

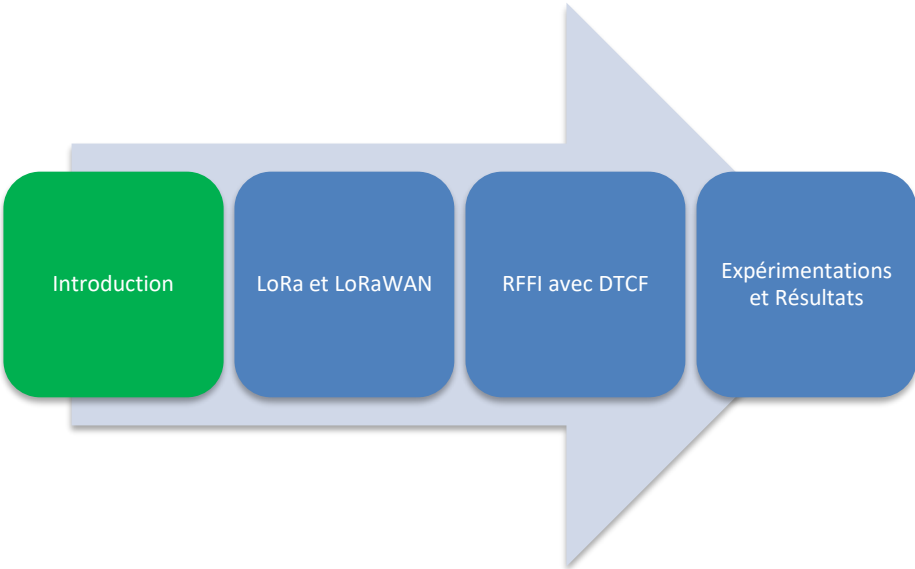
# Identifier des nœuds IoT en espionnant leur signal radio

Arnaud Tulippe-Hecq

Directeur : Professeur Bruno Quoitin

Département d'Informatique  
Faculté des Sciences  
Université de Mons

27 juin 2024



Introduction

LoRa et LoRaWAN

RFFI avec DTCF

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 identifiants d'un appareil
- Nécessité d'une nouvelle approche basée sur les propriétés physiques des signaux RF.

## Objectifs

- Analyser la technologie LoRa, en particulier sa modulation
- Analyser les propriétés physiques du signal radio d'un nœud via une méthode de RFFI

