APSYS .Lab

Spark the future. Craft tomorrow.

LAAS CNRS

INJECTABLE: injection de trafic malveillant dans une connexion Bluetooth Low Energy

SSTIC, 2 juin 2021 - Rennes

Romain CAYRE[a,b] **- Florent GALTIER**[a] **-** Guillaume AURIOL[a] - Vincent NICOMETTE[a] - Mohamed KAÂNICHE[a] - Géraldine MARCONATO[b]

[a] prenom.nom@laas.fr / [b] prenom.nom@airbus.com

AN **AIRBUS** COMPANY

PLAN DE LA PRÉSENTATION

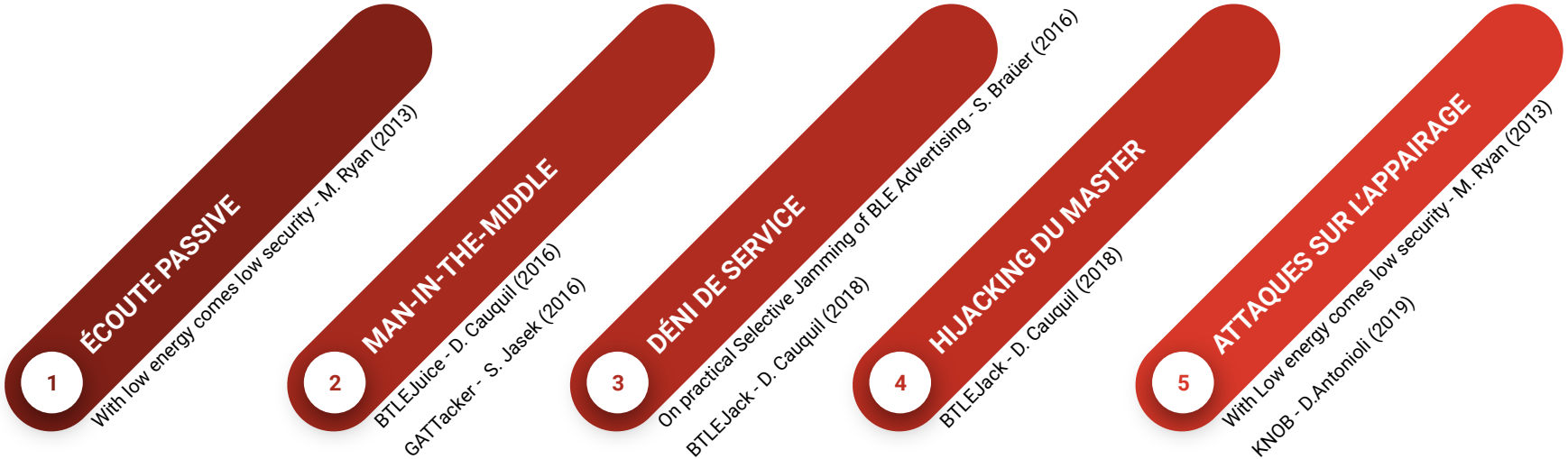
- **Introduction et pré-requis**
- **Description de la vulnérabilité**
- **Scénarios d'exploitation et analyse de sensibilité**
- **Contre-mesures**

INTRODUCTION ET PRÉ-REQUIS

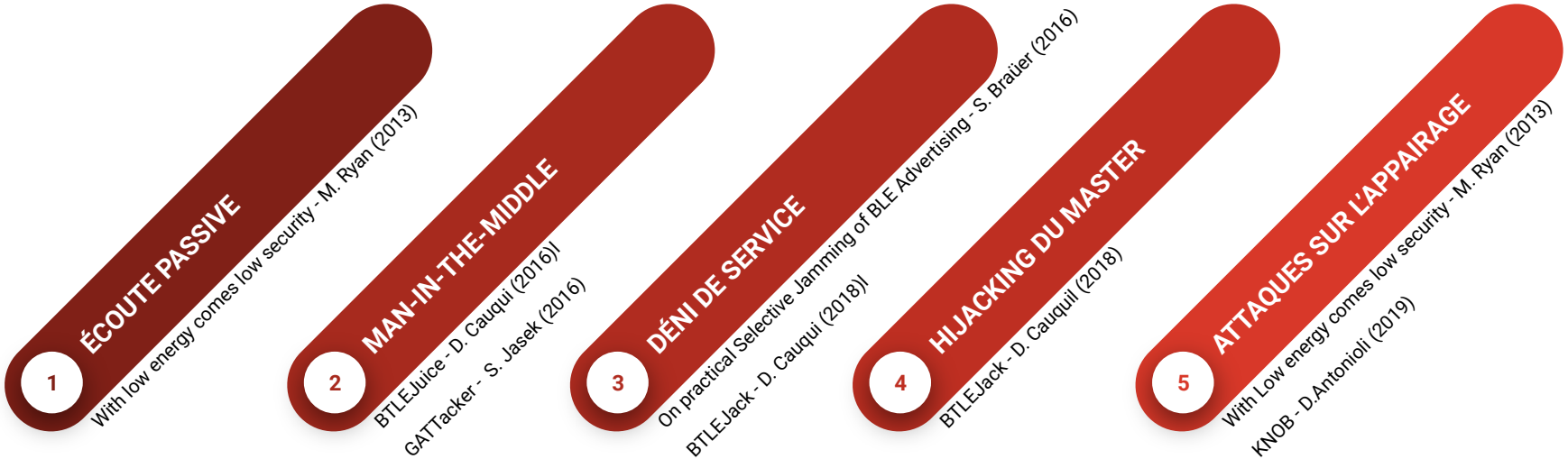
BLUETOOTH LOW ENERGY

- Introduit dans la version 4.0 de la spécification
- Faible consommation énergétique
- Faible complexité
- Massivement déployé (téléphones, tablettes, objets connectés, …)
- Mécanismes de sécurité pertinents mais globalement peu utilisés

