

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

COMME EXIGENCE PARTIELLE
À L'OBTENTION DE LA
MAÎTRISE EN GÉNIE ÉLECTRIQUE
M. Sc. A.

PAR
Olivier BILODEAU ROBITAILLE

TECHNIQUES DE BROUILLAGE AVANCÉES UTILISANT UN TRAITEMENT DE
SIGNAL RAPIDE

MONTREAL, LE 25 JUIN 2014



Olivier Bilodeau Robitaille, 2014



Cette licence [Creative Commons](https://creativecommons.org/licenses/by-nc-nd/4.0/) signifie qu'il est permis de diffuser, d'imprimer ou de sauvegarder sur un autre support une partie ou la totalité de cette œuvre à condition de mentionner l'auteur, que ces utilisations soient faites à des fins non commerciales et que le contenu de l'œuvre n'ait pas été modifié.

PRÉSENTATION DU JURY
CETTE MÉMOIRE A ÉTÉ ÉVALUÉE
PAR UN JURY COMPOSÉ DE :

M. François Gagnon, directeur de mémoire
Département de génie électrique à l'École de technologie supérieure

M. Claude Thibeault, Ph D., président du jury
Département de génie électrique à l'École de technologie supérieure

Dr. Hafedh Trigui, Ph D., examinateur externe
Ultra Electronics TCS

ELLE A FAIT L'OBJET D'UNE SOUTENANCE DEVANT JURY ET PUBLIC

LE 17JUN 2014

À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

REMERCIEMENTS

François Gagnon pour m'avoir accepté comme étudiant.

Yannick Vallée, Pascal Giard et Gaëtan Racid, pour leurs travaux sur le DRFM .

Samuel Gagné et François Richardson, pour leur aide sur le banc de test.

Normand Gravel, pour avoir empêché plusieurs personnes de prendre mon équipement durant les tests.

TECHNIQUES DE BROUILLAGE AVANCÉES UTILISANT UN TRAITEMENT DE SIGNAUX RAPIDE

Olivier BILODEAU ROBITAILLE

RÉSUMÉ

Pour la rédaction de ce mémoire, j'ai effectué des tests de techniques de brouillage avancées uniques à un système capable d'un traitement de signal à très grande vitesse. Ce traitement de signal rapide est possible par l'utilisation de mémorisation RF à l'aide d'un appareil DRFM.

Les signaux utilisés pour les tests sont des communications de téléphonie cellulaire. Les tests sont effectués sur des signaux représentant les plus récents standards commerciaux, soit le WiMAX, le GSM-EDGE et le W-CDMA.

Une fois les tests avec les techniques de brouillage avancé réalisés, j'ai entrepris une deuxième série de tests utilisant des techniques classiques de brouillage sans mémorisation RF. Ces techniques sont implémentées de manière logicielle dans le DRFM. Les tests comparent des méthodes de brouillage en quantifiant l'interférence sur le signal selon la puissance d'émission. Les résultats permettent de connaître les méthodes offrant le plus d'efficacité et les standards avec la meilleure résistance au brouillage.

Mots clé : DRFM, brouillage, communications sans fil, téléphonie cellulaire, WiMAX, CDMA

ADVANCED JAMMING TECHNIQUES USING FAST SIGNAL PROCESSING

Olivier BILODEAU ROBITAILLE

ABSTRACT

This thesis performs tests on advance jamming methods unique to a system using fast signal processing. The signal processing is accomplished using digital radio frequency memory or DRFM.

The jamming is tested on mobile communication signals used by cell phones. The signals are chosen to represent modern standards used in current commercial cell phones applications. These standards are WiMAX, GSM-EDGE and W-CDMA.

A second series of tests is performed using classic jamming methods without digital radio frequency memory. These jamming methods are implemented using software options available in the DRFM equipment. These tests allow for a comparison of all jamming methods base on the interference generated for similar transmission powers. The results offer insight on the most power efficient jamming methods and which standards offer the best resistance to signal jamming.

Keywords: DRFM, Jamming, wireless communications, cell phone, WiMAX, CDMA

TABLE DES MATIÈRES

	Page
INTRODUCTION	1
CHAPITRE 1 Notions de télécommunications	5
1.1 Communication numérique.....	5
1.1.1 Communication numérique RF.....	5
1.1.2 Énergie et puissance.....	8
1.1.3 Quantité d'information et débit binaire.....	9
1.1.4 Modulation IQ.....	10
1.1.5 Détection de données et fiabilité.....	12
1.1.6 Bit de parité.....	13
1.1.7 Codes convolutionnels.....	15
1.1.8 Taux d'erreur binaire	17
1.1.9 Vecteur d'erreur	19
1.2 Bruit et brouillage	21
1.2.1 Bruit thermique	21
1.2.2 Sources d'interférence diverses	24
1.2.3 Évanouissements à courte échelle.....	24
1.2.4 Écoute et détection.....	27
1.2.5 Ajout de bruit blanc (White noise).....	28
1.2.6 Brouillage « spot » et « spot » pulsé.....	29
1.2.7 Brouillage par barrage.....	31
1.2.8 Brouillage par balayage « Sweep jamming »	32
1.2.9 Brouilleur-répéteur.....	32
1.3 Résumé.....	33
CHAPITRE 2 Brouillage par mémorisation RF	35
2.1 Théorie	35
2.1.1 Bande passante.....	36
2.1.2 Architecture du système.....	36
2.1.3 Bruit de quantification	39
2.2 Technique de brouillage avancée.....	40
2.2.1 DRFM utilisé en brouilleur répéteur.....	41
2.2.2 Variation d'amplitude aléatoire	41
2.2.3 Variation du délai aléatoire.....	42
2.2.4 Brouillage indépendant sur les composantes I et Q	43
2.3 Application avancée liée à la problématique	45
2.4 Résumé.....	45
CHAPITRE 3 Environnement de tests	47
3.1 DRFM Lacime	47
3.1.1 Fonctionnement.....	47

3.1.2	Spécifications.....	48
3.1.3	Radio DRFM.....	50
3.2	Techniques de brouillage implémentées.....	50
3.2.1	Variation d'amplitude aléatoire.....	51
3.2.2	Variation du délai de transmission aléatoire.....	53
3.2.4	Technique non implémentée.....	56
3.3	Banc de test.....	57
3.3.1	Équipement.....	59
3.4	Méthodologie.....	60
3.4.1	Standards et signaux.....	60
3.4.2	Description de la prise de mesures.....	61
3.5	Résumé.....	63
CHAPITRE 4 Analyse pour la marque WiMAX.....		65
4.1	WiMAX.....	65
4.2	Signaux générés.....	68
4.3	Effets du brouillage par variation de délai aléatoire.....	70
4.3.1	Variation rapide du délai.....	71
4.3.2	Variation lente du délai.....	73
4.4	Effets du brouillage par variation aléatoire d'amplitude.....	75
4.4.1	Variation rapide de l'amplitude.....	76
4.4.2	Variation lente de l'amplitude.....	77
4.5	Effets techniques classiques.....	79
4.5.1	Bruit blanc.....	80
4.5.2	Spot.....	81
4.5.3	Balayage.....	83
4.5.4	Barrage.....	85
4.6	Analyse.....	87
4.6.1	Techniques avancées.....	87
4.6.2	Techniques classiques et comparaison.....	88
4.7	Résumé.....	89
CHAPITRE 5 Impact sur le standard GSM-EDGE.....		91
5.1	GSM-EDGE.....	91
5.2	Signaux générés.....	92
5.3	Effets du brouillage par variation de délai aléatoire.....	93
5.4	Effets du brouillage par variation aléatoire d'amplitude.....	96
5.5	Effets des techniques classiques.....	99
5.5.1	Bruit blanc.....	99
5.5.2	Spot et balayage.....	100
5.5.3	Barrage.....	103
5.6	Analyse.....	105
5.6.1	Techniques avancées.....	105
5.6.2	Techniques classiques et comparaison.....	106
5.7	Résumé.....	108

CHAPITRE 6 Impacts sur le standard W-CDMA	109
6.1 W-CDMA	109
6.2 Signaux générés	113
6.3 Effets du brouillage par variation de délai aléatoire	114
6.4 Effets du brouillage par variation aléatoire d'amplitude	116
6.5 Effets des techniques classiques	118
6.5.1 Bruit blanc.....	118
6.5.2 Spot et balayage et barrage	119
6.6 Analyse	121
6.7 Résumé.....	123
CHAPITRE 7 Analyse comparative	125
7.1 Impact du traitement sur le signal échantillonné	125
7.2 Limite du EVM sur un signal WiMAX	126
7.3 Comparaison des techniques avancées sur les trois standards.....	127
7.4 Comparaison des performances des techniques classiques sur les trois standard	129
7.5 Comparaison des puissances requises pour nuire à la communication et la couper ..	132
7.6 Résumé.....	136
CONCLUSION	137
RECOMMANDATIONS	139
LISTE DE RÉFÉRENCES BIBLIOGRAPHIQUES.....	149

LISTE DES TABLEAUX

	Page
Tableau 3.1	Équipement R & S avec options utilisées.....59
Tableau 4.1	Caractéristiques des signaux WiMAX utilisés69
Tableau 4.2	Caractéristiques des brouillages par variation de délai utilisé.....71
Tableau 4.3	Caractéristiques des brouillages par variation de délai utilisés75
Tableau 5.1	Caractéristiques du signal GSM-EDGE92
Tableau 5.2	Caractéristiques des brouillages par variation de délai utilisé.....93
Tableau 5.3	Caractéristiques des brouillages par variation de délai utilisée.....96
Tableau 6.1	Caractéristiques du signal W-CDMA.....114
Tableau 6.2	Caractéristiques des brouillages par variation de délai utilisé.....114
Tableau 6.3	Caractéristiques des brouillages par variation de délai utilisé.....116
Tableau 7.1	EVM limite pour un signal WiMAX.....132
Tableau 7.2	SIR requis du DRFM pour nuire et pour couper une communication WiMAX133
Tableau 7.3	SIR requis pour brouiller une communication GSM-EDGE.....134
Tableau 7.4	SIR requis pour brouiller et pour couper une communication W-CDMA135

LISTE DES FIGURES

	Page
Figure 1.1	Schéma fonctionnel d'une communication numérique5
Figure 1.2	Nature et propagation d'une onde électromagnétique6
Figure 1.3	Fréquence d'une onde.....6
Figure 1.4	Plage fréquentielle des communications RF7
Figure 1.5	Conversion fréquentielle hétérodyne.....8
Figure 1.6	Représentation de signaux sinusoïdaux dans un plan complexe10
Figure 1.7	Chaîne I et Q11
Figure 1.8	Constellation 8-PSK utilisant le code de Grey12
Figure 1.9	Constellations M-QAM12
Figure 1.10	Zones de décision pour une constellation 16QAM13
Figure 1.11	Bit de parité14
Figure 1.12	Parité dans deux dimensions.....15
Figure 1.13	Encodeur convolutionnel.....16
Figure 1.14	Diagramme en treillis pour un code convolutionnel 1/316
Figure 1.15	Probabilité de la position d'un signal BPSK18
Figure 1.16	Vecteur d'erreur de magnitude EVM20
Figure 1.17	Propriétés fréquentielles et auto corrélation d'un bruit blanc.....22
Figure 1.18	Courbe de la probabilité d'erreur binaire théorique avec bruit blanc.....23
Figure 1.19	Ombrage25
Figure 1.20	Multitrajet.....25
Figure 1.21	Schéma d'une communication avec brouillage27
Figure 1.22	Un bruit blanc artificiel créé avec Matlab28

Figure 1.23	Brouillage « spot ».....	30
Figure 1.24	Brouillage par barrage	31
Figure 1.25	Brouillage par balayage dans le temps	32
Figure 2.1	Schéma bloc d'un DRFM.....	35
Figure 2.2	Schéma d'un DRFM à bande latérale unique.....	37
Figure 2.3	Détection en quadrature de phase et conversion A/D.....	38
Figure 2.4	Conversion D/A et modulation.....	38
Figure 2.5	Effets de la quantification sur un signal sinusoïdale	40
Figure 2.6	Schéma d'une communication avec un DRFM répéteur.....	41
Figure 2.7	Variation aléatoire de l'amplitude sur un signal sinusoïdal	42
Figure 2.8	Effets d'un délai aléatoire sur un signal sinusoïdal	43
Figure 2.9	Effet de l'inversion d'I et Q sur une constellation QPSK (code de Grey) ..	44
Figure 2.10	Effets d'un délai aléatoire indépendant sur les signaux I et Q	44
Figure 3.1	Schéma bloc DRFM	47
Figure 3.2	Réponse fréquentielle entre les convertisseurs ADC et les convertisseurs DAC	48
Figure 3.3	Chemin des données pour DRFM avec conversion complexe (bande double).....	49
Figure 3.4	Chemin des données pour DRFM sans conversion complexe (bande latérale unique)	49
Figure 3.5	Diagramme fonctionnel simplifié de la radio DRFM Lacime.....	50
Figure 3.6	Chemin des données du code DRFM	51
Figure 3.7	Densité de probabilité d'une variable aléatoire uniforme discrète	52
Figure 3.8	Brouillage par variation d'amplitude.....	53
Figure 3.9	Brouillage par variation de délai	54
Figure 3.10	Cas d'étude : Communication en présence d'un DRFM.....	57

Figure 3.11	Schéma bloc du banc de tests idéal	58
Figure 3.12	Schéma bloc du banc de tests réel	58
Figure 3.13	Progression des puissances lors de la prise de mesures.....	61
Figure 4.1	Groupe de porteuses orthogonales	65
Figure 4.2	Émetteur idéal OFDM	66
Figure 4.3	Récepteur idéal OFDM.....	66
Figure 4.4	Trame WiMAX dans le domaine fréquentiel	68
Figure 4.5	Trame Wimax dans le domaine temporel avec préfix cyclique	68
Figure 4.6	Mesure du spectre d'un signal WiMAX.....	70
Figure 4.7	Préfixe cyclique et multitrajet.....	71
Figure 4.8	Spectre du signal WiMAX avec variation de délai aléatoire rapide.....	72
Figure 4.9	Comparaison des TEB pour un signal WiMAX avec brouillage par délai aléatoire variant chaque 10 échantillons.....	73
Figure 4.10	Spectre du signal WiMAX avec variation de délai aléatoire lente.....	74
Figure 4.11	Comparaison des TEB pour un signal WiMAX avec brouillage par délai aléatoire variant chaque 32 000 échantillons.....	74
Figure 4.12	Spectre du signal WiMAX avec variation d'amplitude aléatoire rapide.....	76
Figure 4.13	Comparaison des TEB pour un signal WiMAX avec brouillage par amplitude aléatoire variant chaque 10 échantillons.....	77
Figure 4.14	Spectre du signal WiMAX avec variation d'amplitude aléatoire lente	78
Figure 4.15	Capture temporelle d'un signal WiMAX avec variation d'amplitude aléatoire	78
Figure 4.16	Comparaison des TEB pour un signal WiMAX avec brouillage par amplitude aléatoire variant chaque 32 000 échantillons.....	79
Figure 4.17	Comparaison des TEB d'un signal WiMAX pour un bruit blanc simulé et pour un bruit blanc émulé	80
Figure 4.18	Spectre du signal WiMAX avec brouillage « spot »	81

Figure 4.19	Effet du brouillage sur des sous-porteuses de données sur constellation 16QAM	82
Figure 4.20	Comparaison des TEB sur un signal WiMAX avec un brouillage « spot » et un bruit blanc théorique	82
Figure 4.21	Progression de l'EVM d'un signal WiMAX pour un brouillage « spot » positionné sur une sous-porteuse pilote.....	83
Figure 4.22	Spectre du signal de brouillage par balayage	84
Figure 4.23	Comparaison des TEB sur un signal WiMAX avec un brouillage par balayage et un bruit blanc théorique	84
Figure 4.24	Spectre du signal de brouillage par barrage émulé.....	85
Figure 4.25	Comparaison des TEB sur un signal WiMAX avec un brouillage barrage et un bruit blanc théorique	86
Figure 5.1	Constellation $3\pi/8$ -8PSK	91
Figure 5.2	Spectre du signal GSM-EGDE	92
Figure 5.3	Constellation $3\pi/8$ -8PSK.....	93
Figure 5.4	Spectre du signal GSM-EDGE avec variation de délai aléatoire rapide	94
Figure 5.5	Constellation GSM-EDGE soumise à un brouillage par variation de délai aléatoire rapide.....	95
Figure 5.6	Spectre du signal GSM-EDGE avec variation de délai aléatoire lente	95
Figure 5.7	Constellation GSM-EGDE soumise à un brouillage par variation de délai aléatoire lente.....	95
Figure 5.8	Comparaison des EVM pour un signal GSM-EDGE avec brouillage par délai aléatoire.....	96
Figure 5.9	Spectre du signal GSM-EDGE avec variation d'amplitude aléatoire rapide.....	97
Figure 5.10	Constellation GSM-EDGE soumise à un brouillage par variation d'amplitude rapide	98
Figure 5.11	Signal GSM-EDGE avec variation d'amplitude aléatoire lente	98
Figure 5.12	Constellation GSM-EDGE soumise à un brouillage par variation d'amplitude rapide.	98

Figure 5.13	Comparaison des EVM pour un signal GSM-EDGE avec brouillage par amplitude aléatoire	99
Figure 5.14	EVM pour un signal GSM-EDGE pour un bruit blanc émulé	100
Figure 5.15	Constellation GSM-EDGE avec brouillage « spot »	101
Figure 5.16	Spectre du signal de brouillage par balayage	101
Figure 5.17	Constellation GSM-EDGE avec brouillage par balayage	102
Figure 5.18	Comparaison des EVM sur un signal GSM-EDGE avec un brouillage « spot », un balayage et un bruit blanc émulé.....	102
Figure 5.19	Spectre du signal de brouillage par barrage émulé.....	103
Figure 5.20	Constellation GSM-EDGE avec brouillage barrage à différentes puissances	104
Figure 5.21	Comparaison des EVM sur un signal GSM-EDGE avec un brouillage barrage et un bruit blanc émulé.....	105
Figure 5.22	Comparaison des EVM pour les brouillages par variation aléatoire de délai et d'amplitude aux 32 000 échantillons....	106
Figure 5.23	Bruit blanc simulée par le DRFM sur 400KHz autour de 2.45GHZ.....	107
Figure 5.24	Comparaison des EVM entre le brouillage « spot » et les brouillages avancés avec variation aux 32 000 échantillons.....	108
Figure 6.1	Codage CDMA	111
Figure 6.2	Étalement spectral par séquence directe.....	112
Figure 6.3	Communication DS-CDMA à utilisateurs multiples.....	112
Figure 6.4	Spectre du signal W-CDMA	113
Figure 6.5	Spectre du signal W-CDMA avec variation de délai aléatoire rapide.....	115
Figure 6.6	Spectre du signal W-CDMA avec variation de délai aléatoire lente.....	115
Figure 6.7	Comparaison des EVM pour un signal W-CDMA avec brouillage par délai aléatoire.....	116
Figure 6.8	Spectre du signal W-CDMA avec variation d'amplitude aléatoire rapide	117
Figure 6.9	Spectre du signal W-CDMA avec variation d'amplitude aléatoire lente...	117

Figure 6.10	Comparaison des EVM pour un signal W-CDMA avec brouillage par amplitude aléatoire.....	118
Figure 6.11	EVM pour un signal W-CDMA pour un bruit blanc émulé	119
Figure 6.12	Spectre du signal de brouillage par balayage	120
Figure 6.13	Spectre du signal de brouillage par barrage émulé.....	120
Figure 6.14	Comparaison des EVM sur un signal W-CDMA avec un brouillage « spot », balayage, barrage et bruit blanc simulé	121
Figure 6.15	Comparaison des EVM pour les brouillages avancés avec un bruit blanc.....	122
Figure 6.16	Superposition de deux signaux CDMA similaires avec un délai fixe	123
Figure 7.1	Effets des variations aléatoires sur le signal de base selon leur vitesse	126
Figure 7.2	EVM du WiMAX avec brouillage par variation de délai aléatoire aux 32 000 échantillons avec limites sur le EVM	127
Figure 7.3	Comparaison des EVM sur les trois standards testés pour le brouillage par variation de délai aléatoire	128
Figure 7.4	Comparaison des EVM sur les trois standards testés pour le brouillage par variation d'amplitude aléatoire	129
Figure 7.5	EVM du brouillage par bruit blanc émulé sur les trois standards testés....	130
Figure 7.6	EVM des techniques de brouillage classiques utilisées sur les trois standards testés.....	131

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

A/D	Analogique à Digital
ADC	Analog to digital converter
BER	Bit Error Rate
CDMA	Code Division Multiple Access
D/A	Digital à Analogique
DAC	Digital to analog converter
DRFM	Digital Frequency Radio Memory
EEI	Engin Explosif Improvisé
EVM	Error Vector Magnitude
FIFO	First In First Out
GSM	Global System for Mobile Communication (Group Spécial Mobile)
GSM-EDGE	Enhanced Data Rates for GSM Evolution
IFFT	Inverse Fast Fourier Transform
MIMO	Multiple Input Multiple Output
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
RF	Radio Fréquence
SNR	Signal noise Ratio
SIR	Signal Interference Ratio
SRAM	Static Random Access Memory
TEB	Taux d'Erreur Binaire
VHDL	VHSIC Hardware Description Language

WiMAX Worldwide Interoperability for Microwave Access

W-CDMA Wideband Codes Division Multiple Access

LISTE DES SYMBOLES ET UNITÉS DE MESURE

Unités de base

m	mètre (unité de longueur)
s	seconde (unité de temps)
K	Kelvin (unité de température)

Constantes

k	constante de Boltzmann
---	------------------------

Unités dérivés

Temps

s	seconde
Ms	milliseconde
μ s	microseconde
ns	nanoseconde

Fréquence

Hz	hertz
MHz	megahertz
GHz	gigahertz
THz	terahertz

Puissance

W	watt
mW	milliwatt

Résistance

Ω	ohms
----------	------

Unités de ratio

dB	déciBel
dBm	ratio en dB de la puissance sur 1 mW

INTRODUCTION

Le but premier de ce projet est d'analyser des méthodes de contre mesure électronique (ECM) de type brouillage sur des signaux de téléphonie mobile (cellulaires). Les méthodes de brouillages principalement ciblées par les tests sont réalisées à l'aide de support matériel.

La guerre électronique est un aspect important de toute opération militaire. Les contre-mesures électroniques (ECM) consistent en des méthodes utilisées pour contrôler le spectre électromagnétique et empêcher son utilisation par une force hostile. Ces méthodes peuvent être séparées en trois catégories : support, protection et attaque (Spezio, 2002).

Le support ECM regroupe les méthodes et les technologies d'obtention de l'information. Le meilleur exemple est le Radar « RAdio Detection And Ranging », qui utilise les ondes radio pour détecter la position des unités sur le terrain. L'écoute des communications radio entre aussi dans cette catégorie, car elle permet d'obtenir de l'information par transmissions interceptées. La protection ECM regroupe les méthodes de protection contre une menace électronique. Des exemples de protection contre les ECM sont le brouillage radar et le cryptage de signal radio.

La dernière catégorie est celle des attaques ECM. La définition généralement acceptée d'une attaque ECM est une méthode de support et de protection simultanées. Une méthode hypothétique de support et de protection simultanées serait une forme de brouillage intelligent capable de différencier une force alliée d'une force ennemie.

Les contre-mesures électroniques existent depuis longtemps, mais le besoin de les appliquer à des signaux de téléphonie mobile est relativement récent. Le marché des technologies cellulaires a connu une très grande expansion durant les 20 dernières années et les appareils mobiles sont maintenant très répandus et accessibles. Ceci a plusieurs avantages, mais peut aussi causer certains problèmes comme l'a révélé la mission canadienne en Afghanistan de 2001 à 2014. La mission des forces canadiennes en Afghanistan a révélé une nouvelle

menace pour les forces militaires de soutien de la paix : les engins explosifs improvisés (EEI). Ces explosifs souvent fabriqués de manière artisanale utilisent souvent des téléphones mobiles comme méthode de détonation à distance. Pour contrer ces attaques, les convois militaires utilisent des brouilleurs très puissants qui empêchent toutes communications mobiles. Cette méthode a comme désavantage majeur de brouiller également leurs propres radios. En cas d'attaque, le convoi doit donc éteindre le brouilleur pour contacter sa base; il risque alors une attaque par un engin explosif improvisé. Une meilleure approche serait un brouilleur qui bloque toutes les communications mobiles sauf celle du convoi. Pour ce faire, il faut modifier les méthodes existantes ou développer de nouvelles méthodes de brouillages.

Les techniques de brouillage avancées présentées se concentrent sur l'aspect protection. Par contre, plusieurs des techniques peuvent ouvrir des possibilités de support. Les techniques de brouillage avancées par traitement de signaux rapide pourraient théoriquement être efficacement contrecarrées. En effet, le récepteur ayant les détails sur le traitement de signal du brouilleur, pourrait effectuer les opérations inverses pour récupérer le signal de base. Une « clé de brouillage », jumelée à une synchronisation entre les radios pourrait alors être utilisée pour bloquer les communications ennemies sans affecter celles entre alliés. Le brouilleur devient en mesure de remplir la fonction d'attaque ECM tout en assurant la protection et le support.

Dans ce mémoire, il est effectuée une comparaison des performances des techniques de brouillage avancées utilisant un traitement de signal rapide et des techniques classiques. La première étape du projet a été la mise en place d'un banc de test capable de générer des signaux cellulaires conforme aux normes et standards commerciaux. La deuxième étape cruciale a été la configuration de l'appareil de mémorisation numérique RF du laboratoire LaCIME pour générer les différents brouillages aux plages de fréquences désirées, suivie d'une modification à son code de contrôle C++ pour aider la prise des mesures. Finalement, une batterie de tests couvrant plusieurs types de brouillages est effectuée. Durant ces tests, les résultats sont enregistrés manuellement puis traités par logiciel pour l'analyse finale.

Pour présenter le projet réalisé, le mémoire commence par un résumé de plusieurs concepts importants des communications sans fil. Ensuite, il fournit une description détaillée des appareils et méthodes utilisés pour les tests. Les chapitres suivants présentent les différents standards de téléphonie cellulaire générés par le banc de test suivi des résultats sous forme graphique. Finalement, les résultats sont comparés et analysés pour terminer sur les conclusions obtenues au terme de l'étude.

CHAPITRE 1

Notions de télécommunications

1.1 Communication numérique

La communication numérique est la transmission de données sous la forme d'impulsion. Cette transmission, qui peut être effectuée entre deux ou plusieurs points, est réalisée à l'aide d'un circuit électronique.

Une communication requiert un canal entre les points. Ce canal peut être un câble ou une fibre optique. La figure 1.1 est un schéma fonctionnel représentant une chaîne de communication.

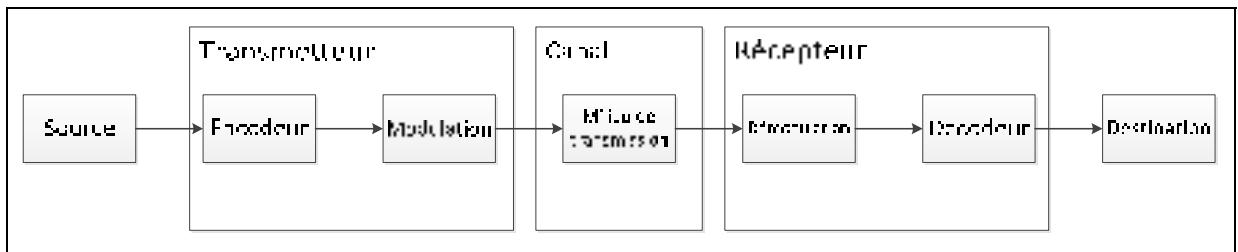


Figure 1.1 Schéma fonctionnel d'une communication numérique
Adaptée de Sen (2000)

L'encodage transforme l'information de base comme la voix en donnée binaire, série de '1' et '0'. Cette étape requiert souvent un échantillonnage du signal de base. La modulation consiste à adapter le signal au canal de transmission. Les étapes inverses sont effectuées à la réception pour recouvrir l'information.

1.1.1 Communication numérique RF

Dans le cas des communications sans fil sur des fréquences radio (RF), le canal de transmission est l'atmosphère terrestre. L'information est transmise à l'aide d'ondes

électromagnétiques. Ces signaux sont définis par plusieurs paramètres. La figure 1-2 montre la variation des composantes électrique et magnétique d'une onde électromagnétique lors de sa propagation.

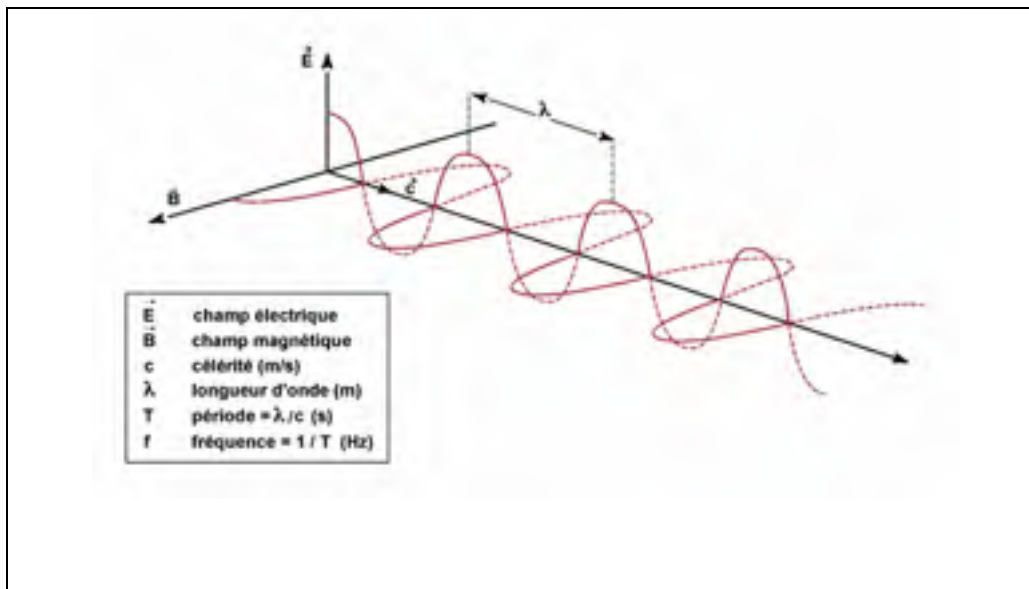


Figure 1.2 Nature et propagation d'une onde électromagnétique
Tirée de Bonn et al. (1992)

Une onde radio est souvent périodique et peut être facilement représentée dans le domaine fréquentiel. La fréquence d'un signal radio représente le nombre de périodes effectuées en une seconde mesuré en hertz (voir la figure 1.3).

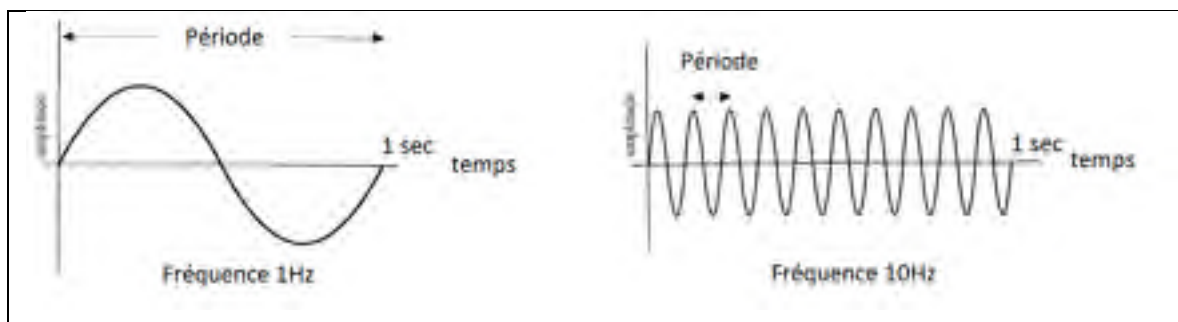


Figure 1.3 Fréquence d'une onde

La période dépend de la longueur de l'onde et de sa vitesse de propagation,

$$F = \frac{1}{T} \quad (1.1)$$

$$T = \frac{\lambda}{c} \quad (1.2)$$

où « F » est la fréquence, « T » est la période, « λ » est la longueur d'onde et « c » est la vitesse de propagation. La majorité des communications RF s'effectuent à des fréquences très élevées. Ceci permet de réduire la taille des antennes, d'avoir accès à de grandes bandes passantes et de bénéficier d'une variété de modes de propagation. La figure 1.4 montre les plages de fréquences utilisées pour les diverses catégories de signaux RF commerciaux utilisées.

10^6	10^5	10^4	10^3	10^2	10^1	10^0	10^{-1}	10^{-2}	λ, m
ELF	VF	VLF	LF	MF	HF	VHF	UHF	SHF	EHF
300 Hz	3 kHz	30 kHz	300 kHz	3 MHz	30 MHz	300 MHz	3 GHz	30 GHz	f

Figure 1.4 Plage fréquentielle des communications RF

Tirée de Stremler (1990)

Pour atteindre ces fréquences, le signal de données, souvent en bande de base, est transposé à une fréquence plus élevée. Cette transposition appelée une conversion fréquentielle hétérodyne est effectuée à l'aide d'un mélangeur et d'une fréquence intermédiaire (voir la figure 1.5).

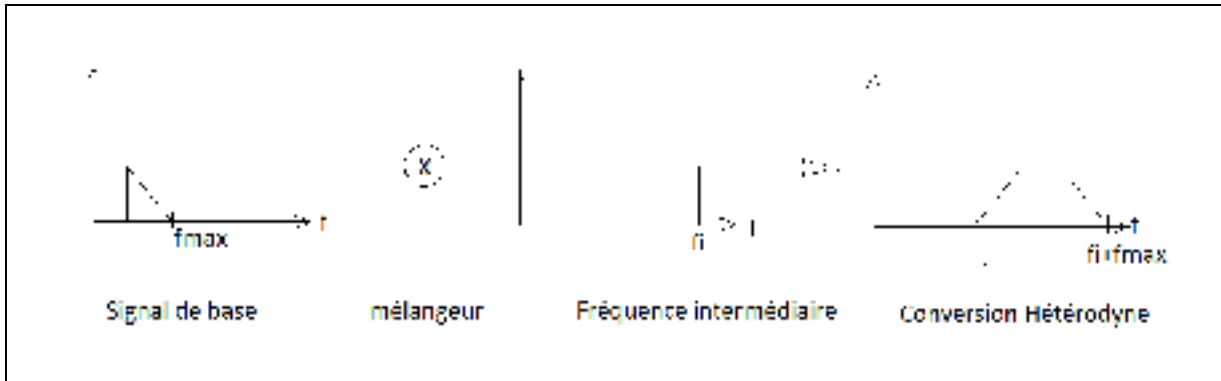


Figure 1.5 Conversion fréquentielle hétérodyne
Adaptée de Stremler (1990)

1.1.2 Énergie et puissance

Un signal radio $s(t)$ est défini comme ayant une énergie ou une puissance. Si le signal $s(t)$ est fini dans le temps, on le définit comme un signal d'énergie. Cette énergie est mesurée avec l'équation 1.3.

$$E = \int_{-\infty}^{\infty} |s(t)|^2 dt \quad (1.3)$$

Si le signal est continu dans le temps, on le définit comme un signal de puissance. La puissance du signal est obtenue par l'équation 1.4.

$$P = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-T/2}^{T/2} |s(t)|^2 dt \quad (1.4)$$

1.1.3 Quantité d'information et débit binaire

Un signal transmis subit une dégradation. Ceci est dû en partie aux imperfections des composantes des systèmes de télécommunications, mais surtout à l'atténuation lors de la transmission (Sen, 2000). Cette perte de puissance est un des principaux facteurs qui limitent la quantité d'information pouvant être transmise. Les mesures de quantité d'information et de vitesse de transfert sont regroupées dans la notion de débit binaire en bits par secondes (b/s). Plus le débit binaire est grand pour une largeur de bande donnée, plus la communication est efficace. Le débit binaire maximal est défini par le canal de transmission. La capacité d'un canal est obtenue à l'aide du théorème de Shannon-Hartley, équation 1.5 (Stremler, 1990) :

$$C = B \log_2 \left(1 + \frac{S}{N} \right) \text{ ou } C = B \log_2 (1 + SNR) \text{ [bits par seconde ou b/s]} \quad (1.5)$$

où « C » est la capacité, « B » est la largeur de bande, « S » est la puissance du signal, « N » est la puissance du bruit et « SNR » est le rapport entre ces deux puissances. La capacité de Shannon est une valeur théorique qui est difficile à atteindre en pratique. Les deux facteurs contrôlables pour augmenter la capacité sont la bande passante B et le SNR, le rapport de puissance entre le signal transmis et le bruit ou les interférences sur le canal. Augmenter la capacité du canal pose plusieurs défis, car les communications RF sont souvent limitées par la bande de fréquences disponible et la puissance du signal diminue rapidement avec la distance (Proakis, 2008). L'équation de la puissance reçue en fonction de la distance est :

$$\frac{P_r}{P_t} = \left(\frac{\lambda}{4\pi R} \right)^2 \quad (1.6)$$

où « Pr » est la puissance au récepteur, « Pt » est la puissance à l'émetteur, « λ » est la longueur d'onde et « R » est la distance entre deux points en mètres. À cause de ces pertes de

puissance dans le canal, l'augmentation de la puissance atteint rapidement des limites matérielles. D'autres méthodes pour améliorer la capacité doivent alors être utilisées.

1.1.4 Modulation IQ

L'utilisation de signaux complexe I et Q (« In phase » et « Quadrature ») pour obtenir une modulation en quadrature et amplitude permet d'augmenter la quantité d'information transmise dans les communications RF. Les signaux IQ ou, en quadrature de phase, sont des signaux dont les phases sont décalées de 90° . Par exemple, un sinus et un cosinus sont par définition déphasés de 90° . La figure 1.6 montre que l'amplitude de ces deux signaux représentés sur un plan complexe prend la forme d'un cercle.

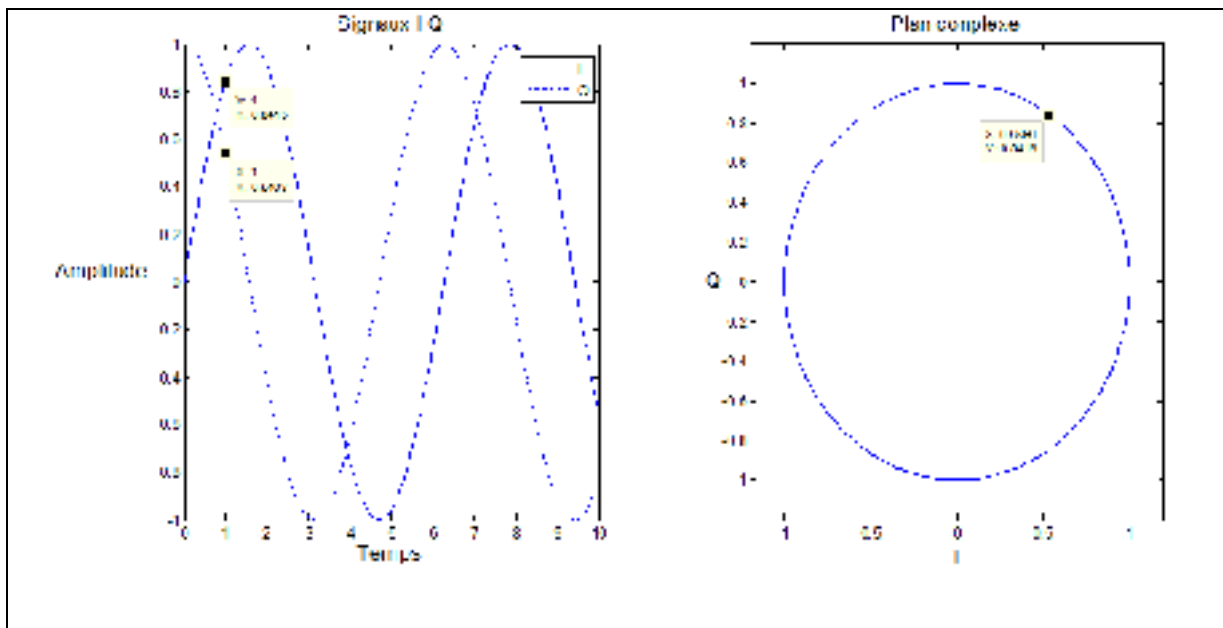


Figure 1.6 Représentation de signaux sinusoïdaux dans un plan complexe

L'amplitude de ces signaux à un moment « t » peut être interprétée comme la position d'un point sur un plan réel et complexe. Le signal « s(t) » résultant d'une modulation en quadrature est :

$$s(t) = I(t) \cos(\omega_c t) - Q(t) \sin(\omega_c t) \quad (1.7)$$

où « I(t) » et « Q(t) » sont les signaux d'information sur l'amplitude des porteuses du signal en phase et en quadrature (Stremmer, 1990). La figure 1.7 montre une chaîne de transmission simplifiée avec une modulation « I » et « Q » utilisant un oscillateur avec une sortie déphasée de 90°.

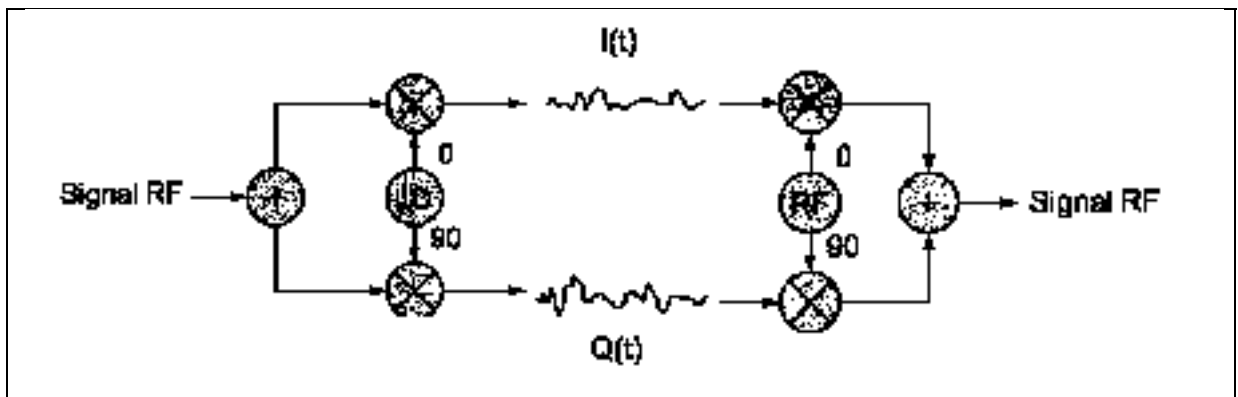


Figure 1.7 Chaîne I et Q
Tirée de Stremmer (1990)

Il est donc possible d'assigner à certaines positions des valeurs distinctes pour ainsi créer une constellation. Ainsi, en modifiant la phase des signaux, il est possible de transmettre une série de points associés à des valeurs binaires. La figure 8 montre une constellation M-PSK à 8 points. Ce type de modulation IQ utilise uniquement une variation de la phase. La position des valeurs binaires est effectuée avec le code de Grey (Proakis, 2008) pour diminuer les nombres de changements de bits sur deux points avoisinants. La figure 1.9 montre plusieurs constellations M-QAM qui utilisent également des variations sur l'amplitude du signal.

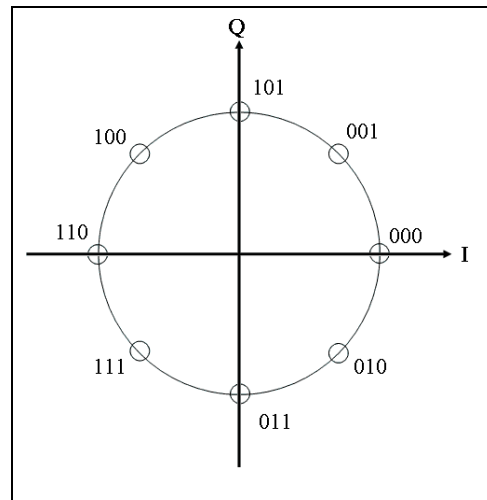


Figure 1.8 Constellation 8-PSK utilisant le code de Grey
Adaptée de Proakis (2008)

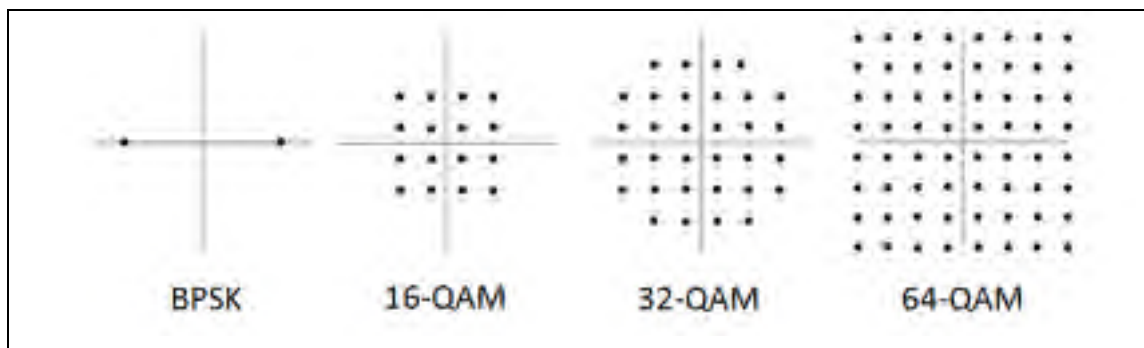


Figure 1.9 Constellations M-QAM
Tirée de Proakis (2008)

1.1.5 Détection de données et fiabilité

Lors de la réception, le signal a été dégradé, ce qui entraîne une modification de sa position. À la suite de la détection, il faut donc prendre une décision sur le signal reçu pour déterminer celui qui est le plus probablement transmis. Plusieurs méthodes existent pour prendre cette décision. La plus simple est la règle du voisin le plus proche. La constellation est divisée en zones de décisions où la valeur du signal reçu est celle du point théorique le plus rapproché

(Proakis, 2008). La figure 1.10 montre un exemple des zones de décision pour un signal 16QAM où « d » est la distance minimale entre deux points de la constellation.

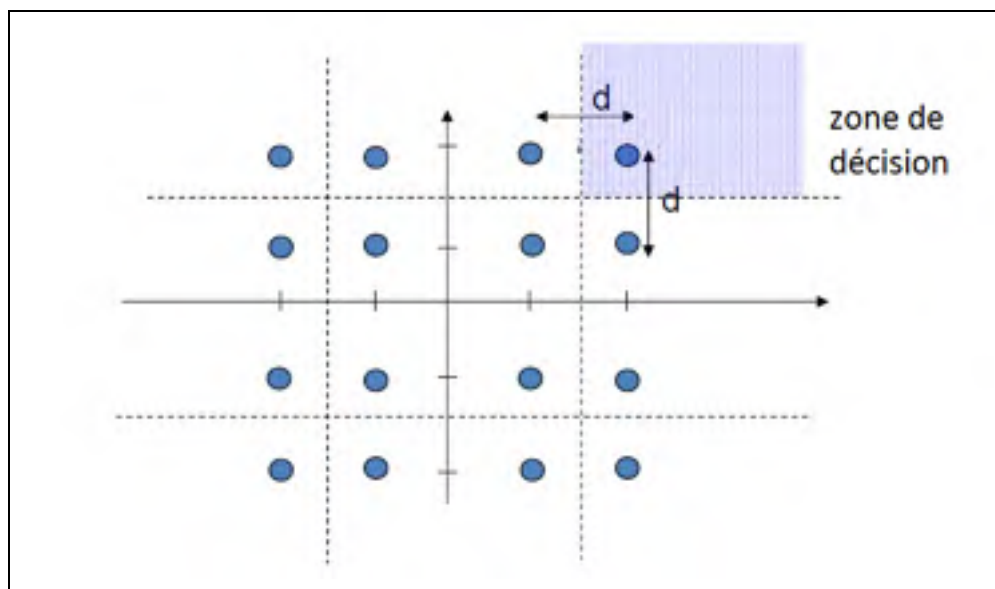


Figure 1.10 Zones de décision pour une constellation 16QAM
Tirée de Proakis (2008)

Si les interférences placent le signal reçu hors de sa zone de détection, il se produit une erreur de décision. Plusieurs techniques existent pour aider à la prise de décision. Ces méthodes utilisent la détection et la correction d'erreurs. Si les erreurs lors de la réception sont corrigées par ces techniques, l'effet sur la communication est similaire à une augmentation du SNR, donc à une augmentation de la capacité. (Proakis, 2008)

1.1.6 Bit de parité

Une méthode simple de contrôle d'erreur consiste à ajouter une information sur la parité des bits. La figure 1.11 montre comment la transmission d'un bit de contrôle peut permettre de détecter une erreur à la réception. Les bits à transmettre sont divisés en trames, si le nombre de bits de valeur « 1 » dans la trame est pair, un bit de contrôle indiquant la parité est ajouté à

celle-ci dans une position réservée. À la réception, la parité de la trame reçue est comparée avec le bit de parité. Si l'information ne correspond pas, une ou plusieurs erreurs sont présentes sur la trame. Cette méthode est limitée pour deux raisons : elle n'apporte aucune information sur le nombre ou la position des erreurs et plusieurs erreurs peuvent tromper la détection (Proakis, 2008).

