APSYS .Lab

Spark the future. Craft tomorrow.

LAAS CNRS

WAZABEE: Attaque de réseaux Zigbee par détournement de puces Bluetooth Low Energy

SSTIC, 5 juin 2020 - Rennes

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

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

AN **AIRBUS** COMPANY

PLAN DE LA PRÉSENTATION

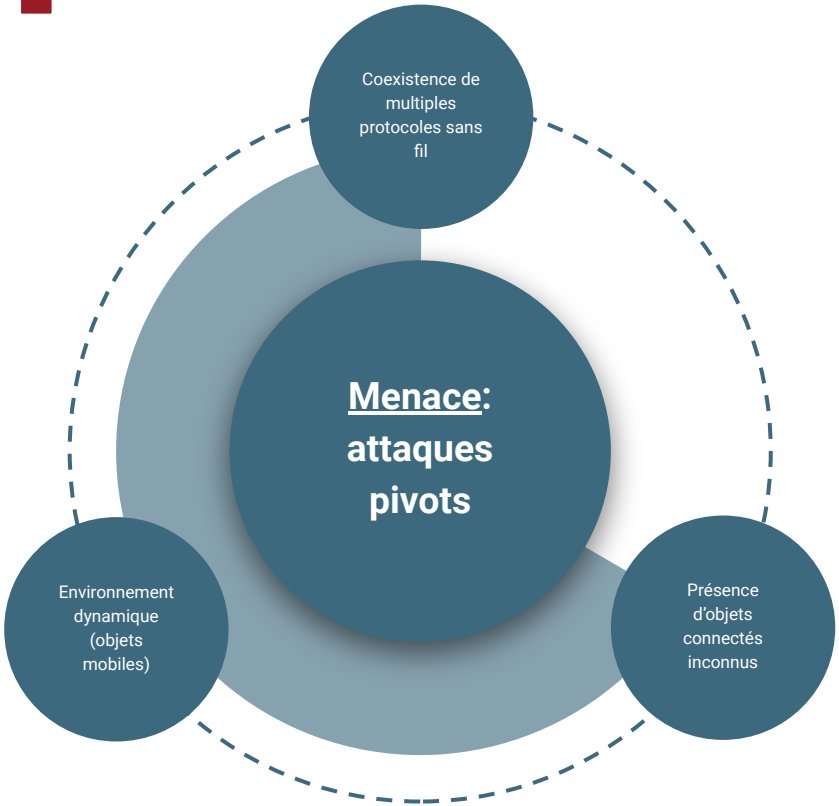
- **Contexte** et **problématique**
- **Présentation** des **protocoles étudiés**
- **Présentation** de **l'attaque WazaBee**
- **Expérimentations**: **implémentation** et **évaluation**
- **Conclusion: enjeux** et **perspectives**

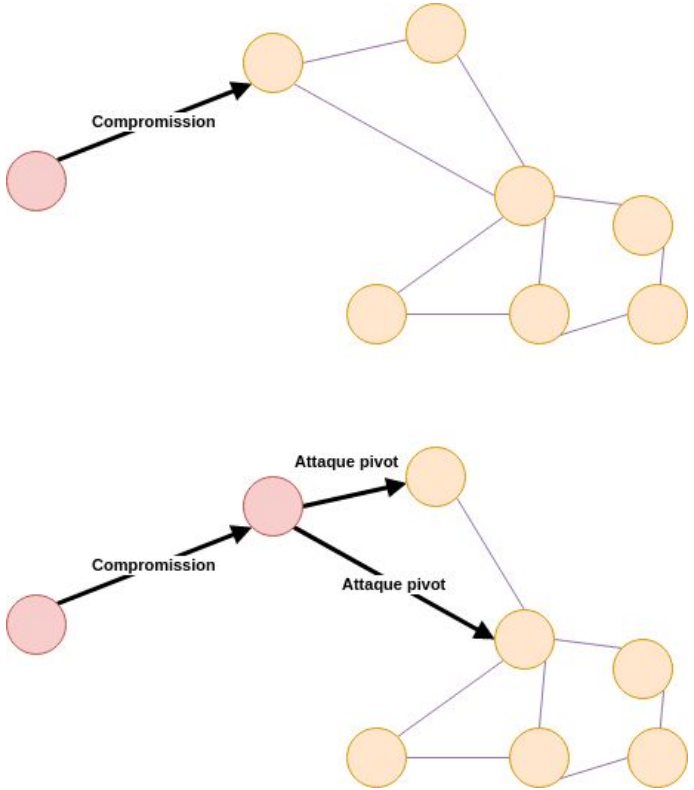
CONTEXTE ET PROBLÉMATIQUE

SÉCURITÉ DES OBJETS CONNECTÉS

Problématiques et enjeux

SÉCURITÉ DES ENVIRONNEMENTS IOT





PROBLÉMATIQUE

Est-il possible de **détourner** le comportement d'un **composant radio** prévu pour communiquer avec un **protocole donné** pour le faire communiquer avec un **protocole différent** ?

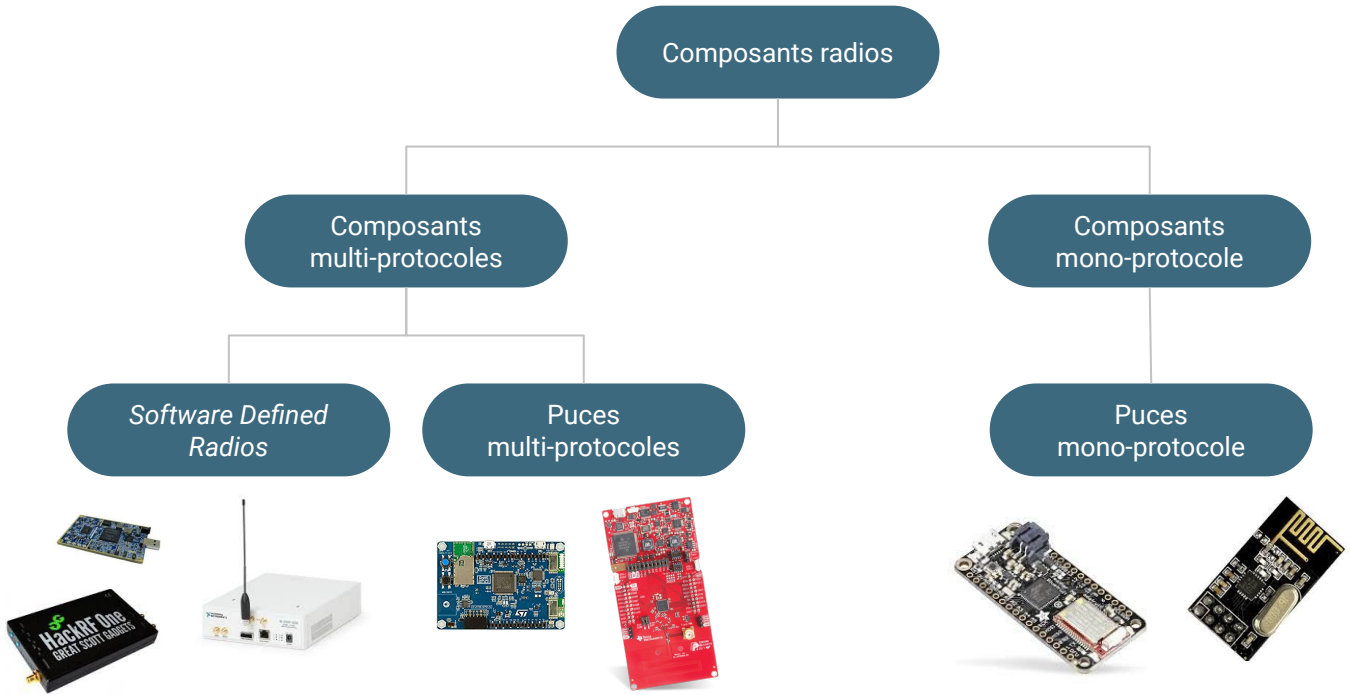
PROBLÉMATIQUE

Est-il possible de **détourner** le comportement d'un **composant radio** prévu pour communiquer avec un **protocole donné** pour le faire communiquer avec un **protocole différent** ?

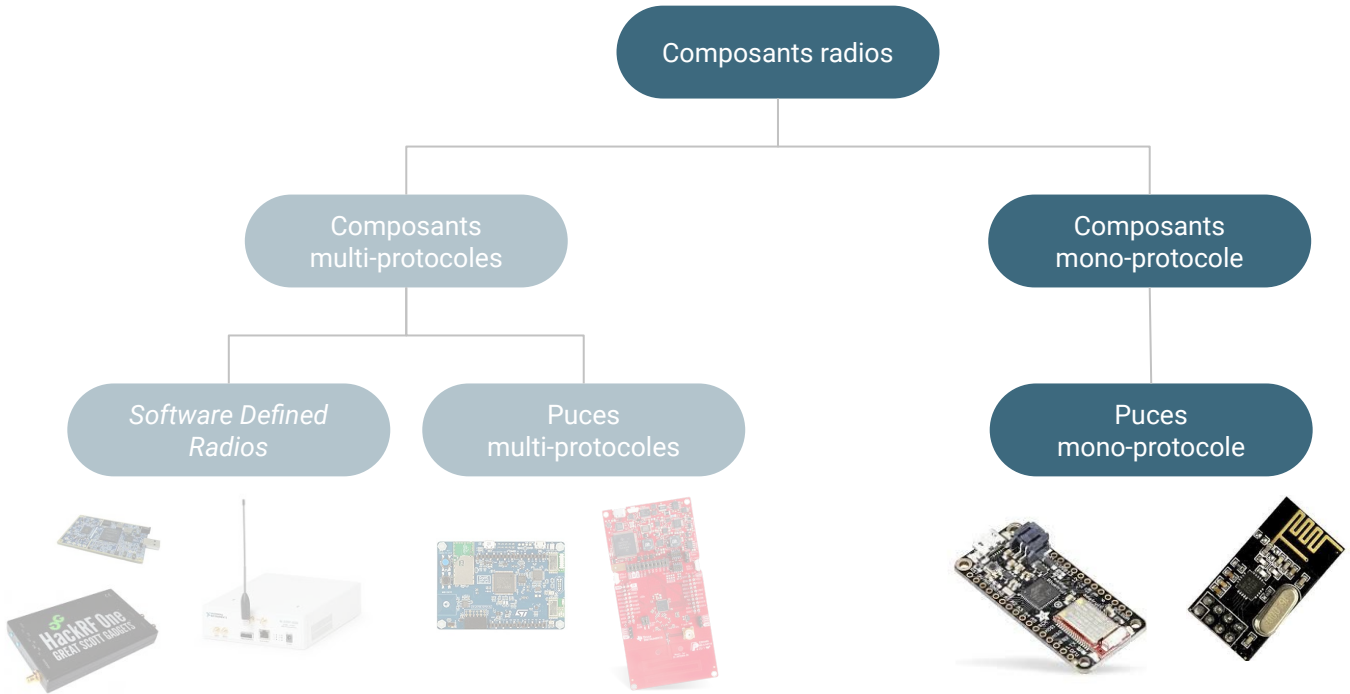
Scénarios offensifs:

