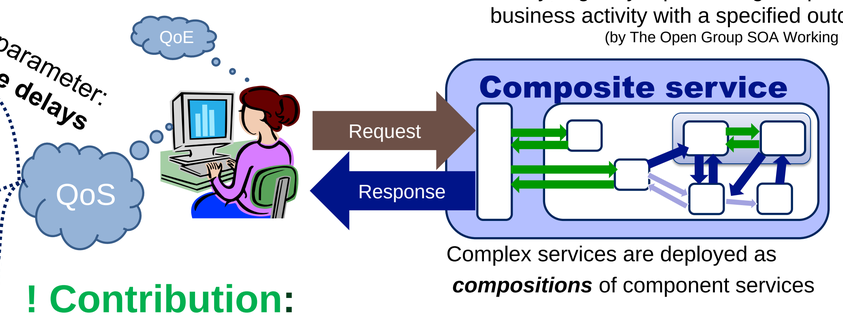
- Propose a finite state model capable of **integrating functional, quality** and **safety requirements** for complex services.
- **Define a composition** for the proposed model for describing communicative behavior of complex services.
- Develop methods for effective **optimal component selection** based on proposed model.

Finite State Machine with Timeouts



Service-oriented architecture

Service – a self-contained unit of functionality, logically representing a repeatable business activity with a specified outcome
(by The Open Group SOA Working Group)

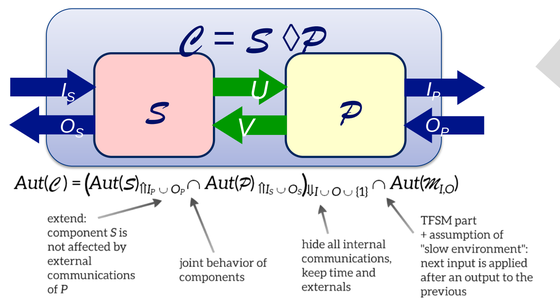


Complex services are deployed as ***compositions*** of component services

! Contribution:

We propose the **time-nondeterministic** extension of the model of an FSM with Timeouts (TFSM).
This extension allows us to describe component services with nondeterministic behavior, and to derive the composition of nondeterministic component services.

Parallel composition



Binary composition can be extended to multiple-component case due to associative nature of parallel composition operator.

COMPOSE

VERIFY

OPTIMIZE

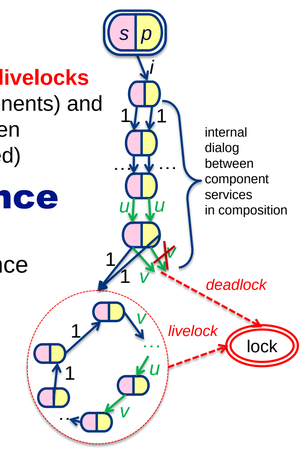
SELECT

Questions to answer:

? Whether the parallel composition of given components satisfies given functional and quality requirements, while providing safe communication between components?

Safety-awareness

We have proposed explicit detection of **livelocks** (infinite internal dialogs between components) and **deadlocks** (when internal dialog between component services cannot be continued)



Functional conformance

We adapt trace-based conformance relations between TFSMs (equivalence and trace inclusion)

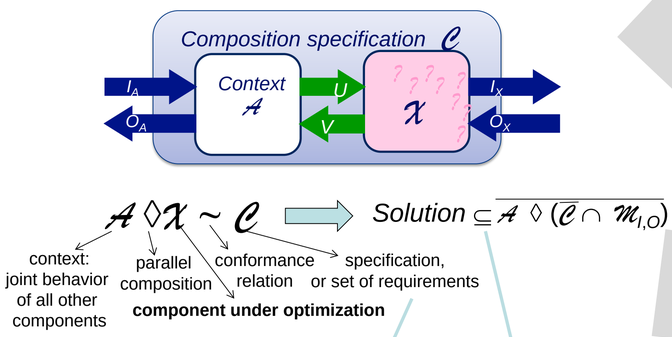
Quality restrictions

Check that composition has output delays within specified intervals

! Contribution:

Checking the **conformance** between models with real values of time variable is a complex issue. Hence, we prove that two given TFSMs are conforming if and only if they are conforming w.r.t. **integer time instances**.

Solve equation



! Contribution:

We have proposed a method for **deriving** the largest solution containing **all permissible component service behaviors**, based on solving TFSM parallel equation.

! Contribution:

We have proposed a method for **minimization of the set of requirements** for service compositions given over finite number of scenarios: the method is based on comparing which parts of the component under optimization are involved in satisfying or violating each required scenario.

Questions to answer:

? Whether it is possible to **optimize** some of the components to ensure that composition meets quality restrictions?

- ...no livelocks and deadlocks? (**safety requirements**)
- ... optimal delays? (**quality requirements**)

! Contribution:

We have proposed algorithms to **extract** restricted solutions with **required properties**:
• minimizing the **size** of the component service;
• choosing optimal **output delays** (max / min);
• **minimizing** the amount of **changes** in given component to derive an optimal one;
• **ensuring safety** of the chosen solutions.

Directions for future work

• Multi-stimuli composition
• Timeout functions for other quality parameters
• Integration of developed methods with service discovery

Auteurs

Olga Kondratyeva

Thesis supervised by
Ana Cavalli
(Telecom SudParis, France)
Nina Yevtushenko (Tomsk State University, Russia)

Partenaires

FONDATION TELECOM

INSTITUT CARNOT Télécom & Société numérique

Acknowledgements

Jury of the thesis:

M. David Sadek (Institut Mines-Télécom)
Prof. Pascal Poizat (Université Paris Ouest)
Prof. Roland Groz (Grenoble INP)
Prof. Sébastien Salva (Université d'Auvergne)
Mme Fatiha Zaïdi (Université Paris-Sud XI)

Main results published in:

- Kondratyeva O., Kushik N., Cavalli A., Yevtushenko N. Using Finite State Models for Quality Evaluation at Web Service Development Steps. International Journal on Service Computing (IJSC), ISSN 2330-4472, 2013. Issue 1(1), pp. 1-12.
- Kondratyeva O., Yevtushenko N., Cavalli A., Solving parallel equations for Finite State Machines with Timeouts. Proceedings of the Institute for System Programming. 2014. Volume 26 (Issue 6), P. 85-98 (peer-review journal, in Russian)
- Kondratyeva O., Yevtushenko N., Cavalli A., Parallel composition of nondeterministic Finite State Machines with Timeouts. Tomsk State University Journal of Control and Computer Science. 2014. Volume 2 (Issue 27). P. 73–81. (peer-review journal, in Russian)
- Kondratyeva O., Kushik N., Cavalli A., Yevtushenko N. Evaluating Quality of Web Services: a Short Survey / Proceedings of the IEEE 20th International Conference on Web Services (ICWS 2013), July 2013. – pp. 587-594. (rank A conference)
- Kondratyeva O., Kushik N., Cavalli A., Yevtushenko N. Evaluating Web Service Quality using Finite State Models / Proceedings of the 13th International Conference on Quality Software (QSIC 2013), July 2013. – pp. 95-102.

Presentation of results:

- Poster presentation at La Journée Futur &Ruptures (l'Institut Mines-Télécom), the best poster award, January 2014
- International Conference on Web Services (ICWS 2013), 27 June – 2 July 2013, Santa Clara, California, USA (rank A conference)
- First Franco-Russian Seminar on Software Verification, Testing, and Quality Estimation, November 2014, Paris, France
- 10th International Summer School on Training And Research On Testing (TAROT 2014), 30 June – 04 July 2014, Porto, Portugal
- Tarragona International Summer School on Trends in Computing (SSTiC 2014), 07 July – 11 July 2014, Tarragona, Spain
- Concours “Ma Thèse en 180 secondes”, 07 April 2014, Université Evry Val d'Essonne, Evry, France

Journée Futur & Ruptures 2016

Janvier 2016

Contact kondratyeva.olga.vic@gmail.com

Generic Autonomic Service Management for Complex Systems

Parties prenantes

Auteurs

Nabila BELHAJ
Djamel BELAÏD
Samir TATA

Partenaires

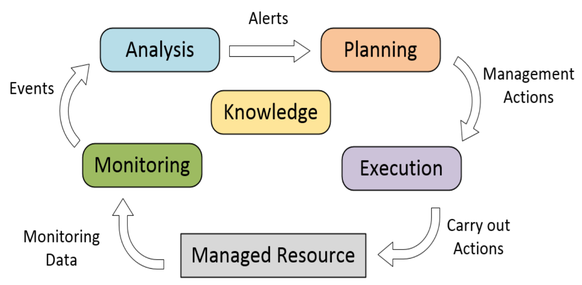
Complex systems and necessity for Autonomic Computing

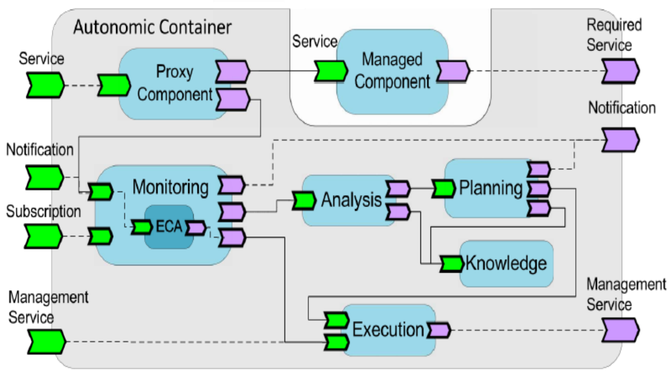
Complex System

- System composed of distributed systems
- Continuous and dynamic evolution due to increasing size
- Complex design with unpredictable behavior

Autonomic Computing

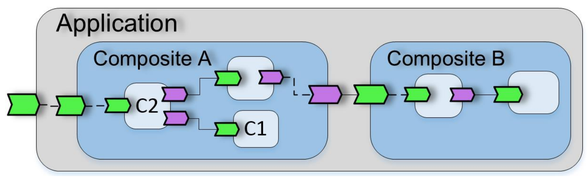
- Self-properties of: Configuration, Optimization, Protection and Healing

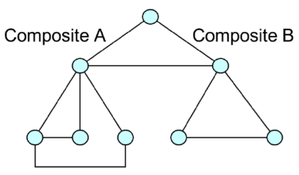




Example - Component-based Applications

- Composite encapsulating components
- Horizontal and vertical relationships exist between components





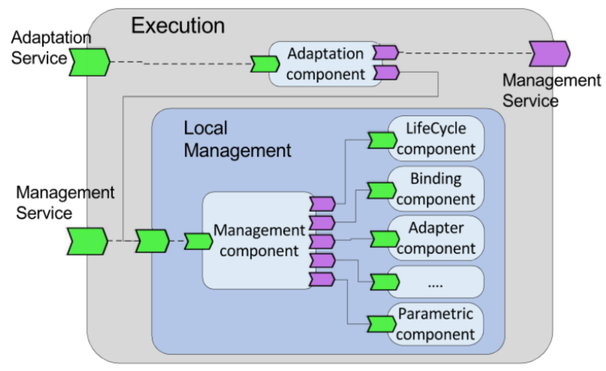
Contribution objectives

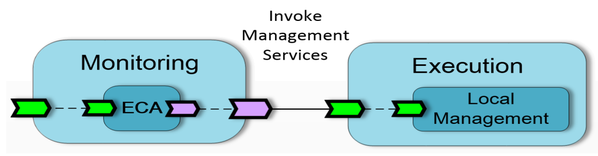
- Free application developers from the burden of management tasks to focus on their business requirements
- Propose a generic and flexible AM for the management of component-based applications
- Make autonomic loops collaborate for the overall management of an application

Structure of the Autonomic Container

- Provides autonomic management facilities and collaboration capabilities
- Separates the functionalities offered by a classical autonomic loop and provides them into separate components in purpose of flexibility and reusability

- The adaptation plan may entail the invocation of the Local Management service for local adaptations or Remote Management services for remote adaptations witch requires collaboration between containers
- The container performs reactive and deliberative autonomic loops

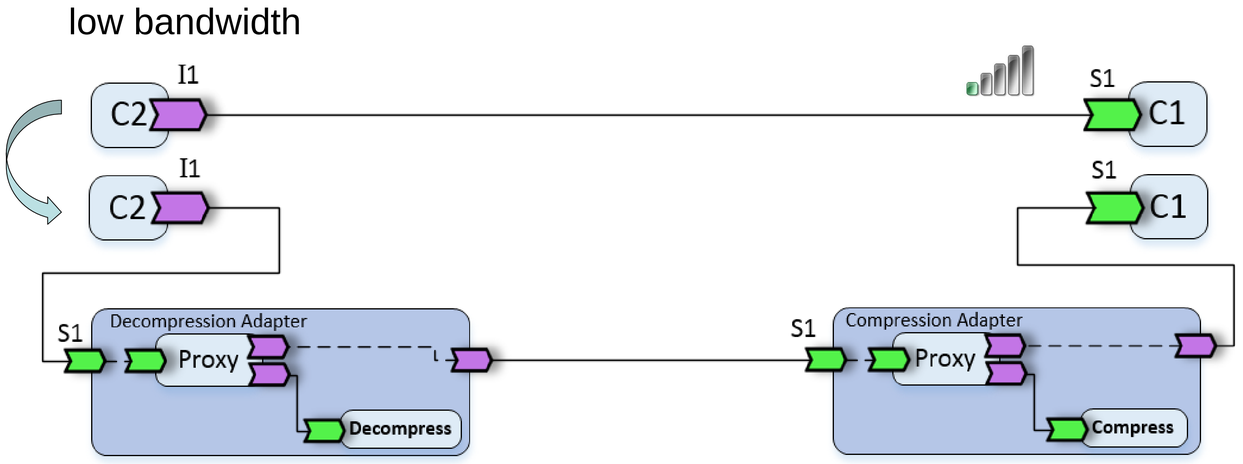




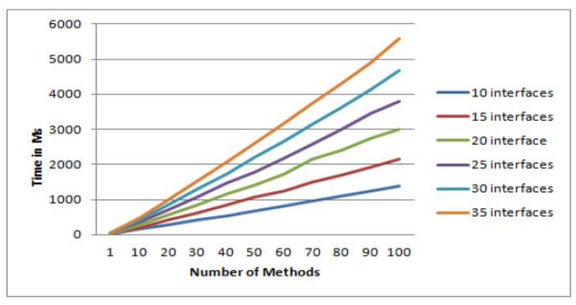
Implementation and Evaluation Results

- Implementing container and components using SCA standard - FraSCAti
- Mapping some of the container's functionalities to REST queries to the PaaS manager when deployed in the Cloud

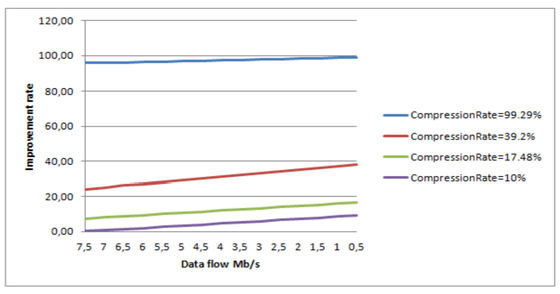
- Evaluation of a performed Adaptation – Horizontal Collaboration
  - Reasonable time for proxy generation even with several implemented interfaces
  - Introduction of the adapters enhances the components' behavior even in low bandwidth



- Settling time of the adaptation



- Accuracy of the adaptation



Future Work

- Investigation of machine learning techniques to support predictive analysis and learning strategies planning
- Investigation of autonomic management and collaboration among containers in Pervasive and Cloud environments

Contact nabila.belhaj@telecom-sudparis.eu Site web http://inf.telecom-sudparis.eu/fr/

Futur et Ruptures Journey
January 2016

Context aware refinement planning for robots in pervasive environments

Authors

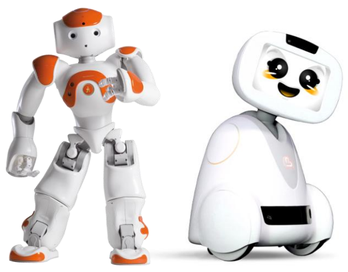
Nathan Ramoly

Amel Bouzeghoub

Béatrice Finance

Robots

- Personal companion robots
- Help users in their everyday life
- Operate in non dedicated environments



Smart Environments

- Enhanced environment with smart devices
- Sensors and actuators
- Provide helps to users (smart homes)

Robots in smart homes: Provide high quality services to users

=> How to handle task planning for robots in smart environments ?