ÉTAT DE L'ART OFFENSIF
ATTAQUES SUR LE PROTOCOLE



ÉTAT DE L'ART OFFENSIF
ATTAQUES SUR LE PROTOCOLE

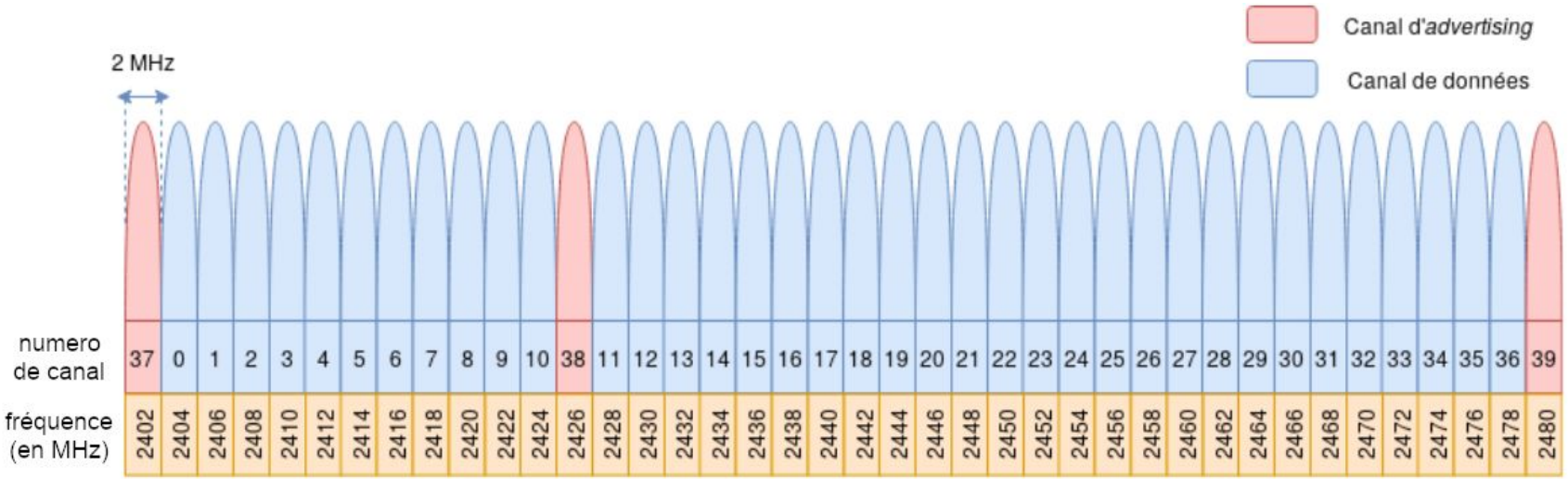


Ce qu'on ne sait pas faire à l'heure actuelle:

- injecter une trame dans une connexion établie
- hijacker le rôle Slave
- établir un Man-in-the-Middle en cours de connexion

