Séminaire Ferroviaire
29 septembre 2022

Virginie DENIAU et Christophe GRANSART

N. Becuwe, F. Valenti A. Nogueira, E. Simon, T. Vantroys, A. Boe, J. Villain, N. Chopinet

Comment sécuriser les communications entre objets ferroviaires connectés ? Réflexions à partir des travaux du projet LoRa-R

Université Gustave Eiffel

Plan

- **Présentation générale du projet LoRa-R**
- **Le LoRa/LoRaWan pour la SNCF**
- **Les menaces étudiées : Interférences EM intentionnelles et non intentionnelles**
- **Mise en œuvre d'une méthodologie d'évaluation**
- **Quelques résultats**
- **Conclusions**

Présentation générale du projet LoRa-R

- **Sécuriser les communications en LoRa des objets connectés ferroviaires face aux risques d'interférences électromagnétiques (EM) et de cyber attaques**
  - Programme Stimule Partenarial
  - Université Gustave Eiffel, IRCICA et SNCF
  - Etudier la susceptibilité des communications LoRa/LoRaWan
    - Face à des interférences EM propres à l'environnement ferroviaire
    - Face à du brouillage intentionnel

LoRa-R

574 INDUSTRIEL Hellemmes

Université Gustave Eiffel

IRCICA

SNCF

Projet soutenu financièrement par la région Hauts-de-France

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE

Région Hauts-de-France

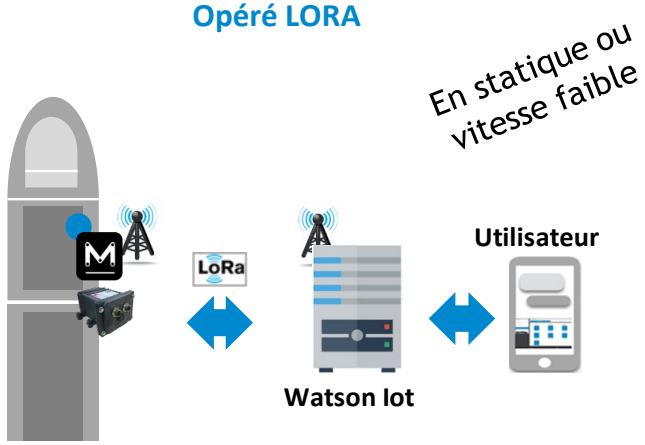
l'Europe s'engage en Hauts-de-France avec le FEDER

Le LoRa/LoRaWan pour la SNCF

- **La transformation digitale de la SNCF**
- **Le passage d'une maintenance préventive à une maintenance prédictive**
- **MARTI-MELI : les capteurs communicants de la SNCF**

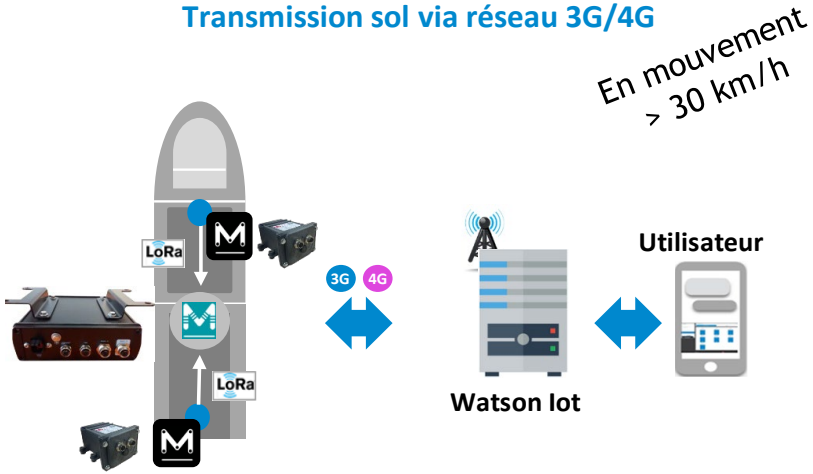
MARTI: Module Agile de Réception et Transmission d'Information *basé sur du LoRa (Long Range)*
MELI: Passerelle LoRa / 4G

