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. Ing.

PAR
Marwen BOUANEN

UN SYSTÈME DE COMMUNICATION OFDM À FAIBLE PROBABILITÉ D'INTERCEPTION

MONTRÉAL, LE 11 JUILLET 2013

PRÉSENTATION DU JURY

CE MÉMOIRE A ÉTÉ ÉVALUÉ

PAR UN JURY COMPOSÉ DE :

M. Claude Thibeault, directeur de mémoire
Département de génie électrique à l'École de technologie supérieure

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

M. Naim Batani, président du jury
Département de génie électrique à l'École de technologie supérieure

M. Jean-Marc Lina, membre du jury
Département de génie électrique à l'École de technologie supérieure

IL A FAIT L'OBJET D'UNE SOUTENANCE DEVANT JURY

LE 21 MAI 2013

À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

REMERCIEMENTS

Je tiens à remercier vivement mes professeurs Claude Thibeault et François Gagnon pour leur aide tout au long de cette maîtrise.

UN SYSTÈME DE COMMUNICATION OFDM À FAIBLE PROBABILITÉ D'INTERCEPTION

Marwen BOUANEN

RÉSUMÉ

Les systèmes OFDM traditionnels présentent des propriétés cyclostationnaires qui peuvent être exploitées afin d'intercepter le signal sans fil transmis. Cependant, une telle possibilité est inacceptable dans les applications militaires où la sécurité est d'une importance extrême. Le préfixe cyclique est le paramètre OFDM le plus important qui génère des caractéristiques cyclostationnaires. Dans le but d'empêcher l'exploitation de ces caractéristiques, nous proposons une combinaison innovatrice de deux techniques qui permettent de réduire considérablement la cyclostationnarité et les propriétés spectrales de la forme d'onde OFDM, tout en conservant les avantages du préfixe cyclique. La taille du préfixe cyclique est variée pseudo-aléatoirement dans chaque symbole OFDM de sorte que les caractéristiques cyclostationnaires soient atténuées. Par ailleurs, une gigue de fréquence pseudo-aléatoire est introduite à la fréquence porteuse afin de masquer les raies spectrales correspondantes aux fréquences des sous-porteuses. Le système conçu génère ainsi une forme d'onde à faible probabilité d'interception. De plus, de bonnes performances sur les canaux à trajets multiples de type Rayleigh sont démontrées. Enfin, une preuve de concept d'un émetteur GNU Radio implémentant un préfixe cyclique de taille pseudo-aléatoire est exposée.

Mots-clés: OFDM, Cyclostationnarité, Raies spectrales, Faible probabilité d'interception.

AN LPI DESIGN FOR SECURE OFDM SYSTEMS

Marwen BOUANEN

ABSTRACT

Traditional OFDM systems present some embedded features that may be exploited in order to intercept the wireless transmitted signal. However, such a possibility is not accepted in military applications where security is a very important issue. Cyclic prefix is one of the most obvious OFDM parameters that induce cyclostationarity features. Aiming to suppress these features, some classical solutions in literature propose to entirely remove the cyclic extension so that additional processing is needed to eliminate the inter-symbol interference. In this work, we propose an innovative combination of two techniques that allow to considerably reduce cyclostationary and spectral features of the OFDM waveform, while maintaining the cyclic prefix advantages. The cyclic-prefix size in each OFDM symbol is varied pseudo-randomly so that cyclostationary features are mitigated. Moreover, a pseudo-random frequency jitter is introduced to the carrier frequency in order to mask subcarrier spectral lines. Once these techniques are applied, the designed system is said to generate a low-probability-of-intercept waveform (LPI).Performance in multipath channels is investigated and shown to be effective. Finally, the feasibility of a GNU Radio transmitter that implements a pseudo-random cyclic prefix is presented.

Keywords: OFDM, Cyclostationarity, Spectral lines, Low probability of interception.

TABLE DES MATIÈRES

Page

INTRODUCTION 1

CHAPITRE 1 Technologie OFDM 3
1.1 Principe de l'OFDM 3
1.1.1 Modulation multi-porteuses 3
1.1.2 Modulation OFDM 5
1.1.3 Préfixe cyclique 6
1.1.4 Modèle en bande de base du système OFDM 6
1.2 Estimation du canal pour les systèmes OFDM 8
1.3 Techniques de synchronisation aveugle pour les systèmes OFDM 10
1.3.1 Algorithmes de synchronisation à base du préfixe cyclique 11
1.3.2 Algorithmes de synchronisation utilisant la cyclostationnarité 12
1.4 Conclusion 14

CHAPITRE 2 Communications OFDM à faible probabilité d'interception 15
2.1 Introduction 15
2.2 Cyclostationnarité des systèmes OFDM 15
2.3 Méthodes de détection de la cyclostationnarité 18
2.3.1 Fonction d'Autocorrélation Cyclique (FAC) 18
2.3.2 Fonction de Densité Spectrale Cyclique (DSC) 20
2.3.3 Densité spectrale de puissance de la transformée au carré du signal 21
2.4 Revue de la littérature des méthodes de suppression de la cyclostationnarité pour les systèmes OFDM 22
2.4.1 Méthodes classiques de suppression de la cyclostationnarité 22
2.4.2 Revue de la littérature des méthodes à insertion d'aléa 23
2.4.3 Effet de l'évanouissement du canal sur l'insertion d'aléa au préfixe cyclique 23
2.5 Conclusion 25

CHAPITRE 3 Système OFDM à faible probabilité d'interception 26
3.1 Introduction 26
3.2 Suppression des caractéristiques cyclostationnaires de l'onde OFDM 26
3.2.1 Préfixe cyclique de taille pseudo-aléatoire 26
3.2.2 Gigue fréquentielle pseudo-aléatoire 30
3.2.3 Analyse des performances sur les canaux sélectifs en fréquence 32
3.3 Résultats de simulation 34
3.3.1 Suppression des propriétés cyclique et spectrale 35
3.3.2 Taux d'erreur binaire 38
3.4 Conclusion 39

CHAPITRE 4 Analyse spectrale de l'onde OFDM à préfixe cyclique aléatoire 40
4.1 Introduction 40
4.2 Moments de second ordre des signaux QAM et PSK à durée d'impulsion aléatoire 41
4.3 Moments de second ordre des signaux OFDM à préfixe cyclique aléatoire.....48
4.4 Validation des expressions de FMSO et DSP des signaux OFDM à préfixe cyclique aléatoire.....51
4.4.1 Validation des expressions de DSP..... 53
4.4.2 Validation des expressions de FMSO 54
4.5 Conclusion.....54

CHAPITRE 5 Implémentation d'un émetteur OFDM à préfixe cyclique aléatoire.....55
5.1 Introduction 55
5.2 Radio logicielle SDR.....55
5.2.1 Principe de la SDR..... 55
5.2.2 Revue de la littérature des projets SDR 57
5.3 Plateforme de développement 58
5.3.1 Plateforme GNU Radio..... 58
5.3.2 Périphérique USRP N210 59
5.3.3 Interface graphique GNU radio 61
5.4 Stratégie d'implémentation 62
5.5 Mesure de performances 65
5.5.1 Scénario de test 65
5.5.2 Analyse de cyclostationnarité 67
5.6 Conclusion.....70

