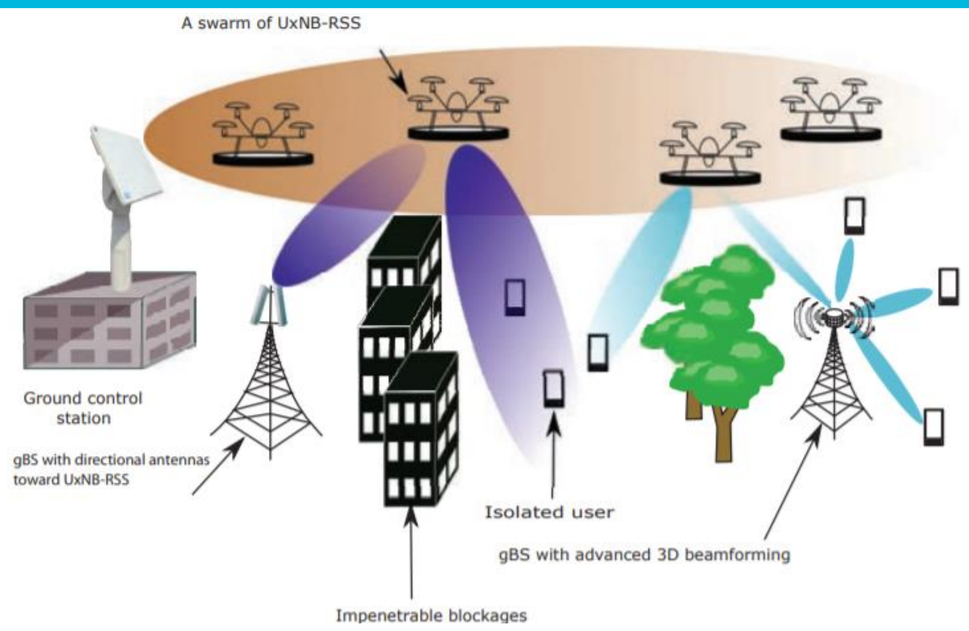
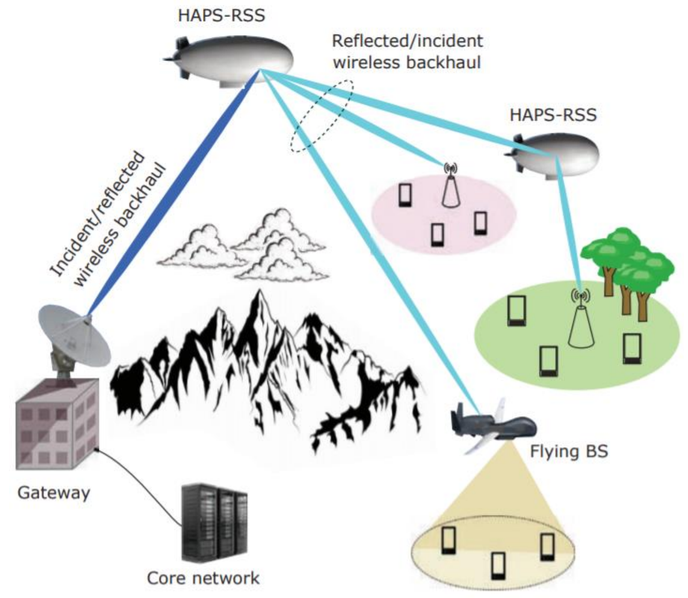
Communications radio avancées

Reconfigurable smart surfaces to support terrestrial communications

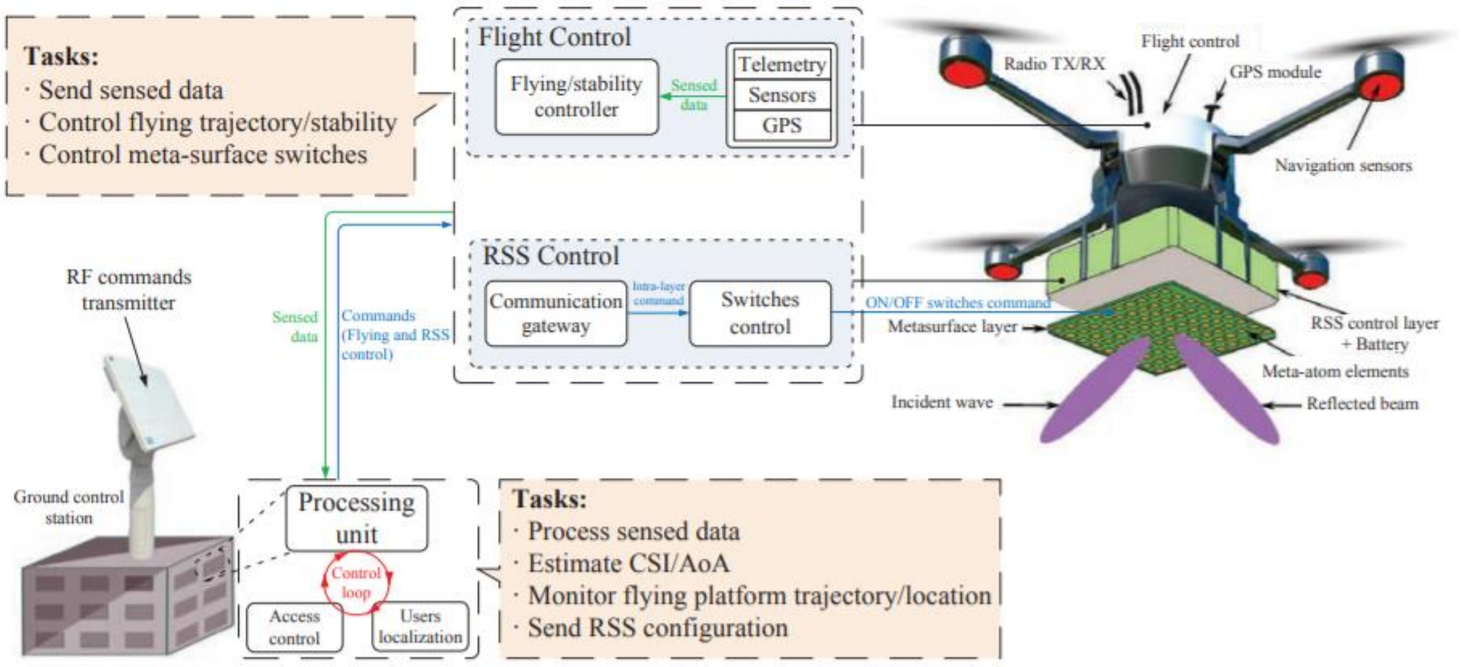


Support communications in urban environment



Support communications in rural environment

- **Problematic**– Meet a significant and temporary demand for communications services. Such demand cannot be met by the existing infrastructure designed to support normal user traffic in frequencies below 6 GHz.
- **Idea**– Reinforce the network infrastructure in such a way that it proactively responds to severe and temporary traffic peaks. The idea is to densify the existing infrastructure by a rapid deployment of high computational capacity stations operating in higher frequencies (mmWave, THz), while the backhaul of these stations will be brought from the sky via unmanned aerial vehicles (UAVs) or high altitude platform stations (HAPSs).



Control architecture of RSS-equipped aerial platforms

- **Reconfigurable smart surfaces (RSS)**– are some software-controlled metallic reflectors made of tiny scattering elements, i.e., metasurfaces, which can be controlled by low-power electronic circuits enabling their configurability over time. Quantifying the performance of RSS-assisted wireless networks, especially in large-scale deployments, requires new analytical tools along with two main directions: i) the development of link-level models for RSSs that allow us to quantify the power scattered by an RSS as a function of its configuration and ii) the amalgamation of the resulting link-level models with stochastic geometry in order to quantify network-level performance metrics (e.g., coverage probability, average rate, etc.).
- **Aerial platforms**–3GPP has considered aerial platforms to be a new radio access for 5G (TR 38.811, TR 22.829, and TS 22.125). Based on their operation altitudes, we distinguish two main types of aerial platforms: UAVs and HAPSs. UAVs operate at low altitudes of a few hundred meters and act as flexible and agile relays or base stations. Their use is generally time-limited, ranging from a few minutes to a few hours due to limited onboard energy. In contrast, HAPSs operate at higher altitudes of 8 to 50 km above ground, with current HAPS projects focusing on the 20 km altitude. They allow wider coverage areas and longer flight times compared to UAVs (e.g., Google Loon's flight record is 312 days).
- **Aerial platforms with aerial platforms to support terrestrial networks**– RSS can be combined with UAV/HAPS and their attendant benefits, namely, agility, flexibility, and rapid deployment, to assist terrestrial cellular networks in a cost-effective manner. Typically, RSS can be carefully mounted on a swarm of UAVs to create an intermediate reflection layer between ground base stations or core network and isolated users or small base stations, respectively. In this way, aerial platform allows smooth mechanical movement of the RSS layer, while the RSS enables digitally tuned reflections of incident signals.

Contact : yassine.hmamouche@imt-atlantique.fr

Parties prenantes

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Auteurs

Yassine Hmamouche
Mustapha Benjillali
Samir Saoudi

Partenaires

Carleton UNIVERSITY

Colloque Réseaux du futur - 14 octobre 2021 IMT Lille-Douai

Classification Adaptative des attaques IEMI et protocolaires sur les réseaux de communication IEEE 802.11n

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

Introduction

- **Communication sans fil** – Les communications par ondes radio sont couramment utilisées. Elles ont une grande capacité à s'étendre dans toutes les directions avec une portée relativement grande. Il est donc important de pouvoir mettre en place des systèmes de surveillance capables d'identifier des attaques envers ces systèmes.
- **Classification adaptative** – La classification adaptative est devenue un champ de recherche qui généralise des approches de classification pour des données non stationnaires.
- **Usage** – Organiser dans des groupes des évènements évoluant dans le temps avec ou sans connaissance des étiquettes associées à ces évènements.
- **Application** – Identification automatique de comportement frauduleux envers les réseaux de communication IEEE 802.11n

Parties prenantes

Université Gustave Eiffel

iemn

ELSAT2020

Auteurs

Jonathan VILLAIN
Virginie DENIAU
Anthony FLEURY
Eric Pierre SIMON
Christophe GRANSART

Partenaires/Financement

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Région Hauts-de-France

l'Europe s'engage en France

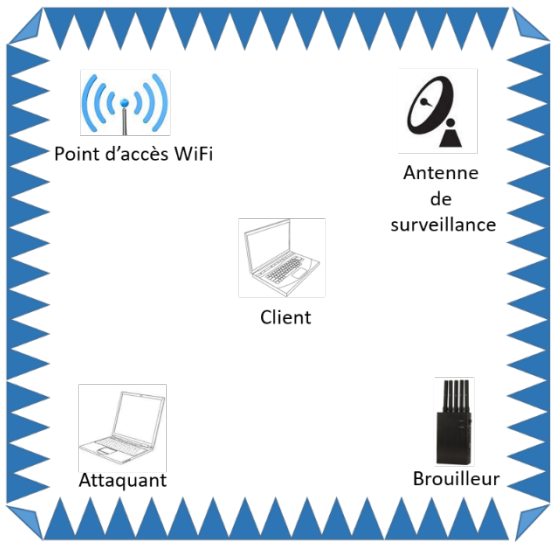


Figure 1: Configuration des acquisitions

Protocole Expérimental

- Le protocole de communication considéré est la norme **IEEE 802.11.n** qui utilise le schéma de modulation **OFDM**
- Le **canal 1** est utilisé (fréquence centrale 2,412 GHz)
- Les attaques considérées sont:
  - Les attaques par brouillage
  - L'attaque par déhautentification (attaque protocolaire)
- Le brouillage de la bande de fréquence **[2,4;2,5]**
- Le temps de balayage de l'analyseur est de **38,2 µs** pour une bande de résolution de **100 kHz**

Self Adaptative Kernel Machine

- Basé sur l'algorithme **One class SVM** développé par Schölkopf (2000).
- Architecture neural de type feed-forward
- Mesure de similarité induite par le noyau RKHS
- Règle de mise à jour (Initialisation ou création, Adaptation, Fusion)

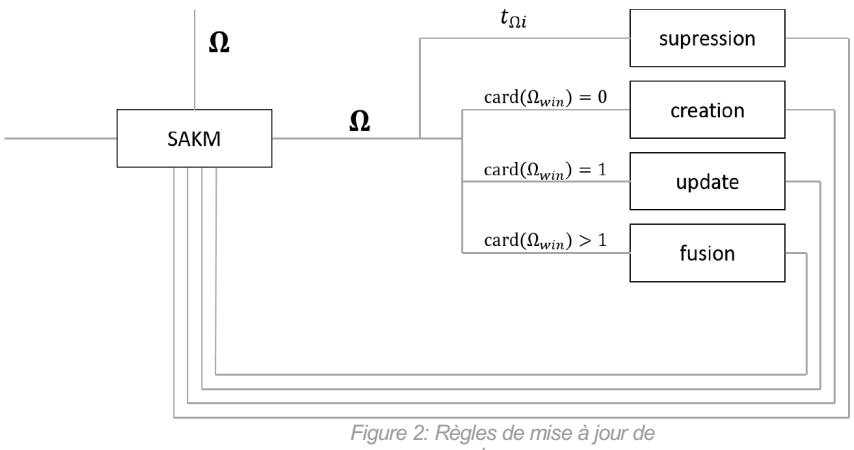


Figure 2: Règles de mise à jour de classes

Résultats

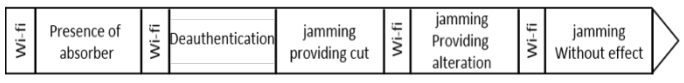
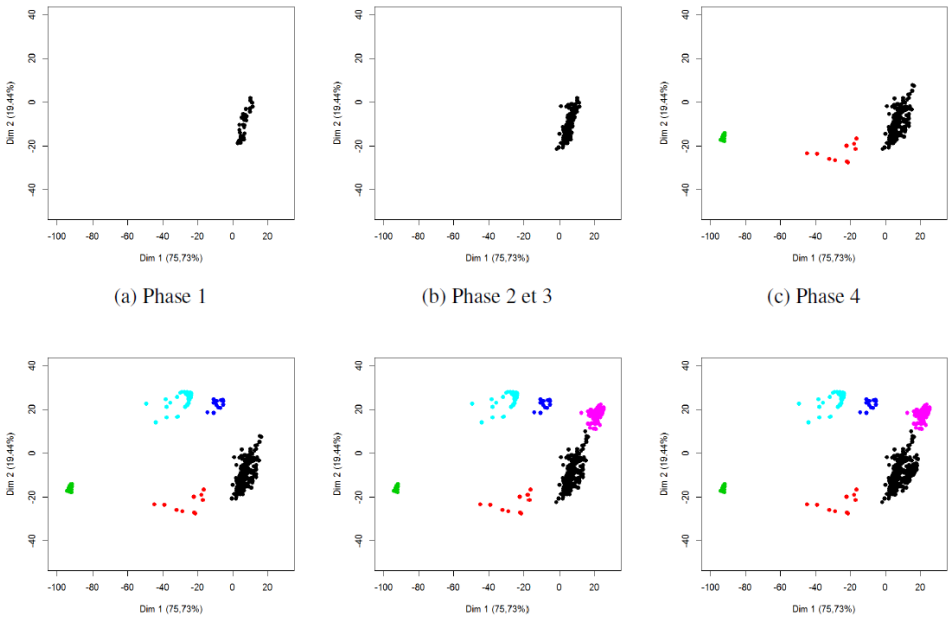


Figure 3: Organisation de le procédure d'acquisition dans le temps

	(b)	(c)	(d)	(e)	(f)
1 (noir)	100 %	100%	7%	4%	36%
2 (vert)	0%	0%	0%	0%	31%
3 (rouge)	0%	0%	100%	100%	33%
4 (bleu clair)	0%	0%	0%	39%	100%
5 (bleu)	0%	0%	0%	57%	0%
6 (violet)	0%	0%	93%	0%	0%

Tableau 1: Répartition des trames de communication dans les différents groupes



(a) Phase 1 (b) Phase 2 et 3 (c) Phase 4

(d) Phase 5 et 6 (e) Phase 7 et 8 (f) Phase 9

Figure 4: Evolution des classes

Contacts : jonathan.villain@univ-eiffel.fr / anthony.fleury@imt-nord-europe.fr

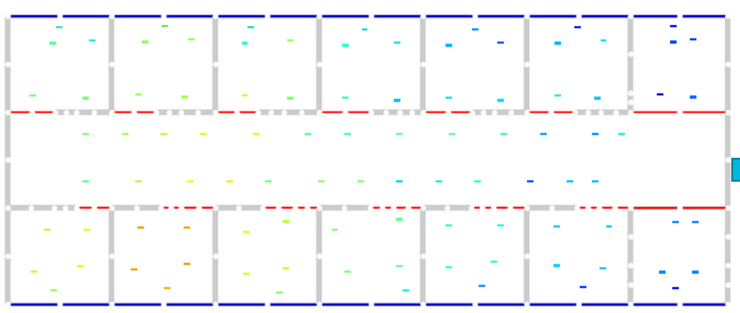
Août 2019 GRETSI Lille
Journée Cybersécurité et IoT. IMT. 14 octobre 2021 - Lille

EME-Net: An Indoor Electromagnetic Field (EMF) Exposure Map Reconstruction Tool

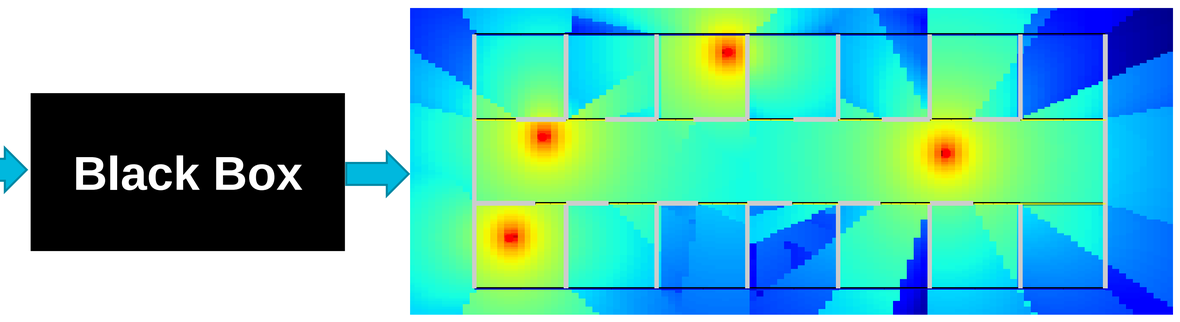
EME-Net is a machine learning tool to facilitate **dosimetry** for electromagnetic field measurement in indoor scenario. To respond to the perception of risks related to EMF exposure and allocate radio resources, estimating the received power and exposure map is a challenge. The designed model learns wireless signal propagation characteristics in a realistic indoor environment with varying locations of Wi-Fi access points .

Approach

An EMF exposure map estimation algorithm is proposed using **U-net** architecture based on **convolutional neural networks**. The power map estimation is transformed into an image reconstruction task by image color mapping, where every pixel value of the image represents received power intensity.



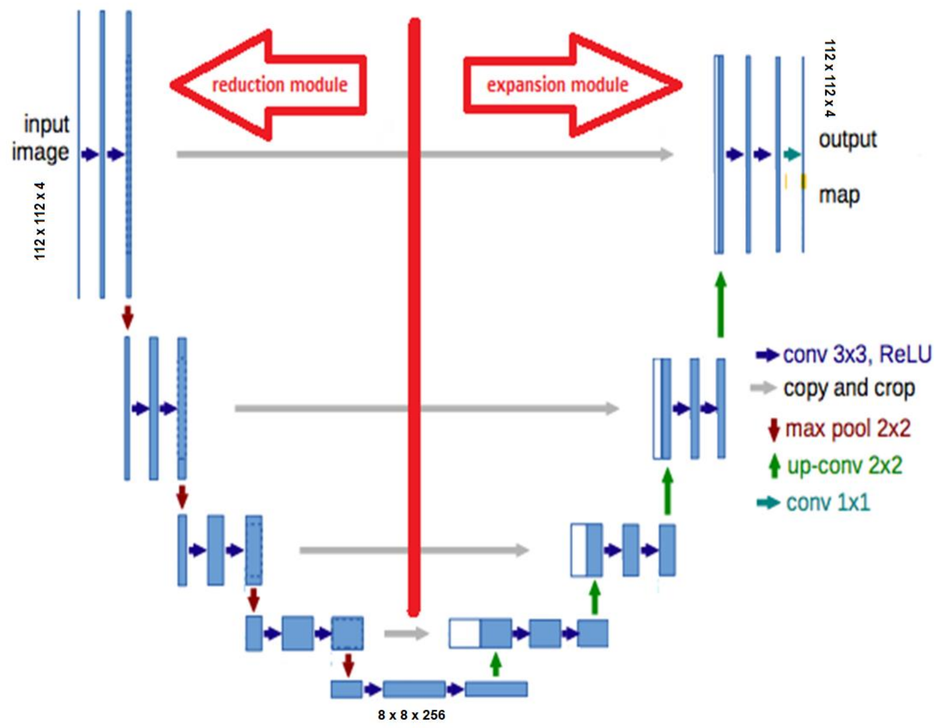
Input image with Pixels as measurement points



Output Image of reconstructed Exposure Map

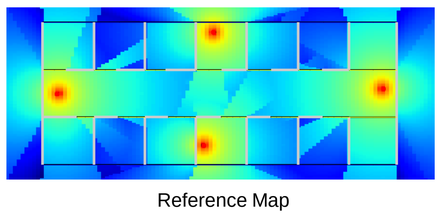
Methodology: U-Net reconstruction Model

A U-Net based CNN model is used to reconstruct exposure map images from incomplete measurement image.

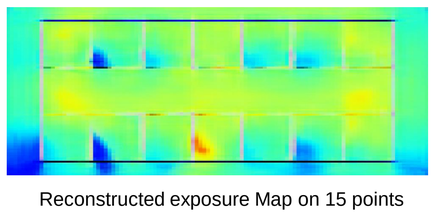


Result:

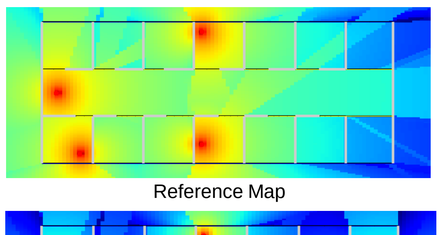
Reconstruction results with increase of pixels from 15, 50, 90 as measurement locations are shown.



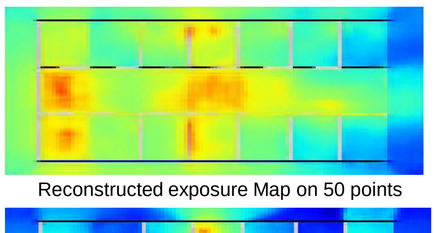
Reference Map



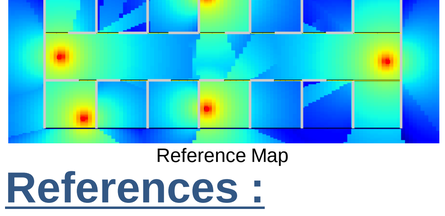
Reconstructed exposure Map on 15 points



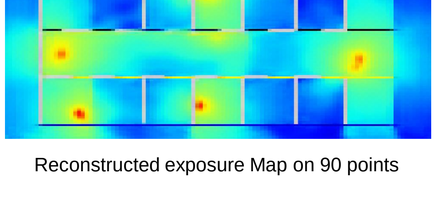
Reference Map



Reconstructed exposure Map on 50 points



Reference Map



Reconstructed exposure Map on 90 points

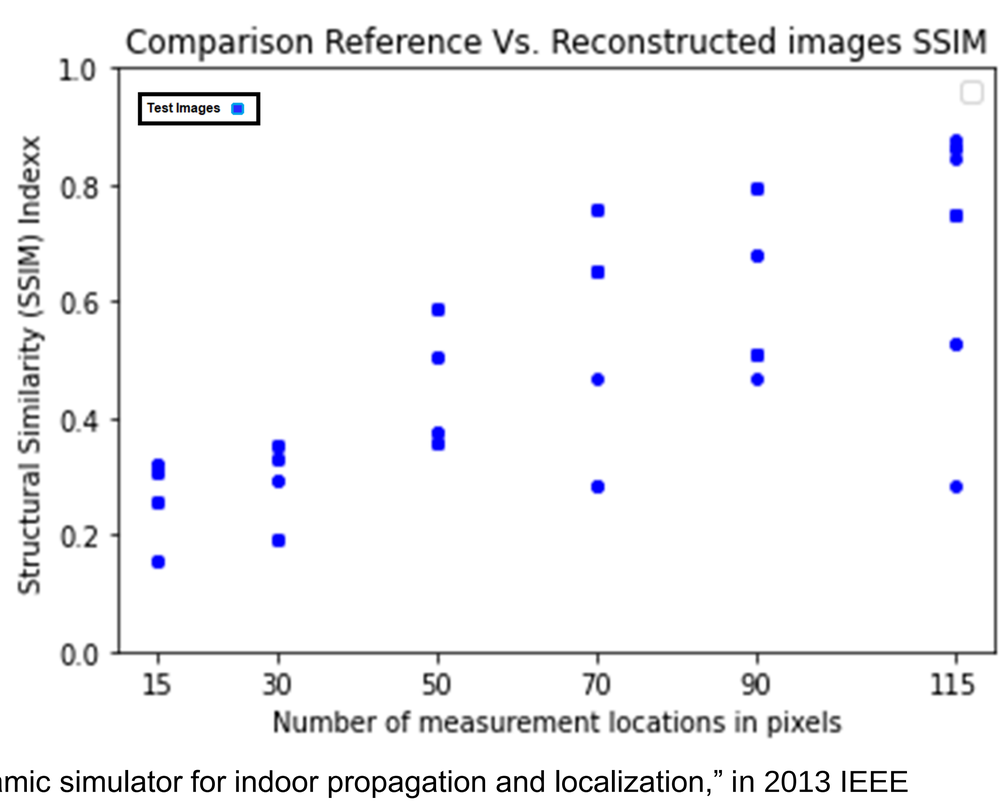
IRCICA-EME Dataset

'PyLayers' - an open source radio-channel wave propagation simulation tool, is used to generate reference power map in dense indoor environment. U-net model was trained on ~12000 images.

PyLayers

Result:

To evaluate the model's performance SSIM index is calculated between reference map and reconstructed images. SSIM value 1 indicates perfect similarity.



References :

[1] N. Amiot, M. Laaraiedh, and B. Uguen, "Pylayers: An open source dynamic simulator for indoor propagation and localization," in 2013 IEEE International Conference on Communications Workshops (ICC). IEEE, 2013, pp. 84–88.

[2] O. Ronneberger, P. Fischer, and T. Brox, "U-net: Convolutional networks for biomedical image segmentation," CoRR, vol. abs/1505.04597, 2015. [Online]. Available: http://arxiv.org/abs/1505.04597

Parties prenantes

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

Authors

Mohammed Mallik
Sofiane Kharbech
Shanshan Wang
Taghrid Mazloum
Joe Wiart
Davy P. Gaillot
Laurent Clavier

Partners

MEL MÉTROPOLE EUROPÉENNE DE LILLE

TELECOM ParisTech

Université de Lille

Centre National de la Recherche Scientifique

IRCICA Research Institute

Acknowledgment

This work is funded by Metropole Europeenne de Lille (MEL)

Power allocation in Uplink Multiband Satellite System with Nonlinearity-Aware Receiver

Arthur Louchart [1] Philippe Ciblat [1] Charly Poulliat [2]

[1]Institut Polytechnique de Paris / Telecom Paris [2]INP-ENSEEIHT

Introduction

We address power allocation for **uplink single-beam satellite system, in presence of nonlinear effects**, due to High-Power Amplifier (HPA) onboard the satellite.

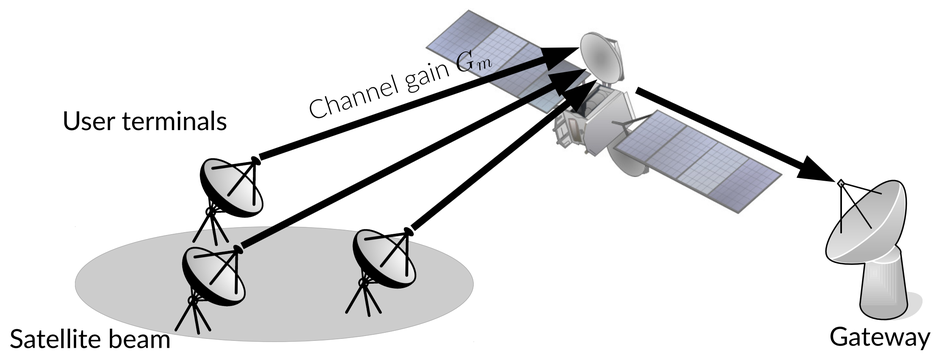


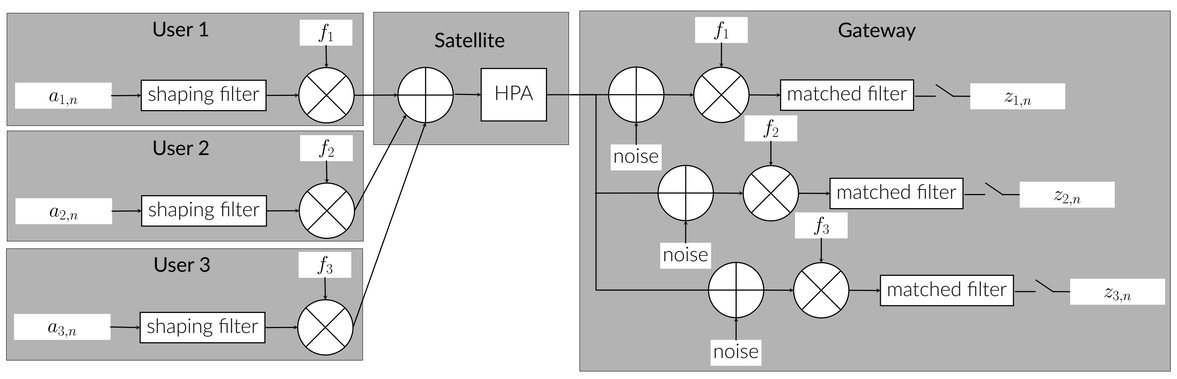
Figure 1. Terrestrial users transmit data to a satellite, which sends it back to the gateway.

Goal: Maximize the system sum-rate by taking into account the nonlinear effects.

System model

Satellite system

- One uplink single-beam satellite,
- M users in the beam with FDMA,
- Perfect satellite-gateway link,
- HPA modeled with Volterra series: $y(t)=\gamma_1 x(t)+\gamma_3 x(t)x(t)x^*(t)$ where γ_1 and γ_3 characterize the nonlinear distortion.



Input-output link

- Users send circularly-symmetric Gaussian symbol sequence $\{a_{m,n}\}_{n\in\mathbb{Z}}$.
- The transmit power of user m is $P_m = \mathbb{E}\left[|a_{m,n}|^2\right]$.
- The gateway receives sequence of samples $z_{k,n} = z^{\mathrm{L}}_{k,n} + z^{\mathrm{NL}}_{k,n} + w_{k,n}$.

We want to find the transmit power of users $\mathbf{p} = [P_1, \cdots, P_M]$.

Data rate expression in presence of nonlinearity

Assuming an optimal decoder that takes into account the nonlinear structure.

- **Nonlinearity-aware receiver**: the data rate of user m is

$$R_m(\mathbf{p}) = \log_2\left(1 + S_m(\mathbf{p})\right) \tag{1}$$

with

$$S_m(\mathbf{p}) = \frac{\left(\mathcal{P}_m^{(\mathrm{L})}\right)^2 + 2\mathcal{P}_m^{(\mathrm{L})}\mathcal{P}_m^{(\mathrm{LNL})} + \left(\mathcal{P}_m^{(\mathrm{LNL})}\right)^2}{\mathcal{P}_m^{(\mathrm{L})}\mathcal{P}_{\mathrm{W}} + \mathcal{P}_m^{(\mathrm{L})}\mathcal{P}_m^{(\mathrm{NL})} - \left(\mathcal{P}_m^{(\mathrm{LNL})}\right)^2}, \tag{2}$$

where

- $\mathcal{P}_m^{(\mathrm{L})} = \mathbb{E}[|z^{\mathrm{L}}_{m,n}|^2]$ is the auto-correlation of the linear part,
- $\mathcal{P}_m^{(\mathrm{NL})} = \mathbb{E}[|z^{\mathrm{NL}}_{m,n}|^2]$ is the auto-correlation of the nonlinear part, and
- $\mathcal{P}_m^{(\mathrm{LNL})} = \mathbb{E}[z^{\mathrm{L}}_{m,n} z^{\mathrm{NL}\,*}_{m,n}]$ is the cross-correlation between the linear and nonlinear parts.

Properties of the terms involved in data rate expression

- **Definition of monomials:** A monomial function takes the following form

$$m(\mathbf{p}) = cP_1^{b_1}\dots P_M^{b_M}$$

where $c \in \mathbb{R}^+$, $P_m \in \mathbb{R}^+$ and $b_m \in \mathbb{R}$.

- **Definition of posynomials:** A posynomial function has the following form

$$p(\mathbf{p}) = \sum_{n=1}^{N} m_n(P_1, \dots, P_K)$$

where $\{m_n\}_{n=1,\cdots,N}$ are monomial functions.

- **Definition of signomials:** A signomial function has the following form

$$s(\mathbf{p}) = p(\mathbf{p}) - q(\mathbf{p})$$

where p and q are posynomial functions.

- $\mathcal{P}_m^{(\mathrm{L})}$ is a monomial, $\mathcal{P}_m^{(\mathrm{LNL})}$ and $\mathcal{P}_m^{(\mathrm{NL})}$ are posynomials [1].
- $S_m(\mathbf{p})$ is a ratio of posynomials over signomials.