Envoi des données bord vers sol sur le réseau Opéré LORA



Acquisition Données
X nb MARTI vers le Sol

Envoi des données bord à la passerelle Transmission sol via réseau 3G/4G

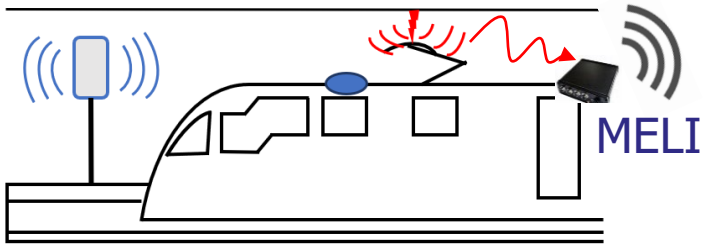


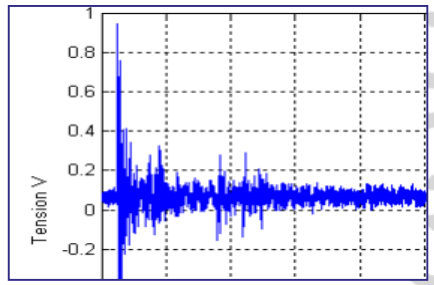
Acquisition Données
X MARTI vers 1 MELI

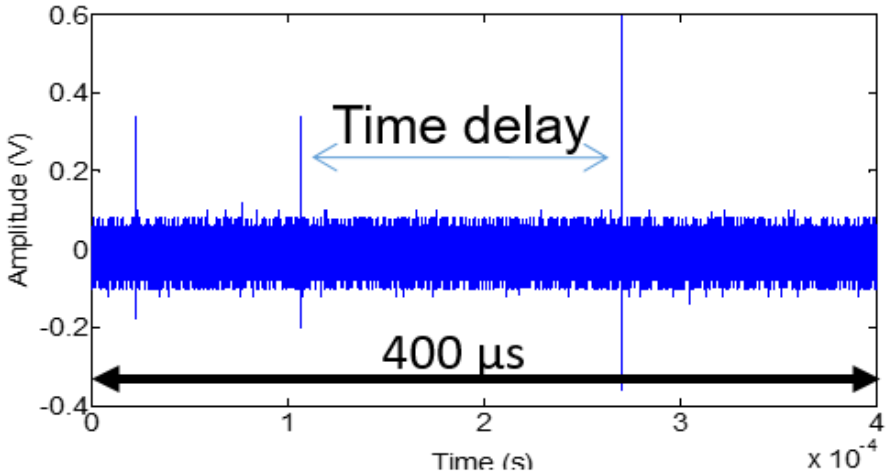
Menaces étudiées

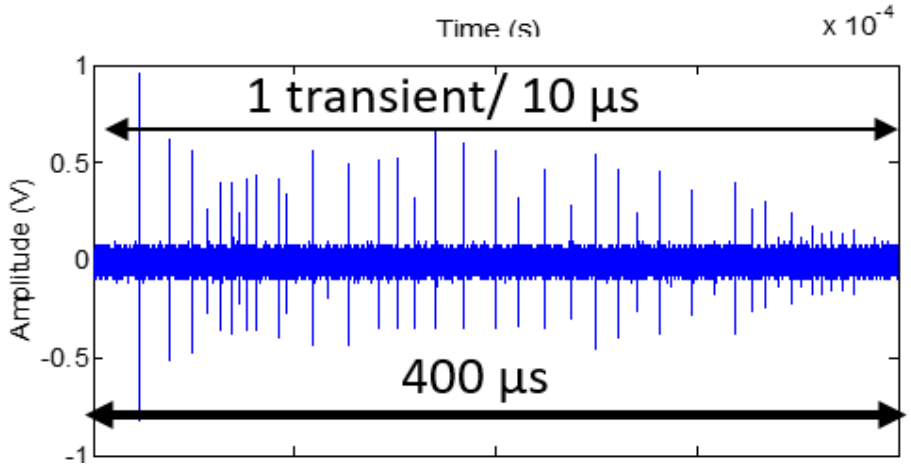
- **Interférences EM non intentionnelles**