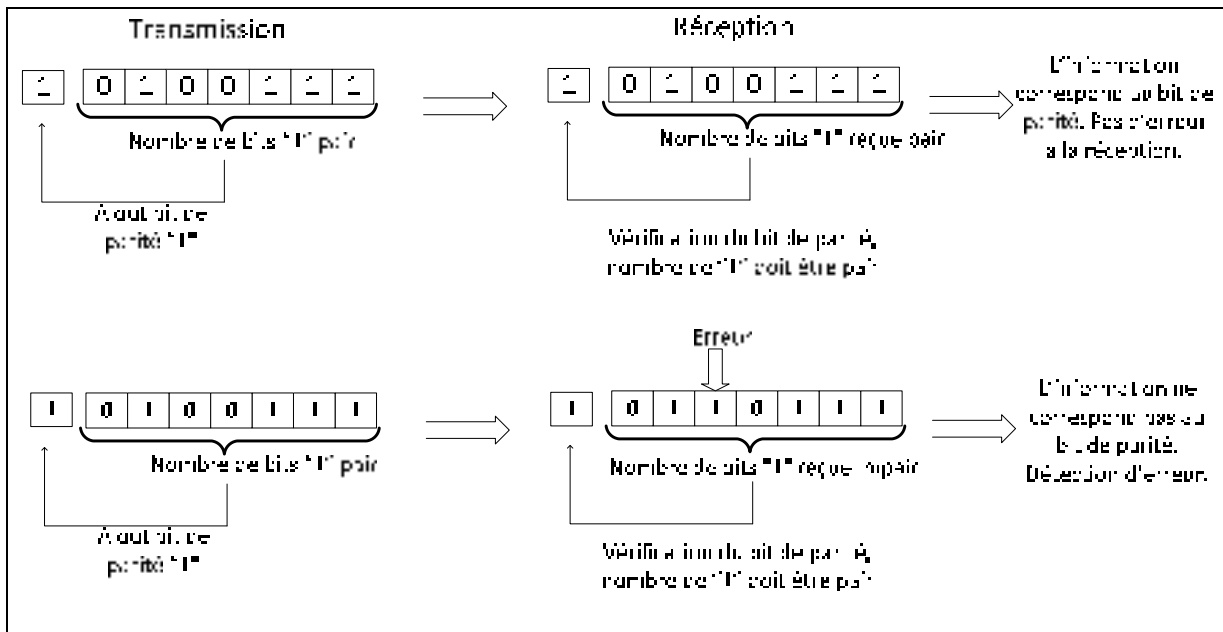


Figure 1.11 Bit de parité
Adapté de Roth (2006)

Une méthode plus complexe consiste à placer l'information dans une matrice et à effectuer la parité dans deux dimensions. La figure 1.12 démontre comment les données utiles peuvent être positionnées pour créer une parité horizontale et verticale. Cette méthode donne une meilleure information sur le nombre et la position des erreurs, mais requiert la transmission de plusieurs bits de contrôles. L'utilisation de matrices pour les données et le contrôle engendra la création de plusieurs méthodes de codage incluant les codes linéaires, les codes cycliques et les codes LDPC (Roth, 2006).

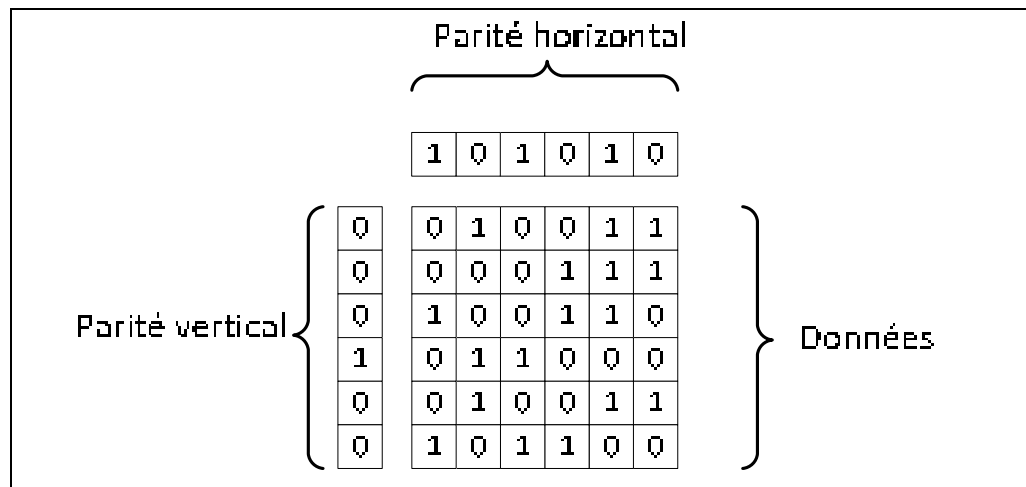


Figure 1.12 Parité dans deux dimensions
Adapté de Roth (2006)

1.1.7 Codes convolutionnels

Une méthode plus complexe développée pour la détection d'erreur utilise des codes dits convolutionnels. Les données sont passées à travers un encodeur avant la transmission et c'est le résultat de l'encodeur qui est transmis par le canal. Un encodeur convolutionnel est constitué d'un registre à états finis ainsi que d'additionneurs modulo 2. La figure 1.13 montre le diagramme d'un encodeur convolutionnel pour un code à une entrée, trois sorties et un registre de trois bits. Le résultat de l'encodeur a un nombre fixe de possibilités selon les données entrées dans le registre. Ceci force la séquence de bits à suivre des chemins connus ponctués par des états stables.

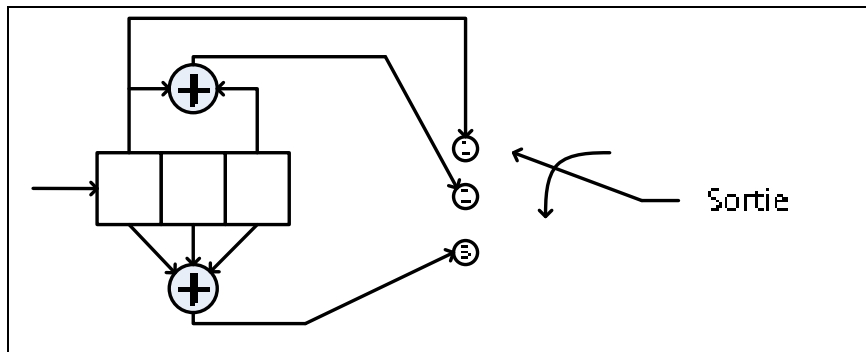


Figure 1.13 Encodeur convolutionnel
Tirée de Proakis (2008)

La progression du signal peut être représentée par un treillis. La figure 1.14 montre le treillis pour un code convolutionnel à une entrée, trois sorties et deux bits de registre. Les lettres « a » « b » « c » et « d » représentent les états du registre. L'ajout d'un nouveau bit dans le registre fait varier cet état de deux manières possibles, suivant la flèche pleine s'il vaut « 0 » ou suivant la flèche pointillée s'il vaut « 1 ». Les bits indiqués sur la flèche représentent les valeurs des sorties de l'encodeur.

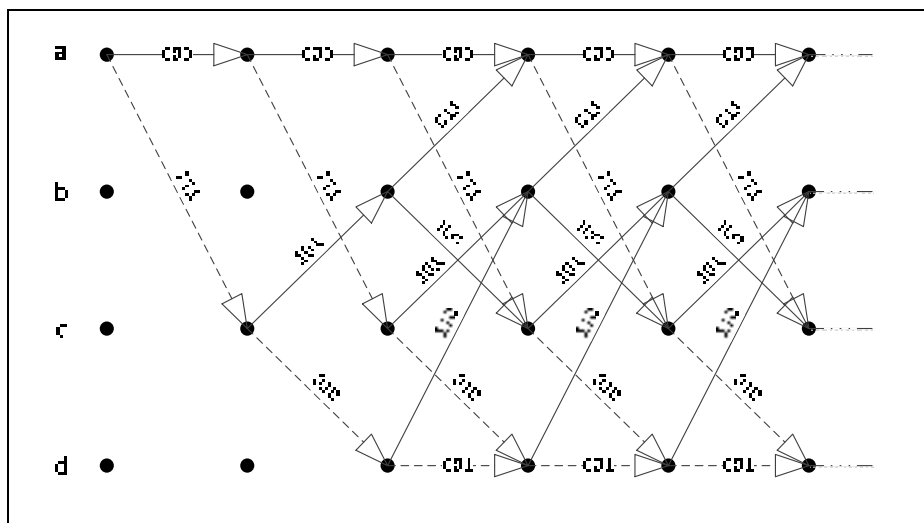


Figure 1.14 Diagramme en treillis pour un code convolutionnel 1/3
Tirée de Proakis (2008)

L'information reçue correspond aux transitions des états du treillis et nous permet de décoder les valeurs entrées dans le registre. Puisque les possibilités de chemin sont limitées, une erreur à la réception entraîne une transition impossible. Cette erreur peut être corrigée en utilisant le chemin possible le plus probable. Les codes convolutionnels permettent une meilleure fiabilité, mais augmentent aussi la quantité de bits qui doivent être transmis. Puisque différentes configurations peuvent obtenir les mêmes résultats, les codes convolutionnels sont souvent décrits par une valeur de performance correspondant au ratio des bits d'information et de codage: $\frac{3}{4}$ ou $\frac{1}{2}$. Par exemple, un code $\frac{3}{4}$ utilise 3 bits en entrée et génère 4 bits en sortie.

Plusieurs méthodes existent pour décoder les codes convolutionnels. La méthode prédominante pour les codes à registre courts (< 10) est l'algorithme de Viterbi (Proakis, 2008). C'est l'algorithme du maximum de vraisemblance trouvant le chemin du treillis qui est le plus proche de la séquence reçue. Au lieu de prendre une décision à chaque transition d'état, l'algorithme de Viterbi garde en mémoire les chemins possibles les plus probables, élimine graduellement les chemins moins plausibles et prend une décision sur le chemin global.

La recherche sur le codage de canal a produit plusieurs méthodes avec différents niveaux de complexité. Les codes les plus récents sont les codes turbo et les codes LDPC. Ces codes sont très complexes, mais ils permettent d'atteindre une capacité très proche de la limite théorique de Shannon (Rüdiger, Richardson et Inc, 2008).

1.1.8 Taux d'erreur binaire

La métrique de performance la plus utilisée lors des communications numériques est le « BER », « bit error rate » ou taux d'erreur binaire « TEB ». Cette mesure donne une indication sur la probabilité qu'une erreur survienne lors de la communication. Elle indique le rapport entre le nombre de bits en erreur et le nombre de bits envoyés (Proakis, 2008). Il est possible de prendre cette mesure directement, mais le TEB diminue très rapidement avec

l'augmentation de la puissance du signal et il devient peu pratique d'attendre la transmission de plusieurs millions de bits avant d'obtenir cette mesure.

$$\text{TEB} = 10^{-12} \Rightarrow \text{une erreur par billion de bits transmis} \quad (1.8)$$

Un calcul théorique du TEB peut être effectué en utilisant les probabilités liées à la position du signal reçu. Pour ce faire, une représentation des signaux de façon vectorielle selon une base orthonormale est utilisée (Proakis, 2008). En posant l'hypothèse que la puissance du signal au moment de l'échantillonnage obéit à une loi normale, on peut représenter le signal selon la probabilité de sa position. La figure 1.15 montre la densité de probabilité de la position d'un signal BPSK. Pour un signal ayant un nombre égal de « 0 » et de « 1 », le seuil de détection est placé à la moitié de la distance minimale. Tous les signaux reçus au-dessus de cette limite sont considérés comme des « 1 ». Inversement, les signaux reçus en dessous de cette limite sont considérés comme des « 0 ». La section où les deux courbes se superposent correspond à la probabilité d'erreur à la réception. Cette valeur dépend de la distance entre les points de la constellation « $d_{\min}$ » qui est déterminée par l'énergie « E_b » par bit utilisée lors de la transmission (Proakis, 2008).

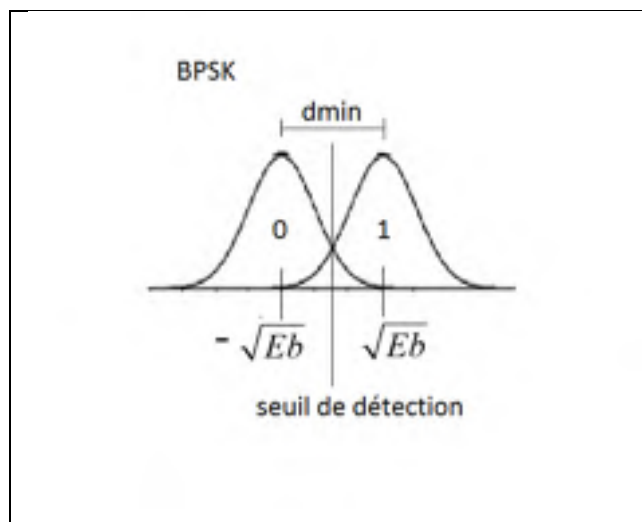


Figure 1.15 Probabilité de la position d'un signal BPSK
Tirée de Proakis (2008)

Selon l'hypothèse que la position du signal est une variable aléatoire gaussienne, il est possible d'obtenir une courbe théorique du TEB selon le type de constellation utilisé (Proakis, 2008). La fonction $Q(x)$:

$$Q(x) = P[N(0,1) > x] = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-\frac{t^2}{2}} dt \quad (1.9)$$

est souvent utilisée pour simplifier la forme des équations. Cette fonction représente la probabilité « P » qu'une variable gaussienne simplifiée « N (0,1) » dépasse la valeur « x ».

Les équations pour la constellation typiquement utilisée sont :

BPSK et QPSK

$$TEB = Q\left(\frac{d_{\min}}{2\sigma}\right) \quad (1.10)$$

M-PSK

$$TEB = \frac{2}{n} Q\left(\frac{d_{\min}}{2\sigma}\right) \quad (1.11)$$

M-QAM

$$TEB = 2 \left(1 - \frac{1}{\sqrt{M}}\right) Q\left(\frac{d_{\min}}{2\sigma}\right) \quad (1.12)$$

où « $d_{\min}$ » est la distance minimale entre deux points de la constellation, « n » est le nombre de bits par symboles, « M » est le nombre de points dans la constellation et « σ » est l'écart type du bruit.

1.1.9 Vecteur d'erreur

Le vecteur d'erreur ou « EVM » est une métrique associée à la couche physique. Elle mesure l'erreur quadratique moyenne sur la position du signal selon la constellation de base. Cette mesure est utilisée pour la majorité des signaux en quadrature de phase et dans les situations

où le BER est difficile à mesurer comme les communications multiporteuses (Schmogrow et al., 2012). La figure 1.16 montre la mesure du vecteur « $E_{err, i}$ » sur une constellation 16QAM. Le vecteur d'erreur EVM est défini comme :

$$EVM = \frac{1}{I} \sum_{i=1}^I |E_{r,i} - E_{t,i}|^2 \quad (1.13)$$

où $E_{t,i}$ est le vecteur de position du point « i » transmis, « $E_{r,i}$ » est le vecteur de position du point « i » reçue et « I » est le nombre de points transmis.

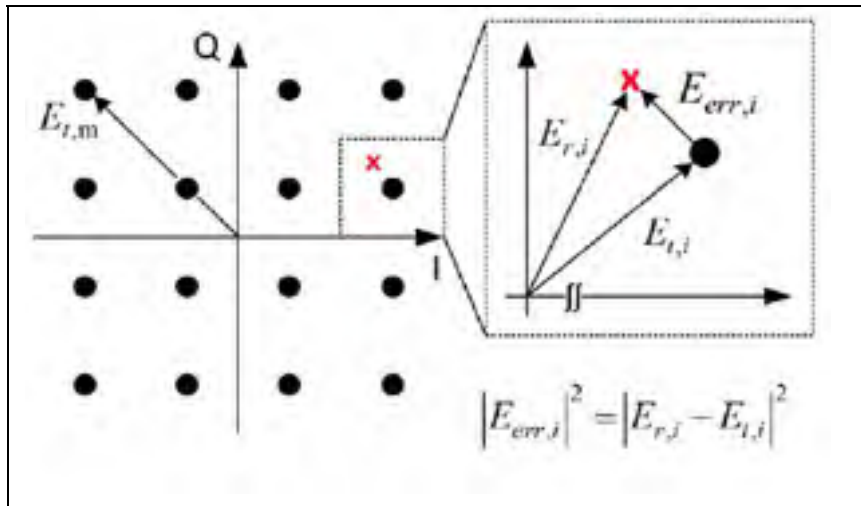


Figure 1.16 Vecteur d'erreur de magnitude EVM
Tirée de Schmogrow et al. (2012)

1.2 Bruit et brouillage

Tel que mentionné précédemment, la capacité d'un canal à transmettre de l'information est une quantité mesurable obtenue par le théorème de Shannon (Stremler, 1990).

$$C = B \log_2 \left(1 + \frac{S}{N} \right) \text{ ou } C = B \log_2 (1 + SNR) \quad (1.14)$$

La capacité ou la quantité d'information pouvant être transmise dépend de la bande passante B et du rapport signal à bruit SNR (Stremler, 1990). En plus de la perte naturelle de puissance de l'onde électromagnétique, le rapport SNR dépend de plusieurs facteurs dont le bruit ainsi que les évanouissements à courte échelle du signal. Les principales composantes du SNR sont les suivantes.

1.2.1 Bruit thermique

Toutes les communications sans fil sont effectuées en présence de bruit thermique. Ce type de bruit est causé par l'agitation des électrons due à la température ambiante. Le bruit thermique est un processus dit blanc. Il est modélisé comme étant un processus stationnaire et gaussien de moyenne nulle (Proakis, 2008).

Le bruit thermique a les caractéristiques suivantes :

- 1) « blanc » si la densité de puissance est égale pour toutes les fréquences;
- 2) « autocorrélation nulle sauf à l'origine » si le signal ne présente aucune régularité ou répétition;
- 3) sa densité spectrale $S_N(f)$ est obtenue par l'équation 1.15. (Proakis, 2008)

$$S_N(f) = \frac{N_0}{2} = \frac{kT}{2} \quad (1.15)$$

$$k = 1.38 * 10^{-23} \text{ J / K}$$

où « N_0 » est la puissance du bruit, « k » est la constante de Boltzmann et « T » est la température en kelvins. La figure 1.17 montre la densité spectrale de puissance $S_N(f)$ et l'autocorrélation $R_X(\tau)$ pour un bruit blanc idéal.

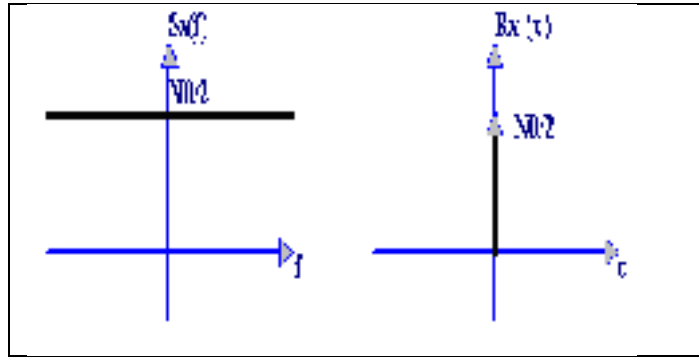


Figure 1.17 Propriétés fréquentielles et auto corrélation d'un bruit blanc
Adapté de Stremler (1990)

En utilisant le bruit thermique comme principale source d'interférence du signal, il est possible de modifier les équations du taux d'erreur binaire pour utiliser la puissance du signal transmis directement plutôt que la distance minimale. En utilisant la variance du bruit thermique $N_0/2$, les équations du taux d'erreur binaire deviennent :

BPSK et QPSK

$$TEB = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \quad (1.16)$$

MPSK utilisant un code de Grey

$$TEB \approx \frac{2}{n} Q\left(\sqrt{2n \frac{E_b}{N_0} \sin\left(\frac{\pi}{M}\right)}\right) \quad (1.17)$$

QAM utilisant un code de Grey

$$TEB \approx \frac{4}{n} \left(1 - \frac{1}{\sqrt{M}}\right) Q\left(\sqrt{\frac{3}{M-1} \frac{nE_b}{N_0}}\right) \quad (1.18)$$

où « E_b » est la puissance par bit, « N_0 » est la puissance du bruit, « n » est le nombre de bits par symbole et « M » est le nombre de points dans la constellation. La figure 1.18 montre les courbes théoriques du TEB selon le rapport de la puissance par bit sur la puissance du bruit. Plus la constellation utilisée est complexe, plus la puissance par bit requise est grande pour atteindre un taux d'erreur faible.

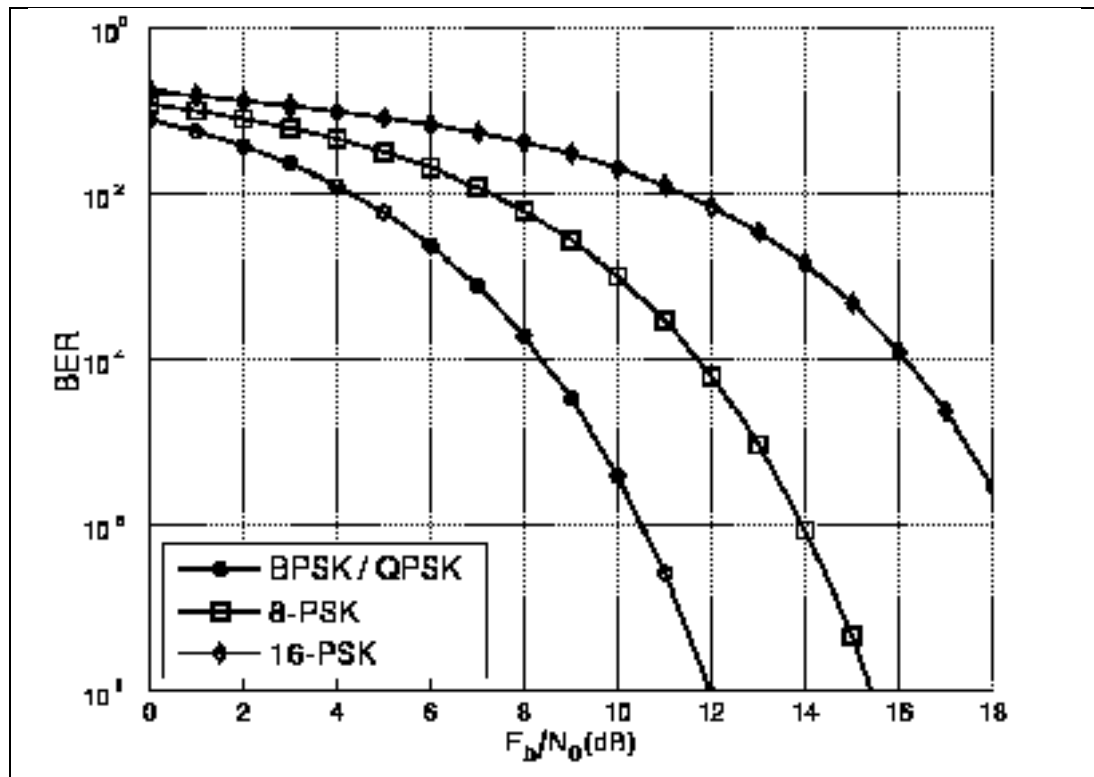


Figure 1.18 Courbe de la probabilité d'erreur binaire théorique avec bruit blanc
Tirée de Proakis (2008)

1.2.2 Sources d'interférence diverses

Ils existent d'autres sources de bruit que le bruit blanc naturel causé par le bruit thermique. Par exemple, pour les communications sans fil, plusieurs sources d'interférences sont possibles.

- 1) présence d'autres communications RF (Interférences interusagers);
- 2) interférence provenant de ligne haute tension;
- 3) orages.

Ces différents facteurs s'ajoutent au bruit thermique et font varier le niveau du bruit selon la position et dans le temps (Proakis, 2008).

1.2.3 Évanouissements à courte échelle

Les communications sans fil sont aussi sujettes à plusieurs sources d'atténuation du signal liées à l'environnement. Ces évanouissements peuvent varier très rapidement dans le temps d'où l'appellation « courte échelle ».

L'ombrage ou « shadowing » est l'impact de la présence d'un obstacle entre la source et la destination du signal. Si cet obstacle est de grande taille, sa présence crée une zone où le signal subit une très forte atténuation. Lorsque le récepteur est mobile, comme dans le cas de la téléphonie cellulaire, l'effet de l'ombrage peut varier rapidement selon l'apparition de l'obstacle (Proakis, 2008). La figure 1.19 montre un schéma de la zone d'ombrage créée par un obstacle entre l'émetteur et le récepteur.

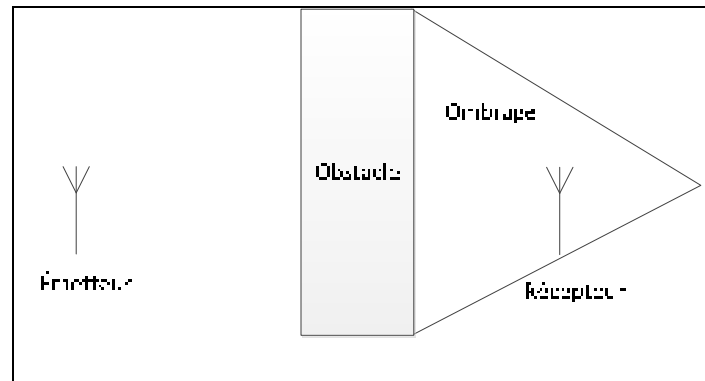


Figure 1.19 Ombrage

Une autre source d'évanouissements à courte échelle est l'effet multitrajet. Une onde électromagnétique qui se propage dans l'air libre subit plusieurs réflexions sur différents obstacles. Par conséquent, le récepteur reçoit le signal par plusieurs chemins ou trajets, tous de longueurs et de temps de propagation différents. Le signal reçu est donc une somme de signaux avec des délais et des atténuations variés, qui peuvent être constructifs ou destructifs. Pour un canal radio mobile, cette interférence varie très rapidement, même pour de courts déplacements (Proakis, 2008). La figure 1.20 montre un schéma d'une communication avec réflexions multiples.

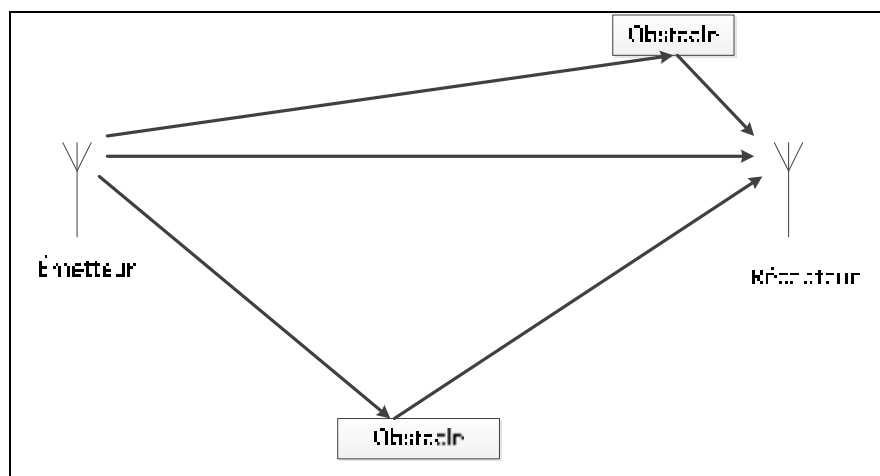


Figure 1.20 Multitrajet

L'équation 1.19 montre le modèle de Rayleigh qui est souvent utilisé pour modéliser la perte de puissance d'un signal dans un canal RF avec évanouissements à courte échelle (Proakis, 2008).

$$P_r(r) = \begin{cases} \frac{2r}{\Omega} e^{\left(-\frac{r^2}{\Omega}\right)} & \text{pour } r \geq 0 \\ 0 & \text{ailleurs} \end{cases} \quad (1.19)$$

$$\Omega = E(R^2)$$

Les performances des canaux avec évanouissements à courte échelle sont bien moindres si comparées à un canal en présence de bruit blanc seulement. La communication requiert un SNR plus élevé pour atteindre le même taux d'erreur (Proakis, 2008).

1.2.4 Écoute et détection

La fonction première d'un système de brouillage est de nuire aux communications. Pour ce faire, il doit soit avoir une connaissance prédéterminée de la position du signal visé ou être en mesure de le détecter. La figure 1.21 montre le schéma d'une communication en présence d'un brouilleur capable d'écouter le signal (S) et d'émettre une interférence (J0).

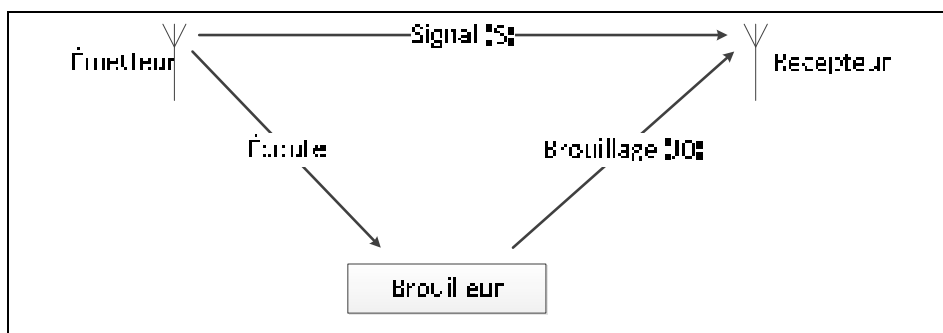


Figure 1.21 Schéma d'une communication avec brouillage.
Adaptée de Sen (2000)

Lorsqu'un brouillage est présent, la capacité du canal devient (Sen, 2000) :

$$C = B \log_2 \left(1 + \frac{S}{N + J_0} \right) \quad (1.20)$$

où « J_0 » est la densité spectrale de puissance du brouilleur s'il est constant et gaussien. Un brouilleur capable de détecter un signal peut aussi être muni de circuit RF pour décoder les signaux reçus et offrir du support en plus de la protection. Par contre, la majorité des techniques classiques de brouillage utilisent le brouilleur comme simple émetteur donc la fonction est de diminuer le rapport SNR jusqu'à ce que la transmission ne soit plus possible. Ces méthodes font abstraction de la modulation. Ils ne font que détecter la présence d'un signal en mesurant la puissance sur le canal. Le signal transmis pour brouiller la communication peut prendre plusieurs formes, décrites dans les sections suivantes.

1.2.5 Ajout de bruit blanc (White noise)

Le théorème de Shannon sur la capacité d'un canal nous indique que la quantité d'information dépend du bruit N présent sur le canal. Donc une augmentation artificielle du bruit entraîne une dégradation de la capacité (Sen, 2000). Un bruit blanc parfaitement aléatoire et gaussien est difficile à reproduire numériquement, mais un algorithme aléatoire peut être utilisé pour créer un signal similaire sur une bande étroite. Le signal est ensuite amplifié et émis sur la bande de fréquences visée, pour ainsi nuire à la capacité du canal (Sen, 2000). La figure 1.22 montre un signal de bruit artificiel ainsi que son autocorrélation. Ce signal pseudo-aléatoire généré avec le logiciel MATLAB a des caractéristiques similaires à un bruit blanc théorique sur un grand nombre d'échantillons (MathWorksInc, 2009).

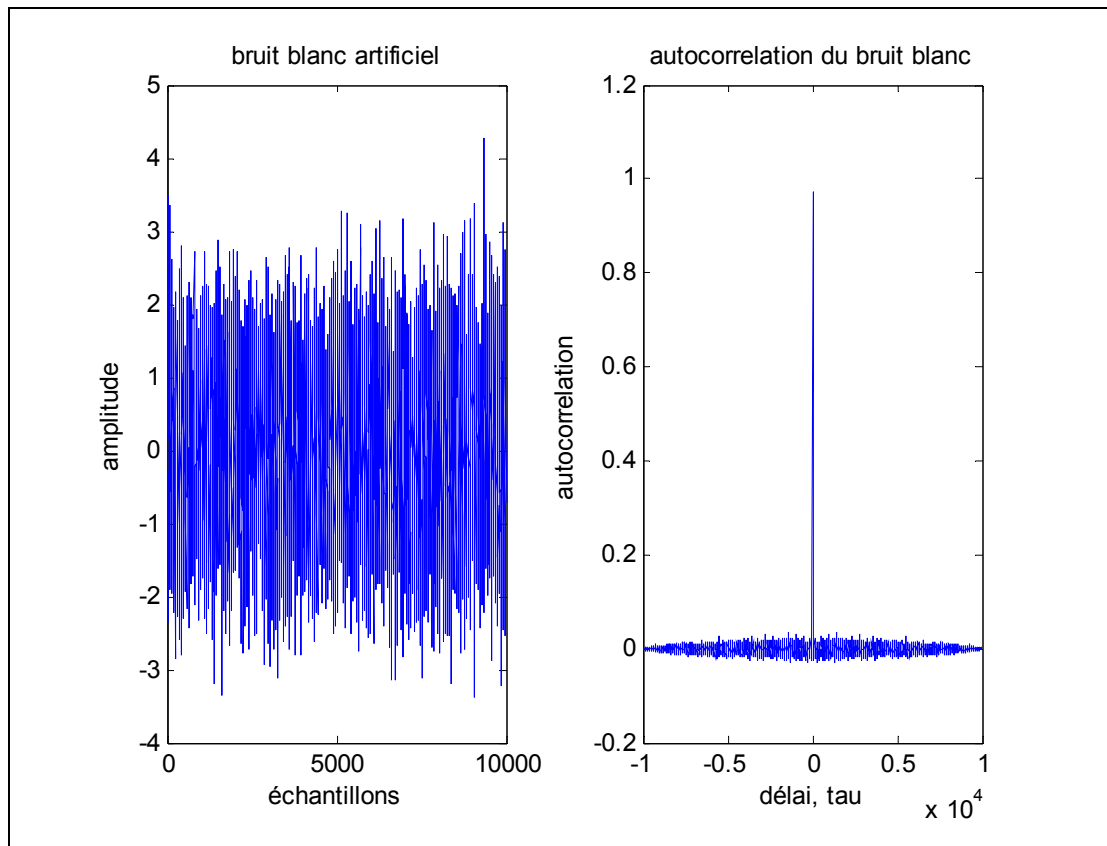


Figure 1.22 Un bruit blanc artificiel créé avec Matlab
Adaptée de MathWorksInc (2009)

La puissance du brouillage est

$$J_0 = \frac{P}{W} \quad (1.21)$$

où « P » est la puissance reçue du brouilleur et « W » est la bande de fréquences visée. L'avantage principal de cette méthode est qu'elle est simple à implémenter. Par contre, cette méthode peut être très couteuse en puissance surtout pour brouiller une large bande de fréquences. De plus, plusieurs méthodes existent pour maximiser le rapport SNR en présence de bruit blanc, ce qui rend le brouillage moins efficace. Le récepteur à filtre adapté en est un exemple (Proakis, 2008).

1.2.6 Brouillage « spot » et « spot » pulsé

Le type de brouillage « spot » consiste à envoyer un signal très étroit en fréquence. Placé au bon endroit, ce signal créera une interférence avec la communication visée. Une méthode simple est d'utiliser un signal sinusoïdal à la fréquence désirée avec une phase aléatoire et une très haute puissance (Sen, 2000). La forme du signal d'interférence est :

$$I(t) = \sqrt{2} A \cos(2\pi fc + \theta) \quad (1.22)$$

où « θ » est une variable aléatoire entre 0 et 2π . La figure 1.23 montre un exemple de brouillage « spot ».

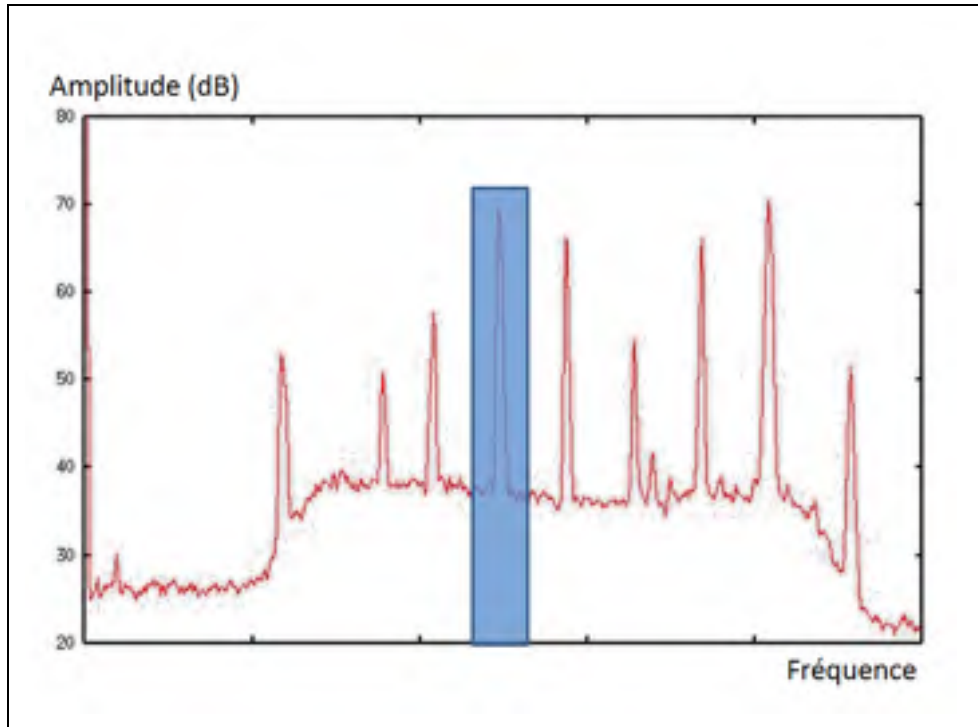


Figure 1.23 Brouillage « spot »

Pour diminuer les besoins énergétiques, le signal peut être envoyé de manière intermittente, ce type de bruit est dit pulsé. Une optimisation du cycle d'émission peut apporter un impact plus grand sur le signal qu'une émission continue avec la même puissance instantanée (Sen, 2000). La puissance du brouillage est :

$$P = J_0 / \rho \quad (1.23)$$

où « ρ » est la fraction de temps d'émission. La capacité du canal devient :

$$C = (1 - \rho) \log_2 \left(1 + \frac{S}{N} \right) + \rho \log_2 \left(1 + \frac{S}{N + \frac{J_0}{\rho}} \right) \quad (1.24)$$

L'utilisation d'une bande de fréquences étroite permet de concentrer la puissance du brouilleur et d'avoir un plus grand impact sur le SNR avec les ressources disponibles. L'inconvénient majeur de ce type de brouillage est que son impact diminue grandement sur les communications à large bande comme l'ODFM et devient presque nul sur les modulations à étalement de spectre comme de CDMA (Proakis, 2008).

1.2.7 Brouillage par barrage

Pour contrer les limites du brouillage « spot », il est possible de générer un bruit continu sur une large bande de fréquences. Comme le montre la figure 1.24, la puissance disponible est alors distribuée également sur toute la plage de fréquence ciblée (Sen, 2000). Pour être efficace, ce type de brouillage demande une grande puissance à l'émetteur ce qui entraîne de très hauts coûts en énergie et en équipement. De plus, ce brouillage cause un rayonnement électromagnétique très puissant autour de l'émetteur.

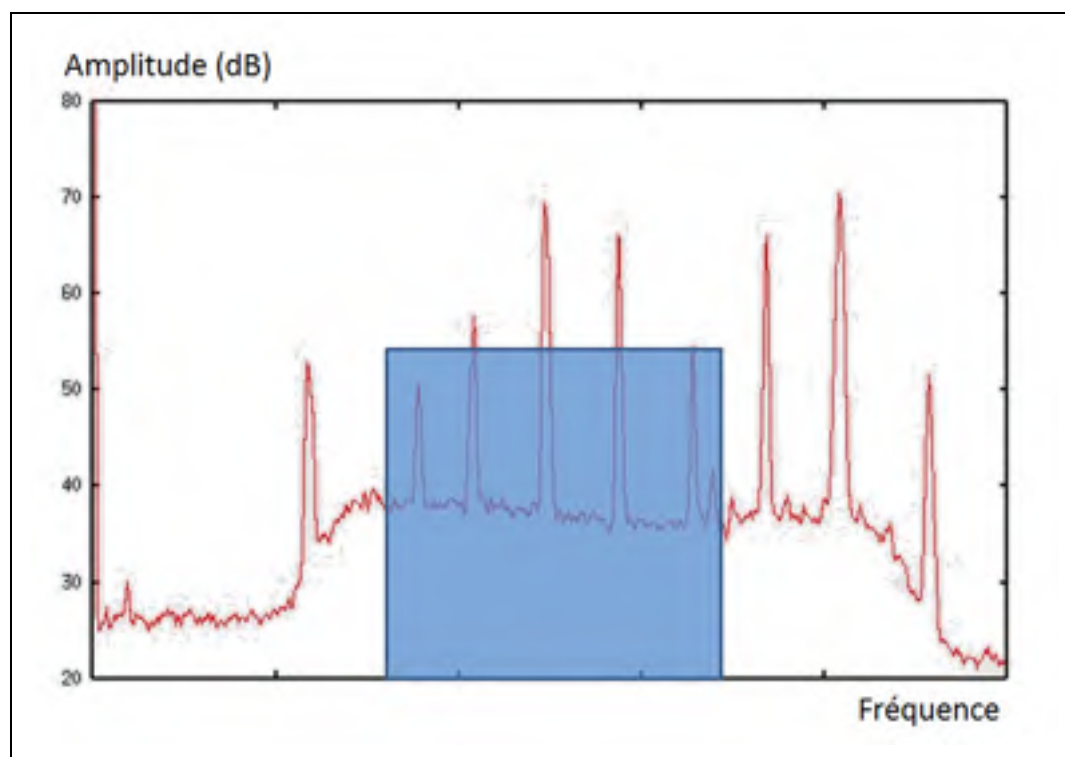


Figure 1.24 Brouillage par barrage

1.2.8 Brouillage par balayage « Sweep jamming »

Le brouillage par balayage utilise un signal simple et varie sa fréquence pour couvrir une plus grande plage du spectre. La variation de la fréquence du signal est souvent linéaire, constante et à des intervalles de temps fixes. L'impact du brouillage dépend donc du choix de la plage de fréquence, de la taille du saut en fréquence effectué (Δf) et du temps entre chaque saut de fréquence. Comme pour le bruit pulsé, une optimisation de ces paramètres permet une efficacité plus grande pour la puissance disponible (Sen, 2000). La figure 1.25 montre la progression d'un brouillage par balayage dans le temps.

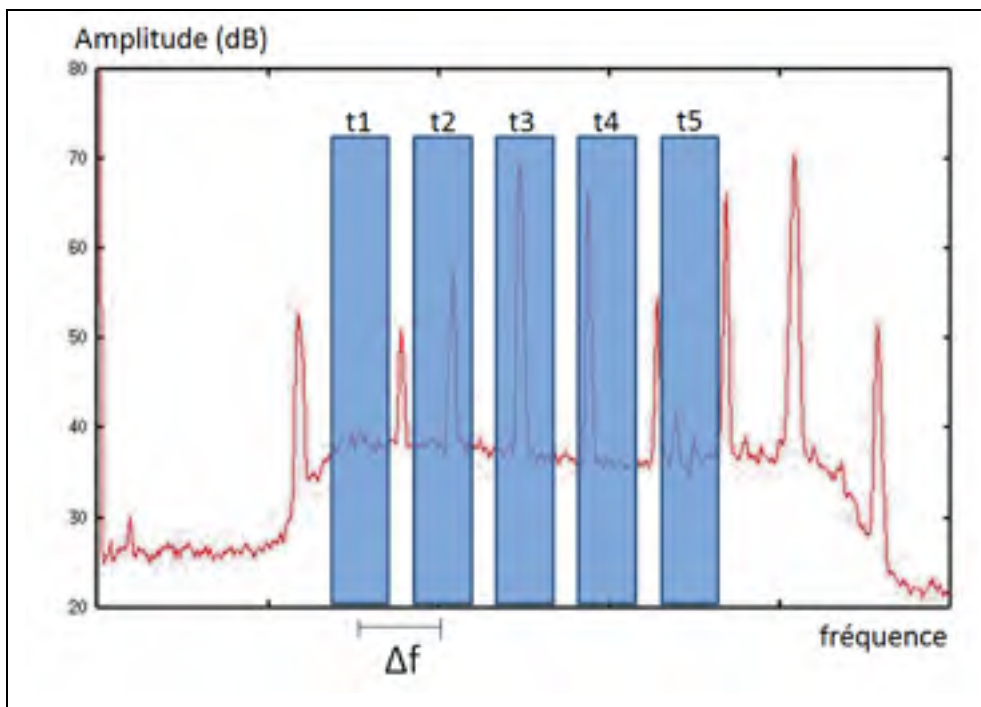


Figure 1.25 Brouillage par balayage dans le temps

1.2.9 Brouilleur-répéteur

Une méthode courante pour contrer le brouillage est le saut de fréquence. Dans ce type de communications, l'émetteur et le récepteur changent rapidement la fréquence porteuse utilisée suivant un modèle pseudo-aléatoire. Un brouilleur standard n'a pas d'information sur

position fréquentielle du signal dans le temps et ne peut donc pas brouiller efficacement un tel signal.

Déjouer un signal à saut de fréquence requiert des brouilleurs plus sophistiqués appelés brouilleurs-répéteurs. Ces brouilleurs écoutent continuellement la bande de fréquences visée et utilisent un traitement de signaux rapide pour concentrer leur puissance au meilleur endroit dans le temps. Pour être efficaces, ils doivent détecter le signal assez rapidement pour percevoir le signal ciblé entre deux sauts de fréquence. Il faut aussi qu'il soit positionné de sorte que le brouillage soit reçu avant le saut subséquent.

1.3 Résumé

Pour résumer, les communications numériques ont comme but le transfert d'information. La quantité et qualité de l'information transmise dépend de la capacité. Cette valeur est une propriété du canal de transmission lié à l'atténuation du signal et à la présence de bruit. Plusieurs techniques existent pour améliorer la capacité et ainsi permettre des communications plus rapides et plus fiables. À l'opposé, un brouilleur cherche à diminuer la capacité du canal pour rendre la communication impossible. Pour y parvenir, les méthodes de brouillage les plus courantes augmentent le niveau du bruit sur le canal pour diminuer la capacité. Un défi majeur du brouillage est comment utiliser la puissance du brouilleur. Un compromis doit être fait entre la largeur de bande passante affectée et le niveau du bruit ajouté. Dans le but de résoudre ce compromis, le chapitre suivant présente comment un traitement de signal rapide peut être utilisé pour cibler la puissance du brouilleur directement sur les communications en utilisant une mémorisation numérique du signal.