1. Motivations/Problem

- Classical planner (STRIPS, HTN, etc.) limitation:
  - Highly variable context => outdated plan
  - Data unavailable at planning => incorrect plan
- Smart environment constraints:
  - Numerous sensors => data overflow
  - Limited devices => useless query
  - Energy, memory, processing, etc…

2. Objectives

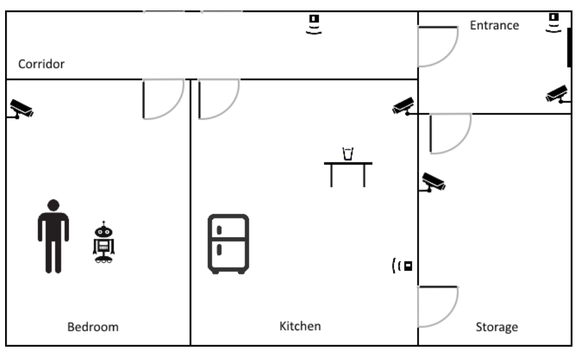
- Use an adapted planning paradigm
- Handle context sensitive plan
- Observe partially and smartly the context

3. Solutions

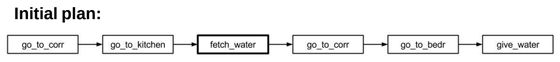
- **Dynamic HTN**: Task planner based on HTN
- Plan created on the fly, step by step
- Context observation at runtime through time window
- Partial context observation based on preconditions

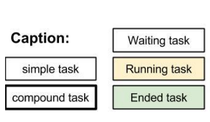
Running example:

The robot is asked to fetch some water for the user

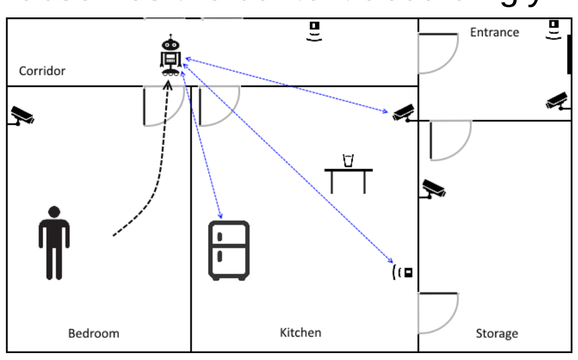


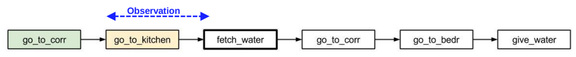
Initial plan:



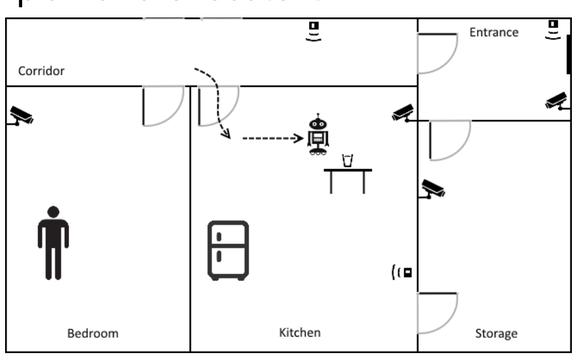


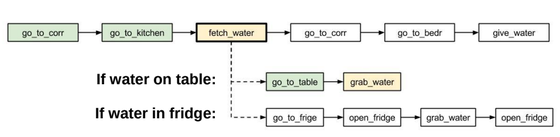
The robot will soon need to refine a task (fetch_water): it observes the context accordingly



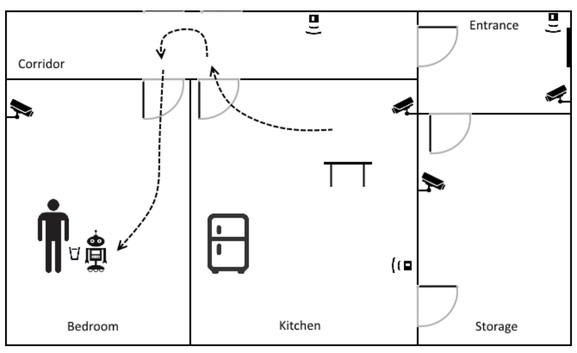


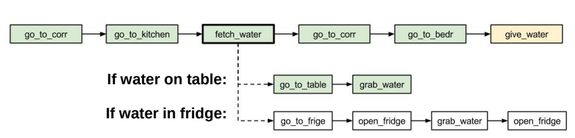
The robot uses the updated partial context to select a sub-plan and execute it





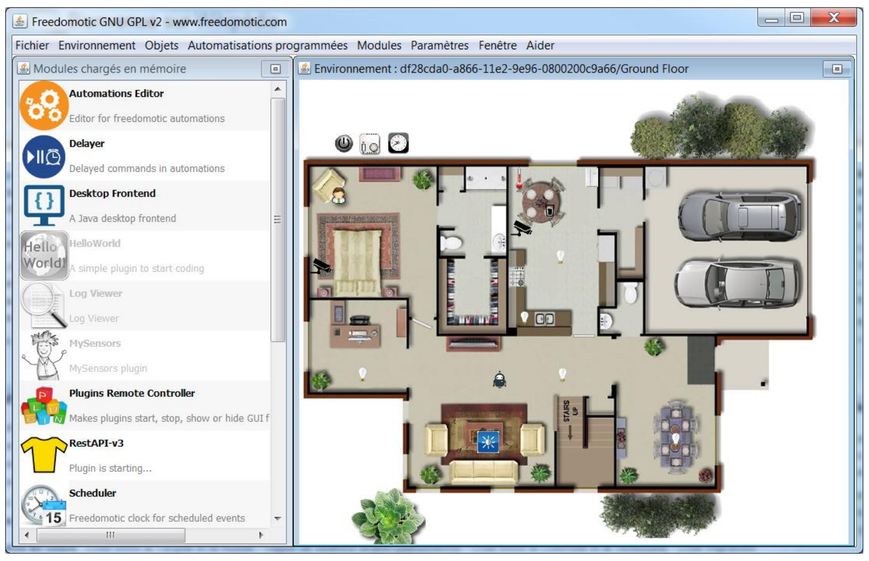
The robot has delivered a drink, the user is happy



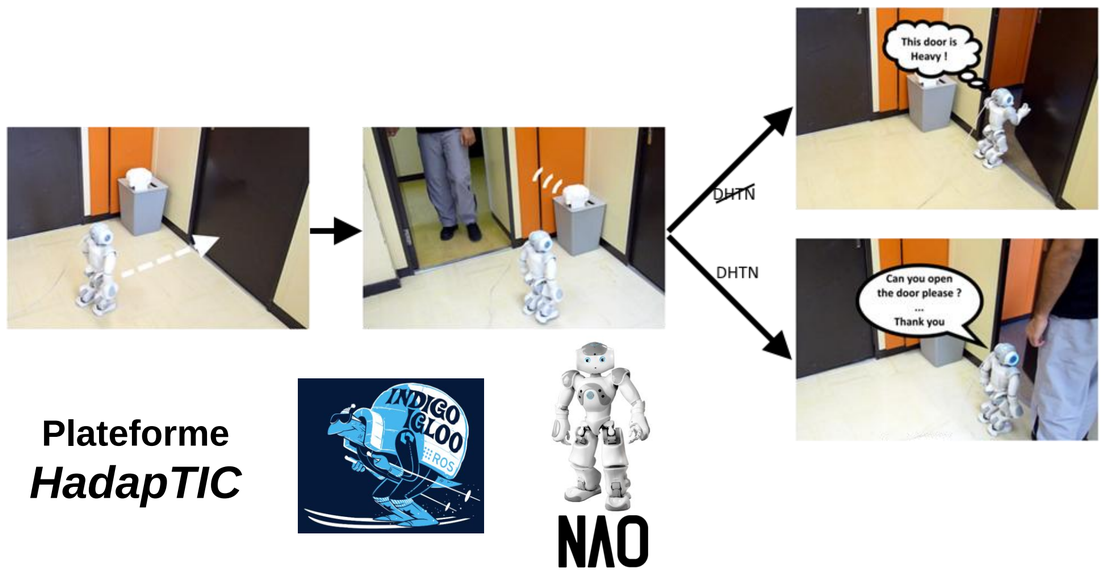


Implementation:

Simulation



Real robot



Plateforme *HadapTIC*

NAO

Journée Futur et Ruptures

Janvier 2015

Contact nathan.ramoly@telecom-sudparis.eu

Site web www.nara.wp.tem-tsp.eu

Personal data in networks: incentives and fair monetization

Parties prenantes

EURECOM
Sophia Antipolis

Auteurs

Michela Chessa

Patrick Loiseau

Collaborations:

Jens Grossklags (PennState)

Stratis Ioannidis (Northeastern)

Partenaires

Incentives for high quality data release

Context and challenges

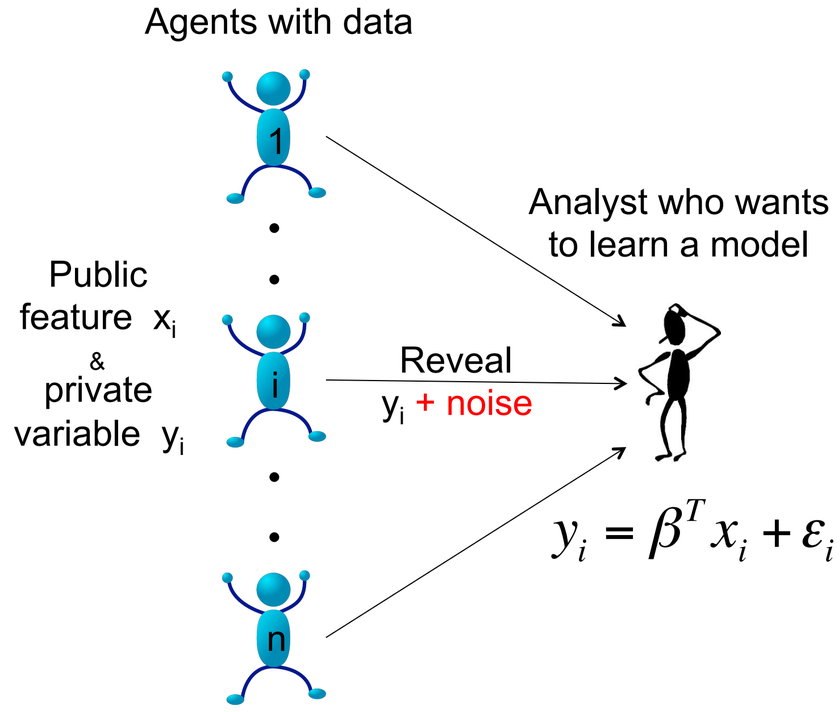
- Useful data gathered from external agents
  - ➢ Need to incentivize agents to provide high quality data

General model

- Linear regression as a non-cooperative game
  - Users max f(estimation precision) – cost(added noise)
- ➢ Information as a public good quantified by estim. precision

Main results

- Incentive compatibility of GLS
  - Users reveal the variance added truthfully (almost)
- New incentive mechanism
  - Impose maximum added noise (with drop-out option)
  - Procedure to compute the optimal maximum imposed
  - Increases aggregate precision (simple, non-monetary, efficient)



Quantifying the value of data in networks

Main problem and challenges

- How to quantify the value of personal data revealed by a user?
  - ➢ It depends on the data revealed by other users (externalities)
  - ➢ Externalities are often local (social networks)

Our solution

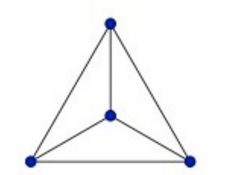
- Propose a cooperative extension of a local public good game
  - Users choose the precision d_i of data revealed

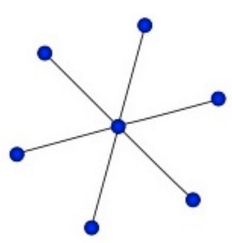
$$U(d_i, d_{-i}, g) = f(d_i + \delta \sum_{j \in N_i(g)} d_j) - k d_i \qquad v(S) = \max_{d_S} \sum_{i \in S} U(d_i, d_{S-i}, g_S)$$

- Quantify value of each user's data by allocation (solution of the cooperative game)
  - ➢ Shapley value, core

Main results

- Game is monotonic and superadditive → core non-empty, Shapley stable for some topologies
- No incentive to hide link, complete graph efficient → dense graphs yield more value





Publications

- M. Chessa, S. Ioannidis and P. Loiseau. Linear Regression and Incentive Compatibility. Preprint, 2015.
- M. Chessa and P. Loiseau. A cooperative game-theoretic approach to quantify the value of personal data in networks. Preprint, 2015.
- M. Chessa and P. Loiseau. The impact of the graph structure on a public good provision game: a cooperative approach with applications to personal data release on social networks. SING11-GTM2015, European meeting on game theory 2015.
- M. Chessa, J. Grossklags and P. Loiseau. A Game-Theoretic Study on Non-Monetary Incentives in Data Analytics Projects with Privacy Implications. CSF '15.
- M. Chessa, J. Grossklags and P. Loiseau. A short paper on the incentives to share private information for population estimates. FC '15.

Journée Futur & Ruptures

Janvier 2016

Contact patrick.loiseau@eurecom.fr

Site web www.eurecom.fr/~loiseau/

Analyse de Séquences Faciales 3D en vue de la Reconnaissance d'Identité et la Détection d'Emotions

Parties prenantes

Auteurs

Taleb Alashkar (Doctorant*)

Boulbaba Ben Amor (Porteur du projet et encadrant de la thèse, Télécom Lille)

Mohamed Daoudi (Directeur de thèse, Télécom Lille)

Stefano Berretti (Collaborateur, Université de Florence, Italie)

*Thèse soutenue le 2/11/2015, Taleb est actuellement post-doctorant à Northeastern University, Boston, USA.

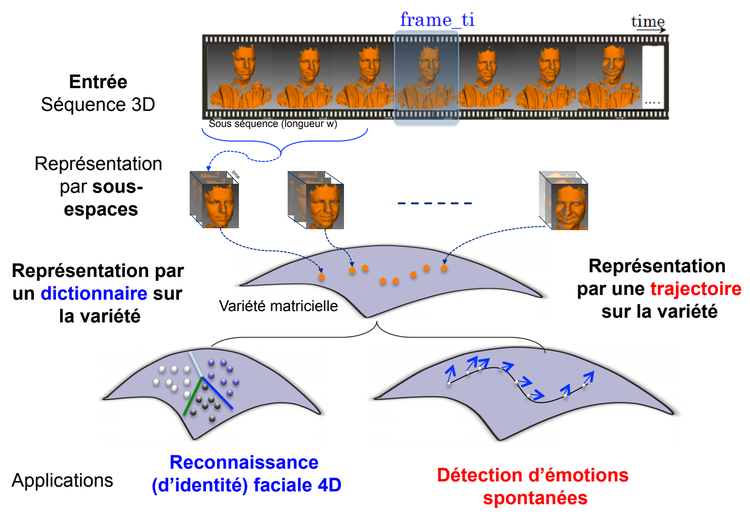
Partenaires

Introduction et défis scientifiques

Quel rôle de la dynamique faciale dans la reconnaissance d'identité et d'émotions?

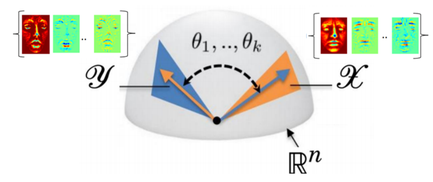
- Motivation à l'analyse faciale 4D (3D+temps)
  - Robustesse aux variations d'illumination et de pose,
  - Richesse en géométrie (forme) et déformations – certaines Unités d'Action (AU) cachées en 2D sont visibles en 3D,
  - Disponibilité de capteurs 4D de haute résolution (e.g. Di4D) et l'émergence de capteurs légers et grand public (e.g. Kinect)

- Défis scientifiques de l'analyse faciale 4D (3D+temps)
  - Le volume important des données (aucune compression!),
  - Données bruitées, peu précises et de faible résolution (dans le cas des données Kinect),
  - Données non-recalées (dans le temps) en présence de transformations rigides (rotation et translation) et non-rigides (expressions faciales),
  - Données manquantes (capteur à une seule vue).



Méthodologie proposée – deux représentations possibles : par des dictionnaires ou des trajectoires.