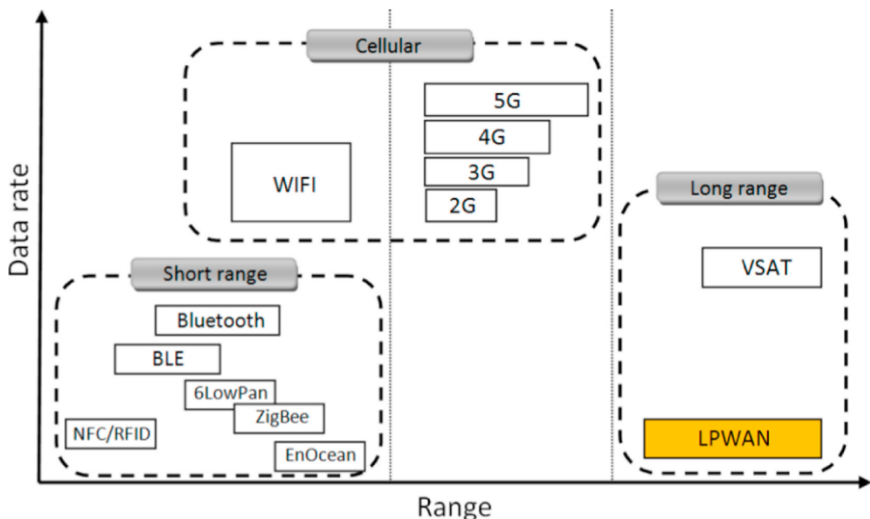


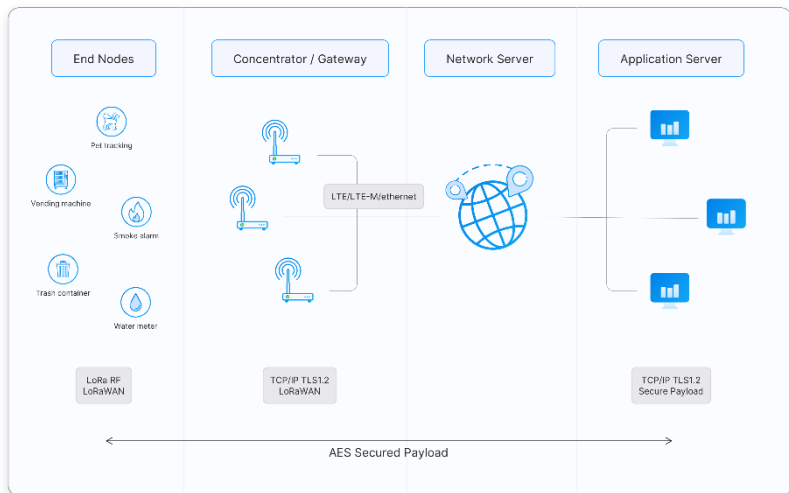
Introduction

LoRa et LoRaWAN

RFFI avec DTCF

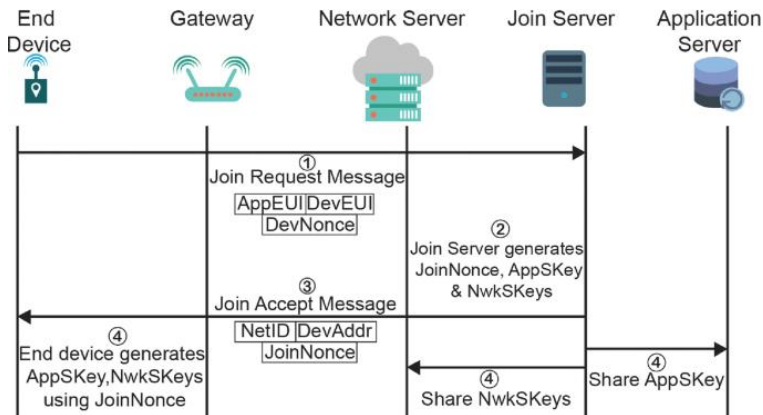
Expérimentations  
et Résultats

Spectre des technologies sans fil<sup>[1]</sup>

Architecture de LoRaWAN<sup>[2]</sup>

# Session LoRaWAN

## Over the Air Activation<sup>[3]</sup>





# Session LoRaWAN

## Activation by Personalization

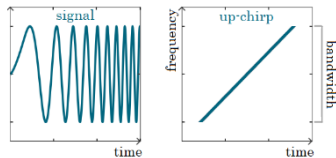
- Adresses et clés hardcodées
- Devices déployés en zone de couverture LoRaWAN
- Pas de join request, ni join accept
- Moins sécuritaire, plus rapide

## LoRa (Long Range)

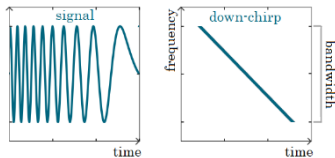
- Couche physique brevetée
- Technologie LPWAN
- Opère sur la bande Industrial Scientific & Medical (ISM, 433-**868** MHz)
- Modulation Frequency Shift Chirp (FSCM)

## Modulation LoRa

- Combinaison entre Chirp Spread Spectrum (CSS) et Frequency Shift Keying (FSK)
- Dépend de la largeur de bande ( $\beta$ ) et du Spreading Factor (SF)
- $2^{SF}$  symboles
- Représentation fréquentielle sous forme de chirps