CHAPITRE 2

Brouillage par mémorisation RF

Le sigle DRFM pour « digital frequency radio memory » désigne une méthode par laquelle un signal RF est reçu, mémorisé et est retransmis numériquement. Les appareils DRFM utilisent une mémoire à port double, couplée à des convertisseurs haute vitesse. Les performances d'un DRFM dépendent de plusieurs facteurs : la vitesse d'échantillonnage, le nombre de bits de quantification et l'architecture du système (Roome, 1990).

2.1 Théorie

La figure 2.1 montre le schéma d'un appareil DRFM standard. Une mémoire haute vitesse est connectée à des convertisseurs analogiques numériques A/D et des convertisseurs numériques analogiques D/A. Un contrôleur gère la mémoire et utilise un oscillateur local pour effectuer la conversion en fréquence hétérodyne.

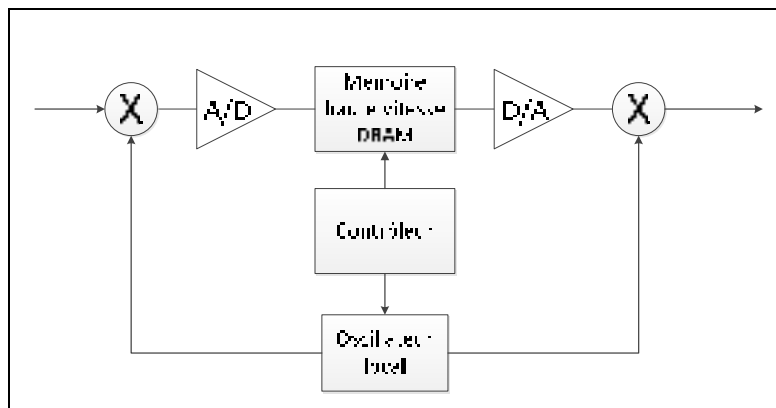


Figure 2.1 Schéma bloc d'un DRFM
Adaptée de Roome (1990)

2.1.1 Bande passante

La bande passante pouvant être mémorisée dépend de la vitesse d'échantillonnage. Le théorème de l'échantillonnage de Nyquist démontre que pour échantillonner un signal sans perte d'information la fréquence d'échantillonnage doit être supérieure au double de la fréquence maximale de ce signal (Stremler, 1990).

L'équation est :

$$f_{sample} \geq 2f_{max} \quad (2.1)$$

$$T_{sample} \leq \frac{1}{2B}$$

où « f_{sample} » est la fréquence d'échantillonnage, « f_{max} » est la fréquence maximale du signal. « T_{sample} » est le temps entre deux échantillons et « B » est la bande passante. Un petit T_{sample} augmente la bande passante B pouvant être mémorisée.

2.1.2 Architecture du système

Un appareil DRFM contient également des composantes RF pour aider la sélection du signal. La bande de fréquences disponible est affectée par les caractéristiques des filtres utilisés dans l'architecture du système. Typiquement, des filtres de type passe-bande et anticrénelage sont utilisés. La figure 2.2 montre un schéma avec les filtres typiquement utilisés pour un DRFM à bande latérale unique. La bande passante du DRFM est :

$$B = a \frac{f_{sample}}{2} \quad (2.2)$$

$$a < 1$$

où « B » est la bande passante, « f_{sample} » est la fréquence d'échantillonnage et « a » est la fraction de la bande passante idéale, laquelle dépend des filtres (Roome, 1990).

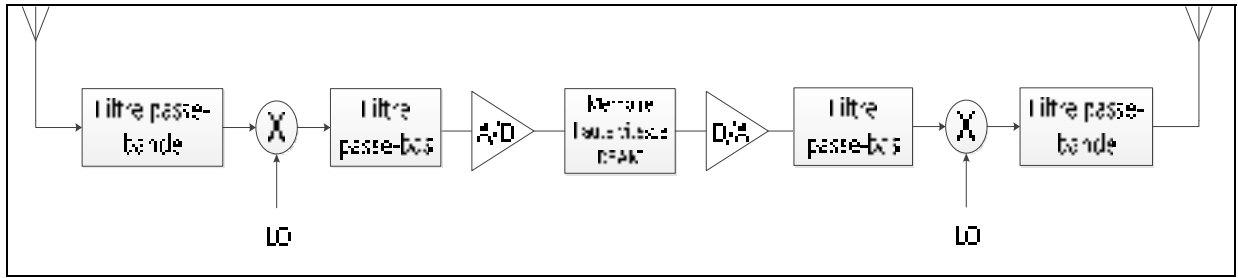


Figure 2.2 Schéma de la chaîne de transmission d'un DRFM à bande latérale unique
Adaptée de Roome (1990)

Une décomposition du signal reçu en composante en quadrature de phase permet une augmentation de la bande passante disponible par un facteur 2. La bande passante du DRFM devient :

$$B = af_{sample} \quad (2.3)$$

$$a < 1$$

où « B » est la bande passante, « f_{sample} » est la fréquence d'échantillonnage et « a » est la fraction de la bande passante idéale, généralement plus élevée que dans le cas de la bande latérale unique (Roome, 1990). Un DRFM à double bande requiert des étapes supplémentaires à la réception et à la transmission. La figure 2.3 est le schéma d'un récepteur effectuant la détection en quadrature de phase. Les signaux en phase « I » et en quadrature « Q » sont numérisés et mémorisés séparément. La figure 2.4 montre le schéma de l'émetteur qui doit effectuer la conversion analogique des signaux et les combiner avant la transmission.

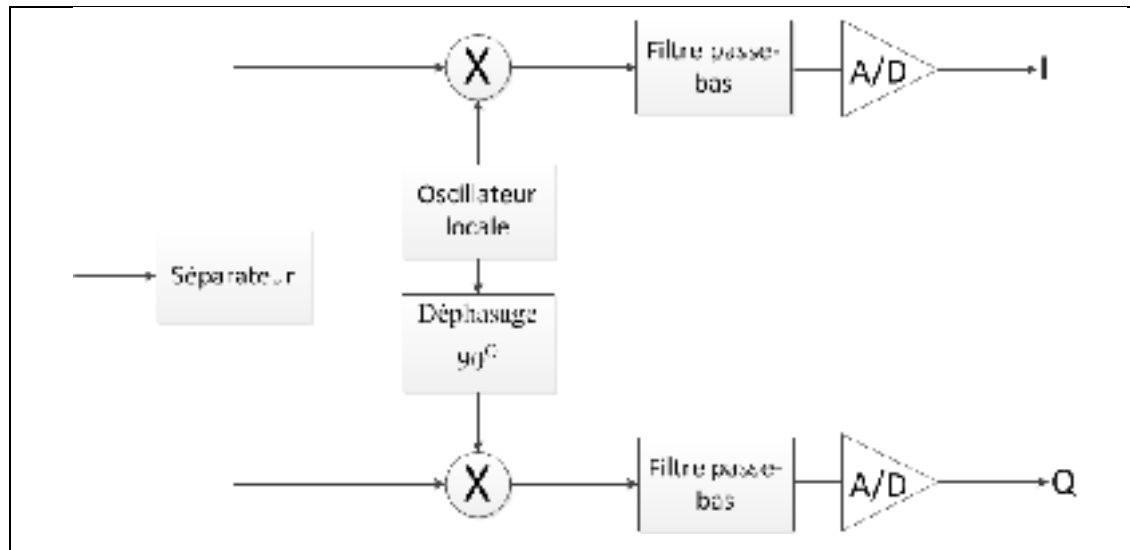


Figure 2.3 Détection en quadrature de phase et conversion A/D
Tirée de Roome (1990)

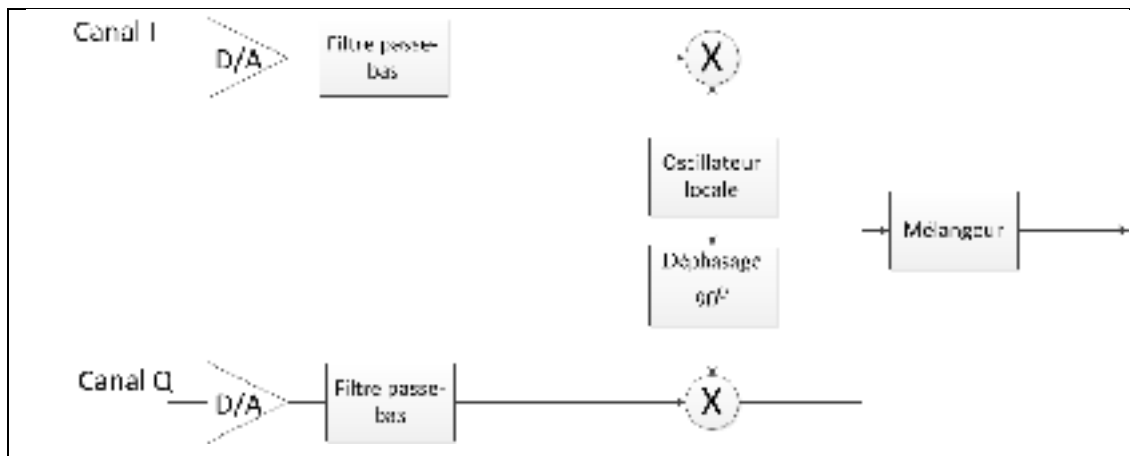


Figure 2.4 Conversion D/A et modulation
Tirée de Roome (1990)

2.1.3 Bruit de quantification

La conception d'un appareil DRFM entraîne un compromis entre la vitesse d'échantillonnage et le nombre de bits par échantillons. À un coût donné, le choix d'un convertisseur plus rapide amène une diminution de la précision ou du nombre de bits. À l'opposé, un convertisseur plus précis, avec plus de bits, diminue la vitesse d'échantillonnage. Le bruit de quantification est un résultat de la conversion d'un signal continue en signal échantillonné. La conversion ajoute des distorsions au signal sous la forme de composantes fréquentielles indésirables. Le rapport du signal au bruit SNR lié à la quantification est calculé avec l'équation 2.4 :

$$SNR = 6.02n + 1.75dB \quad (2.4)$$

où « n » est le nombre de bits du convertisseur (Roome, 1990). Le bruit de quantification peut être diminué à l'aide de filtres d'anticrénelage. La figure 2.5 montre les effets de la quantification et du filtrage sur un signal sinusoïdal. En pratique, le bruit de quantification est aussi affecté par les non-linéarités des convertisseurs (Roome, 1990), ce qui résulte en un bruit de quantification globale spécifique à chaque appareil DRFM. L'ajout de bruit de quantification n'est pas un problème lorsque le DRFM est utilisé comme brouilleur, mais doit être pris en considération lorsqu'il est utilisé comme un répéteur.

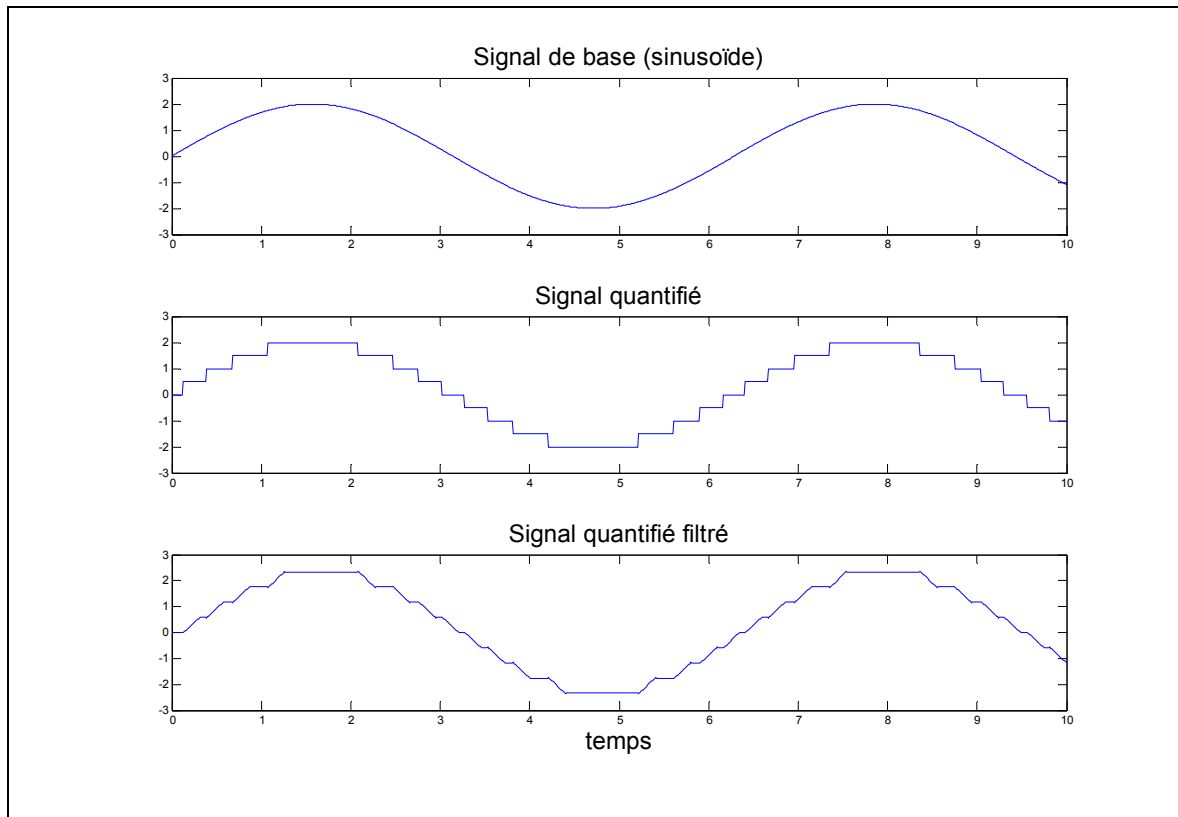


Figure 2.5 Effets de la quantification sur un signal sinusoïdale
Adaptée de MathWorksInc (2009)

2.2 Technique de brouillage avancée

La mémorisation numérique offre un très grand contrôle sur le signal et permet l'utilisation de nouvelles méthodes de brouillages pouvant être appliqués seulement par un traitement numérique du signal. De plus, les DRFM font abstraction du type de modulation utilisé. Ils peuvent ainsi déjouer plusieurs techniques d'antibrouillages comme le saut de fréquences, si sa largeur de bande est suffisamment grande et le traitement assez rapide.

2.2.1 DRFM utilisé en brouilleur répéteur

La présence d'un brouilleur DRFM en mode répéteur est similaire à la présence d'un trajet supplémentaire avec le temps de traitement du signal ajouté au délai de propagation. La figure 2.6 montre une communication en présence d'un DRFM, le signal brouillé par le DRFM sera additionné aux réflexions de la communication de base. Par ce fait, la puissance du signal transmis doit être dans le même ordre de grandeur que celle du chemin principal. Un signal trop faible n'aura aucun effet marqué sur les performances de la communication. Il est possible, avec le DRFM, d'augmenter le délai artificiellement pour accentuer l'effet multitrajet sans modifier le signal de base. Par contre, plusieurs méthodes ont été conçues pour contrer l'effet multitrajets et les performances d'un tel brouillage sont limitées.

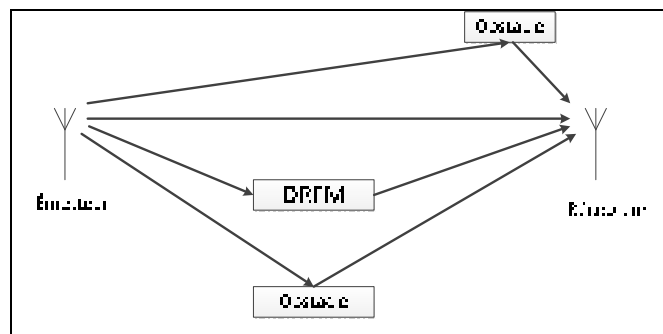


Figure 2.6 Schéma d'une communication avec un DRFM répéteur

2.2.2 Variation d'amplitude aléatoire

La majorité des récepteurs RF ont un contrôle automatique du gain (AGC) pour compenser les variations du canal de transmission. Les AGC sont conçus pour s'adapter plus rapidement que le taux de variation du canal, mais moins rapidement que la modulation pour garder la puissance stable à la réception sans affecter la transmission (Proakis, 2008). Avec un appareil DRFM, il est possible de retransmettre le signal en modifiant très rapidement son amplitude. Une variation d'amplitude rapide ne pourra être compensée par l'AGC, ce qui augmentera les erreurs de décisions. Le signal résultant est similaire à un signal soumis à des évanouissements par ombrages variant rapidement. La figure 2.7 montre les effets de

variations aléatoires de l'amplitude faible et élevée sur un signal sinusoïdal. Un signal avec une variation d'amplitude aléatoire faible reste relativement proche d'un signal de base, mais une variation d'amplitude élevée le rend indéchiffrable. Théoriquement, le type de constellation est un facteur important sur l'efficacité de cette technique puisque des modulations simples sont, à puissance égale, plus résistantes aux variations d'amplitude.

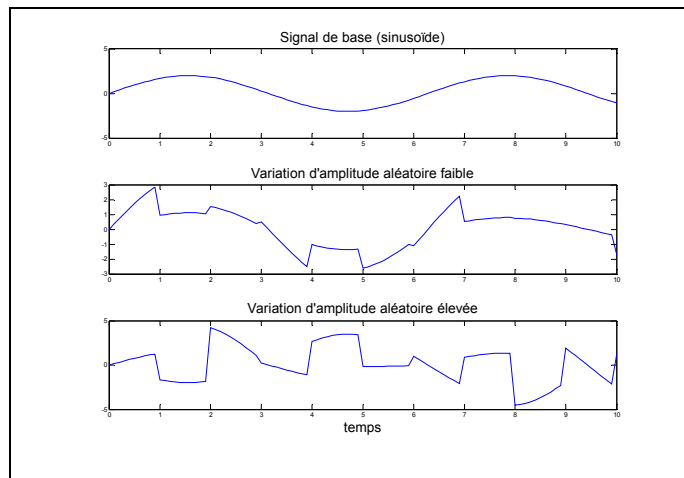


Figure 2.7 Variation aléatoire de l'amplitude sur un signal sinusoïdal
Adaptée de MathWorksInc (2009)

2.2.3 Variation du délai aléatoire

Le délai de transmission du signal provenant du brouilleur peut être contrôlé à l'aide du traitement de signal. Le DRFM peut créer artificiellement un délai de transmission sur le signal et le faire varier aléatoirement. Une variation rapide de ce délai crée un effet multitrajet accentué que le récepteur est incapable de poursuivre et de corriger. La figure 2.8 montre les effets de variations aléatoires du délai faible et élevé sur un signal sinusoïdal. Une variation de délai faible engendre peu de modifications au signal de base. Par contre, le signal avec une variation de délai élevé est très différent du signal de base. Théoriquement, en plus de brouiller le signal, le brouillage par variation de délai peut influencer la réception en modifiant la phase des porteuses et des pilotes, ce qui pourrait rendre cette technique très efficace contre les modulations avancées.

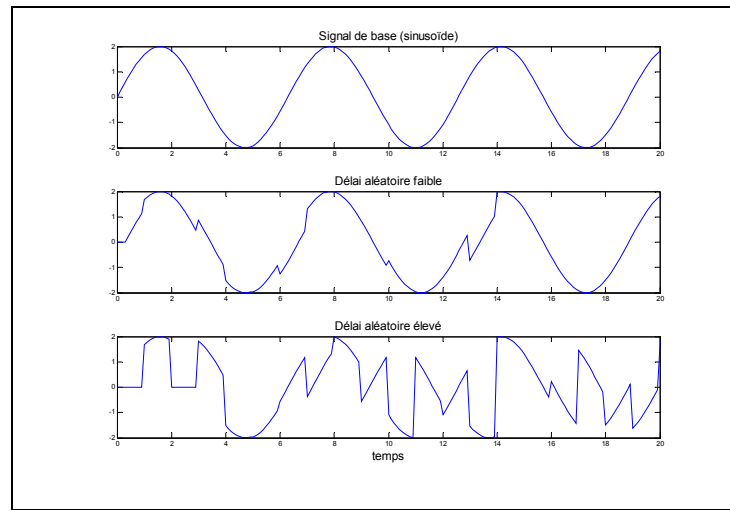


Figure 2.8 Effet d'un délai aléatoire sur un signal sinusoïdal
Adaptée de MathWorksInc (2009)

2.2.4 Brouillage indépendant sur les composantes I et Q

Un DRFM capable d'effectuer une décomposition en quadrature de phase permet d'effectuer des traitements de signaux séparés sur chaque composante. Puisque les composantes en quadrature de phase sont transmises simultanément, elles utilisent le même canal de transmission et subissent généralement les mêmes effets. Un brouillage unique sur chaque composante crée donc des distorsions presque impossibles en termes de propagation dans une communication RF standard. Les systèmes de corrections d'évanouissements tels que les égalisateurs adaptatifs et les récepteurs RAKE (Proakis, 2008) sont donc incapables de les corriger.

Une modification simple est l'inversion des composantes I et Q. Le signal créé est similaire au signal standard, mais avec des points de constellation différents. Théoriquement, si le démodulateur utilise un code convolutionnel, l'effet est accentué. Si les données suivent un chemin impossible, le chemin le plus probable sera très éloigné du chemin correct et la correction sera sans impact. Si le chemin est possible, aucune erreur ne sera détectée. Dans les deux cas, les données décodées seront indéchiffrables pour l'utilisateur. La figure 2.9

montre l'effet d'une inversion I et Q sur les bits reçus pour une constellation QPSK utilisant un code de Grey.

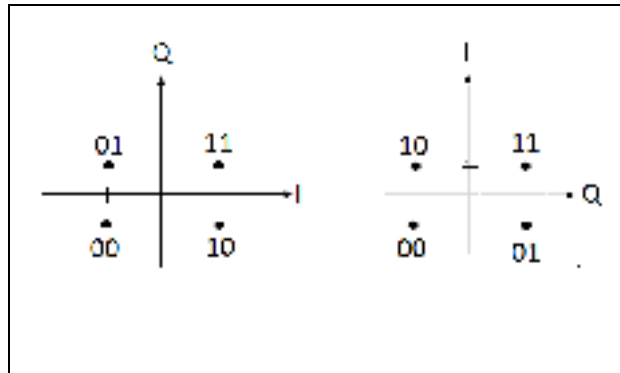


Figure 2.9 Effet de l'inversion d'I et Q sur une constellation QPSK (code de Grey)

La décomposition en quadrature de phase permet aussi d'accentuer les méthodes de brouillage abordées précédemment. Des délais aléatoires sur chaque composante créent des effets multitrajets impossibles naturellement et des variations d'amplitude aléatoire sur chaque composante ne peuvent être compensées par un AGC unique. La figure 2.10 montre l'effet d'un brouillage indépendant sur les composantes I et Q d'un signal complexe simple constitué d'un sinus et d'un cosinus.

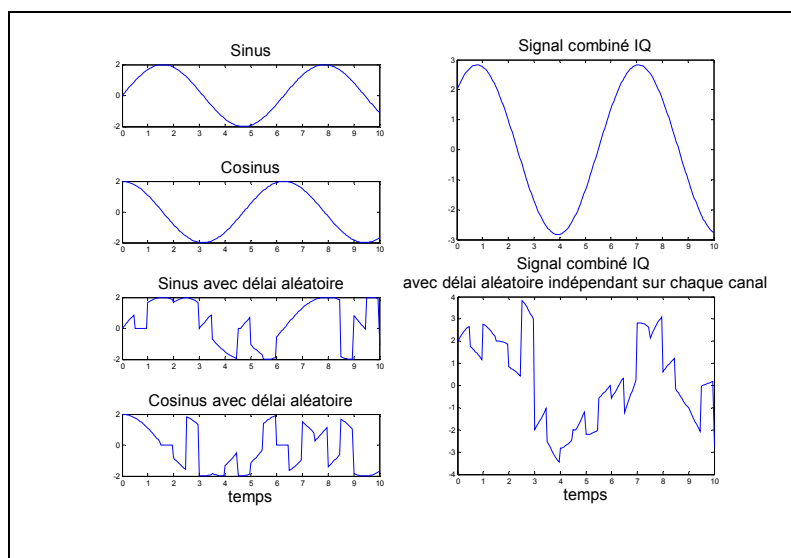


Figure 2.10 Effet d'un délai aléatoire indépendant sur les signaux I et Q
Adaptée de MathWorksInc (2009)

2.3 Application avancée liée à la problématique

Les techniques de brouillage par numérisation RF offrent deux avantages majeurs. Une grande largeur de bande et un contrôle accru sur le traitement du signal. Il est possible d'utiliser ces avantages pour créer un brouillage dont les modifications appliquées au signal sont connues et réversibles. Un récepteur numérique spécial ayant accès aux paramètres du brouillage par mémorisation RF pourrait théoriquement reconstruire le signal en appliquant le traitement de signal inverse. Un tel système permettrait de résoudre la majorité des défis posés par la problématique en offrant une méthode de protection RF sans limiter les communications alliées.

Le système requis pour cette opération présente plusieurs défis. Pour permettre au récepteur de connaître les modifications effectuées sur le signal, l'algorithme pseudo-aléatoire utilisé par le DRFM doit être réalisé de manière synchrone sur les deux appareils. De plus, le brouillage doit être suffisamment efficace pour bloquer les communications indésirables sans causer de pertes d'informations sur la communication principale.

Avant de concevoir une radio DRFM capable de brouiller et de communiquer, l'efficacité des techniques de brouillage avancées proposées doit être testée pour savoir si elles sont capables de répondre aux exigences d'un tel système.

2.4 Résumé

Les techniques de mémorisation numérique RF utilisent des conversions ADC et DAC très rapides pour recevoir, enregistrer et transmettre toutes les communications numériques sur une large bande de fréquences. En ajoutant un traitement numérique sur le signal reçu, on peut créer une méthode de brouillage avancée par traitement de signal rapide. Une radio DRFM peut ainsi brouiller un signal de base en lui superposant une version similaire, mais déformée. Un banc de test capable de tester ces méthodes de brouillage est présenté dans le chapitre suivant.

CHAPITRE 3

Environnement de tests

3.1 DRFM Lacime

Pour des fins de recherche, Yannick Vallée du laboratoire Lacime a conçu un appareil DRFM capable d'effectuer les opérations de numérisation et de traitement de signaux. Le programme implémenté couvre plusieurs fonctions incluant des techniques de brouillage avancées, l'émulation des brouillages classiques et la création de signaux (Lacime, 2013).

3.1.1 Fonctionnement

Le cœur du DRFM est constitué d'une carte d'évaluation Xilinx ML605. Cette carte permet l'utilisation d'un FPGA Virtex 6 en conjonction avec une carte d'acquisition FMC110 de la compagnie 4DSP. La carte d'évaluation fournit les options nécessaires pour programmer et contrôler la carte d'acquisition ainsi que le FPGA. Les opérations de mise en mémoire et de traitement de signaux sont codées en VHDL dans le Virtex 6. Le contrôle des opérations est effectué avec un code C++ qui transmet les commandes par protocole Ethernet au moyen de la carte ML605. La figure 3.1 montre le schéma bloc du DRFM constitué de la carte ML605 et FMC110, le tout contrôlé par ordinateur.

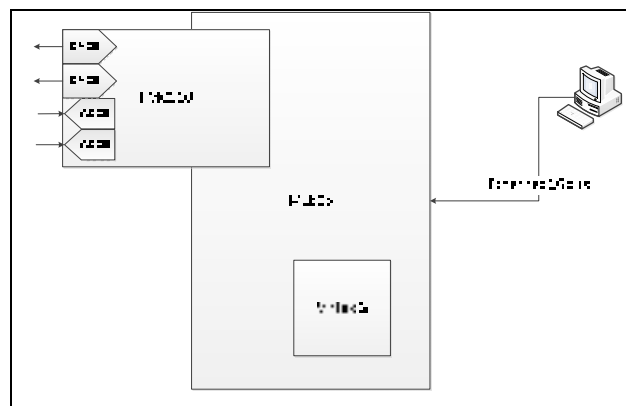


Figure 3.1 Schéma bloc DRFM

3.1.2 Spécifications

Tel que mentionnée au chapitre 2, la bande passante pouvant être contrôlée par un DRFM est définie par la vitesse d'échantillonnages (équation 2.1). Les convertisseurs ADC 1Gsample/sec permettent d'atteindre une bande passante d'environ 500MHz pour un signal simple bande ou d'approximativement 1 GHz pour un signal à bande double. Cette valeur est affectée par les filtres ainsi que par les performances des composantes. La figure 3.2 montre la réponse fréquentielle entre les conversions d'entrée et de sortie (Lacime, 2013). Elle illustre que la réponse du système DRFM n'est pas égale sur toute la plage de 500 MHz. Une étape d'égalisation pourrait être ajoutée pour améliorer la régularité d'amplitude de la réponse, mais n'est pas nécessaire dans le cadre de l'étude.

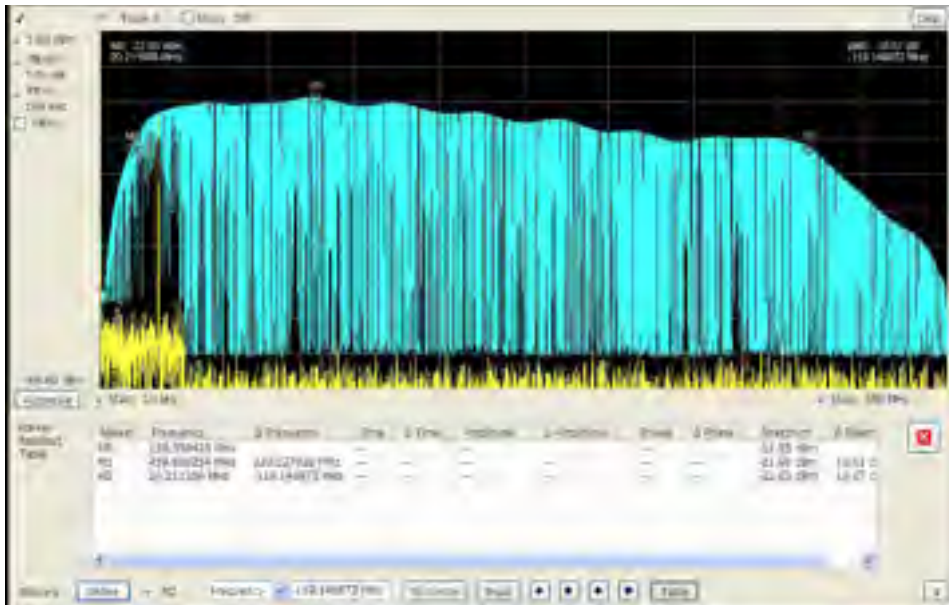


Figure 3.2 Réponse fréquentielle entre les convertisseurs ADC et les convertisseurs DAC

La bande passante pourrait théoriquement être doublée par la décomposition du signal reçu en ses composantes en quadrature de phase. Cette opération ne fonctionne pas au moment de la rédaction de ce mémoire ; le DRFM effectue la conversion du même signal deux fois. La majorité des opérations de fonctionnement et de conversions sont contrôlées à l'aide d'un code VHDL fourni par la compagnie 4DSP, programmé dans le FPGA VIRTEX 6 et modifié pour accommoder la carte ML605. Les figures 3.3 et 3.4 présentent le chemin parcouru par

l'information dans le DRFM avec conversion complexe et sans conversion. Le bloc dénoté DRFM regroupe les différentes partitions de codes VHDL supplémentaires effectuant les opérations de traitements et de génération de signaux. Les opérations de conversions et de traitement de signaux ajoutent à elles seules une latence autour des 215 ns au signal du DRFM (Lacime, 2013).

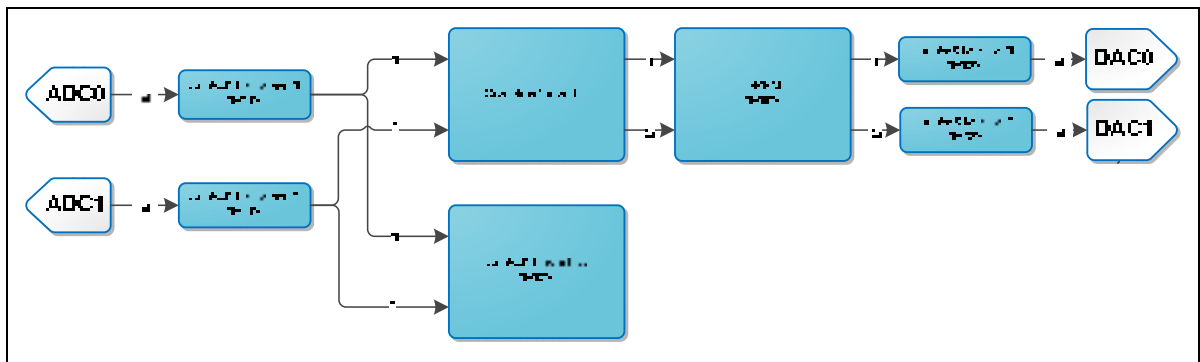


Figure 3.3 Chemin des données pour DRFM avec conversion complexe (bande double)

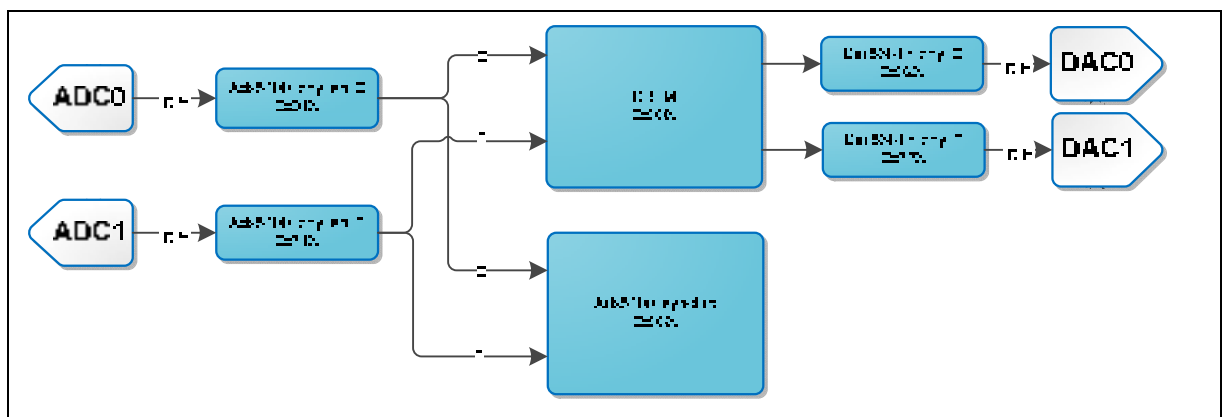


Figure 3.4 Chemin des données pour DRFM sans conversion complexe (bande latérale unique)

3.1.3 Radio DRFM

Pour effectuer des tests sur les plages de fréquences commerciales, le DRFM est intégré à une chaîne RF pour créer une Radio DRFM. Une carte d'évaluation TRF372017 est utilisée pour contrôler la conversion en fréquence hétérodyne. Cette carte fournit la fréquence à l'oscillateur local de la réception et effectue la modulation avant la transmission. Le contrôle de la carte TRF37201 est effectué par port USB, et le système complet peut fonctionner entre les fréquences de 50 MHz à 3,3Ghz. La figure 3.5 illustre le diagramme simplifié de la chaîne de composante RF connectée au cœur du DRFM. Le diagramme fonctionnel complet est inclus dans l'annexe I (Lacime, 2013).

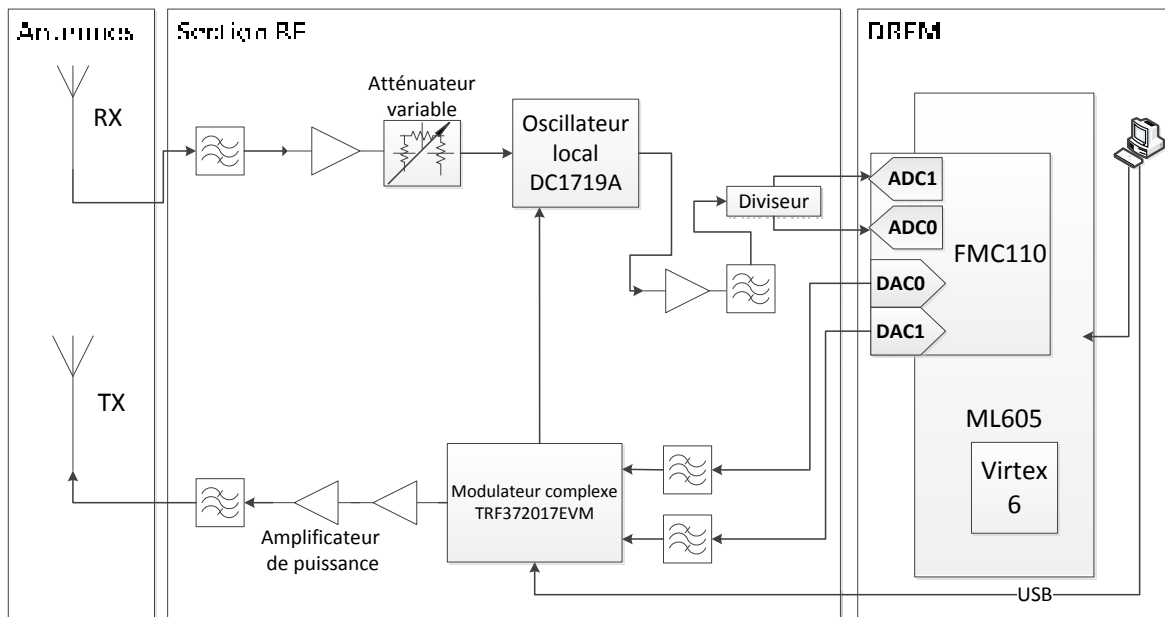


Figure 3.5 Diagramme fonctionnel simplifié de la radio DRFM Lacime

3.2 Techniques de brouillage implémentées

Plusieurs techniques de brouillage ont été programmées dans le DRFM. Les techniques sont réalisées sur le FPGA VIRTEX 6, programmé de façon appropriée avec une compilation d'un code source VHDL. La figure 3.6 présente les différents blocs de codes, associés à des

fonctionnalités de traitement de signal, par lesquels passent les données entre les deux convertisseurs. Chacun des deux chemins de données contient le code pour les techniques avancées. Le programme du DRFM contient également un bloc de code capable de générer des formes d'ondes simples (générateur de signaux) ainsi qu'un bloc capable d'émuler les techniques de brouillage standards (générateur d'interférences). Le bloc générateur de signaux sert à des fins de tests de fonctionnement et le générateur d'interférences sera utilisé pour comparer les techniques de brouillages avancées avec les techniques classiques.

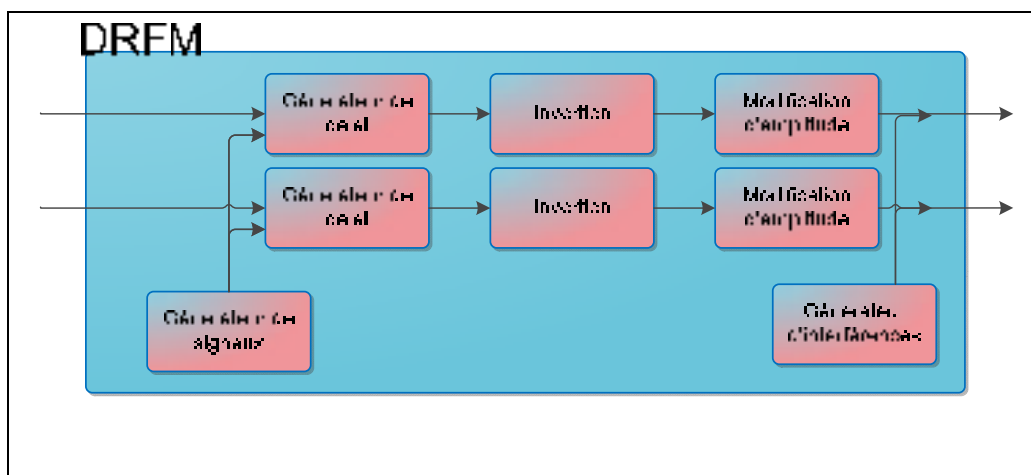


Figure 3.6 Chemin des données du code DRFM
Tirée de Lacime (2013)

3.2.1 Variation d'amplitude aléatoire

La variation de l'amplitude du signal est effectuée par la multiplication des échantillons en mémoire par un entier relatif aléatoire. Ce nombre est obtenu à l'aide d'un algorithme générateur de nombres pseudo-aléatoires uniformes nommés « Mersenne Twister » (Matsumoto et Nishimura, 1998). Cet algorithme est utilisé pour générer des nombres aléatoires ayant une distribution continue sur 32 bits. La figure 3.7 illustre la distribution de la fonction de probabilité d'une valeur aléatoire uniforme discrète (Papoulis, 2002). Contrairement à une distribution parfaitement uniforme, toutes les valeurs ne peuvent être atteintes, ce qui risque d'affecter les performances du brouillage.

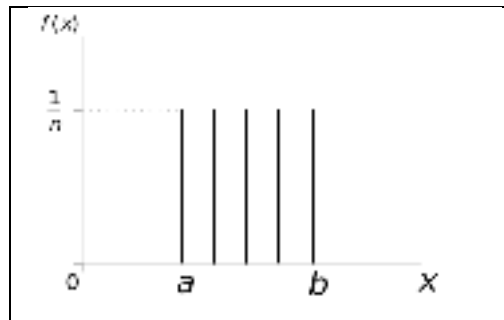


Figure 3.7 Densité de probabilité d'une variable aléatoire uniforme discrète

Les valeurs obtenues sont ensuite tronquées de 1 à 12 bits selon les paramètres du brouillage et utilisées comme valeurs de multiplication. L'impact sur le signal dépend du nombre de bits, un entier à 12 bits aura un impact plus grand qu'un entier à 6 bits. Peu importe le nombre de bits, le multiplicateur traite cette valeur comme une fraction entre 0 et 1. Plus l'entier est long (nombre de bits), plus cette fraction peut être proche de 0. Le résultat de l'opération est presque toujours une diminution du niveau du signal de base et est exempt d'inversion. Cette méthode n'est pas la plus efficace, mais elle permet de limiter le niveau de sortie du signal et de diminuer les risques de bris d'équipements (Lacime, 2013). La valeur de multiplication varie à un intervalle d'échantillonnage fixe pouvant être choisi entre 1 et 32 768, une valeur temporelle approximative entre 1 ns et 32 μ s. La figure 3.8 présente le schéma bloc du brouillage ainsi que son effet sur un signal sinusoïdal si l'amplitude varie à chaque 10 μ s. Les limites de l'entier de multiplication et le nombre d'échantillons entre deux variations sont définis dans le registre associé au brouillage par variation d'amplitude aléatoire (annexe IV) (Lacime, 2013).

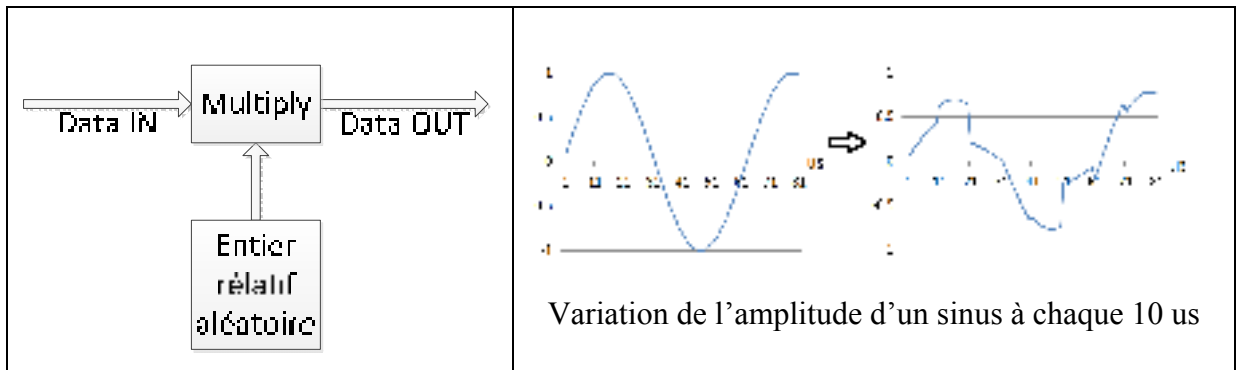


Figure 3.8 Brouillage par variation d'amplitude

3.2.2 Variation du délai de transmission aléatoire

La variation du délai de transmission du signal est réalisée à l'aide d'un mémoire vive à doubles ports et à pointeur variable. Le signal échantillonné est enregistré dans une mémoire vive SRAM pour créer une mémoire tampon circulaire. Ensuite, l'adresse de lecture du pointeur de sortie est modifiée aléatoirement en utilisant une variable aléatoire obtenue avec un algorithme « Mersenne Twister » (Matsumoto et Nishimura, 1998). Le décalage temporel des échantillons est similaire à un délai de propagation. Le changement de délai est effectué à un intervalle fixe d'échantillonnage pouvant être choisis entre 1 et 32 768, une valeur temporelle approximative entre 1 ns et 32 us. La taille maximale du délai dépend de la taille de notre mémoire et de la taille du nombre aléatoire. Pour notre système, la valeur aléatoire est limitée à 12 bits, ce qui permet un délai maximal pouvant être atteint d'environ 4 us. Il est aussi important de considérer la latence du système DRFM qui ajoute déjà un délai autour de 215 ns au signal. La figure 3.9 présente le schéma bloc du brouillage et son effet sur un signal sinusoïdal pour un changement de délai toutes les microsecondes. Les limites de la variation du délai et le nombre d'échantillons entre deux variations sont définis dans le registre associé au brouillage par variation de délai aléatoire (annexe IV) (Lacime, 2013).

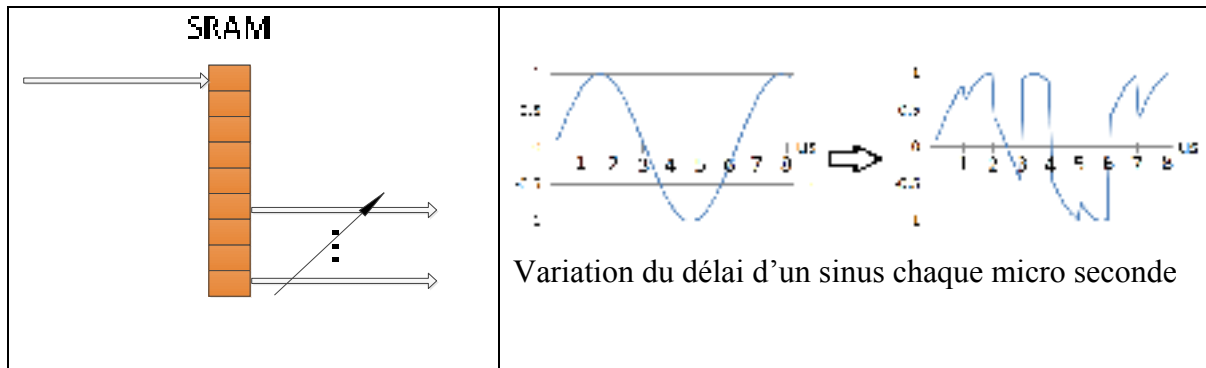


Figure 3.9 Brouillage par variation de délai

3.2.3 Techniques classiques

Les brouilleurs classiques n'ont généralement pas la capacité d'effectuer les opérations de traitement de signaux. Tel que mentionné au chapitre 2, ces systèmes utilisent des signaux à haute puissance pour nuire aux communications. Pour comparer ces méthodes aux nouvelles méthodes proposées, un code a été ajouté au DRFM. Ce code créé par Gaëtan Racid, est capable de générer ou de simuler la majorité de ces techniques directement et est situé dans le bloc générateur d'interférences de la figure 3.6.