Signaux EM transitoires liés aux pertes de contact caténaire-pantographe









Université Gustave Eiffel

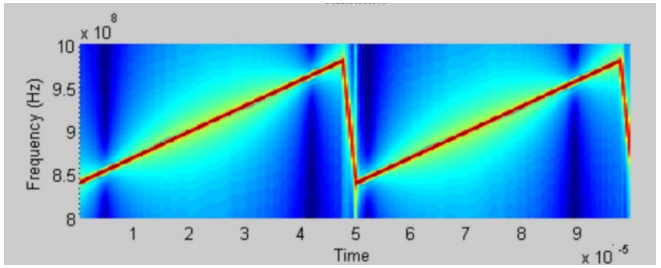
Menaces étudiées

MELI

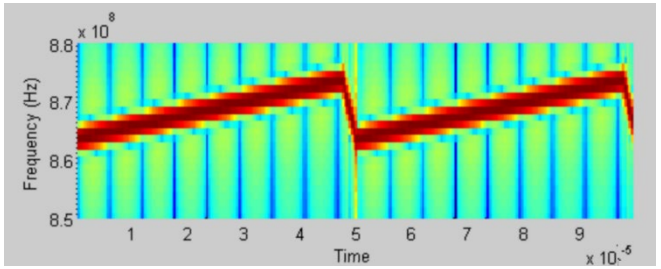
- **Interférences EM intentionnelles**

Brouillage intentionnel des canaux de communication

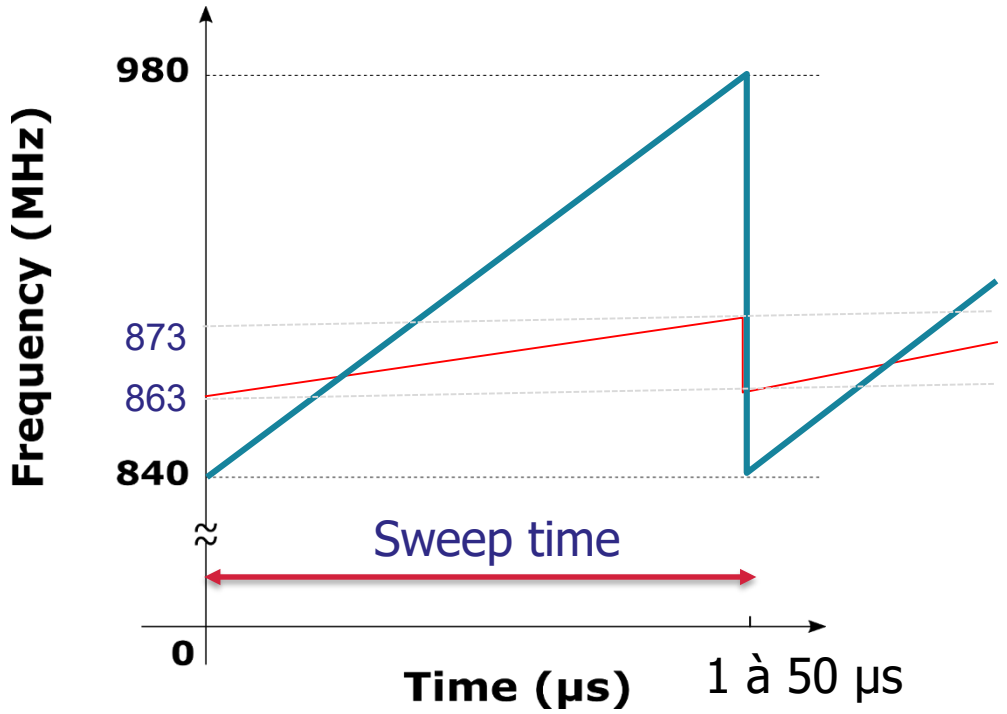
Brouilleur générique pour brouiller différents système de communication