CONCLUSION.....71

RECOMMANDATIONS 73

ANNEXE I Démonstration mathématique (1) 74

ANNEXE II Démonstration mathématique (2) 75

BIBLIOGRAPHIE.....77

LISTE DES FIGURES

Page

Figure 1.1 Division du spectre disponible en N sous-bandes 3

Figure 1.2 Orthogonalité des porteuses dans un système OFDM 4

Figure 1.3 Préfixe cyclique 6

Figure 1.4 Schéma d'un système de communication OFDM en bande de base 7

Figure 1.5 Schéma équivalent d'un système OFDM 8

Figure 1.6 Deux méthodes d'arrangement des sous-porteuses pilotes (cercles noirs) pour estimation du canal dans les systèmes OFDM 9

Figure 1.7 Scénario d'erreur de synchronisation temporelle 10

Figure 1.8 Synchronisation aveugle en utilisant le préfixe cyclique 11

Figure 1.9 Métrique de synchronisation de l'algorithme MV obtenu en utilisant le préfix cyclique 12

Figure 1.10 Fonction d'Autocorrélation Cyclique (FAC) d'une forme d'onde OFDM sur la base du système 802.11a 13

Figure 1.11 Densité Spectrale Cyclique (DSC) d'une forme d'onde OFDM sur la base du système 802.11a 13

Figure 2.1 Implémentation de la DSC 21

Figure 2.2 Densité spectrale de puissance de la transformée au carré du signal 21

Figure 2.3 Insertion de signaux aléatoires en tant que préfixes cycliques 22

Figure 2.4 Réponse impulsionnelle discrète d'un canal invariant à évanouissement lent 24

Figure 3.1 Schéma en block de l'émetteur OFDM proposé avec préfixe cyclique aléatoire 27

Figure 3.2 Calcul de l'intervalle du préfixe cyclique aléatoire à partir de la réponse impulsionnelle du canal 27

Figure 3.3 Implémentation numérique du système OFDM proposé en bande de base 31

Figure 3.4 Fonction d'autocorrélation d'un système OFDM classique (IEEE 802.11) 36

Figure 3.5 Fonction d'autocorrélation du système OFDM proposé 36

Figure 3.6 Spectre d'un signal OFDM classique élevé au carré 37

Figure 3.7 Spectre du signal OFDM proposé élevé au carré 37

Figure 3.8 Courbes de BER en fonction de la longueur de l'étalement temporel du canal 39

Figure 4.1 Signal à modulation d'amplitude à durée d'impulsion aléatoire 41

Figure 4.2 Courbes de DSP selon la norme IEEE 802.11 avec et sans SN (SN : Sous-porteuse nulles) 52

Figure 4.3 Courbes de la DSP agrandies (SN : Sous-porteuse nulles) 52

Figure 4.4 Module de la FMSO du signal OFDM à préfixe cyclique de taille aléatoire 53

Figure 5.1 Diagramme en block d'un émetteur et un récepteur de type SDR 56

Figure 5.2 Graphe d'une application GNU Radio 59

Figure 5.3 Vue de face du périphérique USRP N210 60

Figure 5.4 Interface graphique GRC de la plateforme GNU Radio 61

Figure 5.5 Hiérarchie modulaire de l'application GNU Radio implémentée 63

Figure 5.6 Configuration de la taille du préfixe cyclique à partir de l'interface GRC 64

Figure 5.7 Scénario de test de l'onde OFDM à préfixe cyclique aléatoire. 66

Figure 5.8 Graphe correspondant au scénario de test de l'onde OFDM à préfixe cyclique de taille pseudo-aléatoire 66

Figure 5.9 Fonction d'autocorrélation cyclique du signal OFDM à préfixe cyclique de taille pseudo-aléatoire reçu par la radio « C » 67

Figure 5.10 Fonction d'autocorrélation cyclique du signal OFDM classique à préfixe cyclique de taille fixe 68

Figure 5.11 Spectre du signal OFDM à préfixe cyclique aléatoire élevé au carré 69

Figure 5.12 Spectre du signal OFDM classique élevé au carré
(Δf : Espacement inter-canal) 69

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

BBAG	Bruit blanc additif gaussien
BPSK	Binary phase shift keying
CAN	Convertisseur analogique-numérique
CM	Corrélation maximale
CMC	Critère des moindres carrés
CNA	Convertisseur numérique-analogique
DFE	Decision Feedback Equaliser
DSC	Densité spectrale cyclique
DSP	Densité spectrale de puissance
EQMM	Erreur quadratique moyenne minimale
FAC	Fonction d'autocorrélation cyclique
FMSO	Fonction de moment de second ordre
FPGA	Field-programmable gate array
GRC	GNU Radio Companion
i.i.d	Variables indépendantes et identiquement distribuées
ICC	Interférence co-canal
IEEE	Institute of Electrical and Electronics Engineers
IIS	Interférence inter-symboles
LFSR	Linear feedback shift register
LPI	Low probability of interception
MV	Maximum à vraisemblance
OFDM	Orthogonal frequency-division multiplexing
PC	Préfixe cyclique
PES	Probabilité d'erreur par symbole
PHY	Couche physique

PSK	Phase-shift keying
QAM	Quadrature amplitude modulation
RF	Radio fréquence
RSB	Rapport signal à bruit
SDR	Software Defined Radio
TEB	Taux d’erreur binaire
TFD	Transformée de Fourier discrète
TFDI	Transformée de Fourier discrète inverse
USRP	Universal Software Radio Peripheral

INTRODUCTION

Une faible probabilité d'interception reste toujours un objectif à atteindre pour tout système de communication utilisé dans des applications militaires. Grâce à son efficacité spectrale et son immunité face aux canaux sélectifs en fréquences, la technologie Orthogonal Frequency Division Multiplexing (OFDM) représente un candidat idéal qui, après y avoir introduit des modifications bien appropriées, peut être utilisée dans la conception d'un système de communication OFDM à faible probabilité d'interception. En fait, à cause du préfixe cyclique inséré au début de chaque symbole OFDM, les signaux OFDM génèrent des caractéristiques cyclostationnaires qui peuvent être exploitées une fois que le signal OFDM sans fil est soumis à certaines transformations non-linéaires [1]. En effet, ces caractéristiques cyclostationnaires sont utilisées dans plusieurs algorithmes d'estimation de paramètres OFDM et de synchronisation aveugle [2].

Ce mémoire a pour objectif la conception d'un système de communication OFDM à faible probabilité d'interception. Dans ce sens, deux techniques à insertion d'aléa sont définies afin de réduire les propriétés cyclostationnaires du signal OFDM et ainsi réduire sa probabilité d'interception. En premier lieu, un préfixe cyclique de taille pseudo-aléatoire est introduit au niveau du modulateur OFDM. Ensuite, une gigue fréquentielle pseudo-aléatoire est introduite à la fréquence porteuse du signal. Les performances du système OFDM proposé sur un canal de Rayleigh sélectif en fréquences sont évaluées. De plus, les expressions exactes du moment de second ordre, ainsi que la densité spectrale de puissance de la forme d'onde OFDM à préfixe cyclique pseudo-aléatoire, sont exprimées pour la première fois.