Problem statement

Goal: Solve the following Problem P1 to obtain the optimal power allocation $\mathbf{p}^\star$.

$$\mathbf{p}^\star = \arg\max_{\mathbf{p}} \sum_{m=1}^{M} R_m \text{ s.t. } 0 \le P_m \le P_{\max}\ \forall m \tag{P1}$$

Problem P1 boils down to **Signomial Programming**.

Resolution for Signomial Programming

1. Formulate an equivalent problem thanks to the monotonic increase of the log function,

$$\mathbf{p}^\star = \arg\max_{\mathbf{p}} \prod_{m=1}^{M} (1 + S_m) \quad \text{s.t.} \quad 0 \le P_m \le P_{\max}\ \forall m. \tag{P2}$$

2. Introduce slack variables $t_m \in \mathbb{R}^{+*}$ to move the term $1 + S_m(\mathbf{p})$ in the constraint set,

$$\mathbf{p}^\star = \arg\min_{\mathbf{p},\mathbf{t}} \prod_{m=1}^{M} t_m^{-1} \quad \text{s.t.} \quad 0 \le P_m \le P_{\max} \quad \forall m \tag{P3}$$

$$\frac{\mathcal{P}_m^{(\mathrm{L})} + 2\mathcal{P}_m^{(\mathrm{LNL})} + \mathcal{P}_m^{(\mathrm{NL})} + \mathcal{P}_{\mathrm{W}}}{\mathcal{P}_m^{(\mathrm{NL})} + \mathcal{P}_{\mathrm{W}} - \left(\mathcal{P}_m^{(\mathrm{L})}\right)^{-1}\left(\mathcal{P}_m^{(\mathrm{LNL})}\right)^2} \ge t_m \quad \forall m. \tag{3}$$

3. Rewrite the ratio of signomials (3) into ratio of posynomials [2],

$$\frac{t_m\left(\mathcal{P}_m^{(\mathrm{NL})} + \mathcal{P}_{\mathrm{W}}\right)}{D_m(\mathbf{p},\mathbf{t})} \le 1 \quad \forall m \tag{4}$$

where $D_m(\mathbf{p},\mathbf{t})$ is a posynomial function defined as

$$D_m(\mathbf{p},\mathbf{t}) = \mathcal{P}_m^{(\mathrm{L})} + 2\mathcal{P}_m^{(\mathrm{LNL})} + \mathcal{P}_m^{(\mathrm{NL})} + t_m\left(\mathcal{P}_m^{(\mathrm{L})}\right)^{-1}\left(\mathcal{P}_m^{(\mathrm{LNL})}\right)^2 + \mathcal{P}_{\mathrm{W}}. \tag{5}$$

4. Use SCA procedure with monomial approximation of the denominator (5),

$$\mathbf{p}_i^\star = \arg\min_{\mathbf{p},\mathbf{t}} \prod_{m=1}^{M} t_m^{-1} \quad \text{s.t.} \quad 0 \le P_m \le P_{\max} \quad \forall m \tag{P3'}$$

$$\left(\widetilde{D}_m^{(i-1)}(\mathbf{p},\mathbf{t})\right)^{-1} t_m\left(\mathcal{P}_m^{(\mathrm{NL})} + \mathcal{P}_{\mathrm{W}}\right) \le 1 \quad \forall m \tag{6}$$

where $\widetilde{D}_m^{(i-1)}(\mathbf{p},\mathbf{t})$ is the monomial approximation of $D_m(\mathbf{p},\mathbf{t})$ at the point $\mathbf{p}_i$ which satisfies SCA condition [3].

Numerical results

- $M = 6$ where 2 users have rainy conditions,
- Channel gains are obtained with users location,
- Ideal pre-amplifier G_{amp} before HPA,
- $P_{\max} = 50\mathrm{W}$,
- SRRC with roll-off 0.25 for all users.

Data rate expression of user m for nonlinearity-agnostic receiver: $\underline{R}_m = \log_2\left(1 + \frac{\mathcal{P}_m^{(\mathrm{L})}}{\mathcal{P}_m^{(\mathrm{NL})} + \mathcal{P}_{\mathrm{W}}}\right)$.

Data rate expression of user m for AWGN (without nonlinearity): $C_m = \log_2\left(1 + \frac{\mathcal{P}_m^{(\mathrm{L})}}{\mathcal{P}_{\mathrm{W}}}\right)$.

Problem with nonlinearity-aware receiver

- P^{naive}: $P_m = P_{m'}$ and 1-D search,
- $P^\star$: proposed algorithm.

Problem with nonlinearity-agnostic receiver

- $\underline{P}^{\mathrm{naive}}$: $P_m = P_{m'}$ and 1-D search,
- $\underline{P}^\star$: proposed algorithm.

In dotted line the solution is evaluated with $\underline{R}_m$.

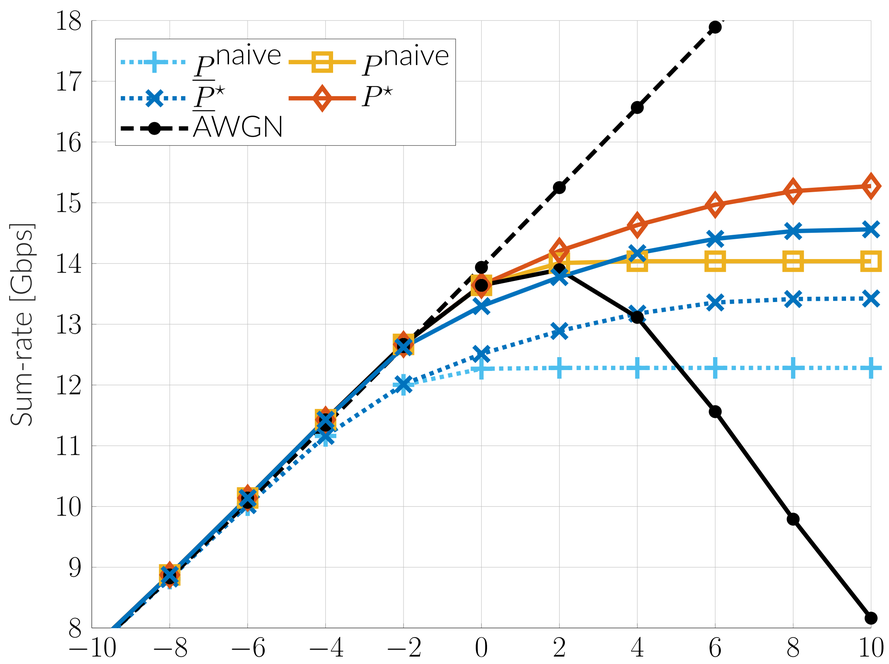


Figure 2. Sum-rate vs. pre-amplifier gain G_{amp}

- Higher sum-rate when the receiver exploit the nonlinear effects.
- Gain when the optimization is done with data rate of nonlinearity-aware receiver.
- Sum-rate obtained for AWGN (when nonlinear effects are ignored) is bad.

Conclusion & Perspective

We have proposed algorithm for **power allocation when high-power amplifer operates in nonlinear regime**.

For future works, we will consider satellites belonging to different operators, leading to distributed resource allocation.

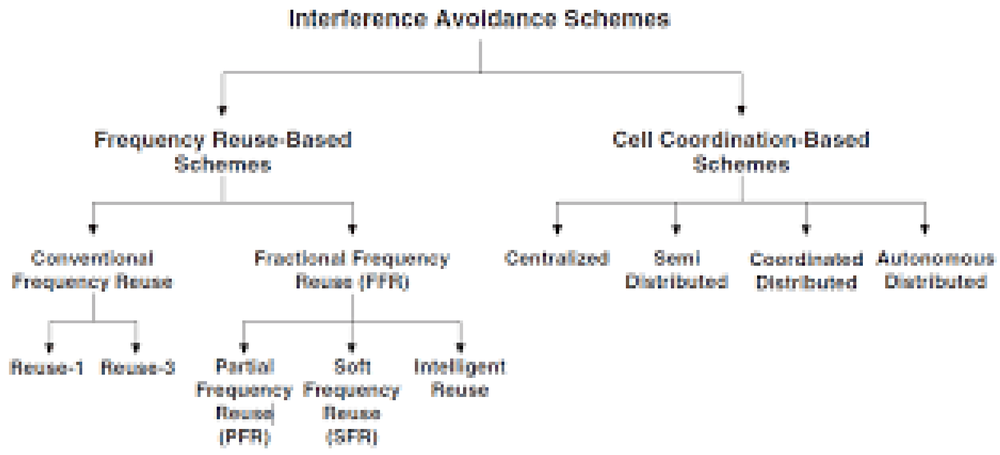
References

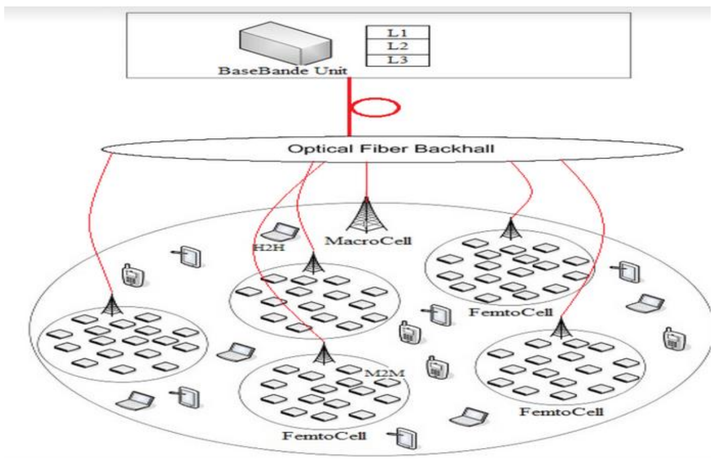
[1] A. Louchart, P. Ciblat, and C. Poulliat, "Sum-capacity of uplink multiband satellite communications with nonlinear impairments," in *International Conference on Communications (ICC)*, Montreal, Canada, 2021, pp. 1–6.

[2] M. Avriel and A. C. Williams, "Complementary geometric programming," *SIAM J. Appl. Math.*, vol. 19, no. 1, pp. 125–141, 1970.

[3] A. Louchart, P. Ciblat, and C. Poulliat, "Power allocation in uplink multiband satellite system with nonlinearity-aware receiver," in *Signal Processing Advances in Wireless Communications (SPAWC)*, Lucca, Italy, 2021, pp. 1–5.

Hetnets and 5G Frequency Interference mitigation and power control for efficient resource allocation.





Parties prenantes

Auteurs

Hakima Chaouchi
Professeur
Telecom Sud Paris
Institut Mines Telecom
Institut Polytechnique de Paris

Partenaires

Publications

[1] Amel Bouaziz, Ahlem Saddoud, Lamia Chaari, Hakima Chaouchi, “Adaptive V2X User Selection and Resource Allocation for Ultra-Dense 5G HetNet Network”, International Wireless Communications and Mobile Computing, IWCMC 2021.

[2] Amel Bouaziz, Ahlem Saddoud, Lamia Chaari, Hakima Chaouchi, “QoS-Aware Resource Allocation and Femtocell Selection for 5G Heterogeneous Networks”, Telecommunication Systems Journal, 24/06/2021

[3] G. Giambene, T. Bourgeau, H. Chaouchi et al., “Iterative multi-level soft frequency reuse with load balancing for heterogeneous LTE-A systems," IEEE Transactions on Wireless Communications, vol. 16, no. 2, pp. 924{938, 2017.

[4] MSP Fonseca, A Munaretto, C Mendes, H Chaouchi “ A resource management framework for 802.11 wireless access networks”, Wireless Networks Journal, 2016

[5] G. Giambene, Vahn Le, T. Bourgeau, H. Chaouchi et al “Soft frequency reuse schemes for heterogeneous LTE systems” IEEE ICC 2015.

[6] H Xiong, D Zhang, L Wang, H Chaouchi “EMC3: Energy-efficient data transfer in mobile crowdsensing under full coverage constraint”, IEEE Transactions on Mobile Computing, 2015.

Frequency reuse Planning

Novel Multi-level Soft Frequency Reuse with frequency and power combination

- **Multilevel Soft Frequency Reuse** *(MSFR)* –planning of two-layer cellular systems, taking both the co-tier and cross-tier interference into account.
- **Different Power and Frequency**– The users in three different regions of a macro/micro cell adopt distinct frequency segments and different transmission power levels.

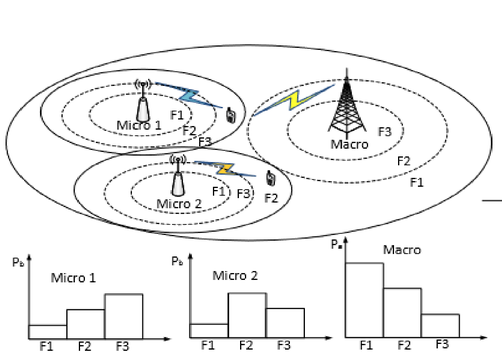


Fig. 1: MSFR frequency reuse plan

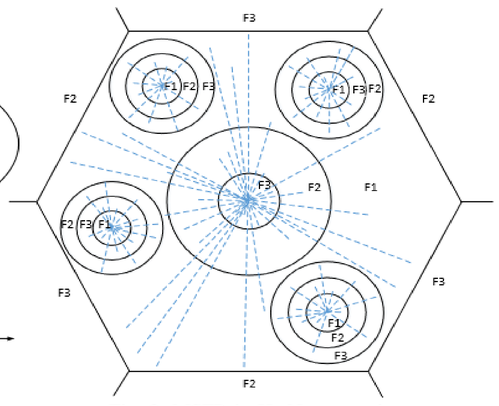
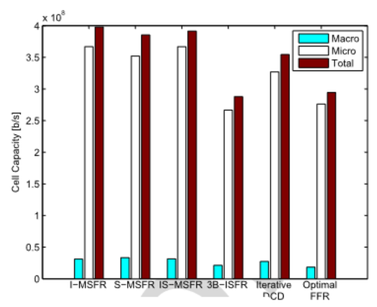


Fig. 2: MSFR in HetNet scenario

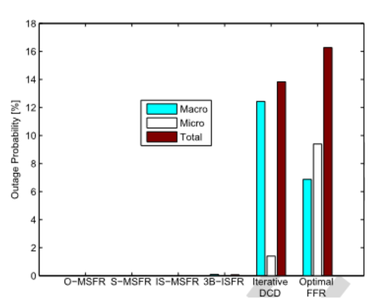
- We introduce a *Multi-level SFR* (MSFR) scheme, where each cell is divided into three parts (central, intermediate, edge), using different frequency segments and transmission power control levels to improve SINR conditions.
- We propose a joint optimization problem for UE association (including cell-offloading), frequency selection, and MSFR power control; then, an iterative method is adopted to solve this problem.
- Finally, we present two low-complexity approaches for cell association, frequency selection, and power control that achieve a comparable performance as I-MSFR.

Algorithm 1 I-MSFR Algorithm

1: Run Step #1 to obtain the starting point $\boldsymbol{\alpha}^{(0)}$.
2: Run Step #2 to the obtain optimal cell association and frequency selection $\mathbf{X}$ with current $\boldsymbol{\alpha}^{(0)}$ and corresponding $\phi^{(0)}$.
3: **repeat**
4: Given $\phi^{(k)}$, $\mathbf{X}^{(k)}$ and $\boldsymbol{\alpha}^{(k)}$ at iteration k.
5: Run Step #3 to the obtain optimal power control vector $\boldsymbol{\alpha}^{(k+1)}$ with given $\mathbf{X}^{(k)}$.
6: Run Step #2 to obtain the optimal $\mathbf{X}^{(k+1)}$ with current $\boldsymbol{\alpha}^{(k+1)}$ and achieve $\phi^{(k+1)}$.
7: **until** $\frac{|\phi^{(k+1)}-\phi^{(k)}|}{\phi^{(k)}} < \zeta$



Cell capacity comparison for different schemes.

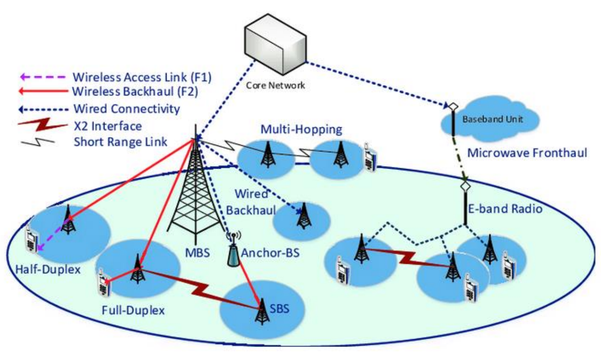


Outage probability comparison for different schemes.

NOMA based 5G/Beyond/6G efficient Power based ressource allocation in the context of Wired/Wireless Backhauling

Research Perspectives

- To study the potential gains of using SFR in 5G and beyond networks.
- Propose a hybrid SFR-NOMA based architecture.
- To study the fundamental limits such as capacity, throughput, sum rate etc. for the proposed architecture.
- To study the impact of practical consideration and its impact on the capacity, throughput, sum rate etc.
- To implement these algorithms in real time lab setup (using software defined radios (SDRs)), and highlight and assess the potential gains for wireless networks.



Wireless backhauling of 5G small cells: Challenges and solution approaches

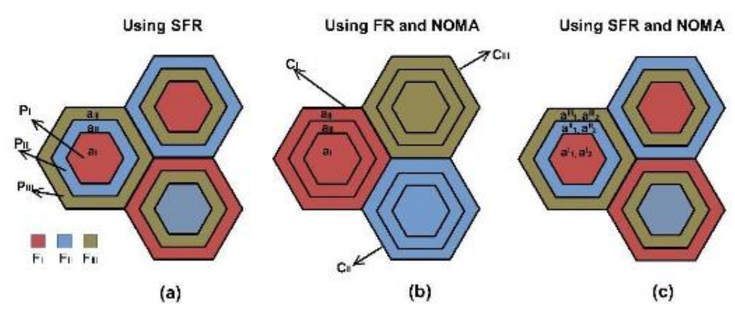


Fig. 1: An illustration of the proposed network architecture

Contact : hakima.chaouchi@telecom-sudparis.eu

Réseaux et services du futur

Software-Defined Networking (SDN) :

Towards Adaptive Distributed SDN Controllers for large-scale networks

Parties prenantes

Institut Mines-Télécom

Authors

Fetia Bannour
Sami Souihi
Abdelhamid Mellouk

Partenaires

ensiie Paris | Évry-Courcouronnes

s@movar

TELECOM SudParis

IP PARIS

UNIVERSITÉ PARIS-EST

LiSSi

Contact

fetia.bannour@ensiie.fr

fetia.bannour
@telecom-sudparis.eu

1- What exactly is SDN and Why is it important?

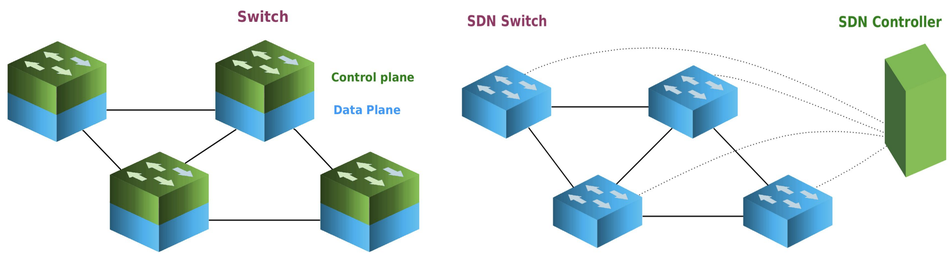
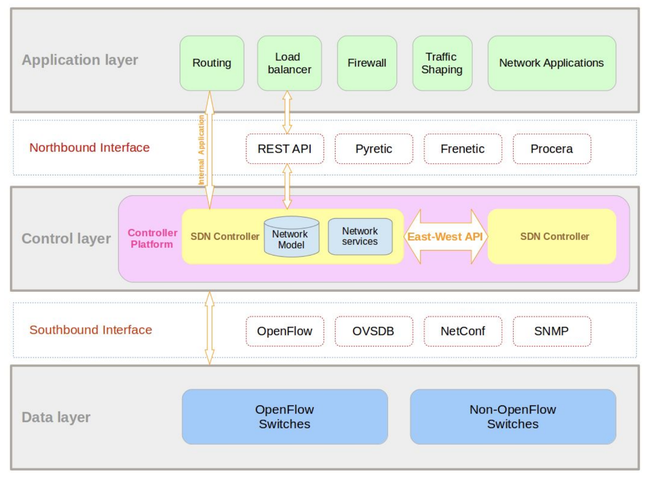


Figure : Conventional Networking Versus Software-Defined Networking

- **Separation** between the Data and Control Planes (abstractions),
- **Centralization** of the Control logic in Software-based controllers

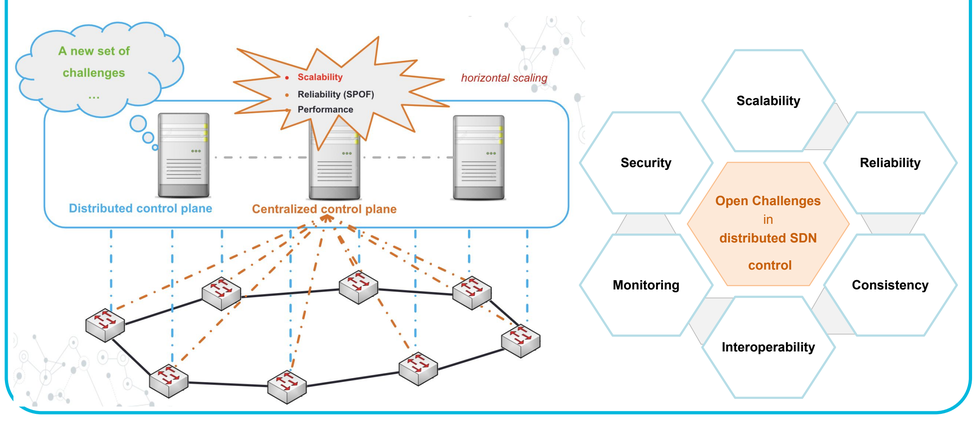
→ Network Programmability, Openness, Innovation, increased Visibility,
→ better Flexibility, better Network Management, Network Automation.

2- The Logically-Centralized SDN Control

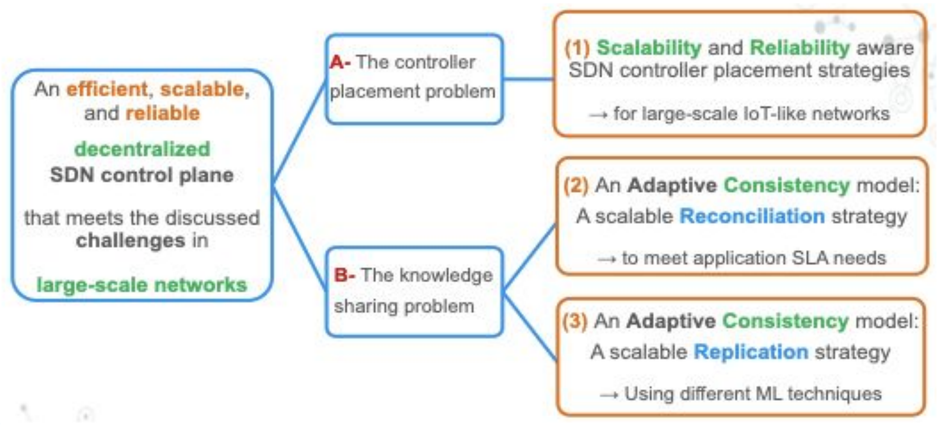


→ Classification of existing SDN controller platforms (ONOS, ODL..) [1]

3- Physically-Centralized vs Physically-Distributed SDN Control

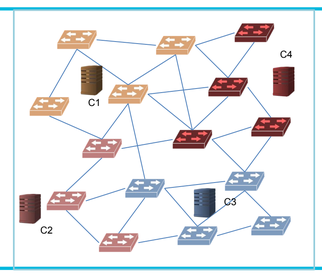


4- Main Contributions



4. A- The Controller Placement Problem

- Finding the appropriate number and locations of the SDN controllers
  → to achieve the best trade-off between performance and reliability criteria
- Multi-criteria placement algorithms, Gradual context-based strategies [2]

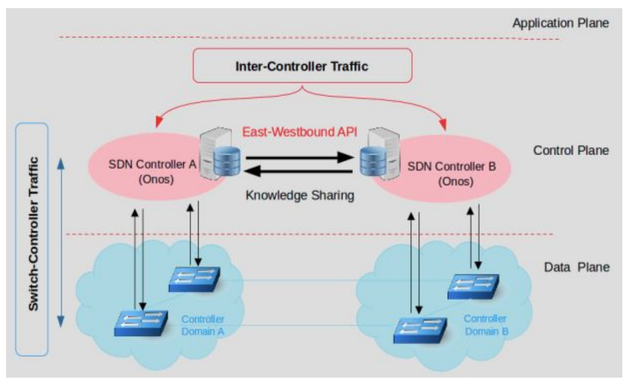


4. B- The Knowledge Sharing Problem

- Inter-controller communication is needed → correct application behavior

→ too much Overhead (performance ↓) especially in large-scale SDNs.

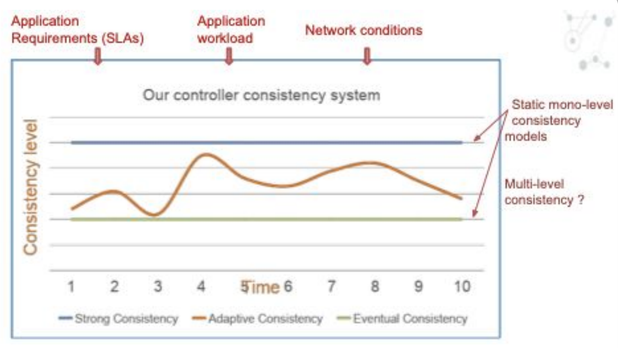
⇒ Need for an **adaptive multi-level consistency** for large-scale SDNs ?

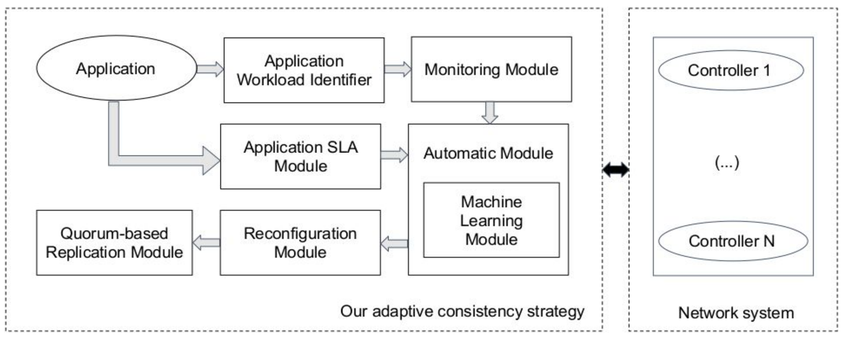


- We propose adaptive and time-varying control consistency models [3] [4]

→ They adapt to changing network and application conditions.

⇒ to satisfy application SLAs & minimize inter-controller overheads at scale.





- In [5], the proposed Quorum-based consistency strategy uses RL (Q-learning). It is implemented on ONOS for our CDN-like application.

5- Ongoing Work and Future Perspectives

- Towards a standardized distributed SDN control plane :
  - Formal modelling/verification of decentralized SDN implementations,
  - Securing the SDN control plane (the inter-controller communications),
  - An interoperable, automated, scalable and reliable SDN control plane,
- Innovative use-cases for the future next-generation networks :
  - Advanced management of softwarized content distribution networks,
  - Application of AI and distributed SDN to the sliced 5G core network.

References

[1] F.Bannour, S.Souihi, and A.Mellouk. Distributed SDN Control: Survey, Taxonomy, and Challenges. IEEE Communications Surveys & Tutorials , 2018

[2] F.Bannour, S.Souihi, and A.Mellouk. Scalability and reliability aware SDN controller placement strategies. In CNSM conference, ManSDN/NFV, Tokyo, 2017

[3] F.Bannour, S.Souihi, and A.Mellouk. Adaptive State Consistency for Distributed ONOS Controllers. In IEEE GLOBECOM conference, Abu Dhabi, UAE, 2018

[4] F.Bannour, S.Souihi, and A.Mellouk. Adaptive Quorum-inspired SLA-Aware Consistency for Distributed SDN controllers. In CNSM, Halifax, NS, Canada,, 2019

[5] F.Bannour, S.Souihi, and A.Mellouk. Adaptive distributed SDN controllers:Application to Content-Centric Delivery networks. FGCS, 2020

Colloque de l'Institut Mines Télécom Lille
Octobre 2021

Study of post-quantum algorithms that can be implemented in practice

Parties prenantes

MINES Saint-Étienne
Une école de l'IMT

WISeKey

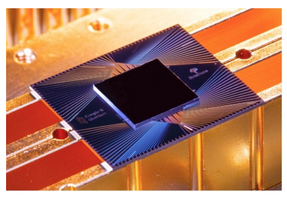
Auteurs

Lina Mortajine
lina.mortajine@emse.fr

Supervisor :
Nadia El Mrabet
nadia.el-mrabet@emse.fr

Context

As we enter the digital era, the need of encryption systems to protect sensitive communications against adversaries is dramatically increasing. An important part of the cryptosystems in use today is based on mathematical problems known to be hard to solve such as the prime factorization or the discrete logarithm problem.
In 1996, Peter Shor developed a quantum algorithm able to solve these problems, which requires the use of a large-scale quantum computer. The research on quantum computing is still in progress (IBM and Google are the leader in the field), however, the current cryptography is not broken yet.

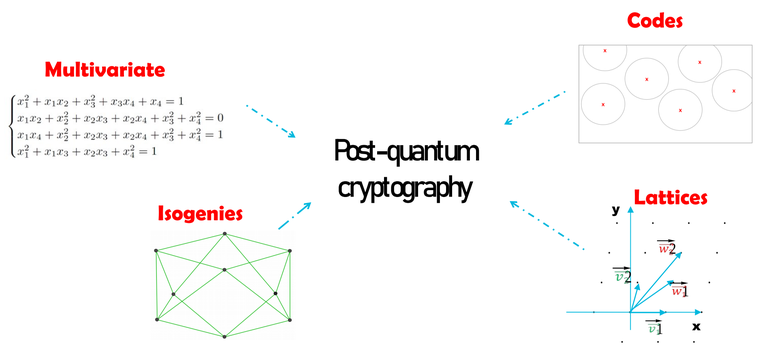


54-qubit chip
© Google

50-qubit computer
© IBM

With the significant advances in the research on quantum computing, the National Institute of Standards and Technology (NIST) has launched in 2016 the post-quantum project:

- Aim: standardize cryptographic algorithms for signature, encryption and key establishment.
- Submissions are based on different mathematical problems for which no classical or quantum algorithms are known to solve them in polynomial time.



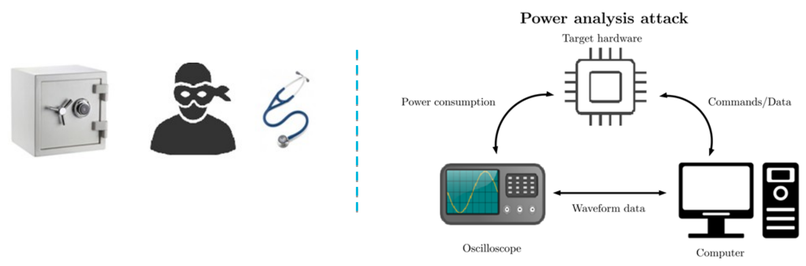
Objectives

- studying and implementing some candidates of the NIST post-quantum standardization on commercialized microcontrollers,
- studying and setting up side-channel attacks against embedded implementations and providing countermeasures.

Methodology

1. Implementation with memory optimizations of the selected candidates on an embedded system.

2. Study of the implemented cryptosystems' vulnerabilities against side-channels attacks such as power analysis.



3. Exploitation of the leakage emanating from the device to recover sensitive data (such as the secret key) by targeting operations that manipulate the secret data.

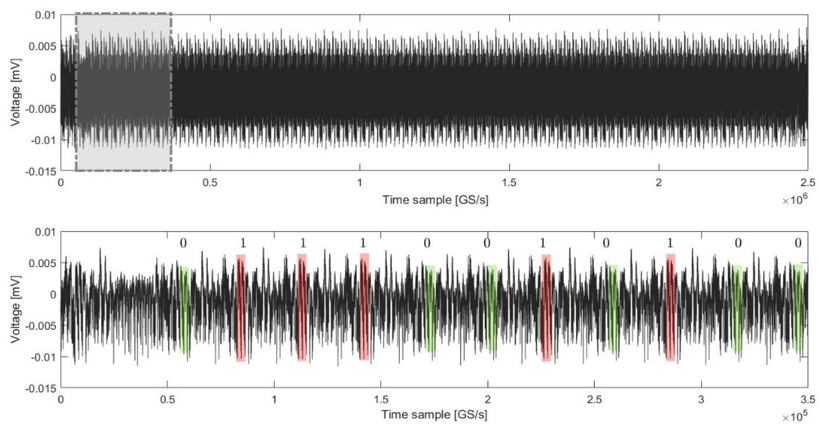


Fig: power consumption analysis of the Gaussian elimination performed in ROLLO-I, a code-based submission

4. Implementation of countermeasures to secure the cryptosystem. This can be done by masking the secret data, adding some "noise" or dummy operations to suppress any kind of leakage.

