



**HAL**  
open science

# Contributions pour le standard IoT LoRa : améliorations du récepteur classique et de sa sécurisation

Clément Demeslay

## ► To cite this version:

Clément Demeslay. Contributions pour le standard IoT LoRa : améliorations du récepteur classique et de sa sécurisation. Réseaux et télécommunications [cs.NI]. Université de Bretagne occidentale - Brest, 2023. Français. NNT : 2023BRES0083 . tel-04832450

**HAL Id: tel-04832450**

**<https://theses.hal.science/tel-04832450v1>**

Submitted on 12 Dec 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# THÈSE DE DOCTORAT DE

L'UNIVERSITÉ DE BRETAGNE OCCIDENTALE

ÉCOLE DOCTORALE N° 644

*Mathématiques et Sciences et Technologies*

*de l'Information et de la Communication en Bretagne Océane*

Spécialité : *Télécommunications*

Par

**Clément DEMESLAY**

**Contributions pour le standard IoT LoRa : améliorations du récepteur classique et de sa sécurisation**

Thèse présentée et soutenue à Brest, le 11 Décembre 2023

Unité de recherche : Lab-STICC, CNRS, UMR 6285

## Rapporteurs avant soutenance :

Jean-François DIOURIS Professeur, Polytech Nantes  
Yannis POUSSET Professeur, Université de Poitiers

## Composition du Jury :

Président :	Pascal CHARGE	Professeur, Polytech Nantes
Examineurs :	Jérôme LOUVEAUX	Professeur, UCLouvain
	Pascal CHARGE	Professeur, Polytech Nantes
	Karine AMIS	Professeur, IMT-Atlantique
	Jean-François DIOURIS	Professeur, Polytech Nantes
	Yannis POUSSET	Professeur, Université de Poitiers
	Philippe ROSTAING	Maître de Conférences, Université de Bretagne Occidentale
Dir. de thèse :	Roland GAUTIER	Professeur, Université de Bretagne Occidentale
Co-dir. de thèse :	Gilles BUREL	Professeur, Université de Bretagne Occidentale

## Invité(s) :

Pierre O. PASQUERO Ingénieur de recherche, DGA-MI Rennes  
Marc LE ROY Professeur, HDR, Université de Bretagne Occidentale  
Anthony FICHE Maître de Conférences, Université de Bretagne Occidentale



## Remerciements

Ce projet de recherche au sein de l'équipe Sécurité, Intelligence et Intégrité de l'Information (SI3) du Lab-STICC a bien sûr été une aventure technique, mais surtout humaine. L'aboutissement, que représente ce mémoire, n'aurait pas pu être sans l'intervention, à plusieurs niveaux, d'un grand nombre de personnes.

Je souhaiterais tout d'abord remercier mes directeurs de thèse Roland Gautier et Gilles Burel pour m'avoir permis de mener à bien toutes les phases de la thèse : exploration des pistes de recherche, consolidation des idées, rédaction et publication des articles, présentations orales pour la valorisation des travaux, démarches administratives et la rédaction du manuscrit. Je les remercie également pour les très nombreux échanges enrichissants que nous avons eu tout au long de la thèse, et m'ayant permis d'adopter des points de vue parfois éloignés.

Je tiens particulièrement à remercier Philippe Rostaing, Maître de Conférences au sein de l'équipe, pour son important investissement dans ce projet, ses idées et propositions d'une grande pertinence, et pour m'avoir permis de consolider mes compétences rédactionnelles, surtout pour les articles.

Je remercie la chaire CyberIoT, sans qui ce projet ambitieux n'aurait pu voir le jour, et pour l'organisation de la journée du pôle T2I3 du Lab-STICC en janvier 2023, où les nombreux échanges que j'ai eus avec les collègues m'ont permis de faire avancer ma thématique de recherche.

Je tiens à remercier les membres du Comité de Suivi Individuel (CSI) : Pascal Chargé et Stéphane Azou, respectivement Maître de Conférences à Polytech Nantes et Professeur à l'ENIB, pour m'avoir aidé à faire le bilan des travaux chaque année passée, et d'avoir proposé très pertinemment la piste du Peak-to-Average Power Ratio (PAPR) LoRa, retenue dans ce manuscrit.

Je remercie également Angela Digulescu, Maître de Conférences à l'ATM de Bucarest en Roumanie, pour m'avoir accueilli au sein de l'ATM lors de ma mobilité de trois mois, réalisée à mi-parcours. Ses conseils et son expertise sur les équipements réels de transmission m'ont permis de prendre conscience de l'écart parfois considérable entre le monde de la théorie et celui du monde réel imprévisible.

Je remercie l'Institut Brestois du Numérique et des Mathématiques (IBNM) pour avoir soutenu financièrement la publication des articles et mon projet de mobilité à l'ATM.

Je remercie aussi le service Direction des Etudes et de la Vie Etudiante (DEVE) de l'Université de Bretagne Occidentale (UBO) pour sa participation au financement de la mobilité à l'ATM.

Je remercie ma mère, qui a toujours été là à mes côtés, et m'a remonté le moral dans les moments difficiles de la thèse.

Je ne remercierai jamais assez mes collègues doctorants de l'équipe : Jean-Baptiste



Fraisse, Zaynab Baydoun, Cristina Despina-Stoian et Hugo Pillin, pour leur bonne humeur et les échanges enrichissants, mais aussi ceux des autres équipes Smart Materials and Related Technologies (SMART) et DH du Lab-STICC, en particulier : Evan Roué, Steven Autret et Karim Kouny, pour leur apport de connaissances sur les premières couches physiques des télécommunications, et de prendre ainsi pleinement conscience de la richesse et la complexité du monde des télécommunications.

Je tiens à remercier les enseignants-chercheurs avec qui j'ai pu travailler dans le cadre de mon service d'enseignement : Ludovic Collin et Koffi Yao, qui m'ont permis de devenir un meilleur pédagogue, et de prendre du recul sur mes travaux.

Je remercie aussi mes co-encadrants, Anthony Fiche et Marc Le Roy. Anthony, pour avoir participé à plusieurs réunions d'avancement, et Marc, pour avoir engagé de futures collaborations avec l'équipe Dispositifs Hyperfréquence (DH) du Lab-STICC dont il fait partie.

Je remercie chaleureusement Pierre O. Pasquero et Alexis Bazin, ingénieurs de recherche au pôle Maîtrise de l'Information (MI) de la Direction Générale de l'Armement (DGA), pour m'avoir accueilli sur le site de Bruz, près de Rennes, lors d'une journée d'échanges en décembre 2021. Les échanges ont été très enrichissants.

Je salue Jean-François Diouris et Yannis Pousset, Professeurs respectivement à Polytech Nantes et au laboratoire xlim de Poitiers, rapporteurs avant soutenance, pour leur lecture méticuleuse du manuscrit et leur retour constructif sur l'amélioration de ce dernier.

Je conclurai en saluant Emanuel Radoi, Professeur au sein de l'équipe et collègue de mes directeurs de thèse, pour sa participation à une de mes réunions d'avancement, et ses conseils m'ayant aidé à consolider mon projet professionnel.

# Table des matières

<b>Introduction générale</b>	<b>22</b>
<b>I Présentation du standard LoRa</b>	<b>24</b>
<b>I.1 Cadre d'application de LoRa : l'IoT</b>	<b>25</b>
I.1.1 Qu'est-ce que l'IoT ?	25
I.1.1.1 Historique	25
I.1.1.2 Problématiques éthiques et encadrement	26
I.1.1.3 Scénarios de communications IoT	26
I.1.2 Des enjeux radicalement différents	27
I.1.2.1 Compromis pour la mise en œuvre d'une télécommunication	28
I.1.2.2 Comparaison avec les standards conventionnels	29
I.1.3 Standards et solutions commerciales IoT	30
I.1.3.1 Standards IoT	30
I.1.3.2 Comparaison croisée	32
<b>I.2 LoRa</b>	<b>35</b>
I.2.1 Applications commerciales et projets	35
I.2.2 Infrastructure LoRaWAN	36
I.2.2.1 Réseaux LoRaWAN	36
I.2.2.2 Mécanismes de sécurité LoRa actuels	37
I.2.3 État de l'art	38
I.2.3.1 Expression analytique du SER	38
I.2.3.2 Schémas de transmission améliorés	39
I.2.3.3 Synchronisation	39
I.2.4 Schéma de modulation LoRa	40
I.2.4.1 Modulation	40
I.2.4.2 Démodulation	44
I.2.4.3 Format de trame	47
I.2.5 Schéma bloc d'une transmission LoRa	48
I.2.5.1 Codage de canal	49
I.2.5.1.1 Codage	50
I.2.5.1.2 Décodage	50
I.2.5.2 Blanchiment et entrelacement	51
I.2.5.2.1 Blanchiment	51
I.2.5.2.2 Entrelacement	51
I.2.5.3 Codage de Gray	52
I.2.6 Synchronisation LoRa	53
I.2.6.1 Désynchronisations CFO, STO et SFO	53

I.2.6.1.1	CFO . . . . .	53
I.2.6.1.2	STO . . . . .	54
I.2.6.1.3	SFO . . . . .	55
I.2.6.2	Impact du CFO, STO et SFO sur la démodulation . . . . .	56
I.2.6.2.1	Impact du CFO . . . . .	56
I.2.6.2.2	Impact du STO . . . . .	58
I.2.6.2.3	Impact conjoint CFO et STO . . . . .	60
I.2.6.2.4	Impact du SFO . . . . .	61
I.2.6.3	Front-end de synchronisation . . . . .	63
I.2.6.3.1	Étape 1 – estimation et correction de $CFO_{frac}$ . . . . .	66
I.2.6.3.2	Étape 2 – pré-estimation de $STO_{frac}$ . . . . .	66
I.2.6.3.3	Étape 3 – pré-corrrection de $STO_{frac}$ et pré-estimation de $CFO_{int}$ et $STO_{int}$ . . . . .	67
I.2.6.3.4	Étape 4 – estimation finale de $STO_{frac}$ . . . . .	69
I.2.6.3.5	Étape 5 – correction de $STO_{frac}$ et estimation finale de $CFO_{int}$ et $STO_{int}$ . . . . .	69
I.2.6.3.6	Étape 6 – synchronisation de la trame . . . . .	70
I.2.6.4	Détection du préambule . . . . .	71
I.2.6.4.1	Détection du préambule par détection de symboles consécutifs identiques . . . . .	72
I.2.6.4.2	Détection du préambule par détection d'énergie . . . . .	73
I.2.6.4.3	Performances de détection du préambule . . . . .	74
I.2.6.4.4	Avantages et inconvénients des détecteurs . . . . .	75
I.2.7	Performances . . . . .	77
I.2.7.1	Performances dans un canal AWGN – synchronisation parfaite . . . . .	77
I.2.7.2	Performances du codage de canal . . . . .	79
I.2.7.3	Performances du front-end de synchronisation et impact du nombre de symboles du préambule . . . . .	80

## **II Améliorations du démodulateur standard LoRa 82**

### **II.1 Expressions analytiques du SER LoRa – canal multi-trajets et interférence LoRa 83**

II.1.1	Modèles de canal multi-trajets et d'interférence LoRa . . . . .	83
II.1.1.1	Modèle de canal multi-trajets . . . . .	83
II.1.1.2	Modèle d'interférence multi-utilisateurs LoRa . . . . .	84
II.1.2	Impact du canal multi-trajets et de l'interférence LoRa sur la démodulation . . . . .	85
II.1.2.1	Impact du canal multi-trajets sur la démodulation . . . . .	85
II.1.2.2	Impact de l'interférence LoRa sur la démodulation . . . . .	86
II.1.3	Résultats de simulation . . . . .	87
II.1.3.1	SER LoRa analytique dans un canal multi-trajets aligné . . . . .	87
II.1.3.2	Comparaison du SER LoRa analytique entre un canal multi-trajets aligné à deux répliques et un canal à décroissance exponentielle . . . . .	89
II.1.3.3	SER LoRa analytique avec interférence multi-utilisateurs . . . . .	89

### **II.2 Récepteur amélioré LoRa RAKE 93**

II.2.1	Récepteur TDEL de la littérature . . . . .	93
--------	--	----

II.2.2	Démodulation LoRa RAKE dans un canal multi-trajets aligné avec synchronisation parfaite . . . . .	94
II.2.2.1	Structure du démodulateur . . . . .	94
II.2.2.2	Réduction de la complexité calculatoire de LoRa RAKE : cand-LoRa RAKE . . . . .	96
II.2.2.3	Résultats de simulation . . . . .	96
II.2.2.3.1	Impact sur les performances SER de LoRa RAKE du seuil d'estimation des trajets du canal multi-trajets . . . . .	97
II.2.2.3.2	Impact du nombre de candidats sur les performances de LoRa RAKE . . . . .	98
II.2.2.3.3	Gain de réduction de complexité calculatoire LoRa RAKE avec candidats . . . . .	99
II.2.2.3.4	Comparaison des performances SER entre LoRa RAKE, d-cand-LoRa RAKE, TDEL et les récepteurs classiques . . . . .	99
II.2.3	Démodulation LoRa RAKE dans un canal multi-trajets non-aligné à deux trajets avec synchronisation temporelle et fréquentielle . . . . .	101
II.2.3.1	Modification du démodulateur LoRa RAKE . . . . .	102
II.2.3.2	Synchronisation LoRa RAKE– compensation de la dérive de phase . . . . .	105
II.2.3.3	Résultats de simulation . . . . .	107
II.2.3.3.1	Performances de l'algorithme de compensation de phase $CFO_{frac}$ . . . . .	107
II.2.3.3.2	Performances dans un canal multi-trajets non-aligné avec ou sans synchronisation parfaite . . . . .	108
<b>III</b>	<b>Brouillage intelligent LoRa</b>	<b>112</b>
<b>III.1</b>	<b>Confidentialité, brouillage et authentification des communications</b>	<b>113</b>
III.1.1	Confidentialité des communications . . . . .	113
III.1.1.1	Scénario de communication . . . . .	113
III.1.1.2	Solutions garantissant la confidentialité . . . . .	114
III.1.1.2.1	Discrétion de la communication . . . . .	114
III.1.1.2.2	Dégradation du signal reçu par l'intercepteur . . . . .	114
III.1.2	Brouillage d'attaque . . . . .	117
III.1.2.1	Comportements du brouilleur . . . . .	118
III.1.2.1.1	Comportement temporel . . . . .	118
III.1.2.1.2	Comportement fréquentiel – brouilleur Band Jamming . . . . .	119
III.1.2.1.3	Comportement fréquentiel – brouilleur Tone Jamming . . . . .	120
III.1.2.2	Brouilleurs et contre-mesures dans la littérature . . . . .	121
III.1.2.2.1	Brouilleurs Hopping et OFDM . . . . .	121
III.1.2.2.2	Brouilleurs radar et GPS . . . . .	122
III.1.3	Authentification . . . . .	123
III.1.3.1	Authentification par le réseau . . . . .	123
III.1.3.2	Authentification par identification radio-fréquence . . . . .	125
<b>III.2</b>	<b>Impact des brouilleurs classiques Band et Tone Jamming sur LoRa</b>	<b>127</b>
III.2.1	Impact des brouilleurs Band et Tone Jamming sur la DFT LoRa . . . . .	127
III.2.1.1	Impact du brouilleur Band Jamming sur la DFT LoRa . . . . .	127
III.2.1.2	Impact du brouilleur Tone Jamming sur la DFT LoRa . . . . .	128

III.2.2	Détecteur LoRa de brouilleurs Band et Tone Jamming . . . . .	129
III.2.2.1	Lois de probabilités des bins DFT . . . . .	129
III.2.2.2	Construction du détecteur . . . . .	130
III.2.2.3	Loi de probabilité de la quantité statistique de détection sous l'hypothèse $H_0$ . . . . .	131
III.2.2.4	Loi de probabilité de la quantité statistique de détection d'un brouilleur Band Jamming sous l'hypothèse $H_1$ . . . . .	132
III.2.2.5	Loi de probabilité de la quantité statistique de détection d'un brouilleur Tone Jamming sous l'hypothèse $H_1$ . . . . .	132
III.2.2.6	Comparaison entre les expressions analytiques et les histogrammes des lois de probabilité sous les deux hypothèses pour le brouilleur Band Jamming . . . . .	132
III.2.3	Résultats de simulation . . . . .	133
III.2.3.1	Influence de la valeur de symbole sur le SER en présence de brouilleur Tone Jamming . . . . .	133
III.2.3.2	Performances analytiques de détection des brouilleurs Band et Single Tone Jamming . . . . .	134
III.2.3.3	Comparaison entre les performances de détection (analytique et simulation) pour les brouilleurs Band et Single Tone Jamming . . . . .	136
III.2.3.4	Impact du nombre de composantes fréquentielles sur la détection du brouilleur Tone Jamming . . . . .	136
<b>III.3</b>	<b>Schéma d'auto-brouillage LoRa partie 1 : modèle, architecture et paramètres</b>	<b>139</b>
III.3.1	Travaux sur la sécurisation de la couche physique LoRa dans la littérature	140
III.3.2	Scénario de communication LoRa . . . . .	141
III.3.3	Forme d'onde d'auto-brouillage . . . . .	142
III.3.3.1	Modulation . . . . .	142
III.3.3.2	Format de trame auto-brouillée . . . . .	145
III.3.3.3	Démodulation par corrélation circulaire . . . . .	145
III.3.3.4	Contraintes sur le choix des symboles d'auto-brouillage . . . . .	146
III.3.3.5	Génération des canaux virtuels et du décalage de symbole de données	149
III.3.3.5.1	Générateur AES . . . . .	149
III.3.3.5.2	Extraction à partir du canal de transmission . . . . .	149
III.3.3.5.3	Algorithme de génération de canaux virtuels . . . . .	150
III.3.3.6	Démodulation par corrélation circulaire améliorée . . . . .	153
III.3.3.7	Comparaison des deux méthodes de démodulation par corrélation circulaire . . . . .	154
III.3.3.7.1	Performances SER . . . . .	154
III.3.3.7.2	Complexité calculatoire . . . . .	156
III.3.4	Réduction du PAPR du schéma d'auto-brouillage . . . . .	157
III.3.4.1	Définition du PAPR . . . . .	157
III.3.4.2	PAPR du schéma d'auto-brouillage . . . . .	158
III.3.4.3	Méthodes de réduction du PAPR dans la littérature . . . . .	160
III.3.4.3.1	Méthodes de pré-distorsion . . . . .	160
III.3.4.3.2	Méthodes de signalisation . . . . .	161
III.3.4.4	Solution de correction du PAPR pour le schéma d'auto-brouillage	161

III.3.4.5 Comparaison de l'impact de la correction du PAPR entre <i>cc1</i> et <i>ccm</i> . . . . .	166
III.3.4.6 Annulation de la correction du PAPR en réception . . . . .	169
<b>III.4 Schéma d'auto-brouillage LoRa partie 2 : traitements au niveau du récepteur et performances</b>	<b>171</b>
III.4.1 Front-end de synchronisation . . . . .	171
III.4.1.1 Schéma bloc . . . . .	171
III.4.1.2 Intérêt d'utiliser <i>cc1</i> pour la synchronisation . . . . .	173
III.4.1.2.1 Sensibilité de <i>ccm</i> à la désynchronisation $STO_{int}$ . . . . .	173
III.4.1.2.2 Compensation de la sensibilité sur $U$ de <i>cc1</i> grâce au moyennage des symboles préambule lors de la synchronisation . . . . .	174
III.4.1.3 Estimation de $STO_{frac}$ par candidats . . . . .	175
III.4.1.4 Impact du nombre de candidats $STO_{frac}$ sur les performances . . . . .	178
III.4.1.5 Impact de l'espacement entre symboles d'auto-brouillage sur la synchronisation . . . . .	179
III.4.1.6 Performances d'estimation de $CFO_{frac}$ avec auto-brouillage . . . . .	181
III.4.1.7 Comparaison des estimateurs $STO_{frac}$ de la littérature et candidats	182
III.4.2 Performances finales du récepteur légitime . . . . .	183
III.4.2.1 Impact du facteur de correction du PAPR sur le SER avec/sans front-end de synchronisation . . . . .	183
III.4.2.2 Impact de $U$ sur le SER avec/sans front-end de synchronisation . . . . .	184
III.4.2.3 Performances en fonction de $U$ et SF . . . . .	185
III.4.3 Détection de trame . . . . .	186
III.4.3.1 Front-end de détection de trame . . . . .	186
III.4.3.1.1 Étape 1 – constitution des paquets de $N_{up}$ symboles . . . . .	187
III.4.3.1.2 Étape 2 – détection du préambule . . . . .	188
III.4.3.1.3 Étape 3 – réalignement des bornes temporelles . . . . .	192
III.4.3.2 Réduction de la complexité calculatoire et modification de la règle de correction du STO . . . . .	195
III.4.3.3 Performances en simulation . . . . .	197
III.4.4 Capacités de démodulation aveugle de EVE . . . . .	199
III.4.4.1 Capacité de détection aveugle de trame . . . . .	200
III.4.4.2 Capacité d'estimation aveugle de $STO_{frac}$ . . . . .	202
III.4.4.3 Capacité de reconstruction aveugle des canaux virtuels . . . . .	203
<b>III.5 Schéma d'auto-brouillage LoRa partie 3 : implémentation sur SDR</b>	<b>209</b>
III.5.1 Présentation du banc de test . . . . .	209
III.5.2 Mise en évidence de la nécessité de la correction du PAPR . . . . .	212
III.5.3 Comparaisons des DFT LoRa entre les signaux SDR et analytique . . . . .	215
III.5.4 Exemple de démodulation complète . . . . .	215
III.5.5 Étude de l'enveloppe complexe et du spectre . . . . .	220
III.5.5.1 Étude de l'enveloppe complexe . . . . .	220
III.5.5.2 Étude du spectre . . . . .	223

**Conclusion et perspectives de recherche** **229**

**Annexes** **248**

A	Estimateur LoRa de la partie fractionnaire CFO . . . . .	248
B	Estimateur LoRa de la partie fractionnaire STO . . . . .	248
C	Expression analytique du SER LoRa dans un canal multi-trajets aligné . . . . .	249
D	Expression analytique du SER LoRa avec interférence multi-utilisateurs LoRa . . . . .	249
E	Expression analytique de la DFT LoRa dans un canal multi-trajets non-aligné . . . . .	251

## Acronymes

<b>3GPP</b>	3rd Generation Partnership Project. 31
<b>AES</b>	Advanced Encryption System. 22, 38, 149
<b>AF</b>	Amplity and Forward. 116
<b>AN</b>	Artificial Noise. 116
<b>ASK</b>	Amplitude Shift Keying. 158
<b>AWGN</b>	Additive White Gaussian Noise. 28, 230
<b>BER</b>	Bit Error Rate. 28, 79
<b>BICM</b>	Bit Interleaved Coded Modulation. 39
<b>BJ</b>	Band Jamming. 23, 112, 119, 127
<b>BU</b>	Bad Urban. 83
<b>CAD</b>	Channel Activity Detection. 140
<b>CDF</b>	Cumulative Density Function. 74
<b>CFO</b>	Carrier Frequency Offset. 53
<b>CR</b>	Coding Rate. 49
<b>CSI</b>	Comité de Suivi Individuel. 3
<b>CSS</b>	Chirp Spread Spectrum. 32
<b>DAC</b>	Digital to Analog Converter. 157
<b>DBPSK</b>	Differential Binary Phase Shift Keying. 31
<b>DEVE</b>	Direction des Etudes et de la Vie Etudiante. 3
<b>DF</b>	Decode and Forward. 117
<b>DFT</b>	Discrete Fourier Transform. 44
<b>DGA</b>	Direction Générale de l'Armement. 4
<b>DH</b>	Dispositifs Hyperfréquence. 4
<b>DNN</b>	Dense Neural Network. 126
<b>DQPSK</b>	Differential Quad Phase Shift Keying. 31
<b>DSSS</b>	Direct Sequence Spread Spectrum. 32, 114, 144
<b>FBJ</b>	Full Band Jamming. 120, 127
<b>FD</b>	Full-Duplex. 117
<b>FFT</b>	Fast Fourier Transform. 94, 153
<b>FHSS</b>	Frequency Hopping Spread Spectrum. 114, 121, 141
<b>GMSK</b>	Gaussian Minimum Shift Keying. 31
<b>GPS</b>	Global Positioning System. 122, 209
<b>IBNM</b>	Institut Brestois du Numérique et des Mathématiques. 3
<b>ICS</b>	Interleaved Chirp Spreading. 39
<b>IoT</b>	Internet of Things. 25
<b>ISI</b>	Inter Symbol Interference. 58, 83
<b>ISM</b>	Industrial Scientific Medical. 19, 40, 42



## Acronymes

<b>LFM</b>	Linear Frequency Modulated. 122
<b>LFSR</b>	Linear Feedback Shift Register. 121
<b>LoRa</b>	Long Range. 31, 229
<b>LPC</b>	Linear Predictive Coding. 126
<b>LTE</b>	Long Term Evolution. 25
<b>LTE-M</b>	Long Term Evolution - Machine. 31
<b>MDFH</b>	Message Driven Frequency Hopping. 121
<b>MI</b>	Maîtrise de l'Information. 4
<b>MIC</b>	Message Integrity Control. 38
<b>MIMO</b>	Multiple Input Multiple Output. 116, 209
<b>MMSE</b>	Minimum Mean Square Error. 232
<b>MTJ</b>	Multi Tone Jamming. 121
<b>MUSIC</b>	Multiple Signal Classification. 123
<b>NB-IoT</b>	Narrow Band IoT. 31
<b>NJR</b>	Noise-to-Jam Ratio. 132
<b>OFDM</b>	Orthogonal Frequency Division Multiplexing. 31, 121, 157
<b>PAPR</b>	Peak-to-Average Power Ratio. 3, 157, 231
<b>PBJ</b>	Partial Band Jamming. 120, 127
<b>PDF</b>	Probability Density Function. 73
<b>PLL</b>	Phase Locked Loop. 126
<b>ppm</b>	Partie Par Million. 53
<b>PSK</b>	Phase Shift Keying. 158
<b>QAM</b>	Quadrature Amplitude Modulation. 41, 121, 158
<b>RFF</b>	Radio Frequency Fingerprinting. 125
<b>RFID</b>	Radio Frequency Identification. 25
<b>RIS</b>	Reflective Intelligent Surface. 233
<b>RPMA</b>	Random Phase Multiple Access. 30
<b>RSSI</b>	Received Signal Strength Indication. 125, 140, 149
<b>SAA</b>	Small Argument Approach. 131
<b>SAR</b>	Synthetic Aperture Radar. 122
<b>SC</b>	Secrecy Capacity. 116
<b>SDR</b>	Software Defined Radio. 23, 40, 53, 112, 209, 231
<b>SER</b>	Symbol Error Rate. 23, 28, 59, 76, 229
<b>SF</b>	Spreading Factor. 41
<b>SFO</b>	Sampling Frequency Offset. 53
<b>SI</b>	Self Interference. 117
<b>SI3</b>	Sécurité, Intelligence et Intégrité de l'Information. 3
<b>SIR</b>	Signal to Interference Ratio. 89
<b>SJR</b>	Signal-to-Jam Ratio. 133
<b>SMART</b>	Smart Materials and Related Technologies. 4
<b>SNR</b>	Signal to Noise Ratio. 28, 230

<b>SOP</b>	Secrecy Outage Probability. 116
<b>STJ</b>	Single Tone Jamming. 121, 132
<b>STO</b>	Sampling Temporal Offset. 53, 231
<b>TDEL</b>	Time Delay Estimation LoRa. 82, 93
<b>TJ</b>	Tone Jamming. 23, 112, 119, 127
<b>TSL</b>	Three Spectral Lines. 66
<b>TVWS</b>	TV White Space. 31
<b>UBO</b>	Université de Bretagne Occidentale. 3
<b>UNB</b>	Ultra Narrow Band. 31
<b>ZF</b>	Zero Forcing. 170, 232

# Table des figures

I.1.1	Relations entre les principales caractéristiques d'une transmission . . . .	29
I.1.2	Différences majeures de compromis entre les standards IoT et standards classiques . . . . .	30
I.1.3	Principaux standards IoT . . . . .	32
I.2.1	Transceiver LoRa SX1276 . . . . .	35
I.2.2	Architecture LoRaWAN . . . . .	37
I.2.3	Classes de capteurs LoRaWAN . . . . .	37
I.2.4	Chiffrement et authentification LoRaWAN . . . . .	39
I.2.5	Représentation temps-fréquence de symboles LoRa, $SF = 2$ . . . . .	42
I.2.6	Évolution de la durée symbole et du débit LoRa en fonction de SF et $B$ . . . . .	43
I.2.7	Comparaison entre la forme d'onde continue et celle discrète d'un signal LoRa, $SF = 7$ . . . . .	45
I.2.8	Représentation temps-fréquence de la démodulation d'un symbole LoRa $a = 2$ et $SF = 3$ . . . . .	45
I.2.9	Processus de dechirp du signal LoRa reçu . . . . .	46
I.2.10	Schéma bloc du démodulateur LoRa . . . . .	47
I.2.11	Exemple de démodulation LoRa en AWGN pour plusieurs valeurs de SNR, $SF = 7$ . . . . .	47
I.2.12	Format de trame LoRa au niveau de la couche physique . . . . .	48
I.2.13	Schéma bloc de transmission LoRa . . . . .	49
I.2.14	Schéma d'entrelacement LoRa pour le codage de canal de Hamming(7, 4) . . . . .	52
I.2.15	Premier modèle STO . . . . .	55
I.2.16	Second modèle STO . . . . .	55
I.2.17	Impact du CFO sur le spectrogramme LoRa . . . . .	57
I.2.18	Impact du CFO sur la DFT LoRa . . . . .	57
I.2.19	Impact du STO sur le spectrogramme LoRa . . . . .	58
I.2.20	Impact du STO sur la DFT LoRa . . . . .	59
I.2.21	Impact de $STO_{frac}$ sur les performances de démodulation . . . . .	60
I.2.22	Impact de la présence conjointe du CFO et STO sur la DFT LoRa . . . . .	61
I.2.23	Impact du SFO sur le spectrogramme LoRa . . . . .	62
I.2.24	Impact du SFO sur la DFT LoRa . . . . .	63
I.2.25	Front-end de synchronisation LoRa de la littérature [4] . . . . .	65
I.2.26	Performances des deux détecteurs de préambule LoRa de la littérature [76] et [79], $SF = 7$ . . . . .	75
I.2.27	Performances SER LoRa des deux récepteurs non-cohérent et cohérent en fonction de SF . . . . .	78
I.2.28	Performances du front-end de synchronisation de la littérature et impact du nombre de symboles pilotes, $SF = 7$ . . . . .	79

I.2.29	Performances du front-end de synchronisation de la littérature et impact du nombre de symboles pilotes, $SF = 7$ . . . . .	80
II.1.1	Illustration d'un canal à deux trajets . . . . .	84
II.1.2	Illustration d'une interférence multi-utilisateurs LoRa . . . . .	84
II.1.3	Impact du canal multi-trajets (aligné ou non-aligné) sur la DFT LoRa . . . . .	86
II.1.4	Impact de l'interférence multi-utilisateurs LoRa sur la DFT, $a_2^- \neq a_2$ . . . . .	86
II.1.5	Impact de l'interférence multi-utilisateurs LoRa sur la DFT, $a_2^- = a_2$ . . . . .	87
II.1.6	SER LoRa analytique du récepteur non-cohérent dans un canal multi-trajets aligné, $SF = 7$ . . . . .	88
II.1.7	SER LoRa analytique du récepteur non-cohérent dans un canal multi-trajets aligné pour plusieurs valeurs de SF . . . . .	88
II.1.8	Comparaison du SER LoRa analytique entre un canal multi-trajets aligné à deux répliques et un canal à décroissance exponentielle, $SF = 7$ . . . . .	90
II.1.9	SER LoRa analytique avec interférence multi-utilisateurs, $SF = 7$ . . . . .	90
II.2.1	Illustration du démodulateur LoRa RAKE au bin $a' = a$ . . . . .	95
II.2.2	Impact du seuil de détection de trajets du canal multi-trajets sur le SER de cand-LoRa RAKE, $SF = 7$ . . . . .	97
II.2.3	Impact du nombre de candidats sur le SER de cand-LoRa RAKE, $SF = 7$ et $SF = 10$ . . . . .	98
II.2.4	Pourcentage de réduction moyen du nombre de candidats d-cand-LoRa RAKE sélectionnés en fonction du SNR pour plusieurs valeurs de seuil $\lambda_{cand}$ , $SF = 7$ . . . . .	99
II.2.5	Comparaison des performances SER entre LoRa RAKE, d-cand-LoRa RAKE, TDEL et les récepteurs classiques dans un canal multi-trajets aligné avec synchronisation parfaite, $SF = 7$ . . . . .	100
II.2.6	Exemples de démodulation LoRa RAKE dans un canal multi-trajets non-aligné à deux trajets . . . . .	103
II.2.7	Évolution de l'estimation des gain complexes en fonction des paramètres du canal multi-trajets non-aligné . . . . .	104
II.2.8	Évolution de l'énergie du bin d'intérêt LoRa RAKE en fonction des paramètres du canal multi-trajets non-aligné . . . . .	104
II.2.9	Évolution au cours du temps de l'énergie du bin d'intérêt (composante réelle) pour plusieurs résidus $CFO_{frac}$ , $SF = 7$ . . . . .	106
II.2.10	Performances du schéma de correction de phase $CFO_{frac}$ , $SF = 7$ . . . . .	108
II.2.11	Comparaison des performances SER de LoRa RAKE, TDEL et du récepteur classique cohérent, $SF = 7$ – synchronisation parfaite . . . . .	110
II.2.12	Comparaison des performances SER de LoRa RAKE, TDEL et du récepteur classique cohérent, $SF = 7$ – front-end de synchronisation activé . . . . .	110
II.2.13	Régions SNR et $k_1$ de dominance de performances entre LoRa RAKE et TDEL . . . . .	111
III.1.1	Scénario de communication confidentielle en présence d'un intercepteur . . . . .	114
III.1.2	Illustration du principe d'étalement de spectre DSSS . . . . .	115
III.1.3	Illustration du principe de saut de fréquence FHSS . . . . .	115
III.1.4	Scénario de communication en présence d'un brouilleur d'attaque . . . . .	117
III.1.5	Comportements dans le domaine temporel d'un brouilleur . . . . .	118

III.1.6	Illustration du comportement fréquentiel d'un brouilleur de type Band Jamming . . . . .	119
III.1.7	Illustration du comportement fréquentiel d'un brouilleur de type Tone Jamming . . . . .	120
III.1.8	Principe d'authentification par le réseau . . . . .	124
III.1.9	Principe d'authentification par identification radio-fréquence . . . . .	125
III.2.1	Exemples de démodulation LoRa en présence d'un brouilleur Tone Jamming, $SF = 7$ . . . . .	129
III.2.2	Valeurs de symboles minimisant et maximisant les performances de démodulation en présence d'un brouilleur Tone Jamming, $SF = 7$ . . . . .	130
III.2.3	Lois de probabilité et histogrammes de la quantité statistique du détecteur, avec et sans brouillage Band Jamming, $SF = 7$ . . . . .	133
III.2.4	Performances SER en présence d'un brouilleur Tone Jamming et impact de la valeur du symbole, $SF = 7$ . . . . .	134
III.2.5	Performances de détection des brouilleurs Band Jamming et Single Tone Jamming, en fonction de $D$ et du NJR, pour plusieurs valeurs de probabilité de fausse alarme, $SF = 7$ . . . . .	135
III.2.6	Performances de détection des brouilleurs Band Jamming et Single Tone Jamming en fonction du NJR et $D$ – comparaison entre les expressions analytiques et la simulation, $SF = 7$ . . . . .	136
III.2.7	Performances de détection du brouilleur Tone Jamming en fonction du NJR et du nombre de composantes de brouillage, $SF = 7$ . . . . .	137
III.3.1	Scénario de communication avec schéma d'auto-brouillage LoRa . . . . .	142
III.3.2	Illustration du principe d'auto-brouillage dans le domaine fréquentiel LoRa	143
III.3.3	Exemple de symboles auto-brouillés dans le domaine fréquentiel LoRa, $SF = 7$ . . . . .	144
III.3.4	Exemple de démodulations classique et <b>cc1</b> d'un symbole auto-brouillé, $SF = 7$ . . . . .	147
III.3.5	Impact de $A_{max}^{interf}$ sur les performances de démodulation <b>cc1</b> , $SF = 7$ . . . . .	148
III.3.6	Exemple d'exécution de l'algorithme de génération de canal virtuel . . . . .	151
III.3.7	Probabilités de non satisfaction de la contrainte $A_I \leq A_{max}^{interf}$ de l'algorithme de génération de canal virtuel, $SF = 7$ . . . . .	153
III.3.8	Impact de $U$ sur les démodulations <b>cc1</b> et <b>ccm</b> , $SF = 7$ . . . . .	155
III.3.9	Comparaison des performances SER entre <b>cc1</b> et <b>ccm</b> , $SF = 7$ . . . . .	155
III.3.10	Comparaison des complexités calculatoires entre les démodulations <b>cc1</b> et <b>ccm</b> , $SF = 7$ . . . . .	157
III.3.11	Illustrations du PAPR de symboles LoRa auto-brouillés, $SF = 7$ . . . . .	160
III.3.12	Évolution au cours du temps de la composante de correction du PAPR en fonction du facteur de correction du PAPR, $SF = 7$ . . . . .	164
III.3.13	Évolution au cours du temps de l'enveloppe d'un symbole auto-brouillé en fonction du facteur de correction du PAPR, $SF = 7$ . . . . .	165
III.3.14	Exemple de démodulations classique et <b>ccm</b> d'un symbole auto-brouillé avec correction du PAPR maximale, $SF = 7$ . . . . .	165
III.3.15	Impact de la correction du PAPR sur l'amplitude du pic d'intérêt <b>ccm</b> , $SF = 7$ . . . . .	166
III.3.16	Comparaison des démodulations <b>cc1</b> et <b>ccm</b> , sans correction du PAPR et avec correction du PAPR maximale, $SF = 7$ . . . . .	167

III.3.17	Comparaison de la sensibilité à la correction du PAPR entre <i>cc1</i> et <i>ccm</i> , $SF = 7$ . . . . .	168
III.3.18	Comparaison de l'impact de $U$ et $f$ sur les performances SER de <i>cc1</i> et <i>ccm</i> , $SF = 7$ . . . . .	168
III.3.19	Impact de l'annulation de la correction du PAPR en réception sur les performances SER de <i>ccm</i> , $SF = 7$ . . . . .	170
III.4.1	Front-end de synchronisation utilisé dans le schéma d'auto-brouillage . .	172
III.4.2	Comparaison de l'impact du STO entre <i>cc1</i> et <i>ccm</i> , $SF = 7$ . . . . .	174
III.4.3	Compensation de la sensibilité sur $U$ de <i>cc1</i> grâce au moyennage des symboles de préambule lors de la synchronisation, $SF = 7$ . . . . .	175
III.4.4	Exemple de fonctionnement de l'estimateur $STO_{frac}$ par candidats, $SF = 7177$	
III.4.5	Impact du nombre de candidats $STO_{frac}$ sur les performances de démodulation avec synchronisation, $SF = 7$ . . . . .	178
III.4.6	Résidu $STO_{frac}$ minimal en fonction de $STO_{frac}$ et du nombre de candidats $STO_{frac}$ . . . . .	179
III.4.7	Impact de $A_I$ sur l'estimateur $STO_{frac}$ par candidats, $SF = 7$ , $\epsilon_{eq} = 1$ .	180
III.4.8	Impact de $A_I$ sur l'estimateur $STO_{frac}$ par candidats, $SF = 7$ , $\epsilon_{eq} = 2$ .	181
III.4.9	Comparaison des performances d'estimation de $CFO_{frac}$ (résidu maximal) LoRa jam ( $f = 1$ ) vs. LoRa jam mod ( $f = 0.5$ et $f = 1/U$ ), $SF = 7$ . . .	182
III.4.10	Comparaison des performances d'estimation $STO_{frac}$ (résidu maximal) entre l'estimateur de la littérature et celui par candidats proposé, $SF = 7$	183
III.4.11	Impact du facteur de correction du PAPR sur les performances du schéma d'auto-brouillage, avec/sans front-end de synchronisation, $SF = 7$ . . . .	184
III.4.12	Impact de $U$ sur les performances du schéma d'auto-brouillage avec correction maximale du PAPR, avec/sans front-end de synchronisation, $SF = 7185$	
III.4.13	Performances du schéma d'auto-brouillage en fonction de $U$ et SF avec front-end de synchronisation actif . . . . .	186
III.4.14	Front-end de détection de trame utilisé dans le schéma d'auto-brouillage	187
III.4.15	Effet de fenêtre glissante temporelle du module de détection de trame du schéma d'auto-brouillage . . . . .	188
III.4.16	Densité de probabilité et histogramme du critère de détection de préambule pour plusieurs valeurs de $U$ sous l'hypothèse $H_0$ , $SF = 7$ . . . . .	190
III.4.17	Probabilité de fausse alarme de détection de préambule théorique biaisée et réelle pour plusieurs valeurs de $U$ , $SF = 7$ . . . . .	191
III.4.18	Exemple d'exécution du module de détection de préambule, $SF = 7$ . . .	192
III.4.19	Illustration du décalage des bornes temporelles de trame et du ré-alignement nécessaire, $\widehat{idx}_{start} = idx_{start}$ . . . . .	193
III.4.20	Illustration du décalage des bornes temporelles de trame et du ré-alignement nécessaire, $\widehat{idx}_{start} = idx_{start} + 1$ . . . . .	193
III.4.21	Exemple d'estimation du ré-alignement des bornes temporelles de trame, $SF = 7$ . . . . .	195
III.4.22	Évolution du premier et du second résidu minimal de réalignement de borne temporelle de trame en fonction de $STO_{int}$ et $\Delta$ , $SF = 7$ . . . . .	197
III.4.23	Probabilités de non et bonne détection de préambule en fonction de $\Delta$ , $SF = 7$ . . . . .	198
III.4.24	Probabilités de non et bonne détection du préambule en fonction de $U$ , $SF = 7$ . . . . .	199

III.4.25	Étapes de la démodulation que EVE peut réaliser parfaitement en aveugle, en aveugle de façon dégradée, et de façon quasiment impossible . . . . .	200
III.4.26	Comparaison des performances de non-détection de préambule entre BOB et EVE, $SF = 7$ . . . . .	201
III.4.27	Comparaison des performances de mauvaise détection de préambule entre BOB et EVE, $SF = 7$ . . . . .	201
III.4.28	Comparaison du critère $A_{p,\beta,max}$ entre BOB et EVE, $SF = 7$ . . . . .	202
III.4.29	Comparaison des performances d'estimation $STO_{frac}$ entre BOB et EVE, $SF = 7$ . . . . .	203
III.4.30	Exemple d'extraction de bins dans la DFT LoRa pour la reconstruction du canal virtuel par EVE, $SF = 7$ . . . . .	204
III.4.31	Évolution de la probabilité de reconstruction de canal virtuel conduisant à une démodulation correcte pour EVE, en fonction du seuil et du facteur de correction du PAPR, $SF = 7$ . . . . .	206
III.4.32	Fréquence maximale d'actualisation des canaux virtuels de payload en fonction de $U$ pour plusieurs probabilités de démodulation correcte du payload . . . . .	207
III.5.1	SDR Ettus Research B210 . . . . .	210
III.5.2	Banc de test de transmissions SDR . . . . .	211
III.5.3	Front-end d'émission et réception SDR . . . . .	211
III.5.4	Impact du facteur de correction du PAPR sur la DFT LoRa SDR, $SF = 7$ . . . . .	213
III.5.5	Impact du facteur de correction du PAPR sur la ccm SDR, $SF = 7$ . . . . .	213
III.5.6	Impact au cours du temps du facteur de correction du PAPR sur la ccm SDR, $SF = 7$ . . . . .	214
III.5.7	Comparaison des DFT LoRa entre les signaux SDR synchronisés et analytiques pour plusieurs valeurs de $U$ , $SF = 7$ . . . . .	215
III.5.8	Exemple d'exécution du front-end de détection de trame sur SDR, $U = 5$ , $SF = 7$ . . . . .	217
III.5.9	Exemple d'exécution du front-end de synchronisation et de la démodulation sur SDR, $U = 5$ , $SF = 7$ . . . . .	217
III.5.10	Exemple d'exécution du front-end de détection de trame sur SDR, $U = 30$ , $SF = 7$ . . . . .	219
III.5.11	Exemple d'exécution du front-end de synchronisation et de la démodulation sur SDR, $U = 30$ , $SF = 7$ . . . . .	219
III.5.12	Comparaison des amplitudes des bins d'intérêt et voisins directs entre les signaux analytiques et SDR pour $U = 5$ et $U = 40$ , $SF = 7$ . . . . .	220
III.5.13	Enveloppes au cours du temps de signaux auto-brouillés reçus sur SDR pour plusieurs valeurs de $U$ , $SF = 7$ . . . . .	221
III.5.14	Spectre et waterfall d'un signal LoRa legacy ( $U = 1$ ) SDR, 250 kHz et $SF = 7$ . . . . .	224
III.5.15	Waterfall et spectre de signaux LoRa jam mod SDR pour $B = 125$ kHz, avec/sans correction du PAPR, $U = 5$ et $SF = 7$ . . . . .	225
III.5.16	Waterfall de signaux LoRa jam mod SDR pour $B = 250$ kHz et $B = 500$ kHz, avec/sans correction du PAPR, $U = 5$ et $SF = 7$ . . . . .	226
III.5.17	Waterfall de signaux LoRa jam mod SDR pour $U = 20$ et $U = 30$ , $B = 250$ kHz, avec/sans correction du PAPR et $SF = 7$ . . . . .	228
18	Illustration de l'effet d'un canal multi-trajets non-ligné . . . . .	252

# Liste des tableaux

I.1.1	Comparaison entre les standards IoT et les standards conventionnels . . .	30
I.1.2	Comparaison entre les standards IoT et les standards conventionnels : RPMA, Sigfox, Weightless, NB-IoT, LTE-M et LoRa [33, 47]. . . . .	33
I.2.1	Principales notations utilisées dans la Section I.2.4 . . . . .	41
I.2.2	Bandes Industrial Scientific Medical (ISM) dans les régions du monde [80]	42
I.2.3	Exemple de codage de Gray LoRa pour $SF = 3$ . . . . .	52
I.2.4	Exemple de $CFO_{int}$ estimés en fonction du signe de $CFO$ . . . . .	68
I.2.5	Interactions entre les paramètres de synchronisation $CFO_{frac}$ , $CFO_{int}$ , $STO_{frac}$ , $STO_{int}$ et leur estimation . . . . .	70
I.2.6	Cas de mauvaise détection du préambule . . . . .	71
I.2.7	Avantages et inconvénients du détecteur de préambule LoRa par détection de symboles consécutifs identiques [76] . . . . .	76
I.2.8	Avantages et inconvénients du détecteur de préambule LoRa par détection d'énergie [79] . . . . .	76
II.2.1	Pourcentage de réduction moyen du nombre de candidats de d-cand-LoRa RAKE en fonction du SNR pour deux valeurs de seuil $\lambda_{cand}$ , $SF = 7$ . . .	101
III.3.1	Principales notations utilisées dans la Section III.3 . . . . .	140
III.3.2	Avantages et inconvénients des méthodes de correction du PAPR de la littérature . . . . .	162
III.3.3	Avantages et inconvénients des démodulateurs ccl et ccm . . . . .	169
III.4.1	Seuils de détection de préambule pour plusieurs valeurs de $U$ , $P_{fa} = 10^{-5}$ et $SF = 7$ . . . . .	191
III.4.2	Avantages et inconvénients d'augmenter $U$ . . . . .	207
III.4.3	Avantages et inconvénients de diminuer $\Delta_{payload}$ . . . . .	207
III.5.1	Caractéristiques techniques des SDR Ettus Research B210 . . . . .	210
III.5.2	Paramètres SDR et d'auto-brouillage utilisés pour les transmissions SDR	212



# Liste des algorithmes

1	Algorithme de compensation de phase $CFO_{frac}$ et de démodulation LoRa RAKE ( $F = 1$ ou $F = 2$ ) . . . . .	106
2	Algorithme de génération de canal virtuel . . . . .	152
3	Démodulateur <code>ccl</code> . . . . .	156
4	Démodulateur <code>ccm</code> . . . . .	156
5	Algorithme d'estimation $STO_{frac}$ par candidats . . . . .	176

# Contributions scientifiques

## ARTICLES DE JOURNAUX

---

**1 – Theoretical Performance of LoRa System in Multi-Path and Interference Channels** *C. Demeslay, P. Rostaing et R. Gautier, IEEE IoT Journal, 2021*

DOI : <https://doi.org/10.1109/JIOT.2021.3114439>

**2 – Simple and Efficient LoRa Receiver Scheme for Multi-Path Channel** *C. Demeslay, P. Rostaing et R. Gautier, IEEE IoT Journal, 2022*

DOI : <https://doi.org/10.1109/JIOT.2022.3151257>

**3 – A Novel Scheme for Secure and Discrete LoRa Communications** *C. Demeslay, R. Gautier et P. Rostaing, MDPI Sensors, Physical Layer Special Issue, 2022*

DOI : <https://doi.org/10.3390/s22207947>

**4 – A PAPR Reduction Scheme for LoRa Self-Jamming Signals** *C. Demeslay, R. Gautier, P. Rostaing, A. Digulescu, C. Despina-Stoian, et G. Burel (manuscrit soumis dans la revue IEEE IoT Journal, en attente de la décision de la revue)*

**5 – A RAKE-like coherent LoRa receiver for Non-Aligned Multi-Path Channels** *C. Demeslay, P. Rostaing et R. Gautier (manuscrit soumis dans la revue IEEE Transactions on Wireless Communications, en attente de la décision de la revue)*

## ARTICLES DE CONFÉRENCES

---

**Band & Tone Jamming Analysis and Detection on LoRa Signals** *C. Demeslay, R. Gautier, A. Fiche et G. Burel, SPI2021 Workshop, ENSTA Bretagne, Brest, France, 21-23 Juin 2021*

DOI : <https://doi.org/10.48550/arXiv.2107.07782>

## Introduction générale

L'Internet des Objets (IoT) a connu un important essor cette dernière décennie, avec de plus en plus d'équipements connectés, allant de simples capteurs placés dans des champs relevant différentes métriques (température, humidité, etc.), aux villes connectées de demain, ou l'avènement de l'Industrie 4.0 répondant aux nouveaux besoins et assurant une meilleure productivité. Le nombre d'équipements IoT devrait considérablement augmenter, pour doubler d'ici à l'horizon 2030, avec près de 30 milliards d'équipements actifs [1]. Les équipements IoT se caractérisent par l'absence d'intervention humaine, des contraintes de faible consommation, de bas coût et de fiabilité.

Aujourd'hui, plusieurs standards IoT existent : NB-IoT, sigfox, LTE-M ou encore LoRa, regroupés dans les solutions Low Power Access Network (LPWAN). LoRa est actuellement un des leaders des solutions LPWAN, avec des équipements facilement accessibles dans le commerce, et a attiré une vive attention de la communauté scientifique, avec de nombreux travaux cherchant à mieux comprendre les propriétés particulières de la modulation LoRa, ses performances, mais aussi proposer des améliorations. On peut citer par exemple l'augmentation de la capacité des réseaux LoRa [2, 3], la proposition d'algorithmes de synchronisation performants [4, 5], ou encore des méthodes de démodulation robustes à la présence de signaux d'interférence LoRa [6]. Cependant, peu de travaux ont pris en compte deux problématiques importantes :

1. L'impact des canaux multi-trajets sur la démodulation LoRa n'est pas encore totalement cerné dans la littérature et des études supplémentaires sont nécessaires pour mieux comprendre ce phénomène. De plus, peu de récepteurs améliorés prenant en compte l'effet d'un canal multi-trajets ont été proposés et ceux-ci offrent des performances perfectibles.
2. Bien que des mécanismes permettant d'assurer la sécurisation des communications LoRa soient présents au niveau des couches réseau, où les données à transmettre sont chiffrées par des algorithmes de chiffrement tels que Advanced Encryption System (AES), aucun n'est présent au niveau de la couche physique. Cette dernière, premier maillon de la chaîne de télécommunications, regroupe le design de la forme d'onde à transmettre et les processus de modulation et démodulation, et doit donc pouvoir offrir également des mécanismes de sécurisation afin de renforcer de façon complémentaire la sécurité actuelle du standard LoRa.

Ainsi, cette thèse, intitulée *Contributions pour le standard IoT LoRa : améliorations du récepteur classique et de sa sécurisation*, a eu pour objectif de proposer des améliorations pour ces deux axes et les principales contributions ont été les suivantes :

1. L'amélioration du récepteur classique, avec une étude approfondie de l'impact des canaux multi-trajets sur la démodulation et la proposition du récepteur cohérent LoRa RAKE, basé sur une philosophie d'égalisation canal RAKE.
2. La proposition d'un schéma d'auto-brouillage LoRa ajoutant une sécurisation au niveau de la couche physique, réduisant fortement la capacité de démodulation d'intercepteurs et améliorant donc la confidentialité. Ce schéma a été motivé par les contributions de l'axe précédent et une étude réalisée où nous évaluons l'impact des

brouilleurs classiques de la littérature Band Jamming (BJ) et Tone Jamming (TJ) sur la démodulation LoRa.

Ce manuscrit présente ces contributions et est organisé comme suit.

Le Chapitre I présente le standard LoRa. En Section I.1, nous présentons en détail ce qu'est l'IoT : son histoire, ses enjeux techniques et économiques, les différents standards existants et nous replaçons LoRa dans cette grande famille. Nous présentons ensuite en détail LoRa en Section I.2 : l'infrastructure réseau LoRaWAN, le schéma de modulation, les composants du front-end du récepteur LoRa, la problématique cruciale de la synchronisation avec les différents algorithmes existants dans la littérature, et enfin quelques résultats de simulation pour caractériser les performances de LoRa.

Les contributions du premier axe sont présentées dans le Chapitre II. Nous proposons d'abord en Section II.1 une étude évaluant l'impact d'un canal multi-trajets sur la démodulation avec le calcul de l'expression analytique du Symbol Error Rate (SER), critère crucial pour l'évaluation des performances de démodulation. Nous montrons aussi qu'une interférence venant d'un autre signal LoRa a un impact similaire. Cette étude nous a permis de développer le récepteur amélioré LoRa RAKE exploitant de façon constructive l'énergie des trajets du canal et améliorant ainsi les performances de démodulation. Il est présenté en Section II.2.

Les contributions du second axe sont présentées dans le Chapitre III. Nous commençons par rappeler en Section III.1 le contexte général sur la sécurisation des communications dans lequel le schéma d'auto-brouillage permettant de renforcer la confidentialité a été développé : la confidentialité, le brouillage et l'authentification. Ensuite, nous présentons en Section III.2 les résultats de notre étude sur l'impact des brouilleurs classiques de la littérature BJ et TJ. Ces derniers nous ont apporté des éléments de compréhension pour le développement du schéma. Le schéma d'auto-brouillage est présenté en trois parties dans les Sections III.3, III.4 et III.5. Premièrement, le modèle, l'architecture et les paramètres du schéma sont présentés en Section III.3. Ensuite, le front-end de synchronisation dédié pour le schéma est introduit en Section III.4 et des résultats de simulation sont présentés pour évaluer le comportement et les performances obtenus. Enfin, en Section III.5, nous effectuons plusieurs expérimentations sur des dispositifs de type Software Defined Radio (SDR) afin de valider la viabilité du schéma sur équipements réels.

# Chapitre I

## Présentation du standard LoRa

Dans ce chapitre, nous présentons le standard LoRa retenu pour la thèse. Nous introduisons d'abord en Section I.1 le cadre global d'utilisation des équipements LoRa : l'IoT. Nous y présentons les différents standards IoT existants, faisons une comparaison entre eux et avec les standards plus conventionnels, et nous justifions l'intérêt de choisir LoRa pour la thèse. Puis, en Section I.2, nous présentons LoRa à proprement parler : son architecture réseau LoRaWAN, une revue de l'état de l'art, ses propriétés de modulation, les traitements nécessaires au niveau du récepteur, ainsi que ses performances.

# I.1. Cadre d'application de LoRa : l'IoT

Dans cette partie, nous présentons d'abord en Section I.1.1 ce qu'est l'IoT : son histoire, son impact sur les sociétés et quelques scénarios typiques d'utilisation d'IoT. Ensuite, les différences fondamentales entre l'IoT et les standards plus conventionnels (Section I.1.2) sont abordées. Puis enfin une présentation des différents standards IoT existants et leurs principales différences (Section I.1.3) est faite.

## I.1.1. Qu'est-ce que l'IoT ?

D'après l'office québécois de la langue française [7], L'Internet des Objets ou Internet of Things (IoT) en anglais est défini comme suit :

*« L'ensemble des objets connectés à Internet capables de communiquer avec des humains, mais aussi entre eux, grâce à des systèmes d'identification électronique, pour collecter, transmettre et traiter des données avec ou sans intervention humaine ».*

Nous remarquons aisément que la spécificité de l'IoT réside dans la capacité à collecter des données, issues de leur environnement proche. Cela est assez différent des schémas de communication classique comme les réseaux d'opérateurs, Long Term Evolution (LTE) par exemple, où les données sont issues essentiellement du terminal utilisateur et directement destinées à être émises sur l'Internet. Dans ce qui suit, nous présentons l'évolution des usages de l'IoT au cours de l'histoire, ainsi que les principaux scénarios de communication IoT qu'il est possible de trouver aujourd'hui.

### I.1.1.1. Historique

La première solution technologique s'apparentant à de l'IoT remonte à 1982 sur le campus de l'université Carnegie Mellon University aux USA [8] où une machine de vente de Coca-Cola modifiée a été installée, lui permettant de transmettre son inventaire de vente et un état de service sur le réseau embryonnaire d'alors, ARPANET.

L'article *The Computer of the 21st Century* de 1991 [9] présente une première définition rigoureuse du concept de l'IoT avec la suggestion d'usages concrets, dans l'industrie principalement, et de ses premiers enjeux : le faible coût de mise en place et de maintenance de l'infrastructure, la capacité des équipements IoT à se fondre dans l'environnement et les problématiques liées à la sécurisation des communications.

Tout au long de la décennie 1990 et jusqu'au début des années 2000, des travaux universitaires ont consolidé les concepts et proposé des architectures et infrastructures IoT [10, 11]. Ce n'est qu'à la fin des années 1990 que l'IoT a réellement commencé à être déployé, avec la volonté d'accélérer les processus industriels dans les usines avec l'utilisation de dispositifs de type Radio Frequency Identification (RFID) pour le suivi de la chaîne

## I.1. Cadre d'application de LoRa : l'IoT

de production [12, 13, 14].

Les années 2010 ont permis l'ouverture de l'IoT à d'autres usages comme les villes intelligentes et est aujourd'hui largement répandu. Cet aspect est traité plus en détail en Section I.1.1.3. Depuis, une explosion de l'IoT a eu lieu avec un nombre toujours plus croissant d'équipements en service et une prédiction d'un marché pesant près de 177 milliards de dollars US à l'horizon 2026 [15].

### I.1.1.2. Problématiques éthiques et encadrement

L'IoT a pu voir le jour grâce à l'évolution de la technologie avec la réduction continue des coûts de fabrication des équipements, mais également grâce à l'acceptation progressive par le grand public et les instances d'autorité. En effet, comme tout bouleversement technologique, il est légitime d'émettre des réserves sur la pertinence d'un tel changement pouvant soulever des questions éthiques. Nous pouvons remonter aussi loin que 1936 avec le film *Les temps modernes* de Chaplin où l'on trouve une satire sur la course sans fin à la technologie ainsi qu'à la déshumanisation des emplois de l'industrie d'alors et à l'exploitation humaine par les machines.

Aujourd'hui, l'IoT fait face à de vives critiques de la part des médias. Par exemple, le média public Canadien CBC, dans son podcast au titre éloquent *The Internet of Unsecure Things* [16], dénonce le décalage entre la promesse d'un meilleur futur offert par l'IoT et la réalité, avec des enjeux et besoins parfois artificiels et de nombreuses questions éthiques à résoudre. Le média américain CNBC rapporte également les problématiques liées à l'exploitation des données de santé sensibles par les montres connectées [17].

Les régulateurs et instances gouvernementales ont proposé différents textes afin d'encadrer l'usage et d'apporter des éléments juridiques. Par exemple, un texte a été proposé en 2019 par le gouvernement britannique [18] proposant de mettre en place un label attestant de la sécurité des équipements IoT et seuls les industriels le possédant seraient autorisés à en vendre. Les éléments de sécurisation seraient par exemple l'usage d'identifiants uniques et non ré-initialisables, un engagement à fournir un suivi de mises à jour de sécurité, ou encore une plus grande transparence sur les potentielles vulnérabilités des équipements.

En France, il n'y a pas de texte ciblant directement l'IoT, mais plutôt un encadrement sur l'usage des données potentiellement sensibles pouvant y être issues. Cela peut par exemple se concrétiser par l'autorisation à titre exceptionnel de l'exploitation de données médicales dans le cadre d'une étude universitaire par exemple [19, 20].

### I.1.1.3. Scénarios de communications IoT

De nos jours, les usages pour l'IoT ont considérablement évolué, mais gardent une forte composante industrielle. Aujourd'hui, de nombreux équipements IoT sont présents dans les usines et entreprises afin d'optimiser la productivité. Ce secteur d'activité, communément appelé *industrie 4.0* en est aujourd'hui à sa quatrième révolution. L'*industrie 1.0* représente les premiers procédés de mécanisation technologique apparus à la fin du *XVIII<sup>ème</sup>* et tout au long du *XIX<sup>ème</sup>* siècle. On y trouve principalement les machines à

vapeur. L'*industrie 2.0* est l'avènement de la production de masse au début du *XX<sup>ème</sup>* siècle avec les premières lignes d'assemblage développées pour le secteur de l'automobile, avec en tête la Ford modèle T. Cette révolution a été succédée dès les années 1950 par l'*industrie 3.0* avec l'apparition de l'automatisation par robots des lignes d'assemblage, réduisant drastiquement les coûts de fabrication, offrant ainsi au plus grand nombre des produits jusque là inaccessibles comme l'électroménager par exemple. Enfin, l'*industrie 4.0* entamée au cours des années 2000 présente en quelque sorte la numérisation des usines avec un contrôle et suivi toujours plus poussé des équipements et une nouvelle problématique majeure : la sécurisation des communications [21]. Elle consiste en l'usage de nouveaux procédés de fabrication (impression 3D par exemple), de la traçabilité par marquage numérique (QR codes par exemple) et surtout de l'interfaçage sécurisé avec l'Internet où l'IoT y occupe une place décisive.

L'IoT est aussi fortement présent pour des usages grand public [22, 23]. On y trouve :

- l'avènement récent des enceintes connectées avec assistants vocaux : Google Now ou Amazon Alexa par exemple,
- les montres connectées Apple Watch ou Android Wear,
- les maisons connectées : ampoules intelligentes, domotique, etc,
- les équipements médicaux avec le suivi du diabète par exemple,
- l'électroménager avec les réfrigérateurs, congélateurs et robots divers et variés.

L'IoT trouve une place particulière au sein des villes intelligentes ou *Smart Cities*. Les villes intelligentes reflètent la volonté d'améliorer la vie des citoyens en rendant la ville adaptative et efficace grâce à des dispositifs connectés [24, 25]. Ces dispositifs peuvent être très variés, allant des lampadaires pilotés à distance permettant de réduire la consommation énergétique, l'optimisation du trafic par de la signalisation intelligente ou encore le suivi de la pollution urbaine par un réseau de capteurs disséminés dans la ville.

Enfin, nous trouvons l'IoT dans d'autres secteurs d'activité tels que l'agriculture avec la surveillance en temps réel des cultures [26] ou le médical, avec un suivi plus poussé des pathologies des patients grâce à des capteurs discrets [27, 28] et l'explosion des téléconsultations à cause de la pandémie COVID-19 [29].

## I.1.2. Des enjeux radicalement différents

Dans cette partie, nous nous focalisons sur les différences fondamentales existant entre l'IoT et les schémas de communication traditionnels tels que le LTE. En premier, les compromis nécessaires à la mise en œuvre d'une transmission de télécommunication performante sont rappelés. Puis dans un second temps, une comparaison des standards de communication IoT avec d'autres standards plus conventionnels est menée.



### I.1.2.1. Compromis pour la mise en œuvre d'une télécommunication

L'objectif d'une transmission de télécommunication est d'acheminer de l'information d'un émetteur à un récepteur distant, de façon la plus fiable possible. Plusieurs éléments caractérisent une transmission :

- la puissance d'émission,
- la portée du signal,
- le schéma de modulation employé,
- le débit,
- les performances de démodulation (Symbol Error Rate (SER) ou Bit Error Rate (BER)),
- la bande passante du signal,
- la consommation énergétique,
- les différents post-traitements au niveau du récepteur.

Un paramètre important dans l'évaluation des performances d'une transmission est le Signal to Noise Ratio (SNR). Il est défini par :

$$\begin{aligned} SNR &= \frac{P_r}{\sigma^2} \\ SNR_{dB} &= 10 \times \log_{10}(SNR) \end{aligned} \quad (\text{I.1.1})$$

avec  $P_r$ , la puissance du signal reçu et  $\sigma^2$ , la puissance du bruit thermique, ou Additive White Gaussian Noise (AWGN), au niveau du récepteur. Ce dernier est aléatoire, mais suit la loi statistique bien connue : la loi normale. Un signal reçu purement AWGN,  $w(t)$ , a ses amplitudes à moyenne nulle et de variance  $\sigma^2$  :

$$w(t) \sim \mathcal{N}(\mu = 0, \sigma^2) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}} \quad (\text{I.1.2})$$

En pratique, il est souhaitable d'avoir un SNR le plus élevé possible, avec un signal reçu se dégageant clairement du bruit. Une transmission idéale offrirait :

- un débit maximal,
- un minimum de bande passante,
- une grande portée et robustesse du signal,
- une consommation énergétique faible.

Malheureusement, en pratique, il n'est pas possible de satisfaire ces critères simultanément et des compromis doivent être trouvés. La Figure I.1.1 présente les relations entre les principales caractéristiques d'une transmission. Nous constatons les comportements fondamentaux suivants :

1. Pour une puissance d'émission fixe, le SNR se dégrade progressivement avec la distance (Figure I.1.1a).
2. Plus le SNR se dégrade, plus les performances de démodulation se dégradent (Figure I.1.1b). Une modulation plus lente conservera plus longtemps de bonnes performances.
3. Pour une contrainte de SNR fixe, améliorer les performances de démodulation nécessite un traitement au niveau du récepteur plus lourd (Figure I.1.1c). Cela entraîne une

plus grande complexité de calcul, une latence de traitement plus élevée et un coût énergétique et matériel plus important.

4. Augmenter le débit nécessite d'élargir la bande passante du signal (Figure I.1.1d). Le spectre fréquentiel basse fréquence est aujourd'hui pratiquement saturé et toutes les bandes de fréquences jusqu'à 6 GHz sont occupées [30]. Pour un opérateur de télécommunications, une faible portion du spectre lui est attribuée. Ainsi, ce dernier doit donc optimiser au maximum la ressource fréquentielle et cela passe notamment par le choix de schémas de modulation offrant un débit maximal dans une bande passante minimale.

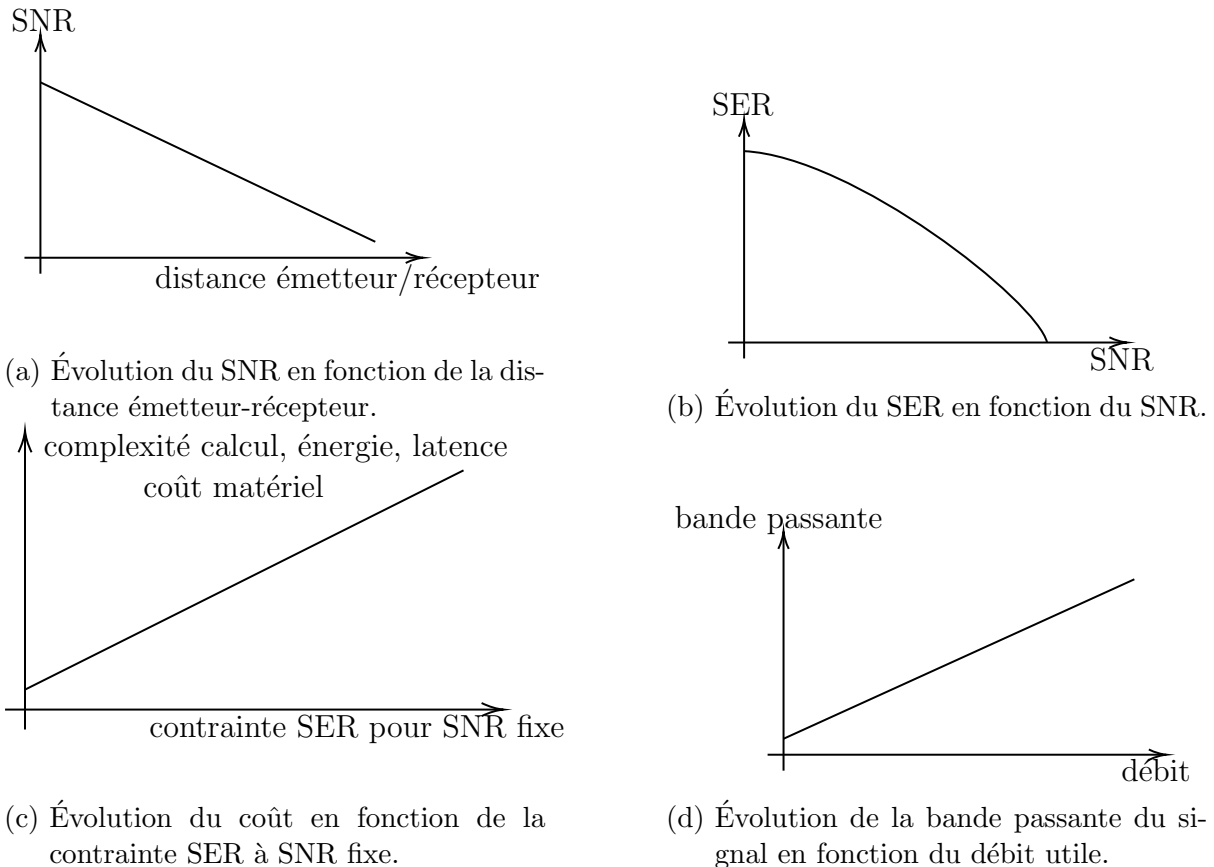


FIGURE I.1.1. – Relations entre les principales caractéristiques d'une transmission

### I.1.2.2. Comparaison avec les standards conventionnels

Les standards IoT se différencient radicalement des schémas conventionnels de transmission en termes de compromis de performances réalisés (voir Section I.1.2.1). La Figure I.1.2 illustre les différences de compromis en termes de débit, de portée et de coût pour différents standards : LTE, 5G, WiFi et IoT. Là où le WiFi et surtout la 5G misent sur l'augmentation forte des débits pour une portée plus faible et au prix d'un coût important, les standards IoT cherchent avant tout à offrir une transmission robuste à grande portée et des coûts associés faibles. En effet, en termes de débit, les écarts d'ordre de grandeur sont considérables. La 5G peut offrir un débit pratique dépassant 1 Gbit/s alors que les standards IoT n'offrent que quelques dizaines de kbit/s, au mieux. Le WiFi propose des débits proches de ceux de la 5G, mais avec une portée bien plus faible, ne

dépassant pas la centaine de mètres. Cela vient de la contrainte forte de ne pas dépasser des puissances d'émissions trop importantes pour un usage domestique. Le coût du WiFi est intermédiaire, mais reste plus proche du LTE et de la 5G que de l'IoT.

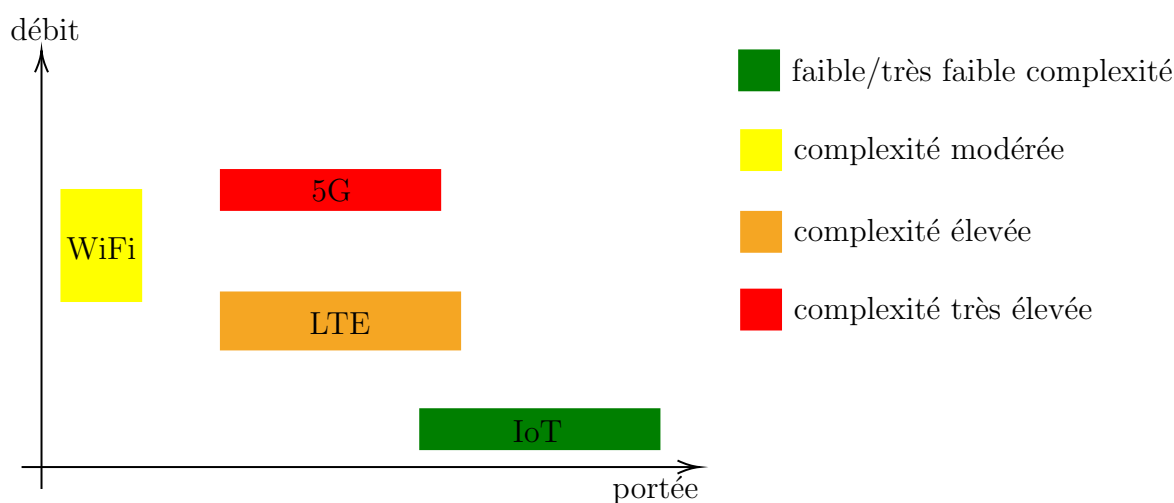


FIGURE I.1.2. – Différences majeures de compromis entre les standards IoT et standards classiques

Le Tableau I.1.1 donne quelques chiffres de comparaison entre les standards IoT et d'autres standards plus classiques [31, 32, 33].

	LTE	5G	WiFi 802.11ac	IoT
Débit descendant (Mbit/s)	300	10000-50000	6900	0.1
Portée (km)	32	0.5	0.1	63
Coût énergétique	fort	très fort	fort	très faible
Coût matériel	fort	très fort	modéré	très faible/faible
Complexité du récepteur	forte	très forte	modérée	très faible/faible

TABLE I.1.1. – Comparaison entre les standards IoT et les standards conventionnels

### I.1.3. Standards et solutions commerciales IoT

Dans cette partie, nous présentons les principaux standards IoT existants : leur histoire, leurs spécificités techniques, leur modèle économique pour ensuite les comparer.

#### I.1.3.1. Standards IoT

L'IoT tel que nous le connaissons aujourd'hui a réellement pris son essor à la fin des années 2000 et de nombreux standards ont été développés depuis, avec les principaux présentés en Figure I.1.3. Historiquement, la société américaine Ingenu a proposé dès 2008 ses premières solutions IoT. Elles reposent sur une technologie propriétaire nommée Random Phase Multiple Access (RPMA) offrant une grande capacité multi-utilisateurs, jusqu'à deux millions d'équipements par point d'accès, une grande portée (ville de Dallas et sa banlieue couverte avec seulement 17 antennes par exemple) et des terminaux

ayant une autonomie pouvant dépasser 10 ans [34, 35]. Les solutions RPMA d'Ingenu sont principalement déployées aux USA avec de nombreuses villes et infrastructures couvertes, mais Ingenu projette son expansion de façon mondiale, avec un déploiement au Canada ou Chili par exemple et plus récemment en Europe.

En 2009, la société française Sigfox est créée et offre dès 2010 ses premières solutions [36]. La technologie Sigfox se caractérise par l'usage de l'Ultra Narrow Band (UNB) offrant de très bas débits dans une bande très étroite. Ainsi, les capteurs Sigfox ne peuvent transmettre que de très courts messages, d'une taille maximale de 12 octets, pour une trame de 26 octets ! Sigfox propose ses solutions par un système d'abonnement avec un nombre limité de messages pouvant être envoyés chaque jour : 140 sur la voie montante et seulement 4 sur la voie descendante. Sigfox est majoritairement déployé en France et au Maghreb et a connu des difficultés. Cette dernière a été placée en redressement judiciaire en janvier 2022, mais pas moins de neuf entreprises ont été intéressées par son rachat [37], avec son acquisition en avril 2022 par la société UnaBiz [38], preuve d'un secteur porteur très dynamique.

D'un point de vue plus open-source, nous pouvons citer le consortium Weightless SIG, formé par les entreprises britanniques Neul, Cable & Wireless, CSR ou encore ARM. Ce dernier propose un protocole dédié, une technologie et une interface de communication avec les instances de régulation. Plusieurs technologies sont proposées : Weightless-N, Weightless-P et Weightless-W. Weightless-N exploite l'UNB avec une modulation classique Differential Binary Phase Shift Keying (DBPSK) à faible débit et une couche de chiffrement AES dédiée [39]. Weightless-P est une variante plus performante de Weightless-N avec une modulation à plus gros débit Differential Quad Phase Shift Keying (DQPSK) ou Gaussian Minimum Shift Keying (GMSK) [40]. Weightless-W quant à elle propose d'utiliser la section TV White Space (TVWS) du spectre, de 400 à 800 MHz environ, où de nombreuses portions sont inexploitées avec des signaux portant robustes et étant de bons candidats pour des applications IoT [41]. Weightless a finalisé en 2021 sa première puce Weightless-W [42].

Le consortium 3rd Generation Partnership Project (3GPP) a également proposé deux adaptations du standard LTE pour les applications IoT : Long Term Evolution - Machine (LTE-M) et Narrow Band IoT (NB-IoT). LTE-M et NB-IoT reposent sur le même schéma de modulation Orthogonal Frequency Division Multiplexing (OFDM) utilisé par le LTE, mais avec des paramètres plus restreints, NB-IoT étant une variante plus basse consommation de LTE-M. Ainsi, LTE-M s'adresse surtout à des applications IoT nécessitant des débits intermédiaires, de l'ordre de quelques Mbit/s et NB-IoT est plus adapté pour un déploiement massif de réseaux de capteurs avec de fortes contraintes de portée et une meilleure pénétration des obstacles [43]. De nombreux opérateurs proposent des solutions LTE-M ou NB-IoT aujourd'hui. LTE-M a par exemple été déployé en France par Orange dès 2019, par Bouygues Telecom en septembre 2021 et par SFR en septembre 2022 [44]. Il est à noter que LTE-M et NB-IoT sont directement intégrés dans le standard 5G.

Enfin, Long Range (LoRa) a été introduit en 2012 avec le dépôt d'un brevet par l'entreprise française Cycleo [45] et a été ensuite racheté par la compagnie américaine Semtech la même année. LoRa est à la fois une infrastructure réseau de part le standard LoRaWAN et un schéma de modulation. L'infrastructure LoRaWAN est présentée plus en

détail dans la Section I.2.2. La modulation LoRa repose sur la technologie Chirp Spread Spectrum (CSS) avec des signaux de type chirp dont la fréquence croît linéairement dans le temps, offrant une bonne portée pouvant dépasser 30 km et de bonnes performances de démodulation. Depuis 2015, le consortium LoRa Alliance existe et a pour but d'accélérer le déploiement de LoRa en unifiant les solutions technologiques des différents partenaires tels que Amazon, Arduino ou encore Cisco [46].



FIGURE I.1.3. – Principaux standards IoT

### I.1.3.2. Comparaison croisée

Le Tableau I.1.2 présente une comparaison des différents standards IoT présentés dans la section précédente. Nous reportons pour chaque standard : les bandes d'opération, la largeur de bande, la technologie de la couche physique, le débit (voies montantes et descendantes, uplink et downlink en anglais, respectivement), l'efficacité spectrale (uplink et downlink) et la portée maximum atteignables, à partir de [33, 47]. L'efficacité spectrale est simplement le débit atteint par unité fréquentielle, en bit/s/Hz :

$$\eta = \frac{D_b}{B} \quad (I.1.3)$$

Nous constatons de fortes disparités techniques. Par exemple, Weightless-W, de par sa nature de signaux Direct Sequence Spread Spectrum (DSSS), offre les meilleurs débits mais dans une bande assez élevée, donnant une très faible efficacité spectrale de 0.0013. NB-IoT et LTE-M étant issus du LTE ont des caractéristiques intermédiaires avec des débits proches d'une utilisation de télécommunications classique. En revanche, la portée est moins bonne avec 10 km, au mieux. Sigfox se démarque clairement par des débits extrêmement faibles de 0.1 kbit/s, une bonne efficacité spectrale et une excellente portée dépassant 60 km. Weightless-P offre la meilleure efficacité spectrale, 8 bit/s/Hz avec jusqu'à 100 kbit/s dans 12.5 kHz de bande. Enfin, LoRa semble être un standard assez équilibré avec une portée pouvant dépasser 30 km, des débits atteignant presque 30 kbit/s et une efficacité spectrale de valeur attendue pour des usages IoT de 0.05.

	RPMA	Sigfox	Weightless		
			N	P	W
Bande (MHz)	2400	868.1/915	< 1000	< 1000	470-790
Largeur de bande (MHz)	1000	0.1	N/A	12.5	6000-8000
Couche physique	RPMA	D-BPSK	D-BPSK	D-QPSK	DSSS
Débit (kbit/s) – uplink/downlink	30/30	0.1/0.1	100/-	100/100	10000/10000
$\eta$ (bit/s/Hz) – uplink/downlink	0.03	1	N/A	8	0.0013
Portée (km)	10	63	10	10	10

	NB-IoT	LTE-M	LoRa
Bande (MHz)	LTE	LTE	868.1/915
Largeur de bande (MHz)	180	1400	500
Couche physique	OFDM	OFDM	CSS
Débit (kbit/s) – uplink/downlink	60/30	375/300	27/27
$\eta$ (bit/s/Hz) – uplink	0.33	0.27	0.05
$\eta$ (bit/s/Hz) – downlink	0.66	0.21	0.05
Portée (km)	10	10	30

TABLE I.1.2. – Comparaison entre les standards IoT et les standards conventionnels : RPMA, Sigfox, Weightless, NB-IoT, LTE-M et LoRa [33, 47].

Nous avons retenu pour la thèse le standard LoRa. En effet, ce dernier est assez déployé de nos jours et a attiré ces dernières années une vive attention de la communauté scientifique, où de nombreux travaux ont été réalisés portant sur la connaissance plus fine du standard et proposant des améliorations. Cela a permis de constituer une base bibliographique solide pour proposer nos améliorations du démodulateur standard LoRa. De plus, assez peu de travaux ont proposé des contributions sur la sécurisation de la couche physique LoRa. Ainsi, nous avons pu y apporter aussi des contributions.

La section suivante présente en détail LoRa, donnant au lecteur les bases principales de cette modulation particulière et permettant ainsi à ce dernier de bien appréhender nos contributions apportées sur l'amélioration du démodulateur standard LoRa et du schéma d'auto-brouillage proposé.



## I.2. LoRa

Dans cette section, nous présentons plus en détail le standard LoRa (Long Range). Dans une première partie (Section I.2.1), nous donnons quelques applications LoRa concrètes qu'il est possible de trouver aujourd'hui. Ensuite, nous faisons une introduction rapide de l'infrastructure LoRaWAN et de ses mécanismes de sécurité (Section I.2.2) puis un tour d'horizon des différents travaux LoRa dans la littérature (Section I.2.3). Nous poursuivons en Sections I.2.4 et I.2.5 sur la présentation du schéma de modulation et de démodulation, ainsi que de la chaîne de transmission complète LoRa. Puis nous évaluons dans la Section I.2.6 l'impact de la désynchronisation du signal reçu sur la démodulation et présentons les principaux algorithmes de synchronisation que l'on peut trouver dans la littérature. Ces derniers serviront de point de départ pour le développement du schéma d'auto-brouillage. Enfin, en Section I.2.7, nous présentons quelques résultats de performances permettant de bien caractériser LoRa.

### I.2.1. Applications commerciales et projets

Depuis son introduction, LoRa a connu un véritable essor avec de nombreux équipements présents sur le marché. En effet, dès juillet 2012, les premiers dispositifs émetteur-récepteur (ou transceivers) sont apparus avec les puces SX 1276/1277/1278 librement accessibles sur le marché [48]. Le transceiver SX1276 est illustré en Figure I.2.1. C'est une des particularités et avantages de LoRa, car les autres standards sont beaucoup plus fermés et ne permettent pas l'acquisition aisée de tels dispositifs.



FIGURE I.2.1. – Transceiver LoRa SX1276

Ainsi, de nombreuses compagnies proposent des solutions et services, comme la vente de passerelles, de nombreux capteurs ou encore des interfaces client pour la surveillance du réseau LoRaWAN [49, 50, 51]. Les opérateurs traditionnels offrent aussi des solutions LoRa avec par exemple Orange qui propose des packs contenant un transceiver LoRa,



un accès au réseau LoRaWAN d'Orange et des outils de développement [52]. Ce dernier revendique d'ailleurs la couverture du territoire français à 95% [53].

LoRa a aussi été au cœur de nombreux projets. Les travaux dans [54] proposent d'utiliser des capteurs LoRa pour relever la température de cultures dans des champs. Les auteurs explorent la possibilité d'enfouir les capteurs sous terre afin d'éviter d'éventuels vols de capteurs et évaluent la capacité de pénétration des signaux LoRa dans la terre. Ils concluent qu'un enfouissement jusqu'à 60 cm est possible pour les paramètres de modulation LoRa les plus robustes.

Nous trouvons aussi des travaux sur l'implémentation de LoRa pour des usages domestiques de type maison connectée. Les auteurs dans [55] réalisent un dispositif LoRa basé sur un module Arduino avec des antennes dédiées pour un usage en intérieur et un module de surveillance du matériel interfacé avec une station de base LoRa distante. Ils simulent ensuite un quartier fictif de maisons connectées et réalisent des mesures pour évaluer la portée de communication avec ou sans obstacles majeurs. Ils montrent qu'une communication jusqu'à 180 m est possible, une valeur plus élevée que les signaux WiFi, mettant en évidence la bonne robustesse des signaux LoRa.

Enfin, un système de surveillance en temps réel de l'environnement (température, humidité et qualité de l'air) est proposé dans [56]. Les auteurs démontrent le faible coût d'implémentation offert par LoRa, moins de 200\$ dans l'étude et la bonne portée de communication.

### I.2.2. Infrastructure LoRaWAN

Dans cette partie, nous présentons l'infrastructure LoRaWAN ainsi que ses mécanismes de sécurité actuels, résumés à partir de la très bonne référence [57].

#### I.2.2.1. Réseaux LoRaWAN

Les réseaux LoRa reposent sur l'architecture LoRaWAN, illustrée en Figure I.2.2. Nous remarquons plusieurs canaux de communication. Les capteurs LoRa communiquent avec les passerelles exclusivement avec la modulation LoRa. Le message reçu par cette dernière est ensuite acheminé vers le *Network Server*. Ce dernier a pour mission de valider l'accès au réseau des capteurs par des mécanismes d'authentification et de chiffrement. Ensuite, le message est traité par l'*Application Server* qui trie les messages des capteurs pour les différentes applications associées. Enfin, le message utile est émis vers l'application utilisateur distante.

Nous constatons que cette architecture est principalement pensée pour des communications sur la voie montante. En effet, le trafic sur la voie descendante est réduit au minimum (signalisation principalement). Cependant, les capteurs peuvent dans certains cas exploiter la voie descendante (recevoir une configuration spécifique du réseau par exemple). Cette différenciation se fait au travers des classes. Nous en distinguons trois, comme présenté en Figure I.2.3. *UL* désigne la voie montante et *DL* la voie descendante. La classe A est celle imposant la contrainte énergétique la plus faible aux capteurs. Après chaque message transmis, une première fenêtre est disponible au bout d'une seconde pour

l'éventuelle réception d'un message de la passerelle, puis une deuxième fenêtre est disponible après deux secondes de la transmission initiale. Le reste du temps, le capteur est mis en veille. La classe B est identique à la classe A mais avec plus de fenêtres DL. Ces fenêtres supplémentaires sont synchronisées avec des signaux de synchronisation nommés *Beacon*. Enfin, la classe C active la voie descendante la majeure partie du temps et il n'y a donc plus de mise en veille. Cette classe est la plus proche d'un usage classique de communication (LTE par exemple), mais est aussi la plus énergivore.

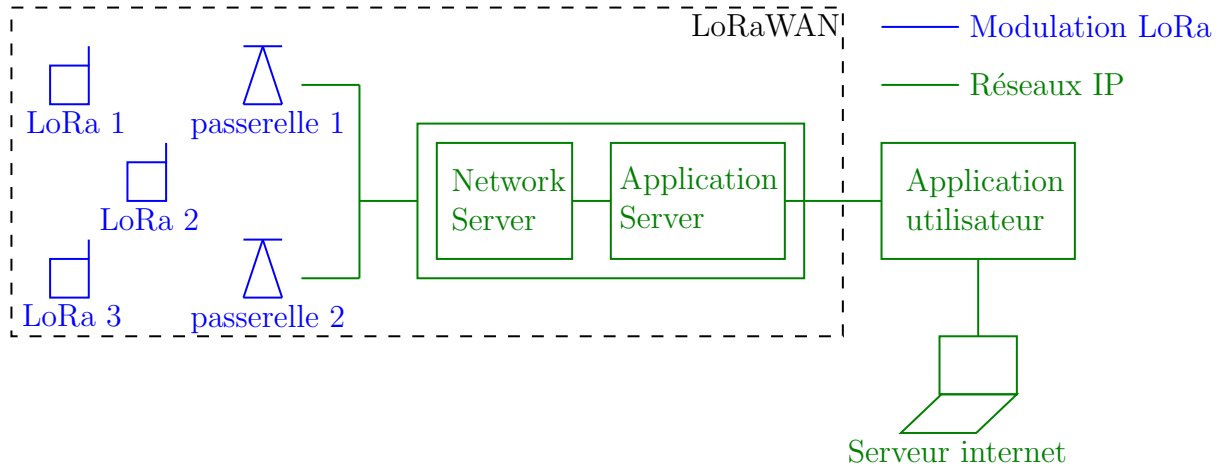


FIGURE I.2.2. – Architecture LoRaWAN

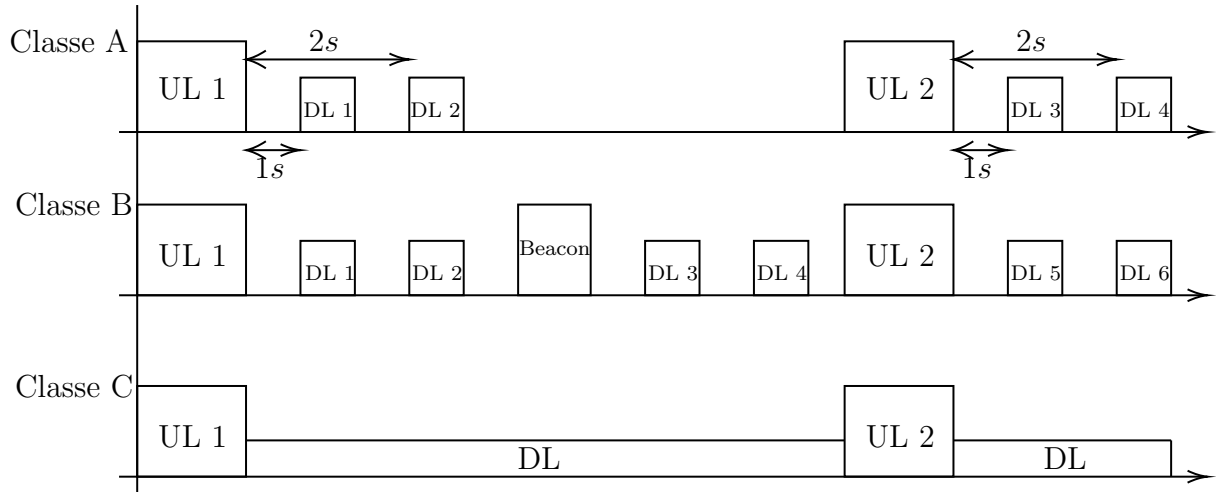


FIGURE I.2.3. – Classes de capteurs LoRaWAN

### I.2.2.2. Mécanismes de sécurité LoRa actuels

Dans cette partie, nous passons en revue les mécanismes de sécurité présents dans le protocole LoRaWAN. Ces derniers répondent à deux aspects de la sécurisation d'une communication : l'authentification et la confidentialité et se font principalement par le biais de chiffrement. Les premières révisions du standard (jusqu'à la révision 1.0.3) proposent les différents identifiants d'authentification suivants [58] :

- *DevEUI*

Cet identifiant est l'équivalent de l'adresse MAC que l'on trouve pour les équipements classiques IP. Il est unique et attribué en usine par le fabricant du transceiver.

- *DevNonce*

Le DevNonce est un identifiant généré aléatoirement à chaque communication. La passerelle retient en mémoire tous les DevNonce utilisés précédemment. Si elle en reçoit un déjà utilisé, elle refusera alors le message arrivant. Le DevNonce est extrait à partir de l'exploitation des propriétés aléatoires du canal (variations de la puissance de signal reçue, phase etc.) afin de constituer une séquence binaire pseudo aléatoire [59].

- *AppEUI*

AppEUI donne un identifiant à chaque application. Il est similaire aux ports Internet utilisés dans le modèle OSI.

La version 1.0.4 a apporté plusieurs corrections, avec notamment le changement de nom du AppEUI en *JoinEUI* [60]. Ce dernier spécifie quels pré-requis techniques sont nécessaires : version de LoRaWAN supportée, compatibilité ascendante, etc. Plus important, le fonctionnement du DevNonce est modifié. Il devient maintenant un compteur initialisé à 0 en usine et incrémenté à chaque accès au réseau. Il ne doit en aucun cas être réinitialisé au cours de la vie du capteur. Ainsi, ce dernier doit être conservé dans une mémoire non volatile. Cela apporte plus de contraintes pour les fabricants, mais renforce la sécurité.

La confidentialité est assurée par du chiffrement Advanced Encryption System (AES). La Figure I.2.4 présente le schéma de chiffrement utilisé dans LoRa. Les données à transmettre sont chiffrées en AES avec la clef *AppSKey*. Ces dernières, concaténées avec l'entête applicative, sont ensuite chiffrées à nouveau avec la clé *NwkSKey* et servent à produire un nouveau champ nommé Message Integrity Control (MIC) et ajouté après. Au niveau de la couche MAC, la trame se compose donc d'une entête MAC ajoutée au début, de la trame applicative chiffrée et du MIC. Le capteur LoRa et le Network Server doivent posséder la même clef *NwkSKey* afin que le Network Server puisse correctement calculer le MIC et authentifier la trame reçue. Il est à noter que l'utilisation de l'AES nécessite une infrastructure supplémentaire pour la création et la diffusion des clefs de chiffrement.

### I.2.3. État de l'art

LoRa a suscité un vif engouement par la communauté scientifique. L. Vangelista et son article *The LoRa Modulation* en 2015 a été la première contribution scientifique significative à poser les bases théoriques de la modulation LoRa [61]. Cela a ouvert de nombreuses perspectives de recherche. Dans ce qui suit, nous retraçons les principaux axes de recherche rencontrés dans la littérature : les études analytiques sur les performances de démodulation, de nouveaux schémas de transmission améliorés et enfin les problématiques de synchronisation.

#### I.2.3.1. Expression analytique du SER

La majeure partie des travaux LoRa a consisté dans un premier temps à mieux caractériser la modulation LoRa. Les travaux [62, 63, 64] ont apporté de nouveaux éléments

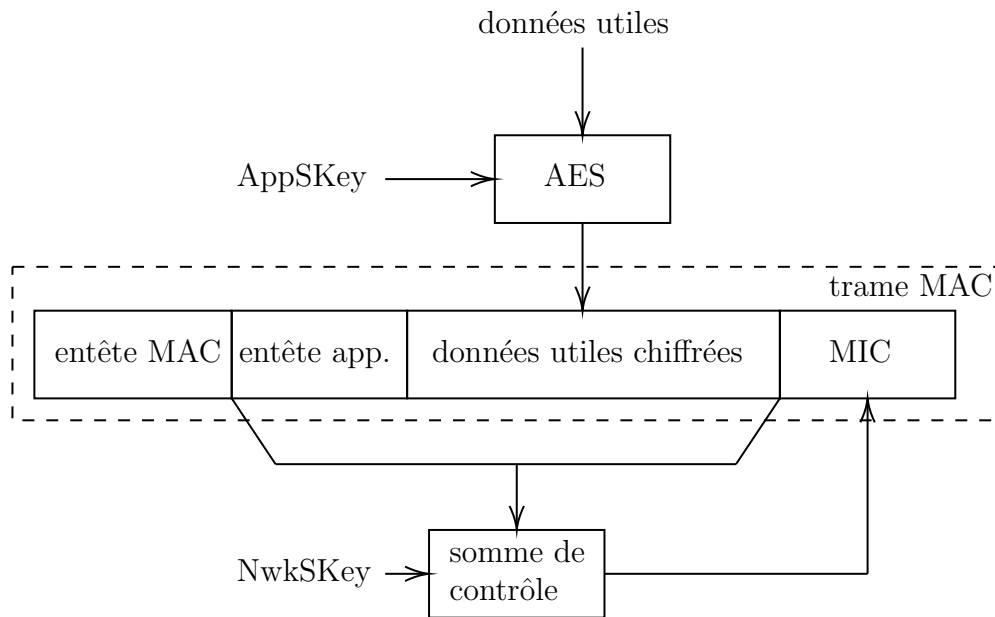


FIGURE I.2.4. – Chiffrement et authentification LoRaWAN

théoriques [62], étudié les propriétés d'orthogonalité [63] et spectrale des signaux LoRa [64]. Ces travaux ont permis ensuite d'étudier les performances théoriques de LoRa où des expressions approchées du SER sont obtenues pour des transmissions sans codage de canal [65, 66, 67]. Il a été également montré dans [68] l'avantage d'utiliser une démodulation cohérente des signaux LoRa en lieu et place de la démodulation classique non-cohérente. La démodulation cohérente implique l'exploitation de l'information de phase dans le signal reçu contrairement à la démodulation non-cohérente. Elle offre de meilleures performances mais ajoute une contrainte de synchronisation de phase.

### I.2.3.2. Schémas de transmission améliorés

Certains travaux ont proposé des améliorations au schéma de modulation LoRa actuel. Par exemple, il a été proposé d'utiliser dans [69] une approche par corrélation entre le signal reçu et un signal de référence contenu dans le préambule de la trame afin d'améliorer la robustesse aux canaux multi-trajets. Le récepteur amélioré offre d'assez bonnes performances, mais surtout une faible complexité d'implémentation. Le codage de canal a aussi été considéré. Les auteurs dans [70] ont obtenu une expression analytique du BER en considérant le codage de canal de Hamming classique, tandis que de nouveaux schémas de codage sont proposés exploitant le principe de Bit Interleaved Coded Modulation (BICM) [71, 72]. Enfin, des travaux portant sur l'augmentation de la capacité des réseaux LoRa ont été engagés. R. Joerg *et al.* en sont les principaux contributeurs avec une approche de codage de canal dans [2] et surtout une modification des formes d'ondes avec le concept prometteur Interleaved Chirp Spreading (ICS) [3, 73, 74]. Il permet d'augmenter de près de 50% la capacité du réseau au prix d'une perte de performances très faible.

### I.2.3.3. Synchronisation

Le brevet LoRa déposé en 2012 [45] décrit assez bien la modulation dans son ensemble ainsi que l'émetteur, mais très peu de choses sont dites sur le récepteur. Or, les traite-

ments cruciaux et donc valeurs ajoutées d'un standard se font au niveau du récepteur, avec notamment la synchronisation. Cette dernière est primordiale, elle permet de réaligner temporellement le signal reçu, ainsi que d'éliminer les déformations du signal dues aux imperfections des composants matériels et sans elle, pas de transmission possible. Ainsi, une part non négligeable des travaux a porté sur l'analyse de l'impact de la désynchronisation sur la démodulation et le développement d'algorithmes de synchronisation dédiés.

Dans [75], une présentation simple et claire des principales désynchronisations est faite. Les algorithmes de synchronisation les plus complets ont été proposés dans [76, 77]. Les auteurs de [76] ont ensuite amélioré leur schéma dans [4] pour proposer finalement de meilleures performances que [77]. D'autres études se focalisent sur un autre aspect important de la synchronisation : la détection du signal. Dans [78], une expression théorique de la probabilité de détection est obtenue, en utilisant le schéma de démodulation LoRa conventionnel. Les auteurs dans [79] proposent quant à eux un détecteur de signal LoRa plus abouti offrant de bonnes performances théoriques, mais est malheureusement très sensible aux imperfections matérielles, limitant fortement son utilisation en pratique.

Enfin, certains algorithmes de la littérature ont été validés sur de vraies transmissions LoRa avec des équipements de type Software Defined Radio (SDR) (radio logicielle en français) [5]. Les expérimentations réalisées ont prouvé leur pertinence et robustesse, ouvrant la porte pour une utilisation adaptée de ces derniers dans le schéma d'auto-brouillage.

### I.2.4. Schéma de modulation LoRa

Dans cette section, nous présentons les bases d'une transmission LoRa (la modulation et la démodulation), le format de trame et le schéma bloc complet émetteur/récepteur avec les différents traitements effectués par ces derniers. Les principales notations utilisées dans cette section sont reportées dans le Tableau I.2.1.

#### I.2.4.1. Modulation

Les signaux LoRa sont émis sur les bandes radio libres Industrial Scientific Medical (ISM) avec des fréquences porteuses qui varient en fonction de la région du monde (voir Tableau I.2.2, d'après [80]). Par exemple, la fréquence centrale pour LoRa est généralement 868.1 MHz en Europe et 915 MHz aux USA. Ils reposent sur les formes d'ondes bien connues de type *chirp* dont la fréquence croît linéairement dans le temps et sont de largeur de bande réglable  $B \in \{125, 250, 500\}$  kHz. De plus, chaque canal LoRa est espacé d'une bande de garde de 75 kHz. En bande de base, cela correspond à avoir un signal de support fréquentiel  $\nu \in [-B/2; B/2]$  Hz.

$SF$	Spreading Factor	$M$	Nombre de formes d'ondes : $2^{SF}$
$F_s$	Fréquence d'échantillonnage	$T_s$	Période d'échantillonnage
$T$	Durée symbole	$B$	Largeur de bande
$t$	Indice temporel	$\nu$	Indice fréquentiel
$k$	Indice temporel discret	$n$	Indice fréquentiel discret
$i$	Indice de symbole	$p$	Indice de bloc de détection de trame
$a$	Valeur du symbole LoRa	$x_a[k]$	Forme d'onde associée au symbole $a$
$P_s$	Puissance du symbole LoRa	$x_0^*[k]$	Downchirp local de démodulation
$w[k]$	Composante de bruit AWGN	$r[k]$	Signal reçu
$\tilde{x}_a[k]$	Symbole dechirpé : $\tilde{x}_a[k] = x_a[k]x_0^*[k]$	$\tilde{X}_a[n]$	Symbole démodulé : $\tilde{X}_a[n] = \text{DFT}\{\tilde{x}_a[k]\}[n]$
$\hat{b}$	Estimée de $b$	$\langle b \rangle$	Moyenne de $b$
$N_{up}$	Nombre de symboles upchirp dans le préambule	$N_{down}$	Nombre de symboles downchirp dans le préambule
$N_{pre}$	Nombre de symboles dans le préambule : $N_{pre} = N_{up} + N_{down}$	$N_d$	Nombre de symboles de payload
$F_c$	Fréquence porteuse	$\Delta_f$	Résidu de porteuse en bande de base
$CFO$	Carrier Frequency Offset	$CFO_{int}$	Partie entière du CFO
$CFO_{frac}$	Partie fractionnaire du CFO	$STO$	Sampling Temporal Offset
$STO_{int}$	Partie entière du STO	$STO_{frac}$	Partie fractionnaire du STO
$R$	Facteur de sur-échantillonnage pour la simulation et la correction de $STO_{frac}$	$SFO$	Sampling Frequency Offset
$H_0$	Hypothèse de signal reçu purement AWGN	$H_1$	Hypothèse de signal reçu LoRa
$idx_{start}$	Indice de début de trame	$\lambda_{preamble}$	Seuil de détection de trame
$P_{fa}$	Probabilité de fausse alarme de détection de trame	$P_{wd}$	Probabilité de mauvaise détection de trame
$P_{md}$	Probabilité de non fonctionnement de détection de trame	$P_{nd}$	Probabilité de non détection de trame

TABLE I.2.1. – Principales notations utilisées dans la Section I.2.4

Comme toute modulation numérique, l'émetteur constitue des blocs de bits, les convertit en symboles, génère les formes d'ondes associées à chaque symbole et les transmet. La taille des blocs de bits est appelée dans le langage LoRa le Spreading Factor (SF) et a pour valeurs  $SF \in \{7, 8, \dots, 12\}$ . Ainsi, l'émetteur a à disposition  $M = 2^{SF}$  symboles différents et donc  $M \in \{128, 256, \dots, 4096\}$ . Cela est assez différent des modulations classiques de type Quadrature Amplitude Modulation (QAM) par exemple où  $M$  ne dépasse pas 256.

Région	Fréquences (MHz)
Europe, Russie, Inde, Afrique	863-870
USA	902-928
Canada	779-787
Asie	433
Australie	915-928
Chine	779-787, 470-510

TABLE I.2.2. – Bandes Industrial Scientific Medical (ISM) dans les régions du monde [80]

La Figure I.2.5 présente la représentation temps-fréquence, ou spectrogramme, des signaux LoRa associés aux symboles  $a \in \{0, 1, 2, 3\}$ , pour  $SF = 2$ , pour garder la figure lisible. Nous notons  $T$ , la durée d'un symbole LoRa. Le fonctionnement est le suivant : A  $t = 0$ , le signal LoRa a une fréquence initiale  $\nu_{init}^{(a)}$ . Cette dernière croît linéairement jusqu'à atteindre la borne fréquentielle supérieure  $\nu = B/2$  à  $t = \tau_a$  où une discontinuité apparaît. Ainsi, la fréquence est ré-initialisée à  $\nu = -B/2$ . Le signal continue ensuite à progresser linéairement pour retrouver  $\nu = \nu_{init}^{(a)}$  à  $t = T$ , la durée symbole.

D'après la figure, nous remarquons aisément que c'est la fréquence initiale  $\nu_{init}^{(a)}$  qui porte l'information du symbole et que le symbole  $a = 0$  correspond à une rampe unique, sans discontinuité. Ce signal particulier est appelé *upchirp* dans la littérature. Par construction graphique, nous remarquons que la pente fréquentielle vaut  $\nu_{slope} = B/T$  et :

$$\nu_{init}^{(a)} = -\frac{B}{2} + a\frac{B}{M} \quad (\text{I.2.1})$$

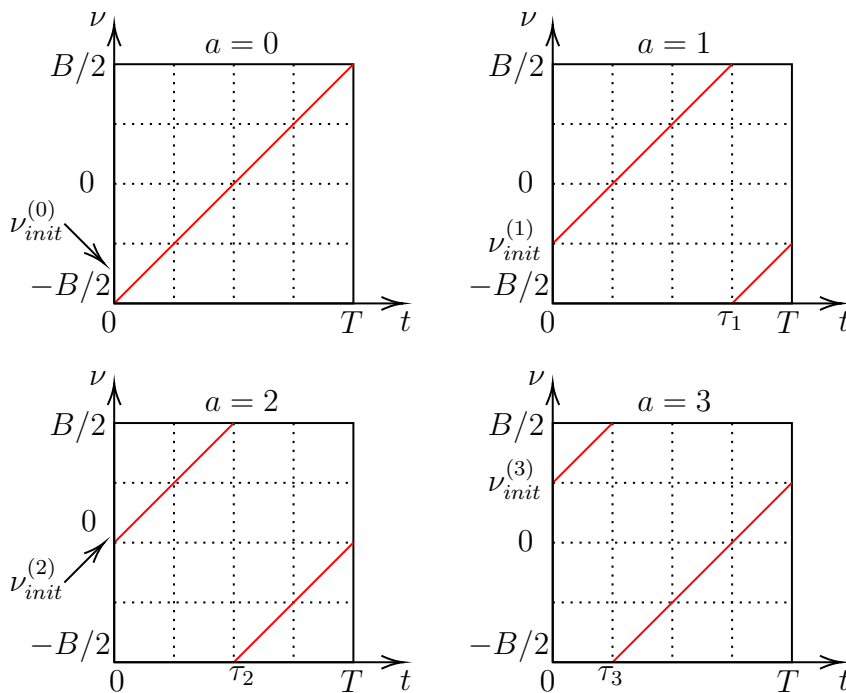


FIGURE I.2.5. – Représentation temps-fréquence de symboles LoRa,  $SF = 2$

La durée symbole est facilement obtenue par la relation  $T = M/B$ . Il est à noter que LoRa a des durées symbole longues, jusqu'à plus de 32 ms pour  $SF = 12$  et  $B = 125$  kHz, là où d'autres standards comme le LTE ont des valeurs beaucoup plus faibles, de l'ordre de quelques dizaines de  $\mu s$  généralement. Ainsi, le débit (et donc l'efficacité spectrale) est très faible, ne dépassant pas 27.4 kbit/s ( $SF = 7$  et  $B = 500$  kHz) et descendant même jusqu'à 0.366 kbit/s pour  $B = 125$  kHz et  $SF = 12$ . L'évolution de ces grandeurs en fonction de SF et  $B$  est représentée en Figure I.2.6.