Afin d'obtenir une preuve de concept du système proposé, une implémentation d'un émetteur OFDM à préfixe cyclique aléatoire sur la plateforme GNU Radio a été effectuée. Pour ce faire, un scénario de test a été établi : Un émetteur OFDM à préfixe cyclique pseudo-aléatoire est implémenté sur une radio de type GNU Radio. D'autre part, une radio jouant le rôle d'un intercepteur malicieux est supposée essayer d'intercepter le signal transmis en effectuant certaines transformations non-linéaires. Après avoir assujetti l'onde OFDM reçue au niveau

de la radio malicieuse à ces transformations, il a été démontré que l'émetteur conçu est caractérisé par un faible niveau de cyclostationnarité et ainsi une faible probabilité d'interception.

Ce mémoire fait donc l'objet des contributions suivantes:

- la conception d'un système de communication OFDM à faible probabilité d'interception implémentant un préfixe cyclique de taille pseudo-aléatoire ainsi qu'une gigue de fréquence pseudo-aléatoire;
- l'analyse des performances du système proposé sur un canal de Rayleigh sélectif en fréquences;
- le développement des expressions du moment de second ordre ainsi que la densité spectrale de puissance de l'onde OFDM à préfixe cyclique pseudo-aléatoire ;
- une démonstration de faisabilité d'un émetteur OFDM à préfixe cyclique pseudo-aléatoire en l'implémentant sur la plateforme GNU Radio.

Le reste du mémoire est structuré comme suit : le premier chapitre présente un survol de la technologie OFDM. Les principales étapes d'une communication OFDM classique y sont détaillées. Le deuxième chapitre passe en revue les caractéristiques cyclostationnaires des signaux OFDM. De plus, des méthodes de détection et de suppression de la cyclostationnarité sont exposées. Dans le troisième chapitre, nous proposons un système de communication OFDM à faible probabilité d'interception. Une analyse des performances du système proposé y est réalisée ainsi qu'une analyse du niveau de cyclostationnarité de la forme d'onde conçue. Le quatrième chapitre présente une analyse spectrale d'une onde OFDM à préfixe cyclique pseudo-aléatoire. Le cinquième chapitre propose une implémentation d'un émetteur OFDM à préfixe cyclique de taille aléatoire sur la plateforme GNU Radio. Une analyse du niveau de la cyclostationnarité y est aussi exposée. Ensuite, un résumé du présent mémoire a été établi dans la conclusion. Enfin, des recommandations pour des futurs travaux ont été proposées afin d'ouvrir de plus vastes horizons de recherche.

CHAPITRE 1

TECHNOLOGIE OFDM

1.1 Principe de l'OFDM

1.1.1 Modulation multi-porteuses

La modulation mono-porteuse consiste à transmettre l'information à travers un canal en la transportant sur une seule onde porteuse à un débit D (symboles par seconde). Cependant, une fois transmis dans un canal à évanouissement multi-trajets, un symbole peut être distordu à cause de l'Interférence Inter-Symbole (IIS).

Afin de combattre l'IIS, la modulation multi-porteuses a été introduite dans [3]. Le spectre disponible W est divisé en N sous-canaux, appelés aussi sous-porteuses, de largeur W/N (*Voir* Figure 1.1).

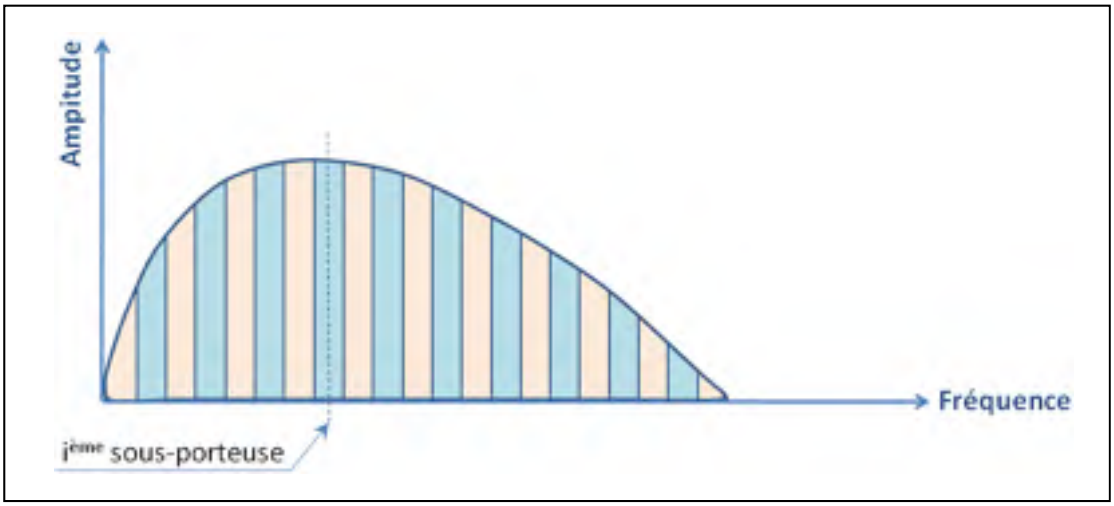


Figure 1.1 Division du spectre disponible en N sous-bandes

Les données sont divisées en blocks de N symboles et elles sont transmises parallèlement en modulant les N sous-porteuses. Ainsi, le signal multi-porteuses peut être écrit comme étant la somme de porteuses modulées tel que :

$$s(t) = \sum_{m=-\infty}^{+\infty} \sum_{k=0}^{N-1} x_{k,m} \Psi_k (t - m\, T_s)\,, \tag{1.1}$$

où $T_s = N/D$ est la durée symbole, Ψ_k la forme d'onde de la $k^{ième}$ sous-porteuse et $x_{k,m}$ le symbole dans le $m^{ième}$ intervalle temporel et modulant la $k^{ième}$ sous-porteuse.

En choisissant N suffisamment grand, la durée symbole T_s peut largement excéder l'étalement temporel maximal du canal τ_{max}. Il en résulte aussi des sous-canaux d'une largeur W/N suffisamment étroite par rapport à la bande de cohérence B_{coh}, ($W/N \ll B_{coh}$). Par conséquent, les sous-bandes peuvent être considérées à évanouissement plat. Cependant, pour des canaux variables dans le temps, les performances peuvent aussi se dégrader à cause des symboles de longues durées : le canal peut varier considérablement pendant la durée d'un symbole si le temps de cohérence du canal T_{coh} est petit par rapport à T_s, de sorte que la démodulation du signal devienne impossible. Ainsi, afin d'assurer la fiabilité de la communication OFDM, N doit vérifier l'inégalité suivante [4, chapitre 3] :

