Communications radio avancées
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).

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

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 événements évoluant dans le temps avec ou sans connaissance des étiquettes associées à ces événements.

► Application – Identification automatique de comportement frauduleux envers les réseaux de communication IEEE 802.11n

Protocol 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 Adaptive Kernel Machine

► Basé sur l’algorithme One class SVM développé par Schölkopf (2000).

► Architecture neural de type feed-forward

► Mesure de similitude induite par le noyau RKHS

► Règle de mise à jour (Initialisation ou création, Adaptation, Fusion)

Résultats

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

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (noir)</td>
<td>100 %</td>
<td>100%</td>
<td>7%</td>
<td>4%</td>
<td>36%</td>
</tr>
<tr>
<td>2 (vert)</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>31%</td>
</tr>
<tr>
<td>3 (rouge)</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
<td>100%</td>
<td>33%</td>
</tr>
<tr>
<td>4 (bleu clair)</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>39%</td>
</tr>
<tr>
<td>5 (bleu)</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>57%</td>
<td>0%</td>
</tr>
<tr>
<td>6 (violet)</td>
<td>0%</td>
<td>0%</td>
<td>93%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Figure 1: Configuration des acquisitions

Figure 2: Règles de mise à jour de classes

Figure 3: Organisation de la procédure d’acquisition dans le temps

Figure 4: Evolution des classes

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

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.

Acknowledgment
This work is funded by Metropole Européenne de Lille (MEL)

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

Arthur Louchart 1 Philippe Ciblat 1 Charly Poulliat 2

1Institut Polytechnique de Paris / Telecom Paris
2INP-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.

System model

Satellite system

- One uplink single-beam satellite, 
- M users in the beam with FDMA, 
- Perfect satellite-gateway link.

Input-output link

- Users send circularly-symmetric Gaussian symbol sequence (\(a_{mn}\))
- The transmit power of user \(m\) is \(P_m = \mathbb{E} \left[|a_{mn}|^2\right]\) 
- The gateway receives sequence of samples \(z_{mn} = Z_{mi} + jZ_{ni} + a_{mn}\). We want to transmit the power of users \(P = \{P_1, \cdots, P_M\}\).

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

\[
R_m(p) = \log \left(1 + S_m(p)\right)
\]

with

\[
S_m(p) = \frac{P_{NL}^m + P_{NL,NL}^m + m}{P_{NL}^m + 2P_{NL,NL}^m + P_{NL}^m}\]

where

- \(P_{NL}^m = \mathbb{E}[S_m^2]\) is the auto-correlation of the linear part,
- \(P_{NL,NL}^m = \mathbb{E}[S_mS_n]\) is the cross-correlation of the nonlinear part, and
- \(P_{NL,NL}^m = \mathbb{E}[S_m^2S_n]\) 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

\[
m(p) = c_{1}p_1 \cdots c_{d}p_d
\]

where \(c_i \in \mathbb{R}^+\), \(P_x \in \mathbb{R}^+\), and \(a_{mn} \in \mathbb{R}\).

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

\[
p(p) = \sum_{k=1}^{N} m_k(p_1, \cdots, p_d)
\]

where \(m_k \in \mathbb{R}^+\) are monomial functions.

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

\[
m(p) = p(p) - g(p)
\]

where \(p\) and \(g\) are posynomial functions.

- \(P_{NL}^m\) is a monomial, \(P_{NL,NL}^m\) and \(P_{NL,NL}^m\) are posynomials [1],
- \(S_m(p)\) is a ratio of posynomials over signomials.

Problem statement

Goal: Solve the following Problem P1 to obtain the optimal power allocation \(p^*\).

\[
p^* = \arg \max_{p} \sum_{m=1}^{M} R_m(p) \text{ s.t. } 0 \leq P_m \leq P_{max} \forall m
\]

(P1)

Resolution for Signomial Programming

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

\[
p' = \arg \max_{p'} \prod_{m=1}^{M} \left(1 + S_m(p')\right) \text{ s.t. } 0 \leq P_m \leq P_{max} \forall m
\]

(P2)

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

\[
p' = \arg \max_{p'} \prod_{m=1}^{M} t_m \text{ s.t. } 0 \leq P_m \leq P_{max} \forall m
\]

(P3)

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

\[
t_m \left(\frac{P_{NL,NL}^m}{P_{NL}^m + P_{NL}^m}\right) \leq 1 \forall m
\]

(4)

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

\[
p' = \arg \max_{p'} \prod_{m=1}^{M} t_m \text{ s.t. } 0 \leq P_m \leq P_{max} \forall m
\]

(5)

Numerical results

- \(M = 6\) where 2 users have rainy conditions,
- Channel gains are obtained with users location,
- Ideal pre-amplifier \(G_{m0}\) before HPA,
- \(P_{m0} = 50W\), SRRC with roll-off 0.5 for all users.