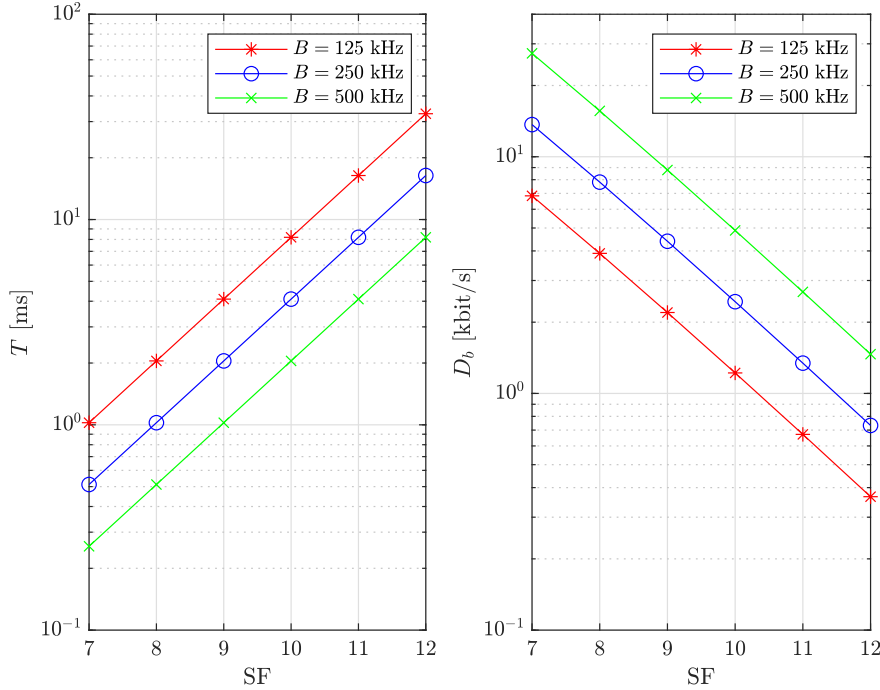


FIGURE I.2.6. – Évolution de la durée symbole et du débit LoRa en fonction de SF et  $B$

Les auteurs dans [64] ont obtenu une expression théorique du signal LoRa. Cette dernière est obtenue en analysant d'abord la fréquence et la phase instantanée. La première vaut :

$$\nu(t; a) = \begin{cases} a \frac{B}{M} + \frac{B}{T}t - \frac{B}{2} & \text{si } t \in [0, \tau_a] \\ a \frac{B}{M} + \frac{B}{T}t - \frac{3B}{2} & \text{si } t \in [\tau_a, T] \end{cases} \quad (\text{I.2.2})$$

avec :

$$\tau_a = T \times \left(1 - \frac{a}{M}\right) \quad (\text{I.2.3})$$

La phase instantanée vaut donc :

$$\phi(t; a) = 2\pi \int_0^t \nu(b, a) db = \begin{cases} 2\pi \left( a \frac{B}{M}t + \frac{B}{2T}t^2 - \frac{B}{2}t \right) & \text{si } t \in [0, \tau_a] \\ 2\pi \left( a \frac{B}{M}t + \frac{B}{2T}t^2 - \frac{3B}{2}t \right) & \text{si } t \in [\tau_a, T] \end{cases} \quad (\text{I.2.4})$$

D'après l'équation (I.2.4), nous pouvons remarquer qu'au passage d'un symbole à un autre consécutif, il n'y a pas de discontinuité de phase i.e.  $\phi(0; a) = \phi(T; a) = 0 \forall a$ . Cette propriété est très intéressante d'un point de vue pratique : le risque de subir des distorsions engendrées par les composants matériels est limité. Cela permet de synthétiser



## I.2. LoRa

des signaux LoRa de qualité, même sur des transceivers à bas coûts. Le signal complexe LoRa transmis a pour expression finale :

$$x_a(t) = e^{j\phi(t;a)} = \begin{cases} e^{2j\pi t(\nu_{init}^{(a)} + \frac{B}{2T}t)} & \text{si } t \in [0, \tau_a] \\ e^{2j\pi t(\nu_{init}^{(a)} + \frac{B}{2T}t - B)} & \text{si } t \in [\tau_a, T] \end{cases} \quad (\text{I.2.5})$$

Le récepteur reçoit le signal en équation (I.2.5) et l'échantillonne pour obtenir une séquence d'échantillons sur laquelle il estimera le symbole reçu. Pour limiter la complexité calculatoire, le récepteur travaille à la fréquence d'échantillonnage minimale  $F_s = B$  (ou fréquence de Nyquist). Ainsi,  $T_s = 1/F_s = 1/B$ . En fixant  $t = kT_s = k/B$  ( $k$ , l'indice temporel discret) dans l'équation (I.2.5), des simplifications apparaissent et cette dernière s'écrit simplement :

$$x_a[k] = e^{2j\pi k[\frac{a}{M} - \frac{1}{2} + \frac{k}{2M}]}, \quad k \in \{0, 1, \dots, M-1\} \quad (\text{I.2.6})$$

Les formes d'ondes pour différents symboles sont orthogonales entre elles [61], soit :

$$\langle x_{a_1}[k], x_{a_2}[k] \rangle = \sum_{k=0}^{M-1} x_{a_1}[k] x_{a_2}^*[k] = \begin{cases} 1 & \text{si } a_1 = a_2 \\ 0 & \text{sinon} \end{cases} \quad (\text{I.2.7})$$

En revanche, l'orthogonalité n'est pas valable pour des formes d'ondes issues de valeurs de SF différentes [63].

La forme d'onde discrète obtenue est alors exprimée sur  $M$  échantillons et la bande de fréquence est découpée en  $M$  bins espacés de  $B/M$  Hz avec  $n \in \{0, 1, \dots, M-1\}$ , l'indice de bin. La fréquence initiale devient alors le  $a^{\text{ème}}$  bin :  $n_{init}^{(a)} = a$ . Notons que la puissance d'un symbole LoRa vaut  $P_s = \mathbb{E}[|x_a[k]|^2] = 1$ , pour tout  $a$ . Par soucis de simplicité, la puissance sera toujours fixée à  $P_s = 1$  si non précisé dans le texte.

La Figure I.2.7 présente les formes continue et celle discrète d'un signal LoRa obtenues dans les équations (I.2.5) et (I.2.6), respectivement, pour la partie réelle,  $a = 64$  et  $SF = 7$ . Les cercles rouges représentent les valeurs des  $M$  échantillons. Nous voyons que la fréquence croît linéairement positivement jusqu'à  $t = T/2$ , puis négativement jusqu'à la fin de la durée signal.

### I.2.4.2. Démodulation

La Figure I.2.8 présente de façon intuitive la manière de retrouver le symbole transmis à partir du signal  $x_a[k]$ . Nous remarquons qu'il suffit de multiplier ce dernier par un upchirp à rampe négative (aussi appelé *downchirp*, noté  $x_0^*[k]$ ). Graphiquement, cela revient en fait à sommer modulo  $M$  les courbes de  $x_a[k]$  et  $x_0^*[k]$ . Ainsi, une unique composante fréquentielle apparaît, au bin  $n = a$ . Le récepteur peut facilement estimer cette fréquence avec la transformée de Fourier discrète (Discrete Fourier Transform (DFT) en anglais).

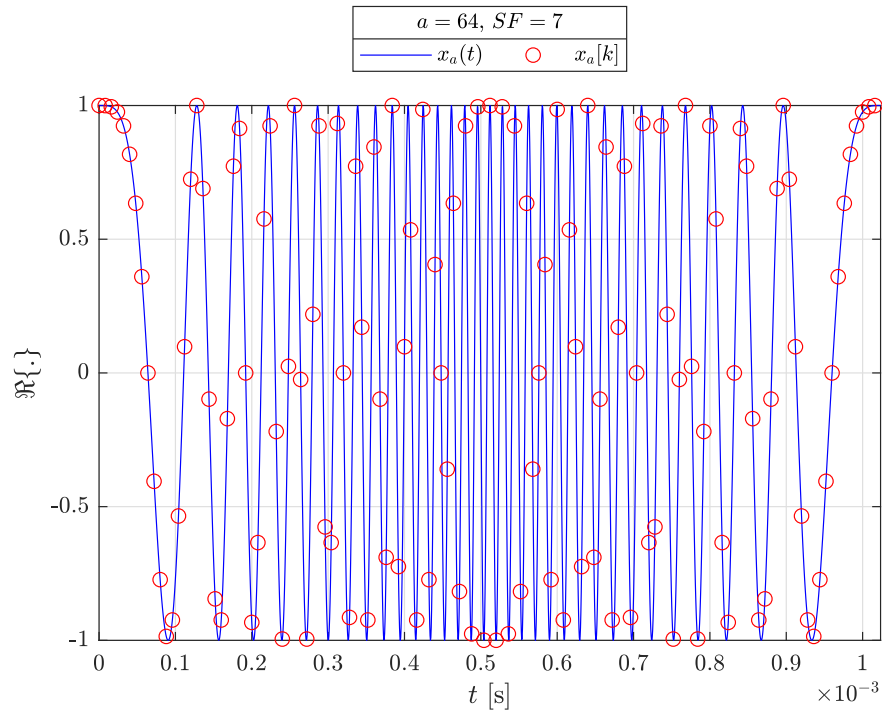


FIGURE I.2.7. – Comparaison entre la forme d'onde continue et celle discrète d'un signal LoRa,  $SF = 7$

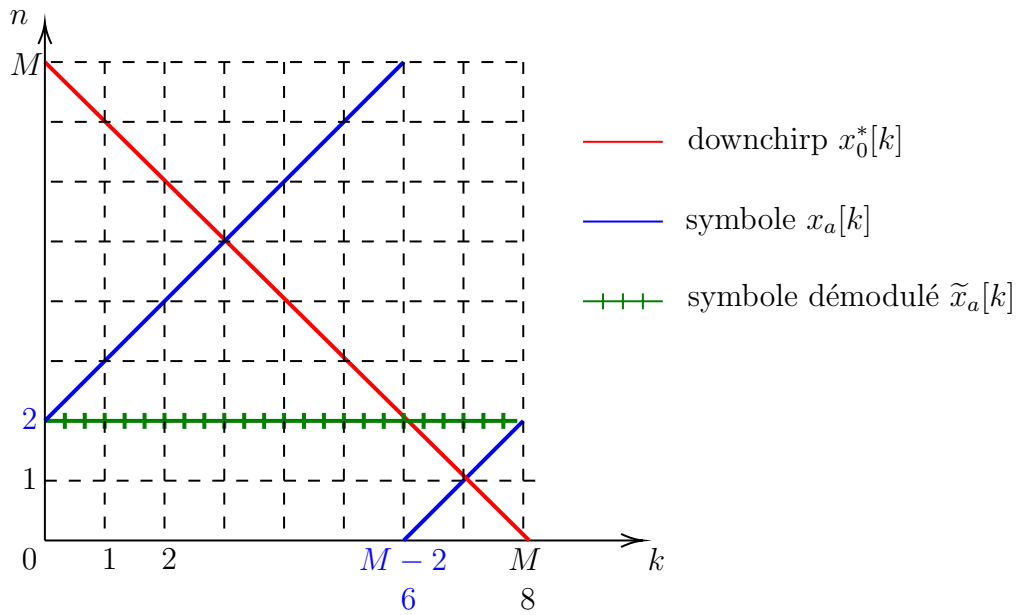


FIGURE I.2.8. – Représentation temps-fréquence de la démodulation d'un symbole LoRa  $a = 2$  et  $SF = 3$

## I.2. LoRa

En pratique, le signal reçu est contaminé par du bruit AWGN (voir Section I.1.2.1). Ainsi, nous avons le signal discret :

$$r[k] = x_a[k] + w[k] \quad (\text{I.2.8})$$

avec  $w[k]$ , la composante AWGN complexe, circulaire, de moyenne nulle et de variance  $\mathbb{E}[|w[k]|^2] = \sigma^2$ . La multiplication du signal reçu par un downchirp, opération *dechirp* pour obtenir le signal *dechirpé*, peut s'écrire :

$$\tilde{r}[k] = r[k]x_0^*[k] = x_a[k]x_0^*[k] + w[k]x_0^*[k] = \tilde{x}_a[k] + \tilde{w}[k] \quad (\text{I.2.9})$$

Nous notons que l'opération dechirp ne modifie pas les propriétés statistiques du bruit, soit  $\tilde{w}[k] \sim \mathcal{CN}(0, \sigma^2)$ . Ce processus est présenté en Figure I.2.9. Le signal est ensuite démodulé (voir Figure I.2.10). Cela revient à développer l'équation (I.2.9) et calculer sa DFT. Nous considérons pour l'instant uniquement la composante sans bruit. Nous obtenons alors :

$$\tilde{x}_a[k] = e^{2j\pi k[\frac{a}{M} - \frac{1}{2} + \frac{k}{2M}]} e^{-2j\pi k[-\frac{1}{2} + \frac{k}{2M}]} = e^{2jk\pi \frac{a}{M}} \quad (\text{I.2.10})$$

$$\tilde{X}_a[n] = \text{DFT}\{\tilde{x}_a[k]\}[n] = \sum_{k=0}^{M-1} \tilde{x}_a[k] e^{-2j\pi k \frac{n}{M}} = \sum_{k=0}^{M-1} e^{-2jk\pi \frac{n-a}{M}} = M\delta[n-a] \quad (\text{I.2.11})$$

La DFT comporte une unique composante en  $n = a$  d'amplitude  $M$  (facteur  $M$  du à l'opération DFT) et donc  $\tilde{X}_a[n \neq a] = 0$ . Le signal reçu dechirpé a pour expression :

$$\tilde{R}[n] = \tilde{X}_a[n] + \tilde{W}[n] = M\delta[n-a] + \tilde{W}[n] \quad (\text{I.2.12})$$

La présence de bruit fait alors varier l'énergie en  $n = a$  et introduit de l'énergie dans les autres composantes  $n \neq a$ . Le symbole peut-être estimé de manière non-cohérente par l'équation (I.2.13) ou cohérente par l'équation (I.2.14).

$$\hat{a}_{NCOH} = \arg \max_n \left| \tilde{R}[n] \right| \quad (\text{I.2.13})$$

$$\hat{a}_{COH} = \arg \max_n \Re\{\tilde{R}[n]\} \quad (\text{I.2.14})$$

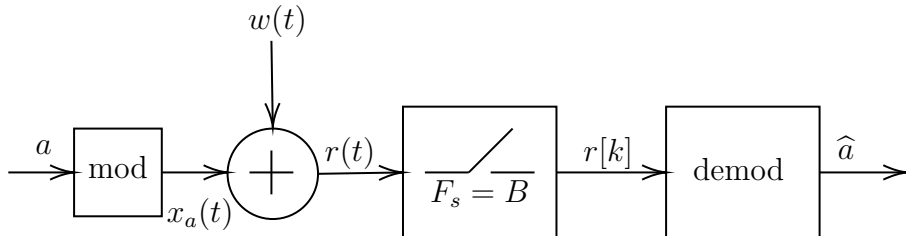


FIGURE I.2.9. – Processus de dechirp du signal LoRa reçu

Les auteurs dans [65] ont montré que la démodulation cohérente donne de meilleures performances en AWGN que la démodulation non-cohérente, avec un gain de l'ordre de 0.8 dB. Cela est montré en Figure I.2.27.

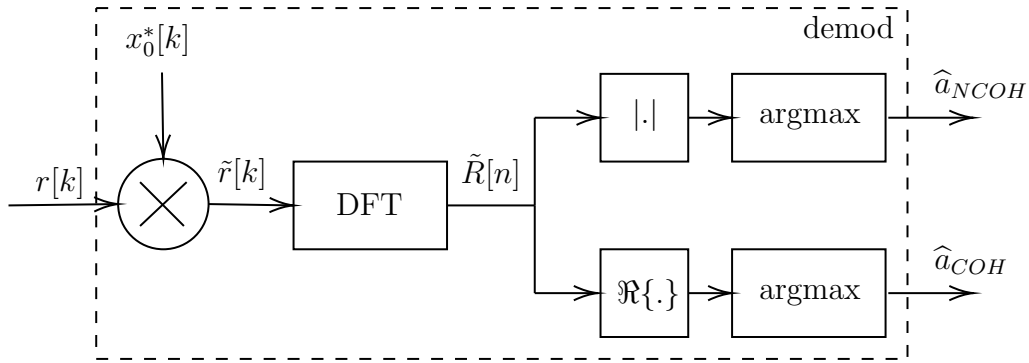
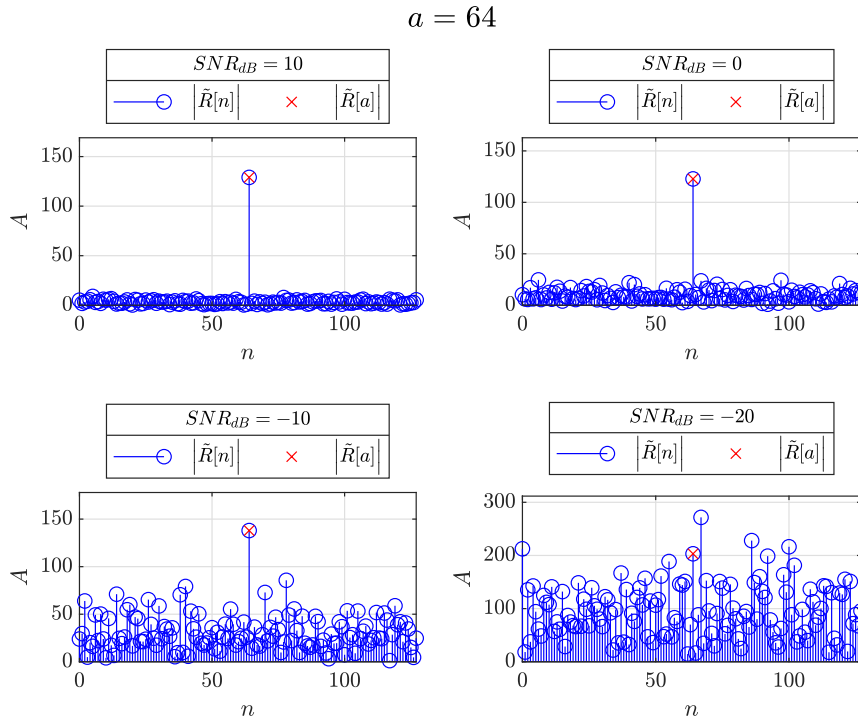


FIGURE I.2.10. – Schéma bloc du démodulateur LoRa

La Figure I.2.11 montre un exemple de démodulation non-cohérente d'un symbole LoRa avec  $a = 64$ , pour plusieurs valeurs de  $SNR_{dB} \in \{10, 0, -10, -20\}$  et  $SF = 7$ . Nous affichons également le bin en  $|\tilde{R}[a]|$ . D'après la figure, nous constatons que plus le SNR est faible, plus la puissance du signal LoRa reçu est faible par rapport au niveau de bruit. Ainsi, le symbole LoRa se retrouvera progressivement noyé dans ce dernier avec  $SNR_{dB} = -20$ , empêchant toute démodulation correcte. Les performances en présence d'AWGN en fonction de SF sont présentées en Section I.2.7.1.


 FIGURE I.2.11. – Exemple de démodulation LoRa en AWGN pour plusieurs valeurs de SNR,  $SF = 7$ 

### I.2.4.3. Format de trame

En pratique, l'émetteur met en forme les informations à transmettre dans un format particulier connu du récepteur. Ce format ne comporte pas seulement les données utilis-

teur, mais également des informations supplémentaires pour assurer différentes fonctions telles que la vérification d'intégrité des messages, des fonctionnalités protocolaires de plus haut niveau et surtout des mécanismes de synchronisation, inhérents à la couche physique (présentés en détail dans la Section I.2.6.3). La trame LoRa au niveau de la couche physique est représentée sur la Figure I.2.12 qui est issue d'une synthèse des références [45, 81, 77]. La trame comporte :

- un préambule permettant la synchronisation,
- un entête de couche physique optionnel contenant diverses informations comme la taille du payload ou l'utilisation de codes correcteurs d'erreurs,
- les données à transmettre (payload) issues de la couche MAC (voir Figure I.2.4),
- une somme de contrôle CRC permettant de vérifier l'intégrité de la trame reçue.

Le préambule suit quant à lui le format suivant :

- un nombre variable  $N_{up}$  de symboles upchirp  $x_0$ . Généralement,  $N_{up} = 8$ , une valeur offrant un bon compromis entre robustesse de synchronisation et perte de débit utile,
- deux symboles d'identification réseau LoRaWAN ( $N_{ID} = 2$ ) ayant pour valeur  $a_{ID}$  et  $M - a_{ID}$ ,
- deux symboles downchirp  $x_0^*$  suivis d'un quart de symbole downchirp, soit  $N_{down} = 2.25$ . L'usage du dernier quart de symbole downchirp n'est pas explicitement donné dans le brevet LoRa [45] et les travaux dans la littérature sur la synchronisation [81, 75, 76, 4, 77, 5] n'exploitent pas ce dernier.

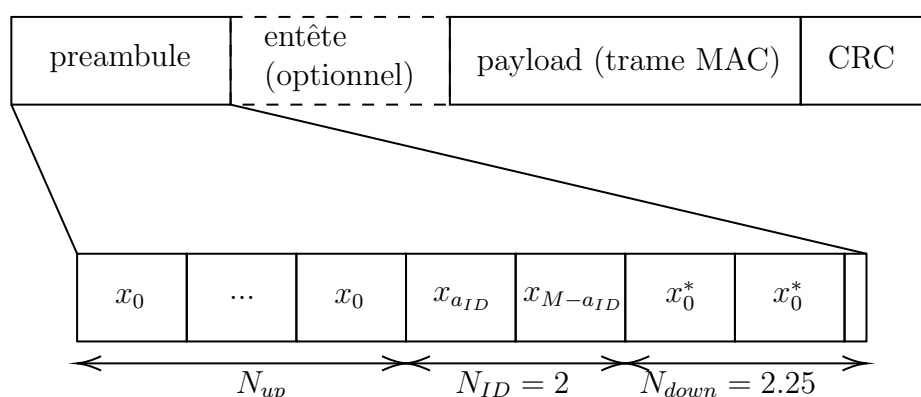


FIGURE I.2.12. – Format de trame LoRa au niveau de la couche physique

Nous noterons par  $N_{pre} = N_{up} + N_{down}$ , le nombre de symboles dans le préambule,  $N_{payload}$ , le nombre de symboles dans le payload et  $N_{frame} = N_{pre} + N_{payload}$ , le nombre total de symboles dans la trame.

## I.2.5. Schéma bloc d'une transmission LoRa

La Figure I.2.13 présente les différents blocs fonctionnels d'une transmission LoRa, pour l'émetteur et le récepteur. Dans ce qui suit, nous présentons les blocs Codage Hamming, Décodage Hamming, Blanchiment, Déblanchiment, Entrelacement, Désentrelacement, Codage Gray et Décodage Gray. Les blocs Synchronisation et Détection préambule seront détaillés dans les Sections I.2.6.3 et I.2.6.4.

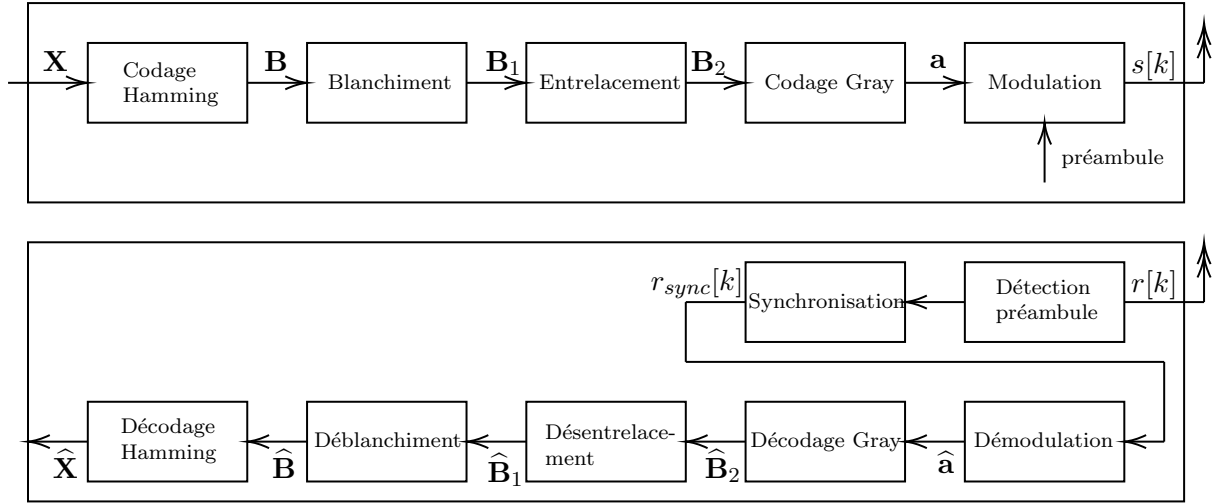


FIGURE I.2.13. – Schéma bloc de transmission LoRa

### I.2.5.1. Codage de canal

Afin d'améliorer la robustesse de la transmission, LoRa utilise du codage de canal. Le codage de canal ajoute  $s$  bits de redondance dans un mot d'information à transmettre de  $d$  bits, pour former un mot code de  $v = d + s$  bits avec  $d < v$ . Le rendement du code est défini par :

$$r_{channel} = \frac{d}{v} \quad (\text{I.2.15})$$

Plus le rendement est élevé ( $r_{channel} \approx 1$ ), moins le code aura de bits de redondance. Le débit utile d'information sera alors plus important, mais au prix d'une plus faible capacité de détection et de correction d'erreurs, définies respectivement par :

$$det_{err} = d_{MIN} - 1 \quad (\text{I.2.16})$$

$$corr_{err} = \left\lfloor \frac{d_{MIN} - 1}{2} \right\rfloor \quad (\text{I.2.17})$$

avec  $d_{MIN}$ , le plus petit nombre de bits différents entre deux mots de code. A l'inverse, un rendement faible maximise les performances de correction du code, au détriment du débit utile. Il y a donc en pratique un compromis entre rendement et capacité de correction à choisir. Notons qu'à chaque mot d'information est associé un mot code.

Dans le cadre de LoRa, le codage de canal de Hamming avec différents rendements est utilisé, noté ici Hamming( $v, d$ ) [45, 82]. Les mots d'information sont de taille fixe  $d = 4$ , tandis que les mots de code sont de taille  $v \in \{5, 6, 7, 8\}$ . Le standard LoRa exprime un peu différemment le rendement en faisant apparaître le nombre  $s$  de bits de redondance, aussi appelé Coding Rate (CR) et vaut :

$$r_{channel,LoRa} = \frac{d}{v} = \frac{4}{4 + CR}, \quad CR \in \{1, 2, 3, 4\} \quad (\text{I.2.18})$$

## I.2. LoRa

Le premier code de Hamming fût développé en 1950 par Richard Hamming et est le Hamming(7, 4) [83]. Ce dernier a une capacité de détection  $det_{err} = 2$  avec  $d_{MIN} = 3$ , et peut corriger à coup sûr une seule erreur i.e.  $corr_{err} = 1$ . Le code de Hamming(8, 4) est une version dite étendue de Hamming(7, 4). Il ajoute à chaque mot de code Hamming(7, 4) un bit de parité. Ainsi, nous avons  $det_{err} = 3$  et  $d_{MIN} = 4$ . Cette variante a l'avantage de pouvoir à la fois détecter une double erreur et corriger une seule erreur dans un mot de code, contrairement à Hamming(7, 4) pouvant faire uniquement l'un ou l'autre. Les codes de Hamming(6, 4) et Hamming(5, 4) ont une capacité de correction  $corr_{err} = 0$ . Ils sont par conséquent peu utiles en pratique, leur seul avantage étant de tout de même pouvoir détecter une erreur et proposer un bon rendement.

Dans les sections I.2.5.1.1 et I.2.5.1.2 suivantes, nous nous concentrons sur le codage de Hamming(7, 4), le plus couramment utilisé pour LoRa. Le codage de Hamming(8, 4) utilise des traitements très proches. Ainsi,  $v = 7$ .

### I.2.5.1.1. Codage

Dans le schéma LoRa, l'émetteur constitue une matrice de bits d'information de taille  $4 \times SF$  et notée  $\mathbf{X}$ . La matrice de mots de code associée, notée  $\mathbf{B}$ , est obtenue par :

$$\mathbf{B} = (\mathbf{G}^T \mathbf{X}) \pmod{2} \quad (\text{I.2.19})$$

avec :

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad (\text{I.2.20})$$

la matrice génératrice définissant le code.  $\mathbf{B}$  de taille  $7 \times SF$ , est ensuite blanchie puis entrelacée. Nous notons par  $\mathbf{b}_i$ , le  $i^{\text{ème}}$  mot de code ( $i^{\text{ème}}$  colonne dans  $\mathbf{B}$ ). Nous remarquons qu'il est possible de constituer 7 symboles codés sur SF bits. Ces 7 symboles seront par la suite codés avec un mapping de Gray.

### I.2.5.1.2. Décodage

En réception, après tous les traitements intermédiaires (décodage de Gray, désentrelacement et déblanchiment), la matrice de syndromes notée  $\mathbf{S}$ , est obtenue grâce à la matrice de parité, notée  $\mathbf{H}$  :

$$\mathbf{S} = \mathbf{H}\hat{\mathbf{B}} \quad (\text{I.2.21})$$

avec :

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \quad (\text{I.2.22})$$

et  $\hat{\mathbf{B}}$ , la matrice des mots de code reçue. La matrice de syndromes indique la présence d'erreurs et leur localisation pour chaque mot de code. Les syndromes sont donc rangés

en ligne. Notons  $\mathbf{s}_i$ , le  $i^{\text{ème}}$  syndrome ( $i^{\text{ème}}$  ligne dans  $\mathbf{S}$ ) du  $i^{\text{ème}}$  mot de code reçu  $\widehat{\mathbf{b}}_i$ ,  $\widehat{\mathbf{b}}_{i,corr}$  le  $i^{\text{ème}}$  mot de code corrigé et  $\widehat{\mathbf{B}}_{corr}$ , la matrice des mots de code corrigés.

En fonction des valeurs du syndrome, le récepteur conclura :

- $\mathbf{s}_i = [0\ 0\ 0]$   
Aucune erreur détectée et donc pas de correction nécessaire. Nous avons donc :  
 $\widehat{\mathbf{b}}_{i,corr} = \widehat{\mathbf{b}}_i$ .
- $\mathbf{s}_i \neq [0\ 0\ 0]$  et un seul bit à 1 à la position  $j$   
Le récepteur détecte la présence d'une erreur à la position  $j = \text{bi2de}(\mathbf{s}_i)$  avec  $\text{bi2de}(\cdot)$ , la fonction de conversion binaire vers décimale. Elle est corrigée en ajoutant modulo 2 un 1 au  $j^{\text{ème}}$  élément :

$$\widehat{\mathbf{b}}_{i,corr} = (\widehat{\mathbf{b}}_i + \mathbf{1}_j) \pmod{2} \quad (\text{I.2.23})$$

où  $\mathbf{1}_j$  dénote le vecteur de zéros sauf à la position  $j$  contenant 1.

- $\mathbf{s}_i \neq [0\ 0\ 0]$  et plusieurs bit à 1 présents  
Le récepteur appliquera la correction en ajoutant modulo 2 au mot de code erroné la colonne d'indice  $l$  dans  $\mathbf{H}$  qui est égale à  $\mathbf{s}_i$  :

$$\widehat{\mathbf{b}}_{i,corr} = (\widehat{\mathbf{b}}_i + \mathbf{h}_l) \pmod{2} \quad (\text{I.2.24})$$

Dans ce cas de figure, la correction apportée sera fautive et le récepteur pourra même dans certains cas ajouter des erreurs.

Une fois les mots de code reçus corrigés, la matrice des mots d'information estimée  $\widehat{\mathbf{X}}$  est obtenue en extrayant les 4 premières colonnes de  $\widehat{\mathbf{B}}_{corr}$ .

## I.2.5.2. Blanchiment et entrelacement

### I.2.5.2.1. Blanchiment

A l'émission, un blanchiment est appliqué sur la matrice des mots de code  $\mathbf{B}$  afin de donner à la séquence pseudo-aléatoire binaire des propriétés statistiques proches de celles de la loi normale (terme blanchiment lié à l'AWGN) [82, 84]. Cela permet d'obtenir un flux de symboles aléatoires presque parfaitement décorrélés. Ainsi, cela réduit la propagation d'erreurs lors de certains processus au niveau du récepteur comme la synchronisation. Le blanchiment n'entraîne pas de baisse de débit.

Notons qu'en simulation, les symboles sont déjà générés aléatoirement et parfaitement indépendants (distribution uniforme sur  $\{0, 1, \dots, M-1\}$ ). Ainsi, sans perte de généralité, ce bloc sera ignoré pour le reste du mémoire.

### I.2.5.2.2. Entrelacement

L'entrelacement réarrange l'ordre des bits entre différents mots de code, afin de réduire statistiquement le nombre d'erreurs par mot de code et donc de favoriser la capacité de correction du code de Hamming. Nous nous arrangeons pour que chaque mot de code entrelacé comporte des bits issus de mots de code différents. Pour LoRa, le schéma d'entrelacement en Figure I.2.14 a été retenu [45, 70, 65] et utilise une permutation à



la fois circulaire et diagonale. Cela est réalisé par le bloc **Entrelacement** prenant en entrée la matrice codée Hamming blanchie  $\mathbf{B}_1$  et sortant sa version entrelacée  $\mathbf{B}_2$ . Le bloc **Désentrelacement** réalise l'opération inverse.

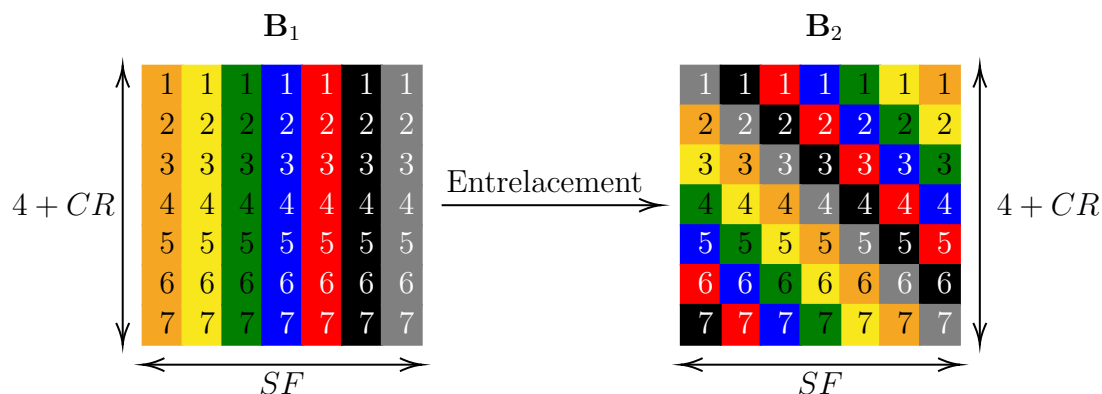


FIGURE I.2.14. – Schéma d'entrelacement LoRa pour le codage de canal de Hamming(7,4)

Les auteurs dans [70] ont obtenu une expression théorique du taux d'erreur trame pour le récepteur non-cohérent avec codage de Hamming, codage de Gray et entrelacement.

### I.2.5.3. Codage de Gray

Le mapping classique (conversion directe de paquets de  $SF$  bits en valeur décimale) peut-être amélioré grâce au codage de Gray. Dans ce dernier, les symboles adjacents sont codés de façon à ce qu'il n'y ait qu'un seul bit différent. Le Tableau I.2.3 donne un exemple de codage de Gray pour  $SF = 3$ .

Valeur de symbole	Mot binaire
0	0 0 0
1	0 0 1
2	0 1 1
3	1 1 1
4	1 0 1
5	1 0 0
6	1 1 0
7	0 1 0

TABLE I.2.3. – Exemple de codage de Gray LoRa pour  $SF = 3$

Si une détection de symbole est erronée à  $\pm 1$  indice près i.e.  $\hat{a} = (a \pm 1) \bmod M$ , il n'y aura qu'un seul bit faux dans le symbole estimé et la capacité de correction de Hamming sera facilitée (correction d'une seule erreur). Statistiquement, les erreurs de démodulation se font en majorité à  $\pm 1$  indice fréquentiel à cause des résidus de désynchronisation (voir Section I.2.6.2.3). Ainsi, avec le codage de Gray combiné avec celui de Hamming, les performances de la transmission LoRa s'améliorent. Le bloc **Codage Gray** reçoit en entrée la matrice de bits codés Hamming, blanchie et entrelacée  $\mathbf{B}_2$ , de taille  $v \times SF$ , et produit alors  $v$  symboles codés sur  $SF$  bits, rangés dans le vecteur  $\mathbf{a}$ . Le bloc **Décodage Gray** réalise l'opération inverse.

## I.2.6. Synchronisation LoRa

Dans cette section, nous présentons en Section I.2.6.1 les principales désynchronisations émetteur-récepteur subies en pratique : la désynchronisation fréquentielle Carrier Frequency Offset (CFO) et les désynchronisations temporelles Sampling Temporal Offset (STO) et Sampling Frequency Offset (SFO). Nous illustrons ensuite en Section I.2.6.2 l'impact de ces désynchronisations sur la démodulation, puis les différents algorithmes de synchronisation que nous pouvons trouver dans la littérature en Section I.2.6.3. Enfin, nous présentons en Section I.2.6.4 un autre aspect important de la synchronisation : la détection de trame.

### I.2.6.1. Désynchronisations CFO, STO et SFO

#### I.2.6.1.1. CFO

En pratique, l'émetteur et le récepteur sont désynchronisés fréquentiellement. Cela vient des oscillateurs locaux réalisant la transposition en fréquence autour de la fréquence porteuse  $F_c$  qui ne sont pas parfaits. En effet, la fréquence porteuse obtenue ne correspond pas parfaitement à celle voulue, un décalage est présent à l'émetteur comme au récepteur :

$$F_c^{Tx} = F_c + \Delta_f^{Tx} \quad (\text{I.2.25})$$

$$F_c^{Rx} = F_c + \Delta_f^{Rx} \quad (\text{I.2.26})$$

Ainsi, le décalage de fréquence porteuse total est :

$$F'_c = F_c + \Delta_f \quad (\text{I.2.27})$$

avec :

$$\Delta_f = \Delta_f^{Tx} + \Delta_f^{Rx} \quad (\text{I.2.28})$$

En fonction de la qualité des oscillateurs,  $\Delta_f$  sera plus ou moins élevé. Dans l'industrie, on exprime généralement ce décalage en Partie Par Million (ppm) par rapport à la fréquence porteuse désirée. Par exemple, pour  $F_c = 868.1$  MHz, avoir  $\pm 5$  ppm correspond à un décalage d'environ 4.34 kHz autour de  $F_c$ . Une valeur de  $\pm 2$  ppm est déjà très bonne, seuls des transceivers de bonne qualité peuvent y prétendre, comme certains dispositifs haut de gamme de type Software Defined Radio (SDR) [85]. Les transceivers LoRa à bas coût ont des valeurs plus élevées, pouvant aller jusqu'à  $\Delta_f = \pm B/4$  [86].

Afin de modéliser plus facilement le CFO, il est judicieux de convertir ce dernier dans le domaine fréquentiel LoRa. Nous exprimons le CFO en nombre de bins fréquentiels de décalage de bande par :

$$\Delta_f = \underbrace{(CFO_{int} + CFO_{frac})}_{CFO} \times \frac{B}{M} \quad (\text{I.2.29})$$

avec  $CFO_{int} \in \pm\{0, 1, \dots, M - 2\}$  et  $CFO_{frac} \in [0; 1]$ . Ainsi,  $\Delta_f = +4.34$  kHz conduit pour  $B = 125$  kHz et  $SF = 7$  à  $CFO \approx 4.44$  et donc  $CFO_{int} = 4$  et  $CFO_{frac} \approx 0.44$ .

### I.2.6.1.2. STO

Le STO est un décalage temporel entre les frontières délimitant les symboles. Supposons que l'émetteur commence sa transmission à  $t = 0$  s. Les frontières symbole seront présentes alors toutes les  $i \times T$  secondes, avec  $i$ , l'indice du symbole transmis ( $i \in \{0, 1, \dots\}$ ). Le récepteur, n'ayant pas commencé l'échantillonnage au même instant que l'émetteur, verra alors un décalage des frontières de  $\tau$  secondes.

De manière similaire au CFO, nous exprimons le STO normalisé par rapport à la période d'échantillonnage LoRa :

$$\tau = \underbrace{(STO_{int} + STO_{frac})}_{STO} \times T_s \quad (\text{I.2.30})$$

avec  $STO_{int} \in \{0, 1, \dots, M - 1\}$  et  $STO_{frac} \in [-0.5; 0.5]$ . Par exemple,  $\tau = 69 \mu\text{s}$  correspond pour  $F_s = B = 125 \text{ kHz}$  à  $STO = 8.675$ , et donc  $STO_{int} = 9$  et  $STO_{frac} = -0.375$ . Si nous avons  $STO = 10.5$  par exemple, nous pouvons alors avoir les deux cas de figure suivants :  $STO_{int} = 10$  et  $STO_{frac} = 0.5$  ou bien  $STO_{int} = 11$  et  $STO_{frac} = -0.5$ .

Notons que la partie fractionnaire du STO n'est pas modélisée de la même manière que celle du CFO ( $0 \leq |STO_{frac}| \leq 0.5$  et  $0 \leq |CFO_{frac}| \leq 1$ ), les algorithmes dans la littérature reposent en effet sur cette modélisation. Contrairement au CFO qui dépend du matériel et ne varie pas ou de façon négligeable au cours de la transmission, le STO est aléatoire à chaque transmission, uniforme sur la durée symbole :  $\tau \sim \mathcal{U}[0; T]$ .

En simulation, nous pouvons simuler le STO de la façon suivante :

1. Générer le flux de symboles à la fréquence d'échantillonnage minimale  $F_s = B$ .
2. Sur-échantillonner le signal d'un facteur  $R$ . Le STO simulé correspondra alors à  $STO_{sps} = \lfloor STO \times R \rfloor / R$  échantillons de décalage. Nous notons  $r_{STO}^{(R)}[k]$  et  $r^{(R)}[k]$ , le signal sur-échantillonné avec et sans désynchronisation STO, respectivement.
3. Le signal est ensuite sous-échantillonné d'un facteur  $R$  pour revenir au traitement à  $F_s = B$  pour obtenir le signal  $r_{STO}[k]$ .

Deux modèles de STO sont possibles, présentés en Figures I.2.15 et I.2.16 et détaillés dans ce qui suit.

Premier modèle STO :

- Ajouter  $STO_{sps}$  échantillons de zéro au début du signal sur-échantillonné et éliminer les  $STO_{sps}$  derniers échantillons, cela afin de conserver un nombre entier de symboles :

$$r_{STO,1}^{(R)}[k'] = 0_{STO_{sps} \times 1} \cup (r^{(R)}[k']H[k' - STO_{sps}]) \quad (\text{I.2.31})$$

avec  $0_{STO_{sps} \times 1}$ , le vecteur colonne de  $STO_{sps}$  zéros,  $k' \in \{0, 1, \dots, (R \times M \times N_{frame}) - 1\}$ , l'indice temporel sur-échantillonné et  $H[k]$ , la fonction échelon discrète.

Second modèle STO :

- Éliminer les  $STO_{sps}$  premiers échantillons du signal sur-échantillonné puis ajouter à la fin  $STO_{sps}$  échantillons de zéros :

$$r_{STO,2}^{(R)}[k'] = (r^{(R)}[k' - STO_{sps}]H[-k'] * \delta[k' - STO_{sps}]) \cup 0_{STO_{sps} \times 1} \quad (I.2.32)$$

avec  $*$ , l'opérateur de convolution et  $\delta[k]$ , la fonction Dirac discrète définie par :

$$\delta[k] = \begin{cases} 1 & \text{si } k = 0 \\ 0 & \text{sinon} \end{cases} \quad (I.2.33)$$

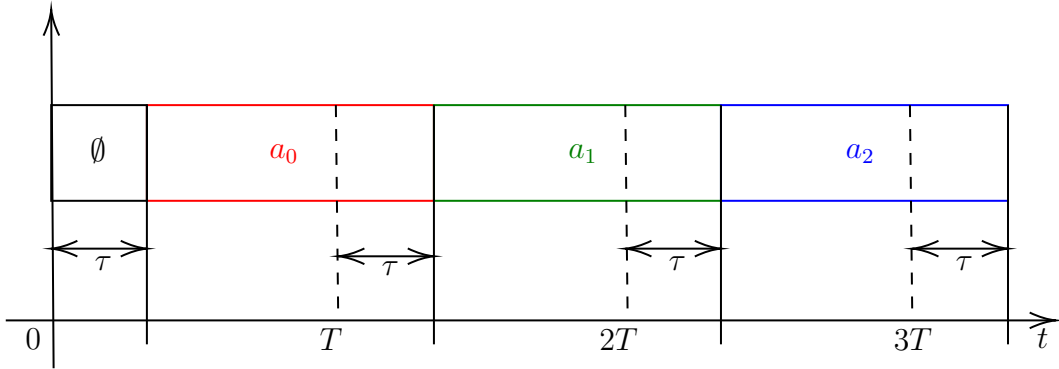


FIGURE I.2.15. – Premier modèle STO

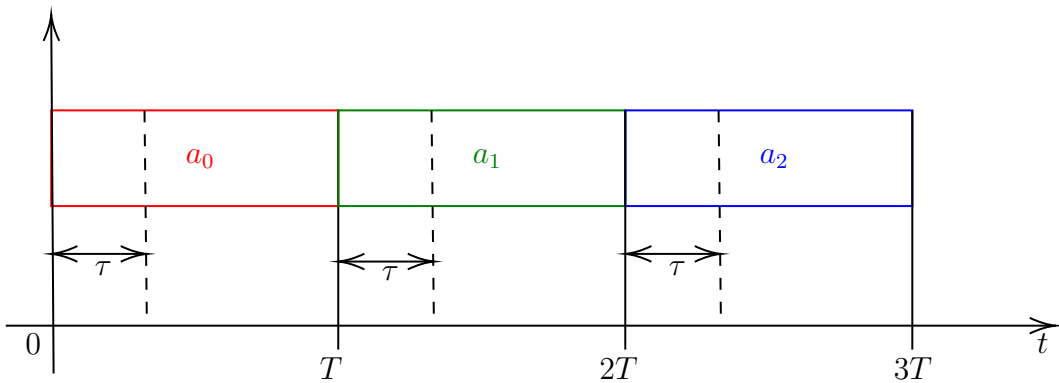


FIGURE I.2.16. – Second modèle STO

### I.2.6.1.3. SFO

Le SFO est quant à lui un décalage entre la fréquence d'échantillonnage souhaitée  $F_s$  et celle obtenue, pour l'émetteur comme pour le récepteur et suit une modélisation similaire à celle du CFO :

$$F_s^{Tx} = F_s + SFO^{Tx} \quad (I.2.34)$$

$$F_s^{Rx} = F_s + SFO^{Rx} \quad (I.2.35)$$

$$F'_s = F_s + SFO \quad (I.2.36)$$

$$SFO = SFO^{Tx} + SFO^{Rx} \quad (I.2.37)$$

La transposition en fréquence porteuse et l'échantillonnage sont généralement réalisés par le même composant, par soucis de réduction de coût [77]. Ainsi, nous obtenons la relation suivante :

$$SFO = \frac{B}{F_c} \times \Delta_f \quad (I.2.38)$$

Plus le CFO est grand, plus le SFO associé le sera également. Pour  $\Delta_f = 4.34$  kHz,  $F_c = 868.1$  MHz et  $B = 125$  kHz, nous obtenons  $SFO = 0.625$  par exemple.

## I.2.6.2. Impact du CFO, STO et SFO sur la démodulation

### I.2.6.2.1. Impact du CFO

Le signal continu reçu uniquement contaminé par le CFO est noté :

$$r_{CFO}(t) = r(t) \times e^{2j\pi\Delta_f t} \quad (I.2.39)$$

Ce dernier, une fois échantillonné à la fréquence  $F_s = B$  s'exprime :

$$r_{CFO}[k] = r[k] \times e^{2j\pi\frac{CFO}{M}k} \quad (I.2.40)$$

La Figure I.2.17 présente l'effet du CFO sur la représentation temps-fréquence d'un symbole LoRa discret. Nous pouvons aisément remarquer d'après la figure que le décalage en fréquence engendré par le CFO a deux effets :

1.  $CFO_{int}$  décale d'un nombre entier de bins la fréquence initiale. Ainsi, le symbole démodulé aura pour valeur :

$$\hat{a}_{CFO_{int}} = (a + CFO_{int}) \mod M \quad (I.2.41)$$

2.  $CFO_{frac}$  apportera des déformations au signal. Cependant, ces dernières ne sont pas intuitivement prédictibles sur le spectrogramme, mais l'effet est clairement perceptible sur la DFT finale et est présenté en Figure I.2.18.

La Figure I.2.18 montre un exemple du symbole  $a = 0$  transmis et démodulé pour différentes valeurs de CFO,  $CFO \in \{0, 20, 40.2, 60.5, 80.8\}$ , sans bruit AWGN et  $SF = 7$ . Nous constatons bien le décalage de la valeur du symbole vers la droite d'après l'équation (I.2.41).  $CFO_{frac}$  vient diffuser l'énergie du bin d'intérêt vers les bins voisins. Plus  $CFO_{frac}$  est proche de 0.5, plus cette diffusion est forte. Ainsi, il devient de plus en plus difficile de démoduler correctement, avec une incertitude maximale entre les bins  $n \in \{a, (a + 1) \mod M\}$  lorsque  $CFO_{frac} = 0.5$ . En présence de bruit AWGN modéré, le symbole démodulé sera :

$$\hat{a}_{CFO} = (a + \lfloor CFO \rfloor) \mod M \quad (I.2.42)$$

avec  $\lfloor . \rfloor$ , la fonction d'arrondi vers l'entier le plus proche. Notons que si  $CFO < 0$ , le décalage est à permutation circulaire gauche et la diffusion d'énergie vers les bins voisins gauche.

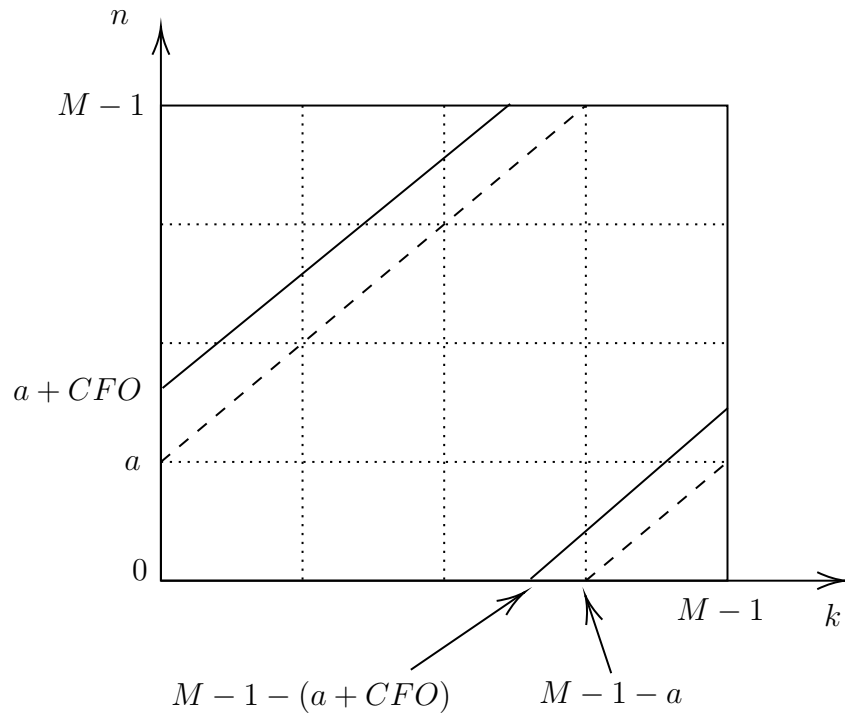


FIGURE I.2.17. – Impact du CFO sur le spectrogramme LoRa

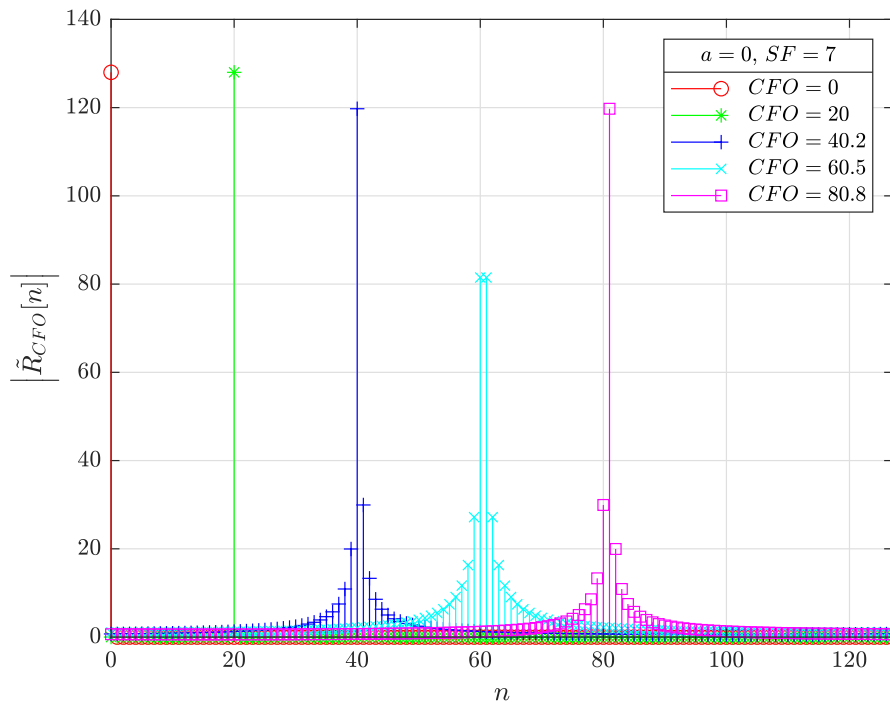


FIGURE I.2.18. – Impact du CFO sur la DFT LoRa

### I.2.6.2.2. Impact du STO

L'effet du STO sur le spectrogramme (modèle 1) est présenté en Figure I.2.19 pour trois symboles consécutifs transmis, avec  $a_0 = a_1$  et  $a_2 > a_1$ . Les références temporelles de l'émetteur et du récepteur sont représentées en pointillé et en trait plein rouge sur la figure, respectivement. D'après la figure, nous constatons :

- Si  $a_0 = a_1$  et  $STO_{frac} = 0$ , le STO vient appliquer une transformation parfaite du symbole  $a_0$  vers le symbole  $(a_0 - STO_{int}) \bmod M$ .
- Si  $a_2 \neq a_1$  et  $STO_{frac} = 0$ , de l'interférence entre symbole Inter Symbol Interference (ISI) est présente. Plus le STO est proche de  $M - 1$ , plus la contribution du symbole suivant sera forte ( $a_1$  sur la figure).
- $STO_{frac}$  viendra appliquer une déformation DFT de façon similaire à  $CFO_{frac}$ .

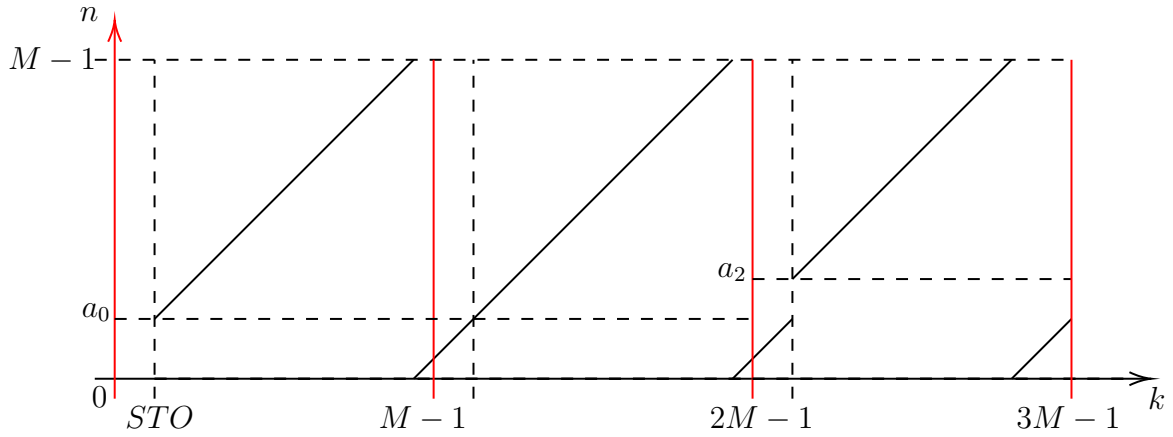


FIGURE I.2.19. – Impact du STO sur le spectrogramme LoRa

La Figure I.2.20 montre l'effet du STO sur la DFT (toujours le premier modèle STO considéré) pour la même configuration que la Figure I.2.18 avec  $a_0 = a_1 = 0$  et  $a_2 = 80$ . Sur la figure, la DFT du  $i^{\text{ème}}$  symbole est affichée. Pour  $i = 1$  (symboles  $a_0$  et  $a_1$  considérés), le comportement est très similaire à celui du CFO sur la Figure I.2.18. En revanche, pour  $i = 2$ , l'ISI est bien visible avec deux groupes de diffusion d'énergie : le premier autour de  $n = (a_1 - \lfloor STO \rfloor) \bmod M = 20$  et le second autour  $n = (a_1 - \lfloor STO \rfloor - a_2) \bmod M = 100$ .

Si nous considérons  $a^-$ , le symbole précédent et  $a$ , le symbole courant, nous avons alors en présence de bruit AWGN modéré le comportement suivant pour le premier modèle STO si  $a^- = a$  :

$$\hat{a}_{STO,1} = (a - \lfloor STO \rfloor) \bmod M \quad (\text{I.2.43})$$

Si  $a^- \neq a$ , nous avons alors :

$$\hat{a}_{STO,1} = \begin{cases} (a - \lfloor STO \rfloor) \bmod M & \text{si } STO \ll M/2 \\ (a - \lfloor STO \rfloor) \bmod M \text{ ou } (a^- - \lfloor STO \rfloor) \bmod M & \text{si } STO \approx M/2 \\ (a^- - \lfloor STO \rfloor) \bmod M & \text{si } STO \gg M/2 \end{cases} \quad (\text{I.2.44})$$

avec une indécision entre  $\hat{a}_{STO,1} = (a - \lfloor STO \rfloor) \bmod M$  et  $\hat{a}_{STO,1} = (a^- - \lfloor STO \rfloor) \bmod M$  de plus en plus marquée à mesure que STO se rapproche de  $M/2$ .

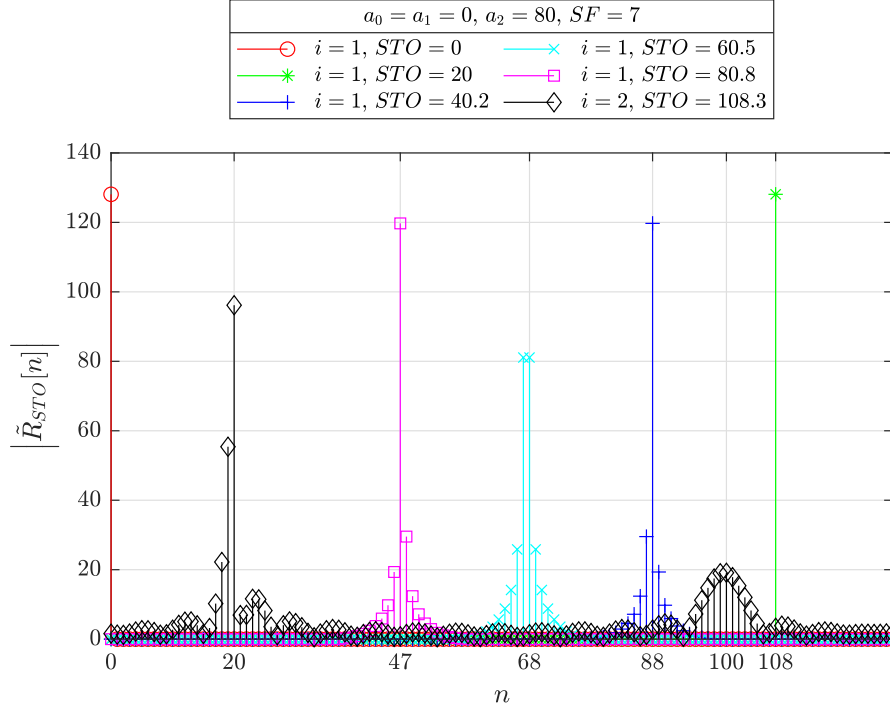


FIGURE I.2.20. – Impact du STO sur la DFT LoRa

Si nous considérons le second modèle STO, le comportement est inversé avec une contribution cette fois du symbole suivant  $a^+$  et un décalage du bin vers la droite. Cela donne pour  $a = a^+$  :

$$\hat{a}_{STO,2} = (a + \lfloor STO \rfloor) \pmod{M} \quad (\text{I.2.45})$$

Pour  $a \neq a^+$ , nous avons :

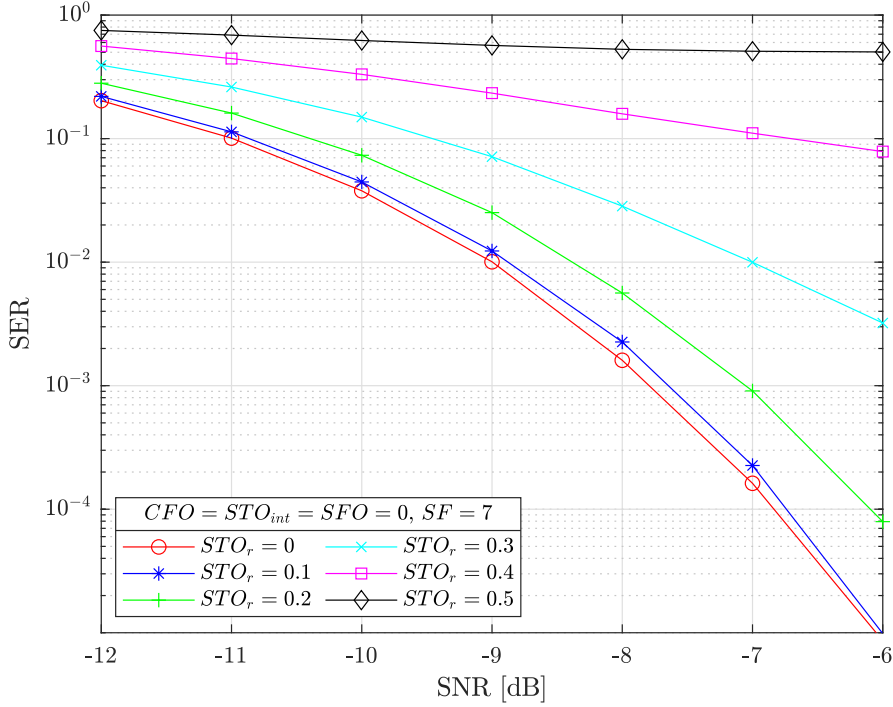
$$\hat{a}_{STO,2} = \begin{cases} (a + \lfloor STO \rfloor) \pmod{M} & \text{si } STO \ll M/2 \\ (a + \lfloor STO \rfloor) \pmod{M} \text{ ou } (a^+ + \lfloor STO \rfloor) & \text{si } STO \approx M/2 \\ (a^+ + \lfloor STO \rfloor) \pmod{M} & \text{si } STO \gg M/2 \end{cases} \quad (\text{I.2.46})$$

Par convention et pour le reste du mémoire, nous considéreront le premier modèle STO.

La Figure I.2.21 présente les performances de démodulation en termes de Symbol Error Rate (SER) pour  $STO_{frac}$  fixé ayant les valeurs  $STO_{frac} \in \{0, 0.1, 0.2, \dots, 0.5\}$ , sans autre désynchronisation i.e.  $CFO = STO_{int} = SFO = 0$  et  $SF = 7$ .

Nous remarquons bien la dégradation progressive des performances à mesure que  $STO_{frac}$  se rapproche de 0.5. Pour cette dernière, nous avons des performances très mauvaises atteignant un palier  $SER \approx 0.50$ . Nous pouvons considérer qu'avoir  $STO_{frac} \leq 0.1$  a un impact quasiment négligeable sur les performances. Avoir  $STO_{frac} = 0.2$  est raisonnable et  $STO_{frac} \geq 0.3$  est à éviter à tout prix. Il est donc indispensable d'estimer et corriger  $STO_{frac}$  en pratique. Le raisonnement sur  $CFO_{frac}$  donne exactement le même comportement.




 FIGURE I.2.21. – Impact de  $STO_{frac}$  sur les performances de démodulation

### I.2.6.2.3. Impact conjoint CFO et STO

En pratique, le signal reçu est contaminé à la fois par le CFO et le STO. D'après ce qui a été vu précédemment, nous pouvons remarquer que le décalage ne se fait pas dans la même direction pour le CFO et STO : vers la droite pour le premier et vers la gauche pour le second. La position du bin d'intérêt est alors :

$$\hat{a}_{CFO,STO} = (a + \lfloor CFO \rfloor - \lfloor STO \rfloor) \bmod M \quad (\text{I.2.47})$$

Ainsi, il n'est pas possible d'extraire indépendamment  $CFO_{int}$  et  $STO_{int}$  par unique lecture de la DFT, puisque le décalage observé est la somme de deux décalages inconnus dans l'équation (I.2.47).

Rappelons que le préambule LoRa possède également des symboles downchirp. Sur ces derniers, le décalage ne possède pas le même comportement. Le CFO décale toujours vers la droite, mais le STO décale cette fois ci vers la droite et non plus vers la gauche. Dans le préambule, nous avons  $a_{down} = 0$  (formes d'onde  $x_0^*[k]$  transmises, voir Section I.2.4.3). Ainsi, le bin d'intérêt downchirp, après désynchronisation, se retrouve à la position :

$$\hat{a}_{down,CFO,STO} = (\lfloor CFO \rfloor + \lfloor STO \rfloor) \bmod M \quad (\text{I.2.48})$$

Connaissant cette propriété particulière, le récepteur peut exploiter conjointement les symboles upchirp et downchirp du préambule pour séparer indépendamment  $CFO_{int}$  et  $STO_{int}$ .

La Figure I.2.22 quantifie l'impact sur la DFT de la présence conjointe du CFO et STO pour  $SF = 7$ . Comme  $CFO_{int}$  et  $STO_{int}$  n'entraînent pas de déformation DFT (un simple décalage du bin d'intérêt, si  $a^- = a$ ), nous choisissons  $CFO \in [0; 1]$  et  $STO \in [0; 1]$ . Le

critère retenu est l'écart d'amplitude entre les bins voisins directs gauche et droit et le bin d'intérêt :

$$\delta_{CFO,STO} = \min \{ \delta^-, \delta^+ \} \in [0; M] \quad (I.2.49)$$

avec :

$$\delta^- = \left| \left| \tilde{R}[a] \right| - \left| \tilde{R}[(a-1) \bmod M] \right| \right| \quad (I.2.50)$$

$$\delta^+ = \left| \left| \tilde{R}[a] \right| - \left| \tilde{R}[(a+1) \bmod M] \right| \right| \quad (I.2.51)$$

$\delta_{CFO,STO}$  élevé signifie donc une faible déformation DFT.

D'après la figure, les cas où la déformation est minimale sont lorsque nous avons  $CFO_{frac}$  et/ou  $STO_{frac}$  nuls. La diagonale droite donne également une faible déformation avec  $\delta_{CFO,STO} > 105$ . Cela correspond à avoir  $CFO + STO$  entier ( $CFO + STO = 1$  dans la figure). Enfin, les cas les plus défavorables (pics voisins très proches de celui d'intérêt) sont lorsque nous avons  $CFO + STO$  donnant une partie fractionnaire égale à 0.5 ( $CFO + STO = 0.5$  dans la figure).

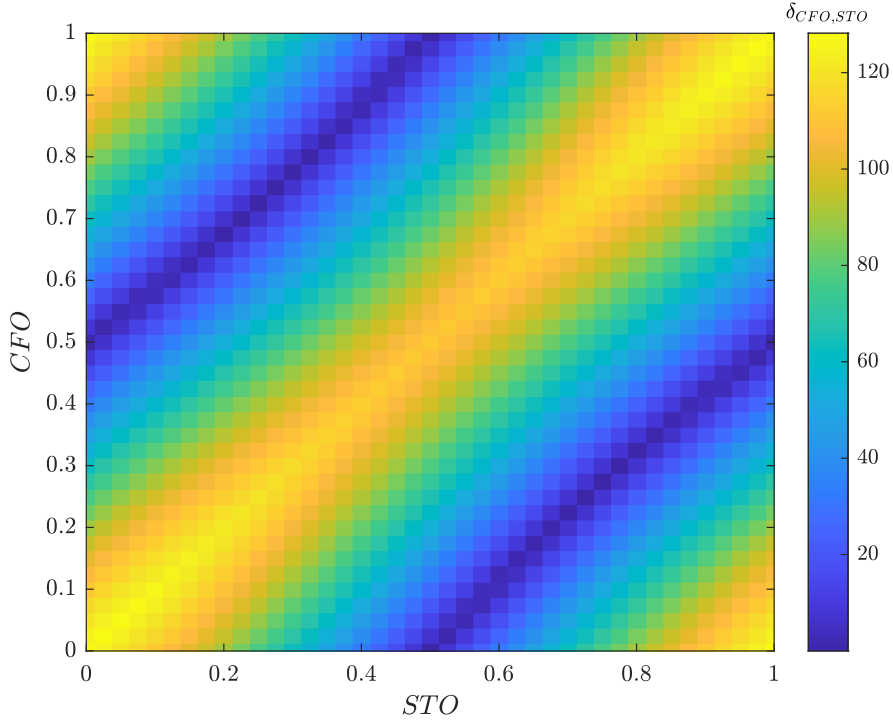


FIGURE I.2.22. – Impact de la présence conjointe du CFO et STO sur la DFT LoRa

#### I.2.6.2.4. Impact du SFO

L'expression d'un flux de symboles LoRa impactés par le SFO a été obtenue dans la littérature [75], et a pour expression :

$$r_{i,SFO}[k] = r_i[k] \times e^{2j\pi k i \left[ \left( \frac{B}{Fs'} \right)^2 - \frac{B}{Fs'} \right]} \quad (I.2.52)$$

avec  $i$ , l'indice de symbole transmis et rappelons  $F'_s = B + SFO$ .

La Figure I.2.23 illustre l'impact du SFO sur la représentation temps-fréquence pour le symbole  $a = 0$ ,  $SFO < 0$  et  $M = 8$  par soucis de lisibilité de figure. Comme la fréquence d'échantillonnage effective est réduite, nous remarquons que l'instant d'échantillonnage se décale progressivement dans le temps, avec un retard accumulé à chaque tap. Dans l'exemple de la figure, à la fin de la durée symbole, l'échantillonneur s'est décalé d'une période d'échantillonnage  $T_s$ . Le décalage sera de plus en plus rapide à mesure que la fréquence d'échantillonnage effective diminue. Si  $SFO > 0$ , l'échantillonneur prend de l'avance.

D'après la figure, l'instant d'échantillonnage effectif se décale de  $\delta_{SFO} = |T'_s - T_s|$  secondes à chaque tap. Ainsi, le décalage d'une période d'échantillonnage  $T_s$  nécessite  $K_{SFO} = T_s/\delta_{SFO}$  taps. Ce décalage se produira alors au bout du symbole  $i = N_{SFO} = \lfloor K_{SFO}/M \rfloor$ .

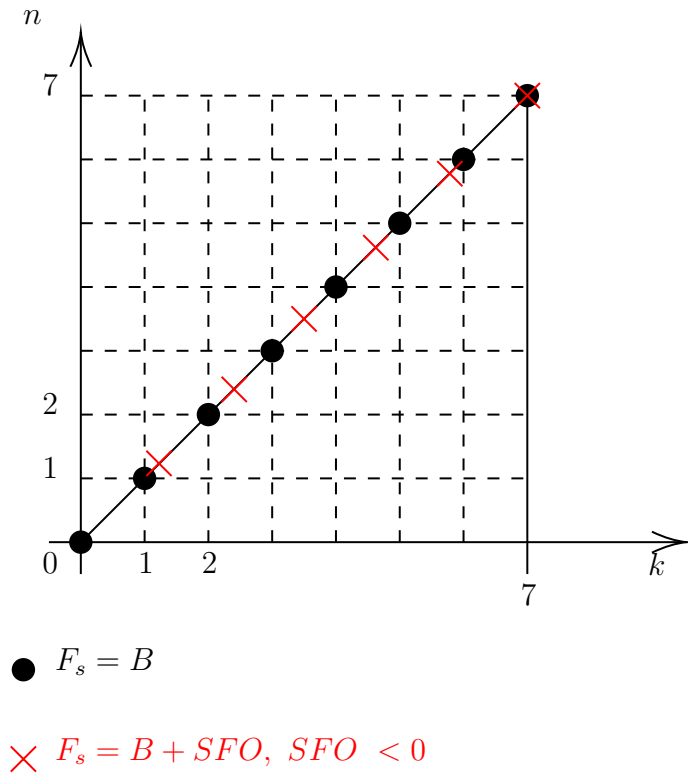


FIGURE I.2.23. – Impact du SFO sur le spectrogramme LoRa

La Figure I.2.24 présente l'évolution au cours du temps de l'amplitude du bin d'intérêt  $n = a_i = 64$  et de ses voisins gauche  $n \in \{a_i - 1, a_i - 2, a_i - 3\}$ , pour  $CFO = 32$  (et donc  $SFO = 18$  Hz),  $F_s = 250$  kHz,  $F_c = 868.1$  MHz et  $SF = 7$ . Nous constatons que le bin d'intérêt cède progressivement son énergie sur les bins voisins gauche (le premier, puis le second, puis le troisième, etc.). Le  $l^{\text{ème}}$  bin voisin gauche aura une énergie maximale tous les  $l \times N_{SFO}$  symboles, avec  $l \in \{1, 2, \dots, M - 1\}$ . Cela donne donc par exemple une diffusion complète sur le premier symbole voisin gauche au  $109^{\text{ème}}$  symbole. Si  $SFO < 0$ , le comportement est inversé avec une dérive dans le temps vers les bins voisins droit.

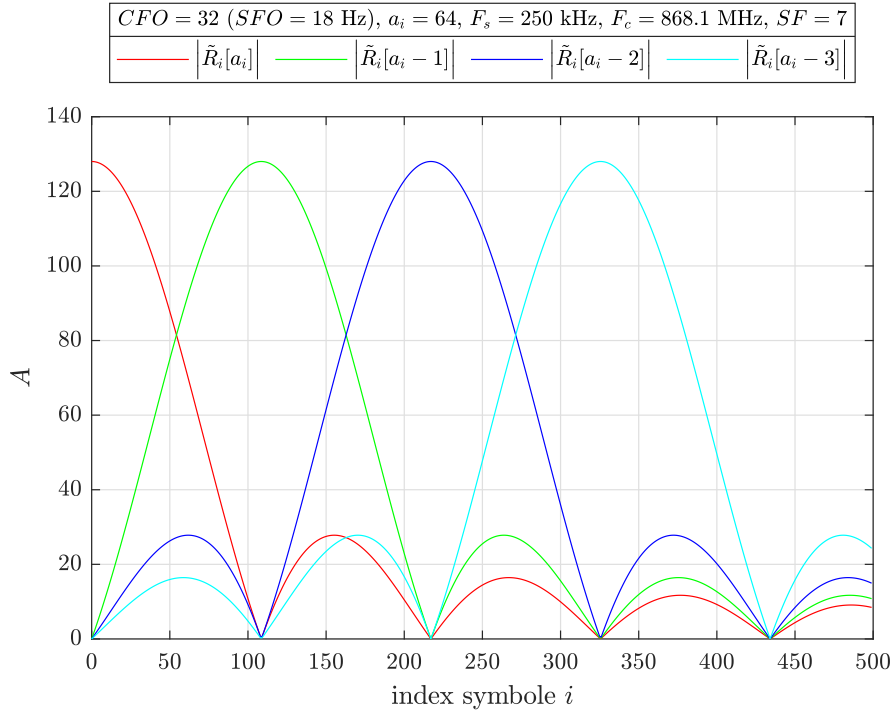


FIGURE I.2.24. – Impact du SFO sur la DFT LoRa

### I.2.6.3. Front-end de synchronisation

Dans la littérature, plusieurs algorithmes de synchronisation LoRa ont été développés [77, 75, 87, 5, 76, 4]. Cependant, tous n'offrent pas les mêmes performances et la même complexité d'implémentation. Il a été décidé de ne retenir que les algorithmes les plus pertinents, offrant un front-end de synchronisation complet et robuste. Les auteurs dans [76] ont proposé un premier front-end prometteur, qu'ils ont par la suite amélioré dans [4] et montrant de meilleures performances que celui proposé dans [77].

Le front-end de synchronisation présenté par la suite repose en grande partie sur celui de [4], et également [5] pour l'estimateur  $CFO_{frac}$  et [75] pour la modélisation du SFO. Un changement sur le format de trame a été choisi dans nos travaux par rapport à celui du standard initial utilisé dans les traitements LoRa. En effet, il y a  $N_{down} = 2.25$  symboles downchirp dans le préambule original (voir Section I.2.4.3). Cependant, aucun des algorithmes de synchronisation proposés n'exploite le dernier quart de symbole. Par conséquent, nous l'avons ignoré. De plus, dans le front-end de synchronisation, une exploitation conjointe des symboles upchirp et downchirp pour l'estimation de  $CFO_{int}$  et  $STO_{int}$  est faite. Afin d'effectuer des traitements équitables entre les symboles upchirp et downchirp, nous avons imposé la contrainte  $N_{down} = N_{up}$ . Comme  $N_{up} = 8$  généralement, nous avons alors  $N_{down} = 8$ . Ce point est expliqué plus en détail dans la Section I.2.6.3.3.

Le front-end de synchronisation doit estimer les quatre inconnues suivantes :  $CFO_{int}$ ,  $CFO_{frac}$ ,  $STO_{int}$  et  $STO_{frac}$  (le SFO est estimé dans l'équation (I.2.38) à partir de  $CFO_{int}$  et  $CFO_{frac}$ ). La difficulté de développer un front-end de synchronisation efficace est de bien maîtriser les impacts du CFO, STO et SFO sur la démodulation et de correctement identifier les dépendances et interactions entre les différents paramètres. Ainsi, l'ordre d'estimation des inconnues est crucial.

Le front-end de synchronisation proposé est illustré en Figure I.2.25 et repose majoritairement sur les travaux dans [4]. Il comporte six étapes principales pouvant comporter une ou deux sous-étapes. Dans chaque bloc de la figure, le numéro d'étape et de sous-étape est indiqué ; bloc 2a pour étape 2, sous-étape a, par exemple. Dans ce qui suit, nous détaillons le fonctionnement de chaque étape avec les équations associées. Nous notons  $r[k]$ , la trame reçue désynchronisée et  $r_i[k]$ , le  $i^{\text{ème}}$  symbole reçu désynchronisé avec  $k \in \{0, 1, \dots, (M \times N_{frame}) - 1\}$ . Nous adoptons aussi la convention de notation suivante : le mot clé *sync* mis en indice d'une variable est toujours suivi de sa signification. Par exemple,  $r_{i, sync, \widehat{CFO}_{frac}, \widehat{CFO}_{int}}[k]$  signifie le  $i^{\text{ème}}$  symbole reçu désynchronisé, mais corrigé en  $CFO_{frac}$  et  $CFO_{int}$  avec les estimées  $\widehat{CFO}_{frac}$  et  $\widehat{CFO}_{int}$ , respectivement.

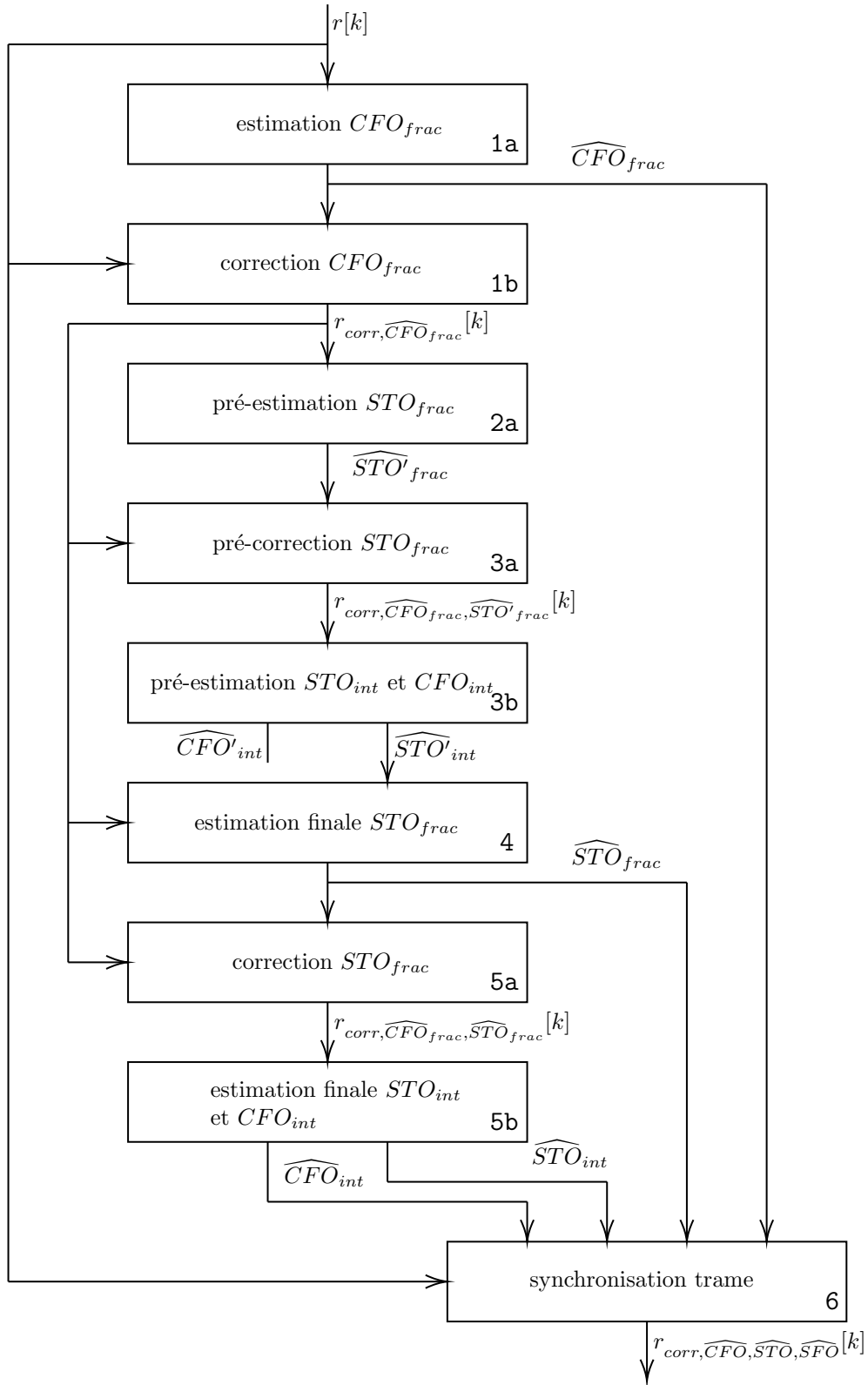


FIGURE I.2.25. – Front-end de synchronisation LoRa de la littérature [4]

### I.2.6.3.1. Étape 1 – estimation et correction de $CFO_{frac}$

Dans [76], il a été montré que  $CFO_{frac}$  peut-être estimé de manière parfaitement indépendante de  $CFO_{int}$  et du STO. Ainsi, ce dernier est estimé et corrigé en premier afin d'éliminer une inconnue pour la suite. L'estimateur est basé sur l'estimateur Three Spectral Lines (TSL) bien connu dans littérature [88] et adapté pour LoRa dans [5]. Le principe est basé sur l'évaluation de l'amplitude des bins voisins gauche et droite du bin d'intérêt. Connaissant les amplitudes attendues sans CFO et sans AWGN ( $|\tilde{R}[n]| = M$  si  $n = a$ , 0 sinon), le récepteur, par lecture des amplitudes de ces trois bins, peut retrouver la valeur du CFO. L'estimateur se trouve dans le bloc 1a et est présenté en détail en Annexe A. Notons que ce dernier n'estime pas parfaitement  $CFO_{frac}$  i.e.  $\widehat{CFO}_{frac} \neq CFO_{frac}$ , cela n'impacte cependant pas les performances de synchronisation puisque le résidu est inférieur à 0.02 en pratique [88].

Lorsque  $CFO > 0$ , l'estimateur donne  $\widehat{CFO}_{frac} \approx CFO_{frac}$ . En revanche, lorsque  $CFO < 0$ , il estime  $\widehat{CFO}_{frac} \approx 1 - CFO_{frac}$ . Par exemple,  $CFO = -0.1$  donnera  $\widehat{CFO}_{frac} \approx 0.9$ . L'identification du signe de  $CFO$  se fait par lecture sur la DFT en exploitant de façon conjointe l'estimée de  $CFO_{int}$  et est expliquée en Remarque 2 dans l'étape 3. Une fois  $CFO_{frac}$  estimé, la trame reçue est corrigée en  $CFO_{frac}$  dans le bloc 1b par :

$$r_{sync, \widehat{CFO}_{frac}}[k] = r[k] \times e^{-2j\pi k \frac{\widehat{CFO}_{frac}}{M}} \quad (I.2.53)$$

Cet estimateur est insensible à la présence de STO et présente de très bonnes performances en AWGN.

### I.2.6.3.2. Étape 2 – pré-estimation de $STO_{frac}$

Rappelons que plus  $STO_{frac}$  est proche de  $\pm 0.5$ , plus la lecture du bin d'intérêt devient difficile à cause de l'incertitude grandissante entre les bins voisins de  $n = a$  (voir Figure I.2.20). Ainsi, une solution proposée dans [4] est d'effectuer une pré-correction  $STO_{frac}$  afin de réduire le plus possible la présence de ce dernier lors de l'estimation de  $CFO_{int}$  et  $STO_{int}$ . L'estimateur  $STO_{frac}$  est également basé sur TSL [89] et est présenté en Annexe B. Nous notons par  $Estimate\_STO_{frac}(\hat{a}_{up, sync, \widehat{CFO}_{frac}}, STO_{int}, \langle \tilde{P}_{up, sync, \widehat{CFO}_{frac}}[n] \rangle)$  la fonction de cet estimateur avec  $\hat{a}_{up, sync, \widehat{CFO}_{frac}}$ , la position estimée du bin d'intérêt dans la DFT moyennée des symboles upchirp du préambule,  $\langle \tilde{P}_{up, sync, \widehat{CFO}_{frac}}[n] \rangle$ , après correction  $CFO_{frac}$  :

$$\langle \tilde{P}_{up, sync, \widehat{CFO}_{frac}}[n] \rangle = \frac{1}{N_{up}} \sum_{i=0}^{N_{up}-1} \tilde{R}_{i, sync, \widehat{CFO}_{frac}}[n] \quad (I.2.54)$$

avec :

$$\hat{a}_{up, sync, \widehat{CFO}_{frac}} = \arg \max_n \left| \langle \tilde{P}_{up, sync, \widehat{CFO}_{frac}}[n] \rangle \right| \quad (I.2.55)$$

Le moyennage réduit la variance de bruit de la DFT résultante d'un facteur  $N_{up}$ . Cela permet de travailler à un SNR équivalent  $SNR'_{dB} = SNR_{dB} + 10 \log_{10}(N_{up})$  et donc

de sensiblement améliorer les performances d'estimation de  $a_{up}$  dans l'équation (I.2.55). L'estimateur nécessite la connaissance de  $STO_{int}$  pour pouvoir correctement estimer, mais est malheureusement inaccessible à ce stade du front-end. L'idée est de considérer ici  $\widehat{STO}_{int} = \widehat{a}_{up, sync, CFO_{frac}}$ . L'estimée de  $STO_{frac}$ , bien que non exacte, sera suffisamment proche de  $STO_{frac}$  pour pouvoir éliminer efficacement ce dernier. La pré-estimation dans le bloc 2a est donc :

$$\widehat{STO}'_{frac} = Estimate\_STO_{frac} \left( \widehat{a}_{up, sync, CFO_{frac}}, \widehat{a}_{up, sync, CFO_{frac}}, \left\langle \tilde{P}_{up, sync, CFO_{frac}} [n] \right\rangle \right) \quad (I.2.56)$$

En fonction de  $\widehat{a}_{up, sync, CFO_{frac}}$ , l'estimateur pourra retourner les deux résultats suivants pour le cas  $STO_{frac} = +0.5$ . Si nous avons  $\widehat{a}_{up, sync, CFO_{frac}} = a_{up}$ , l'estimateur retournera  $\widehat{STO}'_{frac} = +0.5$ , si  $\widehat{a}_{up, sync, CFO_{frac}} = a_{up} + 1$ , l'estimateur donnera  $\widehat{STO}'_{frac} = -0.5$ , de façon cohérente avec le modèle STO.

### I.2.6.3.3. Étape 3 – pré-correction de $STO_{frac}$ et pré-estimation de $CFO_{int}$ et $STO_{int}$

La pré-correction  $STO_{frac}$  par  $\widehat{STO}'_{frac}$  dans le bloc 3a est réalisée en utilisant la technique du sur-échantillonnage utilisée pour simuler le STO (voir Section I.2.6.1.2). A partir du signal de trame reçue sur-échantillonné, le récepteur élimine les  $\widehat{STO}'_{sps} = \widehat{STO}'_{frac} \times R$  premiers échantillons et sous-échantillonne pour revenir à la fréquence minimale  $F_s = B$ .

Une fois  $CFO_{frac}$  éliminé et  $STO_{frac}$  pré-corrigé, le récepteur réalise une estimation initiale de  $CFO_{int}$  et  $STO_{int}$  dans le bloc 3b, en exploitant à la fois les symboles upchirp et downchirp du préambule :

$$\widehat{CFO}'_{int} = \left\lfloor \frac{(\widehat{a}_{up, sync, CFO_{frac}, \widehat{STO}'_{frac}} + \widehat{a}_{down, sync, CFO_{frac}, \widehat{STO}'_{frac}}) \bmod M}{2} \right\rfloor \quad (I.2.57)$$

$$\widehat{STO}'_{int} = \left( \widehat{CFO}'_{int} - \widehat{a}_{up, sync, CFO_{frac}, \widehat{STO}'_{frac}} \right) \bmod M \quad (I.2.58)$$

avec :

$$\widehat{a}_{up, sync, CFO_{frac}, \widehat{STO}'_{frac}} = \arg \max_n \left| \left\langle \tilde{P}_{up, sync, CFO_{frac}, \widehat{STO}'_{frac}} [n] \right\rangle \right| \quad (I.2.59)$$

$$\widehat{a}_{down, sync, CFO_{frac}, \widehat{STO}'_{frac}} = \arg \max_n \left| \left\langle \tilde{P}_{down, sync, CFO_{frac}, \widehat{STO}'_{frac}} [n] \right\rangle \right| \quad (I.2.60)$$

et :

$$\left\langle \tilde{P}_{up, sync, CFO_{frac}, \widehat{STO}'_{frac}} [n] \right\rangle = \frac{1}{N_{up}} \sum_{i=0}^{N_{up}-1} \tilde{R}_{i, sync, CFO_{frac}, \widehat{STO}'_{frac}} [n] \quad (I.2.61)$$



$$\left\langle \tilde{P}_{down, sync, \widehat{CFO}_{frac}, \widehat{STO}'_{frac}}[n] \right\rangle = \frac{1}{N_{down}} \sum_{i=N_{up}}^{N_{pre}-1} \tilde{R}_{i, sync, \widehat{CFO}_{frac}, \widehat{STO}'_{frac}}[n] \quad (I.2.62)$$

Remarque 1 :

Grâce à la contrainte  $N_{down} = N_{up}$  choisie pour le format de trame, le moyennage est effectué de façon identique entre les symboles upchirp et downchirp, la réduction de variance de bruit est donc identique, d'un facteur  $N_{up}$ . Cela permet de donner les mêmes performances d'estimation de  $a_{up}$  et  $a_{down}$  dans les équations (I.2.59) et (I.2.60) et d'éviter un déséquilibre dans l'estimation de  $CFO_{int}$  et  $STO_{int}$ . Nous pouvons remarquer dans l'équation (I.2.58) qu'une erreur sur l'estimation de  $CFO_{int}$  se répercute immédiatement sur celle de  $STO_{int}$ .

Remarque 2 :

Cet estimateur ne peut estimer  $CFO_{int}$  que si  $|CFO| < M/4$ . Le Tableau I.2.4 montre un exemple de CFO estimés en fonction du signe de CFO et en supposant  $CFO_{frac} = STO = 0$ . Nous remarquons clairement que lorsque  $0 \leq CFO < M/4$ , nous avons  $\widehat{CFO}'_{int} \in \{0, 1, \dots, M/4 - 1\}$  et si  $-(M/4 - 1) \leq CFO < 0$ , nous avons  $\widehat{CFO}'_{int} \in \{M/4 + 1, M/4 + 2, \dots, M/2 - 1\}$ . Le cas limite est  $CFO = \pm M/4$ , où nous avons identiquement  $\widehat{CFO}'_{int} = M/4$ . Ainsi, le récepteur peut correctement corriger le CFO uniquement si  $|CFO| < M/4$ . L'estimée finale du CFO est alors :

$$\widehat{CFO}'_{int, corr} = \begin{cases} \widehat{CFO}'_{int} & \text{si } \widehat{CFO}'_{int} < M/4 \quad (CFO \geq 0) \\ (\widehat{CFO}'_{int} - M/2) \bmod M & \text{si } \widehat{CFO}'_{int} > M/4 \quad (CFO < 0) \end{cases} \quad (I.2.63)$$

Cela peut-être une limite, mais en pratique, il est peu probable d'avoir  $|CFO| > M/4$ , même avec des oscillateurs de mauvaise qualité [77]. Pour la suite du mémoire, nous considéreront  $CFO \geq 0$  et donc  $\widehat{CFO}'_{int, corr} = \widehat{CFO}'_{int}$ , sans perte de généralité.

$CFO_{int}$	$\hat{a}_{up, sync, \widehat{CFO}_{frac}, \widehat{STO}'_{frac}}$	$\hat{a}_{down, sync, \widehat{CFO}_{frac}, \widehat{STO}'_{frac}}$	$\widehat{CFO}'_{int}$
1	1	1	1
-1	$M - 1$	$M - 1$	$M/2 - 1$
$M/4 - 1$	$M/4 - 1$	$M/4 - 1$	$M/4 - 1$
$-(M/4 - 1)$	$M - M/4 + 1$	$M - M/4 + 1$	$M/4 + 1$
$M/4$	$M/4$	$M/4$	$M/4$
$-M/4$	$M - M/4$	$M - M/4$	$M/4$

TABLE I.2.4. – Exemple de  $CFO_{int}$  estimés en fonction du signe de CFO

Remarque 3 :

Le STO entraîne de l'ISI sur les derniers symboles upchirp et downchirp du préambule. Comme cette interférence se produit avec le symbole précédent (voir Figure I.2.19), nous auront respectivement de l'interférence entre le dernier symbole upchirp et le premier symbole downchirp (préambule), et entre le dernier symbole downchirp (préambule) et le

premier symbole de payload. Ainsi, les moyennages dans les équations (I.2.61) et (I.2.62) engendreront un symbole déformé. En revanche, cette déformation est assez limitée et n'impacte que très peu les performances de démodulation.

Remarque 4 :

En présence de bruit AWGN et du fait du résidu de pré-correction  $STO_{frac}$ , lorsqu'une erreur de lecture du bin d'intérêt est présente, cela impacte la plupart du temps les bins voisins directs. Le cas  $\hat{a}_{up, sync, \widehat{CFO}_{frac}, \widehat{STO}'_{frac}} = a_{up} + 1$  et  $\hat{a}_{down, sync, \widehat{CFO}_{frac}, \widehat{STO}'_{frac}} = a_{down} - 2$ , malgré les erreurs, peut conduire tout de même à une démodulation correcte. En effet, d'après les équations (I.2.57) et (I.2.58), nous obtenons  $\widehat{CFO}'_{int} = CFO_{int} - 1$  et  $\widehat{STO}'_{int} = STO_{int} - 1$ . La correction du CFO viendra décaler d'une position vers la droite les bins DFT tandis que la correction du STO viendra décaler d'une position vers la gauche, donnant ainsi une démodulation du symbole corrigé correcte (l'ISI due à  $\widehat{STO}'_{int} = STO_{int} - 1$  est négligeable).

#### I.2.6.3.4. Étape 4 – estimation finale de $STO_{frac}$

Avec l'estimation initiale de  $CFO_{int}$  et  $STO_{int}$ , le récepteur affine l'estimation de  $STO_{frac}$  dans le bloc 4a grâce à l'information  $\widehat{STO}'_{int}$  obtenue précédemment :

$$\widehat{STO}_{frac} = Estimate\_STO_{frac} \left( \hat{a}_{up, sync, \widehat{CFO}_{frac}, \widehat{STO}'_{int}}, \left\langle \tilde{P}_{up, sync, \widehat{CFO}_{frac}}[n] \right\rangle \right) \quad (I.2.64)$$

Nous notons  $STO'_{frac, r}$  et  $STO^r_{frac}$ , les résidus des estimations initiale et finale de  $STO_{frac}$  et sont définis par :

$$STO'_{frac, r} = \left| STO_{frac} - \widehat{STO}'_{frac} \right|, \quad STO^r_{frac, r} = \left| STO_{frac} - \widehat{STO}_{frac} \right| \quad (I.2.65)$$

avec  $STO_{frac, r} < STO'_{frac, r}$  si  $\widehat{STO}'_{int} = STO_{int}$ .

#### I.2.6.3.5. Étape 5 – correction de $STO_{frac}$ et estimation finale de $CFO_{int}$ et $STO_{int}$

Le récepteur corrige  $\widehat{STO}_{frac}$  de la même manière que dans le bloc 3a et met à jour l'estimation de  $CFO_{int}$  et  $STO_{int}$ , puisque l'estimation  $\widehat{STO}_{frac}$  est plus fiable que  $\widehat{STO}'_{frac}$ , pour obtenir :

$$\widehat{CFO}_{int} = \left\lfloor \frac{(\hat{a}_{up, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}} + \hat{a}_{down, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}}) \bmod M}{2} \right\rfloor \quad (I.2.66)$$

$$\widehat{STO}_{int} = \left( \widehat{CFO}_{int} - \hat{a}_{up, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}} \right) \bmod M \quad (I.2.67)$$

avec :

$$\hat{a}_{up, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}} = \arg \max_n \left| \left\langle \tilde{P}_{up, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}}[n] \right\rangle \right| \quad (I.2.68)$$

## I.2. LoRa

$$\widehat{a}_{down, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}} = \arg \max_n \left| \left\langle \tilde{P}_{down, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}}[n] \right\rangle \right| \quad (\text{I.2.69})$$

et :

$$\left\langle \tilde{P}_{up, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}}[n] \right\rangle = \frac{1}{N_{up}} \sum_{i=0}^{N_{up}-1} \tilde{R}_{i, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}}[n] \quad (\text{I.2.70})$$

$$\left\langle \tilde{P}_{down, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}}[n] \right\rangle = \frac{1}{N_{down}} \sum_{i=N_{up}}^{N_{pre}-1} \tilde{R}_{i, sync, \widehat{CFO}_{frac}, \widehat{STO}_{frac}}[n] \quad (\text{I.2.71})$$

### I.2.6.3.6. Étape 6 – synchronisation de la trame

Le récepteur possède maintenant toutes les estimées nécessaires  $\widehat{CFO}_{frac}$ ,  $\widehat{CFO}_{int}$ ,  $\widehat{STO}_{frac}$ ,  $\widehat{STO}_{int}$  et  $\widehat{SFO}$ . Il peut dès à présent corriger la trame, en corrigeant d'abord le STO avec  $\widehat{STO} = \widehat{STO}_{int} + \widehat{STO}_{frac}$  (par sur-échantillonnage), puis le CFO avec  $\widehat{CFO} = \widehat{CFO}_{int} + \widehat{CFO}_{frac}$  et enfin le SFO avec  $\widehat{SFO} = \frac{B^2}{M \times F_c} \times \widehat{CFO}$ , d'après l'équation (I.2.38), par :

$$r_{i, sync}[k] = r_{i, sync, \widehat{CFO}, \widehat{STO}, \widehat{SFO}}[k] = r_{i, sync, \widehat{CFO}, \widehat{STO}}[k] \times e^{-2j\pi k i \left[ \left( \frac{B}{B + \widehat{SFO}} \right)^2 - \frac{B}{B + \widehat{SFO}} \right]} \quad (\text{I.2.72})$$

Nous notons  $r_{sync}[k]$ , la trame reçue synchronisée (voir Figure I.2.13). Remarquons que le SFO n'est pas corrigé tout au long de l'exécution du front-end de synchronisation. En effet, la déformation croissante dans le temps de la DFT est quasiment négligeable sur une durée de quelques symboles ( $CFO \leq M/4$ ), comme celle du préambule avec  $N_{pre} = 16$ , généralement. Cela permet de réduire la complexité calculatoire du front-end.

Pour conclure sur ce front-end, le Tableau I.2.5 résume les interactions entre les différents paramètres de synchronisation et leur estimation. La lettre I indique la perturbation de l'estimation du paramètre en colonne  $c$  lorsque le paramètre en ligne  $l$  est présent. La lettre D indique la dépendance du paramètre en ligne  $l$  pour l'estimation du paramètre en colonne  $c$  et les lettres ID indiquent la non perturbation du paramètre en ligne  $l$  sur l'estimation du paramètre en colonne  $c$ .

	$\widehat{CFO}_{frac}$	$\widehat{CFO}_{int}$	$\widehat{STO}_{frac}$	$\widehat{STO}_{int}$
$CFO_{frac}$	-	I	I	I
$CFO_{int}$	ID	-	ID	D
$STO_{frac}$	ID	I	-	I
$STO_{int}$	ID	ID	D	-

TABLE I.2.5. – Interactions entre les paramètres de synchronisation  $CFO_{frac}$ ,  $CFO_{int}$ ,  $STO_{frac}$ ,  $STO_{int}$  et leur estimation

### I.2.6.4. Détection du préambule

Dans cette partie, nous présentons les deux détecteurs de préambule proposés dans la littérature [76, 79], évaluons leurs performances comparées et discutons de leurs limites. Le premier est simple, intuitif et exploite les propriétés du préambule, tandis que le second est plus générique et est basé sur un détecteur d'énergie.

Le front-end de synchronisation peut fonctionner, à condition que le récepteur ait correctement détecté le préambule. En effet, ce dernier ne sachant pas quand l'émetteur va lui envoyer une trame doit être capable de détecter son arrivée à tout moment. Ainsi, le récepteur reçoit en temps réel des blocs de  $M$  échantillons et doit à partir de ces derniers détecter le préambule. Nous noterons  $r_i[k]$  le  $i^{\text{ème}}$  bloc formé et  $idx_{start}$ , l'indice  $i = idx_{start}$  où la trame débute (premier symbole upchirp du préambule).

Notons aussi par  $H_0$  et  $H_1$ , les hypothèses que le  $i^{\text{ème}}$  bloc  $r_i[k]$  soit purement AWGN (période de silence) ou contienne un symbole LoRa de la trame transmise, respectivement :

$$H_0 = \begin{cases} 1 & \text{si } i \in I_{H_0} \\ 0 & \text{sinon} \end{cases}, \quad H_1 = \begin{cases} 1 & \text{si } i \in I_{H_1} \\ 0 & \text{sinon} \end{cases} \quad (\text{I.2.73})$$

avec :

$$I_{H_0} = \{\dots, idx_{start} - 2, idx_{start} - 1, idx_{start} + N_{frame}, idx_{start} + N_{frame} + 1, \dots\} \quad (\text{I.2.74})$$

$$I_{H_1, preamble} = \{idx_{start}, idx_{start} + 1, \dots, idx_{start} + N_{pre} - 1\} \quad (\text{I.2.75})$$

$$I_{H_1, payload} = \{idx_{start} + N_{pre}, idx_{start} + N_{pre} + 1, \dots, idx_{start} + N_{frame} - 1\} \quad (\text{I.2.76})$$

$$I_{H_1} = I_{H_1, preamble} \cup I_{H_1, payload} \quad (\text{I.2.77})$$

l'ensemble des indices de blocs purement AWGN, de symboles préambule, payload et trame, respectivement. Le détecteur peut être mis en défaut de différentes manières présentées dans le Tableau I.2.6. Nous relevons les cas de mauvaise détection (détecter ailleurs dans la trame), de fausse alarme (détecter dans une période de silence), de non détection et enfin de non fonctionnement (conduit à une démodulation erronée et inclut tous les autres cas en supposant l'hypothèse  $H_1$ ). Nous y associons les probabilités  $P_{wd}$ ,  $P_{fa}$ ,  $P_{nd}$ ,  $P_{md}$ , respectivement. Notons aussi  $P_d$ , la probabilité de détection sans erreur, sous l'hypothèse  $H_1$ .

Type d'erreur	Erreur
Mauvaise détection (préambule)	$\widehat{idx}_{start} \neq idx_{start}, \widehat{idx}_{start} \in I_{H_1, preamble}, H_1$
Mauvaise détection (payload)	$\widehat{idx}_{start} \neq idx_{start}, \widehat{idx}_{start} \in I_{H_1, payload}, H_1$
Fausse alarme	$\widehat{idx}_{start} \neq \emptyset, H_0$
Non détection	$\widehat{idx}_{start} = \emptyset, H_1$
Non fonctionnement	$\widehat{idx}_{start} \neq idx_{start}$ ou $\widehat{idx}_{start} = \emptyset, H_1$

TABLE I.2.6. – Cas de mauvaise détection du préambule

### I.2.6.4.1. Détection du préambule par détection de symboles consécutifs identiques

Le premier détecteur proposé dans [76] exploite de façon pragmatique la propriété de symboles consécutifs identiques dans le préambule. La probabilité de trouver  $S$  symboles LoRa consécutifs identiques vaut :

$$p_a(S) = (p_a)^S \quad (\text{I.2.78})$$

avec :

$$p_a = \mathbb{P}[a = b] = \frac{1}{M} \quad (\text{I.2.79})$$

la probabilité d'avoir le symbole  $a = b$  uniforme sur  $\{0, 1, \dots, M - 1\}$ . Plus  $S$  augmente, plus la probabilité diminue. Ainsi, rencontrer  $S = N_{up}$  symboles identiques ( $a = 0$ ) dans le payload est très faible. Elle vaut par exemple  $p_a(S = N_{up}) \approx 1.38 \times 10^{-17}$  pour  $N_{up} = 8$  et  $SF = 7$ . Le récepteur peut donc aisément séparer le préambule du payload et le détecter sous l'hypothèse  $H_1$  par :

$$d_{preamble}(p) = \begin{cases} 1 & \text{si } \frac{\sum_{j=p \times S}^{(p+1) \times S-1} c_j}{S} = 1 \\ 0 & \text{sinon} \end{cases} \quad (\text{I.2.80})$$

avec :

$$c_i = \begin{cases} 1 & \text{si } \hat{a}_i \in \{(a_{ref} - h) \bmod M, \dots, (a_{ref} + h) \bmod M\} \\ 0 & \text{sinon} \end{cases} \quad (\text{I.2.81})$$

$$a_{ref} = \arg \max_n \left| \tilde{R}_{p \times S}[n] \right| \quad (\text{I.2.82})$$

$$\hat{a}_i = \arg \max_n \left| \tilde{R}_i[n] \right| \quad (\text{I.2.83})$$

et  $i = p \times S + j$  avec  $p \in \{0, 1, \dots\}$  et  $j \in \{1, 2, \dots, S - 1\}$ ,  $h \in \{0, 1, \dots, M/2 - 1\}$ . Si  $d_{preamble}(p) = 1$  dans l'équation (I.2.80), le récepteur conclut alors  $\widehat{id}x_{start} = p \times S$ .

Idéalement, il serait souhaitable de pouvoir parfaitement détecter la succession de tous les symboles upchirp du préambule i.e.  $S = N_{up}$ . Cependant, cette contrainte est difficile à satisfaire en pratique, la probabilité d'avoir un symbole ne respectant pas l'équation (I.2.81) pour  $S$  fixé augmente lorsque le SNR se dégrade. De plus, il serait souhaitable d'avoir  $\hat{a}_i = a_{ref}$ , ce qui est également très restrictif, puisque les symboles évalués sont désynchronisés et la probabilité d'avoir le pic max correspondant à un voisin du bin d'intérêt est élevée. Ainsi, nous autorisons la recherche à  $\pm h$  autour du bin d'intérêt dans l'équation (I.2.81). Ces assouplissements permettent d'améliorer grandement la capacité de détection, mais au prix cependant d'une augmentation de la probabilité de fausse alarme. Dans [76], les auteurs choisissent  $S = 3$  et  $h = 1$ , donnant un assez bon compromis.

### I.2.6.4.2. Détection du préambule par détection d'énergie

Les auteurs dans [79] ont proposé un détecteur de préambule basé sur la détection d'énergie. Le détecteur constitue des blocs de  $N_{up}$  symboles reçus, moyenne les DFT et détecte le préambule par seuillage :

$$\left| \left\langle \tilde{P}_p[n] \right\rangle \right| \underset{H_0}{\overset{H_1}{\geq}} \lambda_{preamble} \quad (\text{I.2.84})$$

avec :

$$\left\langle \tilde{P}_p[n] \right\rangle = \frac{1}{N_{up}} \sum_{j=p}^{p+N_{up}-1} \tilde{R}_j[n] \quad (\text{I.2.85})$$

et  $p \in \{0, 1, \dots\}$ . Le détecteur valide la détection si au moins un bin dépasse le seuil fixé. Nous avons alors  $\widehat{id}x_{start} = p$ . En fonction de l'hypothèse dans laquelle nous nous trouvons et du bin considéré, la densité de probabilité Probability Density Function (PDF) associée sera différente.