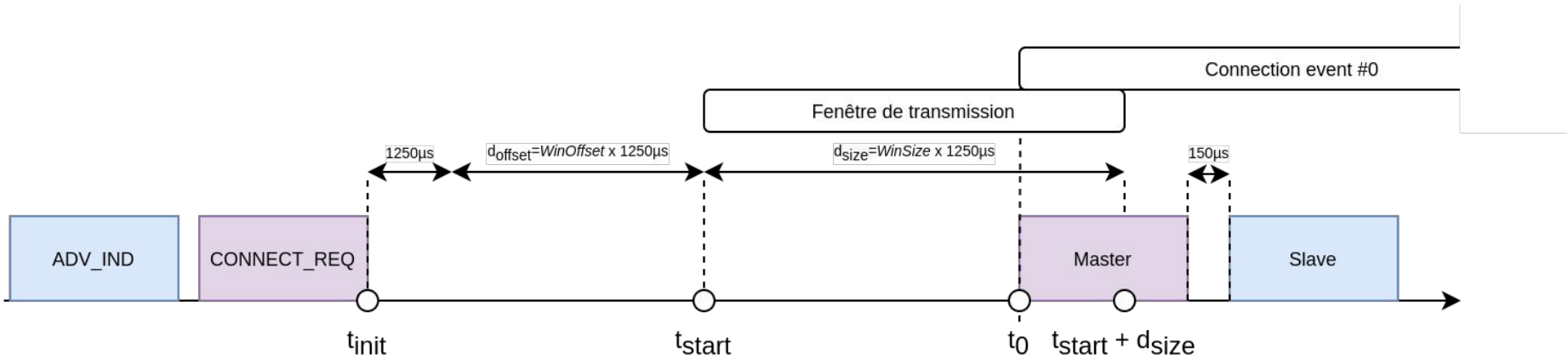
BLUETOOTH LOW ENERGY

COUCHE PHYSIQUE



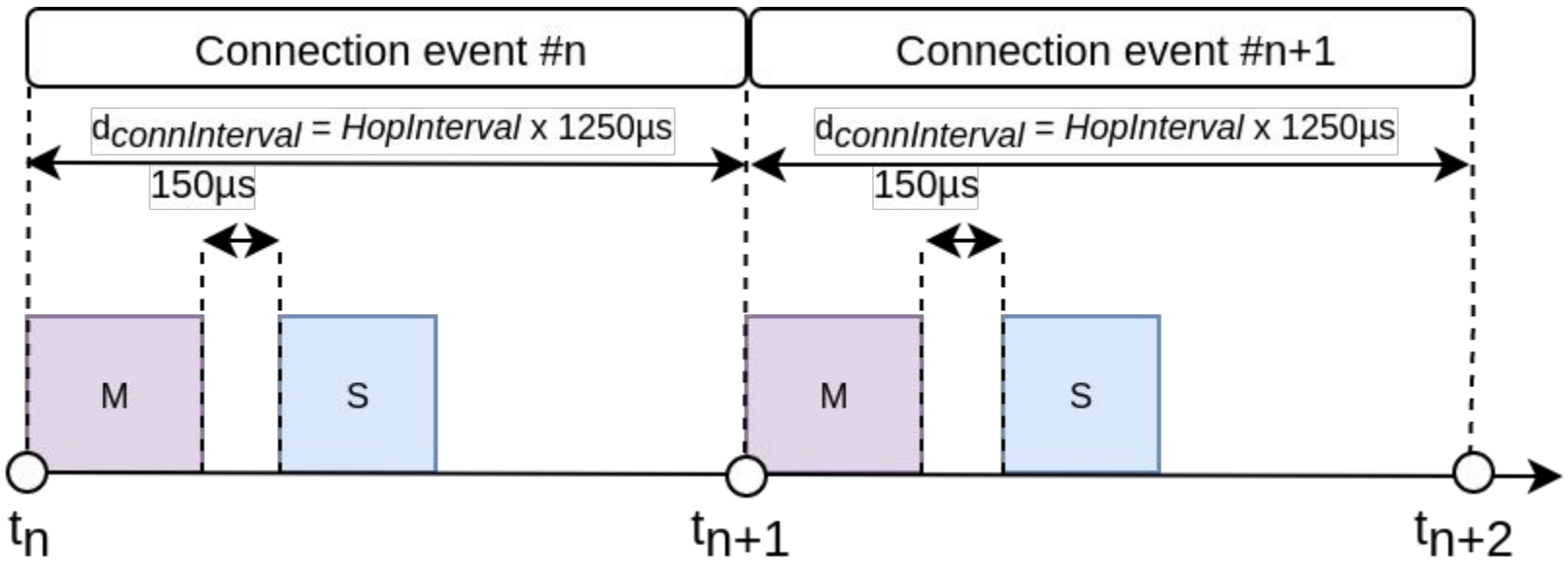
BLUETOOTH LOW ENERGY

INITIATION DE LA CONNEXION



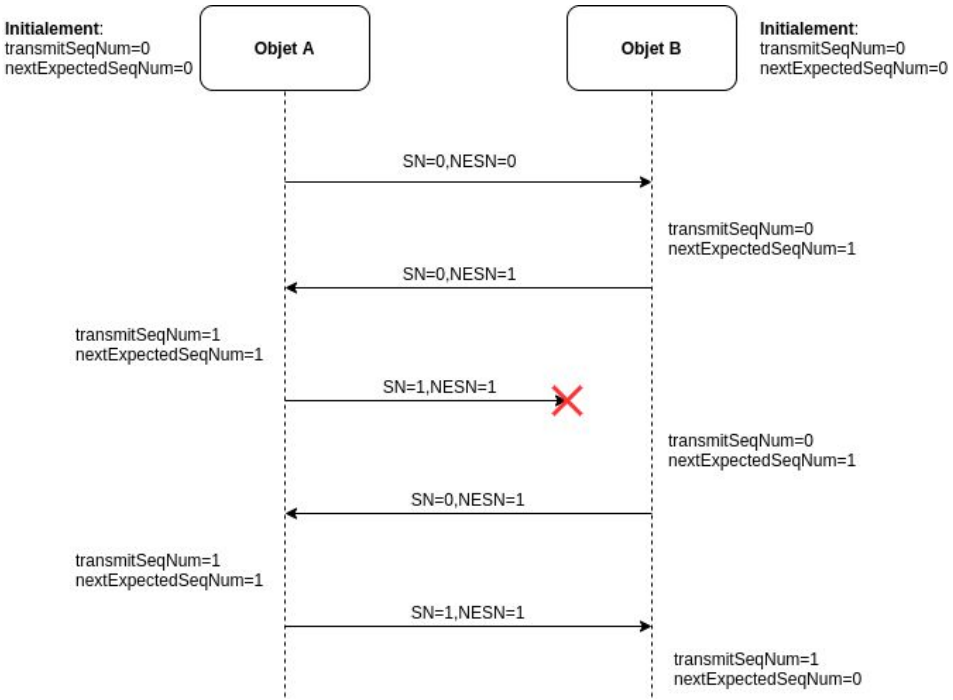
BLUETOOTH LOW ENERGY

CONNECTION EVENTS



BLUETOOTH LOW ENERGY

COMPTEURS



BLUETOOTH LOW ENERGY

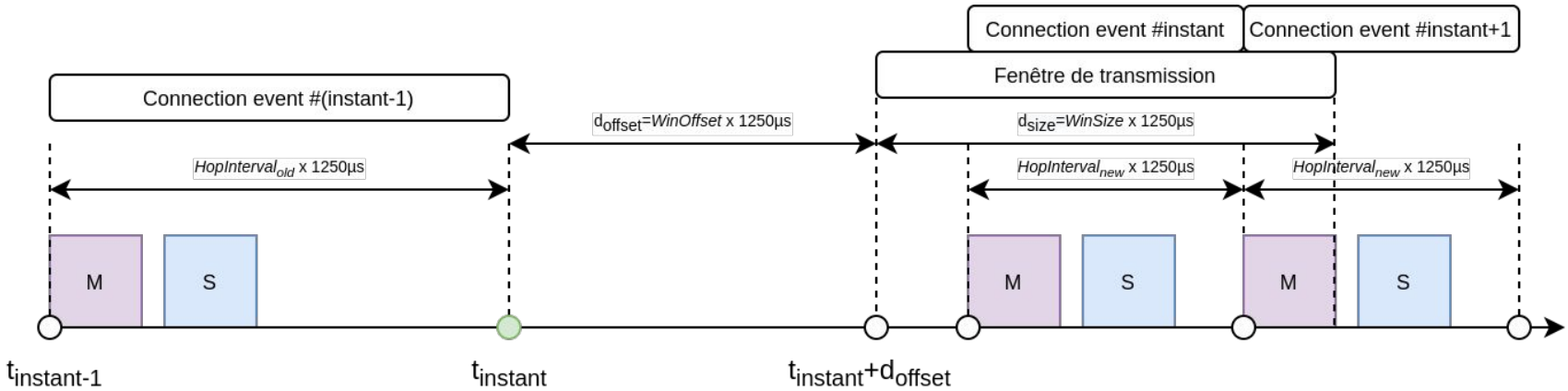