Data rate expression of user \(m\) for nonlinearity-agnostic receiver: \(R_m = \log \left(1 + \frac{\gamma_m}{P_{m0}}\right)\)

Data rate expression of user \(m\) for AWGN (without nonlinearity): \(C_m = \log \left(1 + \frac{\gamma_m}{P_{m0}}\right)\)

Problem with nonlinearity-aware receiver

- \(p^{\text{up}}\) vs. \(P_{\text{pre}}\) and 1-D search,
- \(P^{\text{pre}}\) proposed algorithm.

In dotted line the solution is evaluated with \(R_m\).

Problem with nonlinearity-agnostic receiver

- \(R^{\text{up}}\) vs. \(P_{\text{pre}}\) and 1-D search,
- \(R^{\text{pre}}\) proposed algorithm.

- Higher sum-rate when the receiver exploits 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 amplifier operates in non-linear regime.

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

References

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

Frequency Planning

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

- **Multi-level 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.

- 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 1-MSFR.

**Algorithm 1: MSFR Algorithm**

1. Run Step 1 to obtain the starting point $a^{(0)}$.
2. Run Step 2 to obtain the optimal cell association and frequency selection $X$ with current $a^{(m)}$ and corresponding $Y^{(m)}$.
3. Set $m = m + 1$.
4. Compute $a^{(m)}(X)$ and $a^{(m)}(X^*)$ at iteration $m$.
5. Run Step 3 to obtain the optimal power control vector $a^{(m)}$ with gain $Y^{(m)}$.
6. Run Step 4 to obtain the optimal $X^{(m)}(a^{(m)})$ with current $a^{(m)}$ and achieve $a^{(m+1)}(X^*)$.

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

Research Perspectives

- To study the potential gains of using SFR in 5G and beyond networks.
- To 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.

Contact: hakima.chaouchi@telecom-sudparis.eu
Réseaux et services du futur
Software-Defined Networking (SDN): Towards Adaptive Distributed SDN Controllers for large-scale networks

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

- **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.

![Figure: Conventional Networking Versus Software-Defined Networking](image)

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

1. Scalability and Reliability aware SDN controller placement strategies → for large-scale IoT-like networks
2. An Adaptive Consistency model A scalable Reconciliation strategy → to meet application SLA needs
3. An Adaptive Consistency model A scalable Replication strategy → Using different ML techniques

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**


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

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.

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.
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.

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

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.

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.

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.

Isogenies between elliptic curves: a toy example

$E: y^2 = x^3 + x$
$E': y^2 = x^3 - 4x$

Isogeny $\phi$ defined on $\mathbb{F}_11$ such that $\phi(x, y) = \left( \frac{x^2 + 1}{x}, \frac{y^2}{x^2} \right)$

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.

Introduction

- Physical attacks are particularly effective threats to strike confidentiality, integrity or authenticity of systems.
- Several protections have been proposed such as:
  - Software-based Control Flow Integrity (CFI),
  - Hardware-based monitoring of the control-flow or code integrity (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.

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.

Use Case: Pin Code Verification

- Its function is to compare a user pin to the correct one for authentication.
- 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.

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 executed 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
Contexte et Objectifs

Mieux vivre chez soi

► Viellissement de la population Assister les personnes en perte de dépendance

► Des services Adapter et personnaliser intelligemment des services domotiques

Méthode

Des capteurs aux activités

Résultats

► 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 reconnaissance des AVQ

► Modèle du langage construit une représentation contextualisée robuste pour le transfert de connaissances
Software Defined Network approach for IoT technologies

When SDN meets IoT

A new network behavior

► Routing, scheduling and resource allocation are 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

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 developed in current SDN for IoT approaches

My research on software-defined IoT networks

Research axis on SDN for IoT

- Conditional rules enable adaptability
- Multi-path centralized routing
- Programmable MAC layer?
- PCE, PSE and statefulness
- Towards SDR enabling

Controller discovery included with TSC association

Architecture proposal

Controller Implementation

Contact: amaury.bruniaux@imt-atlantique.fr
Disaster Protection in Inter-DataCenter Networks leveraging Cooperative Storage

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**

**Cooperative Disaster Protection leveraging CSS**
- 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.

Simulations and numerical results

**Performance on spectrum utilization and storage space**
- 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

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

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].