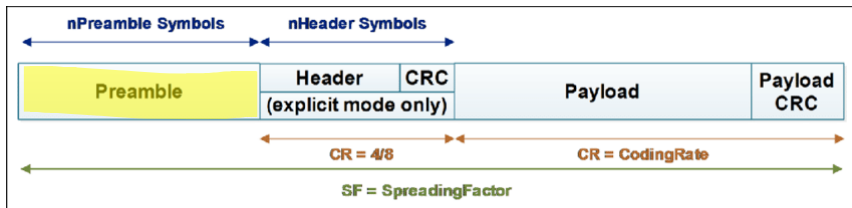


Upchirp

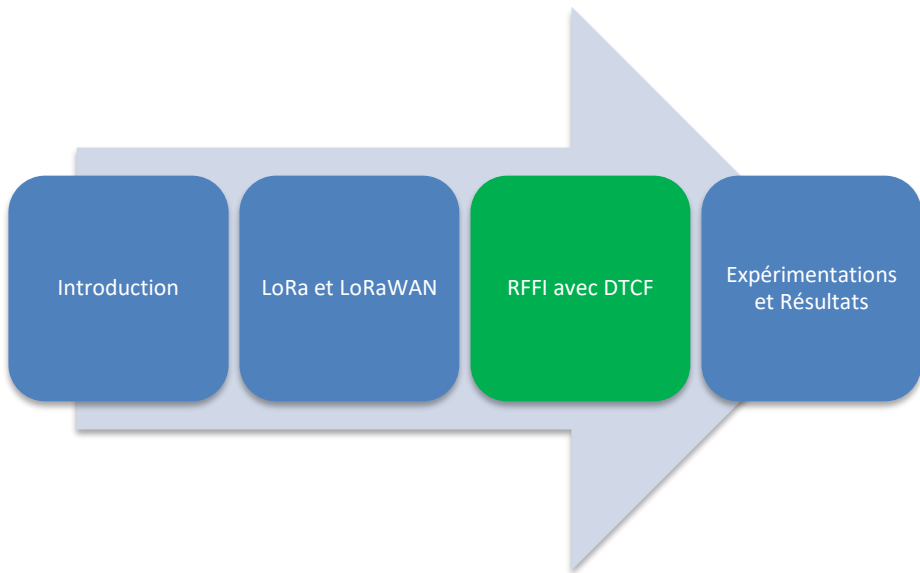


Downchirp<sup>[4]</sup>

## Structure l'un paquet LoRa<sup>[5]</sup>



Preamble (12,25 chirps)



# Radio Frequency Fingerprinting Identification (RFFI)

- Différentes techniques
- Propriétés physiques des signaux RF

Jiang et al. EURASIP Journal on Wireless Communications and Networking (2019) 2019:223  
<https://doi.org/10.1186/s13638-019-1542-x>

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.

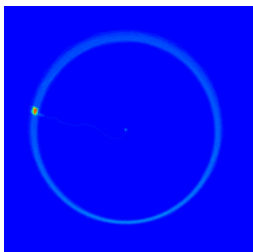
**Keywords:** Internet of Things, LoRa, RF fingerprinting, Wireless identification, Constellation trace figure

## Article de référence

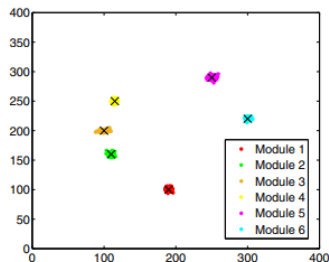
Par Yu Jiang, Linning Peng, Aiqun Hu, Sheng Wang, Yi Huang et Lu Zhang [6]

## Méthode des DCTFs

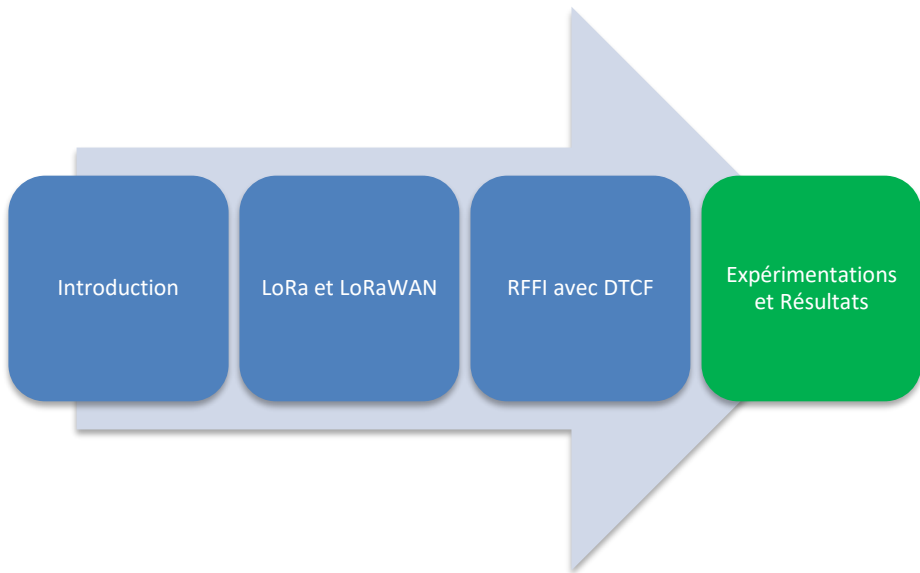
- Récupération des échantillons I/Q du signal modulé
- Traitement différentiel des données
- Plots des données dans le plan complexe
- Récupération du centre de la signature