🎯 Attaques pivots inter-protocoles 🎯 Attaques par canaux cachés

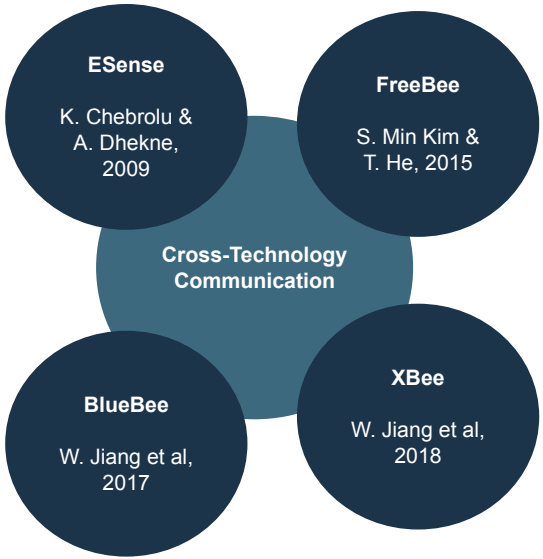
ÉTAT DE L'ART DES ATTAQUES INTER-PROTOCOLES

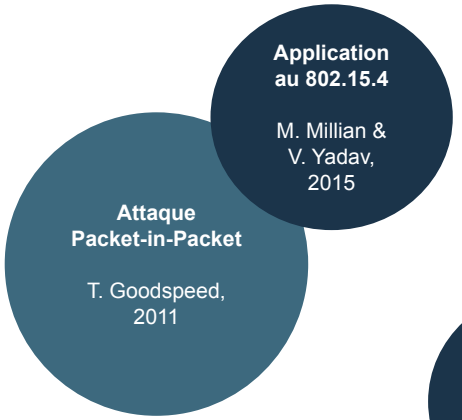


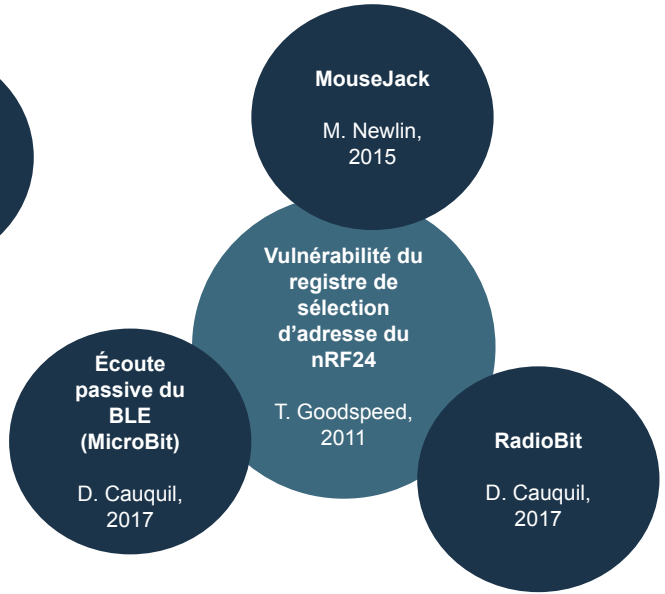
ÉTAT DE L'ART DES ATTAQUES INTER-PROTOCOLES



ÉTAT DE L'ART DES ATTAQUES INTER-PROTOCOLES



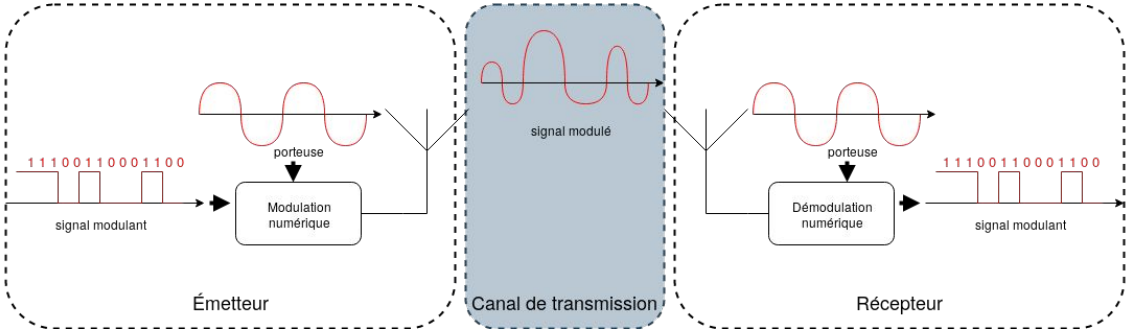


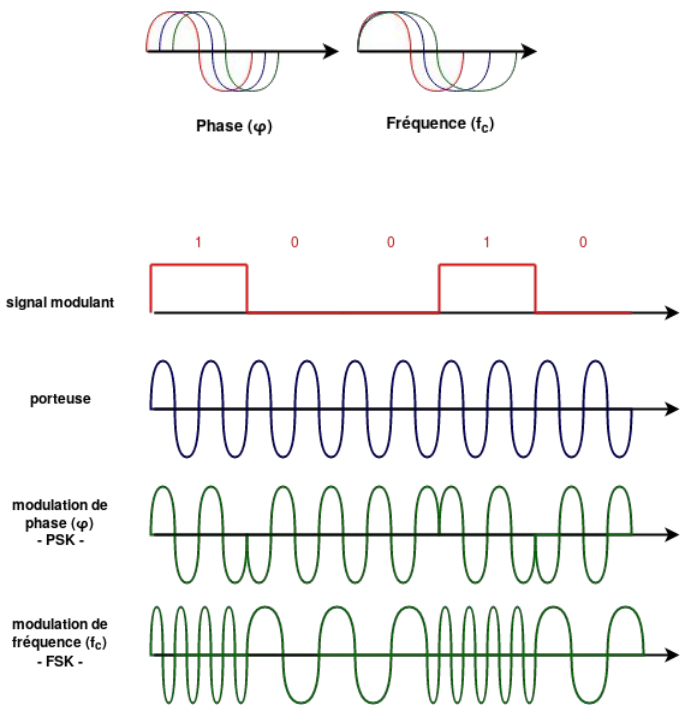


ÉTAT DE L'ART DES ATTAQUES INTER-PROTOCOLES

PRÉSENTATION DES PROTOCOLES ÉTUDIÉS

RAPPELS - MODULATION NUMÉRIQUE



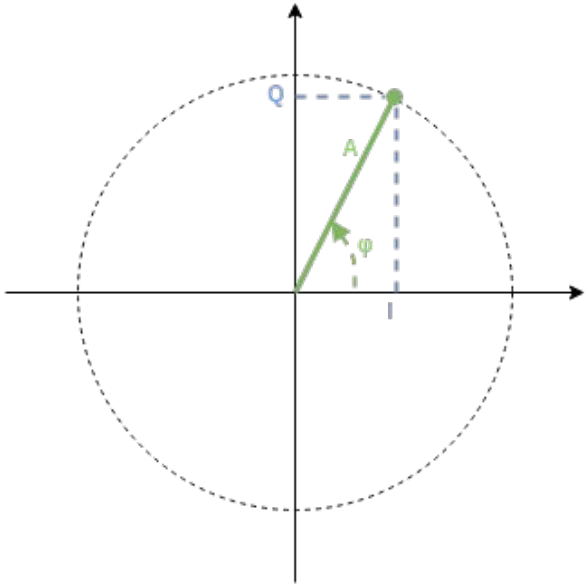


La **modulation numérique** est définie comme le processus par lequel un signal numérique (le **signal modulant**) est transformé en un signal **adapté au canal de transmission**. Cette transformation s'effectue généralement en faisant **varier les caractéristiques** d'une onde sinusoïdale (la **porteuse**) en fonction des données à transmettre: le signal résultant est nommé **signal modulé**.

RAPPELS - MODULATION NUMÉRIQUE

Signal modulé:

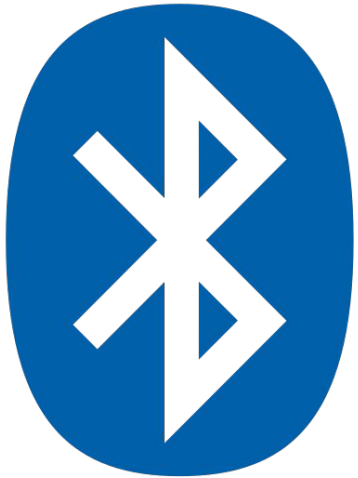
$$s(t) = A(t)\cos(2\pi f_c t + \varphi(t))$$
$$= I(t)\cos(2\pi f_c t) - Q(t)\sin(2\pi f_c t)$$



avec:

- $I(t) = A(t)\cos(\varphi(t))$ la composante dite “en phase”
- $Q(t) = A(t)\sin(\varphi(t))$ la composante dite “en quadrature”

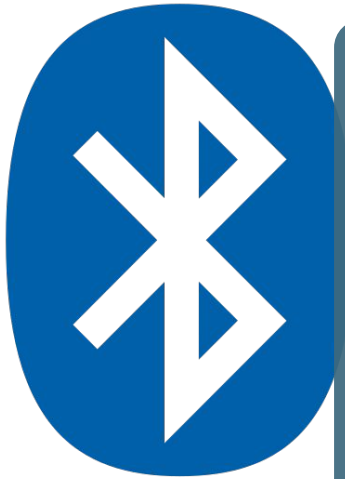
BLUETOOTH LOW ENERGY - PRÉSENTATION GÉNÉRALE



Bluetooth

SMART

BLUETOOTH LOW ENERGY - PRÉSENTATION GÉNÉRALE



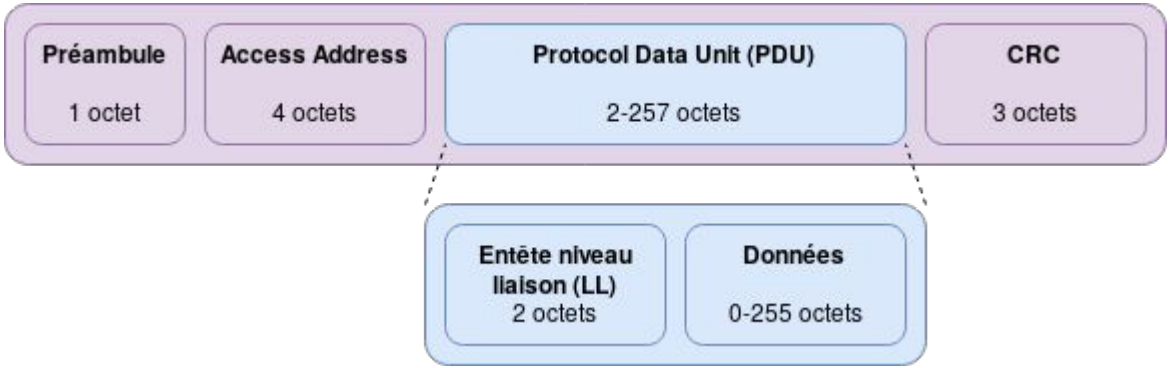
Introduit dans la version 4.0 de la spécification

Faible consommation énergétique

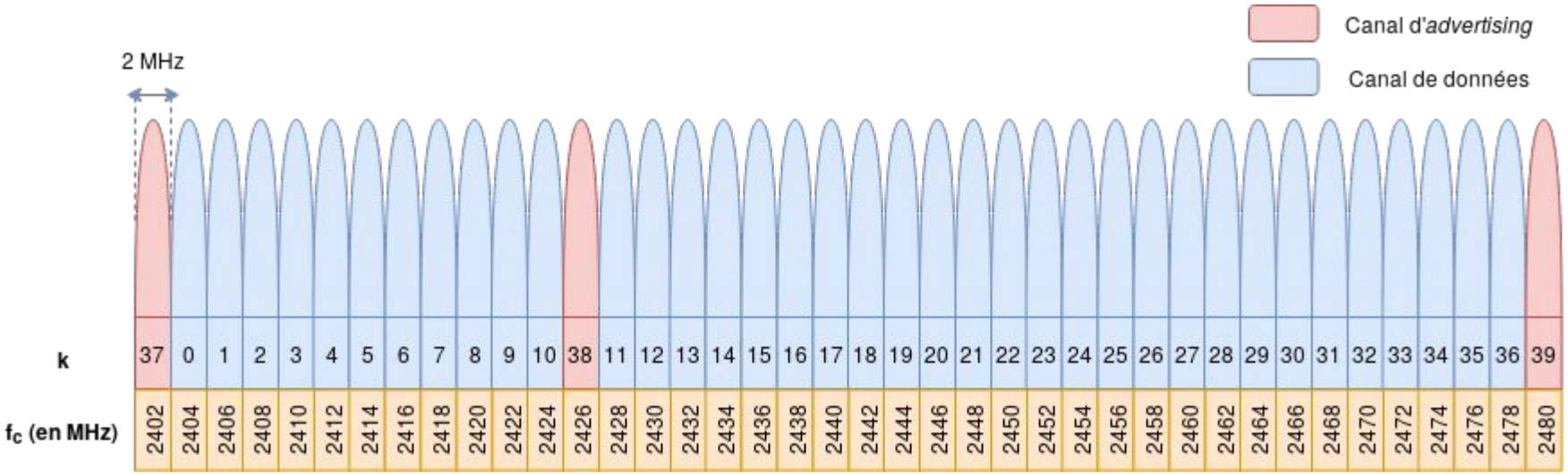
Faible complexité

Massivement déployé (téléphones, tablettes, …)

