

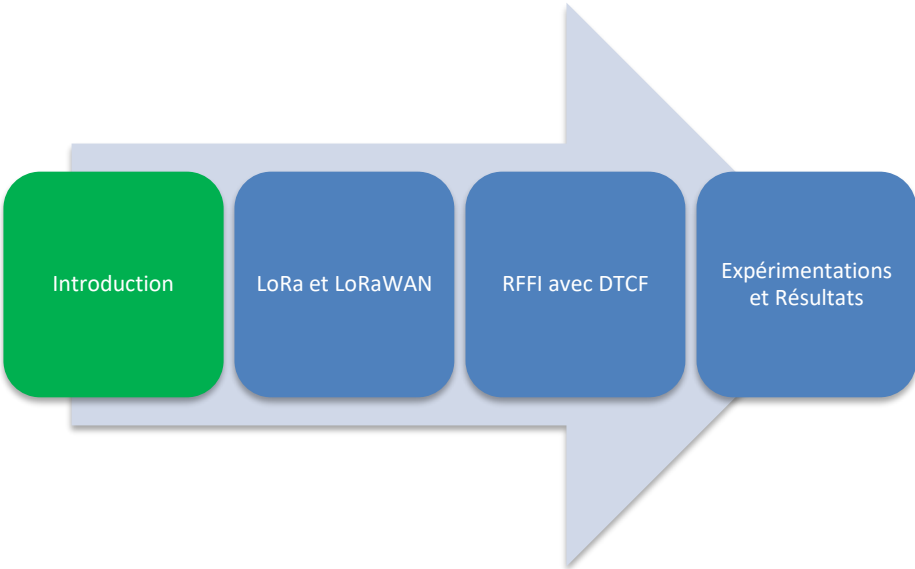
# Identifier des nœuds IoT en espionnant leur signal radio

Arnaud Tulippe-Hecq

Directeur : Professeur Bruno Quoitin

Département d'Informatique  
Faculté des Sciences  
Université de Mons

26 juin 2024



Introduction

IoT et LoRaWAN

LoRa et RFFI

Expérimentations  
et Résultats

## Contexte :

- Expansion de l'Internet of Things (IoT)
- Menaces de failles de sécurité de plus en plus sophistiquées
- Plus possible d'uniquement se fier aux identifiant d'un appareil
- Nécessité d'une nouvelle approche basée sur les propriétés physiques des signaux RF.

## Objectif :

- Analyser les propriétés physiques du signal radio d'un nœud utilisant la technologie LoRa via une méthode de RFFI