Trace d'un device



Centre de différents devices

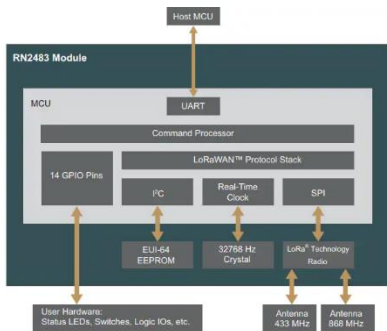




# Matériel

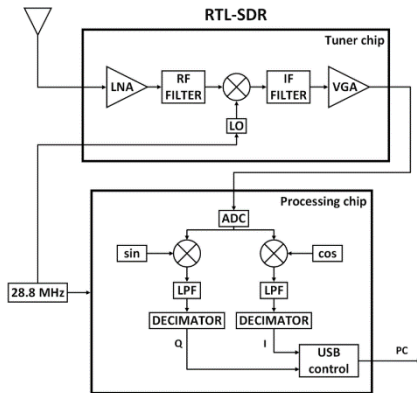
## Emetteur

### Module RN2483<sup>[7]</sup>

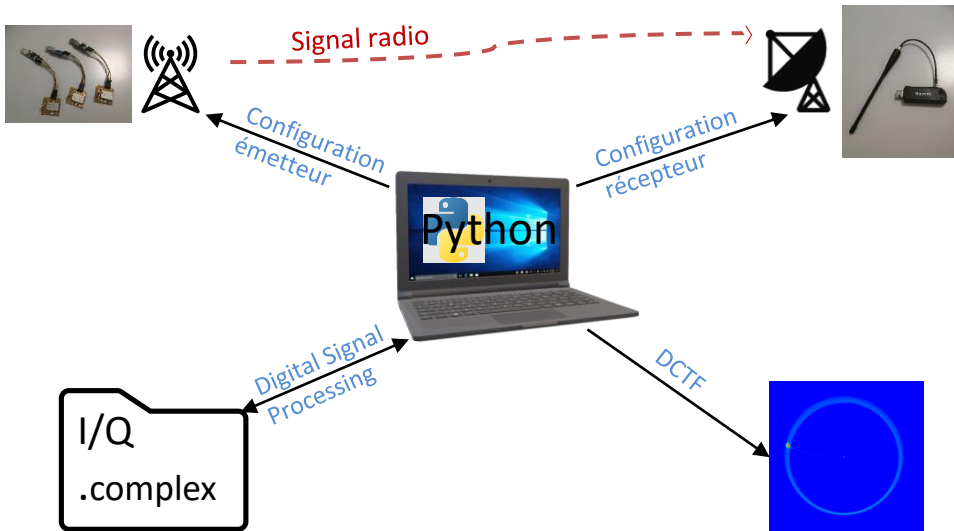


## Récepteur

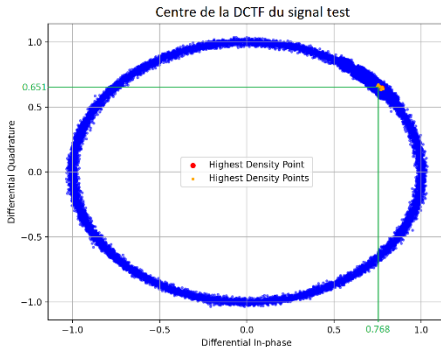
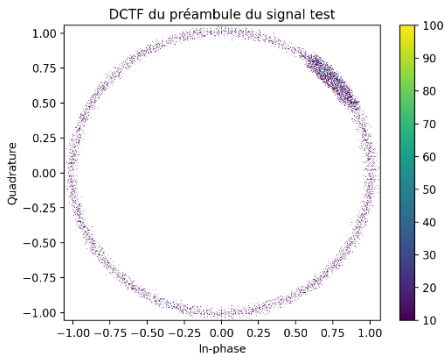
### RTL-SDR R820T2<sup>[8]</sup>