$$\frac{W}{B_{coh}} \ll N \ll DT_{coh}\,, \tag{1.2}$$

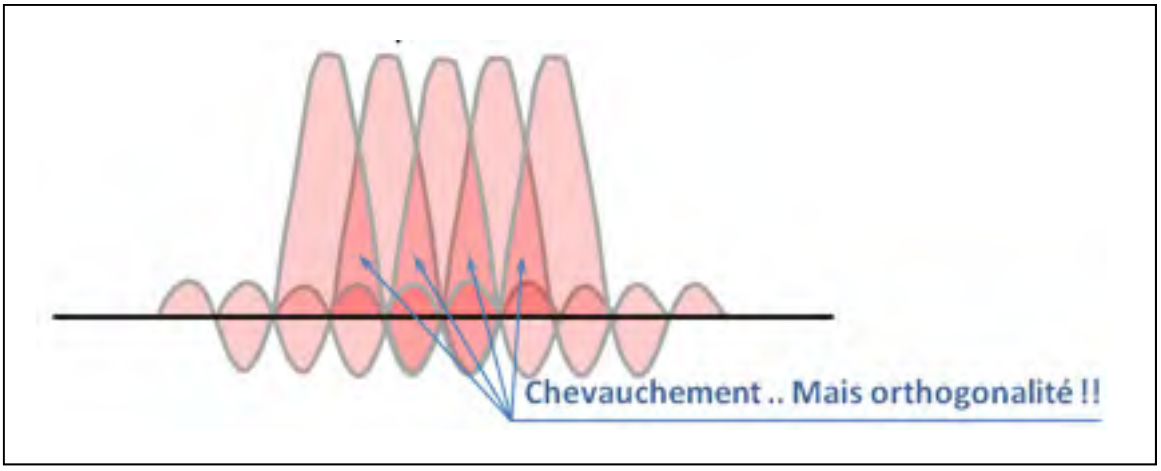


Figure 1.2 Orthogonalité des porteuses dans un système OFDM

1.1.2 Modulation OFDM

L'Orthogonal Frequency Division Multiplexing (OFDM) est une modulation multi-porteuses qui consiste à diviser le spectre fréquentiel disponible en plusieurs sous-canaux, tel qu'illustré à la Figure 1.1. Ces sous-porteuses se chevauchent mais elles sont orthogonales, résultant ainsi en une haute efficacité spectrale. La fonction Ψ_k de la forme d'onde susmentionnée s'écrit donc :

$$\Psi_k(t)= \begin{cases} \frac{1}{\sqrt{T_s}} e^{j2\pi f_k t}, & t \in [0, T_s], \\ 0 & \text{ailleurs,} \end{cases} \tag{1.3}$$

où $f_k = f_0 + {}^{k}/_{T_s}$ est la fréquence de la sous-porteuse $k = 0, 1, \dots, N$. f_0 est un décalage fréquentiel imposé à la transmission. L'espacement entre les sous-porteuses est $\Delta f = {}^{W}/_{N}$ (= ${}^{1}/_{T_s}$ si $\Psi_k$est de support [0 T_s]).

Étant donné que la transformée de Fourier de Ψ_k est donnée par $T_s ex\,p(-j\pi f T_s) \frac{sin(\pi f T_s)}{\pi f T_s}$, le spectre du signal OFDM est représenté dans la Figure 1.2. Grâce à l'orthogonalité des sous-porteuses se traduisant par $\int_0^{T_s} \Psi_k(t)\Psi_l^*(t)dt = \delta(k-l)$, la démodulation du symbole transmis peut être effectuée par l'opération suivante :

$$y_{k,m} = \int_{mT_s}^{(m+1)T_s} s(t)\Psi_k^*(t - m\,T_s)\,, \tag{1.4}$$

Dans [5], une implémentation basée sur la transformée de Fourier discrète inverse (TFDI) a été proposée pour le modulateur OFDM. Dans le même ouvrage, le démodulateur, quant à lui, est basé sur la transformée de Fourier discrète (TFD).

1.1.3 Préfixe cyclique

L'orthogonalité des sous-porteuses est maintenue en insérant un préfixe cyclique (PC) évitant ainsi le phénomène de l'interférence co-canal (ICC). En fait, le PC est une copie de la dernière partie du symbole OFDM placée devant le symbole tout en occupant la durée de l'intervalle de garde. Un choix approprié de la longueur de PC, dépassant l'étalement temporel du canal, permet d'éviter l'interférence inter-symboles (IIS). Il permet aussi de convertir la convolution linéaire du signal émis en une convolution circulaire. Par conséquent, un égaliseur fréquentiel simple peut être utilisé dans le récepteur OFDM afin de récupérer les données transmises. Cependant, l'énergie transmise augmente en fonction du préfixe cyclique. Une perte du rapport signal à bruit (RSB) à cause de l'insertion du PC peut être notée comme :

$$RSB_{perte} = -10log_{10}\left(1 - \frac{T_{cp}}{T}\right) \tag{1.5}$$

où T_{cp} est la longueur du préfixe cyclique et $T = T_s + T_{cp}$ la longueur du symbole OFDM transmis. Ceci entraine une diminution de l'efficacité spectrale d'un facteur pouvant atteindre $D\left(1 - \frac{T_{cp}}{T}\right)$.

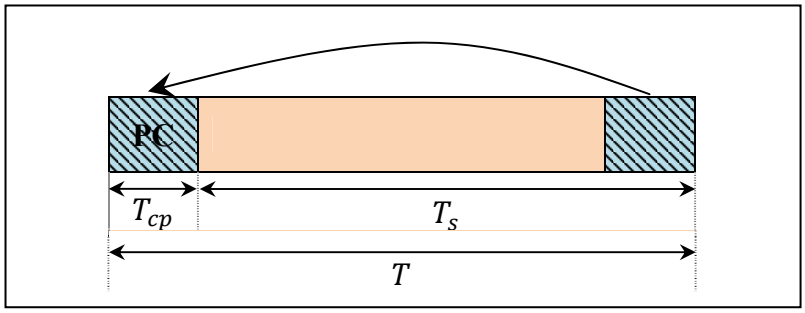


Figure 1.3 Préfixe cyclique

1.1.4 Modèle en bande de base du système OFDM

En échantillonnant le signal OFDM continu à une fréquence $1/T_s$, une implémentation numérique du système OFDM en bande de base est possible telle qu'illustrée à la Figure 1.4.

Ce modèle est basé sur les opérations TFDI, TFD, ainsi que le préfixe cyclique. Un symbole OFDM transmis est représenté sous forme d'un vecteur $\boldsymbol{X}_m = [x_{0,m} \quad x_{1,m} \quad \cdots \quad x_{N-1,m}]^T$ où $\{x_{k,m}\}_{0\leq k\leq N-1}$ sont des symboles de type QAM (Modulation d'Amplitude en Quadrature). Après avoir appliqué une opération TFDI à chaque vecteur $\boldsymbol{X}_m$, un préfixe cyclique de longueur N_g est ajouté à chaque symbole OFDM résultant. Au récepteur, une opération TFD est appliquée au signal OFDM reçu **r** afin de récupérer les symboles QAM transmis.

Le canal de transmission est modélisé par une réponse impulsionnelle $h(t)$ suivie d'un bruit $n(t)$ blanc additif gaussien (BBAG) avec :

$$h(t) = \sum_{k=1}^{N} a_k \delta(t - \tau_k)\,, \tag{1.6}$$

où a_k est une variable aléatoire gaussienne complexe.