Les bins purement AWGN (hypothèse  $H_0$  et  $\forall n$  ou hypothèse  $H_1$  et  $n \neq a_{up}$ ) suivent une loi de Rayleigh, tandis que le bin contenant l'énergie du symbole (hypothèse  $H_1$  et  $n = a_{up}$ ) suit une loi de Rice. Elles sont reportées dans les équations (I.2.86) et (I.2.87).

$$f_1(x) = f_{Rayleigh}(x, \beta_1), \quad x \geq 0 \quad (\text{I.2.86})$$

$$f_2(x) = f_{Rice}(x, \beta_1, M) \quad (\text{I.2.87})$$

avec :

$$\beta_1 = \sqrt{\frac{M\sigma^2}{2N_{up}}} \quad (\text{I.2.88})$$

Les lois sont définies par :

$$f_{Rayleigh}(x, \beta) = \frac{x}{\beta^2} e^{-\frac{x^2}{2\beta^2}} \quad (\text{I.2.89})$$

$$f_{Rice}(x, \beta, \mu) = \frac{x}{\beta^2} e^{-\frac{(x^2+\mu^2)}{2\beta^2}} I_0\left(\frac{x\mu}{\beta^2}\right) \quad (\text{I.2.90})$$

avec  $\beta$ , le paramètre d'échelle,  $\mu$  et  $I_0(\cdot)$ , le paramètre de décentrage et la fonction de Bessel modifiée d'ordre zéro respectivement pour la loi de Rice.

Plus le SNR diminue, plus les densités s'élargissent. Ainsi, pour un seuil fixé, nous obtiendrons des probabilités de fausse alarme et de non détection croissantes. Le récepteur fixe une contrainte de probabilité de fausse alarme  $P_{fa}$  et calcule le seuil par :

$$\lambda_{preamble} = F_1^{-1}(1 - P_{fa}, \beta_1) \quad (\text{I.2.91})$$

avec :

$$F_1(x, \beta) = 1 - e^{-\frac{x^2}{2\beta^2}} \quad (\text{I.2.92})$$

$$F_1^{-1}(x, \beta) = \beta\sqrt{-2\ln(1-x)} \quad (\text{I.2.93})$$

la fonction de répartition Cumulative Density Function (CDF) et son inverse, de la loi de probabilité  $f_1(x)$ , respectivement. D'après les équations (I.2.91) et (I.2.88), le seuil  $\lambda_{\text{preamble}}$  est obtenu en exploitant la connaissance du niveau de bruit du récepteur ( $\sigma^2$ ). Dans [79], ce dernier est supposé parfaitement connu, ce qui n'est pas le cas dans la réalité et doit donc être estimé. Cependant, pendant les périodes de silence, le récepteur peut obtenir une très bonne estimation i.e.  $\hat{\sigma}^2 \approx \sigma^2$  ne nécessitant pas d'être actualisée régulièrement. En effet, la puissance du bruit dépend de la bande (fixe) et de la température ambiante qui varie peu au cours d'une journée. Pour ne pas alourdir cette partie, l'expression théorique de la probabilité de détection  $P_d$  ne sera pas donnée mais est calculée dans [79].

### I.2.6.4.3. Performances de détection du préambule

Dans cette partie, nous évaluons en simulation les performances des deux détecteurs de préambule. La procédure de simulation est la suivante. Nous générons soit une trame LoRa de paramètres  $N_{\text{up}} = N_{\text{down}} = 8$ ,  $N_{\text{payload}} = 10$  et  $SF = 7$ , soit une trame ne comportant que du bruit AWGN, de façon équiprobable, ceci afin de simuler les hypothèses  $H_1$  et  $H_0$ , respectivement. Nous exécutons les deux détecteurs en recherchant le début du préambule dans toute la trame reçue. Nous utilisons les mêmes paramètres  $S = 3$  et  $h = 1$  que les auteurs ont choisi pour le détecteur [76], et une contrainte de fausse alarme  $P_{fa} = 10^{-2}$ , ainsi qu'une connaissance parfaite du niveau de bruit ( $\hat{\sigma}^2 = \sigma^2$ ) pour le détecteur [79].

La Figure I.2.26 présente les performances de détection évaluées, comme la probabilité de non fonctionnement du détecteur ( $P_{md}$ ), en fonction du SNR pour  $SNR_{dB} \in \{-18, -17, \dots, 10\}$ . Nous considérons les cas de synchronisation parfaite ( $CFO = STO = SFO = 0$ ) et de non synchronisation, avec le CFO, le STO et le SFO aléatoires pour cette dernière, avec  $CFO \in [0; M/4-1]$ ,  $STO \in \{0, 1/R, \dots, M-1-1/R\}$ ,  $R = 10$ ,  $F_c = 868.1$  MHz et  $B = 125$  kHz.

Nous remarquons que dans le cas parfaitement synchronisé, le détecteur dans [79] donne de bien meilleures performances que celui dans [76], avec  $P_{md} < 0.08$  pour  $SNR_{dB} \geq -18$  et est quasiment constant, là où [76] ne donne des performances satisfaisantes qu'à partir de  $SNR_{dB} = -7$ . En revanche, la désynchronisation impacte beaucoup plus [79], avec  $P_{md}$  très élevé pour  $SNR_{dB} \leq 0$  ( $> 0.42$ ) et valant encore  $P_{md} \approx 0.03$ , pour  $SNR_{dB} = 10$ . Cela vient du fait que les désynchronisations,  $CFO_{frac}$  et  $STO_{frac}$  surtout, déforment énormément la statistique utilisée dans [79] (synchronisation parfaite assumée) et rend donc le détecteur incohérent. Le détecteur dans [76] est beaucoup plus consistant, avec une perte inférieure à 2.5 dB pour  $0.1 \leq P_{md} \leq 0.9$ . Cependant,  $P_{md}$  ne converge pas vers 0 pour ce dernier, avec un niveau minimal  $P_{md} \approx 0.02$ .

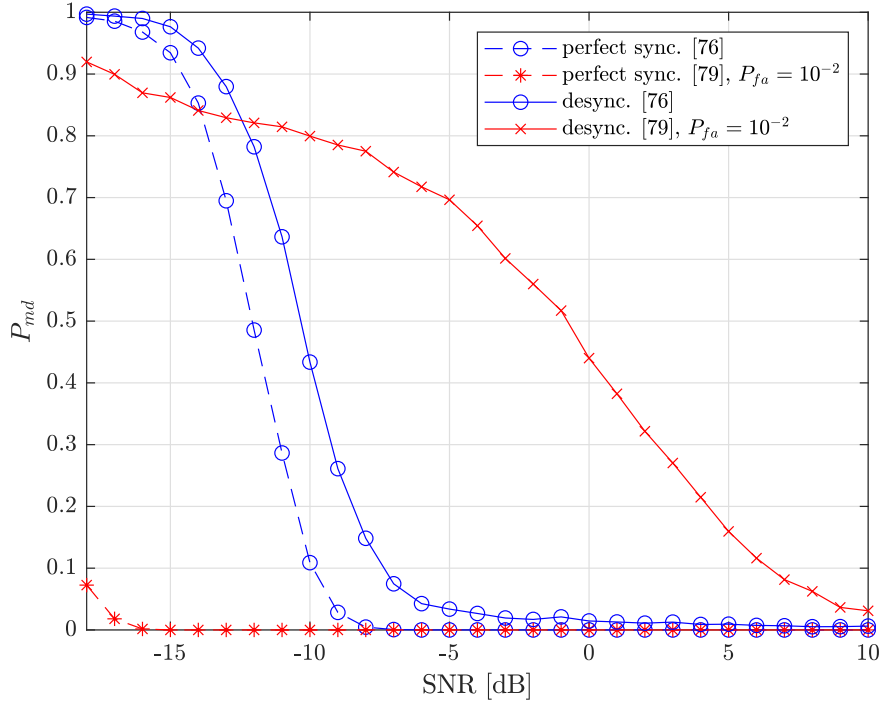


FIGURE I.2.26. – Performances des deux détecteurs de préambule LoRa de la littérature [76] et [79],  $SF = 7$

#### I.2.6.4.4. Avantages et inconvénients des détecteurs

Les Tableaux I.2.7 et I.2.8 résument les point forts et points faibles de ces deux détecteurs. Le premier a l'avantage d'avoir une complexité calculatoire assez faible et est facilement implantable sur de vrais équipements LoRa. En revanche, il offre des performances de détection moyennes et a surtout deux gros points faibles :

1. Il ne pourra jamais garantir une probabilité de fausse alarme arbitrairement nulle sous l'hypothèse  $H_0$ , contrairement à [79].
2. Une forte incertitude d'estimation  $\widehat{idx}_{start}$  autour de  $idx_{start}$  est présente lors de la transition de l'hypothèse  $H_0$  vers  $H_1$ .

Pour le premier point faible, la probabilité de fausse alarme sous l'hypothèse  $H_0$  (avoir  $S$  symboles consécutifs purement AWGN espacés entre eux de  $\pm h$  bins) vaut :

$$P_{fa}(S, h, M) = (p_{e,idx_{start}}(h, M))^{S-1} \quad (\text{I.2.94})$$

avec :

$$p_{e,idx_{start}}(h, M) = \frac{2h+1}{M} \quad (\text{I.2.95})$$

du fait d'avoir  $2h+1$  symboles candidats dans l'ensemble  $\{0, 1, \dots, M-1\}$ . Cette probabilité n'est pas si faible pour  $SF = 7$ , nous obtenons par exemple  $P_{fa}(S, h, M) \approx 5.5 \times 10^{-4}$  pour  $S = 3$  et  $h = 1$ .

Pour le second point faible, pour  $S = 3$ , supposons que les deux premiers symboles du préambule soient correctement démodulés i.e.  $\widehat{a}_{idx_{start}} = \widehat{a}_{idx_{start}+1} = (\lfloor CFO \rfloor - \lfloor STO \rfloor)$



## I.2. LoRa

mod  $M$  (voir équation (I.2.48)). Cela est normalement le cas en pratique à SNR modéré,  $CFO_{frac} \leq 0.3$  ou  $CFO_{frac} \geq 0.7$  et  $|STO_{frac}| \leq 0.3$ . Si le symbole précédent le préambule, d'indice  $idx_{start} - 1$ , vaut  $\hat{a}_{idx_{start}-1} = \hat{a}_{idx_{start}}$ , alors le détecteur conclura  $\hat{idx}_{start} = idx_{start} - 1$  et un décalage d'un symbole sera présent, conduisant à un Symbol Error Rate (SER) de presque 100% (supposant une synchronisation parfaite). Ce cas de figure a une probabilité d'apparition assez élevée. D'après l'équation (I.2.95), pour  $h = 1$  et  $SF = 7$ , il vaut  $p_{e,idx_{start}}(1, 128) \approx 0.023$ .

Pour toutes ces raisons, ce détecteur n'est pas réellement exploitable en pratique.

Le second détecteur, quant à lui, donne de bien meilleures performances de détection, mais à condition d'être parfaitement synchronisé, ce qui est irréaliste. Prendre en compte la désynchronisation dégrade immédiatement les performances et donne un comportement incohérent (voir Figure I.2.26). De plus, le récepteur doit avoir une bonne estimation du niveau de bruit pour ne pas entraîner de biais, ajoutant plus de complexité calculatoire.

Ainsi, le second détecteur n'est pas exploitable en usage réel dans l'état, mais avec des améliorations, ce dernier peut se révéler convaincant. Il a servi de base au détecteur de trame développé pour le schéma d'auto-brouillage présenté en Section III.4.3.1.

Avantages	Inconvénients
Faible complexité calculatoire.	Performances de détection moyennes.
Implémentation facile sur équipements existants.	Probabilité de fausse alarme $P_{fa}$ pour $SF = 7$ pas si faible sous l'hypothèse $H_0$ .
	Incertitude d'estimation $\hat{idx}_{start}$ autour de $idx_{start}$ (transition hypothèse $H_0$ vers $H_1$ ).

TABLE I.2.7. – Avantages et inconvénients du détecteur de préambule LoRa par détection de symboles consécutifs identiques [76]

Avantages	Inconvénients
Très bonnes performances si synchronisation parfaite.	Connaissance du niveau de bruit nécessaire.
	Très grosse sensibilité à la désynchronisation.

TABLE I.2.8. – Avantages et inconvénients du détecteur de préambule LoRa par détection d'énergie [79]

## I.2.7. Performances

Dans cette section, nous évaluons les performances de LoRa sous différents aspects : les performances dans un canal AWGN en évaluant l'impact de  $SF$  pour les récepteurs non-cohérent et cohérent (Section I.2.7.1), les performances du codage de canal de Hamming (Section I.2.7.2), et enfin en Section I.2.7.3 les performances du front-end de synchronisation présenté en Section I.2.6.3. Nous utilisons les paramètres de simulation suivants :

- $N_{up} = N_{down} = 8$ , pour l'estimation de  $CFO_{int}$  et  $STO_{int}$  dans le front-end de synchronisation.
- $B = 125$  kHz et  $F_c = 868.1$  MHz, pour l'estimation du SFO dans le front-end de synchronisation.
- $R = 10$ , pour la simulation et la correction de  $STO_{frac}$  dans le front-end de synchronisation.
- $CFO \in [0; M/4-1]$  (voir Remarque 2 dans la Section I.2.6.3.3) et  $STO \in \{0, 1/R, 2/R, \dots, M-1-1/R\}$ .

### I.2.7.1. Performances dans un canal AWGN – synchronisation parfaite

Les performances LoRa dans un canal AWGN (synchronisation parfaite i.e.  $CFO = STO = CFO = 0$ ) pour les démodulateurs non-cohérent et cohérent ont été calculées analytiquement dans notre première contribution LoRa [90]. Notons  $P_d$ , la probabilité de détection symbole :

$$P_d = 1 - \mathbb{P}[\hat{a} \neq a] \quad (\text{I.2.96})$$

Les expressions ont été obtenues en évaluant la probabilité que les bins purement AWGN ( $n \neq a$ ) soient inférieurs au bin d'intérêt  $n = a$ , pour les deux récepteurs :

$$\begin{aligned} P_{d,NCOH}(\tilde{W}) &= \mathbb{P}[|R[n \neq a]| < |R[a]|] = \prod_{\substack{0 \leq n \leq M-1 \\ n \neq a}} \mathbb{P}\left[|\tilde{W}[n]| < |M + \tilde{W}[a]|\right] \\ &= F_{Rayleigh}\left(|M + \tilde{W}[a]|, \sqrt{\frac{M\sigma^2}{2}}\right)^{M-1} \quad (\text{I.2.97}) \end{aligned}$$

$$\begin{aligned} P_{d,COH}(\tilde{W}) &= \mathbb{P}[\Re\{R[n \neq a]\} < \Re\{R[a]\}] = \prod_{\substack{0 \leq n \leq M-1 \\ n \neq a}} \mathbb{P}\left[\Re\{\tilde{W}[n]\} < \Re\{M + \tilde{W}[a]\}\right] \\ &= F_{Normal}\left(\Re\{M + \tilde{W}[a]\}, 0, \sqrt{\frac{M\sigma^2}{2}}\right)^{M-1} \quad (\text{I.2.98}) \end{aligned}$$

avec  $\tilde{W}[n]$ , la composante de bruit AWGN dechirpée DFT,  $F_{Rayleigh}(x, \eta)$  et  $F_{Normal}(x, \mu, \eta)$ , les fonctions de répartition des lois de Rayleigh (paramètre  $\beta$ ) et normale (paramètres de moyenne  $\mu$  et d'écart type  $\eta$ ), respectivement.

Dans les équations (I.2.97) et (I.2.98), une CDF est évaluée en un point qui est aléatoire. Évaluer une telle probabilité n'est pas trivial. Il a été décidé dans l'article d'utiliser

la procédure d'approximation numérique Gauss-Hermite pour obtenir une estimation des performances moyennes à partir de la réalisation  $\tilde{W}[n]$ , en échantillonnant la loi de probabilité normale ou Rayleigh avec un nombre minimal de points [91]. L'expression obtenue par cette procédure vaut :

$$P_{e,NCOH} = \mathbb{E}[1 - P_{d,NCOH}(\tilde{W})] \quad (I.2.99)$$

$$= \frac{1}{\pi\sigma_w^2} \int_{\mathbb{C}} (1 - P_{d,NCOH}(w)) e^{-\frac{|w|^2}{\sigma_w^2}} dw = \frac{1}{\pi} \int_{\mathbb{C}} (1 - P_{d,NCOH}(\sigma_w w)) e^{-|w|^2} dw \quad (I.2.100)$$

$$\approx \frac{1}{\pi} \sum_{n,m=1}^N \left(1 - P_{d,NCOH}(\sigma\sqrt{M}(w_n + jw_m))\right) p_n p_m \quad (I.2.101)$$

avec  $\mathbb{E}[\cdot]$ , l'opérateur espérance mathématique,  $\sigma_w = \sqrt{M}\sigma^2$ ,  $N$ , le nombre de points Gauss-Hermite ( $N = 20$  choisi ici),  $w_i$  et  $p_i$  avec  $i \in \{0, 1, \dots, N - 1\}$ , les nœuds (abscisses) et poids des  $N$  points formés avec la règle Gauss-Hermite [91].

La Figure I.2.27 présente la probabilité  $P_e = 1 - P_d$  évaluée pour les deux récepteurs et pour toutes les valeurs de SF. Nous remarquons les deux résultats importants suivants :

- Augmenter SF d'une unité donne un gain d'environ 2.5 dB. Ainsi, la transmission sera de plus en plus robuste à mesure que SF augmente, mais au prix d'une perte de débit (voir Figure I.2.6).
- Le récepteur cohérent a un gain de l'ordre de 0.8 dB sur le récepteur non-cohérent, quel que soit SF. Cela est intéressant, mais nécessite une resynchronisation de la phase au niveau du récepteur où cette dernière doit être estimée.

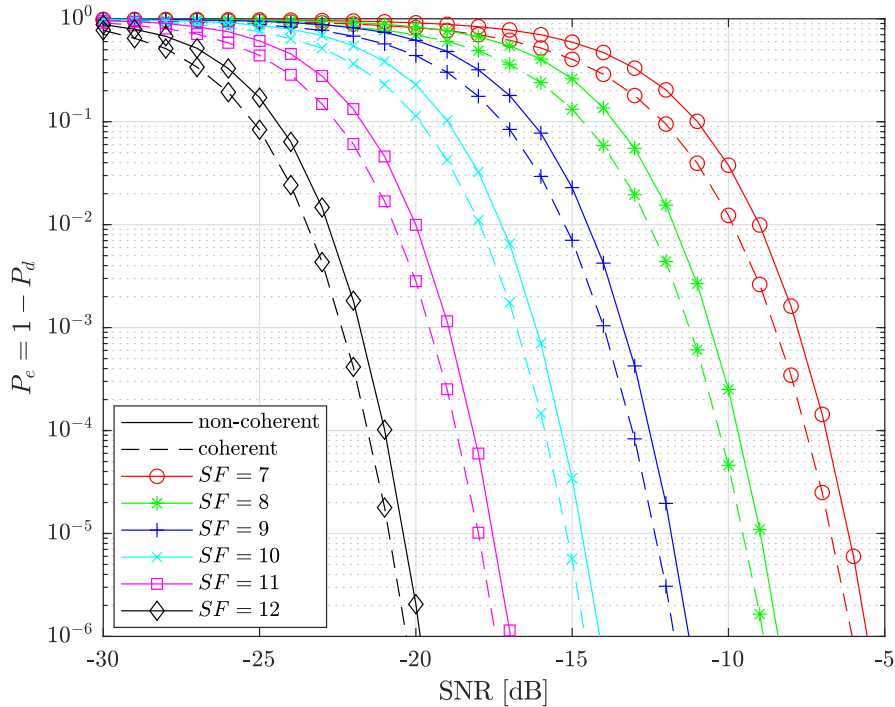


FIGURE I.2.27. – Performances SER LoRa des deux récepteurs non-cohérent et cohérent en fonction de SF

Ainsi, tous les traitements du récepteur effectués pour une valeur de SF plus élevée que 7 donneront un gain de performances de l'ordre de :

$$G(SF) = 2.5 \times (SF - 7) \quad (I.2.102)$$

Dans le mémoire, la majorité des simulations sont effectuées pour  $SF = 7$ , ayant la plus faible complexité calculatoire. Les performances pour des valeurs plus élevées de SF peuvent donc être obtenues avec la Règle (I.2.102).

### I.2.7.2. Performances du codage de canal

La Figure I.2.28 présente les performances du codage de canal en termes de taux d'erreur binaire (Bit Error Rate (BER)) pour les trois scénarios suivants : 1) codage de canal complet (codage de Hamming, codage de Gray et entrelacement actifs), type de ligne '-.-', 2) codage de canal sans entrelacement, type de ligne '- -' et 3) codage de canal désactivé, type de ligne '-'. Ce dernier permet d'évaluer le gain de performances par rapport à une transmission non codée. Nous utilisons le paramètre Hamming  $CR = 3$ . Nous considérons également une désynchronisation CFO afin de mettre en évidence l'intérêt du codage de canal en présence de désynchronisation. Nous balayons l'ensemble des désynchronisations CFO possibles, de la plus favorable à la plus défavorable i.e. de  $CFO = 0$  à  $CFO = 0.5$ , voir Section I.2.6.2. Nous prenons en compte aussi les valeurs intermédiaires  $CFO \in \{0.2, 0.4\}$ .

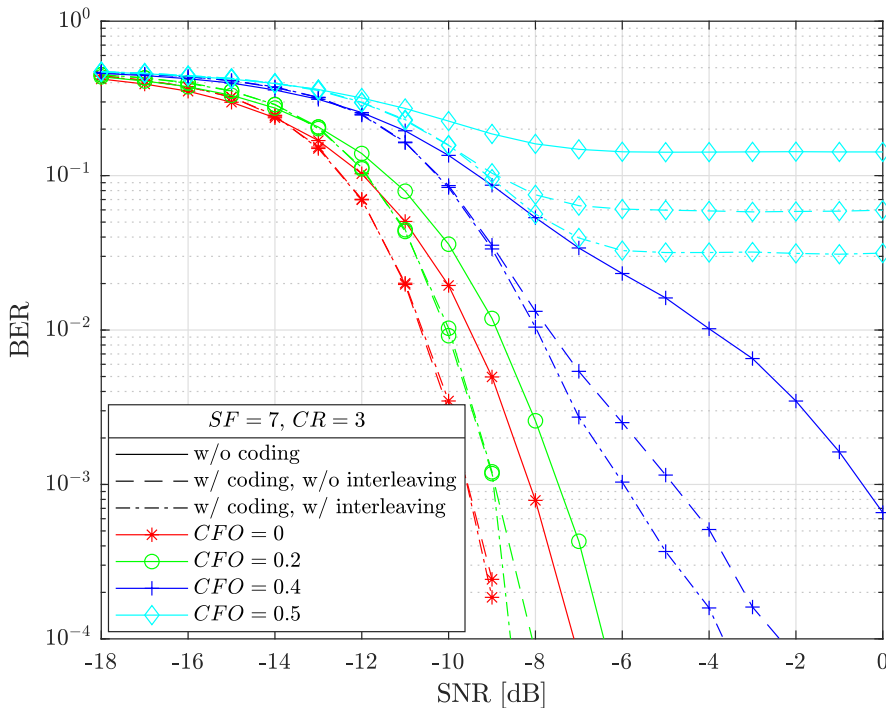


FIGURE I.2.28. – Performances du front-end de synchronisation de la littérature et impact du nombre de symboles pilotes,  $SF = 7$

D'après la Figure I.2.28, il est possible de remarquer que le gain du codage de canal est peu significatif pour des niveaux de désynchronisation CFO faibles ( $CFO \in \{0, 0.2\}$ ), avec un gain inférieur à 1 dB. Malgré la capacité du codage de canal à corriger les erreurs symbole à  $\pm 1$  bin, le cas  $CFO = 0.5$  reste très défavorable, avec un palier BER atteint

un peu plus faible que les autres scénarios ( $BER \approx 3.1 \times 10^{-2}$  avec entrelacement contre  $BER \approx 1.4 \times 10^{-1}$  sans codage). En revanche, le gain est très net pour  $CFO = 0.4$ , de l'ordre de 2.8 dB à  $BER = 10^{-3}$ . L'entrelacement apporte un gain maximal de 1 dB. Nous aurions pu aussi considérer à la place une désynchronisation  $STO$ . Cela donnerait des résultats très proches, en considérant par exemple  $STO \in \{0, 0.2, 0.4, 0.5\}$ .

Nous pouvons conclure que le codage de canal est plus pertinent pour des valeurs intermédiaires de désynchronisation :  $0.3 \leq CFO \leq 0.4$  ou  $0.3 \leq STO \leq 0.4$ .

### I.2.7.3. Performances du front-end de synchronisation et impact du nombre de symboles du préambule

La Figure I.2.29 présente les performances du front-end de synchronisation présenté en détail dans la Section I.2.6.3, en évaluant l'impact du nombre de symboles du préambule sur le SER obtenu lors de la démodulation du payload. Nous faisons varier  $N_{up} = N_{down} \in \{2, 3, 4, 6, 8\}$  et nous comparons avec les performances en synchronisation parfaite ( $CFO = STO = SFO = 0$ ). Ces dernières représentent la borne optimale de performances atteignables.

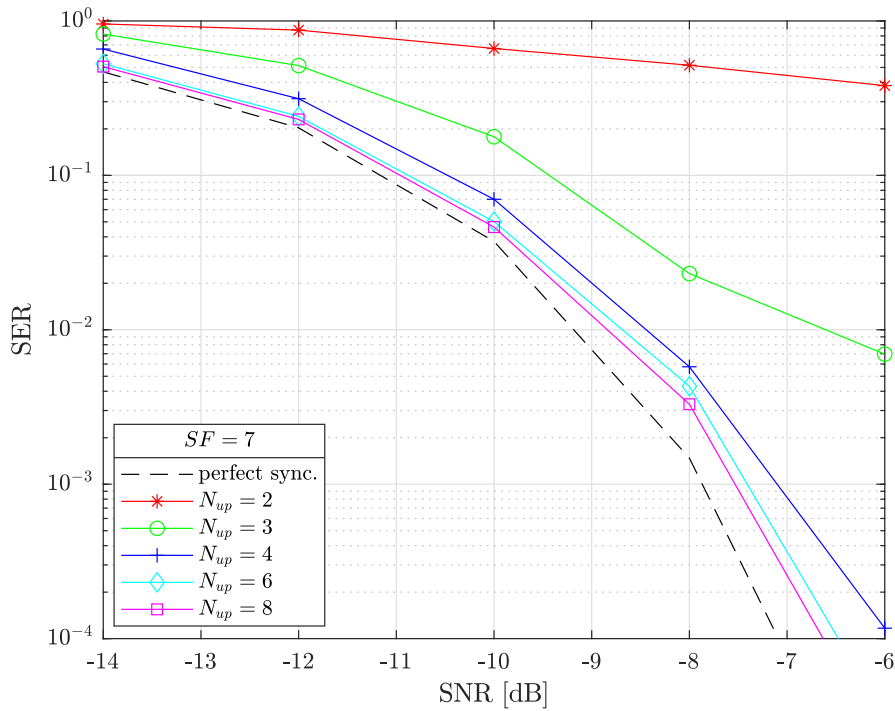


FIGURE I.2.29. – Performances du front-end de synchronisation de la littérature et impact du nombre de symboles pilotes,  $SF = 7$

Nous remarquons que pour la valeur par défaut  $N_{up} = 8$ , le front-end fonctionne bien, avec une perte limitée à 0.3 dB. Diminuer  $N_{up}$  dégrade naturellement les performances avec des performances catastrophiques pour  $N_{up} = 2$ . Cela s'explique par plusieurs sources d'erreurs :

- L'estimateur  $CFO_{frac}$  devient de plus en plus inconsistant à mesure que  $N_{up}$  diminue. Ainsi, le résidu moyen  $CFO_{frac}$  augmente et impactera de plus en plus le processus de moyennage des DFT pour l'estimation de  $CFO_{int}$  et  $STO_{int}$  dans les équations

(I.2.61) et (I.2.62), du fait de la dérive de phase présente (d'après l'équation (I.2.40)). Cela impactera donc l'estimation de ces deux paramètres.

- Lors de l'estimation de  $CFO_{int}$  et  $STO_{int}$ , la variance du bruit est diminuée d'un facteur  $N_{up}$ . Cette réduction sera de plus en plus faible avec  $N_{up}$  diminuant et les performances se dégraderont.
- Les erreurs d'estimation de  $CFO_{int}$  et  $STO_{int}$ , plus importantes, se répercuteront sur celle de  $STO_{frac}$ .

Nous avons présenté dans cette Section I.2 le standard LoRa : l'architecture réseau LoRaWAN, les propriétés de la modulation, les différents éléments qui constituent la chaîne de transmission, la problématique de la synchronisation avec les solutions proposées dans la littérature, ainsi que quelques résultats de simulation montrant les performances de LoRa.

Dans le chapitre suivant, nous présentons deux contributions que nous avons apportées afin d'améliorer le démodulateur LoRa classique : le calcul des expressions théoriques du SER dans un canal multi-trajets dans [90], et le récepteur amélioré LoRa RAKE dans [92] et [93]. Ces travaux nous ont permis d'affiner la compréhension du standard LoRa et de pouvoir ainsi développer le schéma d'auto-brouillage LoRa.

# Chapitre II

## Améliorations du démodulateur standard LoRa

Nous avons apporté plusieurs contributions sur LoRa, nous permettant d'acquérir de l'expertise sur ce standard, de mieux comprendre ses propriétés, et de donner des pistes sur le développement d'un schéma d'auto-brouillage LoRa améliorant la confidentialité et présenté dans les Sections III.3 et III.4. Dans cette section, nous présentons les principaux résultats de nos contributions [90, 92, 93] portant sur :

- Dans [90], le calcul des expressions analytiques du SER lors de transmissions dans un canal multi-trajets aligné (modèle présenté en Section II.1.1), ou en présence d'un autre utilisateur LoRa utilisant le même SF. Ce point est présenté en Section II.1.
- Le développement du récepteur cohérent amélioré LoRa RAKE, exploitant l'énergie des répliques du canal multi-trajets et comparé à un autre récepteur de la littérature [69] (nommé ici Time Delay Estimation LoRa (TDEL)) dans [92]. Nous considérons dans l'étude un canal multi-trajets aligné et une synchronisation parfaite. Les travaux ont été étendus au cas du canal multi-trajets non-aligné avec prise en compte de la synchronisation, dans [93]. Les deux publications sont présentées en Section II.2.

# II.1. Expressions analytiques du SER LoRa – canal multi-trajets et interférence LoRa

Dans cette section, nous résumons et donnons les principaux résultats de notre article *Theoretical Performance of LoRa System in Multi-Path and Interference Channels* [90]. Certains éléments de l'étude ont été volontairement omis pour ne pas alourdir cette section. Nous présentons d'abord en Section II.1.1 les modèles de canal multi-trajets et d'interférence LoRa considérés pour évaluer l'impact de ces derniers sur la démodulation en Section II.1.2. Puis en Section II.1.3, nous présentons les principaux résultats de simulation obtenus.

## II.1.1. Modèles de canal multi-trajets et d'interférence LoRa

### II.1.1.1. Modèle de canal multi-trajets

Nous considérons le modèle de canal multi-trajets suivant :

$$h(t) = \sum_{l=0}^{L-1} \alpha_l \delta(t - \tau_l) \quad (\text{II.1.1})$$

avec  $L$ , le nombre de trajets et  $\alpha_l = |\alpha_l|e^{j\pi\phi_l}$ , le gain complexe du  $l^{\text{ème}}$  trajet arrivant avec un retard de  $\tau_l$  secondes. Nous exprimons ici le gain des répliques en fonction de celui du trajet principal. Nous avons donc les relations suivantes :

$$|\alpha_0| = 1, \quad \phi_0 = 0, \quad \tau_0 = 0, \quad \phi_l \in [0; 2[ \quad \forall l > 0, \quad \tau_{l+1} > \tau_l, \quad 0 \leq l \leq L - 2 \quad (\text{II.1.2})$$

Comme  $\tau_l$  est réel, il est possible de le décomposer de façon similaire au CFO et au STO, par une partie entière plus une partie fractionnaire d'une période d'échantillonnage LoRa par :

$$\tau_l = k_l \times T_s = (k_{l,int} + k_{l,frac}) \times T_s \quad (\text{II.1.3})$$

avec :

$$k_{l,int} = \lfloor k_l \rfloor, \quad k_{l,frac} = k_l - k_{l,int} \quad (\text{II.1.4})$$

Pour des canaux de référence comme le canal multi-trajets Bad Urban (BU) modélisé pour le standard GSM [94], l'étalement maximal  $\tau_{L-1}$  n'excède généralement pas quelques microsecondes. Par exemple, pour  $\tau_l = 2 \mu\text{s}$ , cela correspond à avoir  $k_l = 1$  pour LoRa avec  $B = 500 \text{ kHz}$ . Ainsi, en pratique, nous avons  $k_{L-1} \ll M$ , et donc de l'Inter Symbol Interference (ISI) présente uniquement avec le symbole précédent sur quelques



échantillons, comme illustré en Figure II.1.1 pour un canal à deux trajets. Si  $k_{l,frac} = 0 \forall l$ , nous parlons alors de canal multi-trajets aligné, avec des retards multiples de la période d'échantillonnage, et de canal multi-trajets non-aligné sinon.

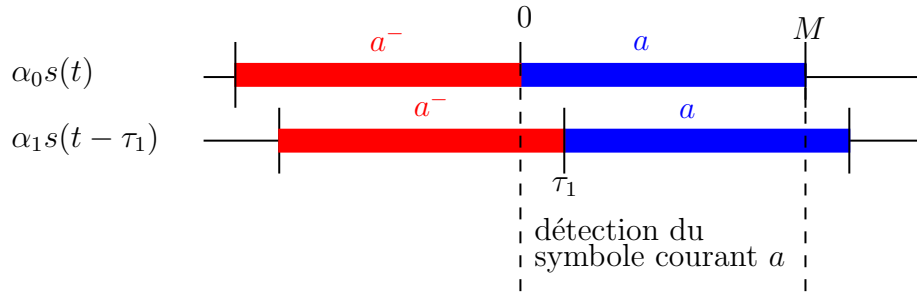


FIGURE II.1.1. – Illustration d'un canal à deux trajets

### II.1.1.2. Modèle d'interférence multi-utilisateurs LoRa

Le modèle d'interférence multi-utilisateurs LoRa est assez proche du modèle de canal multi-trajets, et est illustré en Figure II.1.2, avec  $a_1^-$ ,  $a_1$  et  $a_1^+$ , les symboles précédent, courant et suivant de l'utilisateur 1 (et de même pour l'utilisateur 2). Nous supposons que le signal de l'utilisateur 1 arrive en premier et que le récepteur est synchronisé sur ce dernier. Le signal reçu est donc la superposition des signaux des deux utilisateurs :

$$r(t) = s_1(t) + \rho s_2(t - \tau) \quad (\text{II.1.5})$$

avec  $s_1(t)$  et  $s_2(t)$ , les signaux LoRa des deux utilisateurs,  $\rho = |\rho|e^{j\pi\beta}$ , le gain complexe du signal de l'utilisateur 2 et  $\tau$ , le retard d'arrivée pouvant également être décomposé en partie entière et fractionnaire d'une période d'échantillonnage :

$$\tau = z \times T_s = (z_{int} + z_{frac}) \times T_s \quad (\text{II.1.6})$$

avec :

$$z_{int} = \lfloor z \rfloor, \quad z_{frac} = z - z_{int} \quad (\text{II.1.7})$$

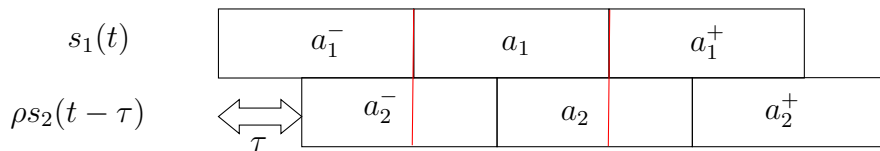


FIGURE II.1.2. – Illustration d'une interférence multi-utilisateurs LoRa

Il est à noter qu'une collision avec un signal LoRa ayant un SF différent, bien que non orthogonale, n'impacte que peu la démodulation du signal d'intérêt, si les signaux sont parfaitement superposés i.e.  $z = 0$  [63].

Dans [90], nous considérons dans l'étude un canal multi-trajets aligné avec  $k_l \in \{0, 1, \dots, M - 1\}$  en supposant  $\phi_l = 0$ . Il est en effet montré dans l'article que  $\phi_l$  a un impact assez négligeable lorsque le canal multi-trajets est aligné. De même, l'interférence LoRa est supposée alignée i.e.  $z_{frac} = 0$ .

## II.1.2. Impact du canal multi-trajets et de l'interférence LoRa sur la démodulation

### II.1.2.1. Impact du canal multi-trajets sur la démodulation

Lorsque le canal multi-trajets est aligné, l'expression du signal reçu dechirpé avant DFT peut s'exprimer par :

$$\tilde{r}[k] = x_0^*[k]r[k] = \tilde{\alpha}_0 e^{2j\pi k \frac{a}{M}} + \sum_{l=1}^{L-1} \tilde{\alpha}_l e^{2j\pi k \frac{a-k_l}{M}} + x_0^*[k]w[k] \quad (\text{II.1.8})$$

avec :

$$\tilde{\alpha}_l = \alpha_l e^{-2j\pi k_l \left[-\frac{1}{2} - \frac{k_l}{2M}\right]} \quad (\text{II.1.9})$$

et :

$$\bar{a} = \begin{cases} a^- & \text{pour } k \in \{0, 1, \dots, k_l - 1\} \text{ (symbole précédent)} \\ a & \text{pour } k \in \{k_l, k_l + 1, \dots, M - 1\} \text{ (symbole courant)} \end{cases} \quad (\text{II.1.10})$$

Comme l'étalement du canal multi-trajets est faible en pratique ( $k_{L-1} \ll M$ ), nous pouvons négliger la contribution du symbole précédent et supposer  $\bar{a} = a$  dans l'équation (II.1.8).

En appliquant la DFT, nous obtenons :

$$\tilde{R}[n] = \text{DFT}\{\tilde{r}[k]\}[n] = M\tilde{\alpha}_0\delta[n-a] + M\sum_{l=1}^{L-1} \tilde{\alpha}_l[a]\delta[n-(a-k_l)] \quad (\text{II.1.11})$$

Lorsque le canal multi-trajets est non-aligné, les expressions sont plus complexes, puisqu'un bin pourra contenir des composantes de différents trajets en fonction des retards de ces derniers. De plus, en fonction des phases  $\phi_l$  des signaux des trajets, le résultat peut-être très différent. L'expression théorique de la DFT LoRa dans un canal multi-trajets non-aligné est donnée en Annexe E.

La Figure II.1.3 montre l'effet d'un canal multi-trajets aligné ou non-aligné sur la démodulation du symbole  $a = 80$  ( $a^- = a$ ), ayant une seule réplique de valeurs  $k_1 \in \{0, 4, 10.25, 20.5, 30.75\}$ ,  $\phi_1 = 0$ , et  $SF = 7$ . Nous observons que le comportement est assez similaire à celui du STO (voir Figure I.2.20). D'après la figure et l'équation (II.1.11), chaque réplique ajoute un pic, décalé de  $\lfloor k_l \rfloor$  positions vers la gauche. La partie fractionnaire vient diffuser l'énergie sur les bins voisins, vers la gauche. Plus  $k_{l,frac}$  est proche de 0.5, plus la diffusion est importante et plus l'incertitude de démodulation entre les bins en  $n \in \{a, (a-1) \bmod M\}$  est grande.

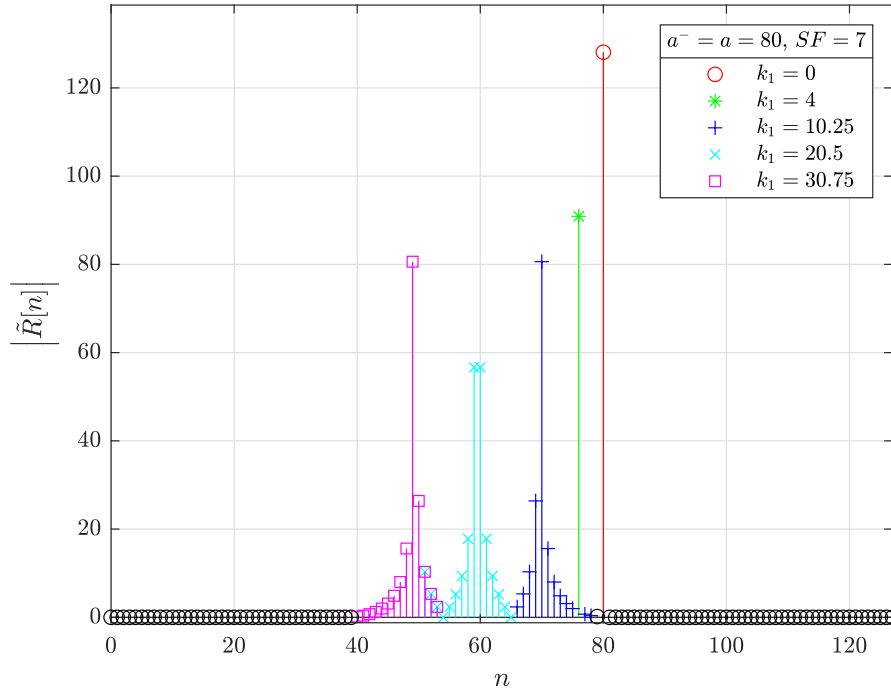
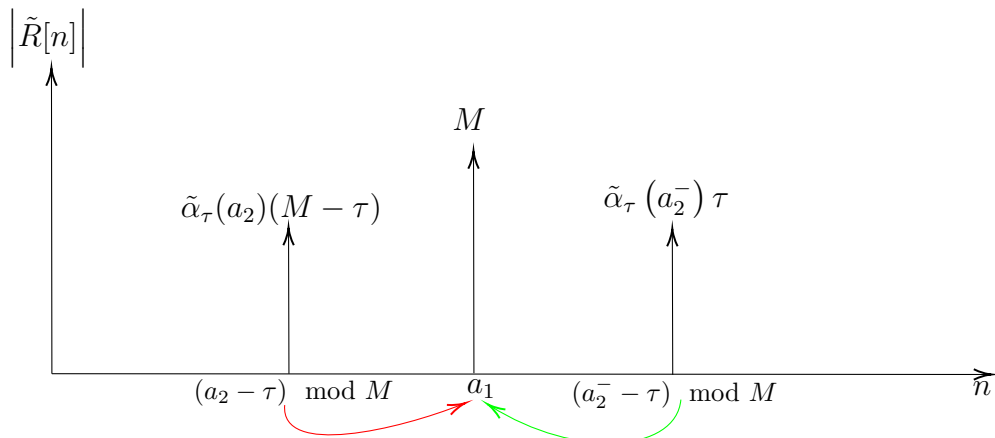


FIGURE II.1.3. – Impact du canal multi-trajets (aligné ou non-aligné) sur la DFT LoRa

### II.1.2.2. Impact de l'interférence LoRa sur la démodulation

Les Figures II.1.4 et II.1.5 illustrent l'impact sur la DFT de l'interférence multi-utilisateurs LoRa. D'après les figures, nous relevons les cas suivants possibles :

- $a_2^- \neq a_2$  (Figure II.1.4)
  1.  $(a_2 - \tau) \bmod M \neq a_1$  et  $(a_2^- - \tau) \bmod M \neq a_1$  : trois pics sont présents sur la DFT.
  2.  $(a_2 - \tau) \bmod M = a_1$  et  $(a_2^- - \tau) \bmod M \neq a_1$  : l'énergie du bin  $n = (a_2 - \tau) \bmod M$  vient s'ajouter à celui en  $n = a_1$  (flèche rouge).
  3.  $(a_2 - \tau) \bmod M \neq a_1$  et  $(a_2^- - \tau) \bmod M = a_1$  : l'énergie du bin  $n = (a_2^- - \tau) \bmod M$  vient s'ajouter à celui en  $n = a_1$  (flèche verte).


 FIGURE II.1.4. – Impact de l'interférence multi-utilisateurs LoRa sur la DFT,  $a_2^- \neq a_2$

- $a_2^- = a_2$  (Figure II.1.5)
  1.  $(a_2 - \tau) \bmod M \neq a_1$  : deux pics sont présents sur la DFT.
  2.  $(a_2 - \tau) \bmod M = a_1$  : l'énergie du bin  $n = (a_2 - \tau) \bmod M$  vient s'ajouter à celui en  $n = a_1$  (flèche bleue).

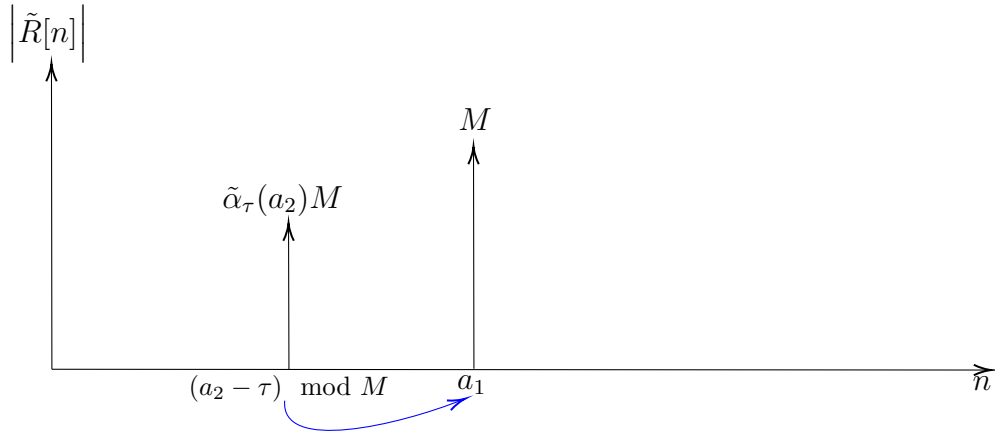


FIGURE II.1.5. – Impact de l'interférence multi-utilisateurs LoRa sur la DFT,  $a_2^- = a_2$

## II.1.3. Résultats de simulation

Les expressions analytiques du SER LoRa pour le cas du canal multi-trajets aligné et celui de l'interférence multi-utilisateurs LoRa ont été obtenues dans [90], pour les deux récepteurs non-cohérent et cohérent. Seules les expressions pour le récepteur non-cohérent sont données en Annexes C et D. Celles du récepteur cohérent peuvent être trouvées dans [90]. Le comportement SER est très proche, avec globalement le même gain de 0.8 dB vu en Figure I.2.27. L'expression analytique du SER avec une interférence multi-utilisateurs LoRa nécessite de décomposer les cinq cas possibles dans les Figures II.1.4 et II.1.5. Les développements sont présentés en Annexe D.

### II.1.3.1. SER LoRa analytique dans un canal multi-trajets aligné

Les Figures II.1.6 et II.1.7 présentent le SER analytique du récepteur non-cohérent (équation (C.14)) dans un canal multi-trajets aligné ayant deux trajets. Sur la Figure II.1.6, nous considérons plusieurs couples de valeurs  $k_1$  et  $\alpha_1$ , avec  $k_1 \in \{1, 3, 5, 7, 9, 11\}$  et  $\alpha_1 \in \{0, 0.2, 0.4, 0.6, 0.8, 0.9\}$ , et  $SF = 7$ . Sur la Figure II.1.7, nous fixons  $k_1 = 1$  et évaluons pour  $\alpha_1 \in \{0, 0.4, 0.8\}$  et  $SF \in \{7, 8, 9, 10\}$ . Notons que  $\alpha_1 = 0$  revient au cas AWGN. Nous remarquons les comportements suivants :

- Sur les deux figures, pour  $k_1$  fixé, augmenter  $\alpha_1$  dégrade progressivement les performances.
- D'après la Figure II.1.6, pour  $\alpha_1 \leq 0.2$ , l'impact est négligeable tandis que pour  $\alpha_1 \geq 0.6$ , la perte est très importante par rapport au cas AWGN, atteignant environ 15 dB pour  $\alpha_1 = 0.9$  à  $SER = 10^{-4}$ .
- D'après la Figure II.1.6, pour  $\alpha_1$  fixé, avoir la réplique proche du trajet direct et donc  $k_1$  faible donne de moins bonnes performances.

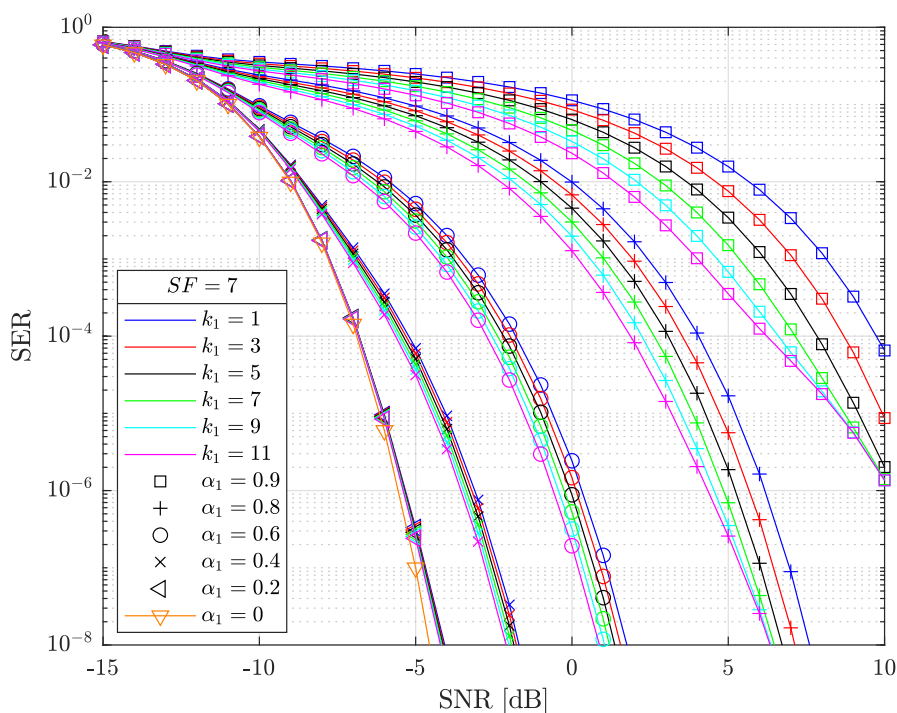


FIGURE II.1.6. – SER LoRa analytique du récepteur non-cohérent dans un canal multi-trajets aligné,  $SF = 7$

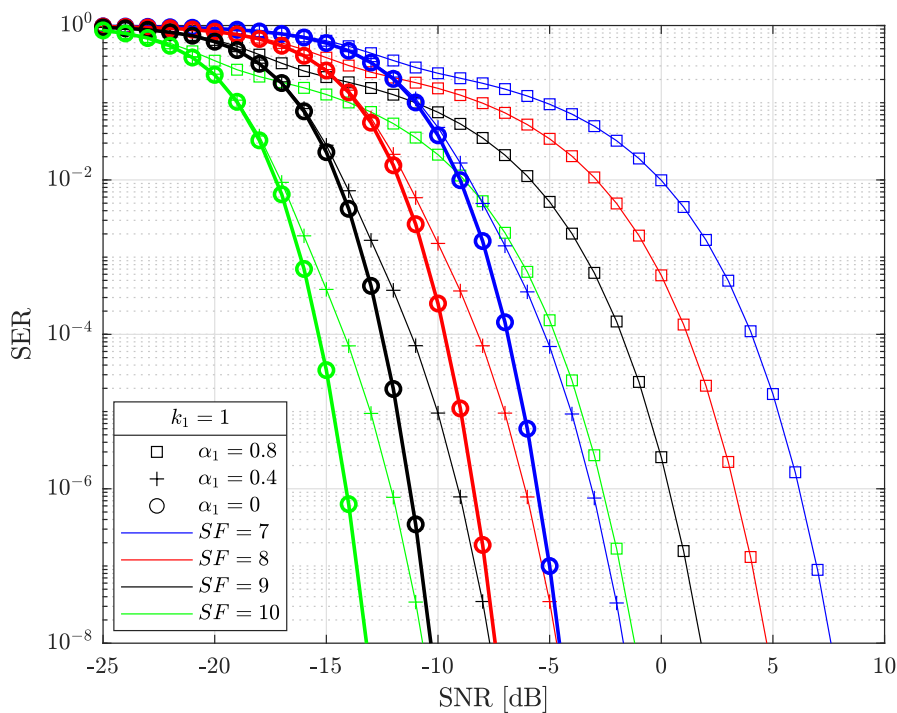


FIGURE II.1.7. – SER LoRa analytique du récepteur non-cohérent dans un canal multi-trajets aligné pour plusieurs valeurs de  $SF$

- D'après la Figure II.1.7, pour  $\alpha_1$  fixé, augmenter SF réduit progressivement la perte de performances par rapport au cas idéal AWGN ( $\alpha_1 = 0$ ). Pour  $\alpha_1 = 0.8$ , nous relevons une perte à  $SEER = 10^{-8}$  de 12.19 dB pour  $SF = 7$ , 12.16 dB pour  $SF = 8$ , 12.12 dB pour  $SF = 8$  et 11.98 dB pour  $SF = 10$ .  $SF = 11$  et  $SF = 12$  donnent des pertes de 11.89 dB et 11.83 dB (non affiché sur la Figure II.1.7 par soucis de clarté).

### II.1.3.2. Comparaison du SER LoRa analytique entre un canal multi-trajets aligné à deux répliques et un canal à décroissance exponentielle

Nous supposons ici toujours le récepteur non-cohérent dans un canal multi-trajets aligné, avec soit un canal à deux trajets ou un canal à décroissance exponentielle. Ils sont dénotés par  $h_1[k]$  et  $h_2[k]$  respectivement, et ont pour expression :

$$h_1[k] = 1 + \alpha\delta[k - 1], \quad \alpha \in \mathfrak{R} \quad (\text{II.1.12})$$

$$h_2[k] = \sum_{l=0}^{K-1} \alpha^l \delta[k - l], \quad \alpha \in \mathfrak{R} \quad (\text{II.1.13})$$

avec  $K$  satisfaisant la contrainte  $|\alpha|^K \leq 0.2$ . Le canal à décroissance exponentielle est assez réaliste, puisqu'en pratique, plus une réplique est éloignée dans le temps, moins son gain sera fort, statistiquement. Nous cherchons alors à savoir à quel point l'ajout de répliques avec gains à décroissance exponentielle dégrade le SER par rapport à une seule réplique forte.

La Figure II.1.8 compare le SER théorique pour  $\alpha \in \{0.7, 0.8\}$  et  $SF \in \{7, 10\}$ . Nous remarquons que quelque soit la valeur de SF, le canal  $h_2$  ne dégrade que très peu les performances par rapport au canal  $h_1$ , avec une perte légèrement marquée pour  $5 \times 10^{-1} \leq SER \leq 10^{-1}$  mais nulle sinon. Ainsi, seule la réplique la plus forte dominera réellement les performances. Nous pouvons donc conclure que LoRa est sensible principalement à la présence d'une ou deux répliques significatives.

### II.1.3.3. SER LoRa analytique avec interférence multi-utilisateurs

La Figure II.1.9 montre le SER LoRa analytique pour une interférence multi-utilisateurs, obtenu avec les expressions théoriques en Annexe D. Nous considérons  $SF = 7$ ,  $z = M/2$  (voir l'équation (II.1.6)) et plusieurs valeurs de Signal to Interference Ratio (SIR),  $SIR_{dB} \in \{0, 2, 4, 6, 8, 10\}$ . Le SIR est défini par :

$$SIR = \frac{P_1}{P_2} = \frac{1}{P_2} \quad (\text{II.1.14})$$

avec  $P_1$  et  $P_2$ , les puissances des signaux reçus des utilisateurs 1 et 2, respectivement. Plus le SIR est élevé, moins l'utilisateur 2 interfère avec l'utilisateur 1. Le SER analytique dans le cas AWGN est aussi montré (équivalent à avoir  $P_2 = 0$ ), afin d'évaluer la perte de performances induite par la présence de l'autre utilisateur LoRa.

Nous constatons que l'impact est très faible si  $SIR_{dB} \geq 10$ . Diminuer le SIR dégrade bien entendu les performances, avec le cas catastrophique  $SIR_{dB} = 0$  ( $P_2 = P_1$ ), où le

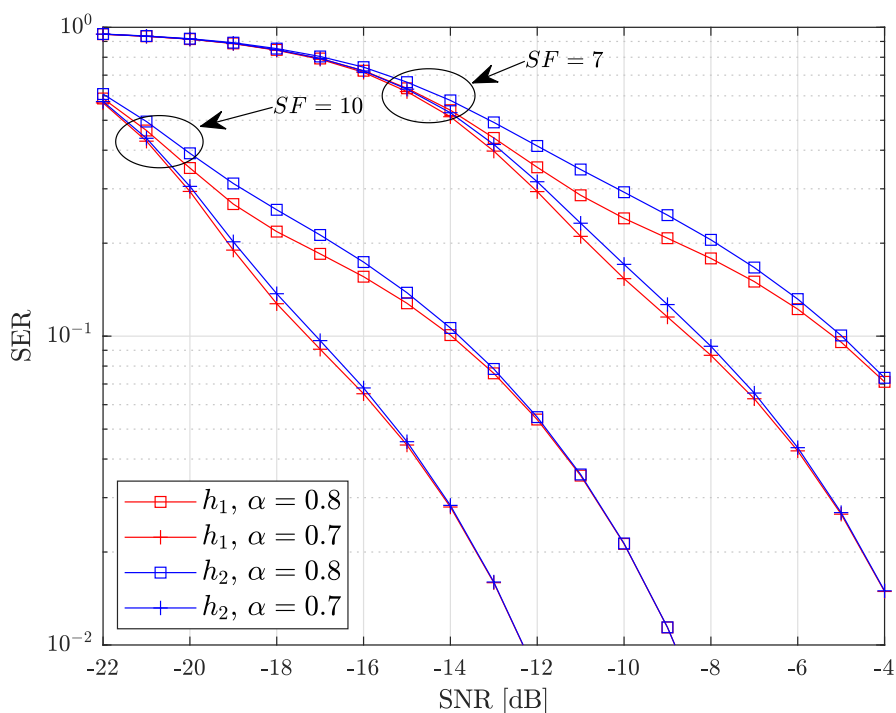


FIGURE II.1.8. – Comparaison du SER LoRa analytique entre un canal multi-trajets aligné à deux répliques et un canal à décroissance exponentielle,  $SF = 7$

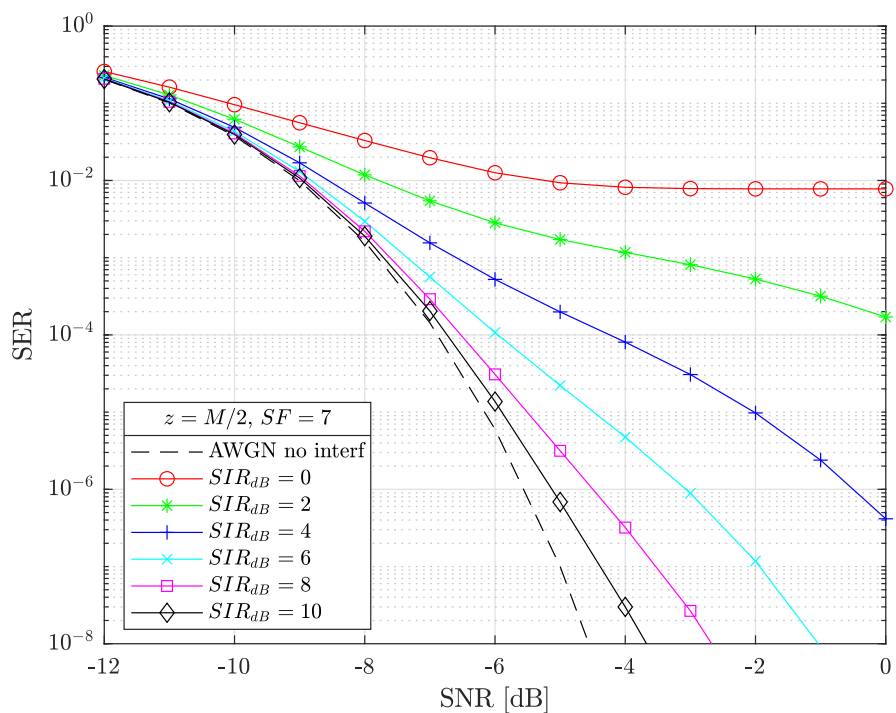


FIGURE II.1.9. – SER LoRa analytique avec interférence multi-utilisateurs,  $SF = 7$

SER converge vers le palier  $SER \approx 8 \times 10^{-3}$ . Les performances sont également mauvaises pour  $SIR_{dB} \in \{2, 4\}$ . Nous pouvons conclure que LoRa est sensible à l'interférence multi-utilisateurs si  $SIR_{dB} \leq 6$ . Notons que le paramètre de retard  $z$  influe aussi sur le SER mais dans une moindre mesure, avec les performances s'améliorant à mesure que  $z$  se rapproche de  $M/2$  [90]. Nous avons donc dans la Figure II.1.9 les performances les plus optimistes.

Pour conclure sur cette section, nous pouvons rappeler les points importants suivants :

- Les effets d'un canal multi-trajets et d'une interférence multi-utilisateurs LoRa sont similaires.
- Les performances SER sont dominées par la réplique canal ayant le gain le plus élevé. Ainsi, seul un ou deux trajets significatifs peuvent être considérés pour une étude analytique ou le développement d'un récepteur LoRa amélioré (voir Section II.2).
- Un gain de réplique de canal inférieur à 0.2 (normalisé par rapport au signal d'intérêt) a un impact négligeable sur la démodulation. Les performances sont en revanche très fortement dégradées si cette valeur est supérieure à 0.5.
- Une interférence multi-utilisateurs LoRa a un impact beaucoup plus fort qu'un canal multi-trajets : un SIR de 6 dB et moins suffit à fortement dégrader les performances.

Notons que l'obtention d'une expression théorique du SER dans un canal multi-trajets non-aligné (contrairement au cas du canal multi-trajets aligné dans [90]) pourrait faire l'objet d'une étude future.





## II.2. Récepteur amélioré LoRa RAKE

Dans cette partie, nous présentons les principaux résultats obtenus dans nos articles *Simple and Efficient LoRa Receiver Scheme for Multi-Path Channel* [92] et *A RAKE-like coherent LoRa receiver for Non-Aligned Multi-Path Channels* [93], où nous proposons le récepteur amélioré LoRa RAKE exploitant l'énergie des répliques de canal multi-trajets, motivé par notre étude dans [90]. Il est comparé à un autre récepteur amélioré de la littérature, nommé Time Delay Estimation LoRa (TDEL) [69].

Nous présentons d'abord en Section II.2.1 le récepteur TDEL. Puis, nous présentons en Section II.2.2 notre récepteur LoRa RAKE et sa variante cand-LoRa RAKE ayant une complexité calculatoire réduite, pour le scénario d'un canal multi-trajets aligné avec synchronisation parfaite [92], et montrons qu'il surpasse le récepteur TDEL. Ensuite, nous étendons en Section II.2.3 les travaux pour le scénario plus réaliste d'un canal multi-trajets non-aligné à deux trajets, où la réplique est proche du trajet direct, avec prise en compte de la synchronisation temporelle et fréquentielle [93]. Nous montrons que LoRa RAKE nécessite une compensation de phase pour pouvoir fonctionner correctement. Le fonctionnement de cette dernière est présenté en détail et des résultats de simulation sont montrés afin de déterminer lequel de LoRa RAKE et TDEL donne les meilleures performances SER en fonction des conditions du canal multi-trajets et du SNR.

### II.2.1. Récepteur TDEL de la littérature

Dans [69], le récepteur TDEL a été développé afin de rendre la démodulation LoRa plus robuste en présence d'un canal multi-trajets. Ce récepteur fonctionne comme suit :

1. Les DFT des  $N_{up}$  symboles upchirp de préambule sont moyennées afin de réduire la variance du bruit lors de la démodulation pour obtenir  $\langle \tilde{P}[n] \rangle$  (voir l'équation (I.2.61)).
2. Dans la DFT moyennée, les bins ayant une faible magnitude (inférieure à un seuil) sont mis à zéro :

$$\langle \tilde{P}[n] \rangle = \begin{cases} 0 & \text{si } \left| \langle \tilde{P}[n] \rangle \right| < \rho_{TDEL} \\ \langle \tilde{P}[n] \rangle & \text{sinon} \end{cases} \quad (\text{II.2.1})$$

avec :

$$\rho_{TDEL} = \lambda_{TDEL} \times \max_n \left| \langle \tilde{P}[n] \rangle \right| \quad (\text{II.2.2})$$

et  $\lambda_{TDEL} \in ]0; 1[$ . Cela permet d'éliminer des bins purement AWGN dans le processus de démodulation et améliore donc les performances.

3. TDEL estime enfin le symbole par inter-corrélation circulaire :

$$\hat{a}_{i,TDEL} = \arg \max_m F_i[m] \quad (\text{II.2.3})$$

avec :

$$F_i[m] = \sum_{n=0}^{M-1} \left| \left\langle \tilde{P}[n] \right\rangle \tilde{R}_i[(n-m) \bmod M] \right| \quad (\text{II.2.4})$$

TDEL a les trois avantages suivants :

- Il possède une complexité calculatoire faible : il nécessite peu d'étapes intermédiaires et l'inter-corrélation circulaire peut être implémentée de façon optimisée grâce aux algorithmes de type Fast Fourier Transform (FFT).
- Il ne nécessite pas d'estimer le canal multi-trajets.
- Le récepteur est insensible aux erreurs de synchronisation sur  $CFO_{int}$ , grâce aux propriétés d'inter-corrélation. Il est également peu sensible aux erreurs de synchronisation sur  $STO_{int}$ . En effet, la DFT des symboles payload sera fortement déformée, uniquement si  $\widehat{STO}_{int}$  est très éloigné de  $STO_{int}$ , où de l'ISI sera alors très présente. Comme en pratique, nous avons la plupart du temps  $\widehat{STO}_{int} = (STO_{int} \pm 1) \bmod M$ , la déformation DFT sera alors très faible et l'impact sur les performances négligeable.

En revanche, TDEL, de part sa nature purement non-cohérente, a des performances sous-optimales au sens AWGN. Des récepteurs améliorés cohérents tels que LoRa RAKE donneront les meilleures performances dans ce cas (voir Figure I.2.27).

## II.2.2. Démodulation LoRa RAKE dans un canal multi-trajets aligné avec synchronisation parfaite

Dans cette section, nous présentons le récepteur LoRa amélioré LoRa RAKE que nous avons proposé dans l'article *Simple and Efficient LoRa Receiver Scheme for Multi-Path Channel* [92] pour un canal multi-trajets aligné avec synchronisation parfaite. Nous introduisons d'abord en Section II.2.2.1 la structure du récepteur. Ensuite, nous proposons en Section II.2.2.2 une variante reposant sur une approche par candidats permettant de réduire la complexité calculatoire de LoRa RAKE. Enfin, nous présentons en Section II.2.2.3 quelques résultats de simulation pour évaluer les performances de LoRa RAKE.

### II.2.2.1. Structure du démodulateur

Dans [92], nous avons développé le récepteur LoRa RAKE pour le cas d'un canal multi-trajets aligné en supposant une synchronisation parfaite, ayant pour but d'exploiter de manière constructive l'énergie du canal présente dans les bins voisins du bin d'intérêt (voir Figure II.1.3), et reprenant la philosophie du récepteur RAKE, bien connu dans la littérature [95]. Le front-end de réception LoRa RAKE est présenté en Figure II.2.1.

La démodulation initiale est réalisée de façon normale : dechirp et calcul de la DFT. Le récepteur estime ensuite les coefficients du canal multi-trajets aligné à partir des symboles upchirp du préambule moyennés, et en utilisant un seuil de détection en magnitude. Ce seuil, noté  $\rho_{path}$ , est défini comme une fraction  $\lambda_{path}$  de la magnitude du bin  $n = a = 0$  (le symbole dans le préambule vaut  $a = 0$ ) :

$$\rho_{path} = \lambda_{path} \times \left| \left\langle \tilde{P}_{aligned}[0] \right\rangle \right|, \quad \lambda_{path} \in ]0; 1[ \quad (\text{II.2.5})$$

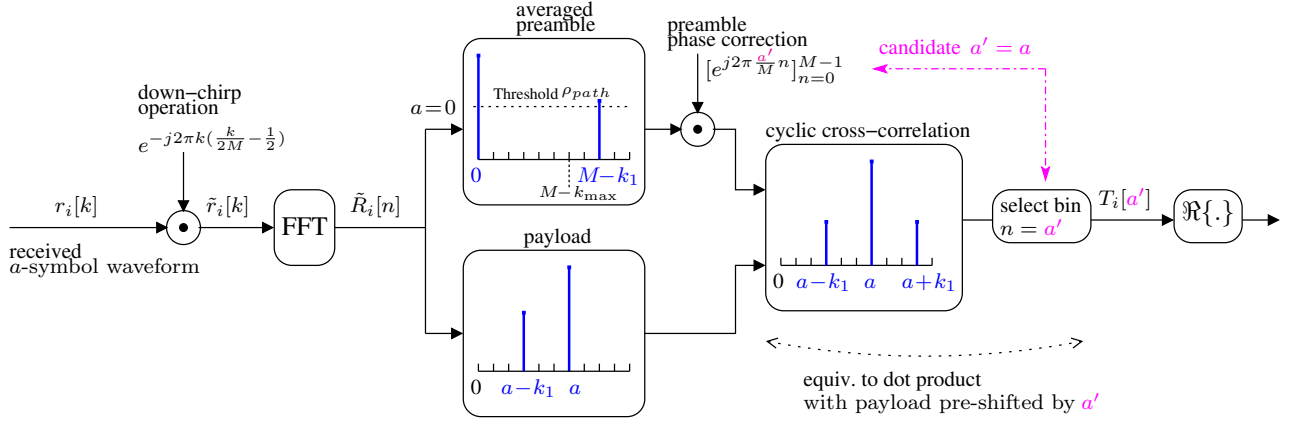


FIGURE II.2.1. – Illustration du démodulateur LoRa RAKE au bin  $a' = a$

avec :

$$\left\langle \tilde{P}_{aligned}[n] \right\rangle = \frac{1}{N_{up}} \sum_{i=0}^{N_{up}-1} \tilde{P}_i[n] \quad (\text{II.2.6})$$

Tous les bins dépassant  $\rho_{path}$  sont alors considérés comme un trajet du canal, et les indices des bins retenus sont mémorisés (rangés dans l'ensemble  $\mathcal{S}$ ). Nous supposons que l'étalement du canal est inférieur à une valeur  $k_{max}$ , i.e.  $k_{L-1} \leq k_{max}$ . Ainsi, parmi les indices dans  $\mathcal{S}$ , ceux étant inférieurs à  $M - k_{max}$  sont éliminés et l'ensemble  $\mathcal{S}$  est actualisé (suppression des indices et tri par ordre décroissant en commençant par  $n = 0$ ). Nous notons  $\hat{L} = |\mathcal{S}|$ , le nombre de trajets estimés. Les coefficients du canal  $\tilde{\alpha}_l$  sont alors estimés par :

$$\hat{\alpha}_l = \frac{\left\langle \tilde{P}_{aligned}[s_l] \right\rangle}{M - l} \quad (\text{II.2.7})$$

avec  $s_l$ , le  $l^{ème}$  indice dans  $\mathcal{S}$ . Le récepteur combine de façon constructive l'énergie des trajets pour chaque symbole possible, selon une structure RAKE :

$$T_i[a'] = \sum_{l=0}^{\hat{L}-1} \hat{\alpha}_l^* [a'] \tilde{R}_i[(a' - l) \bmod M] \quad (\text{II.2.8})$$

avec  $i$ , l'indice de symbole,  $a'$ , le symbole candidat ( $a' \in \{0, 1, \dots, M - 1\}$ ), et :

$$\hat{\alpha}_l [a'] = \hat{\alpha}_l e^{-2j\pi l \frac{a'}{M}} \quad (\text{II.2.9})$$

Le symbole est alors démodulé par :

$$\hat{a}_i = \arg \max_{a'} \Re\{T_i[a']\} \quad (\text{II.2.10})$$

Ce récepteur est cohérent, il donne donc les meilleures performances au sens AWGN (voir Figure I.2.27).

### II.2.2.2. Réduction de la complexité calculatoire de LoRa RAKE : cand-LoRa RAKE

Le récepteur LoRa RAKE doit effectuer une recherche exhaustive sur l'ensemble des symboles possibles, soit  $M$  candidats potentiels, d'après l'équation (II.2.8). Cela peut donc poser une contrainte sur la complexité calculatoire pour une implémentation réelle, surtout si SF est grand. La complexité calculatoire du récepteur LoRa RAKE peut-être réduite en diminuant le nombre de candidats. Pour cela, nous pouvons adopter deux approches. Elles sont regroupées sous le type de démodulation que nous appellerons cand-LoRa RAKE.

Premièrement, nous pouvons choisir les  $N_c$  bins ayant la plus forte magnitude dans la DFT LoRa, pour chaque symbole de payload. Comme le nombre de candidats est fixe, le gain de réduction de complexité calculatoire est constant et vaut  $M/N_c$ . Cette solution est notée f-cand-LoRa RAKE.

Deuxièmement, nous pouvons réutiliser une approche par seuil (comme pour la sélection des trajets dans l'équation (II.2.5)), en retenant uniquement les bins dont la magnitude est supérieure à un seuil dans la DFT LoRa du symbole de payload :

$$\rho_{cand} = \lambda_{cand} \times \max_n \left| \tilde{R}[n] \right|, \quad \lambda_{cand} \in ]0; 1[ \quad (\text{II.2.11})$$

Nous notons cette approche d-cand-LoRa RAKE. Les candidats retenus, rangés dans l'ensemble  $\mathcal{A}$ , sont donc ceux supérieurs à  $\rho_{cand}$ . Nous notons  $N_c = |\mathcal{A}|$ , le nombre de candidats. Le choix de  $\lambda_{cand}$  est important. Une valeur faible garantira  $a \in \mathcal{A}$  (et donc une démodulation correcte possible), mais au prix d'un gain de réduction de complexité calculatoire plus faible. Inversement, choisir  $\lambda_{cand}$  grand réduira grandement la complexité, mais au risque de ne pas avoir  $a \notin \mathcal{A}$ , et donc aboutir sur une erreur de démodulation. Cette approche permet d'avoir un nombre de candidats dynamique qui s'adapte aux conditions du SNR. En effet, plus le SNR est élevé, plus la probabilité de sélectionner un bin autre que  $n = a$  diminue, pour  $\lambda_{cand}$  fixe. Le nombre moyen  $N_c$  sera alors plus faible et le gain, plus important. Bien que l'équation (II.2.11) nécessite des opérations supplémentaires (calcul du module de la DFT, recherche de la valeur maximale dans la DFT et extraction des bins supérieurs à  $\rho_{cand}$ ), elle engendre un surcoût calculatoire qui est largement compensé par la réduction du nombre de candidats et qui ne dépend pas du seuil  $\lambda_{cand}$  [92].

La démodulation cand-LoRa RAKE reste la même, mais pour  $a' \in \mathcal{A}$  dans les équations (II.2.8) et (II.2.10).

### II.2.2.3. Résultats de simulation

Dans cette section, nous présentons plusieurs résultats de simulation : l'impact sur les performances SER de cand-LoRa RAKE du seuil d'estimation des trajets du canal multi-trajets, l'impact du nombre de candidats sur les performances SER de f-cand-LoRa RAKE, l'évaluation du gain de réduction de complexité calculatoire offert par cand-LoRa RAKE, et une comparaison des performances SER entre LoRa RAKE, d-cand-LoRa RAKE, TDEL et les récepteurs classiques.

Dans les simulations, nous considérons un canal multi-trajets réaliste à deux trajets, noté  $C_1$ , et ayant la réponse impulsionnelle suivante :

$$C_1[k] = \alpha_0\delta[k] + \alpha_1\delta[k - 5], \quad \alpha_0 = 1, \quad \alpha_1 = 0.8 \quad (\text{II.2.12})$$

Les performances SER sont obtenues par tirages de Monte-Carlo. A chaque tirage, une trame comportant  $N_d = 1000$  symboles de payload est générée. Le SER est calculé sur ces  $N_d$  symboles de payload, tandis que l'estimation du canal multi-trajets est effectuée pour chaque trame. Le nombre de tirages  $N_{trials}$  doit donc être suffisamment élevé ( $N_{trials} = 1000$  ici) pour obtenir des performances d'estimation du canal statistiquement fiables. De plus, nous fixons  $k_{max} = 10$ . Ainsi, en fonction du seuil  $\lambda_{path}$ , le nombre maximal de trajets supplémentaires retenus sera de 8 pour le canal  $C_1$ .

### II.2.2.3.1. Impact sur les performances SER de LoRa RAKE du seuil d'estimation des trajets du canal multi-trajets

La Figure II.2.2 monte l'impact du seuil d'estimation des trajets du canal multi-trajets  $\lambda_{path}$  sur les performances SER de LoRa RAKE pour  $SF = 7$ . Pour cela, nous estimons le canal multi-trajets sur le préambule selon les équations (II.2.5), (II.2.6) et (II.2.7), démodulons le payload avec LoRa RAKE à partir du canal multi-trajets estimé (équation (II.2.8)), et relevons le SER du payload démodulé, pour plusieurs valeurs du seuil  $\lambda_{path} \in \{0.2, 0.4, 0.6, 0.8\}$ . Sur la figure, la courbe portant la mention "L known" signifie que le nombre de trajets est parfaitement connu (ici deux pour  $C_1$ ). Le récepteur choisira alors les  $L - 1$  bins dans l'intervalle  $M - k_{max} \leq n \leq M - 1$  ayant les magnitudes les plus grandes (récepteur synchronisé sur le premier trajet).

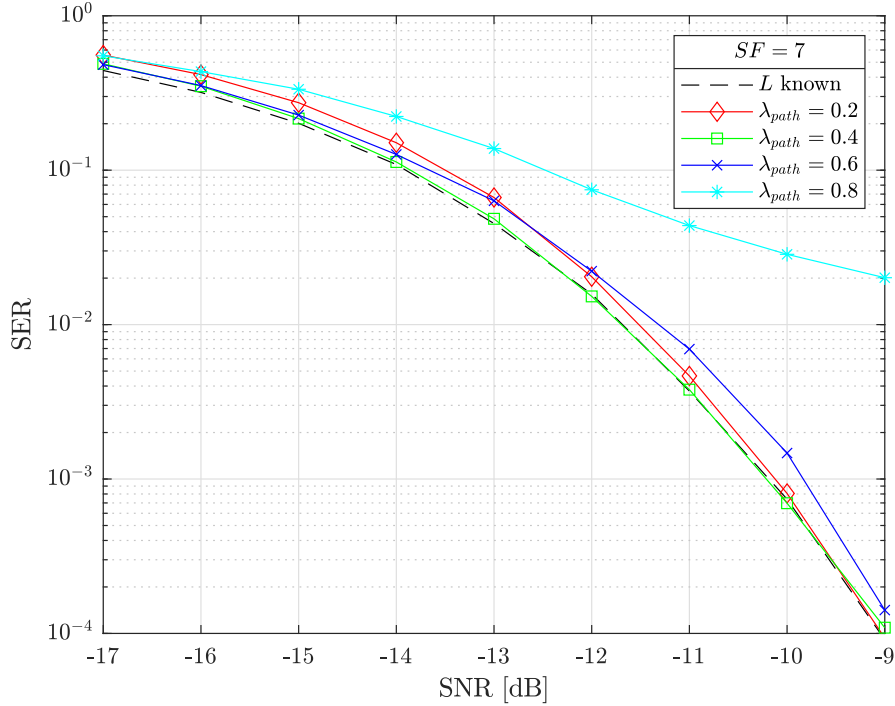


FIGURE II.2.2. – Impact du seuil de détection de trajets du canal multi-trajets sur le SER de cand-LoRa RAKE,  $SF = 7$

## II.2. Récepteur amélioré LoRa RAKE

D'après la Figure II.2.2, nous constatons que choisir  $\lambda_{path}$  trop élevé conduira à une dégradation importante du SER, puisque les deux trajets d'intérêt seront régulièrement manqués (écart important entre  $\lambda_{path} = 0.6$  et  $\lambda_{path} = 0.8$  sur la figure). Pour  $\lambda_{path} \leq 0.6$ , les performances sont très proches, avec  $\lambda_{path} = 0.4$  donnant cependant les meilleures performances. Notons qu'à faible SNR ( $SNR_{dB} < -13$ ),  $\lambda_{path} = 0.6$  donne de meilleures performances que  $\lambda_{path} = 0.2$ , mais le comportement est inversé pour des SNR plus favorables ( $SNR_{dB} \geq -12$ ).

### II.2.2.3.2. Impact du nombre de candidats sur les performances de LoRa RAKE

La Figure II.2.3 évalue l'impact du nombre de candidats sur le SER de f-cand-LoRa RAKE, pour deux couples de SF :  $SF = 7$  ( $SNR_{dB} = -13.6$  et  $SNR_{dB} = -11.6$ ) et  $SF = 10$  ( $SNR_{dB} = -21.1$  et  $SNR_{dB} = -19.1$ ). Nous supposons une estimation parfaite des coefficients du canal  $\tilde{\alpha}_l$  i.e.  $\hat{\tilde{\alpha}}_l = \tilde{\alpha}_l$ , obtenus dans l'équation (II.1.9). Pour cela, nous relevons le SER en fonction du nombre de candidats normalisé,  $N_c^{norm} = N_c/M$ , de  $1/M$  à 1.  $N_c^{norm} = 1$  correspond à LoRa RAKE classique où les  $M$  candidats sont retenus (courbes avec le type de ligne '-' sur la figure) et  $N_c^{norm} = 1/M$  correspond à avoir un seul candidat et une réduction de complexité calculatoire maximale.

D'après la Figure II.2.3, nous remarquons que pour  $N_c^{norm} < 0.1$ , les performances sont dégradées, quelque soit la valeur du SNR et de SF. La convergence vers les performances optimales est atteinte rapidement et plus rapide pour SF plus grand. En effet, pour  $SF = 10$ , la convergence est atteinte à partir de  $N_c^{norm} \approx 0.4$ , contre  $N_c^{norm} \approx 0.7$  pour  $SF = 7$ . Ainsi, le gain de réduction de complexité calculatoire sera plus important pour SF grand.

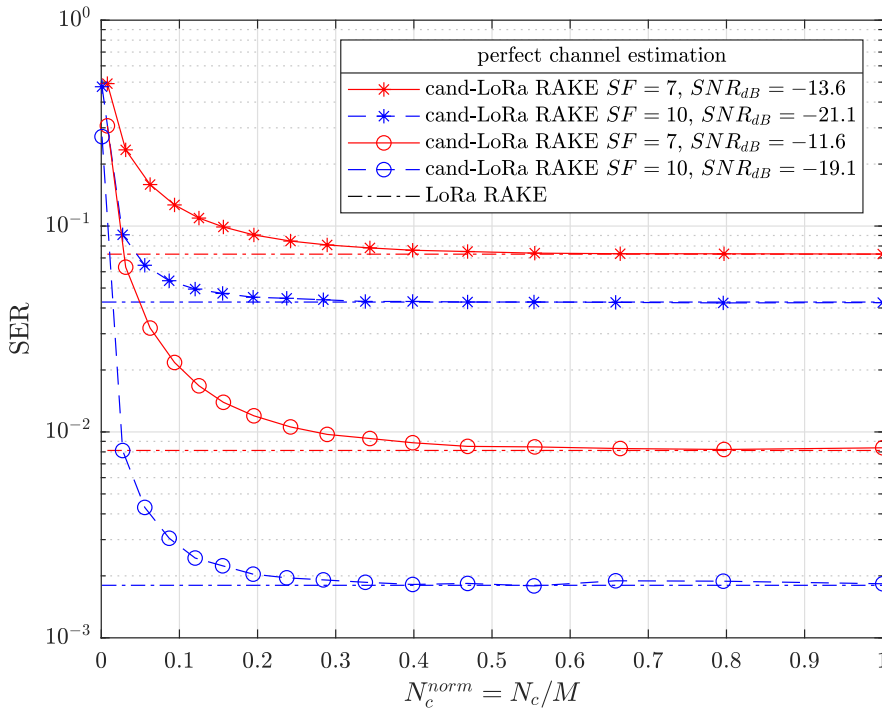


FIGURE II.2.3. – Impact du nombre de candidats sur le SER de cand-LoRa RAKE,  $SF = 7$  et  $SF = 10$

### II.2.2.3.3. Gain de réduction de complexité calculatoire LoRa RAKE avec candidats

La Figure II.2.4 montre le pourcentage de réduction du nombre de candidats d-cand-LoRa RAKE, défini par :

$$N_c^{mean,norm} = 100 \times (1 - N_c^{mean}/M) \quad (II.2.13)$$

en fonction du SNR, et pour plusieurs valeurs de seuil  $\lambda_{cand} \in \{0.2, 0.3, 0.4, 0.5, 0.6\}$  et  $SF = 7$ .

D'après la figure, nous constatons que plus le SNR augmente, plus le nombre de candidats sélectionnés diminue, pour atteindre le niveau minimal  $N_c^{mean,norm} = 1 - 2/M \approx 98.4\%$  quelque soit la valeur de  $\lambda_{cand}$ , soit les deux trajets du canal  $C_1$ . Plus  $\lambda_{cand}$  est faible, plus le nombre de candidats est élevé. Nous avons par exemple à  $SNR_{dB} = -8$  une réduction  $N_c^{mean,norm} \approx 43.8\%$  (environ 70 candidats) pour  $\lambda_{cand} = 0.2$  contre  $N_c^{mean,norm} \approx 97.7\%$  (environ 3 candidats) pour  $\lambda_{cand} = 0.6$ . Ainsi, plus le SNR sera favorable, plus le gain de réduction de complexité calculatoire sera intéressant, pour des performances s'améliorant progressivement.

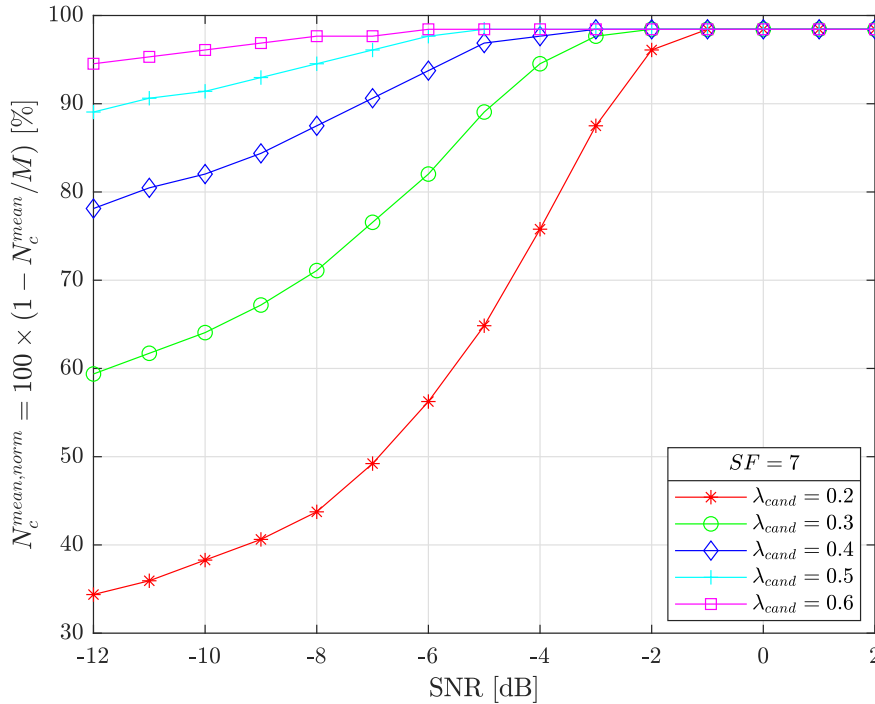


FIGURE II.2.4. – Pourcentage de réduction moyen du nombre de candidats d-cand-LoRa RAKE sélectionnés en fonction du SNR pour plusieurs valeurs de seuil  $\lambda_{cand}$ ,  $SF = 7$

### II.2.2.3.4. Comparaison des performances SER entre LoRa RAKE, d-cand-LoRa RAKE, TDEL et les récepteurs classiques

La Figure II.2.5 compare les performances SER dans le canal  $C_1$  entre LoRa RAKE, d-cand-LoRa RAKE, TDEL et les récepteurs classiques, pour  $\lambda_{path} = 0.4$  (valeur donnant de très bonnes performances, voir Figure II.2.5), avec synchronisation parfaite, et  $SF = 7$ .



## II.2. Récepteur amélioré LoRa RAKE

Pour TDEL, nous choisissons la même valeur  $\lambda_{TDEL} = 0.2$  que pour les résultats présentés dans l'article [69]. Les récepteurs classiques sont ceux cohérent (équation (I.2.14)) et non-cohérent (équation (I.2.13)) dans le canal multi-trajets, et cohérent dans un canal plat AWGN. Pour ce dernier, afin d'avoir une comparaison équitable avec les autres récepteurs, la puissance de l'unique trajet est identique à celle du canal  $C_1$ , i.e.  $\alpha_0^{AWGN} = \sqrt{(\alpha_0)^2 + (\alpha_1)^2} = \sqrt{1 + 0.8^2} \approx 1.28$ . Ainsi, il représente les performances optimales, comme constaté sur la figure, et est équivalent au démodulateur cand-LoRa RAKE dans ce canal plat AWGN avec une estimation parfaite du coefficient. Pour d-cand-LoRa RAKE, nous affichons ses performances pour  $\lambda_{cand} = 0.3$  et  $\lambda_{cand} = 0.5$ .

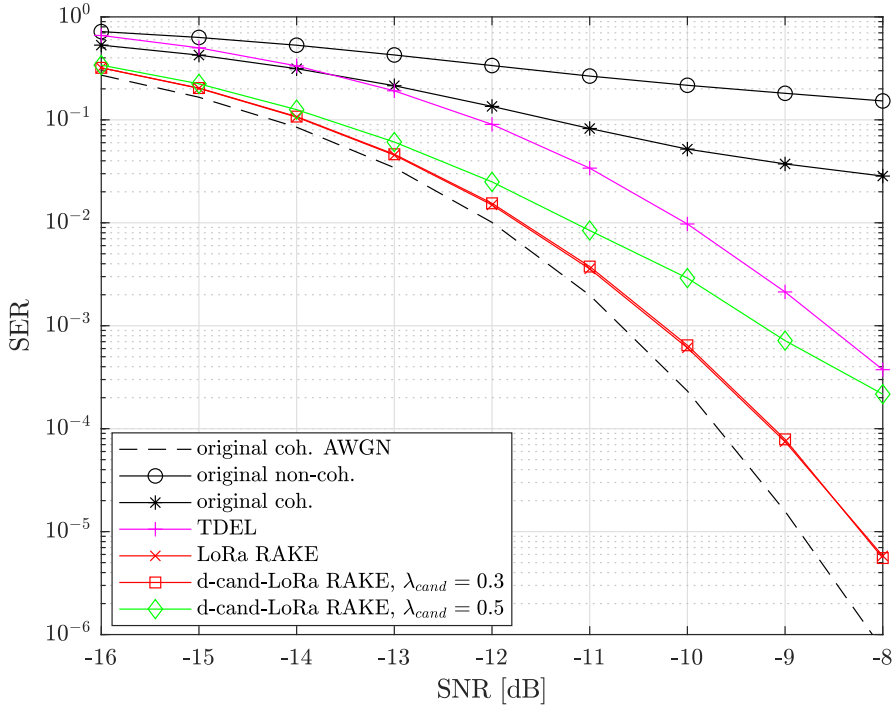


FIGURE II.2.5. – Comparaison des performances SER entre LoRa RAKE, d-cand-LoRa RAKE, TDEL et les récepteurs classiques dans un canal multi-trajets aligné avec synchronisation parfaite,  $SF = 7$

D'après la Figure II.2.5, nous remarquons tout de suite que LoRa RAKE donne de meilleures performances que TDEL, avec un gain de l'ordre de 1.6 dB à  $SER = 10^{-3}$ . Cela est possible grâce à la nature cohérente de LoRa RAKE, contrairement à TDEL où la composante de bruit AWGN est renforcée lors de la démodulation. Nous voyons aussi que LoRa RAKE et d-cand-LoRa RAKE ( $\lambda_{cand} = 0.3$ ) ont pratiquement les mêmes performances. Ainsi,  $\lambda_{cand} = 0.3$  est une valeur bien choisie, donnant des performances très proches de celles optimales LoRa RAKE. De plus, la perte par rapport au cas AWGN idéal est très raisonnable, environ 0.7 dB à  $SER = 10^{-5}$ . La dégradation de performances par rapport à LoRa RAKE est beaucoup plus marquée pour d-cand-LoRa RAKE utilisant  $\lambda_{cand} = 0.5$ , surtout à SNR favorable ( $SNR_{dB} \geq -10$ ), où la perte s'amplifie (environ 1 dB à  $SER = 10^{-3}$  contre plus de 1.5 dB à  $SER = 10^{-4}$ ). Les récepteurs classiques dans le canal multi-trajets ont des performances très mauvaises ( $SER > 10^{-2}$ ), du fait de la présence du second trajet vu comme une interférence pour ces récepteurs. Notons que le récepteur classique cohérent conserve tout de même de meilleures performances.

### II.2.3. Démodulation LoRa RAKE dans un canal multi-trajets non-aligné à deux trajets avec synchronisation temporelle et fréquentielle

Le Tableau II.2.1 reporte le pourcentage de réduction moyen du nombre de candidats sélectionnés par d-cand-LoRa RAKE ( $N_c^{mean, norm}$  dans l'équation (II.2.13)), pour les valeurs de seuil  $\lambda_{cand}$  et de SNR considérés sur la Figure II.2.5 ( $\lambda_{cand} \in \{0.3, 0.5\}$ ,  $SNR_{dB} \in \{-16, -15, \dots, -8\}$  et  $SF = 7$ ). Nous constatons bien la réduction importante du nombre de candidats. Pour  $\lambda_{cand} = 0.3$ , la réduction est d'environ 55.5% à  $SNR_{dB} = -16$  et augmente pour des valeurs de SNR plus élevées, pour atteindre 71% à  $SNR_{dB} = -8$ . Choisir  $\lambda_{cand} = 0.5$  permet de réduire encore la complexité calculatoire. Nous avons en effet une réduction supérieure à 86%, mais au prix d'une baisse de performances en termes de SER.

SNR [dB]	-16	-15	-14	-13	-12	-11	-10	-9	-8
$\lambda_{cand} = 0.3$	55.5	56.3	57.0	58.6	59.4	61.7	64.1	67.2	71.1
$\lambda_{cand} = 0.5$	86.7	87.5	88.3	88.9	89.1	90.6	91.4	93.0	94.5

TABLE II.2.1. – Pourcentage de réduction moyen du nombre de candidats de d-cand-LoRa RAKE en fonction du SNR pour deux valeurs de seuil  $\lambda_{cand}$ ,  $SF = 7$

### II.2.3. Démodulation LoRa RAKE dans un canal multi-trajets non-aligné à deux trajets avec synchronisation temporelle et fréquentielle

Dans cette section, nous présentons l'extension du récepteur LoRa RAKE pour le scénario plus réaliste où nous prenons en compte 1) un canal multi-trajets ayant une réplique non-alignée de magnitude forte et proche du trajet direct et 2) la synchronisation temporelle STO et fréquentielle CFO. L'objectif est également d'évaluer lequel de LoRa RAKE ou TDEL donne les meilleures performances SER en fonction des conditions du canal multi-trajets et du SNR. Dans l'étude, nous considérons uniquement LoRa RAKE puisque les récepteurs f-cand-LoRa RAKE et d-cand-LoRa RAKE ont été présentés en détail dans notre article [92] et pourraient être ré-utilisés dans le contexte d'un canal multi-trajets non-aligné. Les travaux ont été soumis dans l'article *A RAKE-like coherent LoRa receiver for Non-Aligned Multi-Path Channels* dans la revue *IEEE Transactions on Wireless Communications* [93].

Dans [93], nous nous concentrons sur le canal multi-trajets non-aligné à deux trajets i.e.  $L = 2$  ayant une réplique significative i.e.  $|\alpha_1| \geq 0.2$ , de retard inférieur à celui d'une période d'échantillonnage LoRa i.e.  $k_1 < 1$ . Pour un canal multi-trajets ayant plus que deux trajets ( $L > 2$ ), les répliques de faible magnitude ( $|\alpha_l| < 0.2$ ) ont un faible impact, comme mis en évidence en Section II.1.3.2. Nous exprimons l'écart relatif de phase entre les deux trajets par :

$$\Delta_\phi = \phi_1 - \phi_0 = \phi_1 \in [0; 2[ \quad (\text{II.2.14})$$

Nous nous intéressons à répondre aux questions suivantes :

- Quel est l'impact du canal multi-trajets non-aligné à deux trajets sur la DFT LoRa ?

## II.2. Récepteur amélioré LoRa RAKE

- Quelles sont les performances de LoRa RAKE dans un canal multi-trajets non-aligné à deux trajets ?
- Comment le canal multi-trajets non-aligné à deux trajets impacte la synchronisation et donc les performances ?
- Lequel de LoRa RAKE ou TDEL donne les meilleures performances en fonction des conditions du canal multi-trajets et du SNR ?

### II.2.3.1. Modification du démodulateur LoRa RAKE

Dans le cas du canal multi-trajets non-aligné à deux trajets, le récepteur fait l'hypothèse que seuls deux trajets significatifs sont présents, avec une réplique non-alignée proche du trajet direct. Il peut donc supposer que l'énergie du canal multi-trajets n'est présente uniquement qu'aux bins  $n = a_i$  et  $n = (a_i - 1) \bmod M$  (synchronisation parfaite). Le récepteur peut adopter les deux stratégies suivantes :

- Exploiter l'énergie du canal multi-trajets contenue dans le bin principal  $n = a_i$  et celle éventuellement contenue dans le bin voisin direct  $n = (a_i - 1) \bmod M$ . Nous notons  $F$ , le nombre de bins à exploiter dans la DFT. Ici,  $F = 2$ .
- Uniquement exploiter l'énergie du bin principal  $n = a_i$  ( $F = 1$ ). Cette solution peut paraître sous-optimale : toute l'énergie du canal multi-trajets potentielle n'est pas exploitée. Cependant, il sera montré qu'en fonction des paramètres  $k_1$  et  $\Delta_\phi$ , cette solution peut-être tout de même intéressante.

Du fait du caractère non-aligné du canal multi-trajets, les gains complexes estimés dans la DFT ne seront pas les mêmes que ceux théoriques pour le canal multi-trajets aligné i.e.  $\hat{\alpha}_i \neq \tilde{\alpha}_i$ , si  $k_1 < 1$ . Nous notons ce gain par  $\hat{\gamma}_l$  pour bien différencier. Le récepteur LoRa RAKE devient alors pour  $F = 2$  :

$$T_i[a'] = \hat{V}_i^{(0)}[a'] + \hat{V}_i^{(1)}[a'] \quad (\text{II.2.15})$$

avec :

$$\hat{V}_i^{(0)}[a'] = \hat{\gamma}_0^* \tilde{R}_i[a'], \quad \hat{V}_i^{(1)}[a'] = \hat{\gamma}_1^* e^{2j\pi \frac{a'}{M}} \tilde{R}_i[(a' - 1) \bmod M] \quad (\text{II.2.16})$$

$$\hat{\gamma}_0 = \frac{\langle \tilde{P}_{non-aligned}[0] \rangle}{M}, \quad \hat{\gamma}_1 = \frac{\langle \tilde{P}_{non-aligned}[M - 1] \rangle}{M - 1} \quad (\text{II.2.17})$$

et  $\langle \tilde{P}_{non-aligned}[n] \rangle$ , la DFT des symboles upchirp de préambule moyennés, déformés par le canal multi-trajets non-aligné. Pour la première stratégie ( $F = 1$ ), LoRa RAKE se réduit simplement par :

$$T_i[a'] = \hat{V}_i^{(0)}[a'] = \hat{\gamma}_0^* \tilde{R}_i[a'] \quad (\text{II.2.18})$$

La Figure II.2.6 montre un exemple de démodulation LoRa RAKE pour un canal multi-trajets non-aligné à deux trajets, pour  $|\alpha_1| = 0.8$ ,  $a^- = a$ , et plusieurs combinaisons de  $k_1$  et  $\Delta_\phi$  avec  $k_1 \in \{0.2, 0.5, 0.8\}$  et  $\Delta_\phi \in \{0, 0.5, 1\}$ . La figure est obtenue en développant l'équation (II.2.15) et utilisant les équations (E.35) à (E.42) en Annexe E. Il n'y a pas de bruit AWGN. D'après la figure, si la réplique est proche du trajet principal ( $k_1$  faible) et

### II.2.3. Démodulation LoRa RAKE dans un canal multi-trajets non-aligné à deux trajets avec synchronisation temporelle et fréquentielle

en opposition de phase ( $\Delta_\phi \approx 1$ ), alors il y a addition destructive et la démodulation sera très fortement impactée. Pour  $k_1 = 0.2$  et  $\Delta_\phi = 1$ , le pic n'a qu'une amplitude d'environ 12.6, contre presque 400 lorsque le canal est favorable ( $k_1 = 0.2$  et  $\Delta_\phi = 0$ ).

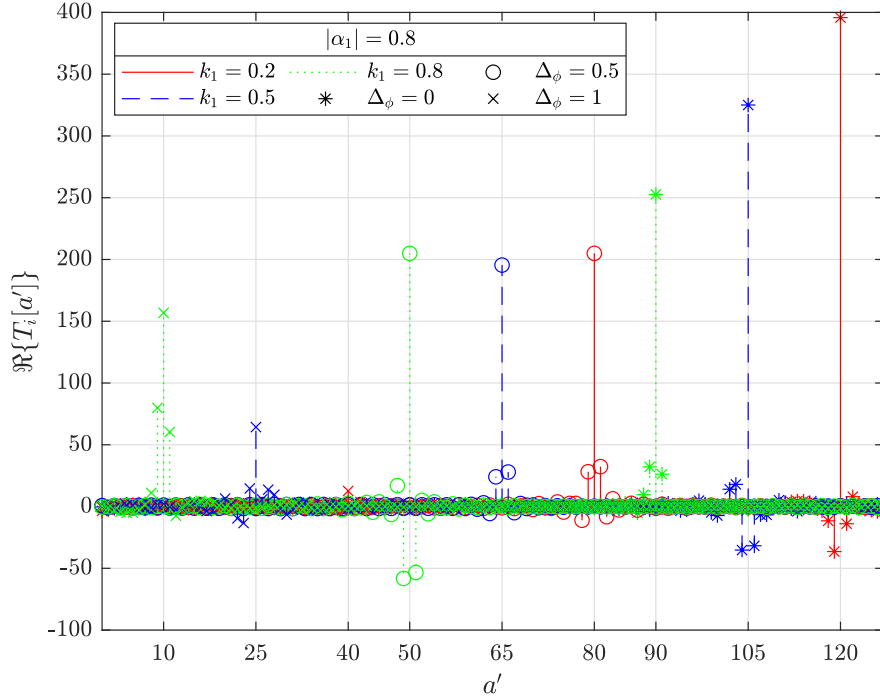


FIGURE II.2.6. – Exemples de démodulation LoRa RAKE dans un canal multi-trajets non-aligné à deux trajets

La Figure II.2.7 présente l'évolution de l'estimation des gains complexes  $|\tilde{\gamma}_0|$  et  $|\tilde{\gamma}_1|$  en fonction de  $k_1 \in \{0, 0.1, \dots, 1\}$  pour plusieurs valeurs  $\Delta_\phi \in \{0, 0.5, 0.6, 1\}$  et  $|\alpha_1| = 0.8$ . Nous affichons également les coefficients estimés  $|\tilde{\alpha}_0|$  et  $|\tilde{\alpha}_1|$  dans le cas du canal multi-trajets aligné ( $k_1 = 0$  et  $k_1 = 1$ ).

Nous remarquons que :

- $|\tilde{\gamma}_1|$  ne dépend pas de  $\Delta_\phi$ . Plus  $k_1$  croît, plus de l'énergie est présente dans le bin voisin et donc  $|\tilde{\gamma}_1|$  croît aussi. Nous avons égalité ( $|\tilde{\gamma}_0| = |\tilde{\alpha}_0|$  et  $|\tilde{\gamma}_1| = |\tilde{\alpha}_1|$ ) si  $k_1 = 0$  et  $k_1 = 1$ , respectivement.
- En revanche,  $|\tilde{\gamma}_0|$  dépend de  $\Delta_\phi$ . Plus  $\Delta_\phi$  augmente, plus de l'énergie du canal est perdue, avec les cas les plus favorables  $\Delta_\phi = 0$  et  $\Delta_\phi = 1$ , respectivement. Par exemple, pour  $k_1 = 0$  et  $\Delta_\phi = 0$ , nous avons  $|\tilde{\gamma}_0| = |\alpha_0| + |\alpha_1| = 1 + 0.8 = 1.8$ . Pour  $k_1 = 0$  et  $\Delta_\phi = 1$ , nous avons  $|\tilde{\gamma}_0| = |\alpha_0| - |\alpha_1| = 1 - 0.8 = 0.2$ . Notons que plus  $\Delta_\phi$  se rapproche de 0.6, moins la perte d'énergie est sensible à  $k_1$ .

La Figure II.2.8 montre, quant à elle, l'évolution de l'énergie du bin d'intérêt LoRa RAKE  $\Re\{T_i[a'] = a\}$  en fonction de  $k_1 \in \{0, 0.1, \dots, 1\}$  et  $\Delta_\phi \in \{0, 0.025, \dots, 1\}$  pour  $|\alpha_1| = 0.8$ ,  $a^- = a$  et  $SF = 7$ . Elle est obtenue en développant l'équation (II.2.18) et utilisant les équations (E.44), (E.45) et (E.47) en Annexe E. Avoir  $a^- \neq a$  n'influe que très peu le résultat car l'ISI engendrée par le canal multi-trajets est faible avec  $k_1 \leq 1$ . Nous avons aussi ajouté le contour représentant l'énergie contenue dans le bin d'intérêt LoRa RAKE équivalent au récepteur cohérent classique utilisé dans un canal plat AWGN ( $\Re\{T_i[a]\} = \Re\{\tilde{R}_i[a]\} = M$ ).

## II.2. Récepteur amélioré LoRa RAKE

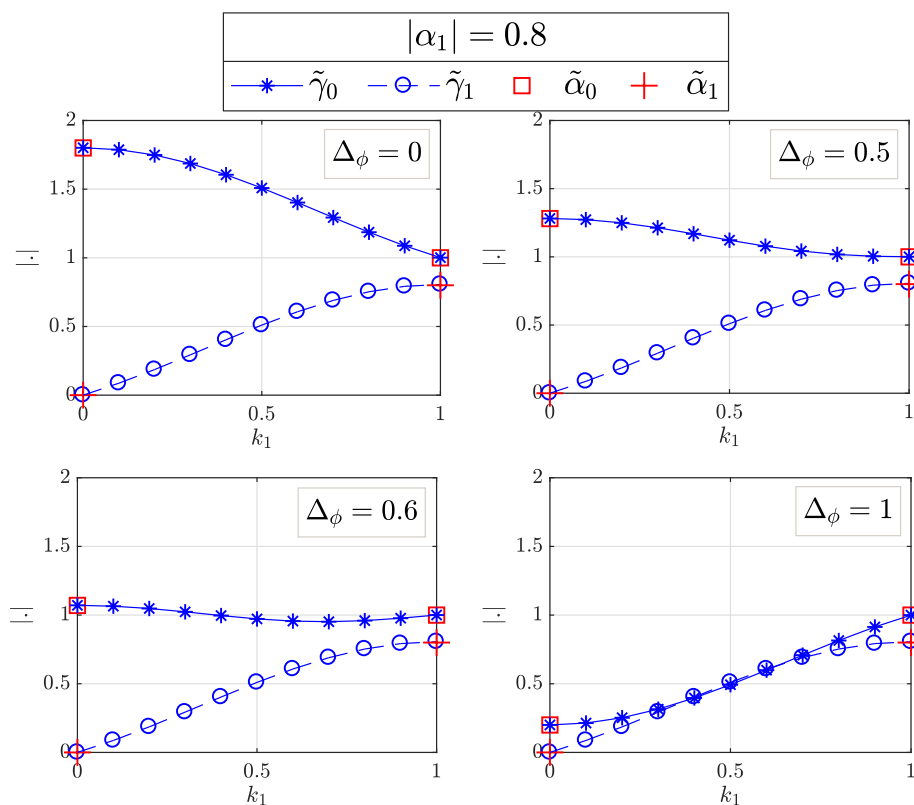


FIGURE II.2.7. – Évolution de l'estimation des gain complexes en fonction des paramètres du canal multi-trajets non-aligné

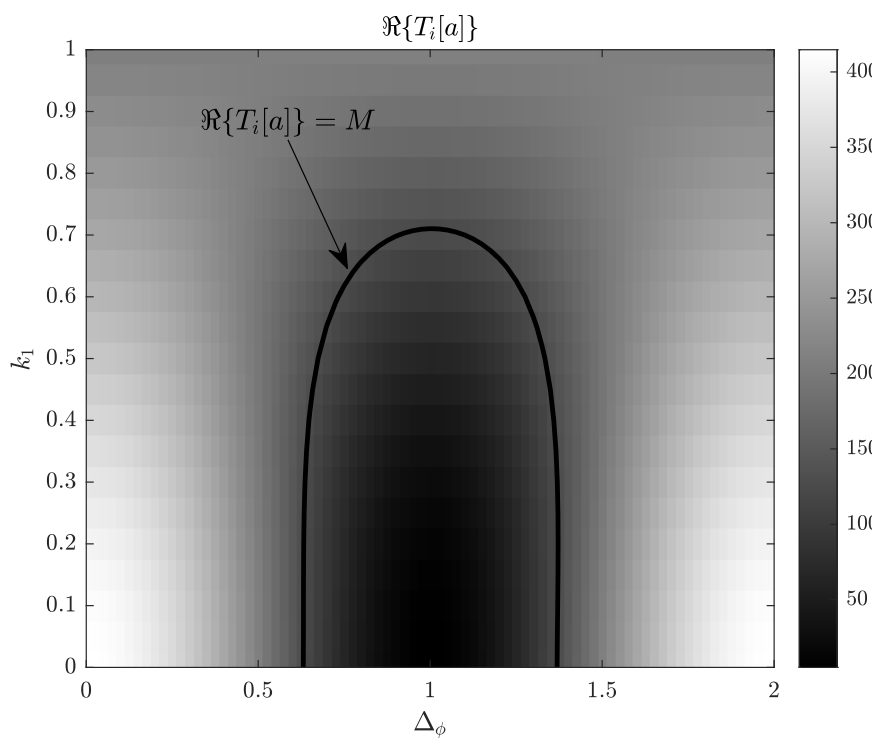


FIGURE II.2.8. – Évolution de l'énergie du bin d'intérêt LoRa RAKE en fonction des paramètres du canal multi-trajets non-aligné

Nous retenons les principaux comportements suivants :

- L'évolution est symétrique autour de  $\Delta_\phi = 1$ . Ainsi, nous nous attendons à ce que les performances SER soient symétriques :  $SER(\Delta_\phi = b) = SER(\Delta_\phi = 2 - b)$ .
- Le cas le plus favorable est lorsque  $k_1 \approx 0$  et  $\Delta_\phi \approx 0$ , où il y a une interférence pleinement constructive.
- Le cas le plus défavorable est lorsque  $k_1 \approx 0$  et  $\Delta_\phi \approx 1$ , où il y a une interférence pleinement destructive.
- Pour  $k_1 \approx 0$ , augmenter  $\Delta_\phi$  diminue progressivement l'énergie. Plus  $k_1$  augmente, plus cette dégradation disparaît, avec une énergie quasiment uniforme lorsque  $k_1 = 1$ .
- Pour  $\Delta_\phi$  fixé, augmenter  $k_1$  diminue progressivement l'énergie, sauf si  $0.6 \leq \Delta_\phi \leq 1.4$ .