Brouilleur spécifique au brouillage du LoRa/LoRaWan



Signaux de brouillage intentionnel



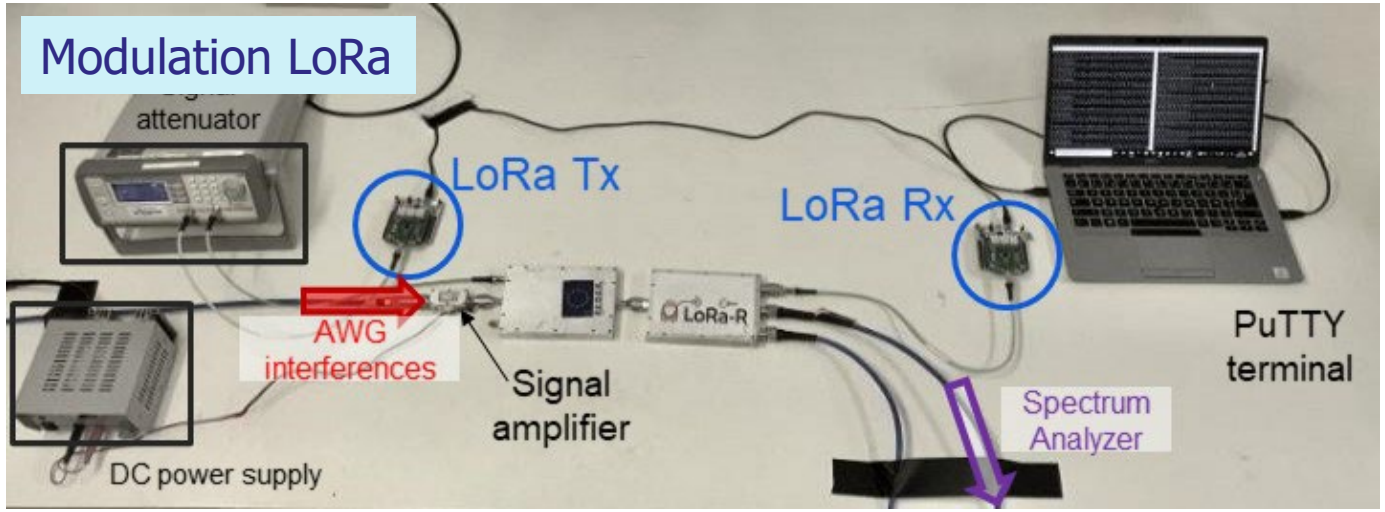
Université Gustave Eiffel

Méthodologie d'évaluation

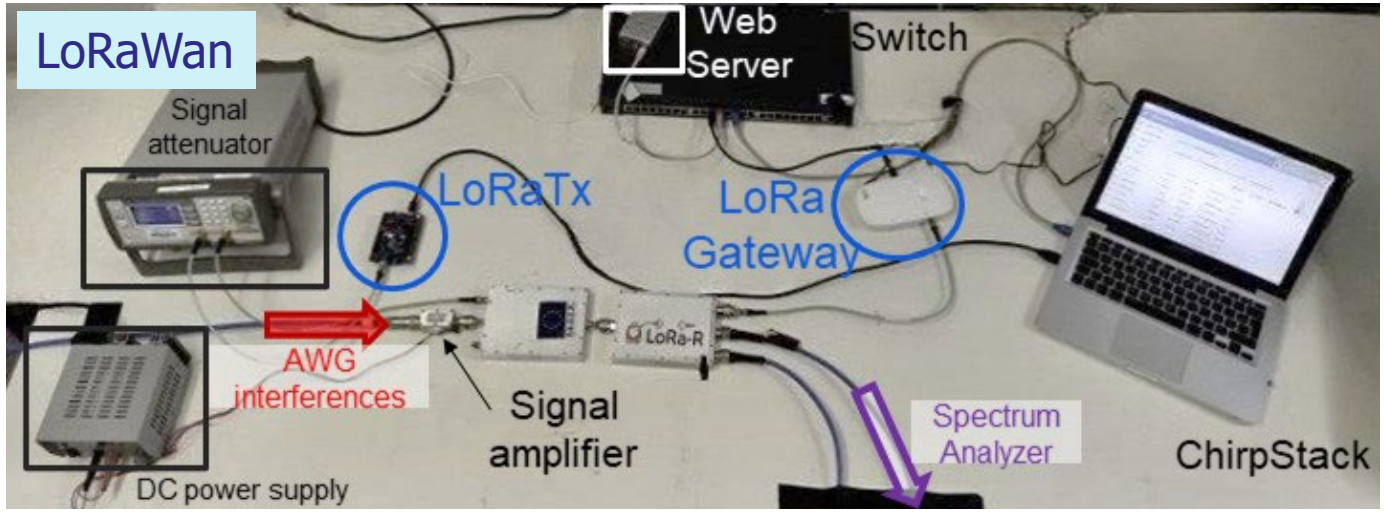
Problématiques à considérer

- LoRa ou LoRaWan
- Définition des applications représentatives, choix des trames, architectures applicatives (logicielles et matérielles), tests en classes A, B ou C….
- Indicateurs pertinents de défaillance
- Mise en œuvre de scénarios de perturbations représentatifs, durée des séquences, répétées ou statistiquement variables…
- Protocole d'application des interférences ou attaques, augmentation de puissance progressive ou par pas, application d'un niveau minimal, …
- Répétabilité des mesures, nombre d'essais, analyse des résultats…