5. Verification of the countermeasures effectiveness.

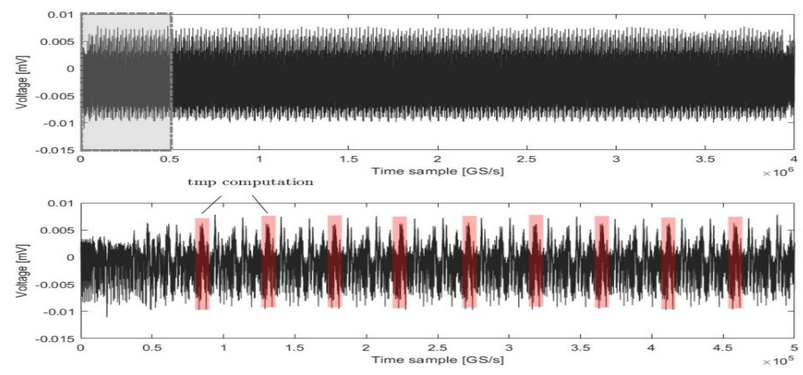


Fig: power consumption analysis of the Gaussian elimination with countermeasures

Three post-quantum candidates have been studied :

- ROLLO [code-based candidate] and NTRU [lattice-based candidate] : public key encryptions and key encapsulation mechanisms
- Crystals-Dilithium[lattice-based candidate] : signature scheme

Conclusion

The research in quantum computing is constantly increasing and it is essential to be prepared for the transition towards post-quantum cryptography. The integration of new algorithms in microcontrollers is very challenging due to the constraints of these technologies (memory size, power consumption, speed execution, security against SCA), thus, the pre-study allows us to see what it takes to integrate post-quantum algorithms and the integration costs.

Resistance of isogeny-based cryptographic implementations to a fault attack

Parties prenantes

MINES Saint-Étienne — Une école de l'IMT

CEA tech — From research to industry

Auteurs

Élise Tasso[1]
elise.tasso2@cea.fr
Luca De Feo[2]
Nadia El Mrabet[3]
Simon Pontié[1]

[1] CEA-Leti, Université Grenoble Alpes, F-38000 Grenoble, France
CEA-Tech, Centre CMP, Équipe Commune CEA Tech – Mines Saint-Étienne, F-13541 Gardanne, France

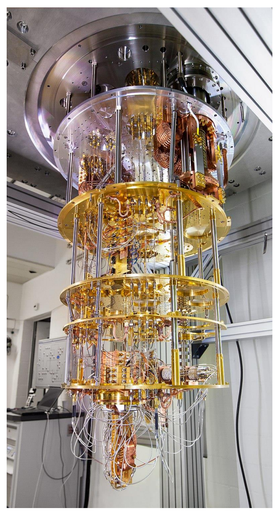
[2] IBM Research, Zürich, Switzerland

[3] Mines Saint-Étienne, CEA-Tech, Centre CMP, F-13541 Gardanne, France

Context

- post-quantum threat
- NIST post-quantum cryptography standardization contest

Post-quantum cryptography is an essential tool to secure the networks of the future.

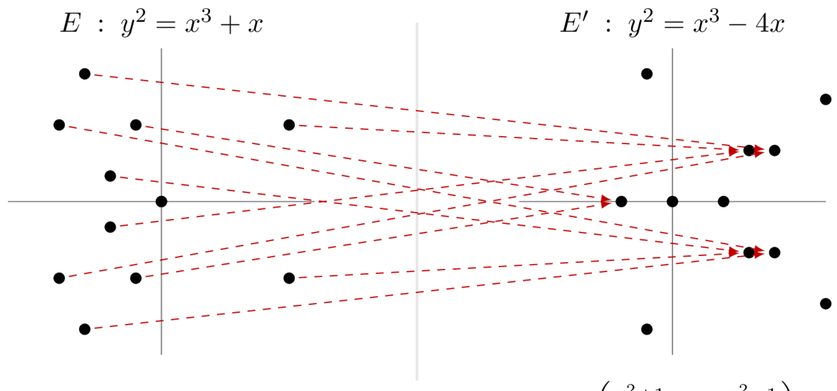


Post-quantum computer at the IBM Research laboratories in Zurich (source: IBM Research)

SIKE (Supersingular isogeny key encapsulation) is

- one of the candidates for encryption and key exchange,
- the only one based on isogenies.

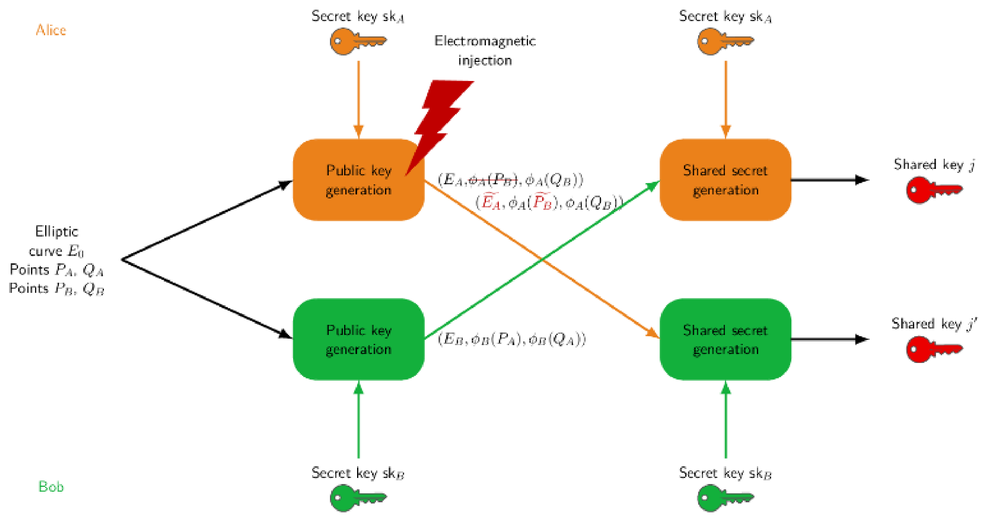
Isogenies between elliptic curves : a toy example



Isogeny ϕ defined on $\mathbb{F}_{11}$ such that $\phi(x, y) = \left(\frac{x^2+1}{x}, \quad y\frac{x^2-1}{x^2}\right)$

Ti's theoretical fault attack (2017)

Principle: recover Alice's secret key using both her correct public key and an altered version of her public key.



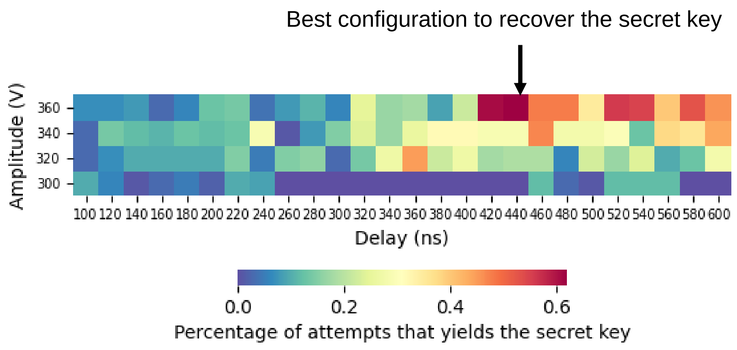
Questions

1. Is the attack exploitable in practice ?
2. What are suitable countermeasures ?

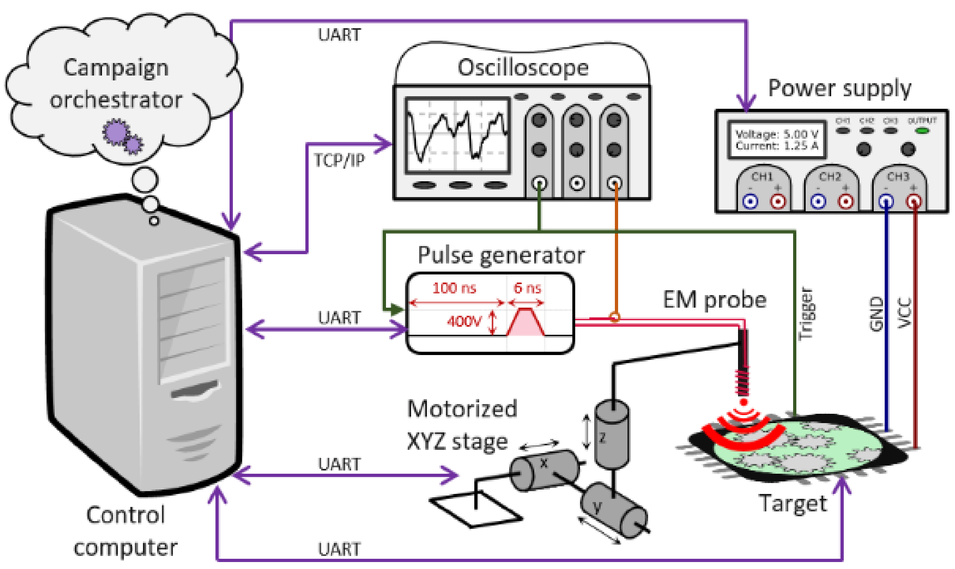
Our work

Ti's attack in practice

Target: ARM v8 software implementation of the round 3 SIKE key exchange (isogen function) on a system on chip with four A53 Cortex cores.
Method: electromagnetic fault injection.
Results: 1,040,000 attempts to recover the secret key in 4.5 days, success every 3 minutes and 18 seconds.



Campaign setup



Countermeasure

- Avoiding to compute twice the public key using the same secret is an easy countermeasure.
- But it does not suffice in a multipartite key exchange, thus we add an intrinsic countermeasure: a verification at the end of the public key generation.

Conclusion

- We characterize the threat to the SIKE protocol.
- There are few constraints on the fault required to perform the attack in laboratory.
- Our countermeasure has both a small overhead and a high probability to detect a fault.

Protect IOT Applications From Physical Fault Attacks.

Coordination

MINES Saint-Étienne
Une école de l'IMT

Auteurs

Anthony ZGHEIB
Olivier POTIN
Jean-Baptiste RIGAUD
Jean-Max DUTERTRE

Partenaires

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

FROM RESEARCH TO INDUSTRY cea tech

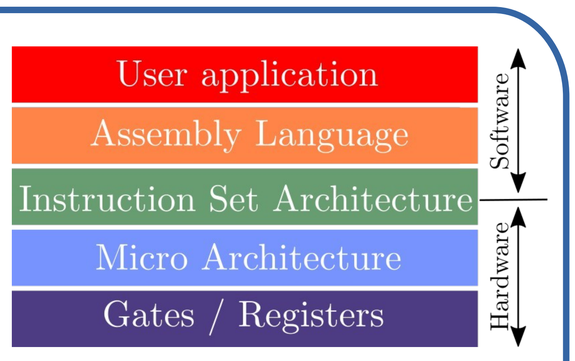
INVIA a Thales company

PROJET FINANCÉ PAR L'ANR - PROJECT FUNDED BY THE ANR

SIS SCIENCES INGÉNIERIE SANTÉ UNIVERSITÉ DE LYON
ÉCOLE DOCTORALE 488

Introduction

- Physical attacks are particularly effective threats to strike **confidentiality**, **integrity** or **authenticity** of systems[1].
- Several protections have been proposed such as :
  - Software-based **Control Flow Integrity (CFI)[2].**
  - Hardware-based monitoring of the **control-flow** or **code integrity** [3,4] (at the price of high overheads).



- **Most of the protection do not cover all levels of a system [software, Instruction Set Architecture (ISA), hardware] giving vulnerabilities for malicious users.**

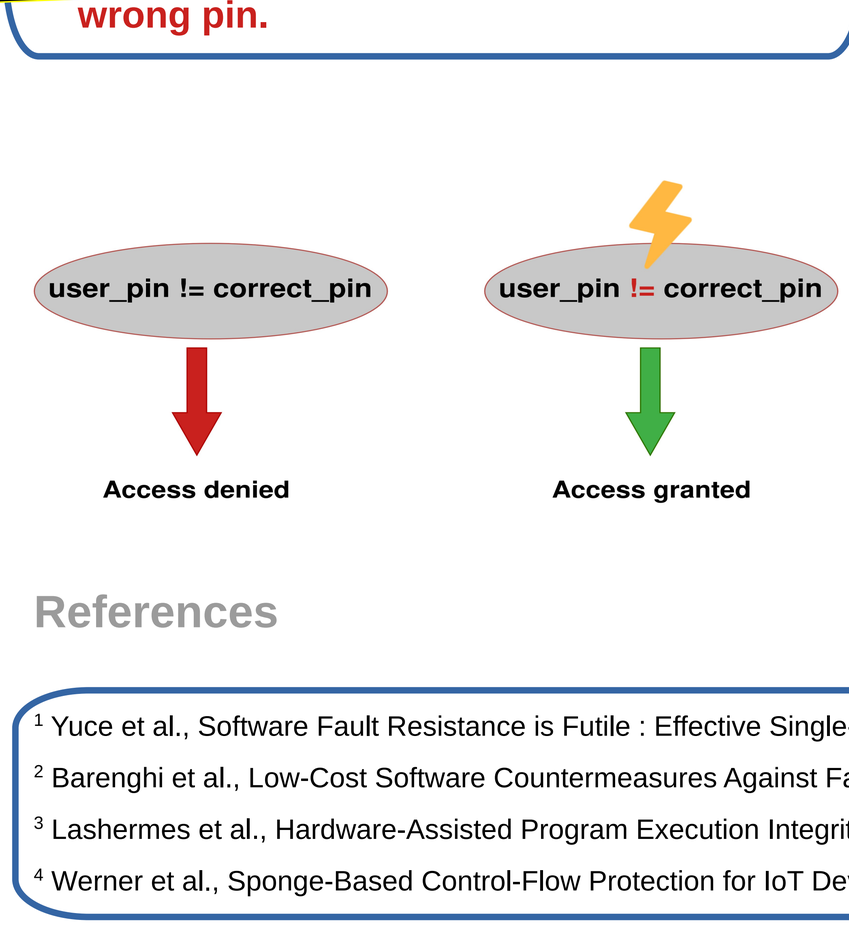
PhD Thesis Objectives*

- Perform fault injection attacks on Reduced Instruction Set Computer (RISC) architecture cores like **RISC-V** cores.
- Develop protection schemes with a hardware/software co-design approach.
- Ensure the **Control Flow and Execution Integrity (CFEI)** against powerful physical attacks.

Use Case : Pin Code Verification

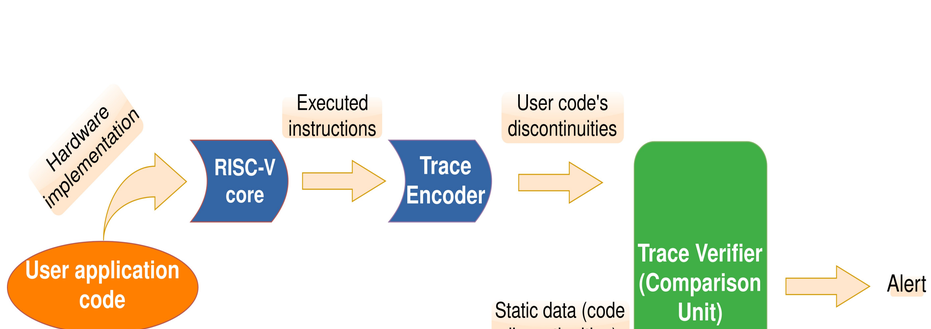
- Its function is to compare a user pin to the correct one for authentification.
- If the code pins do not match, access is not granted.
- Program behavior is altered when a fault is injected.

⚠ **Access could be granted even with the wrong pin.**



Exploited Solution

- Report the user code's discontinuities via a trace encoder.
- Generate static data from the application code's analysis.
- Verify the branch and jump instructions' correctness.
- Two threat models could be detected :
  - **A skip on branch or jump instructions.**
  - **Their substitution with other instructions.**



Perspectives

- Upgrade the solution to verify the **CFEI** of an application against powerful physical attacks :
  - Verify the correctness of all instructions at the first core's stage (Instruction Fetch Stage).
  - Check that all exeuted instructions within the core are unaltered (till the last core's stage).
- Design a protection to cover the **data integrity** in **RISC-V** pipeline stages.

References

[1] Yuce et al., Software Fault Resistance is Futile : Effective Single-Glitch Attacks, 2016

[2] Barenghi et al., Low-Cost Software Countermeasures Against Fault Attacks: Implementation and Performances Trade Offs, 2010

[3] Lashermes et al., Hardware-Assisted Program Execution Integrity: HAPEI. In: NordSec 2018: 23rd Nordic Conference on Secure IT Systems, 2018

[4] Werner et al., Sponge-Based Control-Flow Protection for IoT Devices, 2018

*This work is part of the ANR COFFI project (ANR-18-CE39-0003)

Contact : zgheib@emse.fr

Reconnaissance d'activités humaines dans un appartement connecté

Du capteur à l'activité

Parties prenantes

DELTA DORE
Smart is the new power

Doctorant

Damien Bouchabou

Encadrants

Sao Mai Nguyen*
Christophe Lohr*
Benoit Leduc**

Directeur de thèse

Ioannis Kanellos*

Partenaires

CHAIRE MOD Maintien @ Domicile

Lab-STICC

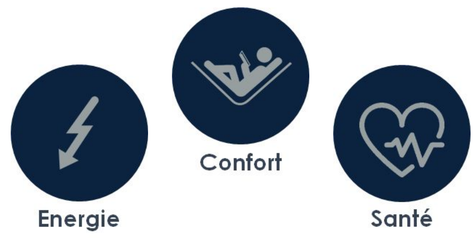
Mots clés :
Human Activity Recognition, Smart Home, Ambient Assisting Living, Language Model, ELMo, Contextualized Model, Sensors Embedding.

* IMT Atlantique (Brest)
** Delta Dore (Bonemain)

Contexte et Objectifs

Mieux vivre chez soi

- **Vieillissement de la population** Assister les personnes en perte de dépendance
- **Des services** Adapter et personnaliser intelligemment des services domotiques



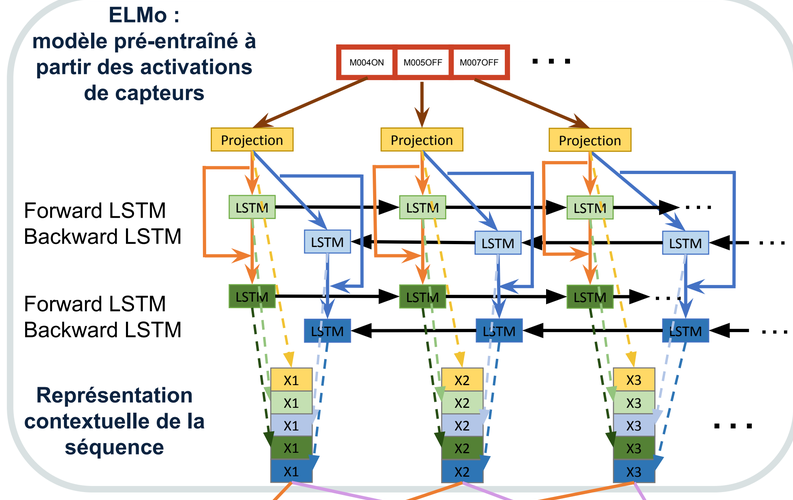
Méthode

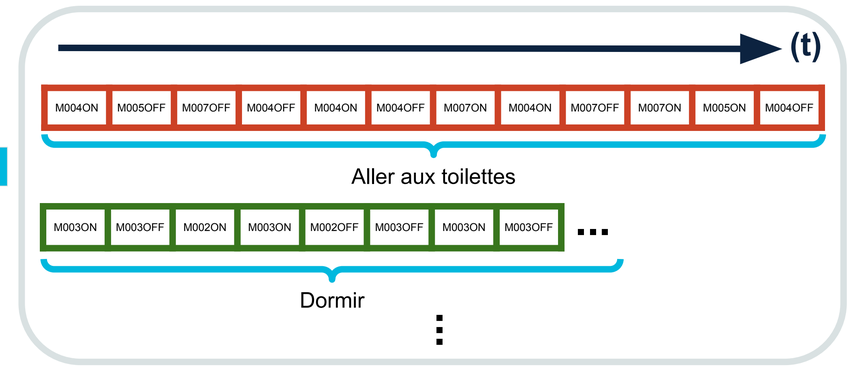
Des capteurs aux activités

Enregistrement des activations de capteurs

```
2010-11-04  05:40:51.303739  M004  ON   Bed_to_Toilet  begin
2010-11-04  05:40:52.342105  M005  OFF
2010-11-04  05:40:57.176409  M007  OFF
2010-11-04  05:40:57.941486  M004  OFF
2010-11-04  05:43:24.021475  M004  ON
2010-11-04  05:43:26.273181  M004  OFF
2010-11-04  05:43:26.345503  M007  ON
2010-11-04  05:43:26.793102  M004  ON
2010-11-04  05:43:27.195347  M007  OFF
2010-11-04  05:43:27.787437  M007  ON
2010-11-04  05:43:29.711796  M005  ON
2010-11-04  05:43:30.279021  M004  OFF  Bed_to_Toilet  end
2010-11-04  05:43:45.7324    M003  ON   Sleeping       begin
2010-11-04  05:43:52.044085  M003  OFF
2010-11-04  05:43:53.185335  M002  ON
2010-11-04  05:43:53.253809  M003  ON
2010-11-04  05:43:59.493281  M002  OFF
2010-11-04  05:44:04.048766  M003  OFF
2010-11-04  05:44:06.14204   M003  ON
2010-11-04  05:44:11.229146  M003  OFF
                    ⋮
```

Encodage de la séquence et représentation contextuelle





Encodage des activations de capteurs ("mots") et segmentation en activités ("phrases")

Classification de la séquence d'activations de capteurs depuis la représentation contextuelle de chaque activation

Résultats

Séquences d'activités encodées par le modèle ELMo sur le dataset Aruba de CASAS (P. Rashidi and D. Cook IEEE 2009)

	Aruba				Milan				Cairo			
	No Embedding	Liciotti	W2V	ELMo	No embedding	Liciotti	W2V	ELMo	No Embedding	Liciotti	W2V	ELMo
Accuracy	95.01	96.52	96.59	**96.76**	82.24	**90.54**	88.33	90.14	81.68	84.99	82.27	**89.12**
Precision	94.69	96.11	96.23	**96.43**	82.28	90.08	88.28	**90.2**	80.22	83.17	82.04	**88.41**
Recall	95.01	96.50	96.59	**96.69**	82.24	**90.45**	88.33	90.31	81.68	82.98	82.27	**87.59**
F1-score	94.74	96.22	96.32	**96.42**	81.97	90.02	87.98	**90.1**	80.49	82.18	81.14	**87.48**
Balance Accuracy	77.73	79.96	**81.06**	79.98	67.77	74.31	73.61	**78.25**	70.09	77.52	69.38	**87.00**
Weighted Precision	79.75	82.30	82.97	**88.64**	79.6	82.03	84.42	**87.56**	68.45	80.03	77.56	**86.83**
Weighted Recall	77.73	**80.71**	81.06	79.17	67.77	75.51	73.62	**78.75**	70.09	73.82	69.38	**84.78**
Weighted F1 score	77.92	81.21	81.43	**81.93**	71.81	77.74	76.59	**82.26**	68.47	74.84	70.95	**84.71**

Comparatif sur trois datasets de CASAS

- **Performances :** classifications améliorées.
- **Généralisation :** l'approche permet le transfert de connaissances d'une maison à une autre, avec une topologie différente.
- **Multi-résidents :** 1 ou 2 personnes avec, éventuellement, des animaux de compagnie.

Conclusion

- Importance d'une **représentation sémantique contextualisée** pour la reconaissance des AVQ
- **Modèle du langage** construit une représentation contextualisée robuste pour le transfert de connaissances

Contact : dbouchabou@deltadore.com / damien.bouchabou@imt-atlantique.fr

Octobre 2021 Colloque IMT Nord Europe : Réseau du futur

Software Defined Network approach for IoT technologies

Institut Mines-Télécom

Partners

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Université de Strasbourg

Author

Amaury Bruniaux

Supervisors

Julien Montavont
Nicolas Montavont
Thomas Noël
Georgios Papadopoulos

Key words

Internet of Things (IoT), Software Defined Network (SDN), Controller, IEEE Std 802.15.4, Quality of Service, Contiki OS

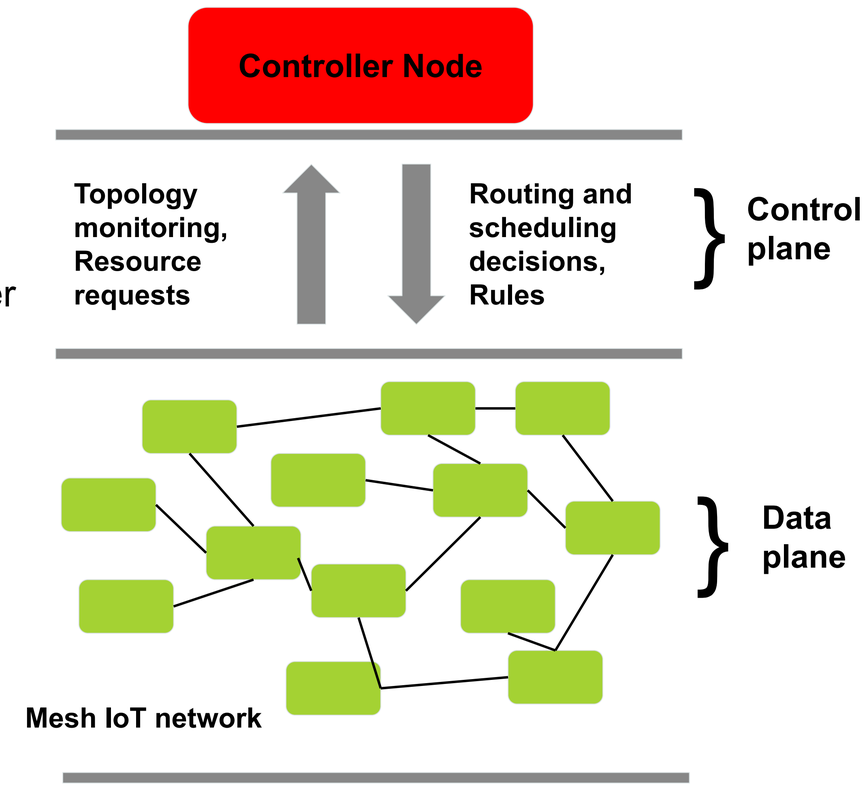
Relevant references

- Galluccio, L. et al. "SDN-WISE : Design, prototyping and experimentation of a stateful SDN solution for WIreless SEnsor networks". In proc. of the IEEE Conference on Computer Communications (INFOCOM), 2015.
- Margi, Cíntia B., Renan Cerqueira Afonso Alves, Gustavo A. Nunez Segura and Doriedson A. G. Oliveira. “Software-Defined Wireless Sensor Networks Approach: Southbound Protocol and Its Performance Evaluation.” *Open J. Internet Things* 4 (2018): 99-108.
- M. Baddeley, R. Nejabati, G. Oikonomou, M. Sooriyabandara and D. Simeonidou, "Evolving SDN for Low-Power IoT Networks," *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, 2018, pp. 71-79, doi: 10.1109/NETSOFT.2018.8460125.

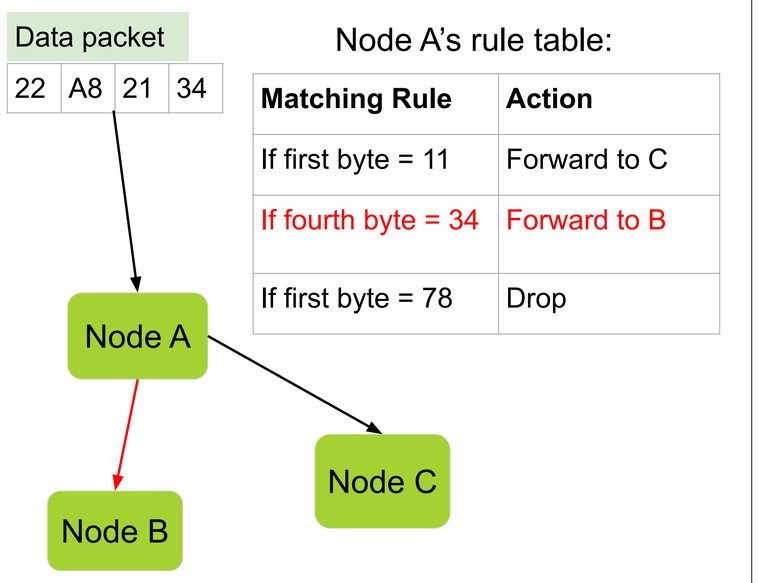
When SDN meets IoT

A new network behavior

- Routing, scheduling and resource allocationare no longer distributed, a centralized unit handles both.
- Nodes forward data packets by applying rules installed by the controller.
- Nodes provide to the controller a global view of the topology.
- Control plane and data plane are separated.
- Goals
  - to make the network programmable
  - to improve QoS



Structure of the Software-defined IoT network



Simplified example of the forwarding of a data packet

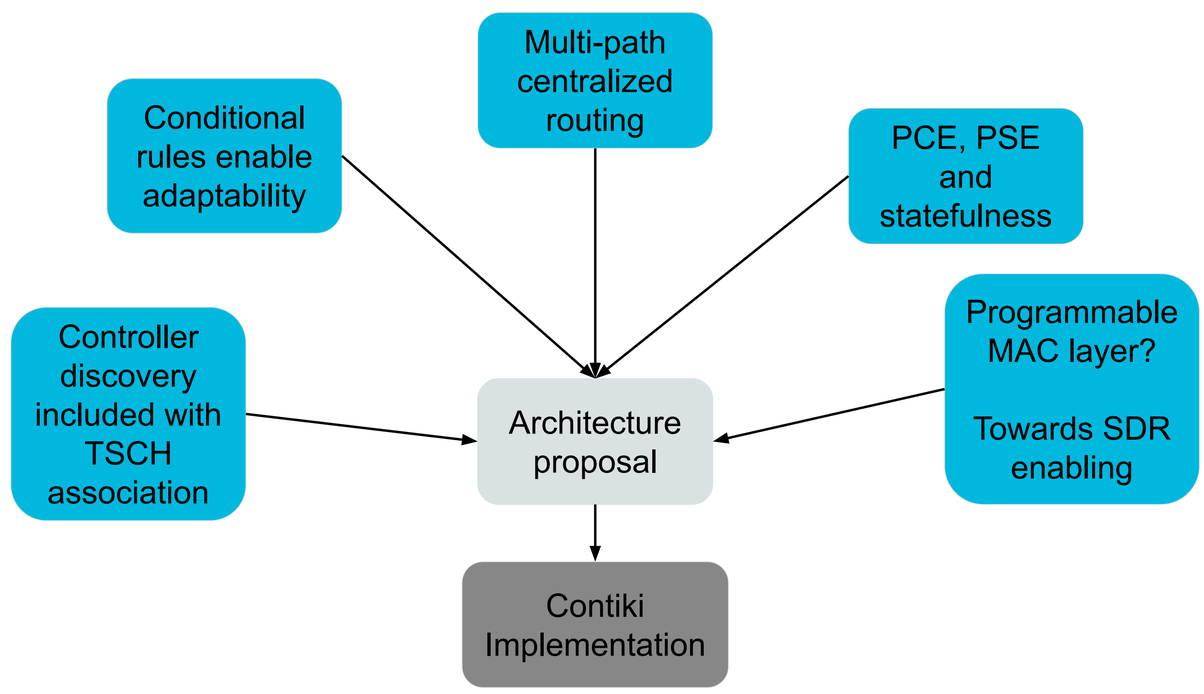
A new approach with new issues

Challenges for a software-defined IoT network

- Topology discovery: nodes need to be able to discover the controller and to give it their topology information in an efficient way.
- Lossy communication with the controller.
- Node memory size: only a limited quantity of rules can be stored.
- How to fully take advantage of a centralized unit?
- Short-term adaptability:
  - according to IETF RAW working group, the control plane and the data plane have different time scales
  - nodes forwarding packets need to adapt to varying radio conditions
  - this is not developped in current SDN for IoT approaches

My research on software-defined IoT networks

Research axis on SDN for IoT



Contact : amaury.bruniaux@imt-atlantique.fr

Disaster Protection in Inter-DataCenter Networks leveraging Cooperative Storage

Parties prenantes

Institut Mines-Télécom

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

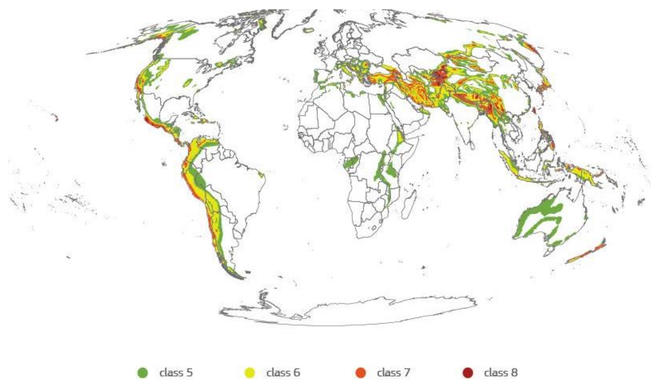
Auteurs

Yuanhao Liu,
Fen Zhou,
Zuqing Zhu,
Tao Shang,
Juan-Manuel Torres-Moreno

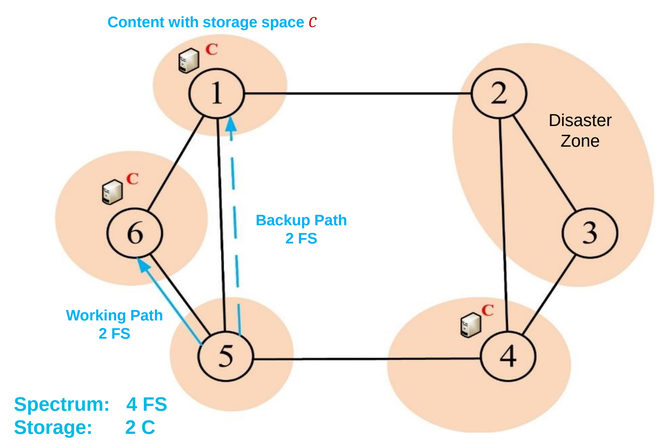
Partenaires

XIDIAN UNIVERSITY 1931

AVIGNON UNIVERSITÉ



Earthquake Hazards Map
Source : Atlas of the Human Planet 2017



Conventional DP

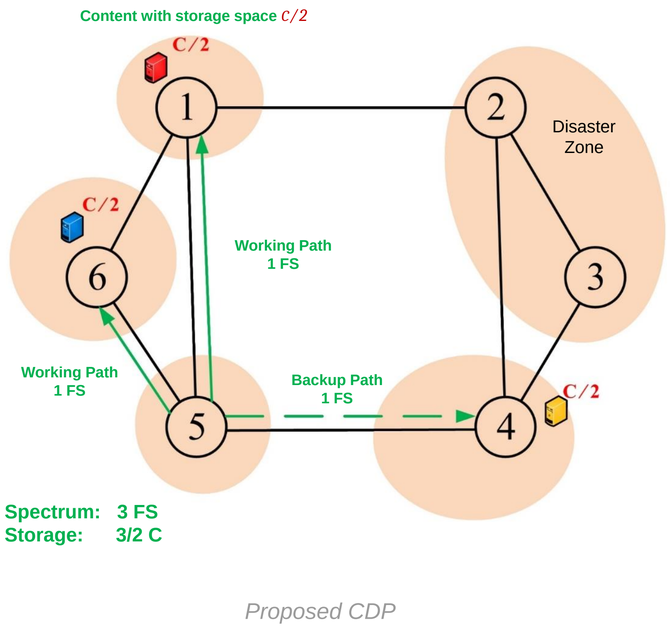
Background for today's optical networks

Conventional Disaster Protection in EO-DCNs

- **Dramatically Data Increasing**
  - 2,142 ZB Internet data in 2035
  - 597 hyperscale datacenters by the end of 2020
- **Elastic Optical Inter-DataCenter Networks** *(EO-DCNs)*
  - Big data storage and cloud services
  - Higher spectrum efficiency, huge capacity, lower latency, and higher availability
- **Disaster Failure** – An average loss of 402,542 dollars in the USA and 212,254 dollars in the UK in 2018.
- **Dedicated End-to-content Backup Path Protection** *(DP)* –
  - Mirrored storage
  - Dedicated end-to-content path protection

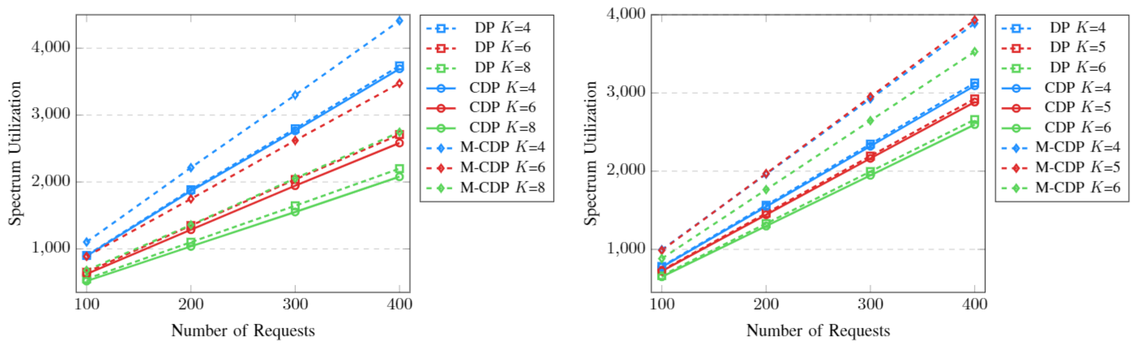
The proposed disaster protection: CDP

Coopertive Disaster Protection leveraging CSS



Proposed CDP

- **Cooperative Storage System** *(CSS)* - Maximum distance separable (MDS) codes; Encoded and divided into numerous different fragments; Stored spatially in multiple DCs; Negligible overhead.
- **Cooperative DP** *(CDP)*
  - **Content partition and placement (leveraging CSS)**
  - **Adaptive working path and one shared protection path**
  - **Modulation format adaption**
  - **Spectrum allocation**
- **Maximum-CDP** *(M-CDP)* – CDP with maximum working paths.
- **Integer linear program** *(optimal solution)* – Joint **spectrum usage** and **maximum frequency slot index** minimization.
- **Heuristic approach for large instances** *(HCDP)* – Greedy search first and global minimization after; Coloring algorithms.