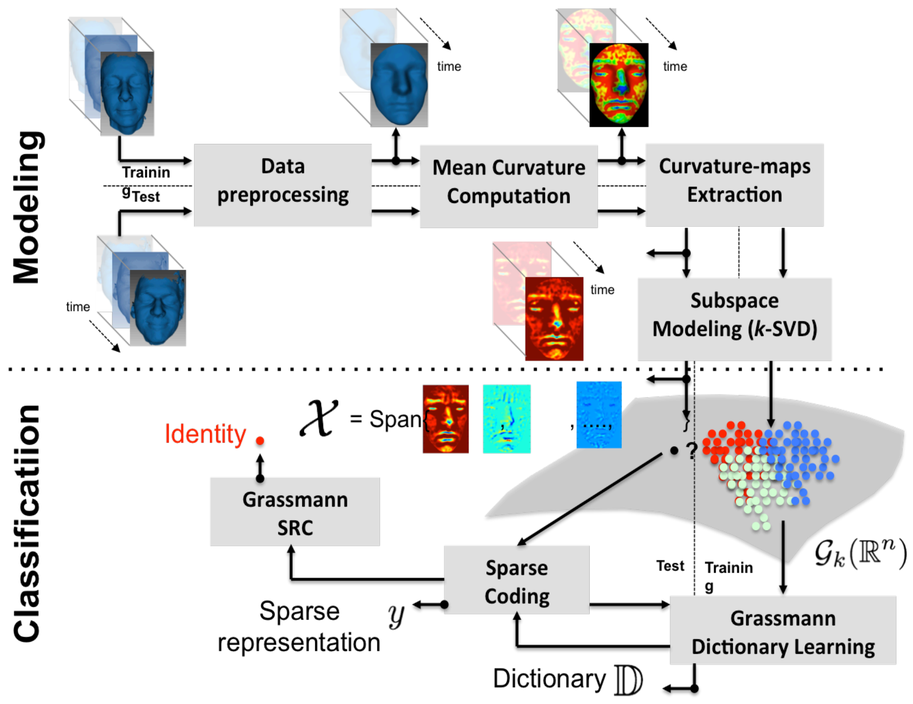
Nécessité d'une **représentation spatio-temporelle** (4D) **compacte**, **robuste** aux bruits d'acquisition et **tolérant** les données manquantes.



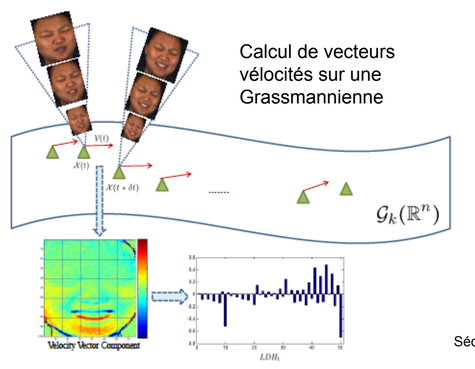
Représentation par **des sous-espaces éléments d'une variété Grassmannienne** (espace de *k*-frames de $\mathbb{R}^n$)

Approches proposées

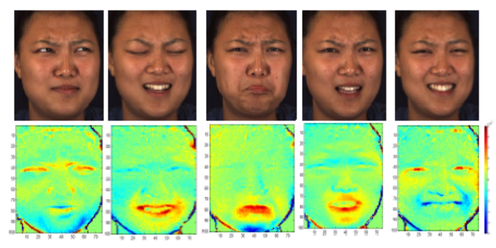
(a) Reconnaissance faciale 4D

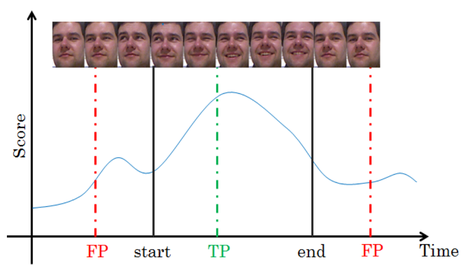


(b) Détection d'émotion à partir de formes 4D

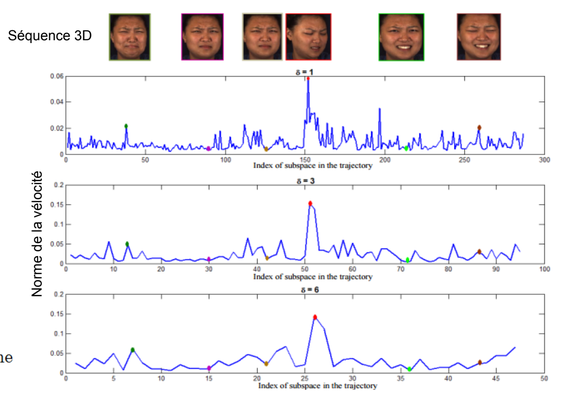


Exemples de vecteurs vélocité calculées sur une trajectoire





Détection **précoce** avec l'algorithme SO-SVM *(Structured Output Support Vector Machine)* – Exemple de détection de **la joie**.



Normes des vecteurs vélocités calculés sur une trajectoire pour trois étapes de dérivation différentes (1, 3, 6) et Effet du changement de pose.

Résultats obtenus

(a) Reconnaissance faciale 4D

BU-4DFE Di4D DB

ED – Dépendant de l'expression

Method	RR (%)
Gabor-wavelet on 2D videos (from [6])	85.09
LLE on static 3D (from [6])	82.34
PCA on static 3D (from [6])	80.78
LDA on static 3D (from [6])	91.37
ST-HMM on 4D (proposed in [6])	97.47
GNN on 4D	**93.69**
GGDA on 4D	**98.08**
GSR on 4D	**100**

ED – Dépendant de l'expression & **EI** – Indépendant de l'expression

Method	EI – RR (%)	ED – RR (%)
2D video A-HMM [32] (from [6])	67.05	93.97
4D ST-HMM [6]	94.37	97.47
4D GSR	84.13	100

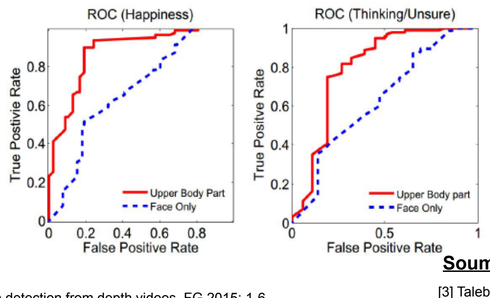
Temps nécessaire pour le traitement

Processing Step	Processing time (s) Sun et al. [6]	This work
One 3D frame processing	15	1
One probe recognition	5	0.73
Full video processing - 100 frames	1500	90

(b) Détection des états de joie et de l'incertitude

Cam3D Kinect DB

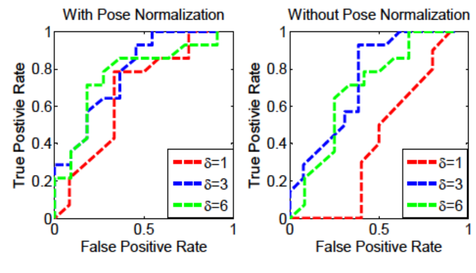
Partie supérieure du corps vs. visage



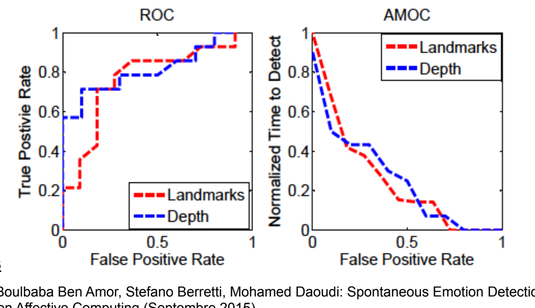
(c) Détection de la douleur physique

BP4D-Sponteneous Di4D DB

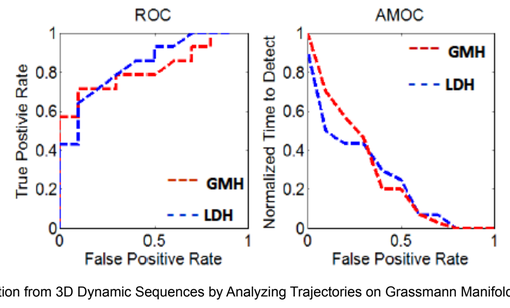
Effet de l'augmentation de l'étape de dérivation



Profondeur vs. Landmarks



Approche globale vs. locale



Publications

[1] Taleb Alashkar, Boulbaba Ben Amor, Stefano Berretti, Mohamed Daoudi: Analyzing trajectories on Grassmann manifold for early emotion detection from depth videos. FG 2015: 1-6

[2] Taleb Alashkar, Boulbaba Ben Amor, Mohamed Daoudi, Stefano Berretti: A Grassmannian Framework for Face Recognition of 3D Dynamic Sequences with Challenging Conditions. ECCV Workshops (4) 2014: 326-340

Soumissions

[3] Taleb Alashkar, Boulbaba Ben Amor, Stefano Berretti, Mohamed Daoudi: Spontaneous Emotion Detection from 3D Dynamic Sequences by Analyzing Trajectories on Grassmann Manifolds. Soumis à IEEE Transactions on Affective Computing (Septembre 2015).

[4] Taleb Alashkar, Boulbaba Ben Amor, Mohamed Daoudi, Stefano Berretti: A Grassmann Framework for 4D Facial Shape Analysis. Soumis à Pattern Recognition (Décembre 2015).

journée de restitution du Programme « Futur & Ruptures »

Janvier 2016

Contact boulbaba.benamor@telecom-lille.fr

Site web http://pagesperso.telecom-lille.fr/benamor/

Ultra-low Bitrate Compression of Crowded Public Scenes

Parties prenantes

TELECOM ParisTech

UNIVERSITY OF ALBERTA

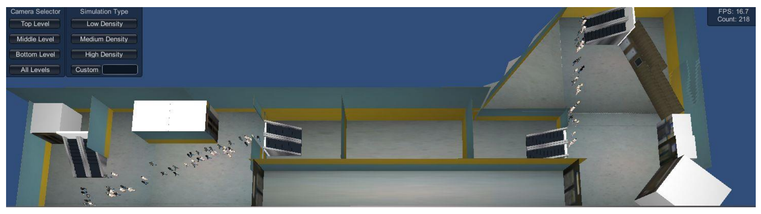
Auteurs

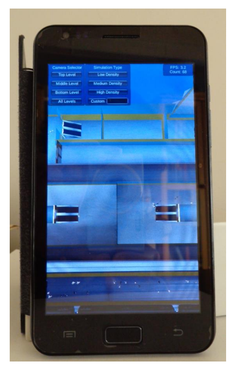
A. Basu, Univ. of Alberta

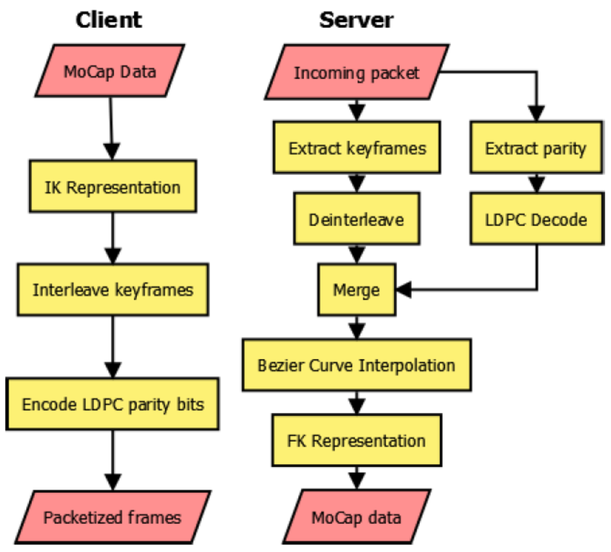
F. Dufaux, Télécom ParisTech

Abstract

- Ultra-low bitrate privacy preserving compression of crowded public scenes is important for a variety of applications like real-time mobile visualization, security and interactive online games.
- Given the ubiquity of wireless handheld devices, it is important to tune applications to these platforms. We target crowd visualization on wireless and handheld devices combining compression, 3D modeling and interactive visualization.
- Key words: Crowd Motion Compression, Privacy, Robust Transmission



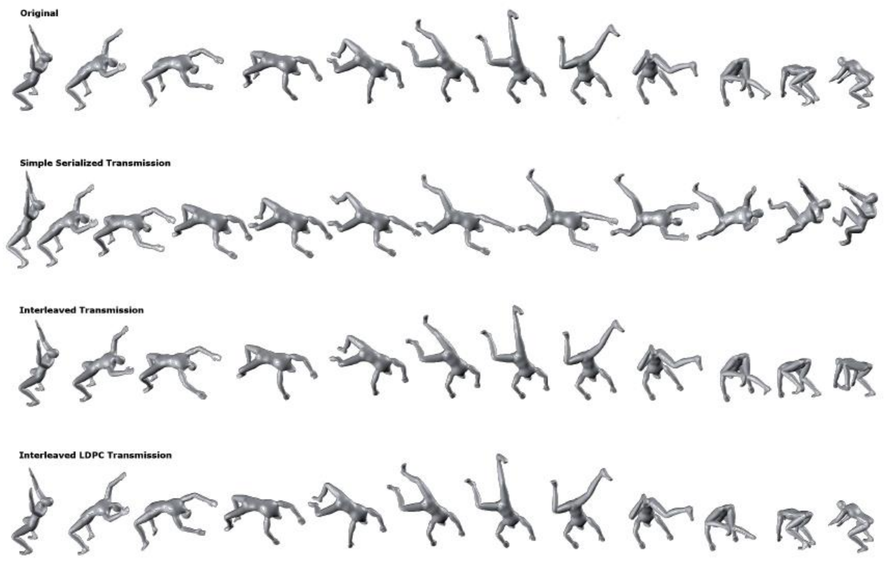





```
struct PACK_FRAGMENT {
    int joint_id;
    long long key_time;
    TRANSFORMATION_TYPE key_type;
    float val_x,val_y,val_z;
};
```

Robust transmission of Motion Capture Data

- Inverse Kinematics representation
- Interleaved Low-Density Parity-Check (LDPC)
- To preserve visual quality, Bezier cubic splines is applied for keyframe interpolation
- Results: simple serialized transmission, interleaved transmission, interleaved LDPC transmission



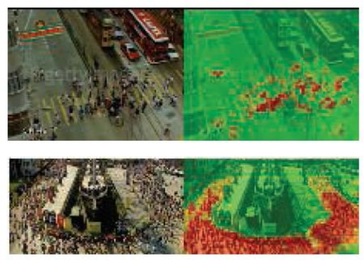
Partenaires

FONDATION TELECOM

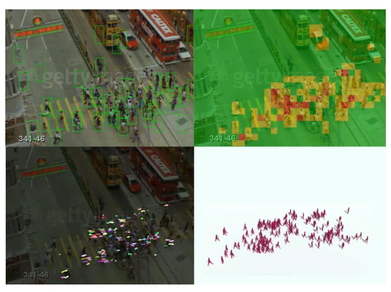
INSTITUT CARNOT Télécom & Société numérique

Crowd Simulation

- Targeting low bandwidth mobile devices
- Based on video scene features:
  - Crowd density computation
  - Optical flow at macro level
  - Affine rectification
  - Robust object tracking
- Synthesizing MoCap data
  - ~ 260 bps per person
  - ~ 8 kbps for 30 characters



Density estimation:
green=low, yellow=medium, red=high



Automatic motion tracking and modeling

Outcome and publications

- The project has established ongoing collaboration between Télécom ParisTech and the Univ. of Alberta.
- A.C. Furtado, I. Cheng, A. Basu, F. Dufaux, “Robust Transmission of Motion Capture Data using Interleaved LDPC and Inverse Kinematics”, EUROGRAPHICS 2016 (submitted).
- A.C. Furtado, I. Cheng, A. Basu, F. Dufaux, “Crowd Simulation based on Video Scene Features for Low Bandwidth Mobile Devices” (in preparation).
- N.K. Kottayil, I. Cheng, F. Dufaux, A. Basu, “A Color Intensity Invariant Low Level Feature Optimization Framework for Image Quality Assessment” Signal, Image and Video Processing (submitted)
- I. Cheng, M. Mohammadkhani, A. Basu, F. Dufaux, “Foveated High Efficiency Video Coding for Low Bit Rate Transmission”, in Proc. IEEE International Symposium on Multimedia (ISM 2015), Miami, FL, Dec. 2015 (published).

Contact frederic.dufaux@telecom-paristech.fr

Site web https://webperso.telecom-paristech.fr/dufaux.html

Searching over Encrypted Data

Projet transverse
Cyrus

Involved Schools

INSTITUT Mines-Télécom

TELECOM Bretagne

Colorado State University

Authors

Tarik Moataz
Telecom Bretagne, Rennes
Colorado State University, USA
Nora Cuppens-Boulahia
Telecom Bretagne, Rennes
Frédéric Cuppens
Telecom Bretagne, Rennes
Indrakshi Ray
Colorado State University, USA
Indrajit Ray
Colorado State University, USA

Partners

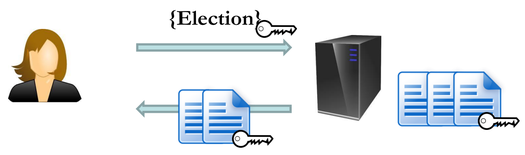
FONDATION TELECOM

INSTITUT CARNOT Télécom & Société numérique

Problem Statement

Thesis's main question:

How can one perform secure search on the encrypted data on the cloud server side while guaranteeing a well-defined security assurance and practical search and storage complexity?