Bancs de Test en LoRa ou LoRaWan

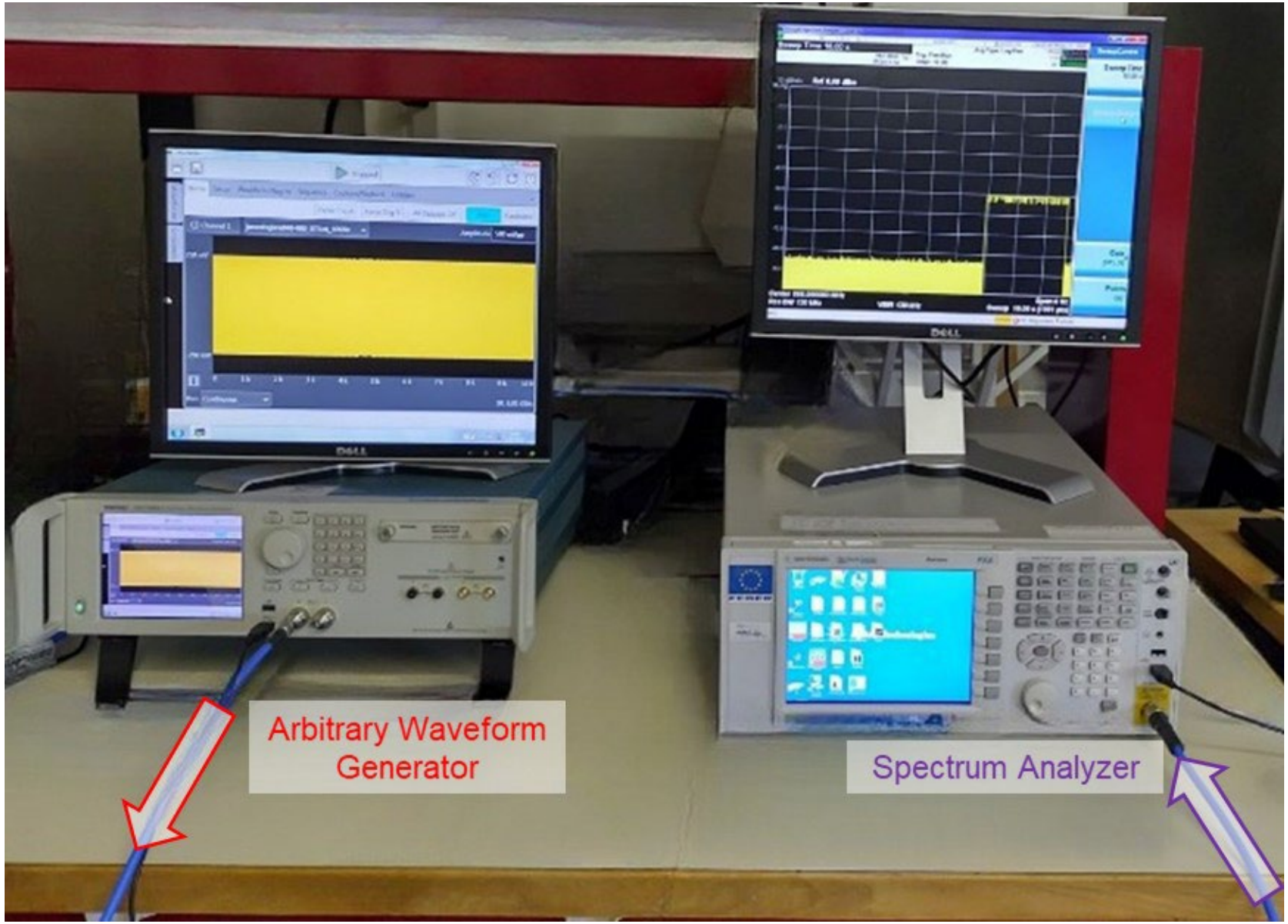


- Hardware : 2 SX 1272 ; programmation en langage C
- Envoi et réception d'une séquence connue avec compteur de trames
- Analyse post-transmission pour déterminer les erreurs
- Indicateurs : nombre de trames perdues / erronées / erreur de compteur



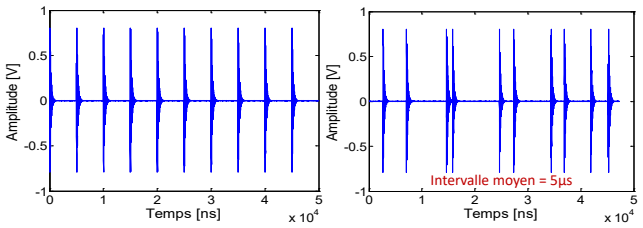
- Hardware : 1 SX 1276 ; programmation en langage C, passerelle KERLINK, serveur applicatif sur Raspberry PI
- Envois de trames et réceptions d'ACK
- Analyse via l'analyseur de spectre et les traces de problèmes de comm.
- Indicateur : perte de l'ACK

Equipements communs du labo

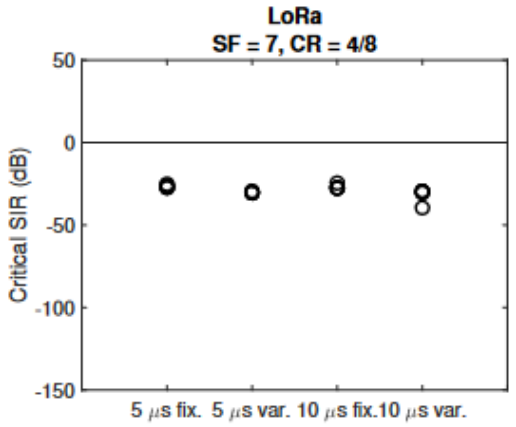


Résultats: LoRa ou LoRaWan

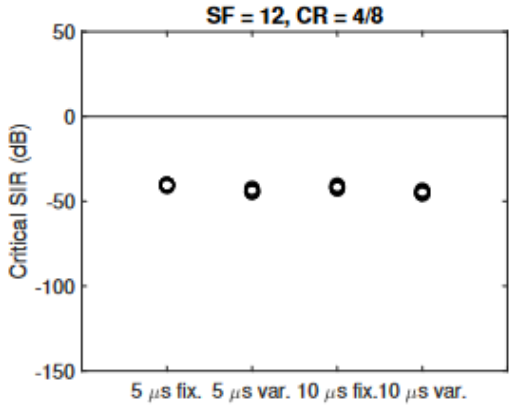
Durée des séquences d'interférences de 50 ou 100 µs



$$SIR = \frac{P\ Signal\ LoRaW}{P\ Interférences}$$

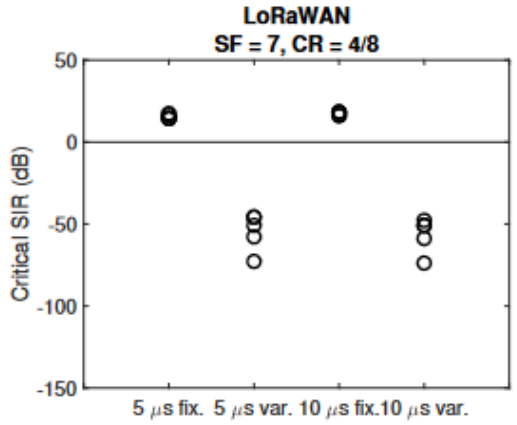


(a)