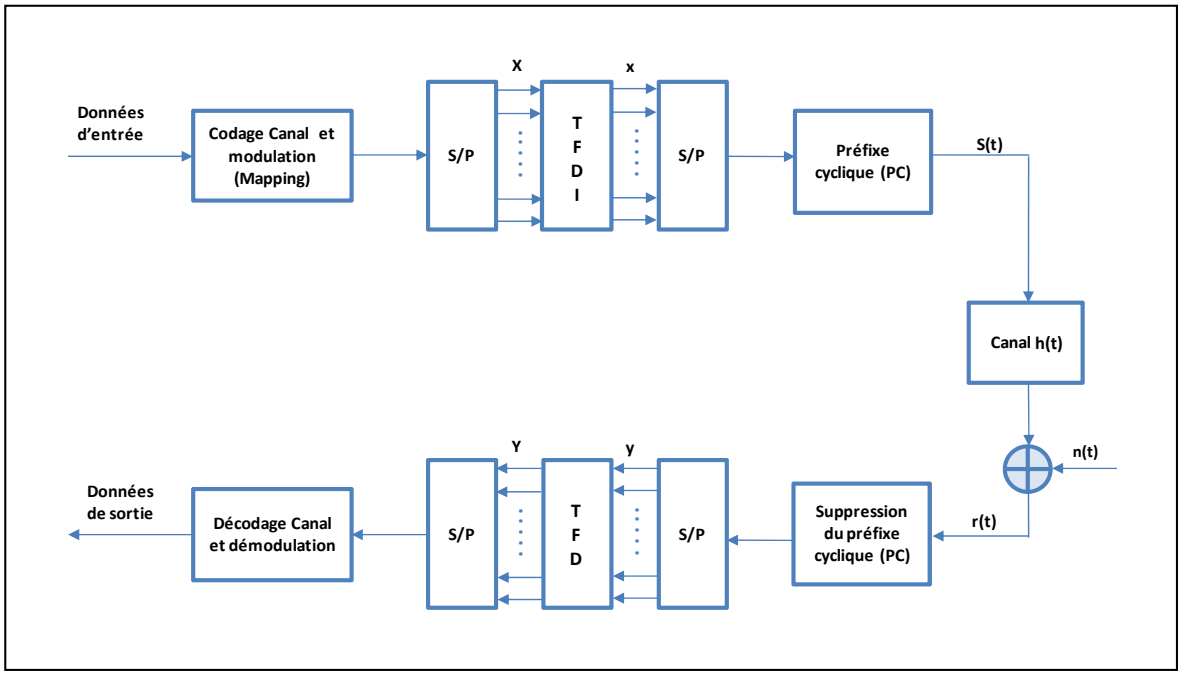


Figure 1.4 Schéma d'un système de communication OFDM en bande de base

D'après [6], un système OFDM est équivalent à une transmission de données sur un ensemble de canaux parallèles tel qu'illustrés dans la Figure 1.5. Au niveau du récepteur, un simple égaliseur est utilisé en divisant le symbole reçu $y_{k,m}$ par son coefficient de canal correspondant afin de récupérer le symbole émis $x_{k,m}$.

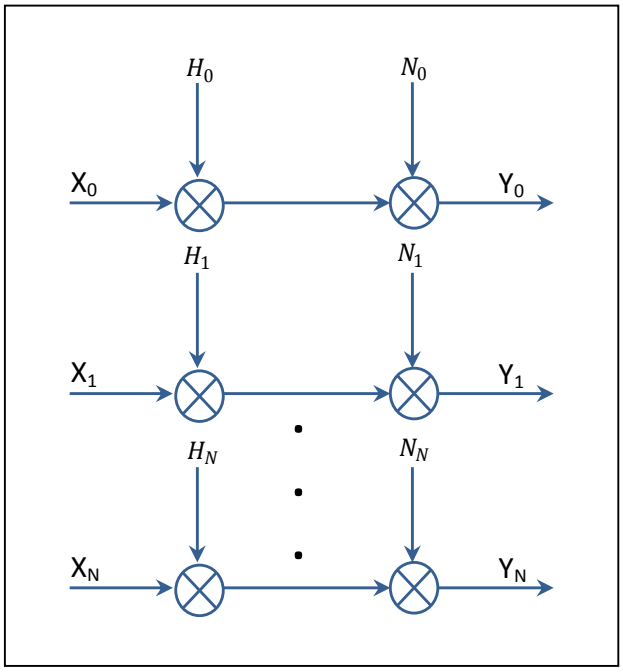


Figure 1.5 Schéma équivalent d'un système OFDM

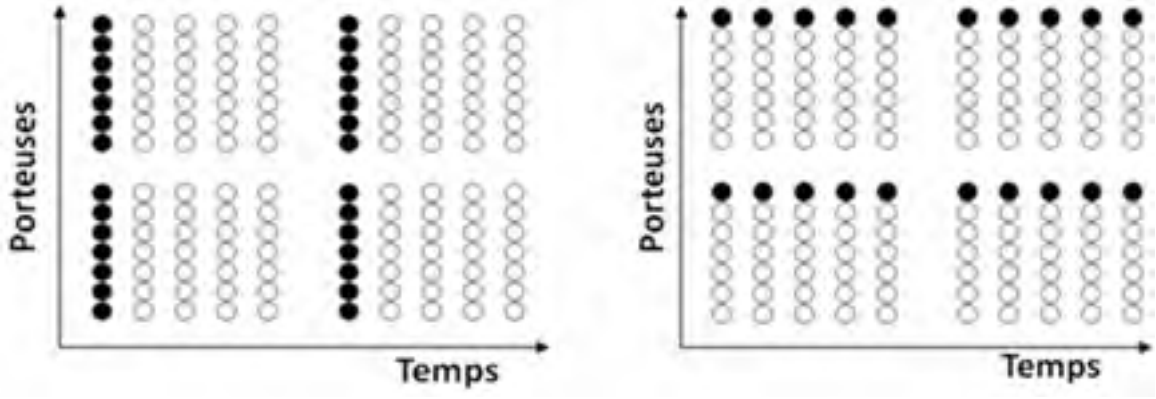
1.2 Estimation du canal pour les systèmes OFDM

Dans un système OFDM, l'une des principales étapes consiste à estimer le canal. Cet estimé sera utilisé au niveau de l'égaliseur à la réception. La conception des estimateurs pour les systèmes OFDM est confrontée par la difficulté de traiter l'information pilote qui n'est autre qu'un signal de référence utilisé par l'émetteur et le récepteur. D'autre part, la conception des estimateurs pour les systèmes OFDM doit présenter une bonne poursuite du canal tout en assurant un faible niveau de complexité [6].

La réponse en fréquence du canal OFDM est considérée comme étant un signal à deux dimensions 2D (Temps, Fréquence). Les estimateurs sont de type : unidimensionnel (1D) ou

bidimensionnel (2D). Les estimateurs 1D sont les plus souvent utilisés dans les systèmes OFDM et sont proposés afin de trouver un compromis entre complexité et précision. Les estimateurs 1D connus sont les estimateurs par pilote de type bloc (*block-type pilot Channel estimator)* ainsi que les estimateurs par pilote de type peigne (*Comb-type pilot Channel estimator*), dans lesquels les signaux pilotes sont insérés en temps et en fréquence, respectivement.

Le canal d'un système OFDM est représenté sous forme d'une grille à deux dimensions (Temps, Fréquence), échantillonnée aux sous-porteuses pilotes et dont les sous-porteuses intermédiaires sont estimées par interpolation. Les estimateurs 1D sont illustrés dans la Figure 1.6. La méthode de type bloc consiste à insérer des symboles pilotes sur toutes les sous-porteuses pilotes d'une manière périodique dans le temps. Cette technique convient pour les canaux à évanouissement lent. Elle peut utiliser le critère des moindres carrés exactes (CMC), le critère du minimum de l'erreur quadratique moyenne minimale (EQMM) ainsi que le critère à Maximum de Vraisemblance (MV). La méthode de type peigne est utilisée pour estimer les canaux à évanouissement rapide. En effet, elle consiste à insérer des symboles pilotes sur des sous-porteuses bien définies et par la suite effectuer une interpolation pour estimer la valeur du canal aux sous-porteuses intermédiaires [6].