(a) Spectrum Utilization versus K (in 8 available DC locations) (b) Spectrum Utilization versus K (in 6 available DC locations)

Spectrum Utilization versus number of available DC locations in US Backbone network using HCDP

QUALITY OF SOLUTION AND EXECUTION TIME IN JOINT ILP MODELS AND THE HCDP.

Method	Joint ILP model				HCDP				
Number of Requests	*Objective*	FS_{total}	*MOFI*	*Time(s)*	*Objective*	FS_{total}	*MOFI*	*Time(s)*	*Gap*
NSFNET Network, 3 DCs at available locations of nodes 2, 5, 6, 9, and 11									
10	**58**	52	6	34	**74**	69	5	4	**18.97%**
20	**117**	107	10	10800	**120**	113	7	17	**2.56%**
30	**190**	174	16	10800	**226**	212	14	32	**18.95%**
40	-	-	-	10800	**279**	266	17	57	-
COST239 Network, 3 DCs at available locations of nodes 1, 2, 7, 8, and 11									
10	**50**	45	5	10800	**51**	45	6	1	**2.00%**
20	**96**	85	10	10800	**88**	80	8	6	**-8.33%**
30	**149**	133	16	10800	**137**	124	13	13	**-8.05%**
40	-	-	-	10800	**199**	165	21	24	-

- No feasible ILP solution is obtained after 3 hours or exhausting all the memory.

Quality of Solution and Execution Time in Joint ILP models and the HCDP

Simulations and numerical results

Performance on spectrum utilization and storage space

- **Test beds** – The NSFNET, US Backbone, and COST239 networks.
- **CDP** with most reduction on **spectrum utilization**: up to 21.6% (compared to DP)
- **M-CDP** with most reduction on **content storage space**: up to 15% (compared to DP)
- **Trade-off** between the **spectrum utilization** and **content storage space**

Contact : fen.zhou@imt-nord-europe.fr

This work has been published on IEEE TNSM and GLOBECOM 2020.

Building the Web of Things with Autonomous Agents

and the Hypermedea Framework

Parties prenantes

Institut Mines-Télécom

MINES Saint-Étienne

Une école de l'IMT

Auteurs

Victor Charpenay

Partenaires

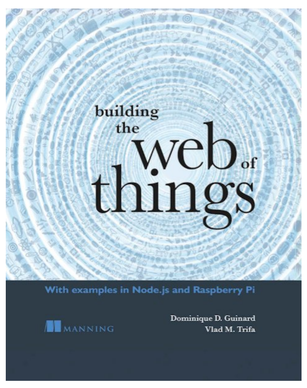
FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

SIEMENS

Universität St.Gallen

UNIVERSITÉ DE LYON

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE



Building the Web of Things
Source : webofthings.org

The Web of Things, after 10 years of experience

Standardized Web Interfaces to Connected Devices

- **2008** – "Putting Things to REST"[1]

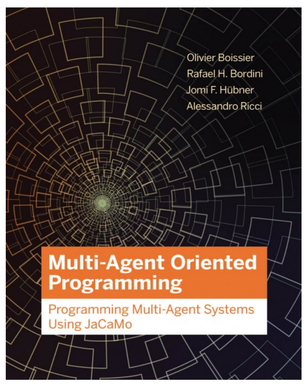
  first publication on the Web of Things (WoT)

- **2015** – "Building the Web of Things"[2]

  practical introduction to WoT with Node.js and Raspberry Pis

- **2019** – "Web of Things Thing Description"[3]

  standard published by the World Wide Web Consortium (W3C) for WoT

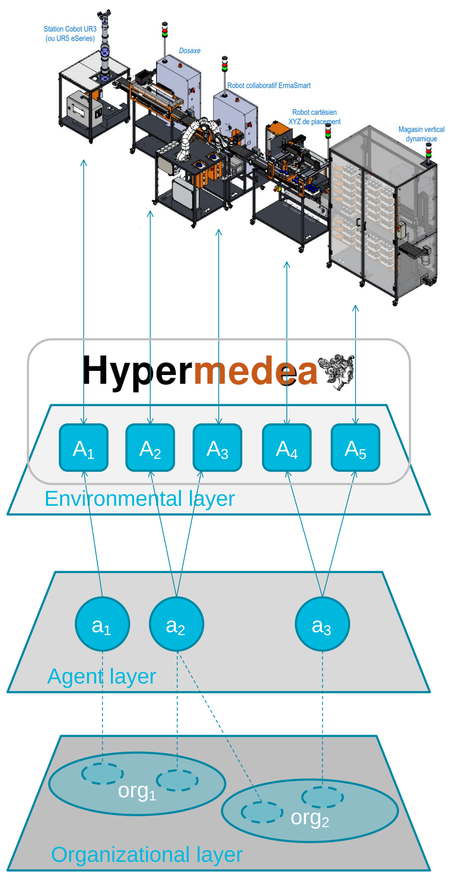


Multi-Agent Oriented Programming
Source : mitpress.mit.edu

An agent-oriented development approach for the Web of Things

Device Control by Autonomous Agents

- The architecture of the Web implies a clear cut between Things (Web servers) and Consumers (Web clients). WoT Consumers act on Things, which in turn observe or act on the physical world; a parallel can be drawn with control systems and systems under control, that is subordinate to the control system.
- In contrast to classical systems studied in control theory, a collection of Things may be heterogeneous and possibly dynamic. The control system must therefore be capable of abstraction and reactivity. In the sense of Russel and Norvig[4], intelligent agent architectures are designed to have such properties.
- The W3C acknowledges the importance of agents by describing network interfaces as collections of affordances (i.e. possible actions on Things). The concept of affordance is used e.g. in robotics for combining planning and acting[5].
- The paradigm of Multi-Agent Oriented Programming (MAOP) is suitable for designing (remote) control systems over Things. It allows organizations of agents to collectively act on a shared environment, through 3 layers of abstraction[6].



The 3 layers of MAOP applied on the IT'm factory, an Industry 4.0 experimentation platform at Mines Saint-Étienne

Technical design of Hypermedea

A Technical Framework

- The JaCaMo framework is a practical implementation of MAOP. It integrates:
  - Jason (agent programming language)
  - CArtAgO (framework based on artifacts as tools available to agents)
  - Moise (language for agent organizations and normative behaviors)
- Hypermedea is an extension of JaCaMo designed for WoT Consumers as intelligent agents. It includes:
  - a WoT Thing artifact *to turn actions on Things into requests to Web servers*
  - a Web crawler artifact *to discover WoT affordances*
  - an automated planning artifact *to build generic plans from available affordances*

https://github.com/Hypermedea/hypermedea

1. E. Wilde (2008), "Putting Things to REST," UC Berkeley iSchool report.
2. D. Guinard and V. Trifa (2015), "Building the Web of Things," Mannings.
3. S. Käbisch *et al*. (2019), "Web of Things (WoT) Thing Description," W3C recommendation. URL: https://www.w3.org/TR/wot-thing-description/.
4. S. Russell and P. Norvig (1995), "Artificial Intelligence: A Modern Approach," Pearson.
5. E. Sahin *et al.* (2007), "To Afford or not to Afford: A New Formalization of Affordances Toward Affordance-Based Robot Control," Adaptive Behavior.
6. O. Boissier *et al.* (2020), "Multi-Agent Oriented Programming: Programming Multi-Agent Systems Using JaCaMo," MIT Press.

Contact : victor.charpenay@emse.fr

Colloque de l'Institut Mines Télécom Lille

Octobre 2021

MRAM/CMOS Hybridization to Secure LWC Algorithms

Parties prenantes

MINES Saint-Étienne

Une école de l'IMT

Auteurs

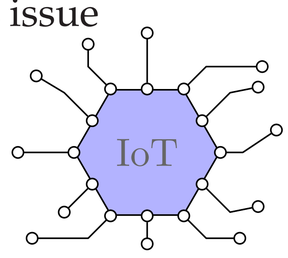
Nathan Roussel

Partenaires

PROJET FINANCÉ PAR L'ANR - PROJECT FUNDED BY THE ANR

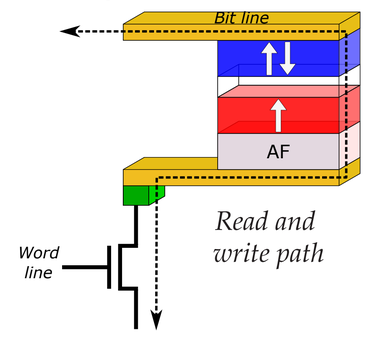
Context

- Microelectronics paved the way to Internet of Things (IoT)
- Low power, small area and security are IoT main constraints
- LightWeight Cryptography (LWC) algorithms are suitable to secure IoT applications
- Secure implementation of LWC to face physical attacks (side-channel or fault-based attacks)
- How to strengthen LWC algorithms with the lowest energy impact ?
- Hybridize Magnetic Random Access Memories (MRAM) and CMOS to adress this issue



MRAM Technology

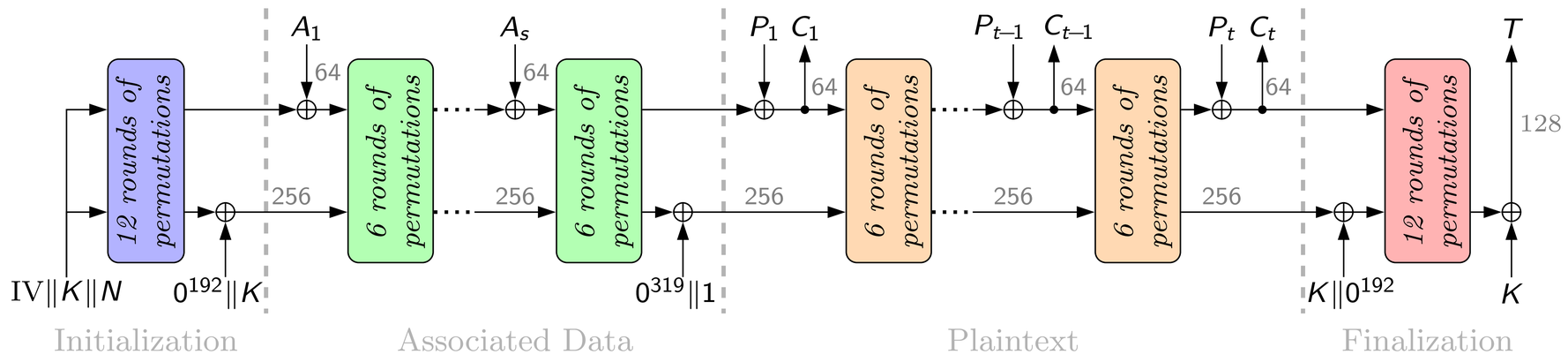
- MRAM cell : Magnetic Tunnel Junction (MTJ) + access transistors
- MTJ composed of an oxide barrier layer sandwiched between two ferromagnetic layers
- Why hybridize MRAM with CMOS ?
  - MRAM compatible with CMOS manufacturing process
  - Low power consumption due to non volatile logic
  - Restore previous state after a physical attack



MRAM cell

LWC Algorithms Use Cases

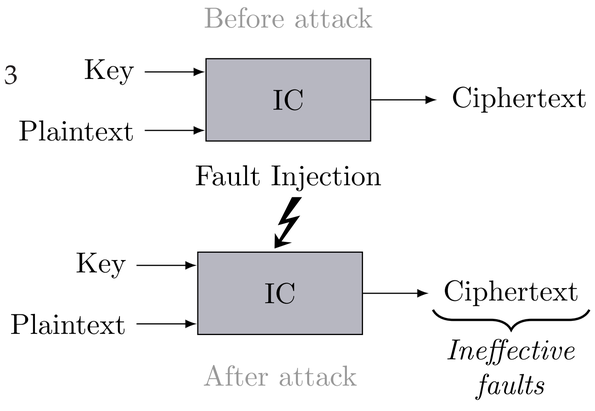
- Multiple implementations of these two LWC algorithms
- **PRESENT** : a Block Cipher [1]
- **ASCON** : an Autenticated Encryption with Associated Data (AEAD) [2]



ASCON-128

Security Characterization of Hybridized Circuits

- Are CMOS/MRAM circuits resilient to side-channel attacks ?
- Are CMOS/MRAM circuits vulnerable to fault injection attacks ?
- New threat has emerged: Statistical Ineffective Fault Attack (SIFA) [3]
  - Fault-based attack exploiting ineffective faults
  - Can circumvent dectection-based countermeasures
  - Could be a threat for CMOS/MRAM circuits ?



SIFA attack principle

1. A. Bogdanov and al., "PRESENT: An Ultra-Lightweight Block Cipher"
2. C. Dobraunig and al., "Ascon v1.2 : Submission to NIST"
3. C. Dobraunig and al., "SIFA: Exploiting Ineffective Fault Inductions on Symmetric Cryptography"

Acknowledgments

- This work is supported by the MISTRAL project (ANR-19-CE39-0010).
- MISTRAL is a collaborative research project founded by the French National Research Agency (ANR).

Contact : nathan.roussel@emse.fr

Nouvelles menaces sur les échanges d'informations dans l'industrie 4.0

Parties prenantes

Une école de l'IMT

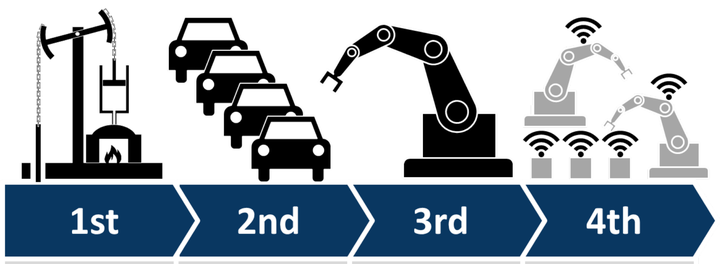
Une école de l'IMT

Auteurs

TSP:
Antoine Lavignotte
Pierre-Olivier Rocher
Nicolas Montes

Mines Saint-Etienne:
Philippe Jaillon
Nicolas Cointe

Partenaires



Contexte

Evolutions des usages industriels et mutations technologiques

► Nouveaux usages

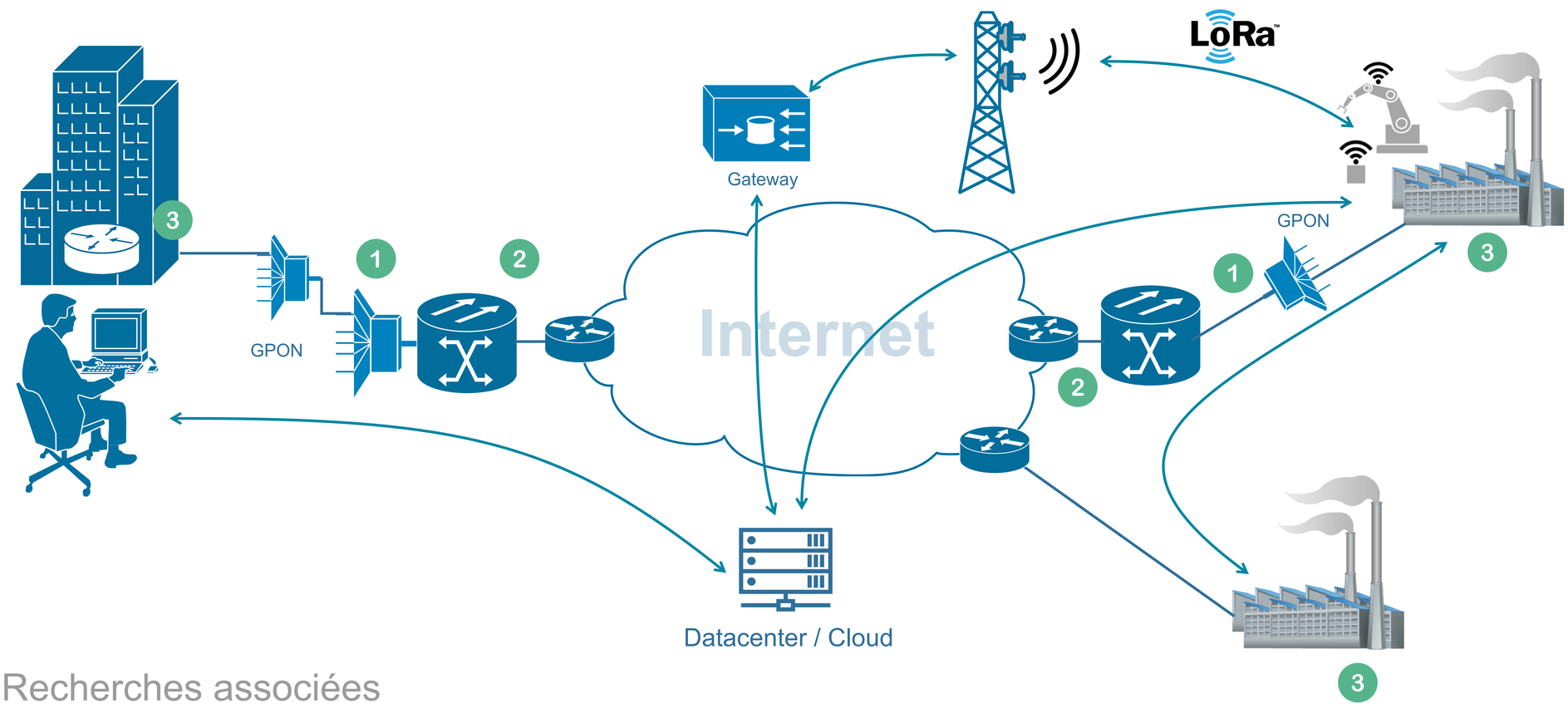
- Entreprise étendue
- Automates de commandes déportés
- Externalisation des données, edge computing

► Convergence des réseaux

- Utilisation d'Ethernet et des technologies IP sur l'ensemble de la chaine (ex: PROFIBUS -> PROFINET)
- Essor de l'IoT au sein des réseaux industriels -> Généralisation de l'IP
- Interconnexions des sites de production via les réseaux opérateurs radio et/ou optiques (5G, GPON, P2P)

Points de criticités

Schéma de l'infrastructure de contrôle d'un réseau industriel

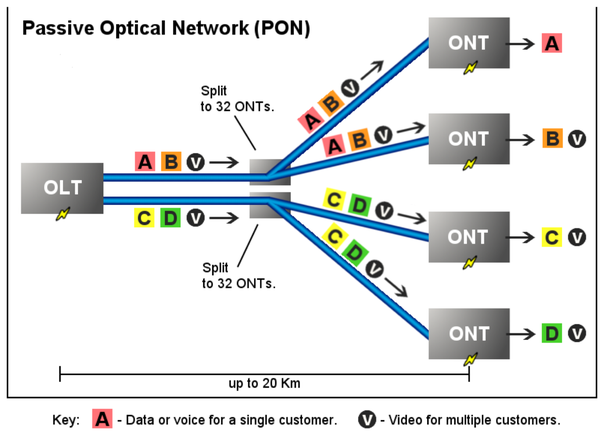


Recherches associées

Travaux en cours

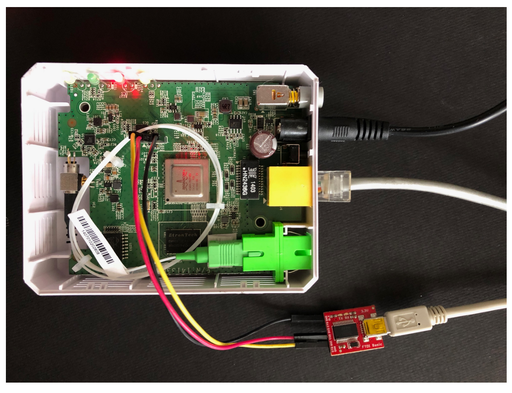
► Résistance des implémentations du protocole GPON (ITU-T G984)

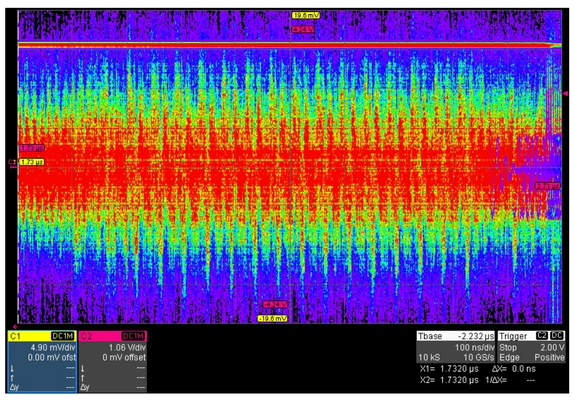
- Développement d'un framework de simulation du protocole et d'outils d'analyse protocolaire.



► Confidentialité et Intégrité des informations transitant sur les réseaux optiques partagés

- Analyse de la sécurité physique du réseau optique (1)
- Observation directe de la lumière présente sur la fibre
- Analyse des composants actifs de l'infrastructure (2)





- Redirection des flux vers un attaquant
- Résistance des ONT aux attaques par canaux cachés (3)
- Découverte des clés de chiffrement par apprentissage (CPA)

Projet financé dans le cadre de l'interCarnot M.I.N.E.S – TSN

Contact : antoine.lavignotte@telecom-sudparis.eu / philippe.jaillon@mines-stetienne.fr

Constrained Semantic Web of Things

Intelligent and decentralized Applications on constrained objects using Semantic Web technologies for Sustainable Agriculture and Smart Buildings

ANR-19-CE23-0012
Feb. 2020 - July 2024
Budget: 1.05M€
HR: 306 person*month
https://coswot.gitlab.io/

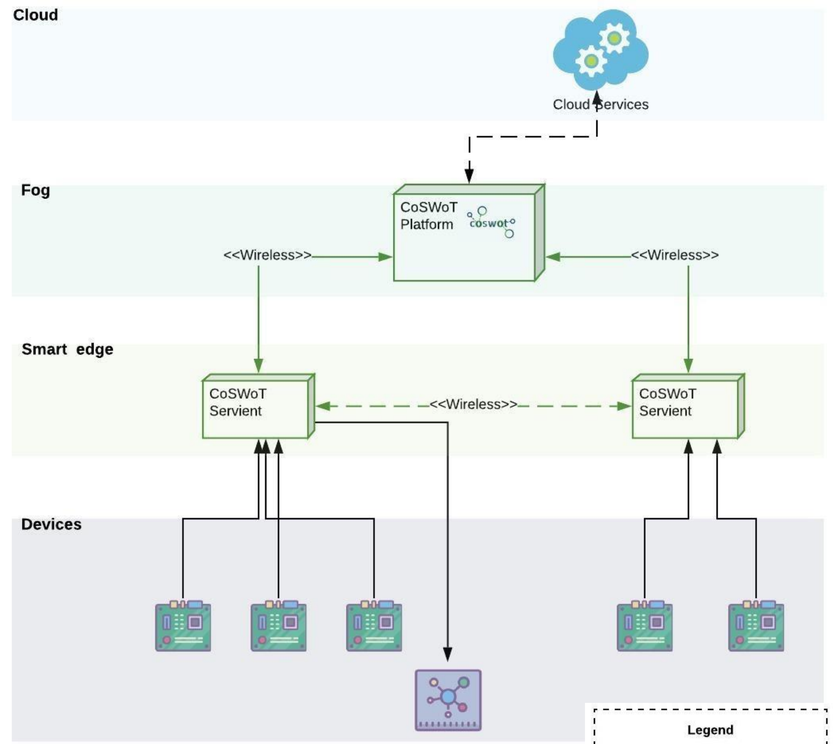
Partenaires

Membres

Ghislain Atemezing,
Fabien Badeig,
Alexandre Bento,
Jean-Pierre Chanet,
Victor Charpenay,
Yann Gripay,
Frédérique Laforest,
Maxime Lefrançois,
Gabriel Martins,
Lionel Médini,
Laure Moiroux,
Catherine Roussey,
Sylvie Servigne,
Kamal Singh,
Gil de Sousa,
Antoine Zimmermann

Problem

- **Internet of Things (IoT)** connects devices with various constraints and heterogeneous protocols and information models
- How to **break down manufacturers' silos?**
- How to **move the processing closer to the data?**



Goal

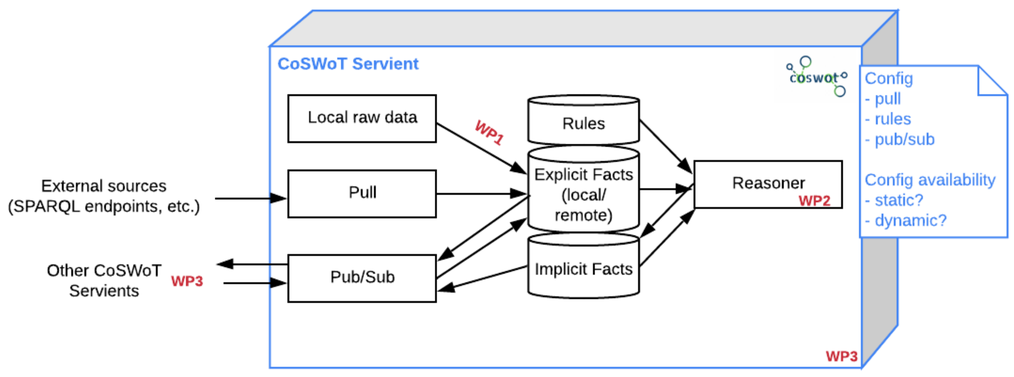
- The **Web of Things (WoT)** integrates Web standards with physical devices
- Build a **WoT platform to enable the development and execution of intelligent and decentralised smart applications** despite the heterogeneity of devices.

Semantic Web technologies for Semantic interoperability

- Bridging the plethora of protocols and information models
- Web-like and lightweight application protocols and data formats
- Ontology-based mediation approaches
- Contribution to standard ontologies for the IoT: W3C SOSA/SSN, ETSI SAREF, W3C Thing Description, ...