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

Contact: victor.charpenay@emse.fr
MRAM/CMOS Hybridization to Secure LWC Algorithms

**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 address 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

**LWC Algorithms Use Cases**
- Multiple implementations of these two LWC algorithms
- **PRESENT**: a Block Cipher
- **ASCON**: an Authenticated Encryption with Associated Data (AEAD)

**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 pre-detection-based countermeasures
  - Could be a threat for CMOS/MRAM circuits?

---

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

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 chaîne (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 protocole.

► Confidencialité et intégrité des informations transitant sur les réseaux optiques partagés
- Analyse de la sécurité physique du réseau optique
- Observation directe de la lumière présente sur la fibre
- Analyse des composants actifs de l’infrastructure

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

Smart Agriculture Use Case
► Automatic irrigation based on weather station
► Field access management for robots
► Crop phenological stage detection
Multi-Hop Network with Multiple Decision Centers under Expected-Rate Constraints

System Model and Description

**Binary Hypothesis Testing against Independence**
- Normal Situation: Correlated Measurements
  \[ H = 0 : X^n, Y^n, Z^n \text{ i.i.d.} \sim P_X \cdot P_Y \cdot P_Z \]
- Alert Situation: Independent Measurements
  \[ H = 1 : X^n, Y^n, Z^n \text{ i.i.d.} \sim P_X \cdot P_Y \cdot P_Z \]
- Goal: To guess correctly the joint distribution
  \[ M_1 = \phi_1^n(X^n), \tilde{H}_Y = g_1^n(M_1, Y^n) \]
  \[ M_2 = \phi_2^n(M_1, Y^n), \tilde{H}_Z = g_2^n(M_1, Z^n) \]

**Types of Errors**
- False Alarm
  \[ \alpha_{1,n} = \Pr[\tilde{H}_Y = 1 | H = 0] \]
- Missed Detection
  \[ \alpha_{2,n} = \Pr[\tilde{H}_Z = 1 | H = 0] \]

**Exponents Region**
\[ E(R_1, R_2, \epsilon_1, \epsilon_2) \]
- Closure of the set of all \((\epsilon_1, \epsilon_2)\)-achievable \((\theta_1, \theta_2)\) s.t.
  \[ \exists (\phi_1^n, \phi_2^n) \] satisfying \(\forall j \in \{1, 2\}\) the rate constraints,
  \[ \lim_{n \to \infty} \alpha_{j,n} \leq \epsilon_j \] and \[ \lim_{n \to \infty} \beta_{j,n} \approx 2^{-n \theta_j} \]

**Main Results**
- Maximum Rate Constraints \((\text{len}(M_j)) \leq n R_j)\)

**Theorem [Hamad, Wigger, Sarkiss‘2021]**
\[ E(R_1, R_2; \epsilon_1, \epsilon_2) \text{ is the set of all } (\theta_1, \theta_2) \text{ pairs satisfying} \]
\[ \theta_1 \leq \min(\eta_{XY}(R_{11}), \eta_{XY}(R_{12})) \],
\[ \theta_2 \leq \min(\eta_{XY}(R_{21}) + \epsilon_{1,2}, \eta_{XY}(R_{22}) + \eta_{XY}(R_{12}) + \eta_{XY}(R_{23})) \]
for some \(\epsilon \in [1 - \epsilon_1 - \epsilon_2, 1 - \max(\epsilon_1, \epsilon_2)]\) and nonnegative rates \(R_{11}, R_{12}, R_{13}, R_{22}, R_{23}\) satisfying
\[ R_1 \geq (1 - \epsilon_1 - \sigma)R_{11} + \sigma R_{12} + (1 - \epsilon_2 - \sigma)R_{13}, \]
\[ R_2 \geq \sigma R_{22} + (1 - \epsilon_2 - \epsilon_1)\sigma R_{23}. \]

**Tradeoff between the Exponents when \(\epsilon_1 \neq \epsilon_2\)**
- **Simplifying Exponents Region and Coding Schemes**
  - \(\epsilon_1 = \epsilon_2\): One exponent term at each decision center
  - \(\epsilon_1 \leq \epsilon_2\): 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
A framework for joint admission control, resource allocation and pricing for network slicing in 5G

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


Contact : tijani.chahed@telecom-sudparis.eu
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), RedeM Communications (UK), Colombia University (USA), The University of Tokyo (Japan), Orange Labs (France), IMT (France), Fraunhofer 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.