MISE À JOUR DES PARAMÈTRES DE CONNEXION

CtrData					
WinSize (1 octet)	WinOffset (2 octets)	Interval (2 octets)	Latency (2 octets)	Timeout (2 octets)	Instant (2 octets)

Figure 2.27: CtrData field of the LL_CONNECTION_UPDATE_IND PDU

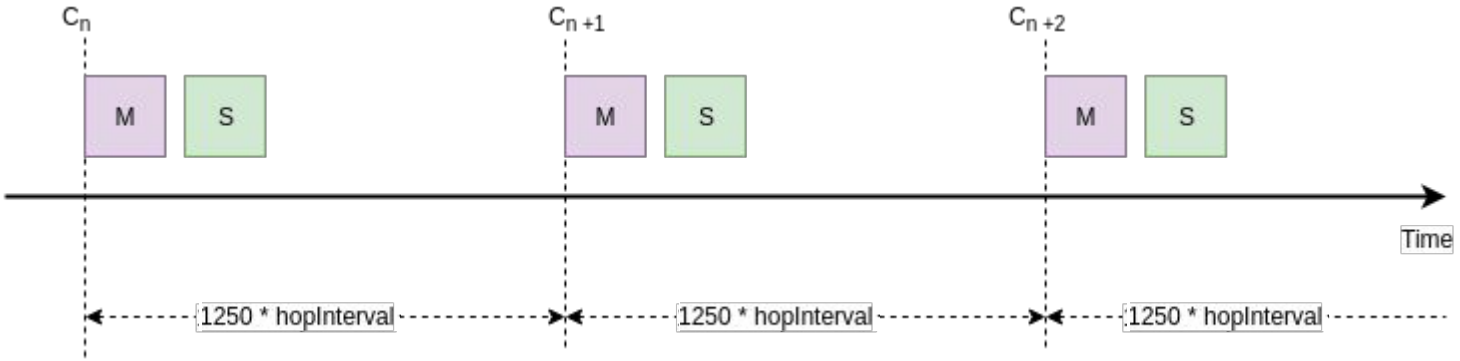
CtrData	
ChM (5 octets)	Instant (2 octets)