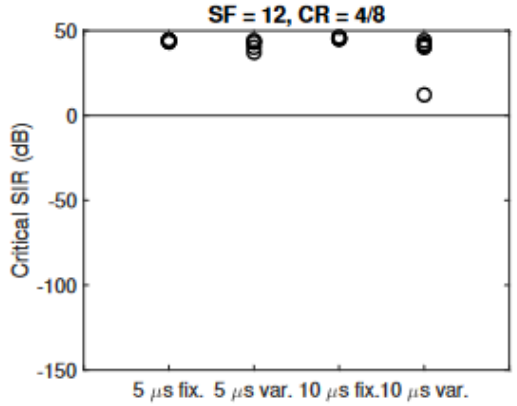


(c)

LoRaWan



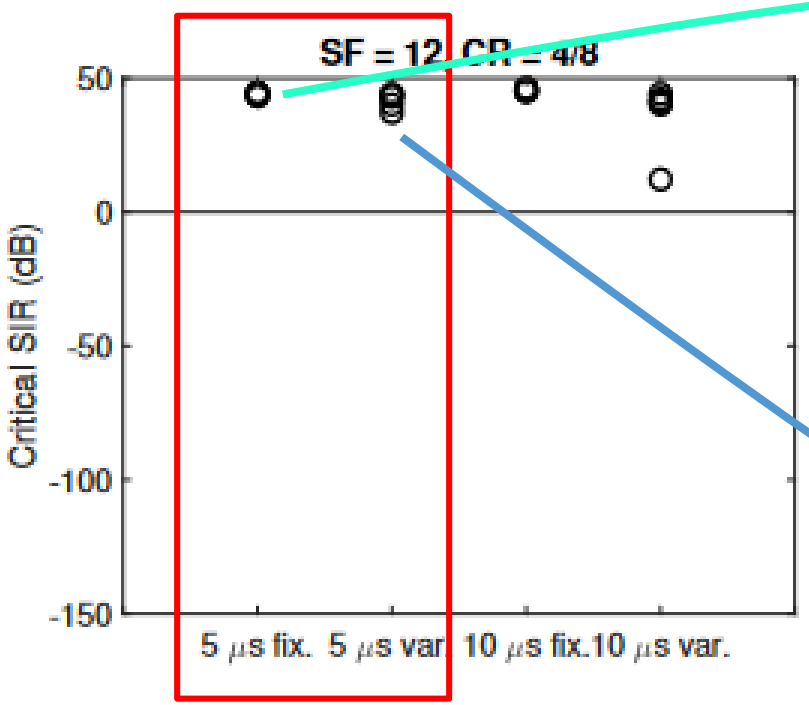
(b)

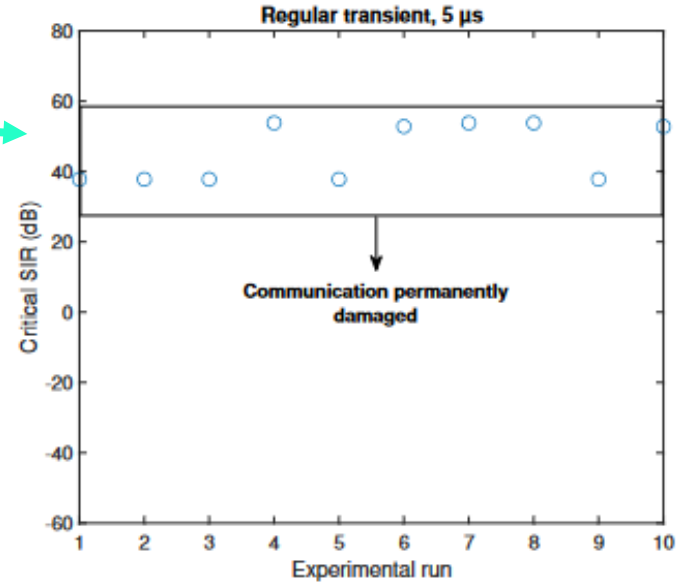


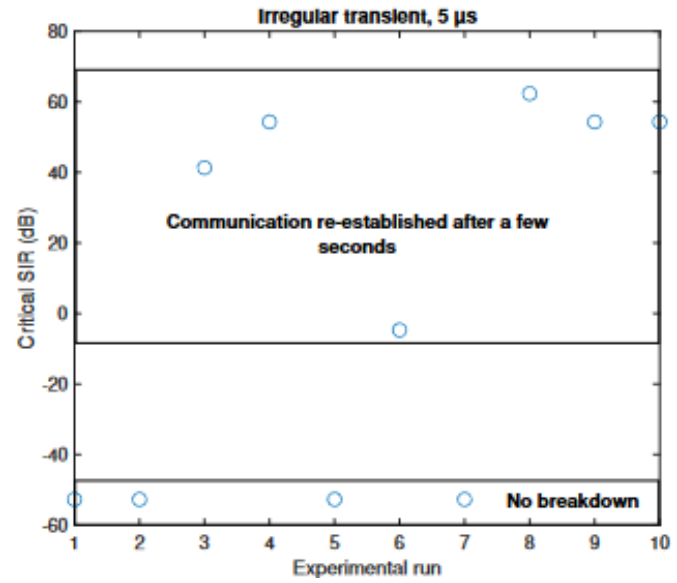
(d)