(a) Méthode de type bloc (b) Méthode de type peigne

Figure 1.6 Deux méthodes d'arrangement des sous-porteuses pilotes (cercles noirs) pour estimation du canal dans les systèmes OFDM

1.3 Techniques de synchronisation aveugle pour les systèmes OFDM

Dans cette section, nous présentons quelques algorithmes de synchronisation aveugle des systèmes OFDM. Ces méthodes n'ont pas besoin d'informations additionnelles de type symboles ou pilotes, dans le processus de synchronisation. En contrepartie, le préfixe cyclique est fortement utilisé dans de tels algorithmes afin de dériver les paramètres de synchronisation temporelle et fréquentielle.

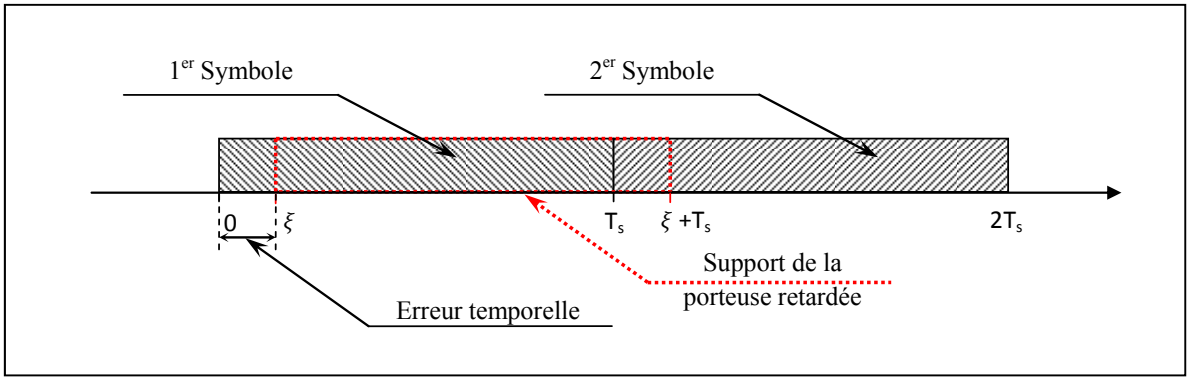


Figure 1.7 Scénario d'erreur de synchronisation temporelle

Avant de démoduler le signal, le récepteur OFDM doit éviter les erreurs de synchronisation en temps et en fréquence par rapport à l'émetteur. Citons à titre d'exemple, en présence d'une erreur de synchronisation temporelle ξ au niveau du récepteur, le signal reçu est indésirablement projeté sur une version retardée de la porteuse modulée telle qu'illustré dans la Figure 1.7.

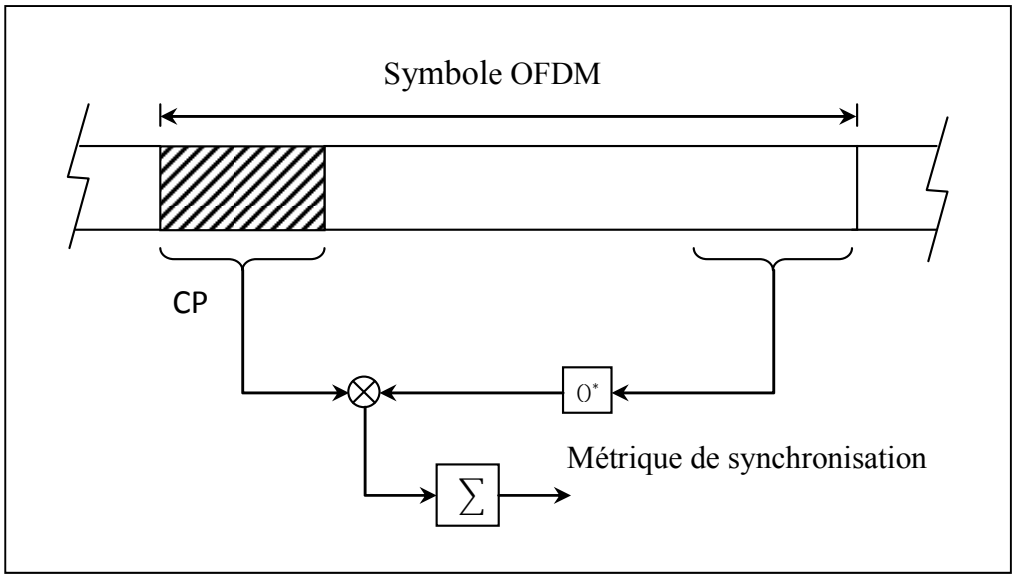


Figure 1.8 Synchronisation aveugle en utilisant le préfixe cyclique

1.3.1 Algorithmes de synchronisation à base du préfixe cyclique

Grâce aux algorithmes de synchronisation à base du préfixe cyclique, les erreurs de synchronisation temporelles et fréquentielles se sont révélées être facilement estimées au niveau du récepteur. Dans [7, 8, 9], un algorithme à maximum de vraisemblance (MV) est présenté. En effet, celui-ci effectue une corrélation d'une partie de taille N_g du signal avec une version retardée de *N* échantillons (*Voir* Figure 1.8). Par conséquent, la recherche de pics de corrélation dans la métrique de synchronisation, illustrée dans la Figure 1.9, permet l'extraction des paramètres de synchronisation. Une fois la synchronisation temporelle est effectuée, l'erreur fréquentielle est facilement déduite.

L'algorithme MV calcule la métrique de synchronisation suivante :

$$\Lambda(m) = \sum_{n=0}^{N_g-1} r(m-n)r^*(m-n+N)\,, \tag{1.7}$$

En utilisant (1.7), la position de synchronisation temporelle est donnée par :

$$\hat{\theta} = \text{argmax}_{\text{m}}\{|\Lambda(m)|\}, \tag{1.8}$$

alors que l'erreur de phase, utilisée pour la synchronisation de la porteuse, s'écrit comme [9] :

$$\hat{\varepsilon} = \frac{1}{2\pi}\angle\Lambda\left(\hat{\theta}\right), \tag{1.9}$$

où $\angle$ désigne l'argument d'un nombre complexe. D'autres algorithmes à base du critère de l'erreur quadratique moyenne minimale (EQMM) [10] et du critère de corrélation maximale (CM) [11] peuvent être utilisés dans le processus de synchronisation.