Figure 2.28: CtrData field of the LL_CHANNEL_MAP_IND PDU

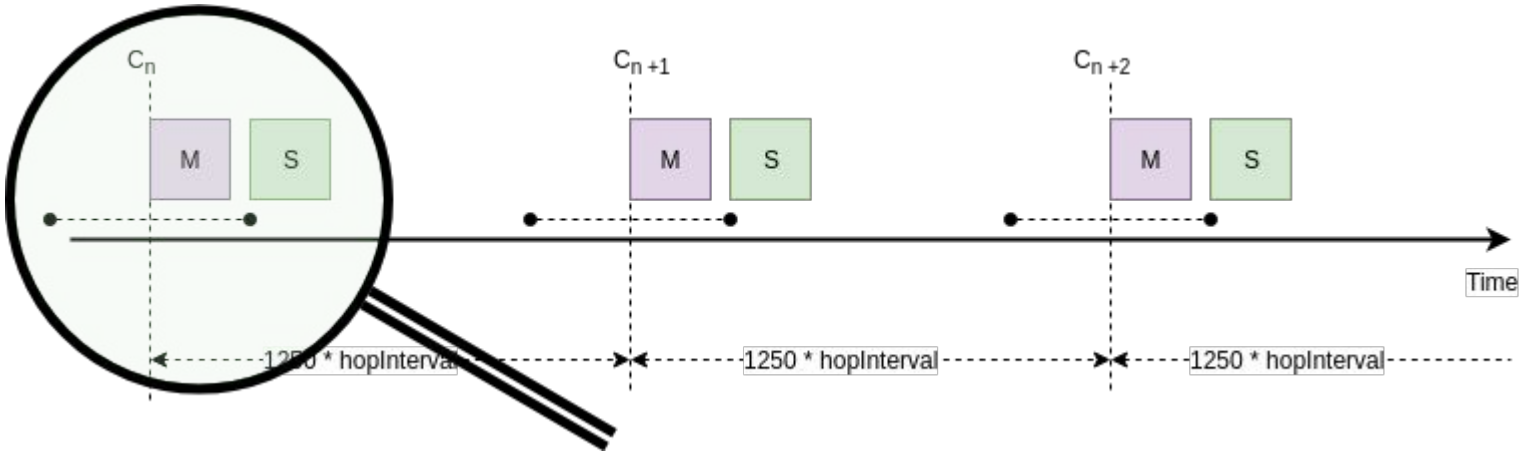


DESCRIPTION DE LA VULNÉRABILITÉ

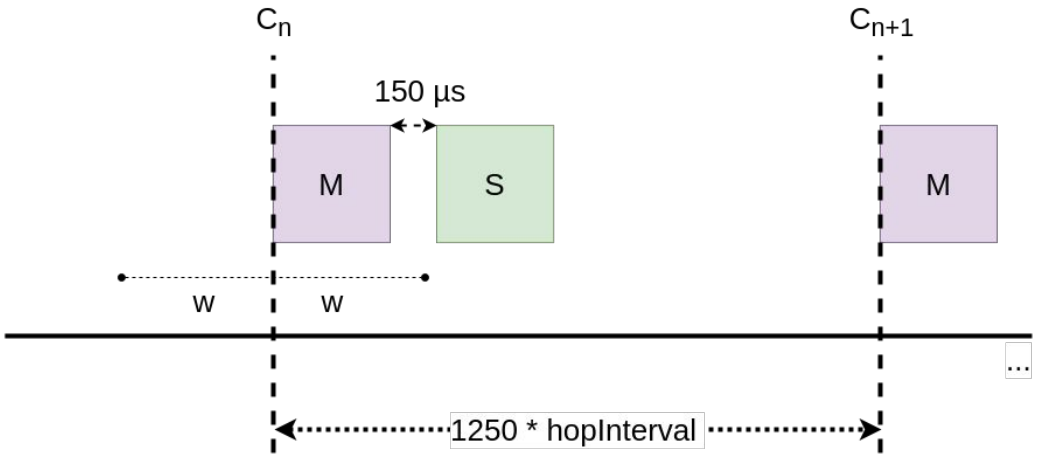
CONNECTION EVENTS (VERSION SIMPLIFIÉE)



CONNECTION EVENTS (DANS LA RÉALITÉ)