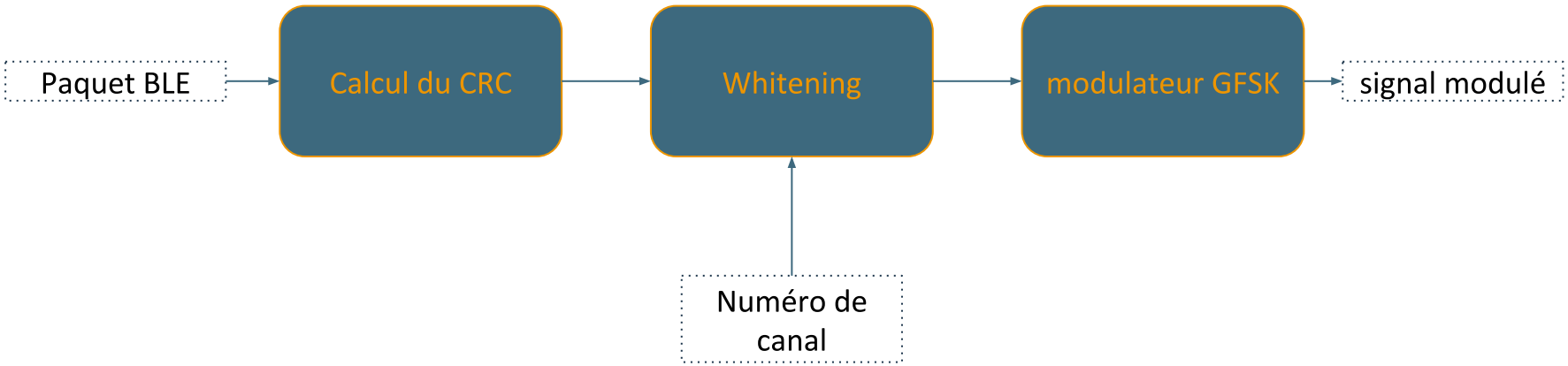
BLUETOOTH LOW ENERGY - FORMAT DE PAQUET



BLUETOOTH LOW ENERGY - CANAUX DE COMMUNICATION



BLUETOOTH LOW ENERGY - WHITENING



BLUETOOTH LOW ENERGY - COUCHES PHYSIQUES

PHY	Modulation	Codage	Débit
LE 1M (BLE classique)	1 Ms/s GFSK	Non	1 Mbps
LE 2M	**2 Ms/s GFSK**	**Non**	**2 Mbps**
LE Coded	1 Ms/s GFSK	Oui	125 / 500 kbps

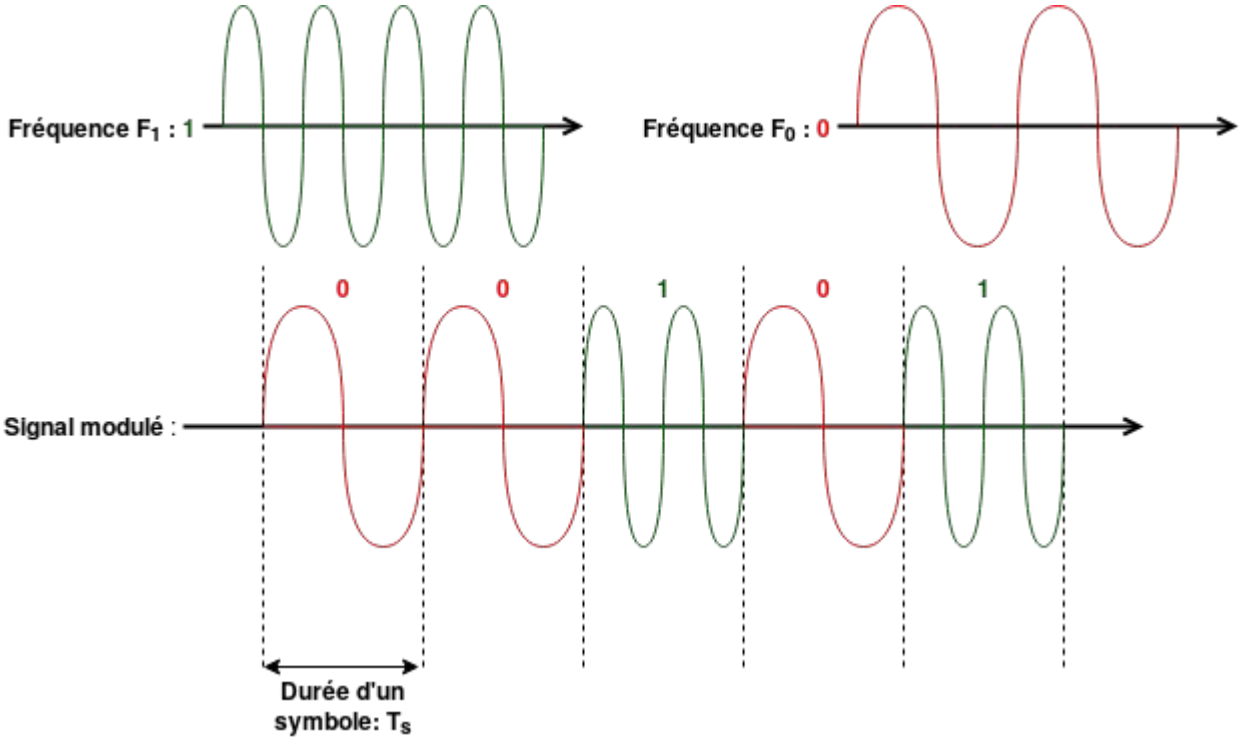
BLUETOOTH LOW ENERGY - MODULATION

$$F_0 = f_c - \Delta f = f_c - \frac{m}{2T_s}$$
$$F_1 = f_c + \Delta f = f_c + \frac{m}{2T_s}$$

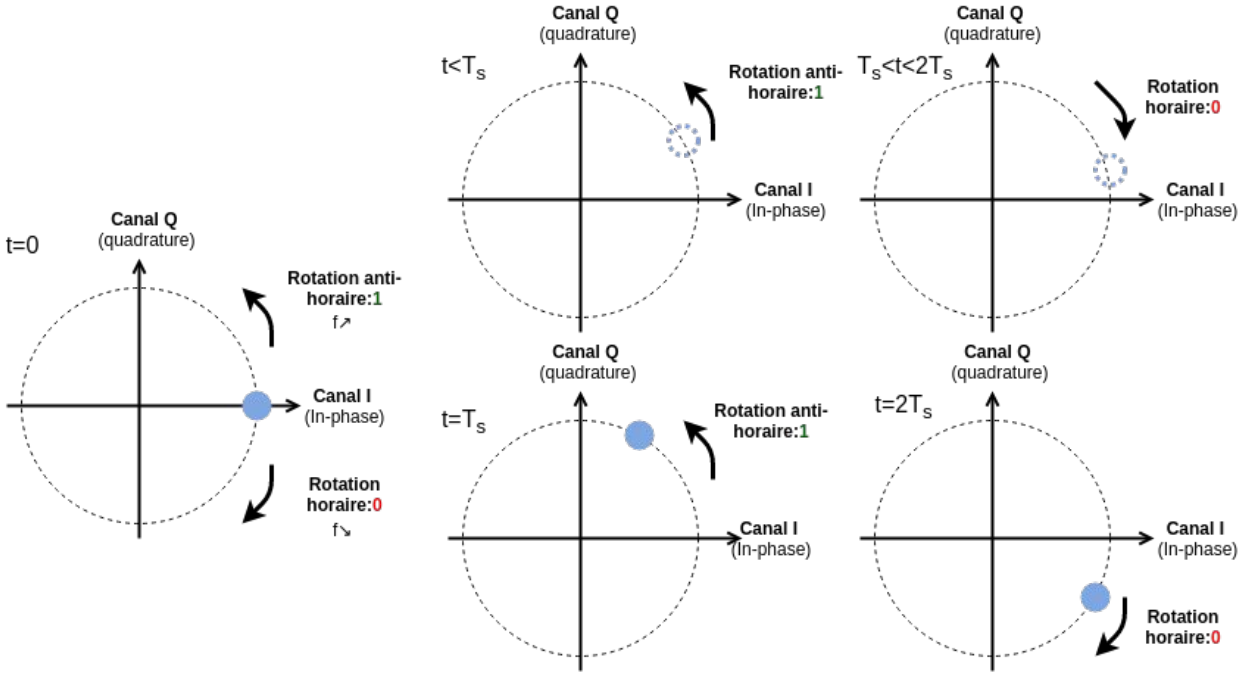
Avec:

- $T_s = 10^{-6}$s (1 Mbits/s) ou
  $T_s = 5 . 10^{-7}$s (2 Mbits/s)

- $0.45 \leq m \leq 0.55$



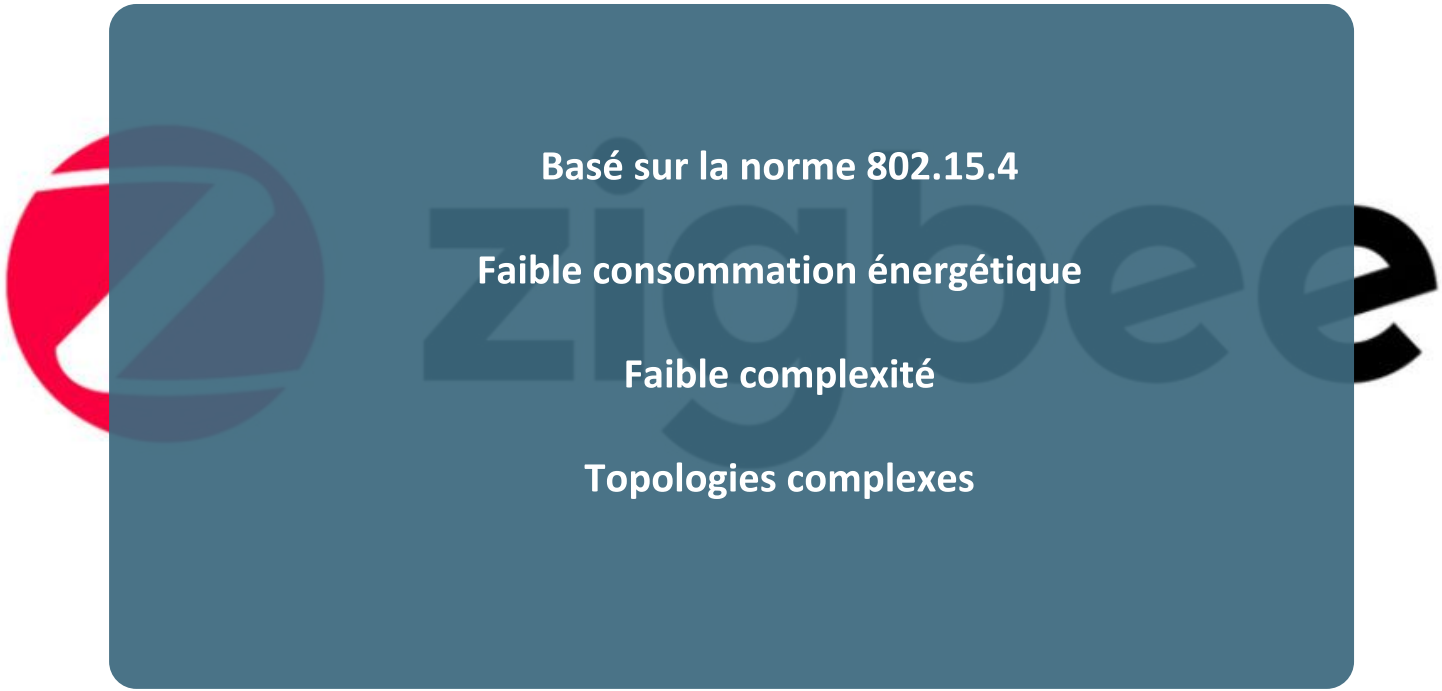
BLUETOOTH LOW ENERGY - MODULATION



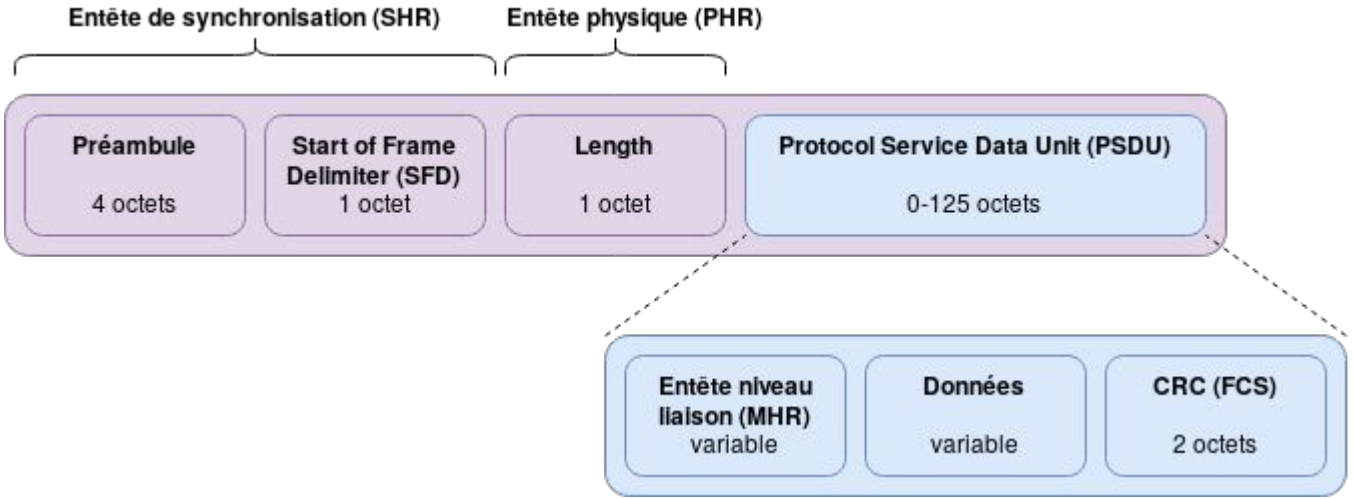
Constellation représentant une 2-FSK **Transmission d'un bit de valeur 1** **Transmission d'un bit de valeur 0**