Distributed reasoning in constrained devices

- Distributed reasoning
- Processing data close to the source (Fog/Edge Computing)
- Stream processing and incremental reasoning
- WoT Servient: first class citizen of our architecture



Smart Building Use Case

- Management of the room ventilation (COVID)
- Management of the comfort (heating)
- Management of the energy consumption

Lyon Tech La Doua

Jumeau numérique du bâtiment Espace Fauriel de la Plateforme Territoire, MINES Saint-Étienne

Smart Agriculture Use Case

- Automatic irrigation based on weather station
- Field access management for robots
- Crop phenological stage detection

Experimental farm of the INRAE Agrotechnopole (Montoldre, Auvergne, France)

LoRa Weather station

Tractor followed by an autonomous robot (effibot)

Contact : maxime.lefrancois@emse.fr

Multi-Hop Network with Multiple Decision Centers under Expected-Rate Constraints

Institut Mines-Télécom

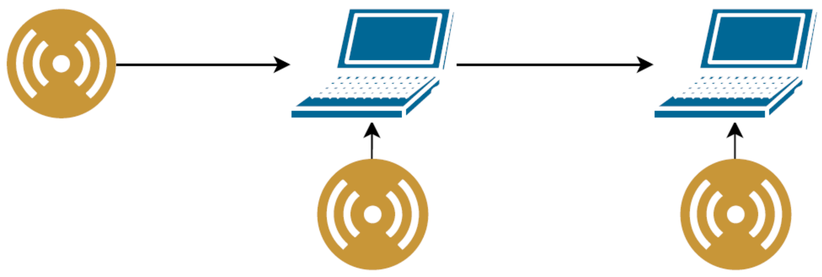
Parties prenantes

TELECOM Paris

IP PARIS

Auteurs

Mustapha Hamad
Michèle Wigger
Mireille Sarkiss



IoT Network with Three Sensors and Two Decision Centers

Motivation

- ► IoT Networks of Sensors with long lasting batteries
- ► Distributed monitoring and alert systems
- ► Short-range wireless communication
- ► Conditionally independent measurements
  - ⇨ Multi-hop Communication with Markov Chain

System Model and Description

► **Binary Hypothesis Testing against Independence**

- Normal Situation: Correlated Measurements

  $\mathcal{H} = 0 : X^n, Y^n, Z^n$ i.i.d. $\sim P_X \cdot P_{Y|X} \cdot P_{Z|Y}$

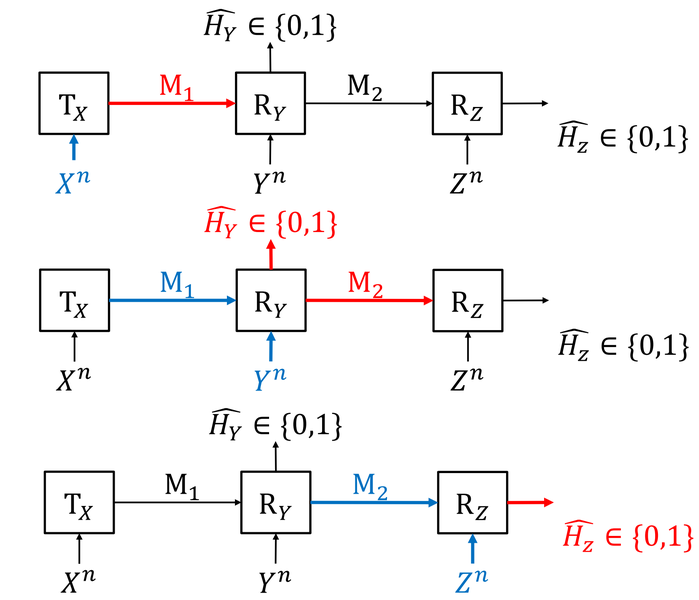
- Alert Situation: Independent Measurements

  $\mathcal{H} = 1 : X^n, Y^n, Z^n$ i.i.d. $\sim P_X \cdot P_Y \cdot P_Z$

- Goal: To guess correctly the joint distribution

- $\mathrm{M}_1 = \phi_1^{(n)}(X^n)$, $\widehat{H_Y} = g_1^{(n)}(\mathrm{M}_1, Y^n)$

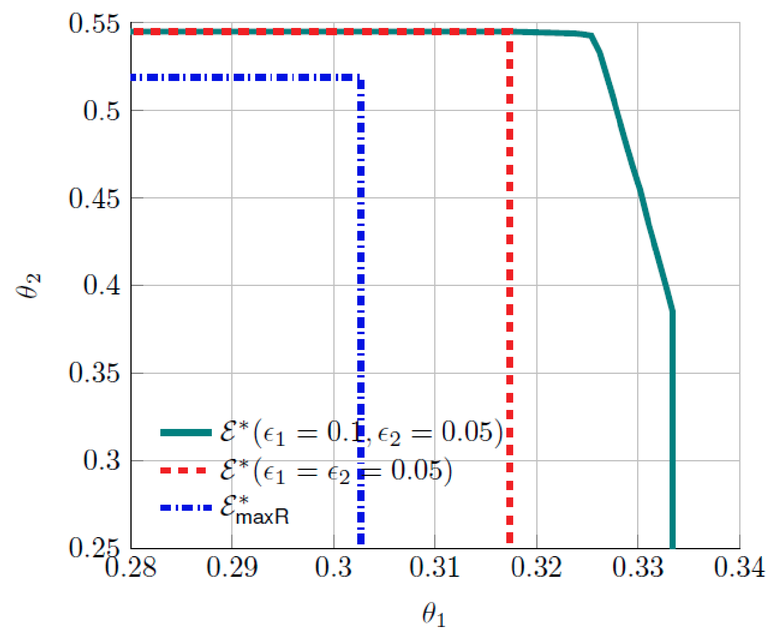
- $\mathrm{M}_2 = \phi_2^{(n)}(\mathrm{M}_1, Y^n)$, $\widehat{H_Z} = g_2^{(n)}(\mathrm{M}_2, Z^n)$



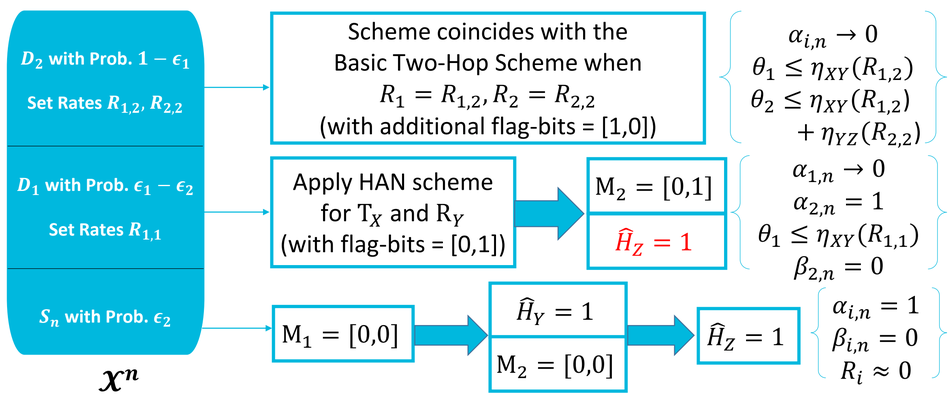
Binary Hypothesis Testing System Model Illustration

► **Types of Errors**

- False Alarm
  - $\alpha_{1,n} = \Pr[\widehat{H_Y} = 1 | \mathcal{H} = 0]$
  - $\alpha_{2,n} = \Pr[\widehat{H_Z} = 1 | \mathcal{H} = 0]$
- Missed Detection
  - $\beta_{1,n} = \Pr[\widehat{H_Y} = 0 | \mathcal{H} = 1]$
  - $\beta_{2,n} = \Pr[\widehat{H_Z} = 0 | \mathcal{H} = 1]$



Numerical Simulation Example of Exponents Regions with $\mathrm{R}_1 = R_2 = 0.5$, $\epsilon_1 = 0.1$, $\epsilon_2 = 0.05$



Simplified Coding Scheme under Expected Rate Constraints when $\epsilon_1 \ge \epsilon_2$

► **Exponents Region** $\mathcal{E}^*(R_1, R_2, \epsilon_1, \epsilon_2)$

- Closure of the set of all (ϵ_1, ϵ_2)-achievable (θ_1, θ_2) s.t. $\exists \{\phi_j^{(n)}, g_j^{(n)}\}$ satisfying $\forall j \in \{1,2\}$ the rate constraints,

$$\overline{\lim_{n\to\infty}} \alpha_{j,n} \le \epsilon_j \quad \text{and} \quad \underline{\lim_{n\to\infty}} \beta_{j,n} \approx 2^{-n\theta_j}$$

Main Results

► **Exact Characterization of the Exponents Region under Expected Rate Constraints** ($\mathbf{E}[\mathbf{len}(\mathrm{M}_j)] \le n R_j$)

- Maximum Rate Constraints ($\mathbf{len}(\mathrm{M}_j) \le n R_j$)

Theorem [Hamad, Wigger, Sarkiss'2021]

$\mathcal{E}^*(R_1, R_2, \epsilon_1, \epsilon_2)$ ***is the set of all*** (θ_1, θ_2) **pairs satisfying**

$$\theta_1 \le \min\{\eta_{XY}(R_{1,1}), \eta_{XY}(R_{1,2})\},$$

$$\theta_2 \le \min\{\eta_{XY}(R_{1,2}) + \eta_{YZ}(R_{2,2}),\ \eta_{XY}(R_{1,3}) + \eta_{YZ}(R_{2,3})\}$$

for some $\sigma \in [1 - \epsilon_1 - \epsilon_2, 1 - \max\{\epsilon_1, \epsilon_2\}]$ **and nonnegative rates** $R_{1,1}, R_{1,2}, R_{1,3}, R_{2,2}, R_{2,3}$ **satisfying**

$$R_1 \ge (1 - \epsilon_1 - \sigma) R_{1,1} + \sigma R_{1,2} + (1 - \epsilon_2 - \sigma) R_{1,3},$$

$$R_2 \ge \sigma R_{2,2} + (1 - \epsilon_2 - \sigma) R_{2,3}.$$

► **Tradeoff between the Exponents when** $\epsilon_1 \ne \epsilon_2$

► **Simplifying Exponents Region and Coding Schemes**

- $\epsilon_1 = \epsilon_2$: **One** exponent term at each decision center
- $\epsilon_1 \le \epsilon_2$: **Two** competing exponents at the Relay, and **One** exponent term at the Receiver

Expected Rate (Bandwidth) Constraint allows for significant boosts and there is a tradeoff between the missed detections at the decision centers

Contact : mustapha.hamad@telecom-paris.fr

Institut Mines-Télécom

A framework for joint admission control, resource allocation and pricing for network slicing in 5G

Parties prenantes

TELECOM SudParis

INSTITUT POLYTECHNIQUE DE PARIS

Auteurs

Walid Ben-Ameur
Lorela Cano
Tijani Chahed

Projet

MAESTRO_5G

ANR

Context

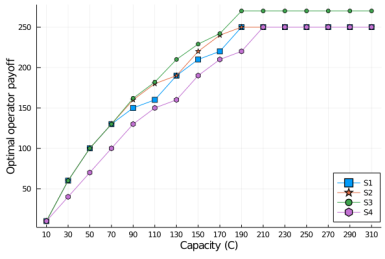
- **5G services:** enhanced Mobile BroadBand (eMBB), Ultra Reliable Low Latency Communications (URLLC) and massive Machine Type Communications (mMTC).
- **Slicing:** end-to-end virtual networks over a single (shared) physical network; each slice can be tailored to support a given type of service.
- **Our focus:** techno-economic interactions in the slice market between the operator (infrastructure provider) and the slice owners (tenants or service providers).
- **Our contribution:** new mathematical framework for the joint admission control, resource allocation and pricing for network slicing in 5G.
- **Related works:** the majority of the literature addresses admission control and resource allocation individually. Only few works optimize pricing alongside admission control and resource allocation: [1] maximizes total users utility, we maximize operator revenues, [2] assumes slices irrational entities performing bidding, we consider them rational, profit maximizing.

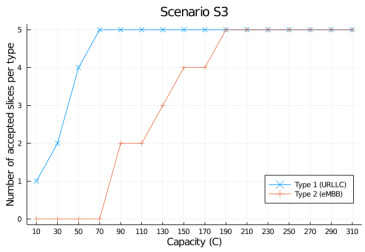
System and model

- **Setting:** one operator, with finite resources, and a set of slices of different types: URLLC and eMBB
- **Slice description:** stochastic demand, in intervals, and QoS requirement which is either deterministic, representative of URLLC, or statistical, representative of eMBB.
- **Interaction:** each slice announces maximum demand depending on its traffic and price announced by operator. In turn, the operator announces prices in each demand interval depending on slice maximum demand interval. Each actor tries to maximize its profit.
- **Model and formulation:** one-leader-multi-follower variant of the Stackelberg game with the operator being the leader and the slices being the followers, formulated as a Mixed Integer Linear Program (MILP).

Numerical results

- **Scenarios:** S1) single resource unit price and conservative capacity constraints for all slice types, S2) with statistical multiplexing for eMBB slices, S3) with slice-type specific resource unit prices, and S4) S2 with aggregate traffic description (vs. detailed traffic description for previous scenarios S1, S2 and S3).
- **Results:**
  - Statistical multiplexing allows for a higher profit for the operator and higher number of accepted slices.
  - By further allowing the resource unit price to be slice-type specific, it benefits both the operator (with a higher profit) and slices (increased number of accepted slices).
  - A detailed description of the slice traffic (as opposed to an aggregate one) can be advantageous for both the operator and slices (again in terms of operator payoff and number of accepted slices).





Publication and references

- Our work will appear in the proceedings of IEEE Globecom'2021, Madrid, December 2021.
- [1] B. Rouzbehani, V. Marbukh, and K. Sayrafian, "A joint admission control & resource management scheme for virtualized radio access networks," in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 1–6, 2019.
- [2] M. Vincenzi, E. Lopez-Aguilera, and E. Garcia-Villegas, "Maximizing infrastructure providers' revenue through network slicing in 5g," *IEEE Access*, vol. 7, pp. 128283–128297, 2019.

Contact : tijani.chahed@telecom-sudparis.eu

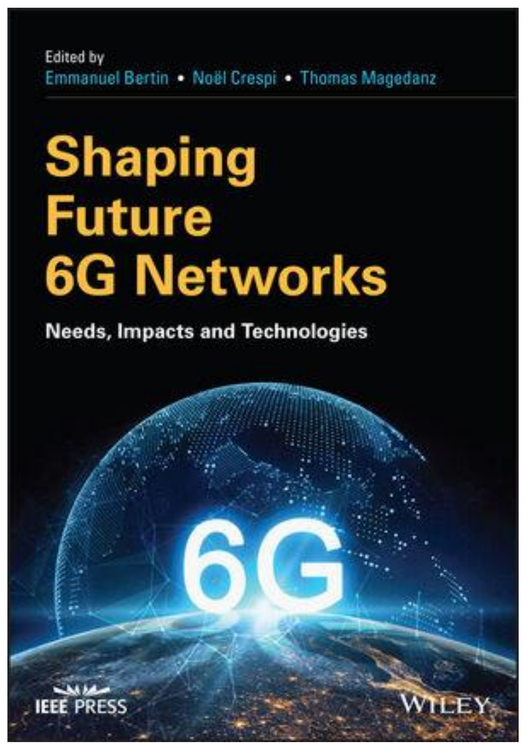
Octobre 2021 Colloque de l'Institut Mines Télécom Lille

Shaping Future 6G Networks:
Needs, Impacts and Technologies

Wiley IEEE book

An edited book published by Wiley (IEEE series)

- **Editors:** Emmanuel Bertin (Orange Labs, France), Noel Crespi (IMT/TSP, France), Thomas Magedanz (Fraunhofer FOKUS, Germany)



- **3 forewords by** Henning Schulzerinne (Columbia University, USA), Peter Stuckmann (European Commission), Akihiro Nakao (University of Tokyo, Japan)
- **Authors from** Ericsson Research (Sweden), University of Padova (Italy), Northeastern University (USA), Université Paris 2 Panthéon-Assas (France), Tsinghua University (China), Huawei Technologies Duesseldorf (Germany), Fraunhofer IIS (Germany), Fraunhofer HHI (Germany), CNRS & Paris-Saclay University (France), China Mobile Research Institute (China), Concordia University (Canada), NVIDIA (Germany), TU Munich (Germany), TU Dresden (Germany), University of Siegen (Germany), Redmill Communications (UK), Colombia University (USA), The University of Tokyo (Japan), Orange Labs (France), IMT (France), Frauhofer FOKUS (Germany)
- *Shaping Future 6G Networks: Needs, Impacts, and Technologies* is a holistic snapshot on the evolution of 5G technologies towards 6G. With contributions from international key players in industry and academia, the book presents the hype versus the realistic capabilities of 6G technologies, and delivers cutting-edge business and technological insights into the future wireless telecommunications landscape.

Shaping Future 6G Networks: Needs, Impacts and Technologies

Editors

Emmanuel Bertin, Orange

Noel Crespi, IMT/TSP

Thomas Magedanz, Fraunhofer FOKUS

Publication

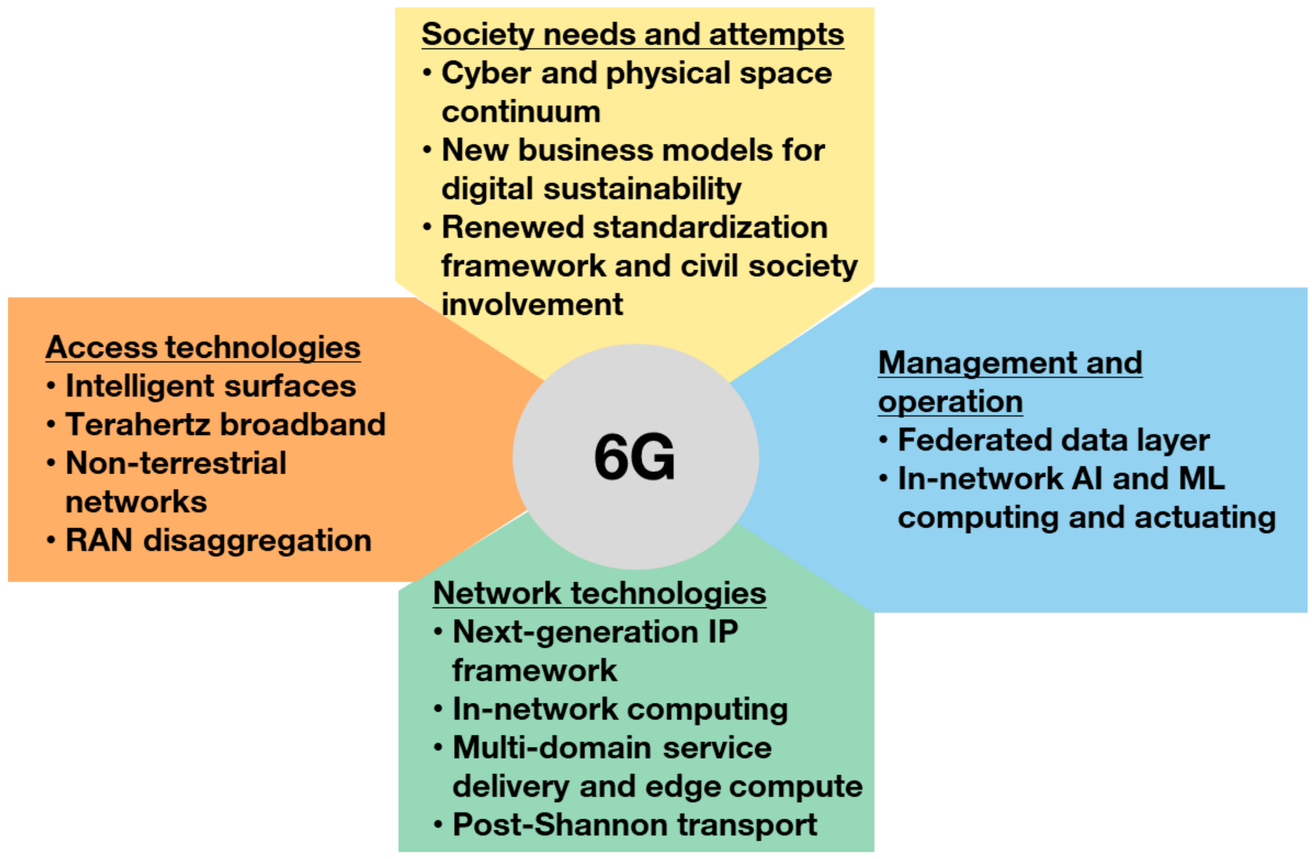
Nov 2021

ISBN: 978-1-119-76551-6

https://www.wiley.com/en-be/Shaping+Future+6G+Networks%3A+Needs%2C+Impacts+and+Technologies-p-9781119765516

You will learn about:

- Forthcoming demand for post 5G networks, including new requirements coming from small and large businesses, manufacturing, logistics, and automotive industry
- Societal implications of 6G, including digital sustainability, strategies for increasing energy efficiency, as well future open networking ecosystems
- Impacts of integrating non-terrestrial networks to build the 6G architecture
- Opportunities for emerging THz radio access technologies in future integrated communications, positioning, and sensing capabilities in 6G
- Design of highly modular and distributed 6G core networks driven by the ongoing RAN-Core integration and the benefits of AI/ML-based control and management
- Disruptive architectural considerations influenced by the Post-Shannon Theory



Contact : noel.crespi@mines-telecom.fr

Blockchain based trust management mechanism for Industry 4.0

Parties prenantes

TELECOM SudParis

IP PARIS

Auteurs

Asma Lahbib
Anis Laouiti

Introduction & Motivation

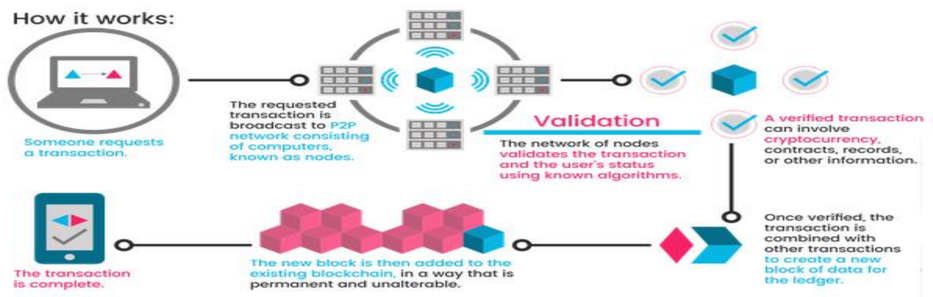
- **Trust** is often needed to produce reaction based on the real time evaluation of entities behaviors during interactions in addition to feedbacks and recommendations gathered from other entities.
- A **secure** and **distributed** based trust system is essential to guarantee trust information confidentiality, integrity and privacy during sharing and storage.
- A proof of existence, of ownership, of access and modification of this information is essential as it will be used later for decision making process.

➡ Keeping a living document trace about the flow of trust information as well as their access in order to guarantee an extra level of transparency, control and notarization during collaboration.

Blockchain based trust system

What is the Blockchain technology ?

• **A digital record** of transactions, that can be any movement of money, goods or secure data. These transactions are hold within blocks chained together through hashes contained within their headers.
• **Secure** It is designed to store information in a way that makes it virtually impossible to add, remove or change data contained within without being detected by participating peers.
• **Distributed** Blockchain is a distributed ledger hold by each participating peer and where verification of established transactions comes after the consensus of all participatings peers.



What blockchain means for Industry 4.0 ?

Structural features	Technology for sharing information….	...which allows for multiple parties...	...whose data is notarized, secure, verified thus trusted...	...forming a public record visible to all
What it means for smart factories	like production data, the origin of goods, entities trust records….	Including machines, Manufacturers, suppliers, customers...	Traceability of goods from suppliers to machines...	Allowed parties have access to data around a product, another entity...
What it means for smart health	Like patients records, prescription medicines, Medical devices trust records….	Including patients, doctors,medical centers, smart cities...	Keeping a complete patient's medical history...	Allowed parties have access to data around patients..

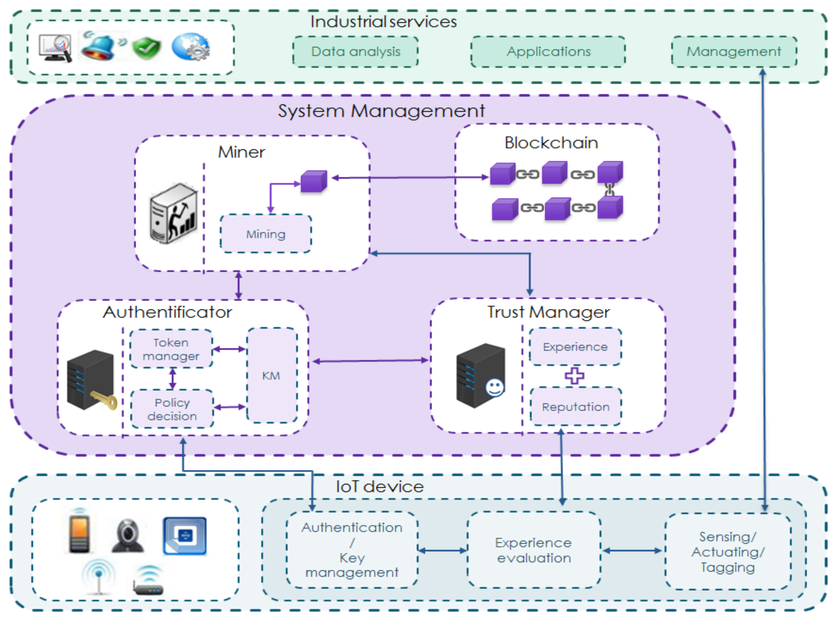
Proposed Approach

Propose a novel trust management system based on the blockchain technology

Defines and evaluate a trust score for each device within the manufacturing zone and securely store and share these scores through the blockchain network guaranteeing their transparency, integrity, authenticity, authorization, traceability and more importantly their notarization.

Implementation conducted using NS3 for the simulation of the IoT network and Multichain for the blockchain network.

Evaluation made regarding the resiliency against attacks, the response time and the percentage of successful transactions



Use cases applications

Extending the proposal to support fine-grained access control polices while allowing different parties to effectively interact and collaborate with each other in a trustful, secure and privacy preserved manner.

The framework relies on smart contracts designed and implemented to support:
- the registration of entities,
- the governability of the consensus mechanism,
- the definition of the access control model
- and the sharing of data while preserving their privacy.

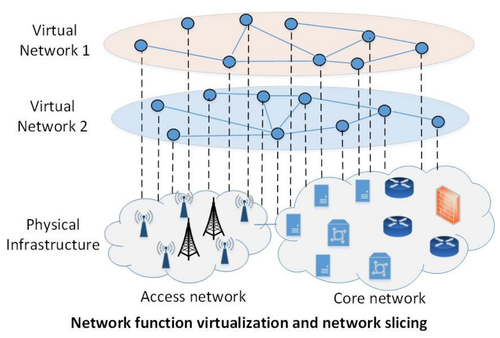
Contact : asma.lahbib@telecom-sudparis.eu
anis.laouiti@telecom-sudparis.eu

Improved Monte Carlo Tree Search For Virtual Network Embedding

Octobre 2021

Colloque de l'Institut Mines Télécom Paris

Network slicing concept



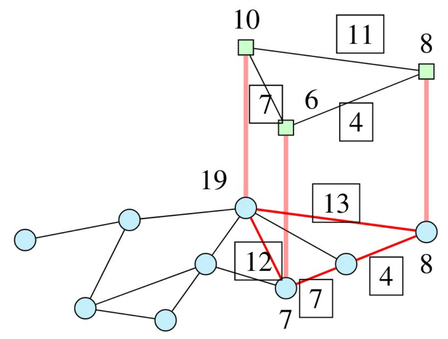
Sliced physical network hosting two slices

- **Support a plethora of usecases** *such as Virtual reality (high throughput, low delays), Autonomous Driving (ultra-low delays, ultra high reliability) or sensor networks (massive number of devices).*
- **One substrate network, multiple slices** *a single physical network hosts virtualized networks (slices) serving customized requests. A slice is scalable and flexible, enabling different usecases to use the same physical network.*
- **Placement problem** *How to place incoming slice demands on physical network in real time efficiently ?*

Virtual network embedding problem definition

- **Physical network** modeled as a graph $G(V, E)$
  - Each node $v_i \in V$ has CPU capacity CPU_i
  - Each edge $(v_i, v_j) \in E$ has bandwdith capacity $BW_{i,j}$
- **Slices** modeled as graphs $H^x(V^x, E^x)$ *(for x^{th} slice)*
  - Each node $v_i \in V^x$ has CPU demand CPU^d_i
  - Each edge $(v_i, v_j) \in E^x$ has bandwdith capacity $Bw^d_{i,j}$

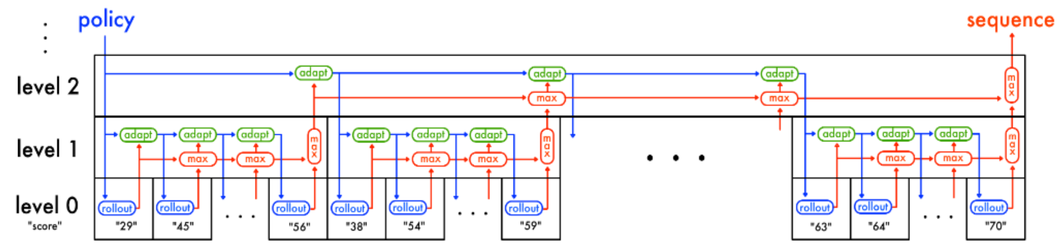
- **Online problem** slices arrive and leave the system over time dynamically. Demands are not known in advance.
- **Objective** **Maximize** total number of **accepted slices** while placing them one by one.



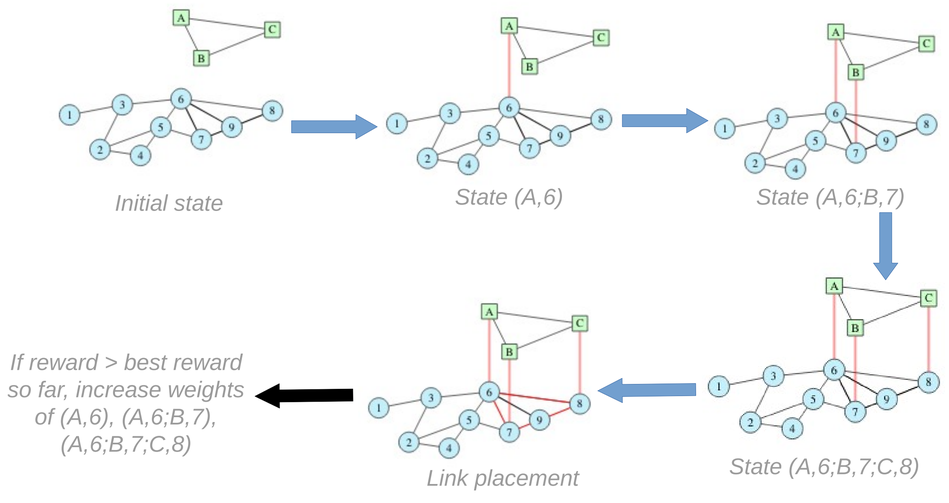
Modeled slice (green) placed on physical network (blue). BW capacities/demands are boxed, other numbers are CPU caps/demands

Used method : Nested rollout policy adaptation

- **Monte Carlo Algorithm** for a given slice H^x, learn to place its node by doing random simulations/rollouts of placements. At the end of each rollout place links using shortest path then calculate reward as $\frac{r_x}{c_x}$, $r_x = \sum_{\forall i,j \in V^x} BW^d_{i,j} + \sum_{\forall v_m \in V^x} CPU^d_m$ and $c_x = \sum_{\forall (i,j) \in E} \widetilde{BW}^x_{i,j} + \sum_{\forall v_i \in V} \widetilde{CPU}^x_i$ and $\widetilde{BW}^x_{i,j}$, $\widetilde{CPU}^x_{i,j}$ are resources used by slice H^x for edge (v_i, v_j) and node v_i
- **Maintain a policy** weighting each intermediate state. Intermediate states belonging to best solution found (*e.g.* solutions **maximizing reward**) are increased after each search (adaptation)
- **Bias rollouts** Using weights from policy (if state has high weight, increase probability of choosing it)
- **Recursive procedure** A level 0 search is a random simulation. A level l > 0 search return the best placement found by N level l -1 searches and adapts weights between each call
- **NRPA.D : Smart weight initialization** Initialize weights according to distance with previously placed nodes instead of 0



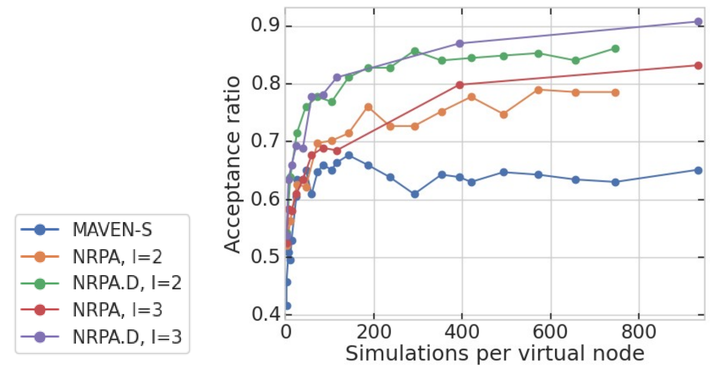
Typical level 2 NRPA execution. Figure from [3].



Example rollout (level 0 NRPA). Blue arrows correspond to random choices. Black arrow is a deterministic choice made by our shortest path algorithm

Numerical results

- **Acceptance improved** from 65 % to 83 % against Monte Carlo Tree Search based MAVEN-S[1]
- **NRPA.D further improves** acceptance to 91 %
- **Random scenario** with 238 slices of size 6 to 12 and 50 nodes physical network



[1] Virtual Network Embedding via Monte Carlo Tree Search, Haeri and Trajkovic, 2017

[2] Improved Monte Carlo Tree Search for Virtual Network Embedding, Elkael, Castel-Taleb, Jouaber, Araldo, Ait Aba, 2021

[3] Stabilized Nested Rollout policy adaptation, Cazenave, Sevestre, Toulemont, 2021

Parties prenantes

TELECOM SudParis

IP PARIS

DAVIDSON CONSULTING

Auteurs

Maxime Elkael
Hind Castel-Taleb
Badii Jouaber
Andréa Araldo
Massinissa Ait Aba

Partenaires

AGENCE NATIONALE DE LA RECHERCHE ANR

Contact : maxime_elkael@telecom-sudparis.eu

A two-stage algorithm for the Virtual Network Embedding problem

Institut Mines-Télécom

Parties prenantes

DAVIDSON CONSULTING

TELECOM SudParis

IP PARIS

Auteurs

Massinissa Ait Aba (1)
Maxime Elkael (2)
Hind Castel-Taleb (2)
Badii Jouaber (2)
Andréa Araldo (2)
David Olivier (1)
(1) Davidson Consulting
(2) Telecom SudParis, SAMOVAR, IP-Paris

Partenaires

AGENCE NATIONALE DE LA RECHERCHE ANR

In the 5G telecommunication network, it is expected to dynamically support new uses

Network Slicing:

► **Heterogeneous QoS requirements:** very high bandwidth, low latency, massive connectivity

► **Virtual Network Request (VNR)/slice:** the services are provided by virtual networks (network slices)

- A slice is a virtual network that is implemented on top of a physical network
- Each slice consists of different VNF chains that runs on physical and logical resources, which can be placed on different physical network domains (Core, RAN, Transport)

► **New challenge:** How to decide for an efficient allocation of Virtual Network Requests on the substrate network?

► **VNE problem:** network slicing can be modeled by the Virtual Network Embedding (VNE) problem

Network Slicing modeled by the Virtual Network Embedding (VNE) problem

Problem definition

► **Physical network:** represented by a graph $G(V, E)$

- Each node $v_j \in V$ is weighted by a maximum amount of resource
- Each edge $e_{j1,j2} \in E$ is weighted by a maximum bandwidth amount

► **Slice:** represented by a graph $H(V^s, E^s)$

- Each node $v_i \in V^s$ is weighted by a computational power demand
- Each edge $e_{i1,i2} \in E^s$is weighted by its bandwidth demand

► **Dynamic system:** slices arrive and leave over time

- Embed each slice request on the physical network respecting routing and resource constraints
- Embed each slice by optimizing the used resources
- Objective: maximize the overall acceptance ratio

Proposed method [1]: phase one

Reduce the number of possible path

► **Select K paths between each two nodes**

- Shortest paths: select the K shortest paths between each two nodes
- Widest paths: select the K paths that provide the highest bandwidth between each two nodes

Proposed method [1]: phase two

Use a mathematical model

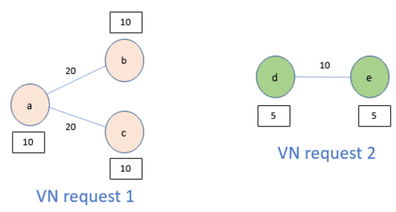
► **Solve a Mixed Integer Programming (MIP) model**

- Use the set of paths calculated in Phase I and a mathematical model to find a feasible solution
- To obtain the optimal solution using the same mathematical model, we have to consider all the possible paths between each two nodes

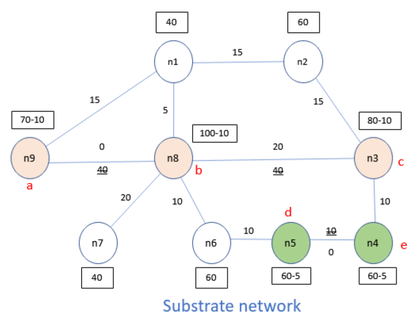
Two ways de embed two slices

Example

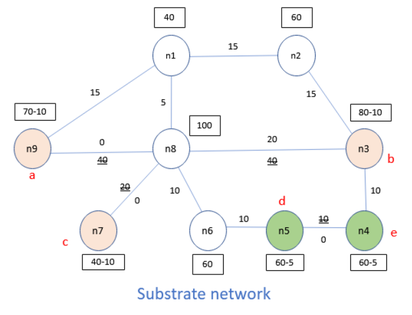
► Two virtual network (slice) requests



► First embedding solution



► Second embedding solution

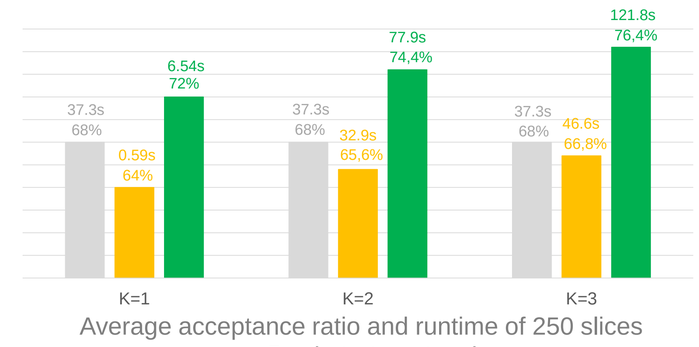


Simulations on randomly generated benchmarks

Numerical results

► Compare the performance of the proposed method using widest and shortest paths (with k ∈ {1,2,3}) to MaVEn-S algorithm [2]

- Random test instance, using random (uniform) resource demands and capacities
- 5 random substrate networks of different sizes (5 to 8 nodes)
- 50 slices for each substrate network (20 to 50 nodes)
- Randomly generated departure and arrival scenario of the slices



Average acceptance ratio and runtime of 250 slices on 5 substrate networks

► Perspectives:

- Manage the dynamic aspect of the VNE problem
- Extend the path limitation technique through meta-heuristics to handle larger instances
- Tests on real 5G network test beds is also planned in a near future

[1] A two-stage algorithm for the Virtual Network Embedding problem. M AIT ABA, M Elkael, B Jouaber, H Castel-Taleb, A Araldo, D Olivier, 2021 IEEE 46th Conference on Local Computer Networks (LCN), 395-398
[2] Soroush Haeri and Ljiljana Trajkovic. Virtual network embedding via montecarlo tree search.IEEE transactions on cybernetics, 48(2):510–521, 2017.