La première technique de brouillage classique implémentée est le brouillage par l'ajout de bruit blanc. Le système utilise une mémoire ROM contenant une série d'échantillons correspondant à la réalisation de plusieurs processus blancs gaussiens. Cette méthode a comme défaut majeur que la série est corrélée à 100 % sur la taille de la mémoire, mais elle est suffisante pour les tests à effectuer.

Pour brouiller une fréquence uniquement, une méthode de brouillage « spot » est élaborée utilisant un accumulateur de phase. Une période de signal sinusoïdal est échantillonnée, puis sauvegardée dans une mémoire ROM double ports. Une fois que la fréquence désirée est connue, le code mesure la taille du saut d'échantillons requis dénoté par « step ». Les échantillons sont ensuite extraits de la mémoire utilisant le saut calculé pour générer la

fréquence requise, puis l'acheminer à la file d'attente FIFO du convertisseur DAC. La fréquence du signal de brouillage F_{out} est :

$$F_{out} = \frac{F_{DAC}}{N} * step \quad (3.1)$$

où « N » est le nombre d'échantillons sauvegardés, « F_{DAC} » est notre fréquence du convertisseur de sortie et « step » est le saut d'échantillons calculé pour atteindre la fréquence désirée. La mémoire utilisée contient 2^{15} (32 768) échantillons pour la période du signal. Cette valeur permet de calculer la fréquence minimale F_{min} :

$$F_{min} = \frac{F_{DAC}}{N} * 1 = \frac{1GHz}{2^{15}} = 30.5KHz \quad (3.2)$$

pouvant être généré par le brouillage « spot ». (Lacime, 2013)

Pour brouiller une plus grande plage de fréquences, une méthode similaire est utilisée afin de créer un brouillage par balayage. Pour implémenter cette méthode, un accumulateur de phase similaire à celui de la méthode « spot » est utilisé. Pour varier la fréquence de brouillage, la valeur du saut d'échantillons utilisé « step » (équation 3.1) varie périodiquement dans un intervalle déterminé. Les caractéristiques de ce brouillage dépendent de plusieurs facteurs. Les fréquences maximale et minimale du brouillage dépendent des valeurs limites du saut d'échantillons. Similairement, l'écart entre deux fréquences consécutives dépend de la taille de la variation du saut d'échantillons. Le temps où chaque fréquence est brouillée ainsi que la longueur de la période totale du balayage dépendent du temps entre deux sauts (Lacime, 2013). Cette méthode de génération de signaux permet de brouiller une grande plage de fréquence sans émettre plusieurs signaux simultanément. Les effets du brouillage correspondent à un brouillage par impulsion « pulse » sur chaque fréquence générée dont la fraction p (équation 1.23) dépend de la plage de fréquence et du temps entre les variations de saut.

La méthode de génération de signal par accumulateur de phase ne permet pas de générer plusieurs signaux simultanément et ne peut créer de brouillage par barrage. La meilleure option est de simuler le brouillage par barrage en générant le brouillage par balayage le plus étroit et le plus rapide possible pour la plage de fréquence visée. Cette méthode nommée « Chirp » varie la fréquence générée le plus souvent possible, c'est-à-dire à chaque échantillon. Le résultat est un spectre de fréquence plus lisse que le brouillage par balayage avec une apparence similaire à un véritable brouillage par barrage. Pour effectuer la variation de fréquence, un nouveau saut d'échantillons est mesuré selon les fréquences de départ et de fin du brouillage :

$$\Delta f = \frac{F2 - F1}{\Delta s} \quad (3.3)$$

$$\Delta step = \Delta f * \frac{F_{DAC}}{N} \quad (3.4)$$

où « Δf » est la déviation de fréquence entre deux échantillons consécutifs, « $F1$ » est la fréquence de départ, « $F2$ » est la fréquence de fin, « Δs » est la durée du brouillage, « $\Delta step$ » est le nouveau saut d'échantillons, « F_{dac} » est la fréquence du convertisseur de sortie et « N » le nombre d'échantillons dans la mémoire de l'accumulateur de phase (Lacime, 2013). La vitesse du traitement de signaux et des convertisseurs de sortie DAC devrait permettre d'atteindre des performances très rapprochées d'un véritable brouillage par barrage.

3.2.4 Technique non implémentée

Une opération de conversion du signal reçue en composantes complexes est programmée dans le DRFM. Cependant, les limites physiques du système empêchent le signal converti de répondre aux contraintes temporelles sur le chemin des données, et rendent le signal inintelligible. Pour cette raison, certaines techniques de brouillage avancées ne peuvent être utilisées avec le DRFM dans son état actuel. Ces techniques sont l'inversion I et Q et l'ajout

d'une variation unique sur les composantes en phase et en quadrature (Lacime, 2013). Une méthode de brouillage par effets multitrajet simple est programmée dans le bloc générateur d'interférences (figure 3.6), mais n'est pas opérationnelle au moment de la rédaction. Les échantillons sont enregistrés dans une mémoire suffisamment grande pour créer un délai additionnel sur le signal en modifiant l'adresse de lecture du pointeur de sortie (Lacime, 2013).

3.3 Banc de test

Tester les méthodes de brouillage par traitement de signaux requiert un banc de test capable de générer les signaux et de mesurer leur performance. La figure 3.10 illustre le cas d'étude d'une communication en présence de la radio DRFM où la radio DRFM se situe entre l'émetteur et le récepteur. Tel que mentionnée au chapitre 2, la présence d'un DRFM consiste en un ajout au signal de base (figure 2.6). Le signal suit donc deux chemins, un avec la présence de la radio DRFM et un avec une simple atténuation.

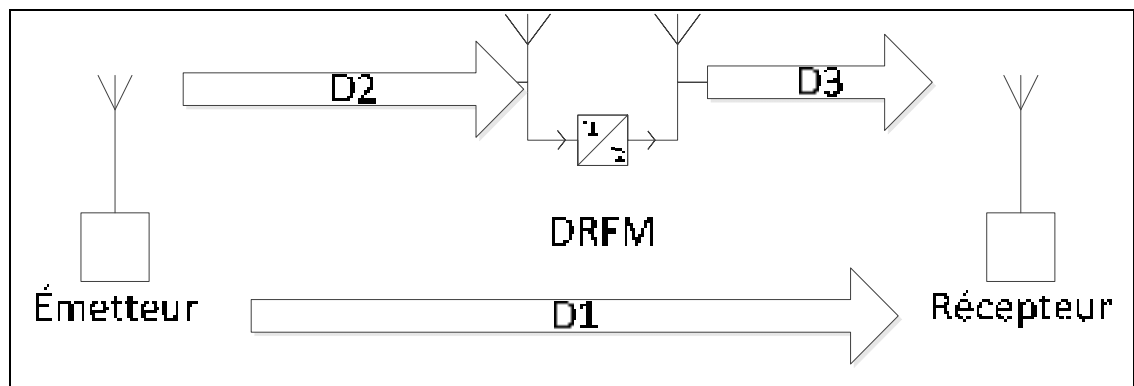


Figure 3.10 Cas d'étude : Communication en présence d'un DRFM

La figure 3.11 présente le schéma du banc de test. Le signal direct est transmis à une puissance d'environ 10 dBm et est atténué de l'ordre de - 60 dB pour simuler les pertes d'un canal RF sur une distance D1 de 10 mètres sans gain d'antenne (équation 1.6). La radio DRFM située à D2 (≈ 3 m) reçoit un signal de - 50 dBm (équation 1.6) qu'elle doit amplifier

avant de le retransmettre. Cependant, ce niveau de puissance à la réception rend la démodulation difficile. Pour faciliter la prise de mesures, un banc de tests plus simple a été conçu, ayant moins d'atténuation et une puissance à la réception plus grande. La figure 3.12 illustre le schéma bloc du banc de test utilisé pour la prise de mesure. La puissance à la réception du signal en chemin direct est de l'ordre de -30 dBm. Cette valeur est choisie pour rester dans la plage optimale de l'analyseur de spectre (R&S, 2011). La radio DRFM reçoit le signal directement et la puissance provenant de la radio DRFM est atténuée de valeurs allant de -70 dBm à -10 dBm.

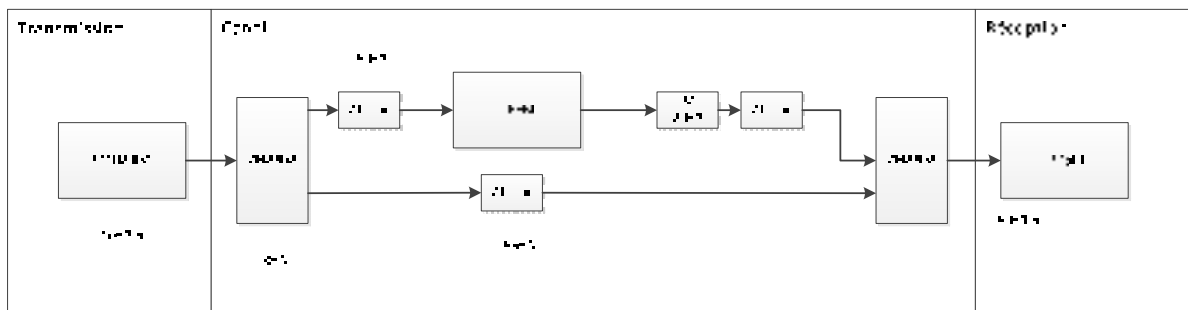


Figure 3.11 Schéma bloc du banc de tests idéal

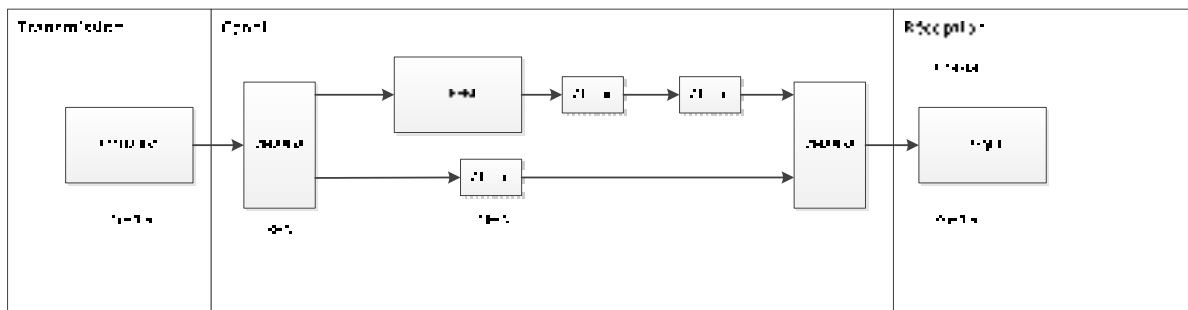


Figure 3.12 Schéma bloc du banc de tests réel

3.3.1 Équipement

Les deux équipements principaux sont le générateur de signaux à la transmission et l'analyseur vectoriel à la réception. Le générateur de signaux utilisé est le « SMU200A » de la compagnie Rhodes & Schwarz. Cet appareil est un générateur de signaux vectoriels capable de générer plusieurs types de modulations suivant les standards de communication sans fil simple et multiporteuse. Le SMU200A effectue aussi la modulation RF avec une plage de fréquence de 100 KHz à 6 GHz (R&S, 2012)]. Le FSQ40 est un analyseur de signaux vectoriel capable de mesurer l'EVM « Error Vector Magnitude » ou le module moyen du vecteur d'erreur de la majorité des standards courants de signaux cellulaires. Sa plage de fréquence, 20 Hz à 40 GHz, couvre toutes les fréquences utilisées par les appareils de téléphonie sans fil (figure 1.4). Le tableau 3.1 présente les options des équipements utilisés dans les tests, les spécifications détaillées des appareils sont données à l'annexe III (R&S, 2012).

Tableau 3.1 Équipement R & S avec options utilisées

SMU200A		FSQ40	
Microprogrammation	02.02.170	Microprogrammation	REV 4.25
Plage de fréquences	100 KHz -- 6 GHz	Plage de fréquences	20 Hz – 40 GHz
Options supplémentaires pertinentes			
SMU-15	Signal OFDM sur mesure	FSQ-K-70	Analyseur de signaux vectoriel
SMU-K242	3GPP FDD	FSQ-K72	WCDMA BTS
SMU-K249	802.16	FSQ-K73	WCDMA MS
		FSG-K93	802.16e

Le canal de transmission utilisé pour les tests consiste en une série de câbles SMA et d'atténuateurs variables. Le signal est d'abord séparé également par un diviseur de puissance, puis des atténuateurs variables ajustent la puissance de chaque branche selon les besoins. L'utilisation de câbles réduit grandement les sources d'interférences naturelles qui seraient présentes dans une communication sans fil normale et permet d'observer plus en détail les effets du brouillage ajouté.

3.4 Méthodologie

3.4.1 Standards et signaux

Les technologies cellulaires ont beaucoup évolué dans les dernières années. Pour que les tests effectués soient pertinents, nous voulons que les signaux générés soient représentatifs des plus récents formats de communications. Les technologies cellulaires modernes sont divisées en générations regroupant plusieurs standards et méthodes. Les standards de signaux sont regroupés en catégorie ou génération. Pour qu'un standard soit considéré comme faisant partie d'une génération il doit remplir les préalables dictés par l'Union internationale des communications. Ces préalables ont plusieurs exigences, dont le débit nominal et l'efficacité spectrale que le standard doit atteindre (International Telecommunication Union, 2011).

La plus récente exigence est la quatrième génération ou 4G. Les deux principaux standards déployés capables de répondre aux exigences du 4G sont le WiMAX et LTE-Advance (Blust, 2012). Le standard Wimax utilise des signaux OFDMA (IEEE 802.16, 2009) alors que le LTE-Advance utilise des signaux hybrides OFDMA/SC-FDMA (International Telecommunication Union, 2012). Pour tester le 4G, le standard WiMAX est utilisé comme base de comparaison pour l'ensemble de la génération. La génération précédente, 3G, regroupe plusieurs standards incluant ceux de CDMA et de GSM. Cette génération est encore utilisée sur plusieurs appareils cellulaires. Les signaux CDMA, « code division multiple access » utilisent l'étalement spectral alors que les signaux GSM « global system for mobile

communication » sont des standards provenant de l'ancienne génération améliorée pour répondre aux demandes de la génération 3G (International Telecommunication Union, 2002). Ces standards ont des caractéristiques très différentes et doivent être testés séparément. Les signaux choisis pour les tests sont le W-CDMA et le GSM-EDGE. Les signaux WiMAX et 3G sont générés à l'aide du logiciel R&SWinQSIM2 de la compagnie Rohde & Shwarz (annexe IV).

3.4.2 Description de la prise de mesures

Pour émuler une communication cellulaire standard, les signaux de test choisis sont émis à une fréquence de 2,45 GHz. La radio DRFM est alors programmée pour écouter sur la plage de fréquence allant de 2,4 GHz à 2,9 GHz. L'efficacité des techniques de brouillage implémentées est testée par progression logarithmique de la puissance émise. Le signal du brouilleur est initialement émis avec une très basse puissance, puis celle-ci est graduellement augmentée jusqu'à ce que la puissance maximale soit atteinte ou que le signal de communication soit indéchiffrable. La figure 3.13 présente la progression de la puissance du DRFM et de la communication RF lors de la prise de mesure, chaque mesure correspond à une augmentation de la puissance du DRFM de 5 dB.

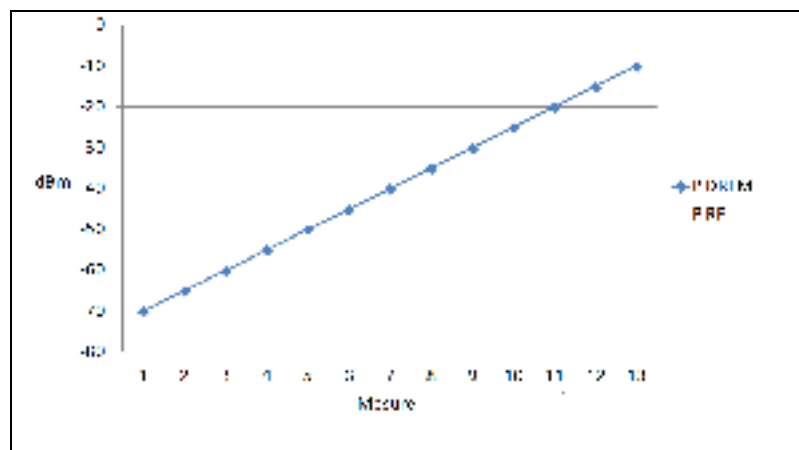


Figure 3.13 Progression des puissances lors de la prise de mesures

Notre but est de tester l'efficacité des nouvelles méthodes de brouillage implémentées dans la radio DRFM. Certains paramètres ont un impact direct sur l'efficacité du brouillage, soit la variation d'amplitude et le délai aléatoire. Ces paramètres sont maximisés, c'est-à-dire qu'ils sont configurés avec la plus grande plage aléatoire de valeurs possibles. L'impact de la rapidité entre deux variations aléatoires est moins certain. Pour mesurer cet impact, deux séries de tests sont effectuées pour chaque standard. Une série de tests utilise une variation rapide du brouillage (chaque ≈ 10 échantillons), et une autre série de tests utilise une variation lente du brouillage (chaque $\approx 32\,000$ échantillons). Chaque standard est également soumis aux techniques de brouillage classiques générées par notre radio DRFM afin de comparer les méthodes de brouillage entre elles.

La métrique standard de mesure d'efficacité pour une technique de brouillage est la mesure du TEB. Par contre, cette mesure est difficile à obtenir, car elle requiert une démodulation et un décodage du signal synchronisé pour comparer les bits envoyés et reçus en temps réel. De plus, dans les cas où le TEB est très bas, obtenir une mesure fiable requiert de très longs temps d'attente. Pour simplifier la prise de mesure, on utilise la métrique EVM qui peut être mesurée directement sur le signal reçu avec l'analyseur de spectre. Pour les standards utilisant des signaux I/Q avec constellations carrées (M-QAM), l'EVM mesuré peut ensuite être converti en TEB utilisant l'équation 3.5 :

$$BER \approx \frac{2\left(1 - \frac{1}{L}\right)}{\log_2 L} Q\left[\sqrt{\frac{3 \log_2 L}{L^2 - 1}} \frac{2}{EVM_{RMS}^2 \log_2 M}\right] \quad (3.5)$$

où « L » est le nombre de niveaux sur chaque dimension de la constellation, « M » est le nombre de points et « EVM_{RMS} » est la mesure moyenne du vecteur d'erreur (Shafik, Rahman et Islam, 2006). Le TEB obtenu est mis en relation au rapport des puissances SIR :

$$SIR = \frac{P_{re\acute{c}ue}}{P_{DRFM}} \quad (3.6)$$

où « SIR » est le rapport signal interférence, « $P_{\text{re\c{c}ue}}$ » est la puissance de la transmission originale à la réception et « P_{DRFM} » est la puissance du signal d'interférence à la réception. Les puissances sont mesurées au récepteur pour obtenir une meilleure comparaison des impacts entre les différents brouillages par traitement de signaux rapide et brouillage par méthodes classiques. La mesure pour les techniques classiques est la puissance totale sur la bande passante du signal de base. Cette méthode nous permet d'obtenir facilement des courbes de performance comparables avec la théorie pour les signaux utilisant des constellations M-QAM. Pour l'analyse des standards n'utilisant pas une constellation IQ carrée, les mesures directes de l'EVM sont utilisées.

3.5 Résumé

En résumé, pour effectuer l'analyse et la comparaison des différentes méthodes de brouillage, un banc de test a été conçu ayant comme élément central une radio DRFM fabriquée par Yannick Vallée pour le laboratoire Lacime (Lacime, 2013). Cette radio DRFM permet via contrôle logiciel d'effectuer tous les brouillages, avancés et classiques, nécessaires à l'étude. Pour la communication numérique, on utilise des appareils SMU200A et FSQ40 de la compagnie Rohde & Schwarz pour générer les signaux cellulaires et effectuer la prise de mesure (R&S, 2012). Les signaux ainsi générés suivent les standards commerciaux utilisés en téléphonie cellulaire, leurs caractéristiques ainsi que les résultats obtenus sont présentés dans les chapitres suivants.

CHAPITRE 4

Analyse pour la marque WiMAX

4.1 WiMAX

Le WiMAX est un format de communication sans fil longue distance basé sur la norme IEEE802.16 (IEEE 802.16, 2009). Il appartient à la quatrième génération de communications sans fil 4G et peut atteindre des débits de 1 Gbit/s (Blust, 2012). Ce standard est surtout utilisé pour fournir une connexion Internet sans fils ainsi que pour la téléphonie cellulaire. Les bandes de fréquences allouées pour le WIMAX sont : 2,3 GHz, 2,5 GHz et 3,5 GHz (R&S, 2006).

La norme 802.16 définit plusieurs aspects de la communication, mais pour une problématique de brouillage, l'information sur la couche physique est la plus pertinente. La couche physique utilise une méthode appelée « orthogonal frequency-division multiplexing » ou OFDM, où les données sont séparées et assignées à différentes sous-porteuses orthogonales (IEEE 802.16, 2009). Des signaux orthogonaux sont positionnés de manière à annuler les interférences lors du décodage. La figure 4.1 illustre comment les sous-porteuses peuvent être agencées pour qu'à leurs sommets l'interférence des autres sous-porteuses soit nulle (Heiskala et John Terry, 2001).

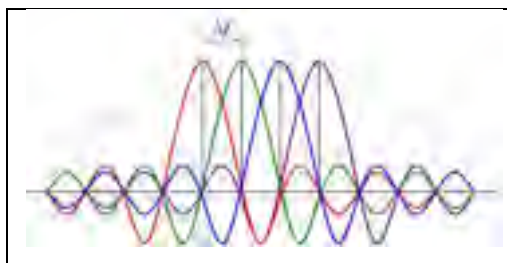


Figure 4.1 Groupe de porteuses orthogonales
Tiré de Heiskala et John Terry (2001)

La figure 4.2 présente un émetteur OFDM idéal (Fith, 2006). Les données sont converties de manière parallèle en points de constellations puis soumises à une transformée de fourrier inverse (IFFT). Le résultat de la transformée est modulé en quadrature de phase et envoyé par une porteuse principale. Le signal ainsi créé est appelé une trame de données, car il contient l'information de plusieurs points de constellation sous la forme d'un résultat de IFFT. À la réception, la trame de données subit l'opération inverse pour décoder les données originales. La figure 4.3 présente un récepteur OFDM idéal qui effectue la transformée de fourrier (FFT) pour récupérer chaque sous-porteuse (Fith, 2006). Le récepteur prend ensuite une décision sur les points de constellations reçus pour recréer le signal original.

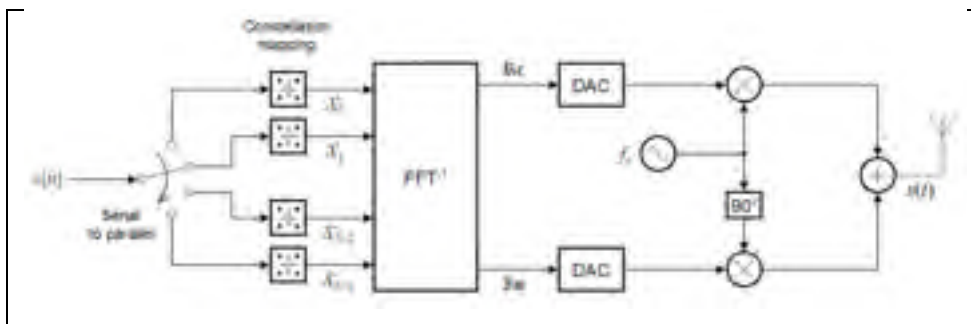


Figure 4.2 Émetteur idéal OFDM
Tirée de Fith (2006)

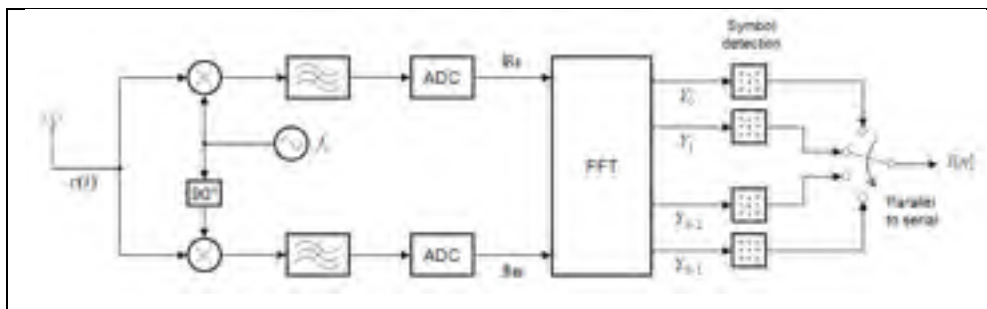


Figure 4.3 Récepteur idéal OFDM
Tirée de Fith (2006)

Ce type de signaux peut être utilisé pour desservir plusieurs utilisateurs. Pour ce faire, un groupe de sous-porteuses est assigné à chaque utilisateur. Cette méthode est appelée « orthogonal frequency-division multiple access » OFDMA et est utilisée dans les versions plus récentes du standard 802.16 (IEEE 802.16, 2009). Une communication OFDM/OFDMA est caractérisée par deux taux de transfert : le taux de symboles par seconde et le taux de données par seconde. Le taux de données par seconde de la transmission est déterminé par le nombre de porteuses de données, lui-même déterminé par la taille de la FFT ainsi que par la modulation utilisée sur chaque porteuse soit : BPSK, QPSK, 16QAM ou 64QAM (IEEE 802.16, 2009).

Une grande difficulté des communications OFDM/OFDMA est la synchronisation des trames (IEEE 802.16, 2009). C'est pourquoi les porteuses ne transportent pas toutes des données, plusieurs porteuses servent de pilotes pour aider à la synchronisation de la trame et d'autres sont utilisées pour créer une zone de garde (IEEE 802.16, 2009). La figure 4.4 présente un exemple de trame WiMAX dans le domaine fréquentiel. Plusieurs sous-porteuses servent de pilotes et une bande de garde est utilisée de chaque côté de la trame. La sous-porteuse correspondant à un voltage DC est supprimée pour faciliter le traitement (IEEE 802.16, 2009). Le nombre de pilotes dépend de la taille de la FFT, elle-même dépendant du nombre d'utilisateurs servis. Pour les communications WiMAX, ou plus précisément pour les communications utilisant le standard 802.16, la taille de la FFT peut être de 125, 256, 512, 1024 et 2048 points (IEEE 802.16, 2009). Un autre aspect important de la communication WiMAX est l'utilisation d'un préfixe cyclique. Lors de la transmission, la fin de la trame ou symbole OFDM est copiée au début. Ceci permet de diminuer l'interférence entre les symboles pouvant être causée par un canal multitrajet comme c'est souvent le cas en communications sans fil. La figure 4.5 montre un exemple de trame OFDM dans le temps utilisant un préfixe cyclique (R&S, 2006).

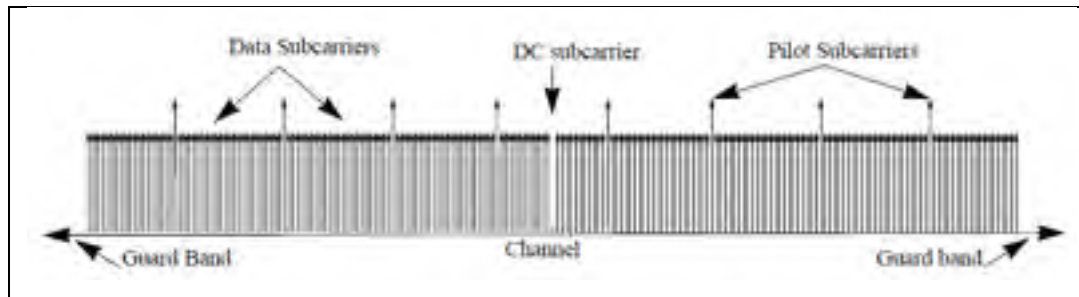


Figure 4.4 Trame WIMAX dans le domaine fréquentiel
Tirée de IEEE 802.16 (2009)

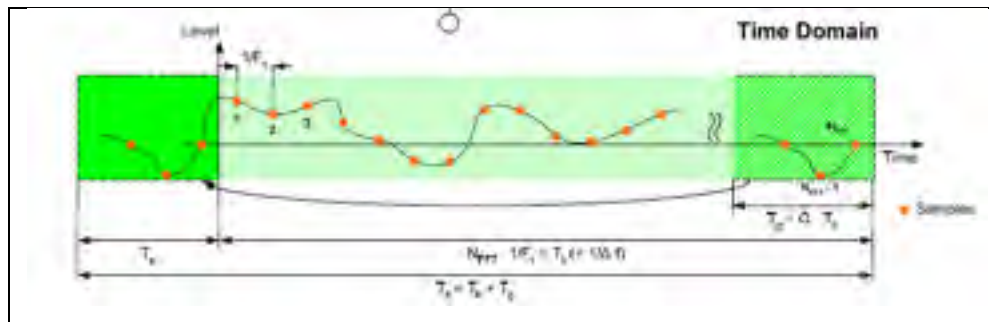


Figure 4.5 Trame Wimax dans le domaine temporel avec préfix cyclique
Tirée de R&S (2006)

4.2 Signaux générés

Les signaux WiMAX peuvent avoir plusieurs formes et même être dynamiques dans le temps. Pour les tests, un signal uniforme dans le temps est utilisé afin de faciliter l'analyse, mais toutes les formes de constellations possibles sont testées. Le tableau 4.1 décrit les caractéristiques des signaux générés pour les tests. La figure 4.6 présente la forme fréquentielle que prend un signal WiMAX avant et après la FFT, les puissances des porteuses orthogonales s'additionnent pour créer un bloc de signaux sur la largeur de la bande passante, ici 7 MHz.

Tableau 4.1 Caractéristiques des signaux WiMAX utilisés

Caractéristiques communes		
Nombre de points de la transformée (Nfft)		256
Bande passante (BW)		7MHz
Temps du symbole (Ts)		5 ms
Tg/Tb (figure 4.5)		$\frac{1}{4}$
Fréquence centrale		2,45 GHz
Caractéristiques par constellation		
BPSK	Nombre de points	2
	Niveaux par dimension	2
	EVM limite	- 13 dB
QPSK	Nombre de points	4
	Niveaux par dimension	2
	EVM limite	- 18.5 dB
16QAM	Nombre de points	16
	Niveaux par dimension	4
	EVM limite	- 25 dB
64QAM	Nombre de points	64
	Niveaux par dimension	8
	EVM limite	- 31dB

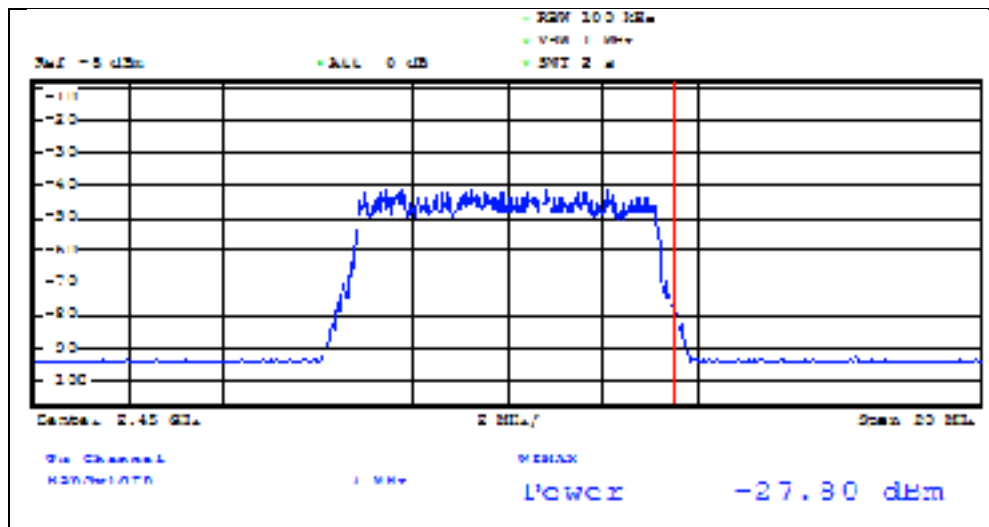


Figure 4.6 Mesure du spectre d'un signal WiMAX

4.3 Effets du brouillage par variation de délai aléatoire

Le brouillage par variation de délai aléatoire tente de nuire à la communication en créant une interférence similaire à un effet multitrajet. Comme mentionné précédemment, les signaux WiMAX utilisent un préfixe cyclique qui permet de contrer les effets d'une propagation multitrajet. La figure 4.7 illustre le temps de garde créé par le préfix cyclique sur le symbole. Aussi longtemps que le délai de propagation $\tau_{\max}$ est plus petit que la durée du préfix cyclique, la réception du symbole devrait s'effectuer sans problème (R&S, 2006). Pour nuire à la communication, notre brouillage par variation de délai devra surpasser la protection du préfixe cyclique. La plage entre deux variations de délai est une valeur fixe entre 1 et 32 768 échantillons. Pour avoir une meilleure perspective sur les effets du brouillage, deux configurations de brouillage sont utilisées : la première avec une variation du délai très rapide, l'autre avec une variation du délai beaucoup plus lente. Le tableau 4.2 décrit les caractéristiques des brouillages utilisés. Pour maximiser les effets du brouillage, une plage maximale de délai est utilisée soit entre 0 et 4 μsec . Les variations entre deux changements de délai sont de 10 échantillons pour le brouillage rapide et de 32 000 échantillons pour le brouillage lent.

Tableau 4.2 Caractéristiques des brouillages par variation de délai utilisé

	Variation rapide	Variation lente
Nombre d'échantillons entre les variations	10	32 000
Inversion du signal	non	non
Plage du délai	0 — 4 μ s	0 — 4 μ s

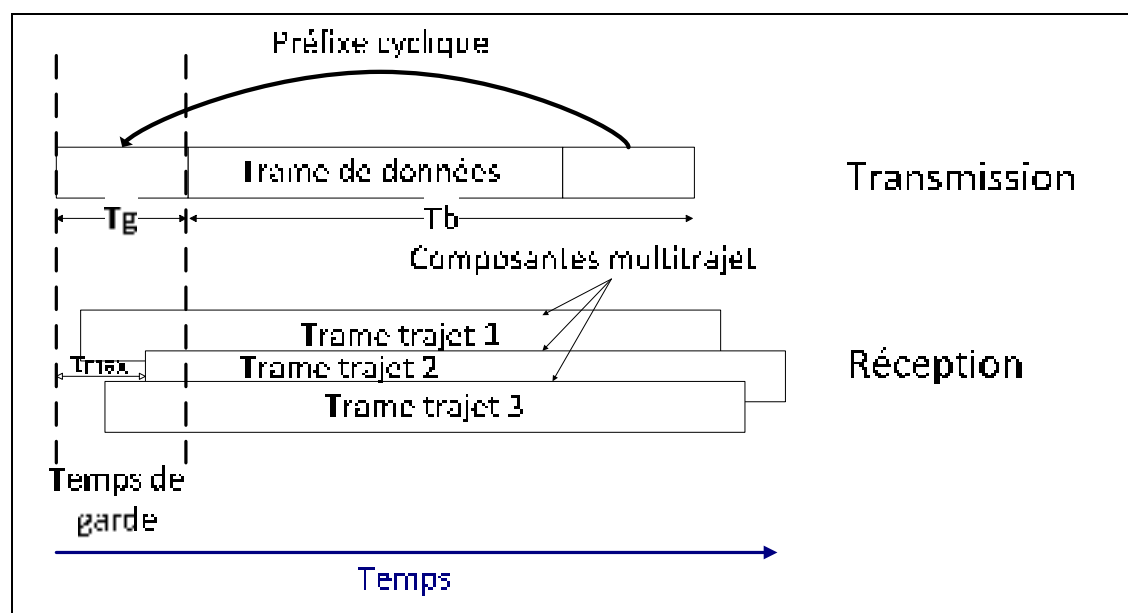


Figure 4.7 Préfixe cyclique et multitrajet

4.3.1 Variation rapide du délai

Pour le brouillage avec variation de délai rapide, le nombre d'échantillons entre chaque variation de délai est de 10, ce qui correspond à un changement à chaque 10 ns. À cette vitesse, le brouillage donne une forme au signal du brouilleur très différente du signal de base. La figure 4.8 montre l'effet du brouillage sur le signal. Beaucoup de bruit est ajouté dans les fréquences latérales et le signal tend vers la forme d'un bruit blanc sur la plage de fréquence du signal WiMAX. La figure 4.9 montre les performances du brouillage en

comparant le TEB de la communication avec le TEB théorique d'un ajout de bruit blanc gaussien sur le canal. On remarque que la performance du brouillage est très similaire aux effets du bruit blanc gaussien, ce qui est attendu étant donné la forme du signal brouillé. Ce type de brouillage fonctionne correctement et permet de dépasser l'EVM limite (tableaux 4.1) sans avoir une puissance supérieure au signal de base à la réception. Par contre, la forme du signal brouillé indique la présence de puissance ailleurs que dans la bande du signal visé. Le BPSK semble être plus affecté que prévu et son taux d'erreur se rapproche de celui du QPSK. Cette différence de performance semble erronée et sera traitée dans la section analyse.

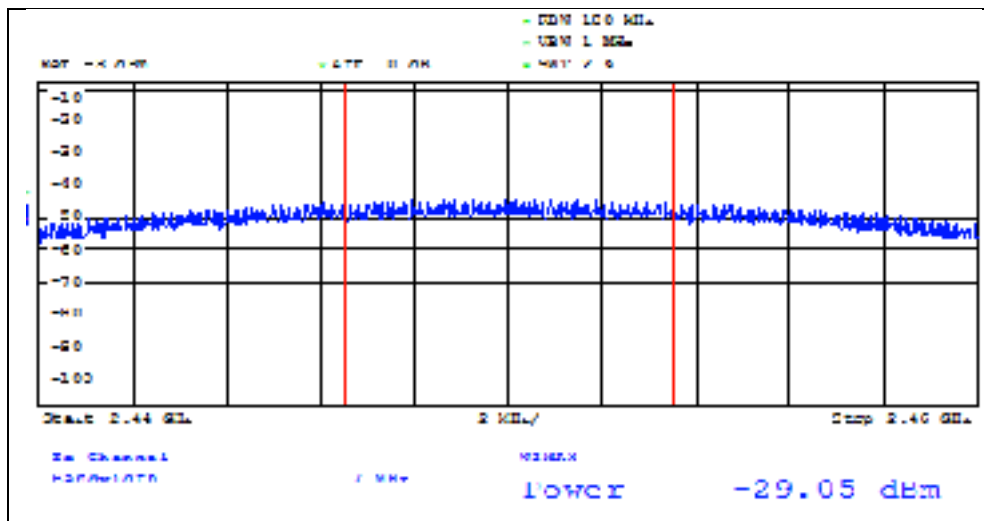


Figure 4.8 Spectre du signal WiMAX avec variation de délai aléatoire rapide

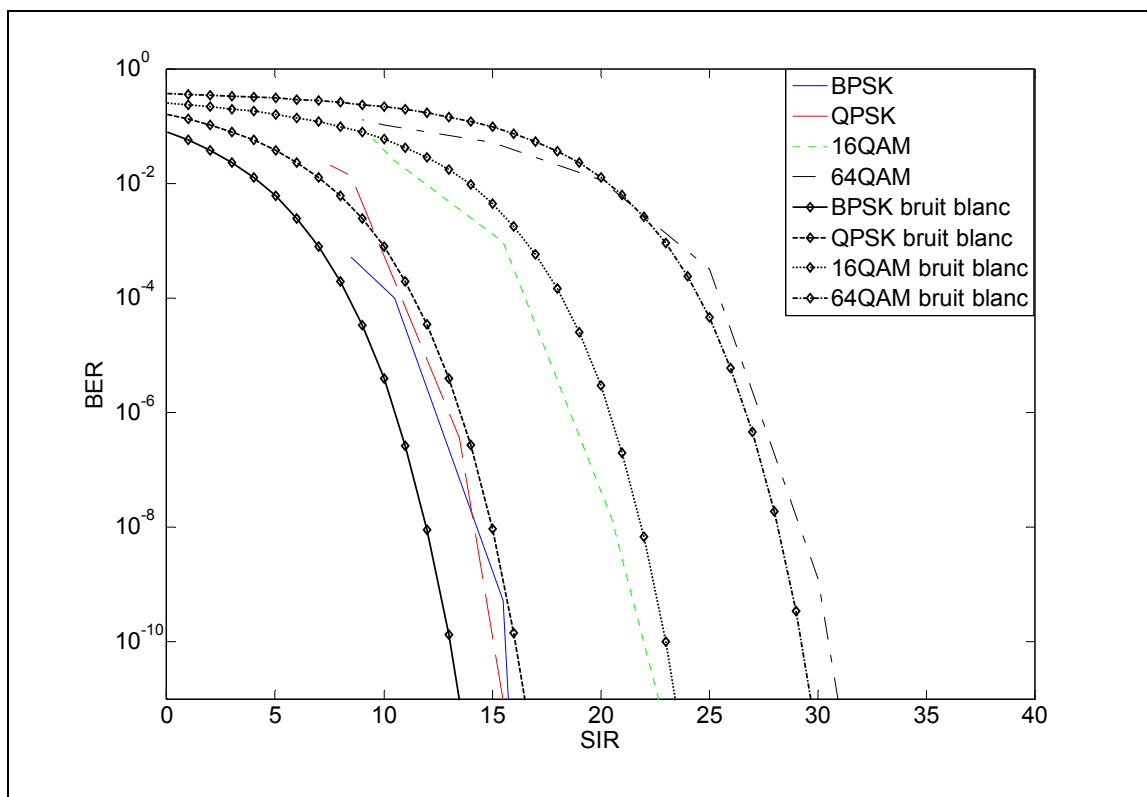


Figure 4.9 Comparaison des TEB pour un signal WiMAX avec brouillage par délai aléatoire variant chaque 10 échantillons

4.3.2 Variation lente du délai

Pour ce brouillage, le changement de délai est beaucoup moins fréquent, chaque 32 000 échantillons, ce qui correspond à un changement de délai à toutes les 32 μ s. Le signal brouillé conserve sa forme originale comme le présente la figure 4.10. La figure 4.11 trace les performances du brouillage en comparant le TEB de la communication avec le TEB théorique d'un ajout de bruit blanc gaussien sur le canal. Les performances sont moindres, mais restent proches des valeurs du bruit blanc. L'EVM limite est atteint à des puissances du même ordre de grandeur que pour la variation rapide, mais moins d'énergie est transmise dans les bandes adjacentes au signal.

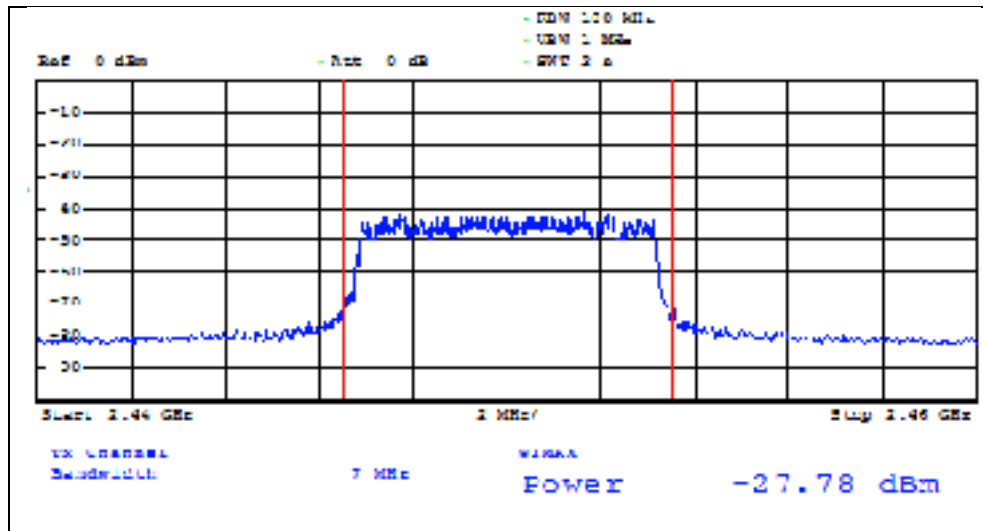


Figure 4.10 Spectre du signal WiMAX avec variation de délai aléatoire lente

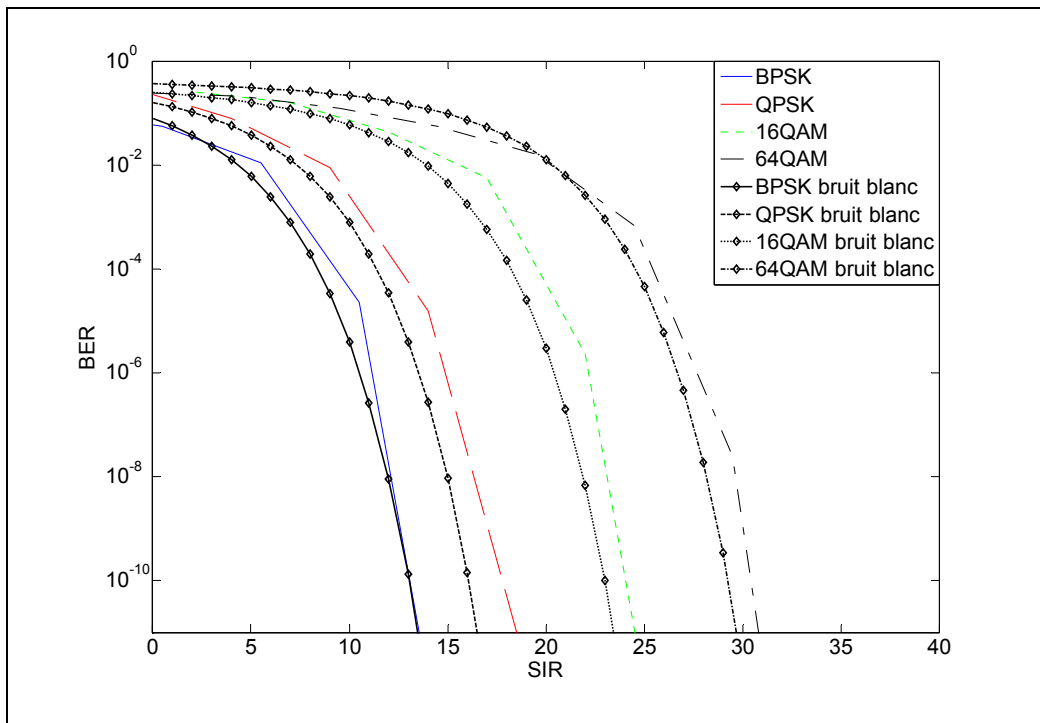


Figure 4.11 Comparaison des TEB pour un signal WiMAX avec brouillage par délai aléatoire variant chaque 32 000 échantillons

4.4 Effets du brouillage par variation aléatoire d'amplitude

Le brouillage par variation d'amplitude tente de créer une variation assez grande et assez rapide pour déjouer les AGC de la réception. Les signaux ODFM comme ceux utilisés dans le standard WiMAX utilisent une transformée de fourrier inverse IFFT, pour envoyer l'information sur la trame de données. L'information transmise est donc une série de points correspondant au résultat de la transformé (R&S, 2006). Puisque aucune démodulation n'est effectuée au DRFM, la présence du brouillage par variation d'amplitude modifie la position des points du résultat de la IFFT. Le signal reconverti est donc une combinaison du signal brouillé et du signal de base ce qui entraîne une modification de la position des points de la constellation. La plage entre deux variations d'amplitude est une valeur fixe entre 1 et 32 768 échantillons. Pour avoir une meilleure perspective sur les effets du brouillage, deux configurations de brouillage sont utilisées : la première avec une variation d'amplitude très rapide, l'autre avec une variation du délai beaucoup plus lente. Le tableau 4.3 décrit les caractéristiques des brouillages utilisés. Pour maximiser les effets du brouillage, la variation d'amplitude utilise le plus grand entier possible capable de réduire le signal à une valeur très proche de 0. Les variations entre deux changements d'amplitude sont de 10 échantillons pour le brouillage rapide et de 32 000 échantillons pour le brouillage lent.