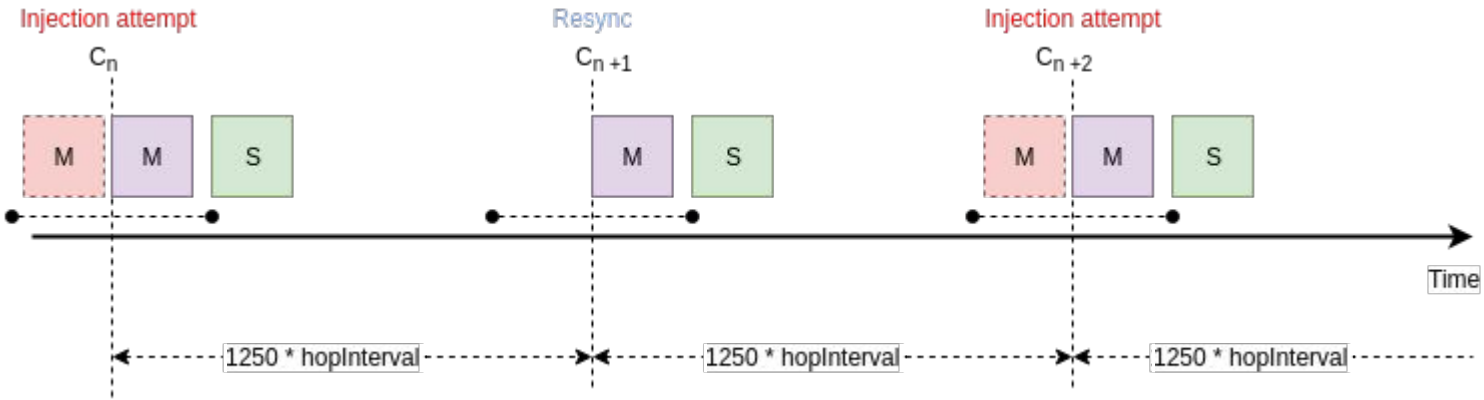


WINDOW WIDENING

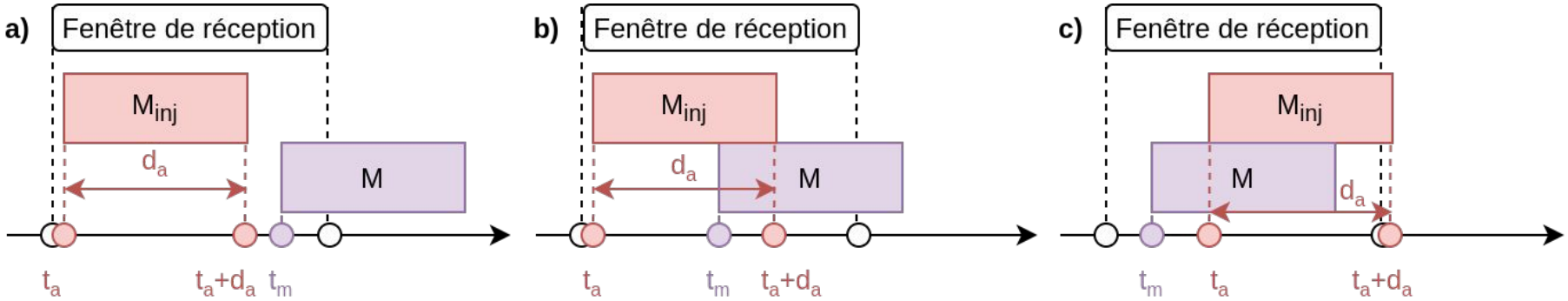


$$windowWidening = \frac{txSCA+rxSCA}{1000000} * (receiveWindowEnd - timeOfLastSync) + 32\mu s$$

INJECTABLE : RACE CONDITION



TROIS ISSUES POSSIBLES ...



SUCCÈS DE L'INJECTION

SUCCÈS POTENTIEL DE L'INJECTION

ÉCHEC DE L'INJECTION

CRITÈRE DE RÉUSSITE

- la trame injectée est transmise avant la trame du Master dans la fenêtre
- le CRC embarqué dans la trame injectée est égal au CRC calculé à la réception de la trame

HEURISTIQUE DE DÉTECTION

- la trame injectée est transmise avant la trame du Master dans la fenêtre de réception

$$t_a + d_a + 150 - 5 < t_s < t_a + d_a + 150 + 5$$

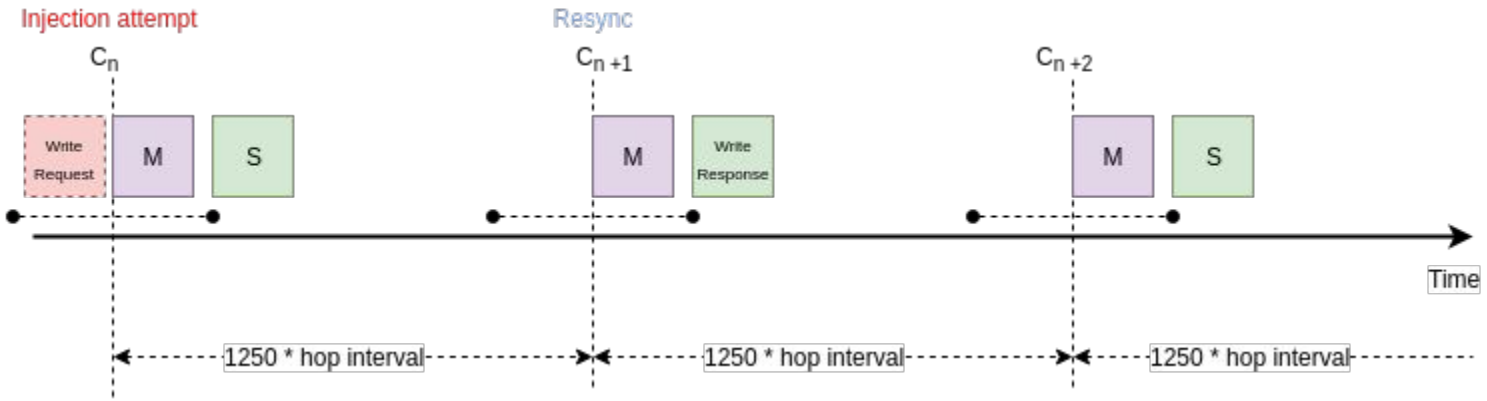
- le CRC embarqué dans la trame injectée est égal au CRC calculé à la réception de la trame