Searching over encrypted data high-level sketch

Possible solution

- **Searchable encryption:** Searching encrypted keywords using encrypted queries in order to retrieve encrypted documents without any leak of information of the content of queries and documents
- **Oblivious RAM**: Cryptographic primitive that enables hiding the search and access pattern . After every access the memory is shuffled .

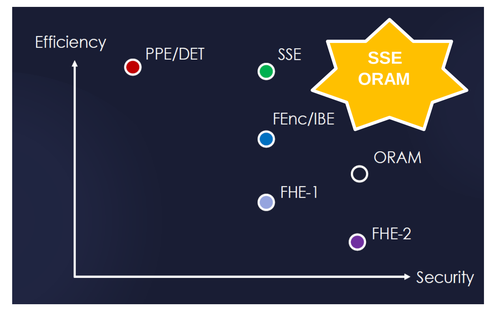
Existing approaches

- ***Exact Search*** over encrypted data [2000].
- ***Range Queries Search*** over encrypted data [2007].
- ***Conjunctive Exact Search*** over encrypted data [2013].
- ***…***

Why Searchable Encryption (SE) ?

Other possible solutions
(Out of the thesis scope)

- Full Hommorphic Encryption, Private Information Retrieval, Property Preserving Encryption, Functional Encryption



**Modified from Seny Kamara talk*

Searchable encryption and ORAM have good balance between Security and Efficiency

Thesis objectives

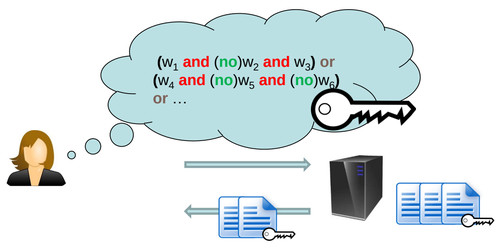
- Exploring the limitations of searchable encryption in order to ***enable the same set of search options as plaintext search.***
- *Exploring* ***ORAM techniques for better efficient constructions***
- Develop ***practical***, ***real-world proof-of-concept*** prototypes that will demonstrate the schemes efficiency and readiness for deployment.

Ph.D. Contributions

Boolean Search (BSSE)

- **Boolean Search (BSSE)** allows searching for disjunctions, conjunctions and negation at the same time on encrypted data.
- Our work represents the ***first*** solution in literature.

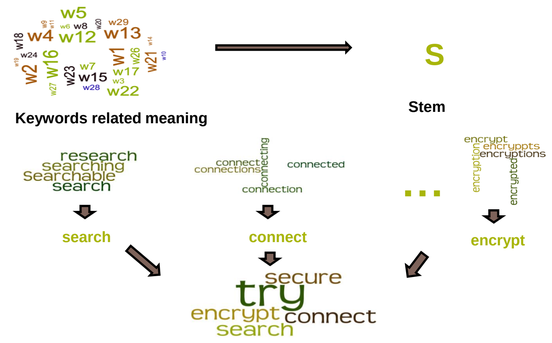
- **Main idea :**
  - Each keyword is considered as a vector in order to perform inner product during the search phase.
  - Boolean symmetric searchable encryption **BSSE** is mainly based on the orthogonalization of the keyword field according to the Gram-Schmidt process.
- The scheme has a ***linear*** search complexity.
- Search queries can be written under the ***disjunctive normal form*** (DNF) or ***conjunctive normal form*** (CNF).
- Security is proven under adaptive chosen keyword attack.



Boolean Search over encrypted data high-level sketch

Semantic Search

- ***Semantic search*** enables the user to search for all documents containing keywords with roughly the same meaning.
- Semantic search over plaintext data is often based on "**stemming algorithms**".
- ***Stemming*** is a general morphological process analyzer aiming first to identify words having the same meaning then to associate them with a unique keyword called the **stem.**



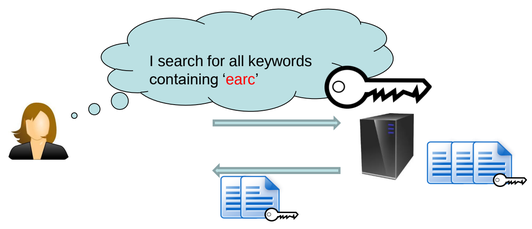
- The scheme consists on mixing the most efficient searchable encryption scheme with the appropriate stemming algorithm.

Substring Search (SED)

- **Substring Search over Encrypted Data (SED)** enables the user to securely search for substrings.
- Our work represents the ***first*** solution in literature.

- **Main Challenges :**
  - Avoid an exponential storage overhead.
  - Threat model for substring search is very hard to define due to the pattern-keyword additional leakage.
  - Avoid a linear search complexity

- Our scheme enables a sublinear search complexity and a linear storage complexity.
- The idea is based on letter orthogonalization instead of keyword orthogonalization in the BSSE.



Substring Search over encrypted data high-level sketch

Privacy-preserving search (PCSSE)

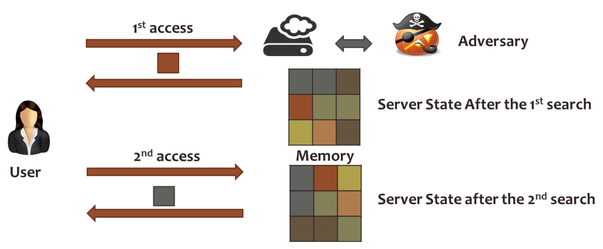
- **Privacy-preserving conjunctive search (PCSSE)** permits the user to hide his ***search pattern*** while performing conjunctive search over encrypted data.

- **Main Challenges :**
  - Prevent any adversary to learn the statistical search behavior of the user.
  - Enable am efficient search for ***moderate*** dataset size.

- PCSSE enables a linear search with a hidden search pattern.
- The security is based on the hardness assumption of the discrete logarithm.

- **Privacy-preserving features :**
  - The scheme permits a client to generate randomized search queries, i.e. every search query is different from previous ones even when the client is searching the same conjunction of keywords.
  - The scheme hides the number of keywords that are submitted in a client's query.
  - The servers do not have any information on the number of keywords contained in each document.

Constant Communication ORAM (C-ORAM)



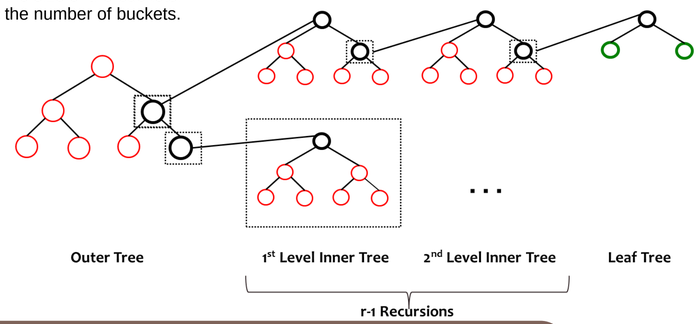
ORAM high level description

- A constant communication blowup with small Block Size in $\Omega(\log^4 N)$ for N blocks.
- New Oblivious-Merge technique.
- Constant client storage overhead.

Recursive ORAM (r-ORAM)

Optimize the search complexity:
- Reduce the height of the binary tree to enhance the communication complexity.

Reduce the storage overhead:
- Reduce the size of the buckets.
- Reduce the number of buckets.



Future Works

- ***Semantic Search*** **:**
  - Improve the semantic search by adding a weight between lexemes of the same stem.
- **Boolean Search :**
  - Search for any general Boolean query with search complexity ***less than linear*** in the number of documents in the corpus.
- **Constant communication ORAM**
  - ORAM without encryption to enhance ORAM efficiency.
- **Resizable ORAM**
  - ORAM with dynamic updates.

Journée Futur et Ruptures

January 2016

Contact tarik.moataz@telecom-bretagne.eu

Site web www.cs.colostate.edu/~tmoataz

Réalisation expérimentale d'intrication multipartite

L'intrication est une ressource au cœur des communications et l'information quantique. Pour être en mesure de trouver de réelles applications il faut augmenter le nombre de qubits intriqués. Dans nos expériences, nous utilisons des processus d'optique non linéaire pour générer des états intriqués en polarisation. Nous utiliserons cette intrication pour réaliser de nouveaux protocoles.

Distribution multi-utilisateur de paires de photons intriqués aux longueurs d'onde telecom

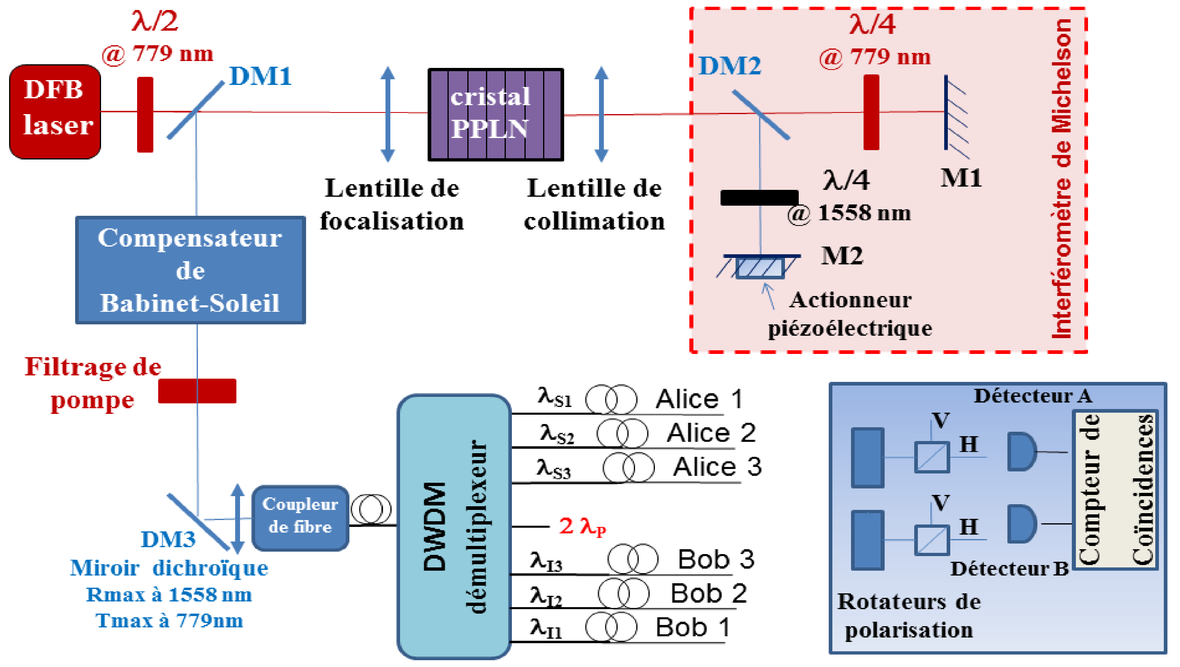
Parties prenantes

Julien Trapateau
Joe Ghalbouni
Adeline Orieux
Eleni Diamanti
Isabelle Zaquine

- Fluorescence paramétrique dans un cristal PPLN (periodically poled lithium niobate).
- Conservation de l'énergie : $h\nu_{pompe} = h\nu_{signal} + h\nu_{idler}$
- Séparation déterministe des photons de la paire par démultiplexage en longueur d'onde en utilisant leur symétrie en fréquence.
- Génération de l'intrication en polarisation par double passage dans un cristal non linéaire :

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle + e^{i\varphi}|VV\rangle\right)$$

- Stabilisation active de la phase à l'aide d'un interféromètre de Michelson.



Auteurs

Julien Trapateau
Joe Ghalbouni
Adeline Orieux
Eleni Diamanti
Isabelle Zaquine

Caractéristiques des démultiplexeurs

Facteur de qualité: $\zeta_Q = \frac{I^2{}_2}{I_{1s}I_{1i}} T_s T_i$,

$I_{1s,i} = \int F(\nu_{s,i} - \nu_c) d\nu_{s,i}$,

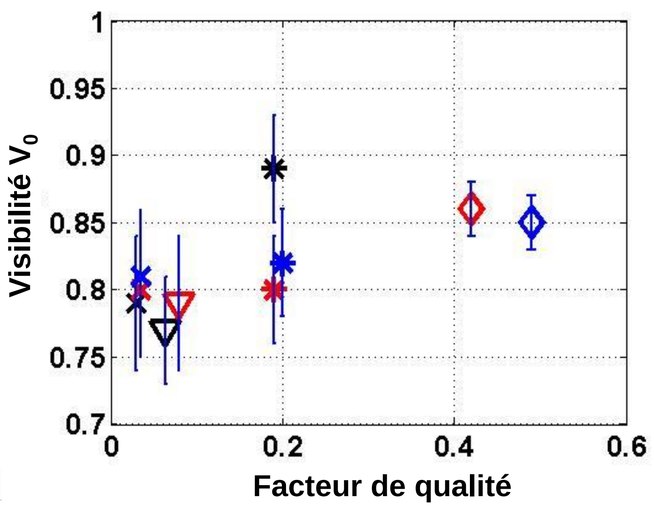
$I_2(\nu_0, \nu_p) = \int F(\nu_s - \nu_0) F(\nu_p - \nu_s - \nu_0) d\nu_s$

T : Transmission maximale ν_c: Fréquence centrale du canal

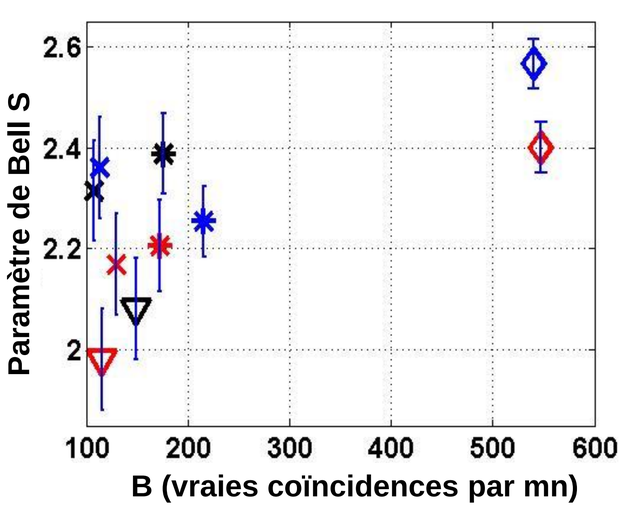
F : Transmission normalisée ν_0 : Fréquence centrale de la paire de canaux

	Technologie du démultiplexeur	*Profil spectral du canal de transmission*
AWG	Arrayed-Waveguide	Flat top
DTF	Dielectric Thin-Film	Flat top
DGFT	Diffraction Grating	Flat top
DGG	Diffraction Grating	Gaussien