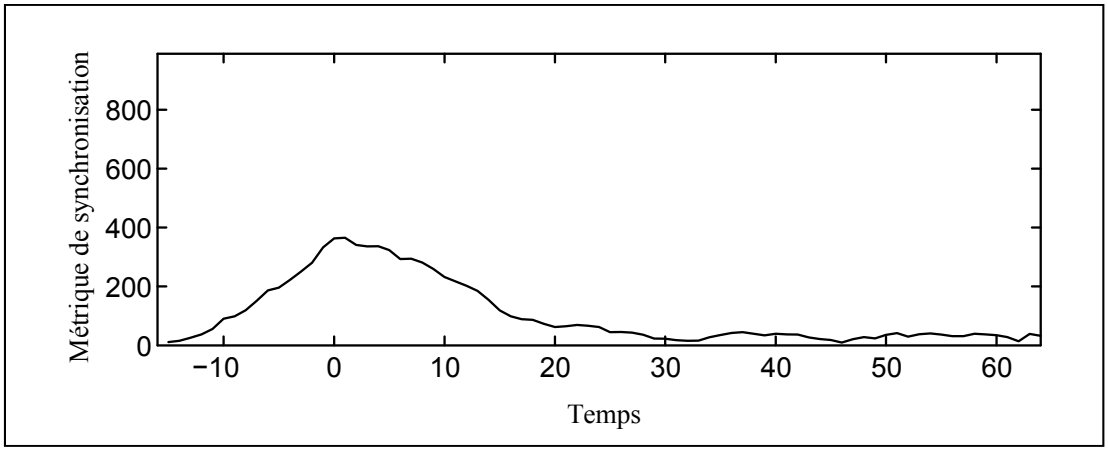


Figure 1.9 Métrique de synchronisation de l'algorithme MV obtenu en utilisant le préfix cyclique
Adaptée de Yucek (2007, p.3)

1.3.2 Algorithmes de synchronisation utilisant la cyclostationnarité

L'estimation aveugle des paramètres dans les systèmes OFDM a été largement étudiée dans la littérature [2, sec. 9]. Plusieurs travaux dans ce contexte sont basés sur l'exploitation des propriétés cyclostationnaires. La cyclostationnarité est clairement manifestée par la réplication du PC dans chaque symbole OFDM.

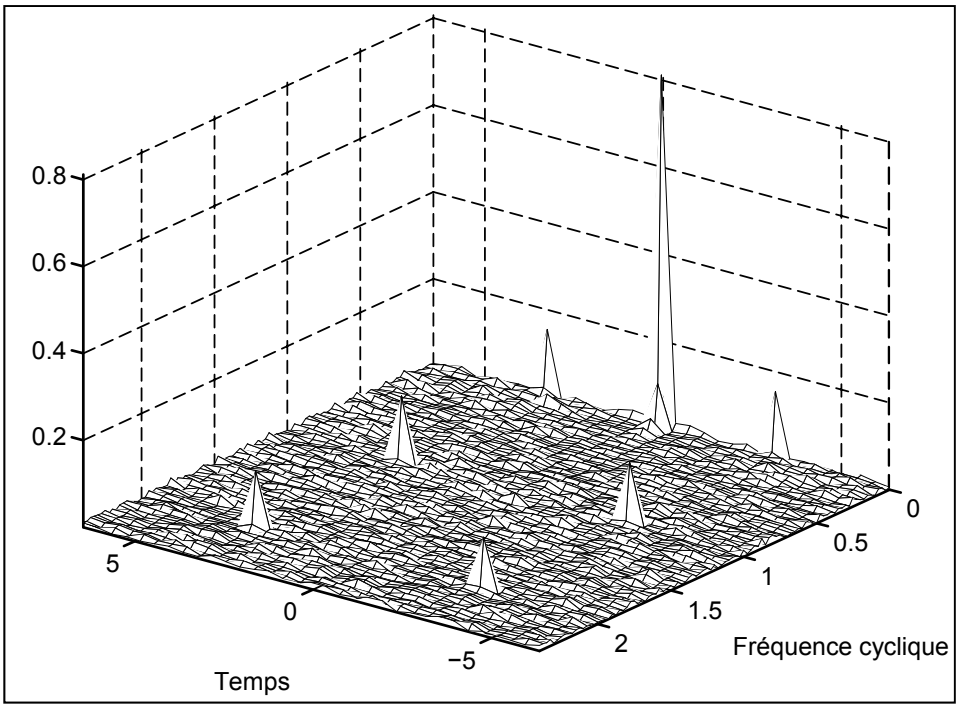


Figure 1.10 Fonction d'Autocorrélation Cyclique (FAC) d'une forme d'onde OFDM sur la base du système 802.11a
Adaptée de Yucek (2007, p.4)

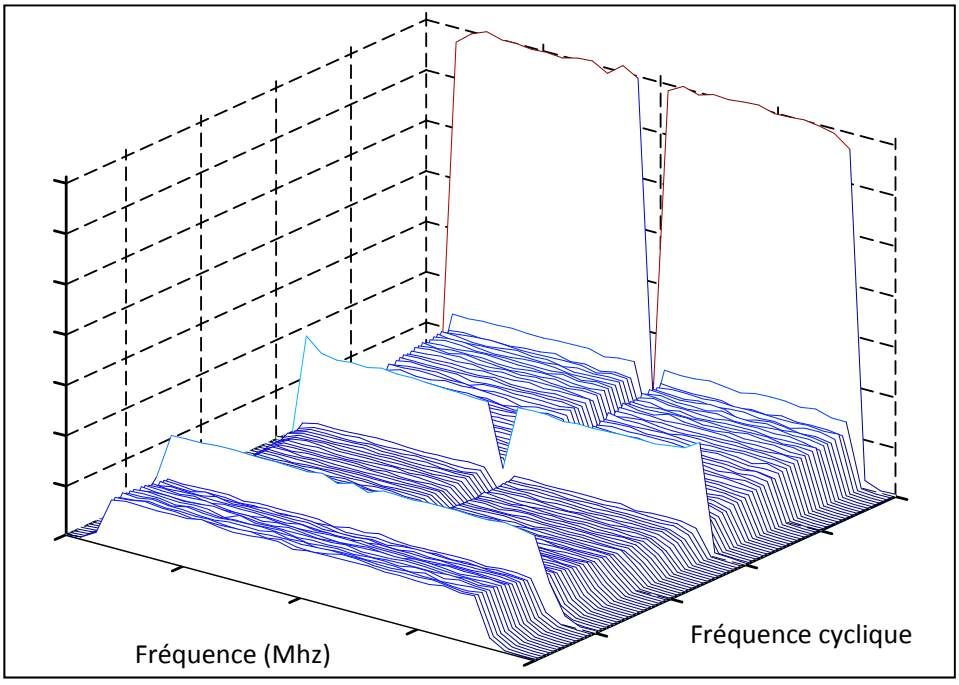


Figure 1.11 Densité Spectrale Cyclique (DSC) d'une forme d'onde OFDM sur la base du système 802.11a
Adaptée de Yucek (2007, p.4)

Les auteurs de [12] suggèrent l'exploitation des statistiques de second ordre dans le processus de synchronisation. En effet, les paramètres de synchronisation sont dérivés après avoir calculé la fonction d'autocorrélation cyclique (FAC) appelée $C[k,\tau]$ où k et τ sont la fréquence cyclique et le délai temporel, respectivement (*Voir* Figure 1.9). Par conséquent, l'erreur de synchronisation fréquentiel θ_e est donnée par :

$$\theta_e = \frac{\arg(C[k,\tau]C[L-k,\tau])}{4\pi\tau}, \quad [k,\tau] \in \mathcal{J} \tag{1.10}$$

alors que l'erreur temporelle n_e s'écrit :

$$n_e = \frac{L}{2\pi k} \arg(C[k,\tau]e^{-j2\pi\theta_e\tau}), \quad [k,\tau] \in \mathcal{J} \tag{1.11}$$

où L est la longueur du symbole OFDM, $\tau \neq 0$, et $k \in [1, L - 1]$. $\mathcal{J}$ une région de $\mathbb{R}^2$ où $C[k,\tau] \neq 0$. En d'autres termes, l'approche exploite les caractéristiques cycliques de la fonction FAC.