ZIGBEE - PRÉSENTATION GÉNÉRALE

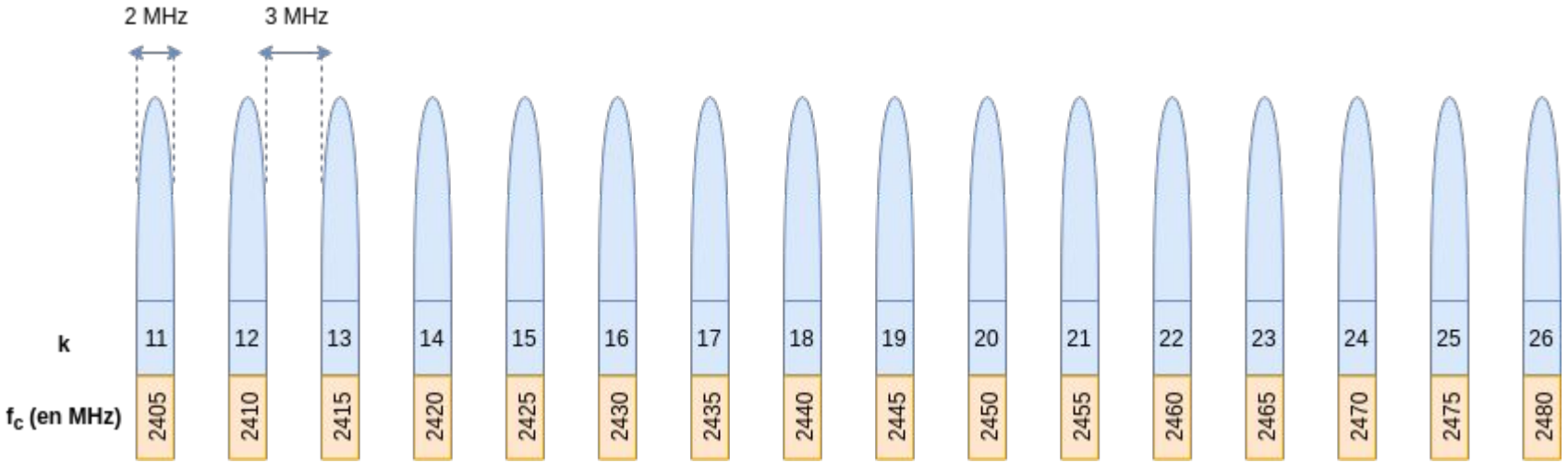
ZIGBEE - PRÉSENTATION GÉNÉRALE



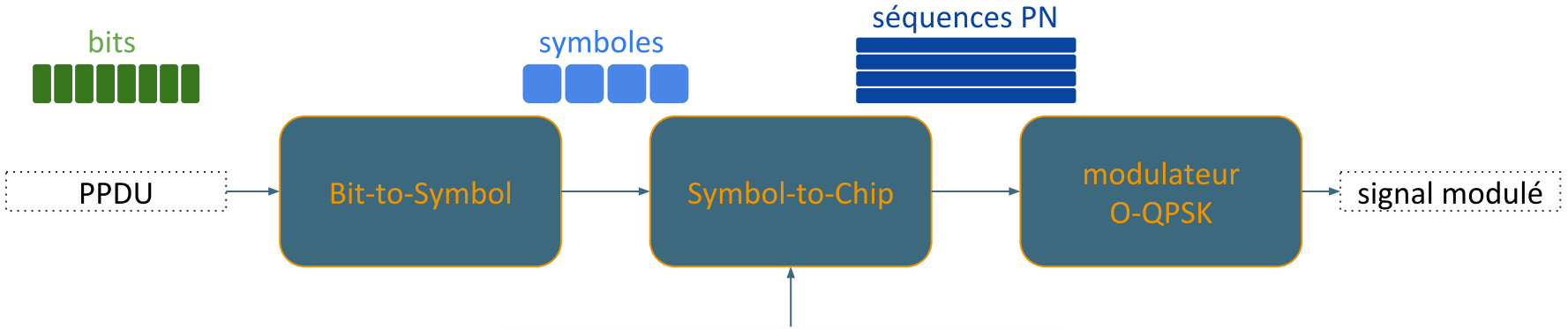
ZIGBEE - FORMAT DE PAQUET



ZIGBEE -CANAUX DE COMMUNICATION

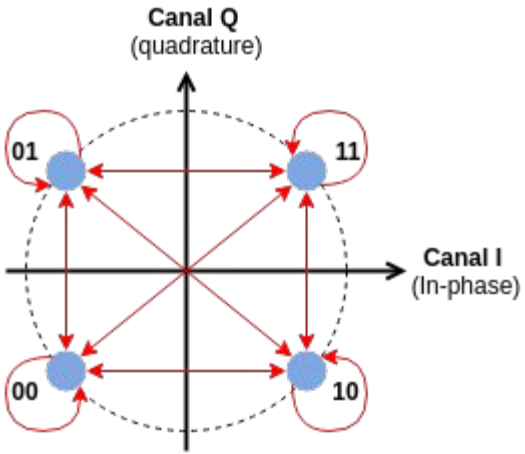


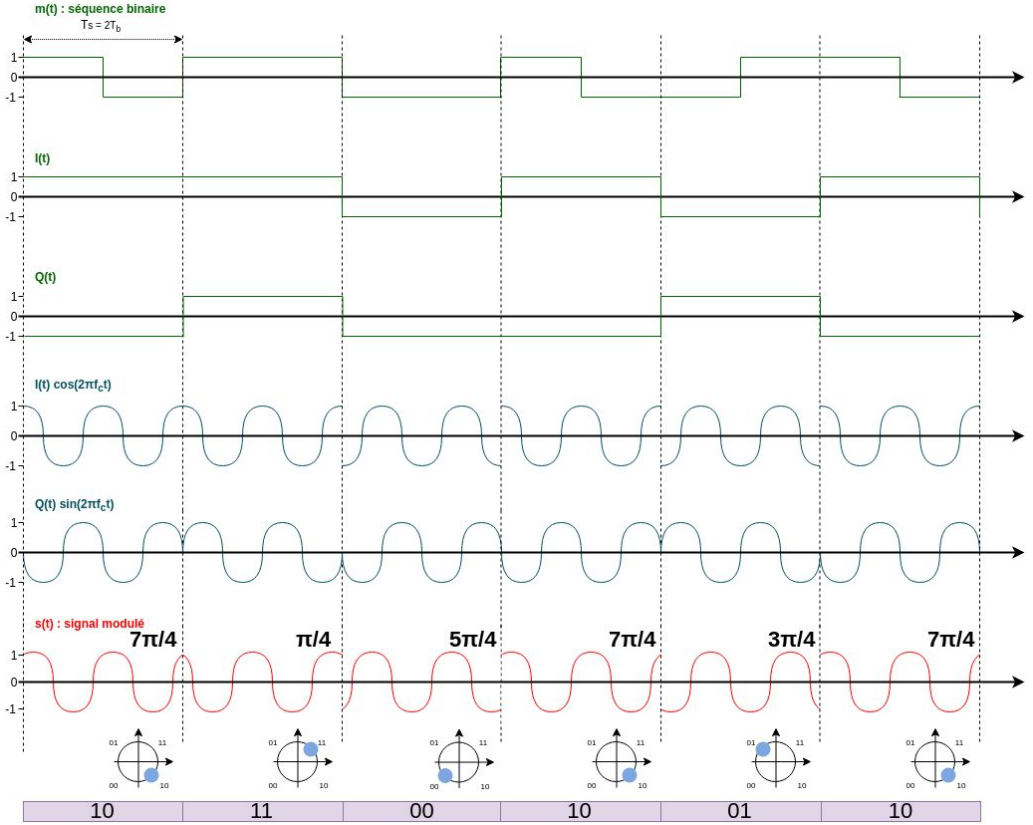
ZIGBEE - DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)



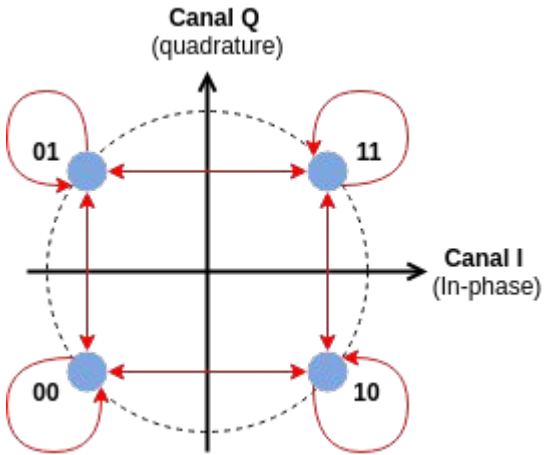
Bloc ($b_0b_1b_2b_3$)	Séquence PN (c_0c_1 ... $c_{30}c_{31}$)
0000	11011001 11000011 01010010 00101110
1000	11101101 10011100 00110101 00100010
0100	00101110 11011001 11000011 01010010
1100	00100010 11101101 10011100 00110101
0010	01010010 00101110 11011001 11000011
1010	00110101 00100010 11101101 10011100
0110	11000011 01010010 00101110 11011001
1110	10011100 00110101 00100010 11101101
0001	10001100 10010110 00000111 01111011
1001	10111000 11001001 01100000 01110111
0101	01111011 10001100 10010110 00000111
1101	01110111 10111000 11001001 01100000
0011	00000111 01111011 10001100 10010110
1011	01100000 01110111 10111000 11001001
0111	10010110 00000111 01111011 10001100
1111	11001001 01100000 01110111 10111000