$$((SN_a + 1) \bmod 2 = NESN_s') \wedge (NESN_a = SN_s')$$

SCÉNARIOS D'EXPLOITATION ET ANALYSE DE SENSIBILITÉ

INJECTABLE : SCÉNARIOS D'EXPLOITATION

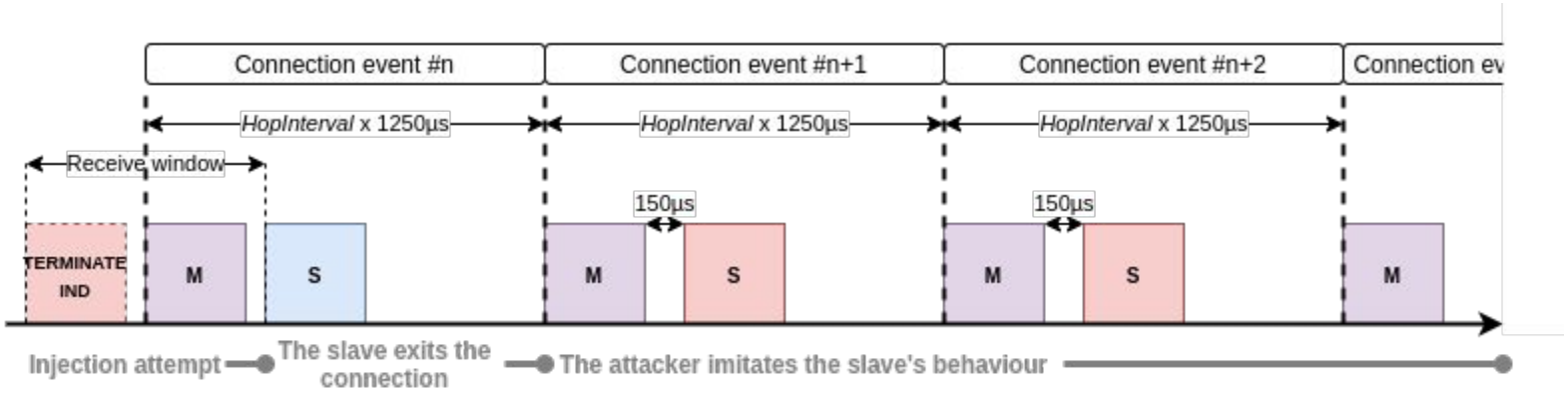
Activation illégitime de fonctionnalités



Démonstration : injection de faux SMS et de faux appels sur une montre connectée

INJECTABLE : SCÉNARIOS D'EXPLOITATION

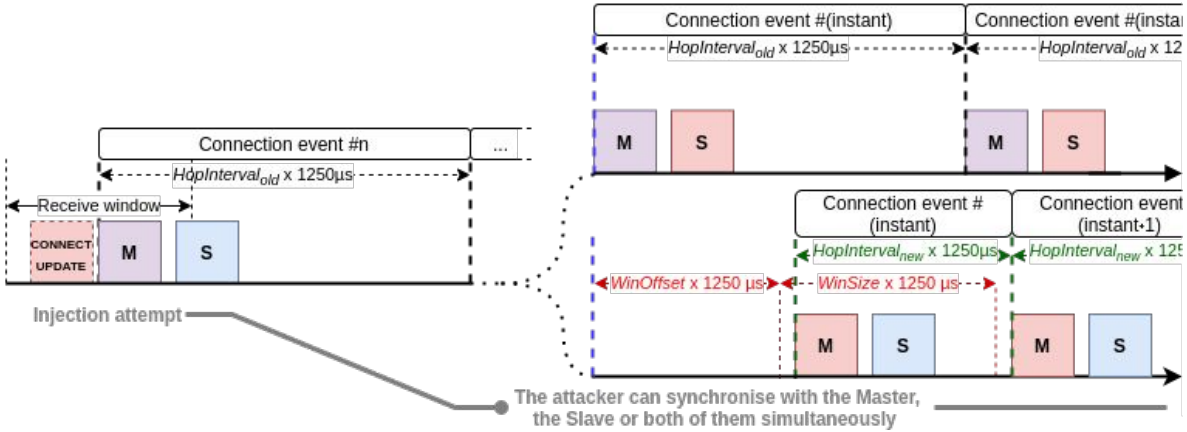
Hijacking du Slave



Démonstration : Hijacking du Slave sur un porte clé connecté

INJECTABLE : SCÉNARIOS D'EXPLOITATION

Hijacking du Master et Man-in-The-Middle



Démonstrations : Hijacking du Master et Man-in-the-Middle sur une ampoule connectée

INJECTABLE : ANALYSE DE SENSIBILITÉ

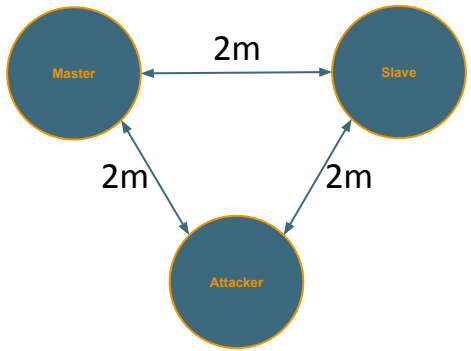
Objectif: évaluer empiriquement l'impact de 3 paramètres sur la réussite de l'attaque:

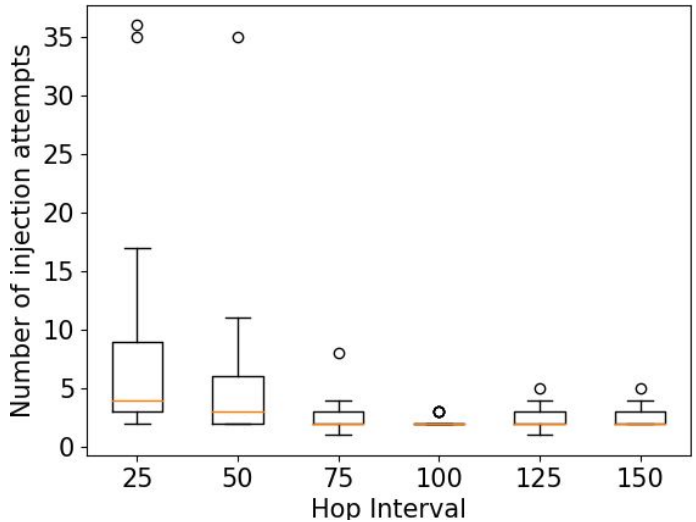
- le *hop interval*
- la taille du *payload*
- la distance entre l'attaquant et la cible