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

Access technologies
- Intelligent surfaces
- Terahertz broadband
- Non-terrestrial networks
- RAN disaggregation

Network technologies
- Next-generation IP framework
- In-network computing
- Multi-domain service delivery and edge compute
- Post-Shannon transport

Society needs and attempts
- Cyber and physical space continuum
- New business models for digital sustainability
- Renewed standardization framework and civil society involvement

Management and operation
- Federated data layer
- In-network AI and ML computing and actuating

Contact: noel.crespi@mines-telecom.fr
Blockchain based trust management mechanism for Industry 4.0

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.

Blockchain based trust system

What blockchain means for Industry 4.0?

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

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**

### Network slicing concept

- **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 bandwidth capacity \( BW_{ij} \)
- **Slices** modeled as graphs \( H^x(V, E^x) \) for \( x \)th slice
  - Each node \( v_i \in V^x \) has CPU demand \( CPU^x_i \)
  - Each edge \( (v_i, v_j) \in E^x \) has bandwidth capacity \( BW^x_{ij} \)
- **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.

### Used method : Nested rollout policy adaptation

- **Monte Carlo Algorithm** for a given slice \( H^* \), 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 \( \sum_{v_i \in V} w_{r_i} CPU_i \) and \( \sum_{v_i \in V} w_{r_i} CPU_i \) are resources used by slice \( H^* \) 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

### 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

---

[2] Improved Monte Carlo Tree Search for Virtual Network Embedding, Elkael, Castill-Taleb, Jouaber, Ait Aba, 2021
A two-stage algorithm for the Virtual Network Embedding problem

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 run 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

**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 $e_{ij} \in E$ is weighted by a maximum bandwidth amount
- **Slice:** represented by a graph $H(V^s, E^s)$
  - Each node $v_j \in V^s$ is weighted by a computational power demand
  - Each edge $e_{ij} \in E^s$ 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 paths**

- **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

**Example**

- Two virtual network (slice) requests
  - First embedding solution
  - Second embedding solution

**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

**Simulations on randomly generated benchmarks**

**Numerical results**

- Compare the performance of the proposed method using widest and shortest paths (with $k \in \{1,2,3\}$) to MaVeS-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

**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

---

Context

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.

<table>
<thead>
<tr>
<th>AR requirements</th>
<th>Latency (ms)</th>
<th>Example of application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Responsiveness</td>
<td>500</td>
<td>Decoration applications</td>
</tr>
<tr>
<td>Mid Responsiveness</td>
<td>100</td>
<td>Photography and Editing</td>
</tr>
<tr>
<td>High Responsiveness</td>
<td>16</td>
<td>AR Maintenance</td>
</tr>
</tbody>
</table>

Research Question

► Can we deploy Augmented Reality using only Edge Embedded Devices?

Methodology

Measurements on real devices

► COCO Dataset

\[ R = \{100 \times 100, 200 \times 200, 300 \times 300, 600 \times 600, 1000 \times 1000\} \]

► Single Shot Detector + MobileNet v2

► Higher resolution, higher accuracy, same inference time.

Theoretical Model

\[ L_n = L_n^w + L_n^p \]

► \( L_n^w \) 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

\[ L_n^w = \sigma \cdot s_n^2 \cdot N \]

\[ L_n^p = \frac{c_k \cdot N}{R} \]

► \( \sigma \) is the number of bits/pixel

► \( s_n^2 \) 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
Edge Cloud, 5G, Deterministic Networking and Data Quality for Critical Applications

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

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, …)

Edge Cloud and real time communication for Critical applications

Constrained decision making: Drone, autonomous vehicle usecase

► 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 guarantee.
A Scalable GraphQL Northbound API for Intent-based SDN Applications

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.

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.

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.
Réseaux denses et à très faible consommation
Gestion dynamique d’un champ de capteurs pour allonger le temps de surveillance

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

Définition du problème étudié

On veut gérer dynamiquement les émissions de capteurs de façon à recevoir des informations périodiquement à chaque pas de temps \( \tau \), 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.

Algorithme de planification périodique = algorithme qui modifie les périodes d’émissions de capteurs entrants dynamiquement dans le SI de sorte que : il existe \( l \in \mathbb{N} \), 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 \( \forall i \in [1,M-1], |t_{i+1} - t_i| > \tau \times i \), alors le nombre de changements de période total imposé par l’algorithme de planification périodique pour \( n \) capteurs est \( M(M-1) + 2n - 1 \).