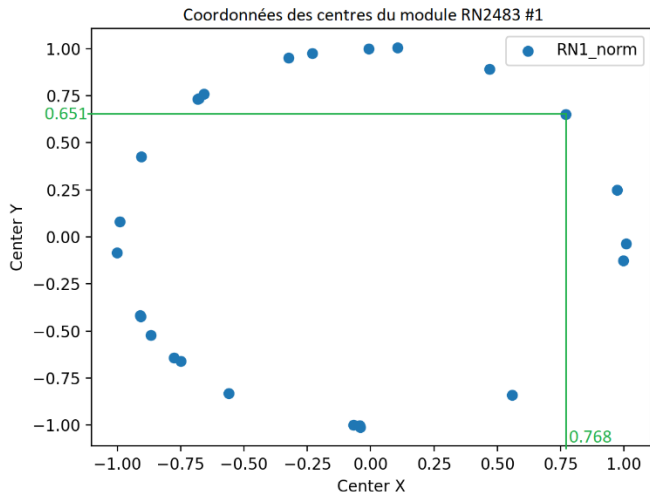
# Configuration de l'expérimentation



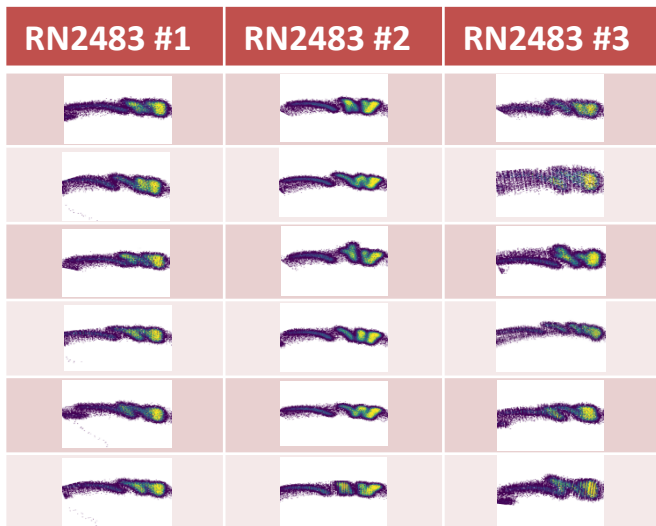
# Résultats pour la capture d'un signal LoRa



# Centres des signatures (25 captures)



# Analyse de la forme géométrique de la signature



## Conclusion

- L'identification des nœuds LoRa via le traitement de leur signature RF (RFFI) non fonctionnelle selon l'article
- Les résultats suggèrent une identification selon la forme géométrique spécifique de la signature
- Approches de deep-learning possibles
- Apports personnels :
  - ✓ Reproduction travail scientifique existant
  - ✓ Choix justifié des équipements
  - ✓ Développement DSP

# 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] Danish, Syed Muhammad, Marios Lestas, Hassaan Khaliq Qureshi, Kaiwen Zhang, Waqar Asif, and Muttukrishnan Rajarajan. "Securing the LoRaWAN join procedure using blockchains." *Cluster Computing* 23 (2020): 2123-2138.
- [4] <https://blog.ttulka.com/lora-spreading-factor-explained/>
- [5] E. Gambi, L. Montanini, D. Pignini, 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.
- [6] 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.
- [7] <https://www.mouser.be/new/microchip/microchip-rn2483-module/>
- [8] N. BniLam, D. Joosens, J. Steckel, and M. Weyn. Low cost AoA unit for IoT applications. In *2019 13th European Conference on Antennas and Propagation (EuCAP)*, pages 1–5. IEEE, 2019