- Pour chaque valeur d'un paramètre, on réalise 25 injections, dans le même environnement et en fixant les autres paramètres
- On compte pour chaque injection le nombre de tentatives avant qu'elle réussisse

INJECTABLE : ANALYSE DE SENSIBILITÉ

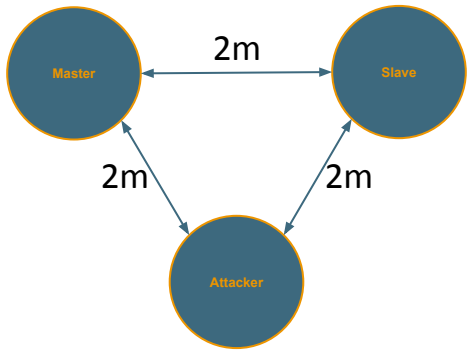
Hop Interval

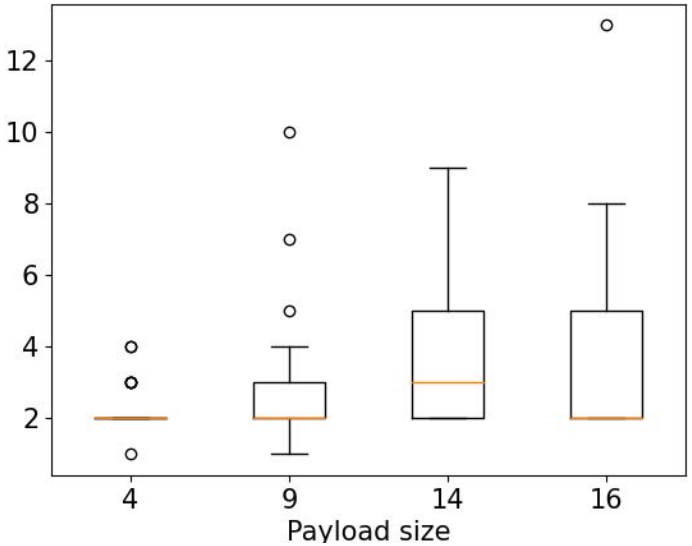




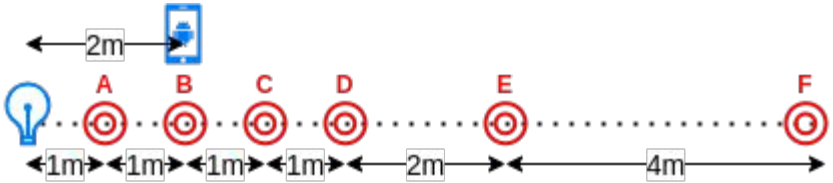
INJECTABLE : ANALYSE DE SENSIBILITÉ

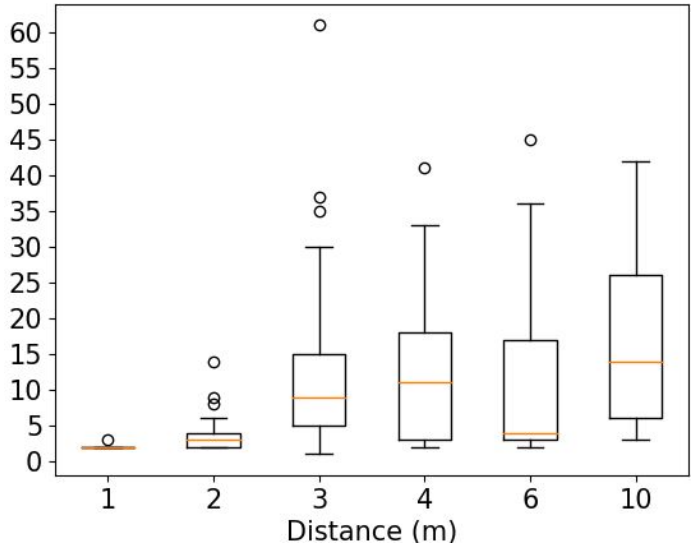
Taille du *payload*





Distance

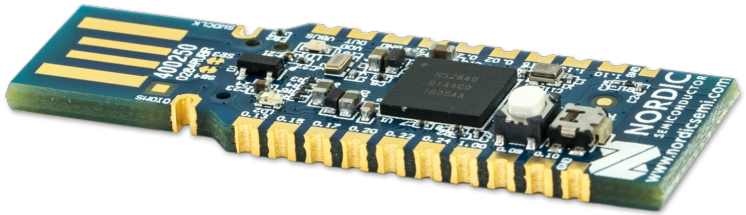

2m
A
B
C
D
E
F
1m
1m
1m
1m
2m
4m


60
55
50
45
40
35
30
25
20
15
10
5
0
1
2
3
4
6
10
Distance (m)

INJECTABLE : IMPLEMENTATION

- Implémentation d'une preuve de concept sur un dongle embarquant un nRF52840

- Code publié en open source sur GitHub (fin Juin, à la demande du Bluetooth SIG)



CONTRE-MESURES

INJECTABLE : CONTRE-MESURES

- Réduction du *window widening*
  - Mais réduit aussi la fiabilité de la connexion légitime
- Activation systématique du chiffrement décrit dans la spécification (encore trop rare aujourd'hui)
- Approches de monitoring

Merci pour votre attention !