Prise en compte de nouvelles perturbations

- Des capteurs peuvent disparaître 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 :

Contact : gwen.maudet@imt-atlantique.fr
Energy-efficient transceivers for Sat-IoT applications

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”

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
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:

\[ r(t) = \sum_{i=1}^{N_i} \sum_{j=1}^{M_j} h_{ij} s_{ij}(t) + n(t) \]

- Co-SF interference
- Number of interfering users \( N_i \) follow a Poisson distribution with parameter \( \lambda \).
- \( x \)-coordinates of the interfering users are uniformly distributed.

IV. Proposed Receivers

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

V. Simulation Result 1

Varying number of interfering users

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

VI. 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.
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 be deployed to operate as a fully autonomous system with no need for third-party services or access.

**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 deploy 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**
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
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

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.

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 (Échanges d’informations, coopératifs, IA embarqué, traitement de données massives)

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

► LPWAN stands for “Low Power Wide Area Network”, 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

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.
  - Analyse OTAA mechanism by extracting the Join-Request Message, Join-Accept Message and the messages 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

► 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
Motivation

Conventional approach:

Joint approach:

Feasible Region

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

\[
R_1 + R_2 \leq I(U_0; U_1; V_1 | S_1) - I(U_0; U_1; Z; V_0; V_1; S_2; Y_1),
\]

\[
R_1 \leq I(U_0; Y_1; V_1 | S_1) + I(U_2; Y_2; V_2 | U_0; S_2)
\]

and

\[
\mathbb{E}[d_k(S_k, \hat{S}_k(X, Z))] \leq D_k
\]

for some

\[
P_{U_0|U_1}P_{X|U_0,U_1}P_{S_1,S_2}P_{Y_1,Y_2,Z|S_1,S_2}P_{U_0|V_0}P_{U_2|U_1,V_2,Z}P_{V_0|S_2,Y_2}
\]

where

\[
s_k^*(x, z) \triangleq \min_{y \in S_k} \sum_{x \in S_x} P_{S_k}(x) d_k(s_k(x), s_k(z))
\]

Example: Two receivers

\[
Y = S = X = (0, 1)
\]

Flipped Input

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

Non-Flipped Input

\[
Y_k = S_k X, \quad k \in \{1, 2\}, \quad Z = (Y_1, Y_2)
\]

Achievable Region Boundary

Feasible capacity-distortions region

Infeasible capacity-distortions region

Proposed joint scheme outperforms the conventional scheme

References

Software and Hardware approaches for Efficient IoT application lifecycle management

A bottom-Up Device Heterogeneity control

An open source IoT framework www.priot.org

Software based Approach for IoT application development, deployment 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, deployment and maintenance) – IoT Device heterogeneity Abstraction layer

**4 Layer IoT Architecture for Invariant Functionalities and Programming Patterns**

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

P-Bus: A Power Bus 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

**R-Bus System Design Concept**

1. R-Bus, we define a modular architecture to improve performance and manageability.
2. The position is based on the concept of bus architecture.
3. To expose modularity at all layers and to enable the specification of power management at the power bus level.

**P-Bus Interface**

- Energy efficient management features
- Power Bus Interface
- Power Bus Command
- Power Bus Interface with external boards

**Contact**: hakima.chaouchi@telecom-sudparis.eu
Blockchain based trust management mechanism for Industry 4.0

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.

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.

Blockchain based trust system

What blockchain means for Industry 4.0 ?

<table>
<thead>
<tr>
<th>Structural features</th>
<th>What it means for smart factories</th>
<th>What it means for smart health</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology for</td>
<td>Like production data, the origin of goods, including machines, manufacturers, suppliers, customers...</td>
<td>Like patients records, prescription medicines, medical devices trust, including patients, doctors, medical centers, smart cities...</td>
</tr>
<tr>
<td>...which allows for multiple parties...</td>
<td>Traceability of goods from suppliers to machines...</td>
<td>Keeping a complete...</td>
</tr>
<tr>
<td>...whose data is notarized, secure, verified thus trusted...</td>
<td>Allowed parties have access to data around a product, another entity.</td>
<td>Allowed parties have access to data around patients...</td>
</tr>
<tr>
<td>...forming a public record visible to all</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What is the Blockchain technology?

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