Partenaires



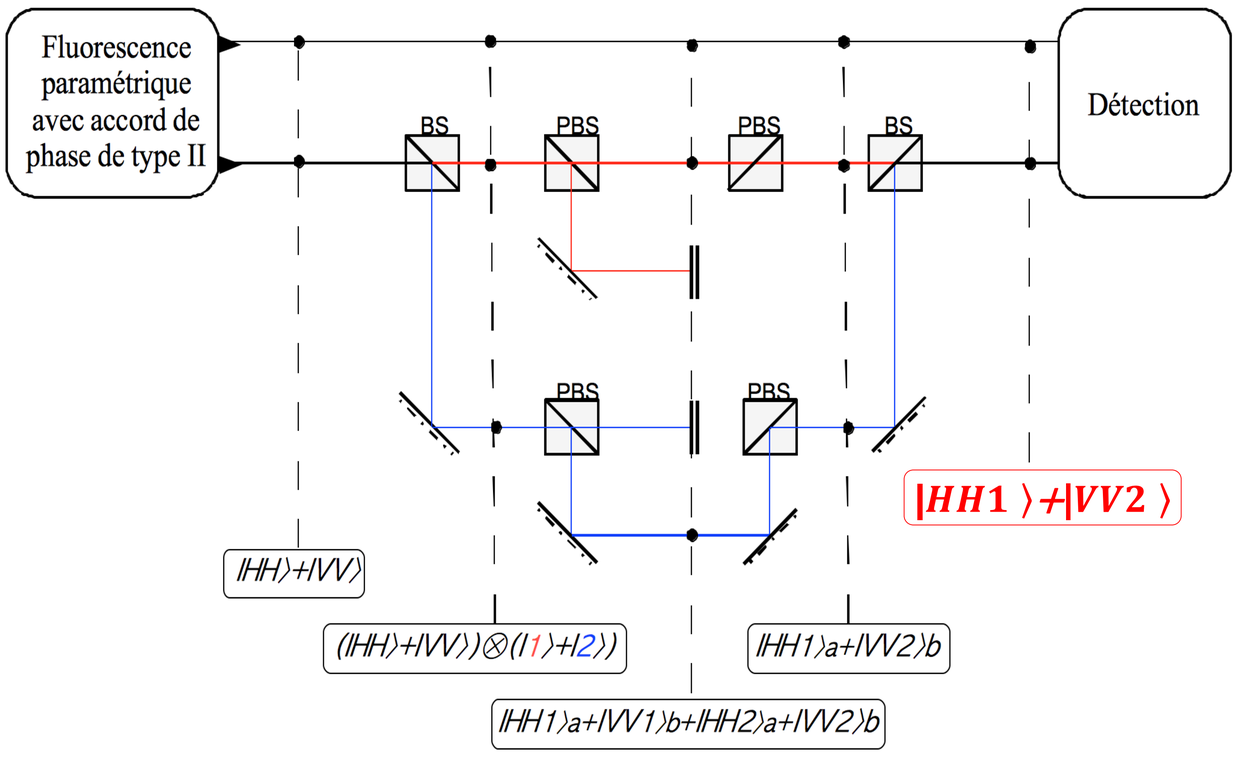
	démux	*Numéro canaux ITU*
◇	DTF	22-26
◇	DTF	21-27
✱	DGG	23-25
✱	DGG	22-26
✱	DGG	21-27
▽	AWG	23-25
▽	AWG	22-26
×	DGFT	23-25
×	DGFT	22-26
×	DGFT	21-27



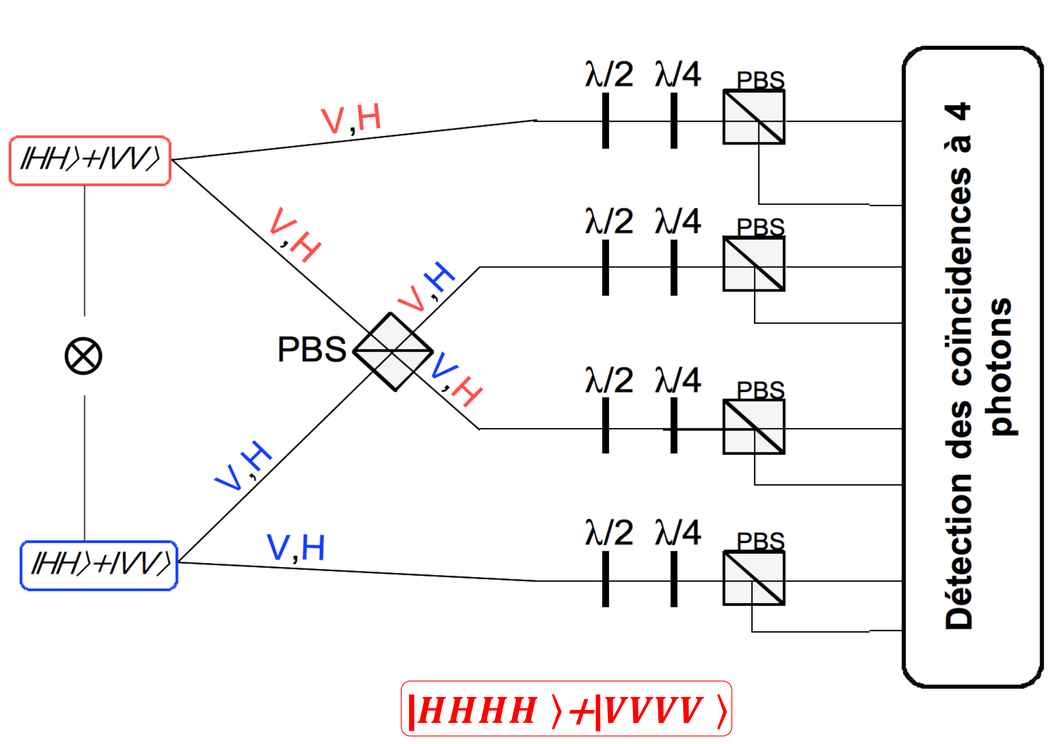
S : Paramètre de Bell
C : nombre de coïncidences
V : Visibilité (bases 0° et 45°)
Fenêtre de détection : 20 ns
Fenêtre de coïncidences : 1 ns
Temps d'intégration : 3 min
λ_p = 779 nm
λ_c = 2 λ_p = 1558 nm

• Multi-user distribution of polarization entangled photon pairs, J.Trapateau, J.Ghalbouni, A.Orieux, E. Diamanti and I.Zaquine J.Appl.Phys. 118, 143106 (2015)

Schéma expérimentaux de réalisation d'états intriqués à plus de 2 qubits



Interféromètre permettant d'obtenir un état à trois qubits avec deux photons.



« Fusion » de deux sources produisant un état intriqué à quatre qubits avec quatre photons.

Janvier 2016

Contact julien.trapateau@gmail.com

Site web http://iq.telecom-paristech.fr

Secure and privacy–preserving collaborative computation for the Internet of Things

Partners

Authors

Amina KERKAR

Maryline LAURENT

Internet of things

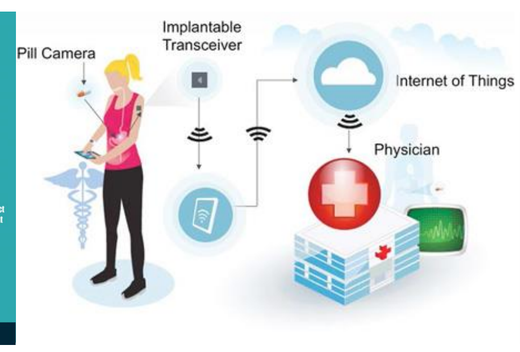
Context

- Network of physical objects
- Objects associated to different physical users
- Sensitivity of data collected and processed locally by users' objects (e.g. health data)

Smart infrastructures

Source : http://blog.smartcitylabs.io/examples-of-internet-of-things/

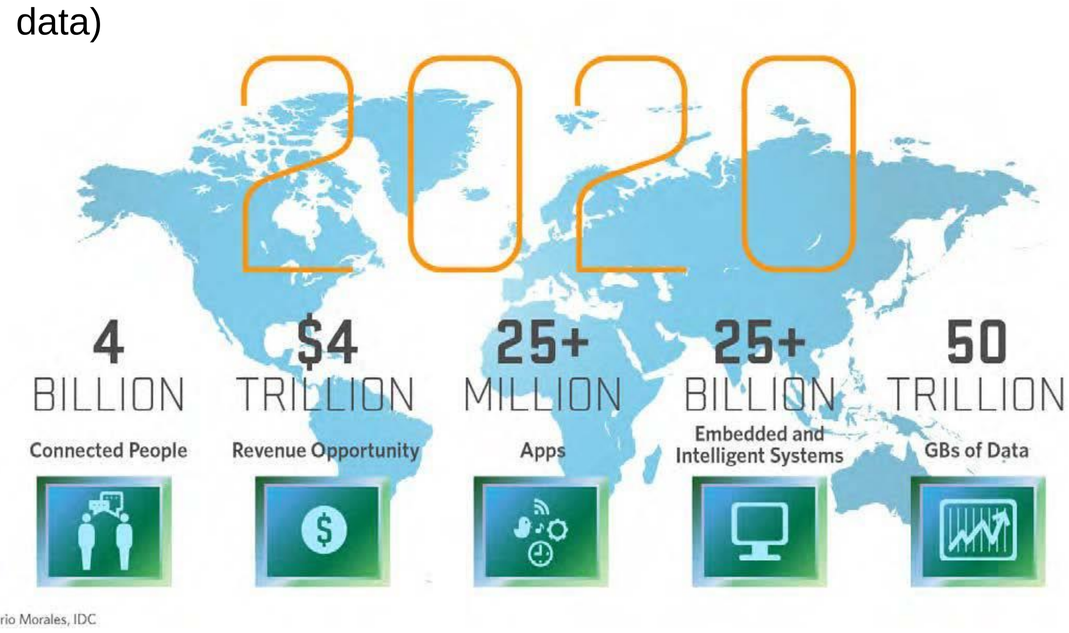
Healthcare



Source : http://www.meddeviceonline.com/doc/how-revolutionizing-healthcare-0001

Security and Surveillance

Source : http://www.pcmag.com/article2/0,2817,2484676,00.asp



Source: Mario Morales, IDC

Data expansion in 2020

Constraints

- Constrained resources of objects (computation, memory, energy)
- Need for data privacy (to counteract data leakage)
- Need for data security (protection against data manipulations)
- Objects can not be trusted

Private and Secure Collaborative Computation

Objective

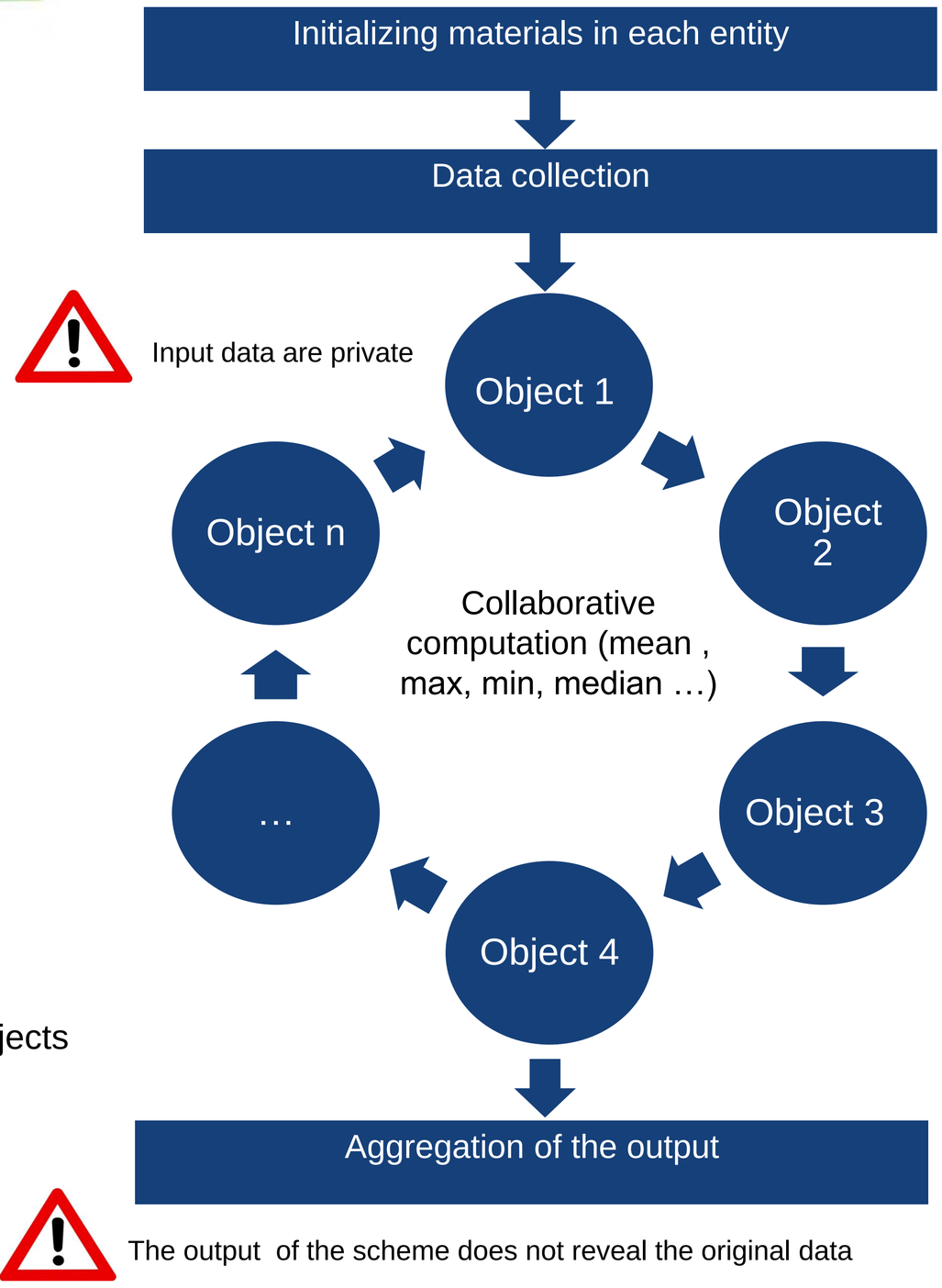
- Aggregating data among a group of objects to offer new services
- Propose statistical computations

Idea

- Use of secure multiparty computing and collaborative asymmetric cryptographic algorithms and lightweight communications based on error-correcting codes cryptography

Privacy and security properties

- Unlinkability between the data and the owner
- Resistance to collisions among users owning different objects
- Verification of the integrity of the output data



Privacy preserving Collaborative computation Scheme

Contact {Maryline.Laurent, Amina.Kerkar}@telecom-sudparis.eu

Site web www-public.tem-tsp.eu/~lauren_m/

Source localization for functional brain imaging with M/EEG

Yousra Bekhti, Roland Badeau, and Alexandre Gramfort

INSTITUT Mines-Télécom

MNE MEG + EEG ANALYSIS & VISUALIZATION

TELECOM ParisTech

Partenaires

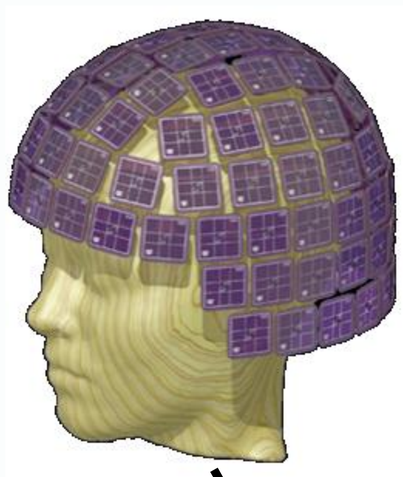
FONDATION TELECOM

INSTITUT CARNOT Télécom & Société numérique

PIPELINE OF SOURCE LOCALIZATION IN MEG

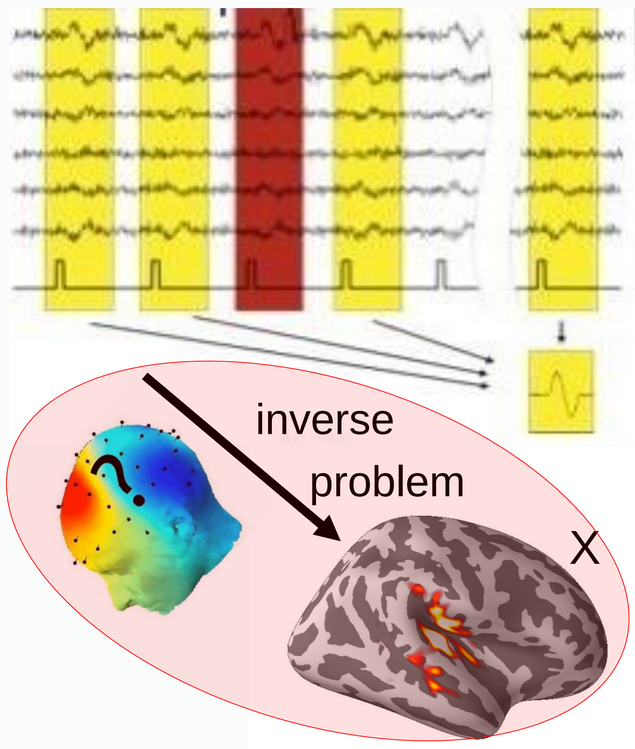
Stimuli (if any)
- auditory
- visual
- somatosensory
- …

Task
- attend/ignore
- detect + react
- detect + count
- imagine
- observe/imitate
- …



Behavioral responses
- limb/finger movement
- speech
- …

MEG data: evoked responses M



MEG device

MY PhD

(PART OF) STATE OF THE ART

○ $M = GX + E$

$$\hat{X} = arg\min_X \frac{1}{2}\|M - GX\|_{Fro}^2 + \mathcal{P}(X)$$

- **MNE:** Minimum Norm Estimate

$$\mathcal{P}(X) = \lambda\|X\|_{Fro}^2$$

- **MxNE:** Mixed Norm Estimate

$$\mathcal{P}(X) = \lambda\|X\|_{2,1}^2$$

- **irMxNE:** Iterative reweighted MxNE

$$\mathcal{P}(X) = \lambda \sum_{s=1}^{S} \sqrt{\|X_s\|_{Fro}}$$

○ **Time-Frequency based solution**

$M = GZ\Phi + E$

$$\hat{Z} = arg\min_Z \frac{1}{2}\|M - GZ\Phi\|_{Fro}^2 + \mathcal{P}(Z)$$

- **TF-MxNE:** Time-frequency MxNE

$$\mathcal{P}(Z) = \lambda_{space}\|Z\|_{2,1} + \lambda_{time}\|Z\|_1$$

- **irTF-MxNE:** iterative reweighted TF-MxNE

$$\mathcal{P}(Z) = \lambda_{space}\|Z\|_{2,0.5} + \lambda_{time}\|Z\|_{0.5}$$

CONTRIBUTIONS

○ **Scanning Method:**

- **RAP-MUSIC:** Recursively applied and projected MUSIC: Signal subspace (Φ_S) correlation to find the best focal sources.

$$arg\ max_{\rho}\,(subcorr_1(\boldsymbol{G}(\rho), \hat{\Phi}_s))$$

Implemented for irMxNE comparison.