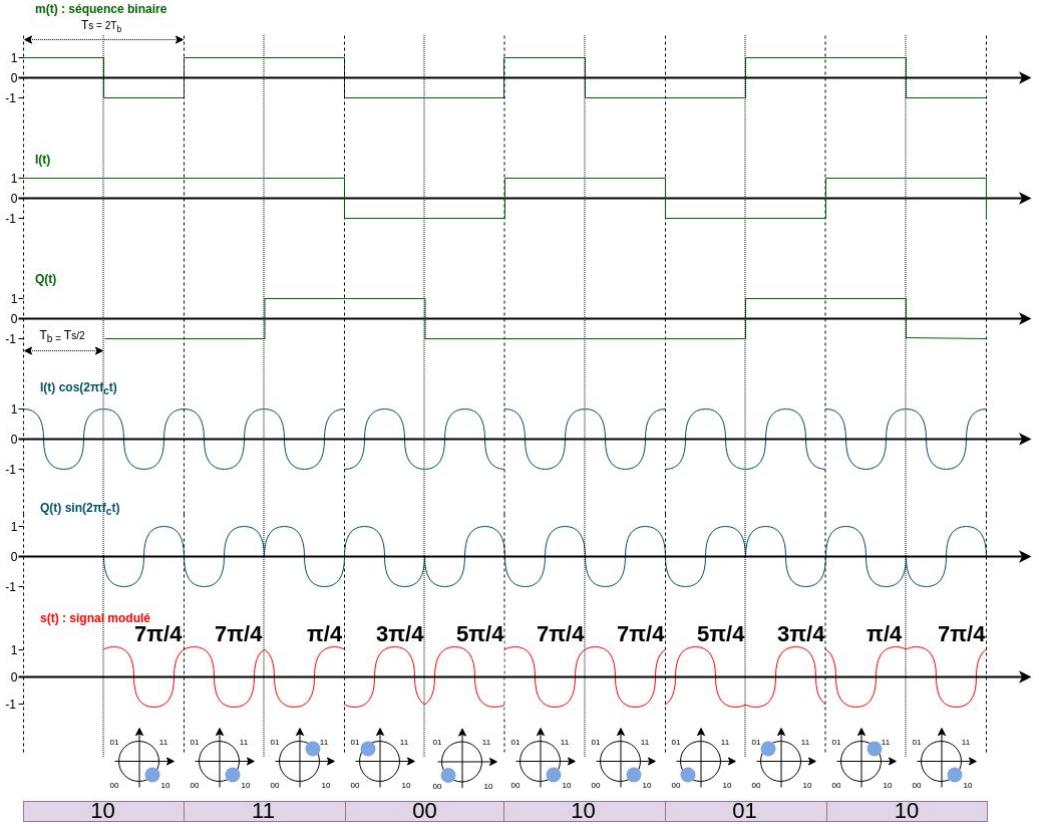
ZIGBEE - MODULATION (QPSK)



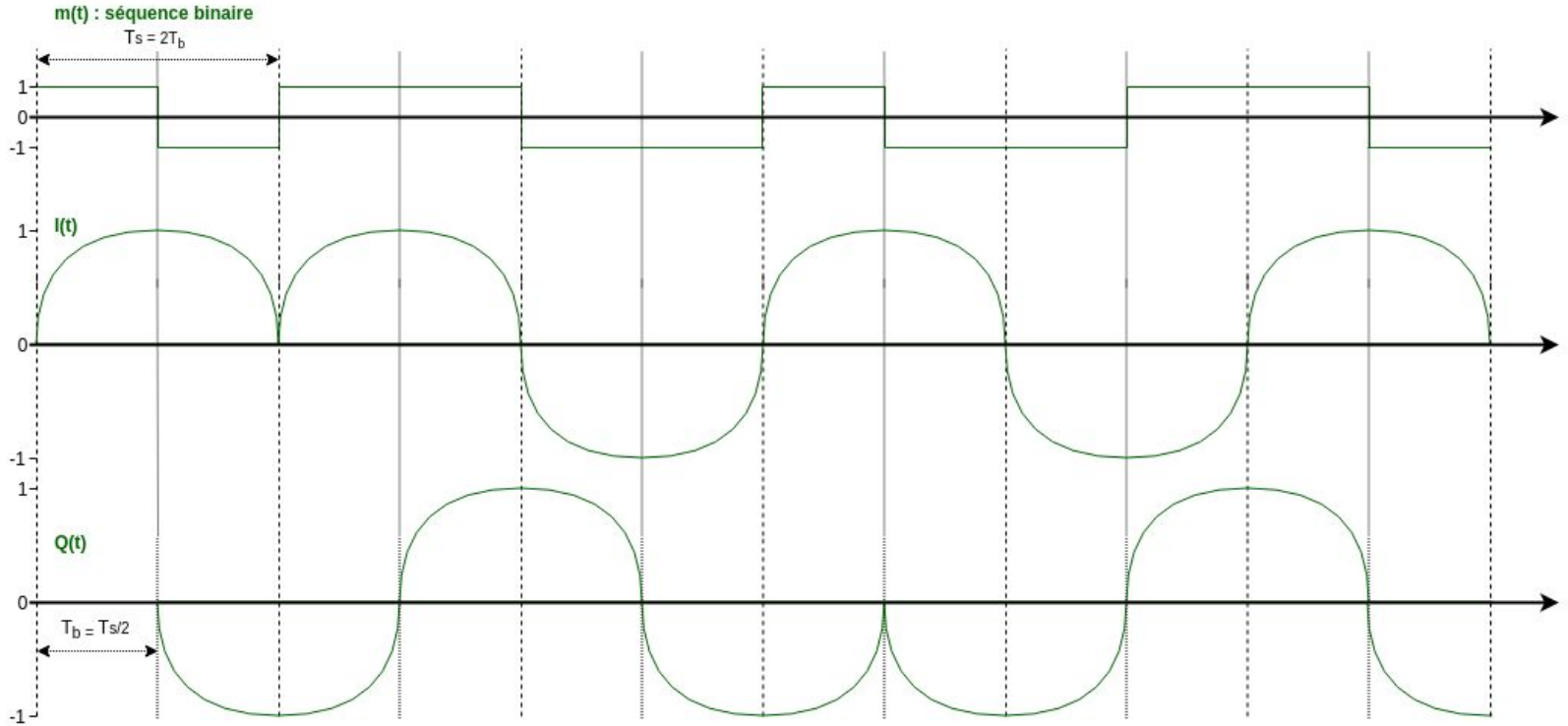


ZIGBEE - MODULATION (O-QPSK)





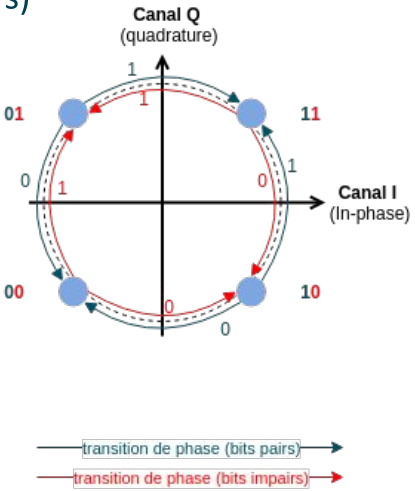
ZIGBEE - MODULATION (O-QPSK À IMPULSION SEMI-SINUSOÏDALE)

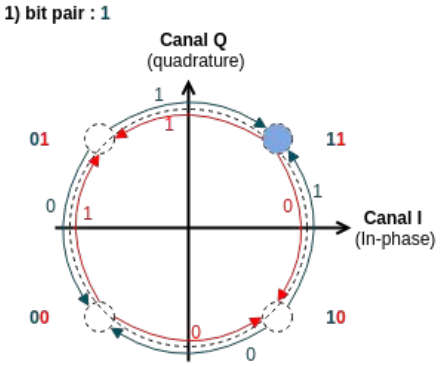


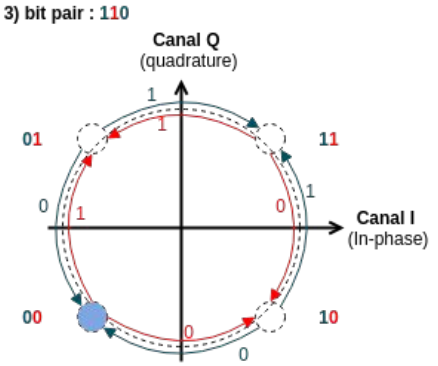
ZIGBEE - MODULATION (O-QPSK À IMPULSION SEMI-SINUSOÏDALE)

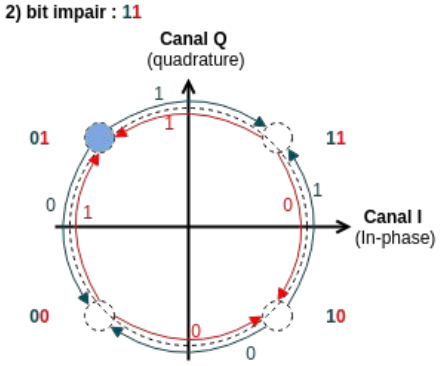
Avec:

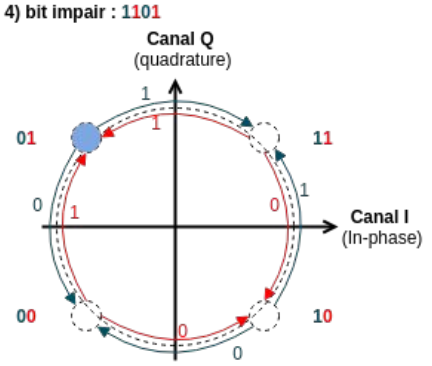
$T_B = 5 . 10^{-7}s$ (2 Mchips/s)











PRÉSENTATION DE L'ATTAQUE WAZABEE

WAZABEE - PRINCIPES THÉORIQUES

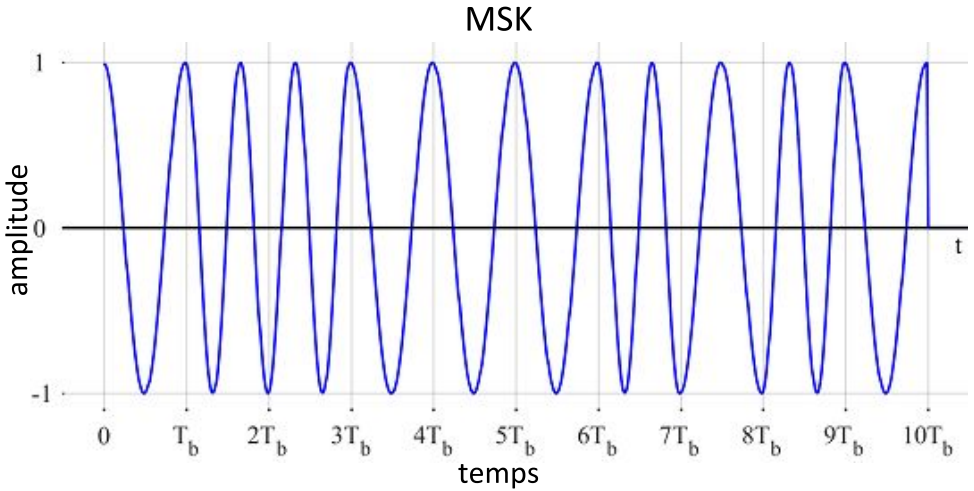
De la GFSK à la MSK

- Amplitude constante, phase continue
- GMSK : équivalent à une GFSK avec m = 0.5 (aux instants d'échantillonnage)
- Dans le cas du BLE: $0.45 \leq m \leq 0.55$
- Si on néglige le filtre gaussien : GMSK ~ MSK (évolution linéaire de la phase de +- $\pi/2$)

WAZABEE - PRINCIPES THÉORIQUES

De la MSK à l'O-QPSK

- Amplitude constante, phase continue et linéaire
- A chaque transition: +π/2 ou -π/2
- Équivalence théorique entre l'O-QPSK (mise en forme par impulsion semi-sinusoïdale) et la MSK, avec le codage adéquat et $T_{b(O\text{-}QPSK)} = T_{S(MSK)}$
- MSK ~ $O\text{-}QPSK_{semi\text{-}sinusoïdale}$



WAZABEE - PRINCIPES THÉORIQUES

Du BLE au Zigbee

Si on néglige le filtre gaussien, on peut faire l'approximation suivante :

BLE = GFSK ~ GMSK ~ MSK ~ O-QPSK$_{\text{semi-sinusoïdale}}$ = 802.15.4 (utilisé par Zigbee)

On peut donc faire les hypothèses suivantes:

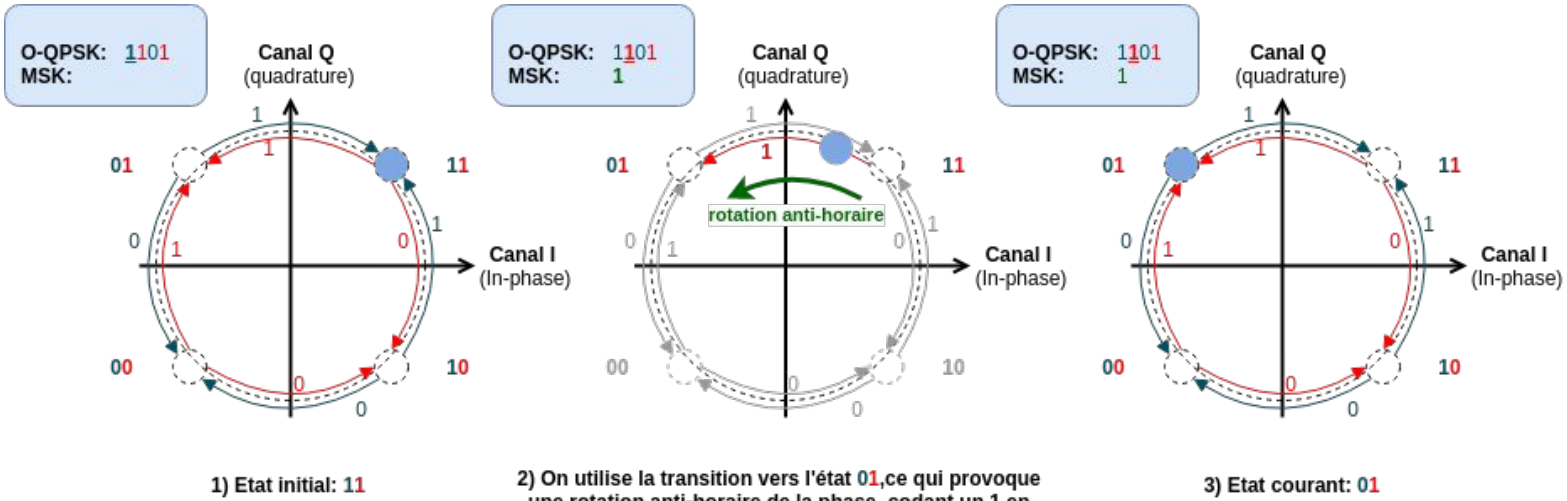
- **Contrôler le message fourni en entrée d'un modulateur GFSK** compatible avec la **spécification du BLE** devrait permettre de **générer un signal modulé** correspondant à une séquence binaire **interprétable par un démodulateur O-QPSK** (mis en forme par une impulsion semi-sinusoïdale) compatible avec la norme **802.15.4**

- Un **message arbitraire modulé par un modulateur O-QPSK** (mis en forme par une impusion semi-sinusoïdale) **compatible avec la norme 802.15.4** devrait générer un signal modulé correspondant à une séquence binaire **interprétable par un démodulateur GFSK** compatible avec **la spécification du BLE**

WAZABEE - GÉNÉRATION DE LA TABLE DE CORRESPONDANCE

Objectif: convertir une séquence PN codée en O-QPSK en une séquence équivalente codée en MSK

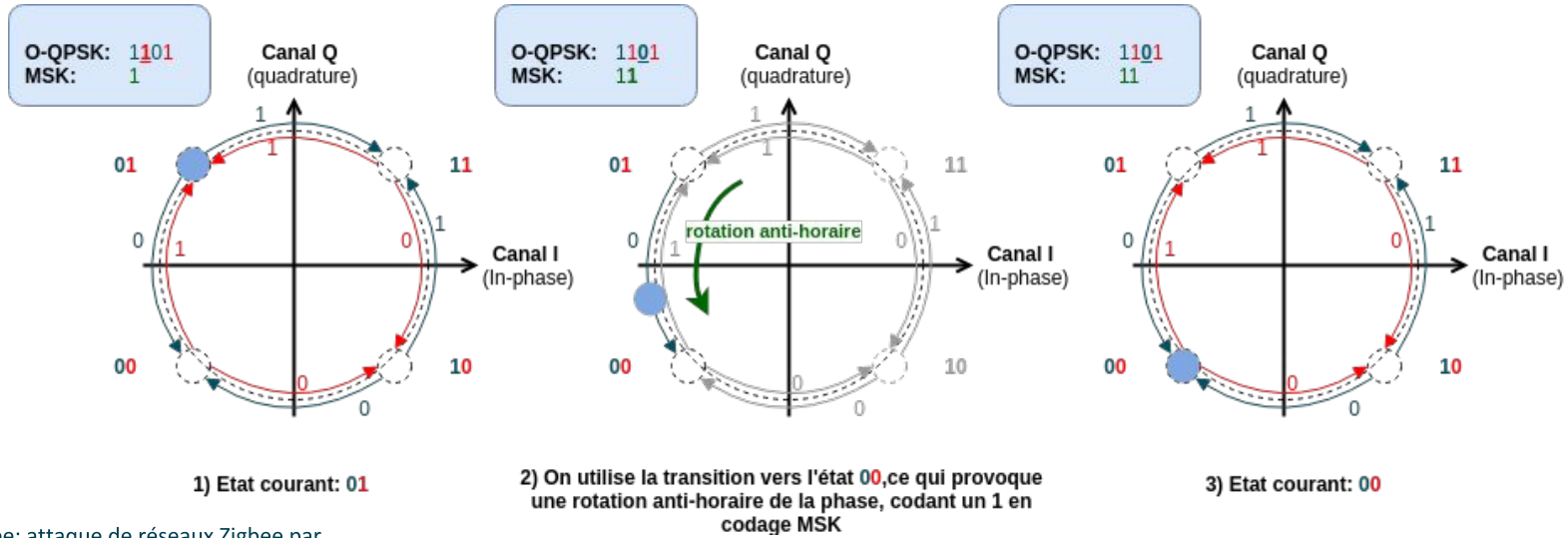
Principe: observer les transitions de phase: une rotation anti-horaire code un 1, une rotation horaire code un 0



WAZABEE - GÉNÉRATION DE LA TABLE DE CORRESPONDANCE

Objectif: convertir une séquence PN codée en O-QPSK en une séquence équivalente codée en MSK

Principe: observer les transitions de phase: une rotation anti-horaire code un 1, une rotation horaire code un 0



1) Etat courant: 01

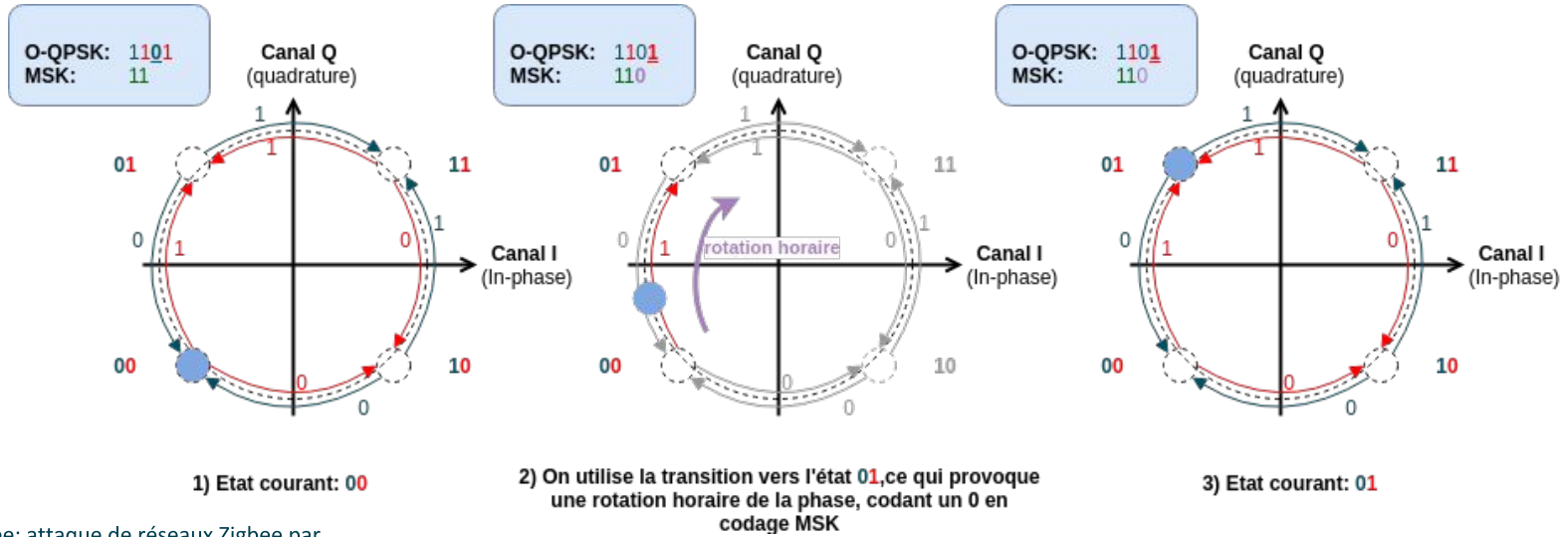
2) On utilise la transition vers l'état 00,ce qui provoque une rotation anti-horaire de la phase, codant un 1 en codage MSK

3) Etat courant: 00

WAZABEE - GÉNÉRATION DE LA TABLE DE CORRESPONDANCE

Objectif: convertir une séquence PN codée en O-QPSK en une séquence équivalente codée en MSK

Principe: observer les transitions de phase: une rotation anti-horaire code un 1, une rotation horaire code un 0



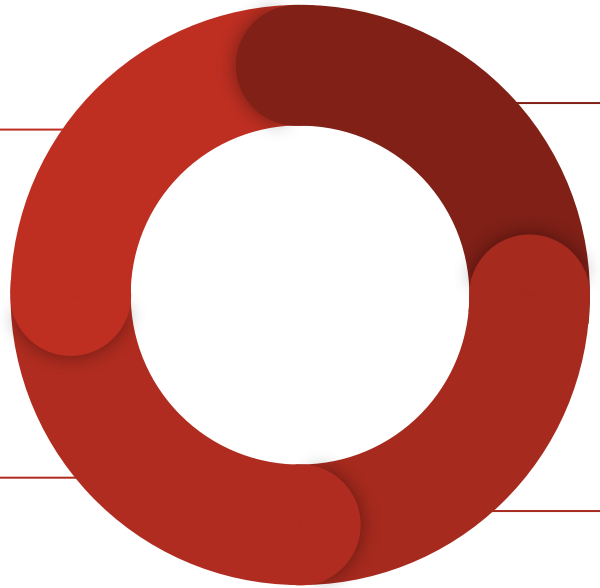
WAZABEE - GÉNÉRATION DE LA TABLE DE CORRESPONDANCE

Bloc $(b_0b_1b_2b_3)$	Séquence PN - codage MSK $(m_0m_1 \ldots m_{29}m_{30})$
0000	11000000111011110101110011011 00
1000	10011100000011101111010111001 10
0100	01011001110000001110111101011 10
1100	01001101100111000000111011110 10
0010	11011100110110011100000011101 11
1010	01110101110011011001110000001 11
0110	11101111010111001101100111000 00
1110	00001110111101011100110111001 10
0001	00111111000100001010001100100 11
1001	01100011111100010000101000110 01
0101	10100110001111110001000010100 01
1101	10110010011000111111000100000 101
0011	00100011001001100011111100010 00
1011	10001010001100100110001111111 000
0111	00010000101000110010011000111 11
1111	11110001000010100011001001100 01

WAZABEE - CONTRAINTES

Contrôler le débit de données

Contrôler la fréquence centrale



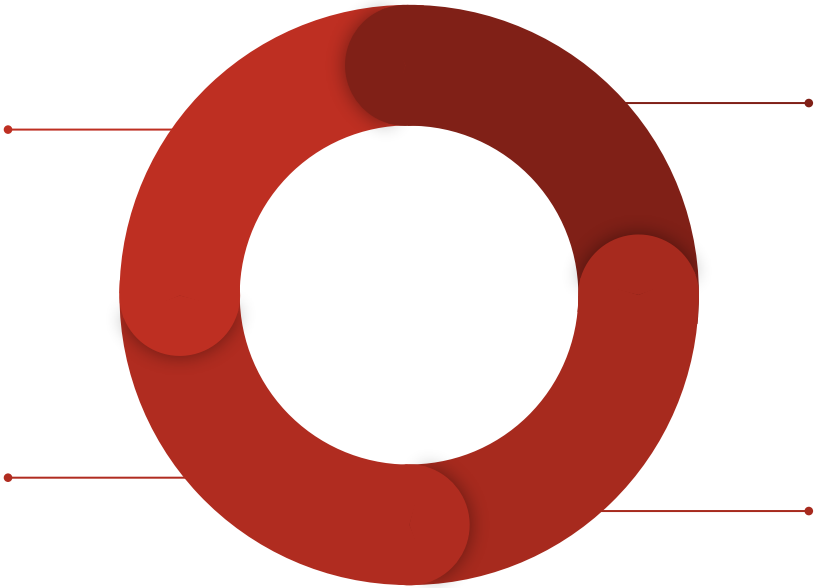
Contrôler les données en entrée du modulateur