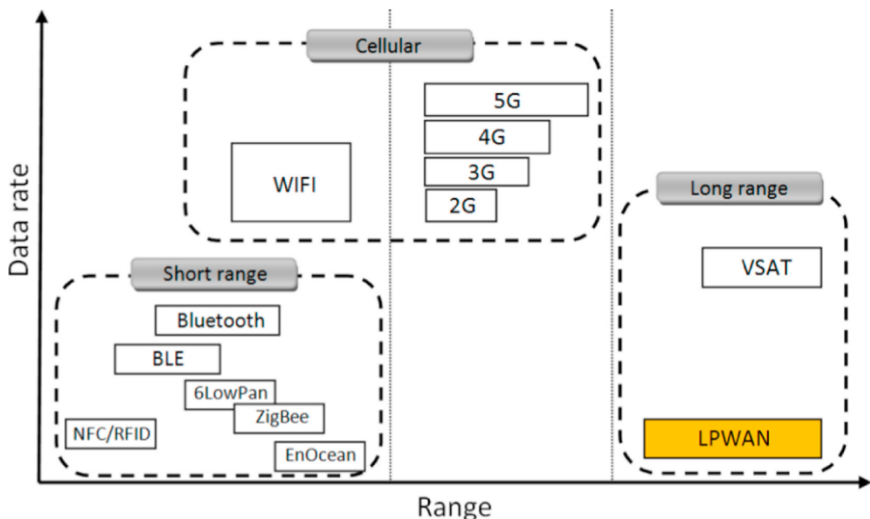
Introduction

IoT et LoRaWAN

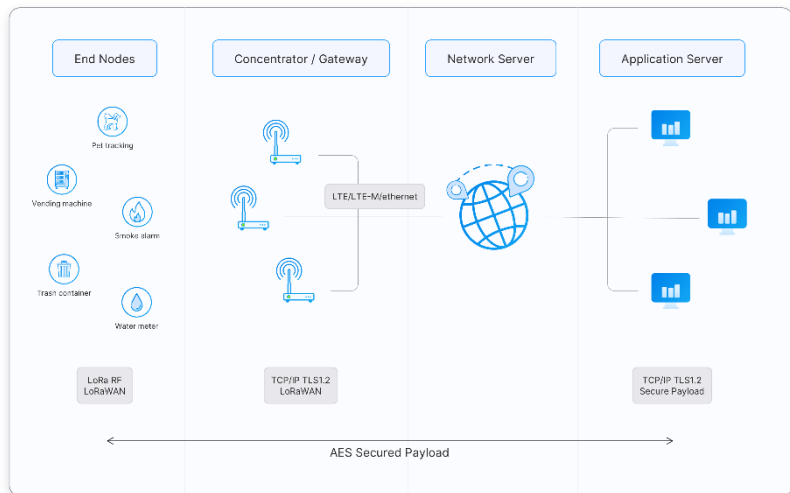
LoRa et RFFI

Expérimentations  
et Résultats

# Spectre des technologies sans fil[1]



# Architecture de LoRaWAN[2]



# Session LoRaWAN

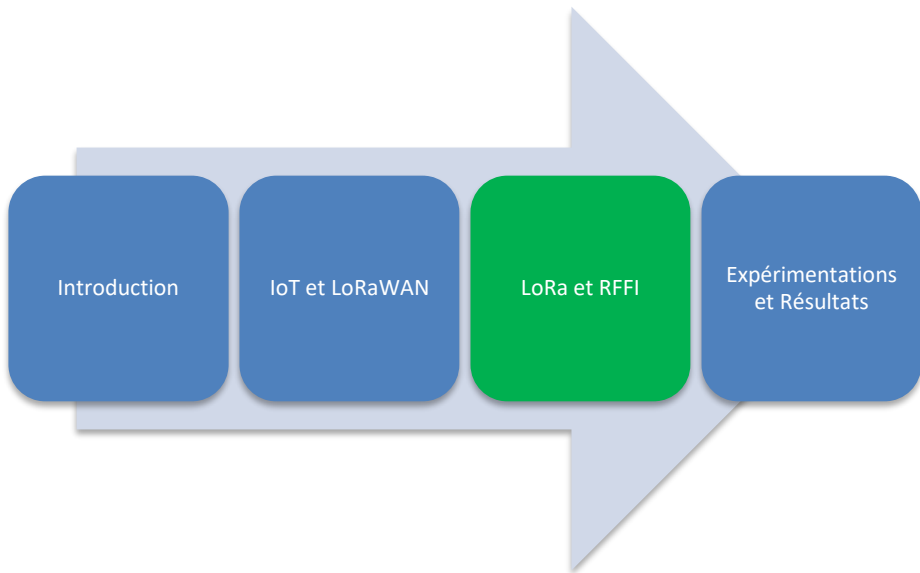
## Over the Air Activation

- Join request (DevEUI, appEUI, code MIC)
- Join accept (DevNonce, NwkSKEY, appSKEY)
- Chiffrement AES

## Activation by Personalisation

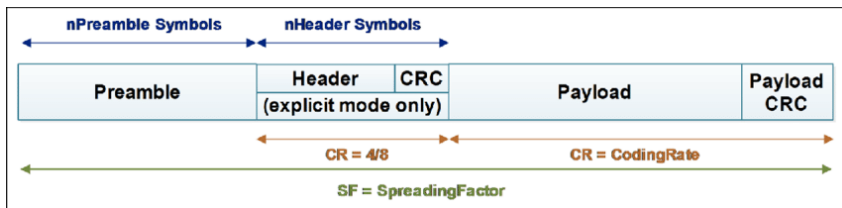
- Adresses et clés hardcodées
- Devices déployés en zone de couverture LoRaWAN
- Pas de join request, ni join accept





## LoRa (Long Range) :

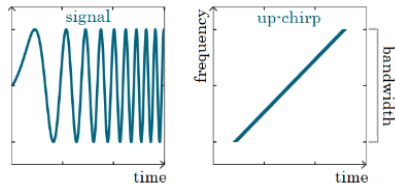
- Technologie LPWAN
- Opère sur la bande ISM (433-868 MHz)
- Modulation FSCM



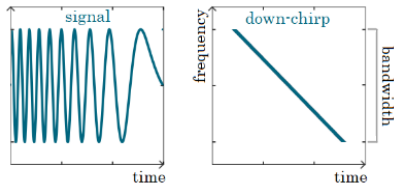
Structure d'un paquet LoRa[3]

## Modulation LoRa:

- Mixe entre CSS et FSK
- Dépend de  $\beta$  et SF
- Contient  $2^{SF}$  symboles
- Représentation fréquentielle sous forme de chirps