TMI 2015 - submitted

PRNI 2016 - WIP

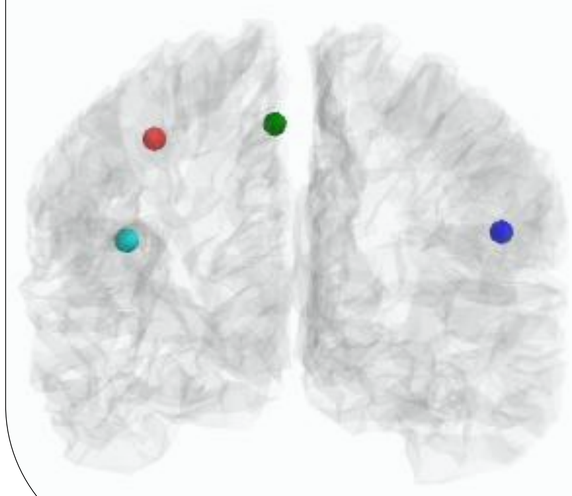
○ **Distributed Method**

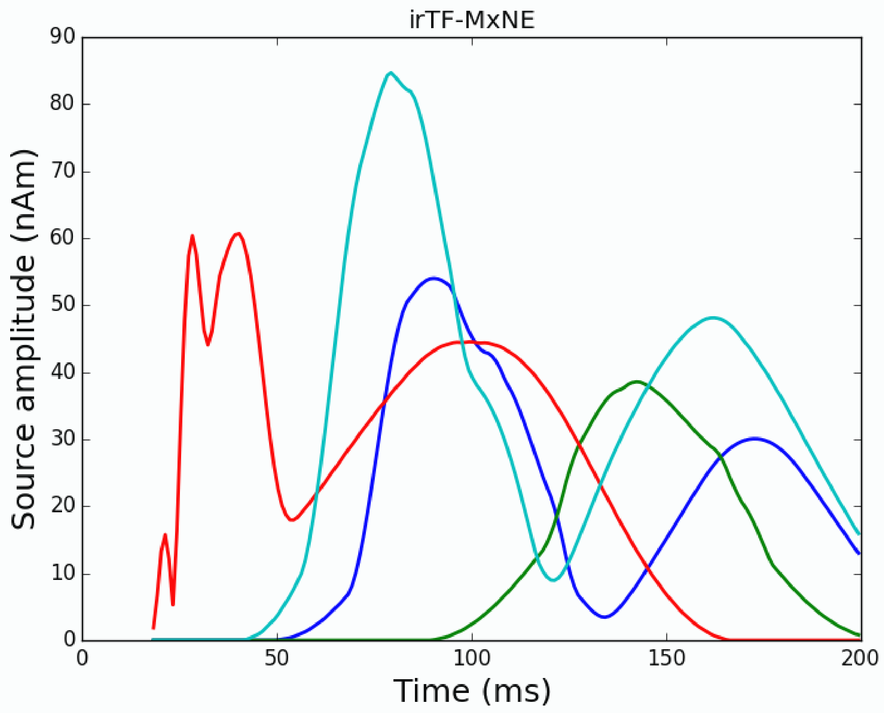
- **irTF-MxNE:** iterative reweighted TF-MxNE with multiple dictionaries.

$M = GZ\Phi + E$

$Z = [Z_1, Z_2]$

$\Phi = [\Phi_1; \Phi_2]$





Publications:

- Strohmeier, D, **Bekhti, Y.,** Haueisen, J., Gramfort, A., The iterative reweighted Mixed-Norm Estimate for spatio-temporal MEG/EEG source reconstruction, IEEE TMI -- State: in revision
- **Bekhti, Y.,** Gramfort, A., van Wassenhove, V., Brain reading with ordered targets using ranking metric, Poster presented at Women in Machine Learning workshop collocated with NIPS, December 2015 – Montréal, Canada.

Janvier 2016 Journée Futur & Ruptures

Contact Yousra.bekhti@gmail.com Site web https://fr.**linkedin**.com/pub/**yousra-bekhti**/56/886/421

Segmentation du cortex cérébral en IRM à 7 teslas pour l'analyse fine de sa morphologie

Parties prenantes

LTCI : Laboratoire Traitement et Communication de l'Information

Département TSI : Traitement du Signal et des Images

Groupe TII : Traitement et Interprétation des Images

Auteurs

Yann Leprince, post-doctorant

Isabelle Bloch, encadrante

Partenaires

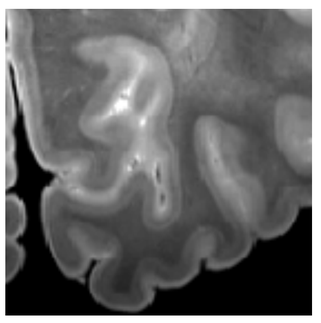
CONTEXTE : L'IRM CÉRÉBRALE À 7 TESLAS

Une technique de pointe pour la recherche sur le cerveau

- L'imagerie par résonance magnétique (IRM) fournit des images 3D des tissus, de manière non invasive et sans rayonnements ionisants.
- En comparaison des imageurs cliniques opérant à 1,5 T ou 3 T (standard), l'augmentation du champ magnétique jusqu'à 7 T :
  - fournit un meilleur rapport signal à bruit intrinsèque, permettant une meilleure résolution spatiale (jusqu'à 0,3 mm environ) ;
  - permet de nouveaux contrastes (sensibilité au fer, à la myéline) ;
  - produit des images entachées de biais en contraste et en intensité.
- Une quarantaine d'appareils sont installés dans le monde, 2 en France dont un chez notre partenaire NeuroSpin (CEA Saclay).

Siemens

Image standard à 3 T (pondération T_1)



Haute résolution à 7 T (pondération T_2)

LE CORTEX CÉRÉBRAL

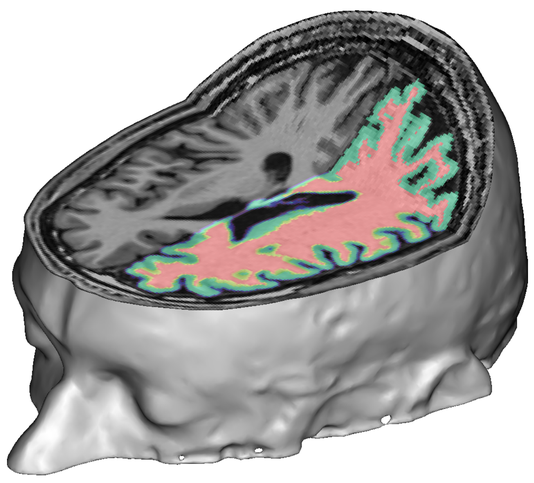
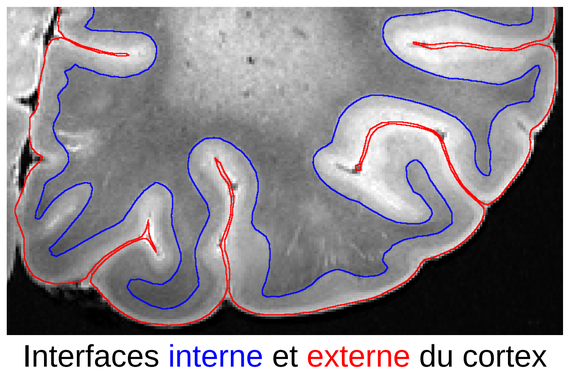


Image composite montrant la segmentation de l'hémisphère gauche (cortex, substance blanche)

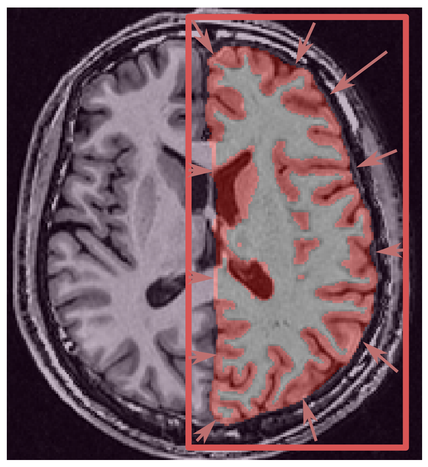
- Le cortex est un manteau de substance grise épais de 2 à 6 mm, fortement plissé, qui recouvre les hémisphères cérébraux.
- C'est le siège des processus cognitifs les plus évolués, donc un objet d'étude privilégié.
- La segmentation du cortex revient à détecter deux interfaces :
  - L'interface interne, qui sépare le cortex de la substance blanche ;
  - L'interface externe, qui sépare le cortex du liquide cérébro-spinal et des méninges.
- Chacune de ces interfaces a la topologie d'une sphère, cette propriété doit être respectée par la segmentation.
- Des logiciels existent pour segmenter les IRM acquises à 3 T (FreeSurfer, Morphologist, etc.)
- La segmentation d'images acquises à 7 T nécessite de nouvelles méthodes, robustes aux hétérogénéités de signal et de contraste.

MODÈLE DÉFORMABLE POUR LA SEGMENTATION

- La méthode de segmentation développée s'appuie sur un modèle déformable basé sur le formalisme des surfaces de niveau : chaque interface est représentée par la surface de niveau 0 d'une fonction $\phi(x, y, z, t)$, évoluant au cours du temps.
- Ce formalisme permet d'intégrer différentes forces dans l'évolution des interfaces : $\frac{\mathrm{d}\phi}{\mathrm{d}t}$
  - Force d'attraction vers les contours, basée sur le gradient de l'image : $\nabla I_\sigma \cdot \nabla\phi$
  - Force de couplage entre les interfaces, permettant de garantir une épaisseur plausible du cortex : $H_\epsilon(\phi_2 - e_{\min}) - H_\epsilon(e_{\max} - \phi_2)$
  - Force de régularisation, basée sur la courbure : $\nabla \cdot \frac{\nabla\phi}{\|\nabla\phi\|}$
  - Force attractive ou répulsive, permettant la correction manuelle au cours de l'évolution de l'algorithme.
- L'évolution des interfaces peut être observée en temps réel, jusqu'à convergence.



Interfaces interne et externe du cortex sur une coupe d'IRM à 7 T



Obtension d'une topologie sphérique par déformation de boîte englobante

GARANTIE TOPOLOGIQUE

- La toplogie sphérique peut être garantie en initialisant la segmentation par une boîte englobante cubique de l'objet, qui est ensuite déformée par érosion itérative.
- L'homotopie est assurée en déformant l'objet par une suite de transformations homotopiques élémentaires, où un seul voxel change de classe.
  - Au sens de la topologie discrète classique, considérant un objet 6-connexe et son complémentaire 26-connexe, la topologie est conservée si le voxel qui change de classe est un point simple (caractérisation locale sur un voisinage 3×3).
  - Un critère analogue, utilisant la topologie non ambiguë, a été implémenté. La topologie de l'objet ne dépend alors plus de la connexité considérée.
- Ces caractérisations pourront être testées à chaque itération du modèle déformable, permettant la préservation de la topologie tout au long du processus.

Journée Futur & Ruptures
26 janvier 2016

Contact yann.leprince@telecom-paristech.org Site web tsi.telecom-paristech.fr

Characterization of the good team and leadership to produce good knowledge: the case of virtual communities

Stakeholders

Authors

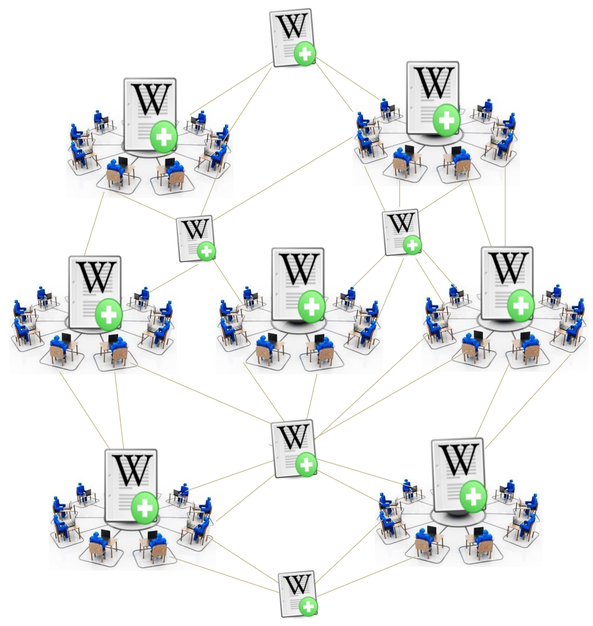
PhD Student:
Amira REZGUI

Thesis supervised by:
Nicolas JULLIEN

Partners

THESIS OVERVIEW

Start 01/11/2014 End 31/10/2017



Context

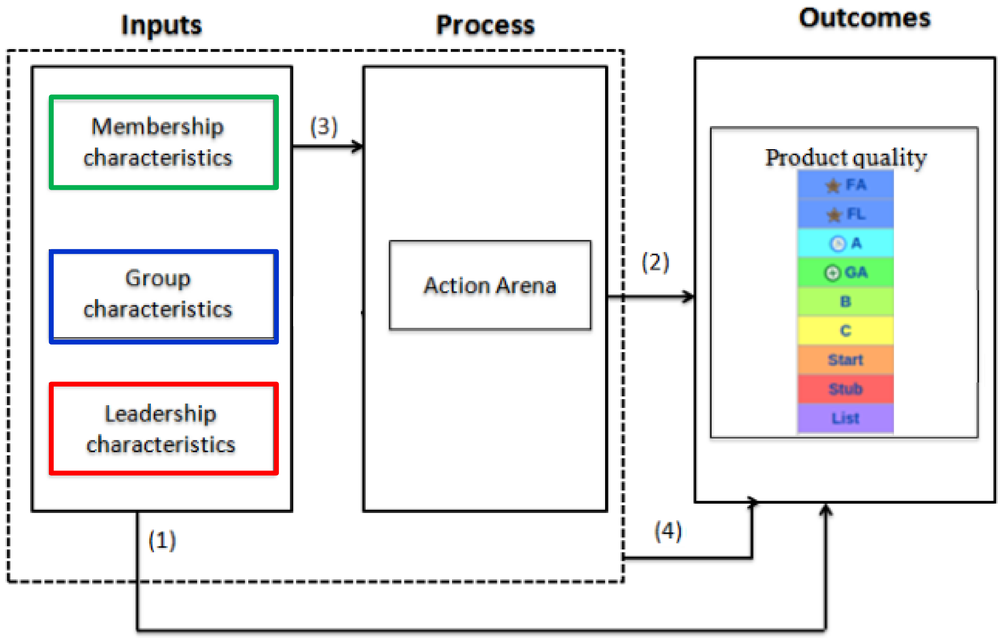
- Online epistemic community: a socio-economic system of open online knowledge production (example Wikipedia).
- As a free and open access online encyclopedia, Wikipedia attracts thousands of volunteer contributors.
- How do online projects work? What do they teach us about online virtual work?

Objective

- To organize a virtual team without traditional organizational structures in order to produce knowledge of quality (high quality articles).
- To predict the most important attributes of a team structure that contribute to produce successful projects.
- To fix the characteristic of a good virtual leadership.

APPROACH AND CONTRIBUTIONS

To understand the production of knowledge in Wikipedia our hypotheses are based on Hess and Ostrom's framework.