Tableau 4.3 Caractéristiques des brouillages par variation de délai utilisés

	Variation rapide	Variation lente
Nombre d'échantillons entre les variations	10	32 000
Inversion du signal	non	non
Taille de l'entier utilisé	12 bits	12 bits

4.4.1 Variation rapide de l'amplitude

Pour le brouillage à variation rapide d'amplitude, le nombre d'échantillons entre chaque variation d'amplitude est de 10, ce qui correspond à un changement chaque 10 ns. La grande vitesse de cette variation d'amplitude est très difficile à compenser par un AGC. La figure 4.12 présente les effets de la variation d'amplitude sur la trame ODFM. Le brouillage a comme effet l'ajout de puissance sur les bandes adjacentes du signal et une diminution de la puissance dans la bande. Les performances de ce type de brouillage sont tracées à la figure 4.13 en comparant le TEB de la communication avec le BER théorique d'un ajout de bruit blanc gaussien sur le canal. Les SIR requis pour atteindre les TEB du bruit blanc sont beaucoup plus élevés et requièrent parfois un signal du DRFM plus puissant que le signal de base. Cette perte d'environ 10 dB peut être attribuée à notre algorithme de génération de nombres aléatoires suivant une loi uniforme discrète.

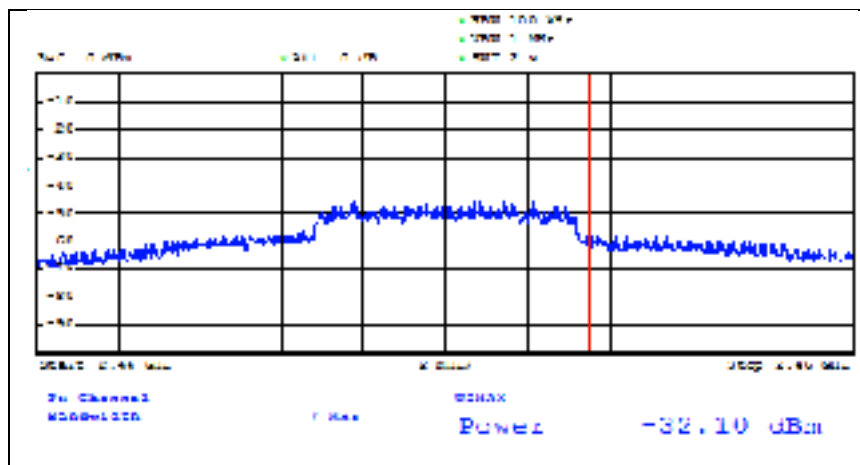


Figure 4.12 Spectre du signal WiMAX avec variation d'amplitude aléatoire rapide

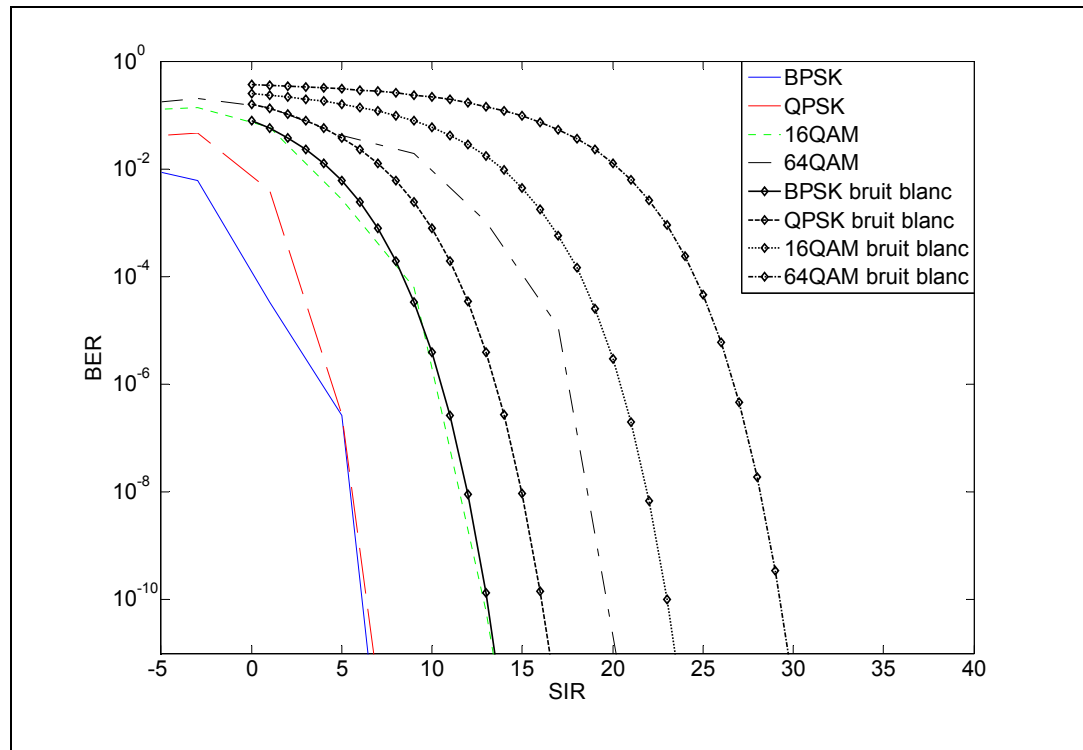


Figure 4.13 Comparaison des TEB pour un signal WiMAX avec brouillage par amplitude aléatoire variant chaque 10 échantillons

4.4.2 Variation lente de l'amplitude

Pour ce brouillage, le changement d'amplitude est beaucoup moins fréquent, chaque 32 000 échantillons, ce qui correspond à un changement d'amplitude toutes les 32 μ s. Le signal brouillé conserve sa forme originale comme présenté à la figure 4.14, mais subit une diminution de puissance importante. Puisque la trame dure 5 ms, elle subit environ 156 variations aléatoires d'amplitude avant la réception complète et la transformation par FFT. Contrairement à la variation rapide d'amplitude, les sauts de variation sont visibles sur la capture de la trame OFDM dans le domaine du temps, comme exposé à la figure 4.15. La figure 4.16 trace les performances du brouillage en comparant le TEB de la communication avec le TEB théorique d'un ajout de bruit blanc gaussien sur le canal. Les performances sont inférieures au brouillage avec variation rapide, surtout pour les modulations simples BPSK et QPSK.

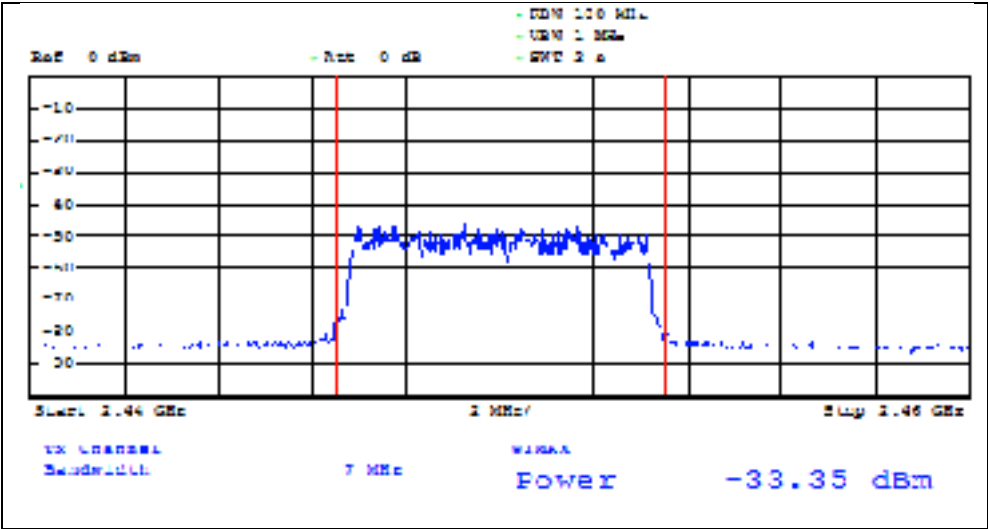


Figure 4.14 Spectre du signal WiMAX avec variation d’amplitude aléatoire lente

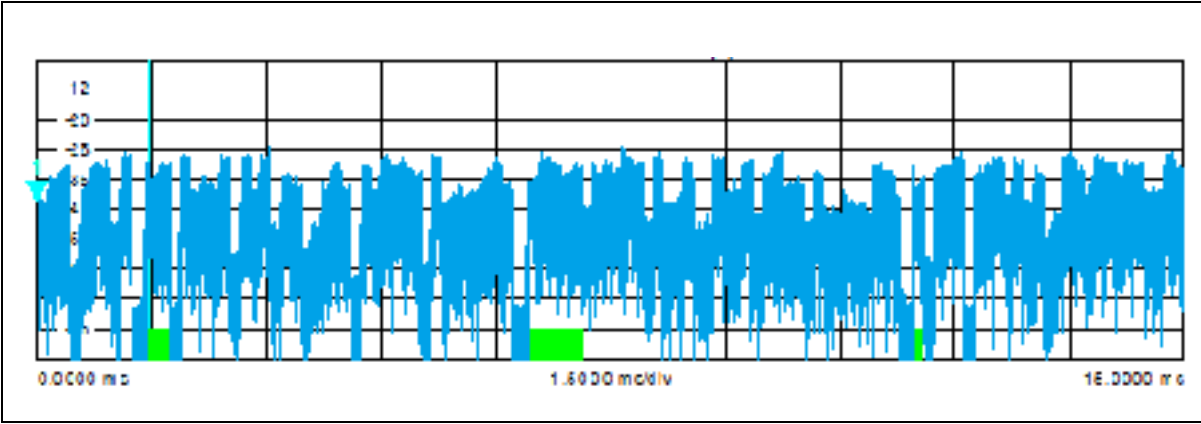


Figure 4.15 Capture temporelle d’un signal WiMAX avec variation d’amplitude aléatoire

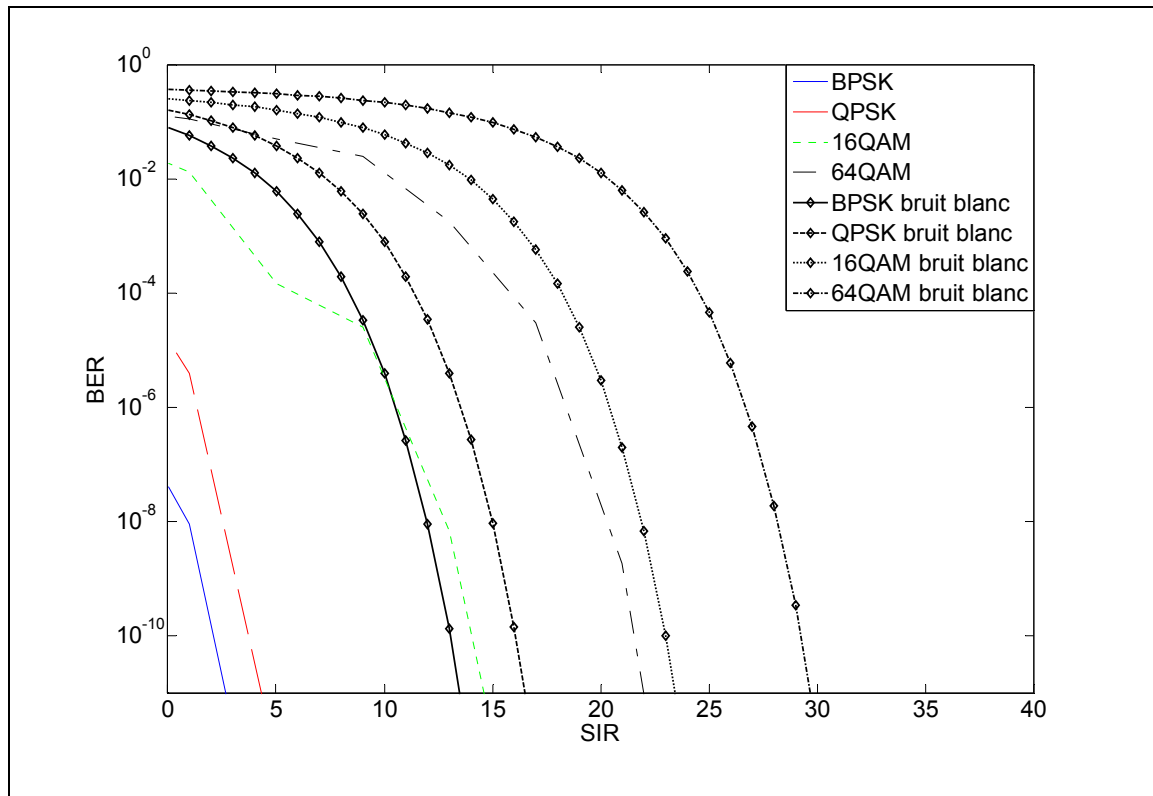


Figure 4.16 Comparaison des TEB pour un signal WiMAX avec brouillage par amplitude aléatoire variant chaque 32 000 échantillons.

4.5 Effets techniques classiques

Pour améliorer nos connaissances sur le comportement du signal WiMAX en présence de brouillage, une série de tests sont réalisés utilisant les méthodes classiques implémentées sur le DRFM. Le brouillage de type bruit blanc, « spot », balayage et barrage est simulé par le DRFM et superposé au signal de base. La puissance du brouillage utilisé pour le SIR est mesurée sur la bande de fréquences du signal de base (7 MHz) et ne tient pas compte de la partie du signal inutile.

4.5.1 Bruit blanc

La radio DRFM est configurée pour émettre du bruit blanc sur toute la bande de fréquences écoutée. La figures 4.17 illustre la comparaison des TEB avec du bruit blanc théorique. Les performances sont très rapprochées. Notre système DRFM est donc capable d'effectuer un brouillage par bruit blanc avec succès. L'utilisation d'un signal de forme OFDM ne semble pas affecter de manière significative la résistance du signal au bruit blanc.

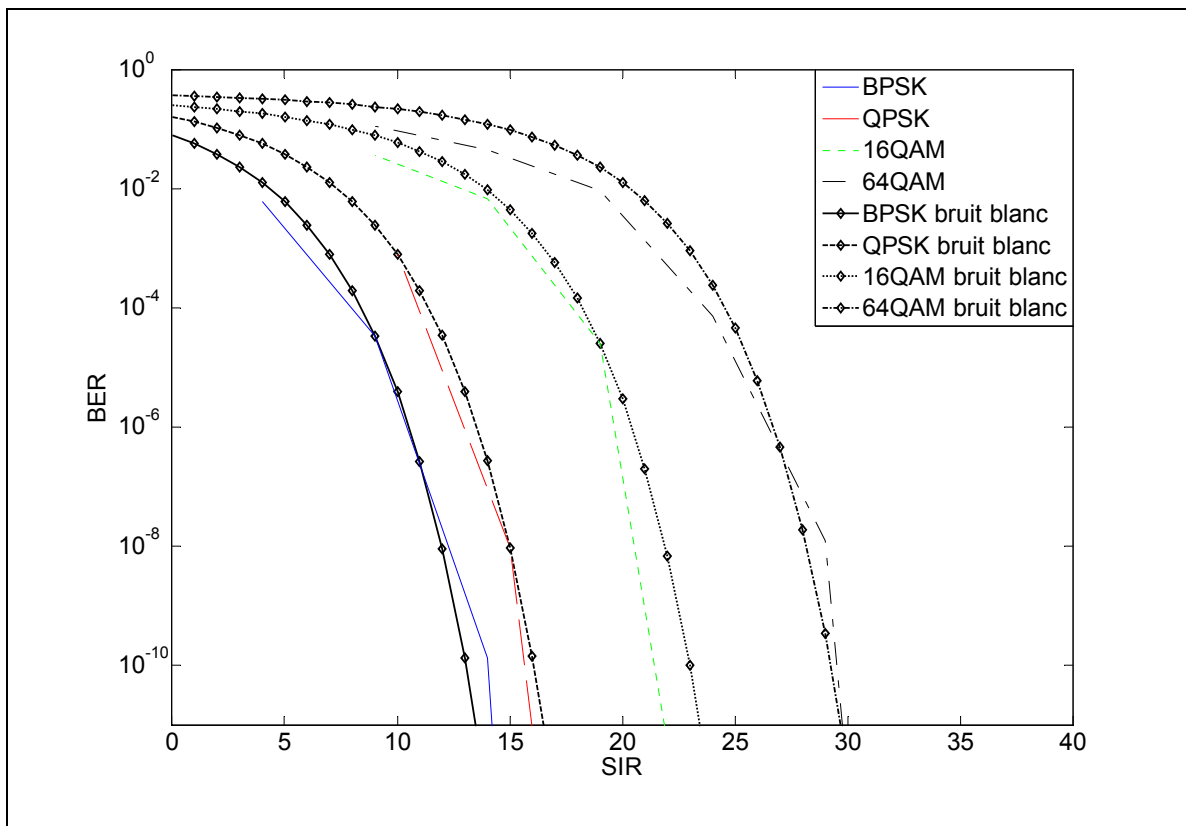


Figure 4.17 Comparaison des TEB d'un signal WiMAX pour un bruit blanc simulé et pour un bruit blanc émulé

4.5.2 Spot

La forme fréquentielle d'un signal « spot » est un signal étroit en fréquence. À la réception, le signal ajouté traversa la FFT et se retrouvera superposé aux porteuses du signal OFDM, comme présenté à la figure 4.18. Le brouillage « spot » interfère donc avec un petit nombre de sous-porteuses. Les rôles des sous-porteuses affectées déterminent son impact. Si le brouillage affecte uniquement des sous-porteuses de données, une dégradation du signal est perçue. L'effet sur l'EVM est moins grand, car la majorité de l'information est intacte. La figure 4.19 affiche la constellation résultante : la majorité des points de données sont inchangés sauf pour ceux provenant des porteuses à la fréquence du brouillage. Lorsque la puissance du signal s'approche de celle de la radio OFDM, l'impact devient plus marqué et la communication peut être complètement brouillée. La perte du signal peut être due à une porteuse pilote adjacente affectée par le brouillage lorsque sa puissance augmente et que sa précision diminue. La figure 4.20 trace les performances du brouillage en comparant le TEB de la communication pour un brouillage « spot » affectant des sous-porteuses de données et le TEB théorique d'un ajout de bruit blanc gaussien sur le canal. Par contre, si le brouillage tombe sur une porteuse pilote, aucun effet sur l'EVM n'est perçu avant que la puissance n'atteigne un seuil. Une fois le seuil atteint, la trame complète est perdue. La figure 4.21 présente la progression de l'EVM dans cette situation.

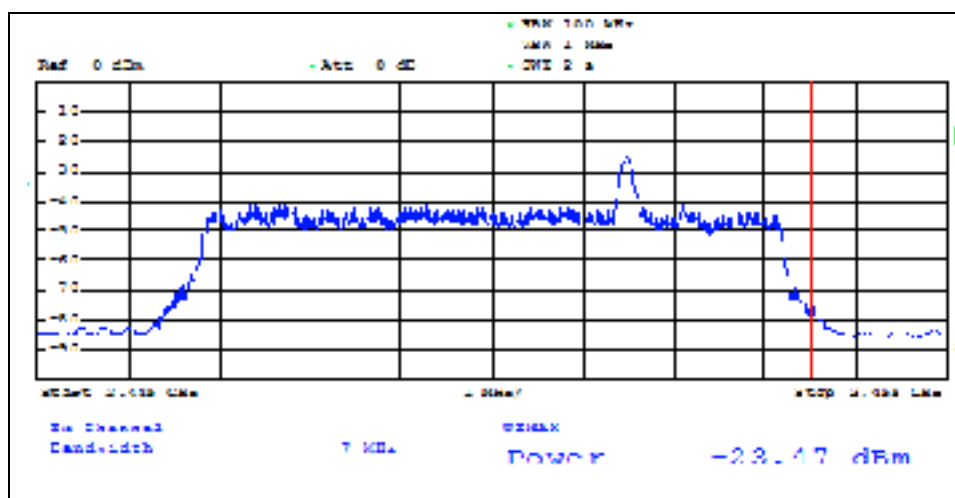


Figure 4.18 Spectre du signal WiMAX avec brouillage « spot »

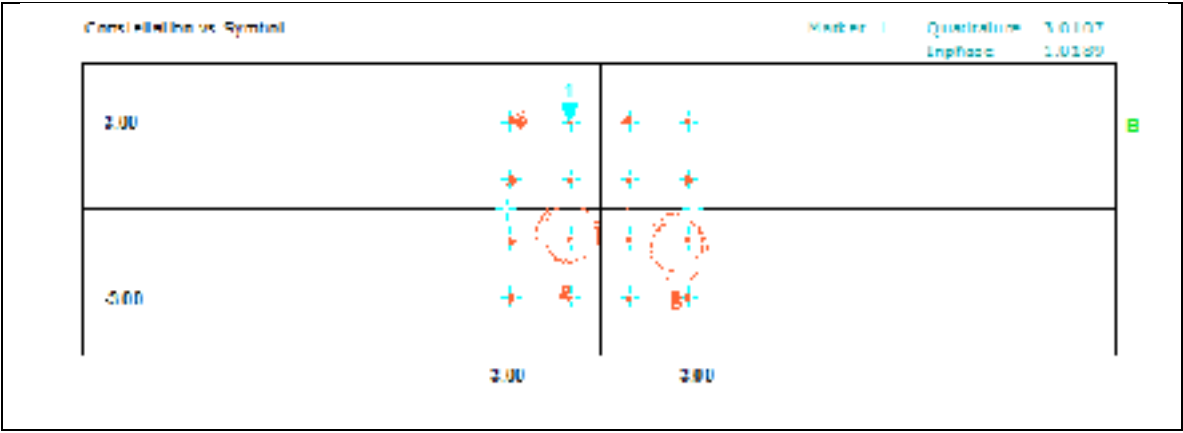


Figure 4.19 Effet du brouillage sur des sous-porteuses de données sur constellation 16QAM

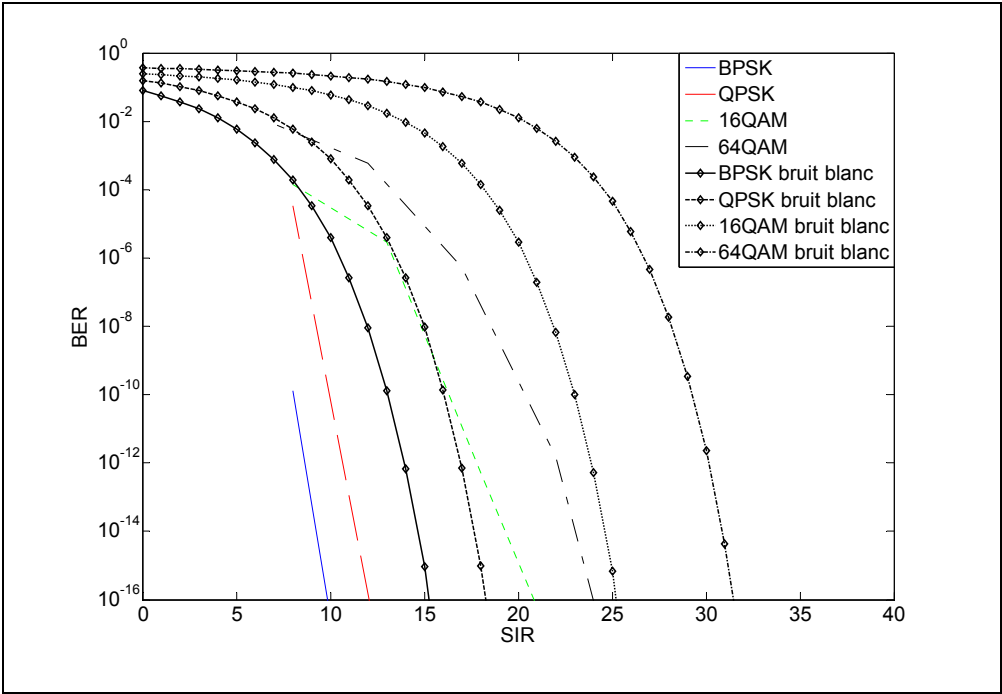


Figure 4.20 Comparaison des TEB sur un signal WiMAX avec un brouillage « spot » et un bruit blanc théorique

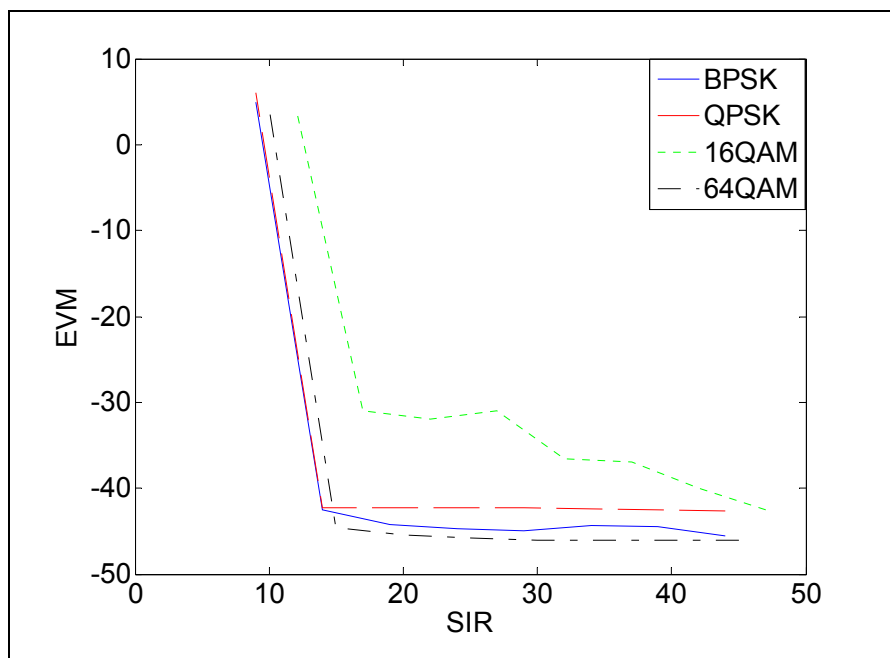


Figure 4.21 Progression de l'EVM d'un signal WiMAX pour un brouillage « spot » positionné sur une sous-porteuse pilote

4.5.3 Balayage

Le brouillage par balayage utilise le même type de signal que le brouillage « spot », mais fait varier la fréquence dans le temps. La figure 4.22 présente la forme du brouillage dans le domaine fréquentiel. Le signal brouille des fréquences séparées de 500 KHz sur 20MHz et chaque fréquence est brouillée pendant 1000 μ s. Sur un signal WiMAX, plus de sous-porteuses se retrouvent affectées, ce qui donne un meilleur brouillage. La figure 4.23 trace les performances du brouillage en comparant le TEB de la communication avec le TEB théorique d'un ajout de bruit blanc gaussien sur le canal. Ce brouillage apporte une légère dégradation des performances de la communication lorsque comparé aux résultats du brouillage « spot ».

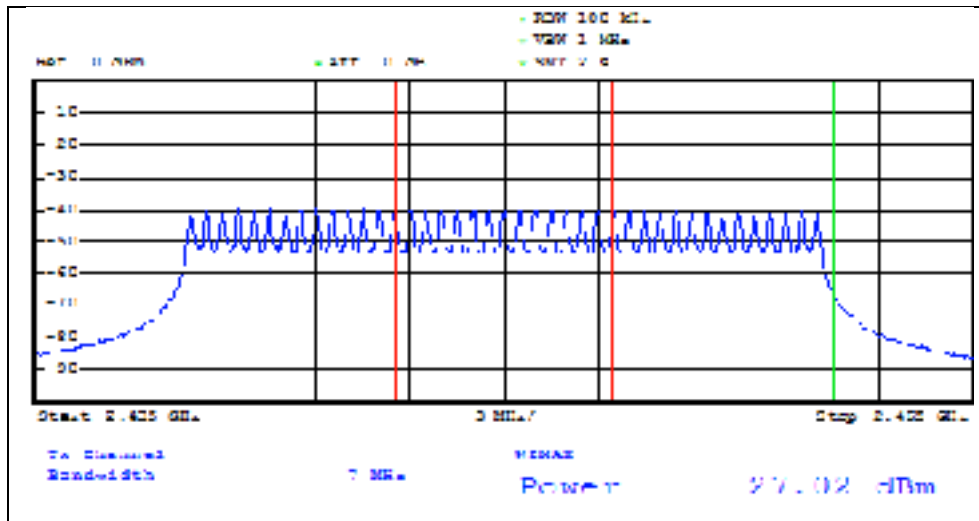


Figure 4.22 Spectre du signal de brouillage par balayage

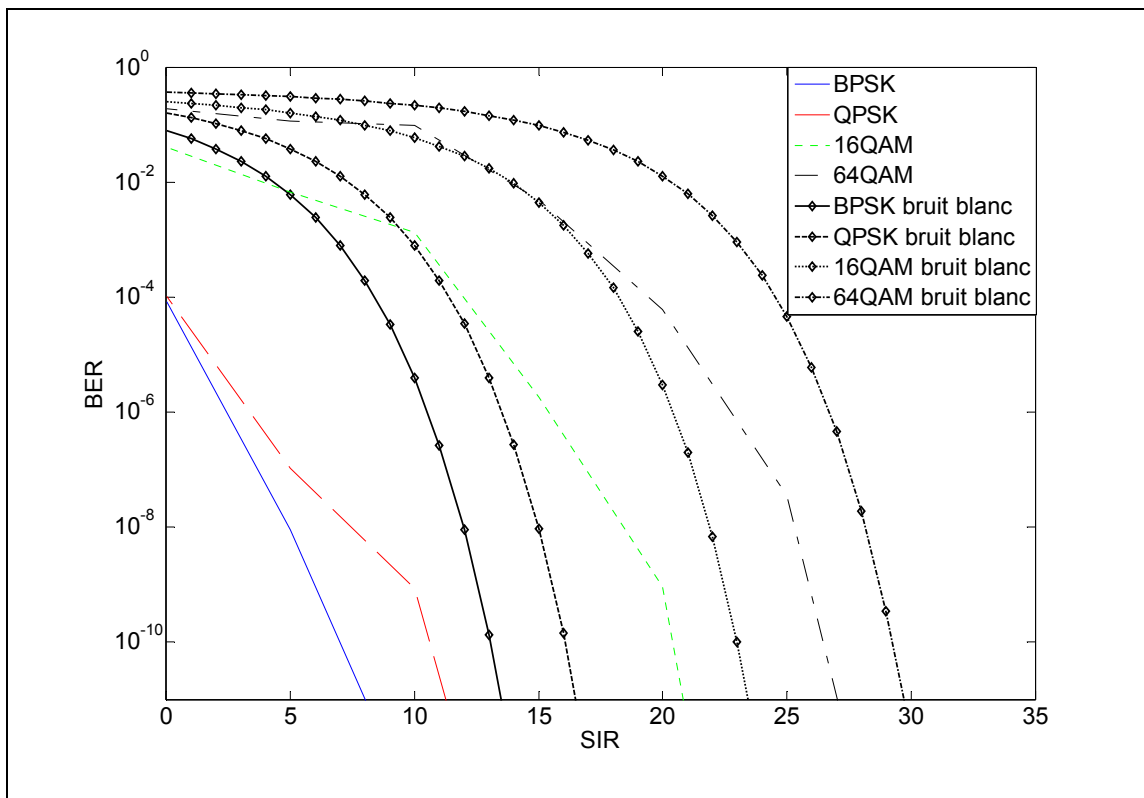


Figure 4.23 Comparaison des TEB sur un signal WiMAX avec un brouillage par balayage et un bruit blanc théorique

4.5.4 Barrage

En maximisant les paramètres du brouillage par balayage, on peut créer un signal très proche d'un brouillage par barrage. La radio DRFM est capable de diminuer l'écart entre les fréquences à 25 KHz et le temps par fréquence à 5 μ s. La figure 4.24 présente la forme du signal de brouillage obtenue. Théoriquement, ce brouillage devrait avoir les meilleures performances parmi les brouillages classiques. La figure 4.25 trace les performances du brouillage en comparant le TEB de la communication avec le TEB théorique d'un ajout de bruit blanc gaussien sur le canal. Ces performances sont similaires à notre bruit blanc simulé. Ce résultat est normal puisque le signal a la forme fréquentielle d'un bruit blanc sur la bande du signal WiMAX.

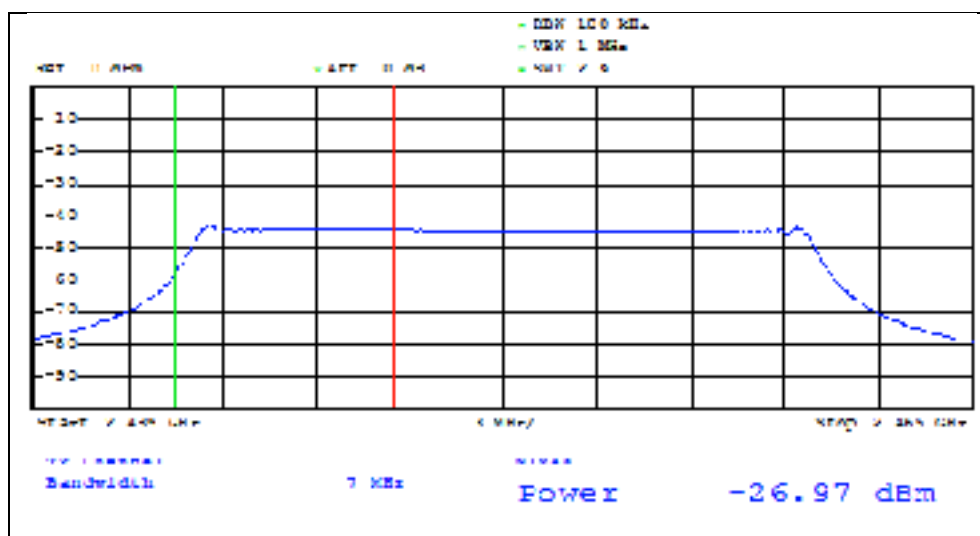


Figure 4.24 Spectre du signal de brouillage par barrage émulé

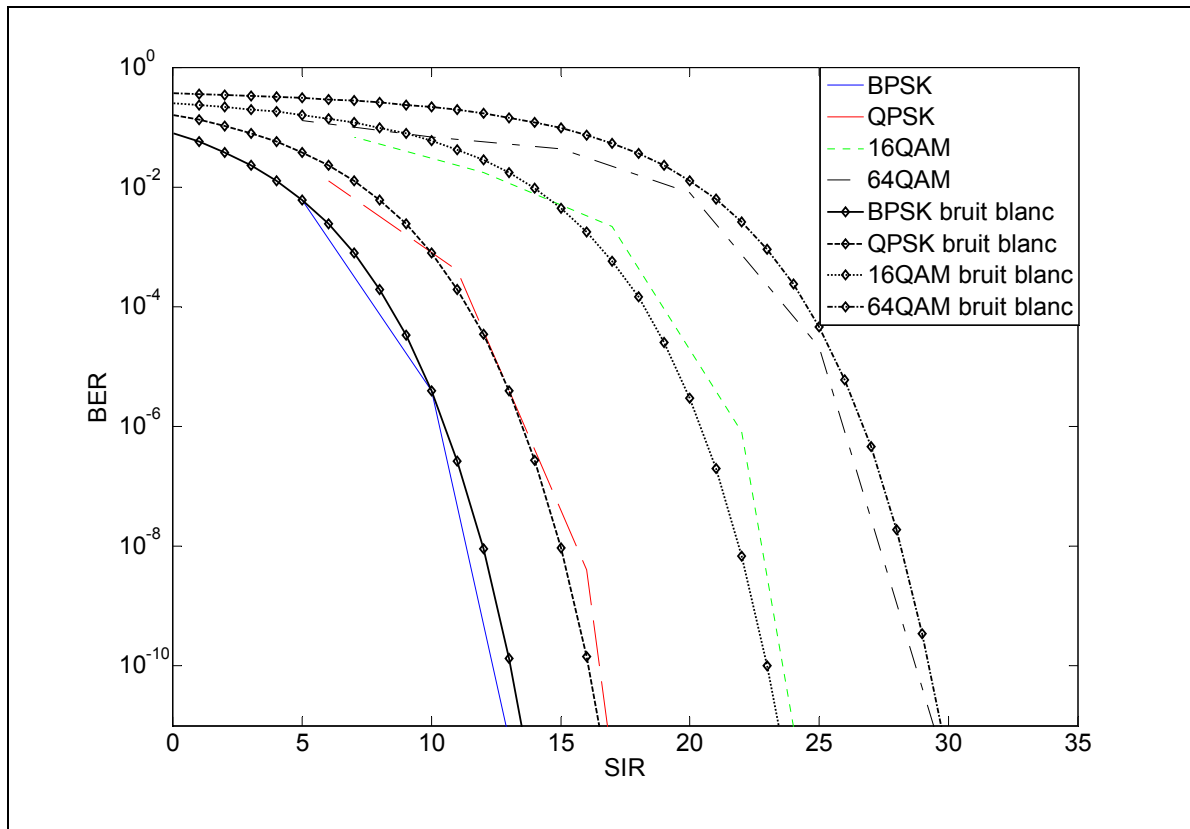


Figure 4.25 Comparaison des TEB sur un signal WiMAX avec un brouillage barrage et un bruit blanc théorique

4.6 Analyse

Les résultats des tests sur le WiMAX donnent une base de comparaison entre les nouvelles méthodes de brouillage, qui utilisent un traitement de signaux rapide, et les méthodes classiques.

4.6.1 Techniques avancées

Les méthodes de brouillage avancées nous montrent que le brouillage par variation de délai aléatoire donne les meilleurs résultats. Le brouillage avec variation rapide et variation lente donne des résultats qui s'approchent d'un brouillage par bruit blanc donc, la variation rapide n'est pas nécessaire pour nuire à la communication. De plus, le signal avec variation de délai lente ajoute moins de puissance dans les bandes adjacentes et donne une meilleure efficacité énergétique. En comparaison, le brouillage par variation d'amplitude est beaucoup moins efficace et une perte allant jusqu'à 13 dB est visible sur les performances. De plus, le brouillage par variation d'amplitude est la seule méthode avancée incapable de bloquer complètement la communication. À très haute puissance, le récepteur était toujours capable de reconnaître la présence de trame, même si aucune information n'était déchiffrable.

Cette différence de performance peut avoir plusieurs causes. Comme mentionnés au chapitre 3, les techniques de brouillage utilisent un générateur de variables aléatoires uniformes discrètes. L'impact de la probabilité liée à ces variables semble avoir beaucoup plus d'impact sur le brouillage par variation d'amplitude que sur celui par variation de délai. Aussi, il est possible que les communications OFDM soient par défaut plus résistantes aux variations d'amplitude qu'aux variations de délai.

La trame OFDM utilisant une modulation BPSK a des comportements intéressants. Dans certaines situations de brouillage, les performances de la communication sont plus basses que les attentes théoriques et semblent avoir le même TEB que le QPSK. Ce comportement est très marqué pour les brouillages avancés avec variation rapide (figures 4.9 et 4.13). D'autres

prises de mesures offrent des résultats similaires. Dans la majorité des autres cas, le BPSK semble suivre les attentes théoriques. Il est donc possible que les mesures du BPSK utilisés soient des anomalies statistiques ou qu'un facteur possiblement liée à la nature unidimensionnelle de la constellation affecte leurs performances.

4.6.2 Techniques classiques et comparaison

L'utilisation de méthodes classiques pour brouiller des signaux WiMAX permet plusieurs observations pertinentes. Premièrement, le brouillage par simulation de bruit blanc donne des résultats compatibles avec la théorie. Les performances du bruit blanc simulé par traitement de signaux sont donc très proches de la réalité.

Le brouillage « spot » a des comportements intéressants. Lorsqu'il est positionné sur des porteuses de données, il a un impact faible sur l'EVM. Par contre lorsqu'il est superposé à un des pilotes de la trame OFDM avec assez de puissance, la communication devient complètement brouillée. Ce comportement peut expliquer pourquoi, à haute puissance, le brouillage « spot » coupe complètement la communication, peu importe sa position. Le signal n'est pas parfait, il a une largeur fréquentielle qui augmente avec sa puissance. Puisque la trame OFDM a plusieurs pilotes répartis sur la plage fréquentielle, le signal de brouillage affectera éventuellement un des pilotes et atteindra le seuil requis pour empêcher le décodage de la trame. Pour le brouillage par balayage, les performances sont meilleures sur l'EVM. Mais même pour des puissances élevées, le récepteur est encore capable de détecter la présence du signal. On suppose qu'aucune des fréquences de brouillage n'est donc superposée directement à un pilote. De plus, puisque la puissance est répartie sur une plage de fréquence de 20 MHz, elle n'est pas suffisante pour affecter indirectement les porteuses pilotes. Après le brouillage par bruit blanc, le brouillage par barrage émulé affiche les meilleures performances. Il est capable de couper complètement la communication puisqu'il est presque assurément superposé aux pilotes. Par contre, son coût en énergie est presque aussi élevé que le bruit blanc.

Basées sur la métrique TEB, les méthodes de brouillages avancées semblent ne pas avoir d'amélioration marquée par rapport aux méthodes classiques. L'avantage principal des techniques avancées reste la capacité à couvrir une large bande de fréquences et à utiliser la puissance du brouilleur plus efficacement.

4.7 Résumé

Le premier standard étudié est le WiMAX. Ce standard est récent et forme avec le LTE la base de la quatrième génération d'appareils cellulaires (Blust, 2012). Sa particularité principale est l'utilisation d'un signal OFDM et d'une transformation FFT pour créer une trame de données qui contient une très grande quantité d'information.

Les résultats obtenus ont révélé plusieurs informations pertinentes. Premièrement, pour les techniques de brouillage avancées, la variation aléatoire de délai offre des performances de brouillage très proche du brouillage classique, alors que la variation d'amplitude aléatoire a une efficacité beaucoup plus faible, autour de -10 dB. Pour les techniques de brouillage classiques, le brouillage « spot » est le moins efficace, car il ne peut couvrir toute la largeur de bande du signal, mais peut être utilisé pour cibler les porteuses pilotes du signal pour avoir un impact très marqué. Des résultats similaires au bruit blanc pour notre brouillage avancé sont encourageants. Cela signifie qu'on peut brouiller le signal avec un impact similaire aux méthodes classiques, tout en apportant les avantages du traitement de signal rapide sur la puissance et la couverture de bande passante.

CHAPITRE 5

Impact sur le standard GSM-EDGE

5.1 GSM-EDGE

Le standard GSM-EDGE « Advance Data Rates for GSM Evolution » est un standard créé à partir de la norme GSM de la génération 2G, mais amélioré pour la génération 3G. Pour répondre aux exigences du 3G, plusieurs changements ont été apportés au standard GSM. Sur la couche physique, la constellation utilisée prend la forme $3\pi/8$ -8PSK. Cette constellation est une constellation 8PSK qui subit une rotation de $3\pi/8$ chaque période de symbole (Furuskar et al., 1999). Cette rotation empêche le signal de passer par zéro, ce qui réduit le facteur de crête du signal (Robertson, 2014). La figure 5.1 illustre la forme de la constellation dans le plan I et Q. Cette constellation, qui ressemble à une constellation 16-PSK, superpose 2 constellations 8-PSK transmises en alternance.

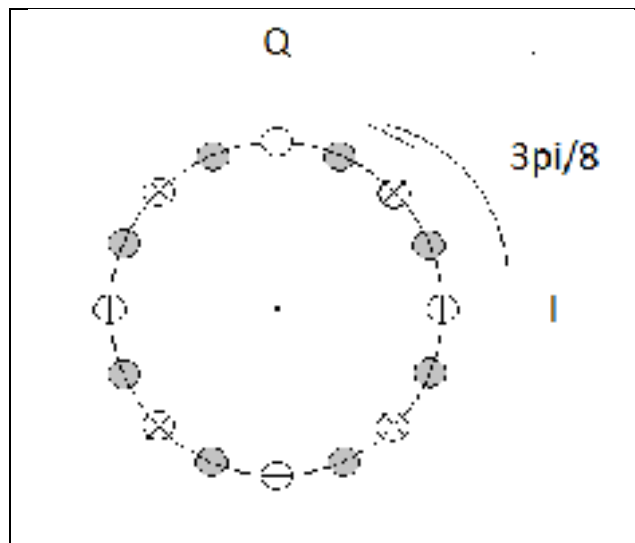


Figure 5.1 Constellation $3\pi/8$ -8PSK

5.2 Signaux générés

Pour tester le standard GSM-EGDE, un signal simple est généré en utilisant le générateur de modulation du SMU-200A. Le tableau 5.1 décrit les caractéristiques du signal. La figure 5.2 présente la forme fréquentielle du signal généré et la figure 5.3 montre la forme de la constellation $3\pi/8$ -8PSK dans le plan I/Q. Les communications GSM-EDGE peuvent utiliser plusieurs porteuses (Robertson, 2014), mais pour les tests, un signal GSM-EDGE classique avec une simple porteuse sera utilisé.

Tableau 5.1 Caractéristiques du signal GSM-EDGE

Fréquence centrale	2,45 GHz
Taux de transfert	270,833ksymb/sec
Filtre	Gaussien linéaire
Constellation	$3\pi/8$ -8PSK EDGE

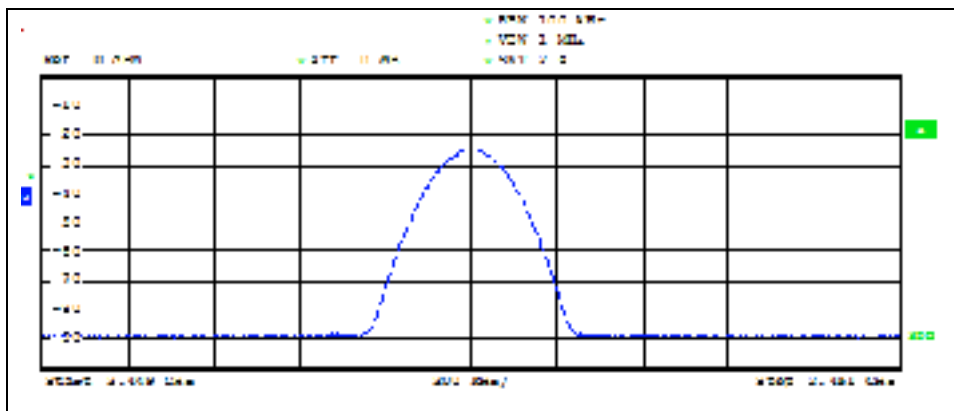


Figure 5.2 Spectre du signal GSM-EDGE

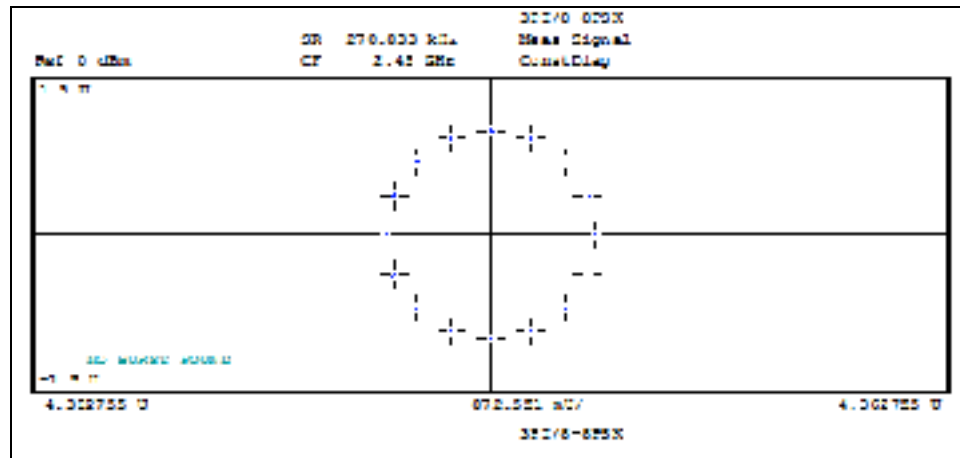


Figure 5.3 Constellation 3pi/8-8PSK

5.3 Effets du brouillage par variation de délai aléatoire

Puisque le standard GSM utilise une modulation relativement simple sur la couche physique, la variation de délai a des effets très variables selon les paramètres du brouillage. Le tableau 5.2 décrit les configurations des brouillages utilisés pour les tests.