Upchirp



Downchirp[4]

## Radio Frequency Fingerprinting Identification (RFFI)

- Différentes techniques
- Propriétés physiques des signaux RF
  - *En particulier, les offsets de fréquences entre les différents émetteurs et le récepteur commun*

Jiang et al. EURASIP Journal on Wireless Communications and Networking (2019) 2019:225  
<https://doi.org/10.1186/s13638-019-1542-z>

EURASIP Journal on Wireless Communications and Networking

### RESEARCH

### Open Access

## Physical layer identification of LoRa devices using constellation trace figure

Yu Jiang<sup>1\*</sup>, Linning Peng<sup>1</sup>, Aiqun Hu<sup>1</sup>, Sheng Wang<sup>1</sup>, Yi Huang<sup>1,2</sup> and Lu Zhang<sup>3</sup>



### Abstract

LoRa wireless technology is a revolutionary wireless network access technology with a wide application prospect. An identification method for LoRa devices based on physical layer fingerprinting is proposed to provide identities for authentication. Contrary to previous works, a differential constellation trace figure is established from the radio frequency (RF) fingerprinting features of LoRa devices, which transforms the feature matching to the image recognition. A classification method based on Euclidean distance of clustering center of LoRa signal is performed to analyze the differential constellation trace figure. The experimental results show that six LoRa transmission modules can be recognized accurately, and even in a low signal-to-noise ratio (SNR) environment, the different LoRa devices can still be distinguished and identified effectively.

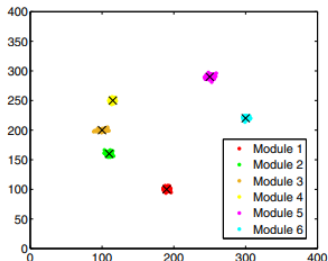
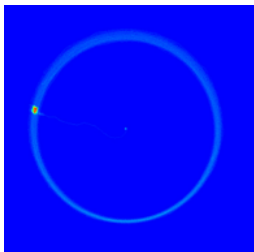
**Keywords:** Internet of Things, LoRa, RF fingerprinting, Wireless identification, Constellation trace figure

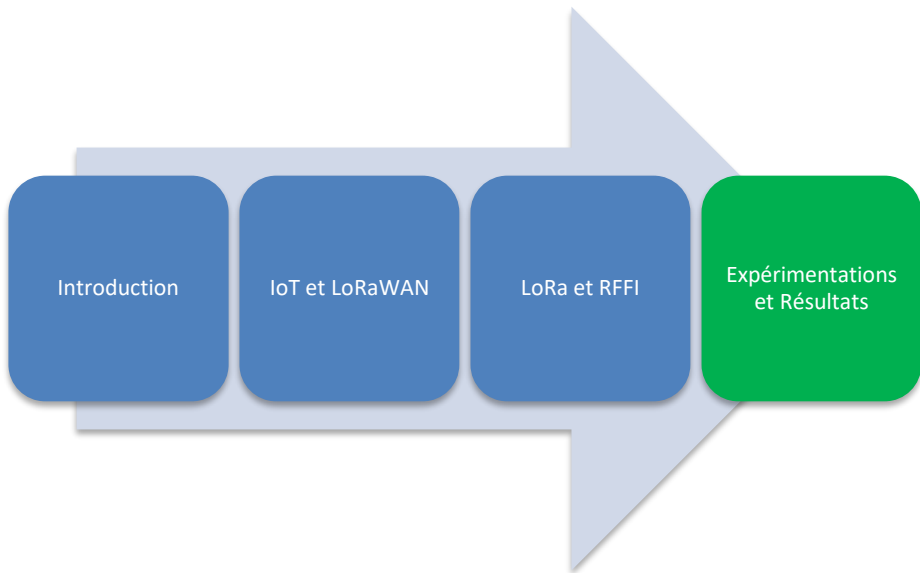
## Article de référence

Par Yu Jiang, Linning Peng, Aiqun Hu, Sheng Wang, Yi Huang et Lu Zhang [5]

## Méthode des DCTFs:

- Récupération des échantillons I/Q du signal modulé
- Application d'une équation différentielle
- Plot des données dans le plan complexe
- Récupération du centre de la signature