We study :

1. The effect of inputs/ or community characteristics on outcomes (product quality)
2. The effect of the process or the way people interact t on outcomes
3. The effect of community characteristics on the way people interact
4. The effect of both the process and community characteristics on outcomes

Hypotheses

1.a Product quality is positively related to membership characteristics

Contribution | Tenure /experience | Past productivity
Concurrent project | In-Project communication | out-Project communication
Reliability | Reputation

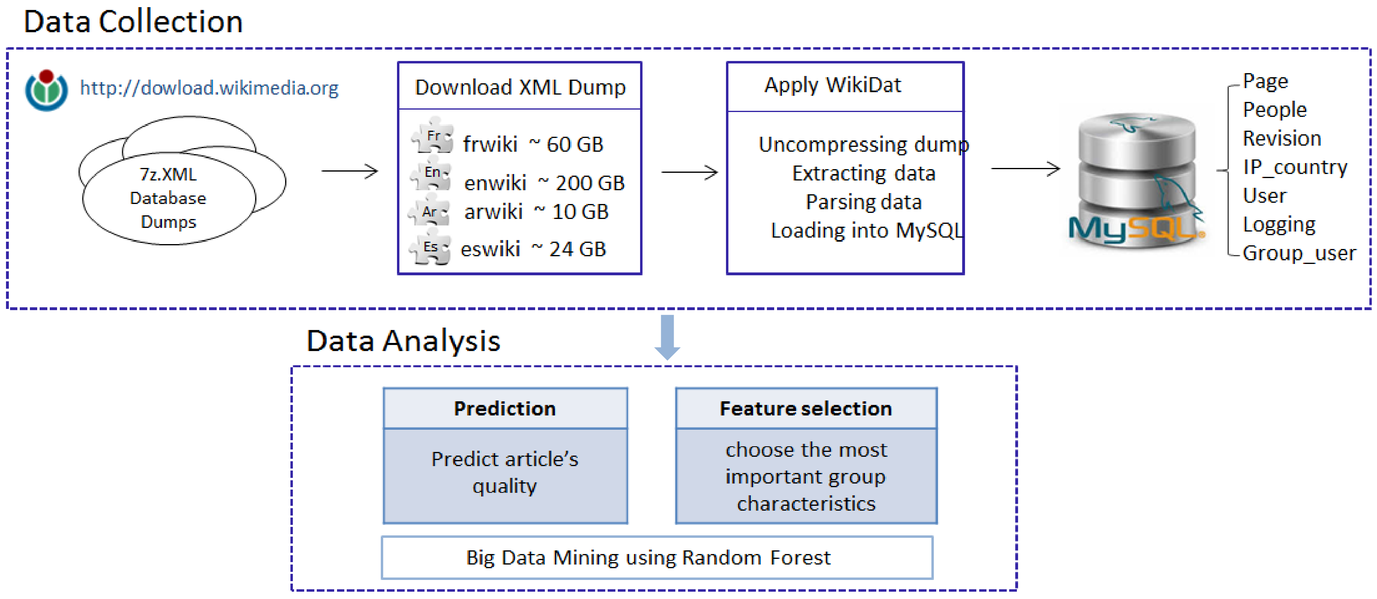
1.b Product quality is positively related to group characteristics

Group size | Tenure diversity | Contribution diversity
Cultural diversity | Interest diversity | Gender diversity
Pre-existing social capital | Reputation diversity

1.c Product quality is positively related to leadership characteristics

1st order leadership:	2nd order leadership:	3rd order leadership:
# initiator Contributions' quantity Communications' quantity Communications' content orientation	Influences team member behavior Reinforces existing structure Distributed	Effects change in structure New norm of behavior and new patterns of authority Centralized

METHODS



Contact amira.rezgui@telecom-bretagne.eu
nicolas.jullien@telecom-bretagne.eu
Site web https://amirarezgui.wp.mines-telecom.fr

« *Culture de collaboration* » & créativité :
Approche développementale et contrastée entre des équipes d'élèves-ingénieurs françaises et japonaises

Auteurs

Mohini Vanhille
Doctorante Psychologie Ergonomique
Financement Fondation Télécom – programme « Futur & Ruptures »

Thèse dirigée par
Françoise Détienne & Michael Baker

Collaboration

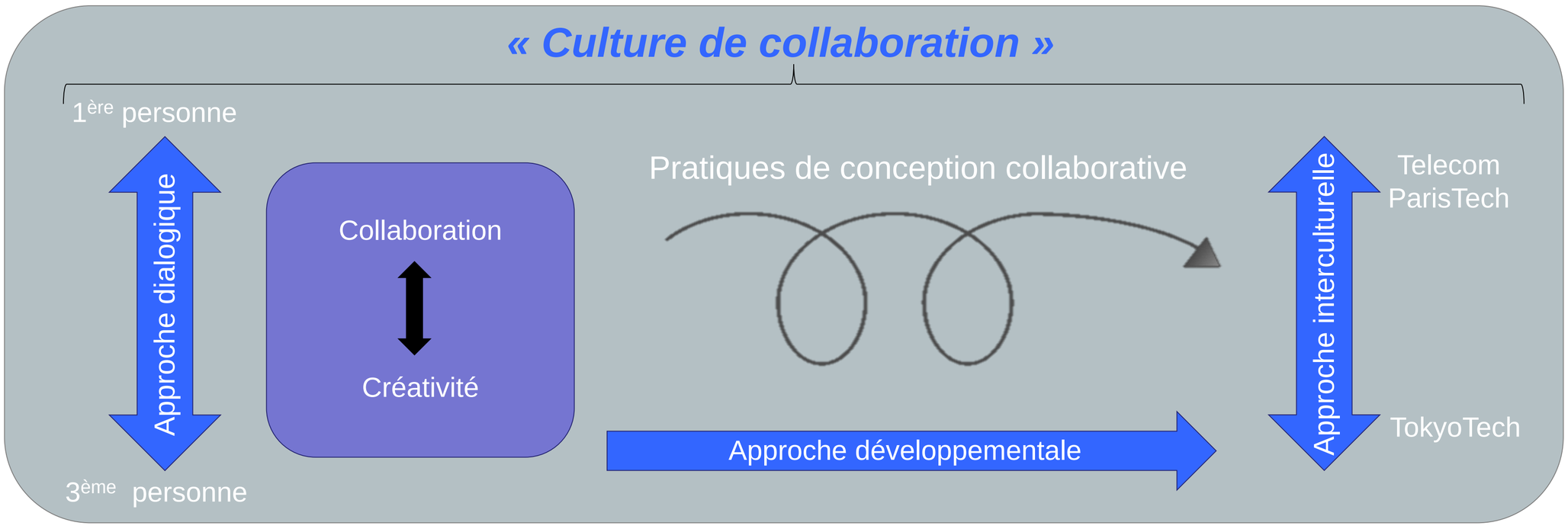
Céline Mougenot
東京工業大学 Tokyo Institute of Technology

Katsumi Watanabe
東京大学 THE UNIVERSITY OF TOKYO

Séjours à TokyoTech (1 semaine – 3 mois)

Partenaires

Objectifs & originalité de la recherche



Analyse des relations entre « *culture de collaboration* » & créativité

Trois approches complémentaires	
Développementale	évolution & stabilisation des pratiques collaboratives en normes & valeurs
Dialogique	articuler les points de vue chercheur/collaborateurs
Interculturelle	influence de la culture nationale (dimensions de Hofestede, 1980; 1991)

Corpus de données (France/Japon)

Des observations sur un terrain privilégié

… mises en contraste avec des données issues d'un projet similaire

Une analyse multi-dimensionnelle (cognitive, sociale & affective) : la méthode Q.C³

Fluidité de la collaboration	Attention conjointe & compréhension mutuelle	Co-Design & Créativité	Argumentation dans la résolution de problèmes	Distribution des ≠ types d'activités	Distributions des rôles	Relations interpersonnelles
Coordination de la communication *(turn taking*) & de l'utilisation du matériel	Focus de l'attention Compréhension mutuelle	Divergence/convergence : Quantité, originalité, diversité des idées Reprise/approfondissement des idées *Premature commitment*	Formes de l'argumentation : • Degré • Compétition vs coopération	• Planification court/long terme • Coordination (sous-tâches, temps) • Distribution entre problème vs interpersonnel • Distribution entre tâche vs hors tâche • Réflexivité	• Rôles: proposant, critique, coordinateur… • Degré de symétrie/de réciprocité des rôles	• Climat socio-relationel • Intensité émotionnelle • Régulation des tensions • Soutien mutuel • Engagement

Basée sur QC: Détienne, F., Baker, M. & Burkhardt, J-M (2012) Quality of collaboration in design meetings: methodological reflexions. Special issue : Perspectives on quality of collaboration in design. *CoDesign*: *International Journal of CoCreation in Design and the Arts*. 8(4), 247-261.

Journée Futur & Ruptures
Janvier 2014

Contact mohini.vanhille@telecom-paristech.fr
LTCI- UMR 5141 - CNRS Télécom ParisTech
Site web www.telecom-paristech.fr

Identités numériques et gestion des informations personnelles

Parties prenantes

Partenaires

Auteurs

Yann Balgobin

Direction :

- **David Bounie**
- **Patrick Waelbroeck**

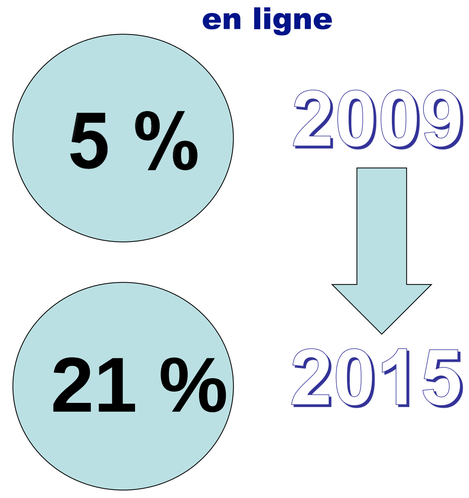
Une identification croissante des individus en ligne

- *Tracking,* surveillance, lutte contre la fraude
- Algorithmes de recommandation
- Développement du *Big Data*

Cette identification peut représenter un coût :

- Exploitation des données personnelles (publicité, *spamming*, *credit scoring*, etc.)
- Vols de données
- Surveillance (par l'Etat, les entreprises, l'employeur, les pairs, etc.)

Refus de partager des informations en ligne



Source : Baromètre ACSEL-CDC de la Confiance des Français dans le numérique

La mise en place de stratégies de dissimulation

44 % des Internautes interrogés utilisent des bloqueurs de publicités

13 % utilisent des extensions de navigateur Internet afin de renforcer leur vie privée en ligne

70 % ont déjà effacé leurs *cookies*

Source : Baromètre ACSEL-CDC de la Confiance des Français dans le numérique (2015)

Autres stratégies :

- Pseudonymat
- Multiplicité des comptes et adresses mail
- PETs (*privacy enhancing tools*)

Quels sont les effets de ces stratégies sur les modèles d'affaires du numérique ?

Projets de recherche

- **Quelle offre d'informations personnelles ?**
- **Moyens de paiement non-bancaires, commerce en ligne et modèles d'affaires des banques**
- **Droit à l'oubli, pseudonymat, *real name policy***
- **Quel avenir pour un service de gestion des identités de type *FranceConnect* ?**

Journéee Futures & Ruptures

Janvier 2016

Contact yann.balgobin@telecom-paristech.fr Site web

Modèles Markoviens pour l'extraction d'information en imagerie SAR

Auteurs

Sylvain Lobry (LTCI/CNES)

Encadrants:

Florence Tupin (LTCI)

Roger Fjørtoft (CNES)

Publications

Publié:

MultiTemp 2015

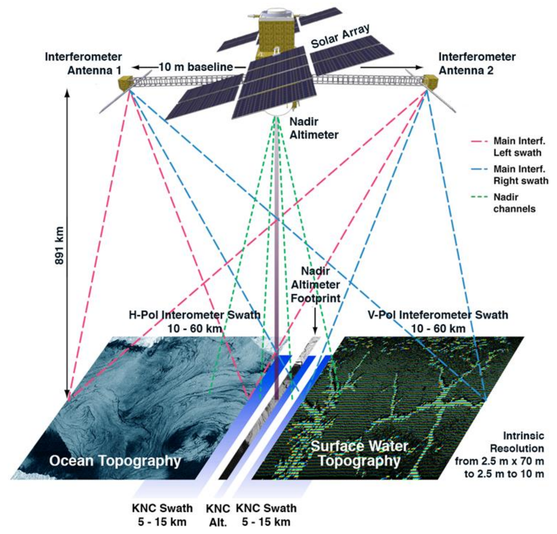
En cours de révision:

EUSAR 2016

JSTARS

Contexte et objectifs de la thèse

- Cette thèse s'inscrit dans le contexte de la mission SWOT (CNES / NASA).
- Objectif: obtenir une mesure globale des hauteurs des différentes surfaces d'eau.
- Objectif de la thèse: proposer des méthodes automatiques d'extraction de surfaces d'eau et de réseaux hydrologiques.
- Utilisation des données interférométriques multi-temporelles acquises par SWOT et d'informations exogènes.
- Deux axes de recherche:
  - La classification des images SAR (Synthetic aperture radar).
  - L'exploitation de séries multi-temporelles.



Caractéristiques de SWOT

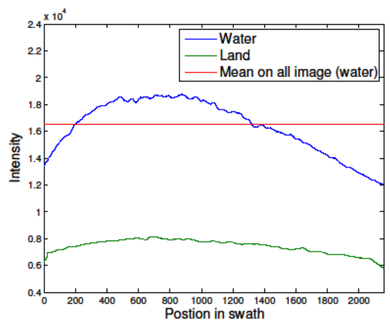
Résolution	Angle d'incidence	Temps de revisite	Bande
2m (azimuth) / 10-70m (fauchée)	1-4°	22 jours	Ka (35.6 GHz / 0.84 cm)

Caractéristiques de SWOT

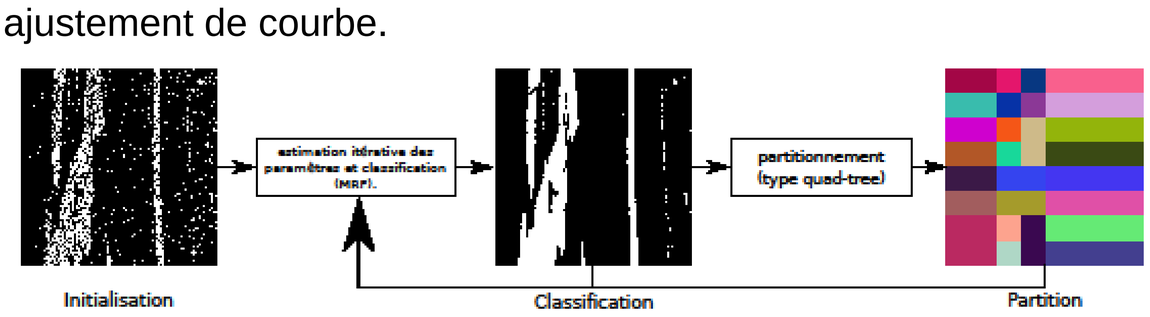
Classification de l'eau

Principe

- Avec la variation de l'angle d'incidence, les paramètres de classe ne sont pas constants dans l'image en distance.
- On propose un modèle Markovien non uniforme avec estimation automatique des paramètres.
- Les paramètres sont estimés localement avec un partitionnement de l'image et globalement avec une régularisation par ajustement de courbe.



Effet de l'estimation globale des paramètres (courbe rouge) par rapport aux paramètres réels (courbe bleu).