Tableau 5.2 Caractéristiques des brouillages par variation de délai utilisé

	Variation rapide	Variation lente
Nombre d'échantillons entre les variations	10	32 000
Inversion du signal	non	non
Plage du délai	0 – 4 μ s	0 – 4 μ s

Le brouillage avec variation de délai rapide fait varier le délai aléatoire chaque 10 échantillons de signal, ce qui correspond à un changement chaque 10 ns. Le signal GSM soumis à ce brouillage perd complètement sa forme originale. La figure 5.4 montre la forme fréquentielle d'un signal GSM avec un délai aléatoire aussi rapide. Son spectre fréquentiel devient très similaire à un bruit blanc et sa puissance est répartie sur une large bande de fréquences comme s'il était soumis à un étalement fréquentiel. La puissance sur la bande de

fréquences du signal diminue d'environ 15 dB une fois la variation enclenchée. Lors du brouillage, la constellation au récepteur subit une dégradation globale comme observé à la figure 5.5.

Le brouillage avec variation de délai lente change le délai aléatoire chaque 32 000 échantillons, ce qui correspond à un changement de délai toutes les 32 μ s. La déformation du signal de base est beaucoup moins marquée comme présenté à la figure 5.6. Plus de puissance est conservée dans la bande de fréquences utilisées pour la communication et la diminution à la crête du signal est d'environ 1 dB. Lors du brouillage, le signal reçu subit aussi des effets différents : la variation du délai fait ressortir l'effet de rotation que subit la constellation à chaque symbole et crée des spirales ou des cercles concentriques, comme observé à la figure 5.7.

La figure 5.8 affiche les EVM de la communication pour les brouillages par délai aléatoire avec variation rapide et lente. Plus l'EVM est grand, plus la communication a des erreurs et plus le brouillage est efficace. Le brouillage avec une variation lente du délai obtient de meilleurs résultats et a une meilleure utilisation de la puissance d'émission. Dans cette situation une variation trop rapide nuit à l'efficacité du brouillage, car plus de puissance est requise pour atteindre le niveau de SIR similaire, et le brouillage résultant est moins efficace.

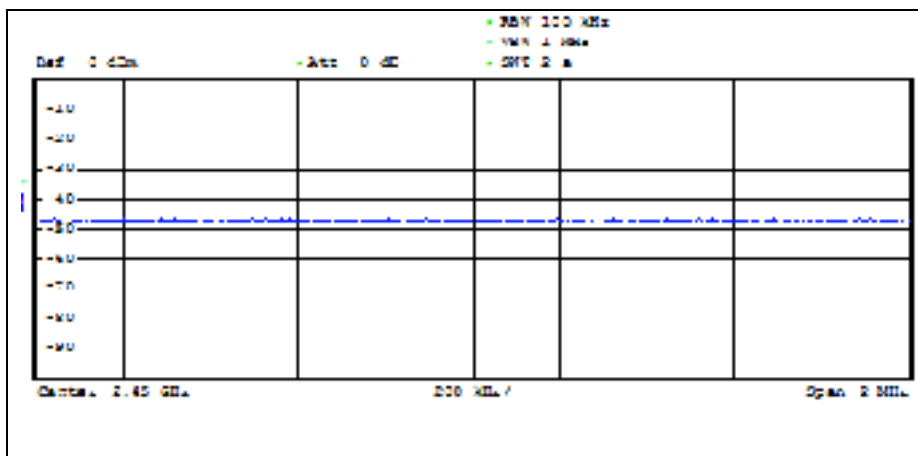


Figure 5.4 Spectre du signal GSM-EDGE avec variation de délai aléatoire rapide

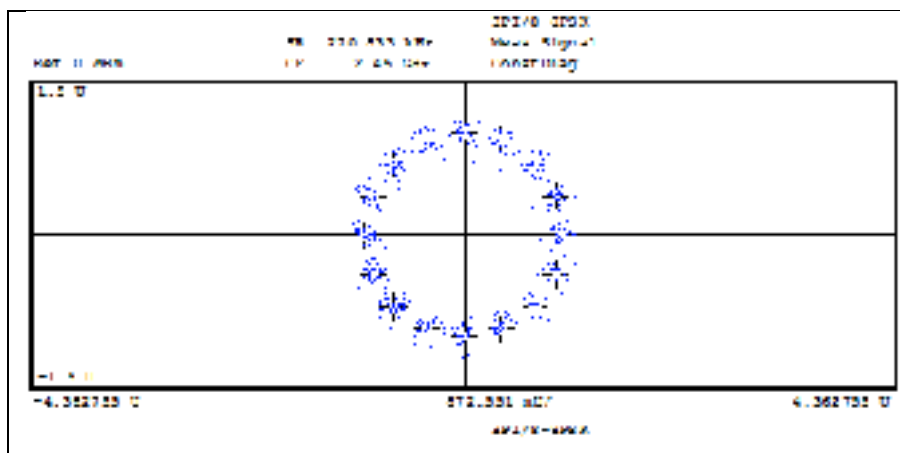


Figure 5.5 Constellation GSM-EDGE soumise à un brouillage par variation de délai aléatoire rapide

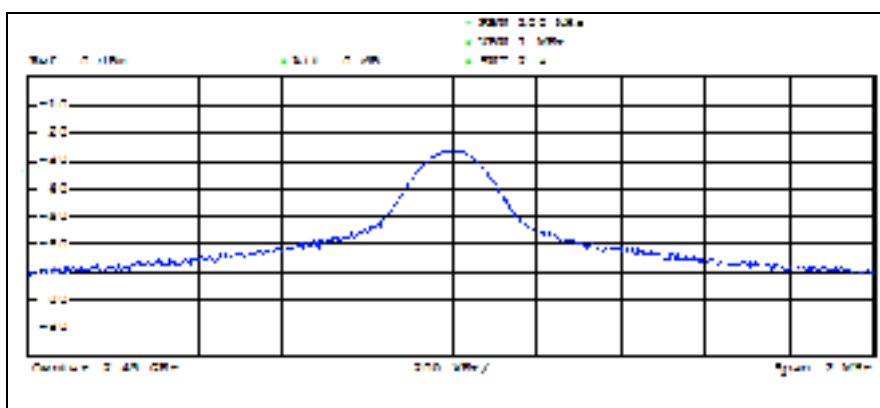


Figure 5.6 Spectre du signal GSM-EDGE avec variation de délai aléatoire lente

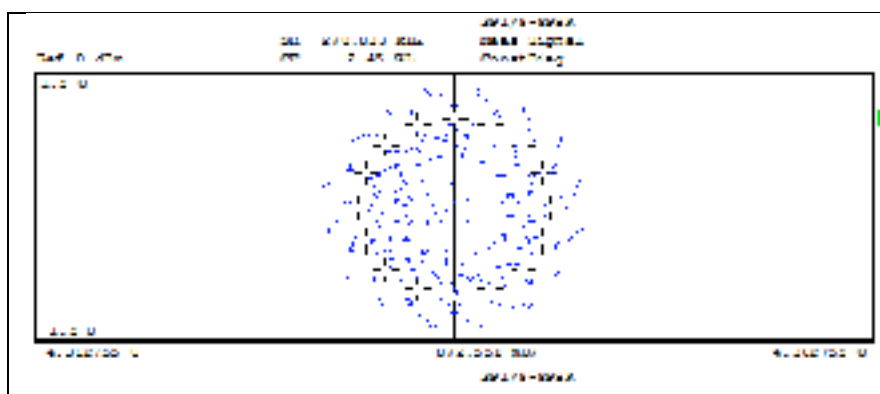


Figure 5.7 Constellation GSM-EDGE soumise à un brouillage par variation de délai aléatoire lente

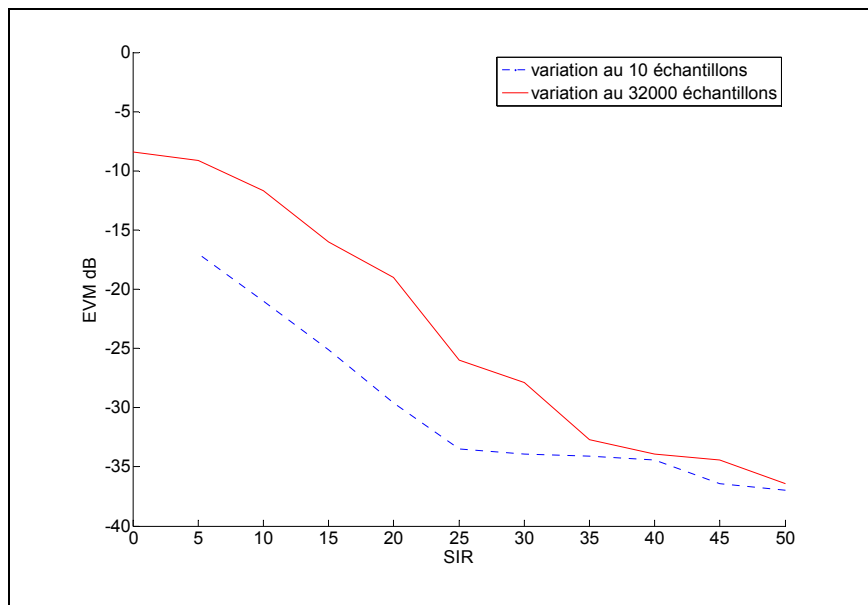


Figure 5.8 Comparaison des EVM pour un signal GSM-EDGE avec brouillage par délai aléatoire

5.4 Effets du brouillage par variation aléatoire d'amplitude

Le brouillage par variation d'amplitude tente de créer une variation assez grande et assez rapide pour déjouer les AGC de la réception. À cause de la variation du module du signal, toutes les mesures de puissance sont prises avant l'application du brouillage. Le tableau 5.3 décrit les configurations des brouillages utilisés pour les tests.

Tableau 5.3 Caractéristiques des brouillages par variation de délai utilisée

	Variation rapide	Variation lente
Nombre d'échantillons entre les variations	10	32 000
Inversion du signal	non	non
Taille de l'entier utilisé	12 bits	12 bits

Pour le brouillage à variation rapide d'amplitude, le nombre d'échantillons entre chaque variation d'amplitude est de 10, ce qui correspond à un changement chaque 10 ns. Une

variation d'amplitude aussi fréquente est très difficile à compenser par un AGC. La figure 5.9 présente la forme du signal GSM soumis à cette variation. La variation très rapide semble créer beaucoup de bruit dans les bandes de fréquences adjacentes au signal et une diminution de la puissance du signal d'environ 6 dB. Comme observé à la figure 5.10, lors du brouillage peu d'effets sont ressentis sur la constellation et, par conséquent, sur l'EVM.

Le brouillage utilisant une variation d'amplitude lente utilise 32 000 échantillons entre les variations, ce qui correspond à un changement d'amplitude toutes les 32 μ s. La figure 5.11 présente la forme du signal résultant. Beaucoup moins de bruit est ajouté aux bandes de fréquences latérales et on remarque des imperfections sur la forme du signal. Lors du brouillage l'effet sur la constellation est aussi beaucoup plus grand. La rotation effectuée par la constellation lui donne une allure unique où la position des points semble différer suivant des droites d'angle variant, comme observé à la figure 5.12.

La figure 5.13 trace la progression des EVM pour les deux configurations du brouillage. Encore une fois, une variation rapide donne de moins bons résultats qu'une variation plus lente, en plus d'être plus coûteuse énergétiquement.

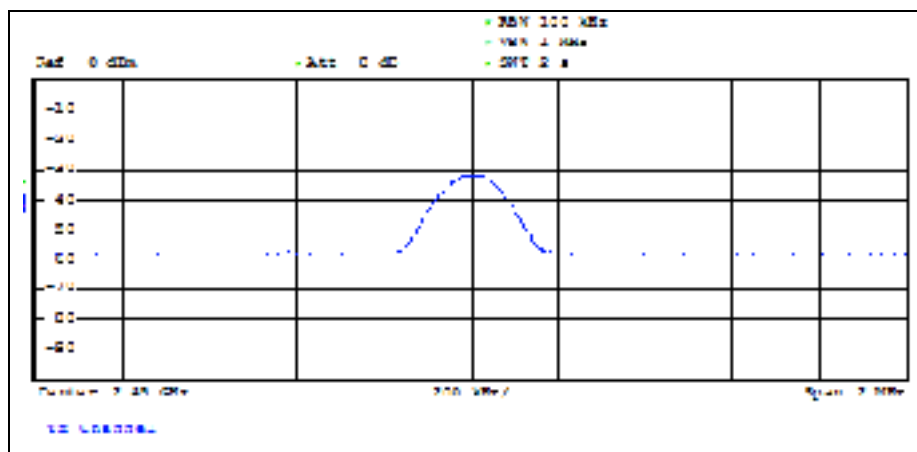


Figure 5.9 Spectre du signal GSM-EDGE avec variation d'amplitude aléatoire rapide

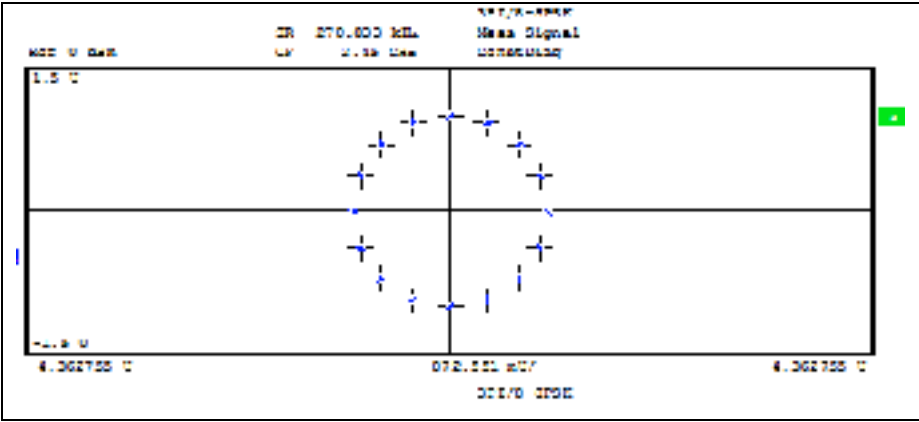


Figure 5.10 Constellation GSM-EDGE soumise à un brouillage par variation d'amplitude rapide

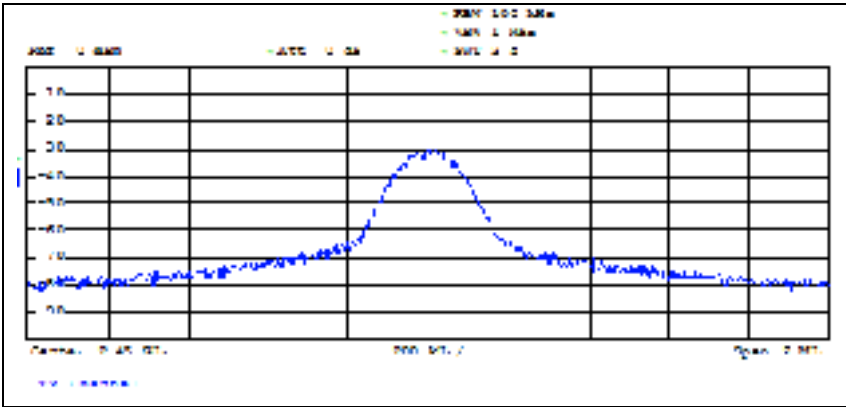


Figure 5.11 Signal GSM-EDGE avec variation d'amplitude aléatoire lente

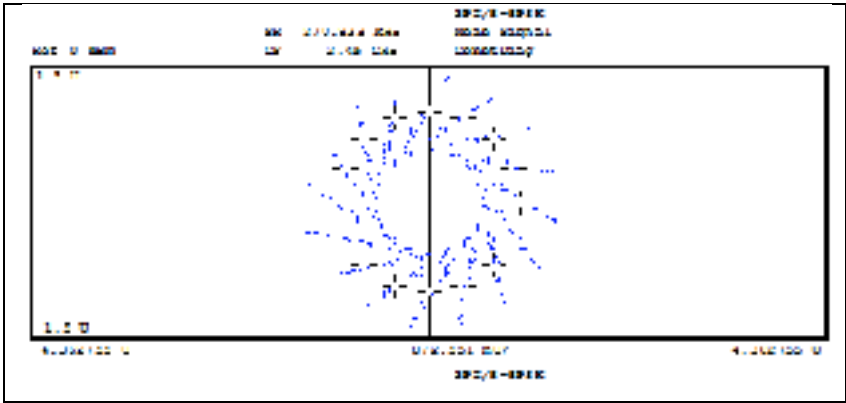


Figure 5.12 Constellation GSM-EDGE soumise à un brouillage par variation d'amplitude rapide.

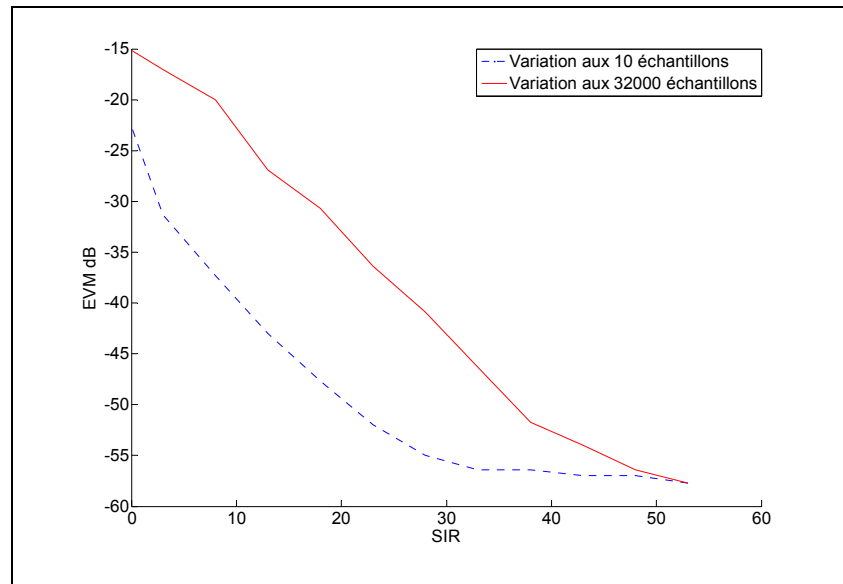


Figure 5.13 Comparaison des EVM pour un signal GSM-EDGE avec brouillage par amplitude aléatoire

5.5 Effets des techniques classiques

Pour améliorer nos connaissances sur le comportement du signal GSM-EDGE en présence de brouillage, une série de tests sont réalisés utilisant les méthodes classiques implémentées sur le DRFM. Un brouillage de type bruit blanc, « spot », balayage et barrage est émulé par le DRFM et superposé au signal de base. La puissance du brouillage utilisé pour le SIR est mesurée sur la bande de fréquences du signal de base 270.83 KHz et ne tient pas compte de la partie du signal inutile.

5.5.1 Bruit blanc

La radio DRFM est configurée pour émettre du bruit blanc sur toute sa bande de fréquences. Il est difficile de comparer cette mesure avec la théorie. La courbe théorique la plus proche serait le 8-PSK, mais cette courbe ne tient pas compte des impacts de la rotation du $3\pi/8$ -8PSK par le GSM-EDGE. La mesure pratique avec bruit blanc peut être utilisée comme

référence pour les autres types de brouillages classiques. La figure 5.14 trace la progression du signal GSM-EDGE en présence de bruit.

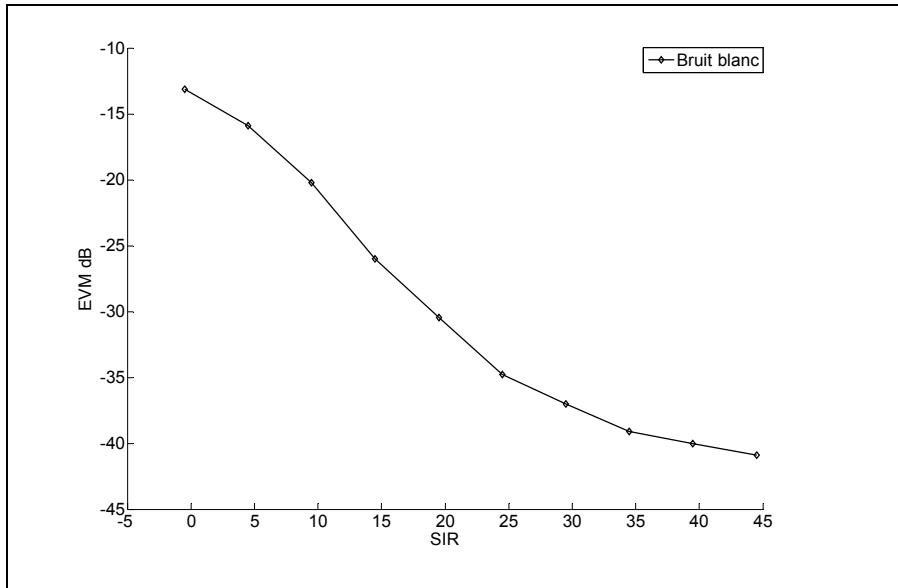


Figure 5.14 EVM pour un signal GSM-EDGE pour un bruit blanc émulé

5.5.2 Spot et balayage

Le signal GSM-EDGE utilisé a une plage de fréquences de 270.833KHz, beaucoup plus petites que les autres standards testés. Le brouillage « spot » doit donc être superposé à cette bande pour avoir un impact significatif. La figure 5.15 illustre l'impact sur la constellation lorsque le brouillage est directement à la fréquence centrale du signal. Tous les points subissent un impact similaire, lié à la puissance et à la phase du signal « spot » au moment de la réception.

Le brouillage par balayage utilise le même type de signal que le brouillage « spot », mais fait varier la fréquence dans le temps. La figure 5.16 présente la forme du brouillage dans le domaine fréquentiel : le signal effectue des sauts de fréquence de 500 KHz sur 10MHz et chaque fréquence est brouillée pendant 1000 μ s. Le signal GSM-EDGE a une bande de

fréquences très étroite comparé au signal de brouillage qui couvre plusieurs MHz. La performance du brouillage dépend grandement de la position des fréquences, les meilleures performances du brouillage surviendront lorsqu'une des fréquences ciblées sera directement superposée au signal de base. Pour assurer des performances maximales, notre signal de brouillage par balayage utilise des sauts de 500KHz, de manière à se superposer au signal GSM-EDGE qui est centré à 2,45GHz. La figure 5.17 montre l'impact sur la constellation, similaire au brouillage « spot », mais avec moins de constance, ce qui est probablement dû à l'intermittence du signal DRFM superposé au signal de base. La figure 5.18 trace la comparaison des EVM obtenus avec les types de brouillage « spot » et balayage. La courbe du bruit blanc est ajoutée à titre comparatif. Le brouillage « spot » obtient de meilleurs résultats, ce qui est attendu puisque sa puissance dans la bande du signal est constante alors que celle du brouillage par balayage est pulsée.

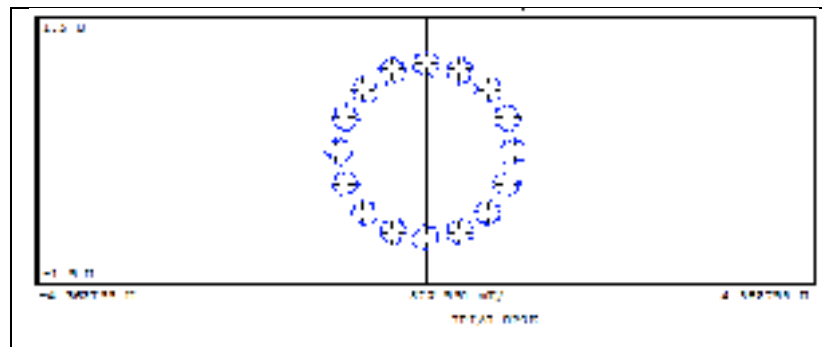


Figure 5.15 Constellation GSM-EDGE avec brouillage « spot »

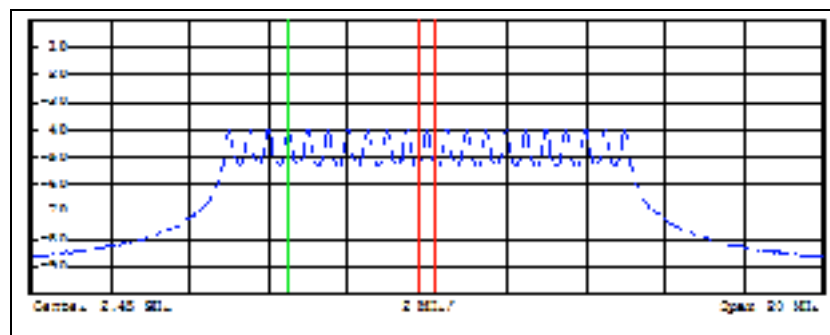


Figure 5.16 Spectre du signal de brouillage par balayage

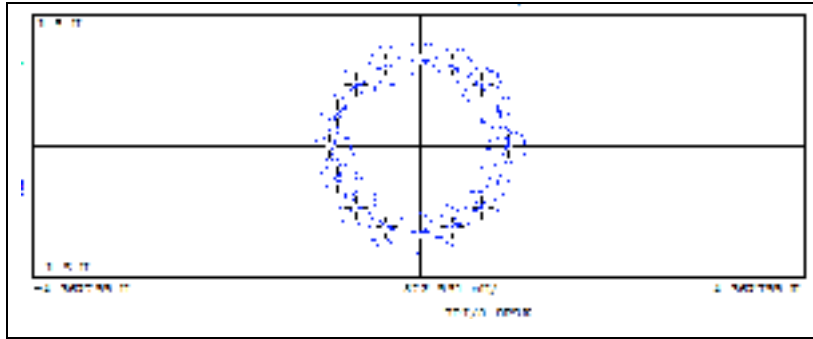


Figure 5.17 Constellation GSM-EDGE avec brouillage par balayage

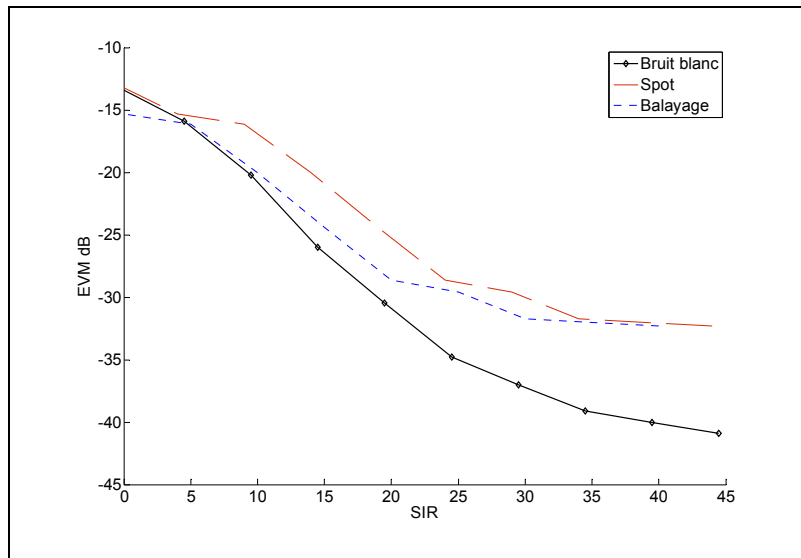


Figure 5.18 Comparaison des EVM sur un signal GSM-EDGE avec un brouillage « spot », un balayage et un bruit blanc émulé

5.5.3 Barrage

En maximisant les paramètres du brouillage par balayage, on peut créer un signal très proche d'un brouillage par barrage. La radio DRFM est capable de diminuer l'écart entre les fréquences à 25 KHz et le temps par fréquence à 5 μ s. Le signal résultant est présenté à la figure 5.19. Les tests utilisant ce type de brouillage obtiennent des effets différents sur la constellation du signal GSM-EDGE, selon la puissance du signal du DRFM. La figure 5.20 dépeint l'évolution de la forme de la constellation selon la puissance de brouillage émise. Un écart de 25 KHz place au moins dix sommets dans la plage de fréquences GSM-EDGE. La variation de la constellation est due à l'interaction entre la rotation de la constellation et les nombreux signaux pulsés superposés au signal de base. La figure 5.21 trace les performances du brouillage en comparant le EVM de la communication et celui obtenu avec un bruit blanc émulé à titre comparatif. La performance du brouillage est entre 2 dB et 5 dB supérieure au bruit blanc simulé.

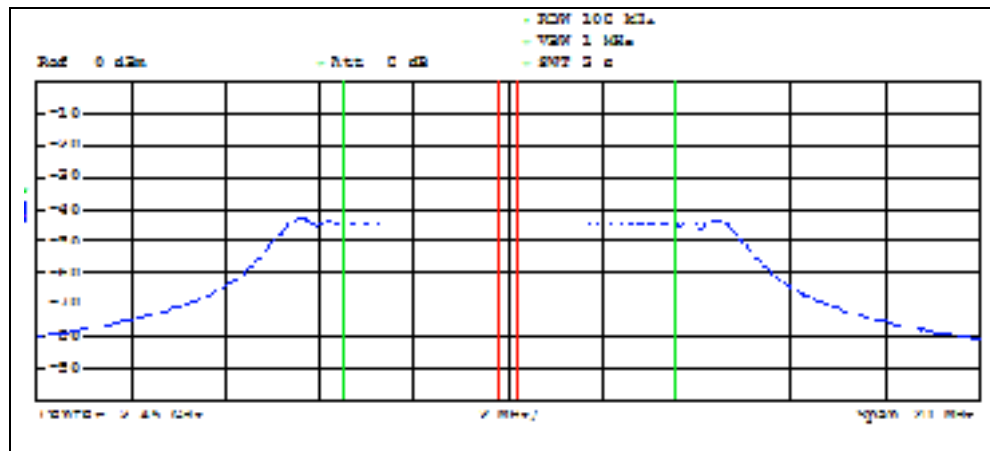


Figure 5.19 Spectre du signal de brouillage par barrage émulé

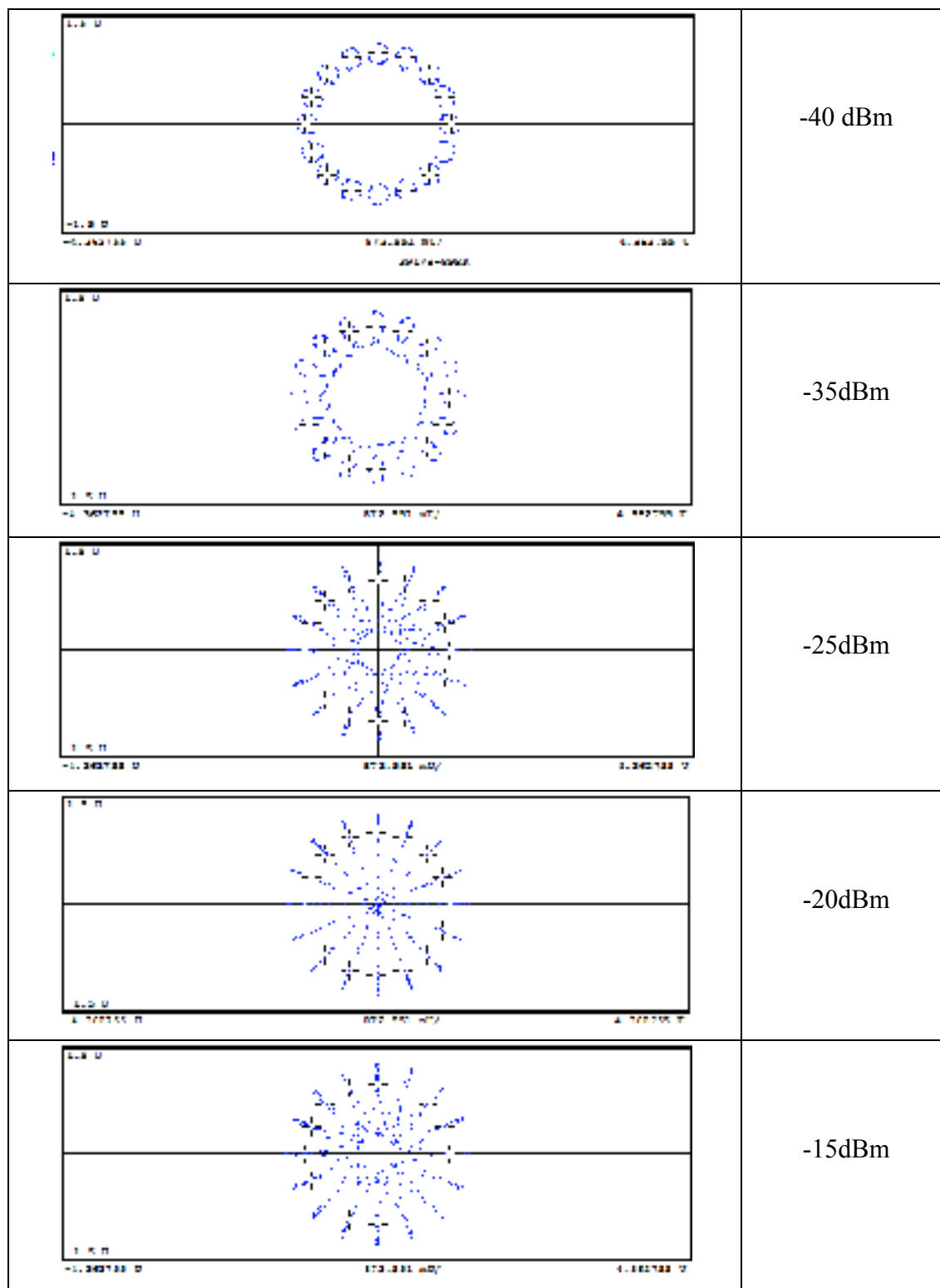


Figure 5.20 Constellation GSM-EDGE avec brouillage barrage à différentes puissances

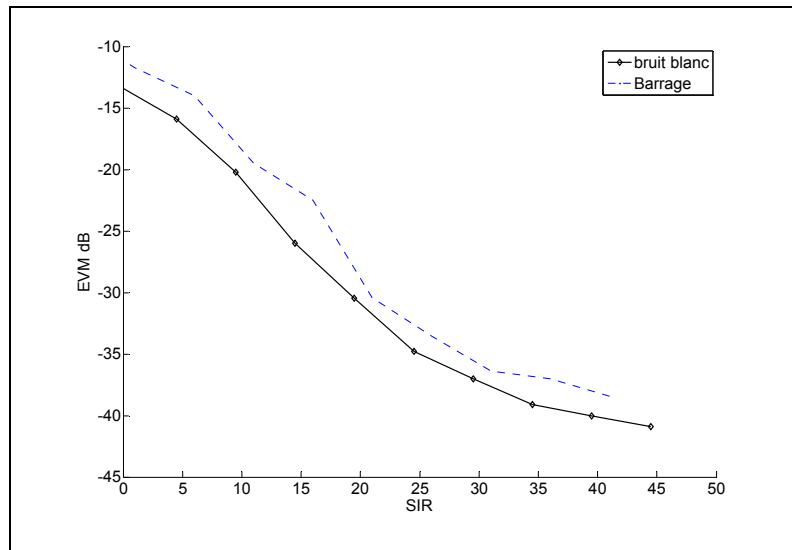


Figure 5.21 Comparaison des EVM sur un signal GSM-EDGE avec un brouillage barrage et un bruit blanc émulé

5.6 Analyse

Le standard GSM-EDGE utilise une modulation relativement simple comparée au WiMAX et au W-CDMA. L'utilisation d'une seule porteuse donne un signal avec une bande de fréquences beaucoup plus petite que les autres signaux, ce qui peut expliquer certains résultats. Les méthodes de brouillage conçues pour couvrir de larges bandes passantes utilisent leur puissance peu efficacement, ce qui peut diminuer leur impact.

5.6.1 Techniques avancées

Les tests de méthodes avancées montrent que la variation très rapide du brouillage n'apporte pas toujours de meilleurs résultats. Dans les deux cas de tests, amplitude et délai, une variation au 32 μ s a donné de meilleurs résultats sur l'EVM. Lorsque la variation est trop rapide, le signal du DRFM subit une déformation importante qui augmente grandement la puissance dans les bandes latérales du signal. Cette déformation est particulièrement visible

dans le brouillage par délai rapide où le signal de base n'est plus visible. La comparaison des deux méthodes lentes montre que le brouillage par variation de délai donne un EVM beaucoup plus haut (entre 8 et 20 dB) pour un même rapport SIR, comme illustré à la figure 5.22.

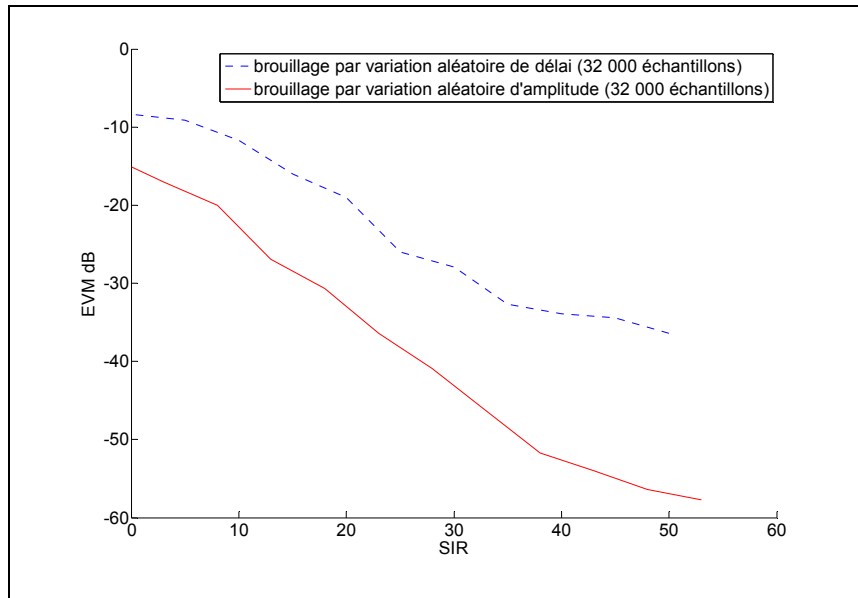


Figure 5.22 Comparaison des EVM pour les brouillages par variation aléatoire de délai et d'amplitude aux 32 000 échantillons

5.6.2 Techniques classiques et comparaison

L'analyse des tests suscite des questions sur les résultats du brouillage par bruit blanc simulé. Il est possible que notre bruit blanc artificiel perde ses caractéristiques « blanc » sur une trop petite plage de fréquences. La figure 5.23 présente la forme du bruit blanc généré sur la plage de 400 KHz utilisée par le signal GSM. Le signal a des variations de puissance visibles qui peuvent influencer ses performances. Avec les méthodes classiques, le brouillage « spot » obtient de meilleurs résultats que le balayage, mais les deux méthodes semblent atteindre des plateaux similaire pour des SIR élevé et faible. Les résultats utilisés pour la comparaison sont ceux de cas optimaux utilisant un positionnement idéal. Le brouillage « spot » est superposé

directement au signal GSM-EDGE et le brouillage par balayage est créé pour qu'une des fréquences ciblées lors du balayage se retrouve aussi superposée directement. Un mauvais positionnement ou un balayage de fréquences trop large ont un impact négatif sur les performances. Par exemple, dans le cas du signal « spot », un signal trop éloigné dans le spectre n'aura aucun impact sur le signal de base. Le brouillage par barrage règle le problème du balayage et offre une efficacité constante, mais a moins d'impact sur la communication.

La figure 5.24 illustre la comparaison des méthodes avancées avec la technique classique la plus efficace, le brouillage « spot ». Le brouillage par délai aléatoire a généralement un meilleur impact sur l'EVM. De plus, la fonction de brouilleur-répéteur du DRFM lui permet de positionner efficacement la puissance d'émission sur sa bande de fréquences sans détection précise du signal de base. À l'opposé, les techniques classiques doivent répartir la puissance sur une plage de fréquences ou effectuer une détection précise de la position du signal sur le spectre. Cependant, la variation du signal trop rapide par le DRFM peut diminuer l'efficacité du brouillage, comme c'est le cas pour une variation aux 10 échantillons.

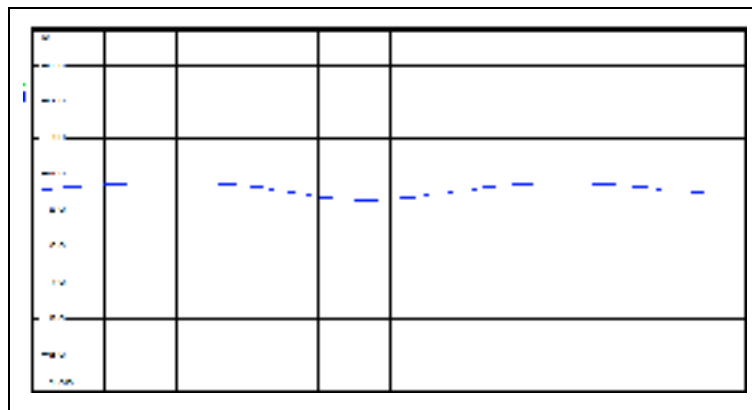


Figure 5.23 Bruit blanc simulée par le DRFM sur 400KHz autour de 2.45GHZ

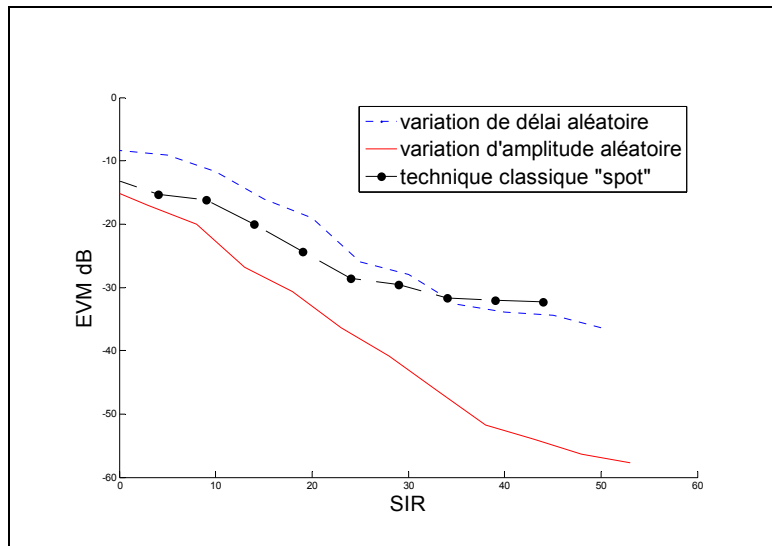


Figure 5.24 Comparaison des EVM entre le brouillage « spot » et les brouillages avancés avec variation aux 32 000 échantillons

5.7 Résumé

Dans ce chapitre, les techniques de brouillage sont utilisées sur le standard GSM-EDGE. Bien que ce standard soit moins récent, il est encore présent sur plusieurs appareils commerciaux. Il utilise une modulation simple et a une bande passante beaucoup plus petite que les autres standards testés, soit 270.83 kHz. Pour les techniques de brouillage classiques, la petite taille du signal sur le spectre de fréquence rend le brouillage « spot » la méthode la plus efficace. Cependant, les résultats du brouillage par variations de délai aléatoire sont très prometteurs et même parfois supérieurs au brouillage « spot ». La taille du signal de base n'a pas d'importance pour le DRFM puisque sa fonction d'écouteur-répéteur assure que la puissance est toujours sur la fréquence du signal, tout en couvrant une grande largeur de bande passante.

CHAPITRE 6

Impacts sur le standard W-CDMA

6.1 W-CDMA

La génération 3G des appareils mobiles utilise plusieurs systèmes différents ayant comme point commun l'utilisation d'une forme de CDMA (International Telecommunication Union, 2002). Le CDMA, qui signifie « code division multiple access », est une technique de communication sans fil qui utilise l'étalement de spectre. Deux méthodes sont généralement utilisées : l'étalement par saut de fréquence et l'étalement par séquence directe. L'étalement de spectre a plusieurs avantages. Le premier est de rendre la communication plus sécuritaire, car un récepteur sans le code de la communication ne peut le décoder.

Le CDMA par saut de fréquence (FH-CDMA) consiste à faire varier la fréquence d'émission du signal selon un patron prédéterminé. Le code de cette communication correspond à l'information sur l'ordre des fréquences utilisées. Cette méthode permet aussi de diminuer les effets multitrajets si le saut de fréquence est plus rapide que le délai des trajets avec réflexion. (Proakis, 2008)

Le CDMA par séquence directe (DS-CDMA) effectue l'étalement de spectre en multipliant le signal de base, un signal NRZ, par une série de bits à une fréquence plus élevée nommés « chips », comme illustré à la figure 6.1. Le résultat de la multiplication a la forme (Stremmer, 1990):

$$s(t) = m(t)c(t) \cos(2\pi f_p t + \phi) \quad (6.1)$$

où « $s(t)$ » est le signal transmis, « $m(t)$ » est le signal de base, « $c(t)$ » est le signal de codage « chips », « f_p » est la fréquence de la porteuse et « ϕ » est la phase du signal « s ». Le signal de base $m(t)$ subit un étalement de sa puissance sur une bande passante correspondant aux

taux de codage ou « chip rate » comme présentés à la figure 6.2. Il est possible de superposer plusieurs signaux sur la même bande de fréquences en utilisant des codes avec peu ou pas de corrélations. Le signal devient :

$$s(t) = \sum_{i=1}^M m_i(t - \tau_i) c_i(t - \tau_i) \cos(2\pi f_p t + \phi_i) \quad (6.2)$$

où « $s(t)$ » est le signal transmis, « $m(t)$ » est le signal de base, « $c(t)$ » est le signal de codage « chips », « f_p » est la fréquence de la porteuse, « ϕ_i » est la phase du signal « s » et « τ » est le délai de propagation (Stremmer, 1990).

À la réception, une opération de désétalement est effectuée sur le signal. Pour chaque canal, le récepteur multiplie le signal par le code correspondant. Le signal devient alors :

$$w(t) = m_k(t - \tau_k) + \left[\sum_{\substack{i=1 \\ i \neq k}}^N m_i(t - \tau_i) c_i(t - \tau_i) c_k(t - \tau_k) \cos(2\pi f_p t + \phi_i - \phi_k) \right] \quad (6.3)$$

où « m_k » est le signal du canal désiré, « c_k » est le code associé au signal, « m_i » représente les signaux des autres canaux et « c_i » les codes des autres signaux. Puisque les codes sont choisis de manière à avoir une corrélation faible, on peut simplifier la formule utilisant l'approximation :

$$\int_s c_k(t - \tau_k) c_j(t - \tau_k) << 1 \quad (6.4)$$

où « c_k » et « c_j » sont des signaux de codes différents. Après un filtrage adapté, le résultat de la sommation dans l'équation 6.3 est donc négligeable et on y retrouve le signal de base

(Stremler, 1990). La figure 6.3 illustre le schéma d'une communication CDMA avec plusieurs mutileurs sur un même spectre de fréquence. En plus de décoder le signal, cette opération est effectuée sur tous les autres signaux présents sur la bande de fréquences. Tout signal indésirable, comme du bruit ou une interférence, subit un étalement de spectre à la réception, ce qui diminue grandement son impact sur le SNR (Proakis, 2008). La puissance du brouilleur sur le signal décodé devient :

$$P_r = \frac{P_i}{T_s / T_c} \quad (6.5)$$

où « P_r » est la puissance du brouillage après décodage, « P_i » est la puissance de brouillage à la réception, « T_s » est la période des symboles et « T_c » est la période des bits du code. Le rapport de la période d'un symbole sur la période d'un bit de code est appelé gain de traitement.