Contrôler les données en sortie du démodulateur

WAZABEE - CONTRAINTES

Contrôler le débit de données

Utiliser le mode *PHY 2M*



Contrôler les données en entrée du modulateur

Contrôler la fréquence centrale

Contrôler les données en sortie du démodulateur

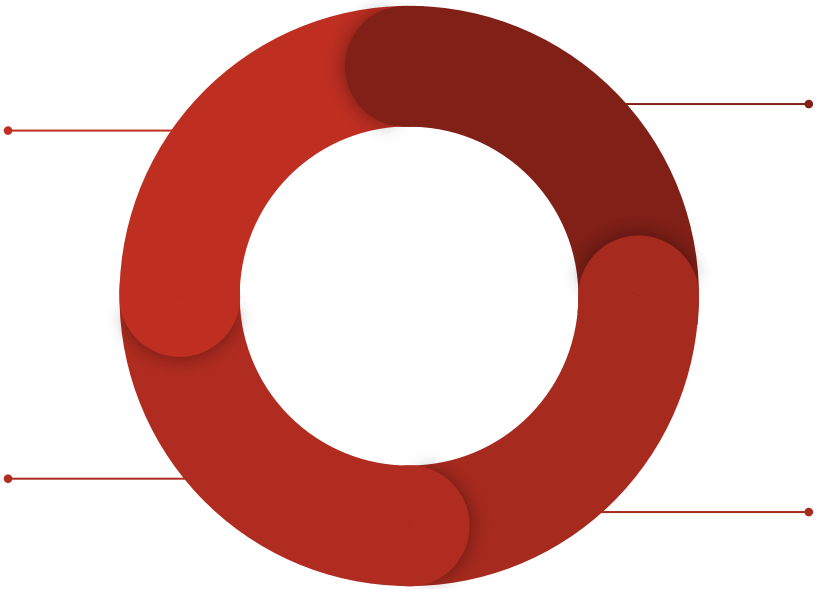
WAZABEE - CONTRAINTES

Contrôler le débit de données

Utiliser le mode *PHY 2M*

Contrôler la fréquence centrale

Contrôle direct ou superposition de canaux



Contrôler les données en entrée du modulateur

Contrôler les données en sortie du démodulateur

WAZABEE - CONTRAINTES

Contrôler le débit de données

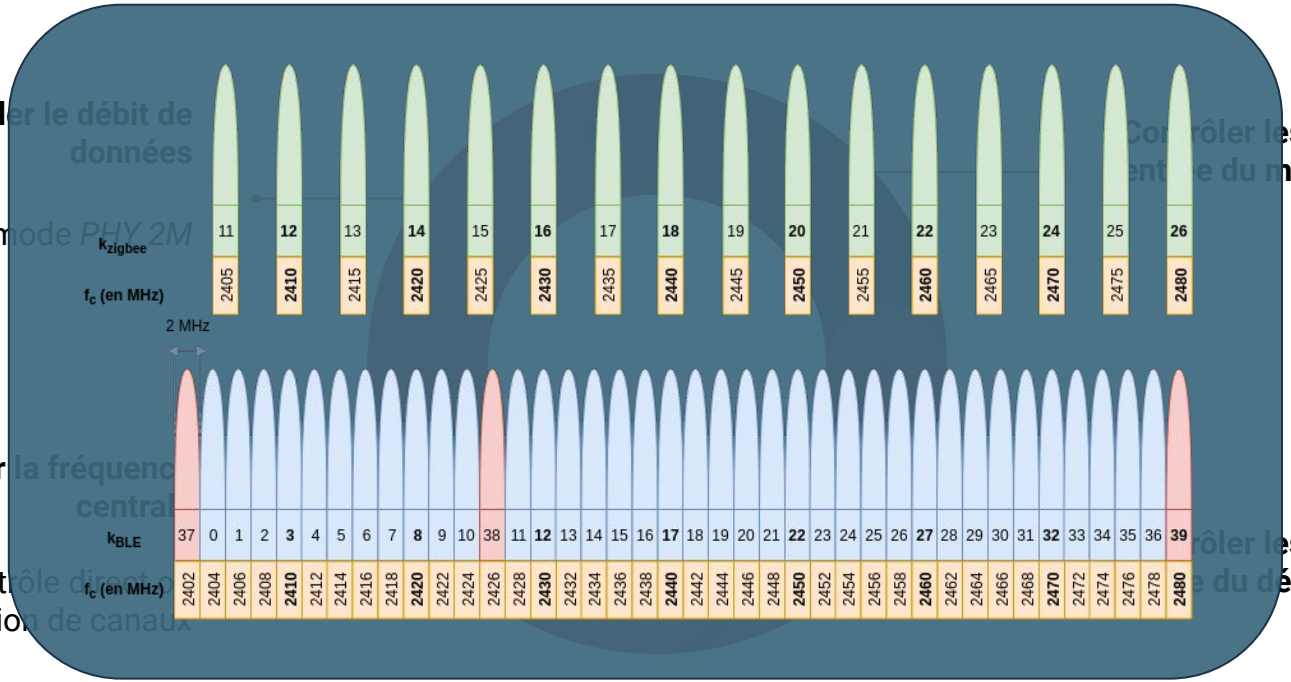
Utiliser le mode *PHY 2M*

Contrôler la fréquence centrale

Contrôle direct sur la superposition de canaux

Contrôler les données en entrée du modulateur

Contrôler les données en entrée du démodulateur



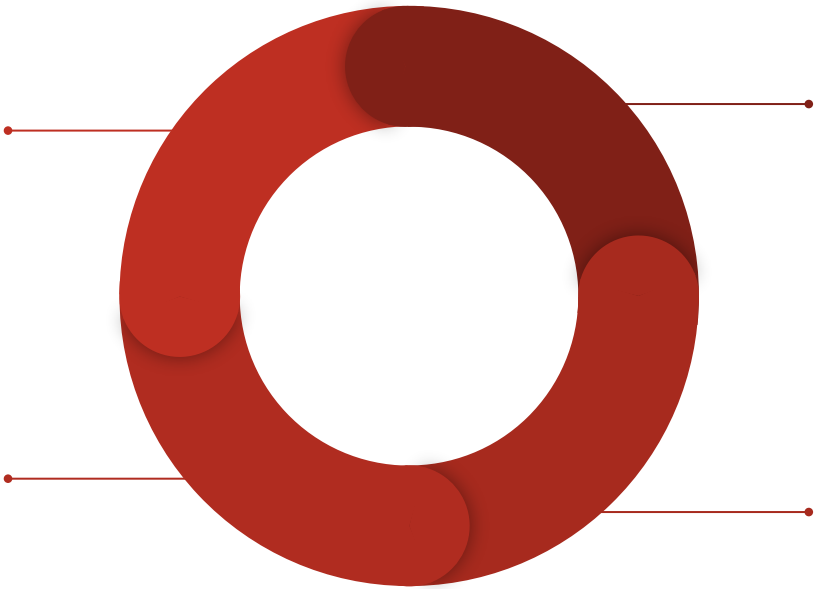
WAZABEE - CONTRAINTES

Contrôler le débit de données

Utiliser le mode *PHY 2M*

Contrôler la fréquence centrale

Contrôle direct ou superposition de canaux



Contrôler les données en entrée du modulateur

Désactiver ou annuler le *whitening*

Contrôler les données en sortie du démodulateur

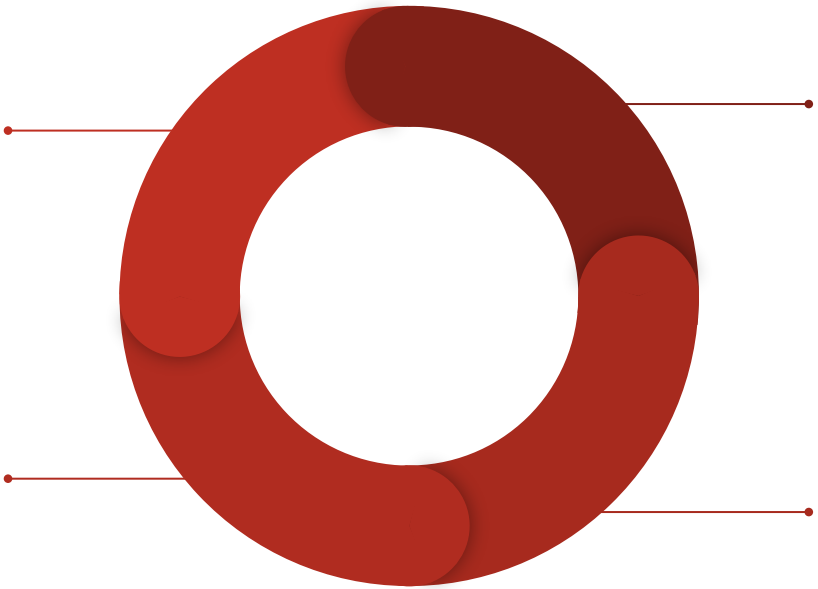
WAZABEE - CONTRAINTES

Contrôler le débit de données

Utiliser le mode *PHY 2M*

Contrôler la fréquence centrale

Contrôle direct ou superposition de canaux



Contrôler les données en entrée du modulateur

Désactiver ou annuler le *whitening*

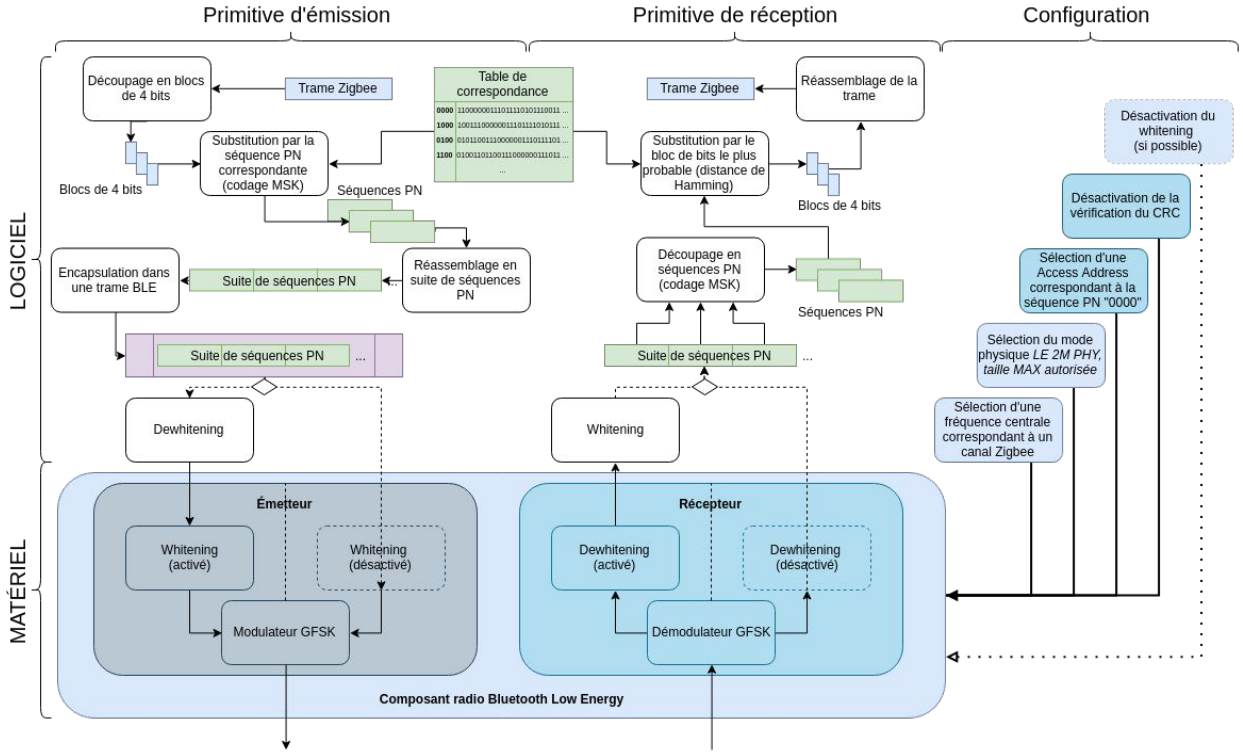
Contrôler les données en sortie du démodulateur