### II.2.3.2. Synchronisation LoRa RAKE– compensation de la dérive de phase

La synchronisation  $CFO_{frac}$  n'étant pas parfaite, un résidu est présent lors de la démodulation des symboles payload. Il s'exprime par :

$$CFO_{frac}^r = CFO_{frac} - \widehat{CFO}_{frac} \quad (\text{II.2.19})$$

Ce résidu a pour effet d'engendrer une dérive de phase croissante dans le temps et s'exprime pour la DFT LoRa par :

$$\tilde{R}_i^{CFO_{frac}^r}[n] \approx \tilde{R}_i[n] \times e^{2j\pi i CFO_{frac}^r n} \quad (\text{II.2.20})$$

Ainsi, pour tout récepteur cohérent comme LoRa RAKE, une compensation de phase est nécessaire, là où un récepteur non-cohérent comme TDEL sera insensible. La Figure II.2.9 montre l'évolution de l'énergie du bin d'intérêt (composante réelle) au cours du temps pour le cas parfaitement synchronisé ( $CFO_{frac}^r = 0$ ) et pour deux valeurs de résidu  $CFO_{frac}^r \in \{0.01, 0.04\}$  et  $SF = 7$ . Nous observons que la perte d'énergie est très rapide, avec une opposition de phase atteinte dès le 12<sup>ème</sup> symbole pour  $CFO_{frac}^r = 0.04$ , une valeur de résidu portant assez bonne en pratique.

Dans [93], nous avons développé un algorithme simple de compensation de phase et donnant d'assez bonnes performances. Dans cet algorithme, nous estimons avec LoRa RAKE pour chaque symbole de payload la dérive de phase constatée depuis le symbole précédent (dérive de phase cumulative). L'algorithme est présenté en algorithme 1 et comporte deux étapes principales :

1. La dérive de phase est d'abord estimée à partir du dernier symbole downchirp de préambule (lignes 2 et 3 dans l'algorithme). Cela a l'avantage d'offrir une lecture de phase robuste. En effet, pour lire correctement la phase, le bin d'intérêt dans la DFT doit être extrait de façon efficace. C'est le cas ici où la position de ce dernier est parfaitement connue dans le préambule ( $a = 0$ ), à condition que la synchronisation  $CFO_{int}$  et  $STO_{int}$  soit bonne. De plus, la dérive de phase relative avec le premier symbole payload sera faible ( $\beta = CFO_{frac}^r$ ), impactant faiblement LoRa RAKE.
2. Pour chaque symbole payload, la phase totale est d'abord corrigée dans la DFT (lignes 6 et 7), puis le bin d'intérêt est estimé (lignes 8 et 9) et enfin la phase du symbole courant est lue (ligne 10).

## II.2. Récepteur amélioré LoRa RAKE

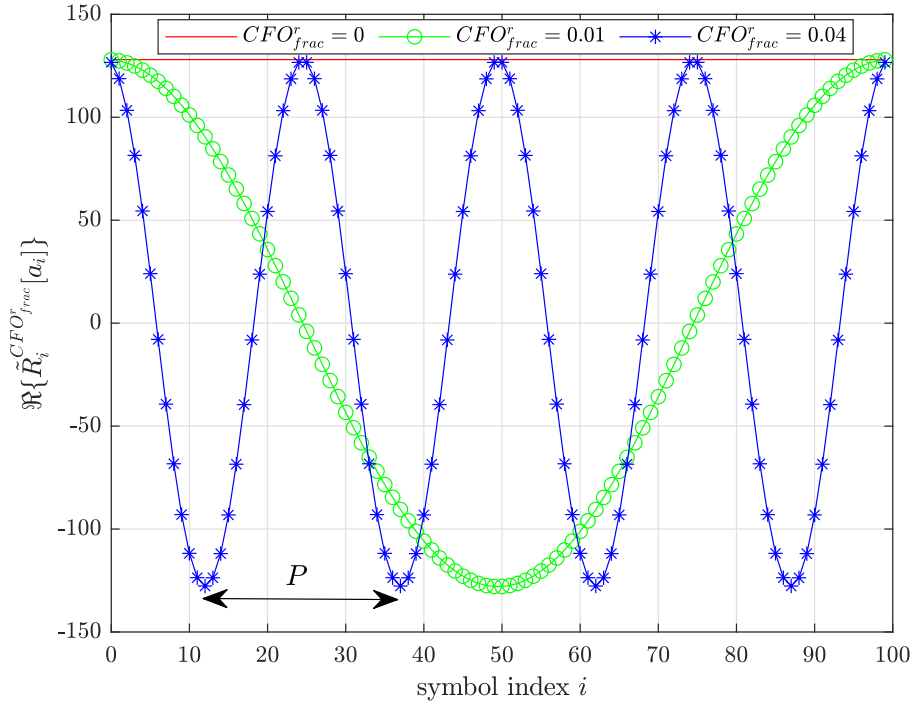


FIGURE II.2.9. – Évolution au cours du temps de l'énergie du bin d'intérêt (composante réelle) pour plusieurs résidus  $CFO_{frac}$ ,  $SF = 7$

---

**Algorithm 1:** Algorithme de compensation de phase  $CFO_{frac}$  et de démodulation LoRa RAKE ( $F = 1$  ou  $F = 2$ )

---

**inputs:**  $\{\tilde{\mathbf{R}}_i\}_{i=0}^{N_d-1}$  %DFT des symboles reçus mises en vecteurs (dernier symbole downchirp ( $i = 0$ ) et symboles payload ( $i \in \{1, 2, \dots, N_d\}$ ),  $\hat{\gamma}_0$  et  $\hat{\gamma}_1$  (seulement si  $F = 2$ ) %coefficients complexes du canal multi-trajets estimés dans l'équation (II.2.17)

- 1  $\hat{\mathbf{a}} := \mathbf{0}_{N_d}$  initialisation vecteur de taille  $N_d$
- 2 compute  $\mathbf{T}_0[0]$  %Équation (II.2.15) ( $F = 2$ ) ou équation (II.2.18) ( $F = 1$ )
- 3  $\hat{\beta} = \text{angle}(\mathbf{T}_0[0])$  % estimation phase  $CFO_{frac}$  dans le dernier symbole downchirp préambule
- 4  $\hat{\beta}_{cum} = 0$
- 5 **for**  $i = 1$  to  $N_d - 1$  **do**
- 6      $\hat{\beta}_{cum} := \hat{\beta}_{cum} + \hat{\beta}$  %phase cumulative  $CFO_{frac}$
- 7      $\tilde{\mathbf{R}}_i := \tilde{\mathbf{R}}_i \times e^{-j\hat{\beta}_{cum}}$  %compensation de phase cumulative  $CFO_{frac}$  en corrigeant tout le vecteur  $\tilde{\mathbf{R}}_i$
- 8     compute  $\mathbf{T}_i[a'] \forall a'$  %Équation (II.2.15) ou équation (II.2.18)
- 9      $\hat{\mathbf{a}}[i] := \arg \max_{a'} \Re\{\mathbf{T}_i[a']\}$  démodulation dans l'équation (II.2.10)
- 10      $\hat{\beta} := \text{angle}(\mathbf{T}_i[\hat{\mathbf{a}}[i]])$
- 11 **return**  $\hat{\mathbf{a}}$

---

Cet algorithme est assez léger puisque la correction de phase et l'estimation du symbole se font de manière conjointe dans la même itération. Les performances de cette solution sont présentées en Figure II.2.10 dans la Section II.2.3.3.1.

### II.2.3.3. Résultats de simulation

Dans cette section, nous présentons les performances de LoRa RAKE : celles du schéma de compensation de phase  $CFO_{frac}$  présenté en Section II.2.3.2 et celles en termes de SER, avec ou sans synchronisation parfaite. Nous utilisons les paramètres de simulation suivants :

- $SF = 7$ .
- $N_{up} = N_{down} = 8$ , pour l'estimation de  $CFO_{int}$  et  $STO_{int}$  dans le front-end de synchronisation.
- Le récepteur LoRa RAKE peut adopter les deux stratégies de choisir  $F = 2$  ou  $F = 1$ , en équations (II.2.15) et (II.2.18), respectivement.
- Le canal multi-trajets a les paramètres  $|\alpha_1| = 0.8$  et les deux valeurs  $k_1 = 0.1$  et  $k_1 = 0.9$ . Ces deux valeurs représentent les cas extrêmes de performances optimales et défavorables.
- $B = 125$  kHz et  $F_c = 868.1$  MHz, pour l'estimation du SFO dans le front-end de synchronisation.
- $\lambda_{TDEL} = 0.2$ , pour le récepteur TDEL (voir équations (II.2.2) et (II.2.3)), comme utilisé dans [69].
- $R = 10$ , pour les simulations du canal multi-trajets non-aligné, de  $STO_{frac}$  et pour la correction de  $STO_{frac}$  dans le front-end de synchronisation.
- $CFO \in [0; M/4 - 1]$  (voir Section I.2.6.3.3) et  $STO \in [0; M - 1]$ .

#### II.2.3.3.1. Performances de l'algorithme de compensation de phase $CFO_{frac}$

La Figure II.2.10 présente les performances du schéma de compensation de phase  $CFO_{frac}$  avec ou sans résidu  $CFO_{frac} = 0.03$  ( $CFO_{int} = STO_{int} = SFO = 0$ ) et  $SF = 7$ . D'après la figure, nous pouvons remarquer :

- Sans correction de phase (courbe avec marqueur triangle), le récepteur ne peut pas fonctionner correctement, à cause de la dérive de phase rapide, même pour un faible  $CFO_{frac}$  avec ici  $CFO_{frac} = 0.03$  (voir Figure II.2.9).
- Activer la correction de phase dans le cas désynchronisé fait perdre en performances lorsque  $k_1$  est éloigné ( $k_1 = 0.9$ ), surtout à faible SNR, où nous constatons une perte d'environ 1.2 dB (à  $SER = 10^{-1}$  et  $F \in \{1, 2\}$ ). En effet, à faible SNR, la détection du bin d'intérêt sera fortement impacté (ligne 9 de l'algorithme 1). Ainsi, la phase lue pour le symbole courant sera mauvaise. Cette erreur se répercutera alors sur les symboles suivants. Cependant, ce comportement s'estompera progressivement à mesure que le SNR s'améliore. Les performances convergeront alors vers celles du cas parfaitement synchronisé. Cela est clairement visible sur la figure.
- Comme la majorité de l'énergie du canal est contenue dans le bin  $n = a_i$  lorsque  $k_1 = 0.1$ , LoRa RAKE avec  $F = 1$  donne pratiquement les mêmes performances que LoRa RAKE avec  $F = 2$ . Cependant, lorsque  $k_1 = 0.9$ , une part non négligeable de l'énergie du canal est présente dans le bin voisin  $n = (a_i - 1) \bmod M$ . Ainsi, la présence de ce bin voisin apparaît comme une source d'interférence et dégrade



finalement les performances.

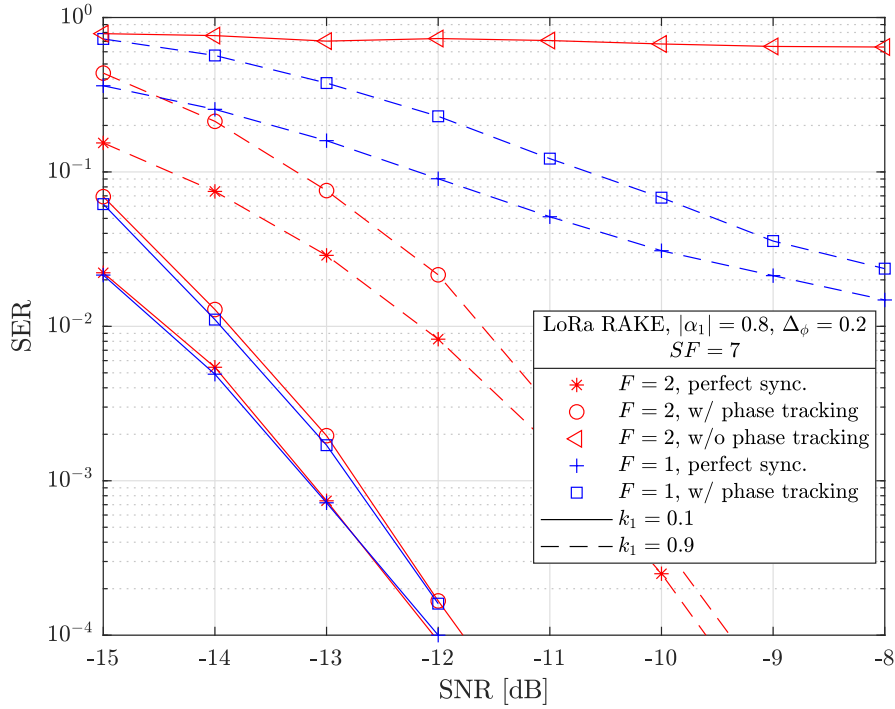


FIGURE II.2.10. – Performances du schéma de correction de phase  $CFO_{frac}$ ,  $SF = 7$

### II.2.3.3.2. Performances dans un canal multi-trajets non-aligné avec ou sans synchronisation parfaite

Les Figures II.2.11 et II.2.12 montrent les performances en termes de SER de LoRa RAKE ( $F = 1$  et  $F = 2$ ), TDEL, et du récepteur classique cohérent en fonction de  $\Delta_\phi$ , pour  $|\alpha_1| = 0.8$  et  $SNR_{dB} = -10$ . Nous considérons le cas de synchronisation parfaite avec  $CFO = STO = SFO = 0$  (Figure II.2.11), et celui réaliste avec synchronisation active (Figure II.2.12) utilisant le front-end de synchronisation présenté en Section I.2.6.3.

Pour le cas parfaitement synchronisé (Figure II.2.11), nous pouvons observer les comportements suivants :

- Pour tous les récepteurs, plus  $\Delta_\phi$  se rapproche de 1, plus les performances se dégradent, surtout si la réplique est proche du trajet direct ( $k_1 = 0.1$ ). Cela est cohérent avec la Figure II.2.8, où la quantité LoRa RAKE est faible et uniforme si  $k_1 \approx 1$  mais élevée et ayant de fortes variations si  $k_1 \approx 0$ .
- Si  $k_1 = 0.1$  (proche de 0), LoRa RAKE avec  $F = 1$  et  $F = 2$  ont exactement les mêmes performances. TDEL montre des performances légèrement moins bonnes que LoRa RAKE et le récepteur classique cohérent, comme attendu, est le moins bon.
- Le gain de LoRa RAKE ( $F = 2$ ) sur TDEL et le récepteur classique cohérent est clairement visible lorsque  $k_1 = 0.9$ . En effet, même dans le cas le plus défavorable  $\Delta_\phi = 1$ , LoRa RAKE donne de meilleures performances que les autres dans le cas le plus favorable  $\Delta_\phi = 0$ , avec  $SER \approx 1.8 \times 10^{-3}$  contre  $SER \approx 5.5 \times 10^{-3}$  (TDEL). Nous

### II.2.3. Démodulation LoRa RAKE dans un canal multi-trajets non-aligné à deux trajets avec synchronisation temporelle et fréquentielle

remarquons que TDEL a des performances intermédiaires, plus proches du récepteur classique cohérent que LoRa RAKE ( $F = 1$ ).

- Pour  $k_1 = 0.9$ , LoRa RAKE ( $F = 1$ ) et le récepteur classique cohérent ont des performances identiques (les moins bonnes), montrant que même si une correction de phase est appliquée au bin d'intérêt  $n = a_i$  pour LoRa RAKE, ce dernier est en fait perturbé par la présence du bin voisin et n'offre aucun gain sur le récepteur classique cohérent.

Activer la synchronisation change le comportement général. Nous pouvons dresser les conclusions suivantes :

- Le récepteur classique cohérent et LoRa RAKE ( $F = 1$ ) sont virtuellement identiques. Cela vient du fait que la correction de phase est appliquée de façon identique entre les deux, et LoRa RAKE ( $F = 1$ ) n'exploite l'énergie que d'un seul bin. Ce dernier est donc équivalent au récepteur classique cohérent.
- Si  $k_1 \approx 0$  ( $k_1 = 0.1$  sur la figure), le comportement reste inchangé pour LoRa RAKE et TDEL. Cela s'explique par le fait que  $k_1 = 0.1$  est une valeur favorable, l'impact du canal multi-trajets sur la synchronisation est faible. Nous constatons une légère baisse de performances due à la synchronisation non parfaite. Par exemple, pour LoRa RAKE ( $F = 1$  ou  $F = 2$ ) et  $\Delta_\phi = 0.6$ , nous avons  $SE_R \approx 5 \times 10^{-3}$  et  $SE_R \approx 10^{-2}$  entre les deux figures. Le gain de LoRa RAKE sur TDEL est légèrement plus faible.
- Lorsque  $k_1 \approx 1$  ( $k_1 = 0.9$  sur la figure), les performances sont très différentes de la Figure II.2.11 :
  - Le gain de LoRa RAKE ( $F = 2$ ) sur TDEL est très fortement réduit si  $\Delta_\phi \leq 0.5$ . Pour  $\Delta_\phi \geq 0.6$ , LoRa RAKE et TDEL sont presque identiques.
  - LoRa RAKE avec  $F = 1$  montre des résultats intéressants. On s'attendrait pour ce dernier à avoir des performances largement moins bonnes que LoRa RAKE ( $F = 2$ ), dans la mesure où une part non négligeable d'énergie du canal dans le bin voisin n'est pas exploitée. Cela n'est pas le cas ici, où les performances sont presque identiques pour  $\Delta_\phi \leq 0.4$ . Cela vient d'un comportement différent concernant les résidus de désynchronisation  $STO_{frac}$ . En effet, le front-end de synchronisation est fortement perturbé quand  $k_1 = 0.9$ , conduisant à des résidus  $STO_{frac}$  plus importants. Les deux récepteurs ne se comportent pas de la même manière. A cause de ce résidu, l'ajout de la quantité du bin voisin  $\hat{V}_i^{(1)}[a']$  dans l'équation (II.2.15) ( $F = 2$ ) conduit à un ajout destructif et la quantité finale  $T_i[a']$  est déformée. Cela dégrade donc les performances.
  - Pour  $0.4 < \Delta_\phi \leq 0.8$ , LoRa RAKE avec  $F = 2$  fonctionne mieux que LoRa RAKE avec  $F = 1$ .
  - Nous pouvons aussi remarquer que LoRa RAKE ( $F = 2$ ) et TDEL ont une légère amélioration des performances pour  $\Delta_\phi = 0.7$ . Ce n'est pas un biais statistique. Une explication possible serait que le couple  $\{\Delta_\phi = 0.7, k_1 = 0.9\}$ , combiné avec l'effet du bruit AWGN, génère statiquement un pic d'intérêt plus fort, réduisant alors les erreurs de synchronisation et/ou de démodulation du payload.

## II.2. Récepteur amélioré LoRa RAKE

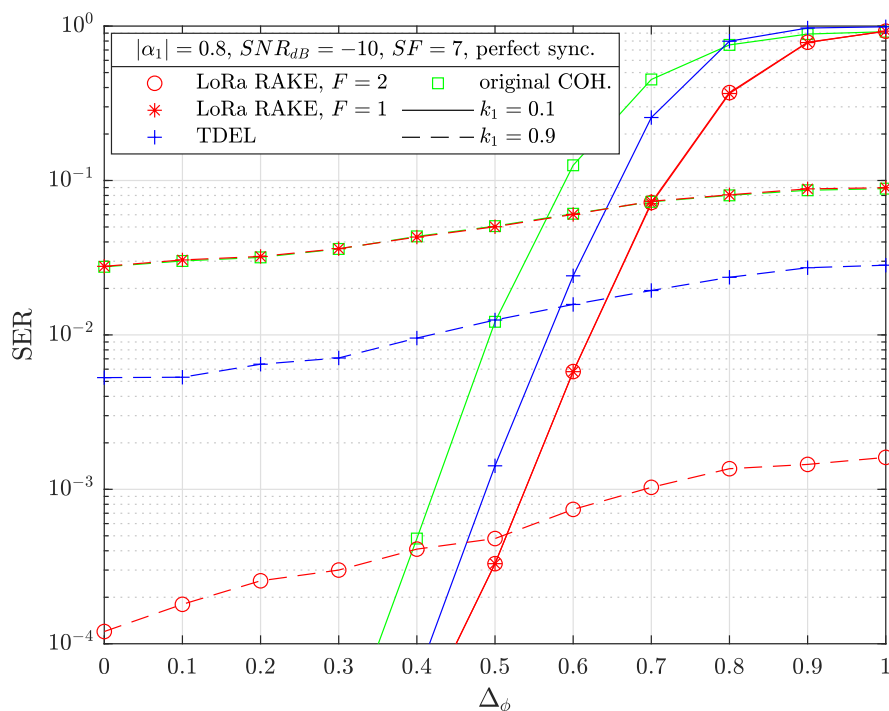


FIGURE II.2.11. – Comparaison des performances SER de LoRa RAKE, TDEL et du récepteur classique cohérent,  $SF = 7$  – synchronisation parfaite

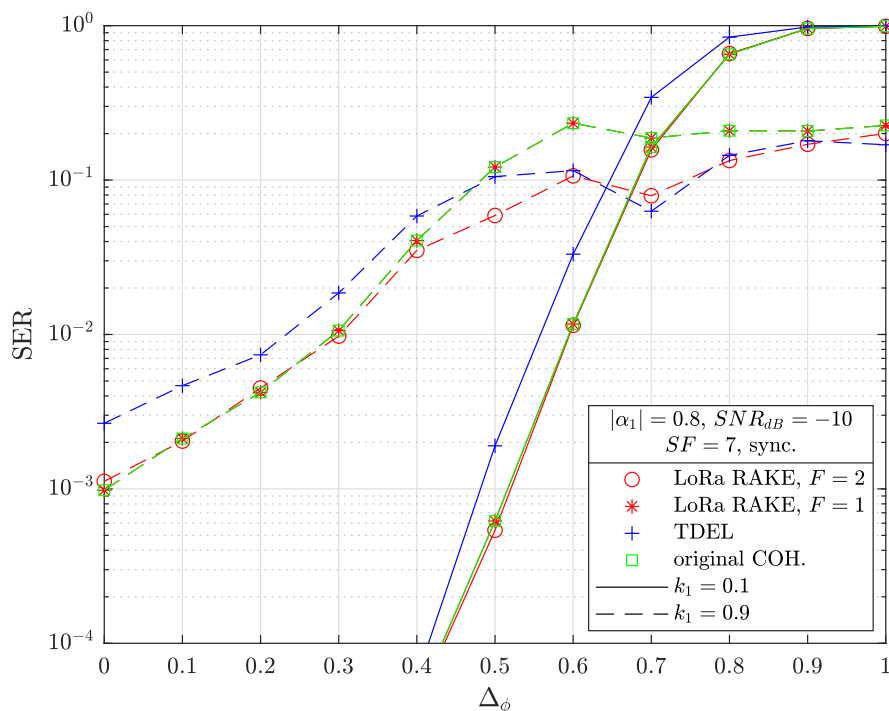


FIGURE II.2.12. – Comparaison des performances SER de LoRa RAKE, TDEL et du récepteur classique cohérent,  $SF = 7$  – front-end de synchronisation activé

La Figure II.2.13 montre pour quelles régions de SNR et de valeurs de  $k_1$ , LoRa RAKE ou TDEL est le plus performant, pour une réplique ayant une magnitude élevée ( $|\alpha_1| = 0.8$ ), pour tout  $\Delta_\phi$ . Nous voyons que LoRa RAKE donne de meilleures performances lorsque le SNR est bas ( $SNR_{dB} \leq -10$ ) et/ou lorsque la réplique est assez proche du trajet direct ( $k_1 \leq 0.4$ ), situation tout à fait probable en pratique. TDEL n'a un gain systématique que pour des SNR plus élevés ( $SNR_{dB} \geq -4$ ) et pour une réplique éloignée ( $k_1 > 0.4$ ), du fait de sa nature non-cohérente.

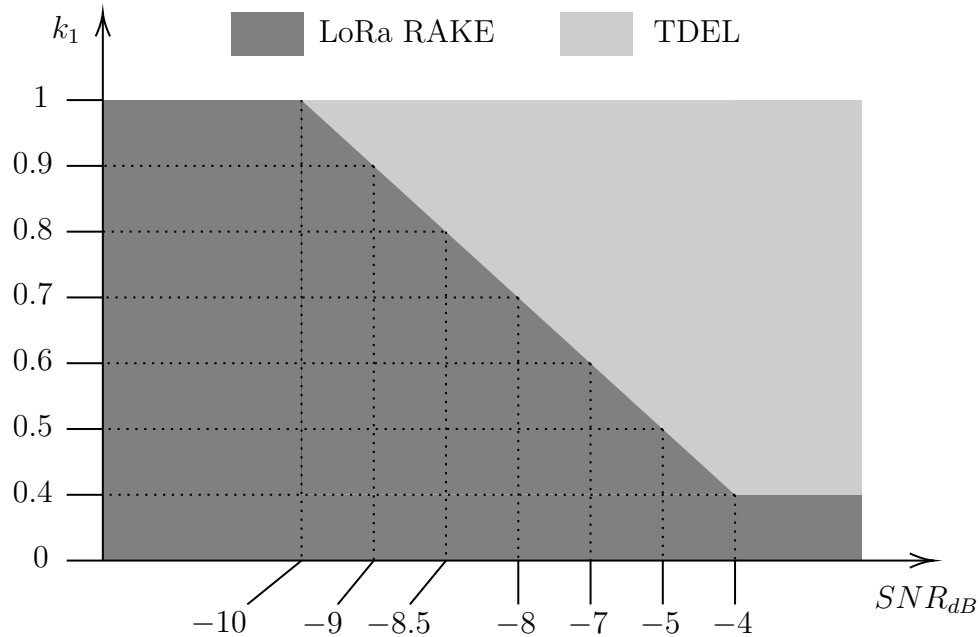


FIGURE II.2.13. – Régions SNR et  $k_1$  de dominance de performances entre LoRa RAKE et TDEL

Pour conclure sur cette section, nous pouvons récapituler les points suivants importants :

- LoRa RAKE a de meilleures performances que TDEL si le SNR est bas et/ou lorsque la réplique est assez proche du trajet direct.
- Les algorithmes de synchronisation LoRa, dans leur état actuel, sont un facteur limitant de performances, pouvant réduire le gain de performances apporté par une approche cohérente telle que LoRa RAKE (voir Figure II.2.12). Nous mettons ainsi en lumière le besoin de travaux supplémentaires sur le développement conjoint d'algorithmes de synchronisation et d'exploitation du canal multi-trajets pour améliorer encore les performances de récepteurs cohérents améliorés comme LoRa RAKE.
- Un récepteur non-cohérent est une solution plutôt équilibrée, avec des performances intéressantes et une complexité calculatoire un peu plus avantageuse qu'un récepteur cohérent.

# Chapitre III

## Brouillage intelligent LoRa

Dans ce chapitre, nous présentons nos contributions portant sur le brouillage intelligent LoRa. Nous replaçons d'abord en Section III.1 le contexte général dans lequel s'applique le brouillage intelligent pour LoRa. Ensuite, nous présentons en Section III.2 notre étude de l'impact des brouilleurs classiques de type Band Jamming (BJ) et Tone Jamming (TJ) sur la démodulation non-cohérente LoRa (article [96]). Enfin, nous présentons en Sections III.3 et III.4 notre schéma d'auto-brouillage proposé (articles [97, 98]), améliorant la confidentialité et la discrétion d'une transmission LoRa, et évalué sur dispositifs matériels de type Software Defined Radio (SDR) en Section III.5.

# III.1. Confidentialité, brouillage et authentification des communications

Dans cette section, nous faisons un rapide tour d’horizon sur les concepts et travaux que l’on peut trouver dans la littérature sur la sécurisation des communications. Nous les présentons selon les trois grands axes de recherche : la confidentialité (Section III.1.1), le brouillage d’attaque (Section III.1.2) et l’authentification (Section III.1.3).

## III.1.1. Confidentialité des communications

La confidentialité a pour but de minimiser le risque d’interception par une entité tierce (intercepteur) d’une information sensible échangée entre deux entités coopératives. Cela peut se traduire par l’échange de coordonnées bancaires, d’informations médicales ou de secret industriel par exemple. Les standards de communication actuels proposent tous des mécanismes sophistiqués de confidentialité, et une grande attention est portée par la communauté scientifique, avec de nombreux travaux proposant de nouvelles solutions alternatives aux méthodes de chiffrement classiques et regroupées sous l’appellation en anglais de *physical layer security*. Dans cette Section, nous introduisons d’abord le scénario de communication (Section III.1.1.1). Ensuite, nous présentons les solutions permettant de garantir la confidentialité (Section III.1.1.2), regroupées en deux familles : la discrétion de la communication (Section III.1.1.2.1) et la dégradation du signal reçu par l’intercepteur (Section III.1.1.2.2).

### III.1.1.1. Scénario de communication

Le scénario considéré est présenté en Figure III.1.1. Il a été proposé en 1975 par Wyner [99], appelé *wiretap channel*, et est aujourd’hui la base de toutes les études sur cet axe de recherche. L’entité ALICE transmet une information sensible (notée X sur la figure) à BOB qui doit être gardée secrète d’une entité tierce, EVE, présente dans le voisinage de ALICE. Y et Z représentent l’information reçue par BOB et EVE à travers leurs canaux respectifs,  $c_{A/B}$  et  $c_{A/E}$ . De plus, EVE est placée à une distance raisonnable de ALICE pour pouvoir détecter a minima la transmission (SNR suffisamment élevé). Deux approches sont possibles pour assurer la confidentialité :

- Rendre l’interception très difficile pour EVE.  
Le signal doit être quasiment indétectable.
- Rendre le signal intercepté difficilement lisible pour EVE.  
Cela revient à dégrader le plus possible le canal  $c_{A/E}$ .

Dans ce qui suit, nous présentons plus en détail ces deux approches.

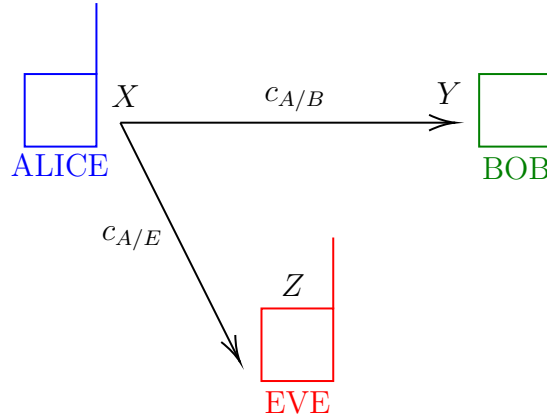


FIGURE III.1.1. – Scénario de communication confidentielle en présence d’un intercepteur

### III.1.1.2. Solutions garantissant la confidentialité

#### III.1.1.2.1. Discrétion de la communication

Dans la littérature, il existe principalement deux approches pour rendre discrète une communication : l’étalement de spectre par séquence d’étalement (Direct Sequence Spread Spectrum (DSSS)) et le saut de fréquence (Frequency Hopping Spread Spectrum (FHSS)) [83]. Les Figures III.1.2 et III.1.3 illustrent le principe du DSSS et du FHSS.

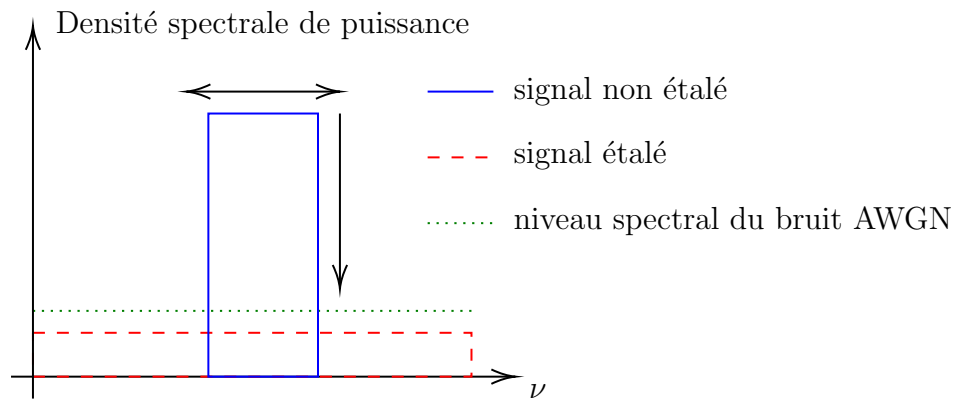
Le DSSS multiplie chaque symbole avec une séquence d’étalement spécifique à chaque utilisateur (Figure III.1.2b). La séquence possède des valeurs dans un ensemble fini (binaires généralement, ici  $\pm 1$ ) et possède une nouvelle valeur à chaque sous-division symbole ou *chip*, de durée  $T_c = T/N$ , avec  $N$ , la longueur de la séquence ou facteur d’étalement et  $T$ , la durée symbole. Cette opération a pour effet d’élargir la bande du signal tout en réduisant son niveau spectral de puissance, d’un facteur de la longueur de la séquence (Figure III.1.2a). Si l’étalement est suffisamment important ( $N$  grand), le signal généré se retrouvera sous le niveau de bruit et sa détection sera alors difficile. La confidentialité est garantie par la non-connaissance stricte de la séquence d’étalement par EVE.

Dans le schéma FHSS, à chaque nouveau symbole, l’émetteur choisit aléatoirement un canal (fréquence porteuse différente, notée  $v_i$  sur la Figure III.1.3) sur lequel émettre. Cela impacte fortement l’intercepteur puisque ce dernier ne peut pas écouter sur tous les canaux en même temps et ne peut pas, en principe, connaître le canal choisi, du fait de l’utilisation de générateurs de séquences pseudo-aléatoires.

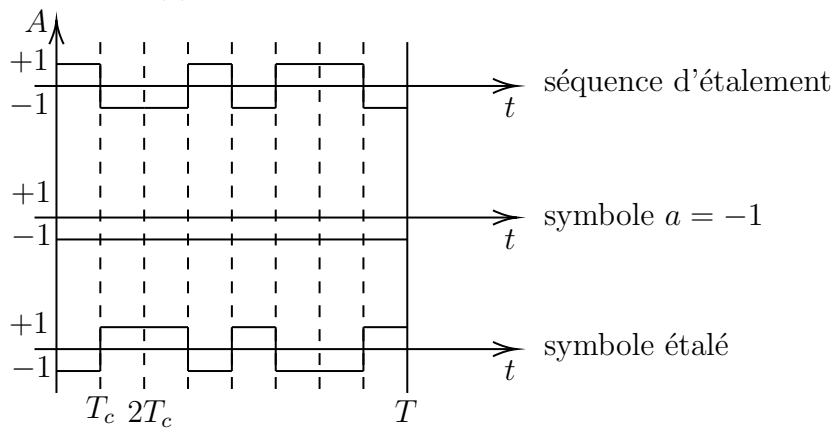
#### III.1.1.2.2. Dégradation du signal reçu par l’intercepteur

Comme les canaux  $c_{A/B}$  et  $c_{A/E}$  ne sont pas parfaits (atténuations, déformations, etc.), l’information  $X$  est donc altérée et on a alors  $Y \neq X$  et  $Z \neq X$ , d’après la Figure III.1.1. La capacité des deux canaux (quantité maximale d’information que l’on peut transmettre à travers le canal pour une probabilité d’erreur arbitrairement faible) est définie par :

$$C_B = \log_2(1 + SNR_B), \quad C_E = \log_2(1 + SNR_E) \quad (\text{III.1.1})$$



(a) Domaine fréquentiel



(b) Domaine temporel

FIGURE III.1.2. – Illustration du principe d'étalement de spectre DSSS

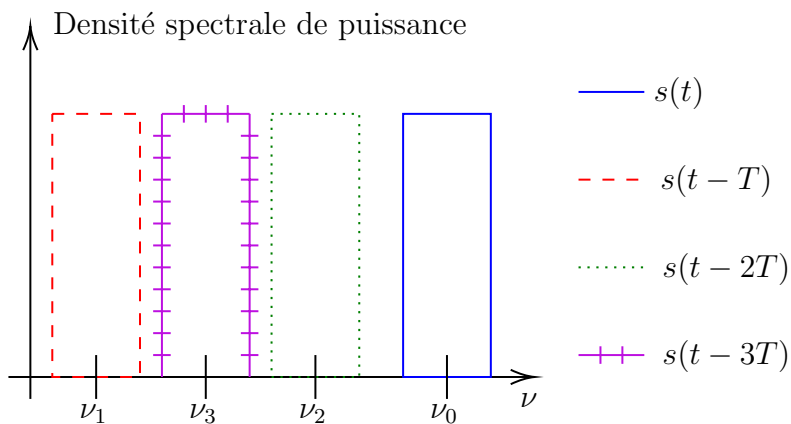


FIGURE III.1.3. – Illustration du principe de saut de fréquence FHSS



### III.1. Confidentialité, brouillage et authentification des communications

et exprimée en bit/s/Hz. La Secrecy Capacity (SC) (écart de capacité entre BOB et EVE) est définie par :

$$SC = \max \{C_B - C_E, 0\}, \quad SC \geq 0 \quad (\text{III.1.2})$$

Si la capacité de  $c_{A/E}$  est suffisamment faible, EVE ne pourra pas obtenir l'information de façon fiable ( $C_E$  faible) et la confidentialité sera donc bonne. Cependant,  $c_{A/B}$  doit aussi conserver une capacité minimale, sinon cela signifie que BOB ne sera pas plus capable de retrouver l'information que EVE. De plus, en pratique, le SNR fluctue dans le temps. La SC dans l'équation (III.1.2) est donc une mesure instantanée. La Secrecy Outage Probability (SOP) est un indicateur statistique quantifiant la perte de confidentialité en regroupant les contraintes précédentes :

$$SOP(\lambda_B, \lambda_{SC}) = 1 - \mathbb{P}[C_B \geq \lambda_B; SC \geq \lambda_{SC}] \quad (\text{III.1.3})$$

Elle représente l'inverse de la situation où l'on souhaite que BOB puisse décoder au moins  $\lambda_B$  bits d'information par seconde par Hz et que la SC soit d'au moins  $\lambda_{SC}$ . L'objectif pour maximiser la confidentialité est donc de dégrader le plus possible le canal de EVE (avoir  $C_E$  faible), tout en préservant une bonne capacité pour le récepteur légitime.

La majorité des études sur l'amélioration de la confidentialité portent sur les schémas de communication Multiple Input Multiple Output (MIMO), où les émetteurs et récepteurs utilisent plusieurs antennes. Les premiers travaux ont porté sur l'extension des travaux de Wyner pour le cas MIMO avec canaux AWGN [100, 101, 102]. Deux types majeurs de solutions ont été proposés pour optimiser la SC : l'usage de bruit artificiel (Artificial Noise (AN)) et l'utilisation de relais.

Le concept d'AN a été initialement proposé par Negi et Goel en 2005 dans [103]. Le principe est que ALICE ajoute à son signal d'information un signal de brouillage judicieusement choisi, afin de perturber au maximum la démodulation par EVE, sans impacter BOB. Il est montré que l'AN a de très bonnes performances si ALICE a une connaissance parfaite de tous les canaux. En revanche, dans le cas d'une connaissance imparfaite, l'AN peut dans certains cas dégrader les performances de BOB et donc réduire la SC. Les auteurs dans [104] analysent la stratégie à adopter pour l'AN si ALICE a une connaissance imparfaite des canaux. Ils montrent qu'il vaut mieux dans ce cas chercher à perturber EVE (diminuer  $c_E$ ) plutôt que d'essayer d'améliorer la qualité du signal reçu par BOB (augmenter  $c_B$ ). Plusieurs améliorations ont été proposées pour améliorer le schéma d'AN classique. Par exemple, dans [105], les auteurs proposent d'utiliser deux types de signaux de brouillage, pour le scénario où l'on souhaite privilégier l'impact sur EVE plutôt que les performances de démodulation pour BOB (terrain de guerre par exemple). L'AN peut aussi être utilisé par une entité supplémentaire (brouilleur coopératif, *friendly jammer* en anglais) placée dans le réseau ayant pour rôle de protéger la communication entre ALICE et BOB [106, 107]. L'intérêt de cette approche est que le brouilleur coopératif peut s'alimenter directement à partir des signaux environnants (sans avoir besoin d'alimentation supplémentaire) en utilisant les méthodes de récolte d'énergie (*energy harvesting*). Cela améliore grandement l'efficacité énergétique du réseau et offre des résultats prometteurs.

Les relais ont été initialement proposés afin d'augmenter la portée des communications. Ils peuvent utiliser deux types de relayage : l'amplification puis retransmission (Amplity

and Forward (AF)) ou le décodage puis retransmission (Decode and Forward (DF)). Dans l'AF, le relais reçoit le signal tel quel, l'amplifie et le retransmet à la destination, tandis que dans le DF, le relais démodule le signal reçu pour extraire l'information, reconstruit le signal à partir de l'information décodée et retransmet. Les relais ont rapidement montré un potentiel dans la lutte des intercepteurs grâce au degré de liberté supplémentaire offert. Les auteurs dans [108] évaluent quelle est la stratégie de relais optimale et concluent que l'AF est celle offrant le meilleur compromis entre maximisation de la SC et complexité calculatoire. On peut citer aussi par exemple les travaux [109, 110, 111] où l'optimisation est réalisée pour différents scénarios (un ou plusieurs récepteurs légitimes, connaissance parfaite ou imparfaite des différents canaux, relais non fiable, etc.).

L'AN et les relais ont aussi été employés dans le contexte du Full-Duplex (FD), schéma de communication prometteur, où l'équipement peut émettre et recevoir des signaux en même temps et ce dans la même bande de fréquence [112]. Le FD améliore considérablement l'efficacité spectrale puisqu'il n'y a plus de séparation entre canaux d'émission et réception. L'enjeu majeur du Full-Duplex dans la recherche aujourd'hui est de minimiser l'auto-interférence (Self Interference (SI)) induite. En effet, le signal transmis a une puissance bien supérieure à celle du signal reçu (jusqu'à 100 dB d'écart), la bonne démodulation du signal reçu est donc impossible sans annulation préalable du signal émis. Les travaux dans [113, 114, 115] cherchent alors à optimiser à la fois la configuration MIMO, trouver le bon comportement du ou des relais, et de minimiser la SI.

### III.1.2. Brouillage d'attaque

Avec le nombre grandissant d'équipements communicants, la menace de brouilleurs souhaitant perturber les communications, dit *brouilleurs d'attaque*, est de plus en plus palpable. En effet, il est de nos jours aisé de se procurer des équipements réalisant des fonctions de brouillage à coût modéré [116]. Le scénario de brouillage d'attaque est présenté en Figure III.1.4.

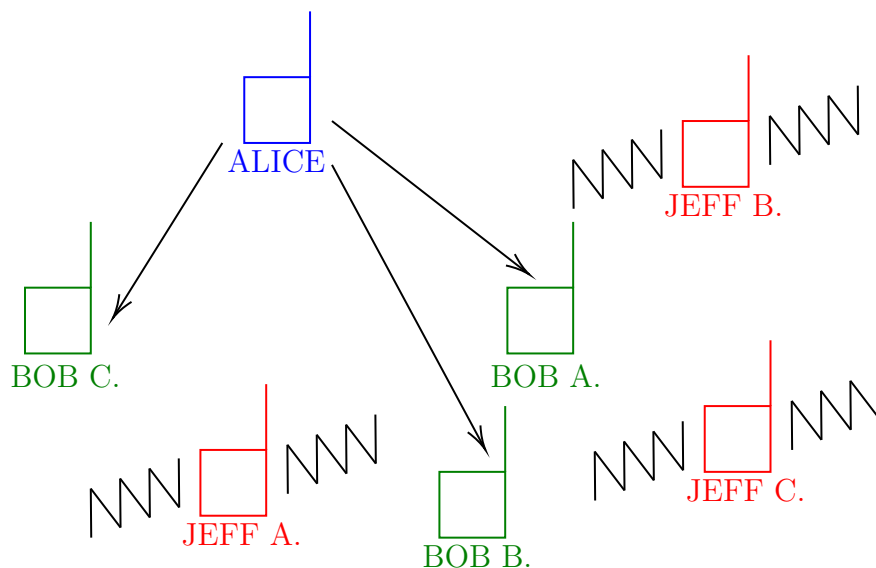


FIGURE III.1.4. – Scénario de communication en présence d'un brouilleur d'attaque

Un émetteur ALICE transmet une information à trois récepteurs légitimes, BOB A., BOB B. et BOB C. Une entité malveillante place alors un ou plusieurs équipements de brouillage (ici trois, JEFF A., JEFF B. et JEFF C.) dans le voisinage afin de perturber le plus possible la restitution de l'information par les récepteurs BOB. Dans ce scénario, l'entité malveillante doit alors choisir la meilleure stratégie pour arriver à ses fins tandis que les émetteurs/récepteurs légitimes doivent adopter des solutions pour contrer une éventuelle attaque. Dans ce qui suit, nous présentons les différents comportements du brouilleur dans les domaines temporel et fréquentiel (Section III.1.2.1). Ensuite, nous présentons les principaux brouilleurs et contre-mesures proposées dans la littérature, pour différents schémas de modulation (Section III.1.2.2). Ces éléments d'état de l'art posent les bases pour l'étude que nous avons proposée dans [96] sur l'impact des brouilleurs classiques Band et Tone Jamming sur la modulation LoRa, présentée en Section III.2.

#### III.1.2.1. Comportements du brouilleur

##### III.1.2.1.1. Comportement temporel

Le brouilleur peut adopter plusieurs stratégies sur son comportement dans le domaine temporel [117]. La Figure III.1.5 les présente.

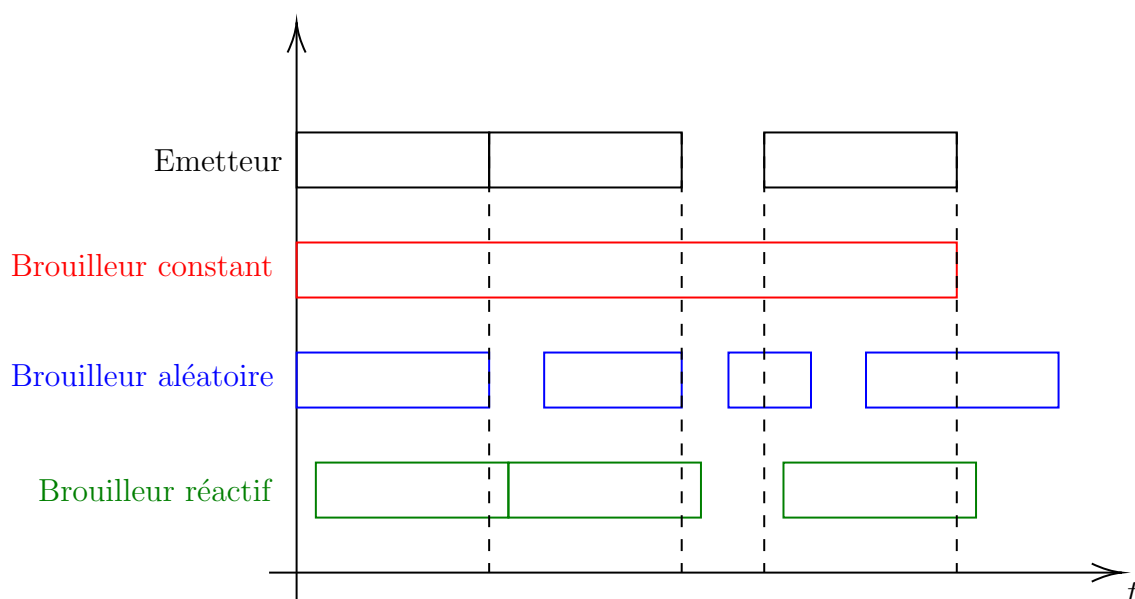


FIGURE III.1.5. – Comportements dans le domaine temporel d'un brouilleur

Une première solution est de rendre le brouilleur actif en permanence (brouilleur constant sur la figure). Ce dernier est le plus efficace du point de vue de la perturbation de la communication, puisqu'une transmission sera à coup sûr à minima perturbée, mais peu efficace du point de vue énergétique, puisque le brouilleur doit être en permanence alimenté. De plus, il est facilement détectable.

On trouve ensuite le brouilleur aléatoire, où ce dernier a des créneaux de brouillage de durée et d'occurrence aléatoires, complètement décorrélés de l'émetteur. Les créneaux de brouillage sont définis afin de satisfaire un compromis entre impact sur la transmission et consommation énergétique. Il est donc plus équilibré que le brouilleur constant.

Enfin, le brouilleur réactif est le plus intelligent des trois puisque ce dernier ne transmet son signal de brouillage uniquement après détection du signal utile à brouiller. Il est optimal selon les critères précédents, mais pose d'autres problématiques puisqu'il doit 1) pouvoir détecter de façon fiable le signal utile et 2) transmettre le plus rapidement possible son signal de brouillage. Cela introduit des critères supplémentaires de détection (probabilités de détection correcte, de non détection et de fausse alarme) et de délais. Le brouilleur réactif peut aussi être exploité comme moyen de contre-mesure avec l'utilisation de brouilleurs coopératifs [118].

### III.1.2.1.2. Comportement fréquentiel – brouilleur Band Jamming

Le brouilleur peut aussi donner différents comportements à son signal de brouillage dans le domaine fréquentiel [117, 119, 96]. Les comportements les plus répandus sur lesquels la majorité des équipements de brouillage et travaux de recherche s'appuient sont les Band Jamming (BJ) et Tone Jamming (TJ). Le BJ est présenté en Figure III.1.6.

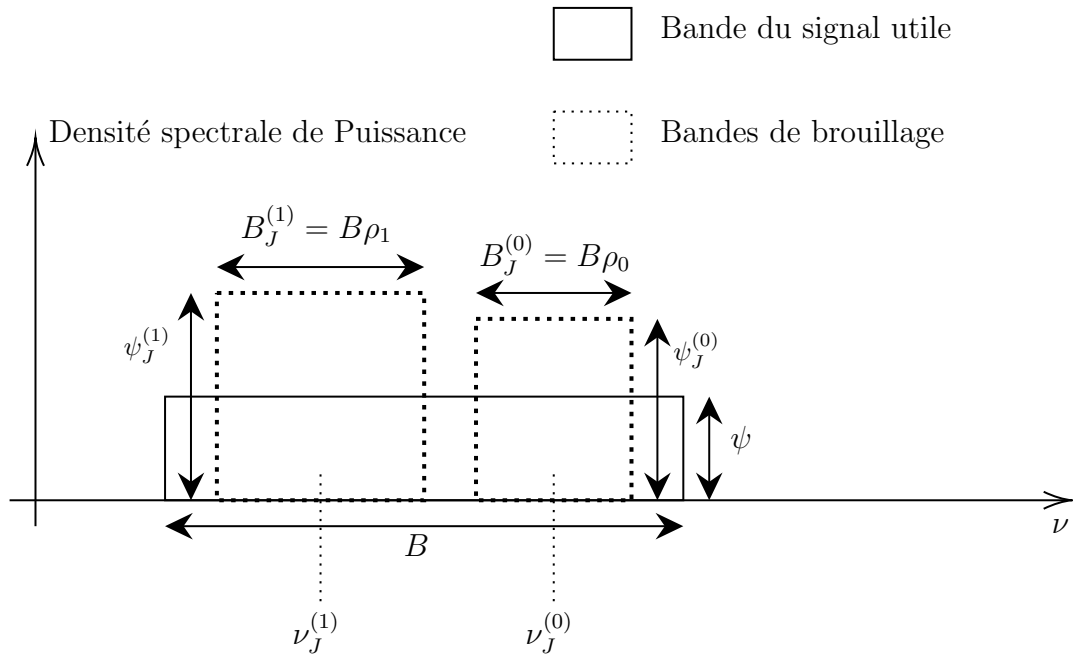


FIGURE III.1.6. – Illustration du comportement fréquentiel d'un brouilleur de type Band Jamming

Nous notons  $B$  et  $\psi$ , la largeur de bande et le niveau spectral de puissance du signal utile, respectivement. Le brouilleur génère un signal de brouillage comportant  $V$  bandes fréquentielles de brouillage ( $V = 2$  sur la figure), issues de bruit AWGN filtré, et venant se superposer sur celle du signal utile. La  $v^{\text{ème}}$  ( $v \in \{0, 1, \dots, V-1\}$ ) bande de brouillage a la largeur :

$$B_J^{(v)} = B \times \rho_v, \quad \rho_v \in ]0; 1] \quad (\text{III.1.4})$$

et le niveau spectral :

$$\psi_J^{(v)} = \psi / \rho_v \quad (\text{III.1.5})$$

avec la contrainte :

$$\sum_{v=0}^{V-1} B_J^{(v)} \times \psi_J^{(v)} = \sigma_{BJ}^2 \quad (\text{III.1.6})$$

où  $\sigma_{BJ}^2$  est la puissance de brouillage BJ totale disponible.

Ainsi, pour respecter la contrainte de puissance de brouillage dans l'équation (III.1.6), plus la largeur d'une bande de brouillage donnée diminue, plus son niveau spectral augmente. Lorsqu'il n'y a qu'une seule bande de brouillage ( $V = 1$ ) de largeur maximale ( $\rho_0 = 1$ ), nous parlons de Full Band Jamming (FBJ) et de Partial Band Jamming (PBJ) sinon. Le choix du nombre de bandes de brouillage et de leurs paramètres doit être choisi avec soin afin de perturber au mieux la démodulation au niveau de la cible.

### III.1.2.1.3. Comportement fréquentiel – brouilleur Tone Jamming

Le brouilleur TJ transmet dans la bande du signal utile un certain nombre de signaux de brouillage sinusoïdaux purs, à fréquence et puissance choisies, comme illustré en Figure III.1.7.

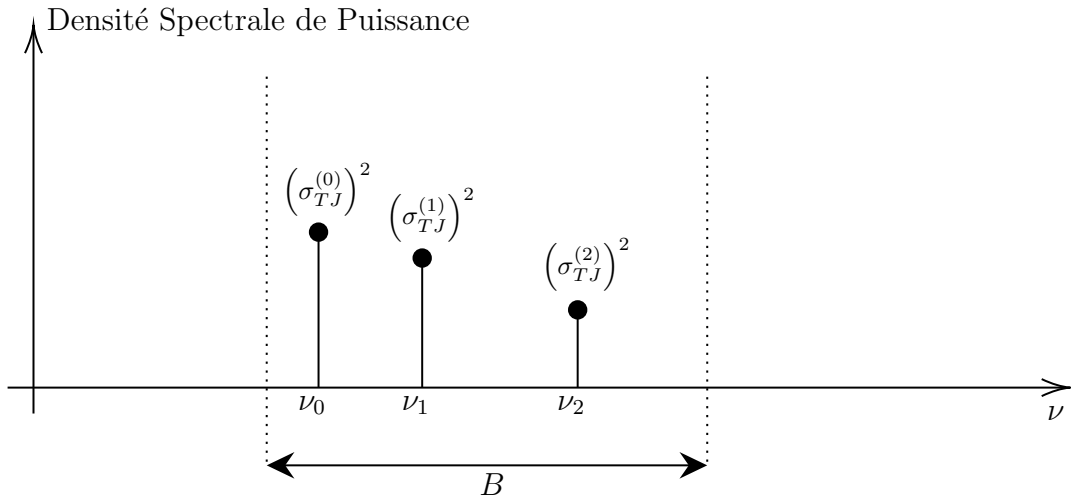


FIGURE III.1.7. – Illustration du comportement fréquentiel d'un brouilleur de type Tone Jamming

Le nombre de composantes de brouillage est noté  $V$ . Chaque composante, d'indice  $v$  ( $v \in \{0, 1, \dots, V - 1\}$ ), a la fréquence  $\nu_v$  et la puissance associée  $(\sigma_{TJ}^{(v)})^2$ . Le signal de brouillage discret résultant a pour expression :

$$s_{TJ}[k] = \sum_{v=0}^{V-1} s_{TJ}^{(v)}[k] = \sum_{v=0}^{V-1} (\sigma_{TJ}^{(v)})^2 e^{2j\pi\nu_v k + j\phi_v} \quad (\text{III.1.7})$$

avec  $\phi_v$ , la phase de la sinusoïde de brouillage et :

$$\sum_{v=0}^{V-1} (\sigma_{TJ}^{(v)})^2 = \sigma_{TJ}^2 \quad (\text{III.1.8})$$

avec  $\sigma_{TJ}^2$ , la puissance de brouillage TJ totale disponible. L'allocation de puissance peut être uniforme, donnant  $(\sigma_{TJ}^{(v)})^2 = \sigma_{TJ}^2/V$  ou bien non-uniforme. L'allocation uniforme est la stratégie optimale pour le brouilleur si ce dernier ne possède aucune information a priori sur le signal utile [119]. S'il y a qu'une seule composante de brouillage ( $V = 1$ ),

nous parlons de Single Tone Jamming (STJ) et de Multi Tone Jamming (MTJ) sinon.

De même que pour le brouilleur BJ, le choix des paramètres TJ doit être choisi avec soin afin d'obtenir un impact suffisamment important. Les travaux dans la littérature ont montré que le brouilleur TJ est généralement plus efficace que le brouilleur BJ, mais est aussi plus facilement détectable par le récepteur légitime [119].

### III.1.2.2. Brouilleurs et contre-mesures dans la littérature

Dans cette section, nous présentons quelques brouilleurs et contre-mesures proposés dans la littérature [120]. Ils sont classés en deux catégories selon le type de modulation : les brouilleurs développés pour les schémas de modulation de type *hopping* et OFDM (présentés en Section III.1.2.2.1) et ceux de type radar et GPS (présentés en Section III.1.2.2.2).

#### III.1.2.2.1. Brouilleurs Hopping et OFDM

##### Brouilleurs Hopping :

Dans [121] et [122], les auteurs proposent une amélioration de la robustesse des transmissions de type Frequency Hopping Spread Spectrum (FHSS) (voir Section III.1.1.2.1) aux brouilleurs BJ et ceux utilisant des signaux de brouillage ayant des caractéristiques très proches à celles du signal d'intérêt (corrélation temporelle et spectre fréquentiel similaires par exemple). Elle est nommée Message Driven Frequency Hopping (MDFH). Les auteurs montrent qu'en choisissant un schéma d'allocation aléatoire de fréquence directement en fonction des données transmises, et non en fonction d'un générateur d'aléa indépendant communément utilisé (Linear Feedback Shift Register (LFSR) par exemple), cela diminue le risque de collision des signaux d'intérêt et de brouillage, et donc le taux d'erreur de démodulation. Le schéma est évalué pour des brouilleurs ayant une puissance de brouillage proche de celle du signal d'intérêt (cas le plus défavorable puisque ayant un fort impact et difficile à détecter), et dans le cas multi-utilisateurs.

Les auteurs dans [123] proposent une forme d'onde limitant l'impact d'un brouilleur STJ utilisant une allocation fréquentielle aléatoire. Elle est développée en minimisant un critère d'inter-corrélation entre le signal de brouillage et celui d'intérêt, sous l'hypothèse que la fréquence STJ est parfaitement connue. Les résultats montrent de bonnes performances, même dans le cas où la fréquence STJ n'est pas parfaitement connue.

##### Brouilleurs OFDM :

Le schéma Orthogonal Frequency Division Multiplexing (OFDM) a aussi suscité de nombreux travaux sur l'impact de brouilleurs d'attaque. Rappelons que l'OFDM est un schéma découpant la largeur de bande totale en un certain nombre de sous-porteuses et associe à chacune un symbole issu d'une modulation numérique classique (Quadrature Amplitude Modulation (QAM) par exemple) [83]. Ainsi, la majorité des traitements se font dans le domaine fréquentiel. L'OFDM offre une bonne robustesse aux canaux multi-trajets et ne nécessite pas de traitements complexes au niveau du récepteur.

### III.1. Confidentialité, brouillage et authentification des communications

Les auteurs dans [124] comparent l'impact du brouilleur lorsque celui-ci brouille avec un signal AWGN toutes les sous-porteuses, uniquement celles servant à la synchronisation (sous-porteuses pilotes), ou bien en mettant en défaut la phase d'égalisation en optimisant le signal de brouillage. Les résultats montrent que la perturbation de l'égalisation a le plus grand impact, tandis que celle du brouillage AWGN sur toutes les sous-porteuses est la moins efficace. Dans [125], les auteurs montrent qu'en ne brouillant qu'un certain nombre de sous-porteuses pilotes avec des niveaux de puissance non-uniformes optimise l'impact du brouilleur.

Enfin, les auteurs proposent dans [126] une optimisation du signal de brouillage pour le cas généralisé MIMO, où le récepteur légitime optimise lui aussi son signal afin de réduire au maximum l'impact du brouilleur. L'étude montre que si le brouilleur a une connaissance parfaite de tous les canaux, l'impact sera maximal. L'impact diminuera progressivement à mesure que la connaissance des canaux se dégrade.

#### III.1.2.2.2. Brouilleurs radar et GPS

##### Brouilleurs radar :

Historiquement, la plupart des méthodes de brouillage ont été développées pour les systèmes radar de surveillance ou d'imagerie (Synthetic Aperture Radar (SAR)) [117]. Ils exploitent le principe de modulation Linear Frequency Modulated (LFM), où un signal de type chirp est employé, offrant une très bonne résolution spectrale et donc une localisation précise de la cible ou résolution de l'image SAR acquise. Les méthodes consistent en deux types d'approches : 1) gêner la lecture du signal reçu en brouillant avec un signal ayant des propriétés proches de celles du bruit AWGN (séquence pseudo-aléatoires par exemple), nommé *blanket jamming* en anglais, ou 2) introduire des fausses signatures radar afin de tromper l'interprétation des résultats.

Les auteurs dans [127, 128] proposent d'utiliser du *blanket jamming* pour des applications de surveillance et SAR, respectivement. Dans [128], il est choisi de brouiller non pas le récepteur mais la zone d'intérêt directement. Cela permet de pouvoir brouiller indépendamment de la position du récepteur. Les auteurs dans [129] comparent l'efficacité de brouillage utilisant une seule fausse signature, plusieurs fausses signatures (de fréquence pure ou ayant une largeur de bande fixe). Ils montrent que le brouillage avec plusieurs fausses signatures de largeur de bande fixe est le plus efficace. Dans [130], les auteurs utilisent les deux méthodes de brouillage et montrent que l'utilisation conjointe permet de réduire la consommation énergétique pour un impact préservé.

##### Brouilleurs GPS :

Les dispositifs Global Positioning System (GPS) sont aussi victimes de brouillage [120]. Le GPS utilise une transmission par étalement de spectre par séquence directe (voir Figure III.1.2). Les séquences d'étalement utilisées sont celles de Gold [83]. Elle offrent de bonnes propriétés d'auto et d'inter-corrélation afin d'assurer une bonne capacité de synchronisation et de minimiser les interférences multi-utilisateurs, respectivement. Deux types de séquences de Gold sont utilisées dans le GPS : les séquences C/A et P [131]. Les secondes sont exclusivement réservées à un usage militaire, elle ne sont donc pas publiques.

L'impact des brouilleurs TJ et BJ (et leurs versions répétitives temporellement, avec une fréquence de répétition fixée et actifs pendant un certain pourcentage du temps) est bien connu dans la littérature. Par exemple, dans [132], les auteurs les comparent et montrent que le brouilleur TJ est le plus efficace.

La majorité des travaux porte sur le développement de contre-mesures. Par exemple, les auteurs dans [133] emploient une méthode de séparation aveugle de sources pour extraire du signal reçu la composante de brouillage. Dans [134], un algorithme d'estimation des directions d'arrivée des signaux de brouillage, exploitant l'approche éprouvée Multiple Signal Classification (MUSIC), est utilisé afin d'éliminer le signal de brouillage. Les auteurs dans [135] s'inspirent des méthodes de focalisation spatiale de faisceau (*beamforming* en anglais) de MIMO pour ainsi annuler l'effet du brouillage. Enfin, il est proposé dans [136] une méthode où le signal reçu est projeté sur un espace orthogonal à celui d'interférence. Cela est possible en exploitant la propriété que le signal GPS a une puissance très inférieure à celle du brouilleur. Ainsi, le signal reçu est dominé par le signal de brouillage et peut donc facilement être identifié et annulé.

### III.1.3. Authentification

Dans cette section, nous présentons l'axe important de sécurisation des communications : l'authentification, qui a pour but d'autoriser ou non des équipements à communiquer dans un réseau. L'authentification aujourd'hui se fait principalement par deux moyens : l'authentification par le réseau en utilisant les couches applicatives, et celle exploitant les propriétés physiques du signal reçu au niveau de la couche physique. Elles sont présentées respectivement en Sections III.1.3.1 et III.1.3.2.

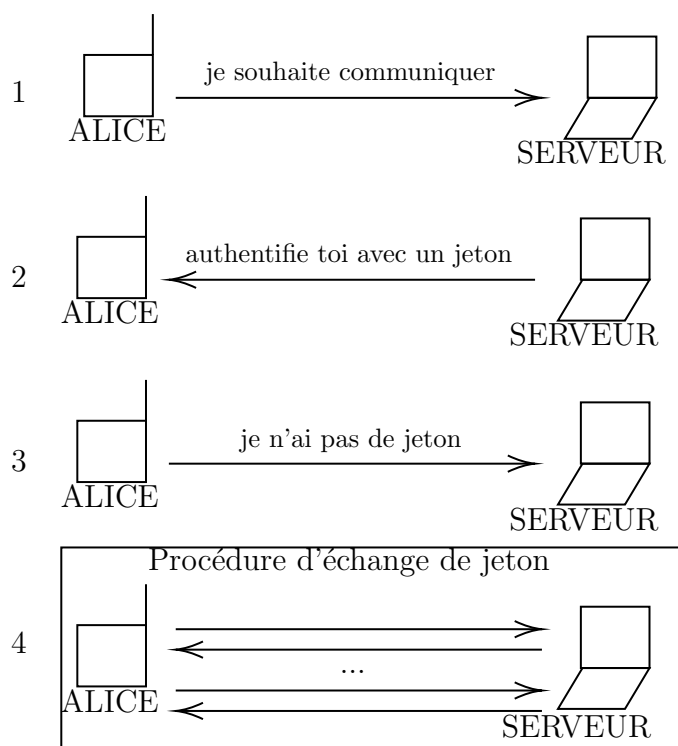
#### III.1.3.1. Authentification par le réseau

Le principe d'authentification par le réseau est présenté en Figure III.1.8, en deux étapes : l'accès au réseau (Figure III.1.8a) puis la communication (Figure III.1.8b). A la mise en service de son équipement, ALICE souhaite effectuer une première communication vers BOB. Pour cela, elle doit d'abord accéder au réseau et s'authentifier auprès d'un serveur d'authentification (Figure III.1.8a). Elle le contacte et ce dernier lui impose de s'authentifier en utilisant un jeton (étapes 1 et 2). A cette étape, elle n'a pas encore de jeton et en informe le serveur (étape 3). Une procédure est alors initiée (étape 4) où le serveur transmet à ALICE de façon sécurisée le jeton. L'enjeu majeur pour cette phase est la bonne construction du jeton (par méthodes de chiffrement principalement) et sa transmission sécurisée, de façon à ce qu'il ne soit pas volé, donnant ainsi la possibilité à un équipement non-désirable d'entrer dans le réseau et/ou d'usurper son identité.

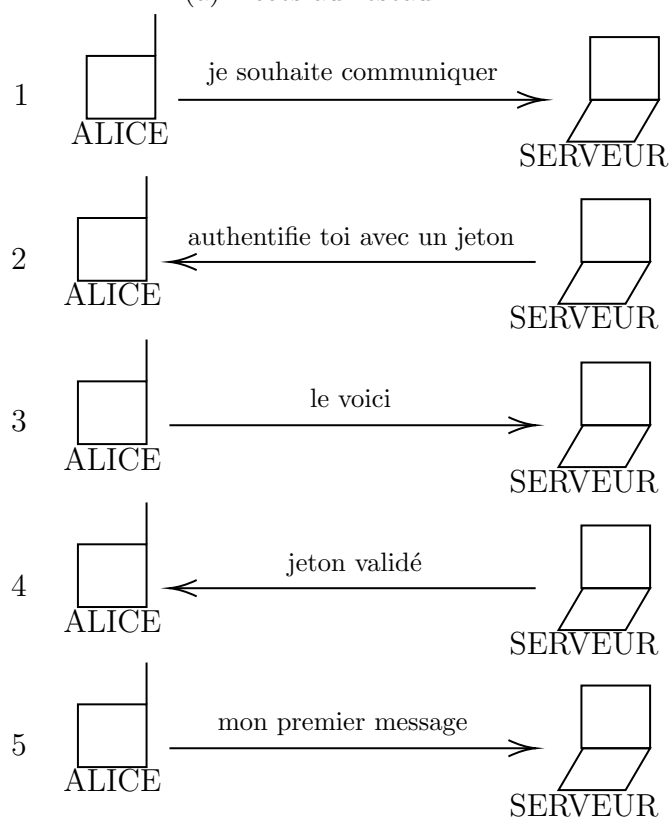
Une fois la phase d'accès au réseau terminée, ALICE peut commencer à communiquer avec BOB en faisant à chaque fois valider son jeton (étapes 2, 3 et 4 sur la Figure III.1.8b). Le jeton doit être renouvelé régulièrement pour limiter les risques d'usurpation.



### III.1. Confidentialité, brouillage et authentification des communications



(a) Accès au réseau



(b) Communication

FIGURE III.1.8. – Principe d'authentification par le réseau

Il existe de nombreux travaux sur l'authentification dans la littérature. Par exemple, les auteurs dans [137] proposent une architecture d'authentification dans un logement en ajoutant une passerelle, elle-même authentifiée, afin de réduire le nombre de vérifications des jetons et optimiser ainsi le trafic. Dans [138], les auteurs se concentrent sur la génération, la diffusion et la gestion des jetons en utilisant des méthodes cryptographiques (*blockchain* en anglais) pour des applications de véhicules connectés. Enfin, il est proposé dans [139] une méthode d'authentification groupée pour des applications multi-utilisateurs.

### III.1.3.2. Authentification par identification radio-fréquence

Une autre approche pour authentifier les équipements est d'exploiter les propriétés physiques du signal reçu, en réalisant de l'identification radio-fréquence, Radio Frequency Fingerprinting (RFF) en anglais [140]. Le schéma de principe est présenté en Figure III.1.9.

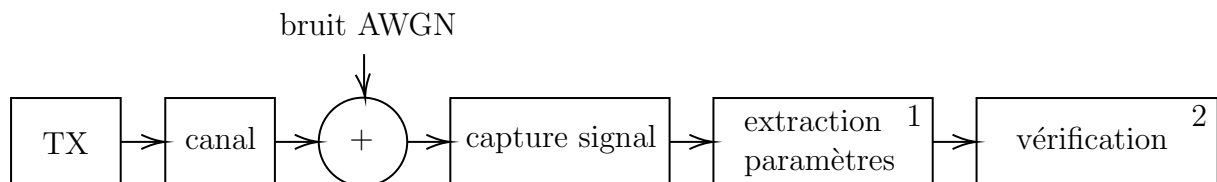


FIGURE III.1.9. – Principe d'authentification par identification radio-fréquence

Un équipement de surveillance est placé dans le réseau et a pour but de détecter et de déterminer si les transmissions en cours sont autorisées ou non. Cette décision se déroule en deux phases, après interception du signal. La première est l'extraction de paramètres permettant de discriminer la transmission (étape 1 sur la figure) puis de vérifier la légitimité de la transmission à partir de ces paramètres (étape 2).

Dans l'étape 1, les paramètres sont la plupart du temps issus des spécificités des équipements. En effet, chaque équipement est unique, de part ses imperfections matérielles ou de sa calibration. On peut citer comme imperfection matérielle : le décalage en fréquence (CFO), les signaux transitoires caractéristiques (par exemple ceux émis lors de l'initialisation de l'équipement), l'évolution de la puissance instantanée ou du contenu spectral (*waterfall*) au cours du temps ou encore les déformations du signal démodulé numériquement, comme la désynchronisation entre les voix I et Q. Ils peuvent aussi provenir de l'effet du canal sur le signal en suivant par exemple les fluctuations au cours du temps de la puissance du signal reçu (Received Signal Strength Indication (RSSI)).

La phase de vérification (étape 2) suit la stratégie suivante. Avant le déploiement de l'équipement, les paramètres cibles sont extraits et stockés dans une base de données. À chaque transmission interceptée, l'équipement de surveillance compare ces mêmes paramètres estimés avec ceux de la base de données. S'ils sont trop éloignés pour chaque équipement enregistré, il conclut que l'équipement en question n'a pas été au préalable déclaré et est donc un intrus. La comparaison est réalisée majoritairement avec des méthodes de classification de type deep learning ou machine learning [141].

### III.1. Confidentialité, brouillage et authentification des communications

Les références [142, 143, 144, 145] donnent un aperçu varié sur les différentes approches RFF. Dans [142], les auteurs authentifient des signaux OFDM en analysant le waterfall et réalisent la classification avec des réseaux de neurones Dense Neural Network (DNN). Dans [143], ce sont les signaux Bluetooth qui sont étudiés, en les décomposant par paquets d'ondelettes et en y extrayant des coefficients Linear Predictive Coding (LPC). L'apprentissage sur ces coefficients est effectué avec l'algorithme décisionnel bien connu *random forest*. Les études [144] et [145] se concentrent sur l'exploitation des composants matériels pour la RFF. Les auteurs choisissent dans [144] de développer un design d'antennes ayant des signatures électromagnétiques spécifiques afin de faciliter la RFF. Enfin, la dérive en fréquence des oscillateurs locaux est exploitée dans [145]. Il est montré que les variations de la tension de contrôle de la Phase Locked Loop (PLL) interne est un bon indicateur pour discriminer les équipements.

## III.2. Impact des brouilleurs classiques Band et Tone Jamming sur LoRa

Notre contribution *Band & Tone Jamming Analysis and Detection on LoRa signals* [96] a porté sur l'étude de l'impact des brouilleurs classiques de type Band Jamming (BJ) et Tone Jamming (TJ) sur la démodulation LoRa. Les hypothèses de travail sont les suivantes :

- Nous supposons les synchronisations temporelle et fréquentielle parfaites.
- Le brouilleur est supposé parfaitement réactif (voir Section III.1.2.1.1). Le signal de brouillage est alors parfaitement aligné temporellement avec celui d'intérêt LoRa.
- Le récepteur légitime possède une information précise du niveau de bruit i.e.  $\hat{\sigma}^2 \approx \sigma^2$ .
- Les résultats de simulation sont présentés pour  $SF = 7$  uniquement. Considérer  $SF > 7$  n'apporte qu'un gain de performances SER de 2.5 dB à chaque incrément de SF, comme expliqué en Section I.2.7.1 (voir Règle (I.2.102)). Cela ne change donc pas les conclusions.

Les modèles de brouilleur BJ et TJ ont été présentés en Sections III.1.2.1.2 et III.1.2.1.3, respectivement. Dans ce qui suit, nous commençons par évaluer l'impact de ces brouilleurs sur la démodulation LoRa (Section III.2.1) pour ensuite présenter un détecteur LoRa de ces derniers (Section III.2.2) et enfin des résultats de simulation (Section III.2.3).

### III.2.1. Impact des brouilleurs Band et Tone Jamming sur la DFT LoRa

#### III.2.1.1. Impact du brouilleur Band Jamming sur la DFT LoRa

Nous supposons que le signal BJ possède une seule bande de largeur réglable. En effet, nous avons observé que le fait d'avoir plusieurs bandes n'a pas d'impact marqué sur la démodulation LoRa. Ainsi  $B_J^{(0)} = B_{BJ}$  et  $\rho_0 = \rho$ , d'après la Figure III.1.6. Il peut-être généré comme un bruit AWGN, filtré en fréquence pour respecter la contrainte de largeur de bande avec :

$$B_{BJ} = B \times \rho, \quad \rho \in ]0; 1] \quad (\text{III.2.1})$$

Le signal reçu dechirpé en présence du brouilleur est alors :

$$\tilde{R}_{BJ}[k] = \tilde{X}_a[k] + \tilde{S}_{BJ}[k] + \tilde{W}[k] \quad (\text{III.2.2})$$

avec  $\tilde{S}_{BJ}[k]$ , la DFT LoRa de la composante de brouillage BJ. Il a été montré en simulation dans [96] que la paramètre  $\rho$  a un impact négligeable sur la démodulation, un brouilleur Partial Band Jamming (PBJ) ( $\rho < 1$ ) ou Full Band Jamming (FBJ) ( $\rho = 1$ ) sont en fait équivalents pour LoRa. Par conséquent, nous pouvons considérer la démodulation en présence du brouilleur BJ comme une démodulation classique AWGN, mais avec un

niveau de bruit AWGN effectif sur la DFT plus élevé, avec  $(\sigma^2)' = M(\sigma^2 + \sigma_{BJ}^2)$ , et donc un SNR équivalent plus faible  $SNR_J = SNR - 10 \log_{10}(\sigma_{BJ}^2)$ .

### III.2.1.2. Impact du brouilleur Tone Jamming sur la DFT LoRa

Le signal TJ a pour expression :

$$s_{TJ}[k] = \sum_{v=0}^{V-1} s_{TJ}^{(v)}[k] = \sum_{v=0}^{V-1} \left( \sigma_{TJ}^{(v)} \right)^2 e^{2j\pi\nu_v k + j\phi_v} \quad (\text{III.2.3})$$

$$\nu_v = \frac{u_v}{M}, \quad u_v \in [0; M - 1]$$

avec  $V$ , le nombre de composantes fréquentielles de brouillage supposées en phase i.e.  $\phi_v = 0$ ,  $\left( \sigma_{TJ}^{(v)} \right)^2 = \sigma_{TJ}^2/V$ , la puissance de brouillage (supposée homogène, stratégie optimale d'allocation de puissance [119]), et  $u_v$ , la fréquence normalisée LoRa de la  $v^{\text{ème}}$  composante de brouillage. De façon similaire au BJ, le signal reçu dechirpé est :

$$\tilde{R}_{TJ}[k] = \tilde{X}_a[k] + \tilde{S}_{TJ}[k] + \tilde{W}[k] \quad (\text{III.2.4})$$

avec  $\tilde{S}_{TJ}[k]$ , la DFT LoRa de la composante de brouillage TJ. Contrairement au brouilleur BJ, l'impact sur la DFT pour le brouilleur TJ dépend grandement de ses paramètres et du symbole transmis.

La Figure III.2.1 montre la DFT obtenue sans bruit pour le symbole transmis  $a = 64$  ( $SF = 7$ ), contaminé par une ou deux composantes TJ avec  $\sigma_{TJ}^2 = 2$ , et pour les cas suivants :  $V = 1$  ( $u_0 = 20$  ou  $u_0 = 20.5$ ) et  $V = 2$  ( $u_0 = 20$  et  $u_1 = 25$ ). Nous constatons que pour cet exemple, le bin  $n = a$  est impacté de la même manière pour tous les cas, avec une perte d'énergie valant  $M - \left| \tilde{X}_a[n] + \tilde{S}_{TJ}[n] \right| \approx 12$ . Si  $V = 1$  et  $u_0$  entier, une interférence constante est présente dans les bins  $n \neq a$  et vaut  $\sqrt{M\sigma_{TJ}^2}$  (16 ici). Si  $V = 1$  mais  $u_0$  non entier, nous constatons des déformations dans la DFT. Le motif de déformation est centré autour de  $\sqrt{M\sigma_{TJ}^2}$  (16 ici) et est nul en  $n = (a + \lfloor u_0 \rfloor + 1) \bmod M$  ( $n = 85$  ici), si la partie fractionnaire de  $u_0$  vaut 0.5. Plus la partie fractionnaire de  $u_0$  se rapproche de 0.5, plus la déformation a une oscillation importante autour de la valeur moyenne. Pour  $V = 2$  et  $u_v$  entier, nous remarquons la présence d'un motif de déformation quasi sinusoïdal, contenant  $\min \{ (u_1 - u_0) \bmod M, (u_0 - u_1) \bmod M \}$  périodes sur la DFT (5 ici). Le motif est en revanche beaucoup plus imprévisible pour  $V > 1$  et  $u_v$  non entier.

Pour  $V = 1$ , l'amplitude du pic d'intérêt  $n = a$  dépend de  $a$  et de  $u_0$ . Comme nous avons dans ce cas  $\left| \tilde{S}_{TJ}[n] \right| = \sqrt{M\sigma_{TJ}^2}$  (constant pour tout  $n$ ) et  $\Im\{\tilde{X}_a[a]\} = 0$ , nous observerons un gain de magnitude  $G = \Re\{\tilde{S}_{TJ}[a]\}$ . Si ce gain est positif, nous aurons alors une amélioration des performances SER et une dégradation sinon. Les valeurs de symbole conduisant à l'amélioration et à la dégradation maximale des performances SER peuvent être simplement trouvées par :

$$a_{min} = \arg \min_n \Re\{\tilde{S}_{TJ}[n]\}$$

$$a_{max} = \arg \max_n \Re\{\tilde{S}_{TJ}[n]\} \quad (\text{III.2.5})$$

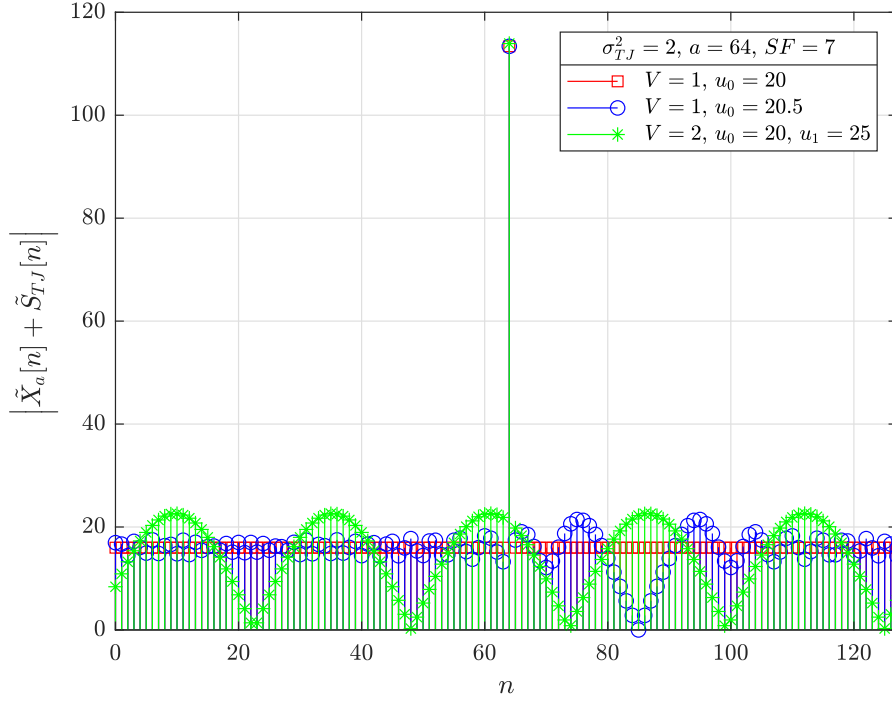


FIGURE III.2.1. – Exemples de démodulation LoRa en présence d'un brouilleur Tone Jamming,  $SF = 7$

La Figure III.2.2 montre la démodulation de deux symboles ayant les valeurs  $a_{min} = 3$  (cas le plus défavorable) et  $a_{max} = 67$  (cas le plus favorable), pour  $\sigma_{TJ}^2 = 2$  et  $u_0 = 20$ . Nous voyons bien l'écart de magnitude assez important entre les deux cas avec pour  $a = a_{min}$ ,  $|\tilde{X}_a[n] + \tilde{S}_{TJ}[a]| = 112$  et pour  $a = a_{max}$ ,  $|\tilde{X}_a[n] + \tilde{S}_{TJ}[a]| = 144$ , conduisant à un gain ou une perte de magnitude de  $\sqrt{M\sigma_{TJ}^2} = 16$  par rapport à une transmission sans brouilleur.

## III.2.2. Détecteur LoRa de brouilleurs Band et Tone Jamming

### III.2.2.1. Lois de probabilités des bins DFT

Le récepteur peut détecter la présence d'un brouilleur en observant les déformations engendrées sur la DFT et en utilisant un critère statistique. Nous notons  $H_0$  et  $H_1$ , les hypothèses d'absence et de présence de brouilleur, respectivement. Commençons par donner les lois de probabilité des bins  $|\tilde{R}[n \neq a]|$ . Pour ces derniers, il n'y a pas d'énergie du symbole d'intérêt. Nous avons alors la relation  $|\tilde{R}[n \neq a]| = |\tilde{S}[n \neq a] + \tilde{W}[n \neq a]|$ . Sous l'hypothèse  $H_0$ , les bins suivent une loi de Rayleigh, avec :

$$\begin{aligned} f_{X_{H_0}}(t) &= f_{Rayleigh}(t, b_{X_{H_0}}) \\ b_{X_{H_0}} &= \sqrt{M\sigma^2/2} \end{aligned} \quad (\text{III.2.6})$$

Sous l'hypothèse  $H_1$ , pour le brouilleur BJ, comme l'effet est presque identique à un bruit AWGN, la DFT sera vue comme comportant une composante de bruit AWGN plus

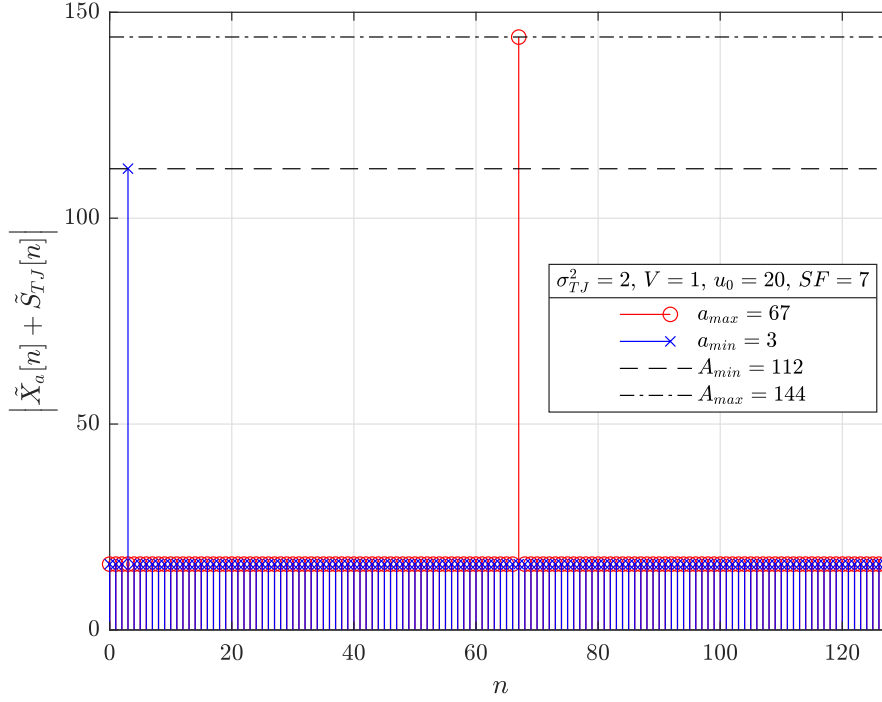


FIGURE III.2.2. – Valeurs de symboles minimisant et maximisant les performances de démodulation en présence d'un brouilleur Tone Jamming,  $SF = 7$

forte. Les bins suivent donc toujours une loi de Rayleigh :

$$\begin{aligned} f_{X_{H_1}^{BJ}}(t) &= f_{Rayleigh}(t, b_{X_{H_1}^{BJ}}) \\ b_{X_{H_1}^{BJ}} &= \sqrt{M(\sigma^2 + \sigma_{BJ}^2)/2} \end{aligned} \quad (\text{III.2.7})$$

Sous l'hypothèse  $H_1$ , pour le brouilleur STJ ( $u_0$  entier), les bins en  $n \neq a$  suivent quant à eux une loi de Rice :

$$\begin{aligned} f_{X_{H_1}^{TJ}}(t) &= f_{Rice}(t, \sigma_{X_{H_1}^{TJ}}, \mu_{X_{H_1}^{TJ}}) \\ \sigma_{X_{H_1}^{TJ}} &= b_{X_{H_0}} \\ \mu_{X_{H_1}^{TJ}} &= \sqrt{M\sigma_{TJ}^2} \end{aligned} \quad (\text{III.2.8})$$

### III.2.2.2. Construction du détecteur

Le récepteur calcule d'abord la quantité suivante, en choisissant aléatoirement  $D$  bins dans la DFT, différent du bin d'intérêt  $n = a$  :

$$z = \sum_{d=0}^{D-1} \frac{|\tilde{R}[n_d]|}{b_{X_{H_0}}}, \quad n_d \neq a \quad (\text{III.2.9})$$

Cette quantité est ensuite soumise à un seuil :

$$z \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_{detect} \quad (\text{III.2.10})$$

Si la quantité est supérieure au seuil, nous détectons la présence du brouilleur. Dans l'équation (III.2.9), le récepteur doit éliminer le bin d'intérêt  $n = a$ . Pour cela, il peut éliminer dans la DFT tous les bins étant supérieurs à un seuil (considérés comme comportant le signal d'intérêt) par :

$$\tilde{R}[n] = \begin{cases} 0 & \text{si } |\tilde{R}[n]| > \lambda \\ \tilde{R}[n] & \text{sinon} \end{cases} \quad (\text{III.2.11})$$

Ce seuil peut-être obtenu par un critère de fausse alarme de type Neyman-Pearson par :

$$\lambda = F_{Rayleigh}^{-1}(1 - P_{fa}, b_{X_{H_0}}) \quad (\text{III.2.12})$$

avec  $P_{fa}$ , la probabilité de fausse alarme et  $F_{Rayleigh}^{-1}(\cdot, \cdot)$ , la fonction de répartition inverse de la loi de Rayleigh.

D'après l'équation (III.2.9), la quantité  $z$  est la somme de lois de Rayleigh ou de Rice (équations (III.2.7) et (III.2.8)). La loi résultante n'est pas simple, mais a été obtenue dans la littérature et est basée sur l'approche Small Argument Approach (SAA) [146, 147]. L'expression dans [146] a l'avantage d'être généralisée pour tout  $D$ , mais introduit un biais à mesure que  $D$  augmente, contrairement à [147] qui est exacte mais uniquement valable pour  $D \leq 16$ . Dans l'article [96], l'expression dans [146] a été retenue, donnant un biais raisonnable.

### III.2.2.3. Loi de probabilité de la quantité statistique de détection sous l'hypothèse $H_0$

Sous l'hypothèse  $H_0$ , les expressions de la loi de probabilité, notée  $f(t)$ , et de fonction de répartition, notée  $F(t)$  sont :

$$f_{Z_{H_0}}^{SAA}(t) = \frac{t^{2L-1} e^{-\frac{t^2}{2b_{Z_{H_0}}^{SAA}}}}{2^{D-1} (b_{Z_{H_0}}^{SAA})^D (D-1)!^{(1)}} \quad (\text{III.2.13})$$

$$F_{Z_{H_0}}^{SAA}(t) = 1 - e^{-\frac{t^2}{2b_{Z_{H_0}}^{SAA}}} \sum_{l=0}^{D-1} \frac{\left(\frac{t^2}{2b_{Z_{H_0}}^{SAA}}\right)^l}{l!^{(1)}} \quad (\text{III.2.14})$$

avec :

$$b_{Z_{H_0}}^{SAA} = \frac{1}{D} [(2L-1)!^{(2)}]^{1/D} \quad (\text{III.2.15})$$

et :

$$x!^{(c)} = 1 \times (1+c) \times (1+2c) \times \dots \times x \quad (\text{III.2.16})$$

Le seuil, valable pour les deux brouilleurs, est obtenu par rapport à l'hypothèse  $H_0$  et vaut :

$$\lambda_{detect} = \left(F_{Z_{H_0}}^{SAA}\right)^{-1} (1 - P_{fa}^{detect}) \quad (\text{III.2.17})$$

avec  $P_{fa}^{detect}$ , la probabilité de fausse alarme de détection de brouilleur.



### III.2.2.4. Loi de probabilité de la quantité statistique de détection d'un brouilleur Band Jamming sous l'hypothèse $H_1$

Pour le brouilleur BJ, les expressions de la loi de probabilité et de fonction de répartition pour l'hypothèse  $H_1$  sont les mêmes que sous l'hypothèse  $H_0$ , mais en remplaçant  $b_{Z_{H_0}^{SAA}}$  dans l'équation (III.2.15) par  $b_{Z_{H_1}^{BJ,SAA}}$  :

$$b_{Z_{H_1}^{BJ,SAA}} = \frac{1 + \frac{\sigma_{BJ}^2}{\sigma^2}}{D} [(2D - 1)!]^{1/D} \quad (\text{III.2.18})$$

### III.2.2.5. Loi de probabilité de la quantité statistique de détection d'un brouilleur Tone Jamming sous l'hypothèse $H_1$

Des expressions théoriques biaisées de la loi de  $z$  pour le brouilleur Single Tone Jamming (STJ) ( $u_0$  entier) ont également été obtenues dans la littérature [148, 149], jusqu'à  $D = 10$  dans [149], ou pour un nombre limité de valeurs Noise-to-Jam Ratio (NJR) dans [148]. Le NJR est défini par  $NJR = \sigma^2/\sigma_{BJ}^2 \equiv \sigma^2/\sigma_{TJ}^2$ . Pour réduire le biais, nous utilisons l'approximation de la loi de Rice i.e. si  $NJR_{dB} \rightarrow \infty$ , la loi  $f_{Z_{H_1}^{STJ}}(t)$  tend vers  $f_{Z_{H_0}^{BJ,SAA}}(t)$  (notée  $f_{Z_{H_1}^{STJ^+}}(t)$ ) et si  $NJR_{dB} \rightarrow -\infty$ ,  $f_{Z_{H_1}^{STJ}}(t)$  tend alors vers une loi normale :

$$\begin{aligned} f_{Z_{H_1}^{STJ^-}}(t) &= \mathcal{N}(t, \mu_{Z_{H_1}^{STJ^-}}, \sigma_{Z_{H_1}^{STJ^-}}) \\ \mu_{Z_{H_1}^{STJ^-}} &= \frac{\sqrt{M(\sigma^2/2 + \sigma_{TJ}^2)D}}{b_{X_{H_0}}}, \quad \sigma_{Z_{H_1}^{STJ^-}} = 1 \end{aligned} \quad (\text{III.2.19})$$

Dans les simulations, nous choisissons  $f_{Z_{H_1}^{STJ^-}}(t)$  si  $NJR_{dB} < 0$ ,  $f_{Z_{H_1}^{STJ^+}}(t)$  sinon. Les fonctions de répartition associées sont notées  $F_{Z_{H_1}^{STJ^-}}(t)$  et  $F_{Z_{H_1}^{STJ^+}}(t)$ . Nous évaluons les performances de détection selon les probabilités de non détection  $P_{md}^{BJ}$  et  $P_{md}^{TJ}$ , pour une contrainte de fausse alarme  $P_{fa}^{detect}$  fixée. Elle sont définies par :

$$P_{md}^{BJ} = \int_{-\infty}^{\lambda_{detect}} f_{Z_{H_1}^{BJ,SAA}}(t) dt = F_{Z_{H_1}^{BJ,SAA}}(\lambda_{detect}) \quad (\text{III.2.20})$$

$$P_{md}^{STJ} = \begin{cases} \int_{-\infty}^{\lambda_{detect}} f_{Z_{H_1}^{STJ^-}}(t) dt = F_{Z_{H_1}^{STJ^-}}(\lambda_{detect}) & \text{si } NJR_{dB} < 0 \\ \int_{-\infty}^{\lambda_{detect}} f_{Z_{H_1}^{STJ^+}}(t) dt = F_{Z_{H_1}^{STJ^+}}(\lambda_{detect}) & \text{sinon} \end{cases} \quad (\text{III.2.21})$$

Pour  $V > 1$ , il n'y a pas d'expressions théoriques des lois de probabilité et de répartition dans la littérature. Elles sont donc estimées par approximation numérique (tirages de Monte-Carlo).

### III.2.2.6. Comparaison entre les expressions analytiques et les histogrammes des lois de probabilité sous les deux hypothèses pour le brouilleur Band Jamming

La Figure III.2.3 montre la comparaison entre les expressions analytiques et les histogrammes de  $z$  obtenus en simulation ( $D = 8$ ), pour les deux hypothèses. Le SNR ici est défini par rapport au signal d'intérêt i.e.  $SNR = P_s/\sigma^2 = 1/\sigma^2$ . Nous avons utilisé dans

la figure  $NJR_{dB} = SNR_{dB} = -5$  et  $SF = 7$ . Nous remarquons bien la présence du biais entre théorie et simulation, mais qui reste malgré tout raisonnable.

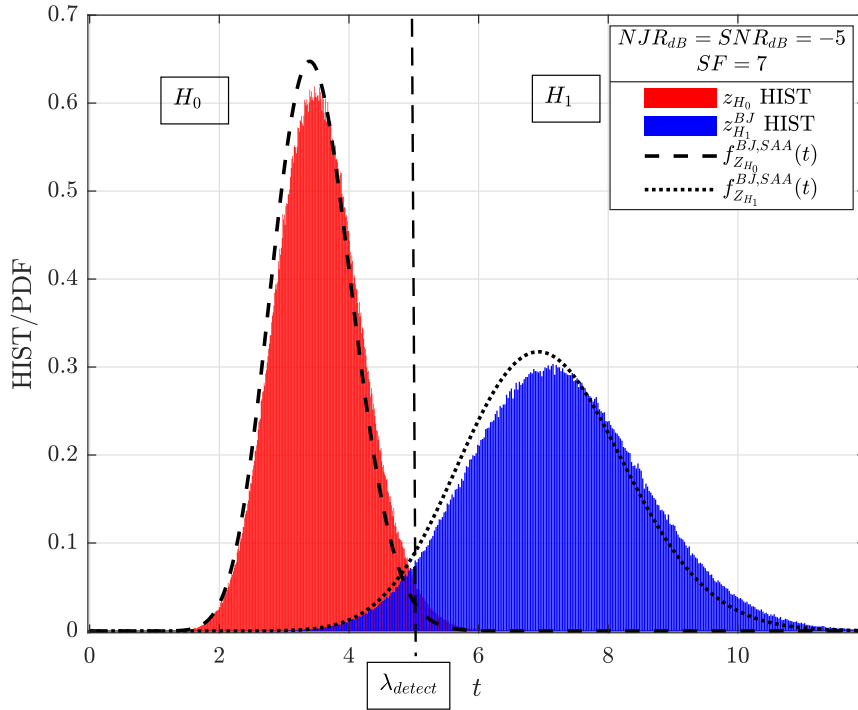


FIGURE III.2.3. – Lois de probabilité et histogrammes de la quantité statistique du détecteur, avec et sans brouillage Band Jamming,  $SF = 7$

### III.2.3. Résultats de simulation

#### III.2.3.1. Influence de la valeur de symbole sur le SER en présence de brouilleur Tone Jamming

La Figure III.2.4 présente les performances SER (simulation) en fonction du Signal-to-Jam Ratio (SJR), défini par  $SJR = P_s / \sigma_{TJ}^2$ , en présence d'un brouilleur TJ, pour  $V = 1$  et  $V = 2$ ,  $SNR_{dB} = -8$  et  $SF = 7$ . Les composantes fréquentielles  $u_v$  sont supposées ici entières et les performances sont obtenues avec des valeurs aléatoires de symboles, sauf pour les deux courbes avec motif '+', où les valeurs de symboles minimisant et maximisant les performances ( $a_{min}$  et  $a_{max}$ ) sont choisies (voir Section III.2.1.2). Nous avons aussi ajouté les performances en AWGN (hypothèse  $H_0$ ) comme point de comparaison.

Nous pouvons remarquer que la présence du brouilleur impacte de façon modérée les performances. Nous constatons en effet une baisse du SER, passant d'environ  $1.5 \times 10^{-3}$  à environ  $2 \times 10^{-2}$ , pour  $SJR_{dB} = -5$ . La valeur de  $V$  n'a pratiquement pas d'impact sur les performances. Cela est aussi vrai si  $u_v$  est non entier (non montré pour conserver la clarté de la figure). Passer de la valeur de symbole la plus favorable  $a_{max}$  à la plus défavorable  $a_{min}$  entraîne une baisse importante, passant d'environ  $5.5 \times 10^{-4}$  à environ  $6.5 \times 10^{-2}$  à  $SJR_{dB} = -5$ . Notons qu'avoir  $a = a_{max}$  améliore moins les performances qu'avoir  $a = a_{min}$  ne les dégrade. Les performances moyennes sur  $a$  sont donc plus proches du cas

### III.2. Impact des brouilleurs classiques Band et Tone Jamming sur LoRa

$a = a_{min}$ . De façon évidente, à mesure que le SJR augmente i.e. la puissance du brouilleur diminue, les performances en présence de ce dernier convergent vers celles AWGN.

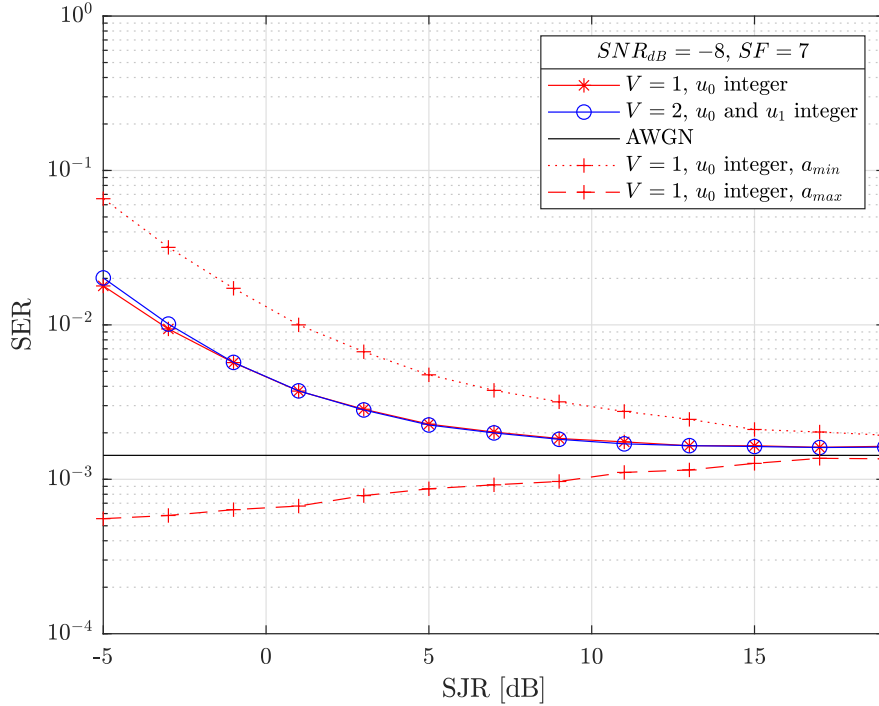


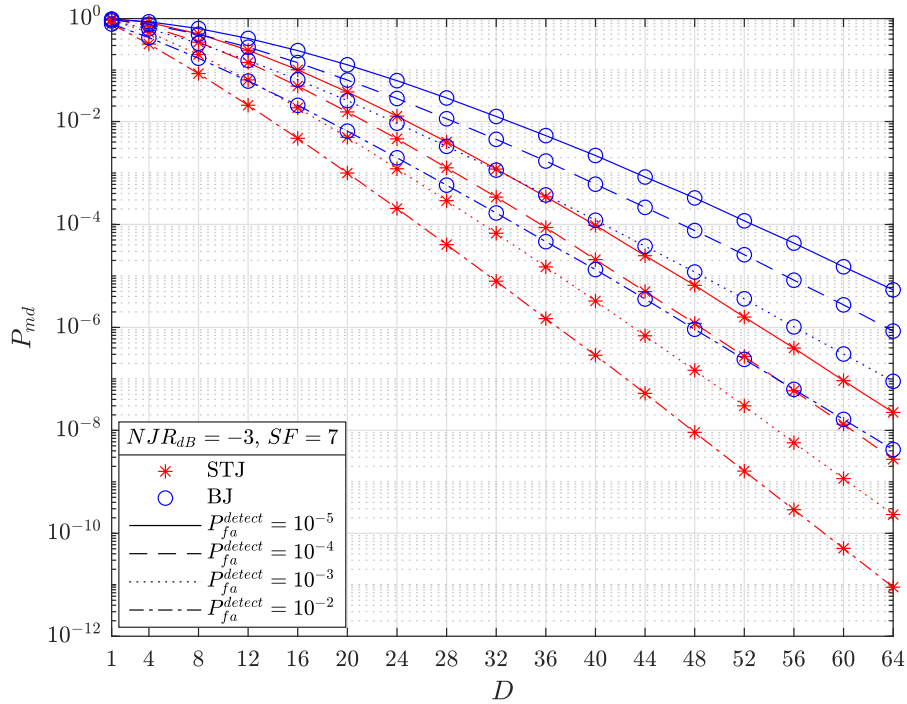
FIGURE III.2.4. – Performances SER en présence d'un brouilleur Tone Jamming et impact de la valeur du symbole,  $SF = 7$

#### III.2.3.2. Performances analytiques de détection des brouilleurs Band et Single Tone Jamming

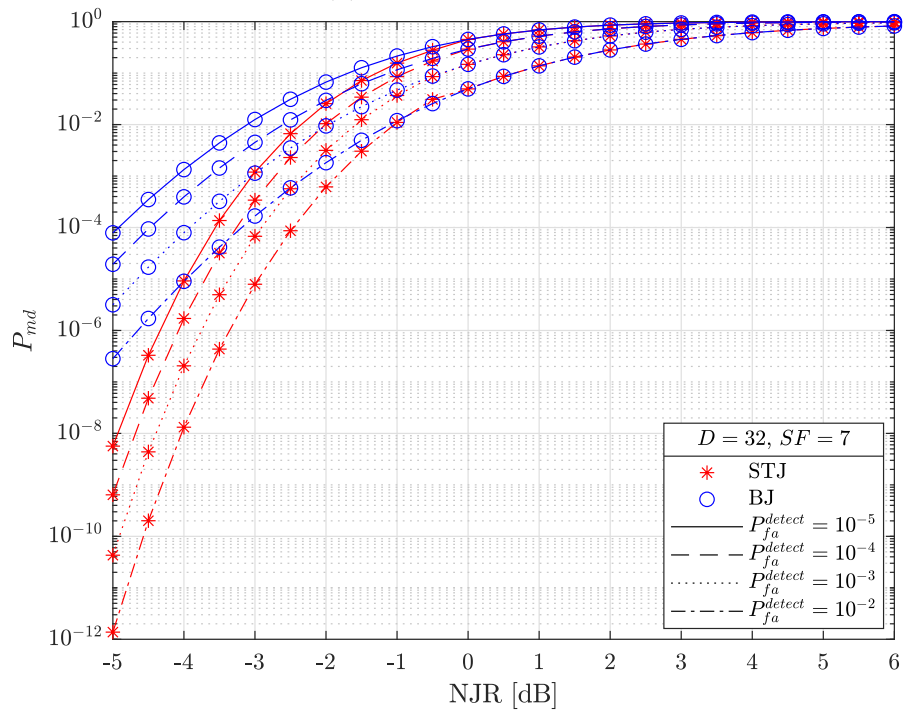
La Figure III.2.5a montre les performances de détection (probabilité  $P_{md}$ , d'après l'équation (III.2.20) pour le brouilleur BJ et l'équation (III.2.21) pour le brouilleur STJ (hypothèse  $u_0$  entier)) en fonction de  $D$  pour les brouilleurs BJ et STJ, pour plusieurs valeurs de probabilité de fausse alarme  $P_{fa}^{detect} \in \{10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}\}$ , et  $NJR_{dB} = -3$ . La Figure III.2.5b montre les mêmes résultats, mais en fonction de NJR pour  $D = 32$ .