Université Gustave Eiffel

Résultats:



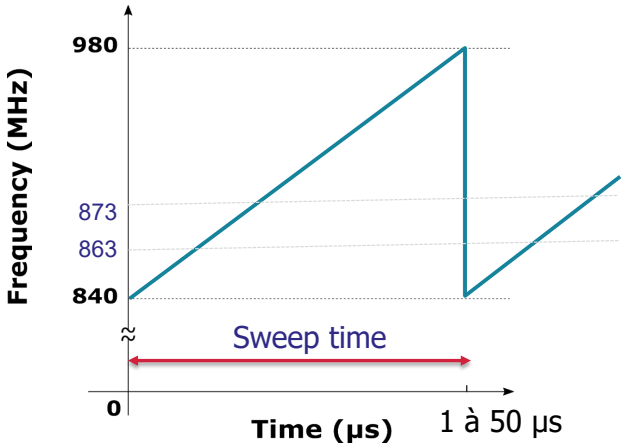




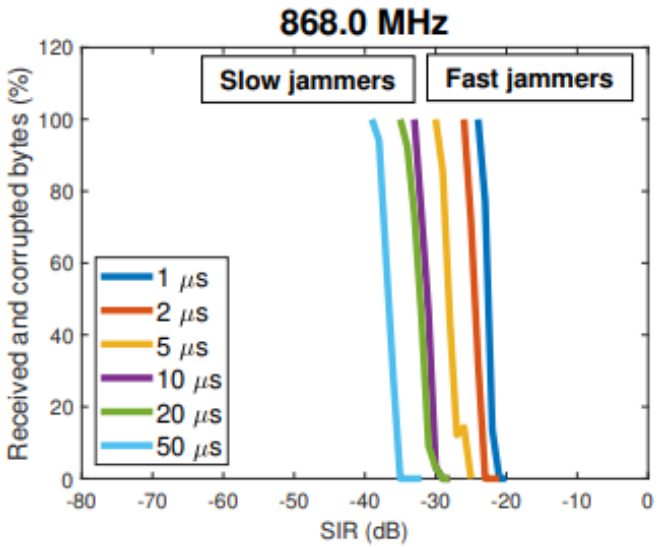
Séquences de 50 µs → Séquences de 500 µs