Contact : Massinissa.ait-aba@davidson.fr

Colloque de l'Institut Mines Télécom Paris
Octobre 2021

On The Deployability of Augmented Reality Using Embedded Edge Devices

A. B. Ameur, A. Araldo and F. Bronzino, "On the Deployability of Augmented Reality Using Embedded Edge Devices," *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 2021, pp. 1-6, doi: 10.1109/CCNC49032.2021.9369590.

Parties prenantes

TELECOM SudParis — INSTITUT POLYTECHNIQUE DE PARIS

Auteurs

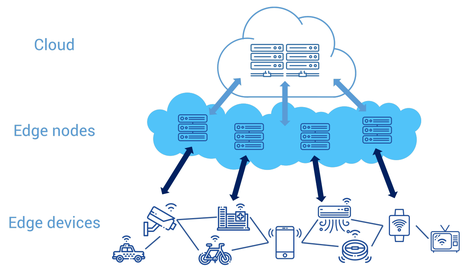
Ayoub Ben Ameur
Francesco Bronzino
Andrea Araldo

Partenaires

NOKIA Bell Labs

Context

Edge computing



Mobile Edge Computing Infrastructure
https://www.alibabacloud.com/fr/knowledge/what-is-edge-computing

- **Rapid growth of IoT**
- **Huge amount of data offloaded to the cloud**
- **Heavy computational burden**

Problem: Cloud *not suitable for realtime-based application such as AR.*

Solution: Bring the computational resources closer to the end user.

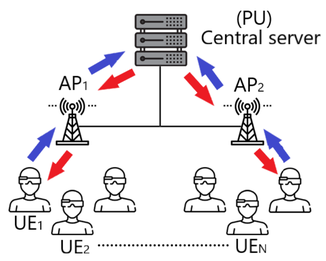
AR requirements	Latency (ms)	Example of application
Low Responisveness	500	Decoration applications
Mid Responisveness	100	Photography and Editing
High Responisveness	16	AR Maintenance

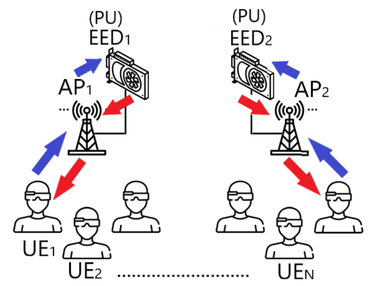
Google

NVIDIA

Research Question

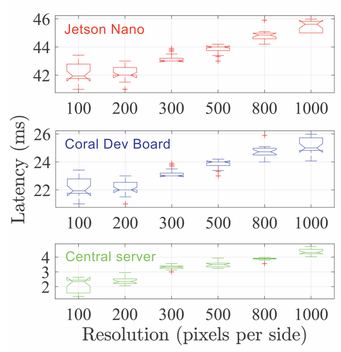
- **Can we deploy Augmented Reality using only Edge Embedded Devices?**





Methodology

Measurements on real devices

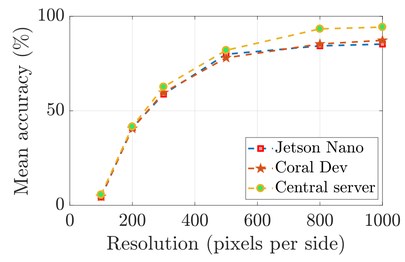


Inference Time vs. Frame Resolution

- **COCO Dataset**

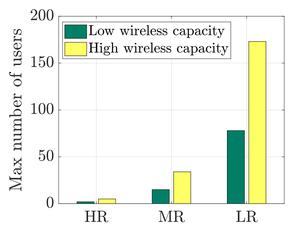
$$\mathcal{K} = \{100\times100, 200\times200, 300\times300, 600\times600, 1000\times1000\}$$

- **Single Shot Detector + MobileNet v2**
- Higher resolution, higher accuracy, same inference time.



Mean Accuracy vs. Frame Resolution

Theoretical Model

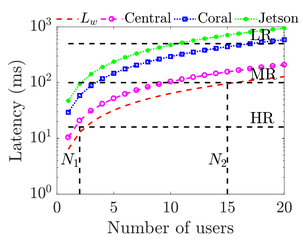


Max number of users supported by the wireless channel

$$L_n = L_n^w + L_n^p$$

- L_n^w is the wireless latency: time to send frame from **AP** to **PU**
- L_n^p is the processing latency: time to run the model on a frame

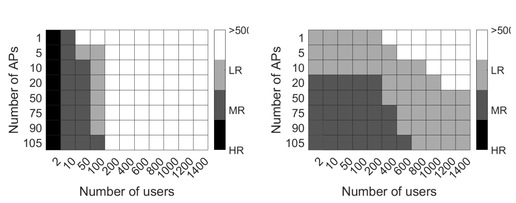
$$L_n^w = \frac{\sigma \cdot s_k^2 \cdot N}{R} \qquad L_n^p = \frac{c_k}{F} N$$



System latency vs. number of users

- σ is the number of bits/pixel
- s_k^2 is the frame resolution
- N is the number of users
- R is the data rate of the wireless link

Simulations



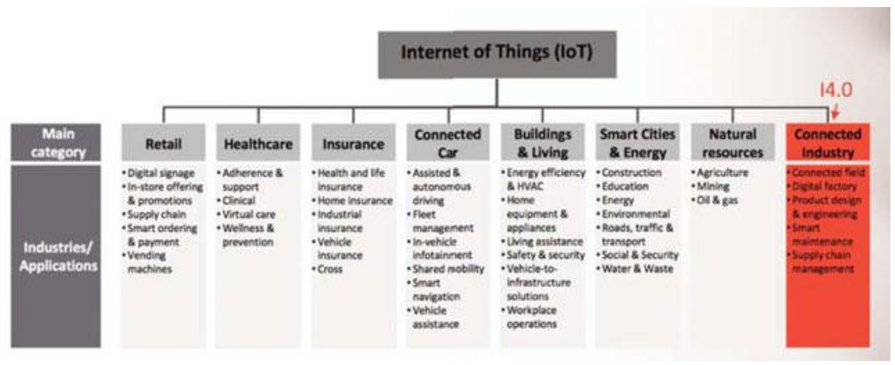
- **High responsiveness** requirements is still achievable only with Central server but without any remarkable improvement of the system performance.
- The distributed architecture keeps achieving the **Mid responsiveness** by reaching 600 users with such data-rate and the **Low responsiveness** requirements.

Contact : ayoub.ben_ameur@telecom-sudparis.eu

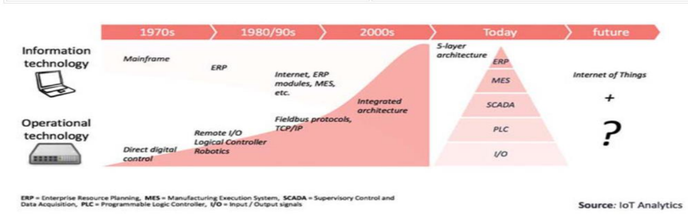
Institut Mines-Télécom

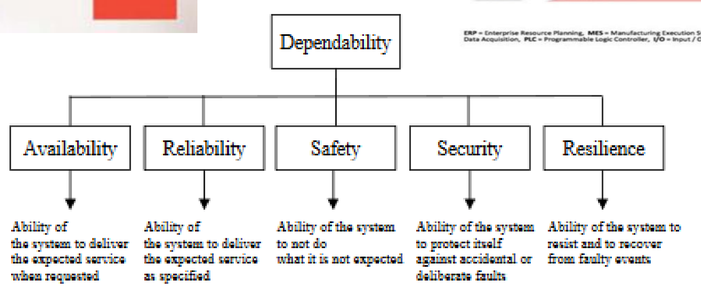
Edge Cloud, 5G, Deterministic Networking and Data Quality for Critical Applications

The case of Industrial automation/IIoT and real time decision making.



IT	OT
Frequent updates & upgrades running for years	Very few updates; usually installed and left
Interconnected with the internet	Isolated from the Internet
Focus: Privacy, Reliability, Security	Focus: Safety, Reliability, Resilience
Weakness: Resilience	Weakness: Security





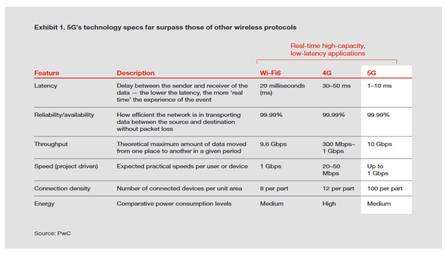


Exhibit 1. 5G's technology specs far surpass those of other wireless protocols

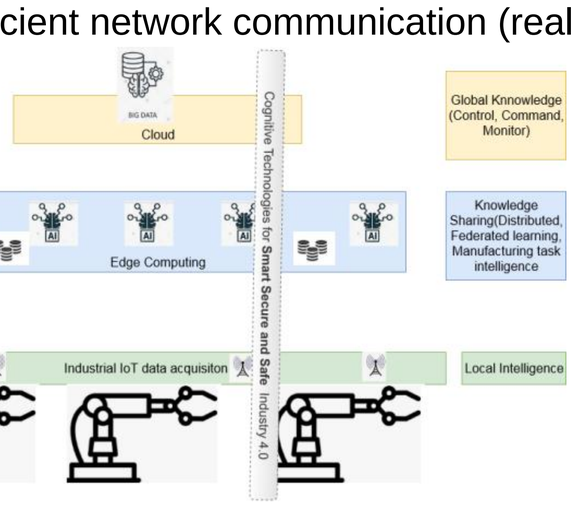
Feature	Description	Wi-Fi6 (Real-time high-capacity, low-latency applications)	4G (Real-time high-capacity, low-latency applications)	5G (Real-time high-capacity, low-latency applications)
Latency	Delay between the sender and receiver of the data — the lower the latency, the more "real time" the experience of the event	20 milliseconds (ms)	30–50 ms	1–10 ms
Reliability/availability	How efficient the network is in transporting data between the source and destination without packet loss	99.99%	99.99%	99.99%
Throughput	Theoretical maximum amount of data moved from one place to another in a given period	9.6 Gbps	300 Mbps–1 Gbps	10 Gbps
Speed (project driven)	Expected practical speeds per user or device	1 Gbps	20–50 Mbps	Up to 1 Gbps
Connection density	Number of connected devices per unit area	8 per part	12 per part	100 per part
Energy	Comparative power consumption levels	Medium	High	Medium

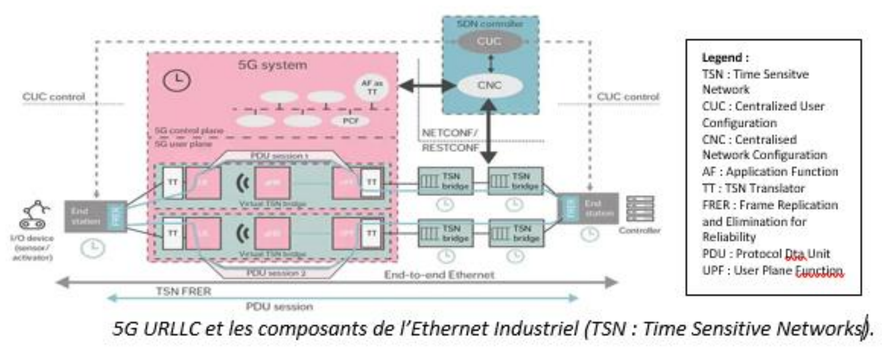
Source: PwC

Edge Cloud and deterministic networking for Industrial automation usecase

Three layer architecture for Industrial IoT

- **Industrial automation Intelligence functions** –Planning of the placement of these function in the three layer architecture.
- **Industrial automation function quality of service management**– Combining the characteristics of edge cloud for efficient industrial data storage and processing and 5G/6G networks for efficient network communication (real time, high bandwidth, …)



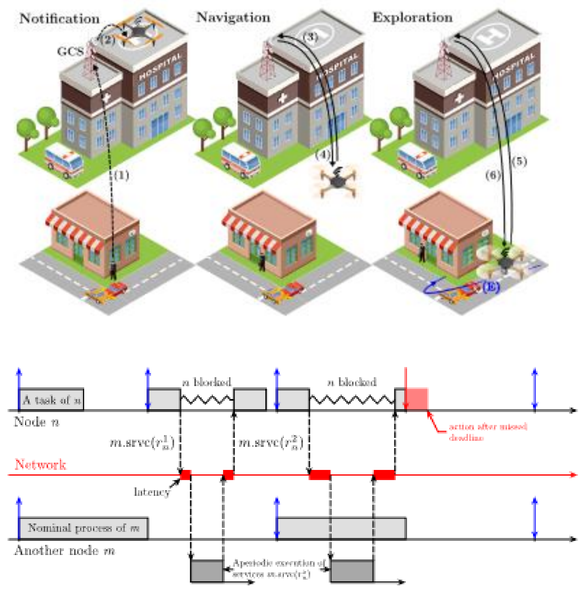


5G URLLC et les composants de l'Ethernet Industriel (TSN : Time Sensitive Networks).

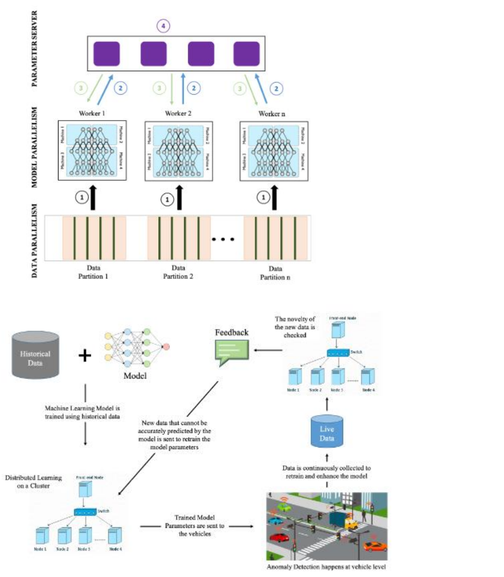
Edge Cloud and real time communication for Critical applications

Constrained decision making: Drone, autonomous vehicle usecases

- Hierarchical vs Distributed edge Cloud architecture design
- Time sensitiveness requirement analysis (Critical decision making for navigation, IoT data acquisition and anomaly detection, …)
- Edge Cloud architecture combination with the network architecture to maximise the quality of service required by the critical application.
- Edge Cloud and network architecture optimisation for AI algorithms quality of service garrantee.



Critical Drone navigation Process usecase.



Autonomous Vehicle critical navigation process assisted with AI

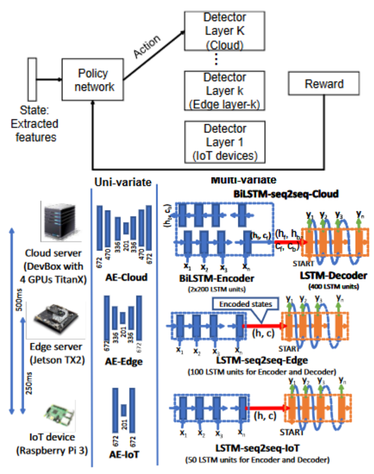


Fig. 1: Hierarchical Edge Computing System testbed (first column), and architecture of autoencoder models for univariate dataset (second column), and architecture of LSTM-seq2seq models for multivariate dataset (third column).

Hierachical Edge Cloud Demonstrator for IoT/Industrial IoT data anomaly detection

Contact : hakima.chaouchi@telecom-sudparis.eu

Parties prenantes

TELECOM SudParis

IP PARIS

Auteurs

Hakima Chaouchi
Professeur
Telecom Sud Paris
Institut Mines Telecom
Institut Polytechnique de Paris

Partenaires

ntw. CodEUrope cea

Publications

[1] Yannick Fourastier, Hakima Chaouchi et al "AI-assisted Distributed Applications at Edge for Industrial Field Autonomous Systems", Sensor sand Transuders Journal 2021

[2] Yannick Fourastier, Hakima Chaouchi, al "Industrial field autonomous systems: AI-assisted distributed applications at Edge" International Conference on Advances in Signal Processing and Artificial Intelligence, 2021

[3] Mao V. Ngo, Hakima Chaouchi et al, "Contextual-Bandit Anomaly Detection for IoT Data in Distributed Hierarchical Edge Computing"
IEEE ICDS 2020

[4] Naman Negi, Ons Jelassi, Hakima Chaouchi, "Distributed online Data Anomaly Detection for connected vehicles", IEEE ICAIIC 2020

[5] Sebti Mouelhi, al et Hakima Chaouchi, "Predictive Formal Analysis of Resilience in Cyber-Physical Systems"
IEEE Access Journal 2019

[6] Emine Laarouchi, al, Hakima Chaouchi "Safety and degraded mode in civilian applications of unmanned aerial systems"
IEEE DASC 2018

[7] Hakima Chaouchi et al
« Technical Specification D2.1 - Data processing and management framework for IoT and smart cities and communities", ITU Technical Specification Series

[8] UF1 : Les objets connectés et la 5G- Quelles promesses?
Les entretiens de Toulouse 2021
Hakima Chaouchi

Novembre 2015 Lille 14 Octobre 2021. Colloque de l'Institut Mines Télécom. Thématique Phare Internet des objets et réseaux du futur.

A Scalable GraphQL Northbound API for Intent-based SDN Applications

Auteurs

Fetia Bannour
Stefania Dumbrava
Damien Lu

Partenaires

Contact

fetia.bannour@ensiie.fr

stefania.dumbrava@ensiie.fr

damien.lu@ensiie.fr

Introduction & Context

- ***SDN*** : an emergent network architecture paradigm, decoupling the control logic from the data plane (hardware).
- Increased interest in ***suitable abstractions*** for network management & application development.

→ Southbound API : the first, highly popular standard → the OpenFlow communication protocol.
→ Northbound (NB) API : lack of a unifying formalism → use of ad-hoc controller-based APIs or REST APIs.

Challenges & Motivation

- Difficult to design a proper Northbound API for SDN applications [1].
- Limited scalability & verbosity of commonly used REST APIs.
- Leverage the expressivity of the novel GraphQL query language [3].
- Develop a web-scalable NB interface that easily integrates with graph databases.

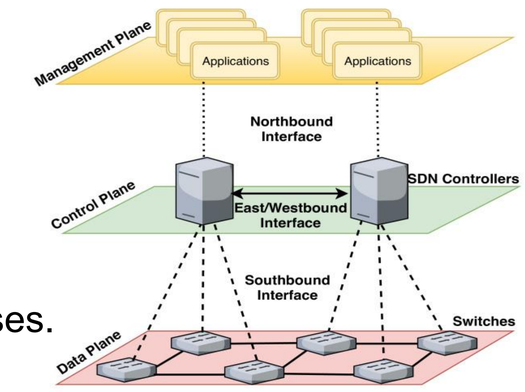
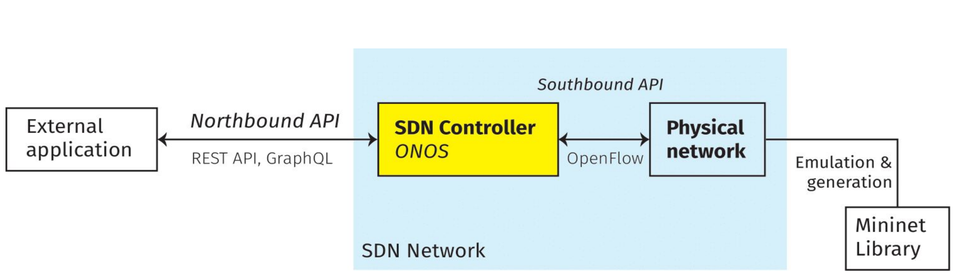
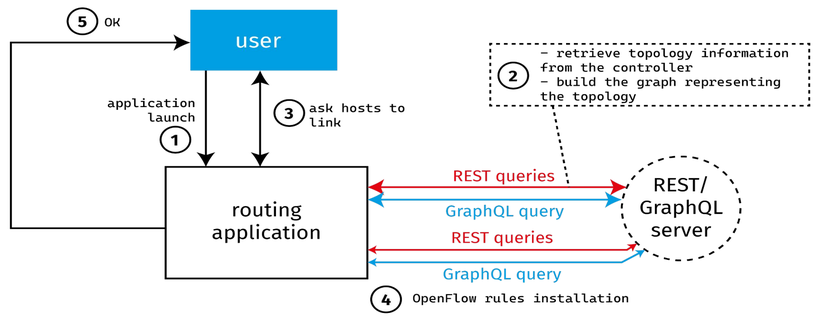


Fig: Schematic view of an SDN topology [2]

Methodology & Implementation

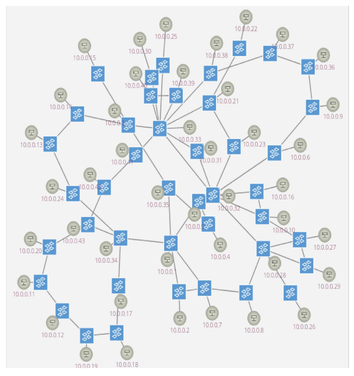
- Develop a GraphQL API for the ONOS SDN controller [4] (instead of its native REST API).
- Design an intent-based routing application [5] that uses GraphQL for its Northbound API.
- Render the approach dynamic: propagate network changes detected by the controller to the application.





Experimental Analysis & Results

- Generate synthetic & real-world emulated network topologies using the ONOS controller.
- Compare the performance of GraphQL & REST for our routing application.
- Record the time & number of queries needed to install & express intents for both APIs.



Renater real network topology

Size of the topology:
43 hosts, 112 links, 43 switchs

Time needed to generate intent rules with GraphQL compared to REST : **-28,00%**

Number of REST queries : 48440

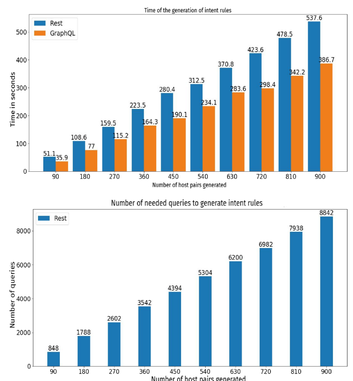
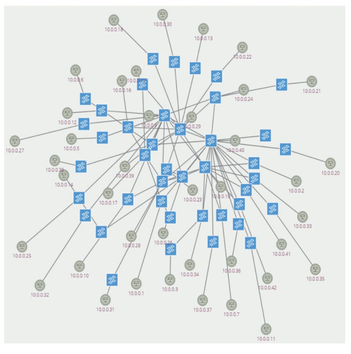


Fig: Renater topology in ONOS



China Telecom real network topology

Size of the topology:
40 hosts, 132 links, 42 switchs

Time needed to generate intent rules with GraphQL compared to REST : **-27,15%**

Number of REST queries : 33392

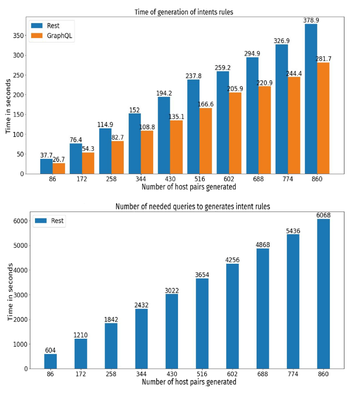


Fig: China Telecom topology in ONOS

Conclusion & Perspectives

- Our GraphQL API outperforms the REST API:
  - ***more efficient*** (approx. 27% speed-up) &
  - ***less verbose*** (1 query vs. up to 9K REST requests).
- The results show the feasibility of our approach.
- Interesting future research directions for developing web-scalable network applications that use graph query languages & graph database techniques [6].
- Ongoing integration of our GraphQL API with the state-of-the-art Neo4j graph database.
- Exploration of its usage for enhancing interoperability between different controller technologies.

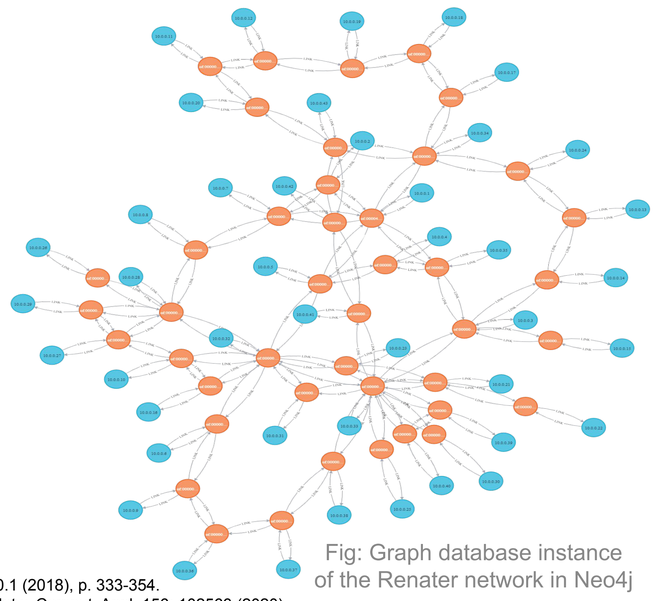


Fig: Graph database instance of the Renater network in Neo4j

References

[1] Fetia Bannour, Sami Souihi, Abdelhamid Mellouk. *Distributed SDN control : Survey, taxonomy, and challenges*. In: IEEE Communications Surveys & Tutorials 20.1 (2018), p. 333-354.
[2] Zohaib Latif, Kashif Sharif, Fan Li, Md. Monjurul Karim, Sujit Biswas, Yu Wang: *A comprehensive survey of interface protocols for software defined networks*. J. Netw. Comput. Appl. 156: 102563 (2020)
[3] GraphQL specification: https://spec.graphql.org
[3] ONOS documentation: https://wiki.onosproject.org/
[4] Taufik Irfan, Rifqy Hakimi, Aris Riddianto, Eueung Mulyana. ONOS Intent Path Forwarding using Dijkstra Algorithm. In Proc. ICEEI, p. 549-554, 2019.
[5] Sherif Sakr, Angela Bonifati, Hannes Voigt, Alexandru Iosup, Stefania Dumbrava et al. *The Future Is Big Graphs: A Community View on Graph Processing Systems*, Communications of the ACM, September 2021, Vol. 64 No. 9, p. 62-71.
[6] Neo4j documentation: https://neo4j.com/.

November 2021 Colloque de l'Institut Mines Télécom Lille

Réseaux denses et à très faible consommation

Gestion dynamique d'un champ de capteurs pour allonger le temps de surveillance

Partie prenante

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Auteur

Gwen MAUDET

Encadrants

Mireille BATTON – HUBERT

Patrick MAILLE

Laurent TOUTAIN

Partenaires

MINES Saint-Étienne

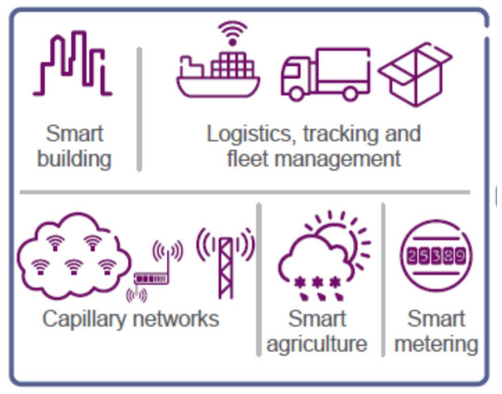
Une école de l'IMT

CHAIRE ValaDoE

Contexte

Massive IoT : grande quantité de capteurs, sur batteries et répartis spatialement dans un environnement.

- Environnement dynamique : des capteurs rentrent et repartent du SI (système d'information)
- Possibilité d'agir sur la fréquence d'échantillonnage des capteurs : on peut allonger ou raccourcir la période d'envoi d'informations
- Temps de surveillance limité par la capacité énergétique des capteurs



Uses cases Massive IoT
Source : lora-alliance

Définition du problème étudié

On veut gérer dynamiquement les émissions de capteurs de façon à recevoir des informations périodiquement à chaque pas de temps τ, et pendant le plus de temps possible.

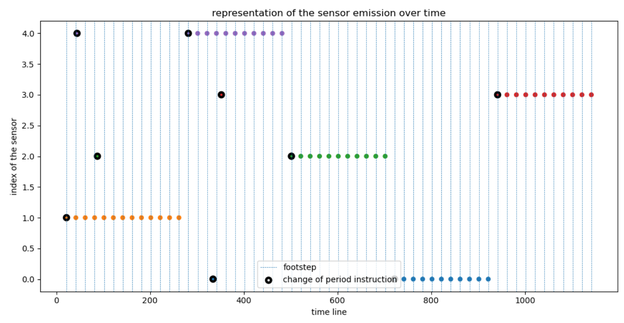
- Dynamicité du champ de capteurs: les n capteurs s'allument pour la première fois aux instants $(t_i)_{i\in[1,n]}$, et sont intégrés dynamiquement dans le SI. Le nombre de capteurs considérés par le SI varie dans le temps.
- Variation de l'énergie des capteurs : capacité énergétique initiale. Consommation de l'énergie a chaque émission, ainsi qu'a chaque modification de la période d'un capteur.

Algorithme de planification périodique = algorithme qui modifie les périodes d'émissions de capteurs entrants dynamiquement dans le SI de sorte que : il existe $l \in N$, tel que l'ensemble contenant les émissions de chaque capteur (hormis leur première émission), représente exactement et sans doublons l'ensemble $E(l) := \{t_0 + k\,\tau, k \in [1, l]\}$.

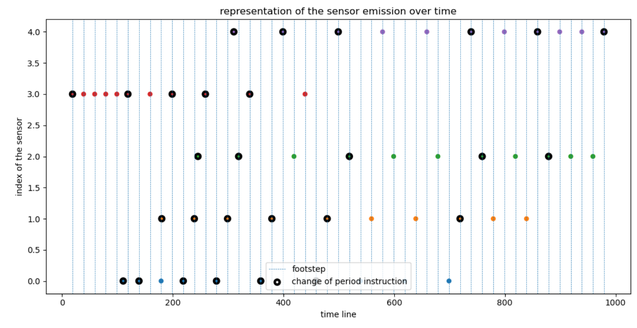
Premiers résultats

2 premiers algorithmes de planification périodique

- « un à un »



- « Tous ensemble »



Nouvelle approche

On fixe $M \in [1, n]$ comme étant la taille de l'ensemble des capteurs qui envoient de l'information au SI, chacun à tour de rôle. Si un capteur meurt, un autre prend le relai, et ce jusqu'à épuisement de l'énergie de tous les capteurs.

Résultat analytique

Propriété : si on considère $\forall i \in [1, M-1], |t_{i+1} - t_i| > \tau * i$, alors le nombre de changements de période total imposé par l'algorithme de planification périodique pour n capteurs est $\mathbf{M(M-1) + 2n - 1}$

Prise en compte de nouvelles perturbations

- Des capteurs peuvent disparaitre du système sans prévenir – la durée de vie des capteurs ne peut pas être très bien prédite
- Les messages gateway-capteurs peuvent ne pas être reçus correctement

Création de solutions plus robustes : plus couteux énergétiquement – diminue le temps de surveillance

Références liées au sujet :
- Maulin Raval, Shubhendu Bhardwaj, Aparna Aravelli, Jaya Dofe, andHardik Gohel. " Smart energy optimization for massive iot using artificial intelligence. " *Internet of Things*, 13:100354, 2021.
-N. Kaur and S. K. Sood, "An Energy-Efficient Architecture for the Internet of Things (IoT)", *IEEE Systems Journal*, vol. 11, no. 2, pp. 796-805, June 2017, doi: 10.1109/JSYST.2015.2469676

Contact : gwen.maudet@imt-atlantique.fr

Energy-efficient transceivers for Sat-IoT applications

Parties prenantes

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Auteurs

Karine AMIS
Frédéric GUILLOUD
Anouar JERBI

Partenaires

ThalesAlenia Space
a Thales / Leonardo company

TéSA
Télécommunications Spatiales et Aéronautiques

UNIVERSITÀ DI PARMA

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

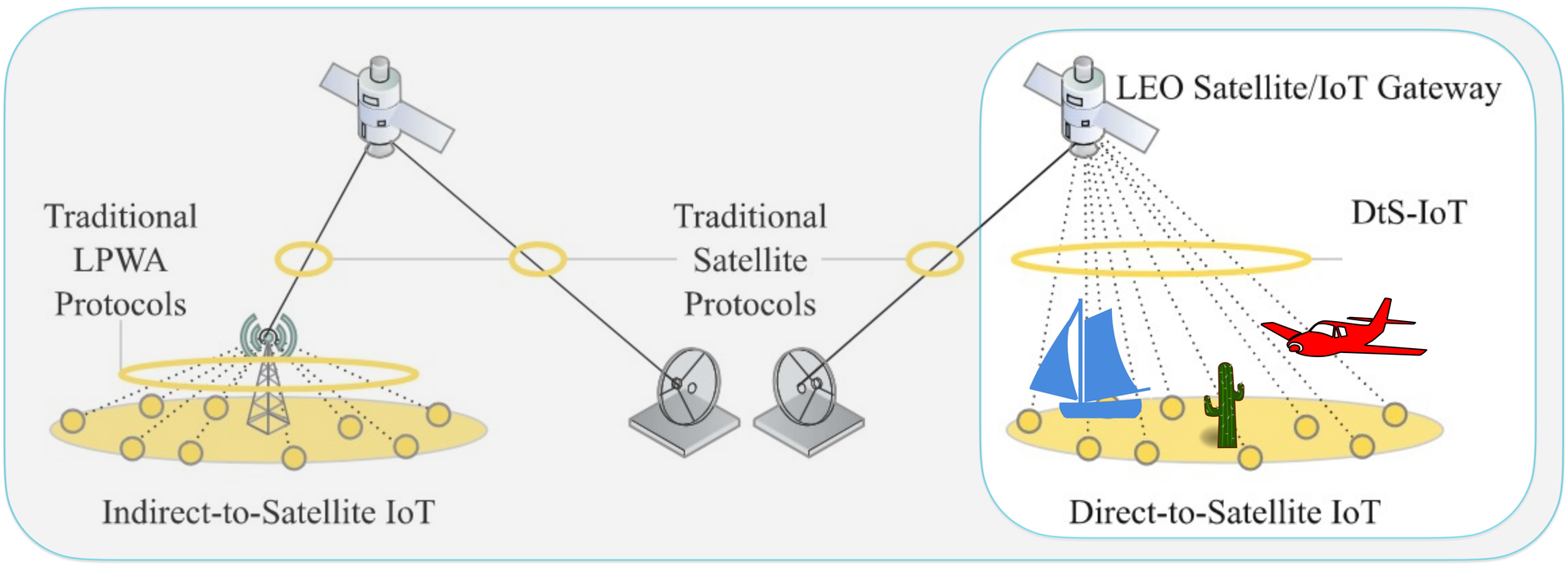
CLS
COLLECTE LOCALISATION SATELLITES

MITSUBISHI ELECTRIC
Changes for the Better

Sat-IoT Strategies

Dedicated or Add-Ons Communication Segment?