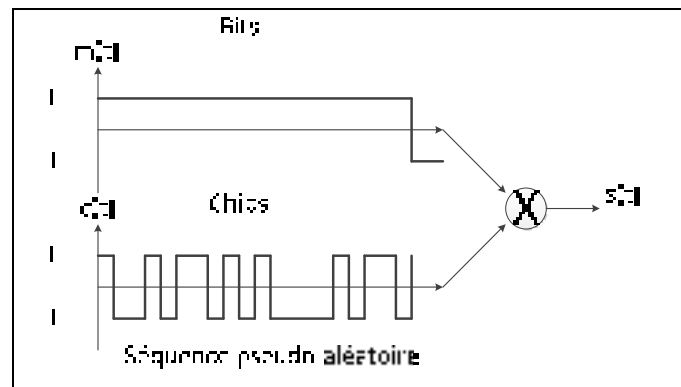


Figure 6.1 Codage CDMA

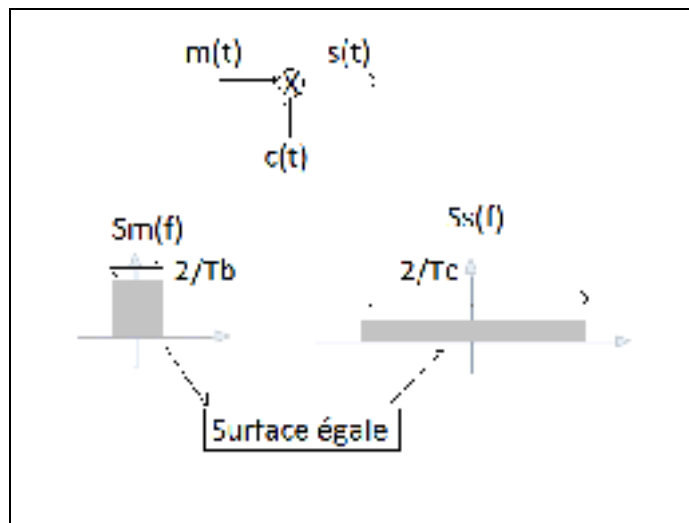


Figure 6.2 Étalement spectral par séquence directe

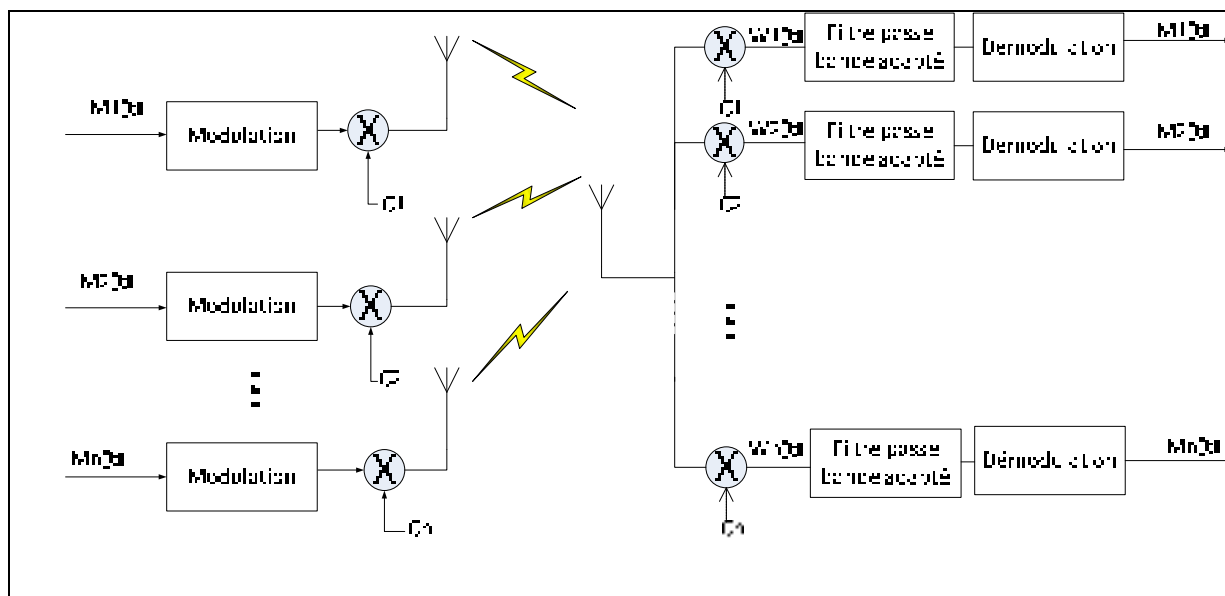


Figure 6.3 Communication DS-SS à utilisateurs multiples

6.2 Signaux générés

Le standard CDMA utilisé pour les tests est le W-CDMA ou « Wideband CDMA ». Le W-CDMA est un des différents standards utilisant l'étalement de spectre par séquence directe. Son appellation « large bande » provient de son étalement spectral supérieur au CDMA2000 et au TD-SCDMA (International Telecommunication Union, 2002). Le signal généré pour les tests est un signal W-CDMA provenant d'une station de base cellulaire. Le signal provenant d'une station de base est plus intéressant, car il doit communiquer avec plusieurs mobiles simultanément, donc utiliser plusieurs canaux superposés dans sa bande de fréquences. Les caractéristiques du signal sont décrites dans les tableaux 6.1 et la figure 6.4 montre la forme du signal avec étalement spectral. Pour les tests, l'EVM sur le symbole est utilisé afin de mesurer l'efficacité du brouillage.

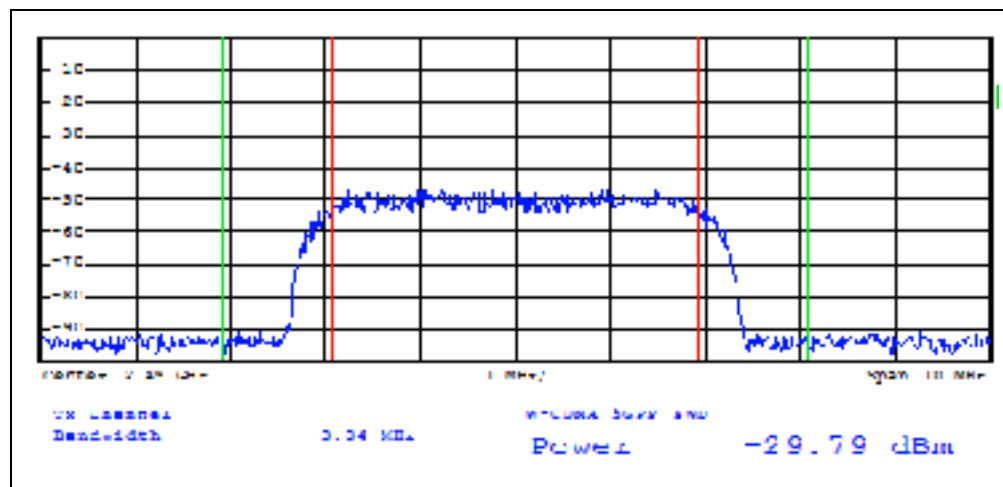


Figure 6.4 Spectre du signal W-CDMA

Tableau 6.1 Caractéristiques du signal W-CDMA

Fréquence centrale	2,45 GHz
Version 3GPP	9
Direction	Downlink/Forward
Taux de symboles	15 Ksps
Taux de codage (Chip rate)	3,84 Mcps
Bande passante	3,84 MHz
Gain de traitement	256
Filtre	Cosinus surélevé $\alpha=0,22$
Canaux actifs	68

6.3 Effets du brouillage par variation de délai aléatoire

Le brouillage par variation de délai aléatoire devrait avoir un impact important sur le décodage du signal. La superposition du signal de base et du signal brouillé varie durant l'opération de décodage, ce qui affecte tous les délais présents dans l'équation 6.3. Le tableau 6.2 décrit les configurations des brouillages utilisés pour les tests.

Tableau 6.2 caractéristiques des brouillages par variation de délai utilisé

	Variation rapide	Variation lente
Nombre d'échantillons entre les variations	10	32 000
Inversion du signal	non	non
Plage du délai	0 — 4 μ s	0 — 4 μ s

Le brouillage avec variation rapide, fait varier le délai aléatoire chaque 10 échantillons de signal, ce qui correspond à un changement chaque 10 ns. La figure 6.5 présente l'impact de la variation sur le signal CDMA. La forme du signal du DRFM est très différente du signal

CDMA original et la puissance dans la bande du signal original est diminuée d'environ 3 dB. Le brouillage avec variation lente change le délai aléatoire chaque 32 000 échantillons, ce qui correspond à un changement de délai toutes les 32 μ s. La figure 6.6 montre la forme du signal W-CDMA résultant : le signal est identique et la puissance dans la bande est similaire. La figure 6.7 trace la progression des courbes EVM pour les deux configurations du brouillage par variation de délai aléatoire. Les deux courbes ont des résultats similaires. Le nombre d'échantillons entre les variations de délai semble avoir un impact minime sur la performance du brouillage.

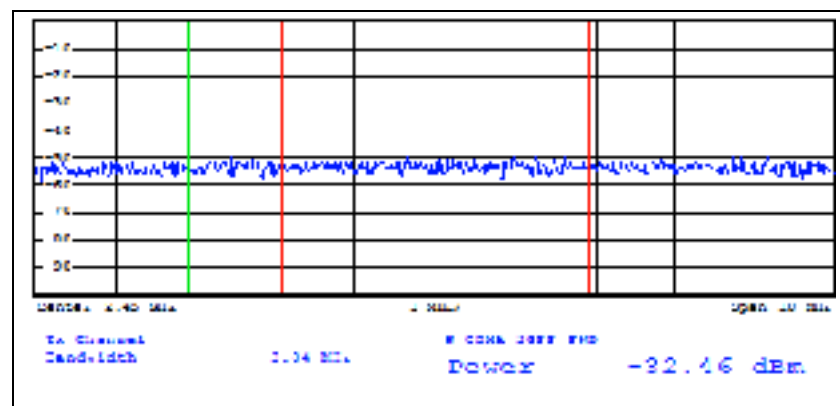


Figure 6.5 Spectre du signal W-CDMA avec variation de délai aléatoire rapide

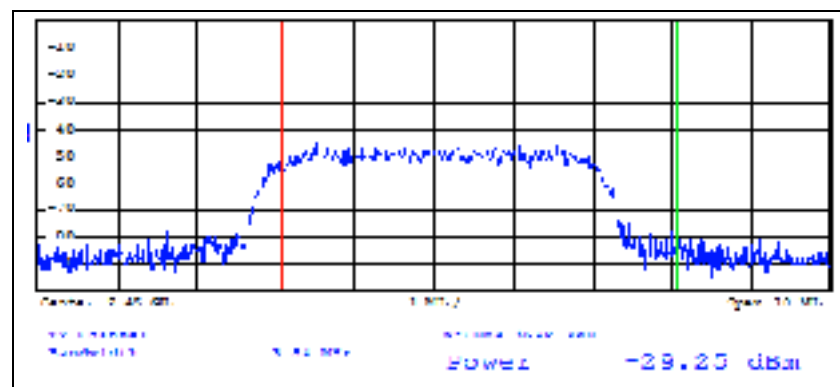


Figure 6.6 Spectre du signal W-CDMA avec variation de délai aléatoire lente

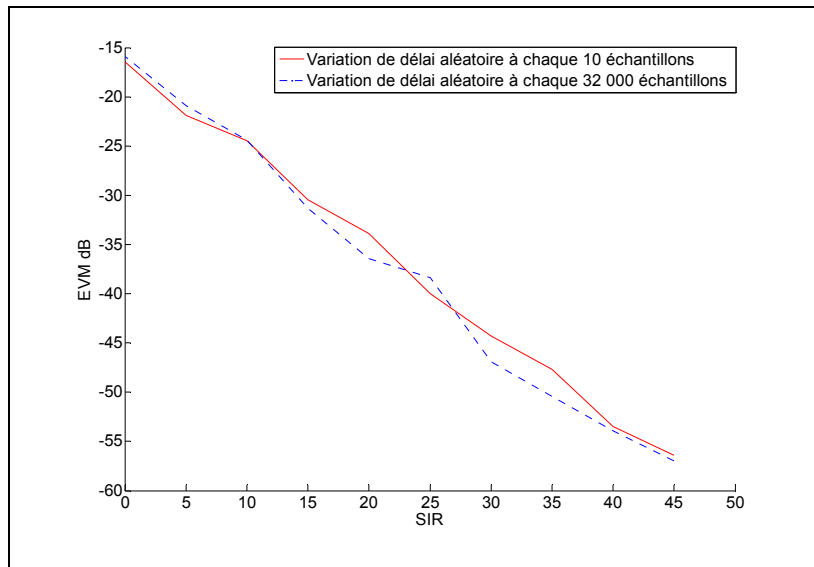


Figure 6.7 Comparaison des EVM pour un signal W-CDMA avec brouillage par délai aléatoire

6.4 Effets du brouillage par variation aléatoire d'amplitude

Le brouillage par variation aléatoire d'amplitude tente de créer une variation assez grande et assez rapide pour déjouer les AGC de la réception. À cause de la variation du module du signal, toutes les mesures de puissance sont prises avant l'application du brouillage. Le tableau 6.3 décrit les configurations des brouillages utilisés pour les tests.

Tableau 6.3 Caractéristiques des brouillages par variation de délai utilisé

	Variation rapide	Variation lente
Nombre d'échantillons entre les variations	10	32 000
Inversion du signal	non	non
Taille de l'entier utilisé	12 bits	12 bits

Pour le brouillage à variation rapide d'amplitude, le nombre d'échantillons entre chaque variation d'amplitude est de 10, ce qui correspond à un changement chaque 10 ns. La figure

6.8 présente la forme du signal CDMA soumis à une variation d'amplitude aléatoire rapide. La forme du signal est similaire au signal de base, mais avec une augmentation marquée de la puissance dans les bandes latérales. Le brouillage avec une variation d'amplitude lente, utilise 32 000 échantillons, ce qui correspond à un changement d'amplitude toutes les 32 μ s. La figure 6.9 montre l'impact du brouillage par variation d'amplitude lente sur le signal. Le niveau du signal sur sa bande passante subit des variations de puissance visibles. La puissance totale sur la bande est diminuée, car comme mentionné au chapitre 3, le brouillage par variation d'amplitude effectue une diminution aléatoire du niveau du signal. La figure 6.10 trace la progression des EVM pour les deux configurations du brouillage. Les deux courbes sont similaires, mais le brouillage avec variation lente a généralement de meilleurs résultats.

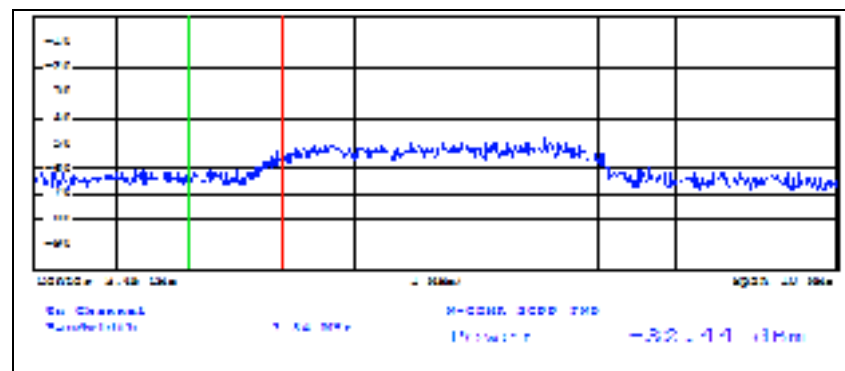


Figure 6.8 Spectre du signal W-CDMA avec variation d'amplitude aléatoire rapide

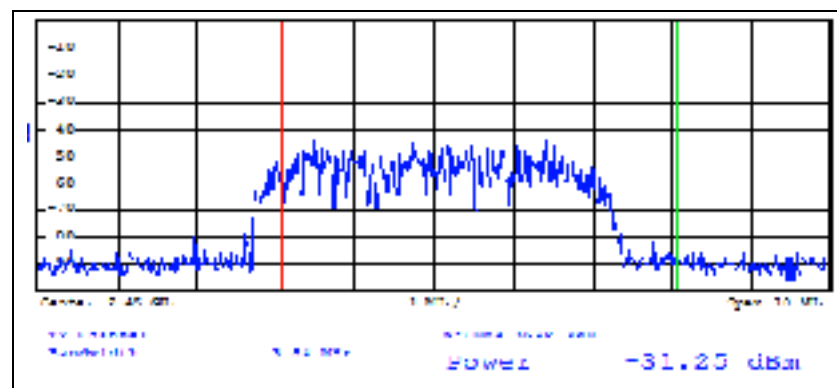


Figure 6.9 Spectre du signal W-CDMA avec variation d'amplitude aléatoire lente

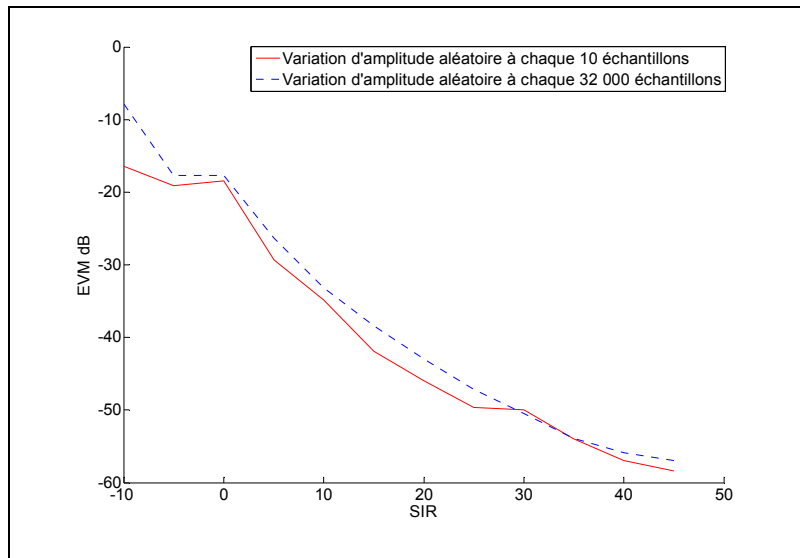


Figure 6.10 Comparaison des EVM pour un signal W-CDMA avec brouillage par amplitude aléatoire

6.5 Effets des techniques classiques

Pour améliorer nos connaissances sur le comportement du signal W-CDMA en présence de brouillage, une série de tests sont réalisés utilisant les méthodes classiques implémentées sur le DRFM. Les brouillages de type bruit blanc, « spot », balayage et barrage sont émulsés et superposés au signal DRFM. La puissance du brouillage utilisé pour le SIR est mesurée sur la bande de fréquences du signal de base 3,84 MHz et ne tient pas compte de la partie du signal inutile.

6.5.1 Bruit blanc

La radio DRFM est configurée pour émettre du bruit blanc sur toute la bande de fréquences. Puisque le bruit blanc est non corrélé et de densité de puissance constante, l'opération de désétalement ne modifie pas sa nature. Un bruit blanc multiplié par un code pseudo-aléatoire donne un bruit blanc de même densité de puissance. La figure 6.11 présente la progression de l'EVM pour ce brouillage par bruit blanc simulé. La progression de l'EVM est presque

linéaire avec une pente moyenne approximative de moins 1. Cette courbe servira de référence pour les autres techniques de brouillage.

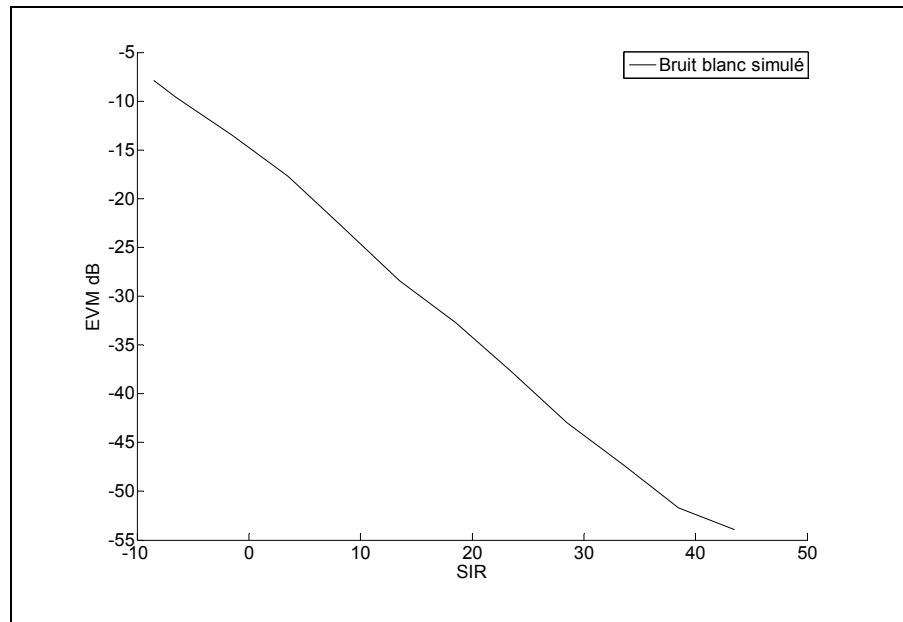


Figure 6.11 EVM pour un signal W-CDMA pour un bruit blanc émulé

6.5.2 Spot et balayage et barrage

Le signal de brouillage « spot » est positionné au centre de la bande de 3,84MHz. Notre brouillage par balayage utilise un saut de fréquence de 500 KHz sur 10 MHz pour une durée de 500 us par fréquence. Puisque le signal W-CDMA couvre une bande de 3,84 MHz, plusieurs des sommets du signal sont positionnés dans la bande de fréquences du signal, comme illustré à la figure 6.12. En maximisant les paramètres du brouillage par balayage, on peut créer un signal très proche d'un brouillage par barrage. La radio DRFM est capable de diminuer l'écart entre les fréquences à 25 KHz et le temps par fréquence à 5 μ s, la figure 6.13 montre le signal résultant.

La progression de l'EVM du signal W-CDMA avec les brouillages « spot », balayage, barrage et bruits blanc émulé est illustrée à la figure 6.14. Toutes les courbes d'EVM suivent la même progression.

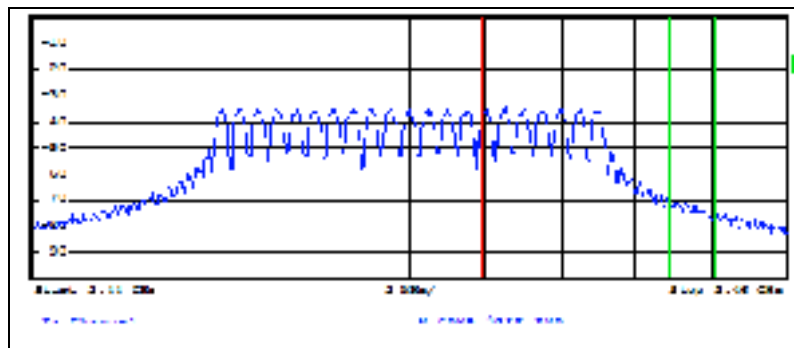


Figure 6.12 Spectre du signal de brouillage par balayage

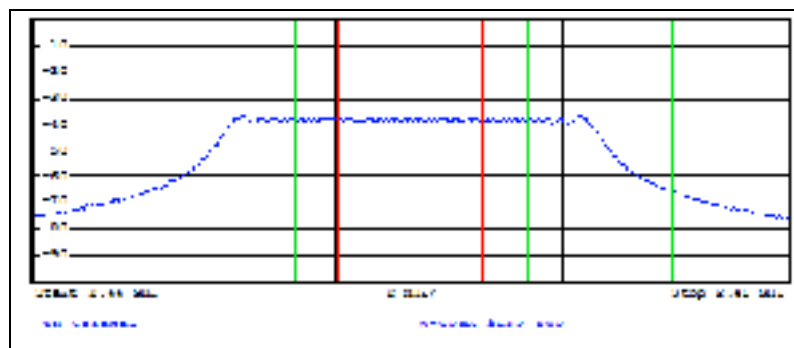


Figure 6.13 Spectre du signal de brouillage par barrage émulé

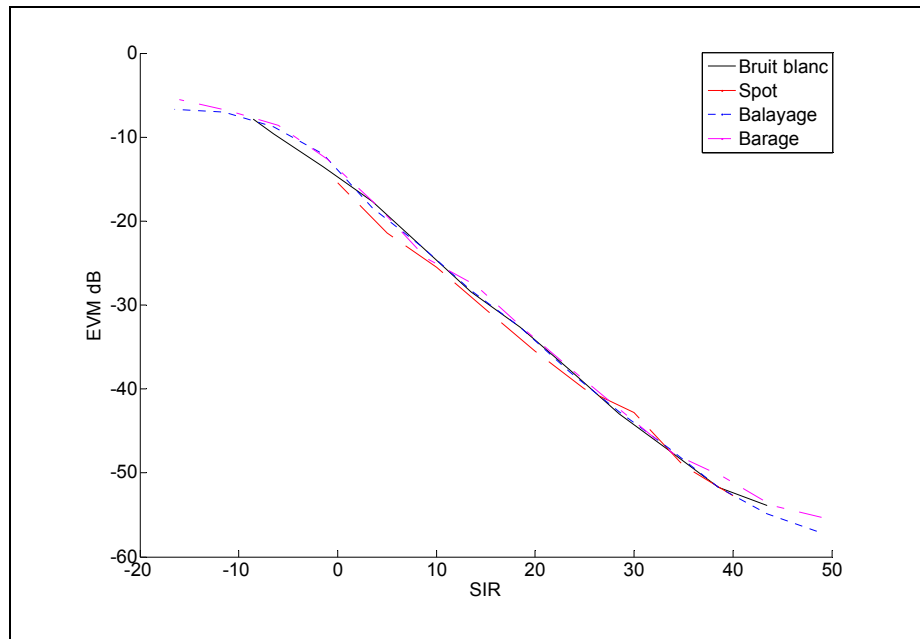


Figure 6.14 Comparaison des EVM sur un signal W-CDMA avec un brouillage « spot », balayage, barrage et bruit blanc simulé

6.6 Analyse

Les courbes d'EVM pour les techniques classiques ont toutes des résultats très rapprochés, comme le montre la figure 6.14. Toute interférence sur la bande passante du CDMA subit un étalement spectral lors du décodage. Cette opération a donc un effet similaire, peu importe le type de brouillage utilisé. L'impact sur le signal de base dépend donc uniquement de la puissance du signal de brouillage, aussi longtemps que celui-ci est dans la bande de fréquences occupée par le signal de base.

Une comparaison des techniques de brouillage avec traitement de signaux rapide montre que le brouillage par variation de délai a des meilleures performances que le brouillage par variation d'amplitude. La figure 6.15 trace la comparaison des performances pour les brouillages avec une variation aléatoire de délai et d'amplitude aux 32 000 échantillons. Le niveau de l'EVM pour le brouillage par délai est très proche de celui par bruit blanc. Les variations aléatoires sur signal ont comme effet de transformer le code CDMA et de diminuer

sa corrélation avec le code de base. Le signal résultant du DRFM n'est donc pas reconnu et subit le même traitement que toutes les autres sources de bruit. Comme pour les techniques classiques, seule la puissance du signal et non sa forme affecte les performances de la communication. En se basant sur cette observation, il est possible de conclure que la diminution d'efficacité du brouillage par variation d'amplitude aléatoire est uniquement due à la diminution de puissance apportée par le traitement de signal.

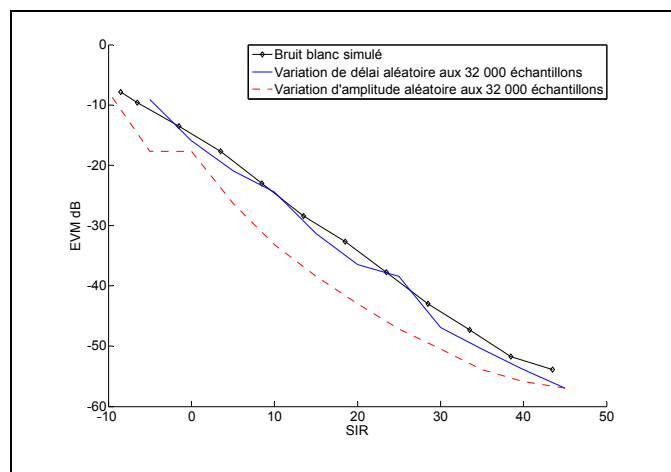


Figure 6.15 Comparaison des EVM pour les brouillages avancés avec un bruit blanc

Un autre cas à considérer est celui où le DRFM retransmet le signal tel quel. Une sélectivité en fréquence apparaît alors sur le canal comme présenté à la figure 6.16. Puisque le code reste inchangé, le signal est reconnu par le récepteur et désécalé avec le signal de base. Le code se trouve décalé d'environ 1 bit de code puisque le délai de traitement du DRFM est de 217 ns et que chaque bit de code a une durée de 260 ns. Cette interférence multitrajet semble avoir un impact majeur, mais peut facilement être contrée par un récepteur RAKE.

Le récepteur RAKE est conçu spécialement pour contrer les effets des canaux multitrajet. Il effectue un décodage du signal en parallèle pour chaque trajet individuel (Stremler, 1990). Le signal est soumis aux codes CDMA à des délais différents. Les signaux obtenus sont recombinaés pour créer une diversité spatiale et éviter les évanouissements. Notre analyseur de signaux n'utilise pas de récepteur RAKE et ne peut donc pas contrer un simple effet à

deux trajets. Pour le brouilleur, il est possible de déjouer un récepteur RAKE si la variation de délai est assez rapide pour empêcher le récepteur de suivre les changements.

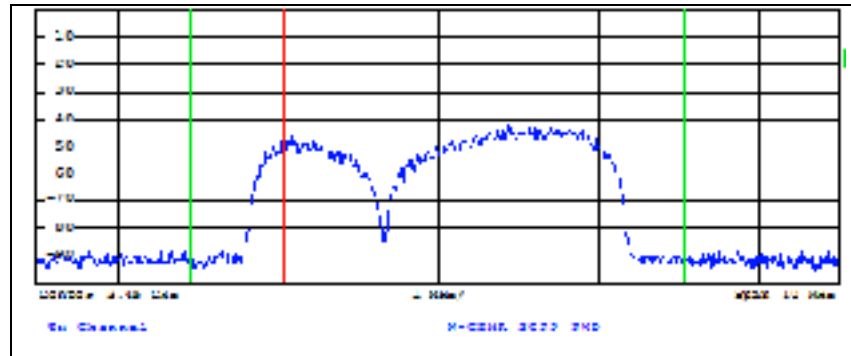


Figure 6.16 Superposition de deux signaux CDMA similaires avec un délai fixe

Une comparaison entre les méthodes avec traitement de signal avancé et les méthodes classiques montre qu'aucune méthode ne semble avoir une efficacité accrue sur le CDMA par séquence directe. Tous les brouillages subissent l'étalement spectral et ont le même impact sur la communication. Par contre, le DRFM a l'avantage de couvrir une large bande et d'envoyer sa puissance directement sur la bande du signal sans détection précise, ce qui lui donne un avantage contre les communications DS-CDMA. De plus, sa vitesse de traitement lui permettrait d'avoir une bonne efficacité sur le FH-CDMA.

6.7 Résumé

Le W-CDMA est le dernier standard testé dans le cadre de ce mémoire. Ce standard est unique à cause du codage des données qui entraîne un étalement fréquentiel à l'émetteur et un désétalement au récepteur. Comme les résultats le démontrent, ces opérations confèrent au signal une résistance accrue au brouillage, peu importe la méthode utilisée. De plus, on remarque encore que le brouillage par variations d'amplitude a un impact moins grand sur le signal que la méthode par variations aléatoires du délai. La prochaine étape du mémoire est la comparaison des résultats sur les trois standards simultanément pour avoir une vision globale des performances de nos techniques de brouillage.

CHAPITRE 7

Analyse comparative

7.1 Impact du traitement sur le signal échantillonné

L'objectif principal de cette thèse est de tester les méthodes de brouillages utilisant le traitement de signaux rapide du DRFM. Si l'on observe l'effet des traitements de signaux rapides sur le signal de base, on peut remarquer une augmentation de la puissance sur les bandes latérales du spectre de fréquence. La figure 7.1 illustre la progression de la forme du signal pour différents temps ou nombres d'échantillons entre les variations aléatoires. Plus la vitesse des variations du signal est courte, plus la puissance se répartit dans les bandes latérales du signal. Ce phénomène explique pourquoi les brouillages avec variation rapide sont souvent moins performants : moins de puissance est sur la bande du signal visé pour une même puissance à l'émission.

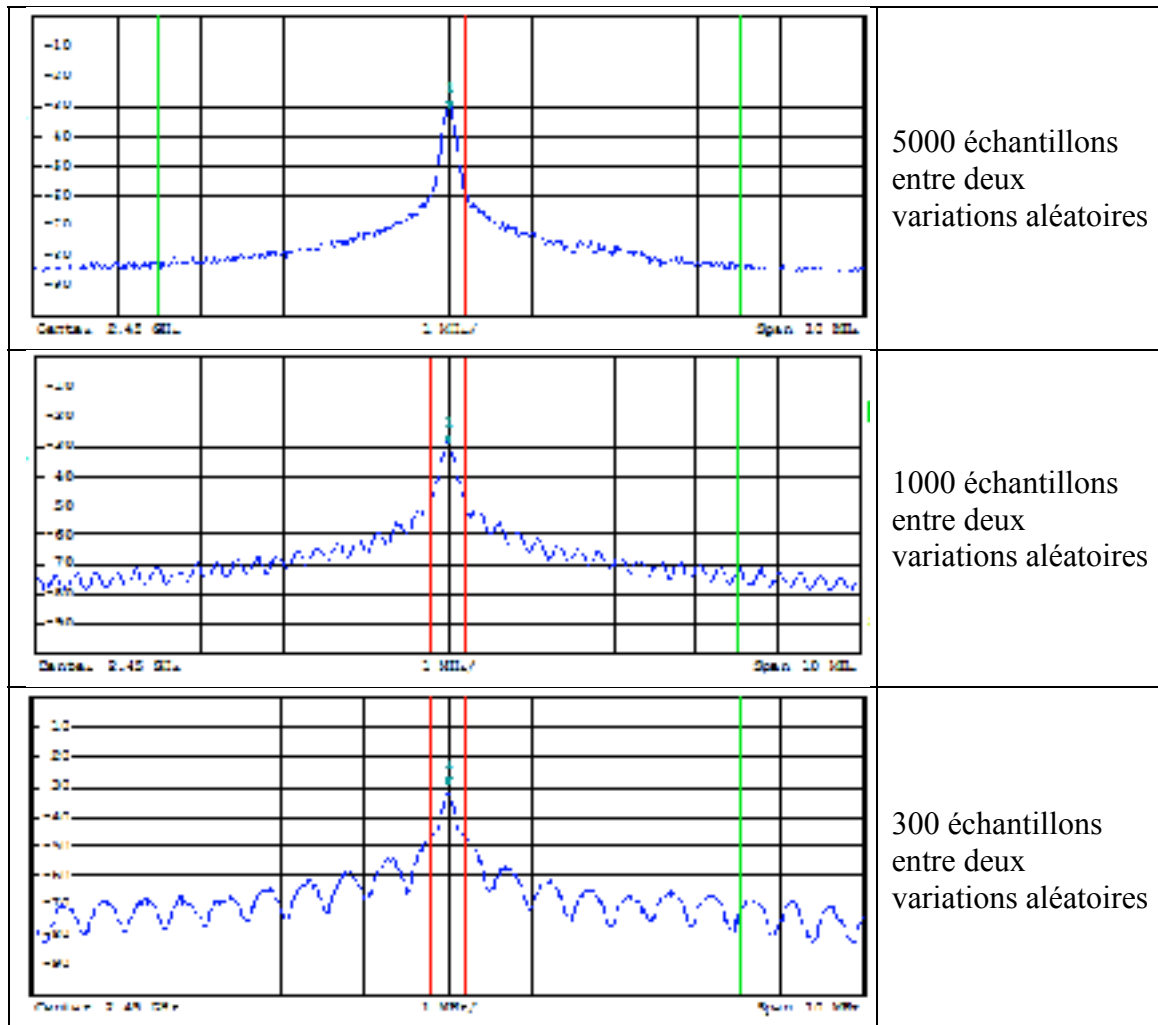


Figure 7.1 Effets des variations aléatoires sur le signal de base selon leur vitesse

7.2 Limite du EVM sur un signal WiMAX

Les mesures des EVM pour les différents signaux WiMAX donnent des résultats très similaires. L'impact sur la communication dépend du niveau limite de l'EVM pour nuire à la communication. Cette valeur change selon la modulation utilisée, comme le montre la figure 7.2. À cause de cette similarité, seule la courbe de l'EVM pour le BPSK est présentée pour les comparaisons avec les autres standards. Plusieurs communications multiporteuses

diminuent dynamiquement la modulation en présence d'interférence. Le BPSK est donc souvent le standard qui sera utilisé si un brouillage est présent.

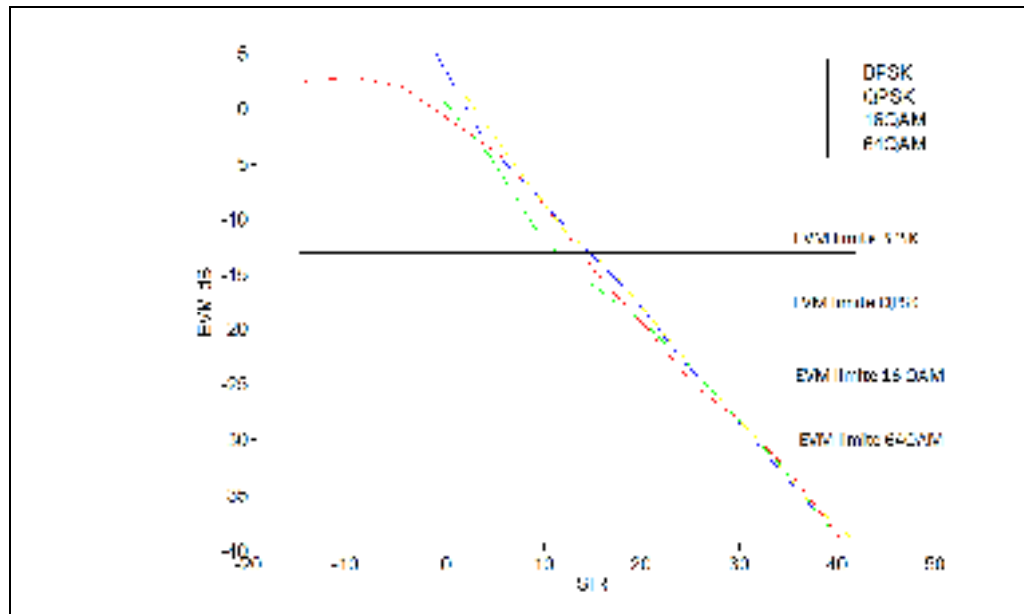


Figure 7.2 EVM du WiMAX avec brouillage par variation de délai aléatoire aux 32 000 échantillons avec limites sur le EVM

7.3 Comparaison des techniques avancées sur les trois standards

Les résultats des tests peuvent être utilisés pour comparer séparément chaque méthode de brouillage avancée et ainsi voir quel standard est le plus affecté par le brouillage. Notre première nouvelle méthode est celle utilisant une variation de délai aléatoire sur le signal. En utilisant l'EVM comme source de comparaison, on peut observer ses effets sur les 3 standards cellulaires utilisés pour les tests. La figure 7.3 trace les EVM des communications en présence d'un brouillage par variation de délai rapide (19 ns) et lent (32 μ s). On remarque facilement que le standard W-CDMA est le plus résistant à ce type de brouillage. Si l'on augmente la vitesse de la variation du délai pour créer un brouillage par variation de délai rapide, les résultats restent similaires pour le WiMAX et le CDMA, mais ont moins d'impact

sur le GSM-EDGE. Ceci est probablement dû à la transformation de la forme du signal lors de la variation rapide du signal qui diminue la puissance du brouillage sur la plage de fréquences du signal de base.

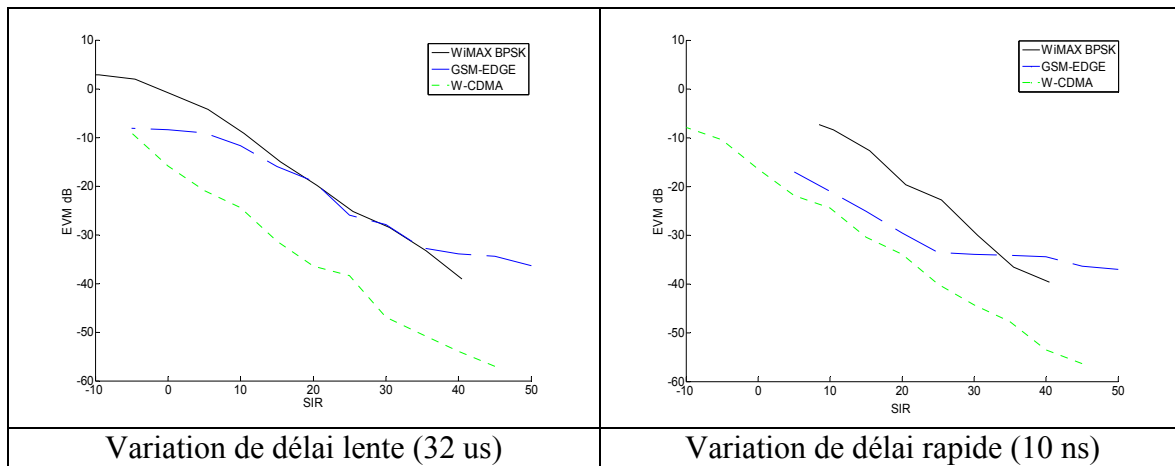


Figure 7.3 Comparaison des EVM sur les trois standards testés pour le brouillage par variation de délai aléatoire

La deuxième méthode de brouillage implémentée avec le traitement de signaux rapide est la variation d'amplitude aléatoire. La figure 7.4 illustre la progression des EVM des standards utilisés pour une variation de l'amplitude aux 32 000 échantillons et aux 10 échantillons. Les EVM sont moins élevés que pour le brouillage par variation de délai et l'impact sur le CDMA est encore une fois plus bas que sur les deux autres standards. Pour le brouillage par variation d'amplitude rapide (10 ns), les performances du brouillage sur le GSM-EDGE sont moindres alors que celles sur les deux autres standards sont meilleures. Les standards W-CDMA et WiMAX sont donc plus affectés par une variation d'amplitude rapide qu'une variation plus lente. L'étalement de la puissance est probablement la cause de la performance moindre sur le GSM-EDGE puisque la plage de fréquences utilisées est beaucoup moins grande.

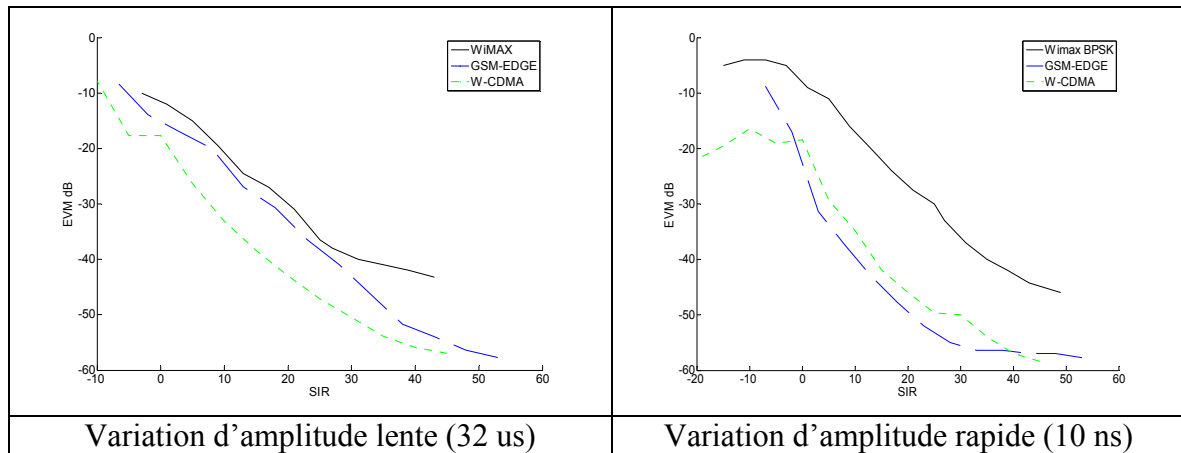


Figure 7.4 Comparaison des EVM sur les trois standards testés pour le brouillage par variation d'amplitude aléatoire

De manière générale, le brouillage par variation de délai aléatoire obtient de meilleures performances, plus d'interférence, que la variation d'amplitude aléatoire. La perte de performance du brouillage par variation d'amplitude est probablement due à la distribution normale discrète utilisée pour faire varier l'amplitude. La même distribution est utilisée pour le délai, mais une variation du délai donne un résultat sur le signal beaucoup moins prévisible qu'une variation de l'amplitude. Le CDMA est généralement le standard qui est le moins affecté par les brouillages avec traitement de signaux rapide. L'utilisation du codage par séquence directe offre donc une très bonne résistance aux techniques de brouillage DRFM. L'opération d'étalement des signaux indésirables dans la bande de fréquences écoutée est très difficile à contrer puisque brouiller le signal en conservant le code intact entraîne plusieurs complications.

7.4 Comparaison des performances des techniques classiques sur les trois standard

La même comparaison sur les trois standards utilisés peut être effectuée pour les techniques de brouillage classiques. Le bruit blanc émulé par le DRFM devrait théoriquement avoir un impact similaire à une diminution du SNR et diminuer la capacité du canal selon l'équation (1.5). La figure 7.5 trace les EVM obtenus en présence de bruit blanc. Le W-CDMA est le

standard qui suit la progression logarithmique implicite. Le WiMAX et le GSM semblent converger vers un EVM minimal, probablement dû au bruit et à l'atténuation du banc de test.

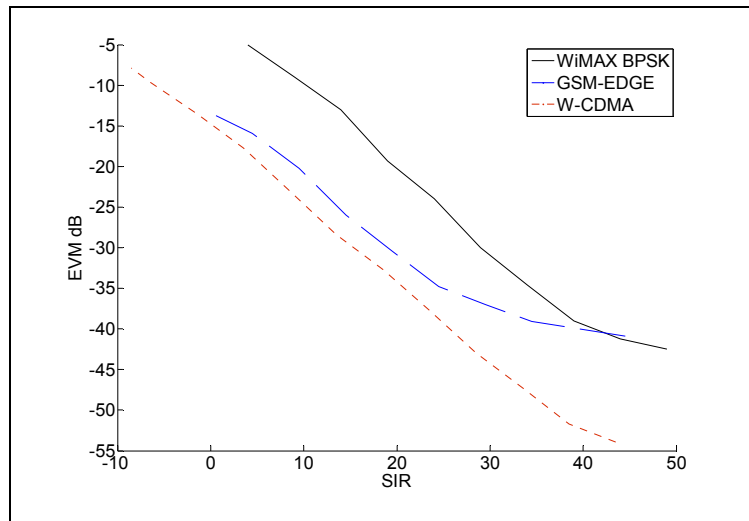


Figure 7.5 EVM du brouillage par bruit blanc émulé sur les trois standards testés

La figure 7.6 présente les impacts des brouillages « spot », balayage et barrage. Le brouillage « spot » concentre sa puissance sur une très petite plage de fréquences. Pour le GSM-EDGE, puisque les signaux de brouillage et de communication sont très étroits, l'impact du brouillage dépend de la position adéquate du signal du brouilleur. Si le brouillage est centré sur la communication, l'impact sera très grand même à faible puissance, car toute la puissance de l'émetteur couvre toute la bande du signal. Si, à l'opposé, le signal du brouilleur n'est pas positionné correctement, aucun impact ne sera perçu sur la communication. Le WiMAX compense son EVM avec les porteuses non affectées par le brouillage « spot » et subit moins d'impact que pour un bruit blanc. La position du brouillage peut aussi changer son impact sur le WiMAX, comme mentionné au chapitre 4. Si un des pilotes utilisés pour la synchronisation de la trame est visé par le brouillage « spot » avec assez de puissance, la trame se perd complètement. Le brouillage par balayage a un impact beaucoup moins grand sur le GSM-EDGE. Puisque la puissance du brouillage sur le signal est maintenant répartie sur une plus large bande, moins de puissance se trouve dans la bande du signal que pour un brouillage « spot » directement superposé. Similairement, le brouillage par barrage simulé augmente la courbe de l'EVM sur le GSM-EDGE, mais sans atteindre le niveau précédemment obtenu par le brouillage « spot ». Les standards W-CDMA et WiMAX quant

à eux, ont des courbes similaires peu importe la méthode utilisée. Le W-CDMA effectue un étalement du brouillage, peu importe la forme qu'il prend. L'impact sur le EVM reste similaire d'une méthode à l'autre.