D'après la Figure III.2.5, nous pouvons constater les comportements suivants :

- Plus  $D$  augmente, plus les performances s'améliorent, avec un écart énorme entre  $D = 1$  ( $P_{md} \approx 1$ ) et  $D = 64$  ( $P_{md} \approx 10^{-11}$  ( $P_{md} \approx 1$ ) pour le brouilleur STJ et  $P_{fa}^{detect} = 10^{-2}$ ). Cela se comprend de façon assez intuitive : un seul bin est insuffisant pour pouvoir décider de façon fiable.
- Plus la contrainte de probabilité de fausse alarme est forte ( $P_{fa}^{detect}$  faible), plus les performances se dégradent. Nous constatons des pertes sur  $D$  et NJR d'environ 8 et 0.4 dB, respectivement, en divisant à chaque fois  $P_{fa}^{detect}$  d'un facteur 10.
- Le brouilleur STJ est beaucoup mieux détecté que le brouilleur BJ, avec des gains sur  $D$  et NJR d'environ 16 et 1.5 dB, pour  $P_{fa}^{detect}$  fixé. Cela se comprend dans la mesure où le signal de brouillage BJ est très proche d'un bruit AWGN et est donc plus difficile à discriminer contrairement au signal de brouillage TJ étant plus caractéristique.



(a) En fonction de  $D$



(b) En fonction du NJR

FIGURE III.2.5. – Performances de détection des brouilleurs Band Jamming et Single Tone Jamming, en fonction de  $D$  et du NJR, pour plusieurs valeurs de probabilité de fausse alarme,  $SF = 7$

### III.2.3.3. Comparaison entre les performances de détection (analytique et simulation) pour les brouilleurs Band et Single Tone Jamming

La Figure III.2.6 compare les performances de détection obtenues en simulation et par les expressions théoriques (équation (III.2.20) pour le brouilleur BJ et équation (III.2.21) pour le brouilleur STJ (hypothèse  $u_0$  entier)) en fonction du NJR. Nous comparons pour trois valeurs  $D \in \{4, 16, 64\}$ . Pour les simulations, nous fixons la probabilité de détection de bin d'intérêt  $P_{fa} = 10^{-3}$  dans l'équation (III.2.12). Pour le brouilleur STJ en simulation,  $u_0$  est entier aléatoire uniforme dans  $\{0, 1, \dots, M - 1\}$ .

A nouveau, nous observons la supériorité de détection du brouilleur STJ sur le brouilleur BJ. Pour  $D = 4$ , la théorie et la simulation collent bien, avec un écart très faible et constant (moins de 0.05 dB). Augmenter  $D$  introduit un biais raisonnable, donnant un écart jusqu'à 1 dB pour le brouilleur STJ et  $D = 64$ .

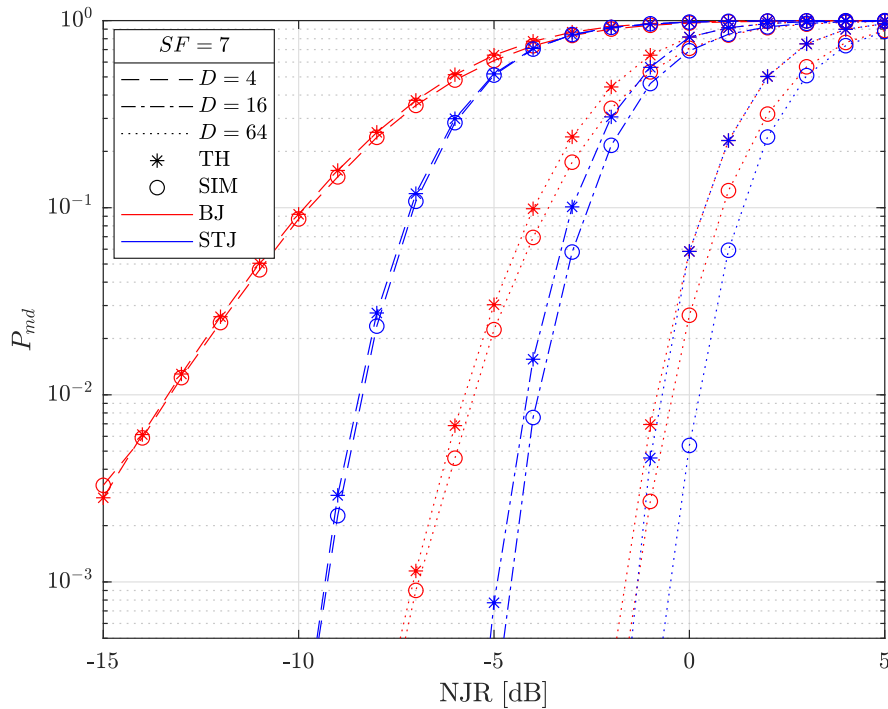


FIGURE III.2.6. – Performances de détection des brouilleurs Band Jamming et Single Tone Jamming en fonction du NJR et  $D$  – comparaison entre les expressions analytiques et la simulation,  $SF = 7$

### III.2.3.4. Impact du nombre de composantes fréquentielles sur la détection du brouilleur Tone Jamming

La Figure III.2.7 montre l'impact du nombre de composantes de brouillage TJ ( $V$ ) sur les performances de détection du brouilleur TJ en fonction du NJR. Nous considérons les valeurs  $V \in \{1, 2, 3, 4\}$ ,  $D = 8$ ,  $P_{fa}^{detect} = 10^{-5}$ , et nous affichons les performances de détection du brouilleur BJ pour pouvoir comparer. De plus, pour  $V > 1$ , la loi de probabilité  $f_{Z_{H_1}}^{MTJ}(t)$  (et donc sa fonction de répartition) est estimée de façon numérique

par tirages de Monte-Carlo puisqu'il n'y a pas d'expression analytique dans la littérature.

Nous pouvons conclure que passer de  $V = 1$  à  $V > 1$  engendre une perte de performances non négligeable. Cela vient du fait que les bins dans la DFT ont une déformation beaucoup plus variable en fonction de  $n$  lorsque  $V > 1$  (voir Figure III.2.1). Les performances de détection dépendent donc grandement des bins  $n_d$  choisis dans l'équation (III.2.9). Certaines valeurs de magnitude lues engendreront un biais important dans la statistique finale  $z$  dans l'équation (III.2.9). Ainsi, avoir  $V > 2$  ne changera pas beaucoup les performances, comme nous pouvons le constater sur la figure avec  $V = 3$  donnant des performances un peu plus élevées que  $V \in \{2, 4\}$ .  $V \in \{3, 4\}$  donnent légèrement de meilleures performances que celles du brouilleur BJ.

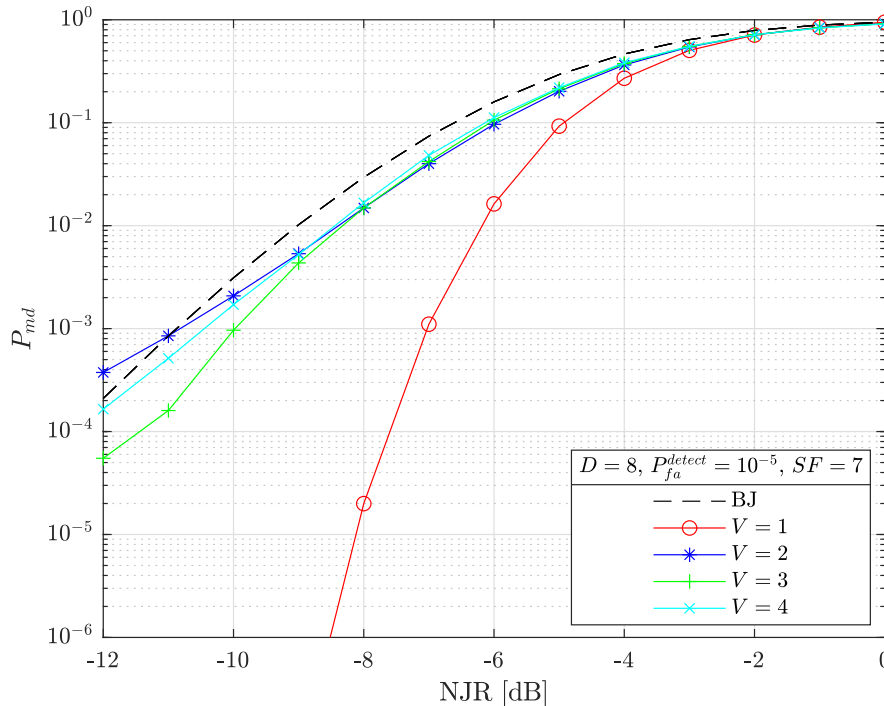


FIGURE III.2.7. – Performances de détection du brouilleur Tone Jamming en fonction du NJR et du nombre de composantes de brouillage,  $SF = 7$

Pour conclure sur cette Section III.2, nous pouvons récapituler les points importants suivants :

- Un brouilleur TJ est plus efficace qu'un brouilleur BJ pour impacter la démodulation.
- La détection d'un brouilleur STJ ( $V = 1$ ) est plus efficace que celle d'un brouilleur BJ. Si le brouilleur TJ utilise plusieurs composantes fréquentielles ( $V \geq 2$ ), les performances de détection se dégradent fortement, pour se rapprocher de celles du brouilleur BJ.
- Finalement, il sera beaucoup plus efficace de perturber efficacement la démodulation en choisissant un signal de brouillage ayant les mêmes propriétés qu'un signal LoRa (voir Section II.1).



### III.3. Schéma d'auto-brouillage LoRa partie 1 : modèle, architecture et paramètres

Dans cette section, nous présentons le modèle, l'architecture et les différents paramètres de notre schéma d'auto-brouillage LoRa, améliorant la confidentialité et la discrétion de la communication. Nous présentons d'abord quelques travaux dans la littérature portant sur la même thématique en Section III.3.1, puis le scénario de communication considéré en Section III.3.2. Nous présentons ensuite en Section III.3.3 la forme d'onde d'auto-brouillage proposée, sa démodulation ainsi que ses propriétés. Une amélioration de cette dernière est présentée en Section III.3.4, visant à réduire le PAPR, phénomène de distorsion pouvant fortement limiter les capacités d'implémentation sur de vrais équipements. Les principales notations utilisées sont reportées dans le Tableau III.3.1 et celles utilisées précédemment sont consultables dans le Tableau I.2.1.

$U$	Nombre de symboles d'auto-brouillage	$m_u$	$u^{\text{ème}}$ délai du canal virtuel
$u$	Indice de symbole d'auto-brouillage	$\epsilon_u$	Espacement entre le $u^{\text{ème}}$ et $u^{\text{ème}} + 1$ symbole d'auto-brouillage
$\mathbf{m}$	Vecteur des délais du canal virtuel	$P_{jam} = 1/U$	Puissance de chaque symbole d'auto-brouillage
$x_{a,jam}[k]$	Forme d'onde auto-brouillée associée au symbole $a$	$S_{jam}[k]$	Composante d'auto-brouillage
$\tilde{R}_{jam}[n]$	DFT LoRa de la forme d'onde auto-brouillée	$\mathbf{cc1}$	Démodulation par inter-corrélation circulaire classique
$F_{ccl}[m]$	Inter-corrélation circulaire classique	$\hat{a}_{ccl}$	Symbole estimé par inter-corrélation circulaire classique
$A_I$	Pic maximal d'interférence d'inter-corrélation circulaire	$A_{max}^{interf}$	Contrainte de pic maximal d'interférence d'inter-corrélation circulaire
$\epsilon_{min}$	Espacement minimal entre symboles d'auto-brouillage		
$\mathbf{ccm}$	Démodulation par inter-corrélation circulaire modifiée	$F_{ccm}[m]$	Inter-corrélation circulaire modifiée



$\hat{a}_{ccm}$	Symbole estimé par inter-corrélation circulaire modifiée		
$f$	Facteur de correction du PAPR	$V_{jam}[k]$	Composante de correction du PAPR
$x_{a,jam,mod}[k]$	Forme d'onde auto-brouillée avec correction du PAPR	$\tilde{R}_{jam,mod}[n]$	DFT LoRa de la forme d'onde auto-brouillée avec correction du PAPR
$F_{ccl,mod}[m]$	Inter-corrélation circulaire classique avec correction du PAPR	$F_{ccm,mod}[m]$	Inter-corrélation circulaire modifiée avec correction du PAPR
$\mathcal{S}_{STO_{frac}}$	Ensemble des symboles candidats	$\nu$	Nombre de blocs d'écart par rapport à celui de début de trame
$\lambda_{preamble}$	Seuil de détection de préambule LoRa	$p$	Indice de bloc de symbole
$c_p$	Nombre d'échantillons de réaligement des bornes temporelles	$\Delta$	Facteur de réduction de complexité du schéma de réaligement des bornes temporelles
$\mathcal{B}(\Delta)$	Ensemble de décalages candidats pour le réaligement des bornes temporelles	$STO_{residue}(\Delta)$	Résidu STO après réaligement des bornes temporelles

TABLE III.3.1. – Principales notations utilisées dans la Section III.3

### III.3.1. Travaux sur la sécurisation de la couche physique LoRa dans la littérature

Dans la littérature, la majorité des travaux ont porté sur l'étude des brouilleurs d'attaque visant à perturber le plus possible la démodulation du récepteur légitime. Ces brouilleurs, nommés brouilleurs réactifs reposent sur l'émission de signaux LoRa afin de créer une collision avec le signal d'intérêt, empêchant la bonne démodulation pour le récepteur légitime. Cette méthode est beaucoup plus efficace que les brouilleurs classiques de type Band et Tone Jamming (voir Section III.2).

Dans [150, 151, 152, 153], un brouilleur réactif est implémenté sur des transceivers LoRa commerciaux. Le brouilleur doit être capable de correctement détecter le signal d'intérêt et d'émettre ensuite le signal de brouillage LoRa le plus rapidement possible, afin que la collision soit efficace (signal de brouillage aligné temporellement avec celui d'intérêt). Un module de détection du signal d'intérêt ou Channel Activity Detection (CAD) basé sur la lecture du Received Signal Strength Indication (RSSI) est proposé en ce sens. Dans chacun des articles, les auteurs évaluent les performances du brouilleur en évaluant les capacités de détection, le délai de transmission du signal de brouillage et l'impact sur la démodulation, en fonction des différents paramètres de transmission : largeur de bande, SF et puissance de brouillage. Les principales conclusions sont que l'impact

est efficace, si le brouilleur utilise la même valeur de SF, la même bande, une puissance de brouillage équivalente à celle du signal d'intérêt et un bon alignement. Les auteurs dans [153] étudient plus en détail l'effet du désalignement, ainsi que des imperfections du matériel comme le CFO, pouvant réduire les performances de brouillage. Les compromis entre coût énergétique, coût matériel et efficacité du brouilleur sont intensivement discutés.

Les auteurs dans [154] proposent de bloquer l'accès au réseau d'un équipement LoRa, grâce à l'utilisation d'un signal de brouillage suffisamment fort permettant de réduire les fluctuations du RSSI. En effet, pour l'accès au réseau, l'équipement génère une clé d'accès aléatoire à partir des fluctuations du RSSI et la soumet à la passerelle. Si la clé reçue par la passerelle est identique à une clé déjà soumise par cet équipement, l'accès lui est refusé. Le signal de brouillage réduit les fluctuations du RSSI, augmentant ainsi la probabilité de générer la même clé. Ce comportement est exploité dans l'article pour la mise en place d'un détecteur de brouilleur et est basé sur une approche statistique.

Assez peu de travaux ont porté sur la confidentialité des transmissions LoRa [155, 156]. Dans [155], les auteurs proposent d'utiliser un schéma de saut de fréquence (Frequency Hopping Spread Spectrum (FHSS)), où la fréquence porteuse change de façon aléatoire, rendant beaucoup plus difficile le bon fonctionnement de brouilleurs réactifs. La solution proposée permet de contrer efficacement le brouilleur tout en permettant d'augmenter la capacité du réseau. Il est proposé dans [156] un schéma de chiffrement ajoutant un décalage aléatoire au symbole de données, inconnu d'un intercepteur. Ce décalage global contient une partie entière décalant d'un nombre entier de bins le pic d'intérêt dans la DFT LoRa et d'une partie fractionnaire diffusant l'énergie sur les bins voisins, rendant la détection plus difficile.

### III.3.2. Scénario de communication LoRa

La Figure III.3.1 présente le scénario considéré pour le schéma d'auto-brouillage. Il est complémentaire à celui évoqué lors de la présentation du principe de confidentialité en Section III.1.1.1. Il y a trois entités : ALICE, BOB et EVE. ALICE et BOB communiquent entre eux en s'échangeant des informations sensibles qui ne doivent pas être interceptées par EVE, présente dans le voisinage de ALICE et BOB. Nous supposons que ALICE est un capteur LoRa émettant de courts messages vers la passerelle BOB. Ce sens de communication est le plus courant en pratique, le capteur renvoyant à intervalle régulier des données de température par exemple. Nous nous intéressons à sécuriser également l'autre sens de communication, constituant généralement des messages de signalisation réseau. EVE a un comportement entièrement passif i.e. ALICE et BOB ne peuvent pas la détecter par des méthodes d'analyses spectrales, et cette dernière est placée suffisamment proche géographiquement pour qu'elle puisse détecter la transmission i.e. avoir des valeurs de SNR cohérentes avec le standard LoRa (voir Figure I.2.27).

Dans l'étude, nous supposons que les canaux séparant les entités sont non sélectifs en fréquence i.e. un seul trajet plus ou moins atténué ( $L = 1$  dans l'équation (II.1.1)). Nous avons déjà étudié en détail l'impact des canaux sélectifs en fréquence sur la démodulation, avec nos contributions [90, 92, 93] (voir Section II.1 et II.2). Nous avons ainsi décidé

de nous concentrer pour cette étude sur les canaux AWGN, afin de bien cerner les performances et comportements du schéma d'auto-brouillage proposé. Les algorithmes d'égalisation développés peuvent être transposés à ce dernier, donnant des résultats analogues à ce qui est obtenu avec une transmission LoRa classique. Nous supposons aussi la *réciprocité* des canaux i.e. le canal entre deux entités est identique, quelque soit le sens de communication (noté par  $c_{A/B}$ ,  $c_{B/A}$ , etc. sur la figure). Cela est généralement le cas en pratique et peut être exploité dans le développement du schéma (voir Section III.3.3.5.2).

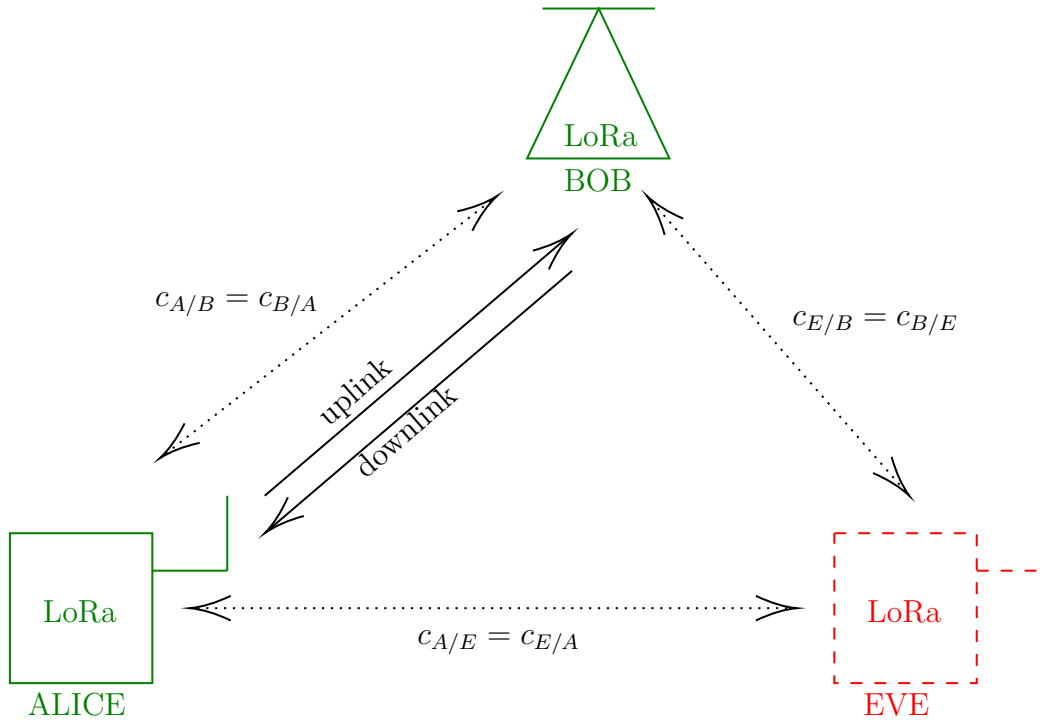


FIGURE III.3.1. – Scénario de communication avec schéma d'auto-brouillage LoRa

### III.3.3. Forme d'onde d'auto-brouillage

#### III.3.3.1. Modulation

La Figure III.3.2 montre une illustration de la forme d'onde d'auto-brouillage pour tout SF. L'émetteur vient superposer  $U - 1$  symboles d'auto-brouillage au symbole d'intérêt, donnant  $U$  symboles présents dans la DFT LoRa. Ces symboles d'auto-brouillage sont à des positions parfaitement connues du récepteur légitime, mais pas par EVE. Ainsi, cette dernière aura de fortes difficultés à démoduler puisqu'elle verra la présence de  $U$  pics dans la DFT, ne sachant pas où se trouve le symbole d'intérêt, contrairement au récepteur légitime qui exploitera de façon constructive l'information des symboles d'auto-brouillage pour démoduler.

Cette approche capitalise sur les résultats de notre étude de l'impact des brouilleurs classiques Band et Tone Jamming sur LoRa, où il est finalement bien plus efficace de perturber la démodulation LoRa avec des signaux LoRa (voir Section III.2), et des travaux dans [156]. Dans ce dernier, les auteurs offrent une solution certes simple et élégante,

mais ne proposent pas de front-end de synchronisation adapté pour le récepteur légitime, élément pourtant fondamental pour une implémentation réelle.

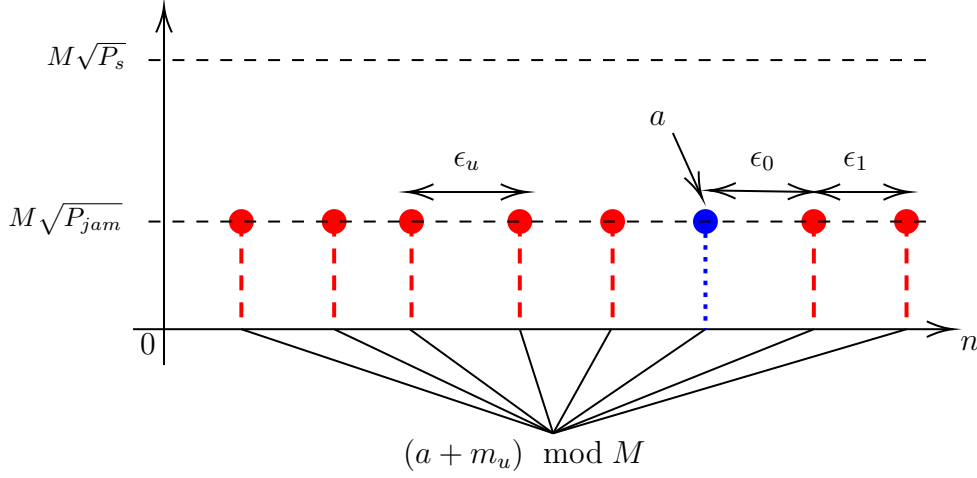


FIGURE III.3.2. – Illustration du principe d'auto-brouillage dans le domaine fréquentiel LoRa

Les  $U$  symboles sont modélisés par un décalage par rapport au symbole d'intérêt  $a$  par :

$$a_{u,jam} = (a + m_u) \bmod M, \quad u \in \{0, 1, \dots, U - 1\} \quad (\text{III.3.1})$$

avec  $m_u$  et  $a_{u,jam}$ , le décalage du  $u^{\text{ème}}$  symbole et le symbole résultant, respectivement. Par convention, le symbole d'indice  $u = 0$  est celui d'intérêt. Nous avons donc  $a_{0,jam} = a$  avec  $m_0 = 0$ . Notons  $\mathbf{m}$ , le vecteur contenant l'ensemble des décalages :

$$\mathbf{m} = [0 \ m_1 \ \dots \ m_{U-1}] \quad (\text{III.3.2})$$

et  $\mathbf{a}_{jam}$ , le vecteur contenant l'ensemble des symboles (bins) présents dans la DFT LoRa :

$$\mathbf{a}_{jam} = [a \ a_{1,jam} \ \dots \ a_{U-1,jam}] \quad (\text{III.3.3})$$

Nous notons aussi  $\epsilon_u$ , l'espacement entre deux symboles consécutifs :

$$\epsilon_u = (a_{u+1,jam} - a_{u,jam}) \bmod M, \quad u \in \{0, 1, \dots, U - 2\} \quad (\text{III.3.4})$$

et son vecteur associé :

$$\boldsymbol{\epsilon} = [\epsilon_0 \ \epsilon_1 \ \dots \ \epsilon_{U-2}] \quad (\text{III.3.5})$$

L'émetteur choisit de répartir la puissance de chaque symbole  $P_{u,jam}$  de façon uniforme. Nous avons ainsi :

$$P_{u,jam} = P_{jam} = \frac{P_s}{U} = \frac{1}{U} \quad (\text{III.3.6})$$

Cette stratégie est optimale au sens de la théorie du jeu [119], où elle est le meilleur compromis entre garantir les meilleures performances de démodulation pour le récepteur légitime et impacter de façon significative EVE.

La Figure III.3.3 montre une illustration de la DFT LoRa de deux symboles auto-brouillés  $a_0 = 10$  et  $a_1 = 74$  pour  $SF = 7$ . Chacun possède des décalages différents, de valeurs  $\mathbf{m}_0 = [0\ 29\ 70\ 107]$  et  $\mathbf{m}_1 = [0\ 15\ 25\ 59]$ . On observe bien sur la figure les positions  $n \in \{10, 39, 80, 117\}$  pour le premier symbole et la permutation circulaire réalisée pour le second symbole, donnant les positions  $n \in \{5, 74, 89, 99\}$ , d'après l'équation (III.3.1).

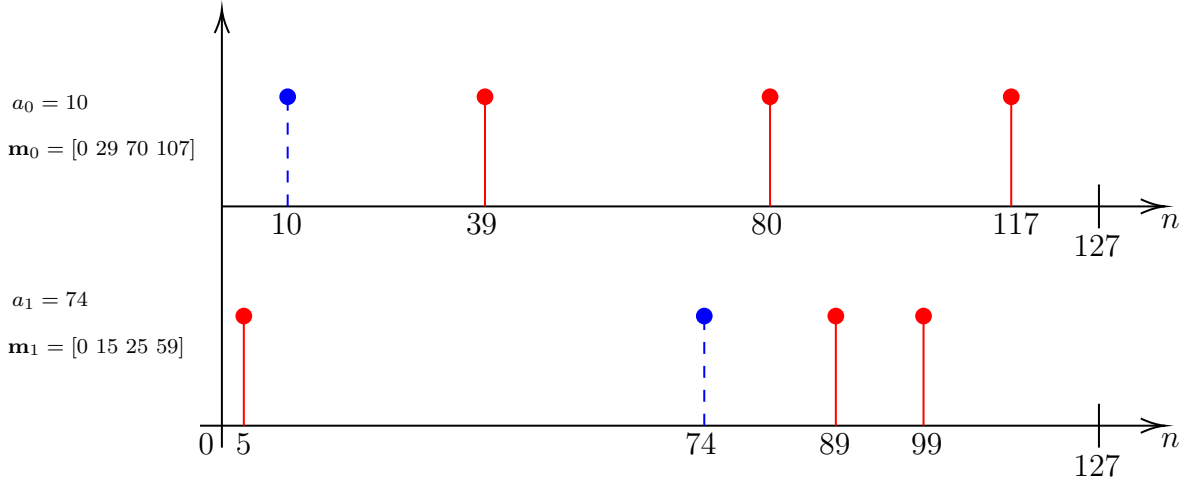


FIGURE III.3.3. – Exemple de symboles auto-brouillés dans le domaine fréquentiel LoRa,  $SF = 7$

L'expression du signal auto-brouillé vaut alors :

$$\begin{aligned}
 x_{a,jam}[k] &= \sqrt{P_{jam}} \sum_{u=0}^{U-1} e^{2j\pi k \left[ \frac{a+m_u}{M} - \frac{1}{2} + \frac{k}{2M} \right]} = \sqrt{P_{jam}} \sum_{u=0}^{U-1} x_{a+m_u}[k] \\
 &= x_a[k] \underbrace{\sqrt{P_{jam}} \sum_{u=0}^{U-1} e^{2j\pi k \frac{m_u}{M}}}_{S_{jam}[k]}
 \end{aligned} \tag{III.3.7}$$

avec  $S_{jam}[k]$ , la composante d'auto-brouillage.

Le schéma d'auto-brouillage peut aussi avoir les deux autres interprétations suivantes :

- Simuler l'effet d'un canal aligné afin de perturber EVE. Par analogie et d'après la Figure II.1.3, le symbole d'intérêt serait le trajet direct et les symboles d'auto-brouillage les répliques d'un canal virtuel aligné ayant les retards  $m_u$ . La différence majeure vient du fait que le vrai canal est inconnu et estimé à partir du préambule connu du récepteur (BOB ou EVE).
- Méthode d'étalement spectral de type Direct Sequence Spread Spectrum (DSSS). En effet, les méthodes DSSS viennent réduire la puissance du signal d'intérêt d'un facteur  $N$  en élargissant sa bande de ce même facteur avec une séquence d'étalement, réduisant de fait les capacités de détection du signal. Ici, le nombre de symboles  $U$  représente le niveau d'étalement spectral ( $N = U$ ) mais dans le domaine fréquentiel LoRa, du fait qu'il y ait la contrainte  $P_{jam} = 1/U$ . Les délais  $m_u$  jouent quant à eux le rôle de la séquence d'étalement.

### III.3.3.2. Format de trame auto-brouillée

Chaque symbole dans la trame est auto-brouillé (symboles de préambule upchirp et downchirp et payload). Notons  $\mathbf{m}_{up}$ ,  $\mathbf{m}_{down}$  et  $\mathbf{m}_{i,payload}$ , les canaux virtuels appliqués aux symboles de préambule upchirp, downchirp et au  $i^{\text{ème}}$  symbole de payload, respectivement, et de valeurs  $m_{u,up}$ ,  $m_{u,down}$  et  $m_{u,i,payload}$ . L'expression du signal de la trame est alors :

$$s[k] = x_{up,jam}[k] + x_{down,jam}[k - N_{up}M] + x_{payload,jam}[k - N_{pre}M] \quad (\text{III.3.8})$$

avec :

$$x_{up,jam}[k] = \sum_{i=0}^{N_{up}-1} x_0[k - iM] \sqrt{P_{jam}} \sum_{u=0}^{U-1} e^{2j\pi[k-iM] \frac{m_{u,up}}{M}} \quad (\text{III.3.9})$$

$$x_{down,jam}[k] = \sum_{i=N_{up}}^{N_{pre}-1} x_0^*[k - iM] \sqrt{P_{jam}} \sum_{u=0}^{U-1} e^{-2j\pi[k-iM] \frac{m_{u,down}}{M}} \quad (\text{III.3.10})$$

$$x_{payload,jam}[k] = \sum_{i=N_{pre}}^{N_{payload}-1} x_{a_i,payload}[k - iM] \sqrt{P_{jam}} \sum_{u=0}^{U-1} e^{2j\pi[k-iM] \frac{m_{u,i,payload}}{M}} \quad (\text{III.3.11})$$

Le symbole de données peut être chiffré en ajoutant un décalage aléatoire inconnu de EVE, comme proposé dans [156] :

$$a_{i,payload,scramb} = (a_{i,payload} + l_{i,payload}) \bmod M \quad (\text{III.3.12})$$

avec  $l_{i,payload}$ , le décalage aléatoire du  $i^{\text{ème}}$  symbole de données  $a_{i,payload}$ . Cette fonction peut-être aussi vue comme une méthode de brouillage binaire ou *scrambling*, régulièrement proposée dans la littérature pour les communications DSSS [157], le chiffrement d'images ou de flux vidéo [158, 159], par exemple.

Les méthodes de chiffrement classiques reposent généralement sur l'hypothèse implicite que le flux binaire intercepté par EVE est obtenu sans erreur de démodulation i.e.  $\hat{a}_i = a_{i,payload,scramb}$ . Cela pourrait avantager des méthodes aveugles de compromission de clé (ici les canaux virtuels et décalages  $l_{i,payload}$ ). Le schéma d'auto-brouillage apporte une contribution complémentaire à la cryptographie en garantissant que EVE ne puisse pas facilement démoduler et donc retrouver exactement  $\hat{a}_i = a_{i,payload,scramb}$ . Ce point est développé plus en détail dans la Section III.4.4.3.

### III.3.3.3. Démodulation par corrélation circulaire

Dans cette section, nous présentons la méthode de démodulation employée par le récepteur légitime ainsi que les contraintes à respecter sur le choix des valeurs des canaux virtuels, afin de préserver de bonnes performances de démodulation pour ce dernier. D'après l'équation (III.3.7), le symbole reçu après opération downchirp et DFT a pour

expression :

$$\tilde{R}_{jam}[n] = \tilde{X}_{a,jam}[n] + \tilde{W}[n] = M\sqrt{P_{jam}} \sum_{u=0}^{U-1} \delta[n - (a + m_u)] + \tilde{W}[n] \quad (\text{III.3.13})$$

Une solution simple de démodulation pour le récepteur légitime et inspirée des travaux dans [69] est de réaliser une inter-corrélation circulaire entre le symbole démodulé et le canal virtuel associé :

$$F_{ccl}[m] = \sum_{n=0}^{M-1} \left| \tilde{R}_{jam}[n] \tilde{S}_{ref}[(n - m) \bmod M] \right| \quad (\text{III.3.14})$$

avec :

$$\tilde{S}_{ref}[n] = \frac{1}{\sqrt{P_{jam}}} \sum_{u=0}^{U-1} \delta[n - m_u] \quad (\text{III.3.15})$$

et  $m$  désignant l'indice d'inter-corrélation. Le terme ccl dans l'équation (III.3.14) désigne l'inter-corrélation circulaire classique. Le symbole est alors estimé par :

$$\hat{a}_{ccl} = \arg \max_m F_{ccl}[m] \quad (\text{III.3.16})$$

Ce récepteur sera noté à partir de maintenant **cc1**, par soucis de concision.

Notons que ce dernier est non-cohérent, d'après l'équation (III.3.14). Notre étude du récepteur cohérent LoRa RAKE (voir Section II.2) a mis en évidence la bonne viabilité des récepteurs non-cohérents. En effet, bien que ces derniers soient sous-optimaux dans les canaux plats AWGN purs (voir Figure I.2.27), ils se révèlent cependant être très intéressants pour un usage réel, avec une plus faible sensibilité aux désynchronisations temporelles et fréquentielles, et nécessitant une complexité calculatoire plus faible.

La Figure III.3.4 montre un exemple de démodulation **cc1** pour  $U = 4$ ,  $\mathbf{m} = [0 \ 4 \ 10 \ 84]$ ,  $a = 0$ ,  $SNR_{dB} = 0$  et  $SF = 7$ . A gauche, le résultat de la DFT LoRa (équation (III.3.13)) et à droite, la démodulation **cc1**. Nous voyons que sans la connaissance préalable du canal virtuel, EVE verra dans de bonnes conditions de SNR  $U$  pics dans la DFT (quatre sur la figure), rendant la démodulation difficile. En revanche, pour le récepteur légitime ALICE ou BOB, grâce à **cc1**, le symbole est parfaitement démodulé (bin avec motif 'x' sur la figure). On observe la présence de pics parasites sur la **cc1** (bins avec motif '+'). Ces pics parasites doivent être atténués afin d'impacter le moins possible les performances de démodulation. Ainsi, les valeurs du canal virtuel ne doivent pas être choisies totalement aléatoirement, mais doivent respecter des contraintes qui sont présentées dans la partie suivante.

### III.3.3.4. Contraintes sur le choix des symboles d'auto-brouillage

Dans cette partie, nous négligeons l'influence du bruit dans l'équation (III.3.13) i.e.  $\tilde{W}[n]$  et donc  $\tilde{R}_{jam}[n] = \tilde{X}_{a,jam}[n]$ .

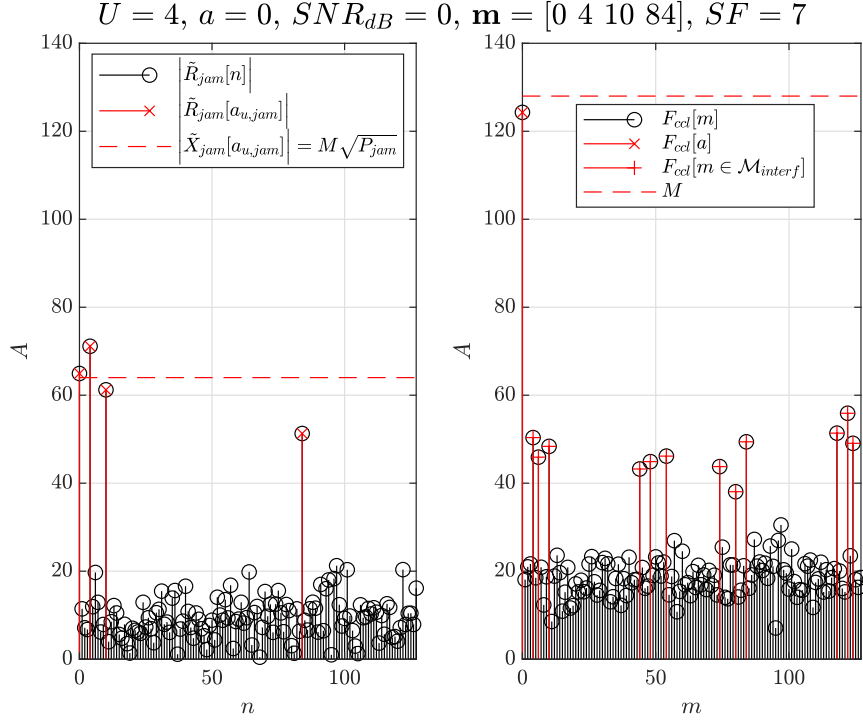


FIGURE III.3.4. – Exemple de démodulations classique et ccl d'un symbole auto-brouillé,  $SF = 7$

D'après les équations (III.3.14) et (III.3.15), les pics d'interférence d'inter-corrélation circulaire sont aux bins contenus dans l'ensemble  $\mathcal{M}_{interf}$  avec :

$$\mathcal{M}_{interf} = \sum_{\substack{\{u_1, u_2\}=0 \\ u_1 \neq u_2}}^{U-1} \delta[m - (m_{u_1} - m_{u_2}) \bmod M] \quad (\text{III.3.17})$$

et ont des amplitudes pouvant prendre leurs valeurs dans l'ensemble :

$$\mathcal{A}_{interf} = \left\{ \frac{1}{U}, \frac{2}{U}, \dots, 1 \right\} \quad (\text{III.3.18})$$

en supposant l'équation (III.3.14) normalisée i.e.  $F_{ccl}[m] = F_{ccl}[m]/M$ .

Pour un canal virtuel donné, nous notons  $A_I$ , l'amplitude maximale normalisée rencontrée dans les bins  $m \neq a$  de ccl par :

$$A_I = \max_m \sum_{\{u_1, u_2\}=0}^{U-1} \frac{1}{U} \delta[m - (m_{u_1} - m_{u_2}) \bmod M] \quad (\text{III.3.19})$$

Les performances se dégraderont avec l'augmentation des amplitudes des pics d'interférence d'inter-corrélation (proches de 1), et de leur nombre dans la DFT. Le cas le plus défavorable étant  $A_I = 1$ , où le récepteur légitime aura une incertitude maximale entre le symbole d'intérêt et un des pics d'interférence. Ce cas se présente si tous les symboles sont équidistants i.e.  $\epsilon_u = \epsilon_{u+1} \forall u \in \{0, 1, \dots, U-2\}$ . Nous choisissons comme critère pour réduire l'impact sur les performances (et éliminer les cas d'équidistance)



### III.3. Schéma d'auto-brouillage LoRa partie 1 : modèle, architecture et paramètres

de limiter l'amplitude maximale des pics d'interférence. Nous devons donc satisfaire la contrainte :

$$A_I \leq A_{max}^{interf} \quad (\text{III.3.20})$$

avec  $A_{max}^{interf}$ , la valeur maximale  $A_I$  autorisée. En effet, de façon similaire à l'étude du canal multi-trajets à décroissance exponentielle en Section II.1.3.2, le pic d'interférence maximal contribuera majoritairement dans la dégradation des performances de démodulation, ceux inférieurs peuvent donc être négligés pour le choix du critère. L'ensemble des amplitudes présentes avec la contrainte devient alors :

$$\mathcal{A}_{interf}(A_{max}^{interf}) = \left\{ \frac{1}{U}, \frac{2}{U}, \dots, \frac{u'}{U} \right\} \quad (\text{III.3.21})$$

avec  $u'$ , l'entier le plus grand tel que  $u'/U \leq A_{max}^{interf}$ .

La Figure III.3.5 montre l'impact de  $A_{max}^{interf}$  sur le SER de cc1 pour  $U = 8$  avec synchronisation parfaite et  $SF = 7$ . Pour chaque tirage, nous choisissons aléatoirement un canal virtuel respectant la contrainte  $A_I \leq A_{max}^{interf}$  avec  $A_{max}^{interf} \in \{0.125, 0.25, \dots, 0.75\}$  et les performances sont moyennées sur les tirages. Nous pouvons voir que pour  $A_{max}^{interf} \leq 0.5$ , l'impact est faible, avec une perte inférieure à 0.5 dB à  $SER = 10^{-4}$ . Augmenter au delà dégrade de façon beaucoup plus marquée, avec une perte atteignant presque 3 dB à  $SER = 10^{-4}$  pour  $A_{max}^{interf} = 0.75$ . Choisir en pratique  $A_{max}^{interf} = 0.5$  est un bon compromis entre performances et diversité de canal virtuel. En effet, plus  $A_{max}^{interf}$  est faible (contrainte forte), moins il y a de canaux virtuels possibles satisfaisant cette dernière (voir Section III.3.3.5.3).

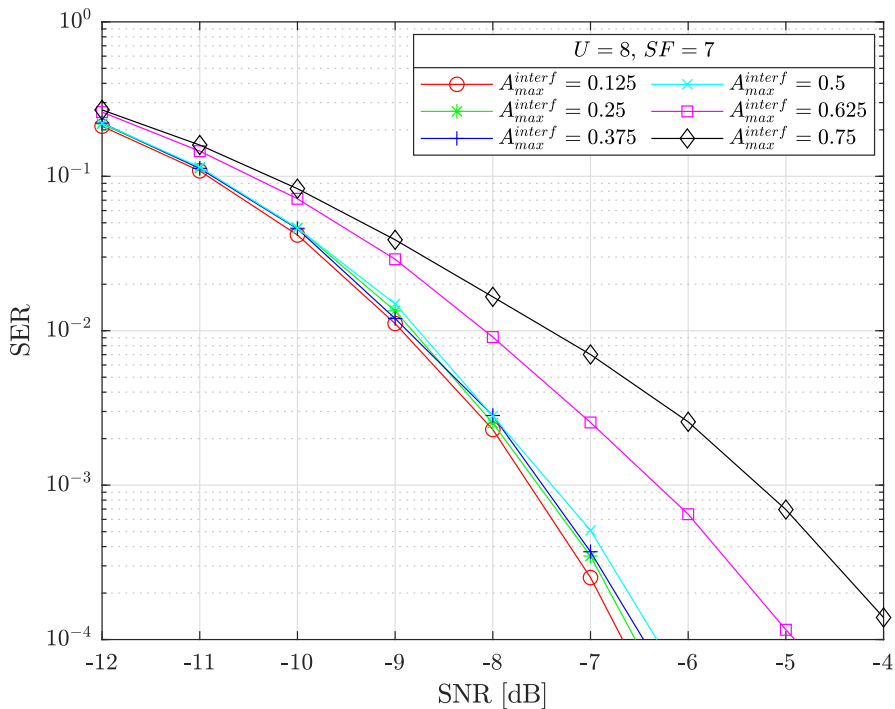


FIGURE III.3.5. – Impact de  $A_{max}^{interf}$  sur les performances de démodulation cc1,  $SF = 7$

Une autre contrainte importante à respecter est d'avoir un espacement minimal d'au

moins un bin entre les symboles, soit :

$$\epsilon_u > 1, \quad \forall u \in \{0, 1, \dots, U - 2\} \quad (\text{III.3.22})$$

Nous le notons dans la forme plus compacte  $\epsilon_{min} > 1$ . En effet, avoir des pics côte à côte impacte fortement l'algorithme de synchronisation  $STO_{frac}$  utilisé pour le schéma d'auto-brouillage et est discuté en Section III.4.1.5 en étudiant l'impact sur ce dernier lorsque la contrainte n'est pas respectée. A partir de maintenant, nous choisissons pour le reste du mémoire  $A_{max}^{interf} = 0.5$  et  $\epsilon_{min} > 1$ , sauf indication contraire.

### III.3.3.5. Génération des canaux virtuels et du décalage de symbole de données

Dans cette partie, nous présentons comment l'émetteur et le récepteur légitime génèrent les canaux virtuels et le décalage aléatoire de symbole de données. Ils sont extraits à partir d'un flux binaire qui doit être le moins corrélé possible i.e. avoir idéalement  $P[b = 0] = P[b = 1] = 1/2$  avec  $b$ , le bit dans le flux binaire. Dans la littérature, deux approches sont possibles : 1) utilisation d'un générateur reposant sur une méthode de cryptographie de type Advanced Encryption System (AES) et 2) extraction d'un flux binaire à partir des propriétés aléatoires du canal de transmission. Nous les présentons dans ce qui suit.

#### III.3.3.5.1. Générateur AES

L'algorithme AES est utilisé dans le standard LoRa au niveau des couches supérieures pour la génération de clés de chiffrement de données [60]. Ce dernier peut tout à fait être réutilisé ici. En effet, certains travaux dans la littérature ont proposé des contributions en ce sens. Dans [160], le coût énergétique de l'AES classique sur le fonctionnement de LoRaWAN est évalué en étudiant l'impact de la taille de la clé de chiffrement de 128, 192 ou 256 bits. D'autres travaux ont proposé des améliorations visant à réduire le coût énergétique tout en préservant la confidentialité, dans [161] par exemple.

#### III.3.3.5.2. Extraction à partir du canal de transmission

Une autre approche prometteuse consiste à exploiter les propriétés aléatoires du canal de transmission, pouvant alors servir de générateur binaire aléatoire [162, 163]. Les fluctuations au cours du temps de la puissance du signal reçu (Received Signal Strength Indication (RSSI)) peuvent être une bonne source d'aléa [164, 165]. Les variations de la phase d'un signal, aléatoire uniforme sur  $[0; 2\pi[$ , peuvent aussi être utilisées [166, 167]. Ces méthodes reposent sur deux hypothèses fondamentales : 1) la réciprocité du canal entre ALICE et BOB (considérée pour le scénario de communication d'auto-brouillage, voir Section III.3.2) et 2) la décorrélation des canaux  $c_{A/B}$  (entre l'émetteur légitime ALICE et le récepteur légitime BOB) et  $c_{A/E}$  (entre l'émetteur légitime ALICE et EVE), afin que cette dernière ne puisse pas extraire la même séquence binaire. La deuxième hypothèse est valable, à condition que EVE soit à une distance d'au moins une demi longueur d'onde du récepteur.

Ces deux hypothèses ont été validées expérimentalement à de multiples reprises. Par exemple, les auteurs dans [168] ont démontré la validité de ces deux hypothèses pour des signaux de type radio FM, où l'émetteur et le récepteur légitime sont assez éloignés

géographiquement. Les différentes méthodes de la littérature proposent des débits d'extraction binaire de l'ordre de quelques dizaines de bits par seconde, et des mécanismes de réconciliation sont utilisés afin de corriger les éventuelles erreurs dans les flux binaires obtenus par ALICE et BOB [169]. La réconciliation doit être sécurisée de façon à ce que EVE ne puisse pas intercepter le flux binaire, et peut-être réalisée par exemple en utilisant du CRC. Une couche supplémentaire de confidentialité peut-être appliquée au flux via des méthodes de hachage (hash) [162].

### III.3.3.5.3. Algorithme de génération de canaux virtuels

Les canaux virtuels sont générés à partir des propriétés aléatoires du canal de transmission et sont parfaitement indépendants des symboles de données à transmettre. Par lecture des phases aléatoires d'un signal pilote par exemple, l'émetteur et le récepteur peuvent générer un flux binaire aléatoire. A partir de ce flux, les canaux virtuels sont ensuite créés. Afin que le récepteur puisse correctement démoduler, ce dernier doit avoir exactement le même canal virtuel que l'émetteur et donc le même flux binaire. Cela nécessite la réciprocité des canaux  $c_{A/B}$  et  $c_{B/A}$  i.e. les canaux ont les mêmes variations entre les deux entités, et que des mécanismes de correction soient utilisés, afin de corriger les éventuelles erreurs entre les flux binaires constitués par les deux entités. On suppose que ces contraintes sont satisfaites et que les entités ont donc un flux binaire parfaitement identique, converti ensuite en entiers, de la même manière que pour un symbole (paquets de SF bits, même SF que pour la transmission). Les entiers sont notés  $b_v$ , avec  $v \in \{0, 1, \dots\}$ , l'indice de l'entier et  $b_v \in \{0, 1, \dots, M - 1\}$ . Nous nous intéressons ici à créer un algorithme simple permettant de générer les canaux virtuels à partir des  $b_v$ , satisfaisant la contrainte d'espacement entre deux symboles consécutifs  $\epsilon_{min} > 1$  et celle d'amplitude maximale d'interférence d'inter-corrélation circulaire  $A_I \leq A_{max}^{interf}$ .

Afin de rendre clair les explications, nous montrons en Figure III.3.6 les différentes étapes de l'exécution de l'algorithme, pour la génération d'un canal virtuel avec  $SF = 7$  et  $U = 4$ . Rappelons que le premier trajet virtuel vaut  $m_0 = 0$ . Ainsi, l'algorithme doit donc générer  $U - 1 = 3$  autres trajets virtuels.

A l'initialisation, l'algorithme forme un bloc à partir de trois entiers consécutifs dans le flux, noté  $\mathbf{S}$ , et de valeurs  $S_b$  avec  $b \in \{0, 1, 2\}$ . Nous supposons ici  $\mathbf{S} = [b_0 \ b_1 \ b_2] = [27 \ 65 \ 99]$ . Le premier trajet virtuel  $m_0$  est positionné en  $n = 0$ . Afin de respecter la contrainte  $\epsilon_{min} > 1$ , les bins voisins gauche et droite sont verrouillés. Il reste donc  $128 - 3 = 125$  bins disponibles pour l'allocation du trajet virtuel suivant, et ont pour valeurs l'ensemble  $\mathcal{L} = \{2, 3, \dots, 126\}$ . La  $l^{\text{ème}}$  valeur de  $\mathcal{L}$  est notée  $L_l$ .

A la première itération ( $u = 1$ ), le second trajet virtuel  $m_1$  est créé, comme la  $S_0^{\text{ème}}$  valeur dans  $\mathcal{L}$ , avec permutation circulaire :

$$m_1 = L_c = 29, \quad \text{avec } c = S_0 \bmod (M - 3u) = 27 \bmod 125 = 27 \quad (\text{III.3.23})$$

De même, les bins voisins gauche et droits du nouveau bin obtenu en  $n = m_1 = 29$  sont verrouillés, pour donner  $\mathcal{L} = \{2, 3, \dots, 27, 31, \dots, 126\}$ .

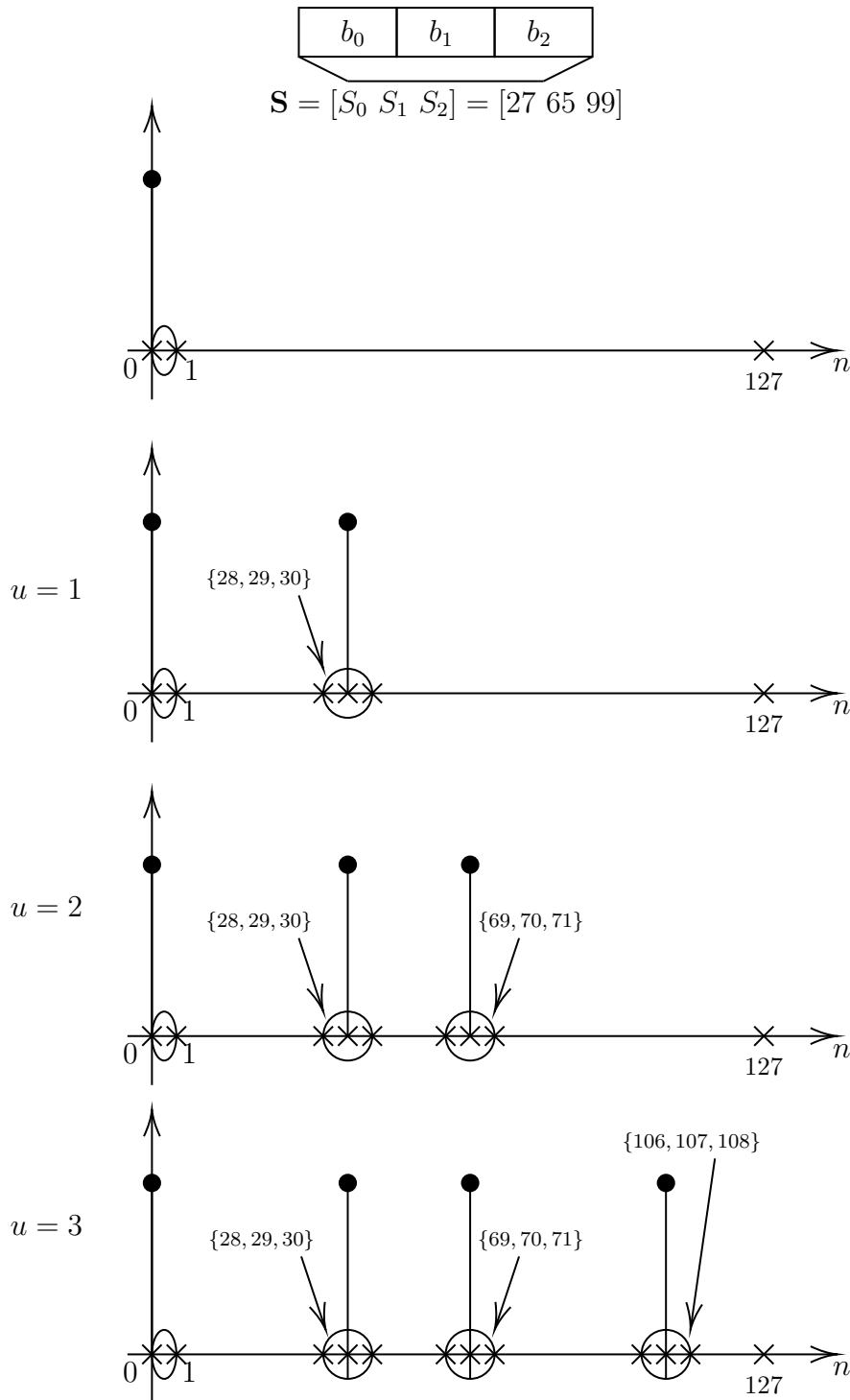


FIGURE III.3.6. – Exemple d'exécution de l'algorithme de génération de canal virtuel

A la deuxième itération ( $u = 2$ ), le troisième trajet virtuel  $m_2$  est produit, comme la  $S_1^{\text{ème}}$  valeur dans  $\mathcal{L}$  :

$$m_2 = L_c = 70, \quad \text{avec } c = S_1 \pmod{(M - 3u)} = 65 \pmod{122} = 65 \quad (\text{III.3.24})$$

et  $\mathcal{L} = \{2, 3, \dots, 27, 31, \dots, 68, 72, \dots, 126\}$ . Le dernier trajet virtuel  $m_3$  est obtenu de

la même manière à la dernière itération ( $u = 3$ ) :

$$m_3 = L_c = 107, \quad \text{avec } c = S_2 \pmod{(M - 3u) = 99} \pmod{119} = 99 \quad (\text{III.3.25})$$

Nous avons donc  $\mathbf{m} = [0 \ 29 \ 70 \ 107]$ . Comme à chaque itération, nous éliminons 3 valeurs dans  $\mathcal{L}$ , la taille de l'ensemble à chaque itération est donc :

$$|\mathcal{L}| = M - 3u \quad (\text{III.3.26})$$

Une fois les trajets virtuels générés, la contrainte  $A_I \leq A_{max}^{interf}$  est vérifiée en calculant  $A_I$  dans l'équation (III.3.19). Si elle est satisfaite (c'est le cas ici pour  $A_{max}^{interf} = 0.5$ , où nous avons  $A_I = 0.25$ ), l'algorithme est terminé et le canal virtuel suivant peut-être généré. Sinon, tant que la contrainte n'est pas respectée, on ré-exécute la procédure, mais avec le bloc  $\mathbf{S}$  initial ayant subi une permutation circulaire droite, d'un indice à chaque fois, noté  $\mathbf{S}_p$ , avec  $\mathbf{S}$  ayant subi  $p$  permutations. Ici, nous aurions par exemple  $\mathbf{S}_1 = [b_2 \ b_0 \ b_1] = [99 \ 27 \ 65]$ . Nous avons donc  $U - 2$  permutations possibles. Si au bout des permutations, la contrainte n'est toujours pas respectée, le bloc d'entiers consécutif suivant est testé en réinitialisant la permutation à  $p = 0$ , et ainsi de suite.

L'algorithme 2 donne la structure algorithmique généralisée pour tout SF et  $U$ .

---

**Algorithm 2:** Algorithme de génération de canal virtuel

---

**inputs:**  $A_{max}^{interf}$  %amplitude maximale d'interférence d'inter-corrélation circulaire  
 $M$  %ordre de modulation LoRa  
 $\mathbf{S}_0$  %bloc d'entiers aléatoires extraits sans permutation circulaire droite

- 1  $U = |\mathbf{S}_p| + 1$  %taille du canal virtuel à générer
- 2  $p = 0$  %indice de permutation
- 3  $A_I = 1$
- 4 **while**  $A_I > A_{max}^{interf}$  **do**
- 5     **if**  $p \geq U - 1$  **then**
- 6         **return**  $\mathbf{m} = \emptyset$
- 7      $\mathbf{m} = \mathbf{0}$  %vecteur du canal virtuel
- 8      $\mathcal{L} = \{0, 1, \dots, M - 1\}$  %positions des bins disponibles dans la DFT LoRa
- 9     élimination des bins  $\{0, 1, M - 1\}$  dans  $\mathcal{L}$
- 10    **for**  $u = 1$  **to**  $U - 1$  **do**
- 11         sélection de l'entier d'indice  $u - 1$  dans  $\mathbf{S}_p$  :  $S_{u-1}$
- 12         génération du  $u^{\text{ème}}$  trajet virtuel :  $m_u := S_{u-1} \pmod{|\mathcal{L}|}$
- 13         ajout du trajet virtuel  $m_u$  dans le vecteur  $\mathbf{m}$
- 14         élimination des bins  $n \in \{m_u - 1, m_u, m_u + 1\} \pmod{M}$  dans  $\mathcal{L}$
- 15     calcul de  $A_I$
- 16     **if**  $A_I \leq A_{max}^{interf}$  **then**
- 17         **return**  $\mathbf{m}$
- 18     **else**
- 19          $p = p + 1$
- 20         application permutation circulaire droite :  $\mathbf{S}_p$

---

La Figure III.3.7 montre les probabilités de générer un canal virtuel ne respectant pas la

contrainte  $A_I \leq A_{max}^{interf}$  pour les cas 1) du premier coup i.e. avoir  $p = 1$  dans l'algorithme 2 et 2) au bout de toutes les permutations possibles ( $p = U - 1$ ), en fonction de  $A_{max}^{interf}$ , pour  $U \in \{5, 10, 15, 20\}$  et  $SF = 7$ . Elles sont notées  $P[A_I > A_{max}^{interf}]$  et  $P[A_{I,recon} > A_{max}^{interf}]$ , respectivement. Par structure algorithmique, la contrainte  $\epsilon_{min} > 1$  est toujours respectée.

D'après la Figure III.3.7, nous pouvons voir que plus la contrainte  $A_I \leq A_{max}^{interf}$  est stricte ( $A_{max}^{interf}$  faible), plus la probabilité de non respect de cette dernière à la première itération est élevée. Nous avons des probabilités supérieures à 0.17 pour  $A_{max}^{interf} \leq 0.3$  pour toutes les valeurs de  $U$ . La méthode par permutation circulaire se révèle être assez efficace, surtout si  $A_{max}^{interf}$  est intermédiaire et  $U$  assez élevé. Nous avons par exemple pour  $U = 20$  et  $A_{max}^{interf} = 0.3$ ,  $P[A_I > A_{max}^{interf}] \approx 0.63$ . Les permutations font tomber cette probabilité à environ 0.01. Nous remarquons la présence d'un plateau entre  $A_{max}^{interf} = 0.2$  et  $A_{max}^{interf} = 0.3$  pour  $U = 5$ . Cela vient du fait que pour  $U = 5$ , nous avons  $\mathcal{A}_{interf} = \{0.2, 0.4, 0.6, 0.8, 1\}$ .  $A_{max}^{interf} = 0.3$  ne faisant pas partie de l'ensemble, les performances seront donc identiques à celles de  $A_{max}^{interf} = 0.2$ .

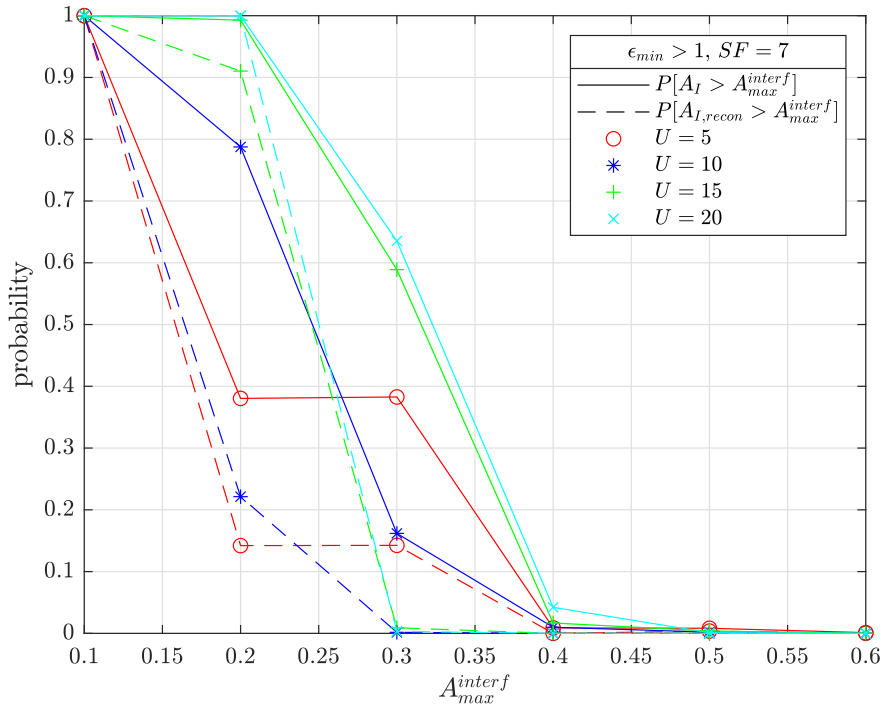


FIGURE III.3.7. – Probabilités de non satisfaction de la contrainte  $A_I \leq A_{max}^{interf}$  de l'algorithme de génération de canal virtuel,  $SF = 7$

### III.3.3.6. Démodulation par corrélation circulaire améliorée

La démodulation `ccl` a l'avantage d'être simple et peu coûteuse à implémenter. En effet, l'inter-corrélation circulaire peut-être réalisée avec des algorithmes très optimisés reposant sur l'implémentation informatique de la DFT, avec l'algorithme Fast Fourier Transform (FFT) :

$$F_{ccl}[m] = \text{IFFT} \left\{ \text{FFT} \{ \tilde{\mathbf{R}}_{jam} \}[m] \times \left( \text{FFT} \{ \tilde{\mathbf{S}}_{ref} \}[m] \right)^* \right\} \quad (\text{III.3.27})$$

avec  $\text{FFT}\{\cdot\}$  et  $\text{IFFT}\{\cdot\}$ , les fonctions de DFT et DFT inverse numériques, respectivement.  $\tilde{\mathbf{R}}_{jam}$  et  $\tilde{\mathbf{S}}_{ref}$  sont les vecteurs de  $\tilde{R}_{jam}[n]$  et  $\tilde{S}_{ref}[n]$  dans l'équation (III.3.14).

Cependant, de part sa nature purement non-cohérente, elle a le gros inconvénient de voir sa sensibilité au bruit AWGN augmenter à mesure que  $U$  croît. Cela limite donc fortement son application en pratique. Ainsi, la variante **ccm** (inter-corrélation circulaire modifiée) est proposée, réduisant considérablement la sensibilité au bruit AWGN, sans déformer le motif d'auto-brouillage.

**ccm** a comme approche de ne plus projeter le signal reçu sur l'unique downchirp de référence  $x_0^*[k]$ , mais sur l'ensemble des trajets virtuels. Nous avons alors :

$$\tilde{r}_{jam,ccm}[k] = \sum_{u=0}^{U-1} r_{jam}[k] x_{m_u}^*[k] \quad (\text{III.3.28})$$

Dans l'équation (III.3.28), l'exploitation de chaque trajet virtuel avant démodulation non-cohérente finale permet de réduire l'influence du bruit AWGN. De plus, la fonction d'inter-corrélation circulaire est faite de façon implicite. La démodulation finale est identique au récepteur non-cohérent classique :

$$\hat{a}_{ccm} = \arg \max_m F_{ccm}[m] \quad (\text{III.3.29})$$

avec :

$$F_{ccm}[m] = \left| \tilde{R}_{jam,ccm}[m] \right| = |\text{DFT}\{\tilde{r}_{jam,ccm}[k]\}[m]| \quad (\text{III.3.30})$$

La Figure III.3.8 compare **cc1** et **ccm** pour les valeurs de  $U = 4$  et  $U = 12$  avec  $a = 0$ ,  $SNR_{dB} = 0$  et  $SF = 7$ . La meilleure robustesse de **ccm** sur  $U$  est clairement visible sur la figure, où les pics parasites d'inter-corrélation circulaire de **cc1** sont plus élevés et beaucoup plus nombreux que pour **ccm** pour  $U = 12$ .

### III.3.3.7. Comparaison des deux méthodes de démodulation par corrélation circulaire

#### III.3.3.7.1. Performances SER

La Figure III.3.9 compare les performances SER entre **cc1** et **ccm** pour  $U \in \{5, 10, 15, 20\}$  et  $SF = 7$ . Les performances d'une transmission LoRa non-cohérente classique i.e.  $U = 1$  (noté *LoRa legacy* dans la légende de la figure) servent ici de référence afin d'évaluer la dégradation de performances des deux démodulateurs proposés.

D'après la figure, nous voyons bien que la perte de performances en fonction de  $U$  pour **ccm** est bien plus faible que pour **cc1**. En effet, pour **cc1**, nous avons une perte régulière d'environ 1 dB à chaque incrément de  $U$  de 5 unités, pour atteindre une perte par rapport à LoRa legacy à  $U = 20$  de plus de 4 dB à  $SER = 10^{-3}$ . **ccm** a une perte vraiment faible jusqu'à  $U = 10$  (environ 0.25 dB) et limitée à 1.2 dB pour  $U = 20$ .

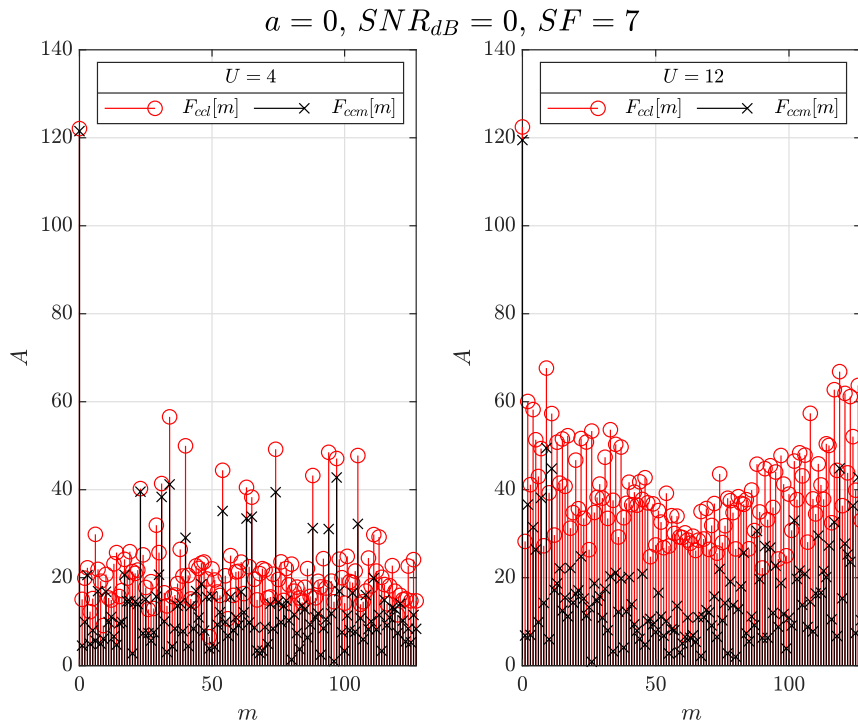


FIGURE III.3.8. – Impact de  $U$  sur les démodulations ccl et ccm,  $SF = 7$

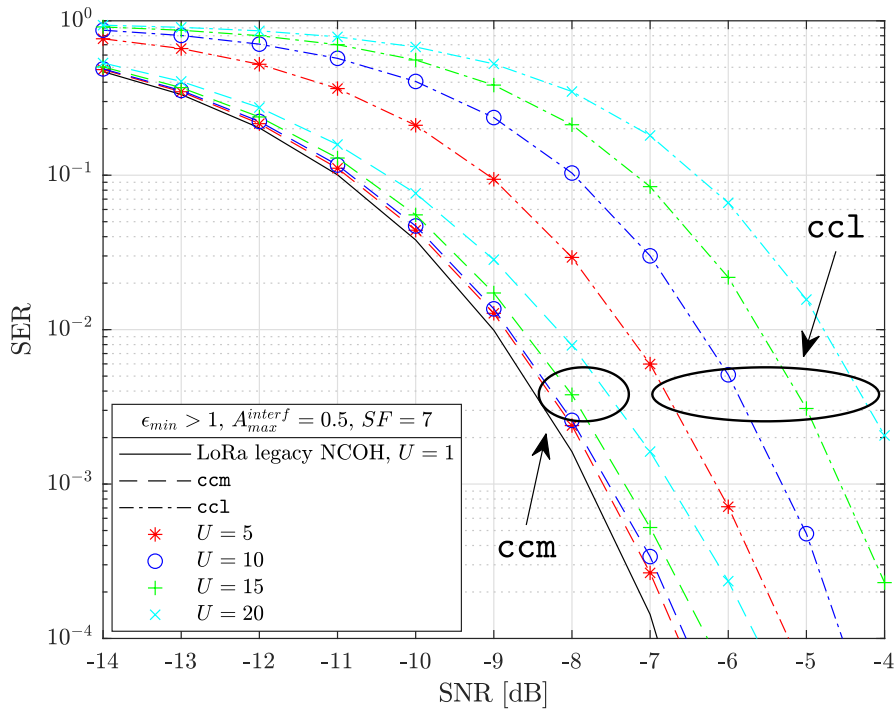


FIGURE III.3.9. – Comparaison des performances SER entre ccl et ccm,  $SF = 7$



### III.3.3.7.2. Complexité calculatoire

Les algorithmes 3 et 4 montrent l'implémentation numérique des démodulateurs `ccl` et `ccm`, respectivement. Les mêmes traitements sont appliqués pour pouvoir les comparer de façon équitable i.e. traitements à partir du  $i^{\text{ème}}$  bloc de  $M$  échantillons à la fréquence d'échantillonnage  $F_s = B$ .

---

**Algorithm 3:** Démodulateur `ccl`


---

**inputs :**  $\{\mathbf{r}\}_{k=0}^{M-1}$  %symbole reçu  
 $\{\mathbf{m}\}_{u=0}^{U-1}$  %vecteur de trajets virtuels  
 $M$  %ordre de modulation LoRa

- 1 génération du downchirp local :  $\mathbf{x}_0^*$
- 2  $\tilde{\mathbf{R}}_{jam} := \text{abs}(\text{FFT}(\mathbf{r} \odot \mathbf{x}_0^*))$
- 3  $\tilde{\mathbf{S}}_{ref} := \mathbf{0}_M$  %initialisation vecteur de zéros de taille  $M$
- 4  $\tilde{\mathbf{S}}_{ref}[\mathbf{m} \bmod M] := M\sqrt{1/U}$
- 5  $\mathbf{F}_{ccl} := \text{IFFT} \left\{ \text{FFT} \{ \tilde{\mathbf{R}}_{jam} \} \times \left( \text{FFT} \{ \tilde{\mathbf{S}}_{ref} \} \right)^* \right\}$
- 6 **return**  $s = \arg \max(\mathbf{F}_{ccl})$

---



---

**Algorithm 4:** Démodulateur `ccm`


---

**inputs :**  $\{\mathbf{r}\}_{k=0}^{M-1}$  %symbole reçu  
 $\{\mathbf{m}\}_{u=0}^{U-1}$  %vecteur de trajets virtuels  
 $M$  %ordre de modulation LoRa

- 1  $\mathbf{f}_{ccm} := \mathbf{0}_M$  %initialisation vecteur de zéros de taille  $M$
- 2 **for**  $u = 0$  **to**  $U - 1$  **do**
- 3     génération du downchirp local :  $\mathbf{x}_{\mathbf{m}[u]}^*$
- 4      $\mathbf{f}_{ccm} := \mathbf{f}_{ccm} + \mathbf{r} \odot \mathbf{x}_{\mathbf{m}[u]}^*$
- 5  $\mathbf{F}_{ccm} := \text{abs}(\text{FFT}(\mathbf{f}_{ccm}))$
- 6 **return**  $s = \arg \max(\mathbf{F}_{ccm})$

---

La Figure III.3.10 compare la complexité de `ccl` et `ccm` en terme de vitesse d'exécution, en fonction de  $U$ . Pour cela, nous compilons en langage C (langage de bas niveau, plus réaliste par rapport à un usage IoT) les fonctions MATLAB des deux algorithmes 3 et 4, et nous réalisons un grand nombre de démodulations d'un unique symbole. A chaque itération, nous relevons le temps d'exécution des deux démodulateurs à l'aide des fonctions MATLAB `tic(.)` et `toc(.)`. Nous calculons à la fin des tirages les temps d'exécution moyens, notés  $t_{exec,ccl,avg}(U)$  et  $t_{exec,ccm,avg}(U)$  (fonction de  $U$ ), en excluant la première itération du fait de l'initialisation des registres du processeur et du chargement en mémoire. Cela engendrerait sinon un biais dans les résultats. Nous choisissons d'afficher non pas la durée d'exécution absolue mais le rapport des durées entre `ccl` et `ccm` :

$$t_{exec,ratio}(U) = \frac{t_{exec,ccm,avg}(U)}{t_{exec,ccl,avg}(U)} \quad (\text{III.3.31})$$

Cela permet de limiter la dépendance des résultats au matériel utilisé. Nous montrons

aussi les relations linéaires  $f(U) = U$  et  $f(U) = 1$ , par soucis de comparaison.

D'après la Figure III.3.10, nous observons que `ccm` est plus lourd que `ccl` ( $t_{exec,ratio} > 1$ , au delà de la courbe  $f(U) = 1$ ), avec une complexité croissante avec  $U$ . Cela vient de la boucle sur  $U$  réalisée par `ccm` (lignes 2 à 4 de l'algorithme 4) qui ralentit l'exécution. Cependant, nous aurions pu nous attendre à avoir le cas défavorable d'une évolution linéaire i.e. avoir  $t_{exec,ratio}(U) = U$  (ligne '-' sur la figure). Ici, cela n'est pas le cas, où la droite est clairement moins raide. Par algorithme de régression linéaire, la fonction estimée est  $t_{exec,ratio}(U) \approx 0.47 \times U + 0.60$ .

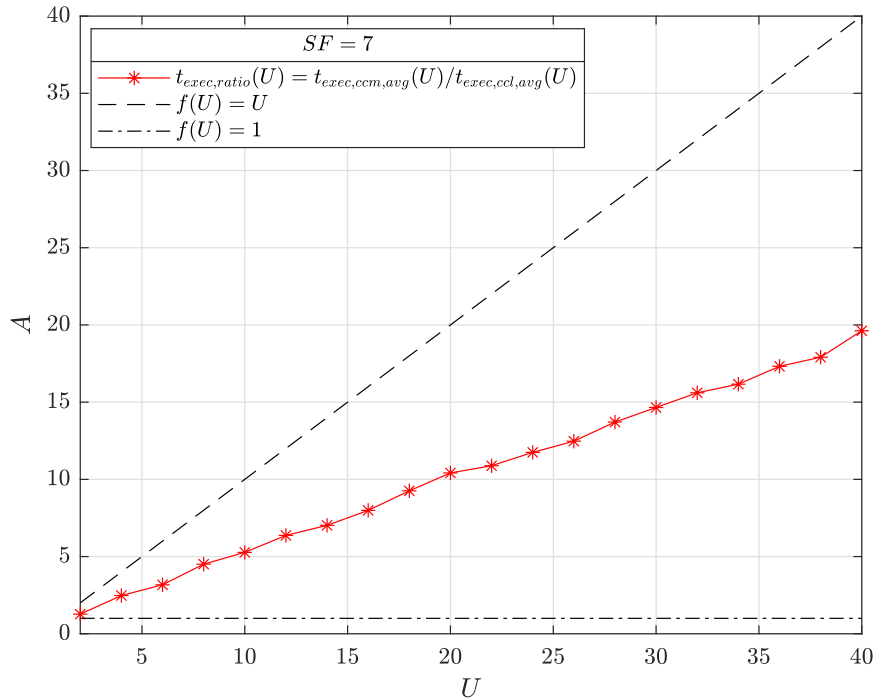


FIGURE III.3.10. – Comparaison des complexités calculatoires entre les démodulations `ccl` et `ccm`,  $SF = 7$

## III.3.4. Réduction du PAPR du schéma d'auto-brouillage

### III.3.4.1. Définition du PAPR

Dans cette section, nous présentons la solution proposée permettant de réduire le Peak-to-Average Power Ratio (PAPR), pouvant fortement limiter la viabilité du schéma d'auto-brouillage pour un usage réel. Cette solution a été proposée dans un article soumis dans la revue IEEE IoT Journal [98]. Le PAPR provient des fortes variations d'enveloppe du signal dans le domaine temporel. Ces dernières mettent en saturation les composants matériels de l'émetteur (convertisseur Numérique vers Analogique notamment, Digital to Analog Converter (DAC)), déformant le signal synthétisé. Ainsi, le récepteur recevra un signal déformé, réduisant les performances de démodulation, voir même donnant un signal inexploitable dans certains cas.

L' Orthogonal Frequency Division Multiplexing (OFDM) est le principal schéma de modulation souffrant de ce phénomène. Dans l'OFDM, plusieurs composantes fréquentielles

(ou sous-porteuses) sont transmises simultanément, chacune associée à un symbole issu d'une constellation numérique (Amplitude Shift Keying (ASK), Phase Shift Keying (PSK) ou Quadrature Amplitude Modulation (QAM)). Le symbole OFDM transmis (dans le domaine temporel donc) est obtenu par IFFT du vecteur de symboles à transmettre, noté  $\mathbf{a}$  :

$$x[k] = \text{IFFT}\{\mathbf{a}\}[k] = \frac{1}{\sqrt{P_s}} \sum_{n=0}^{N-1} a_n e^{2j\pi k \frac{n}{N}} \quad (\text{III.3.32})$$

avec  $a_n$ , le  $n^{\text{ème}}$  symbole dans  $\mathbf{a}$  et  $N$ , la taille du vecteur  $\mathbf{a}$ , mais aussi le nombre de sous-porteuses. D'après l'équation (III.3.32), nous remarquons qu'en fonction des valeurs dans  $\mathbf{a}$ , l'enveloppe :

$$A[k] = |x[k]|^2 \quad (\text{III.3.33})$$

fluctuera au cours du temps. Plus cette dernière fluctue, plus le risque de mise en saturation du DAC augmente, entraînant une distorsion du signal. Il serait donc souhaitable d'avoir idéalement  $A[k] = P_s \forall k$ , afin d'avoir une enveloppe constante, ne mettant pas en saturation le DAC. Le PAPR quantifie cette fluctuation par la relation simple, pour un  $\mathbf{a}$  donné :

$$\text{PAPR}(\mathbf{a}) = \frac{\max_k A[k]}{\mathbb{E}_t[A[k]]} = \frac{A_{max}}{A_{mean}} \geq 1 \quad (\text{III.3.34})$$

avec  $\mathbb{E}_t[\cdot]$ , l'opérateur d'espérance mathématique temporelle, défini par :

$$\mathbb{E}_t[x[k]] = \frac{1}{M} \sum_{k=0}^{M-1} x[k] \quad (\text{III.3.35})$$

De par la forte variabilité de  $A_{max}$  pouvant être présente, le PAPR est généralement exprimé en échelle logarithmique :

$$\text{PAPR}_{dB}(\mathbf{a}) = 10 \times \log_{10}(\text{PAPR}(\mathbf{a})) \quad (\text{III.3.36})$$

Lorsque  $A_{max} = A_{mean}$ , il n'y a pas de PAPR ( $\text{PAPR}_{dB}(\mathbf{a}) = 0$ ). Comme  $A[k]$  dépend de  $\mathbf{a}$ , le PAPR est une fonction de ce dernier. De plus, comme les symboles sont aléatoires, le PAPR est aussi aléatoire. Ainsi, le PAPR est évalué pour les systèmes OFDM de façon statistique, en évaluant la probabilité que ce dernier dépasse une certaine valeur.

### III.3.4.2. PAPR du schéma d'auto-brouillage

Une forte analogie entre l'OFDM et le schéma d'auto-brouillage LoRa est présente. En effet, dans l'équation (III.3.7),  $U$  symboles sont additionnés dans le domaine fréquentiel LoRa. Ce dernier est assez proche du domaine fréquentiel OFDM. Le nombre de sous-porteuses correspond alors au nombre de symboles dans la DFT LoRa i.e.  $N = U$  et les symboles  $a_{u,jam}$  aux symboles  $a_n$  de la constellation. Dans ce qui suit, nous évaluons le PAPR du schéma d'auto-brouillage.

Rappelons qu'un signal LoRa classique ( $U = 1$ ) ne possède pas de PAPR puisque

### III.3.4. Réduction du PAPR du schéma d'auto-brouillage

$A_{max} = A_{mean} = P_s = 1$  dans l'équation (I.2.6). Notons  $A_{jam}[k]$ ,  $A_{jam,max}$  et  $A_{jam,mean}$ , leur équivalent pour l'auto-brouillage LoRa, pour différencier de l'OFDM :

$$A_{jam}[k] = |x_{a,jam}[k]|^2 \quad (III.3.37)$$

$$A_{jam,max} = \max_k A_{jam}[k] \quad (III.3.38)$$

$$A_{jam,mean} = \mathbb{E}_{\mathbf{a}_{jam}} [\mathbb{E}_t[A_{jam}[k]]] \quad (III.3.39)$$

avec  $\mathbb{E}_{\mathbf{a}_{jam}}[\cdot]$ , la moyenne sur les vecteurs  $\mathbf{a}_{jam}$  (équation (III.3.3)). Le PAPR du schéma d'auto-brouillage est alors :

$$PAPR = \frac{\max_k |x_{a,jam}[k]|^2}{\mathbb{E}_{\mathbf{a}_{jam}} [\mathbb{E}_t[|x_{a,jam}[k]|^2]]} = \frac{\max_k A_{jam}[k]}{\mathbb{E}_{\mathbf{a}_{jam}} [\mathbb{E}_t[A_{jam}[k]]]} = \frac{A_{jam,max}}{A_{jam,mean}} \quad (III.3.40)$$

Pour calculer le PAPR,  $A_{jam}[k]$  doit être calculé dans l'équation (III.3.40). Ce dernier vaut à partir des équations (III.3.37) et (III.3.7) :

$$A_{jam}[k] = |x_{a,jam}[k]|^2 = |x_a[k]S_{jam}[k]|^2 = |S_{jam}[k]|^2 = S_{jam}[k]S_{jam}^*[k] \quad (III.3.41)$$

$$\begin{aligned} &= \frac{1}{U} \sum_{u_1=0}^{U-1} \sum_{u_2=0}^{U-1} e^{2j\pi k \frac{mu_1 - mu_2}{M}} = \frac{1}{U} \sum_{\substack{\{u_1, u_2\}=0 \\ m_{u_1} = m_{u_2}}}^{U-1} e^{2j\pi k \frac{mu_1 - mu_2}{M}} + \frac{1}{U} \sum_{\substack{\{u_1, u_2\}=0 \\ m_{u_1} \neq m_{u_2}}}^{U-1} e^{2j\pi k \frac{mu_1 - mu_2}{M}} \\ &= 1 + \frac{1}{U} \sum_{\substack{\{u_1, u_2\}=0 \\ m_{u_1} \neq m_{u_2}}}^{U-1} e^{2j\pi k \frac{mu_1 - mu_2}{M}} \end{aligned} \quad (III.3.42)$$

Il est facile de voir que la somme dans l'équation (III.3.42) est maximisée lorsque  $k = 0$ . Nous avons alors :

$$A_{jam,max} = A_{jam}[0] = 1 + \frac{U^2 - U}{U} = U. \quad (III.3.43)$$

Nous avons également :

$$A_{jam,mean} = \mathbb{E}_{\mathbf{a}_{jam}} [\mathbb{E}_t[A_{jam}[k]]] = 1 + \frac{1}{U} \frac{1}{M} \sum_{k=0}^{M-1} \underbrace{\left( \sum_{\substack{\{u_1, u_2\}=0 \\ m_{u_1} \neq m_{u_2}}}^{U-1} e^{2j\pi k \frac{mu_1 - mu_2}{M}} \right)}_{=0} = 1 \quad (III.3.44)$$

en utilisant la propriété :

$$\sum_{k=0}^{M-1} \alpha^k = \frac{1 - \alpha^M}{1 - \alpha}. \quad (III.3.45)$$

Le PAPR est donc finalement :

$$PAPR = \frac{A_{jam,max}}{A_{jam,mean}} = \frac{U}{1} = U. \quad (III.3.46)$$

Nous avons la relation linéaire simple  $PAPR(U) = U$ . Le PAPR du schéma d'auto-brouillage est donc parfaitement déterministe, un résultat différent de l'OFDM. En effet, ici, il n'y a pas de dépendance sur les symboles transmis  $\mathbf{a}_{jam}$ , contrairement à l'OFDM qui dépend de  $\mathbf{a}$  dans l'équation (III.3.34). Cela vient du fait que la puissance est répartie uniformément sur l'ensemble des symboles i.e.  $P_{jam} = 1/U$ . Cela ne serait pas le cas sinon.

La Figure III.3.11 montre un exemple de l'enveloppe  $A_{jam}[k]$  de quatre signaux LoRa auto-brouillés, pour  $U \in \{2, 3, 4, 8\}$  et  $\mathbf{m} = [0\ 19\ 26\ 61\ 77\ 91\ 118\ 121]$ . Pour chaque valeur de  $U$ , nous sélectionnons les  $U$  premières valeurs dans  $\mathbf{m}$ . D'après la figure et l'équation (III.3.42), nous remarquons que le motif est symétrique autour de  $k = M/2$ . Pour  $U = 2$ , nous avons un motif quasi sinusoïdal ayant  $m_1$  périodes, tandis que pour  $U > 2$ , le motif est beaucoup plus chaotique. Nous voyons bien visuellement que  $A_{jam,mean} = P_s = 1$ . Naturellement, d'autres valeurs de  $\mathbf{m}$  donneront un motif d'enveloppe différent.

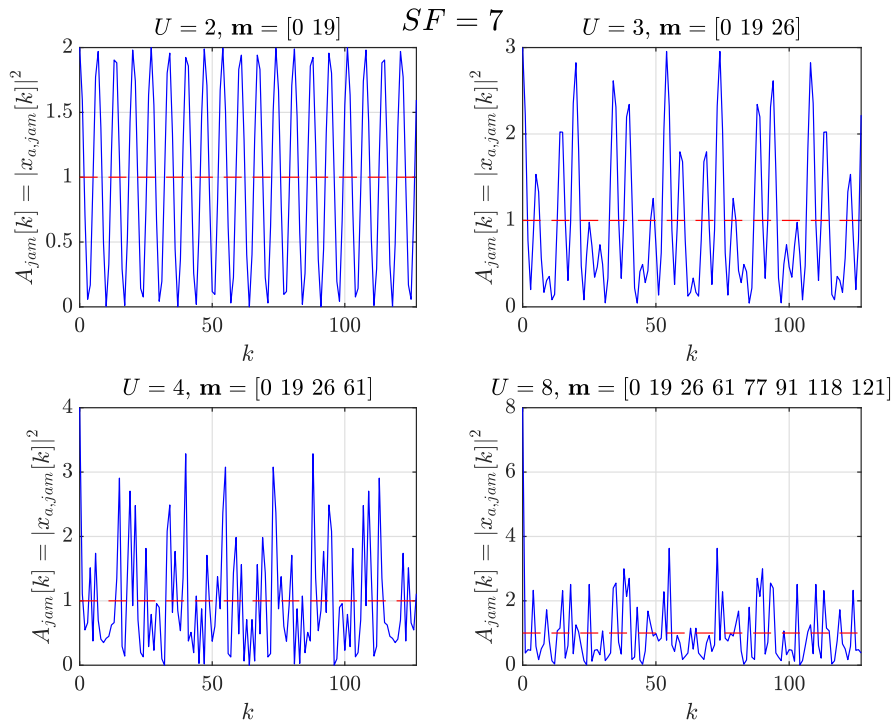


FIGURE III.3.11. – Illustrations du PAPR de symboles LoRa auto-brouillés,  $SF = 7$

### III.3.4.3. Méthodes de réduction du PAPR dans la littérature

Nous présentons dans cette partie les méthodes de réduction de PAPR déjà existantes dans la littérature dont la solution proposée pour le schéma d'auto-brouillage s'inspire. La majorité des solutions de réduction du PAPR dans la littérature portent sur l'OFDM, et peuvent être classées en deux grandes familles : les méthodes de pré-distorsion et de signalisation [170].

#### III.3.4.3.1. Méthodes de pré-distorsion

Les méthodes de pré-distorsion appliquent délibérément à l'émission une déformation de l'enveloppe afin de réduire le PAPR. Une solution communément employée est d'écarter

tous les échantillons dont la magnitude est supérieure à un seuil [171, 172]. Plus l'écrêtage est agressif (seuil bas), plus la correction du PAPR sera forte, mais le signal résultant en sera d'autant plus déformé. Ainsi, un compromis est nécessaire entre correction du PAPR et déformation du signal. D'autres travaux [173, 174] proposent d'utiliser une fenêtre de pondération afin d'adoucir les variations d'enveloppe du signal. La fenêtre doit être judicieusement choisie afin de satisfaire le même compromis. Il est aussi possible d'appliquer certaines transformations (aussi appelées *compand functions* en anglais) sur le signal afin de réduire statistiquement le PAPR rencontré [175, 176, 177], ou bien soustraire au signal un autre signal ayant des propriétés permettant une réduction du PAPR [178].

#### III.3.4.3.2. Méthodes de signalisation

Les méthodes de signalisation offrent une approche différente : elles apportent une modification du schéma de modulation, permettant de réduire le PAPR. Les modifications sont parfaitement connues de l'émetteur et du récepteur. Pour l'OFDM, cela revient généralement à appliquer une correction de phase sur chaque symbole, afin que le symbole OFDM temporel ait statistiquement un PAPR plus faible. Cela se réduit à un problème d'optimisation de recherche de phases, où de nombreux algorithmes sont employés [179, 180, 181]. Une autre possibilité est d'appliquer une déformation non-linéaire sur la constellation numérique afin de produire des symboles  $a_n$  donnant un PAPR réduit [182]. Cela a montré de bons résultats, mais est possible au détriment d'une augmentation de la puissance d'émission. Enfin, une solution proposée est d'utiliser les sous-porteuses habituellement non utilisées (bande de garde par exemple), en mettant à la place des symboles judicieusement choisis afin de réduire le PAPR [183, 184]. Les méthodes de signalisation nécessitent le partage d'une information entre l'émetteur et le récepteur (phases optimisées par exemple). Cela pose donc des contraintes sur le partage de l'information et de la synchronisation non négligeables. Des travaux ont proposé des schémas réduisant la quantité d'informations nécessaire [185, 186], mais au coût d'une baisse d'efficacité de la correction du PAPR.

Le Tableau III.3.2 donne les défauts et avantages des deux grandes familles de méthodes de réduction du PAPR. Les méthodes de pré-distorsion sont réputées pour avoir une faible complexité et être transparentes pour le récepteur, tandis que les méthodes de signalisation ont généralement un compromis correction du PAPR / distorsion signal plus avantageux.

#### III.3.4.4. Solution de correction du PAPR pour le schéma d'auto-brouillage

L'objectif est de réduire le PAPR au maximum, tout en préservant le plus possible les propriétés d'auto-brouillage i.e. avoir  $U$  pics bien identifiés dans la DFT LoRa. Notre solution retenue fait partie de la famille des méthodes de pré-distorsion. En effet, dans un environnement exigeant de fortes contraintes sur la consommation énergétique comme LoRa, il est judicieux d'avoir une solution apportant peu de complexité calculatoire, des modifications minimales sur le schéma de modulation, et une totale transparence pour le récepteur (voir Tableau III.3.2). De plus, la dégradation de la capacité de démodulation constatée est raisonnable, même pour une correction du PAPR très agressive. Notre philosophie est de venir appliquer un facteur d'échelle sur l'enveloppe globale du signal. La non linéarité d'un seuil d'écrêtage (certains échantillons altérés et d'autres non) détruit

Méthode	Avantages	Inconvénients
Pré-distorsion	Faible complexité calculatoire.  Transparence pour le récepteur.	Déformation du signal importante si correction du PAPR forte → perte de performances de démodulation.
Signalisation	Perte de performances de démodulation modérée si correction du PAPR forte.	Complexité calculatoire.  Nécessite la connaissance d'une information commune entre l'émetteur et le récepteur.

TABLE III.3.2. – Avantages et inconvénients des méthodes de correction du PAPR de la littérature

rapidement les propriétés d'auto-brouillage, contrairement à un facteur d'échelle appliquant une correction homogène sur tous les échantillons.

Notons  $PAPR_{in}$  et  $PAPR_{out}$ , les PAPR du signal auto-brouillé avant et après correction du PAPR, respectivement. Nous appliquons le facteur d'échelle  $f$  pour obtenir le PAPR désiré en sortie :

$$PAPR_{out} = PAPR_{in} \times f \quad (\text{III.3.47})$$

Comme  $PAPR_{in} = U$  (voir équation (III.3.46)), le facteur d'échelle a donc pour valeurs :

$$f \in [1/U; 1] \quad (\text{III.3.48})$$

Ainsi,  $f = 1$  ne donne pas de correction, et  $f = 1/U$  applique une correction maximale. Par exemple, pour  $U = 8$ ,  $f = 0.25$  donnera un PAPR en sortie  $PAPR_{out} = 2$ , soit une réduction d'un facteur quatre. L'expression du coefficient appliqué à chaque échantillon est noté  $V_{jam}[k]$  et vaut :

$$V_{jam}[k] = \sqrt{1 + \frac{(1 - |S_{jam}[k]|^2) \times \frac{U - PAPR_{out}}{U - 1}}{|S_{jam}[k]|^2}} \quad (\text{III.3.49})$$

D'après l'équation (III.3.49),  $V_{jam}[k]$  peut-être simplifié pour les valeurs extrêmes de  $f$  :

$$V_{jam}[k] = \begin{cases} 1 & \text{si } f = 1 \\ \frac{1}{|S_{jam}[k]|} & \text{si } f = 1/U \end{cases} \quad (\text{III.3.50})$$

La Figure III.3.12 montre un exemple de  $|V_{jam}[k]|$  pour  $U = 4$ , le même canal virtuel

### III.3.4. Réduction du PAPR du schéma d'auto-brouillage

qu'en Figure III.3.11,  $f \in \{1, 0.75, 0.5, 1/U\}$  et  $SF = 7$ .



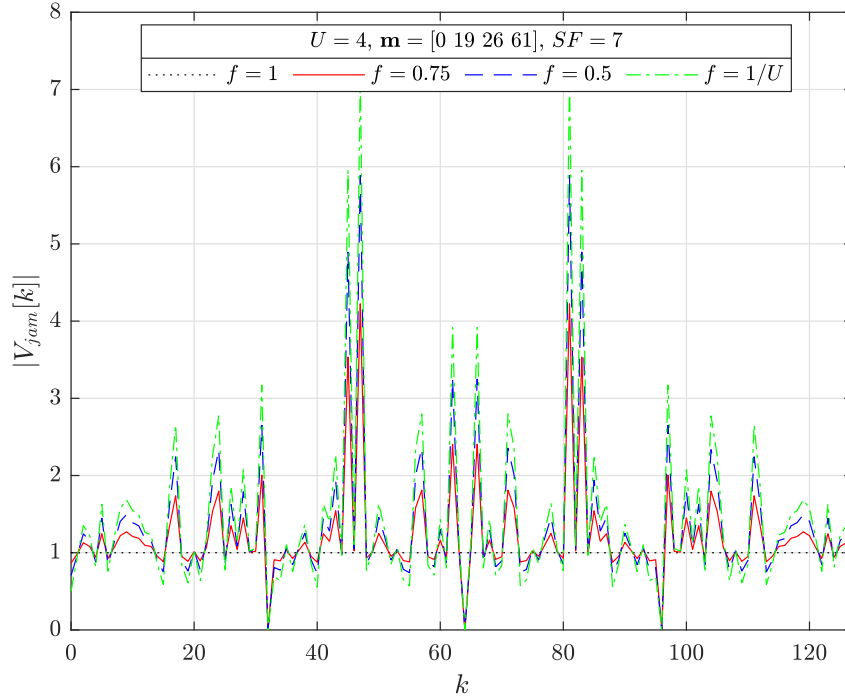


FIGURE III.3.12. – Évolution au cours du temps de la composante de correction du PAPR en fonction du facteur de correction du PAPR,  $SF = 7$

Le signal auto-brouillé corrigé en PAPR et son enveloppe sont alors :

$$x_{a,jam,mod}[k] = x_{a,jam}[k] \times V_{jam}[k] \quad (\text{III.3.51})$$

$$A_{jam,mod}[k] = |x_{a,jam,mod}|^2 \quad (\text{III.3.52})$$

et  $\tilde{R}_{jam,mod}[n]$ ,  $F_{ccl,mod}[m]$  et  $F_{ccm,mod}[m]$ , la DFT et les démodulations **ccl** et **ccm** avec correction du PAPR, respectivement. Dans le mémoire, nous notons aussi LoRa jam mod et LoRa jam, les schémas d'auto-brouillage avec et sans correction du PAPR, respectivement.

La Figure III.3.13 montre un exemple d'enveloppe complexe d'un signal LoRa auto-brouillé obtenue pour différents facteurs de correction du PAPR  $f \in \{1, 0.75, 0.5, 1/U\}$ ,  $U = 4$ , le même canal virtuel qu'en Figure III.3.11 et  $SF = 7$ . On voit bien l'effet de compression progressive de l'enveloppe pour atteindre un PAPR nul lorsque la correction est maximale.

La Figure III.3.14 montre un exemple de DFT et démodulation **ccm** obtenues pour une correction du PAPR maximale ( $f = 1/U$ ) pour  $U = 8$ ,  $\mathbf{m} = [0 \ 14 \ 32 \ 39 \ 52 \ 67 \ 83 \ 87]$ ,  $a = 0$  et  $SF = 7$ . Nous ajoutons également les amplitudes du cas sans correction du PAPR :  $|\tilde{R}_{jam}[a_{u,jam}]| = M\sqrt{P_{jam}}$  et  $F_{ccm}[a] = M$ . Nous constatons bien la déformation dans la DFT, où une perte d'énergie pour la plupart des bins d'intérêt est présente i.e.  $|\tilde{R}_{jam}[a_{u,jam}]| < M\sqrt{P_{jam}}$ , et des bins parasites en plus de ceux d'inter-corrélation circulaire ayant cependant des amplitudes modérées. Nous avons ici  $|\tilde{R}_{jam,mod}[n \neq a_{u,jam}]| < 13$ . La **ccm** est impactée de la même façon, avec  $F_{ccm,mod}[a] \approx 113$  au lieu de  $F_{ccm}[a] = M = 128$ , soit une baisse d'environ 12%.

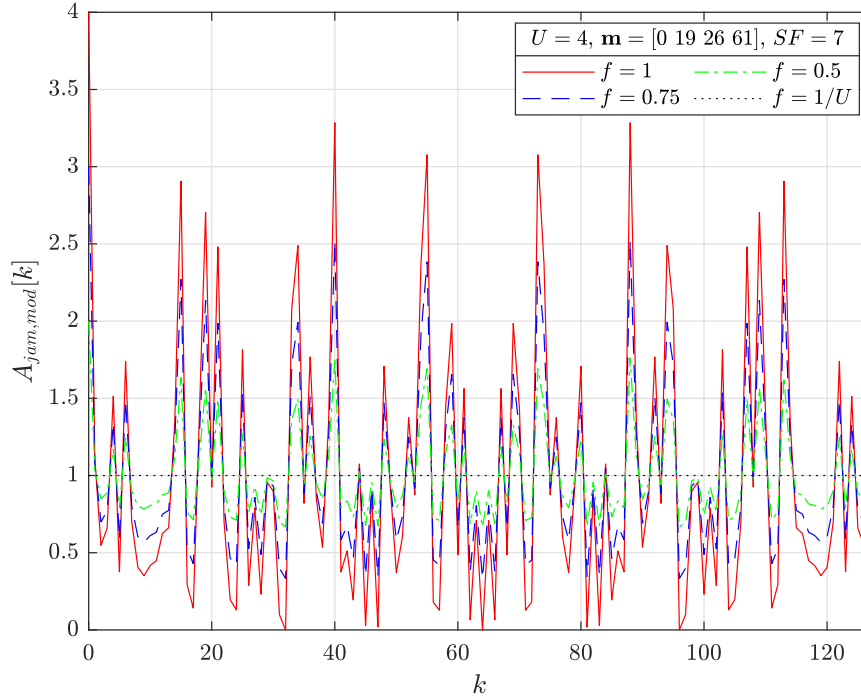


FIGURE III.3.13. – Évolution au cours du temps de l'enveloppe d'un symbole auto-brouillé en fonction du facteur de correction du PAPR,  $SF = 7$

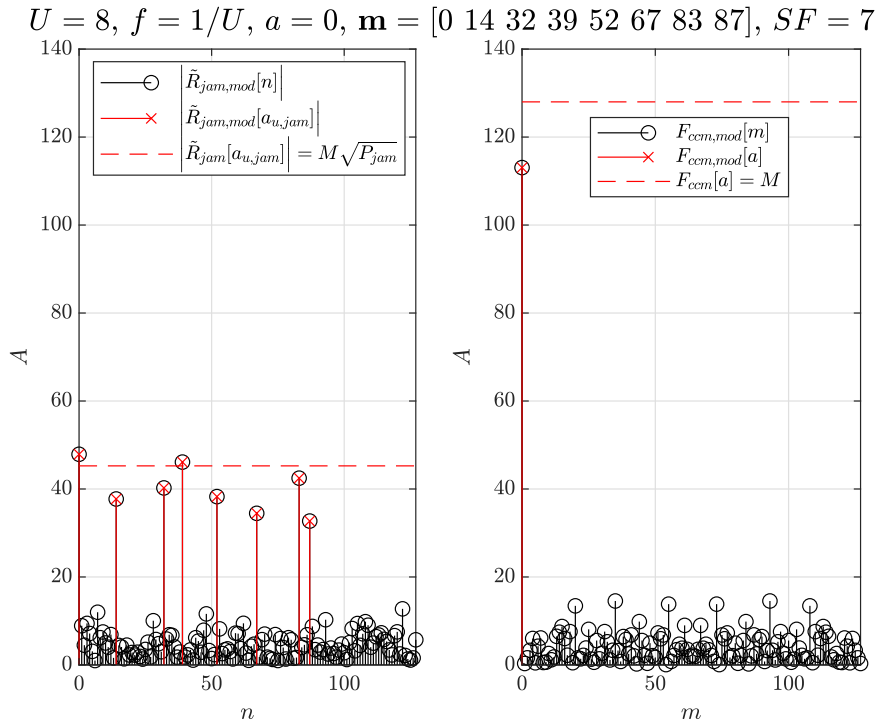


FIGURE III.3.14. – Exemple de démodulations classique et ccm d'un symbole auto-brouillé avec correction du PAPR maximale,  $SF = 7$

La Figure III.3.15 montre l'évolution de l'amplitude du bin d'intérêt  $F_{ccm,mod}[a]$  en fonction de  $U$  et pour  $f \in \{1, 0.75, 0.5, 0.25, 1/U\}$ . Nous réalisons un grand nombre de tirages où à chaque fois, un canal virtuel et un symbole différent sont choisis. Nous réalisons la transmission sans bruit AWGN ni désynchronisation, démodulons, et relevons ensuite l'amplitude du pic d'intérêt. A la fin des tirages, nous calculons et affichons la valeur moyenne des amplitudes relevées.

D'après la Figure III.3.15, lorsqu'il n'y a pas de correction du PAPR i.e.  $f = 1$ , il n'y a pas de perte d'énergie ( $F_{ccm,mod}[a] = M$ ). Plus la correction du PAPR est forte et/ou  $U$  élevé, plus la perte d'énergie est importante. Par exemple, pour  $U = 40$ , nous avons un rapport d'amplitudes entre  $f = 1$  et  $f = 1/U$  d'environ  $95/M \approx 0.74$ . Également, pour  $f = 1/U$ , nous avons un rapport d'amplitudes entre  $U = 2$  et  $U = 40$  d'environ  $95/115 \approx 0.83$ . Ainsi, comme l'amplitude du pic d'intérêt diminue progressivement avec  $f$  et  $U$ , les performances SER se dégraderont. Cela est montré après en Figure III.3.18.

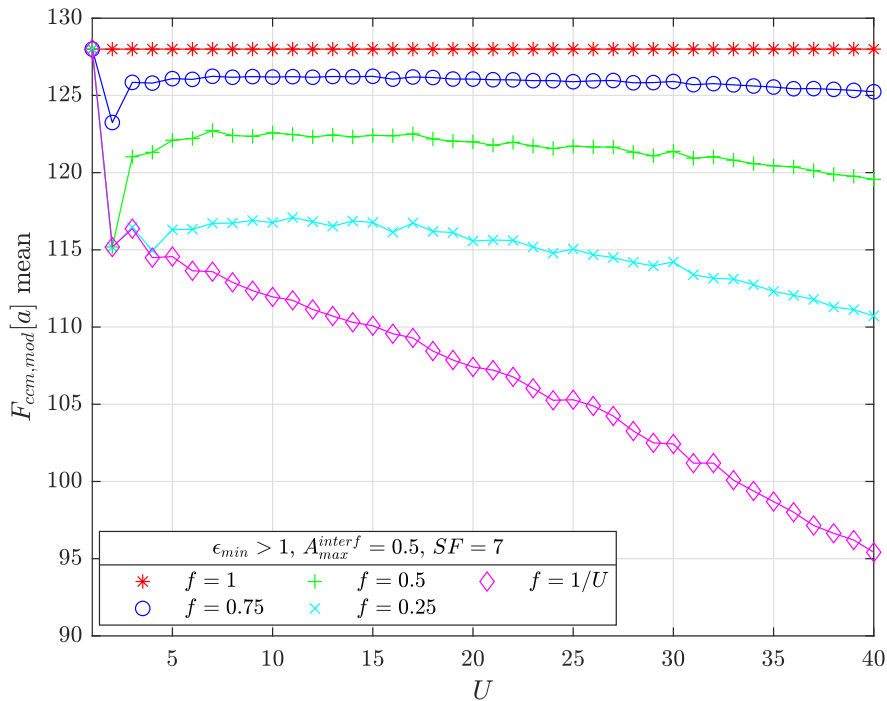


FIGURE III.3.15. – Impact de la correction du PAPR sur l'amplitude du pic d'intérêt  $c_{cm}$ ,  $SF = 7$

### III.3.4.5. Comparaison de l'impact de la correction du PAPR entre $c_{c1}$ et $c_{cm}$

La Figure III.3.16 compare les démodulations  $c_{c1}$  et  $c_{cm}$  sans correction du PAPR (gauche) et avec correction maximale  $f = 1/U$  (droite), pour  $U = 20$ ,  $a = 0$  et  $SF = 7$ . Il n'y a pas de bruit AWGN, ni de désynchronisation. Ainsi, sans correction du PAPR,  $c_{c1}$  et  $c_{cm}$  sont parfaitement identiques. En revanche, le comportement est très différent lorsque cette dernière est active. Nous constatons immédiatement que  $c_{c1}$  est bien plus déformée que  $c_{cm}$ . Nous avons en effet des bins parasites en plus de ceux d'inter-corrélation circulaire bien plus élevés et nombreux. La moitié des bins ont une amplitude qui dépasse 40 là où  $c_{cm}$  donne des amplitudes ne dépassant pas 20. Ainsi,  $c_{cm}$  aura de bien meilleures

performances. Notons que l'amplitude du bin d'intérêt  $m = a$  est inchangée.