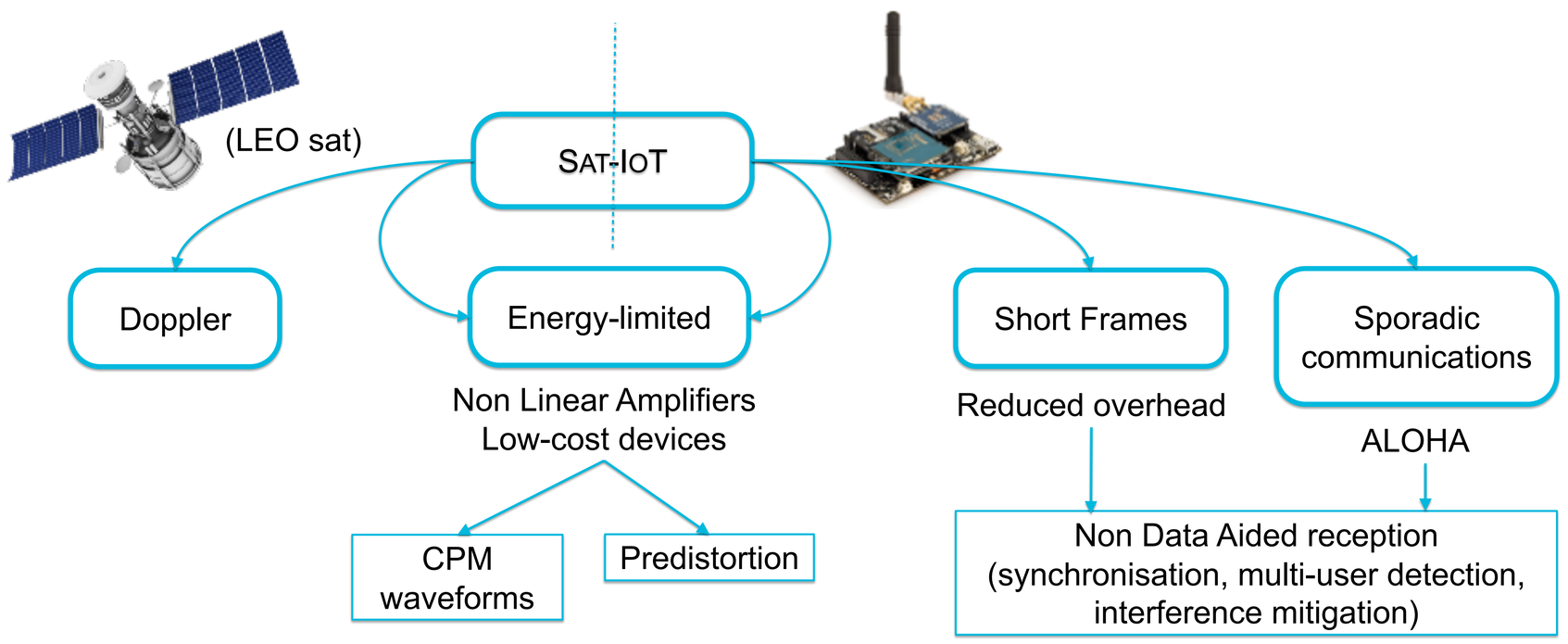
- Many IoT transceivers are concerned with **Low-Power Wide-Area** (LPWA) Communications.
- Direct to Satellite Communication (DtS): choose between
  - Design ad-hoc LPWA standards for Satellites
  - or “pick up terrestrial ones”



Fraire J.A., Céspedes S., Accettura N. (2019) Direct-To-Satellite IoT - A Survey of the State of the Art and Future Research Perspectives. In: Palattella M., Scanzio S., Coleri Ergen S. (eds) Ad-Hoc, Mobile, and Wireless Networks. ADHOC-NOW 2019. Lecture Notes in Computer Science, vol 11803. Springer, Cham. https://doi.org/10.1007/978-3-030-31831-4_17

Main issues

Facing both IoT & Satellite Communications constraints



Past and Ongoing Contributions: predistortion, coding, waveforms.

Focus on Continuous Phase Modulations (CPM)

- Enhanced spectral efficiency through precoding
- Coherent detection with reduced-complexity / robust towards parameters uncertainties
- Compressed-sensing techniques for multi-user detection in CPM-based sporadic communications
- Detection with blind Doppler-compensation in Sat-IoT
- Synchronisation for AIS systems

Contact : {karine.amis, frederic.guilloud}@imt-atlantique.fr

Octobre 2021 Colloque « réseaux du futur » de l'Institut Mines Télécom Paris

Signal Detection for Uplink in LoRa Networks with Neural Network

Angesom Tesfay, Eric Simon, Sofiane Kharbech, Laurent Clavier

Institut Mines-Télécom

Parties prenantes

Université de Lille

Auteurs

Angesom A. Tesfay
Eric P. Simon
Sofiane Kharbech
Laurent Clavier

Partenaires

Institut Mines-Télécom

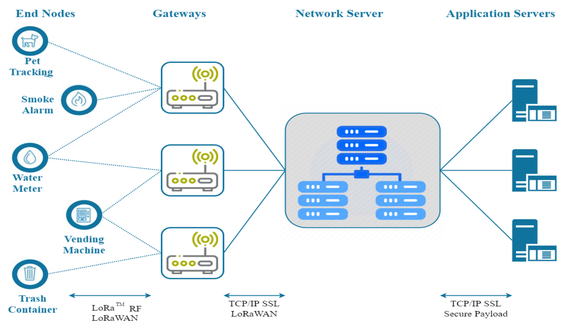
iemn

IRCICA

I. General context

LoRa (Long Range)

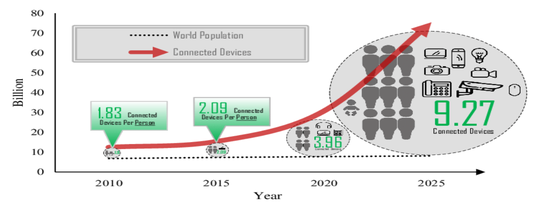
- LoRa is a low-power wide-area network (LPWAN) communication technique.
- LoRaWAN networking protocol is designed to wirelessly connect battery operated "things" to the internet.
- LoRa is based on chirp spread spectrum (CSS) modulation technique.
- Star-of-stars topology



II. Motivations

Interference in IoT

- Large-scale connectivity.

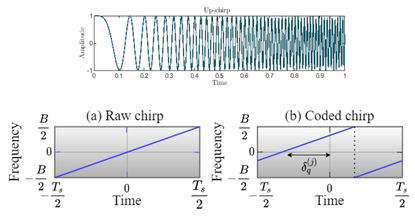


- LoRaWAN provides different bandwidths and spreading factors (SF) for transmission.
- When two or more devices are transmitting over the same frequency band, and SF
  - collision occurs at the receiver, hence **scalability** is limited.
  - one packet can be decoded due to the *capture effect*, if the desired signal is stronger than the interfering one.
- How “capture effect” will behave in machine learning-based receiver?

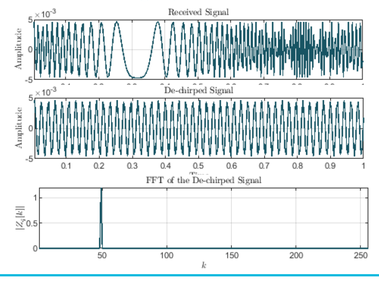
III. System Model

LoRaPHY: How is the information encoded?

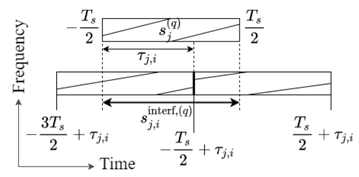
Transmitted signal: chirps are used (linearly increasing frequency) and shifted in time to encode the information.



Decoding system in LoRa



Co-SF Interference

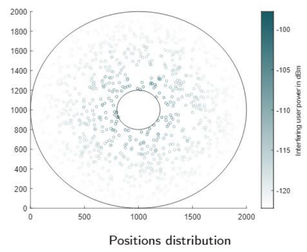


The received sampled signal (for symbol q) is:

$$r^{(q)}[n] = \underbrace{h_j s_j^{(q)}[n]}_{\text{user signal}} + \underbrace{\sum_{i \in \mathcal{I}} h_i s_{j,i}^{\text{interf},(q)}[n]}_{\text{interfering signals}} + \underbrace{w^{(q)}[n]}_{\text{complex Gaussian noise}}$$

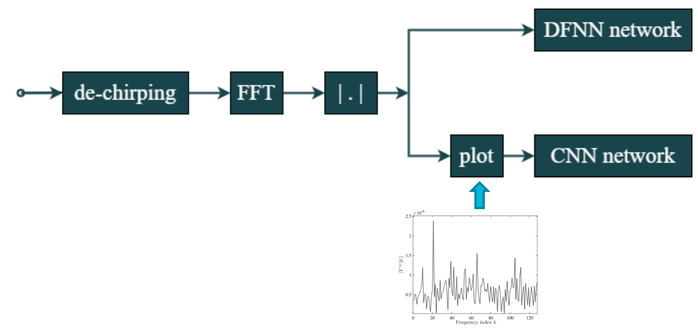
Interfering users

- Number of interfering users N_i follows a Poisson distribution with parameter λ.
- xy-coordinates of the interfering users are uniformly distributed.

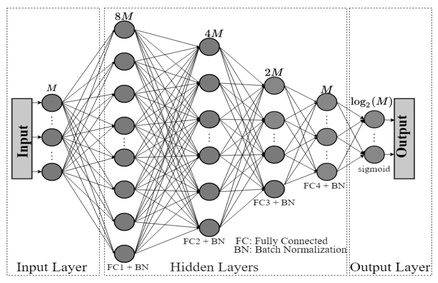


IV. Proposed Receivers

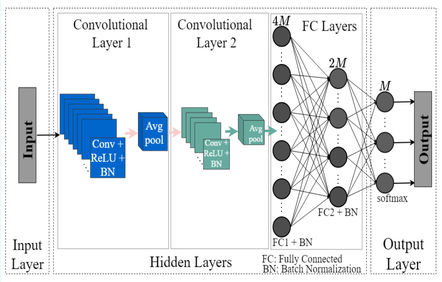
Deep-learning based receivers block diagram



A. Deep Feedforward Neural Network-based receiver (DFNN)

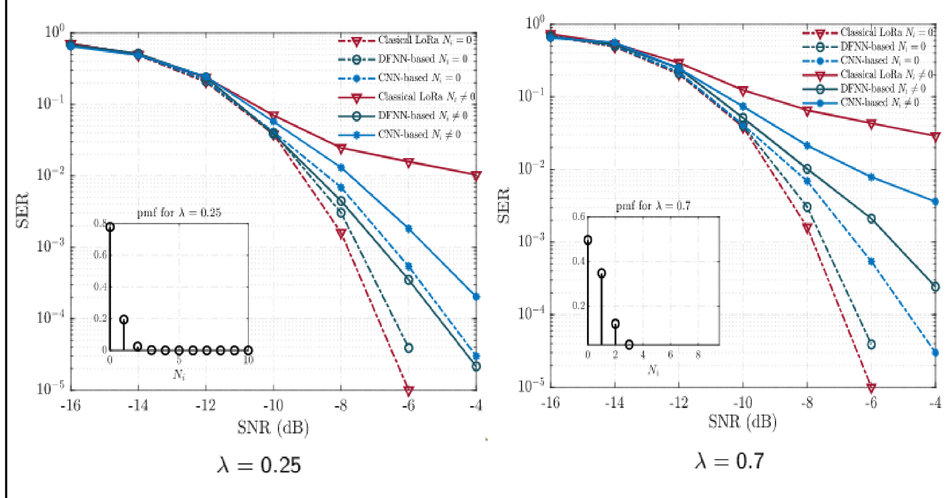


B. Convolutional Neural Network-based (CNN)



V. Simulation Result 1

Varying number of interfering users

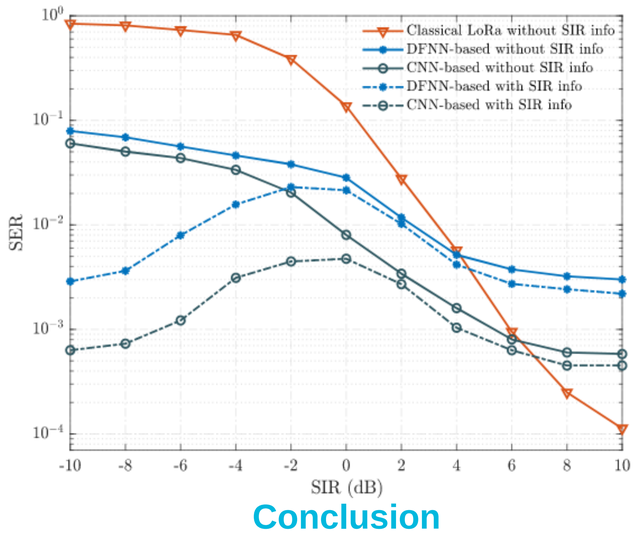


$\lambda = 0.25$ $\lambda = 0.7$

The plot inside show the probability related to the number of interfering users.

Simulation Result 2

Capture effect: $N_i = 1$, and SNR for the selected user is set to -6 dB



Conclusion

- Deep learning-based approach seems to be a promising candidate to tackle the issue of interference in LoRa networks due to the exponential growth of connected devices.
- SIR estimation technique could be combined with the deep learning-based decoder to improve the receiver's performance further.

Contact : angesom.tesfay@univ-lille.fr

Colloque de l’Institut Mines Télécom Paris
Novembre 2015

IMMUNet: Wireless System For Monitoring Automation Machines

IMMUNet provides a technical solution to facilitate the **dependable (predictive) maintenance for industrial machines** with moving or removable parts. It features high reliability and low energy consumption while being easy-to-use and cheap-to-deploy/own. The solution can bInternete deployed to operate as a fully autonomous system with no need for third-party services or access.

Parties prenantes

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

Auteurs

Giampaolo Cuozzo
Chiara Buratti
Roberto Verdone,
Konstantin Mikhaylov,
Laurent Clavier,
Lala Rajaorisoa
Dheeraj R. Kumar
Carles Antón Haro
Guillaume Villemaud

Partenaires

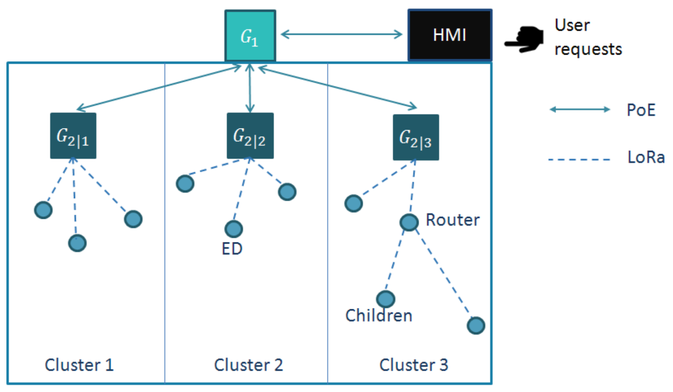
System

Tags equipped with multiple sensors sending data via wireless links to a final gateway connected to the PLC of the automatic machine.

Upon requests from the user sensors can take measurements and send the data to the gateway.

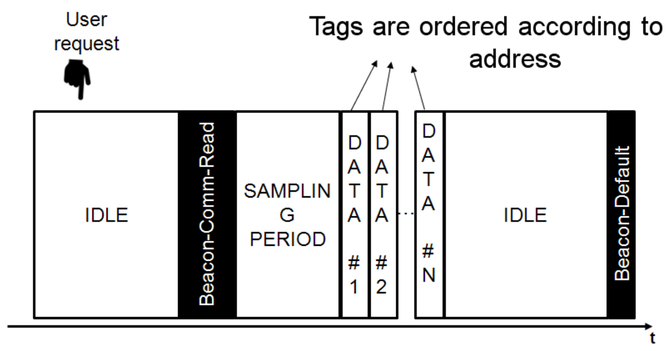
Architecture

Hierarchical and flexible architecture: multiple second-level gateways, connected to the same first-level gateway, can de deployed to cover large machines with different electromagnetically-isolated sections.



Technology

LoRa at 2.4 GHz (Bandwidth 1625 kHz, 40 channels available, Max. payload size 250 bytes, Max tx range of km in LOS)

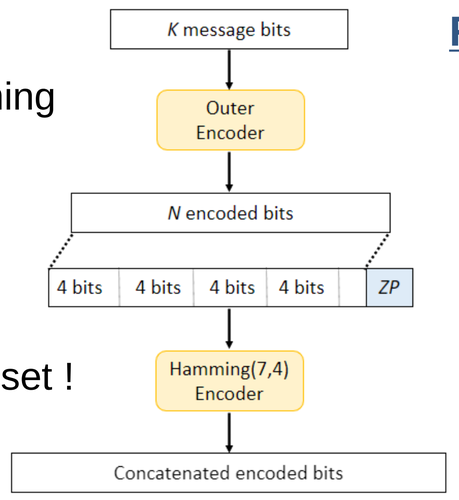


Reliability:

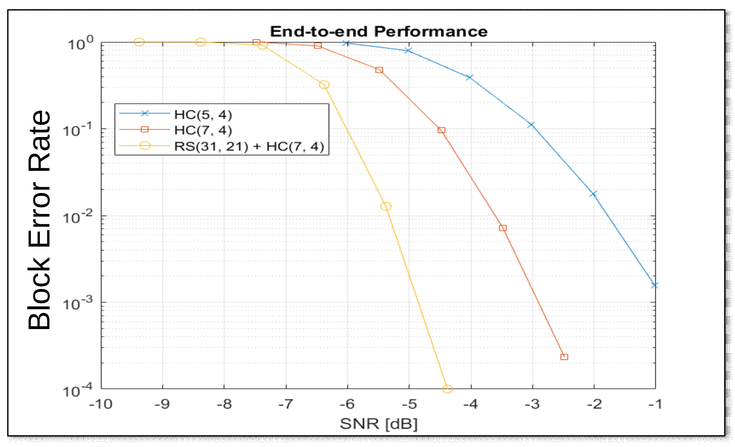
LoRa's weak coding scheme Hamming (5,4) replaced by a hybrid one:

- Outer layer: Reed Solomon - FEC
- Inner layer: Hamming (7, 4) - 1 bit correction

...no changes to existing LoRa chipset !

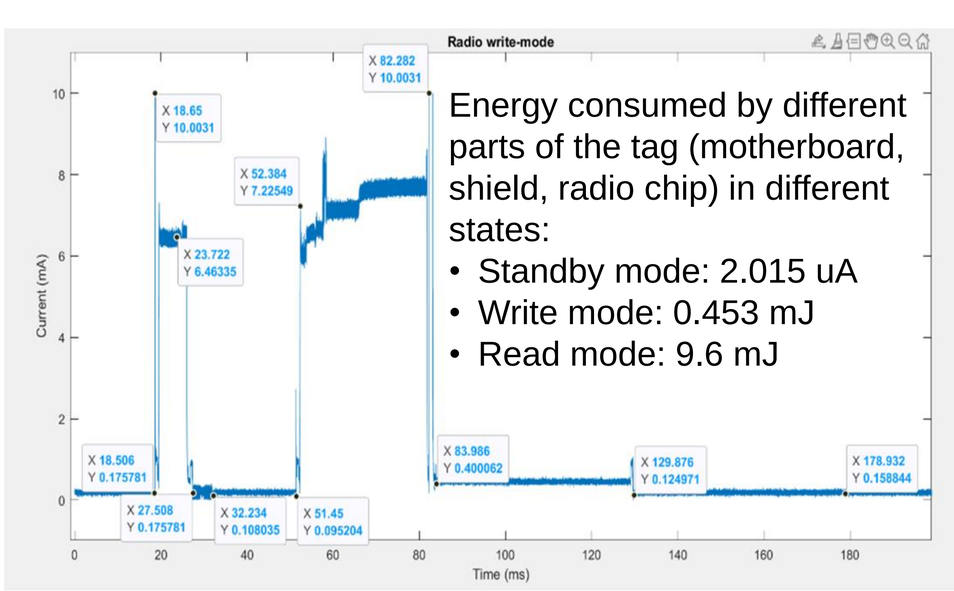


Results: Reliability



Significant gain in reliability to counter the noisy environment!

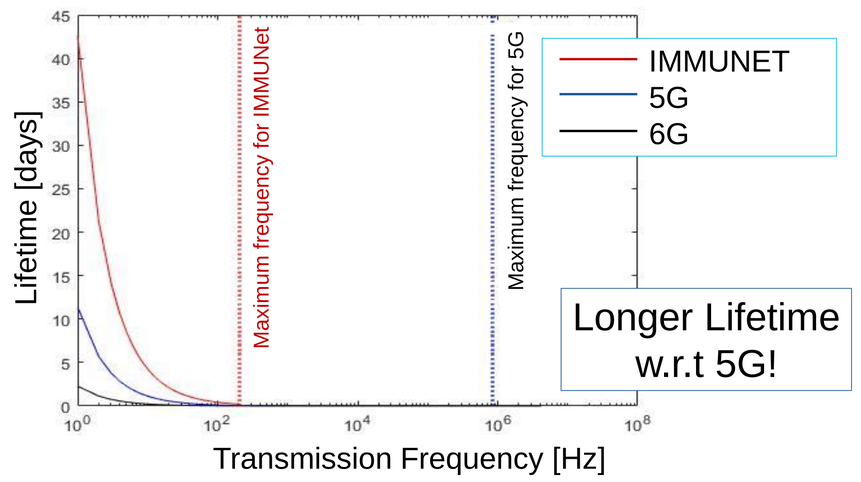
Results: Energy Consumption



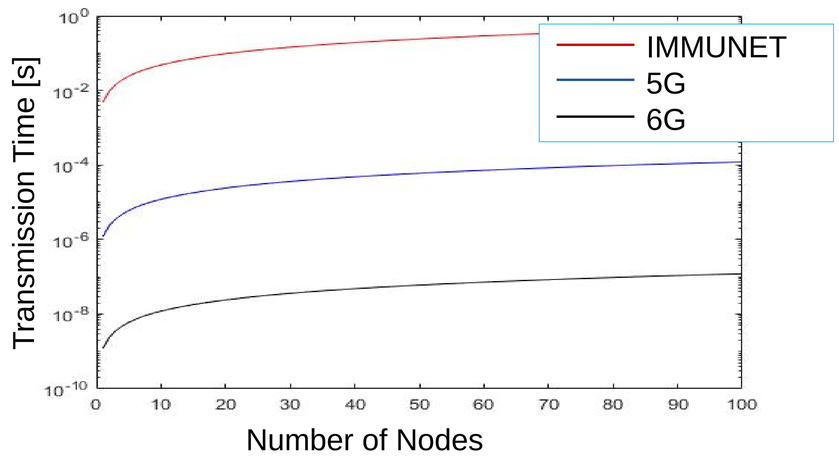
Energy consumed by different parts of the tag (motherboard, shield, radio chip) in different states:

- Standby mode: 2.015 uA
- Write mode: 0.453 mJ
- Read mode: 9.6 mJ

Total energy consumed per measuring/reporting phase: 23.34 mJ
Battery of 5.000 J and data measured/reported every 5 minutes → **Lifetime of one year!**



Results: Latency



Latency in the order of tens of ms

Acknowledgment

This work was developed in the framework of the **COST Innovators Grant**, IG15104 IMMUNet.

Contact : laurent.clavier@imt-nord-europe.fr

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

L'IoT pour l'optimisation de la performance énergétique des bâtiments intelligents

Technologies numériques pour l'amélioration de la performance énergétique des bâtiments

Vers des bâtiments durables et moins énergivores

- ► **Réduire la consommation énergétique et les émissions de carbone**
- ► **Accélérer l'adoption de technologies d'efficacité énergétique et d'énergies renouvelables**
- ► **Développer des techniques de rénovation plus efficaces et plus adaptées**
- ► **Renforcer le processus de digitalisation des bâtiments**

Parties prenantes

SYSTÈMES NUMÉRIQUES

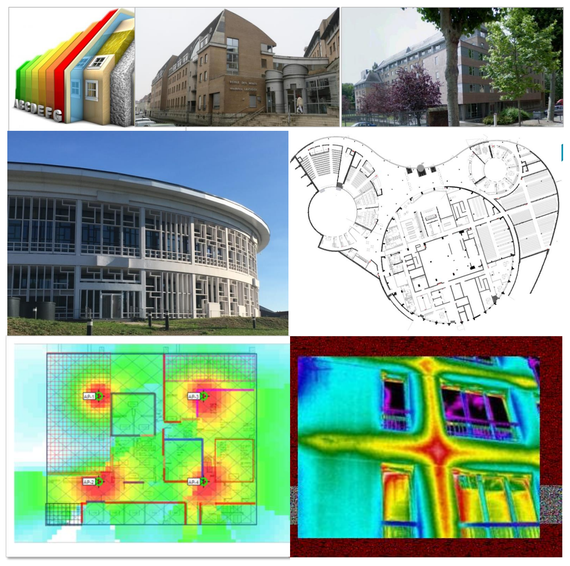
Auteurs

Lala Rajaoarisoa
Laurent Clavier
M. Sayed-Mouchaweh

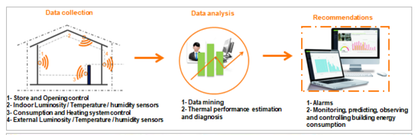
Optimisation de la conception et l'exploitation des bâtiments intelligents

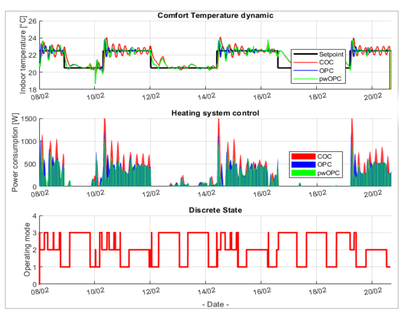
Estimation, contrôle et diagnostic

- ► **Mise en œuvre des méthodes innovantes et rapides pour le suivi et le pilotage des bâtiments grâce aux OBJETS mobiles et connectés.**
  - Modélisations et caractérisations avancées de la performance thermique et énergétique du bâtiment, du composant seul, ainsi que le couplage composant - bâtiment,
  - Analyse des modes de consommations, d'usage et d'exploitation du bâtiment,
  - Développement de technique avancée pour diagnostiquer la performance énergétique par les mesures en proposant des indicateurs robustes, pertinents et adaptés.



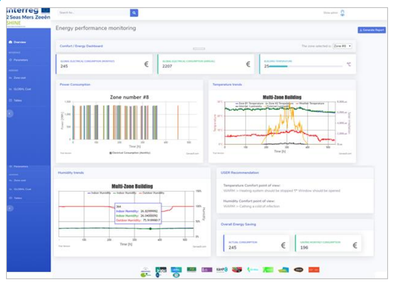
Mesurer et analyser la consommation

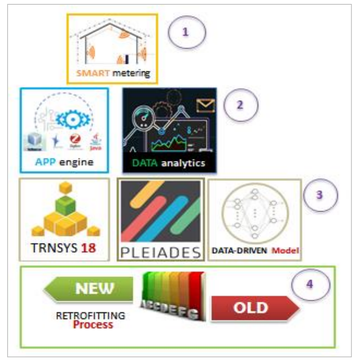




Contrôler et pérenniser la performance

Visualiser, observer et superviser les installations



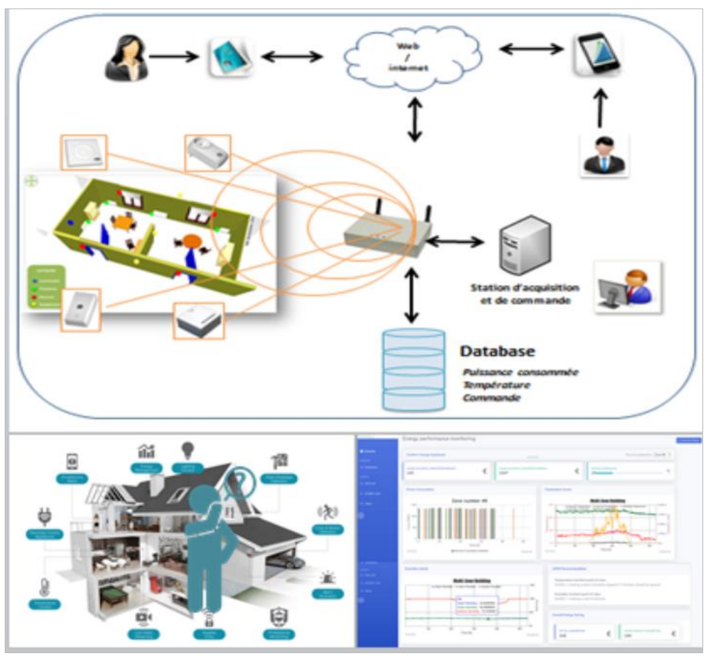


Traitement et analyse des données

Fiabilité, Résilience et Robustesse des objets

Efficacité énergétique, performance et disponibilité des objets

- ► **Développement de méthodes de mesures, d'instrumentation et d'analyse déportées fiables** (inter-connectivité des objets dans différentes zones thermiques, interopérabilité)
- ► **Mise en œuvre de techniques avancées pour améliorer l'autonomie et la disponibilité des objets connectés** (perte de communication, faible autonomie, etc.)
- ► **Développement et déploiement de l'intelligence embarquée dans les capteurs et les dispositifs périphériques connectés** (Echanges d'informations, coopératifs, IA embarqué, traitement de données massives)



Contact : lala.rajaoarisoa@imt-nord-europe.fr

Improving Security of LoRaWAN Architecture and OTAA based Communications

Parties prenantes

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

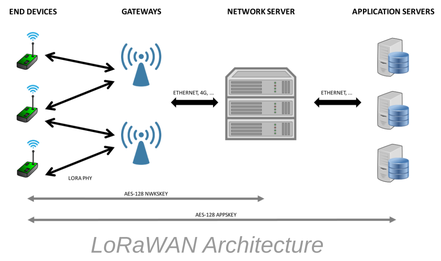
UMONS
Université de Mons

Auteurs

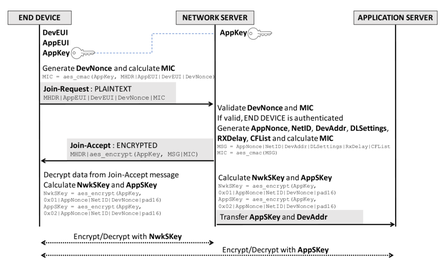
Phithak THAENKAEW
Ahmed MEDDAHI
Bruno QUOITIN

Partenaires

NECTEC
a member of NSTDA



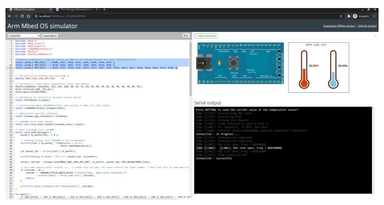
LoRaWAN Architecture



OTAA v1.0.2 Sequence Diagram

Introduction

- **LPWAN** stands for “**L**ow **P**ower **W**ide **A**rea **N**etwork”, A wireless type of communication, designed for sending "**small" data** packages over **long distances**,while operating **on a battery**. There are number of competing technologies in the LPWAN space such as: NB-IoT, Sigfox, **LoRa** and others.
- **LoRa** and **LoRaWAN** – LoRa is the **physical** layer. LoRaWAN is the **network**.
- **OTAA** is the preferred and "**most" secure way** to connect with Network/Application Server or **The Things Network (TTN)**. Devices perform a **join-procedure (authentication)** with the network, during which a dynamic **DevAddr** is assigned and **security keys** are negotiated with the device.
- **AES-128** symmetric key is used for encryption in LoRaWAN communication.
  - Generate MIC (Message Integrity Code)
  - Encrypt the messages communicated between End-Devices and Servers
- Research Direction – Improve the security with a focus on
  - **Authentication** and **identification** in **constrained** environment.
  - Impact of **encryption** mechanism on energy consumption.
  - Scalability



Mbed Simulator

ns-3

Current Status

- Exploring LoRaWAN Architecture and OTAA mechanism by using Simulation tools.
- **Mbed Simulator** is an **open source software** developed by **ARM**.
  - Support LoRaWAN and OTAA.
  - Anaylising OTAA mechanism by extracting the **Join-Request** Message, **Join-Accept** Message and the messeges between End-Device and Application Server from the data communication log of Mbed Simulator.
  - Limitation of Mbed Simulator – No realistic environment features, Support only some parts of LoraWan (End-Device and Gateway), Difficult to scale-out the number of devices (scalability issue).
- **ns-3** is a well-known simulation software with **more features** support.
  - Using ns-3 to simulate a LoRaWAN communication of a single End-Device and Gateway, multiple End-Devices and Gateways, simulate with realistic environment.
  - Limitation of ns-3 – No security module for LoRaWAN communication.