# Matériel

## Emetteurs

Module RN2483



## Récepteur

RTL-SDR R820T2



# Configuration

## Émetteur/récepteur:

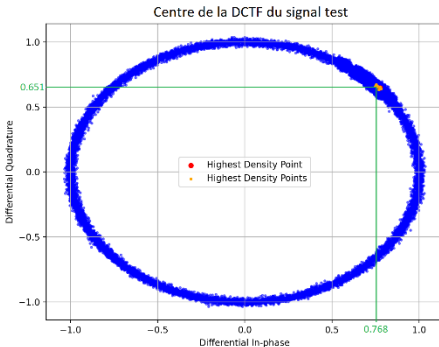
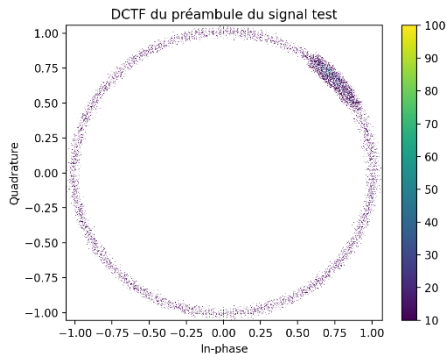
- Fréquence
- Modulation
- Spreading factor
- Largeur de bande
- Puissance
- Coding rate
- Sample rate
- Gain

## Développement Python:

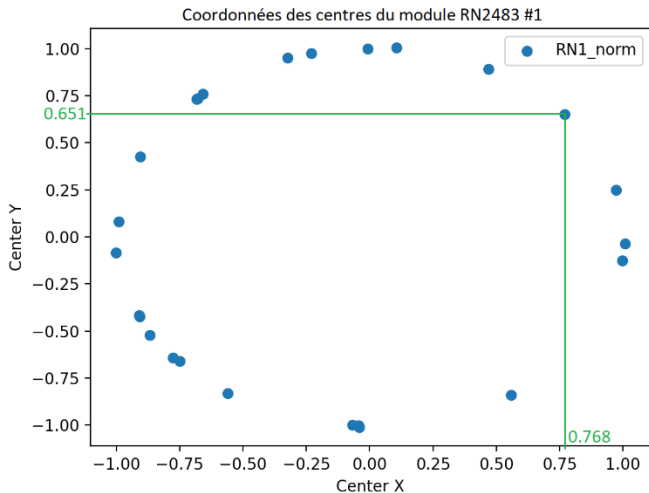
- Génération du signal
- Réception du signal
- Automatisation
- Digital Signal Processing
- Génération des diagrammes
- Application de la méthode DCTF



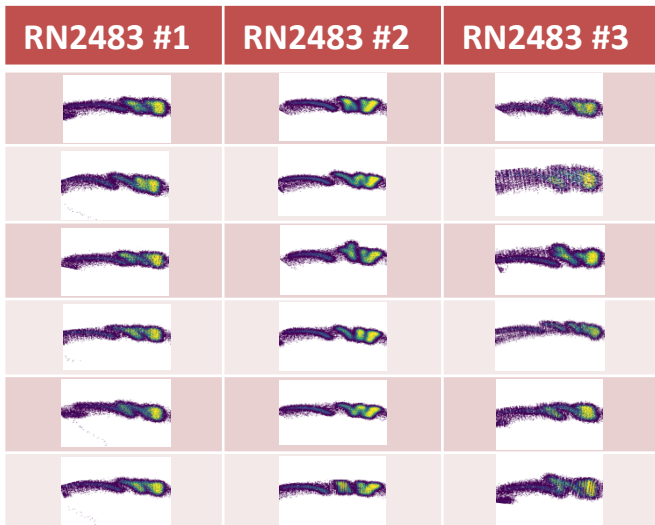
# Résultats pour la capture d'un signal LoRa



# Centres des signatures (25 captures)



# Analyse de la forme géométrique de la signature



## Conclusion

- L'identification des nœuds via le traitement de leur signature RF (RFFI) possible
- Les résultats suggèrent une identification selon la forme géométrique spécifique de la signature

## Références

- [1] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT express, 5(1) :1–7, 2019
- [2] <https://www.thethingsnetwork.org/docs/lorawan/architecture/>
- [3] E. Gambi, L. Montanini, D. Pigni, G. Ciattaglia, and S. Spinsante. A home automation architecture based on LoRa technology and Message Queue Telemetry Transfer protocol. International Journal of Distributed Sensor Networks, 14 :155014771880683, 10 2018.
- [4] <https://blog.ttulka.com/lora-spreading-factor-explained/>
- [5] X. Wu, Y. Jiang, and A. Hu. Lora Devices Identification Based on Differential Constellation Trace Figure. In Artificial Intelligence and Security : 6th International Conference, ICAIS 2020, Hohhot, China, July 17–20, 2020, Proceedings, Part I 6, pages 658–669. Springer, 2020.