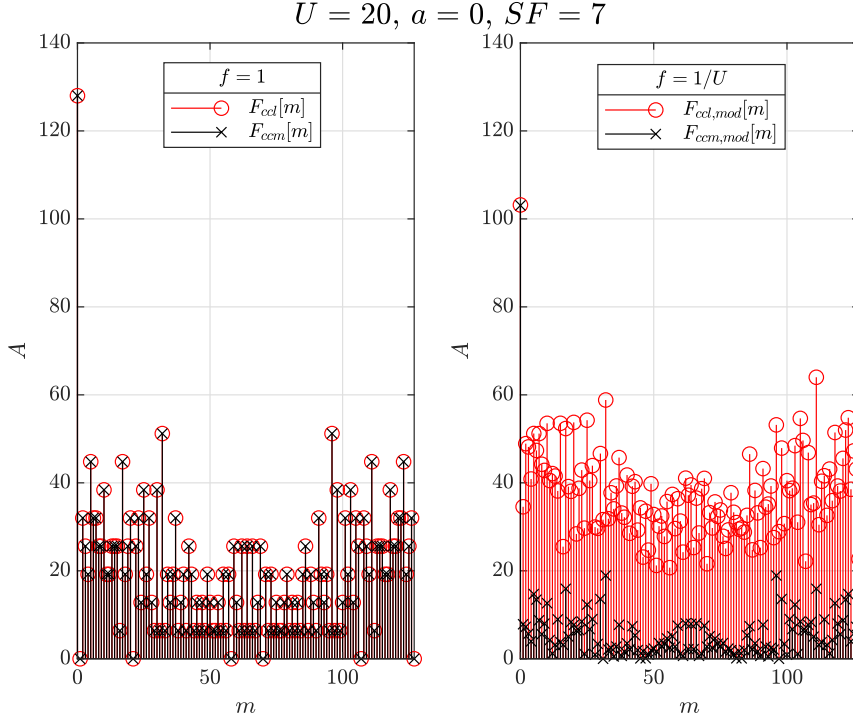


FIGURE III.3.16. – Comparaison des démodulations `ccl` et `ccm`, sans correction du PAPR et avec correction du PAPR maximale,  $SF = 7$

La Figure III.3.17 compare également l'impact de la correction du PAPR entre `ccl` et `ccm`, mais sur un grand nombre de réalisations de symboles et de canaux virtuels, sans bruit AWGN. Nous définissons pour cela le critère suivant :

$$r_{ccl} = \frac{\sum F_{ccl,mod}[m \neq a]}{F_{ccl,mod}[m = a]}, \quad r_{ccm} = \frac{\sum F_{ccm,mod}[m \neq a]}{F_{ccm,mod}[m = a]} \quad (\text{III.3.53})$$

Il quantifie le niveau de déformation engendré par la correction du PAPR, comme la somme des amplitudes des bins parasites sur celle du bin d'intérêt. Ainsi, plus le critère est faible, moins la déformation est prononcée. Sur la figure, nous considérons  $U = 8$ ,  $f = 1/U$ ,  $\epsilon_{min} > 1$ ,  $A_{max}^{interf} = 0.5$ ,  $SF = 7$  et  $N_{trials} = 1600$  tirages. Nous affichons le critère pour `ccl` et `ccm`, en normalisant par rapport à la valeur maximale rencontrée lors des tirages de `ccl`.

D'après la Figure III.3.17, nous retrouvons de façon cohérente avec la Figure III.3.16 la meilleure robustesse de `ccm`, avec un critère beaucoup plus favorable. En effet, la valeur moyenne est d'environ 0.16 pour `ccm` contre environ 0.74 pour `ccl`, donnant un rapport d'environ 4.7. De plus, la variance est beaucoup plus faible pour `ccm`, avec un rapport de variances d'environ 17.7.

La Figure III.3.18 montre l'impact de la correction du PAPR ( $f \in \{1, 1/U\}$ ) sur le SER de `ccl` et `ccm` en fonction de  $U$  ( $U \in \{5, 20\}$ ), en supposant une synchronisation parfaite et  $SF = 7$ .

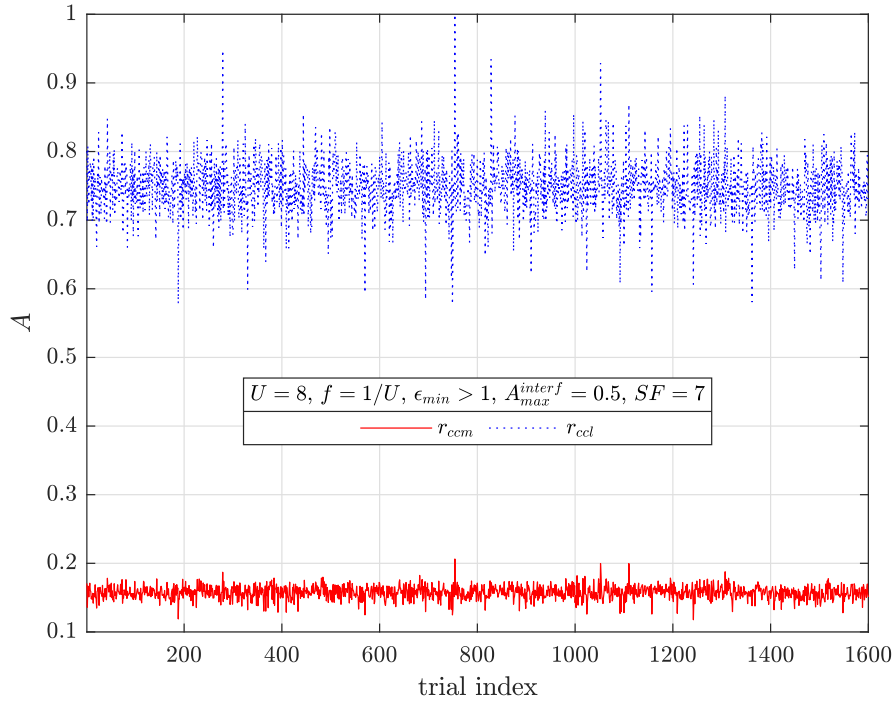


FIGURE III.3.17. – Comparaison de la sensibilité à la correction du PAPR entre ccl et ccm,  $SF = 7$

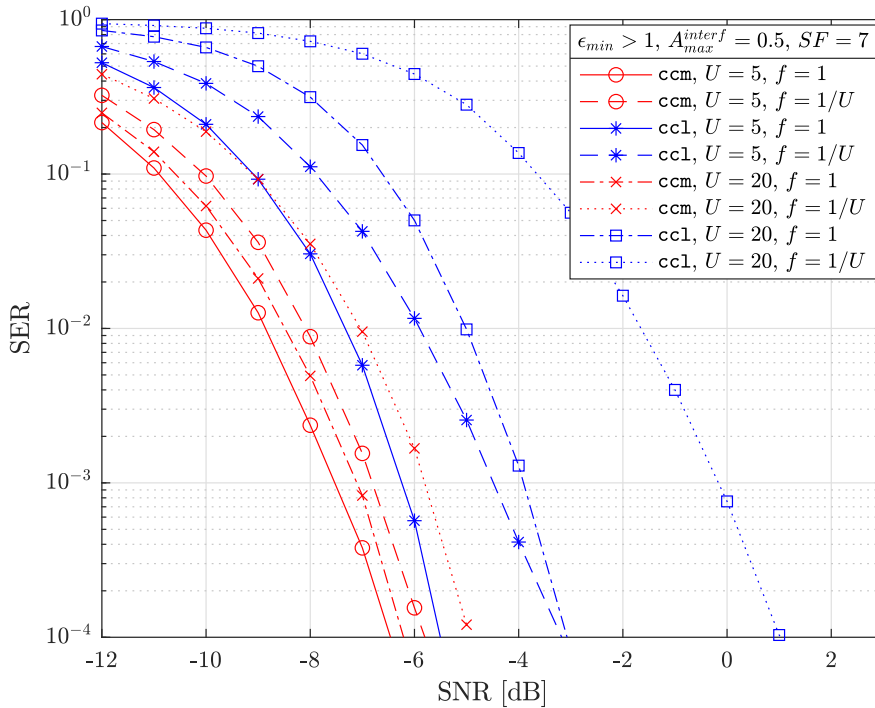


FIGURE III.3.18. – Comparaison de l'impact de  $U$  et  $f$  sur les performances SER de ccl et ccm,  $SF = 7$

D'après la Figure III.3.18, nous voyons que pour un démodulateur donné et  $f$  fixé, augmenter  $U$  dégrade les performances, surtout pour ccl. Nous retrouvons exactement les mêmes comportements qu'en Figure III.3.9. Pour un démodulateur donné et  $U$  fixé, plus la correction du PAPR est forte, plus la dégradation des performances est impor-

tante. En revanche, elle est beaucoup plus prononcée pour **cc1**, ce qui est cohérent avec la Figure III.3.17. Nous avons pour  $U = 20$ , une perte entre  $f = 1$  et  $f = 1/U$  d'environ 4.2 dB pour **cc1** à  $SEER = 10^{-4}$ , contre environ 1 dB pour **ccm**. Enfin, nous retrouvons la forte sensibilité sur  $U$  de **cc1** lorsque la correction du PAPR est active, comme vu en Figure III.3.16. Nous avons en effet une perte entre  $U = 5$  et  $U = 20$  ( $f = 1/U$ ) pour **cc1** d'environ 4.2 dB à  $SEER = 10^{-4}$ , contre 1 dB pour **ccm**.

Le Tableau III.3.3 résume les démodulateurs **cc1** et **ccm** en présentant leurs avantages et inconvénients. Nous pouvons conclure que **cc1** a pour seul avantage de présenter une faible complexité calculatoire, tandis que **ccm** est beaucoup plus adapté pour une utilisation pratique, avec une sensibilité sur  $U$  très réduite et une meilleure robustesse à la correction du PAPR.

Récepteur	Avantages	Inconvénients
<b>cc1</b>	Faible complexité calculatoire.	Sensibilité sur $U$ très forte.  Sensibilité à la correction du PAPR importante.
<b>ccm</b>	Sensibilité sur $U$ très réduite.  Sensibilité à la correction du PAPR faible.	Complexité calculatoire plus forte que <b>cc1</b> .

TABLE III.3.3. – Avantages et inconvénients des démodulateurs **cc1** et **ccm**

### III.3.4.6. Annulation de la correction du PAPR en réception

Il est légitime de se poser la question de savoir s'il est pertinent d'éliminer en réception la correction du PAPR introduite à l'émission, afin d'éliminer les déformations de la DFT LoRa, et donc retrouver de bonnes performances de démodulation. Nous appliquons alors la correction suivante :

$$r_{jam,mod,corr}[k] = r_{jam,mod}[k] \times \frac{1}{V_{jam}[k]} \quad (\text{III.3.54})$$

avec  $r_{jam,mod}[k]$  et  $r_{jam,mod,corr}[k]$ , le signal reçu LoRa auto-brouillé corrigé en PAPR à l'émission et le signal reçu LoRa auto-brouillé corrigé en PAPR à l'émission mais avec la correction du PAPR éliminée en réception, respectivement. La démodulation est poursuivie normalement.

La Figure III.3.19 compare les performances SER de **ccm** ( $f = 1/U$ ) avec et sans annulation de la correction du PAPR en réception, pour  $U \in \{5, 20\}$ . Nous voyons sur la figure que sans annulation, nous retrouvons la perte de performances liée à  $U$ , avec une perte d'environ 1.2 dB à  $SEER = 10^{-4}$  entre  $U = 5$  et  $U = 20$ . En revanche, l'annulation entraîne une baisse importante des performances, surtout si  $U$  est élevé, où la perte pour  $U = 20$  est déjà de presque 5 dB à  $SEER = 10^{-3}$ , et s'accroît encore après. Cela vient

du fait que l'opération dans l'équation (III.3.54) est tout à fait similaire à ce que ferait un égaliseur de canal de type Zero Forcing (ZF), où l'effet du canal est inversé [83]. L'inversion entraîne une interaction négative avec la composante de bruit AWGN dans le signal reçu. Ce dernier se retrouve alors amplifié. Ainsi, il ne faut surtout pas éliminer la correction du PAPR par une approche ZF mais conserver le signal tel quel. Cela a l'avantage de conserver la transparence pour le récepteur.

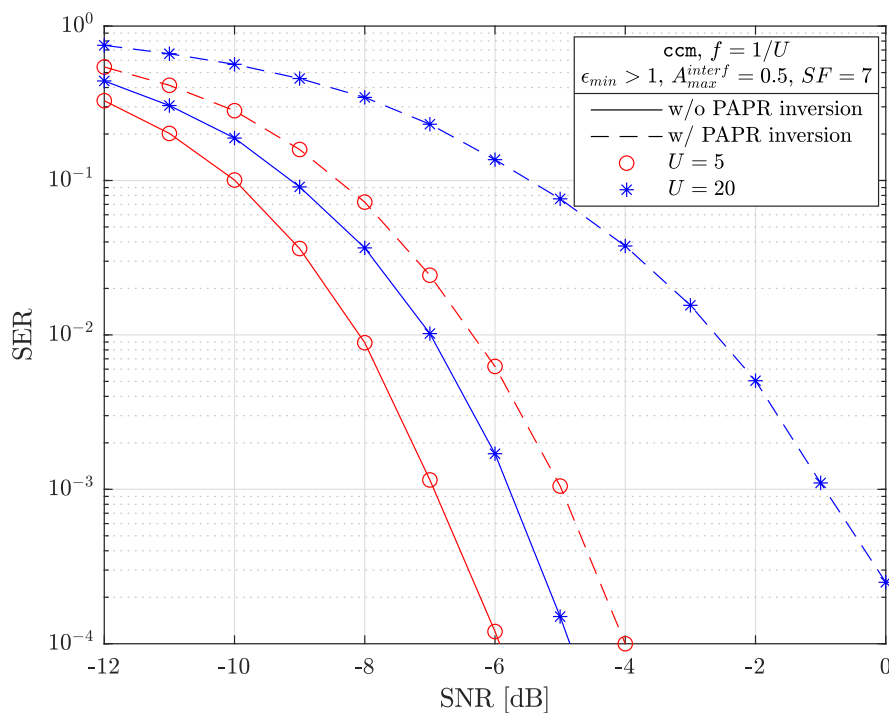


FIGURE III.3.19. – Impact de l'annulation de la correction du PAPR en réception sur les performances SER de ccm,  $SF = 7$

## III.4. Schéma d'auto-brouillage LoRa partie 2 : traitements au niveau du récepteur et performances

Dans cette section, nous présentons les traitements effectués par le récepteur et les performances de notre schéma d'auto-brouillage LoRa. En Section III.4.1, nous présentons le front-end de synchronisation utilisé pour le schéma d'auto-brouillage. Ensuite, nous présentons des résultats de simulation sur les performances du récepteur légitime en Section III.4.2. Nous continuons en Section III.4.3 avec la présentation de notre détecteur de trame LoRa, adapté pour la présence d'auto-brouillage. Dans la Section III.4.4, nous nous plaçons du point de vue de l'intercepteur, en comparant ses performances avec le récepteur légitime, et en explorant les stratégies qu'il peut mettre en place afin d'essayer de démoduler en aveugle.

### III.4.1. Front-end de synchronisation

Dans cette section, nous présentons le front-end de synchronisation utilisé pour le schéma d'auto-brouillage. Il se base sur celui présenté en Section I.2.6.3, mais avec des modifications afin de conserver de bonnes performances lorsqu'il y a des symboles d'auto-brouillage et la correction du PAPR. Dans ce qui suit, nous présentons d'abord en Section III.4.1.1 le front-end de synchronisation sous forme de schéma bloc. Ensuite, nous justifions en Section III.4.1.2 la pertinence d'utiliser  $cc1$  dans le front-end de synchronisation. Nous détaillons le nouveau bloc d'estimation  $STO_{frac}$  par candidats dans la Section III.4.1.3, et terminons par présenter à la fin différentes performances et comportements du front-end dans les Sections III.4.1.4 à III.4.1.7.

#### III.4.1.1. Schéma bloc

La Figure III.4.1 présente le front-end de synchronisation sous forme de schéma bloc. Chaque bloc est numéroté dans l'ordre chronologique d'exécution du front-end. Une étape préalable est la détection du préambule. Nous avons montré dans la Section I.2.6.4 que les détecteurs de préambule proposés dans la littérature sont peu performants ou difficilement applicables en pratique. Nous avons développé au cours de la thèse un détecteur offrant d'assez bonnes performances et prenant en compte au maximum les problématiques d'un usage réel. Il est présenté en détail dans la Section III.4.3. Dans le schéma bloc, le préambule est donc supposé détecté.

Comme pour LoRa legacy, nous estimons d'abord  $CFO_{frac}$  en étape 1a, avec l'estimateur [5]. Il conserve de bonnes performances d'estimation, même avec la correction du PAPR active (voir Section III.4.1.6).  $CFO_{frac}$  est ensuite corrigé en étape 1b.



III.4. Schéma d'auto-brouillage LoRa partie 2 : traitements au niveau du récepteur et performances

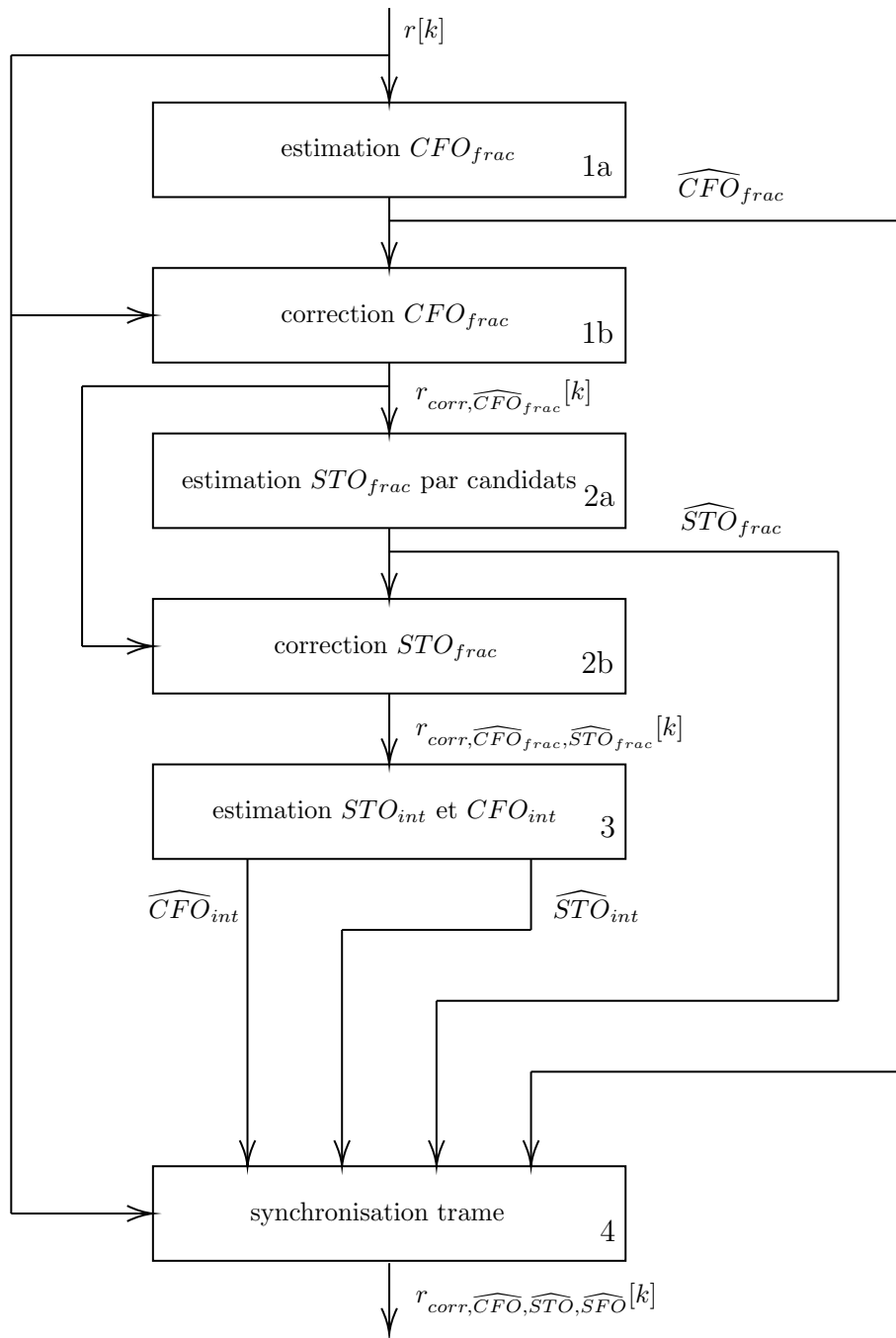


FIGURE III.4.1. – Front-end de synchronisation utilisé dans le schéma d'auto-brouillage

La principale modification du front-end vient de la pré-correction  $STO_{frac}$  permettant d'éliminer le plus possible la sensibilité lors de l'estimation de  $CFO_{int}$  et  $STO_{int}$ . Nous n'avons pas ré-utilisé l'estimateur  $STO_{frac}$  de la littérature [76]. En effet, ce dernier a des performances dégradées en présence d'auto-brouillage, et qui, surtout, deviennent instables à mesure que le SNR diminue. Ainsi, une approche par candidats (bloc 2a), certes plus lourde en complexité calculatoire, a été proposée et offre des performances qui restent stables avec le SNR. L'estimateur par candidats est présenté en détail dans la Section III.4.1.3, et les performances comparées entre les deux estimateurs sont montrées en Section III.4.1.7.  $STO_{frac}$  est ensuite corrigé dans le bloc 2b, toujours par sur-échantillonnage (voir Section I.2.6.3.3).  $CFO_{int}$  et  $STO_{int}$  sont estimés dans le bloc 3 de la même manière que dans le front-end de LoRa legacy, mais en utilisant la démodulation `cc1` au lieu de la démodulation classique par DFT LoRa directe. Enfin, une fois les paramètres de synchronisation  $CFO_{frac}$ ,  $CFO_{int}$ ,  $STO_{frac}$ ,  $STO_{int}$  et  $SFO$  (voir équation (I.2.38)) estimés, la trame complète est synchronisée dans le bloc 4.

### III.4.1.2. Intérêt d'utiliser `cc1` pour la synchronisation

Dans cette partie, nous justifions l'intérêt d'utiliser `cc1` et non `ccm` dans le front-end de synchronisation. En effet, `ccm` a une très forte sensibilité à la désynchronisation  $STO_{int}$ . Il n'est donc pas exploitable pour l'estimation de  $STO_{frac}$  par candidats ou celle de  $CFO_{int}$  et  $STO_{int}$ , puisque le signal reçu est désynchronisé temporellement d'une valeur inconnue à ce moment là. Cela est expliqué en détail dans la Section III.4.1.2.1. De plus, le moyennage des symboles `upchirp` et `downchirp` du préambule (conservé par rapport au front-end de synchronisation classique, voir Section I.2.6.3.3) permet de compenser presque entièrement la perte de performances de `cc1` sur  $U$ , et ce, pour des valeurs assez élevées de  $U$ . Cela est montré en Section III.4.1.2.2.

#### III.4.1.2.1. Sensibilité de `ccm` à la désynchronisation $STO_{int}$

La Figure III.4.2 montre l'impact du STO sur la démodulation `ccm` pour  $U = 8$ , sans correction du PAPR ( $f = 1$ ) et  $SF = 7$ . À gauche de la figure, nous affichons l'évolution de l'amplitude du bin d'intérêt pour `ccm`,  $A_{main} = F_{ccm}[(a - STO_{int}) \bmod M]$ , et celui d'interférence le plus élevé  $A_{inter,max}$ , en fonction du STO, pour les valeurs  $STO \in \{0.1, 0.2, \dots, 127\}$ . Nous considérons une transmission sans bruit AWGN et sans autre désynchronisation i.e.  $CFO = SFO = 0$ . Nous montrons le résultat pour une réalisation d'un canal virtuel. À droite, nous affichons le SER du payload en fonction du STO, pour les valeurs fractionnaires  $STO \in \{0.1, 0.2, \dots, 0.9\}$  et entières  $STO \in \{1, 32, 64, 96, 127\}$ , après synchronisation  $STO_{int}$  (aucune autre désynchronisation), pour  $SNR_{dB} = -6$ . Elle est réalisée en utilisant soit la démodulation `cc1` ou `ccm`. Ainsi, en fonction de la sensibilité au STO des deux démodulateurs, le SER sera plus ou moins impacté.

D'après la Figure III.4.2, nous remarquons que lorsque le STO est uniquement fractionnaire, `cc1` et `ccm` sont impactés de façon normale : plus ce dernier se rapproche de 0.5, plus la diffusion d'énergie sur les bins voisins est importante. En revanche, là où une désynchronisation  $STO_{int}$  entraîne seulement un décalage du bin d'intérêt pour `cc1` sans aucune déformation, `ccm` est très fortement impacté par ce dernier. Pour de nombreuses valeurs de STO, le pic d'interférence maximal dépasse celui d'intérêt ( $STO = 4$  par exemple), conduisant donc à une erreur de démodulation. Le SER de `ccm` est toujours

supérieur à 0.8 pour  $STO > 1$ .

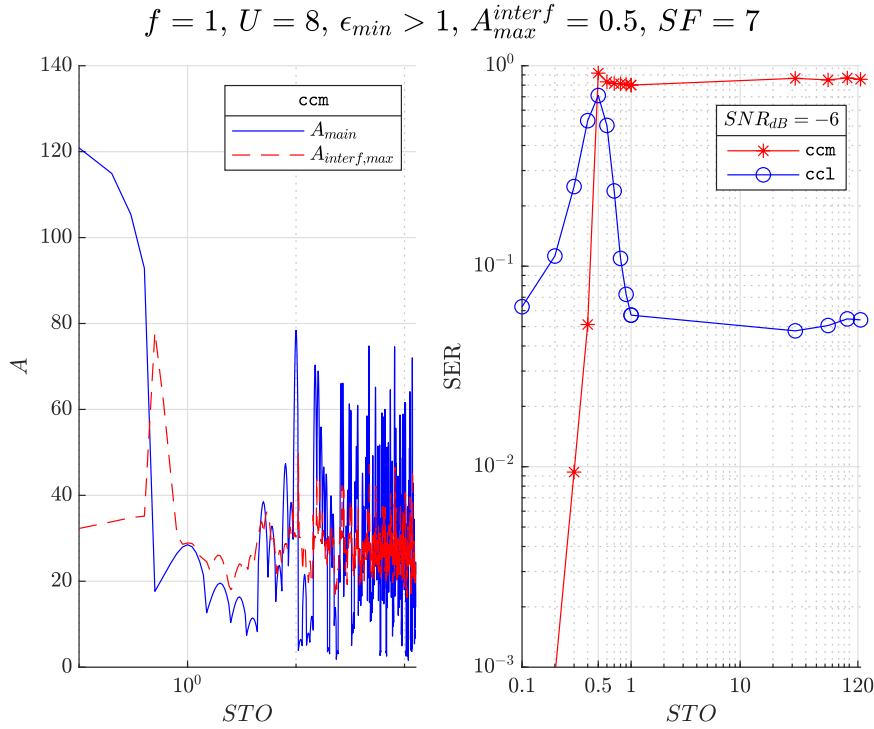


FIGURE III.4.2. – Comparaison de l'impact du STO entre  $cc1$  et  $ccm$ ,  $SF = 7$

Il serait souhaitable d'utiliser  $ccm$  au lieu de  $cc1$  dans le front-end de synchronisation afin d'éliminer la sensibilité sur  $U$  de  $cc1$  et donc d'obtenir de bonnes performances de synchronisation. Cela serait possible uniquement en effectuant une pré-compensation du STO avec une approche par candidat, afin de pouvoir extraire efficacement le bin d'intérêt. Même en supposant une telle pré-compensation parfaite, il sera toujours plus judicieux d'utiliser  $cc1$ . Premièrement, le moyennage des symboles upchirp et downchirp du préambule (toujours opéré avec auto-brouillage, voir Section III.4.1.1) permet de compenser entièrement la perte de performances, même pour des valeurs assez élevées de  $U$ . Cela est expliqué plus en détail dans la Section III.4.1.2.2. Deuxièmement, cela ajouterait une très forte complexité calculatoire. En effet, cela nécessiterait d'utiliser jusqu'à  $C = M \times R = 40960$  candidats pour  $SF = 12$  et  $R = 10$ , une approche peu viable pour une utilisation IoT réelle.

#### III.4.1.2.2. Compensation de la sensibilité sur $U$ de $cc1$ grâce au moyennage des symboles préambule lors de la synchronisation

Nous montrons ici que le moyennage des symboles upchirp et downchirp dans le préambule permet de compenser la perte de performances de  $cc1$  due à la sensibilité sur  $U$ , et donc de préserver de bonnes performances de synchronisation (estimation de  $CFO_{int}$  et  $STO_{int}$ ). Comme une erreur de synchronisation impacte directement la démodulation du payload, pour ne pas dégrader les performances globales, il serait souhaitable d'avoir des performances d'estimation de  $CFO_{int}$  et  $STO_{int}$  au moins aussi bonnes que celle du payload utilisant  $ccm$ . C'est ce que montre la Figure III.4.3 pour une correction du PAPR maximale ( $f = 1/U$ ),  $U \in \{20, 32, 33, 40\}$ , et  $SF = 7$ . Nous supposons une synchronisation parfaite.

D'après la Figure III.4.3, nous constatons :

- Pour des valeurs assez faibles de  $U$ , le moyennage compense très largement, avec un gain positif d'environ 2.2 dB à  $SEER = 10^{-4}$  pour  $U = 20$ , par exemple.
- Augmenter  $U$  diminue progressivement ce gain. Ce dernier tombe à environ 0.8 dB pour  $U = 32$  ( $SEER = 10^{-4}$ ).
- Pour  $U \geq 33$ , le moyennage ne compense plus suffisamment la perte cc1, le gain étant alors négatif. Pour  $U = 33$ , nous avons  $SEER \approx 2 \times 10^{-4}$  contre  $SEER \approx 3.5 \times 10^{-2}$  à  $SNR_{dB} = -4$ .

Ainsi, nous pouvons conclure que la valeur maximale de  $U$  sera limitée en pratique par les performances du front-end de synchronisation lorsque le SNR est modéré ( $SNR_{dB} < 0$ ), et qu'une valeur de  $U$  jusqu'à environ 30 est envisageable en pratique, sans avoir d'impact important sur les performances.

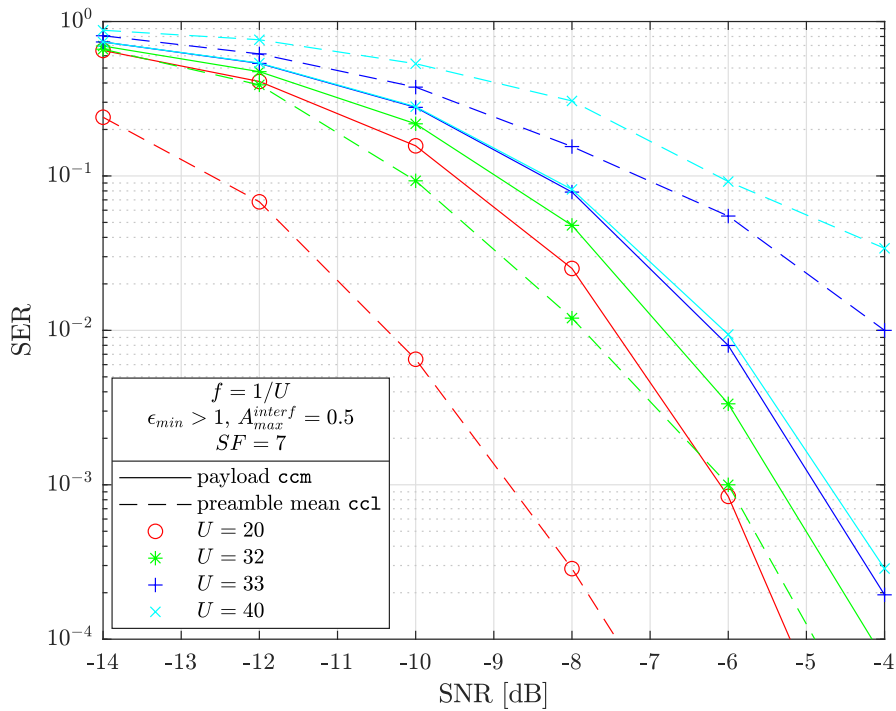


FIGURE III.4.3. – Compensation de la sensibilité sur  $U$  de cc1 grâce au moyennage des symboles de préambule lors de la synchronisation,  $SF = 7$

### III.4.1.3. Estimation de $STO_{frac}$ par candidats

Nous avons développé dans [97] un détecteur statistique du cas  $STO_{frac} \approx 0.5$ , permettant d'éliminer la très forte ambiguïté présente entre le bin d'intérêt et celui voisin dans la DFT lors de l'estimation de  $CFO_{int}$  et  $STO_{int}$ . Rappelons que plus  $STO_{frac}$  se rapproche de 0.5, plus le pic voisin gauche en  $n = (a - 1) \bmod M$  se rapproche du pic d'intérêt en  $n = a$  (voir Figure I.2.20). Pour  $STO_{frac} = 0.5$ , nous avons donc  $|\tilde{R}[(a - 1) \bmod M]| \approx |\tilde{R}[a]|$ . Ce détecteur présente d'assez bonnes performances s'il n'y a pas de correction du PAPR. Malheureusement, comme cette dernière déforme la DFT (voir Figure III.3.14), elle rend le détecteur instable (elle augmente de façon considérable la probabilité de fausse alarme), et cela, même pour des valeurs de SNR

élevées ( $SNR_{dB} > 0$ ). Par conséquent, nous avons abandonné cette approche au profit de la méthode d'estimation  $STO_{frac}$  proposée utilisant des candidats. Nous aurions pu aussi conserver l'estimateur  $STO_{frac}$  de la littérature [76]. Malheureusement, ce dernier voit ses performances dégradées lorsque  $U$  augmente et devient instable si une correction du PAPR est appliquée, même pour un régime SNR favorable. Nous le comparons avec l'estimateur proposé en Section III.4.1.7.

Dans cette partie, nous détaillons le bloc 2a implantant la méthode par candidats. Elle considère un ensemble de candidats  $STO_{frac}$ , noté  $\mathcal{S}_{STO_{frac}}$  avec  $C_{STO_{frac}} = |\mathcal{S}_{STO_{frac}}|$ , le nombre de candidats. Le récepteur retient le candidat ayant le niveau de déformation DFT le plus proche d'une synchronisation  $STO_{frac}$  parfaite i.e.  $STO_{frac} = 0$ . Le récepteur évalue pour cela l'écart de magnitude entre le bin démodulé et celui voisin (gauche ou droit) ayant la plus grande magnitude, pour obtenir une estimation de  $STO_{frac}$ . C'est sur cette approche que repose l'algorithme présenté dans l'algorithme 5. Notons que le modèle  $STO_{frac}$  est légèrement modifié. Dans la Section I.2.6.1.2, nous avons  $STO_{frac} \in [-0.5; 0.5]$ . Ici, nous avons fait le choix de le modéliser par  $STO_{frac} \in [0; 1]$ .

---

**Algorithm 5:** Algorithme d'estimation  $STO_{frac}$  par candidats

---

**inputs:**  $\{\mathbf{r}_i\}_{i=0}^{N_{up}-1}$  %symboles upchirp de préambule désynchronisés  $CFO_{int}$   
 ( $CFO_{frac}$  estimé et corrigé dans les blocs 1a et 1b (voir Figure III.4.1)),  
 $STO$  et  $SFO$   
 $\mathcal{S}_{STO_{frac}}$  %ensemble des candidats  $STO_{frac}$   
 $R$  %facteur de sur-échantillonnage pour la correction  $STO_{frac}$   
 (écart minimal entre les candidats de  $1/R$ )

- 1 **for**  $c = 0$  to  $C_{STO_{frac}} - 1$  **do**
- 2     sélectionner le  $c^{ème}$  candidat :  $STO_{frac}^{cand}$
- 3     corriger le STO des symboles upchirp de préambule par  $\widehat{STO} = STO_{frac}^{cand}$   
 (par sur-échantillonnage) et les déchirper :  $\tilde{\mathbf{r}}_{corr, STO_{frac}^{cand}}^{(i)}[k]$
- 4     moyenner les symboles upchirp de préambule corrigés :  
 $\langle \tilde{\mathbf{p}}_{corr, STO_{frac}^{cand}}[k] \rangle = \frac{1}{N_{up}} \sum_{i=0}^{N_{up}-1} \tilde{\mathbf{r}}_{corr, STO_{frac}^{cand}}^{(i)}[k]$
- 5     calculer l'inter-corrélation  $\mathbf{ccl} : \mathbf{F}_{ccl, corr, STO_{frac}^{cand}}[m]$ , puis normaliser :  

$$\mathbf{F}_{ccl, corr, STO_{frac}^{cand}}[m] = \frac{\mathbf{F}_{ccl, corr, STO_{frac}^{cand}}[m]}{\max_m \mathbf{F}_{ccl, corr, STO_{frac}^{cand}}[m]}$$
- 6     démoduler :  $\hat{a}_{up} = \arg \max_m \mathbf{F}_{ccl, corr, STO_{frac}^{cand}}[m]$
- 7     extraire les bins voisins :
- 8      $A^- = \mathbf{F}_{ccl, corr, STO_{frac}^{cand}}[(\hat{a}_{up} - 1) \bmod M]$
- 9      $A^+ = \mathbf{F}_{ccl, corr, STO_{frac}^{cand}}[(\hat{a}_{up} + 1) \bmod M]$
- 10     sélectionner le bin voisin direct maximal :  $A_{max} = \max \{A^-, A^+\}$
- 11     calculer la quantité :  $\delta_{STO_{frac}}(STO_{frac}^{cand}) = |1 - A_{max}|$
- 12     estimer  $STO_{frac}$  :  $\widehat{STO}_{frac} = \arg \max_{STO_{frac}^{cand} \in \mathcal{S}_{STO_{frac}}} \delta_{STO_{frac}}(STO_{frac}^{cand})$
- 13 **return**  $\widehat{STO}_{frac}$

---

Afin de conserver de bonnes performances d'estimation, il faut choisir un ensemble de candidats ayant un espacement entre candidats le plus homogène possible. Par exemple, pour le facteur de sur-échantillonnage  $R = 10$ , l'ensemble de candidats de taille maximale est  $\mathcal{S}_{STO_{frac}} = \{0, 1/R, 2/R, \dots, 1 - 1/R\}$ , avec donc un espacement entre candidats de  $1/R$  et  $C_{STO_{frac}} = R = 10$ . Notons que le récepteur peut éventuellement choisir un ensemble plus petit afin de réduire la complexité calculatoire, mais au prix d'une baisse de performances. Cela est montré plus en détail en Section III.4.1.4.

La Figure III.4.4 montre un exemple de la quantité  $\delta_{STO_{frac}}(STO_{frac}^{cand})$  pour  $U = 8$ ,  $STO = 88.2$ ,  $CFO = SFO = 0$ ,  $\mathcal{S}_{STO_{frac}} = \{0, 0.1, 0.2, \dots, 0.9\}$  ( $C_{STO_{frac}} = 10$ ), sans bruit AWGN et  $SF = 7$ . D'après la figure, nous constatons bien que l'écart de magnitude entre les deux bins d'évaluation augmente à mesure que  $STO_{frac}^{cand}$  se rapproche de  $STO_{frac}$ , avec un écart presque maximal proche de 1. Nous avons alors  $\widehat{STO}_{frac} = STO_{frac} = 0.2$ . Pour  $STO_{frac}^{cand} = 0.7$ , l'écart est minimal avec  $\delta_{STO_{frac}}(0.7) \approx 0$ . En effet, à cette valeur, la DFT synchronisée ( $R = 10$ ) aura un nouveau STO égal à  $STO - STO_{frac}^{cand} = 87.5$ , avec donc un nouveau  $STO_{frac} = 0.5$ . L'écart de magnitude est alors minimal. Notons que les valeurs candidates voisines à  $STO_{frac}$  sont assez proches du maximal (environ 0.89 dans l'exemple). Ainsi, avec l'effet du bruit AWGN, ces valeurs seront régulièrement sélectionnées conduisant à un résidu  $STO_{frac}$  final  $STO_{frac}^{residue} = 0.1$ , une valeur ayant un faible impact sur la démodulation (voir Figure I.2.21).

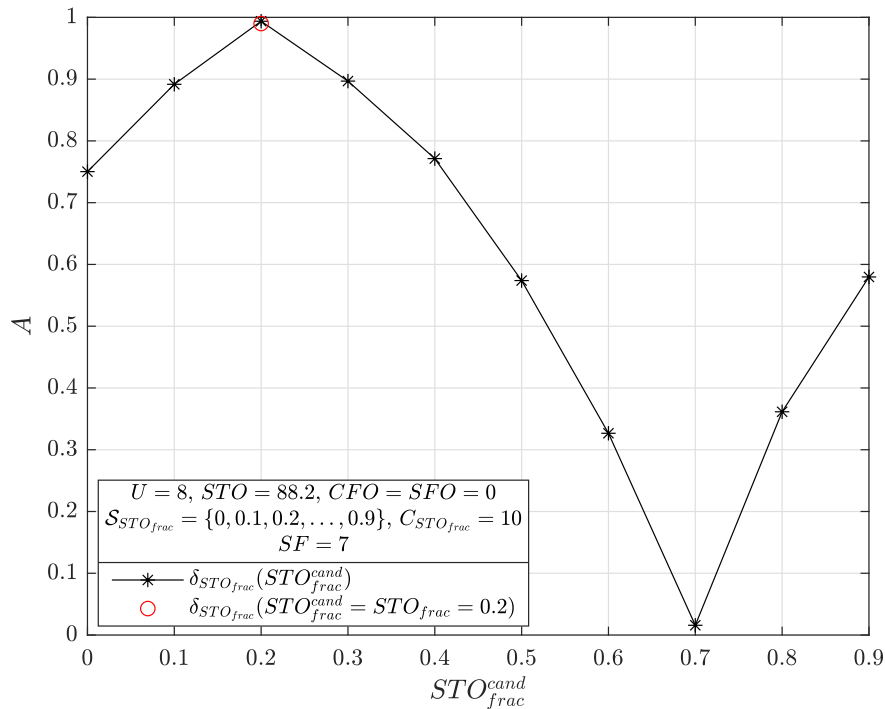


FIGURE III.4.4. – Exemple de fonctionnement de l'estimateur  $STO_{frac}$  par candidats,  $SF = 7$

### III.4.1.4. Impact du nombre de candidats $STO_{frac}$ sur les performances

La Figure III.4.5 montre l'impact du nombre de candidats  $STO_{frac}$  sur les performances de démodulation avec  $U = 8$ ,  $f = 1/U$ ,  $\epsilon_{min} > 1$ ,  $A_{max}^{interf} = 0.5$ ,  $R = 10$  et  $SF = 7$ . Le front-end de synchronisation est entièrement activé (estimation et correction du CFO, STO et SFO), mais avec un nombre variable de candidats :

- $C_{STO_{frac}} = 2$ ,  $\mathcal{S}_{STO_{frac}} = \{0, 0.5\}$ .
- $C_{STO_{frac}} = 5$ ,  $\mathcal{S}_{STO_{frac}} = \{0, 0.2, 0.5, 0.7, 0.9\}$ .
- $C_{STO_{frac}} = 10$ ,  $\mathcal{S}_{STO_{frac}} = \{0, 0.1, 0.2, \dots, 0.9\}$ .

Nous affichons aussi les performances dans le cas parfaitement synchronisé, comme point de comparaison. D'après la figure, nous voyons que la perte de performances en diminuant le nombre de candidats est assez faible.  $C_{STO_{frac}} = 10$  donne bien entendu les meilleures performances et sont très proches du cas parfaitement synchronisé. Passer de  $C_{STO_{frac}} = 10$  à  $C_{STO_{frac}} = 5$  engendre une perte de 0.2 dB à  $SEER = 10^{-3}$ , pour un gain en complexité calculatoire d'un facteur 2. Avoir  $C_{STO_{frac}} = 2$  dégrade plus les performances, de l'ordre de 0.5 dB, mais pour un gain en complexité calculatoire plus important, d'un facteur 5.

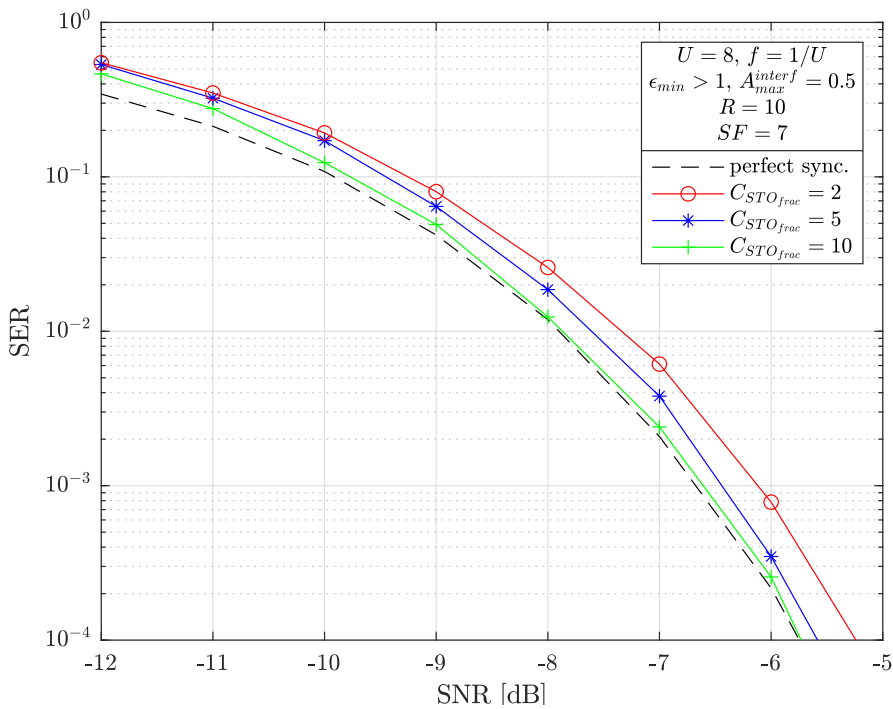


FIGURE III.4.5. – Impact du nombre de candidats  $STO_{frac}$  sur les performances de démodulation avec synchronisation,  $SF = 7$

Notons que pour  $C_{STO_{frac}} < R$ , en fonction de  $STO_{frac}$ , les performances ne seront pas les mêmes. La Figure III.4.6 montre le résidu minimal pouvant être obtenu en fonction de  $STO_{frac}$  pour plusieurs  $\mathcal{S}_{STO_{frac}}$  :

- $C_{STO_{frac}} = 3$ ,  $\mathcal{S}_{STO_{frac}} = \{0, 0.5, 1\}$ .
- $C_{STO_{frac}} = 5$ ,  $\mathcal{S}_{STO_{frac}} = \{0, 0.2, 0.5, 0.7, 0.9\}$ .

- $C_{STO_{frac}} = 10$ ,  $\mathcal{S}_{STO_{frac}} = \{0, 0.1, 0.2, \dots, 0.9\}$ .

D'après la Figure III.4.6, le résidu est nul si  $STO_{frac} \in \mathcal{S}_{STO_{frac}}$ , non nul sinon. Dans de bonnes conditions SNR ( $SNR_{dB} > 0$  par exemple), l'estimateur sélectionnera le candidat le plus proche de  $STO_{frac}$ . Pour  $C_{STO_{frac}} = 3$ , le cas le plus défavorable est lorsque  $STO_{frac} \in \{0.25, 0.75\}$ , donnant un écart de 0.25 avec les candidats les plus proches. De la même manière, pour  $C_{STO_{frac}} = 5$  et  $C_{STO_{frac}} = 10$ , les points défavorables sont atteints pour  $STO_{frac} = 0.35$  et  $STO_{frac} \in \{0.05, 0.15, 0.25, \dots, 0.95\}$ , respectivement. Comme les points défavorables diminuent lorsque  $C_{STO_{frac}}$  augmente (0.25 pour  $C_{STO_{frac}} = 3$ , 0.15 pour  $C_{STO_{frac}} = 5$  et 0.05 pour  $C_{STO_{frac}} = 10$ , respectivement), nous aurons statistiquement de meilleures performances pour des valeurs plus élevées de  $C_{STO_{frac}}$ , ce qui est parfaitement cohérent avec la Figure III.4.5. Pour le reste du mémoire, nous utiliserons  $C_{STO_{frac}} = 10$ , sauf indication contraire.

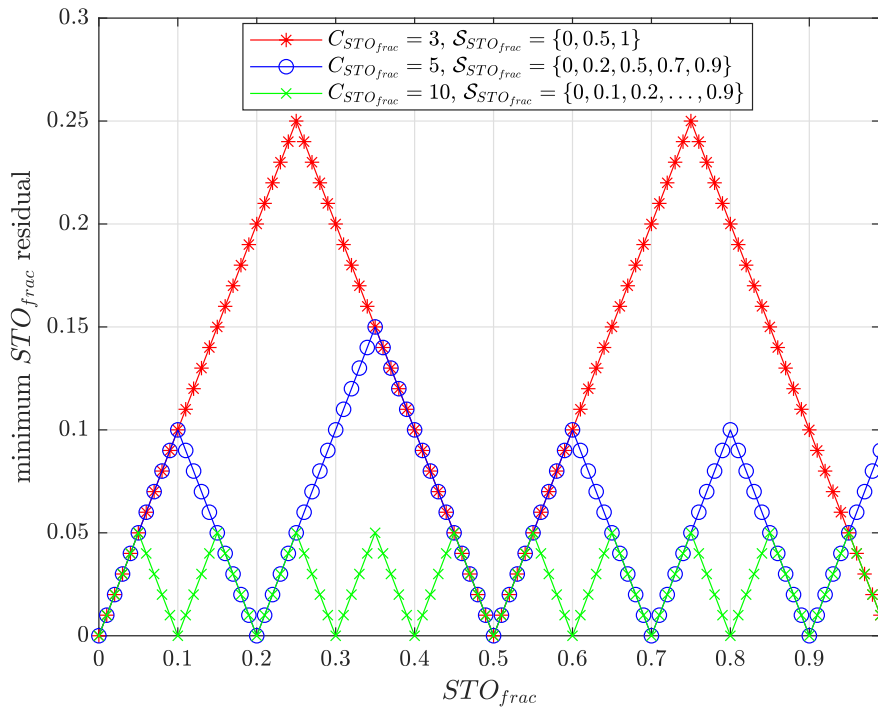


FIGURE III.4.6. – Résidu  $STO_{frac}$  minimal en fonction de  $STO_{frac}$  et du nombre de candidats  $STO_{frac}$

### III.4.1.5. Impact de l'espacement entre symboles d'auto-brouillage sur la synchronisation

Les Figures III.4.7 et III.4.8 mettent en évidence la nécessité de ne surtout pas avoir d'énergie dans le bin voisin d'inter-corrélation i.e. avoir  $\epsilon_u > 1$  pour assurer de bonnes performances de synchronisation, comme mentionné en Section III.3.3.4. Lorsque  $A_I$  est élevé, il y a une dégradation importante des performances en démodulation pure, mais aussi sur l'estimateur  $STO_{frac}$ . Ici, nous choisissons de montrer l'impact sur l'estimateur  $STO_{frac}$ . Pour cela, nous affichons le résidu  $STO_{frac}$  maximal et la probabilité que ce dernier soit supérieur à 0.3 ( $P[STO_{frac}^{residue} > 0.3]$  dans les deux figures), en fonction de  $A_I$ , et pour plusieurs valeurs  $SNR_{dB} \in \{-8, -4, 0\}$ . Rappelons que c'est le nombre d'équidistances entre symboles d'auto-brouillage qui fait augmenter  $A_I$ . Ainsi, plus  $A_I$  est



élevé, plus il y a d'équidistances, notées  $\epsilon_{eq}$ . Pour un même  $A_I$ , il peut y avoir plusieurs valeurs d'équidistance, noté  $\epsilon_{eq}$ . Par exemple, trois symboles ayant  $\epsilon_{eq} = 1$  ou  $\epsilon_{eq} = 4$ . Nous montrons en Figure III.4.7 l'impact important lorsque  $\epsilon_{eq} = 1$  (équivalent à avoir  $\epsilon_u = 1$ ), comparé à une autre valeur respectant  $\epsilon_u > 1$ ,  $\epsilon_{eq} = 2$  (Figure III.4.8). Dans la simulation, l'estimateur  $CFO_{frac}$  est activé et  $CFO_{int}$  et  $STO_{int}$  sont tirés aléatoirement uniformes dans  $\{0, 1, \dots, M/4 - 1\}$  et  $\{0, 1, \dots, M - 1\}$ , respectivement.

Pour les deux figures, nous constatons que les performances se dégradent progressivement à mesure que  $A_I$  augmente, de façon cohérente avec les résultats en Figure III.3.5. Cependant, l'impact est beaucoup plus marqué lorsque  $\epsilon_{eq} = 1$ . Premièrement, le résidu maximal est globalement plus élevé. Pour  $SNR_{dB} = -8$  par exemple, nous avons un écart de résidu maximal entre  $\epsilon_{eq} = 1$  (Figure III.4.7) et  $\epsilon_{eq} = 2$  (Figure III.4.8) de 0, 0.1, 0.1, 0.2, 0.1, 0.1 et 0.1, pour chaque valeur de  $A_I$  (ordre croissant). Nous constatons clairement l'instabilité de l'estimateur lorsque  $\epsilon_{eq} = 1$ , avec une probabilité bien plus élevée pour  $A_I = 0.875$  à faible SNR ( $SNR_{dB} = -8$ ). Nous avons  $P[STO_{frac}^{residue} > 0.3] \approx 0.36$  pour  $\epsilon_{eq} = 1$  contre  $P[STO_{frac}^{residue} > 0.3] \approx 0$  pour  $\epsilon_{eq} = 2$ . Cela vient du fait que pour  $\epsilon_{eq} = 1$ , le pic d'interférence d'inter-corrélation maximal est au bin voisin direct gauche. Cela impacte donc très fortement l'estimée de  $STO_{frac}$  (lignes 10, 11 et 12 dans l'algorithme 5). Notons que l'impact de l'espacement entre symboles d'auto-brouillage sur l'estimateur  $CFO_{frac}$  est quasiment négligeable, même en ayant une équidistance maximale ( $A_I = 1$ ) et  $STO_{frac}$  proche de 0.5.

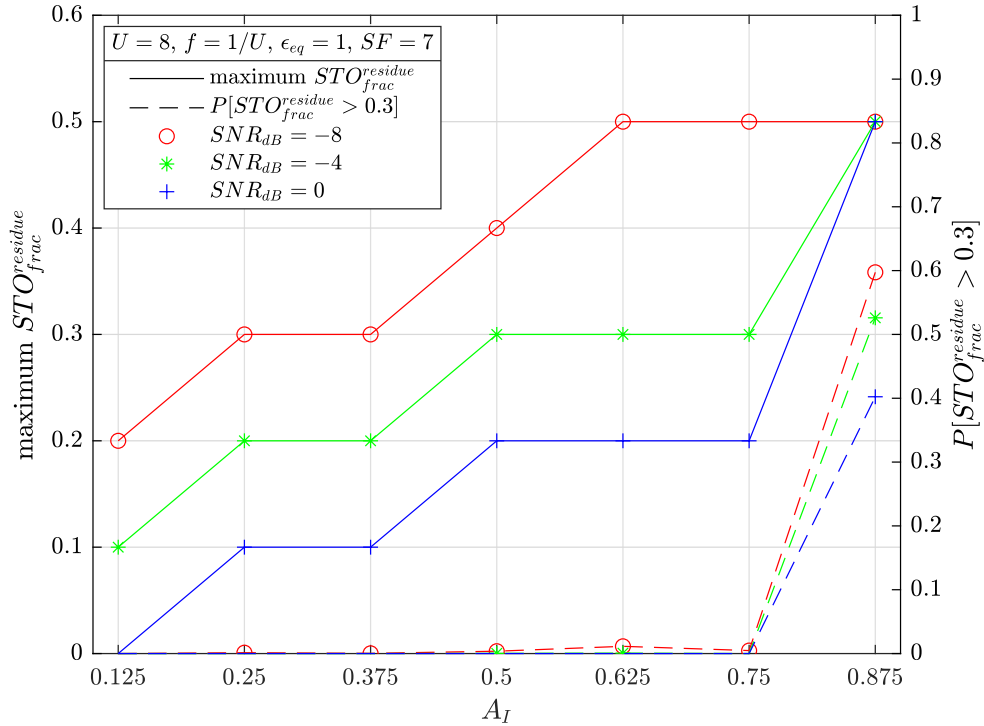


FIGURE III.4.7. – Impact de  $A_I$  sur l'estimateur  $STO_{frac}$  par candidats,  $SF = 7$ ,  $\epsilon_{eq} = 1$

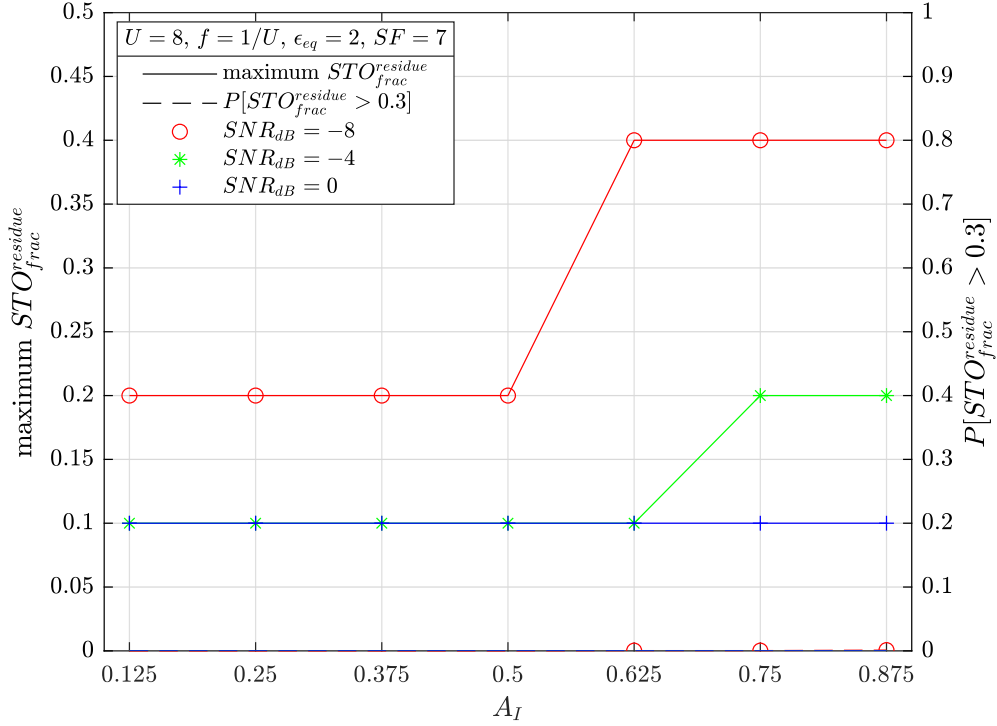


FIGURE III.4.8. – Impact de  $A_I$  sur l'estimateur  $STO_{frac}$  par candidats,  $SF = 7$ ,  $\epsilon_{eq} = 2$

### III.4.1.6. Performances d'estimation de $CFO_{frac}$ avec auto-brouillage

La Figure III.4.9 montre les performances d'estimation de  $CFO_{frac}$  en terme de résidu maximal après synchronisation  $CFO_{frac}$ , en fonction de  $U \in \{1, 2, 4, 6, \dots, 20\}$  pour  $SNR_{dB} \in \{-8, 0\}$  et  $SF = 7$ . Rappelons que la présence de STO ne perturbe pas l'estimation de  $CFO_{frac}$  (voir Tableau I.2.5). Nous supposons une synchronisation STO parfaite et les paramètres du schéma d'auto-brouillage  $\epsilon_{min} > 1$  et  $A_{max}^{interf} = 0.5$ . Nous comparons LoRa jam ( $f = 1$ ) et LoRa jam mod pour une correction du PAPR de moitié ( $f = 0.5$ ) ou maximale ( $f = 1/U$ ).

D'après la Figure III.4.9, nous constatons :

- A fort SNR ( $SNR_{dB} = 0$ ), l'estimateur se comporte de la même manière pour tous les schémas de modulation considérés.
- A faible SNR ( $SNR_{dB} = -8$ ), nous remarquons :
  - Pour  $U \leq 12$ , l'estimateur est peu impacté par le schéma d'auto-brouillage, avec ou sans correction du PAPR. Nous avons en effet un résidu maximal  $CFO_{frac}$  inférieur à 0.08.
  - LoRa jam n'impacte réellement que pour des valeurs très élevées de  $U$  ( $U > 18$ ).
  - LoRa jam mod ( $f = 0.5$ ) est vraiment impacté pour  $U > 16$ .
  - LoRa jam mod ( $f = 1/U$ ) devient plus inconsistant que LoRa jam mod ( $f = 0.5$ ) pour des valeurs plus basses de  $U$ , dès  $U = 14$ .

Nous pouvons conclure que l'ajout d'auto-brouillage (avec ou sans correction du PAPR) a un impact raisonnable sur l'estimateur  $CFO_{frac}$ , si le SNR n'est pas trop faible.

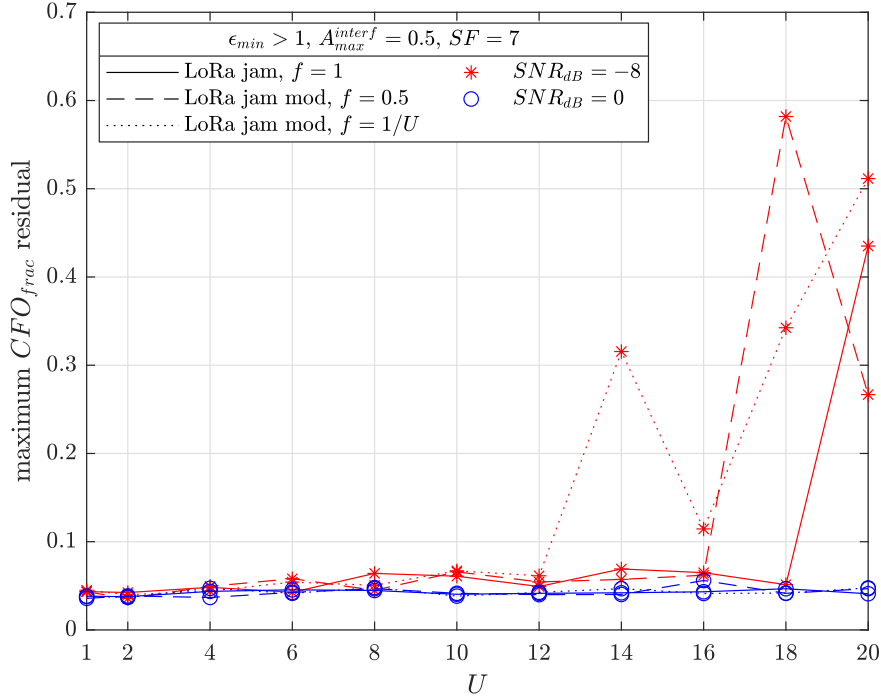


FIGURE III.4.9. – Comparaison des performances d'estimation de  $CFO_{frac}$  (résidu maximal) LoRa jam ( $f = 1$ ) vs. LoRa jam mod ( $f = 0.5$  et  $f = 1/U$ ),  $SF = 7$

### III.4.1.7. Comparaison des estimateurs $STO_{frac}$ de la littérature et candidats

La Figure III.4.10 montre les performances d'estimation  $STO_{frac}$  en terme de résidu maximal  $STO_{frac}$  (avant estimation de  $CFO_{int}$  et  $STO_{int}$ ) pour  $SNR \in \{0, -8\}$ . Par exemple, pour une trame reçue ayant  $STO = 10.1$  et  $\widehat{STO}_{frac} = 0.9$ , nous aurons un nouveau STO égal à  $STO = STO - \widehat{STO}_{frac} = 9.2$ . Le résidu avant estimation de  $CFO_{int}$  et  $STO_{int}$  sera alors  $STO_{frac}^{residue} = 0.2$ . Nous avons les mêmes paramètres qu'en Figure III.4.9, mais en comparant l'estimateur  $STO_{frac}$  de la littérature [76] et celui par candidats, avec  $C_{STO_{frac}} = 10$  (voir Section III.4.1.3). Nous considérons LoRa jam ( $f = 1$ ) et LoRa jam mod ayant une correction du PAPR maximale ( $f = 1/U$ ) et  $CFO_{frac} = 0$ , du fait que la présence de  $CFO_{frac}$  perturbe l'estimation de  $STO_{frac}$  (voir Tableau I.2.5).  $CFO_{int}$  et  $STO_{int}$  sont tirés aléatoirement.

D'après la Figure III.4.10, nous remarquons :

- Pour  $SNR_{dB} = 0$  (gauche) :
  - Pour LoRa jam ( $f = 1$ ), le résidu maximal ne dépasse pas 0.1, quelque soit l'estimateur et la valeur de  $U$  considérés. Cela montre de bonnes performances.
  - La correction du PAPR dégrade rapidement les performances de l'estimateur de la littérature, surtout pour  $U > 10$ , avec une forte inconsistance, où le résidu peut atteindre  $STO_{frac}^{residue} = 1$ , mettant en défaut la démodulation.
  - Même avec une correction du PAPR maximale, l'estimateur par candidats conserve de très bonnes performances, avec  $STO_{frac}^{residue} \leq 0.1$ .

- Pour  $SNR_{dB} = -8$  (droite) :
  - Diminuer le SNR rend inconsistant l'estimateur de la littérature lorsque LoRa jam est utilisé. Par exemple, pour  $U = 10$ , le résidu maximal atteint  $STO_{frac}^{residue} = 0.7$ , une valeur très mauvaise. Utiliser LoRa jam mod ( $f = 1/U$ ) dégrade encore plus les performances à faible SNR. L'estimateur devient rapidement inconsistant avec  $U$ . Pour  $U \geq 10$ , ce dernier ne fonctionne plus.
  - L'estimateur par candidats quant à lui se comporte très bien, avec un résidu maximal qui reste faible ( $STO_{frac}^{residue} \leq 0.2$ ), quelque soit  $U$  ou la correction du PAPR appliquée.

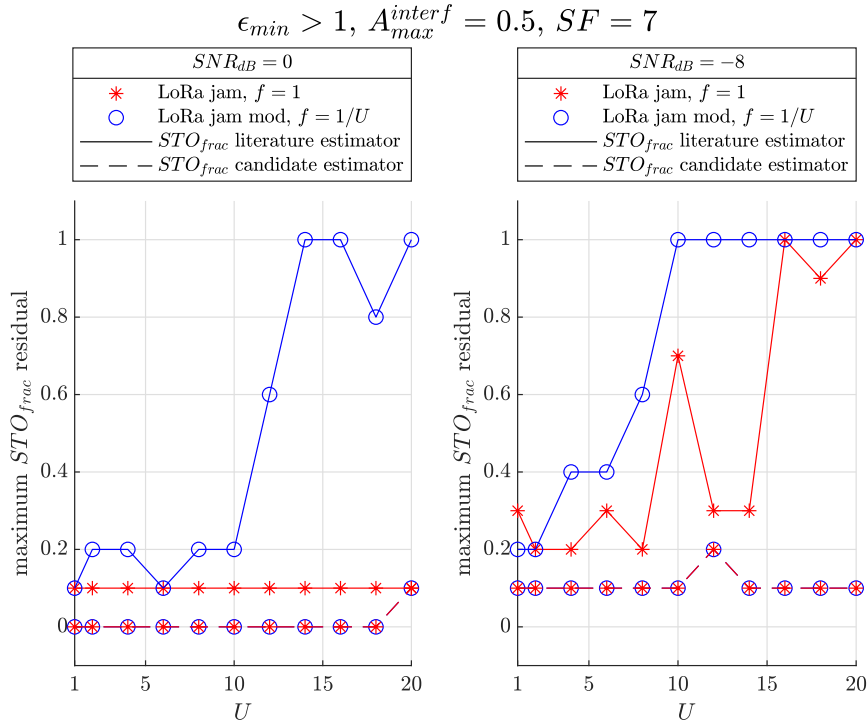


FIGURE III.4.10. – Comparaison des performances d'estimation  $STO_{frac}$  (résidu maximal) entre l'estimateur de la littérature et celui par candidats proposé,  $SF = 7$

## III.4.2. Performances finales du récepteur légitime

Dans cette Section, nous présentons les performances finales du récepteur légitime utilisant le schéma d'auto-brouillage. Elles sont évaluées en fonction de  $U$ , du facteur de correction du PAPR  $f$ , avec ou sans synchronisation active utilisant le front-end de synchronisation présenté en Section III.4.1.

### III.4.2.1. Impact du facteur de correction du PAPR sur le SER avec/sans front-end de synchronisation

La Figure III.4.11 montre les performances SER du schéma d'auto-brouillage pour  $U = 8$  et  $f \in \{1, 0.75, 0.5, 0.25, 1/U\}$ , en considérant une synchronisation parfaite d'une part et la présence de désynchronisation avec front-end de synchronisation actif d'autre

part. Nous affichons aussi les performances d'une transmission LoRa non-cohérente classique (voir équation (I.2.13)) avec synchronisation parfaite, qui servent comme borne optimale de performances.

D'après la Figure III.4.11, le schéma d'auto-brouillage (sans correction du PAPR,  $f = 1$ ) entraîne une perte de performances par rapport à LoRa legacy très raisonnable, de l'ordre de 0.3 dB à  $SEER = 10^{-4}$ . Comme attendu, les performances se dégradent de plus en plus à mesure que la correction du PAPR augmente. Entre  $f = 1$  et  $f = 1/U$ , nous avons une perte d'environ 1.2 dB à  $SEER = 10^{-4}$ , avec front-end de synchronisation actif. Enfin, nous voyons que pour  $U = 8$  et  $f$  fixé, le front-end de synchronisation ne dégrade que très peu les performances. La perte est quasiment négligeable pour  $f \geq 0.75$ , et devient un peu plus perceptible lorsque  $f < 0.75$ , pour atteindre une valeur maximale d'environ 0.1 dB, quelque soit le SNR.

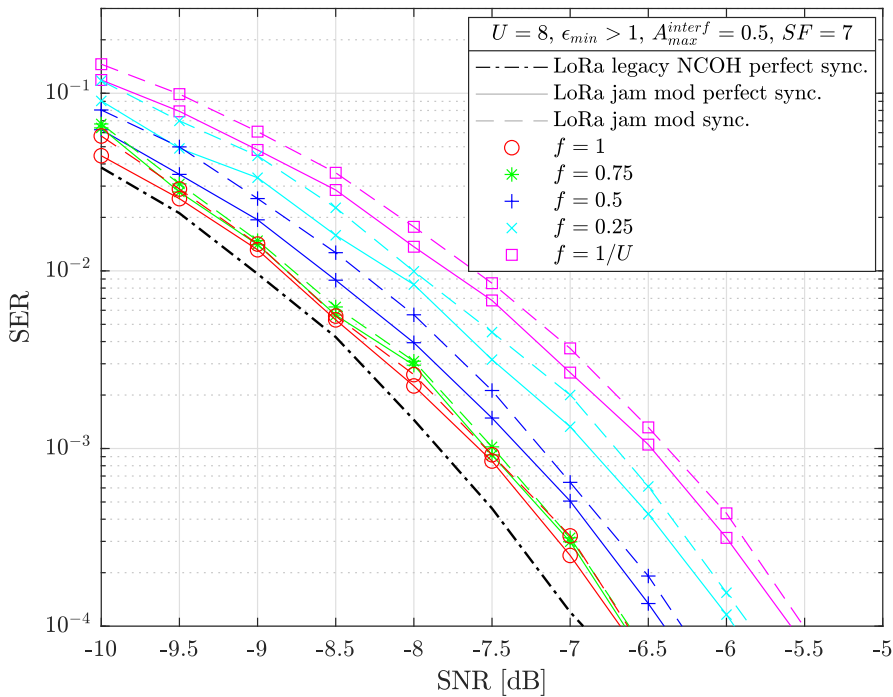


FIGURE III.4.11. – Impact du facteur de correction du PAPR sur les performances du schéma d'auto-brouillage, avec/sans front-end de synchronisation,  $SF = 7$

### III.4.2.2. Impact de $U$ sur le SER avec/sans front-end de synchronisation

La Figure III.4.12 reprend la même comparaison qu'en Figure III.4.11, mais en fonction de  $U \in \{5, 10, 15, 20\}$ , et pour une correction du PAPR maximale ( $f = 1/U$ ). Sur la figure, nous retrouvons le comportement observé sur la Figure III.4.11 : l'activation du front-end de synchronisation n'entraîne pas de dégradation significative des performances. La perte est très faible jusqu'à  $U = 10$ , et devient un peu plus perceptible au delà. Nous avons des pertes à  $SEER = 10^{-4}$  pour  $U = 5$  quasiment négligeables et d'environ 0.2 dB pour  $U = 20$ . Notons aussi que lorsque  $U$  est élevé, les pics d'interférence d'inter-corrélation circulaire ayant une magnitude proche de  $A_{max}^{interf}$  sont plus nombreux statistiquement (voir Figure

III.3.8). Cela réduit donc les performances, mais dans une moindre mesure cependant. Nous pouvons conclure que bien que LoRa legacy donne les meilleures performances dans l'absolu, l'activation conjointe du schéma d'auto-brouillage, de la correction du PAPR et du front-end de synchronisation entraîne une perte de performances assez raisonnable, ne dépassant pas 2.3 dB pour  $U \leq 20$ ,  $f = 1/U$ , avec le front-end de synchronisation actif.

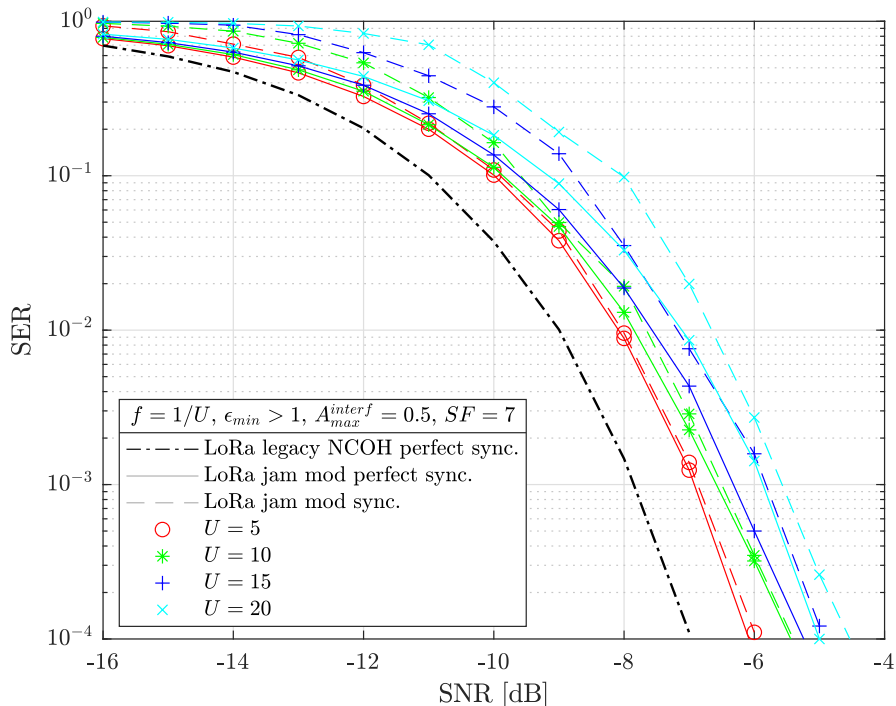


FIGURE III.4.12. – Impact de  $U$  sur les performances du schéma d'auto-brouillage avec correction maximale du PAPR, avec/sans front-end de synchronisation,  $SF = 7$

### III.4.2.3. Performances en fonction de $U$ et $SF$

La Figure III.4.13 montre l'évolution des performances de LoRa jam mod en fonction de  $U$  et  $SF$ , pour  $U \in \{5, 10, 15, 20\}$ ,  $SF \in \{7, 8, 9, 10\}$ ,  $f = 1/U$  et avec front-end de synchronisation actif. Nous affichons aussi celles de LoRa legacy avec synchronisation parfaite, servant de performances de référence.

D'après la Figure III.4.13, nous constatons que le comportement est le même quelque soit  $SF$ . Ainsi, malgré l'espace DFT plus grand permettant de placer plus de symboles ( $M = 1024$  pour  $SF = 10$ , contre  $M = 128$  pour  $SF = 7$ ), il n'y aura pas de gain de traitement lié au schéma d'auto-brouillage. La règle de gain de 2.5 dB de performances SER pour chaque incrément de  $SF$  (voir Règle (I.2.102)) est ici plutôt bien respectée. Nous avons une perte liée à  $U$  un peu plus marquée pour  $SF = 7$ . Cela vient du fait que le nombre moyen de pics d'interférence d'inter-corrélation ayant une amplitude proche de  $A_{max}^{interf} = 0.5$  est non négligeable par rapport au nombre de total de bins  $M$ . Cela impacte de fait les performances. Cela est visible sur la figure, où la perte à  $SER = 10^{-3}$  entre  $U = 5$  et  $U = 20$  est plus importante pour  $SF = 7$ . Nous avons une perte d'environ 1.5 dB pour  $SF = 7$  contre une perte inférieure à 1.2 dB pour les autres valeurs de  $SF$ .

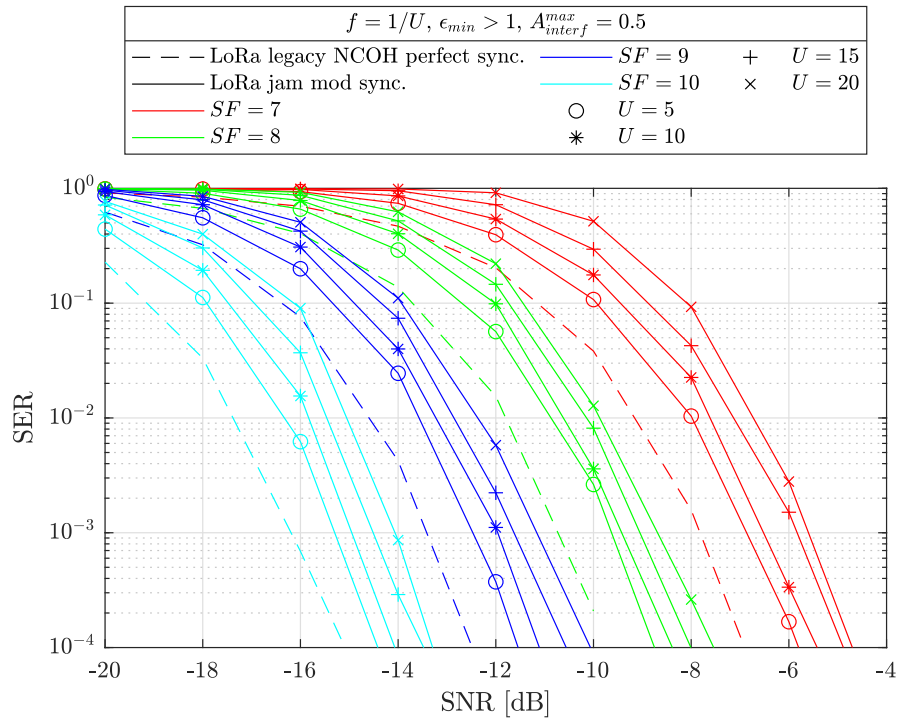


FIGURE III.4.13. – Performances du schéma d'auto-brouillage en fonction de  $U$  et SF avec front-end de synchronisation actif

### III.4.3. Détection de trame

Dans cette section, nous présentons le front-end de détection de trame proposé pour le schéma d'auto-brouillage. Il se base sur une approche par détection d'énergie exploitant au maximum les propriétés d'auto-brouillage. En Section III.4.3.1, nous présentons son schéma bloc et détaillons les principales étapes. Nous présentons ensuite une méthode de réduction de complexité calculatoire en Section III.4.3.2. Enfin, nous montrons quelques résultats de performances en simulation en Section III.4.3.3.

#### III.4.3.1. Front-end de détection de trame

La Figure III.4.14 montre le schéma bloc du front-end de détection de trame. Il complète les travaux des auteurs dans [79] en prenant en compte les désynchronisations CFO et STO en réception. Dans le même esprit que lors de la présentation du front-end de synchronisation (voir Figure III.4.1), nous numérotions les blocs dans l'ordre d'exécution.

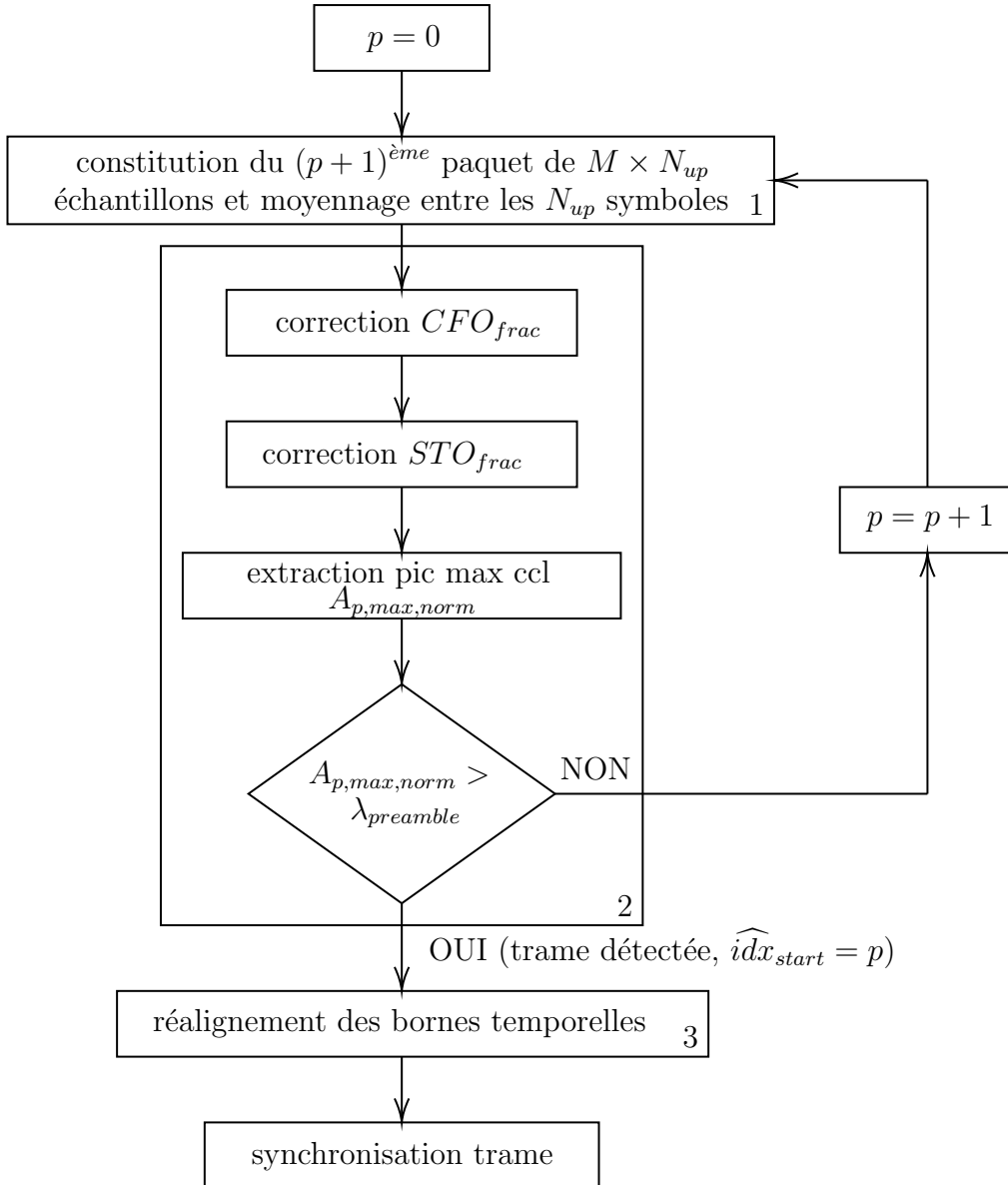


FIGURE III.4.14. – Front-end de détection de trame utilisé dans le schéma d’auto-brouillage

### III.4.3.1.1. Étape 1 – constitution des paquets de $N_{up}$ symboles

Le récepteur constitue un paquet de  $N_{up}$  symboles ( $M \times N_{up}$  échantillons reçus), d’indice  $p$ . Le récepteur doit déterminer la présence ou l’absence de trame LoRa (hypothèses  $H_0$  et  $H_1$ , voir Section I.2.6.4). Si le récepteur ne détecte pas de trame (échantillons de bruit AWGN), il passe au paquet suivant en se décalant d’une période symbole ( $M$  échantillons). Ce processus est illustré en Figure III.4.15 pour  $N_{up} = 4$ , et est équivalent à l’effet d’une fenêtre glissante dans le temps. En cas de détection de trame, le récepteur poursuit sur le traitement supplémentaire effectué dans le bloc 3. Nous décidons de normaliser la puissance du signal reçu par rapport à la puissance du bruit AWGN par :

$$r_p[k] = \frac{r_p[k]}{\hat{\sigma}^2} \quad (\text{III.4.1})$$



avec  $r_p[k]$ , le paquet d'indice  $p$ .

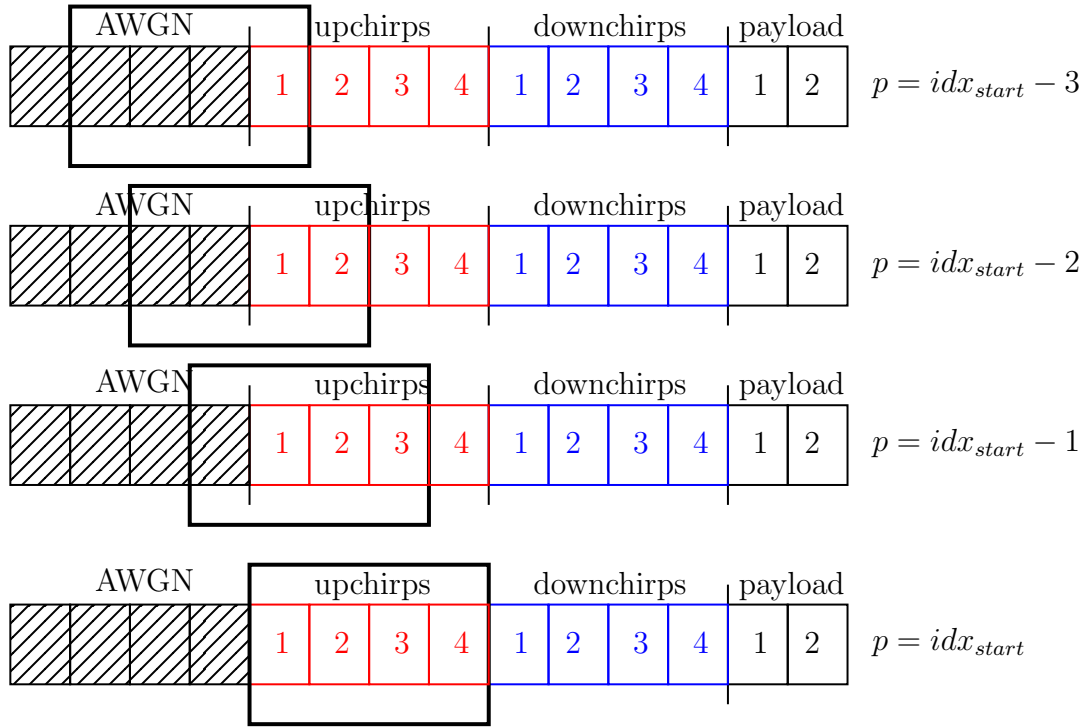


FIGURE III.4.15. – Effet de fenêtre glissante temporelle du module de détection de trame du schéma d'auto-brouillage

### III.4.3.1.2. Étape 2 – détection du préambule

La détection de trame se fait par la détection du préambule LoRa. Elle est réalisée dans le bloc 2 en comparant le niveau de ressemblance entre chaque paquet moyenné et le préambule parfaitement connu. Cette comparaison est possible à condition de normaliser la puissance du paquet (voir équation (III.4.1)). Cela suppose que le récepteur possède une bonne estimée du niveau de bruit i.e.  $\hat{\sigma}^2 \approx \sigma^2$ .

Les désynchronisations  $CFO_{frac}$  et  $STO_{frac}$  réduisent les capacités de démodulation (diffusion de l'énergie sur les bins voisins). Le récepteur doit donc d'abord réaliser une correction de  $CFO_{frac}$  et  $STO_{frac}$  en utilisant l'estimateur  $CFO_{frac}$  de la littérature [76] et l'estimateur  $STO_{frac}$  par candidats présenté en Section III.4.1.3. Les estimées dans le paquet courant  $p$  sont notées  $\widehat{CFO}_{frac,p}$  et  $\widehat{STO}_{frac,p}$ . Nous notons  $r_{p,sync}[k]$ , le paquet pré-synchronisé  $CFO_{frac}$  et  $STO_{frac}$ . La détection se fait alors par :

$$\widehat{idx}_{start} = \begin{cases} p & \text{si } A_{p,max,norm} \geq \lambda_{preamble} \\ \emptyset & \text{sinon} \end{cases} \quad (\text{III.4.2})$$

avec :

$$A_{p,max,norm} = \max_m \langle F_{p,ccl,norm}[m] \rangle \quad (\text{III.4.3})$$

$$\langle F_{p,ccl,norm}[m] \rangle = \frac{\langle F_{p,ccl}[m] \rangle}{\sqrt{\frac{M}{2N_{up}}}} \quad (\text{III.4.4})$$

$$\langle F_{p,ccl}[m] \rangle = \sum_{n=0}^{M-1} \left| \langle \tilde{P}_p[n] \rangle \tilde{S}_{ref}[(n-m) \bmod M] \right| \quad (\text{III.4.5})$$

$$\langle \tilde{P}_p[n] \rangle = \frac{1}{N_{up}} \sum_{i=0}^{N_{up}-1} \tilde{R}_{p+i}[n] \quad (\text{III.4.6})$$

et  $\tilde{S}_{ref}[n]$  dans l'équation (III.4.5) défini dans l'équation (III.3.15). De façon assez intuitive, plus le paquet courant se rapproche du début de préambule, plus la quantité  $A_{p,max,norm}$  augmentera du fait de l'effet de fenêtre glissante temporelle, d'après la Figure III.4.15. Nous aurons donc une énergie maximale lorsque  $p = idx_{start}$ .

Nous notons  $A_{p,max}$ , la statistique de détection non normalisée, utilisée à des fins d'illustration :

$$A_{p,max} = \max_m \langle F_{p,ccl}[m] \rangle \quad (\text{III.4.7})$$

Une fois  $idx_{start}$  estimé, le récepteur corrige  $CFO_{frac}$  et  $STO_{frac}$  sur toute la trame stockée en mémoire avec les estimées  $\widehat{CFO}_{frac,p}$  et  $\widehat{STO}_{frac,p}$ . Nous pouvons remarquer que la statistique de détection dans l'équation (III.4.7) utilise la recherche du pic max (fonction  $\max(\cdot)$  utilisée), et non la lecture sur un même bin dans la DFT (indice  $n = 0$  par exemple si parfaitement synchronisé). Pour  $N$  variables aléatoires indépendantes et identiquement distribuées, la variable aléatoire :

$$Y = \max_n \{X_0, X_1, \dots, X_n, \dots, X_{N-1}\} \quad (\text{III.4.8})$$

possède les probabilités de densité (PDF) et fonction de répartition (CDF) suivantes :

$$f_Y(t) = NF_X^{N-1}(t)f_X(t) \quad (\text{III.4.9})$$

$$F_Y(t) = F_X^N(t) \quad (\text{III.4.10})$$

avec  $f_X(t)$  et  $F_X(t)$ , les densité de probabilité et fonction de répartition communes aux variables aléatoires  $X_n$ . C'est le cas ici, avec chaque bin de corrélation circulaire indépendants les uns des autres sous l'hypothèse  $H_0$ . Nous avons alors  $N = M$ . Pour  $U = 1$  (détection sans auto-brouillage), nous avons :

$$f_{A_{p,max,norm}}(t) = MF_{ccl}^{M-1}(t)f_{ccl}(t) \quad (\text{III.4.11})$$

$$F_{A_{p,max,norm}}(t) = F_{ccl}^M(t) \quad (\text{III.4.12})$$

avec :

$$f_{ccl}(t) = f_{Rayleigh}(t, 1) \quad (\text{III.4.13})$$

$$F_{ccl}(t) = F_{Rayleigh}(t, 1) \quad (\text{III.4.14})$$

La densité de probabilité est alors parfaitement en accord avec l'histogramme obtenu

en simulation. Pour  $U > 1$ , nous pouvons ré-utiliser les expressions en équations (III.2.13) et (III.2.14) (somme de  $U$  lois de Rayleigh) comme expressions de  $f_{ccl}(t)$  et  $F_{ccl}(t)$ , respectivement.

La Figure III.4.16 compare l'expression théorique de la densité de probabilité et l'histogramme de  $A_{p,max, norm}$ , sous l'hypothèse  $H_0$ , pour  $U \in \{1, 5, 10, 15, 20\}$  et  $SF = 7$ , et en supposant  $\hat{\sigma}^2 = \sigma^2$ . Grâce aux normalisations réalisées dans les équations (III.4.1) et (III.4.4), la statistique ne dépend pas du SNR, ni du nombre de symboles de préambule upchirp. Nous remarquons que plus  $U$  augmente, plus la distribution se décale vers la droite (amplitudes statistiquement plus élevées). Nous notons bien l'absence de biais entre théorie et simulation pour  $U = 1$ , et un biais croissant pour  $U > 1$ , avec un élargissement de la distribution. Les fonctions non-linéaires dans les équations (III.4.11) et (III.4.12) (dues à la fonction  $\max(\cdot)$  dans l'équation (III.4.3)) amplifient le biais des PDF et CDF résultantes.

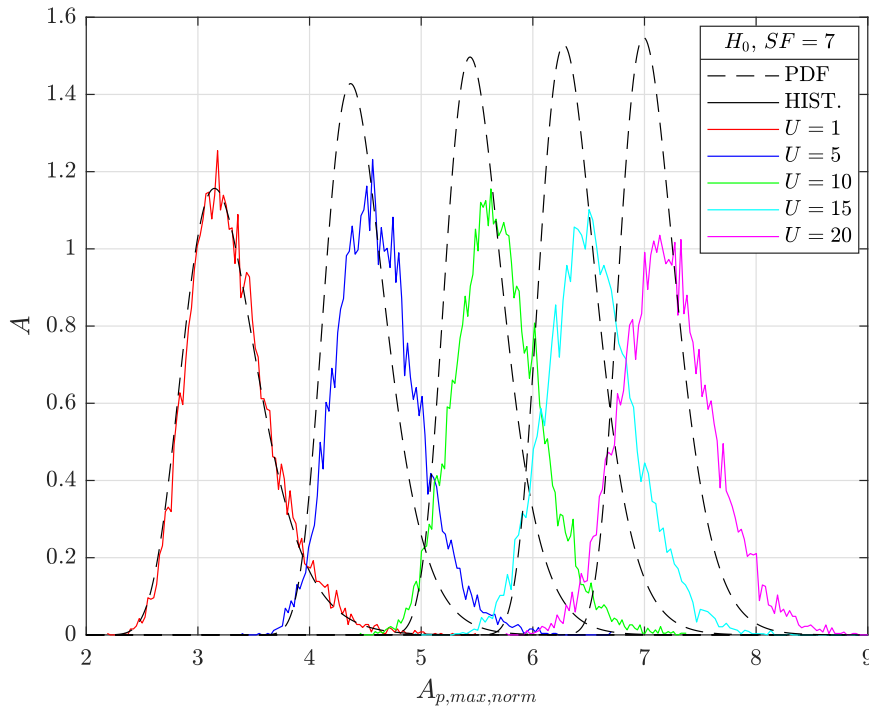


FIGURE III.4.16. – Densité de probabilité et histogramme du critère de détection de préambule pour plusieurs valeurs de  $U$  sous l'hypothèse  $H_0$ ,  $SF = 7$

De la même manière que pour les travaux de détection de brouilleur, le seuil  $\lambda_{preamble}$  est obtenu en respectant une contrainte de probabilité de fausse alarme notée  $P_{fa}$ . Extraire ce seuil directement à partir des expressions théoriques engendrerait un biais dans les performances et ne conduirait donc pas à une comparaison équitable entre les cas sans et avec auto-brouillage. Ainsi, nous décidons d'extraire le seuil de façon numérique, par tirages de Monte-Carlo.

La Figure III.4.17 compare la probabilité de fausse alarme obtenue via l'expression théorique biaisée et réelle en simulation, pour  $U \in \{1, 5, 10, 15, 20\}$  et  $SF = 7$ . D'après la figure, la distribution théorique donne bien entendu une probabilité de fausse alarme biaisée pour  $U > 1$  ( $U = 1$  ne donne pas de biais (voir Figure III.4.16), la courbe de simulation n'est donc pas affichée), mais pas si éloignée, avec un écart de valeur du seuil

s'élargissant légèrement avec  $U$ . Notons que l'élargissement ne dépend pas de SF, du fait de la normalisation dans l'équation (III.4.4).

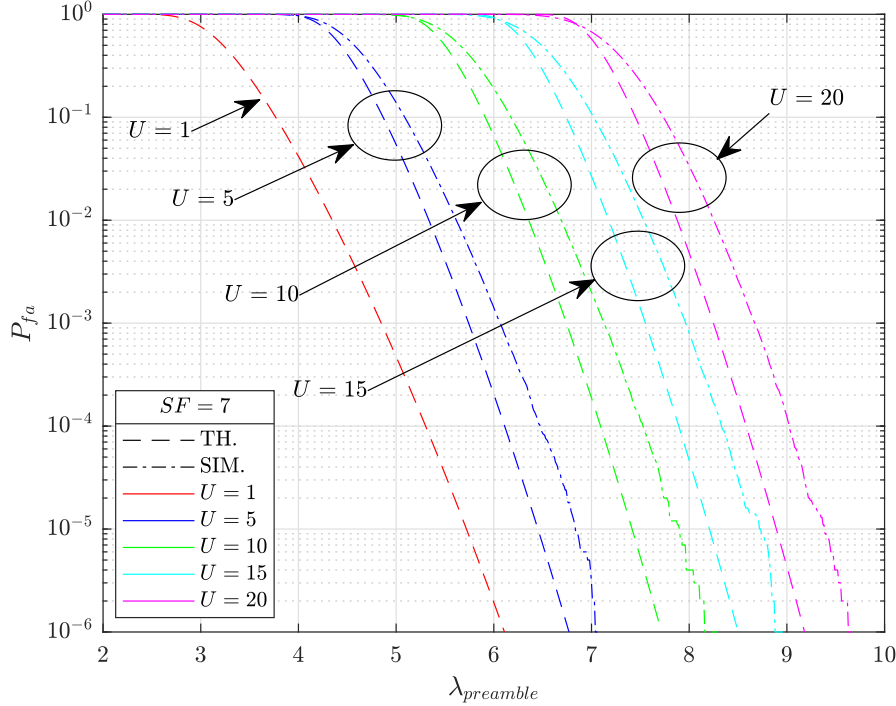


FIGURE III.4.17. – Probabilité de fausse alarme de détection de préambule théorique biaisée et réelle pour plusieurs valeurs de  $U$ ,  $SF = 7$

Le Tableau III.4.1 donne les valeurs de seuil pour quelques valeurs de  $U$ ,  $P_{fa} = 10^{-5}$  et  $SF = 7$ . Ces valeurs seront réutilisées par la suite.

$U$	1	5	10	15	20	30
$\lambda_{preamble}$	5.72	6.83	7.82	8.72	9.38	10.70

TABLE III.4.1. – Seuils de détection de préambule pour plusieurs valeurs de  $U$ ,  $P_{fa} = 10^{-5}$  et  $SF = 7$

La Figure III.4.18 montre un exemple d'exécution du front-end avec détection initiale d'une trame pour trois valeurs de  $STO$ ,  $STO \in \{12, 60, 125\}$ ,  $U = 10$ ,  $\lambda_{preamble} = 7.82$  (voir Tableau III.4.1),  $f = 1/U$ ,  $SNR_{dB} = 0$  et  $SF = 7$ . Dans la simulation, nous introduisons 8 symboles purement AWGN avant le début de la trame (dénnoté par la variable  $N_{zeros}$ ) afin de visualiser le gain progressif en énergie du détecteur.

Nous voyons très clairement sur la figure la montée progressive d'énergie, avec un niveau maximal valant environ 108. Selon la valeur de  $STO$ , l'indice de début de trame estimé ne sera pas le même. Nous avons en effet  $\widehat{id}_{start} = id_{start} = 9$  pour  $STO = 12$ , mais  $\widehat{id}_{start} = id_{start} + 1 = 10$  pour  $STO = 60$  et  $STO = 125$ . Plus  $STO_{int}$  se rapproche de  $M - 1$ , plus la probabilité de choisir  $\widehat{id}_{start} = id_{start} + 1$  est grande, puisque la contribution du symbole courant dans l'ISI diminue à mesure que  $STO_{int}$  augmente. L'énergie s'atténue ensuite pour  $p > id_{start}$ . En effet, le récepteur évalue  $A_{p,max}$  sur des symboles downchirp mais démodulés upchirp, donnant une DFT inexploitable. Notons

que le cas  $\widehat{idx}_{start} \notin \{idx_{start}, idx_{start} + 1\}$  n'arrive uniquement que pour des SNR très faibles, bien inférieurs à ceux donnant de bonnes performances de démodulation.

$$U = 10, f = 1/U, SNR_{dB} = 0, N_{up} = 8, N_{zeros} = 8, SF = 7$$

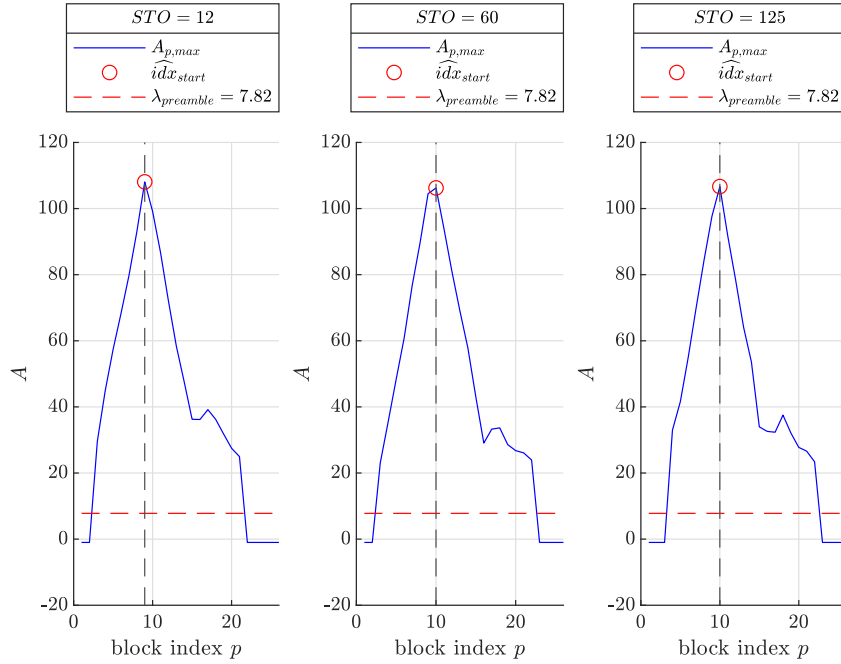


FIGURE III.4.18. – Exemple d'exécution du module de détection de préambule,  $SF = 7$

### III.4.3.1.3. Étape 3 – réalignement des bornes temporelles

Les Figures III.4.19 et III.4.20 montrent une illustration des bornes temporelles pour les deux cas arrivant en pratique  $\widehat{idx}_{start} = idx_{start}$  et  $\widehat{idx}_{start} = idx_{start} + 1$ . Rappelons que la correction de  $STO_{int}$  est équivalente à décaler le signal reçu de  $STO_{int}$  échantillons vers la gauche. Dans le cas  $\widehat{idx}_{start} = idx_{start}$ , il n'y a pas problème, la correction de  $STO_{int}$  après son estimation réalignera correctement le signal. En revanche, le cas  $\widehat{idx}_{start} = idx_{start} + 1$  est problématique. En effet, l'estimateur  $STO_{int}$  donnera toujours  $\widehat{STO}_{int} = STO_{int}$ . La correction alignera en fait les bornes par rapport au symbole suivant et le récepteur sera alors décalé lors de la démodulation du payload avec  $\widehat{a}_i = a_{i+1}$ . Cela vient du fait que dans le second cas, il est nécessaire d'appliquer un décalage du signal de  $M - STO_{int}$  échantillons vers la droite et non vers la gauche, comme le ferait la correction de  $STO_{int}$  (comportement opposé). Il faudrait pour cela avoir systématiquement  $\widehat{idx}_{start} = idx_{start}$ , ce qui n'est pas possible (voir Figure III.4.18).

Une première approche est d'adapter le comportement de correction de  $STO_{int}$  en fonction de  $idx_{start}$  et donc de  $STO_{int}$ . Pour cela,  $STO_{int}$  est normalement estimé, mais à partir du début  $\widehat{idx}_{start}$ , puis il faut décider d'un décalage vers la gauche ou vers la droite. Cette approche fonctionne bien, mais uniquement si  $STO_{int}$  est proche de 0 ou  $M - 1$ . Une valeur  $STO_{int} \approx M/2$  rendant l'incertitude sur  $\widehat{idx}_{start}$  forte (fluctuation aléatoire entre  $\widehat{idx}_{start} = idx_{start}$  et  $\widehat{idx}_{start} = idx_{start} + 1$  importante) empêcherait le bon fonctionnement. Ainsi, utiliser une information préalable de  $STO_{int}$  pour le réalignement pourtant peu coûteuse en complexité calculatoire n'est pas viable en pratique.