Future Works

LoRaWAN Hardware

- Extend **ns-3** with a security module for LoRaWAN.
- Evaluate LoRaWAN data encryption with:
  - Different **key size**.
  - Different encryption **algorithms**.
- Impact of OTAA on performance metrics (power consumption,,,)
- Compare the experimental results from simulations and practical testbed.
- Perform performance evaluation at larger scale (scalability).

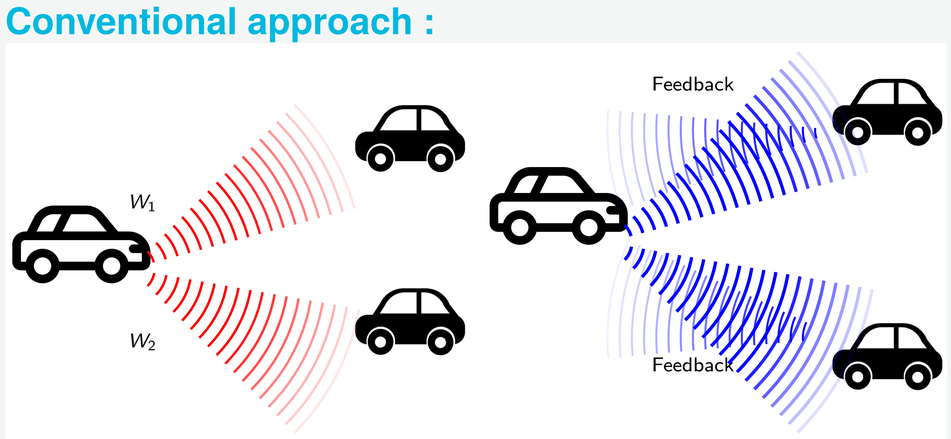
Contact : phithak.thaenkaew@umons.ac.be

Joint Sensing and Communication over Memoryless Broadcast Channels

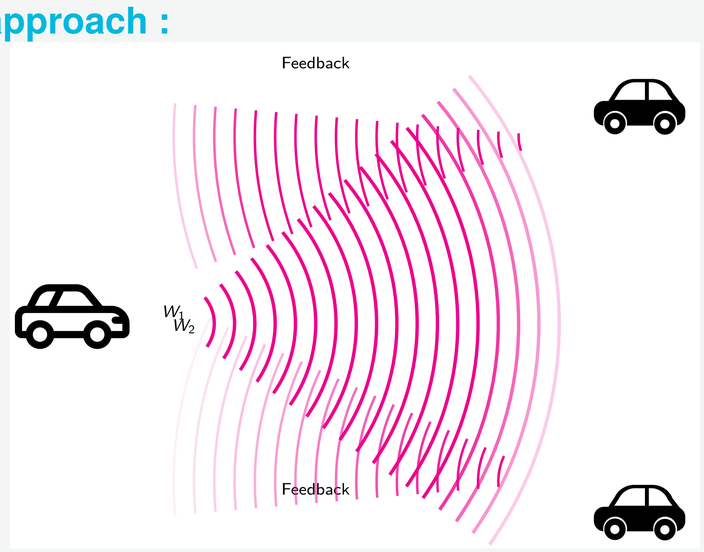
Authors
Mehrasa Ahmadipour
Mari Kobayashi
Michèle Wigger
Giuseppe Caire

Motivation

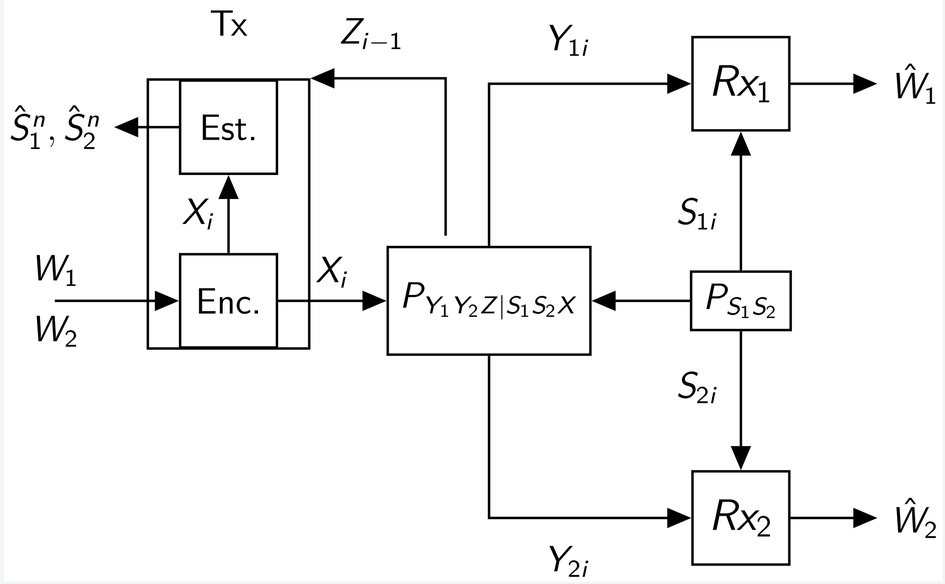
Conventional approach :



Joint approach :

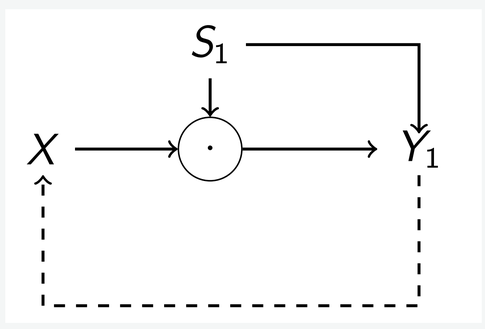


Mathematical Model



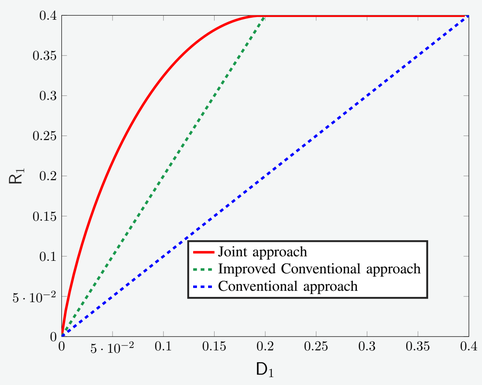
Capacity-Distortion Region $\mathcal{CD}$ (R_1, R_2, D_1, D_2) is achievable if there exist encoder, decoder and estimator s.t.

- $\lim_{n\to\infty} p^n(\text{error}) := \Pr\left(\hat{W}_1 \neq W_1 \quad \text{or} \quad \hat{W}_2 \neq W_2\right) = 0$
- $\overline{\lim}_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}[d_k(S_{k,i}, \hat{S}_{k,i})] \leq D_k, \qquad \text{for} \quad k = 1, 2.$



Single Receiver

- $\mathcal{Y}_1 = \mathcal{S}_1 = \mathcal{X} = \{0, 1\}$
- $Y_1 = S_1 \cdot X$
- $P_X \sim Ber(\frac{1}{2}) \Rightarrow C = P_{S_1}(1)$, $D = \frac{1}{2}\min\{P_{S_1}(1), P_{S_1}(0)\}$
- $P_X(1) = 1 \Rightarrow R = 0, D = 0$



Feasible Region

The convex closure of the set of all (R_1, R_2, D_1, D_2) satisfying

$$R_k \leq I(U_0, U_k; Y_k, V_k \mid S_k) - I(U_0, U_1, U_2, Z; V_0, V_k | S_k, Y_k),$$
$$R_1 + R_2 \leq I(U_1; Y_1, V_1 | U_0, S_1) + I(U_2; Y_2, V_2 | U_0, S_2)$$
$$+ \min_{i\in\{1,2\}} I(U_0; Y_i, V_i \mid S_i) - I(U_1; U_2 | U_0)$$
$$- I(U_0, U_1, U_2, Z; V_1 | V_0, S_1, Y_1) - I(U_0, U_1, U_2, Z; V_2 | V_0, S_2, Y_2)$$
$$- \max_{i\in\{1,2\}} I(U_0, U_1, U_2, Z; V_0 | S_i, Y_i)$$

and

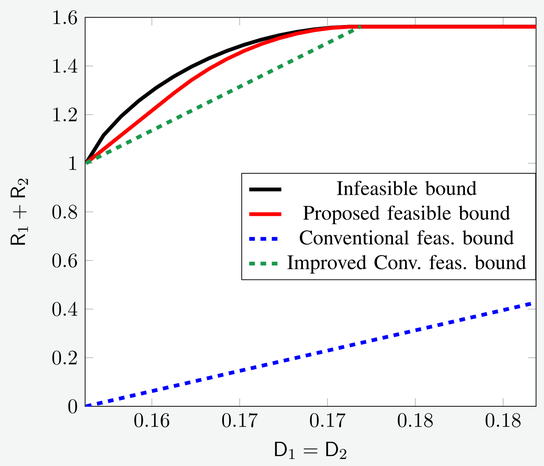
$$\mathbb{E}[d_k(S_k, \hat{s}_k^*(X, Z)))] \leq D_k$$

for some

- $P_{U_0U_1U_2}P_{X|U_0U_1U_2}P_{S_1S_2}P_{Y_1Y_2Z|S_1S_2X}\ P_{V_0V_1V_2|U_0U_1U_2Z}$,

where

- $\hat{s}_k^*(x, z) \triangleq \min_{s'\in\hat{\mathcal{S}}_k} \sum_{s_k\in\mathcal{S}_k} P_{S_k|XZ}(s_k|x, z)$ and $k \in \{1, 2\}$.



Example : Two receivers

- $\mathcal{Y} = \mathcal{S} = \mathcal{X} = \{0, 1\}$

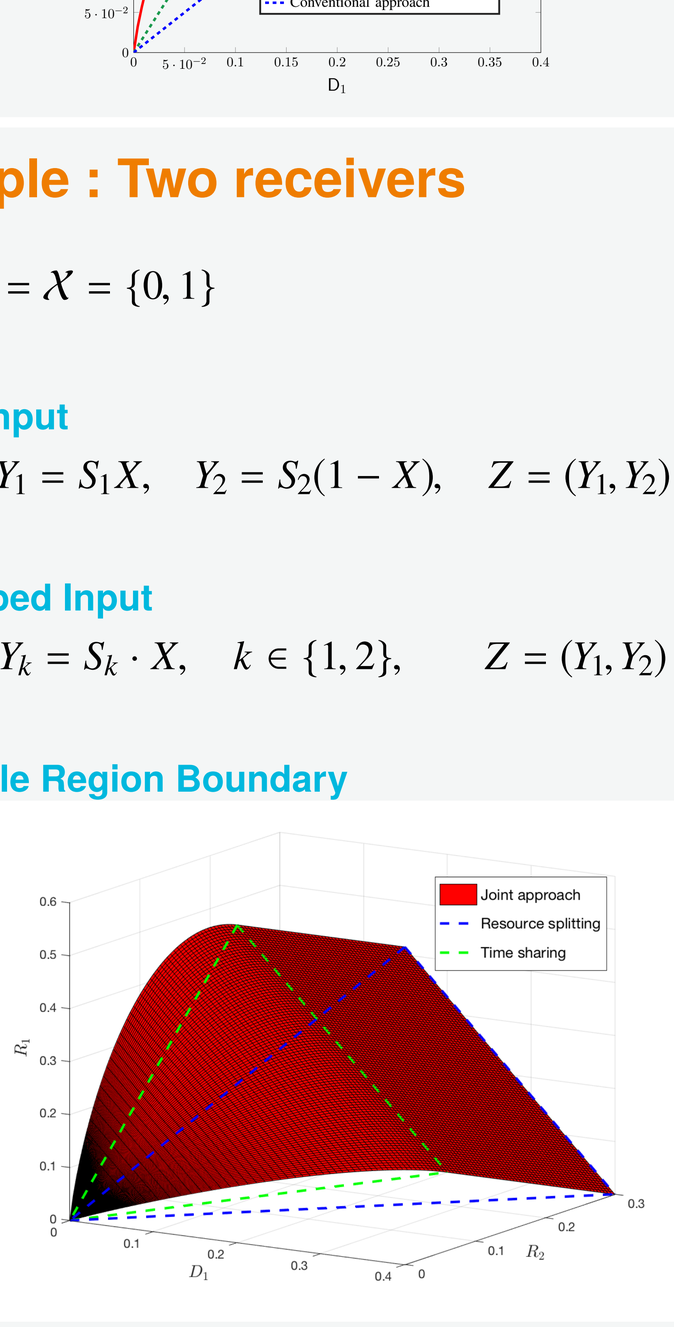
Flipped Input

$$Y_1 = S_1 X, \quad Y_2 = S_2(1 - X), \quad Z = (Y_1, Y_2)$$

Non-Flipped Input

$$Y_k = S_k \cdot X, \quad k \in \{1, 2\}, \qquad Z = (Y_1, Y_2)$$

Achievable Region Boundary



Contributions

- Feasible capacity-distortions region
- Infeasible capacity-distortions region
- Proposed joint scheme outperforms the conventional scheme

References

- An Information-Theoretic Approach to Joint Sensing and Communication M. Ahmadipour, M. Kobayashi, M. Wigger, G. Caire at arXiv :2107.14264
- M. Ahmadipour, M. Wigger and M. Kobayashi, "Joint Sensing and Communication over Memoryless Broadcast Channels," 2020 (ITW)

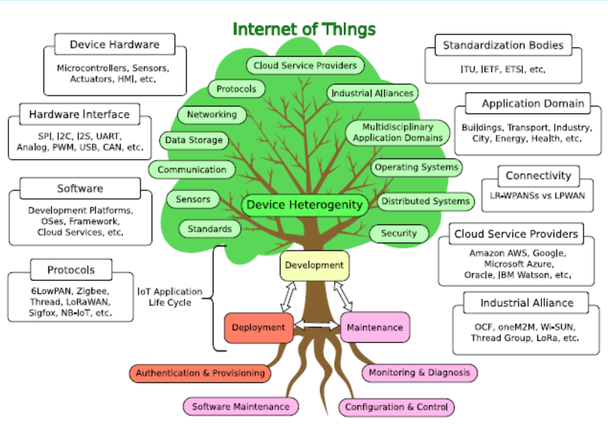
Contact

Mehrasa.ahmadipour@telecom-paris.fr

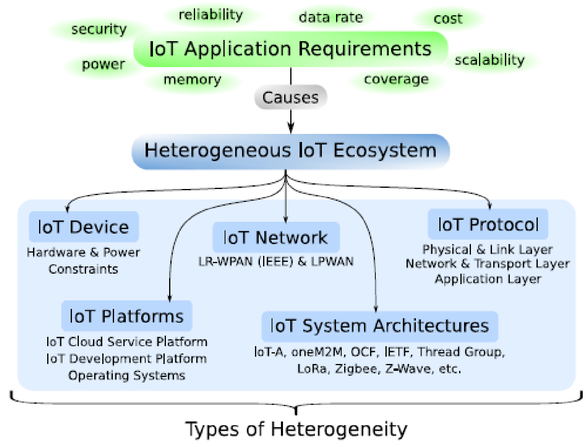
Institut Mines-Télécom

Software and Hardware approaches for Efficient IoT application lifecycle management

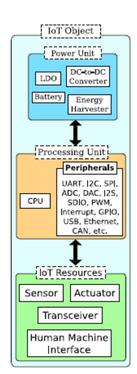
A bottom-Up Device Heterogeneity control

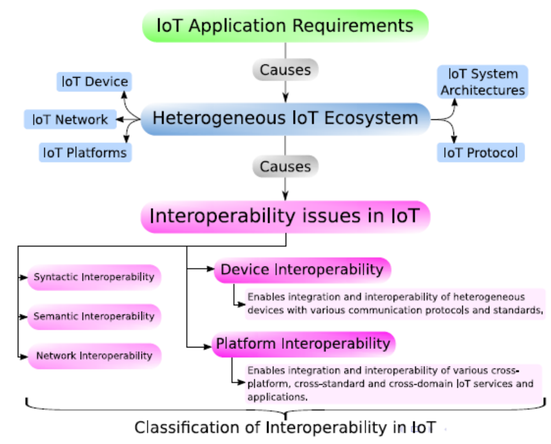


IoT application Development, Deployement, Maintenance Lifecycle and Device Heterogeneity



Types of Heterogeneity





Classification of Interoperability in IoT

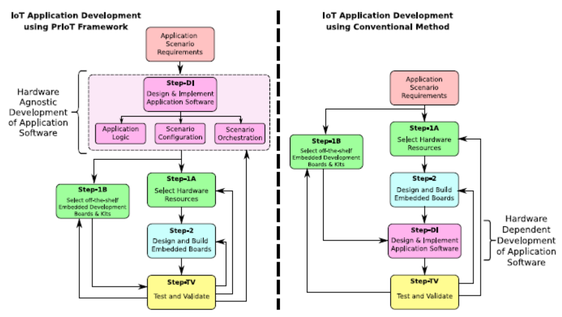
No *common* and *uniform* standard to program heterogeneous device architectures.

CPU Architecture	OSes			Non-OS			Bare metal using vendor specific tools
	RIOT	Zephyr	contiki	mbed	Arduino	Energia	
ARM Cortex-Mx	✓	✓	✗	✓	✓	✗	ARM Mbed
Atmel AVR	✓	✗	✗	✗	✓	✗	Atmel Studio
TI-MSP430	✓	✗	✗	✗	✗	✓	Code Composer Studio
Intel x86	✓	✓	✓	✗	✗	✗	Intel System Studio
ARC	✗	✓	✗	✗	✗	✗	DesignWare ARC
NIOS II	✗	✓	✗	✗	✗	✗	Nios II Embedded Design Suite
Tensilica Xtensa	✗	✓	✗	✗	✗	✗	Xtensa Xplorer IDE
RISC-V	✗	✓	✗	✗	✗	✗	RISC-V GCC
Nordic	✓	✓	✓	✗	✗	✗	nRF5 SDK

Table: Embedded system programming diversity from OSes to bare metal approach

- We proposed a new framework named PrIoT for better IoT application lifecycle management.
- PrIoT introduces an intermediate abstraction between IoT device hardware and IoT application to hide the underlying device heterogeneity.
- We implemented PrIoT as an open source framework - `www.priot.org`

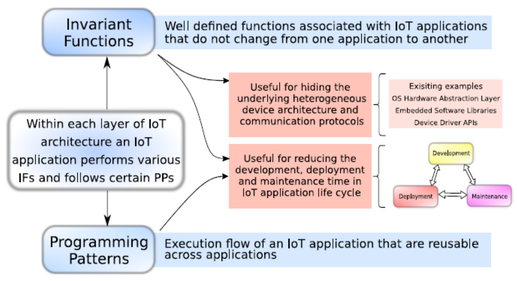
	IoT development Techniques	PrIoT Block	Existing Solution
1	High level language and API	PrIoT-Lang PrIoT-API	Arduino, Energia, mbed and Embedded OSes
2	Hardware abstraction	PrIoT-GI PrIoT-HAL	Embedded OSes
3	Device Configuration and Database	PrIoT-Config PrIoT-Parser PrIoT-Database	PlatformIO
4	User Interface	PrIoT-UI	Node-Red, Blockly
5	IoT service and device management	PrIoT-Orchestrator	Kubernetes

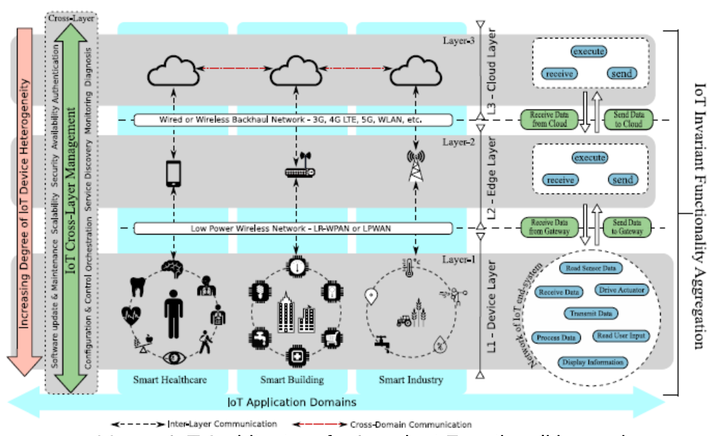


An open source IoT framework www.priot.org

Software based Approach for IoT application development, deployement and maintenance of Heterogeneous Devices

- **IoT Invariant Functionalities** *(IF)*
- **IoT Programming Patterns** *(PP)*
- **Proposed 4 Layer IoT Architecture**
- **PRIOT** *(New IoT framework for easy and efficient development, deployement and maintenance)* – IoT Device heterogeneity Abstraction layer

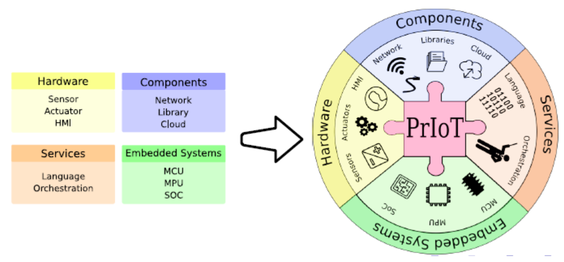




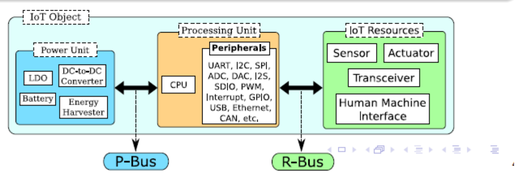
4 Layer IoT Architecture for Invariant Functionalities and Programming Patterns

PrIoT - Prototyping Internet of Things

An open source prototyping framework for **developing**, **deploying** and **maintaining** an IoT application on a distributed network of heterogeneous devices.



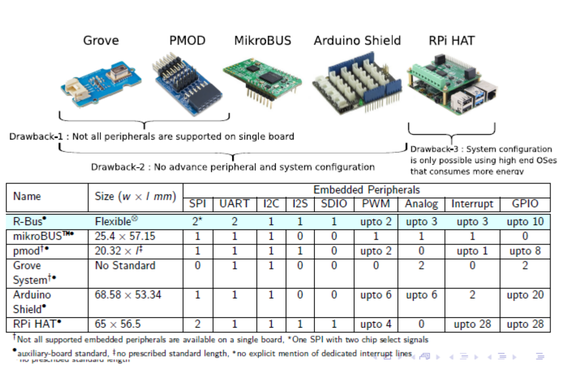
- We proposed two new modular systems named R-Bus (Resource Bus) and P-Bus (Power Bus) for controlling *IoT device peripheral heterogeneity*.
- To reduce the complexity of integrating, replacing and re-configuring IoT devices from various manufacturers that require different hardware and software component.



R-Bus: Ressource Bus for IoT device modular System Design

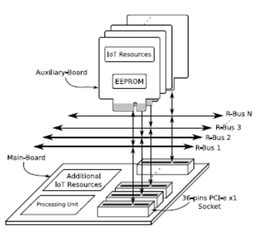
Hardware based approach for Efficient IoT device Heterogeneity control

- Proposed two new modular systems named **R-Bus** (Resource Bus) and **P-Bus** (Power Bus) for controlling IoT device peripheral heterogeneity.
- To reduce the complexity of **integrating, replacing and re-configuring** IoT devices from various manufacturers that require different hardware and software component



Name	Size ($w \times l$ mm)	Embedded Peripherals								
		SPI	UART	I2C	I2S	SDIO	PWM	Analog	Interrupt	GPIO
R-Bus*	Flexible◎	2*	2	1	1	1	upto 2	upto 3	upto 3	upto 10
mikroBUS™*	25.4 × 57.15	1	1	1	0	0	1	1	1	0
pmod†*	20.32 × ?‡	1	1	1	1	0	upto 2	0	upto 1	upto 8
Grove System†*	No Standard	0	1	1	0	0	0	2	0	2
Arduino Shield*	68.58 × 53.34	1	1	1	0	0	upto 6	upto 6	2	upto 20
RPi HAT*	65 × 56.5	2	1	1	1	1	upto 4	0	upto 28	upto 28

†Not all supported embedded peripherals are available on a single board, *One SPI with two chip select signals
*auxiliary-board standard, ‡no prescribed standard length, *no explicit mention of dedicated interrupt lines



R-Bus System Objectives

1. Maximize the number of peripherals on a single board. (To solve drawback-1)
2. To allow system configuration for all classes of devices. (To solve drawback-2,3)

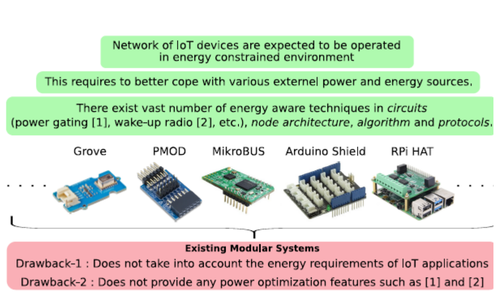
R-Bus System Design Approach

1. In R-Bus, we utilize a *modular architecture* approach to partition the embedded system.
2. The partition is based on the concept of *bus modularity*.
3. In bus modularity all IoT resources modules (*auxiliary-boards*) are connected to a single common module (*main-board*).

P-Bus: A Power Pus for Energy efficient IoT device modular design

IoT Device New Power Interface management

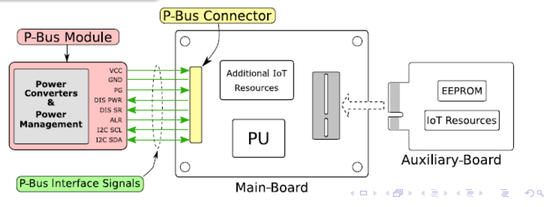
- Proposed modular system named Power-Bus that provides the necessary features required for better power optimization.
- To expose an intelligent homogeneous interface that is usable across various power requirements of IoT applications.
- New Power Gating functionality in Wake up Radio



P-Bus Module
- Expose power management features.
- Provides power to external circuit.

P-Bus Interface
- Interface (signals) to access power management features.

P-Bus Connector
- Connector for adding P-Bus module with external boards.



Contact : hakima.chaouchi@telecom-sudparis.eu

Parties prenantes

TELECOM SudParis

IP PARIS

Auteur

Hakima Chaouchi
Professeur
Telecom Sud Paris
Institut Mines Telecom
Institut Polytechnique de Paris

Online&Licences

priot.org

GPL v3 Free Software Free as in Freedom

Publications

[1] Nahit Pawar, Thomas Bourgeau and Hakima Chaouchi. Study of IoT Architecture and Application Invariant Functionalities. IFIP/IEEE International Symposium on Integrated Network Management (IM 2021), 17-21 May 2021, Bordeaux, France.

[2] Nahit Pawar, Thomas Bourgeau and Hakima Chaouchi. PrIoT Demo: Example of Invariant Functionalities. The IEEE/IFIP International Symposium on Integrated Network Management 2021 (IM 2021), 17-21 May 2021, Bordeaux, France.

[3] Nahit Pawar, Thomas Bourgeau and Hakima Chaouchi. R-Bus: A Resource Bus for Modular System Design. The 10th International Conference on Internet of Things (IoT2020), 6-9 October 2020, Malmo, Sweden.

[4] Nahit Pawar, Thomas Bourgeau and Hakima Chaouchi. R-Bus - A Resource Bus for Modular System Design. International Conference on Embedded Wireless Systems and Networks (EWSN), 17-19 February 2020, Lyon, France.

[5] Nahit Pawar, Thomas Bourgeau and Hakima Chaouchi. Power Gating and Its Application in Wake-Up Radio. International Conference on Embedded Wireless Systems and Networks (EWSN), 17-19 February 2020, Lyon, France.

[6] Nahit Pawar, Thomas Bourgeau and Hakima Chaouchi. Low-cost, Low-power Testbed for Establishing Network of LoRaWAN Nodes. International Conference on Embedded Wireless Systems and Networks (EWSN), 17-19 February 2020, Lyon, France.

[7] Nahit Pawar, Thomas Bourgeau and Hakima Chaouchi. PrIoT: Prototyping the Internet of Things. In 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), 6-8 August 2018, Barcelona, Spain.

Lille 14 Octobre 2021 Colloque de l'Institut Mines Télécom, Thématique Phare Internet des Objets et réseaux du futur.

Blockchain based trust management mechanism for Industry 4.0

Parties prenantes

TELECOM SudParis

IP PARIS

Auteurs

Asma Lahbib
Anis Laouiti

Introduction & Motivation

Trust is often needed to produce reaction based on the real time evaluation of entities behaviors during interactions in addition to feedbacks and recommendations gathered from other entities.
A secure and distributed based trust system is essential to guarantee trust information confidentiality, integrity and privacy during sharing and storage.
A proof of existence, of ownership, of access and modification of this information is essential as it will be used later for decision making process.

➡ Keeping a living document trace about the flow of trust information as well as their access in order to guarantee an extra level of transparency, control and notarization during collaboration.

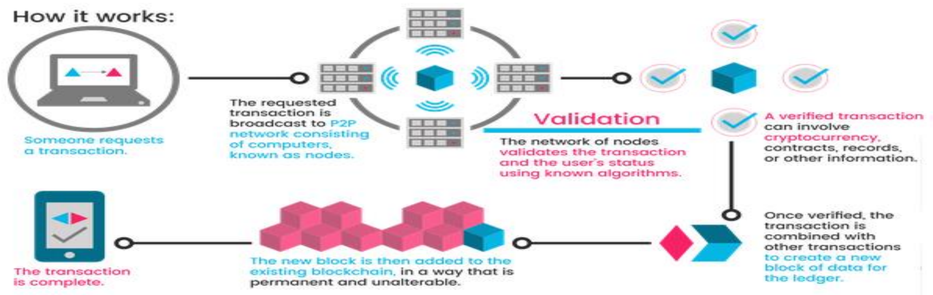
idea Blockchain based trust system

What is the Blockchain technology ?

A digital record of transactions, that can be any movement of money, goods or secure data. These transactions are hold within blocks chained together through hashes contained within their headers.

Secure It is designed to store information in a way that makes it virtually impossible to add, remove or change data contained within without being detected by participating peers.

Distributed Blockchain is a distributed ledger hold by each participating peer and where verification of established transactions comes after the consensus of all participatings peers.



What blockchain means for Industry 4.0 ?

Structural features	Technology for sharing information….	...which allows for multiple parties...	...whose data is notarized, secure, verified thus trusted...	...forming a public record visible to all
What it means for smart factories	like production data, the origin of goods, entities trust records….	Including machines, Manufacturers, suppliers, customers...	Traceability of goods from suppliers to machines...	Allowed parties have access to data around a product, another entity...
What it means for smart health	Like patients records, prescription medicines, Medical devices trust records….	Including patients, doctors,medical centers, smart cities...	Keeping a complete patient's medical history...	Allowed parties have access to data around patients..

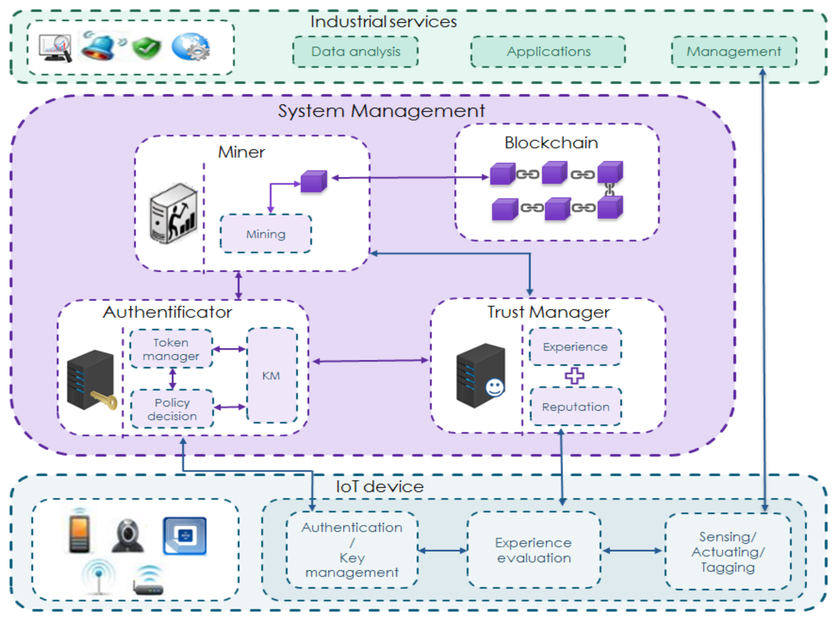
Proposed Approach

Propose a novel trust management system based on the blockchain technology

Defines and evaluate a trust score for each device within the manufacturing zone and securely store and share these scores through the blockchain network guaranteeing their transparency, integrity, authenticity, authorization, traceability and more importantly their notarization.

Implementation conducted using NS3 for the simulation of the IoT network and Multichain for the blockchain network.

Evaluation made regarding the resiliency against attacks, the response time and the percentage of successful transactions



Use cases applications

Extending the proposal to support fine-grained access control polices while allowing different parties to effectively interact and collaborate with each other in a trustful, secure and privacy preserved manner.

The framework relies on smart contracts designed and implemented to support:
- the registration of entities,
- the governability of the consensus mechanism,
- the definition of the access control model
- and the sharing of data while preserving their privacy.

Contact : asma.lahbib@telecom-sudparis.eu
anis.laouiti@telecom-sudparis.eu