Méthode proposée

Résultats

TropiSAR

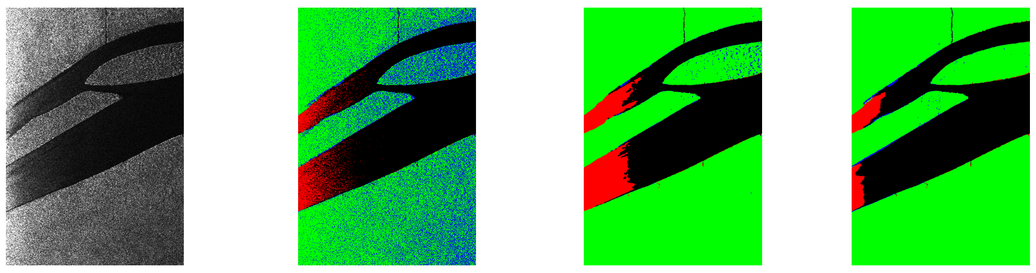


Image d'entrée | Classification initiale Taux d'erreur = 35.6% | MRF Uniforme Taux d'erreur = 11.4% | MRF Non-Uniforme Taux d'erreur = 4.5%

SWOT

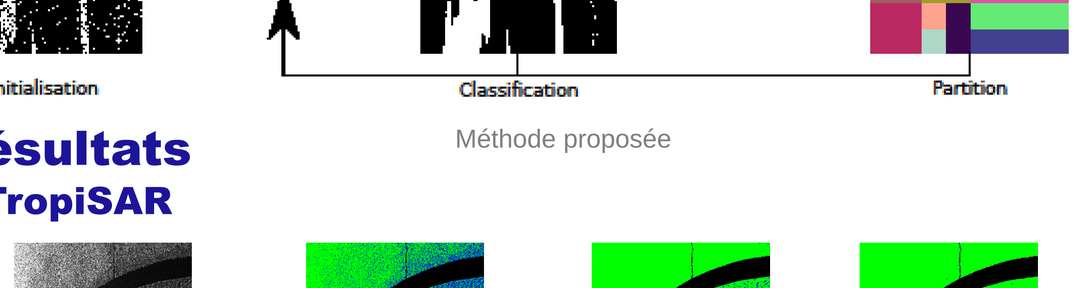


Image d'entrée | Classification initiale Taux d'erreur = 48.5% | MRF Uniforme Taux d'erreur = 5.8% | MRF Non-Uniforme Taux d'erreur = 5.6%

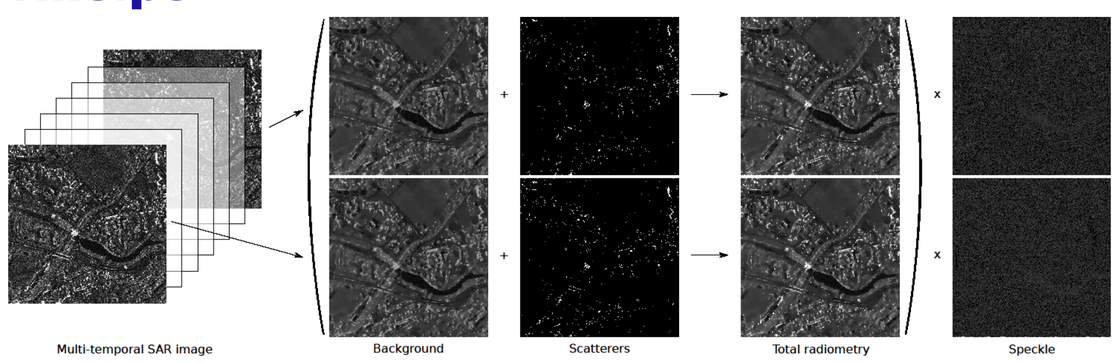
Travaux futurs

- Extraction des réseaux fins (souvent éliminés par les MRFs).
- Utilisation des informations interférométriques et/ou exogènes (satellites optiques et/ou SAR, multi-temporel, masque a priori des surfaces d'eau).

Modèles de décomposition de piles temporelles

Travail effectué avec Loïc Denis (Laboratoire Hubert Curien)

Principe

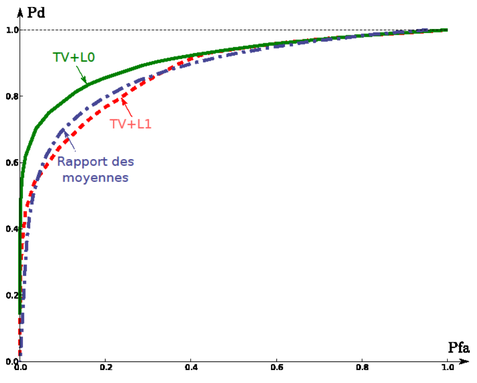


- Régularisation des images SAR nécessaire pour certaines applications.
- Problème difficile à cause de la forte dynamique des images (présence de cibles).
- Décomposition en composantes fond et cibles suivant deux a priori :
  - La variation totale (temporelle et spatiale) pour le fond:

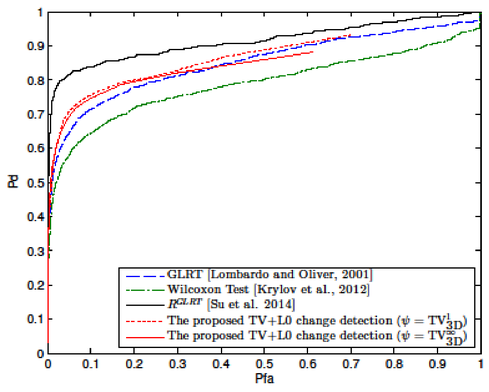
$$TV_{3D}(\boldsymbol{u_b}) = \sum_t \sum_{i \sim j} |u_{b_{t,i}} - u_{b_{t,j}}| + \sum_i \sum_t |u_{b_{t+1,i}} - u_{b_{t,i}}|$$

  - Pseudo-norme L0 pour les cibles: $\|U_s\|_0$
- Modèle applicable à des piles temporelles d'images.
- Minimisation exacte par coupe dans un graphe
- Premières applications à la détection de changement et de cibles.

Résultat



ROC dans le cadre de la détection de cibles



ROC dans le cadre de la détection de changement

Travaux futurs

- Modèles prenant en compte la détection de changement afin d'améliorer la performance dans ce cadre.
- Changer le critère de détection de cible (LMP, GLRT, …)

Contact sylvain.lobry@telecom-paristech.fr Site web www.sylvainlobry.com

Algebraic Coding Theory

Participants

TELECOM ParisTech

Sabancı Üniversitesi

Authors

Steven T. Dougherty

Cem Güneri

Jon-Lark Kim

Buket Özkaya

Lin Sok

Patrick Solé

Partners

FONDATION TELECOM

PRESTIGE
POSTDOCTORAL RESEARCH FELLOWSHIPS IN FRANCE
A MARIE CURIE FELLOWSHIP PROGRAMME

QC COMPLEMENTARY DUAL CODES

Characterization and Asymptotics

- Complete characterization of quasi-cyclic codes that are LCD by using their concatenated structure
- Like quasi-cyclic codes and linear complementary dual codes, quasi-cyclic complementary dual codes are also shown to be asymptotically good.
- Introduction of Hermitian LCD codes and the characterization of their cyclic subclass
- Explicit constructions from LCD codes over larger alphabets
- Optimal and suboptimal examples in addition to the asymptotic performance

m/ℓ	3	5	7	9	11	13	15	17
2	2(3)	3(4)	4(4)	4(6)	5(7)	6(7)	6(8)	6(8)
3	3(4)	5(7)	7(8)	8(10)	9(12)	10(12)	11(14)	
5	7(8)	10(12)	13(16)	15(18)				
7	10(12)							

TABLE 1. Suboptimal QCCD Codes

m	3	5	7	9	11	13	15	17
d	1	3	4*	3	6	7*	5	8*
d*	3	4	4	6	7	7	8	8

TABLE 2. Double Circulant QCCD Codes

GENERALIZED QUASI-CYCLIC CODES

Concatenated Structure and Asymptotics

$$R \cong \mathbb{E}_1 \oplus \cdots \oplus \mathbb{E}_s$$
$$a(x) \mapsto (a(\xi^{u_1}), \ldots, a(\xi^{u_s}))$$

$$R^\ell \cong \mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_s^\ell$$

$$C = C_1 \oplus \cdots \oplus C_s$$

$$\begin{pmatrix} c_{j,0}(\lambda_{1,j}, \ldots, \lambda_{s,j}) \\ c_{j,1}(\lambda_{1,j}, \ldots, \lambda_{s,j}) \\ \vdots \\ c_{j,m_j-1}(\lambda_{1,j}, \ldots, \lambda_{s,j}) \end{pmatrix}_{1 \le j \le \ell}$$

- Development of the algebraic structure based on the known CRT decomposition of GQC codes
- Trace representation of the codewords by using the concatenated structure, which generalizes QC case
- Characterization and analysis of self-dual and complementary dual GQC codes
- Asymptotic results on certain classes of complementary dual GQC codes, along with generalizations of the previous work on QC case
- Explicit constructions from codes over larger alphabets

THE COMBINATORICS OF LCD CODES

Linear Programming Bound and Orthogonal Matrices

- Linear Complementary Dual (LCD) codes intersect with their dual trivially and they are used in counter measures to passive and active side channel analyses on embedded cryptosystems.
- Constructions of LCD codes by using orthogonal matrices, self-dual codes, combinatorial designs and Gray map from codes over certain family of rings
- A linear programming bound on the largest size of an LCD code of given length and minimum distance
- Table of lower bounds for this combinatorial function for modest values of the parameters

```
Magma V2.20-4     Tue Dec 01 2015 16:39:27 on SU13729  [Seed = 2559799791]
Type ? for help.  Type <Ctrl>-D to quit.
>
> U:=function(n,d,k0);
function> R := RealField( );
function> K:=GF(2);
function> f:=function(i,j:k,S)
function|function> S:=0;
function|function> for k:=0 to i do
function|function|for> S:=S+(-1)^k*Binomial(j,k)*Binomial(n-j,i-k);
function|function|for> end for;
function|function> return S;
function|function> end function;
function>
function> P:=Matrix(R, n, n, [<i, j, f(i,j)>: i, j in [1..n]]);
function>
function> B:=Matrix(R,1,n,[<1,j,-Binomial(n,j)>:j in [1..n]]);
function> b:=Transpose(B);
function>
function> b:=HorizontalJoin(ZeroMatrix(R,1,d-1),B);
function> b:=HorizontalJoin(b,ZeroMatrix(R,1,2*n));
function> rhs:=Transpose(b);
function> I2:=ScalarMatrix(R,d-1,1);
function>
function> Z2n:=ZeroMatrix(R,d-1,n-d+1);
function>
function> aux:=HorizontalJoin(I2,Z2n);
function>
function> lhs:=VerticalJoin(aux,P);
function>
function> rel := Matrix(R, 1, n, [<1,j,1>:j in [1..n]]);
function> aux:=ZeroMatrix(R,1,d-1);
function> rel:=HorizontalJoin(aux,rel);
function> rel:=HorizontalJoin(rel,Matrix(R,1,n,[<1,j,-1>:j in [1..n]]));
function> rel:=HorizontalJoin(rel,Matrix(R,1,n,[<1,j,1>:j in [1..n]]));
function> rel:=Transpose(rel);
function>
function> D:=Matrix(R, n, n, [<i, j,Binomial(n,i)>: i, j in [1..n]]);
function>
function> In:=ScalarMatrix(R,n,2^k0);
function>
function> lhs:=VerticalJoin(lhs,P-D+In);
function> lhs:=VerticalJoin(lhs,ScalarMatrix(R,n,1));
function> objective:=Matrix(R,1,n,[<i,j,1>:j in [1..n]]);
function>
function> X:=MaximalSolution(lhs, rel, rhs, objective);
function>
function> return X*Transpose(objective);
function>
function> end function;
>
```


Contact buket.ozkaya@telecom-paristech.fr

Lissage rapide dans des modèles non linéaires et non gaussiens.

Parties prenantes

INSTITUT Mines-Télécom

TELECOM SudParis

Auteurs

Ivan Gorynin
Emmanuel Monfrini
Wojciech Pieczynski

Partenaires

FONDATION TELECOM

INSTITUT CARNOT Télécom & Société numérique

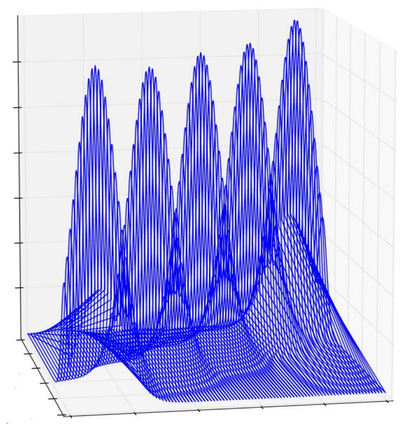
Lissage rapide bayésien exact avec SCGOMSM

Dans un contexte du processus de Markov caché *(X,Y)* à temps discret, stationnaire, avec *X* caché, nous nous intéressons au problème du lissage, *i.e.* à l'évaluation de $\mathbb{E}[X_n|\{Y_t\}_{t=1}^N = \{y_t\}_{t=1}^N]$, où $\{y_t\}_{t=1}^N$ est une observation de *Y*.

- Lorsque *(X,Y)* n'est pas un processus gaussien linéaire, l'estimation exacte de *X a posteriori* n'est pas possible en général et des approximations numériques - telles que EKF, UKF - ou des méthodes de Monte Carlo séquentielles, sont utilisées.
- Une représentation originale (SCGOMSM) est proposée.
- Dans cette représentation, lissage exact et rapide devient possible.
- La méthode proposée est de 10 à 50 fois plus rapide que le lissage particulaire.
- C'est une alternative simple, rapide et affranchie du problème de dégénérescence des poids.

La représentation SCGOMSM

Le SCGOMSM est un modèle auxiliaire, dans lequel lissage exacte et rapide est possible



- L'idée clé de l'utilisation d'un SCGOMSM est d'approcher la distribution stationnaire $p(x_1, y_1, x_2, y_2)$ du processus *(X,Y)* par un mélange gaussien:

$$p(x_1, y_1, x_2, y_2) \approx \sum_{1 \le i,j \le K} c_{ij} p_{ij}(x_1, y_1, x_2, y_2) \qquad (1)$$

où les composants p_{ij} vérifient $p_{ij}(y_2|y_1, x_2) = p_{ij}(y_2|y_1)$. Cette propriété des composantes est cruciale pour l'existence de l'algorithme de lissage rapide dans le SCGOMSM donné par (1).

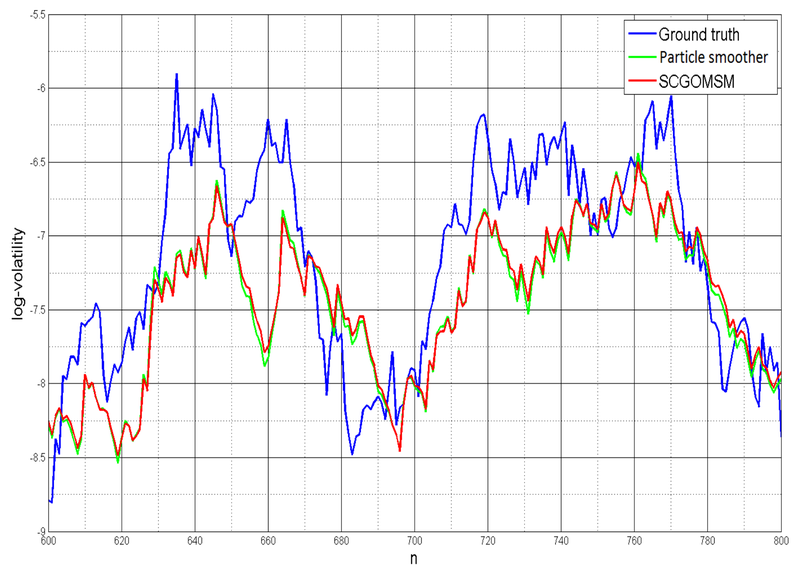
- Les paramètres de la représentation, qui sont les K^2 moyennes, matrices de covariance et coefficients des poids des composants gaussiennes, sont trouvés grâce à l'algorithme EM à partir d'un échantillon «d'entrainement», simulé avec le modèle original du processus *(X,Y)* indépendamment de l'observation $\{y_t\}_{t=1}^N$.
- Pour une observation $\{y_t\}_{t=1}^N$, l'algorithme de lissage de SCGOMSM assure l'estimation de *X a posteriori*. La complexité de cet algorithme est $O(N \times K^2)$.

Exemple d'application

- Un modèle de volatilité stochastique cherche à quantifier les fluctuations d'un actif. Nous avons considéré l'exemple de la volatilité stochastique, dont la distribution stationnaire $p(x_1, y_1, x_2, y_2)$ est donnée par

$$p(x_1, x_2, y_1, y_2) = \mathcal{N}(x_1; 0, \sigma_0^2)\mathcal{N}(x_2; \varphi x_1, \sigma)\mathcal{N}(y_1; 0, \exp(x_1))\mathcal{N}(y_2; 0, \exp(x_2))$$

- L'idée est d'approcher cette distribution par un SCGOMSM, puis d'utiliser l'algorithme de lissage rapide exact dans SCGOMSM.
- Pour *K*=5 l'estimation de *X a posteriori* est proche de celle obtenue par un lissage particulaire avec 1500 particules. Ainsi notre méthode assure un gain en vitesse de facteur 1500/25 = 60, et donne une estimation quasi-optimale.



Contact Ivan.Gorynin@telecom-sudparis.eu
Emmanuel.Monfrini@telecom-sudparis.eu
Wojciech.Pieczynski@telecom-sudparis.eu

Site web http://citi.telecom-sudparis.eu/fr/
http://www-public.tem-tsp.eu/~igorynin/SCGOMSMs/