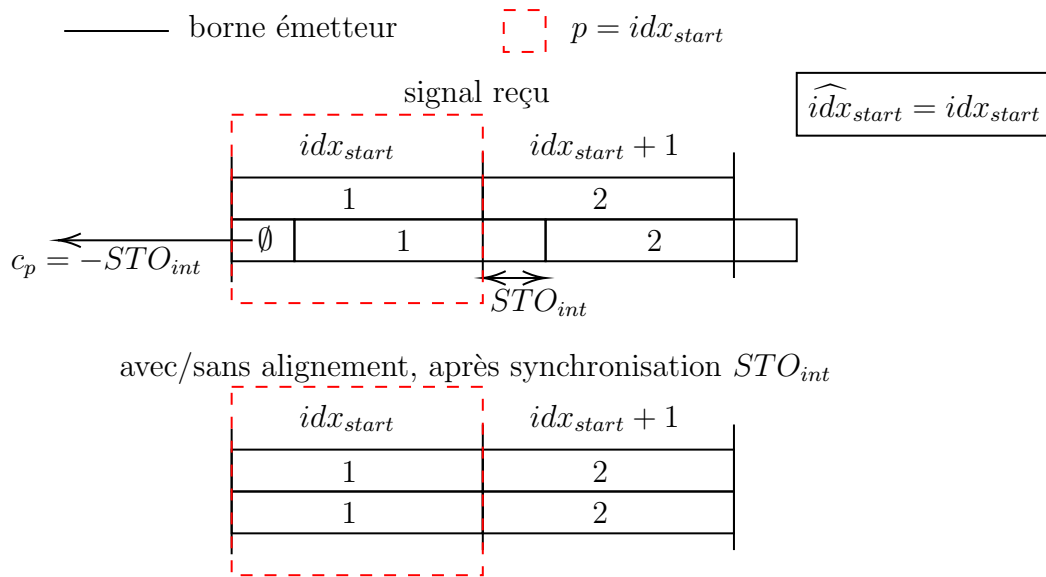


FIGURE III.4.19. – Illustration du décalage des bornes temporelles de trame et du réalignement nécessaire,  $\widehat{idx}_{start} = idx_{start}$

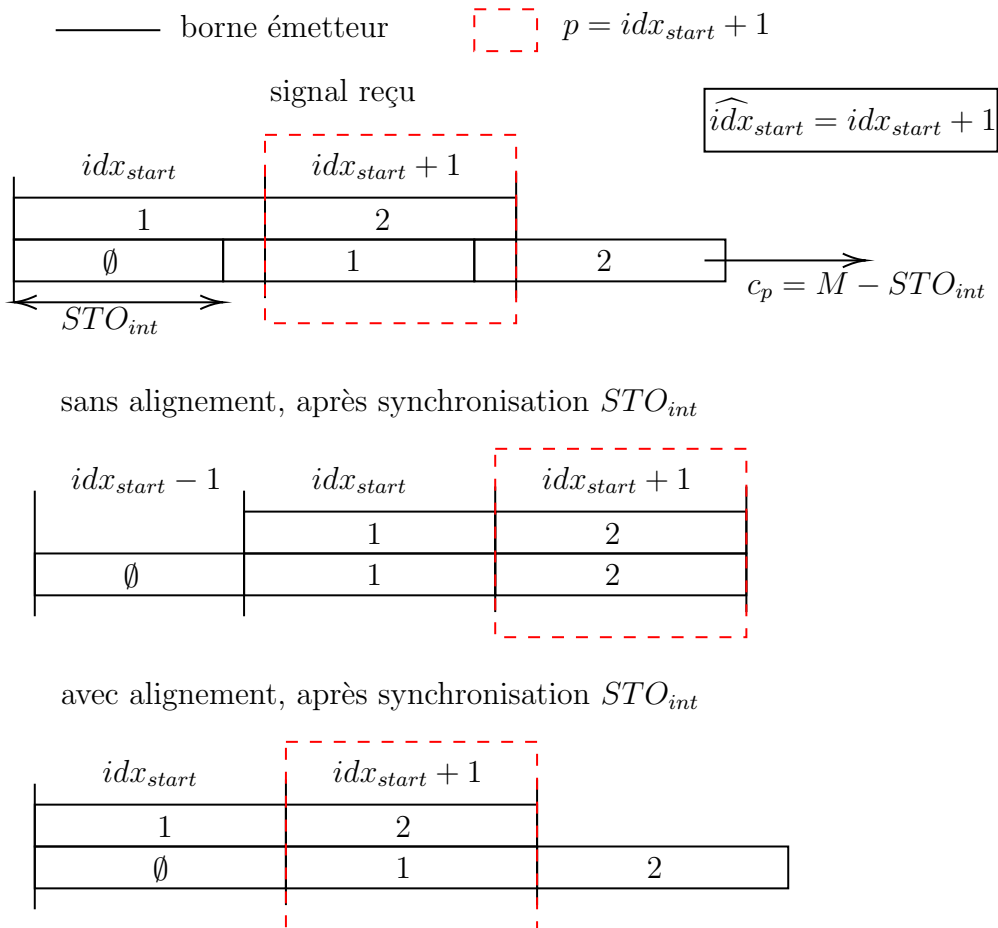


FIGURE III.4.20. – Illustration du décalage des bornes temporelles de trame et du réalignement nécessaire,  $\widehat{idx}_{start} = idx_{start} + 1$

Nous notons  $c_p$ , le nombre d'échantillons de décalage nécessaire à partir de  $p = \widehat{id}x_{start}$ . Pour résoudre ce problème, nous décidons d'utiliser la même approche que pour l'estimation de  $id x_{start}$ , en cherchant le décalage vers la droite (noté  $\beta_p$ ) maximisant l'énergie en partant de  $p = \widehat{id}x_{start} - 1$ . D'après les Figures III.4.19 et III.4.20, nous devons avoir pour les deux cas un décalage vers la droite de  $M + STO_{int}$  et  $STO_{int}$  échantillons, respectivement. Nous avons alors les relations :

$$\beta_p = \begin{cases} M + STO_{int} & \text{si } \widehat{id}x_{start} = id x_{start} \\ STO_{int} & \text{si } \widehat{id}x_{start} = id x_{start} + 1 \end{cases} \quad (\text{III.4.15})$$

$$c_p = \begin{cases} -STO_{int} & \text{si } \widehat{id}x_{start} = id x_{start} \\ M - STO_{int} & \text{si } \widehat{id}x_{start} = id x_{start} + 1 \end{cases} \quad (\text{III.4.16})$$

L'ensemble :

$$\mathcal{B} = \{0, 1, \dots, 2M\} \quad (\text{III.4.17})$$

doit donc être balayé. Le récepteur peut alors réaligner les bornes à partir de :

$$\widehat{c}_p = M - \widehat{\beta}_p \quad (\text{III.4.18})$$

avec :

$$\widehat{\beta}_p = \arg \max_{\beta} A_{p,\beta,max} \quad (\text{III.4.19})$$

D'après les Figures III.4.19 et III.4.20, le signe de  $\widehat{c}_p$  donne la direction du décalage :

- $\widehat{c}_p < 0$  : décalage de  $|\widehat{c}_p|$  échantillons vers la gauche.
- $\widehat{c}_p = 0$  : aucun décalage nécessaire.
- $\widehat{c}_p > 0$  : décalage de  $\widehat{c}_p$  échantillons vers la droite.

La Figure III.4.21 montre un exemple d'évolution de cette énergie en fonction de  $\beta$ , notée  $A_{p,\beta,max}$ , pour  $STO = 36$  et  $STO = 118$  (mêmes autres paramètres qu'en Figure III.4.18). Nous voyons sur la figure le comportement attendu d'augmentation puis de diminution de l'énergie. Sans bruit AWGN et résidu de désynchronisation, le récepteur obtient  $\widehat{c}_p = c_p$ . Ce n'est pas le cas ici mais est assez proche, avec un décalage de 5 et 8 échantillons, respectivement.

$$U = 10, f = 1/U, SNR_{dB} = 0, N_{up} = 8, N_{zeros} = 8, SF = 7$$

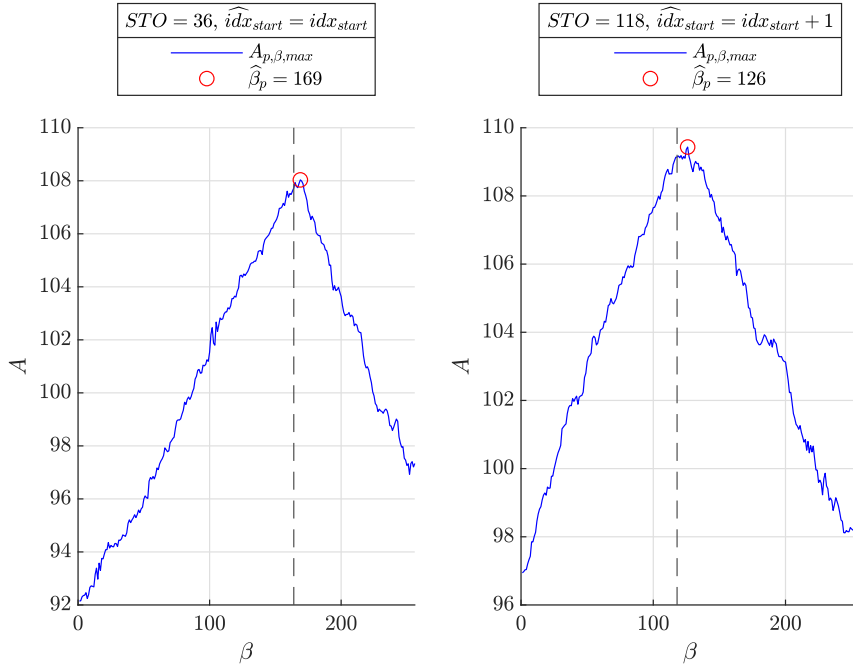


FIGURE III.4.21. – Exemple d'estimation du ré-alignement des bornes temporelles de trame,  $SF = 7$

### III.4.3.2. Réduction de la complexité calculatoire et modification de la règle de correction du STO

Balayer l'ensemble  $\mathcal{B}$  apporte une complexité calculatoire importante. Il faut en effet démoduler avec  $\text{cc1}$   $2M + 1$  fois, puis appliquer une fonction  $\text{argmax}$  pour pouvoir estimer  $c_p$ . En pratique, il est possible de réduire considérablement l'espace de recherche tout en conservant les mêmes performances d'alignement, en terme de STO résiduel, noté  $STO_{residue}$ , après alignement. Si  $\hat{c}_p = c_p$ , alors  $STO_{residue} = 0$ . Si l'ensemble  $\mathcal{B}$  est discrétisé par pas de  $\Delta$  :

$$\mathcal{B}_\Delta = \{0, \Delta, 2\Delta, \dots, \Delta(B(\Delta) - 1)\}, \quad \Delta \leq 2M \quad (\text{III.4.20})$$

avec  $B(\Delta)$  le nombre de valeurs dans  $\mathcal{B}_\Delta$  :

$$B(\Delta) = \left\lfloor \frac{2M}{\Delta} \right\rfloor + 1 \quad (\text{III.4.21})$$

Le nombre d'itérations nécessaires (et donc la complexité calculatoire) est réduit d'un facteur :

$$r_{comp}(\Delta) = \frac{2M + 1}{B(\Delta)} \quad (\text{III.4.22})$$

Pour  $\Delta = 40$  et  $SF = 7$  ( $M = 128$ ), nous avons par exemple  $r_{comp}(40) \approx 36.7$ . En fonction de la valeur de  $STO_{int}$ , le niveau d'alignement minimal ne sera pas le même.



D'après les équations (III.4.18) et (III.4.20), nous avons :

$$STO_{residue,min}(\Delta) = \beta_p - \beta_\Delta(b_{min}) \quad (III.4.23)$$

avec :

$$b_{min} = \arg \min_b |\beta_p - \beta_\Delta(b)| \quad (III.4.24)$$

$\beta_\Delta(b)$ , la valeur dans  $\mathcal{B}_\Delta$  à l'indice  $b$  et  $\beta_p$  défini dans l'équation (III.4.15). Comme exemple, supposons les deux valeurs  $\Delta = 32$  et  $\Delta = 100$ . Nous avons alors :

$$\mathcal{B}_{32} = \{0, 32, 64, 96, 128, 160, 192, 224, 256\}, \quad \mathcal{B}_{100} = \{0, 100, 200\} \quad (III.4.25)$$

Pour  $STO_{int} = 36$  (valeur donnant  $\widehat{id}x_{start} = idx_{start}$  en pratique), nous obtenons  $STO_{residue,min}(32) = 4$  (du fait que  $164 - 100 = 4$ ) et  $STO_{residue,min}(100) = -36$  (du fait que  $164 - 200 = -36$ ), respectivement. L'alignement pour  $\Delta = 32$  est donc meilleur que  $\Delta = 100$ . En fonction du signe de  $STO_{residue}(\Delta)$ , la valeur estimée de  $a_{up}$  lors de la synchronisation ne sera pas la même (et donc l'estimation de  $STO_{int}$ ). En négligeant le bruit AWGN, nous avons la relation suivante :

$$\widehat{a}_{up} = \begin{cases} (a_{up} + \lfloor CFO \rfloor + (M - |STO_{residue}(\Delta)|)) \bmod M & \text{si } STO_{residue}(\Delta) < 0 \\ (a_{up} + \lfloor CFO \rfloor) \bmod M & \text{si } STO_{residue}(\Delta) = 0 \\ (a_{up} + \lfloor CFO \rfloor + |STO_{residue}(\Delta)|) \bmod M & \text{si } STO_{residue}(\Delta) > 0 \end{cases} \quad (III.4.26)$$

Par exemple, pour  $CFO = a_{up} = 0$ ,  $SF = 7$ ,  $STO_{int} = 10$ ,  $STO_{residue}(\Delta) = -2$  et  $STO_{residue}(\Delta) = 3$ , nous avons  $\widehat{a}_{up} = 126$  et  $\widehat{a}_{up} = 3$ , respectivement. Cela vient donc changer le comportement de synchronisation du récepteur (voir équation (I.2.47)). Nous avons alors (en supposant  $a_{up} = 0$  et le CFO corrigé) :

- Si  $\widehat{a}_{up} = \widehat{STO}_{int} \leq M/2$ , nous décalons de  $(\widehat{STO}_{int} + \lfloor \widehat{STO}_{frac} \rfloor) \times R$  échantillons vers la droite.
- Si  $\widehat{a}_{up} = \widehat{STO}_{int} > M/2$ , nous décalons de  $((M - \widehat{STO}_{int}) - \lfloor \widehat{STO}_{frac} \rfloor) \times R$  échantillons vers la gauche.

La Règle (III.4.26) est valable uniquement si  $|STO_{residue}(\Delta)| \leq M/2$ , le comportement est inversé sinon. Comme le récepteur ne connaît pas  $STO_{residue}(\Delta)$ , il ne pourra pas s'adapter. Cela suppose donc d'avoir  $STO_{residue}(\Delta)$  assez faible, et choisir  $\Delta$  en conséquence : suffisamment faible pour garantir  $STO_{residue}(\Delta) \leq M/2$ , mais assez élevé pour ne pas avoir une complexité calculatoire trop importante.

La Figure III.4.22 montre l'évolution du premier et second résidu minimal, notés  $STO_{residue,min}(\Delta)$  et  $STO_{residue,neighbor}(\Delta)$ , respectivement. Par exemple, si  $\Delta = 128$  et  $STO_{int} = 20$ , nous aurons alors  $STO_{residue,min}(\Delta) = 20$  (du fait que  $148 - 128 = 20$ ) et  $STO_{residue,neighbor}(\Delta) = -108$  (du fait que  $148 - 256 = -108$ ). Nous traçons en fonction de  $STO_{int}$  pour plusieurs valeurs  $\Delta \in \{32, 64, 128, 200\}$  et  $SF = 7$ . Nous avons les réductions de complexité calculatoire de facteurs 28.5, 51.4, 85.6 et 128.5, respectivement.

D'après la Figure III.4.22, nous remarquons les points suivants :

- Pour  $\Delta \leq M$ , l'évolution est périodique de période  $M/\Delta$ . Si  $\Delta > M$ , seule une portion de la période est présente.
- $\Delta = 32$  et  $\Delta = 64$  donnent des résidus n'excédant pas  $M/2$  dans tous les cas, et donc de bonnes performances pour ces deux valeurs.
- Pour  $\Delta = 128$ , si le récepteur choisit le candidat voisin le plus proche (ce qui est normalement le cas dans de bonnes conditions SNR et de synchronisation  $CFO_{frac}$  et  $STO_{frac}$ ), le résidu n'excède pas  $M/2$ . En revanche, s'il choisit l'autre candidat voisin, le résidu dépassera  $M/2$  (en valeur absolue) pour presque toutes les valeurs de  $STO_{int}$ .
- $\Delta = 200$  donnera des performances encore moins bonnes que  $\Delta = 128$ , puisque le résidu minimal dépasse  $M/2$  pour  $STO_{int} \leq 5$  et  $STO_{int} \geq 66$ , soit pour la moitié des valeurs de  $STO_{int}$ .

Nous pouvons conclure que choisir  $\Delta = 32$  semble le choix optimal pour  $SF = 7$ , puisqu'il n'y a que  $B(32) = 9$  candidats et donne un risque minimal de dépassement de résidu à  $M/2$ . Choisir  $\Delta = 64$  est éventuellement envisageable pour réduire encore la complexité calculatoire (passage de 9 à 5 candidats). Cela correspond donc à choisir  $\Delta \leq M/2$  pour toute valeur de SF. Il ne faut en tout cas surtout pas choisir  $\Delta \geq M$ , donnant au mieux trois candidats ( $\mathcal{B}_\Delta = \{0, M, 2M\}$ ), une valeur insuffisante.

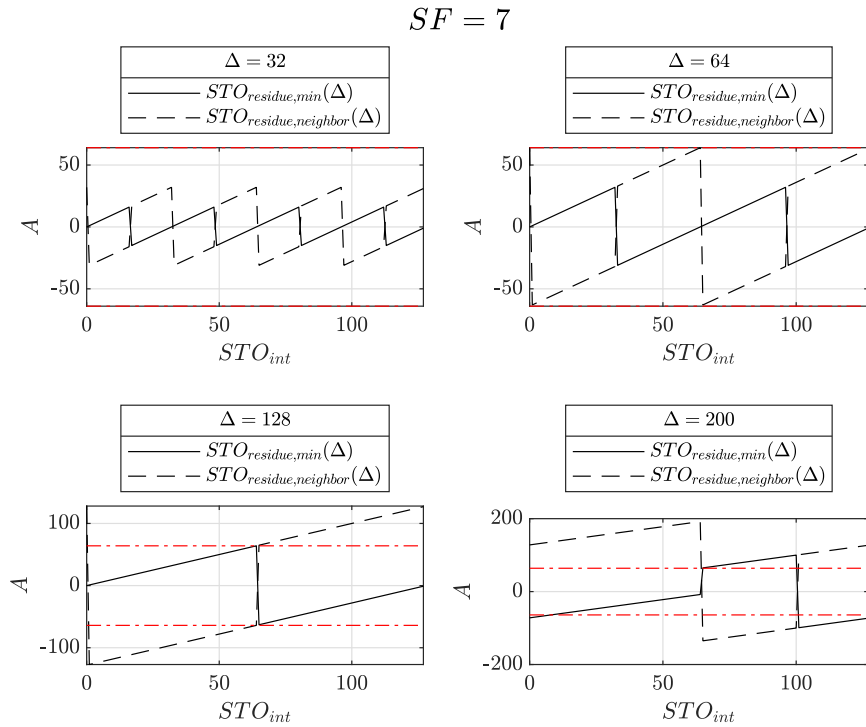


FIGURE III.4.22. – Évolution du premier et du second résidu minimal de réaligement de borne temporelle de trame en fonction de  $STO_{int}$  et  $\Delta$ ,  $SF = 7$

### III.4.3.3. Performances en simulation

Dans cette section, nous présentons les performances de détection de préambule selon les probabilités de :

- non-détection  $P_{nd}$  : avoir  $\widehat{id}x_{start} = \emptyset$  dans l'équation (III.4.2)

### III.4. Schéma d'auto-brouillage LoRa partie 2 : traitements au niveau du récepteur et performances

- bonne détection  $P_{gd}$  : avoir  $\widehat{id}x_{start} \in \{idx_{start}, idx_{start} + 1\}$  et  $|STO_{residue}(\Delta)| \leq M/2$ , permettant d'assurer une bonne synchronisation  $STO_{int}$  par la suite.

La Figure III.4.23 montre l'évolution des deux probabilités en fonction de  $\Delta$  avec  $\Delta \in \{1, 32, 64, 128, 200\}$ ,  $U = 10$ ,  $f = 1/U$ ,  $\lambda_{preamble} = 7.82$  (voir Tableau III.4.1) et  $SF = 7$ . Nous voyons que  $P_{nd}$  donne des performances quasiment identiques entre les valeurs de  $\Delta$ , avec une convergence atteinte à partir de  $SNR_{dB} = -8$  (plus aucun cas de non-détection). En revanche,  $P_{gd}$  montre une grande variabilité en fonction de  $\Delta$ , et de façon cohérente avec les comportements obtenus en Figure III.4.22. Ainsi,  $\Delta = 1$ ,  $\Delta = 32$  et  $\Delta = 64$  ont des performances très proches, pour un gain de complexité calculatoire allant jusqu'à un facteur 51 environ ( $\Delta = 64$ ).  $\Delta = 128$  montre une dégradation par rapport au trois premières valeurs de  $\Delta$  clairement visible pour  $SNR_{dB} > -12$ . La perte est encore plus importante pour  $\Delta = 200$ . L'écart entre  $\Delta = 128$  et  $\Delta = 200$  est beaucoup plus marqué qu'entre  $\Delta = 64$  et  $\Delta = 128$ , suggérant que le candidat  $\beta$  retenu est statistiquement celui le plus proche de  $\beta_p$ , impactant donc fortement les performances pour  $\Delta$  élevé (voir la différence entre  $\Delta = 128$  et  $\Delta = 200$  dans la Figure III.4.22).

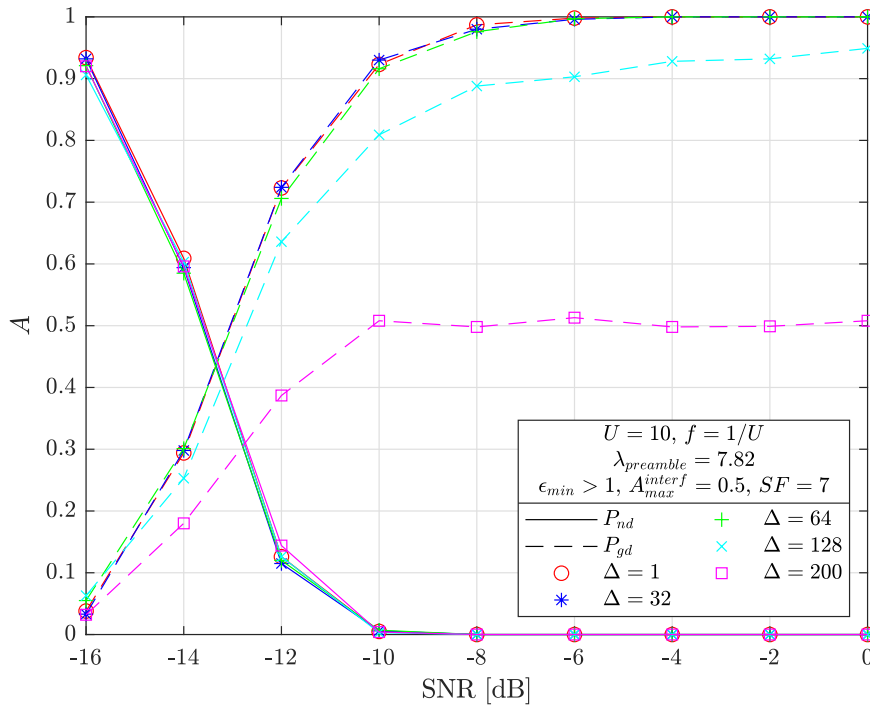


FIGURE III.4.23. – Probabilités de non et bonne détection de préambule en fonction de  $\Delta$ ,  $SF = 7$

La Figure III.4.24 montre toujours l'évolution des deux probabilités, mais en fonction de  $U \in \{1, 5, 10, 15, 20\}$ , et pour  $\Delta$  fixé à  $\Delta = 32$ . Nous constatons que plus  $U$  augmente, plus les performances se dégradent. Avec auto-brouillage ( $U > 1$ ), nous avons par exemple à  $SNR_{dB} = -12$   $P_{gd} \approx 0.28$  pour  $U = 20$  contre  $P_{gd} \approx 0.87$  pour  $U = 5$ . Cependant, nous observons quand même le gain de traitement apporté par  $U$ . En effet, dans le domaine fréquentiel LoRa, sans exploiter la connaissance du canal virtuel, le SNR équivalent sur la DFT est inférieur d'environ  $10 \log_{10}(U)$  dB. Pour  $U = 20$ , nous aurions alors une perte d'environ 13 dB. Ce n'est pas le cas ici, avec une perte contenue à environ 6 dB. Le récepteur légitime atteint la convergence pour toutes les valeurs de  $U$  à partir de  $SNR_{dB} = -8$  et  $SNR_{dB} = -4$  pour la probabilité de non et bonne détection, respectivement.

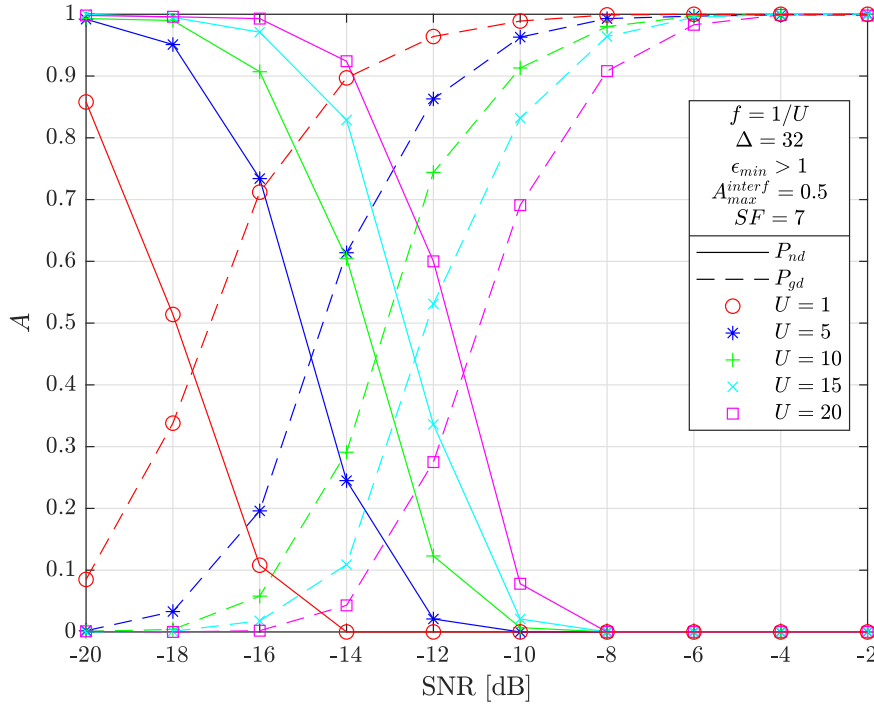


FIGURE III.4.24. – Probabilités de non et bonne détection du préambule en fonction de  $U$ ,  $SF = 7$

### III.4.4. Capacités de démodulation aveugle de EVE

Nous avons étudié jusqu'à présent les performances de détection de trame, de synchronisation et de démodulation du payload, mais uniquement du point de vue du récepteur légitime BOB. Rappelons que BOB exploite l'information des canaux virtuels à chaque étape de la démodulation (détection de trame, synchronisation et démodulation du payload) pour obtenir un gain de traitement, ce qui n'est pas le cas pour EVE. La Figure III.4.25 montre les différentes étapes de la démodulation en les classant en trois catégories, du point de vue de EVE :

- Les étapes que EVE peut réaliser sans connaissance préalable des canaux virtuels. Elle aura alors les mêmes performances que BOB (couleur verte sur la figure).
- Les étapes que EVE peut aussi réaliser sans connaissance des canaux virtuels, mais avec des performances dégradées par rapport à BOB (couleur orange).
- Les étapes qui, sans la connaissance des canaux virtuels, rend la bonne exécution difficile voire impossible pour EVE.

D'après la figure, nous voyons que la seule étape que EVE peut réaliser parfaitement en aveugle est l'estimation de  $CFO_{frac}$ . En effet, l'estimateur n'exploite à aucun moment les canaux virtuels (voir Annexe A) et donne d'assez bonnes performances en présence d'auto-brouillage (voir Section III.4.9).

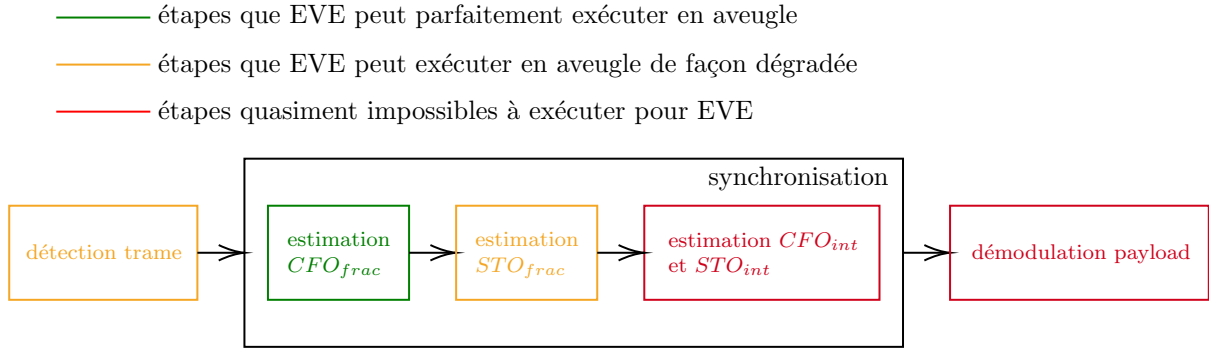


FIGURE III.4.25. – Étapes de la démodulation que EVE peut réaliser parfaitement en aveugle, en aveugle de façon dégradée, et de façon quasiment impossible

La détection de trame et l'estimation de  $STO_{frac}$  peuvent être toutes les deux réalisées de façon dégradée. Ces deux étapes sont donc critiques et les performances doivent être analysées afin d'évaluer les possibilités de démodulation de EVE. L'estimation de  $CFO_{int}$  et  $STO_{int}$  et la démodulation du payload sont en revanche quasiment impossibles.

Nous analysons en Section III.4.4.1 quelles sont les performances de détection aveugle de trame de EVE, et d'estimation de  $STO_{frac}$  en Section III.4.4.2, en les comparant à celles de BOB. Nous supposons ensuite en Section III.4.4.3 que EVE a parfaitement réussi ces deux étapes critiques. Nous évaluons alors quelles sont les chances pour EVE d'estimer en aveugle les canaux virtuels et de se retrouver ainsi dans les mêmes conditions de démodulation que BOB.

### III.4.4.1. Capacité de détection aveugle de trame

Nous comparons ici les performances de détection de trame entre BOB et EVE. Cette dernière peut utiliser le schéma présenté en Section III.4.3 de la même manière que BOB, mais à une différence majeure : elle ne connaît pas le canal virtuel. Ainsi, utiliser la démodulation cc1 revient pour elle à avoir  $\mathbf{m} = 0$ , et donc réaliser une démodulation classique non-cohérente (voir équations (I.2.13) et (III.3.14)). Elle ne profite pas du gain de traitement offert par  $U$  et verra donc ses performances fortement impactées.

Les Figures III.4.26 et III.4.27 montrent les performances en termes de probabilités de non et mauvaise détection,  $P_{nd}$  et  $P_{wd} = 1 - P_{gd}$ , respectivement. Nous considérons les paramètres  $\Delta = 32$ ,  $f = 1/U$ ,  $SF = 7$ , et nous choisissons  $\lambda_{preamble}$  pour chaque valeur de  $U$ , d'après le Tableau III.4.1.

La Figure III.4.26 compare  $P_{nd}$  pour  $U \in \{5, 10, 15, 20\}$ . Nous voyons sur la figure que les performances de BOB sont les mêmes qu'en Figure III.4.24 et sont meilleures que EVE. En effet, nous avons par exemple pour  $U = 20$  et  $SNR_{dB} = -8$ ,  $P_{nd} \approx 0.81$  pour EVE, là où BOB atteint une probabilité pratiquement nulle et dans le régime de convergence. Nous constatons que BOB possède une certaine avance sur EVE. Par exemple, pour  $U = 20$ , ce dernier conserve quand même de meilleures performances que EVE à  $U = 5$ .

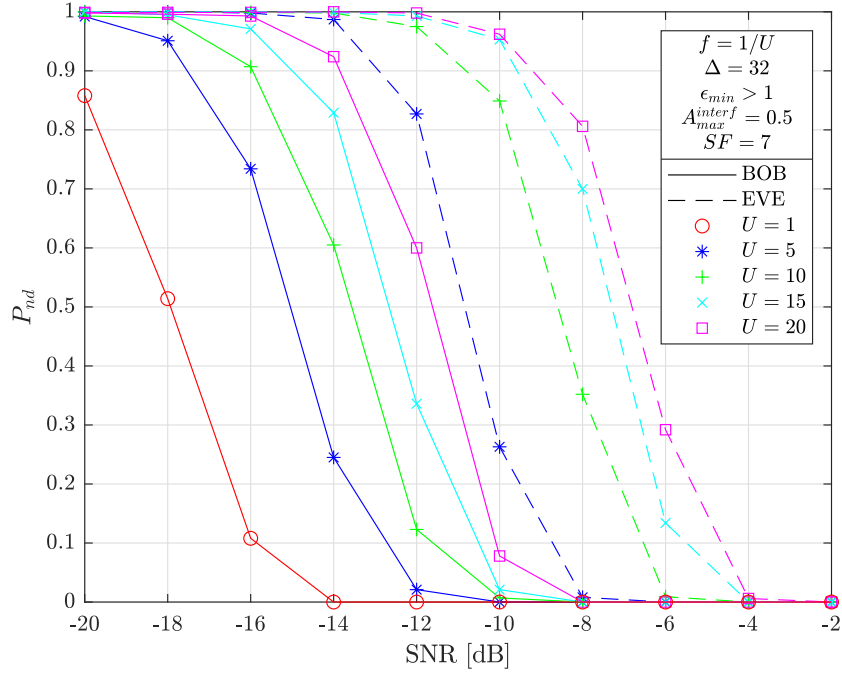


FIGURE III.4.26. – Comparaison des performances de non-détection de préambule entre BOB et EVE,  $SF = 7$

La Figure III.4.27 compare  $P_{wd}$  pour les mêmes paramètres qu'en Figure III.4.26. Les performances de BOB suivent un comportement similaire. Cependant, EVE suit une convergence beaucoup plus lente. En effet, pour  $U = 15$  et  $SNR_{dB} = -4$ , la convergence n'est pas atteinte, avec  $P_{wd} \approx 0.02$ . L'effet est encore plus marqué pour  $U = 20$ , avec  $P_{wd} \approx 0.1$ . Cela vient du fait que plus  $U$  est élevé, plus la statistique de  $\hat{\beta}_p$  est déformée pour EVE (voir Figure III.4.28).

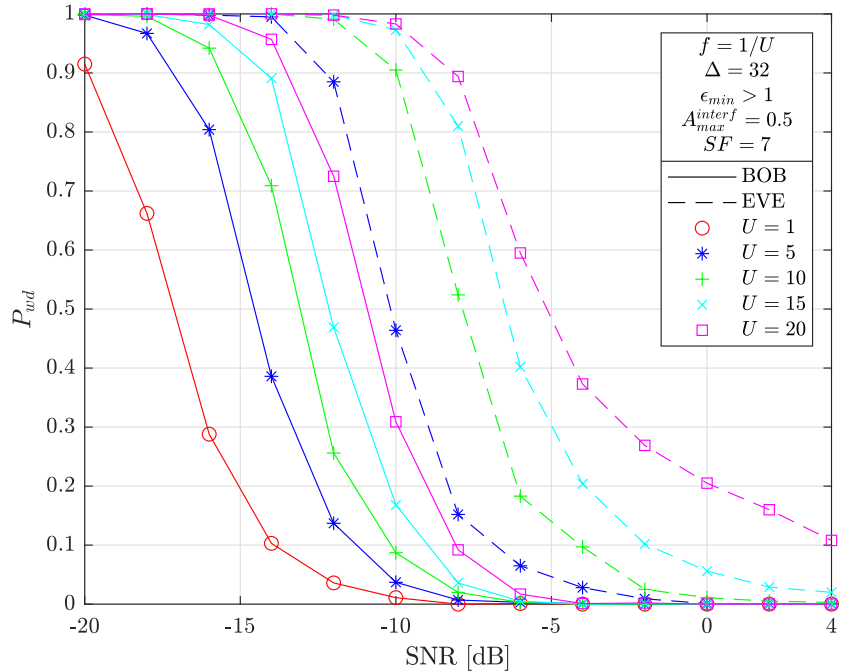


FIGURE III.4.27. – Comparaison des performances de mauvaise détection de préambule entre BOB et EVE,  $SF = 7$

La Figure III.4.28 compare  $A_{p,\beta,max}$  entre BOB (gauche) et EVE (droite) pour  $U = 20$ ,  $f = 1$ ,  $\Delta = 1$ ,  $SNR_{dB} = 0$  et  $SF = 7$ . Nous reportons dans la légende les valeurs de  $STO_{int}$ ,  $\widehat{idx}_{start}$  et  $\widehat{id\hat{x}}_{start}$ , ainsi que les résidus d'estimation  $CFO_{frac}$  et  $STO_{frac}$ , notés  $CFO_{frac}^{residue}$  et  $STO_{frac}^{residue}$ , respectivement. Nous voyons sur la figure que BOB a  $A_{p,\beta,max}$  peu déformé, avec un bon alignement ( $STO_{residue}(\Delta) = 4$ , du fait que  $126 - 122 = 4$ ), mais EVE donne  $A_{p,\beta,max}$  très déformé, engendrant une erreur d'alignement avec  $STO_{residue}(\Delta) = 83$ , du fait que  $204 - 121 = 83$ . Cela ne vient pas des résidus de désynchronisation (nul pour  $STO_{frac}$  et négligeable pour  $CFO_{frac}$ ) ou de la correction du PAPR puisqu'il n'y en a pas ici. En pratique, EVE ne fait pas beaucoup plus d'erreurs que BOB sur l'estimation du début de trame i.e.  $\widehat{id\hat{x}}_{start} \in \{idx_{start}, idx_{start} + 1\}$ , mais en fait majoritairement sur l'alignement initial ( $STO_{residue}(\Delta) > M/2$ ), faisant considérablement augmenter  $P_{wd}$ , comme observé en Figure III.4.27.

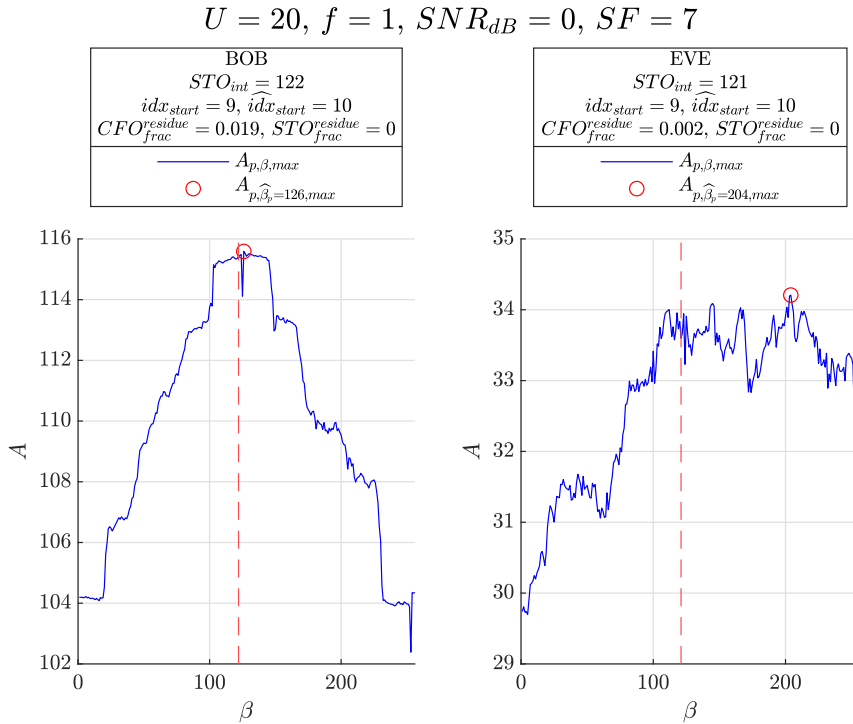


FIGURE III.4.28. – Comparaison du critère  $A_{p,\beta,max}$  entre BOB et EVE,  $SF = 7$

### III.4.4.2. Capacité d'estimation aveugle de $STO_{frac}$

Nous nous intéressons ici à évaluer quelles sont les capacités pour EVE d'estimer en aveugle  $STO_{frac}$ . En pratique, nous avons  $\widehat{id\hat{x}}_{start} \in \{idx_{start}, idx_{start} + 1\}$  lorsqu'il y a détection de trame (voir Figure III.4.18). La forte fluctuation de  $\widehat{id\hat{x}}_{start}$  lorsque  $STO_{int}$  est proche de  $M/2$  impacte de façon négligeable l'estimateur (et également celui de  $CFO_{frac}$ ). EVE peut estimer en aveugle  $STO_{frac}$  en ré-utilisant l'estimateur par candidats proposé (voir Section III.4.1.3) sans avoir la connaissance du canal virtuel.

Des simulations exécutées montrent que pour  $U \leq 30$ , EVE et BOB ont des performances d'estimation  $STO_{frac}$  très proches, avec ou sans correction du PAPR. Cependant, pour  $U > 30$  et avec la correction du PAPR active, les performances de EVE se dégradent progressivement par rapport à BOB, pour devenir inconsistantes, mêmes pour des régimes

SNR élevés. C'est ce que montre la Figure III.4.29, où les performances de BOB ( $\mathbf{m}_{up}$  parfaitement connu) et EVE ( $\mathbf{m}_{up} = 0$ ) sont comparées, pour  $U = 40$ ,  $f \in \{1, 2/U, 1/U\}$ ,  $SNR_{dB} \in \{-4, -2, \dots, 16\}$  et  $SF = 7$ . Nous supposons que BOB et EVE ont parfaitement détecté la trame (i.e.  $STO_{residue}(\Delta) = 0$ ), et que la synchronisation  $CFO_{frac}$  se déroule correctement, avec la présence d'un résidu de désynchronisation  $CFO_{frac}$  valant  $CFO_{frac}^{residue} = 0.01$ . Nous ignorons ici les désynchronisations  $CFO_{int}$  et  $STO_{int}$  i.e.  $CFO_{int} = STO_{int} = 0$ . Dans la simulation, BOB et EVE estiment et corrigent d'abord  $STO_{frac}$ , puis démodulent le payload avec `cc1`, afin d'observer le comportement de l'estimateur. Un résidu  $STO_{frac}$  élevé impactera immédiatement les performances SER (voir Figure I.2.21)).

D'après la Figure III.4.29, nous voyons que pour BOB, l'activation de la correction du PAPR engendre une perte d'un peu plus de 2 dB, sans grande différence entre  $f = 2/U$  et  $f = 1/U$ . Sans correction du PAPR, EVE a une perte assez faible par rapport à BOB, de l'ordre de 1 dB. Cependant, lorsque la correction est active, les performances ne convergent plus vers le comportement désiré d'un SER nul. Nous avons en effet un plateau  $SER > 10^{-2}$ , à la valeur de SNR pourtant très élevée  $SNR_{dB} = 16$ . Ainsi, bien que la correction du PAPR soit perçue négativement du point de vue des performances SER pour le récepteur légitime, cette dernière peut-être utile pour empêcher EVE de correctement démoduler.

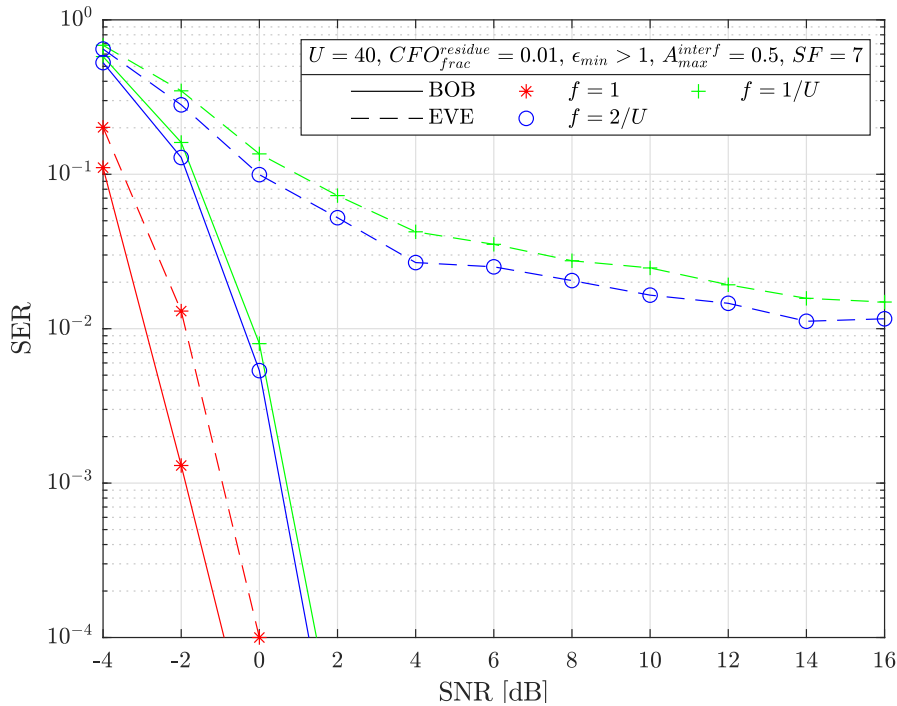


FIGURE III.4.29. – Comparaison des performances d'estimation  $STO_{frac}$  entre BOB et EVE,  $SF = 7$

### III.4.4.3. Capacité de reconstruction aveugle des canaux virtuels

Nous évaluons ici quelles sont les capacités de reconstruction aveugle des canaux virtuels par EVE. Ainsi, cette dernière se retrouverait dans les mêmes conditions de démodulation du payload que BOB, et pourrait éventuellement retrouver  $\hat{a}_i = (a_i + l_i)$



### III.4. Schéma d'auto-brouillage LoRa partie 2 : traitements au niveau du récepteur et performances

mod  $M$  (équation (III.3.12)). Cela favoriserait donc les capacités de méthodes de compromission cryptographique, comme discuté en Section III.3.3.2. EVE peut adopter pour cela la stratégie de lire sur la DFT démodulée les bins les plus significatifs, et supposer que le symbole de payload en fait partie. Pour cela, elle peut utiliser un seuil pour extraire les bins, comme illustré en Figure III.4.30, pour  $U = 30$ ,  $f = 1/U$ ,  $a_i = 0$ ,  $\lambda_{payload} = 0.4$ , sans bruit AWGN et  $SF = 7$ .

Nous notons  $\mathcal{A}_{payload}$ , l'ensemble des bins retenus :

$$\mathcal{A}_{payload} = \text{find}_n \left| \tilde{R}_i[n] \right| > (\lambda_{payload} \times R_{i,max}), \quad \lambda_{payload} \in ]0; 1[ \quad (\text{III.4.27})$$

avec  $\text{find}(\cdot)$ , la fonction retournant les indices des valeurs satisfaisant une condition,  $\lambda_{payload}$ , la valeur du seuil,  $i$ , l'indice de symbole payload et :

$$R_{i,max} = \max_n \left| \tilde{R}_i[n] \right| \quad (\text{III.4.28})$$

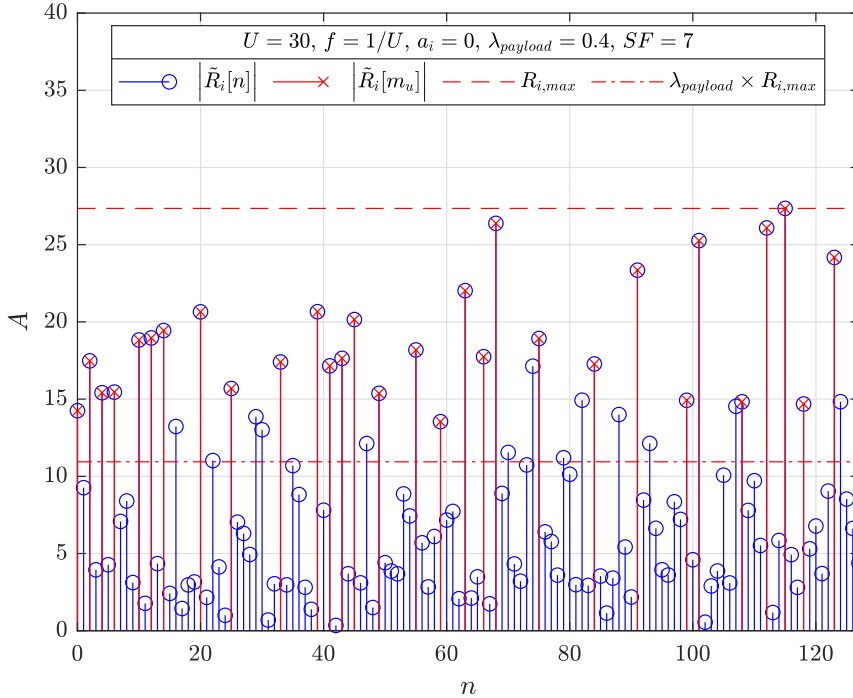


FIGURE III.4.30. – Exemple d'extraction de bins dans la DFT LoRa pour la reconstruction du canal virtuel par EVE,  $SF = 7$

Nous notons aussi  $n_{l,payload}$ , le  $l^{\text{ème}}$  élément dans  $\mathcal{A}_{payload}$ , et  $L_{payload}$ , le nombre de bins retenus ( $L_{payload} = |\mathcal{A}_{payload}|$ ). EVE doit choisir correctement  $\lambda_{payload}$ , de façon à garantir  $a_i \in \mathcal{A}_{payload}$ . Il ne doit pas être trop élevé, sinon nous aurons  $a_i \notin \mathcal{A}_{payload}$ , mais pas trop faible non plus, de façon à limiter le nombre de bins parasites sélectionnés (et donc  $L_{payload}$ ), dus à la correction du PAPR et au bruit AWGN (voir sur la figure), et ainsi ne pas alourdir la complexité calculatoire.

Nous avons  $L$  canaux virtuels candidats. Le  $l^{\text{ème}}$  canal virtuel candidat, noté  $\mathbf{m}_{cand,l}$ , est reconstruit en appliquant un décalage circulaire gauche de  $n_{l,payload}$  bins sur le premier

canal virtuel candidat :

$$\mathbf{m}_{cand,l} = \text{sort}((\mathbf{m}_{cand,0} - n_{l+1,payload}) \bmod M), \quad l \in \{1, 2, \dots, L_{payload} - 1\} \quad (\text{III.4.29})$$

avec  $\text{sort}(\cdot)$ , la fonction de tri croissant. Par exemple, si nous avons  $\mathcal{A}_{payload} = \{0, 4, 18, 74\}$  pour  $U = 4$  et  $SF = 7$ , les canaux virtuels candidats seront  $\mathbf{m}_{cand,0} = [0 \ 4 \ 18 \ 74]$ ,  $\mathbf{m}_{cand,1} = [0 \ 14 \ 70 \ 124]$ ,  $\mathbf{m}_{cand,2} = [0 \ 56 \ 110 \ 114]$  et  $\mathbf{m}_{cand,3} = [0 \ 54 \ 58 \ 72]$ . Si le SNR est très favorable ( $SNR_{dB} \geq 10$ ) et  $a_i \in \mathcal{A}_{payload}$ , la bonne démodulation peut-être garantie (après reconstruction de chaque canal virtuel candidat et démodulation), même si  $\mathbf{m}_{cand,l} \neq \mathbf{m}$ .

Dans ce cas, la démodulation aura plus de pics parasites. Nous définissons  $P_{recon,correct}$ , la probabilité qu'un canal virtuel candidat donne une bonne démodulation :

$$P_{recon,correct} = \frac{1}{L_{payload}} \quad (\text{III.4.30})$$

Intuitivement, lorsque  $\lambda_{payload}$  est correctement choisi i.e.  $a_i \in \mathcal{A}_{payload}$ , nous avons  $L_{payload} = U$ . La probabilité qu'un canal virtuel candidat donne une bonne démodulation est alors maximale, avec :

$$P_{recon,correct,max} = \frac{1}{U} \quad (\text{III.4.31})$$

La Figure III.4.31 montre l'évolution de  $P_{recon,correct}$  en fonction de  $\lambda_{payload}$ , pour  $U \in \{5, 10, 15, 20, 30, 40\}$ ,  $f \in \{2/U, 1/U\}$  et  $SF = 7$ . Nous supposons un régime SNR très favorable, avec  $SNR_{dB} = 20$ . Dans la simulation, pour un tirage donné, si  $a_i \notin \mathcal{A}_{payload}$ , nous décidons  $P_{recon,correct} = 0$ . Nous affichons  $P_{recon,correct}$  moyenné sur les tirages.

Nous voyons sur la figure que si EVE choisit  $\lambda_{payload} > 0.8$ , la convergence est garantie ( $P_{recon,correct} = P_{recon,correct,max}$ ) pour  $U \leq 30$ , mais pas au delà. Cela vient du fait que l'amplitude moyenne des déformations de correction du PAPR devient non négligeable par rapport à ceux d'intérêt. Nous aurons alors toujours au moins un bin supplémentaire sélectionné i.e.  $L > U$ . Plus la correction du PAPR est forte, plus  $L_{payload}$  sera élevé statistiquement pour un seuil donné, et donc  $P_{recon,correct}$  faible. Pour  $\lambda_{payload} = 0.3$  et  $U = 30$  par exemple, nous avons  $P_{recon,correct} \approx 3 \times 10^{-2}$  pour  $f = 2/U$  contre  $P_{recon,correct} \approx 1.9 \times 10^{-2}$  pour  $f = 1/U$ .

En supposant la convergence atteinte i.e.  $P_{recon,correct} = 1/U$  et une actualisation du canal virtuel de payload tous les  $\Delta_{payload}$  symboles, EVE peut correctement démoduler  $a_i$  avec la probabilité :

$$P_{demod}(U, \Delta_{payload}, N_{payload}) = \left(\frac{1}{U}\right)^2 \times \left(\frac{1}{U}\right)^{N_{payload}/\Delta_{payload}} \quad (\text{III.4.32})$$

avec le premier terme représentant la probabilité de correctement estimer en aveugle les canaux virtuels  $\mathbf{m}_{up}$  et  $\mathbf{m}_{down}$  (et donc de se synchroniser) et le second, celle de reconstruction des canaux virtuels du payload.

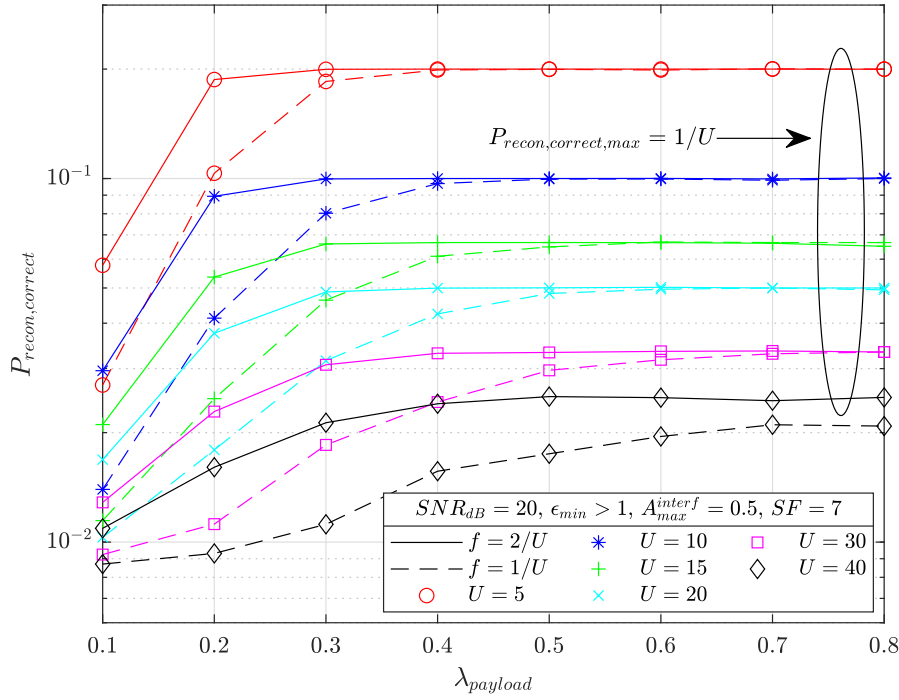


FIGURE III.4.31. – Évolution de la probabilité de reconstruction de canal virtuel conduisant à une démodulation correcte pour EVE, en fonction du seuil et du facteur de correction du PAPR,  $SF = 7$

La Figure III.4.32 montre l'évolution de la valeur maximale  $\Delta_{payload}$  possible, notée  $\Delta_{payload,max}$ , en fonction de  $U$  pour une probabilité  $P_{demod}$  désirée notée  $P_{target}$ , avec  $P_{target} \in \{10^{-30}, 10^{-25}, 10^{-20}, 10^{-18}, 10^{-16}\}$ . Nous sélectionnons pour cela la valeur de  $\Delta_{payload}$  donnant  $P_{demod}(U, \Delta_{payload}, N_{payload})$  dans l'équation (III.4.32) la plus proche de  $P_{target}$ .

D'après la Figure III.4.32, pour  $P_{target}$  fixée, plus  $\Delta_{payload,max}$  est élevé, plus  $U$  devra être élevé. Plus la contrainte  $P_{target}$  est faible, plus  $\Delta_{payload,max}$  pourra être élevé pour  $U$  fixé. A l'inverse, pour une contrainte  $P_{target}$  élevée,  $\Delta_{payload,max}$  devra diminuer pour  $U$  fixé. Nous considérons qu'avoir  $P_{target} = 10^{-16}$  est raisonnablement faible. Cela donne une possibilité d'actualisation jusqu'à  $\Delta_{payload,max} = 12$  symboles pour  $U \geq 34$ . Notons qu'en pratique, le nombre de symboles payload est généralement supérieur à  $N_{payload} = 100$  [60], donnant une probabilité  $P_{demod}(U, \Delta_{payload}, N_{payload})$  pour EVE encore plus faible.

Pour conclure sur les performances de EVE par rapport à celles du récepteur légitime, pour garantir une probabilité de démodulation aveugle minimale pour EVE, deux choix sur le schéma d'auto-brouillage sont possibles : augmenter  $U$  ou diminuer  $\Delta_{payload}$ . Chacune des deux approches ont leurs avantages et inconvénients et sont reportés dans les Tableaux III.4.2 et III.4.3.

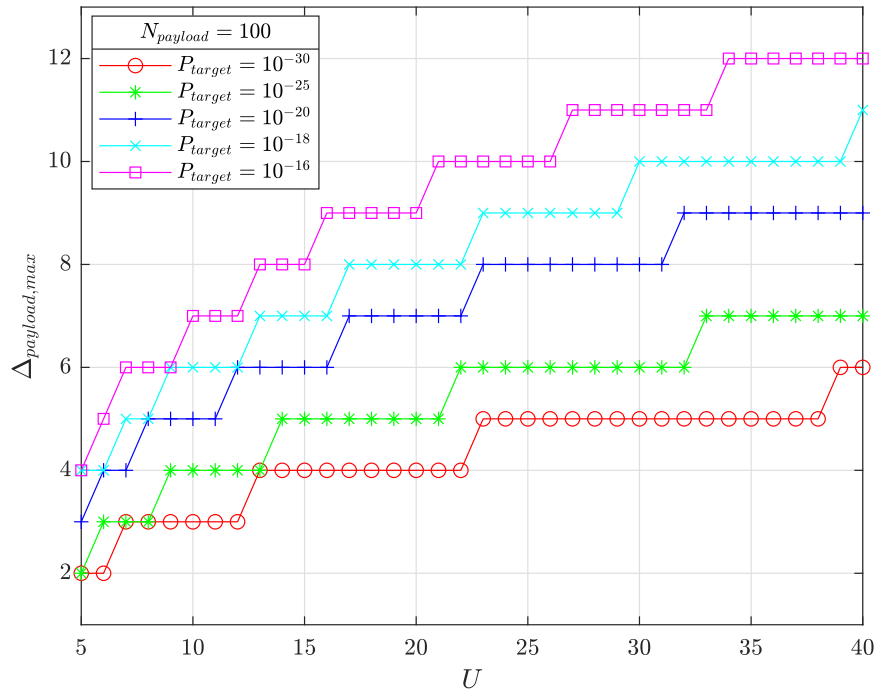


FIGURE III.4.32. – Fréquence maximale d’actualisation des canaux virtuels de payload en fonction de  $U$  pour plusieurs probabilités de démodulation correcte du payload

Avantages	Inconvénients
Diminue les capacités de démodulation aveugle de EVE.	Dégrade les performances du récepteur légitime.
Diminue les capacités de détection de trame de EVE.	

TABLE III.4.2. – Avantages et inconvénients d’augmenter  $U$

Avantages	Inconvénients
Diminue les capacités de démodulation aveugle de EVE.	Contrainte d’actualisation dans le temps du canal virtuel de payload plus forte.
Préserve les performances de démodulation du récepteur légitime (pour $U$ fixé).	

TABLE III.4.3. – Avantages et inconvénients de diminuer  $\Delta_{payload}$



## III.5. Schéma d’auto-brouillage LoRa partie 3 : implémentation sur SDR

Dans cette section, nous présentons la validation du schéma d’auto-brouillage sur équipements réels de type Software Defined Radio (SDR). Ces travaux se sont inscrits dans le cadre d’une mobilité à l’étranger réalisée à l’ATM de Bucarest en Roumanie, lors de la seconde année de thèse. Cette partie est présentée comme suit. Premièrement, nous présentons en Section III.5.1 le banc de test utilisé. Puis, en Section III.5.2, nous mettons en évidence l’apport crucial de la correction du PAPR pour des transmissions réelles avec des équipements SDR. Ensuite, nous menons en Section III.5.3 plusieurs comparaisons entre le comportement des signaux SDR et analytiques, afin de confirmer le bon comportement des signaux réels. Nous montrons en Section III.5.4 des exemples de démodulation complète sur SDR, pour plusieurs valeurs de  $U$ . Enfin, deux études sur l’enveloppe complexe temporelle et le spectre sont menées en Section III.5.5.

### III.5.1. Présentation du banc de test

Les SDR ont acquis beaucoup d’intérêt ces dernières années, que ce soit pour de nombreux amateurs que pour la communauté scientifique. Ils permettent de faire rapidement et à bas coût des études diverses sur les télécommunications : interception de signaux pour rétro-ingénierie, approche pédagogique, expérimentation de nouveaux schémas de transmission, grâce à des outils faciles d’accès évitant de longues et coûteuses phases de développement de code. Aujourd’hui, nous trouvons une grande variété de SDR, allant de modèles d’entrée de gamme pour amateurs comme le HackRF One, à environ 300 euros [187], à des modèles orientés pour la pédagogie comme le Adalm PlutoSDR d’Analog Devices [188], ou encore des modèles très complets et onéreux (plusieurs dizaines de milliers d’euros), principalement dédiés pour la recherche. Nous pouvons citer par exemple le X410 d’Ettus Research [189]. Les outils de développement sont également variés : programmation brute en langages C, C++ ou Python, environnements complets comme GnuRadio ou MATLAB, ou encore des utilitaires pour la visualisation des signaux acquis comme SDR#.

Pendant la thèse, nous avons utilisé des SDR B210 d’Ettus Research. Ils sont illustrés en Figure III.5.1. Ce sont des équipements moyenne gamme offrant plusieurs fonctionnalités : deux couples d’entrées et sorties permettant de réaliser des transmissions Multiple Input Multiple Output (MIMO), un module de réception de signaux Global Positioning System (GPS), et une synchronisation d’horloge externe pour synchroniser deux SDR entre eux.

### III.5. Schéma d'auto-brouillage LoRa partie 3 : implémentation sur SDR

Les principales caractéristiques techniques des SDR B210 sont reportées dans le Tableau III.5.1 et sont issues de la documentation d'Ettus Research [190].



FIGURE III.5.1. – SDR Ettus Research B210

Paramètre	Valeurs
Bandes de fonctionnement	[70; 6000] MHz
MIMO	2x2
Largeur de bande maximale	56 MHz (30.72 MHz en MIMO 2x2)
Fréquence maximale ADC/DAC	61.44 MS/s (échantillons par seconde)
Résolution ADC/DAC	12 bits
Précision fréquence	$\pm 2$ ppm
Puissance d'émission maximale	$> 10$ dBm
Plage de gains d'émission (MATLAB)	$G_{Tx} \in [0; 89.8]$
Plage de gains de réception (MATLAB)	$G_{Rx} \in [0; 60]$

TABLE III.5.1. – Caractéristiques techniques des SDR Ettus Research B210

Deux B210 ont été utilisés. L'un joue le rôle de l'émetteur, l'autre celui du récepteur. Nous utilisons aussi deux antennes omnidirectionnelles VERT900 [191]. Elles mesurent 40 cm de long et sont conçues pour les bandes de fréquence allant de 824 à 960 MHz (136 MHz de largeur de bande) et de 1710 à 1990 MHz (280 MHz de largeur de bande). Ainsi, elles sont parfaitement adaptées pour la transmission de signaux LoRa qui, rappelons le, exploitent les bandes ISM (868.1 MHz en Europe par exemple). Une illustration du positionnement des deux B210 est montrée en Figure III.5.2.

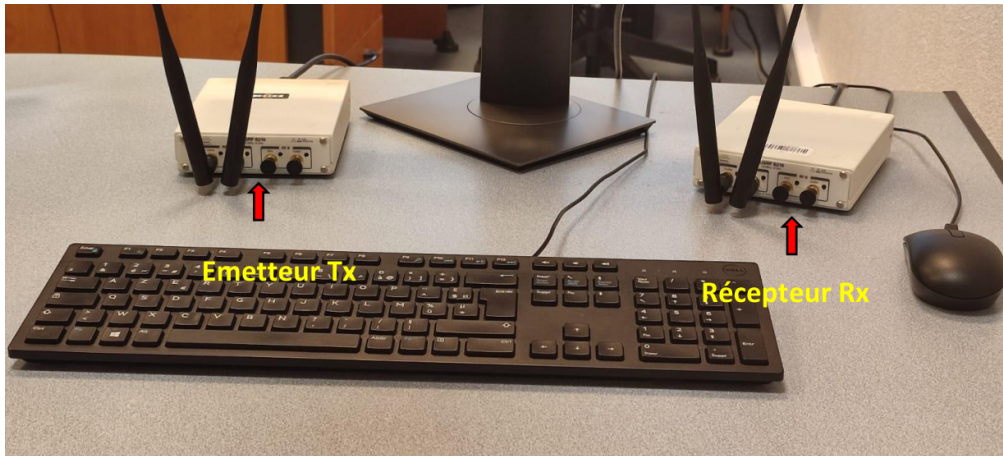


FIGURE III.5.2. – Banc de test de transmissions SDR

L'environnement de travail est celui de MATLAB avec la toolbox d'Ettus Research installée. Cela permet un gain de temps non négligeable puisque tous les scripts et fonctions MATLAB écrits au cours de la thèse peuvent être directement ré-utilisés. MATLAB ne propose cependant pas de possibilité de transmission en temps réel : le récepteur est en attente d'une réception, écoutant en permanence le canal. La fonctionnalité temps réel pourrait éventuellement faire l'objet de travaux futurs. Cela nécessiterait l'utilisation d'un autre environnement de développement le permettant (GnuRadio par exemple) et de devoir ré-écrire les codes.

Pour les transmissions, les deux B210 sont connectés à un PC exécutant trois instances de MATLAB. La première se charge de la transmission, la seconde de la réception, et la troisième effectue le post-traitement des signaux (synchronisation, démodulation, études diverses, etc.). Le front-end d'une transmission typique est présenté en Figure III.5.3, avec les trois instances notées A, B et C, et les B210 émetteur et récepteur, notés SDR Tx et SDR Rx, respectivement. Au niveau de l'émetteur, le traitement demande peu d'opérations : initialisation, préparation du signal à transmettre puis transmission, en soumettant simplement les échantillons complexes du signal en bande de base. Afin que le récepteur reçoive entièrement le signal, ce dernier doit déjà collecter des échantillons au moment où l'émetteur transmet. Ainsi, le récepteur doit être activé avant l'émetteur.

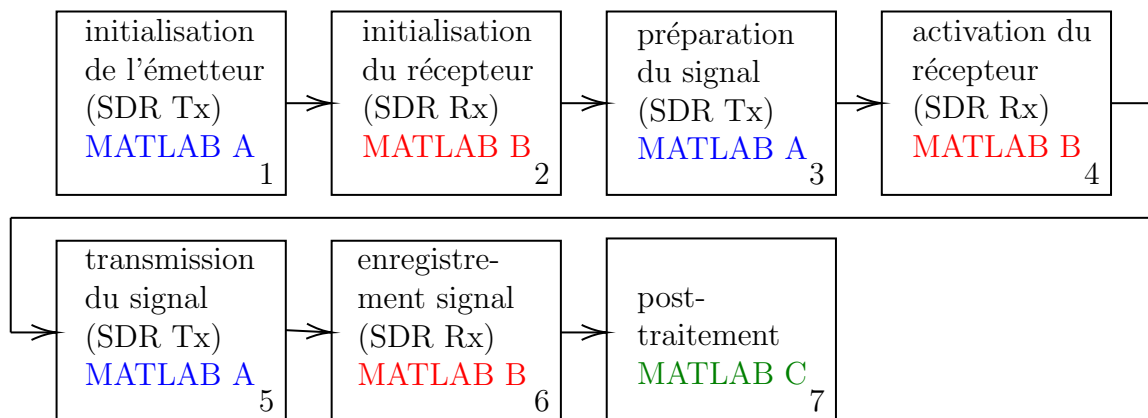


FIGURE III.5.3. – Front-end d'émission et réception SDR



### III.5. Schéma d'auto-brouillage LoRa partie 3 : implémentation sur SDR

Les paramètres SDR et d'auto-brouillage utilisés pour les transmissions sont reportés dans le Tableau III.5.2, si non indiqué autrement.

Paramètre SDR	Valeur
$F_c$	868.1 MHz
$G_{Tx}$ et $G_{Rx}$	40 dB et 0 dB ( $\widehat{SNR}_{dB} > 20$ )
Puissance estimée du bruit AWGN, $\hat{\sigma}^2$	$\approx 1.19 \times 10^{-8}$
Fréquence d'échantillonnage de l'ADC, $F_{ADC}$	5 MHz
Nombre de trames transmises, $N_{frame}$	5
Facteur de sur-échantillonnage (synchronisation), $R$	10
Paramètre d'auto-brouillage	Valeur
$SF$	7
$N_{up} = N_{down}$	8
$N_{payload}$	500
$\epsilon_{min}$	$> 1$
$A_{max}^{interf}$	0.5

TABLE III.5.2. – Paramètres SDR et d'auto-brouillage utilisés pour les transmissions SDR

## III.5.2. Mise en évidence de la nécessité de la correction du PAPR

Le schéma d'auto-brouillage peut avoir une utilisation réelle fortement limitée si la correction du PAPR n'est pas appliquée, du fait de la possible mise en régime non linéaire des composants matériel (saturation du DAC, voir Section III.3.4). Les transmissions SDR réalisées sans correction donnent un signal reçu très déformé, rendant toute démodulation quasiment impossible, et ce, même à très fort SNR. Ainsi, il est impératif de corriger le PAPR. Il est légitime de se poser la question de savoir quel est le niveau minimal de correction à appliquer permettant la réception d'un signal pas ou peu déformé par le matériel.

Pour mettre en évidence cette problématique, nous réalisons la transmission à  $SF = 7$  de quatre trames consécutives ( $N_{frame} = 4$ ) de 500 symboles, pour  $U = 4$ ,  $\mathbf{m} = [0 \ 20 \ 49 \ 67]$  et à très fort SNR ( $\widehat{SNR}_{dB} > 20$ ). La première trame a une correction du PAPR maximale i.e.  $f = 1/U$ . La correction est ensuite progressivement réduite : la deuxième trame a  $f = 0.5$ , la troisième  $f = 0.75$  et la dernière  $f = 1$ . Le signal reçu est détecté puis synchronisé sur la première trame, où le signal est parfaitement exploitable ( $f = 1/U$ ), et nous affichons la DFT LoRa (Figure III.5.4) et la ccm (Figure III.5.5) du 20<sup>ème</sup> symbole de payload ( $a = 45$ ) dans chaque trame.

La puissance de chaque symbole est normalisée par rapport à la puissance estimée. Par exemple, si  $P_r = P_s + \sigma^2 = 2$  avec  $P_s = \sigma^2 = 1$  ( $SNR_{dB} = 0$ ), nous aurons alors si  $\hat{P}_r = P_r$ ,  $P_{s,norm} = P_s/P_r = 0.5$  et  $\sigma_{norm}^2 = \sigma^2/P_r = 0.5$ . La relation  $P_{s,norm} + \sigma_{norm}^2 = 1$  est donc toujours satisfaite. Ainsi, plus le SNR est faible, plus les pics d'intérêt sur la DFT diminueront et se rapprocheront de ceux de bruit AWGN.

### III.5.2. Mise en évidence de la nécessité de la correction du PAPR

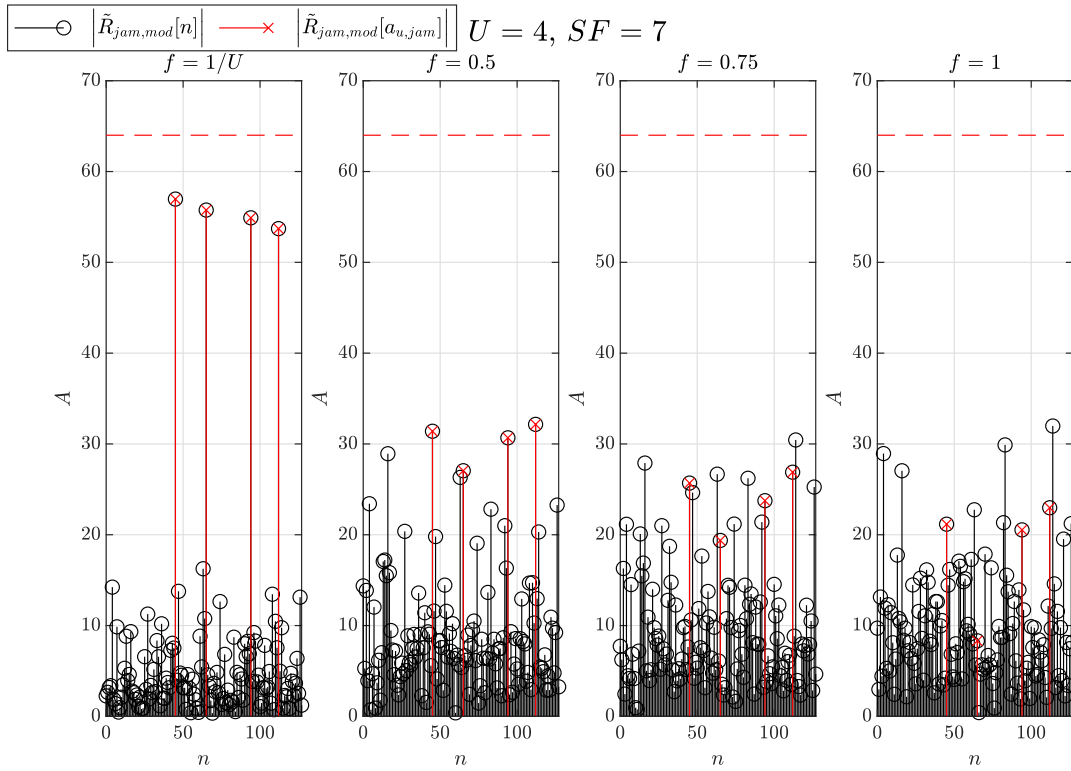


FIGURE III.5.4. – Impact du facteur de correction du PAPR sur la DFT LoRa SDR,  $SF = 7$

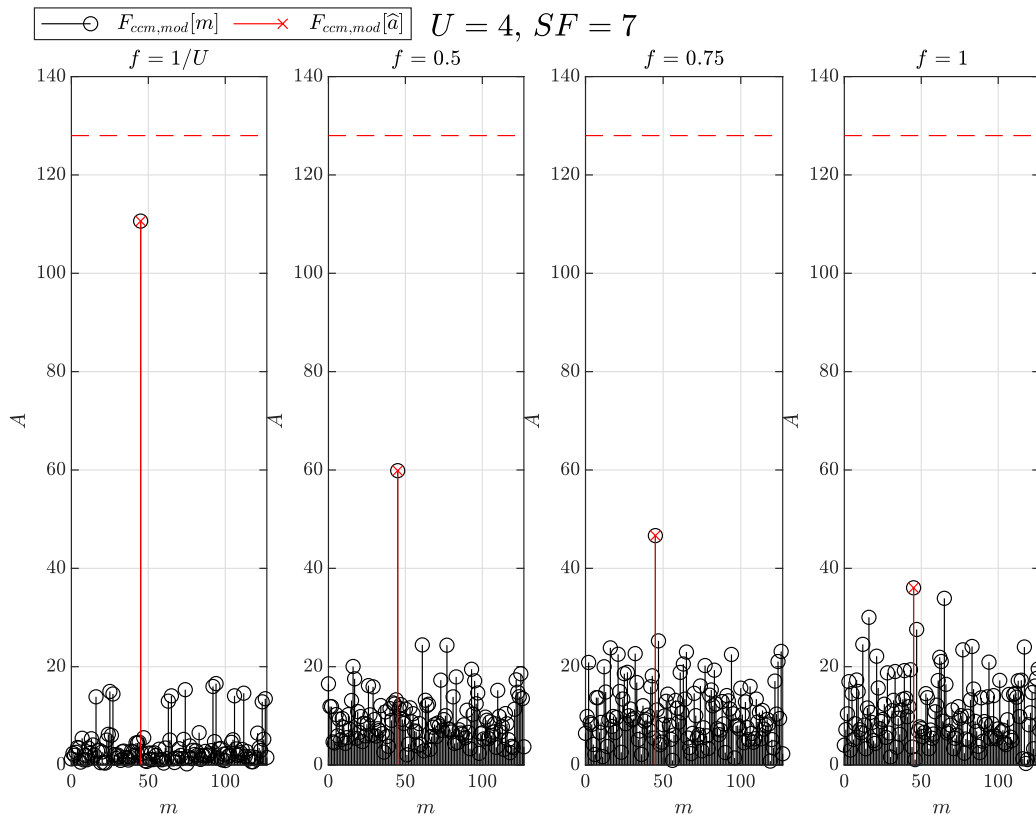


FIGURE III.5.5. – Impact du facteur de correction du PAPR sur la ccm SDR,  $SF = 7$

Les traits pointillés rouge indiquent l'amplitude théorique des bins obtenus en simulation sans bruit AWGN et sans correction du PAPR ( $M\sqrt{1/U} = 64$  pour la DFT LoRa et  $M = 128$  pour la ccm). D'après les deux figures, nous constatons très clairement que lorsque la trame est reçue avec correction maximale, les DFT LoRa et ccm résultantes ont l'allure attendue : quatre pics bien visibles sur la DFT LoRa et un pic sur la ccm concentrant toute l'énergie. Notons la perte d'énergie par rapport au cas idéal en simulation sans correction (amplitude ccm ici d'environ 110 contre  $M = 128$ ), de façon cohérente avec la Figure III.3.15. Nous remarquons bien la perte d'énergie due au manque de correction. La dégradation du signal devient rapidement importante. Pour  $f = 0.5$ , presque la moitié de l'énergie ccm est perdue (amplitude d'environ 60 contre environ 110). L'amplitude du pic d'intérêt se dégrade encore, pour être au niveau de ceux d'interférence d'inter-corrélation circulaire et de distorsion PAPR lorsque  $f = 1$ .

La Figure III.5.6 montre l'évolution de l'amplitude du bin démodulé  $F_{ccm,mod}[\hat{a}]$  au cours des quatre trames. La perte d'énergie est clairement visible avec des niveaux moyens d'amplitude présents : 112 pour  $f = 1/U$ , 45 pour  $f = 0.5$ , 40 pour  $f = 0.75$  et 35 pour  $f = 1$ . Notons que la variance est beaucoup plus importante pour  $f = 0.5$ . Ainsi, il est beaucoup plus judicieux pour l'émetteur d'appliquer une correction maximale du PAPR pour préserver de bonnes performances au niveau du récepteur. A partir de maintenant, nous utiliserons  $f = 1/U$  pour toutes les transmissions SDR.

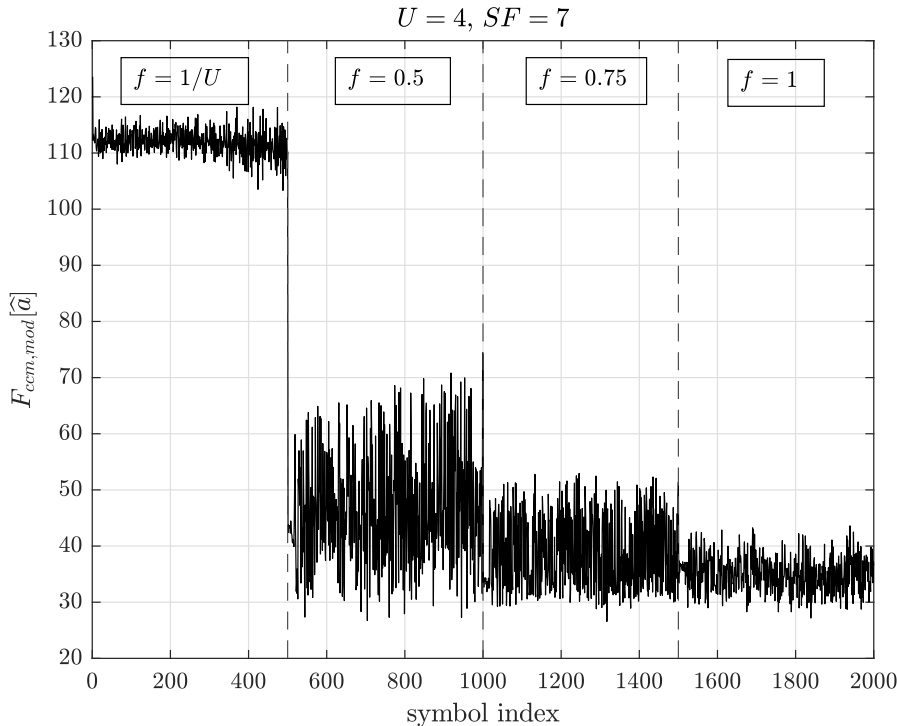


FIGURE III.5.6. – Impact au cours du temps du facteur de correction du PAPR sur la ccm SDR,  $SF = 7$

### III.5.3. Comparaisons des DFT LoRa entre les signaux SDR et analytique

La Figure III.5.7 montre la comparaison des DFT LoRa entre les signaux SDR synchronisés, et ceux analytiques obtenus en simulation, pour  $U \in \{2, 4, 8, 30\}$ ,  $f = 1/U$ , à très fort SNR ( $\widehat{SNR}_{dB} > 20$ ) et  $SF = 7$ . Afin d'avoir une comparaison équitable entre simulation et signaux réels, nous générons les signaux analytiques pour  $SNR_{dB} = 20$  et nous considérons des résidus de désynchronisation  $CFO_{frac}$  et  $STO_{frac}$  de 0.02 et 0.05, respectivement. D'après la figure, nous remarquons que les propriétés d'auto-brouillage sont très bien préservées avec les SDR. Par exemple, pour  $U = 2$ , le motif caractéristique présent aux bins  $n \in \{60, 68, 90, 98\}$  est conservé (entouré en noir sur la figure). Il vient des déformations dues à la correction du PAPR. L'écart est essentiellement dû aux résidus de désynchronisation des signaux SDR qui ne sont pas nuls.

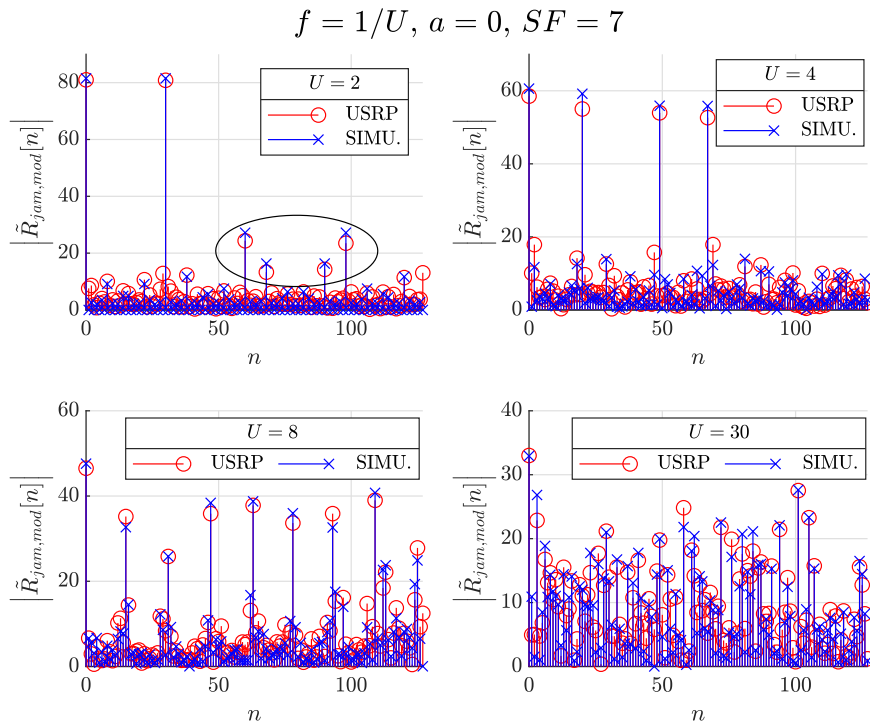


FIGURE III.5.7. – Comparaison des DFT LoRa entre les signaux SDR synchronisés et analytiques pour plusieurs valeurs de  $U$ ,  $SF = 7$

### III.5.4. Exemple de démodulation complète

Les Figures III.5.8 et III.5.9 montrent un exemple complet de réception d'un signal LoRa auto-brouillé. La détection de trame est réalisée avec le détecteur proposé en Section III.4.3 et est illustrée en Figure III.5.8, avec les sous-figures numérotées Figure III.5.8a, Figure III.5.8b, etc., dans l'ordre chronologique d'exécution du front-end. Le mécanisme de ré-alignement des bornes temporelles (présenté en Section III.4.3.1.3) et le résultat du front-end de synchronisation (présenté en Section III.4.1) sont montrés en Figure III.5.9a, tandis que la démodulation du payload est montrée en Figure III.5.9b. Nous avons les paramètres suivants :  $U = 5$ ,  $\mathbf{m}_{up} = \mathbf{m}_{down} = [0 \ 10 \ 31 \ 37 \ 59]$ , canaux virtuels de payload

$\mathbf{m}_{i,payload}$  aléatoires,  $f = 1/U$ ,  $B = 250$  kHz et  $\Delta = 1$  (voir Section III.4.3.2). Nous transmettons consécutivement 5 fois une même trame ( $N_{frame} = 5$ ) de 500 symboles, la démodulation se déroulant normalement i.e.  $SER = 0$ . Nous ne corrigeons pas le SFO, de façon à pouvoir observer une éventuelle dérive d'énergie du bin d'intérêt dans le temps (voir Figure I.2.24). D'après la Figure III.5.8, nous remarquons :

- Le préambule est détecté à partir du 66<sup>ème</sup> paquet de  $M$  échantillons dans la fenêtre d'analyse courante (Figure III.5.8c). Nous constatons la montée progressive de l'énergie, avec une valeur maximale atteinte au 73<sup>ème</sup> paquet. Nous avons donc  $\widehat{idx}_{start} = 73$ .
- Avant la détection du préambule, l'estimateur  $CFO_{frac}$  donne des valeurs aléatoires (Figure III.5.8a). Cela est normal puisque nous sommes dans l'hypothèse  $H_0$  (bruit purement AWGN). Il accroche presque immédiatement à partir de la détection, avec une valeur moyenne d'environ 0.07 et valable jusqu'au 86<sup>ème</sup> paquet (symbole down-chirp du préambule). Ainsi, l'estimateur est assez peu sensible au décalage de paquet (voir Figure III.4.15), même sur SDR.
- L'estimateur  $STO_{frac}$  (Figure III.5.8b) suit un comportement similaire à celui de  $CFO_{frac}$ , avec une valeur estimée constante de 0.3.
- L'estimateur de ré-alignement (Figure III.5.8f) est parfaitement cohérent ici avec la théorie (voir Figure III.4.21), où le motif d'évolution d'énergie est clairement visible.
- Nous avons aussi estimé  $CFO_{frac}$  et  $STO_{frac}$  pour chaque valeur de  $\beta$  (Figures III.5.8d et III.5.8e, respectivement) et affiché l'évolution sur  $\beta$ . Nous voyons que  $\widehat{STO}_{frac}$  est parfaitement stable. En revanche,  $\widehat{CFO}_{frac}$  subit de légères fluctuations, suivant deux plateaux, de valeurs 0.06 et 0.09 environ.

Pour la Figure III.5.9, nous remarquons :

- A partir du préambule extrait au 73<sup>ème</sup> paquet, l'estimation de  $CFO_{frac}$  est d'environ 0.06 (Figure III.5.9a). Nous avons aussi  $\widehat{CFO}_{int} = 0$ . Les deux SDR utilisés sont donc de bonne qualité, avec  $\widehat{CFO} \approx 0.06$ , soit  $\Delta_f \approx 0.06 \times \frac{B}{M} = 117$  Hz.
- L'estimée de  $c_p$  vaut 51. Ainsi, le récepteur a ainsi estimé  $\widehat{idx}_{start} = idx_{start} + 1$  (voir équation (III.4.16)), et un ré-alignement de 51 échantillons vers la droite a été effectué (voir Figure III.4.20). Nous avons également  $STO_{residue}(\Delta) = 0$ . Cette estimée correspond au décalage temporel résiduel après ré-alignement. Ici, le ré-alignement est parfait puisque avoir  $STO_{residue}(\Delta) = 0$  correspondant à avoir  $\widehat{c}_p = c_p$ .
- Enfin, nous affichons l'évolution de l'amplitude du bin d'intérêt  $ccm$  en  $m = \widehat{a}$  et ceux voisins directs gauche et droite en  $m = (\widehat{a} - 1) \bmod M$  et  $m = (\widehat{a} + 1) \bmod M$ , après démodulation. Ils sont notés sur la figure respectivement  $V$ ,  $V^-$  et  $V^+$ . Nous constatons la bonne synchronisation de la trame, avec les bins voisins ayant très peu d'énergie (et donc peu de résidu de désynchronisation).
- Nous remarquons immédiatement une dérive d'énergie pour les bins voisins. Elle est ici vers la droite dans la DFT. En effet, le bin voisin droit a son énergie qui croît, tandis que celui gauche voit son énergie diminuer. Cela suggère la présence d'un SFO négatif (voir Figure I.2.24). Cependant, le bin d'intérêt ne dérive pratiquement pas. De plus, pour  $CFO \approx 0.06$ , nous aurions un SFO d'environ 0.05 d'après l'équation (I.2.38), une valeur donnant une dérive bien plus faible. Ainsi, la dérive des bins voisins n'est a priori pas due au SFO. Nous remarquons enfin la présence d'une légère fluctuation périodique des amplitudes (environ deux périodes sur toute la transmission). Cet effet est étudié plus en détail en Section III.5.5.

$U = 5$ ,  $f = 1/U$ ,  $B = 250$  kHz,  $F_c = 868.1$  MHz,  $G_{Tx} = 40$  dB,  $G_{Rx} = 0$  dB,  $SF = 7$

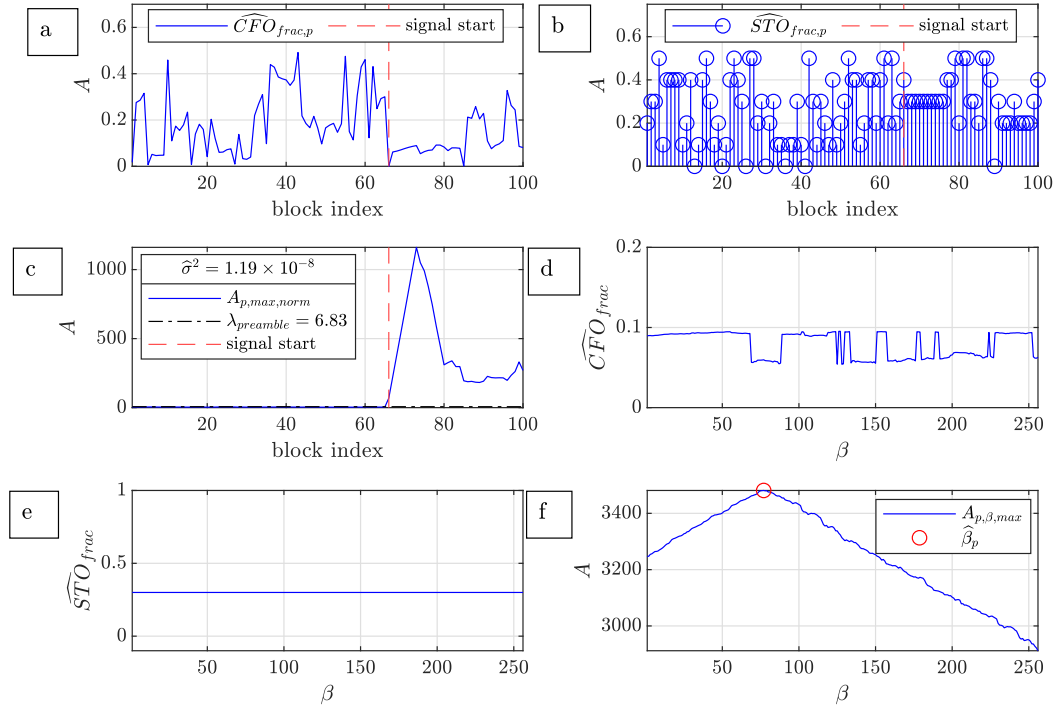


FIGURE III.5.8. – Exemple d'exécution du front-end de détection de trame sur SDR,  $U = 5$ ,  $SF = 7$

$U = 5$ ,  $f = 1/U$ ,  $B = 250$  kHz,  $F_c = 868.1$  MHz,  $G_{Tx} = 40$  dB,  $G_{Rx} = 0$  dB,  $SF = 7$

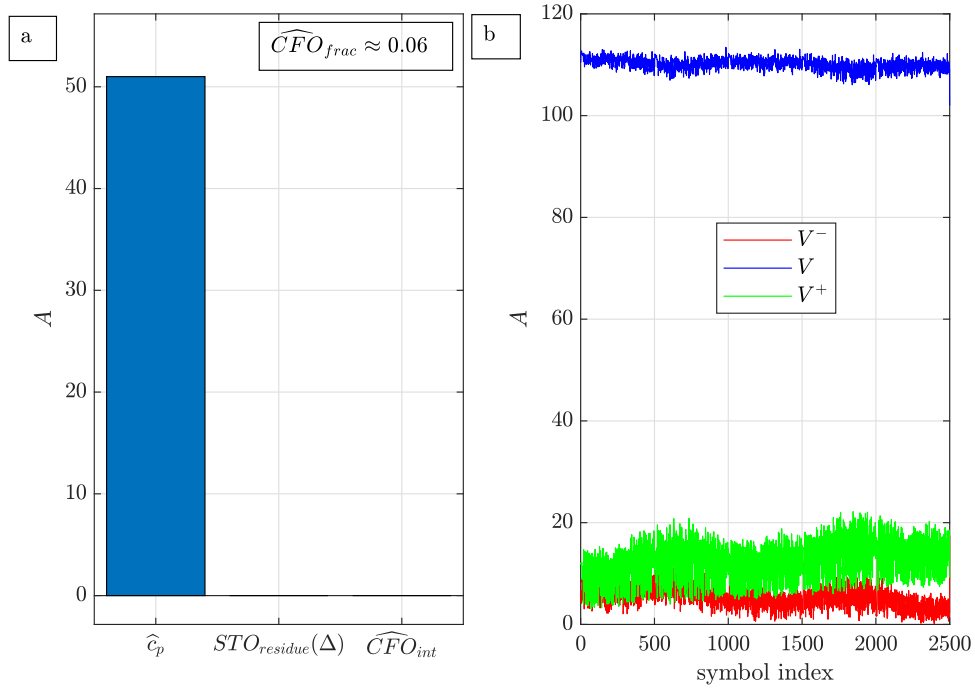


FIGURE III.5.9. – Exemple d'exécution du front-end de synchronisation et de la démodulation sur SDR,  $U = 5$ ,  $SF = 7$

Les Figures III.5.10 et III.5.11 montrent les mêmes résultats, mais pour une transmission réalisée avec  $U = 30$  et  $B = 125$  kHz au lieu de  $B = 250$  kHz.

Par rapport à la transmission avec  $U = 5$  (Figures III.5.8 et III.5.9), nous observons les différences suivantes :

- Comme la largeur de bande est de 125 kHz et non plus 250 kHz ici, le CFO estimé doit être le double, d'après l'équation (I.2.29). C'est globalement le cas ici, avec  $\widehat{CFO}_{frac} \approx 0.22$  (Figure III.5.10d contre  $\widehat{CFO}_{frac} \approx 0.06$  (Figures III.5.8d et III.5.9a).
- Rappelons que pour une correction du PAPR donnée, plus  $U$  est élevé, plus l'amplitude du bin d'intérêt diminue (voir Figure III.3.15). Ainsi, pour  $U = 30$ , nous aurons une amplitude plus faible qu'à  $U = 5$ . Cela est bien le cas ici : nous avons un niveau maximal d'environ 620 pour  $U = 30$  (Figure III.5.10c) contre environ 1160 pour  $U = 5$  (Figure III.5.8c). Cela se retrouve également dans l'amplitude de la ccm synchronisée, avec un niveau moyen d'environ 91 (Figure III.5.11b) contre 110 (Figure III.5.9b).
- Pour  $U = 30$ , le seuil de détection préambule  $\lambda_{preamble}$  est plus élevé que celui analytique. Le seuil devrait valoir théoriquement  $\lambda_{preamble} \approx 10.70$  pour  $P_{fa} = 10^{-5}$  (voir Tableau III.4.1), et non  $\lambda_{preamble} = 14$  utilisé ici. Pour cette transmission, une interférence parasite a été observée avant l'arrivée de la trame (section de bruit purement AWGN), donnant un niveau d'énergie dépassant le seuil (valeur d'environ 13.35 relevée) et mettant alors en défaut le détecteur. Cela est peut-être dû à une interférence sur le canal de transmission ou au niveau du B210. Ainsi, les communications SDR sont tributaires de phénomènes aléatoires que nous ne maîtrisons pas entièrement.
- Il n'y a pas de perte d'énergie progressive dans les bins voisins ccm (Figure III.5.11b), contrairement à la transmission faite avec  $U = 5$ . Cela confirme la non corrélation du SFO avec le comportement observé précédemment.

$U = 30, f = 1/U, B = 125 \text{ kHz}, F_c = 868.1 \text{ MHz}, G_{Tx} = 40 \text{ dB}, G_{Rx} = 0 \text{ dB}, SF = 7$

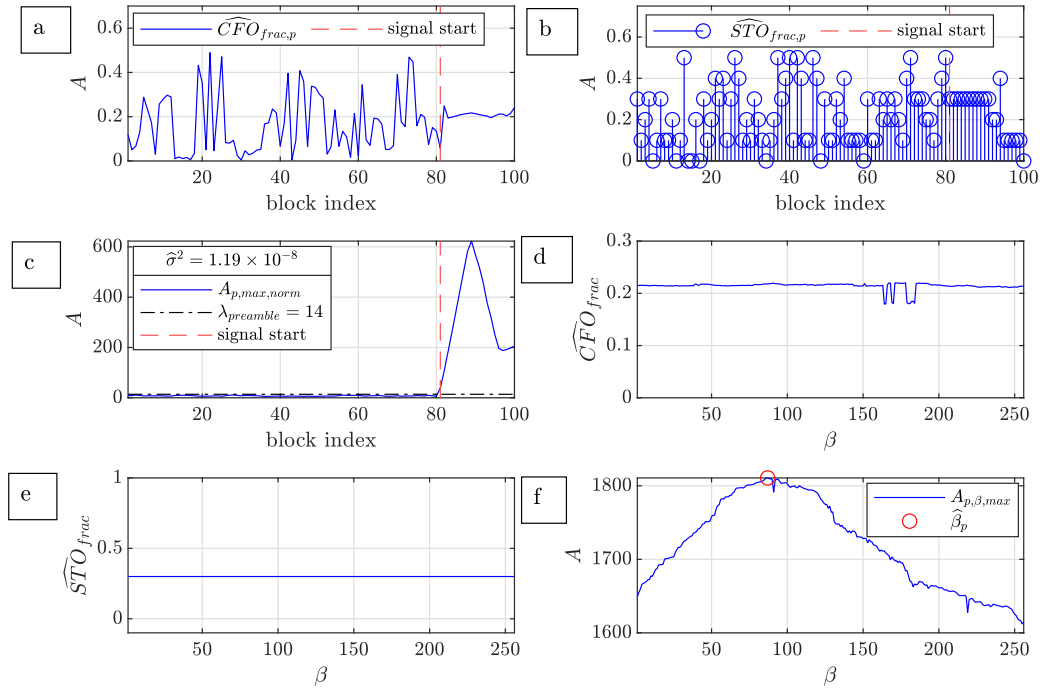


FIGURE III.5.10. – Exemple d'exécution du front-end de détection de trame sur SDR,  $U = 30, SF = 7$

$U = 30, f = 1/U, B = 125 \text{ kHz}, F_c = 868.1 \text{ MHz}, G_{Tx} = 40 \text{ dB}, G_{Rx} = 0 \text{ dB}, SF = 7$

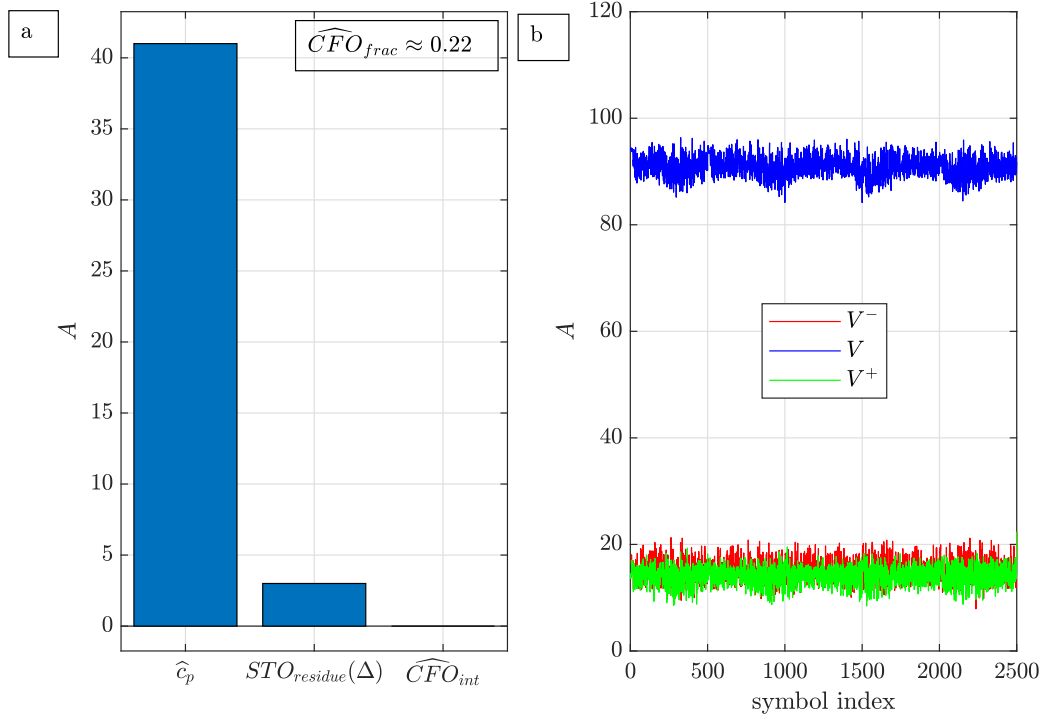


FIGURE III.5.11. – Exemple d'exécution du front-end de synchronisation et de la démodulation sur SDR,  $U = 30, SF = 7$



La Figure III.5.12 compare l'amplitude moyenne du bin d'intérêt (dénoté  $V_{mean}$  sur la figure) et ceux voisins directs gauche et droit (dénotés  $V_{mean}^-$  et  $V_{mean}^+$ ), entre les signaux SDR (mêmes transmissions que précédemment) et analytiques en simulation, pour  $U = 5$  (gauche) et  $U = 40$  (droite). Les canaux virtuels et symboles sont identiques entre SDR et simulation, et un résidu de désynchronisation  $CFO_{frac}$  est introduit ( $CFO_{frac}^{residue} = 0.02$ ) pour les signaux en simulation, afin d'avoir une comparaison équitable.

D'après la Figure III.5.12, les signaux SDR sont bien en accord avec ceux analytiques (surtout pour  $U = 40$ ), avec globalement une légère perte d'énergie pour les signaux SDR. Nous avons par exemple  $V_{mean} \approx 94$  en simulation contre  $V_{mean} \approx 91$  avec SDR, pour  $U = 40$ . Pour  $U = 5$ , les amplitudes des bins voisins ont un écart plus perceptible du fait de la dérive constatée sur la Figure III.5.9.

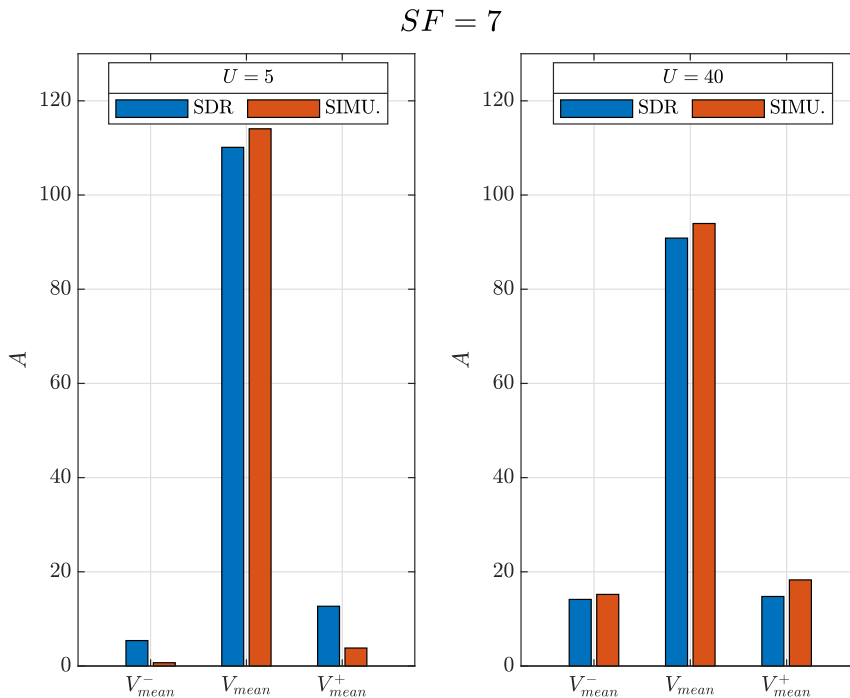


FIGURE III.5.12. – Comparaison des amplitudes des bins d'intérêt et voisins directs entre les signaux analytiques et SDR pour  $U = 5$  et  $U = 40$ ,  $SF = 7$

## III.5.5. Étude de l'enveloppe complexe et du spectre

### III.5.5.1. Étude de l'enveloppe complexe

Nous commençons par étudier l'enveloppe complexe des signaux SDR. La Figure III.5.13 montre les enveloppes complexes issues de signaux SDR LoRa legacy ( $U = 1$ ) et LoRa jam mod ( $U \in \{4, 5, 20\}$ ). Les sous-figures de gauche (1a, 2a, 3a et 4a) montrent le signal reçu des 5 trames tel quel (après sous-échantillonnage à  $F_s = B$ ) et celles de droite (1b, 2b, 3b et 4b) après synchronisation CFO et STO.

D'après la figure, nous voyons que le signal LoRa legacy a une enveloppe supérieure presque constante, avec ou sans synchronisation. Cela est parfaitement cohérent, puisque

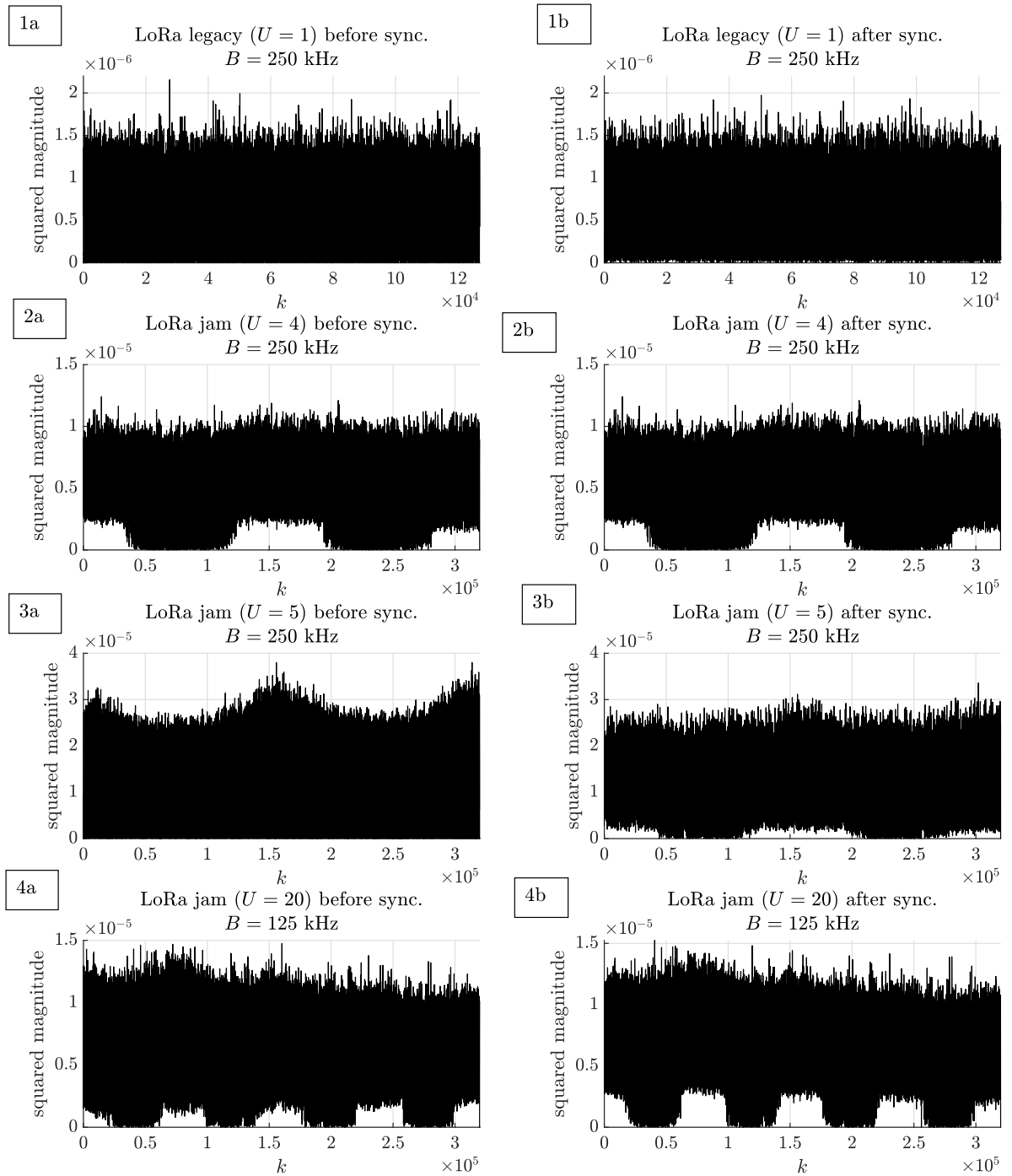


FIGURE III.5.13. – Enveloppes au cours du temps de signaux auto-brouillés reçus sur SDR pour plusieurs valeurs de  $U$ ,  $SF = 7$

le signal LoRa legacy a la propriété  $|x_a[k]|^2 = P_s \forall k$  dans l'équation (I.2.6). En revanche, lorsque l'auto-brouillage est actif, l'enveloppe est clairement modifiée. Nous avons deux motifs différents qui se dégagent, notés motif A et B. Le premier présente une fluctuation périodique de l'enveloppe supérieure et une enveloppe inférieure préservée. Nous pouvons le voir pour  $U = 5$  avant synchronisation, avec deux périodes présentes (sous-figure 3a). Le second présente une enveloppe supérieure beaucoup plus stable, mais voit l'apparition d'un motif périodique ressemblant à des *jambes* pour l'enveloppe inférieure. Cela est le cas par exemple pour  $U = 20$  après synchronisation (sous-figure 4b). Ces motifs n'étant pas présents sur les signaux analytiques, ils viennent forcément des composants matériels des SDR. En faisant le lien entre l'enveloppe obtenue et la synchronisation réalisée, nous observons les comportements suivants pour le motif de jambes :

- Le motif A est présent uniquement avant synchronisation. Il dépend en fait du niveau de désynchronisation temporelle du signal reçu. Plus  $STO_{frac}$  est proche de 0.5, plus l'enveloppe ressemblera au motif A. Pour la transmission faite avec  $U = 4$ , nous avons  $\widehat{STO}_{frac} = 0$ ,  $\widehat{STO}_{frac} = 0.3$  pour celle avec  $U = 5$  et  $\widehat{STO}_{frac} = 0.1$  pour  $U = 20$ .
- Le motif B apparaît si le signal reçu a un niveau de désynchronisation  $STO_{frac}$  faible. Il peut donc être éventuellement présent avant synchronisation ( $STO_{frac}$  aléatoire) mais forcément après synchronisation (résidu faible en principe). Nous le constatons bien sur la figure. Ce motif est étroitement lié à la largeur de bande du signal. Lorsque  $B = 125$  kHz, il y a quatre périodes contre seulement deux pour  $B = 250$  kHz. Des transmissions ont été faites avec  $B = 500$  kHz et ne donnent pas de motif de jambes.