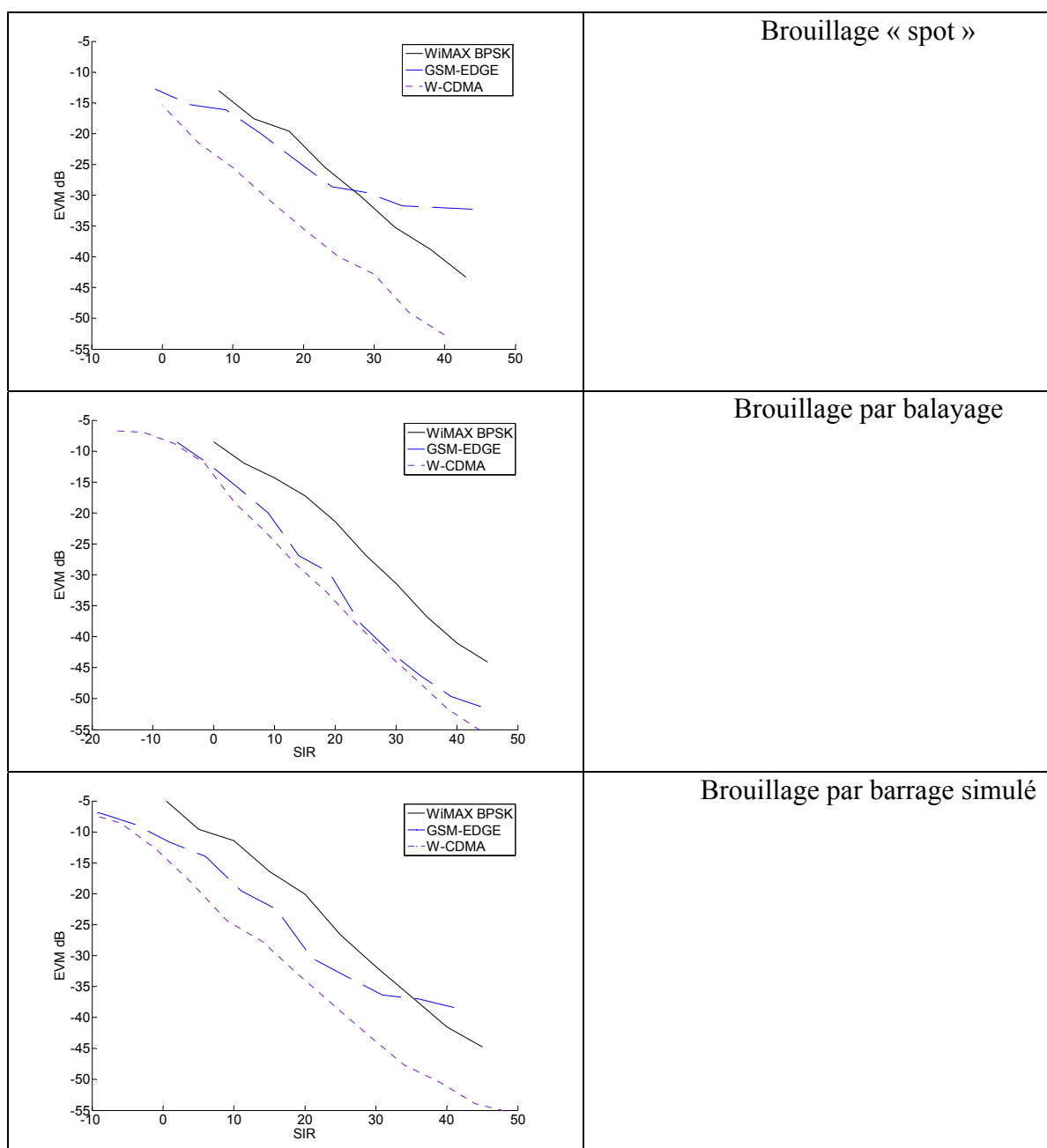


Figure 7.6 EVM des techniques de brouillage classiques utilisées sur les trois standards testés

7.5 Comparaison des puissances requises pour nuire à la communication et la couper

Dans le but de concevoir un système de brouillage appliqué sur un réseau de téléphonie cellulaire, il est intéressant de savoir quel type de brouillage requiert le moins de puissance d'émission pour nuire à la communication. Utilisant les résultats obtenus, il est possible de trouver le SIR à la réception requis pour nuire à la communication et le SIR requis pour que la communication soit indétectable. Pour avoir une comparaison valable entre les méthodes de brouillages, la puissance des techniques de brouillage classiques est mesurée sur la bande passante du signal de base utilisé et non sur leurs spectres de fréquence totaux. Similairement, lorsque le traitement de signal des méthodes avancées modifie la forme du signal de brouillage, la puissance dans la bande de fréquences du signal original est mesurée.

Pour le WiMAX, la communication est considérée comme intelligible lorsque l'EVM dépasse le seuil déterminé par le type de constellation utilisé, lequel est présenté au tableau 7.1. Lorsqu'aucune trame n'est détectée au récepteur, la communication est considérée comme coupée. Le tableau 7.2 décrit les SIR requis pour nuire et pour couper une communication WiMAX selon la constellation. La constellation BPSK est celle qui offre le plus de résistance, à cause de sa limite élevée sur l'EVM. Pour la perte du signal, la majorité des SIR sont dans le même ordre de grandeur. Le brouillage par variation de délai aléatoire a les meilleurs résultats, comparables aux résultats du bruit blanc. Certains brouillages, comme la variation d'amplitude, ne sont pas capables de complètement brouiller la communication de base pour le récepteur. L'information est complètement intelligible, mais le récepteur est encore capable de voir et de décoder le signal WiMAX.

Tableau 7.1 EVM limite pour un signal WiMAX

Constellation	EVM limite
BPSK	- 13 dB
QPSK	- 18,5 dB
16QAM	- 25 dB
64QAM	- 31 dB

Tableau 7.2 SIR requis du DRFM pour nuire et pour couper une communication WiMAX

Technique de brouillage	Constellation	SIR brouillé (dB)	SIR perte de signal (dB)
Variation de délai aléatoire rapide	BPSK	15,5	5,5
	QPSK	13,5	3,5
	16 QAM	25,5	5,5
	64 QAM	30	5
Variation de délai aléatoire lente	BPSK	10,5	Hors de portée
	QPSK	19	- 6
	16 QAM	22	- 3
	64 QAM	29,5	- 5,5
Variation d'amplitude aléatoire rapide	BPSK	5	Hors de portée
	QPSK	5	Hors de portée
	16 QAM	13	Hors de portée
	64 QAM	21	Hors de portée
Variation d'amplitude aléatoire lente	BPSK	1	Hors de portée
	QPSK	1	Hors de portée
	16 QAM	13	Hors de portée
	64 QAM	21	Hors de portée
Bruit blanc	BPSK	14	9
	QPSK	15	10
	16 QAM	19	9
	64 QAM	29	9
Spot (non centré)	BPSK	4	- 1
	QPSK	19	14
	16 QAM	22	12
	64 QAM	20	10
Balayage	BPSK	5	Hors de portée
	QPSK	15	Hors de portée
	16QAM	23	Hors de portée
	64QAM	25	Hors de portée
Barrage	BPSK	10	0
	QPSK	18	- 5
	16QAM	26	- 4
	64QAM	27	- 5

Les tableaux 7.3 et 7.4 affichent les SIR des différentes méthodes de brouillages utilisées pour nuire et pour couper le GSM-EDGE et le W-CDMA. Ces standards n'ont pas de limite précise sur l'EVM. Le GSM-EDGE est mesuré à l'aide d'un analyseur de signaux vectoriels standards. Il est donc difficile de savoir quand la communication est coupée. En se basant sur les limites du QPSK et 16 QAM, on peut considérer arbitrairement que le signal est brouillé lorsque l'EVM atteint - 20 dB. Le brouillage par variation de délai permet d'atteindre cette limite avec un SIR élevé. À l'opposé, le brouillage par variation d'amplitude requiert un signal avec plus de puissance, environ 10 dB, pour obtenir un impact similaire. Dans le cas du brouillage par variation d'amplitude rapide, le signal de brouillage doit être de la même puissance que le signal de base pour atteindre un EVM de - 20 dB. Pour le W-CDMA, la communication est brouillée lorsque les pilotes sont incorrects et est perdue quand la synchronisation de la trame est impossible. Le W-CDMA réagit de manière similaire à la majorité des brouillages. Le brouillage par variation d'amplitude agit de manière unique : ce brouillage est capable d'obtenir de bons résultats à puissances égales, mais perd de l'efficacité si sa puissance devient plus grande que le signal de base. Le récepteur est donc capable de déchiffrer assez d'information du signal avec amplitude aléatoire pour toujours détecter la communication. L'impact du brouillage à puissance égale est augmenté par délai de 217 ns du DRFM.

Tableau 7.3 SIR requis pour brouiller une communication GSM-EDGE

Technique de brouillage	SIR brouillé (dB)
Variation de délai aléatoire rapide	10
Variation de délai aléatoire lente	20
Variation d'amplitude aléatoire rapide	0
Variation d'amplitude aléatoire lente	10
Bruit blanc	10
Spot	15
Balayage	10
Barrage	15

Tableau 7.4 SIR requis pour brouiller et pour couper une communication W-CDMA

Technique de brouillage	SIR brouillé (dB)	SIR perte de signal (dB)
Variation de délai aléatoire rapide	10	- 10
Variation de délai aléatoire lent	10	- 5
Variation d'amplitude aléatoire rapide	0	Hors de portée
Variation d'amplitude aléatoire lente	5	Hors de portée
Bruit blanc	8,5	- 8,5
Spot (non centré)	8,5	- 6,5
Balayage	13,5	- 11,5
Barrage	14	- 6

À partir de ces résultats, on observe que la puissance requise du brouilleur pour nuire et pour couper une communication varie grandement selon le brouillage et le standard utilisé. Comparées à l'utilisation de bruit blanc pour nuire au signal, les techniques de brouillage avancées n'offrent pas de gain substantiel sur le plan de la puissance requise. Couper complètement le signal est beaucoup plus difficile : certaines méthodes de brouillage en sont incapables ou requièrent des puissances hors de portée du banc de test pour y arriver. Le brouillage par variation de délai aléatoire est la méthode qui obtient les meilleures performances en comparaison avec les techniques standards. Il requiert des puissances similaires au bruit blanc pour obtenir les mêmes résultats, mais cible les communications et utilise sa puissance plus efficacement. La variation lente du délai (32 μ s) offre des résultats supérieurs à la variation rapide (10 ns), mais ce paramètre du brouillage pourrait être optimisé pour encore améliorer l'impact du brouillage. En comparaison, le brouillage par variation de délai d'amplitude aléatoire requiert plus de puissance pour brouiller l'information et a de la difficulté à couper les standards utilisant des porteuses pilotes. Pour les techniques classiques, un brouillage « spot » bien positionné semble toujours donner les meilleurs résultats, mais ce type de brouillage requiert une détection rapide et précise du signal de base. Utiliser un balayage en brouillant une plus large bande de fréquences aide, mais au coût de performances réduites.

7.6 Résumé

Une analyse comparative des méthodes de brouillage avancées et classiques supporte les résultats obtenus précédemment. La technique de brouillage par variation de délai aléatoire est capable de brouiller les signaux avec une efficacité comparable aux méthodes classiques, et la variation d'amplitude aléatoire ont une efficacité beaucoup plus faible. Par contre, lorsqu'on cherche à empêcher le récepteur de détecter le signal de base, l'efficacité des méthodes avancées est plus faible. Puisque le signal du brouilleur est similaire au signal de base, même à haute puissance le récepteur perçoit encore la présence d'une communication même si aucune information n'est décodée.

Pour bien comprendre les implications des résultats obtenus, il faut garder en mémoire les facteurs suivants. Premièrement, plutôt que de simuler les communications par logiciel, les mesures ont été effectuées utilisant un banc de test qui génère des signaux cellulaires selon les normes utilisées par l'industrie. Cette méthode permet d'effectuer des tests sur des signaux se propageant à des fréquences élevées similaires à des communications réelles. Simuler des signaux à ces fréquences entraîne plusieurs complications. Ainsi, notre banc de tests nous permet d'être plus proches de la réalité qu'avec une simulation. Finalement, bien que les résultats des méthodes de brouillage par traitement de signal rapide semblent peu impressionnants, il est important de comprendre que leur plus grand avantage est la capacité de couvrir une très grande plage de fréquence sans gaspillage d'énergie. Couvrir une plage de plusieurs mégahertz avec les méthodes classiques requiert une dépense d'énergie immense et constante. Les résultats utilisés pour l'analyse supposent que le brouilleur connaît exactement où est situé le signal ciblé, ce qui n'est pas toujours le cas dans une situation réelle. Pour les méthodes avancées, l'utilisation d'un DRFM nous permet d'utiliser la puissance de l'émetteur uniquement en présence de signal et toujours au bon endroit.

CONCLUSION

Le but premier de ce mémoire était de tester de nouvelles méthodes de brouillage utilisant un traitement de signaux rapide. Pour ce faire, une série de tests ont été effectués au moyen d'une radio capable de mémorisation RF ou DRFM sur des signaux utilisant les standards de communication cellulaire WiMAX, GSM-EDGE et W-CDMA. Ces standards ont été choisis pour représenter différents types de modulation : le WiMAX utilise une modulation OFDM, le GSM-EDGE une modulation simple porteuse et le W-CDMA de l'étalement spectral par séquence directe.

Les deux méthodes de brouillage avancées utilisées consistent à répéter le signal de base avec une variation aléatoire créée par traitement de signaux. Les deux traitements effectués pour les tests sont la variation de délai aléatoire et la variation d'amplitude aléatoire. Une série de tests utilisant des brouillages classiques ont été effectués avec le même banc de test pour comparer les résultats.

À la suite de nos tests, on peut observer que le brouillage par variation de délai aléatoire est la nouvelle méthode la plus efficace pour brouiller une communication. Le brouillage par variation d'amplitude est contraint par la distribution normale et discrète de notre générateur de nombres aléatoires, ce qui limite son efficacité. Le brouillage par variation de délai n'a pas ce problème, à cause de la nature du traitement effectué. Il est possible que les résultats des tests de brouillage par variation d'amplitude soient pondérés à la baisse. La mesure de puissance du signal de brouillage est difficile à prendre avec le traitement, car la puissance varie rapidement avec l'amplitude. Donc, la mesure est prise avant l'application du traitement de signal et si une partie de la puissance se retrouve hors de la bande de fréquences du signal de base, elle n'en tient pas compte, comme c'est le cas pour la variation d'amplitude rapide.

Si la fréquence d'opération de l'émetteur est connue, la comparaison des résultats avec ceux des méthodes classiques montre que les techniques de brouillage avec traitement de signaux rapide n'apportent pas d'augmentation de performance majeure. À des puissances similaires sur la bande passante du signal de base, le bruit blanc est toujours la meilleure méthode pour nuire à la communication.

À la suite de l'analyse des résultats, nous savons maintenant que le brouillage avancé par variation aléatoire de délai offre des performances similaires aux techniques classiques. Donc, il est possible de remplacer les brouilleurs classiques par un brouilleur avancé, et ainsi obtenir les avantages du traitement de signal rapide sans sacrifier l'efficacité du brouillage.

Les techniques de brouillage par traitement de signal rapide ont plusieurs avantages marquants par rapport aux techniques classiques. L'utilisation de la mémorisation RF leur permet de couvrir une grande largeur de bande fréquentielle et d'utiliser la puissance de l'émetteur de manière économe. La puissance disponible à l'émetteur est utilisée uniquement sur la bande de fréquences du signal ciblé et seulement lorsque celui-ci est actif. Il s'agit d'une très grande économie lorsque comparée aux méthodes de brouillage classique, où une grande partie de la puissance est gaspillée. De plus, elles ouvrent la possibilité de contrôler le brouillage sur les signaux. Les variations aléatoires pourraient ainsi être remplacées par un code pseudo-aléatoire pour créer une clé de brouillage permettant de reconstruire le signal à la réception afin pour créer une méthode d'attaque ECM.

Les méthodes de brouillage par traitement de signaux rapide offrent plusieurs possibilités de développement pour répondre aux problématiques émergentes d'un monde où les communications sans fil sont une réalité quotidienne touchant tous les aspects de la vie.

RECOMMANDATIONS

Les tests des différentes techniques de brouillage ont montré que le W-CDMA offre une protection supérieure aux autres standards testés. Ce résultat est peu surprenant, car le CDMA a été conçu pour la communication militaire et la robustesse du signal reste accrue même devant les techniques avancées. Une étude supplémentaire utilisant un récepteur RAKE et les brouillages avancés serait pertinente afin de déterminer la vitesse requise pour déjouer un tel récepteur et de mesurer l'impact sur la démodulation du signal.

Tous les tests réalisés en vue de la rédaction de ce mémoire utilisent une seule antenne pour la communication de base. Cependant, les systèmes de communications plus récents utilisent plusieurs antennes pour offrir une diversité spatiale au signal (Proakis, 2008). Ces systèmes appelés MIMO (Multiple Input Multiple Output) ont la possibilité de modifier les paramètres du canal de propagation et pourraient offrir une protection supplémentaire contre la présence d'un brouilleur. Des tests utilisant des systèmes MIMO seraient la suite logique des travaux présentés dans ce mémoire.

ANNEXE I

DRFM LaCIME

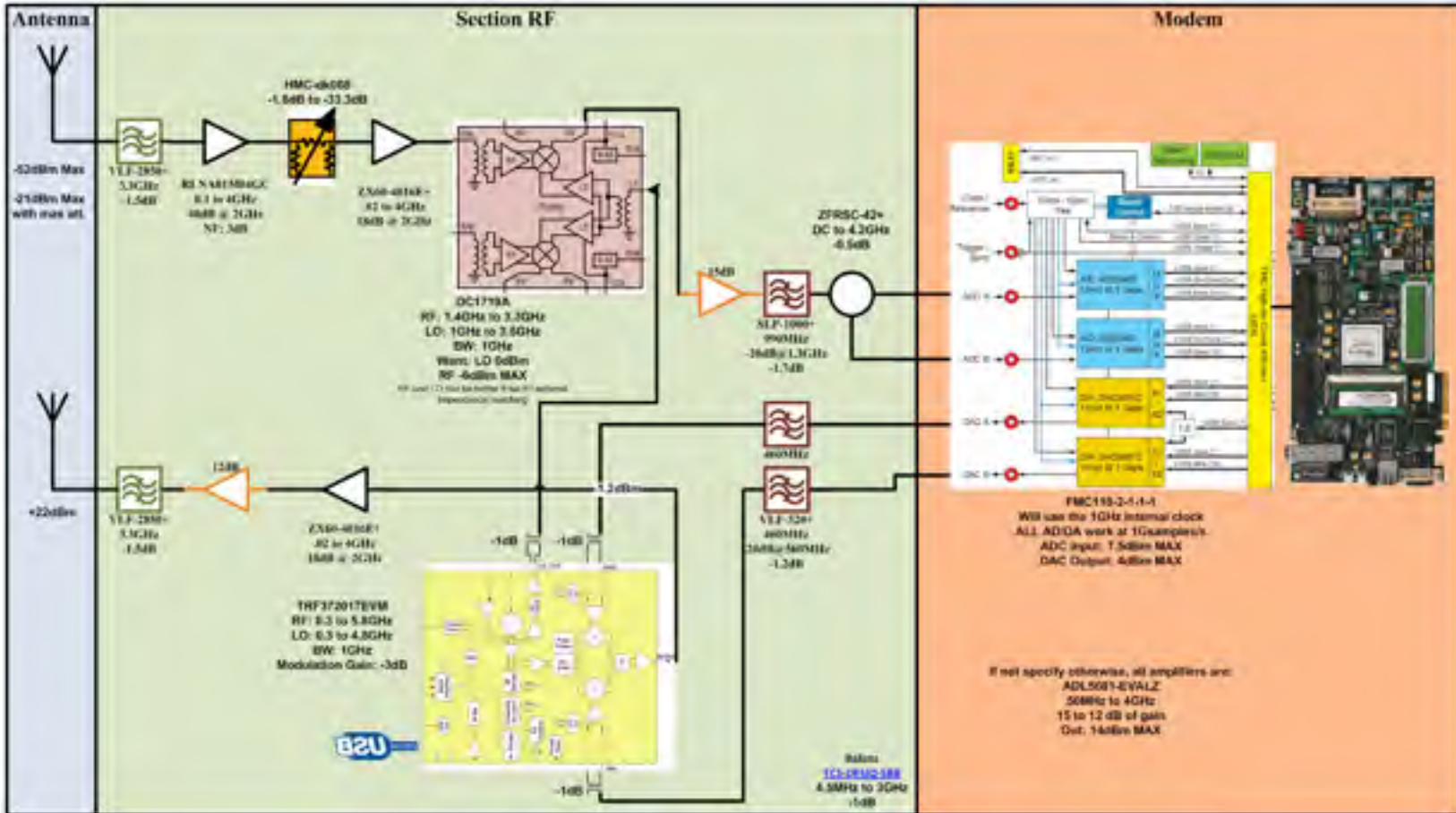


Figure-A I-1 Diagramme fonctionnel de la radio DRFM
Tiré de Lacime (2013)

Tableau-A I-1 Matériel

Description	Part number	Manuf.
Amplifier .01 to 4GHz 15dB	ADL5601-EVALZ	Analog Devices
Amplifier .02 to 4GHz 17dB	ZX60-4016B1	Mini circuits
Cable, SSMC-plug	SCA30315-05	Fairview Microwave Inc.
ADC-DAC Daughterboard	FMC110-2-1-1-1	HDSP
Attenuator	117217-HIMCG24IP4	Hittite
USB kit for attenuator	HIMC-dk008	Hittite
Downconverting Mixer	UC1719A	Linear Technology
Low Pass Filter 990MHz	SPL-1000+	Mini-circuits
Low Pass Filter 460MHz	VLF-3201	Mini-circuits
Low Pass Filter 3.3GHz	VLF-2850+	Mini-circuits
Splitter	2FBSL-421	Mini-circuits
Cable, DC-18GHz	DRG-35M+	Mini-circuits
Balun 4.5MHz to 3GHz	TC1-DESIQ-SBB	National Semi.
INA 0.1 to 4GHz 38dB	BIN401M04CC	RF-lambda
Modulator and LO gen.	TRF372017EVM	TI
FPGA evalBoard	ML605	Xilinx

```

C:\Windows\system32\cmd.exe - fmc110app.exe 1 ml605 1 0

AddrSipFmc110 : 9220

##### CLI #####
1 - Generate a waveform
2 - Enabled looping the data from ADC to DAC
3 - Generate a random delay on DAC 1
4 - Generate a random delay on DAC 2
5 - Generate a random attenuation on DAC 1
6 - Generate a random attenuation on DAC 2
7 - Generate a spot jamming
8 - Generate a sweep jamming
9 - Generate a chirp
10 - Generate a white noise
11 - Add a multi-path
12 - Add a static delay at the input of one ADC
13 - Decrease per two the strength of the jamming
14 - Delete a jamming
15 - Debug - View RAM Content
16 - Exit
CLI>

```

Figure-A I-2 Interface de contrôle

ANNEXE II

R&S WINIQSIM2

Les signaux WiMAX et W-CDMA sont générés à partir du logiciel WINIQSIM2, figure AII-1. Ce logiciel crée un fichier WAV du signal désiré pouvant être généré par le SMU200A. Les signaux WiMAX sont générés utilisant l'interface de la figure AII-2. Le logiciel permet de configurer la trame du signal et de choisir la largeur de la bande passante, le temps de garde, le nombre de porteuses actives avec leurs modulations et le nombre de rafales. La création d'un signal W-CDMA est réalisée en utilisant les interfaces de la figure AII-3.

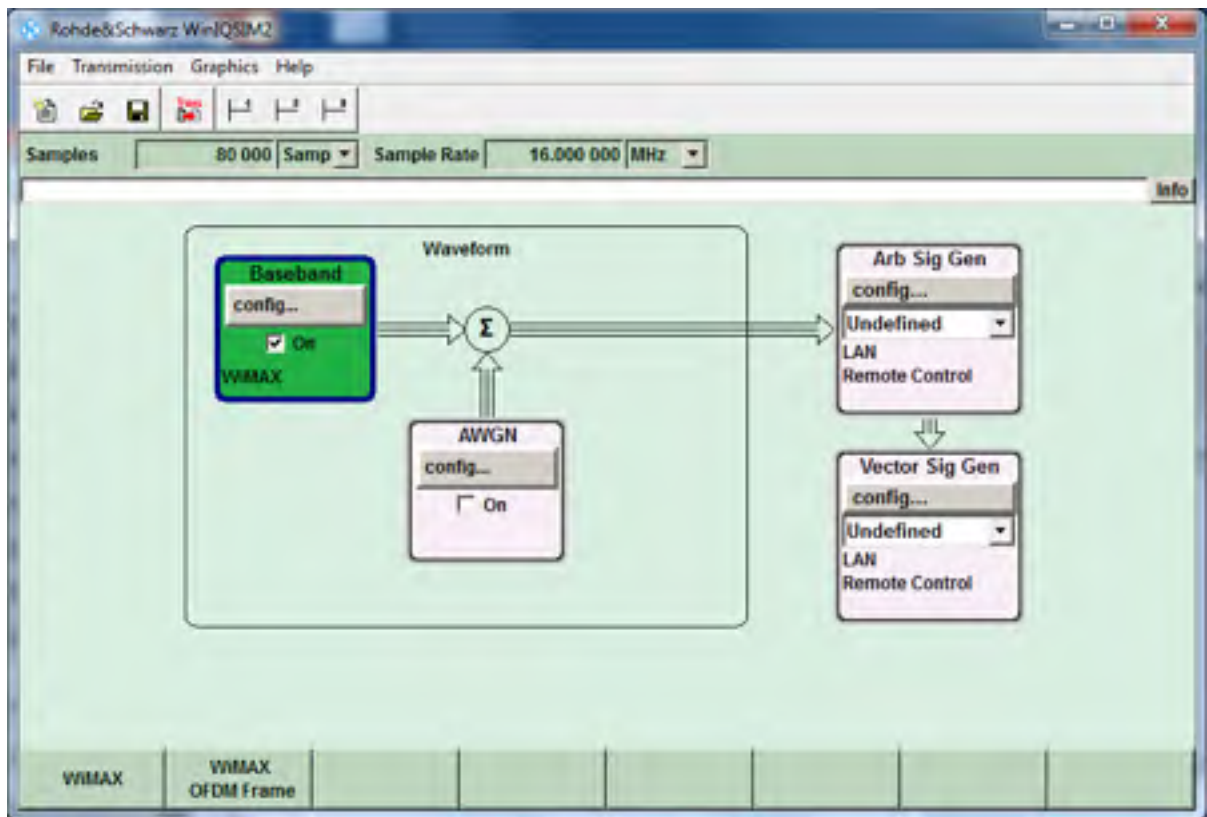


Figure-A II-1 Interface de contrôle WINIQSIM2



Figure-A II-2 Interface pour signaux WiMAX

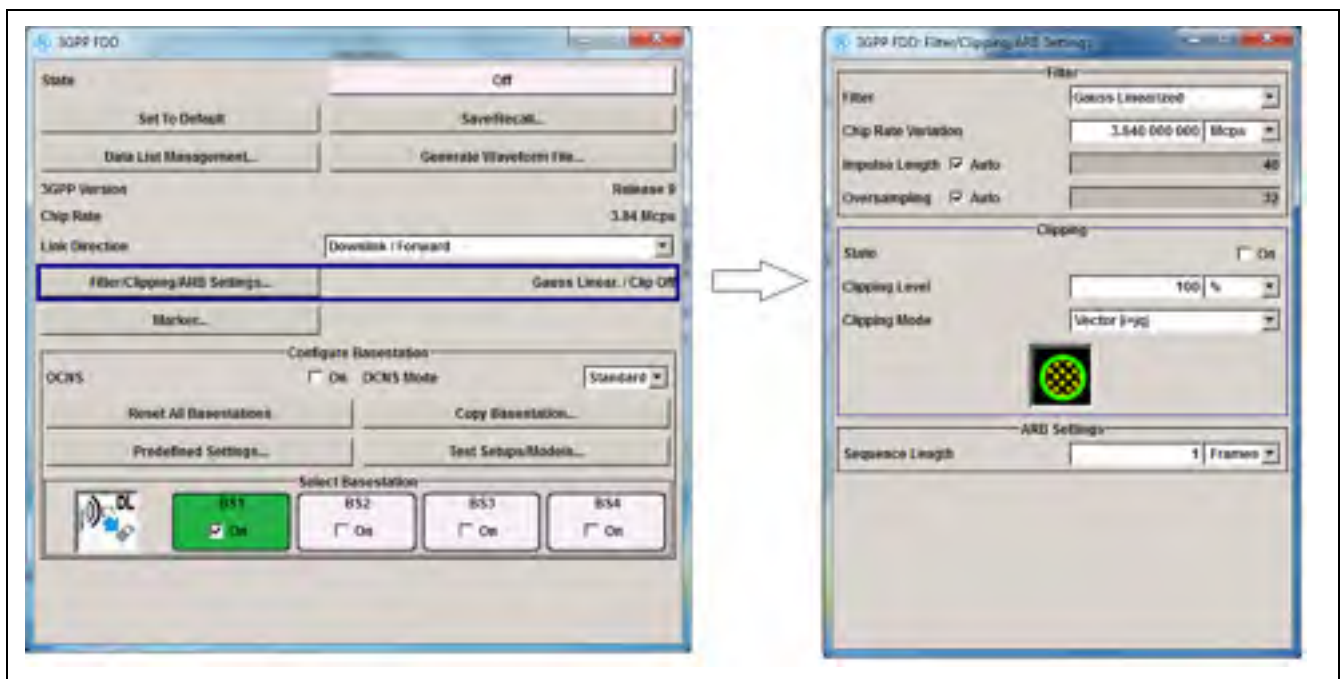


Figure-A II-3 Interface pour signaux 3GPP

ANNEXE III

Équipement R&S

SMU200A (R&S, 2012)

Frequency

Frequency range	under-range	100 kHz to < 300 kHz
	R&S [®] SMU-B102, R&S [®] SMU-B202	up to 2.2 GHz
	R&S [®] SMU-B103, R&S [®] SMU-B203	up to 3 GHz
	R&S [®] SMU-B104	up to 4 GHz
	R&S [®] SMU-B106	up to 6 GHz
Resolution of setting		0.01 Hz
Resolution of synthesis	standard, fundamental frequency range = 750 MHz to 1500 MHz	5 µHz
	with R&S [®] SMU-B22 option	0.2 µHz
Setting time ¹	to within $< 1 \times 10^{-3}$ for $f > 200$ MHz or < 124 Hz for $f < 200$ MHz, with GUI update stopped, after IEEE bus delimiter	< 2 ms, 1.5 ms (typ.)
	ALC state: off (sample & hold)	< 4 ms, 2.5 ms (typ.)
	after trigger pulse in list mode	< 450 µs, 300 µs (typ.) adjustable in 0.1° steps
Phase offset		

Level

Setting range	standard with R&S [®] SMU-B31 or R&S [®] SMU-B36 option	-145 dBm to +20 dBm to +30 dBm
Maximum level	standard	
	$f \leq 3$ GHz	+13 dBm (PEP) ²
	$f > 3$ GHz	+11 dBm (PEP)
	with R&S [®] SMU-B31 or R&S [®] SMU-B36 option	
	$f \leq 3$ GHz	+19 dBm (PEP)
Resolution	$f > 3$ GHz	+17 dBm (PEP)
		0.01 dB
Level uncertainty	for levels > -120 dBm, attenuator mode: auto, temperature range = +15 °C to +28 °C	
	1 MHz $\leq f \leq 3$ GHz	< 0.5 dB
	$f > 3$ GHz	< 0.9 dB
Additional uncertainty with ALC state: off (sample & hold)	This function is needed only for some special applications	< 0.2 dB
Output impedance	standard, ALC state: on	
VSWR in 50 Ω system	$f \leq 3$ GHz	< 1.6, < 1.4 (typ.)
	$f > 3$ GHz	< 1.85, < 1.6 (typ.)
	with R&S [®] SMU-B31 or R&S [®] SMU-B36 option, ALC state: on	
	attenuator mode: normal	
	$f \leq 3$ GHz	< 1.65, < 1.45 (typ.)
	$f > 3$ GHz	< 1.9, < 1.65 (typ.)
	attenuator mode: high power	
	$f \leq 3$ GHz	< 1.7, < 1.5 (typ.)
	$f > 3$ GHz	< 1.9, < 1.65 (typ.)
Setting time ¹	after IEEE bus delimiter, to < 0.1 dB deviation from final value, with GUI update stopped, temperature range = +15 °C to +28 °C	
	ALC state: on	< 2 ms, 1.5 ms (typ.)
	ALC state: off	< 4 ms, 2.5 ms (typ.)
	in list mode after trigger impulse to 0.3 dB deviation from final value	< 450 µs, 300 µs (typ.)
	range switchover with R&S [®] SMU-B31 or R&S [®] SMU-B36 option	< 10 ms
Uninterrupted level setting	attenuator mode: fixed, ALC state: on	
Back-feed (from ≥ 50 Ω source)	setting range	> 20 dB
	maximum permissible RF power in output frequency range for $f > 1$ MHz	
	1 MHz $\leq f \leq 3$ GHz	50 W
	$f > 3$ GHz	10 W
	maximum permissible DC voltage	50 V

FSQ40 (R&S, 2011)

Frequency

Frequency range	R&S®FSQ3	DC coupled	20 Hz to 3.6 GHz
		AC coupled	1 MHz to 3.6 GHz
	R&S®FSQ8	DC coupled	20 Hz to 8 GHz
		AC coupled	1 MHz to 8 GHz
	R&S®FSQ25	DC coupled	20 Hz to 26.5 GHz
Frequency resolution		AC coupled	10 MHz to 26.5 GHz
	R&S®FSQ40	DC coupled	20 Hz to 40 GHz
			0.01 Hz

Reference frequency, internal, nominal	standard OCXO	
Aging per day	after 30 days of continuous operation	1×10^{-8}
Aging per year	after 30 days of continuous operation	1×10^{-7}
Temperature drift	+5 °C to +45 °C	8×10^{-8}
Total error	per year	1.8×10^{-7}
Reference frequency, internal, nominal	R&S®FSQ40 option	
Aging per day	after 30 days of continuous operation	2×10^{-8}
Aging per year	after 30 days of continuous operation	2×10^{-7}
Temperature drift	+5 °C to +45 °C	1×10^{-8}
Total error	per year	5×10^{-8}
External reference frequency	1 MHz to 20 MHz, 1 Hz steps	

Frequency display	with marker or frequency counter	
Marker resolution	1 Hz	
Uncertainty	$\pm(\text{marker frequency} \times \text{reference uncertainty} + 10\% \times \text{resolution bandwidth} + 7 \times \text{span}/(\text{swEEP points} - 1)) \pm 1 \text{ Hz}$	
Marker tuning frequency stepsize	default	span/swEEP points - 1
	marker stepsize = sweep points	span/swEEP points - 1
Frequency counter resolution	selectable	0.1 Hz to 10 MHz
Count accuracy	SN = 25 dB	$\pm(\text{frequency} \times \text{reference error} + 1\% \text{ (best sigE)})$
Display range for frequency axis	0 Hz, 10 Hz to max. frequency	
Resolution	0.1 Hz	
Max. span deviation	1 %	

Spectral purity, SSB phase noise (1 Hz)	f = 640 MHz	
Internal FM	HPBW 10 kHz, RMS	< 1 Hz, nominal
Carrier offset	10 Hz	< -73 dBc, nominal
	10 Hz with option R&S®FSQ40 filter	< -80 dBc, nominal
	100 Hz	< -88 dBc, typ. -104 dBc
	1 kHz	< -116 dBc, typ. -124 dBc
	10 kHz	< -126 dBc, typ. -133 dBc
	100 kHz	< -128 dBc, typ. -133 dBc
	1 MHz	< -140 dBc, typ. -148 dBc
	10 MHz	typ. -160 dBc

Level

Display range	displayed noise floor to +30 dBm	
Maximum input level		
DC voltage	RF input AC coupled	50 V
	RF input DC coupled	0 V
CW RF power	RF attenuation 0 dB	20 dBm (± 0.1 dB)
	RF attenuation ≥ 10 dB	30 dBm (± 1 dB)
Pulse spectral density	97 dBuV/MHz	
Max. pulse voltage	RF attenuation ≥ 10 dB	150 V
Max. pulse energy	RF attenuation ≥ 10 dB, 10 μ s	1 mJ
Intermodulation		
1 dB compression of input mixer	0 dB RF attenuation	± 1.5 dBm, nominal
	≤ 3.6 GHz	± 1.5 dBm, nominal
	≥ 3.6 GHz	± 1.5 dBm, nominal
	R&S®FSQ8	± 10 dBm, nominal
	R&S®FSQ25, R&S®FSQ40	± 7 dBm, nominal
Third-order intercept point (TOI)	level 2 = -10 dBm, $\Delta f = 5 \times \text{BW}$ or 10 kHz, whichever is larger	
	R&S®FSQ3	
	10 MHz $\leq f_c \leq 300$ MHz	≥ 17 dBm, typ. 20 dBm
	300 MHz $\leq f_c \leq 3.6$ GHz	≥ 19 dBm, typ. 25 dBm
	R&S®FSQ8	
	10 MHz $\leq f_c \leq 300$ MHz	≥ 17 dBm, typ. 20 dBm
	300 MHz $\leq f_c \leq 3.6$ GHz	≥ 20 dBm, typ. 25 dBm
	3.6 GHz $\leq f_c \leq 8$ GHz	≥ 19 dBm, typ. 23 dBm
	R&S®FSQ25	
	10 MHz $\leq f_c \leq 300$ MHz	≥ 17 dBm, typ. 20 dBm
	300 MHz $\leq f_c \leq 3.6$ GHz	≥ 22 dBm, typ. 27 dBm
	3.6 GHz $\leq f_c \leq 26.5$ GHz	≥ 12 dBm, typ. 15 dBm
	R&S®FSQ40	
	10 MHz $\leq f_c \leq 300$ MHz	≥ 17 dBm, typ. 20 dBm
	300 MHz $\leq f_c \leq 3.6$ GHz	≥ 20 dBm, typ. 25 dBm
	3.6 GHz $\leq f_c \leq 40$ GHz	≥ 12 dBm, typ. 15 dBm
Second harmonic intercept (SHI)	$f_c \leq 100$ MHz	≥ 35 dBm
	100 MHz $\leq f_c \leq 400$ MHz	≥ 41 dBm, typ. 55 dBm
	400 MHz $\leq f_c \leq 500$ MHz	≥ 42 dBm, typ. 60 dBm
	500 MHz $\leq f_c \leq 1$ GHz	≥ 45 dBm, typ. 50 dBm
	1 GHz $\leq f_c \leq 1.8$ GHz	≥ 35 dBm
	$f_c > 1.8$ GHz	≥ 40 dBm, nominal

ANNEXE IV

Registres DRFM

Présentation des variables utilisées pour le contrôle des brouillages avec traitement de signaux rapide et de leurs limites respectives (Lacime, 2013):

Register name: Custom – Address: 0x001, Default = 0x0F00 -> I
Custom – Address: 0x002, Default = 0x0F00 -> Q

Bit nr.	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Name	Enable	N.D.	N.D.	Inv. Sign		nb Samples		
Bit nr.	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8
Name	Delay length							

Enable: Enabled the delay of both data line.

nb Samples: Define the number of samples between 2 delay changes. This number is between 2^0 and 2^{15} .

Delay Length: The length of the delay in itself is random and of length between 0 and $2^{\text{Delay Length}}$ data samples. (0 and 2 usec) Max value should be 1F

Inv. Sign: Inverse the sign of the signal. (apply complement 2)

Register name: Custom – Address: 0x003, Default = 0x0F00 -> I
 Custom – Address: 0x004, Default = 0x0F00 -> Q

Bit nr.	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Name	Enable	N.D.	N.D.	N.D.		nb Samples		
Bit nr.	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8
Name	Amplitude Ctrl							

Enable: Enable the amplitude modulation.

nb Samples: Define the number of samples between 2 delay changes. This number is between 2^0 and 2^{15} .

Amplitude Ctrl: The maximum modification of the amplitude of the signal. The incoming signal is multiply with `s_random_short` after each *nb Samples*.

with **amplitude_ctrl** select

```
s_random_short <= "111111111111" when x"0",
                  "111111111111" & s_random(31) when x"1",
                  "1111111111" & s_random(31 downto 30) when x"2",
                  "111111111" & s_random(31 downto 29) when x"3",
                  "11111111" & s_random(31 downto 28) when x"4",
                  "1111111" & s_random(31 downto 27) when x"5",
                  "111111" & s_random(31 downto 26) when x"6",
                  "11111" & s_random(31 downto 25) when x"7",
                  "1111" & s_random(31 downto 24) when x"8",
                  "111" & s_random(31 downto 23) when x"9",
                  "11" & s_random(31 downto 22) when x"A",
                  "1" & s_random(31 downto 21) when x"B",
                  s_random(31 downto 20) when OTHERS;
```

LISTE DE RÉFÉRENCES BIBLIOGRAPHIQUES

- 3GPP.org. 2013. « Overview of 3GPP release 13 V0.0.3(2013-09) ». En ligne. 35 p.
http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/ .
Consulté le 15 janvier 2014.
- Bonn, F., Association des universités partiellement ou entièrement de langue française, Uref
et Agence universitaire de la francophonie. 1992. *Précis de télédétection*. Sillery,
Québec: Presses de l'Université du Québec, 4 v. p.
- Blust, Stephen M. 2012 « IMT-Advanced standards for mobile broadband communications ». *ITU News*. En ligne. No. 1, Janvier 2012 <<https://itunews.itu.int/En/2068-IMT-Advanced-standards-for-mobile-broadbandcommunications.note.aspx>>. Consulté 14 janvier 2014.
- Fith, Olivier. 2006 « OFDM transmitter ideal ». En ligne sous GNU Free Documentation License. http://en.wikipedia.org/wiki/File:OFDM_transmitter_ideal.png. Consulté le 20 décembre 2013.
- Furuskar, A., S. Mazur, F. Muller et H. Olofsson. 1999. « EDGE: enhanced data rates for GSM and TDMA/136 evolution ». *Personal Communications, IEEE*, vol. 6, n° 3, p. 56-66.
- Heiskala, Juha, et Ph.D. John Terry. 2001. *OFDM Wireless LANs: A Theoretical and Practical Guide*. Sams, 315 p.
- International Telecommunication Union. 2002. «IMT-2000 Project : What is IMT-2000 ». En ligne. 8 p. http://www.itu.int/osg/imt-project/docs/What_is_IMT2000-2.pdf. Consulté le 14 janvier 2014.
- International Telecommunication Union. 2011. *Collection of the Basic Texts of the International Telecommunication Union: Adopted by the Plenipotentiary Conference*, International Telecommunication Union, Plenipotentiary Conference. [Geneva]: ITU, 681 p.
- International Telecommunication Union. 2012. «Recommendation ITU-R M.2012 : Detail specifications of the terrestrial radio interfaces on International Mobile Telecommunications Advanced (IMT-Advanced) ». En ligne. 113 p.
http://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2012-0-201201-I!!PDF-E.pdf.
Consulté le 15 janvier 2014.
- LaCIME, et Yannick Vallée. 2013. «Generic and fast platform to sample and generate signals ». Document interne LaCIME. 28 p.

- MathWorksInc. 2009. Matlab & simulink : student version, Release 2009a. Natick, Mass.: MathWorks, Inc., v. p.
- Matsumoto, Makoto, et Takuji Nishimura. 1998. « Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator ». *ACM Trans. Model. Comput. Simul.*, vol. 8, n° 1, p. 3-30.
- Papoulis, Athanasios. 2002. *Probability, random variables, and stochastic processes*, 4th ed.. Boston: McGraw-Hill, 852 p.
- Proakis, John G. 2008. *Digital communications*, 5th ed.. Boston: McGraw-Hill, xviii, 1150 p.
- Robertson, Paul et Wireless MSU. « Wireless Technology Seminar:EDGE/GPRS Basics ». En ligne. 34 p. http://www.agilent.com/cm/wireless/pdf/EDGEGPRS_12-00.pdf, Consulté le 14 janvier 2014.
- Rohde & Schwarz. 2011. « R&S®FSQ Signal Analyzer Specifications ». En ligne. 32 p. http://cdn.rohde-schwarz.com/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/FSQ_dat-sw_en.pdf . Consulté le 15 janvier 2014.
- Rohde & Schwarz. 2011. « R&S®SMU200A Vector Signal Generator Operating Manual ». En ligne. 903 p. http://cdn.rohde-schwarz.com/dl_downloads/dl_common_library/dl_manuals/gb_1/smu200a_1/RS_SMU200A_Operating.pdf . Consulté le 15 janvier 2014.
- Rohde & Schwarz. 2011. « R&S®SMU200A Vector Signal Generator Specifications ». En ligne. 48p http://cdn.rohde-schwarz.com/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/SMU_dat-sw-en.pdf. Consulté le 15 janvier 2014.
- Rohde & Schwarz. 2006. « WiMAX General information about the standard 802.16 ». En ligne. 34p. http://cdn.rohde-schwarz.com/dl_downloads/dl_application/application_notes/1ma96/1MA96_0E_WiMAX.pdf . Consulté le 20 décembre 2013.
- Roome, S. J. 1990. « Digital radio frequency memory ». *Electronics & Communication Engineering Journal*, vol. 2, n° 4, p. 147-153.
- Roth, R.M. 2006. *Introduction to Coding Theory*. Cambridge University Press, 566 p.
- Rüdiger, Leo Urbanke., Thomas J. Richardson et Books x Inc. 2008. *Modern coding theory*. Cambridge, New York: Cambridge University Press.

- Schmogrow, R., B. Nebendahl, M. Winter, A. Josten, D. Hillerkuss, S. Koenig, J. Meyer, M. Dreschmann, M. Huebner, C. Koos, J. Becker, W. Freude et J. Leuthold. 2012. « Error Vector Magnitude as a Performance Measure for Advanced Modulation Formats ». *Photonics Technology Letters, IEEE*, vol. 24, n° 1, p. 61-63.
- Sen, Cem. 2000. *Digital Communications Jamming*. Mémoire de maîtrise en génie électrique. Monterey CA: Naval Postgraduate School.
- Shafik, R. A., S. Rahman et R. Islam. 2006. « On the Extended Relationships Among EVM, BER and SNR as Performance Metrics ». In *Electrical and Computer Engineering, 2006. ICECE '06. International Conference on*. (19-21 Dec. 2006), p. 408-411.
- Spezio, A. E. 2002. « Electronic warfare systems ». *IEEE Transactions on Microwave Theory and Techniques*, vol. 50, n° 3, p. 633-644.
- Stremmler, Ferrel G. 1990. *Introduction to communication systems*, 3rd ed. Coll. « Communication systems ». Reading, Mass. Don Mills, Ont.: Addison-Wesley, xix, 757 p.
- Van Trees, Harry L. 2001. *Detection, estimation, and modulation theory*. Coll. « Optimum array processing ». New York: Wiley., v. 653 p.
- Working Group on Broadband Wireless Access Standards. 2009. Advance Air Interface with data rates of 100 Mbits/s mobile and 1Gbits/s fixed. IEEE 802 LAN/MAN Standards Committee, IEEE 802.16. New York (NY) : Institute of electrical and Electronics Engineers, Inc , 2004 p.