Désactiver ou annuler le *dewhitening*

Désactiver la vérification du CRC et configurer la taille maximale

Utiliser l'*Access Address* comme motif de détection

WAZABEE - CONTRAINTES



EXPÉRIMENTATIONS: IMPLÉMENTATIONS ET ÉVALUATIONS

WAZABEE - IMPLÉMENTATIONS

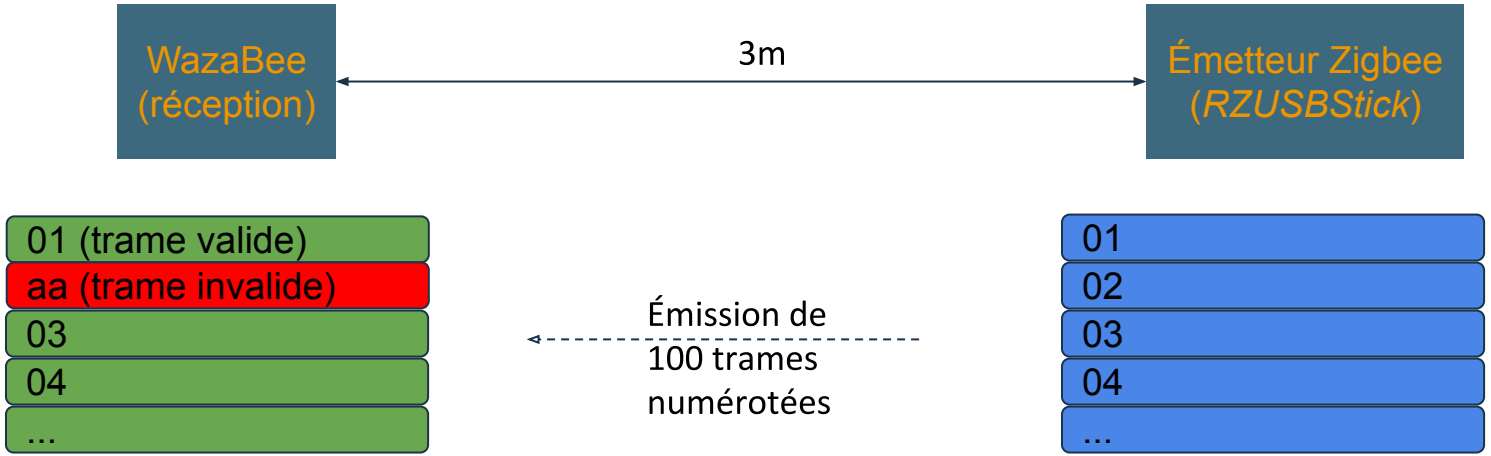
nRF52832 (Adafruit nRF52 Feather)

- carte de développement basée sur le nRF52832
- librairies Arduino disponibles
- vulnérabilité sur le registre de sélection d'adresse
- "facilement détournable"
- configuration par l'intermédiaire de registres

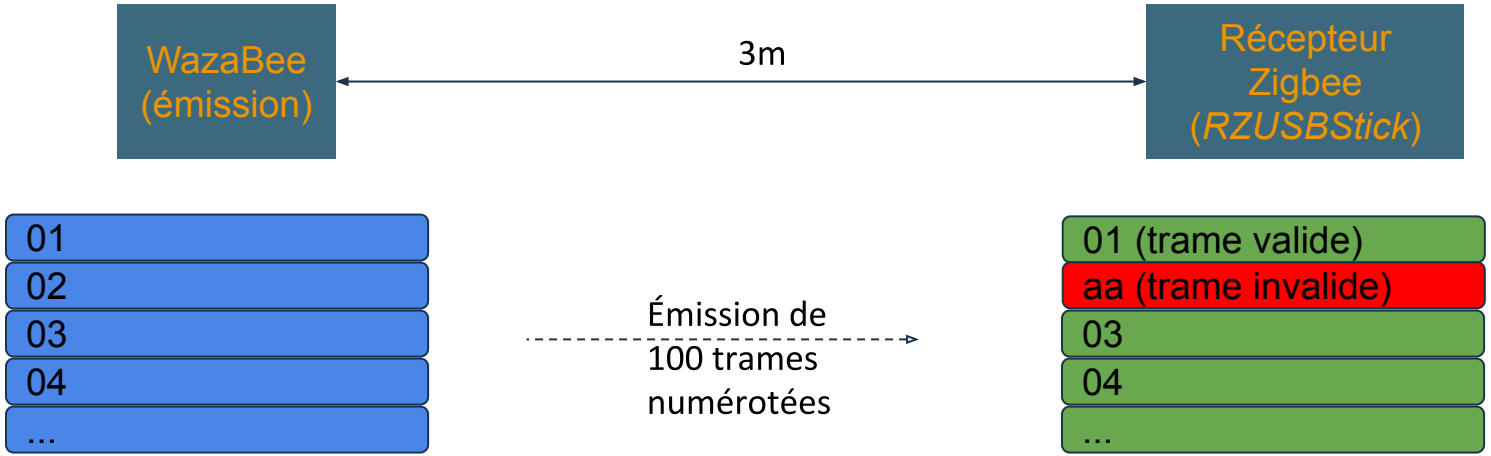
CC1352-R1 (Texas Instruments)

- carte de développement multi-protocoles
- utilisation des commandes BLE 5 uniquement
- supportée par le sniffer *Sniffle*
- peu détournée
- configuration par l'intermédiaire de commandes

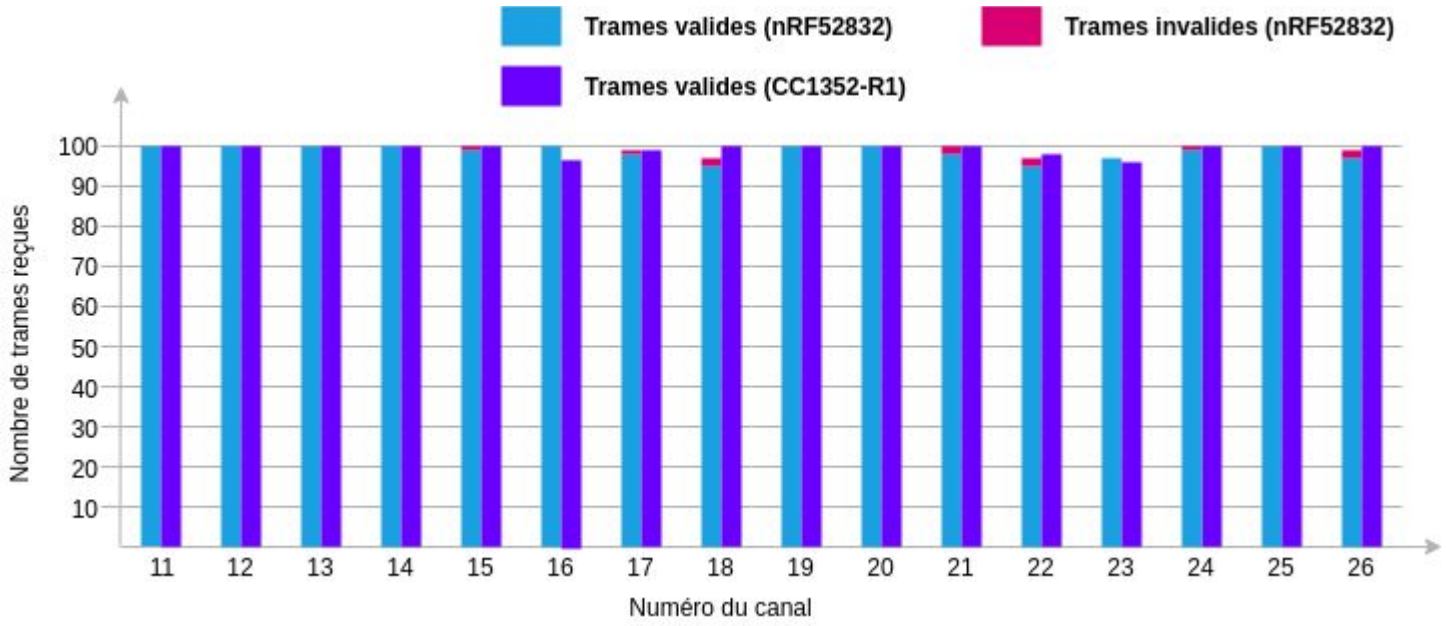
WAZABEE - ÉVALUATION DE LA PRIMITIVE DE RÉCEPTION



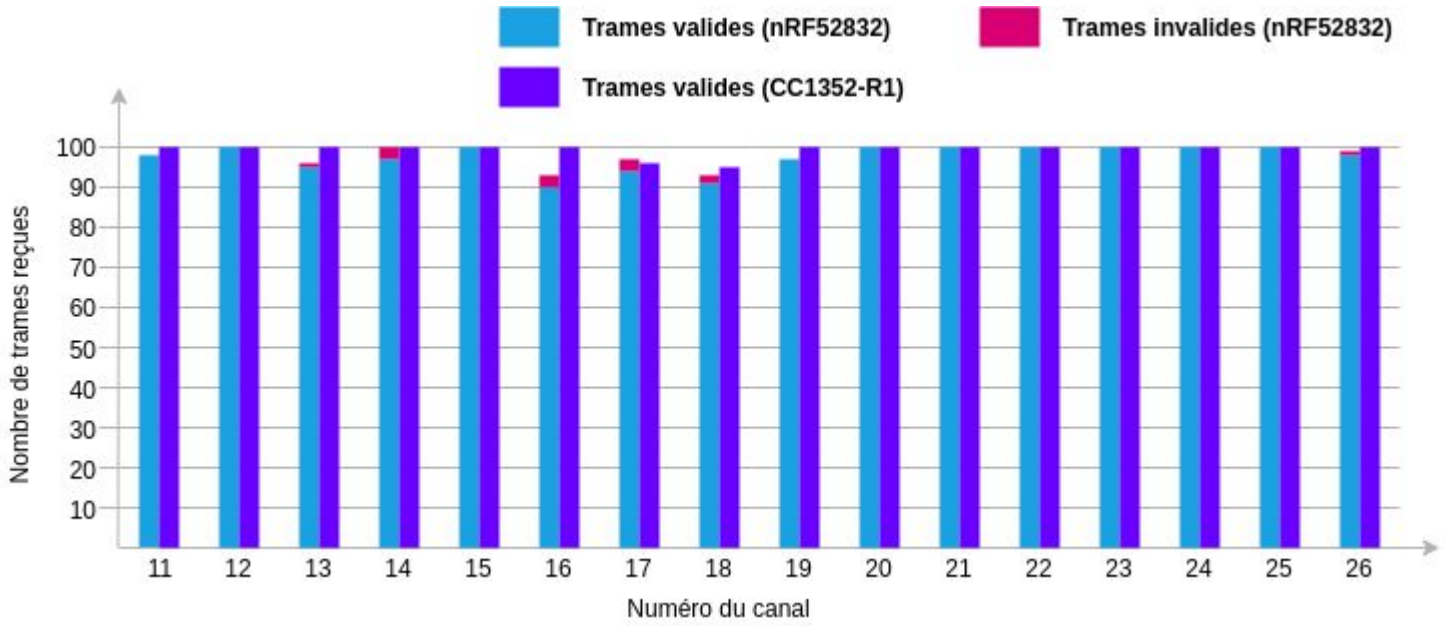
WAZABEE - ÉVALUATION DE LA PRIMITIVE D'ÉMISSION



WAZABEE - RÉSULTATS (PRIMITIVE DE RÉCEPTION)



WAZABEE - RÉSULTATS (PRIMITIVE D'ÉMISSION)



CONCLUSION: ENJEUX ET PERSPECTIVES

CONCLUSION: ENJEUX ET PERSPECTIVES

- **Problématique peu explorée**: à l'interface entre **traitement du signal** et **sécurité**

- Utilisable dans un contexte **d'attaque pivot** ou **d'exfiltration de données**

- **Impact critique:** coexistence de technologies sans fil, mobilité, environnements dynamiques ...

- **Généralisable** à d'autres technologies ?

- Peu de contre-mesures adaptées: **filtrage physique**, **monitoring multi-protocoles** (y compris sur les protocoles non déployés !)

Merci pour votre attention !