Cinq trames consécutives ( $N_{frame} = 5$ ) de 500 symboles sont transmises à chaque fois. Ainsi, d'après la figure, le motif de jambes dure donc environ 625 et 1250 symboles pour  $B = 125$  et  $B = 250$  kHz, respectivement. L'origine de ce dernier n'est pas encore connue à ce jour. Une étude plus poussée montre qu'il n'est pas lié aux éléments suivants :

- Symboles transmis  
Nous aurions  $N_{frame} = 5$  périodes du même motif.
- Fréquence d'échantillonnage de l'ADC  
Des transmissions faites avec  $F_{ADC} = 10$  MHz au lieu de  $F_{ADC} = 5$  MHz donnent exactement le même résultat.
- Antennes utilisées  
Des transmissions faites avec des antennes VERT2450 ( $F_c = 2400$  MHz au lieu de  $F_c = 868.1$  MHz) donnent le même comportement.
- CFO  
La correction du CFO applique uniquement une correction de phase au signal, l'enveloppe n'est donc pas modifiée après synchronisation. Or, nous avons une clairement ici une déformation de l'enveloppe.

Une possible explication viendrait du filtrage numérique appliqué sur le signal reçu par le SDR (filtre de réponse impulsionnelle finie possédant 128 taps, d'après [192]). Cela pourrait alors engendrer des déformations non désirées de l'enveloppe complexe. Une future piste d'exploration serait de réaliser des transmissions en désactivant ou modifiant ce filtre de réception, et d'étudier ainsi les différences de comportement de l'enveloppe complexe.

### III.5.5.2. Étude du spectre

Nous nous intéressons ici à étudier l'impact de la correction du PAPR et du paramètre  $U$  sur l'évolution au cours du temps du contenu spectral (*waterfall* en anglais) de signaux reçus sur SDR. Nous utilisons le logiciel SDR Console [193] offrant une compatibilité avec de nombreux SDR et proposant des outils de visualisation de signaux variés (signal reçu temporel, DFT, waterfall, constellations, etc.). De plus, il offre une grande souplesse pour une visualisation en temps réel.

Les Figures III.5.14, III.5.15 et III.5.16 montrent les résultats obtenus (waterfall et/ou spectre) pour des transmissions réalisées avec  $SF = 7$ . La Figure III.5.14 montre pour LoRa legacy ( $U = 1$ ) pour  $B = 250$  kHz. La Figure III.5.15 montre pour LoRa jam mod ( $U = 5$ ) et  $B = 125$  kHz pour deux transmissions réalisées, les canaux virtuels ont pour valeur  $\mathbf{m} = [0 \ 10 \ 31 \ 37 \ 59]$ . La Figure III.5.16 montre toujours pour LoRa jam mod ( $U = 5$ ), même canal, mais en considérant  $B = 250$  kHz et  $B = 500$  kHz.

Pour LoRa jam mod, la première transmission n'applique pas de correction du PAPR ( $f = 1$ ) tandis que la seconde applique une correction du PAPR maximale ( $f = 1/U$ ). Les deux transmissions sont réalisées consécutivement, de façon à pouvoir les visualiser dans la même fenêtre temporelle. Nous utilisons deux marqueurs fréquentiels positionnés à  $\nu = F_c - B/2$  et  $\nu = F_c + B/2$ , afin d'évaluer la largeur de bande du signal.

Sur l'ensemble des figures, nous remarquons qu'un pic d'énergie est présent avant chaque transmission (environ 1 seconde avant, entouré en rouge sur la Figure III.5.14). Cela provient de l'initialisation du SDR pour la transmission, où la calibration interne des composants est réalisée et vient sans doute de l'étage d'amplification (réglage du niveau de gain) du front-end radio.

Nous voyons sur la Figure III.5.14 que LoRa legacy donne un spectre respectant assez bien la bande  $B = 250$  kHz, avec cependant une légère diffusion d'énergie en dehors de la bande, d'environ 15 kHz sur la partie inférieure et supérieure du spectre, avec un gain inférieur d'au moins 15 dB par rapport à la bande utile. Cela est cohérent avec les résultats obtenus dans [64], où les auteurs montrent que cette diffusion est de plus en plus faible à mesure que SF augmente. Cela vient de la période d'intégration temporelle plus longue du signal, donnant une meilleure résolution spectrale.

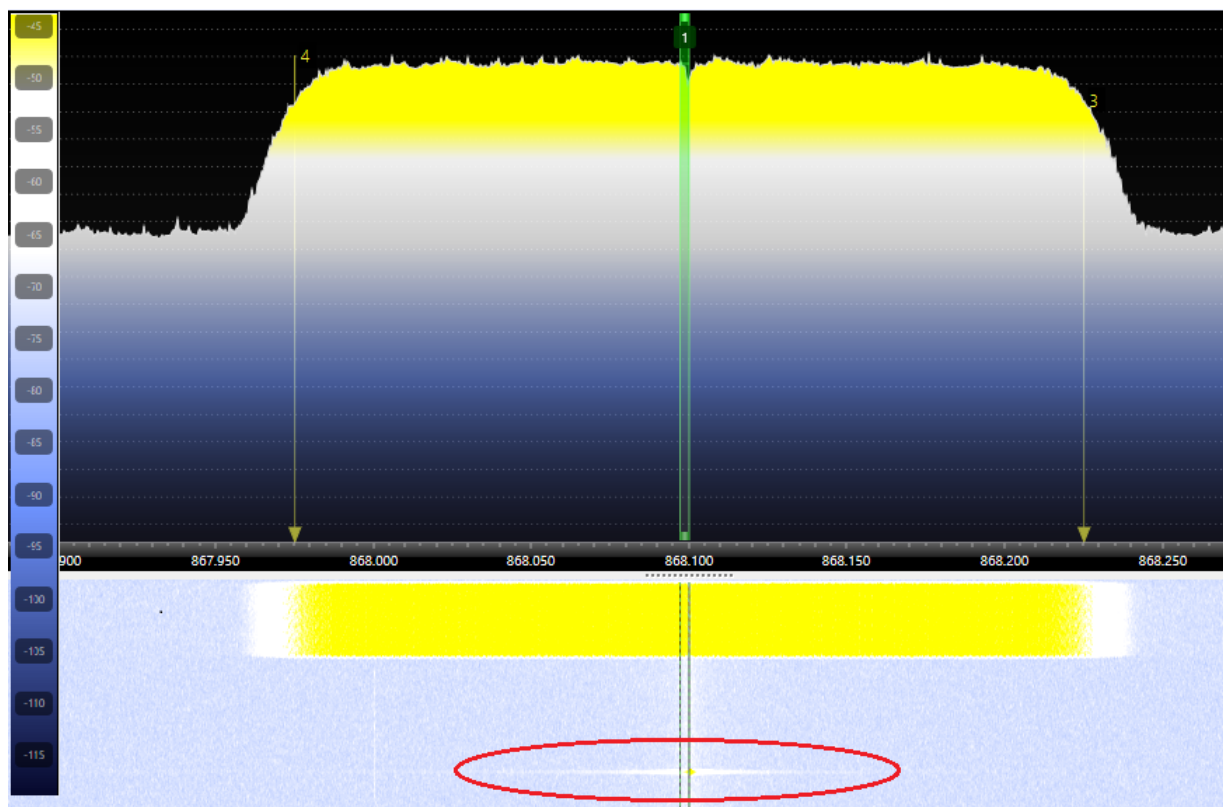


FIGURE III.5.14. – Spectre et waterfall d'un signal LoRa legacy ( $U = 1$ ) SDR, 250 kHz et  $SF = 7$

D'après les Figures III.5.15 et III.5.16, le schéma d'auto-brouillage avec correction maximale du PAPR donne un spectre déformé, avec une diffusion d'énergie dépassant 400 kHz en partie inférieure et supérieure et atténuée d'au moins 10 dB. Nous remarquons qu'elle est périodique et dépend de la largeur de bande du signal. Nous avons quatre, deux et une périodes pour  $B = 125$  kHz (Figure III.5.15a),  $B = 250$  (Figure III.5.16a) et  $B = 500$  kHz (Figure III.5.16b), respectivement. Cette diffusion et le motif de jambes étudié en Section III.5.5.1 sont donc directement liés (voir Figure III.5.16a et la sous-figure III.5.13 2b). Des transmissions réalisées avec d'autres valeurs de canaux virtuels et de SF donnent exactement les mêmes comportements. Sur la Figure III.5.15b, le spectre présenté est celui lorsqu'il y a diffusion de l'énergie pour  $B = 125$  kHz et  $f = 1/U$ . On constate la remontée du niveau d'énergie en dehors de la bande, par rapport au spectre LoRa legacy.

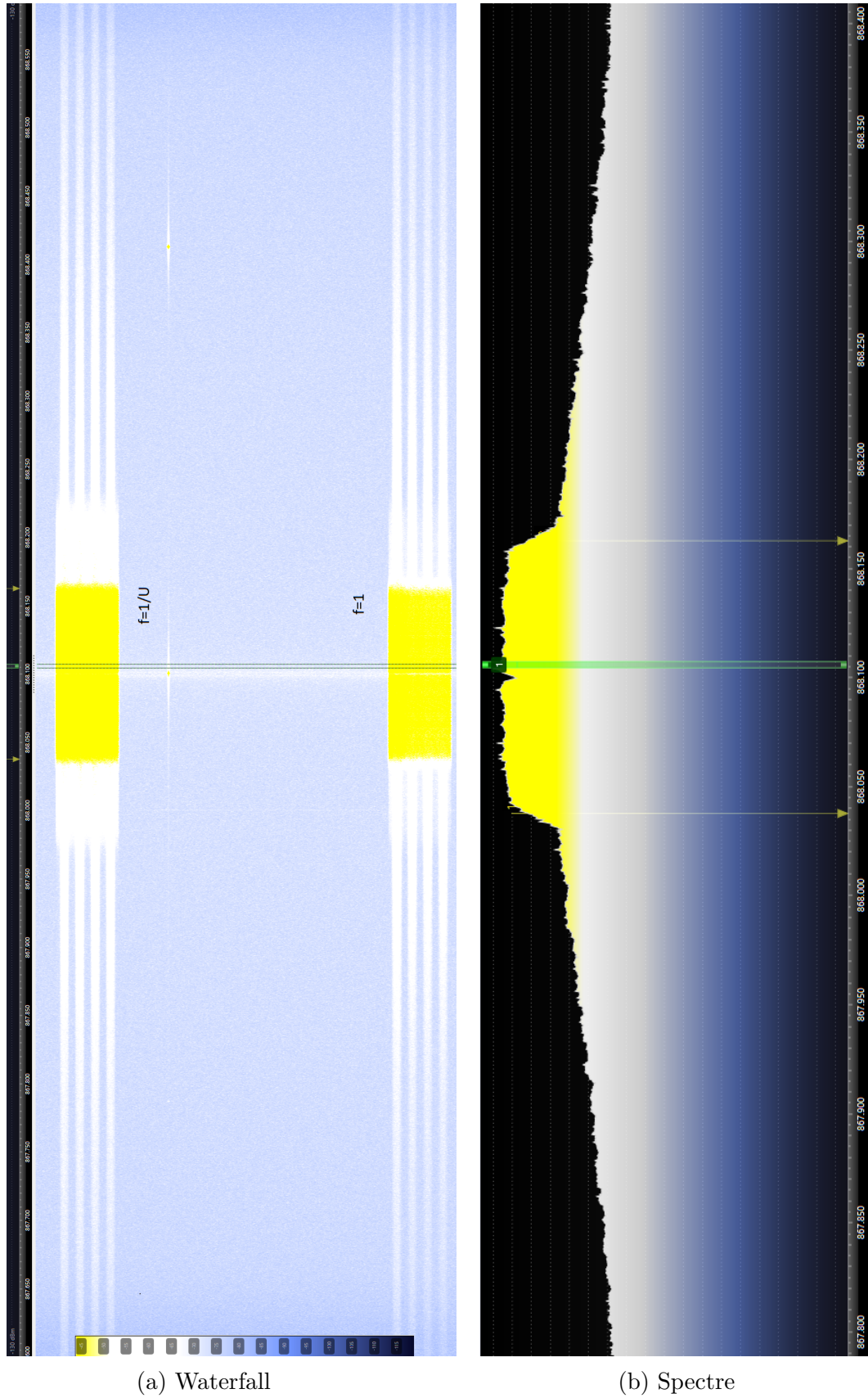


FIGURE III.5.15. – Waterfall et spectre de signaux LoRa jam mod SDR pour  $B = 125$  kHz, avec/sans correction du PAPR,  $U = 5$  et  $SF = 7$



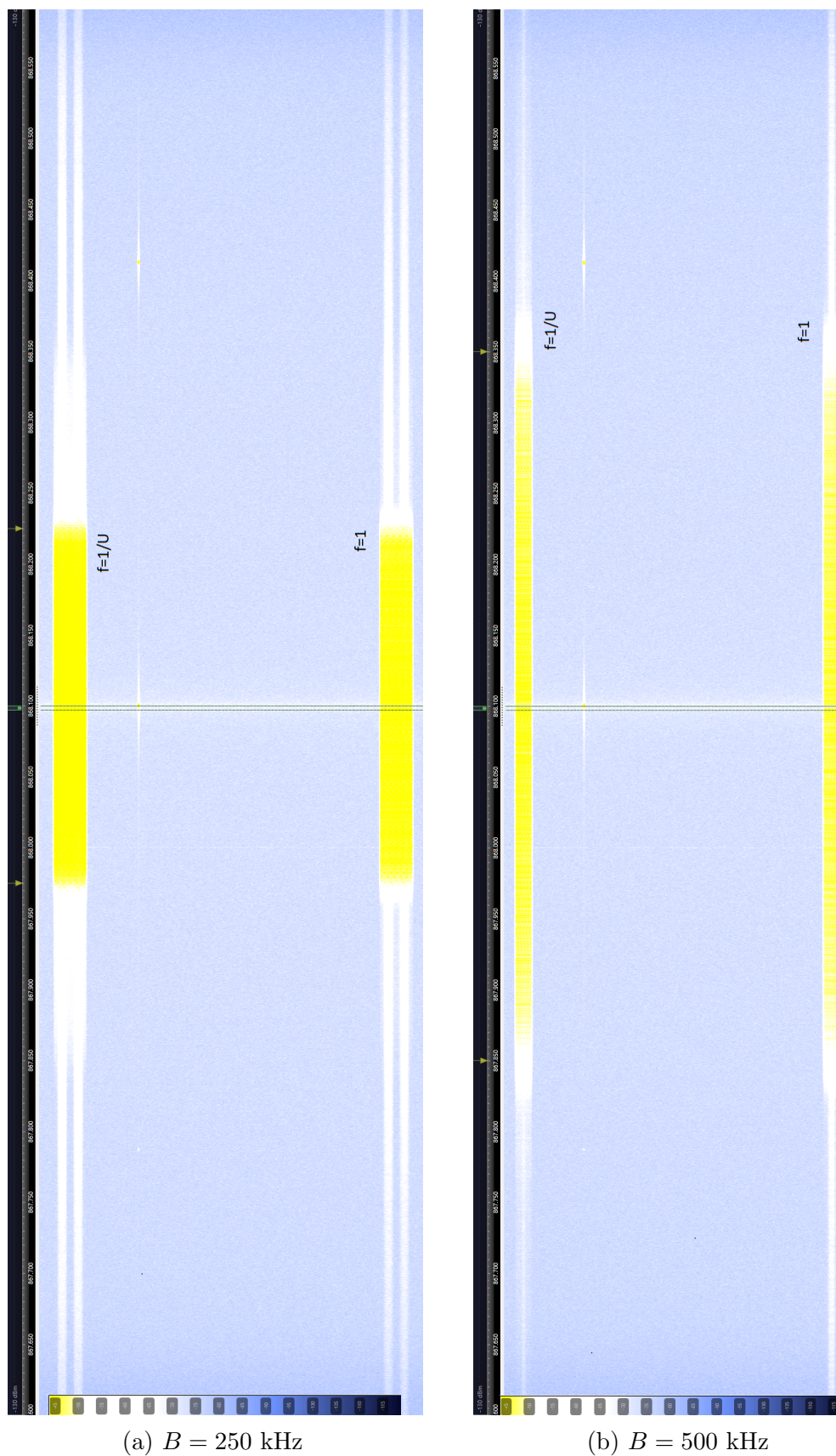


FIGURE III.5.16. – Waterfall de signaux LoRa jam mod SDR pour  $B = 250$  kHz et  $B = 500$  kHz, avec/sans correction du PAPR,  $U = 5$  et  $SF = 7$

La Figure III.5.17 montre l'impact de  $U$  plus élevé sur le waterfall, en utilisant la même démarche pour la réalisation des transmissions, avec  $U = 20$  (Figure III.5.17a) et  $U = 30$  (Figure III.5.17b),  $B = 250$  kHz et  $SF = 7$ . Les canaux virtuels ont pour valeur :

- $U = 20$   
 $\mathbf{m} = [0\ 3\ 8\ 11\ 16\ 21\ 27\ 30\ 36\ 41\ 44\ 49\ 53\ 58\ 61\ 70\ 73\ 76\ 79]$
- $U = 30$   
 $\mathbf{m} = [0\ 3\ 6\ 10\ 13\ 16\ 19\ 23\ 26\ 29\ 33\ 37\ 41\ 45\ 49\ 52\ 55\ 58\ 61\ 65\ 68\ 72\ 76\ 80\ 83\ 87\ 91\ 94\ 97\ 101]$

Nous constatons que le comportement n'est pas altéré avec l'augmentation de  $U$ . Nous voyons en effet le même élargissement de bande et le motif périodique de diffusion d'énergie. D'autres transmissions réalisées avec d'autres canaux virtuels donnent le même comportement.

Pour conclure sur cette partie SDR, nous rappelons les points suivants importants :

- Les signaux LoRa auto-brouillés synthétisés par le SDR B210 d'Ettus Research ne sont pas exploitables sans correction du PAPR. Une correction maximale est vivement recommandée afin d'obtenir un signal parfaitement exploitable en réception.
- La correction du PAPR engendre des diffusions spectrales d'énergie périodiques qui dépendent de la largeur de bande du signal.
- Le motif de jambes observé n'a pas encore d'origine clairement déterminée (mais lié à la diffusion spectrale d'énergie périodique), et pourrait faire l'objet d'une étude future plus poussée.



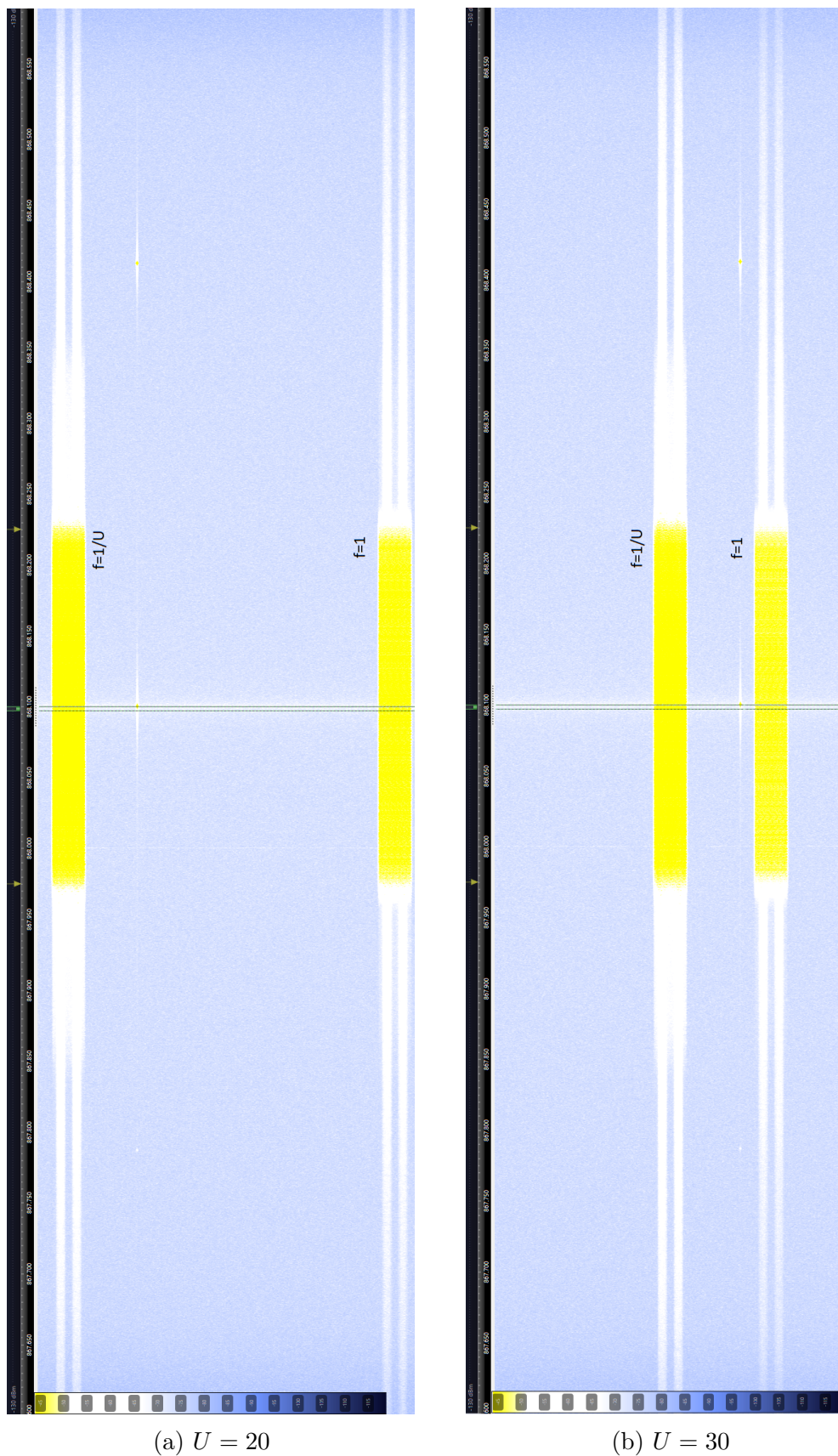


FIGURE III.5.17. – Waterfall de signaux LoRa jam mod SDR pour  $U = 20$  et  $U = 30$ ,  $B = 250$  kHz, avec/sans correction du PAPR et  $SF = 7$

## Conclusion et perspectives de recherche

Nous arrivons au terme de ce mémoire. Pour conclure, nous rappelons d'abord les résultats importants obtenus au cours de la thèse, puis nous évoquons plusieurs perspectives intéressantes pour l'amélioration des travaux et nous ouvrons de nouvelles pistes de recherche.

### Synthèse des résultats obtenus

Cette thèse a apporté plusieurs contributions au standard Long Range (LoRa), selon deux axes principaux : 1) l'amélioration du récepteur classique avec une étude approfondie de l'impact des canaux multi-trajets sur la démodulation et la proposition du récepteur cohérent amélioré LoRa RAKE, basé sur une philosophie d'égalisation de canal RAKE et 2) la proposition d'un schéma d'auto-brouillage LoRa ajoutant une sécurisation au niveau de la couche physique, réduisant fortement la capacité de démodulation d'intercepteurs et améliorant donc la confidentialité.

### Améliorations du récepteur classique LoRa

Le premier axe de la thèse a été l'amélioration du récepteur classique LoRa, avec l'étude des canaux multi-trajets et le développement du récepteur amélioré LoRa RAKE.

Nous avons réalisé en Section II.1 une première étude analytique de l'impact d'un canal multi-trajets, pour le cas où ce dernier est dit aligné (les répliques ont des retards multiple de la période d'échantillonnage) avec synchronisation temporelle et fréquentielle parfaite. Nous avons ainsi proposé une expression théorique du taux d'erreur symbole (Symbol Error Rate (SER)), mis en évidence l'écart important de performances pouvant exister en fonction des paramètres du canal multi-trajets et montré l'effet caractéristique d'un canal multi-trajets à décroissance exponentielle sur LoRa. De plus, nous avons observé qu'une interférence LoRa (signal provenant d'un autre utilisateur LoRa) a un effet proche de celui du canal multi-trajets. Une étude a été menée pour ce scénario, évaluant les performances en fonction du retard du signal d'interférence par rapport au signal LoRa d'intérêt. Les travaux ont été publiés dans l'article *Theoretical Performance of LoRa System in Multipath and Interference Channels* dans la revue *IEEE IoT Journal* [90].

Fort de cette première contribution, nous avons développé en Section II.2 le récepteur cohérent amélioré LoRa RAKE, toujours dans le cas d'un canal multi-trajets aligné. LoRa RAKE exploite de façon constructive l'énergie du trajet principal et celle des éventuelles répliques, dans le domaine fréquentiel LoRa. Une étude analytique approfondie a été menée et plusieurs variantes du récepteur ont été proposées afin de réduire la complexité calculatoire. Nous avons mis en évidence les bonnes performances de LoRa RAKE, surpassant celles d'un autre récepteur non-cohérent proposé dans la littérature (nommé TDEL), ouvrant la voie pour l'usage de récepteurs cohérents, en lieu et place du récepteur LoRa classique non-cohérent. LoRa RAKE a été publié dans l'article *Simple and Efficient LoRa Receiver Scheme for Multi Path Channel*, toujours dans *IEEE IoT Journal* [92].

Les travaux ont ensuite été étendus pour le cas où le canal multi-trajets possède une ou plusieurs répliques à retards inférieurs à une période d'échantillonnage (canal non-aligné), scénario réaliste pour un contexte LoRa, et en prenant en compte les synchronisations

temporelle et fréquentielle au niveau du récepteur. Nous avons adapté les algorithmes de synchronisation de la littérature pour LoRa RAKE et mené une comparaison avec le récepteur TDEL afin de répondre aux questions suivantes : 1) comment le canal multi-trajets non-aligné impacte la synchronisation ? et 2) laquelle des deux approches cohérente ou non-cohérente donne les meilleures performances ? L'étude a montré que LoRa RAKE propose les meilleures performances à bas rapport signal à bruit (Signal to Noise Ratio (SNR)) et pour des répliques proches du trajet direct et qu'en fonction des paramètres du canal, l'impact sur les performances de synchronisation peut-être dramatique. Nous avons montré que les algorithmes de synchronisation sont le principal facteur limitant de performances et que les récepteurs non-cohérents restent tout de même intéressants pour un usage réel. Nous encourageons ainsi le développement d'algorithmes conjoints de synchronisation et d'égalisation. L'article de cette étude, *A RAKE-like coherent LoRa receiver for Non-Aligned Multi-Path Channels*, a été soumis dans la revue *IEEE Transactions on Wireless Communications* [93].

### Sécurisation de la couche physique LoRa : schéma d'auto-brouillage

Le second axe de la thèse a été l'amélioration de la sécurisation de la couche physique LoRa, avec la proposition du schéma d'auto-brouillage conçu pour rendre difficile la démodulation aveugle par des intercepteurs.

Avant de proposer le schéma d'auto-brouillage, nous avons d'abord effectué en Section III.2 une étude de l'impact des brouilleurs classiques de la littérature : Tone Jamming (TJ) et Band Jamming (BJ). Le premier émet un signal de brouillage comportant un ou plusieurs signaux sinusoïdaux purs (composantes fréquentielles) dans la bande du signal utile, et le second est un bruit Additive White Gaussian Noise (AWGN) filtré ayant une largeur de bande et une position fixes dans la bande. Nous avons considéré le scénario d'un canal plat AWGN avec synchronisation parfaite. Nous avons montré que les paramètres du brouilleur BJ ont une influence limitée, et qu'en fonction des composantes fréquentielles du brouilleur TJ et du symbole transmis, l'impact peut-être par contre très important. Nous avons dans un second temps développé un détecteur pour ces brouilleurs. A partir des expressions théoriques des probabilités de détection et des résultats de simulation, nous avons montré que le brouilleur TJ est plus facilement détectable si ce dernier possède une seule composante fréquentielle, et proche du brouilleur BJ sinon. Les résultats ont été présentés lors de la conférence SPI2021 à Brest en 2021 [96].

Le schéma d'auto-brouillage proposé dans les Sections III.3, III.4 et III.5 s'applique pour le scénario où un émetteur et un récepteur légitimes communiquent entre eux et souhaitent garder l'information échangée secrète (information sensible), de façon à ce qu'un intercepteur présent dans le voisinage ne puisse pas démoduler facilement. Pour cela, la forme d'onde LoRa est modifiée de façon à ce que le symbole à transmettre soit passé artificiellement dans un canal virtuel à l'émission (plusieurs répliques du même symbole). Ce canal est uniquement connu par le récepteur légitime, ce dernier peut donc, en exploitant cette connaissance, démoduler le symbole, contrairement à l'intercepteur. Le schéma respecte une contrainte de puissance d'émission constante, quelle que soit la longueur du canal virtuel. Dans le domaine fréquentiel LoRa, cela se traduit par l'étalement du symbole dans la bande. Ainsi, plus le canal virtuel est large, plus l'étalement est important, réduisant de fait les capacités de détection de trame pour l'intercepteur.

Le schéma a été présenté en détail en Sections III.3 et III.4. Les deux démodulateurs *ccl* et *ccm* ont été proposés, chacun ayant leurs avantages et inconvénients. *ccl* possède une plus faible sensibilité à la désynchronisation et une plus faible complexité calculatoire, mais une forte sensibilité au nombre de symboles d'auto-brouillage (dégradation des performances). *ccm* n'a pas cette dégradation de performances sur le nombre de symboles d'auto-brouillage, il est donc parfaitement adapté à la démodulation du payload. Les algorithmes de synchronisation de la littérature les plus pertinents ont été réutilisés et adaptés au schéma d'auto-brouillage, tandis qu'un nouveau front-end de synchronisation est proposé, où un nouveau schéma de correction du Sampling Temporal Offset (STO) par candidats est présenté. Les résultats de simulation obtenus pour des canaux AWGN ont démontré la viabilité du schéma. Le schéma d'auto-brouillage a été publié dans l'article *A Novel Scheme for Discrete and Secure LoRa Communications* dans la revue *MDPI Sensors* [97].

Le schéma d'auto-brouillage génère un Peak-to-Average Power Ratio (PAPR) non nul (fortes variations de la puissance dans le temps par rapport à la puissance moyenne). Il provient de la saturation des composants matériels synthétisant la forme d'onde. Cette saturation engendre des déformations sur le signal généré, dégradant les performances de démodulation en réception et pouvant donc fortement limiter son application en conditions réelles. Ainsi, une méthode de réduction du PAPR a été proposée, conduisant à une seconde modification de la forme d'onde à l'émission permettant de paramétrer le PAPR tout en préservant les propriétés d'auto-brouillage. L'impact de la méthode sur la synchronisation et la démodulation a été étudié en détail. Nous avons montré en simulation qu'avec la méthode, les performances sont dégradées, mais de façon raisonnable, pour l'ensemble des paramètres d'auto-brouillage considérés. La méthode de réduction du PAPR, présentée dans l'article *A PAPR Reduction Scheme for LoRa Self-Jamming Waveform* a été soumise dans la revue *IEEE IoT Journal* [98].

Enfin, l'évaluation du schéma d'auto-brouillage sur plateformes de type Software Defined Radio (SDR) en Section III.5 a fait l'objet d'une mobilité de trois mois à l'ATM de Bucarest en Roumanie. Les expérimentations réalisées montrent la bonne tenue des algorithmes de synchronisation en conditions réelles et l'apport majeur de la réduction du PAPR. En effet, sans cette dernière, la démodulation est presque impossible tant le signal reçu est déformé. La correction du PAPR permet de progressivement retrouver un signal d'auto-brouillage réellement exploitable, pour obtenir les mêmes propriétés que celui analytique lorsque la réduction est maximale. Une fluctuation au cours du temps de l'enveloppe complexe ainsi qu'une diffusion d'énergie dans le domaine spectral sont observées. Leur origine n'est pas encore connue à ce jour, des pistes de recherche ont été proposées, qui pourraient faire l'objet d'investigations plus poussées.

## Perspectives

Nous présentons dans cette section plusieurs perspectives d'amélioration des travaux et de nouvelles pistes de recherche qui ont émergé à la fin de la thèse.

### Amélioration des travaux

Comme mentionné en Section III.5.5, l'origine du motif de fluctuation de l'enveloppe au cours du temps (appelé *motif de jambes*) n'est pas encore exactement connue, mais nous pensons qu'il proviendrait des éléments du front-end, en particulier du filtre de réception numérique configurable. Ainsi, une autre étude pourrait être envisagée, où nous évaluerions l'impact des paramètres du filtre sur l'enveloppe du signal SDR et en simulation, en faisant des comparaisons. Si cette étude ne s'avérait pas concluante, d'autres pistes pourraient être explorées, comme par exemple réaliser des évaluations sur des SDR assez différents techniquement de ceux utilisés.

Nous avons mis en évidence en Section III.3.4.6 qu'une élimination directe de la correction du PAPR en réception (méthode Zero Forcing (ZF)) n'est pas une bonne stratégie, puisque le signal résultant se retrouve déformé, du fait de l'amplification de la composante de bruit AWGN. Les performances de démodulation sont donc fortement dégradées. Cependant, il serait intéressant d'explorer d'autres méthodes d'élimination. Par exemple, utiliser une approche de type Minimum Mean Square Error (MMSE) pourrait éventuellement diminuer la composante de bruit, et réduire ainsi la perte de performances. L'enjeu serait alors de savoir à quel point l'élimination MMSE serait intéressante (se rapprocher le plus possible des performances obtenues sans élimination, voire faire mieux), au prix d'une complexité calculatoire plus importante qui serait à évaluer.

Il serait souhaitable d'obtenir des expressions analytiques du SER pour les récepteurs *ccl* et *ccm*. En effet, certains résultats de simulation déjà obtenus pourraient être confirmés et de nouveaux éléments théoriques seraient alors accessibles, comme des comportements asymptotiques sur le nombre de symboles d'auto-brouillage par exemple. Les différents développements mathématiques de l'expression théorique du SER dans un canal multi-trajets aligné pourraient servir de base. En effet, l'inter-corrélation circulaire peut-être vue comme la superposition du symbole d'intérêt et de nombreuses répliques d'un nouveau canal virtuel issu des interférences de corrélation.

Enfin, l'impact du canal multi-trajets pourrait être étendu au schéma d'auto-brouillage avec une étude similaire à celle réalisée dans notre article *A RAKE-like coherent LoRa receiver for Non-Aligned Multi-Path Channels* soumis dans *IEEE Transactions on Wireless Communications* [93]. Nous pensons que sans correction du PAPR, le comportement serait analogue, du fait de la linéarité du schéma d'auto-brouillage (somme parfaite de symboles d'auto-brouillage). En revanche, une exploration plus poussée serait nécessaire lorsque la correction du PAPR est présente, où l'effet conjoint n'est pas encore connu.

### Futures pistes de recherche

Le développement du schéma d'auto-brouillage nous a donné une nouvelle piste de recherche pour développer un schéma de transmission multi-utilisateurs LoRa, en ré-exploitant les canaux virtuels, mais vus comme une séquence d'étalement. Des travaux ont été engagés et des premiers résultats ont été obtenus, montrant un potentiel certain. Une future publication est prévue pour prouver le concept et encourager de nouveaux travaux sur cette piste.

Enfin, un autre axe de recherche complètement différent est à explorer : les surfaces

intelligentes réfléchissantes (Reflective Intelligent Surface (RIS)) qui ont attiré une vive attention de la communauté scientifique ces dernières années. Les RIS sont des éléments rayonnants rassemblés, placés entre l'émetteur et le récepteur, et ayant pour but de rediriger les signaux réfléchis venant de l'émetteur dans la direction du récepteur. Cela permet de considérablement améliorer la portée de la communication en adaptant le canal de transmission, mais également d'ouvrir la voie pour des méthodes de sécurisation de communication. Par exemple, nous pouvons imaginer le scénario d'une prison où l'on souhaite autoriser les communications des gardiens et interdire celles faites de façon clandestine par les prisonniers. Grâce aux RIS, des zones géographiques comportant un signal de brouillage (les cellules) pourraient être créées, tandis que des zones blanches tout autour seraient mises en place, afin d'assurer un niveau de confidentialité pour les communications légitimes.

## Bibliographie

- [1] STATISTA. *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030*. Juill. 2023. URL : <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> (visité le 27/07/2023).
- [2] T. ELSHABRAWY et J. ROBERT. « Enhancing LoRa Capacity using Non-Binary Single Parity Check Codes ». In : *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. Oct. 2018, p. 1-7.
- [3] T. ELSHABRAWY et J. ROBERT. « Interleaved Chirp Spreading LoRa-Based Modulation ». In : *IEEE Internet of Things Journal* 6.2 (avr. 2019), p. 3855-3863. ISSN : 2372-2541. DOI : 10.1109/JIOT.2019.2892294.
- [4] M. XHONNEUX et al. « A Low-Complexity LoRa Synchronization Algorithm Robust to Sampling Time Offsets ». In : *IEEE Internet of Things Journal* (2021), p. 1-1. DOI : 10.1109/JIOT.2021.3101002.
- [5] J. TAPPAREL et al. « An Open-Source LoRa Physical Layer Prototype on GNU Radio ». In : *2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. 2020, p. 1-5. DOI : 10.1109/SPAWC48557.2020.9154273.
- [6] M. A. B. TEMIM et al. « An Enhanced Receiver to Decode Superposed LoRa-like Signals ». In : *IEEE Internet of Things Journal* (avr. 2020), p. 1-1.
- [7] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. *Internet des objets*. consulté le 21 décembre 2022. 2015. URL : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26529845/internet-des-objets>.
- [8] CARNEGIE MELLON UNIVERSITY. *The "Only" Coke Machine on the Internet*. consulté le 21 décembre 2022. URL : [https://www.cs.cmu.edu/~coke/history\\_long.txt](https://www.cs.cmu.edu/~coke/history_long.txt).
- [9] M. WEISER. « The Computer of the 21st Century ». In : *Scientific American* (1991), p. 94-104. DOI : 10.1038/scientificamerican0991-94.
- [10] R. S. RAJI. « Smart networks for control ». In : *IEEE Spectrum* 31.6 (1994), p. 49-55. DOI : 10.1109/6.284793.
- [11] P. OGOR et L. MARCÉ. *Une architecture générique pour la supervision sûre à distance de machines de production avec Internet*. 2001.
- [12] Cover PAGES. *METRO Group to Introduce RFID Across Process Chain*. consulté le 22 décembre 2022. 2003. URL : <http://www.xml.coverpages.org/METRO-RFID.html>.
- [13] Petrol PLAZA. *RFID Systems at Gas Stations : What's the Difference ?* consulté le 22 décembre 2022. 1997. URL : <https://www.petroplaza.com/knowledge/1826>.
- [14] Supply HOUSE. *Focus on Technology : RFID gets the green light*. consulté le 22 décembre 2022. 2001. URL : <https://www.supplyht.com/articles/86150-focus-on-technology-rfid-gets-the-green-light>.

- [15] GLOBENEWSWIRE. *IoT in Healthcare Market to Reach USD 176.82 Billion by 2026 : Emerging Popularity of Smart Wearables and Remote Patient Monitoring to Add Impetus to Market*. consulté le 22 décembre 2022. 2020. URL : <https://www.globenewswire.com/news-release/2020/02/20/1987603/0/en/IoT-in-Healthcare-Market-to-Rreach-USD-176-82-Billion-by-2026-Emerging-Popularity-of-Smart-Wearables-and-Remote-Patient-Monitoring-to-Add-Impetus-to-Market.html>.
- [16] CBC. *The Internet of Insecure Things*. consulté le 22 décembre 2022. 2013. URL : <https://www.cbc.ca/player/play/2430717625>.
- [17] CNBC. *The biggest security risks of using fitness trackers and apps to monitor your health*. consulté le 22 décembre 2022. 2022. URL : <https://www.cnbc.com/2022/11/26/the-biggest-risks-of-using-fitness-trackers-to-monitor-health.html>.
- [18] GOV.UK. *Plans announced to introduce new laws for internet connected devices*. consulté le 22 décembre 2022. 2019. URL : <https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices>.
- [19] LEGIFRANCE. *DECISION n°DR- 2014-058*. consulté le 22 décembre 2022. 2014. URL : <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000028781717>.
- [20] LEGIFRANCE. *DECISION n°DR- 2013-058*. consulté le 22 décembre 2022. 2013. URL : <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000027166499>.
- [21] L. BASSI. « Industry 4.0 : Hope, hype or revolution ? » In : *2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry (RTSI)*. 2017, p. 1-6. DOI : 10.1109/RTSI.2017.8065927.
- [22] BBC NEWS. *Internet of things blurs the line between bits and atoms*. consulté le 22 décembre 2022. 2011. URL : <https://www.bbc.com/news/business-13632206>.
- [23] FORBES. *12 IoT Devices Already Having A Big Impact In Consumer And Business Markets*. consulté le 21 décembre 2022. 2022. URL : <https://www.forbes.com/sites/forbestechcouncil/2022/03/17/12-iot-devices-already-having-a-big-impact-in-consumer-and-business-markets/?sh=24e138896417>.
- [24] CNIL. *Smart city*. consulté le 21 décembre 2022. URL : <https://www.cnil.fr/fr/definition/smart-city>.
- [25] TACTIS. *Quels sont les exemples de Smart City et ville intelligente en France ?* consulté le 21 décembre 2022. 2021. URL : <https://www.tactis.fr/smart-city-exemples-france/>.
- [26] CBC. *Calgary conference looks at how to apply smart technology to agriculture industry*. consulté le 22 décembre 2022. 2022. URL : <https://www.cbc.ca/player/play/2114997315547>.
- [27] ORDR. *10 Internet of Things (IoT) healthcare examples*. consulté le 22 décembre 2022. 2021. URL : <https://ordr.net/article/iot-healthcare-examples/>.
- [28] WIPRO. *What can IoT do for healthcare*. consulté le 22 décembre 2022. 2022. URL : <https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/>.



- [29] FORBES. *How IoT Is Transforming Healthcare*. consulté le 22 décembre 2022. 2021. URL : <https://www.forbes.com/sites/forbestechcouncil/2021/03/31/how-iot-is-transforming-healthcare/?sh=933986867e55>.
- [30] FEDERAL COMMUNICATIONS COMMISSION – OFFICE OF ENGINEERING AND TECHNOLOGY – POLICY AND RULES DIVISION. *FCC online table of frequency allocations*. consulté le 23 décembre 2022. 2022. URL : <https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf>.
- [31] E. O’CONNELL, D. MOORE et T. NEWE. « Challenges Associated with Implementing 5G in Manufacturing ». In : *MDPI telecom* (2020), p. 48-67. DOI : 10.3390/telecom1010005.
- [32] HUAWAI. *What Are 802.11ac and 802.11ac Wave 2*. consulté le 23 décembre 2022. 2020. URL : <https://support.huawei.com/enterprise/en/doc/ED0C1100081215>.
- [33] C. GOURSAUD et J. M. GORCE. « Dedicated networks for IoT : PHY / MAC state of the art and challenges ». In : *EAI endorsed transactions on Internet of Things* (oct. 2015). DOI : 10.4108/eai.26-10-2015.150597.
- [34] INGENU.COM. *Ingenu – RPMA Technology*. consulté le 26 décembre 2022. URL : <https://www.ingenu.com/>.
- [35] SILICON.FR. *IoT : Ingenu veut bousculer Lora et Sigfox en Europe avec sa technologie RPMA*. consulté le 26 décembre 2022. 2017. URL : <https://www.silicon.fr/iot-ingenu-vise-europe-technologie-rpma-167178.html>.
- [36] SIGFOX.COM. *Sigfox 0G Technology*. consulté le 26 décembre 2022. URL : <https://www.sigfox.com/en/what-sigfox/technology>.
- [37] Le MONDE. *En difficulté, Sigfox attire de multiples prétendants*. consulté le 26 décembre 2022. 2022. URL : [https://www.lemonde.fr/economie/article/2022/03/01/en-difficulte-sigfox-attire-de-multiples-pretendants\\_6115682\\_3234.html](https://www.lemonde.fr/economie/article/2022/03/01/en-difficulte-sigfox-attire-de-multiples-pretendants_6115682_3234.html).
- [38] Le MONDE. *Reprise de Sigfox : Unabiz favori, Ludovic Le Moan jette l’éponge*. consulté le 26 décembre 2022. 2022. URL : <https://toulouse.latribune.fr/entreprises/2022-04-06/reprise-de-sigfox-unabiz-favori-ludovic-le-moan-jette-l-eponge-912992.html>.
- [39] IOTGLOBALNETWORK.COM. *Weightless*. consulté le 26 décembre 2022. URL : <https://www.iotglobalnetwork.com/companies/single/id/954/weightless>.
- [40] IOTGLOBALNETWORK.COM. *Weightless-P*. consulté le 26 décembre 2022. URL : <https://www.iotglobalnetwork.com/products/single/id/914/weightless-p#description>.
- [41] LINK-LABS.COM. *What Is Weightless ?* consulté le 26 décembre 2022. URL : <https://www.link-labs.com/blog/what-is-weightless>.
- [42] LINK-LABS.COM. *L’internet des objets prend son envol avec une première puce “Weightless” ?* consulté le 26 décembre 2022. URL : <https://www.silicon.fr/linternet-des-objets-prend-son-envol-avec-une-premiere-puce-weightless-84126.html>.

- [43] M. KANJ, V. SAVAUX et M. Le GUEN. « A Tutorial on NB-IoT Physical Layer Design ». In : *IEEE Communications Surveys & Tutorials* 22.4 (2020), p. 2408-2446. DOI : 10.1109/COMST.2020.3022751.
- [44] JOURNAL DU NET. *LTE-M : les caractéristiques du réseau*. consulté le 26 décembre 2022. URL : <https://www.journaldunet.fr/web-tech/dictionnaire-de-l-iot/1440680-lte-m-les-caracteristiques-du-reseau-20220923/>.
- [45] O. SELLER et N. SORNIN. *Low power long range transmitter*. Mai 2013.
- [46] LORA ALLIANCE. *LoRa Alliance – Member Directory*. consulté le 26 décembre 2022. URL : [https://lora-alliance.org/member-directory/?sf\\_paged=1](https://lora-alliance.org/member-directory/?sf_paged=1).
- [47] NORDIC SEMICONDUCTOR. *Low power cellular IoT – Enabling a world of everything connected*. consulté le 27 décembre 2022. URL : <https://www.nordicsemi.com/Products/Low-power-cellular-IoT>.
- [48] AMAZON. *SX1276 V2 Lora ESP32*. consulté le 28 décembre 2022. URL : [https://www.amazon.fr/SX1276-dual-core-Bluetooth-Development-Arduino/dp/B078M74MNN/ref=sr\\_1\\_1?\\_\\_mk\\_fr\\_FR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=DFFU4Q6XPVDB&keywords=sx1276&qid=1672224806&sprefix=sx1276%2Caps%2C77&sr=8-1](https://www.amazon.fr/SX1276-dual-core-Bluetooth-Development-Arduino/dp/B078M74MNN/ref=sr_1_1?__mk_fr_FR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=DFFU4Q6XPVDB&keywords=sx1276&qid=1672224806&sprefix=sx1276%2Caps%2C77&sr=8-1).
- [49] KERLINK. *Station Wirnet outdoor LoRaWAN*. consulté le 28 décembre 2022. URL : <https://www.kerlink.fr/solutions-iot/gateways-iot/stations-wirnet-outdoor-lorawan/>.
- [50] ATIM. *Modules Radio & Interfaces*. consulté le 28 décembre 2022. URL : <https://www.atim.com/modules-radio-interfaces/>.
- [51] UBIDREAMS. *Internet des Objets (IOT)*. consulté le 28 décembre 2022. URL : <https://ubidreams.fr/expertises/internet-of-things/>.
- [52] ORANGE BUSINESS SERVICES. *Starter Kit LoRa*. consulté le 28 décembre 2022. URL : <https://developer.orange.com/apis/starter-kit-lora/>.
- [53] ORANGE BUSINESS SERVICES. *Couverture LoRa® Orange*. consulté le 28 décembre 2022. URL : <https://www.orange-business.com/fr/reseau-iot/>.
- [54] A. GEHANI et al. « Application of 915 MHz Band LoRa for Agro-Informatics ». In : *2021 Wireless Telecommunications Symposium (WTS)*. 2021, p. 1-4. DOI : 10.1109/WTS51064.2021.9433712.
- [55] S. OPIPAH et al. « Prototype Design of Smart Home System Base on LoRa ». In : *2020 6th International Conference on Wireless and Telematics (ICWT)*. 2020, p. 1-5. DOI : 10.1109/ICWT50448.2020.9243643.
- [56] S. OD, H-H. HUANG et J-B. WEI. « Apply LoRa Technology to Construct an Air Quality Monitoring IoT System ». In : *2021 IEEE 3rd Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS)*. 2021, p. 88-91. DOI : 10.1109/ECBIOS51820.2021.9510979.
- [57] S. MONTAGNY, UNIVERSITÉ SAVOIE MONT BLANC. *LoRa – LoRaWAN et l’Internet des Objets*. consulté le 30 décembre 2022. URL : <https://www.univ-smb.fr/lorawan/wp-content/uploads/2022/01/Livre-LoRa-LoRaWAN-et-l-Internet-des-Objets.pdf>.

- [58] LORA ALLIANCE. *LoRaWAN® Specification v1.0.3*. consulté le 30 décembre 2022. URL : [https://lora-alliance.org/resource\\_hub/lorawan-specification-v1-0-3/](https://lora-alliance.org/resource_hub/lorawan-specification-v1-0-3/).
- [59] SEMTECH. *Reading channel RSSI during a CAD*. 2014.
- [60] LORA ALLIANCE. *LoRaWAN® 1.0.4 Specification Package*. consulté le 30 décembre 2022. URL : [https://lora-alliance.org/resource\\_hub/lorawan-104-specification-package/](https://lora-alliance.org/resource_hub/lorawan-104-specification-package/).
- [61] L. VANGELISTA. « Frequency Shift Chirp Modulation : The LoRa Modulation ». In : *IEEE Signal Processing Letters* 24.12 (déc. 2017), p. 1818-1821. ISSN : 1558-2361. DOI : 10.1109/LSP.2017.2762960.
- [62] V. FIALHO et F. AZEVEDO. « Wireless Communication Based on Chirp Signals for LoRa IoT Devices ». In : *ISEL Academic Journal of Electronics, Telecommunications and Computers* 4.1 (2018).
- [63] D. CROCE et al. « Impact of LoRa Imperfect Orthogonality : Analysis of Link-Level Performance ». In : *IEEE Communications Letters* 22.4 (2018), p. 796-799.
- [64] M. CHIANI et A. ELZANATY. « On the LoRa Modulation for IoT : Waveform Properties and Spectral Analysis ». In : *IEEE Internet of Things Journal* 6.5 (mai 2019), p. 8463-8470.
- [65] A. MARQUET, N. MONTAVONT et G. Z. PAPADOPOULOS. « Investigating Theoretical Performance and Demodulation Techniques for LoRa ». In : *2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*. Juin 2019, p. 1-6. DOI : 10.1109/WoWMoM.2019.8793014.
- [66] G. FERRÉ et A. GIREMUS. « LoRa Physical Layer Principle and Performance Analysis ». In : *2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*. Déc. 2018, p. 65-68. DOI : 10.1109/ICECS.2018.8617880.
- [67] T. ELSHABRAWY et J. ROBERT. « Closed-Form Approximation of LoRa Modulation BER Performance ». In : *IEEE Communications Letters* 22.9 (sept. 2018), p. 1778-1781. ISSN : 2373-7891. DOI : 10.1109/LCOMM.2018.2849718.
- [68] O. AFISIADIS et al. « On the Advantage of Coherent LoRa Detection in the Presence of Interference ». In : *IEEE Internet of Things Journal* 8.14 (2021), p. 11581-11593. DOI : 10.1109/JIOT.2021.3058792.
- [69] Y. GUO et Z. LIU. « Time-Delay-Estimation-Liked Detection Algorithm for LoRa Signals Over Multipath Channels ». In : *IEEE Wireless Communications Letters* 9.7 (2020), p. 1093-1096. DOI : 10.1109/LWC.2020.2981597.
- [70] O. AFISIADIS, A. P. BURG et A. BALATSOUKAS-STIMMING. « Coded LoRa Frame Error Rate Analysis ». In : (nov. 2019). DOI : arXiv:1911.10245.
- [71] G. BARUFFA et al. « Coded LoRa Performance in Wireless Channels ». In : *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. Sept. 2019, p. 1-6. DOI : 10.1109/PIMRC.2019.8904298.
- [72] T. ELSHABRAWY et J. ROBERT. « Evaluation of the BER Performance of LoRa Communication using BICM Decoding ». In : *2019 IEEE 9th International Conference on Consumer Electronics (ICCE-Berlin)*. Sept. 2019, p. 162-167.

- [73] P. EDWARD et al. « Interleaved Chirp Spreading LoRa as a Parallel Network to Enhance LoRa Capacity ». In : *IEEE Internet of Things Journal* 8.5 (2021), p. 3864-3874. DOI : 10.1109/JIOT.2020.3027100.
- [74] P. EDWARD et al. « Practical Performance Evaluation of Multi-User Interleaved Chirp Spreading LoRa Networks ». In : *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. 2021, p. 1-6. DOI : 10.1109/VTC2021-Fall152928.2021.9625473.
- [75] R. GHANAATIAN et al. « Lora Digital Receiver Analysis and Implementation ». In : *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2019, p. 1498-1502. DOI : 10.1109/ICASSP.2019.8683504.
- [76] M. XHONNEUX, D. BOL et J. LOUVEAUX. « A low-complexity synchronization scheme for LoRa end nodes ». In : *ArXiv e-prints* (déc. 2019).
- [77] C. BERNIER, F. DEHMAS et N. DEPARIS. « Low Complexity LoRa Frame Synchronization for Ultra-Low Power Software-Defined Radios ». In : *IEEE Transactions on Communications* (fév. 2020), p. 1-1. ISSN : 1558-0857. DOI : 10.1109/TCOMM.2020.2974464.
- [78] X. TANG et al. « Performance Analysis of LoRa Modulation with Residual Frequency Offset ». In : *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*. Déc. 2018, p. 835-839. DOI : 10.1109/CompComm.2018.8780636.
- [79] J-M. KANG, D-W. LIM et K-M. KANG. « On the LoRa Modulation for IoT : Optimal Preamble Detection and Its Performance Analysis ». In : *IEEE Internet of Things Journal* (2021), p. 1-1. DOI : 10.1109/JIOT.2021.3108139.
- [80] LORA.READTHEDOCS.IO. *LoRa*. consulté le 2 février 2023. URL : <https://lora.readthedocs.io/en/latest/>.
- [81] P. ROBYNS, W. LAMOTTE et W. THENAERS. « A Multi-Channel Software Decoder for the LoRa Modulation Scheme ». In : *IoTBDS* (jan. 2018). DOI : 10.5220/0006668400410051.
- [82] M. KNIGHT. *Reversing LoRa*. GRCon16. 2016.
- [83] J. G. PROAKIS. *Digital Communications 5th Edition*. McGraw Hill, 2007.
- [84] M. KNIGHT et B. SEEBER. « Decoding LoRa : Realizing a Modern LPWAN with SDR ». In : *Proceedings of the 6<sup>th</sup> GNU Radio Conference – GRCon16* (sept. 2016).
- [85] ETTUS RESEARCH. *USRP B200/B210 Bus Series*. consulté le 16 février 2023. URL : [https://www.ettus.com/wp-content/uploads/2019/01/b200-b210\\_spec\\_sheet.pdf](https://www.ettus.com/wp-content/uploads/2019/01/b200-b210_spec_sheet.pdf).
- [86] SEMTECH. *SX1276 LoRa Connect™ 137MHz to 1020MHz Long Range Low Power Transceiver*. consulté le 16 février 2023. 2020. URL : <https://www.semtech.fr/products/wireless-rf/lora-connect/sx1276#documentation>.
- [87] T. AMELOOT et al. « LoRa Signal Synchronization and Detection at Extremely Low Signal-to-Noise Ratios ». In : *IEEE Internet of Things Journal* (2021), p. 1-1. DOI : 10.1109/JIOT.2021.3117039.

- [88] Y. CUI et W. GANG. « A Noniterative Frequency Estimator With Rational Combination of Three Spectrum Lines ». In : *IEEE Transactions on Signal Processing* 59.10 (2011), p. 5065-5070. DOI : 10.1109/TSP.2011.2160257.
- [89] E. JACOBSEN et P. KOOTSOOKOS. « Fast, Accurate Frequency Estimators [DSP Tips & Tricks] ». In : *IEEE Signal Processing Magazine* 24.3 (2007), p. 123-125. DOI : 10.1109/MSP.2007.361611.
- [90] C. Demeslay, P. Rostaing et R. Gautier. « Theoretical Performance of LoRa System in Multi-Path and Interference Channels ». In : *IEEE Internet of Things Journal* (2021), p. 6830-6843. DOI : 10.1109/JIOT.2021.3114439.
- [91] W. H. PRESS et al. *Numerical Recipes in C : The Art of Scientific Computing*. Cambridge University Press, oct. 1992. ISBN : 0521431085.
- [92] C. Demeslay, P. Rostaing et R. Gautier. « Simple and Efficient LoRa Receiver Scheme for Multi-Path Channel ». In : *IEEE Internet of Things Journal* (2022), p. 15771-15785. DOI : 10.1109/JIOT.2022.3151257.
- [93] C. Demeslay, P. Rostaing et R. Gautier. « A RAKE-like coherent LoRa receiver for Non-Aligned Multi-Path Channels ». In : *IEEE Transactions on Wireless Communications* (manuscrit soumis, en attente de la décision de la revue).
- [94] *Digital land mobile radio communications – COST 207*. Office for Official Publications of the European Communities, avr. 1990. ISBN : 92-825-9946-6.
- [95] R. PRICE et P. E. GREEN. « A Communication Technique for Multipath Channels ». In : *Proceedings of the IRE* 46.3 (1958), p. 555-570. DOI : 10.1109/JRPROC.1958.286870.
- [96] C. Demeslay et al. « Band & Tone Jamming Analysis and Detection on LoRa signals ». In : *SPI 2021* (2021). arXiv : 2107.07782 [eess.SP].
- [97] C. Demeslay et al. « A Novel Scheme for Discrete and Secure LoRa Communications ». In : *MDPI Sensors, Physical Layer Security Special Issue* 22.20 (2022), p. 7947. DOI : 10.3390/s.22207947.
- [98] C. Demeslay et al. « A PAPR Reduction Scheme for LoRa Self-Jamming Waveform ». In : *IEEE Internet of Things Journal* (manuscrit soumis, en attente de la décision de la revue).
- [99] A. D. WYNER. « The wire-tap channel ». In : *The Bell System Technical Journal* 54.8 (1975), p. 1355-1387. DOI : 10.1002/j.1538-7305.1975.tb02040.x.
- [100] A. A. KHISTI et G. W. WORNELL. « Secure Transmission With Multiple Antennas I : The MISOME Wiretap Channel ». In : *IEEE Transactions on Information Theory* 56.7 (2010), p. 3088-3104. DOI : 10.1109/TIT.2010.2048445.
- [101] A. A. KHISTI et G. W. WORNELL. « Secure Transmission With Multiple Antennas—Part II : The MIMOME Wiretap Channel ». In : *IEEE Transactions on Information Theory* 56.11 (2010), p. 5515-5532. DOI : 10.1109/TIT.2010.2068852.
- [102] F. OGGIER et B. HASSIBI. « The Secrecy Capacity of the MIMO Wiretap Channel ». In : *IEEE Transactions on Information Theory* 57.8 (2011), p. 4961-4972. DOI : 10.1109/TIT.2011.2158487.

- [103] R. NEGI et S. GOEL. « Secret communication using artificial noise ». In : *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005*. T. 3. 2005, p. 1906-1910. DOI : 10.1109/VETEFC.2005.1558439.
- [104] X. ZHOU et M. R. MCKAY. « Secure Transmission With Artificial Noise Over Fading Channels : Achievable Rate and Optimal Power Allocation ». In : *IEEE Transactions on Vehicular Technology* 59.8 (2010), p. 3831-3842. DOI : 10.1109/TVT.2010.2059057.
- [105] Y. GU et al. « The Secrecy Capacity Optimization Artificial Noise : A New Type of Artificial Noise for Secure Communication in MIMO System ». In : *IEEE Access* 7 (2019), p. 58353-58360. DOI : 10.1109/ACCESS.2019.2905764.
- [106] D. HE et al. « Secure Communication with Wireless Powered Friendly Jammers under Multiple Eavesdroppers ». In : *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. 2019, p. 1-5. DOI : 10.1109/VTCSpring.2019.8746423.
- [107] W. LIU et al. « Secure Communication With a Wireless-Powered Friendly Jammer ». In : *IEEE Transactions on Wireless Communications* 15.1 (2016), p. 401-415. DOI : 10.1109/TWC.2015.2474378.
- [108] X. CHEN et al. « Large-Scale MIMO Relaying Techniques for Physical Layer Security : AF or DF? ». In : *IEEE Transactions on Wireless Communications* 14.9 (2015), p. 5135-5146. DOI : 10.1109/TWC.2015.2433291.
- [109] K. JAYASINGHEAND et al. « Secure Beamforming Design for Physical Layer Network Coding Based MIMO Two-Way Relaying ». In : *IEEE Communications Letters* 18.7 (2014), p. 1270-1273. DOI : 10.1109/LCOMM.2014.2325861.
- [110] Z. LI et S. HAN. « Research on Physical Layer Security of MIMO Two-way Relay System ». In : *ICC 2022 - IEEE International Conference on Communications*. 2022, p. 3311-3316. DOI : 10.1109/ICC45855.2022.9838316.
- [111] B. FANG et al. « Precoder design for secrecy rate maximization in the DF-based MIMO relay networks ». In : *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*. 2015, p. 1-5. DOI : 10.1109/WCSP.2015.7341097.
- [112] D. KIM, H. LEE et D. HONG. « A Survey of In-Band Full-Duplex Transmission : From the Perspective of PHY and MAC Layers ». In : *IEEE Communications Surveys & Tutorials* 17.4 (2015), p. 2017-2046. DOI : 10.1109/COMST.2015.2403614.
- [113] Y. SUN et al. « Multi-Objective Optimization for Robust Power Efficient and Secure Full-Duplex Wireless Communication Systems ». In : *IEEE Transactions on Wireless Communications* 15.8 (2016), p. 5511-5526. DOI : 10.1109/TWC.2016.2560815.
- [114] F. ZHU et al. « Physical-Layer Security for Full Duplex Communications With Self-Interference Mitigation ». In : *IEEE Transactions on Wireless Communications* 15.1 (2016), p. 329-340. DOI : 10.1109/TWC.2015.2472527.
- [115] S. ZHAO et al. « Secure Beamforming for Full-Duplex MIMO Two-Way Untrusted Relay Systems ». In : *IEEE Transactions on Information Forensics and Security* 15 (2020), p. 3775-3790. DOI : 10.1109/TIFS.2020.3001733.

- [116] JAMMERSPRO. *Portable 10 Bands Jammer PRO10*. consulté le 3 septembre 2023. URL : <https://jammerspro.com/product/portable-10-bands-jammer/>.
- [117] R. POISEL. *Modern Communications Jamming Principles and Techniques, Second Edition*. Artech House, 2011.
- [118] D. S. BERGER et al. « Friendly Jamming on Access Points : Analysis and Real-World Measurements ». In : *IEEE Transactions on Wireless Communications* 15.9 (2016), p. 6189-6202. DOI : 10.1109/TWC.2016.2581165.
- [119] T. LI, T. SONG et Y. LIANG. *Wireless Communications under Hostile Jamming : Security and Efficiency*. Springer, jan. 2018. ISBN : 978-981-13-0820-8. DOI : 10.1007/978-981-13-0821-5.
- [120] H. PIRAYESH et H. ZENG. « Jamming Attacks and Anti-Jamming Strategies in Wireless Networks : A Comprehensive Survey ». In : *IEEE Communications Surveys & Tutorials* 24.2 (2022), p. 767-809. DOI : 10.1109/COMST.2022.3159185.
- [121] L. ZHANG, H. WANG et T. LI. « Anti-Jamming Message-Driven Frequency Hopping—Part I : System Design ». In : *IEEE Transactions on Wireless Communications* 12.1 (2013), p. 70-79. DOI : 10.1109/TWC.2012.120312.111706.
- [122] L. ZHANG et T. LI. « Anti-Jamming Message-Driven Frequency Hopping—Part II : Capacity Analysis Under Disguised Jamming ». In : *IEEE Transactions on Wireless Communications* 12.1 (2013), p. 80-88. DOI : 10.1109/TWC.2012.120312.111707.
- [123] H. JUNG et al. « Design of Anti-Jamming Waveforms for Time-Hopping Spread Spectrum Systems in Tone Jamming Environments ». In : *IEEE Transactions on Vehicular Technology* 69.1 (2020), p. 728-737. DOI : 10.1109/TVT.2019.2954070.
- [124] S. SODAGARI et T. Charmes CLANCY. « Efficient jamming attacks on MIMO channels ». In : *2012 IEEE International Conference on Communications (ICC)*. 2012, p. 852-856. DOI : 10.1109/ICC.2012.6364173.
- [125] P. CUCCARO et G. ROMANO. « Non Uniform Power Allocation Pilot Tone Jamming in OFDM Systems ». In : *2017 40th International Conference on Telecommunications and Signal Processing (TSP)*. 2017, p. 152-155. DOI : 10.1109/TSP.2017.8075957.
- [126] Q. LIU et al. « Disrupting MIMO Communications With Optimal Jamming Signal Design ». In : *IEEE Transactions on Wireless Communications* 14.10 (2015), p. 5313-5325. DOI : 10.1109/TWC.2015.2436385.
- [127] Q. SHI et al. « A novel jamming method against LFM radar using pseudo-random code phase modulation ». In : *2017 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*. 2017, p. 1-5. DOI : 10.1109/ICSPCC.2017.8242394.
- [128] W. WANG et J. CAI. « A Technique for Jamming Bi- and Multistatic SAR Systems ». In : *IEEE Geoscience and Remote Sensing Letters* 4.1 (2007), p. 80-82. DOI : 10.1109/LGRS.2006.886036.
- [129] Y. YANG, W-M. ZHANG et J-H. YANG. « Study on frequency-shifting jamming to linear frequency modulation pulse compression radars ». In : *2009 International Conference on Wireless Communications & Signal Processing*. 2009, p. 1-5. DOI : 10.1109/WCSP.2009.5371387.

- [130] Q. SHI et al. « A novel deceptive and blanket joint jammer ». In : *2017 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*. 2017, p. 1-4. DOI : 10.1109/ICSPCC.2017.8242393.
- [131] H. HUI et W. NA. « A study of GPS jamming and anti-jamming ». In : *2009 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS)*. T. 1. 2009, p. 388-391. DOI : 10.1109/PEITS.2009.5406988.
- [132] E. ELEZI et al. « The effect of Electronic Jammers on GPS Signals ». In : *2019 16th International Multi-Conference on Systems, Signals & Devices (SSD)*. 2019, p. 652-656. DOI : 10.1109/SSD.2019.8893239.
- [133] X. LIAO et W. ZHANG. « A Novel Method for GPS Anti-jamming Based on Blind Source Separation ». In : *2014 Seventh International Symposium on Computational Intelligence and Design*. T. 2. 2014, p. 208-211. DOI : 10.1109/ISCID.2014.130.
- [134] S. S. OZDEMIR et E. AKSOY. « GPS jamming mitigation through Taguchi's optimization method ». In : *2017 25th Telecommunication Forum (TELFOR)*. 2017, p. 1-4. DOI : 10.1109/TELFOR.2017.8249308.
- [135] Y. D. ZHANG et M. G. AMIN. « Anti-Jamming GPS Receiver With Reduced Phase Distortions ». In : *IEEE Signal Processing Letters* 19.10 (2012), p. 635-638. DOI : 10.1109/LSP.2012.2209873.
- [136] L. PING et al. « Adaptive anti-jamming algorithm based on the characteristics of the GPS signal ». In : *2007 International Symposium on Intelligent Signal Processing and Communication Systems*. 2007, p. 192-195. DOI : 10.1109/ISPACS.2007.4445856.
- [137] L. YUN-KYUNG et al. « User authentication mechanism using authentication server in home network ». In : *2006 8th International Conference Advanced Communication Technology*. T. 1. 2006, 4 pp.-506. DOI : 10.1109/ICACT.2006.206017.
- [138] S. GUO et al. « Trust access authentication in vehicular network based on blockchain ». In : *China Communications* 16.6 (2019), p. 18-30. DOI : 10.23919/JCC.2019.06.002.
- [139] K. CHAUDHARY et G. SHINDE. « Survey on group authentication in wireless sensor networks ». In : *2015 International Conference on Pervasive Computing (ICPC)*. 2015, p. 1-5. DOI : 10.1109/PERVASIVE.2015.7087199.
- [140] Y. LI et X. QIN. « A survey of specific emitter identification ». In : *The International Conference on Forthcoming Networks and Sustainability (FoNeS 2022)*. T. 2022. 2022, p. 783-788. DOI : 10.1049/icp.2022.2552.
- [141] Y. LI et L. WANG. « A survey of radio frequency fingerprint feature extraction and recognition based on deep learning ». In : *The International Conference on Forthcoming Networks and Sustainability (FoNeS 2022)*. T. 2022. 2022, p. 776-782. DOI : 10.1049/icp.2022.2551.
- [142] D. LIU, M. WANG et H. WANG. « RF Fingerprint Recognition Based On Spectrum Waterfall Diagram ». In : *2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*. 2021, p. 613-616. DOI : 10.1109/ICCWAMTIP53232.2021.9674155.



- [143] Q. WANG et al. « Novel Multiwavelet-based LPC Random Forest Classifier for Bluetooth RF-Fingerprint Identification ». In : *2022 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*. 2022, p. 1-6. DOI : 10.1109/BMSB55706.2022.9828678.
- [144] J. McMILLEN, G. MUMCU et Y. YILMAZ. « Deep Learning-based RF Fingerprint Authentication with Chaotic Antenna Arrays ». In : *2023 IEEE Wireless and Microwave Technology Conference (WAMICON)*. 2023, p. 121-124. DOI : 10.1109/WAMICON57636.2023.10124899.
- [145] M. AZARMEHR, A. MEHTA et R. RASHIDZADEH. « Wireless device identification using oscillator control voltage as RF fingerprint ». In : *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*. 2017, p. 1-4. DOI : 10.1109/CCECE.2017.7946820.
- [146] M. SCHWARTZ, W.R BENETT et S. STEIN. *Communication Systems and Techniques*. New York :McGraw Hill, 1966.
- [147] J. HU et N. C. BEAULIEU. « Accurate simple closed-form approximations to the distributions and densities of a sum of independent Rayleigh random variables ». In : *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004*. T. 1. 2004, 1092-1095 Vol.1. DOI : 10.1109/ACSSC.2004.1399309.
- [148] J. HU et N. C. BEAULIEU. « Accurate closed-form approximations to Ricean sum distributions and densities ». In : *IEEE Communications Letters* 9.2 (2005), p. 133-135. DOI : 10.1109/LCOMM.2005.02029.
- [149] J. A. LOPEZ-SALCEDO. « Simple Closed-Form Approximation to Ricean Sum Distributions ». In : *IEEE Signal Processing Letters* 16.3 (2009), p. 153-155. DOI : 10.1109/LSP.2008.2012223.
- [150] H. CHIN-YA et al. « Experimental Evaluation of Jamming Threat in LoRaWAN ». In : *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. 2019, p. 1-6. DOI : 10.1109/VTCSpring.2019.8746374.
- [151] E. ARAS et al. « Selective Jamming of LoRaWAN Using Commodity Hardware ». In : *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems : Computing, Networking and Services*. MobiQuitous 2017. Melbourne, VIC, Australia : Association for Computing Machinery, 2017, p. 363-372. ISBN : 9781450353687. DOI : 10.1145/3144457.3144478.
- [152] T. PERKOVIĆ et al. « Low-Cost Implementation of Reactive Jammer on LoRaWAN Network ». In : *Electronics* 10 (avr. 2021), p. 864. DOI : 10.3390/electronics10070864.
- [153] N. HOU, X. XIA et Y. ZHENG. « Jamming of LoRa PHY and Countermeasure ». In : *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*. 2021, p. 1-10. DOI : 10.1109/INFOCOM42981.2021.9488774.
- [154] S. M. DANISH et al. « Network Intrusion Detection System for Jamming Attack in LoRaWAN Join Procedure ». In : *2018 IEEE International Conference on Communications (ICC)*. 2018, p. 1-6. DOI : 10.1109/ICC.2018.8422721.

- [155] A-U-H. AHMAR et al. « CRAM : Robust Medium Access Control for LPWAN using Cryptographic Frequency Hopping ». In : *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. 2020, p. 95-102. DOI : 10.1109/DCOSS49796.2020.00026.
- [156] C. ZHANG et al. « A Novel Physical Layer Encryption Algorithm for LoRa ». In : *IEEE Communications Letters* 25.8 (2021), p. 2512-2516. DOI : 10.1109/LCOMM.2021.3078669.
- [157] H. JAVED, M. R. KHALID et M. S. IQBAL. « A Robust Semi-Blind Approach for Scramble Code Estimation in Non-Cooperative Interception of a Scrambled DSSS Signal ». In : *2020 17th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*. 2020, p. 637-641. DOI : 10.1109/IBCAST47879.2020.9044488.
- [158] H. WANG et al. « Image Encryption Algorithm Based on Double Scrambling ». In : *2019 IEEE International Conference on Mechatronics and Automation (ICMA)*. 2019, p. 2201-2205. DOI : 10.1109/ICMA.2019.8816275.
- [159] M. A. TOUIL et N. ELLOUZE. « Scrambling high dynamic range videos : Scrambling HDR videos ». In : *2016 Future Technologies Conference (FTC)*. 2016, p. 923-925. DOI : 10.1109/FTC.2016.7821713.
- [160] P. THAENKAEW, B. QUOITIN et A. MEDDAHI. « Evaluating the cost of beyond AES-128 LoRaWAN security ». In : *2022 International Symposium on Networks, Computers and Communications (ISNCC)*. 2022, p. 1-6. DOI : 10.1109/ISNCC55209.2022.9851811.
- [161] K-L. TSAI et al. « Low-Power AES Data Encryption Architecture for a LoRaWAN ». In : *IEEE Access* 7 (2019), p. 146348-146357. DOI : 10.1109/ACCESS.2019.2941972.
- [162] J. ZHANG et al. « Key Generation From Wireless Channels : A Review ». In : *IEEE Access* 4 (2016), p. 614-626. DOI : 10.1109/ACCESS.2016.2521718.
- [163] K. REN, H. SU et Q. WANG. « Secret key generation exploiting channel characteristics in wireless communications ». In : *IEEE Wireless Communications* 18.4 (2011), p. 6-12. DOI : 10.1109/MWC.2011.5999759.
- [164] S. MATHUR et al. « Radio-telepathy : Extracting a secret key from an unauthenticated wireless channel ». In : *Proc. 14th Annu. Intl. Conf. Mobile Comput. Netw. (MobiCom)* (sept. 2008), p. 128-139.
- [165] S. N. PREMNATH et al. « Secret Key Extraction from Wireless Signal Strength in Real Environments ». In : *IEEE Transactions on Mobile Computing* 12.5 (2013), p. 917-930. DOI : 10.1109/TMC.2012.63.
- [166] Y. EL HAJJ SHEHADEH et al. « Intelligent mechanisms for key generation from multipath wireless channels ». In : *2011 Wireless Telecommunications Symposium (WTS)*. 2011, p. 1-6. DOI : 10.1109/WTS.2011.5960848.
- [167] Q. WANG et al. « Fast and scalable secret key generation exploiting channel phase randomness in wireless networks ». In : *2011 Proceedings IEEE INFOCOM*. 2011, p. 1422-1430. DOI : 10.1109/INFCOM.2011.5934929.

- [168] S. MATHUR et al. « ProxiMate : Proximity-Based Secure Pairing Using Ambient Wireless Signals ». In : *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*. MobiSys '11. Bethesda, Maryland, USA : Association for Computing Machinery, 2011, p. 211-224. ISBN : 9781450306430. DOI : 10.1145/1999995.2000016.
- [169] Q. WANG, K. XU et K. REN. « Cooperative Secret Key Generation from Phase Estimation in Narrowband Fading Channels ». In : *IEEE Journal on Selected Areas in Communications* 30.9 (2012), p. 1666-1674. DOI : 10.1109/JSAC.2012.121010.
- [170] Y. RAHMATALLAH et S. MOHAN. « Peak-To-Average Power Ratio Reduction in OFDM Systems : A Survey And Taxonomy ». In : *IEEE Communications Surveys & Tutorials* 15.4 (2013), p. 1567-1592. DOI : 10.1109/SURV.2013.021313.00164.
- [171] H. OCHIAI et H. IMAI. « Performance analysis of deliberately clipped OFDM signals ». In : *IEEE Transactions on Communications* 50.1 (2002), p. 89-101. DOI : 10.1109/26.975762.
- [172] K. R. PANTA et J. ARMSTRONG. « Effects of clipping on the error performance of OFDM in frequency selective fading channels ». In : *IEEE Transactions on Wireless Communications* 3.2 (2004), p. 668-671. DOI : 10.1109/TWC.2003.821142.
- [173] G. CHEN, R. ANSARI et Y. YAO. « Improved Peak Windowing for PAPR Reduction in OFDM ». In : *VTC Spring 2009 - IEEE 69th Vehicular Technology Conference*. 2009, p. 1-5. DOI : 10.1109/VETECS.2009.5073593.
- [174] S. CHA et al. « A new PAPR reduction technique for OFDM systems using advanced peak windowing method ». In : *IEEE Transactions on Consumer Electronics* 54.2 (2008), p. 405-410. DOI : 10.1109/TCE.2008.4560106.
- [175] A. CHIDURALA et P. Hari Krishna PRASAD. « Mu-Law companded PTS for PAPR reduction in OFDM systems ». In : *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. 2015, p. 1-4. DOI : 10.1109/ICECCT.2015.7226139.
- [176] T. G. PRATT et al. « OFDM link performance with companding for PAPR reduction in the presence of non-linear amplification ». In : *IEEE Transactions on Broadcasting* 52.2 (2006), p. 261-267. DOI : 10.1109/TBC.2006.875613.
- [177] H. JUN et al. « Peak-to-Average Power Ratio Reduction of OFDM Signals With Nonlinear Companding Scheme ». In : *IEEE Transactions on Broadcasting* 56.2 (2010), p. 258-262. DOI : 10.1109/TBC.2010.2046970.
- [178] P. O. BORJESSON et al. « DMT PAR-reduction by weighted cancellation waveforms ». In : *Proceedings of Radiovetenskap och kommunikation 99 (KVR 99)* (1999), p. 303-307.
- [179] R. BÄUML, R. F. H. FISCHER et J. B. HUBER. « Reducing the Peak-to-Average Power Ratio of Multicarrier Modulation by Selected Mapping ». In : *IEE Electronics Letters* 32 (1996), p. 2056-2057.

- [180] T. MATA, P. BOONSRIMUANG et P. BOONTRA. « A PAPR Reduction Scheme based on Improved PTS with ABC Algorithm for OFDM Signal ». In : *2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*. 2018, p. 469-472. DOI : 10.1109/ECTICon.2018.8619887.
- [181] A. AGGARWAL et T. H. MENG. « Minimizing the Peak-to-Average Power Ratio of OFDM Signals Using Convex Optimization ». In : *IEEE Transactions on Signal Processing* 54.8 (2006), p. 3099-3110. DOI : 10.1109/TSP.2006.875390.
- [182] B. S. KRONGOLD et D. L. JONES. « PAR reduction in OFDM via active constellation extension ». In : *IEEE Transactions on Broadcasting* 49.3 (2003), p. 258-268. DOI : 10.1109/TBC.2003.817088.
- [183] Y. Z. JIAO, X. J. LIU et X. A. WANG. « A Novel Tone Reservation Scheme with Fast Convergence for PAPR Reduction in OFDM Systems ». In : *2008 5th IEEE Consumer Communications and Networking Conference*. 2008, p. 398-402. DOI : 10.1109/ccnc08.2007.95.
- [184] K. PARK et I-C. PARK. « Low-Complexity Tone Reservation for PAPR Reduction in OFDM Communication Systems ». In : *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 20.10 (2012), p. 1919-1923. DOI : 10.1109/TVLSI.2011.2164104.
- [185] H. BREILING, S. H. MULLER-WEINFURTNER et J. B. HUBER. « SLM peak-power reduction without explicit side information ». In : *IEEE Communications Letters* 5.6 (2001), p. 239-241. DOI : 10.1109/4234.929598.
- [186] H-S. JOO et al. « New PTS Schemes for PAPR Reduction of OFDM Signals Without Side Information ». In : *IEEE Transactions on Broadcasting* 63.3 (2017), p. 562-570. DOI : 10.1109/TBC.2017.2711141.
- [187] ELEKSTORSTORE. *GREAT SCOTT GADGETS HackRF One*. consulté le 23 mai 2023. URL : <https://greatscottgadgets.com/hackrf/one/>.
- [188] ANALOG DEVICES. *Adalm-Pluto Software-Defined Radio Active Learning Module*. consulté le 23 mai 2023. URL : <https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html#eb-overview>.
- [189] ETTUS RESEARCH. *Ettus USRP X410 Specifications*. consulté le 23 mai 2023. URL : <https://www.ni.com/docs/fr-FR/bundle/ettus-usrp-x410-specs/page/specs.html>.
- [190] ETTUS RESEARCH. *USRP B200/B210 Bus Series*. consulté le 23 mai 2023. URL : [https://www.ettus.com/wp-content/uploads/2019/01/b200-b210\\_spec\\_sheet.pdf](https://www.ettus.com/wp-content/uploads/2019/01/b200-b210_spec_sheet.pdf).
- [191] ETTUS RESEARCH. *VERT900 Antenna*. consulté le 23 mai 2023. URL : <https://www.ettus.com/all-products/vert900/>.
- [192] ANALOG DEVICES. *RF Agile Transceiver AD9361 Datasheet*. consulté le 14 juillet 2023. URL : <https://www.analog.com/media/en/technical-documentation/data-sheets/AD9361.pdf>.
- [193] SDR-RADIO.COM. *SDR Console*. consulté le 14 juillet 2023. URL : <https://www.sdr-radio.com/console>.

## Annexes

### A. Estimateur LoRa de la partie fractionnaire CFO

La partie fractionnaire du CFO,  $CFO_{frac}$ , est obtenue par :

$$\widehat{CFO} = \left( \frac{\widehat{v} + k_\alpha}{2N_{up}} \right) \text{ mod } 1 \quad (\text{A.1})$$

avec :

$$k_\alpha = \frac{M}{\pi} \times \frac{Q_+^2 - Q_-^2}{c_0(Q_+^2 - Q_-^2) + c_1 Q^2} \quad (\text{A.2})$$

$$Q_- = \left| \tilde{Y}[(\widehat{v} - 1) \text{ mod } M] \right|, \quad Q = \left| \tilde{Y}[\widehat{v}] \right|, \quad Q_+ = \left| \tilde{Y}[(\widehat{v} + 1) \text{ mod } M] \right| \quad (\text{A.3})$$

$$\widehat{v} = \arg \max_{n'} \left| \tilde{Y}[n'] \right|, \quad n' \in \{0, 1, \dots, (2M \times N_{up}) - 1\} \quad (\text{A.4})$$

$$\tilde{Y}[n'] = \text{DFT}\{p_{pad}[k] \odot x_{0,pad}^*[k]\}[n'] \quad (\text{A.5})$$

$$c_0 = \frac{64 \times M}{\pi^5 + 32\pi}, \quad c_1 = \frac{c_0 \pi^2}{4} \quad (\text{A.6})$$

$p_{pad}[k]$  sont les  $N_{up}$  symboles upchirp du préambule reçus avec ajout de  $M \times N_{up}$  zéros à la fin (*zero-padding*). Le downchirp local  $x_{0,pad}^*[k]$  est dupliqué et concaténé  $N_{down} = N_{up}$  fois et comporte également du zero-padding. Nous notons  $\odot$ , le produit élément par élément, ou produit de Hadamard.

### B. Estimateur LoRa de la partie fractionnaire STO

La partie fractionnaire du STO,  $STO_{frac}$ , est estimée à partir de l'approche TSL (comme l'estimateur  $CFO_{frac}$ , voir Annexe A). Elle est obtenue par :

$$\widehat{STO}_{frac} = -\Re \left\{ \frac{W(-\widehat{STO}_{int})Q_+ - W(\widehat{STO}_{int})Q_-}{2Q - W(-\widehat{STO}_{int})Q_+ - W(\widehat{STO}_{int})Q_-} \right\} \quad (\text{B.7})$$

avec :

$$Q_- = \left\langle \tilde{P}_{up, sync, \widehat{CFO}_{frac}} [(\widehat{a}_{up} - 1) \text{ mod } M] \right\rangle \quad (\text{B.8})$$

$$Q = \left\langle \tilde{P}_{up, sync, \widehat{CFO}_{frac}} [\widehat{a}_{up}] \right\rangle \quad (\text{B.9})$$

$$Q_+ = \left\langle \tilde{P}_{up, sync, \widehat{CFO}_{frac}} [(\widehat{a}_{up} + 1) \text{ mod } M] \right\rangle \quad (\text{B.10})$$

$$W(x) = e^{2j\pi \frac{x}{M}} \quad (\text{B.11})$$

et :

$$\left\langle \tilde{P}_{up, sync, CFO_{frac}}[n] \right\rangle = \frac{1}{N_{up}} \sum_{i=0}^{N_{up}-1} \tilde{R}_{i, sync, CFO_{frac}}[n] \quad (\text{B.12})$$

$$\hat{a}_{up} = \arg \max_n \left| \left\langle \tilde{P}_{up, sync, CFO_{frac}}[n] \right\rangle \right| \quad (\text{B.13})$$

où  $\tilde{R}_{i, sync, CFO_{frac}}[n]$  est la DFT du  $i^{\text{ème}}$  symbole LoRa dans la trame reçue corrigée en  $CFO_{frac}$ .

### C. Expression analytique du SER LoRa dans un canal multi-trajets aligné

Pour ne pas alourdir cette annexe, les développements intermédiaires dans [90] ont été omis. La probabilité d'erreur de démodulation pour le récepteur non-cohérent, notée  $P_{e, NCOH}$ , est donnée par :

$$P_{e, NCOH} = \frac{1}{M} P_{e, NCOH,1} + \frac{M-1}{M} P_{e, NCOH,2} \quad (\text{C.14})$$

avec :

$$P_{e, NCOH,1} = 1 - \prod_{l=1}^{L-1} F_{Rice}(|x|, \beta, M|\alpha_l|) F_{Rice}(|x|, \beta, 0)^{M-L} \quad (\text{C.15})$$

$$P_{e, NCOH,2} = 1 - \prod_{l=1}^{L-1} F_{Rice}(|x|, \beta, (M-k_l)|\alpha_l|) F_{Rice}(|x|, \beta, 0)^{M-L} \quad (\text{C.16})$$

et :

$$x = M + \tilde{W}[a], \quad \beta = \sqrt{\frac{M\sigma^2}{2}} \quad (\text{C.17})$$

$\alpha_l$ , le gain complexe du  $l^{\text{ème}}$  trajet et  $F_{Rice}(x, \beta, \mu)$ , la fonction de répartition de la loi de Rice, de paramètre d'échelle  $\beta$  et de décentrage  $\mu$ .

### D. Expression analytique du SER LoRa avec interférence multi-utilisateurs LoRa

Nous donnons ici les expressions analytiques du SER LoRa avec interférence multi-utilisateurs où deux utilisateurs entrent en collision. De façon similaire à l'expression du SER théorique LoRa pour le canal multi-trajets aligné en Annexe C, et d'après les cinq cas de figure présentés sur les Figures II.1.4 et II.1.5, la probabilité d'erreur (valeur moyenne sur  $a_1$ ,  $a_2^-$  et  $a_2$ ) pour le récepteur non-cohérent peut-être décomposée selon les cinq cas par les équations (D.18), (D.20), (D.24), (D.26) et (D.27). Elle est notée  $P_{e, NCOH, interf, c}(z)$ , avec  $z \in \{0, 1, \dots, M-1\}$ , la désynchronisation temporelle du second utilisateur par rapport au premier en nombre de périodes d'échantillonnage (voir Section II.1.1.2) et  $c$ , le numéro de cas. Les résultats en Figure II.1.9 sont obtenus avec ces expressions, en supposant  $P_1 = 1$  dans l'équation (II.1.14).

Cas 1

$$P_{e,NCOH,interf,1}(z) = \frac{M(M-1)(M-2)}{M^3} \left[ 1 - F_{Rice}(|x_1|, \beta, z\sqrt{P_2}) \times F_{Rice}(|x_1|, \beta, (M-z)\sqrt{P_2}) F_{Rice}(|x_1|, \beta, 0)^{M-3} \right] \quad (D.18)$$

avec :

$$x_1 = M + \tilde{W}[a], \quad \beta = \sqrt{\frac{M\sigma^2}{2}} \quad (D.19)$$

Cas 2

$$P_{e,NCOH,interf,2}(z) = \frac{M-1}{M^3} \left[ b(z) \sum_{a=0}^{M/b(z)-1} \left( 1 - F_{Rice}(|x_2(a, z)|, \beta, z\sqrt{P_2}) F_{Rice}(|x_2(a, z)|, \beta, 0)^{M-2} \right) \right] \quad (D.20)$$

avec :

$$x_2(a, z) = M + (M-z)\sqrt{P_2}\tilde{\alpha}(a, z) + \tilde{W}[a] \quad (D.21)$$

$$\tilde{\alpha}(a, z) = e^{-2j\pi z \frac{(a+z) \bmod M}{M}} e^{2j\pi(M-z)\left[-\frac{1}{2} + \frac{M-z}{2M}\right]} \quad (D.22)$$

$$b(z) = \begin{cases} 2^{\log_2(z)} & \text{si } z \text{ paire} \\ 1 & \text{sinon} \end{cases} \quad (D.23)$$

Cas 3

$$P_{e,NCOH,interf,3}(z) = \frac{M-1}{M^3} \left[ b(z) \sum_{a=0}^{M/b(z)-1} \left( 1 - F_{Rice}(|x_3(a, z)|, \beta, (M-z)\sqrt{P_2}) F_{Rice}(|x_3(a, z)|, \beta, 0)^{M-2} \right) \right] \quad (D.24)$$

avec :

$$x_3(a, z) = M + z\sqrt{P_2}\tilde{\alpha}(a, z) + \tilde{W}[a] \quad (D.25)$$

Cas 4

$$P_{e,NCOH,interf,4}(z) = \frac{M(M-1)}{M^3} \left[ 1 - F_{Rice}(|x_1|, \beta, M\sqrt{P_2}) F_{Rice}(|x_1|, \beta, 0)^{M-2} \right] \quad (D.26)$$

## Cas 5

$$P_{e,NCOH,interf,5}(z) = \frac{1}{M^3} \left[ b(z) \sum_{a=0}^{M/b(z)-1} \left( 1 - F_{Rice}(|x_5(a, z)|, \beta, 0)^{M-1} \right) \right] \quad (D.27)$$

avec :

$$x_5(a, z) = M + M\sqrt{P_2}\tilde{\alpha}(a, z) + \tilde{W}[a] \quad (D.28)$$

Le terme  $b$  dans les équations (D.20), (D.24) et (D.27) vient d'une réduction de complexité pour les cas 2, 3 et 5 où les probabilités pour les valeurs de  $a$  paires et impaires sont en fait identiques. La probabilité finale vaut alors :

$$P_{e,NCOH,interf}(z) = \sum_{i=1}^5 P_{e,NCOH,interf,i}(z) \quad (D.29)$$

## E. Expression analytique de la DFT LoRa dans un canal multi-trajets non-aligné

### Modèle de canal multi-trajets non-aligné

Nous considérons un train de symboles transmis :

$$s[k] = \sum_{i=0}^{S-1} x_{a_i}[k - i \times M] \quad (E.30)$$

avec  $i \in \{0, 1, \dots, S-1\}$ , l'indice de symbole. Le signal reçu est :

$$r[k] = \underbrace{h[k] * s[k]}_{m[k]} + w[k] \quad (E.31)$$

avec  $h[k]$ , le canal multi-trajets non-aligné et  $w[k]$ , la composante de bruit AWGN.  $*$  dénote l'opérateur de convolution discrète. Le signal  $m[k]$  est donc la forme d'onde reçue après passage dans le canal multi-trajets non-aligné. Pour simuler le canal multi-trajets non-aligné, la forme d'onde transmise est sur-échantillonnée par un facteur  $R$ . D'après [64], elle a pour expression :

$$x_a[k'] = e^{2j\pi k' \left[ \frac{a}{M} - \frac{1}{2} + \frac{k'}{2M} - \text{step}[k' - (M-a)] \right]} \quad (E.32)$$

avec :

$$k' = \frac{0, 1, \dots, R \times M - 1}{R} \quad (E.33)$$

$\text{step}[v]$  dénote la fonction échelon et est définie par :

$$\text{step}[v] = \begin{cases} 1 & \text{si } v > 0 \\ 0 & \text{sinon} \end{cases} \quad (E.34)$$



Notons que deux définitions du signal sont présentes : de  $k' = 0$  à  $k' = M - a - 1/R$  et de  $k' = M - a$  à  $k' = M - 1/R$ , dénotées respectivement par  $s_a^{(1)}$  et  $s_a^{(2)}$ .

D'après (E.32), nous pouvons voir qu'en fonction du symbole précédent  $a^-$ , du symbole courant  $a$  et du retard  $k_l$  de la réplique, l'expression sera différente. Nous pouvons décomposer selon les quatre cas suivants :

1.  $k_l < a^-$  and  $k_l < a$
2.  $k_l \geq a^-$  and  $k_l < a$
3.  $k_l < a^-$  and  $k_l \geq a$
4.  $k_l \geq a^-$  and  $k_l \geq a$

La Figure 18 illustre ces quatre cas. Dans la figure, les formes d'onde reçues  $s_{a^-}^{(1)}$ ,  $s_{a^-}^{(2)}$ ,  $s_a^{(1)}$  et  $s_a^{(2)}$  ont une expression continue. Après réception (échantillonnage au temps chirp  $F_s = B$ ), l'indice temporel devient discret mais le retard  $\tau_l$  de la réplique reste continu ( $\tau_l = k_l \times T_s$ ) ayant une partie fractionnaire i.e.  $k_l = k_l^{int} + k_l^{frac}$ .

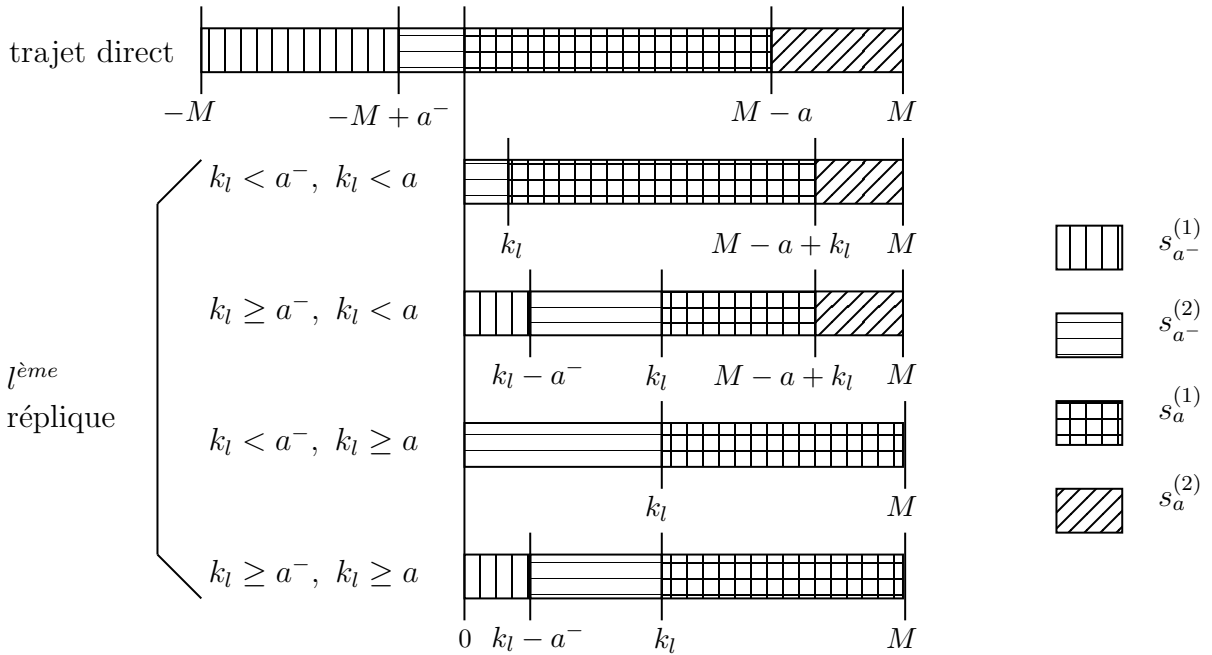


FIGURE 18. – Illustration de l'effet d'un canal multi-trajets non-aligné

### Expression générale de la DFT LoRa dans un canal multi-trajets non-aligné

D'après la Figure 18, l'expression de la DFT LoRa est obtenue par :

$$\tilde{R}[n] = C_0[n; a] + \sum_{l=1}^L \sum_{j=1}^4 1_j[k_l; a^-; a] C_j[n; k_l; a^-; a] + \tilde{W}[n] \quad (\text{E.35})$$

avec les termes  $C_j$  développés dans les équations (E.36), (E.37), (E.38), (E.39), (E.40) (en utilisant les équations (E.41) et (E.42)) pour le trajet direct et les cas 1), 2), 3) et

4), respectivement. La fonction indicateur  $1_j[k_l; a^-; a]$  dans l'équation (E.35) retourne 1 si le cas  $j$  est valide ( $j \in \{1, 2, 3, 4\}$ ) pour  $k_l$ ,  $a^-$  et  $a$  donnés, et 0 sinon.

$$C_0[n; a] = M_0^{(1)}[n; 0; M - a - 1; a] + M_0^{(2)}[n; M - a; M - 1; a] \quad (\text{E.36})$$

$$C_1[n; k_l; a^-; a] = M_l^{(2)}[n; 0; k_l^{int}; a^-]e^{-2j\pi k_l^{frac}} + M_l^{(1)}[n; k_l^{int} + 1; M - a + k_l^{int}; a] \quad (\text{E.37})$$

$$+ M_l^{(2)}[n; M - a + k_l^{int} + 1; M - 1; a]$$

$$C_2[n; k_l; a^-; a] = M_l^{(1)}[n; 0; k_l^{int} - a^-; a^-]e^{-2j\pi k_l^{frac}} + M_l^{(2)}[n; k_l^{int} - a^- + 1; k_l^{int}; a^-] \quad (\text{E.38})$$

$$+ M_l^{(1)}[n; k_l^{int} + 1; M - a + k_l^{int}; a] + M_l^{(2)}[n; M - a + k_l^{int} + 1; M - 1; a]$$

$$C_3[n; k_l; a^-; a] = M_l^{(2)}[n; 0; k_l^{int}; a^-]e^{-2j\pi k_l^{frac}} + M_l^{(1)}[n; k_l^{int} + 1; M - 1; a] \quad (\text{E.39})$$

$$C_4[n; k_l; a^-; a] = M_l^{(1)}[n; 0; k_l^{int} - a^-; a^-]e^{-2j\pi k_l^{frac}} + M_l^{(2)}[n; k_l^{int} - a^- + 1; k_l^{int}; a^-] \quad (\text{E.40})$$

$$+ M_l^{(1)}[n; k_l^{int} + 1; M - 1; a]$$

avec :

$$M_l^{(1)}[n; b_0; b_1; a] = \tilde{\rho}_l[a] \sum_{k=b_0}^{b_1} e^{2j\pi \frac{k}{M}[a-k_l-n]}, \quad M_l^{(2)}[n; b_0; b_1; a] = \tilde{\rho}_l[a] e^{2j\pi k_l} \sum_{k=b_0}^{b_1} e^{2j\pi \frac{k}{M}[a-M-k_l-n]} \quad (\text{E.41})$$

et :

$$\tilde{\rho}_l[a] = \tilde{\rho}_l e^{-2j\pi k_l \frac{a}{M}} \quad (\text{E.42})$$

$$\tilde{\rho}_l = \alpha_l e^{-2j\pi k_l \left[-\frac{1}{2} - \frac{k_l}{2M}\right]} \quad (\text{E.43})$$

## Expression de la DFT LoRa dans un canal multi-trajets non-aligné à deux trajets

Sans perte de généralité, nous considérons uniquement le cas 1). En effet, ce dernier a une probabilité d'occurrence très élevée  $p = 1 - 2/M + 1/M^2$ , valant  $p \approx 0.9844$  pour  $k_1 < 1$  et  $SF = 7$  par exemple. Nous séparons le cas 1) en trois sous-cas :  $k_1 = 0$ ,  $0 < k_1 < 1$  et  $k_1 = 1$ , et calculons les expressions simplifiées de la DFT LoRa au bin d'intérêt  $n = a$  et son voisin gauche en  $n = (a - 1) \bmod M$ . Chaque expression est valable pour le couple  $(a^-, a) \in \{1, 2, \dots, M - 1\}^2$  comme nous sommes dans le cas 1). En développant l'équation (E.35) avec les équations (E.36) et (E.37), nous obtenons :

- $k_1 = 0$  :

$$\tilde{R}[a] = M (1 + |\alpha_1| e^{j\pi \Delta_\phi}), \quad \tilde{R}[(a - 1) \bmod M] = 0 \quad (\text{E.44})$$

Dans ce cas, la réplique est parfaitement superposée sur le trajet direct. Ainsi, l'expression ne dépend plus du symbole courant  $a$ .

- $0 < k_1 < 1$  :

$$\tilde{R}[a] = M + \tilde{\rho}_1 \left[ e^{-2j\pi k_1 \frac{a^-}{M}} + e^{-2j\pi k_1 \frac{a}{M}} \times \left( \sum_{k=1}^{M-a} e^{-2j\pi \frac{k}{M} k_1} + e^{2j\pi k_1} \sum_{k=M-a+1}^{M-1} e^{-2j\pi \frac{k}{M} k_1} \right) \right] \quad (\text{E.45})$$

et :

$$\begin{aligned} \tilde{R}[(a-1) \bmod M] &= \tilde{\rho}_1 \left[ e^{-2j\pi k_1 \frac{a^-}{M}} + e^{-2j\pi k_1 \frac{a}{M}} \times \right. \\ &\left. \left( \sum_{k=1}^{M-a} e^{2j\pi \frac{k}{M} [-k_1+1]} + e^{2j\pi k_1} \sum_{k=M-a+1}^{M-1} e^{2j\pi \frac{k}{M} [-k_1+1]} \right) \right] \end{aligned} \quad (\text{E.46})$$

- $k_1 = 1$  :

$$\tilde{R}[a] = M + \tilde{\rho}_1 \left[ e^{-2j\pi \frac{a^-}{M}} - e^{-2j\pi \frac{a}{M}} \right] \quad (\text{E.47})$$

et :

$$\tilde{R}[(a-1) \bmod M] = \tilde{\rho}_1 \left[ e^{-2j\pi \frac{a^-}{M}} + (M-1)e^{-2j\pi \frac{a}{M}} \right] \quad (\text{E.48})$$

### Expression de la DFT LoRa dans un canal multi-trajets non-aligné à deux trajets avec $a^- = a = 0$

Si nous considérons la DFT LoRa reçue au niveau du préambule ( $a^- = a = 0$ ), nous nous retrouvons alors dans le cas 4). De même, nous décomposons ce cas en deux sous-cas  $0 < k_1 < 1$  et  $k_1 = 1$  :

- $0 < k_1 < 1$  :

$$\tilde{R}[0] = M + \tilde{\rho}_1 \left[ e^{-2j\pi k_1} + \sum_{k=1}^{M-1} e^{-2j\pi \frac{k}{M} k_1} \right] \quad (\text{E.49})$$

$$\tilde{R}[M-1] = \tilde{\rho}_1 \left[ e^{-2j\pi k_1} + \sum_{k=1}^{M-1} e^{2j\pi \frac{k}{M} [-k_1+1]} \right] \quad (\text{E.50})$$

- $k_1 = 1$  :

$$\tilde{R}[0] = M, \quad \tilde{R}[M-1] = M\tilde{\rho}_1 \quad (\text{E.51})$$



**Titre :** Contributions pour le standard IoT LoRa : améliorations du récepteur classique et de sa sécurisation

**Mot clés :** IoT, LoRa, sécurisation couche physique, brouillage, canaux multi-trajets, PAPR

**Résumé :** Cette thèse a pour objectif de proposer des améliorations pour le standard de l'Internet des Objets (IoT) LoRa selon deux axes : 1) la modification du récepteur classique pour améliorer les performances de démodulation en présence d'un canal multi-trajets et 2) proposer une sécurisation de la couche physique pour renforcer la confidentialité des transmissions. Pour le premier axe, une étude de l'impact des canaux multi-trajets est proposée et débouche sur le calcul de l'expression analytique du taux d'erreur symbole LoRa. Fort de cette étude, le récepteur amélioré LoRa RAKE exploitant de façon constructive l'énergie des trajets est conçu et évalué pour le scénario réaliste d'un canal multi-trajets à répliques proches du tra-

jet direct avec prise en compte de la synchronisation. Pour le second axe, une étude de l'impact des brouilleurs classiques Band et Tone Jamming est réalisée et montre les performances sous-optimales de ces brouilleurs. Ainsi, un schéma d'auto-brouillage de la forme d'onde LoRa est proposé, réduisant fortement les capacités de démodulation des intercepteurs, renforçant ainsi le niveau de confidentialité de la transmission. Le Peak-to-Average Power Ratio (PAPR) généré par ce schéma est étudié et une méthode de réduction de ce dernier est proposée. Enfin, des expérimentations sur des matériels de type Software Defined Radio (SDR) sont menées et démontrent la viabilité du schéma d'auto-brouillage.

**Title:** Contributions to the LoRa IoT standard: enhancements of the conventional receiver and its securing

**Keywords:** IoT, LoRa, physical layer security, jamming, multi-path channels, PAPR

**Abstract:** This thesis aims to propose enhancements for the LoRa Internet of Things (IoT) standard in order to 1) improve the demodulation performances in the presence of multi-path channels and 2) develop security mechanisms at the physical layer to strengthen the secrecy of communications. For the first line of contribution, a study of the impact of multi-path channels is conducted and a closed-form expression of the symbol error rate is derived. Capitalizing on this study, the enhanced LoRa RAKE receiver leveraging constructively the paths energy is proposed, for the realistic scenario of channel replicas having delays close to the main path while tak-

ing into account synchronization. For the second line of contribution, the impact of traditional Band and Tone jammers on the LoRa demodulation is investigated and highlights the sub-optimal performances of such jammers. Then, a waveform self-jamming scheme is proposed, considerably reducing demodulation capabilities of interceptors thus further enhancing the secrecy of communications. The induced Peak-to-Average Power Ratio (PAPR) by the scheme is analyzed and a mitigation technique is proposed. Finally, experiments on Software Defined Radio (SDR) equipment are achieved and demonstrate the sustainability of this self-jamming scheme.