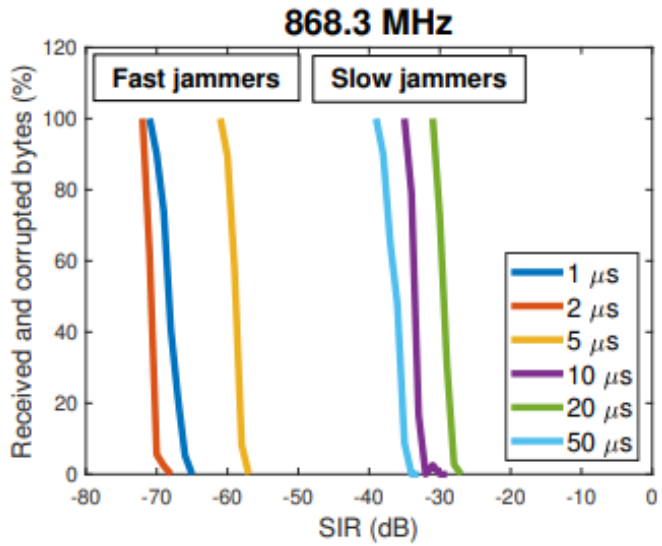
Université Gustave Eiffel

Résultats: Brouillage



$$SIR = \frac{P\ Signal\ LoRaW}{P\ Interférences}$$

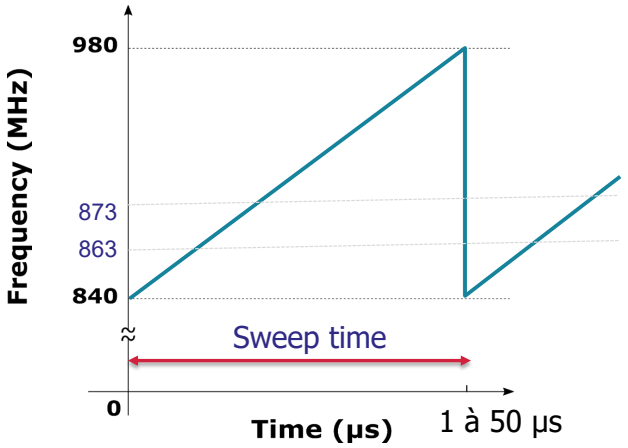




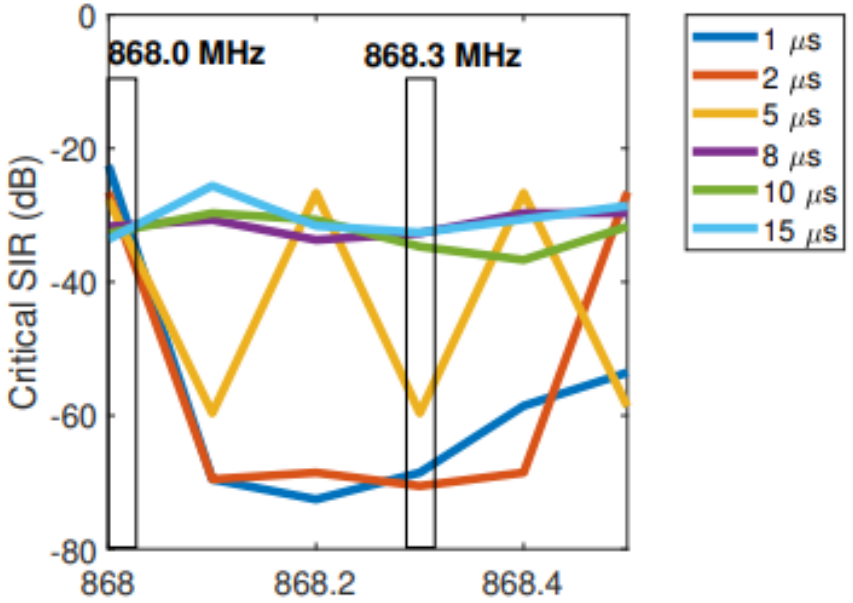
Effet différent selon le canal LoRa

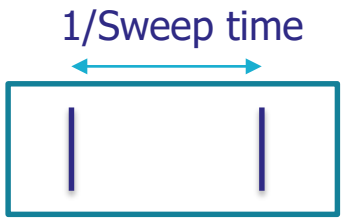
Les brouilleurs « rapides avec 1,2 et 5 µs » sont plus agressifs sur le canal 868 MHz que 863,3 MHz

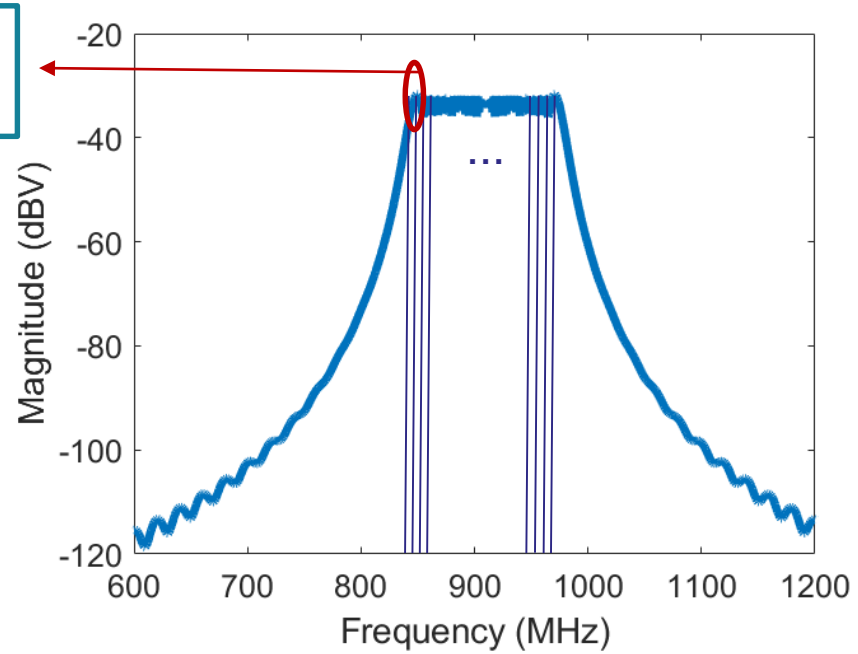
Résultats: Brouillage



$$SIR = \frac{P\ Signal\ LoRaW}{P\ Interférences}$$







Université Gustave Eiffel

Conclusions

- L'analyse de susceptibilité de protocole IoT peut donner des résultats très variables selon la méthodologie de tests (séquences d'interférences ou mode d'attaque, modulation ou protocole complet, indicateurs de défauts…)

- Dans le cas du LoRaWan, des choix de configurations peuvent être faits (SF, répétition des messages, choix du canal…) :
  - en fonction des agressions à éviter et,
  - en fonction des applications et de l'occupation de la ressource

- Besoins d'une méthodologie de test suffisamment harmonisée pour pouvoir comparer des protocoles entre eux, par exemple LoRaWan, Sigfox ou 5G, LTE-M, …

Merci

Questions?

virginie.deniau@univ-eiffel.fr christophe.gransart@univ-eiffel.fr

Université Gustave Eiffel