1.4 Conclusion

Ce chapitre a traité les divers aspects que présente la technologie OFDM. En premier lieu, le principe et les avantages de la modulation OFDM ont été exposés. En second lieu, un survol du processus d'estimation du canal est présenté. Finalement, les techniques de synchronisation aveugleont été abordées. Une attention particulière a été accordée aux techniques de synchrinosation à base du préfixe cyclique. Dans ce contexte, une revue des méthodes exploitantles caractéristiques cyclostationnaires du signal OFDM a été présentée. Celles-ci représentent un échantillon des techniques aveugles que le présent travail vise à combattre afin de concevoir un système OFDM à faible probabilité d'interception, et ce en empéchant une synchronisation aveugle et malicieuse du signal conçu.

CHAPITRE 2

COMMUNICATIONS OFDM À FAIBLE PROBABILITÉ D'INTERCEPTION

2.1 Introduction

Depuis son invention, la modulation OFDM a été considérée comme l'une des technologies de communication les plus efficaces. Ceci est dû à sa capacité à assurer une complexité d'implémentation raisonnable, sa forte immunité face aux évanouissements multi-trajet ainsi que sa capacité à assurer un haut débit dans les environnements mobiles. L'utilisation sans cesse croissante de cette technologie entraîne des considérations importantes en termes de sécurité. Une transmission sans fil fiable implique les éléments suivants : l'authentification efficace des données, la confidentialité, l'intégrité, le contrôle d'accès et la capacité à se protéger contre les diverses attaques [13]. Afin de répondre à ces exigences, les systèmes OFDM classiques utilisent habituellement la cryptographie à la couche applicative. Une telle approche est nécessaire mais insuffisante car elle est susceptible de souffrir d'éventuelles vulnérabilités. Celles-ci pourraient être exploitées par des utilisateurs indésirables en décryptant les données transmises. Par conséquent, d'autres niveaux de sécurité sont nécessaires dans certains scénarios tels que les applications militaires. Dans ce cadre, la sécurité à la couche physique (PHY) a été introduite dans les systèmes OFDM comme étant une solution prometteuse [1].

2.2 Cyclostationnarité des systèmes OFDM

Le préfixe cyclique (PC) est le paramètre OFDM le plus important qui permet d'identifier le signal OFDM. A ce titre, ce préfixe trahit l'identité de la modulation OFDM et peut être utilisé de façon malicieuse. En effet, la présence de PC constitue un obstacle à la sécurisation des systèmes OFDM classiques. Le PC génère des caractéristiques cyclostationnaires de second ordre qui peuvent être indésirablement exploitées pour synchroniser le signal transmis à l'aveugle après avoir estimé les paramètres OFDM.

Considérons le modèle du signal OFDM introduit dans l'équation (1.1) :

$$s(t) = \frac{1}{\sqrt{T}} \sum_{m=-\infty}^{+\infty} \sum_{k=0}^{N-1} x_{k,m} e^{\frac{j2\pi k(t-T_{cp}-mT)}{N}} g(t-mT)\,, \tag{2.1}$$

où $\{x_{k,m}\}$ sont des symboles indépendants et identiquement distribués (i.i.d), centrés, de variance σ^2. N le nombre de sous-porteuses et $g(t)$ la forme de l'impulsion de support [$-T_{cp}$ T_s]. La fonction d'autocorrélation du signal $s(t)$ est définie comme :

$$\begin{aligned} \mathcal{R}_s(t,\tau) &= E\{s(t)s^*(t-\tau)\} \\ &= \frac{1}{T} \sum_m \sum_p \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} E\{x_{k,m} x_{l,p}^*\} \\ &\quad \times E\{g(t-mT)g^*(t-\tau-pT)\} e^{j2\pi k \frac{(t-T_{cp}-mT)}{N}} e^{-j2\pi l \frac{(t-\tau-T_{cp}-pT)}{N}}, \end{aligned} \tag{2.2}$$

où $(.)^*$ représente le conjugué complexe. Sous l'hypothèse que les symboles $x_{k,m}$ sont i.i.d de moyenne nulle, alors $E\{x_{k,m}x_{l,p}^*\} = 0$ pour $m \neq p$ et $k \neq l$, ainsi :

$$\begin{aligned} \mathcal{R}_s(t,\tau) &= \frac{\sigma^2}{T} \sum_m \sum_{k=0}^{N-1} g(t-mT)g^*(t-\tau-mT)\, e^{j2\pi k \frac{\tau}{N}} \\ &= \frac{\sigma^2}{T} \sum_m g(t-mT)g^*(t-\tau-mT) \sum_{k=0}^{N-1} e^{j2\pi k \frac{\tau}{N}}\,. \end{aligned} \tag{2.3}$$

Le terme $\sum_{k=0}^{N-1} e^{2i\pi k \frac{\tau}{N}}$ est une série géométrique de raison $e^{j2\pi \frac{\tau}{N}}$, par conséquent :

$$\sum_{k=0}^{N-1} e^{j2\pi k \frac{\tau}{N}} = \frac{sin(\pi\tau)}{sin(\frac{\pi\tau}{N})} e^{j\pi\left(\frac{N-1}{N}\right)\tau}. \tag{2.4}$$

Ainsi,

$$\mathcal{R}_s(t,\tau) = \frac{\sigma^2}{T}\frac{sin(\pi\tau)}{sin(\frac{\pi\tau}{N})}e^{j\pi\left(\frac{N-1}{N}\right)\tau} \times \sum_m g(t-mT)g^*(t-\tau-mT). \quad (2.5)$$

De (2.5), il est facilement déduit que $\mathcal{R}_s(t,\tau)$ est périodique dans le temps d'une période T :

$$\mathcal{R}_s(t\ +\ T,\tau) =\ \mathcal{R}_s(t,\tau). \quad (2.6)$$

Pour un décalage fixeτ, $\mathcal{R}_s(t,\tau)$peut être développée en série de Fourier avec les coefficients suivants :

$$\mathcal{R}_s^{\gamma}(\tau) = \frac{1}{T}\int_0^T \mathcal{R}_s(t,\tau)e^{-j2\pi\gamma t}dt, \quad (2.7)$$

où γ est la fréquence cyclique. Par conséquent :

$$\mathcal{R}_s^{\gamma}(\tau) = \frac{\sigma^2}{T^2}\frac{sin(\pi\tau)}{sin(\frac{\pi\tau}{N})}e^{j\pi\left(\frac{N-1}{N}\right)\tau}\sum_m \delta\left(\gamma-\frac{m}{T}\right) \times \int_0^T g(t)g^*(t-\tau)e^{-j2\pi\gamma t}dt. \quad (2.8)$$

D'après (2.8), l'expression de $R_s^{\gamma}(\tau)$ est discrète. Celle-ci est composée de plusieurs pics aux fréquences $\gamma_m = \frac{m}{T}$ et est nulle ailleurs, ainsi :

$$\mathcal{R}_s^{\gamma_m}(\tau) = \frac{\sigma^2}{T^2}\frac{sin(\pi\tau)}{sin(\frac{\pi\tau}{N})}e^{j\pi\left(\frac{N-1}{N}\right)\tau}\int_0^T g(t)g^*(t-\tau)e^{-j2\pi\gamma_m t}dt\ . \quad (2.9)$$

Le terme $\mathcal{R}_s^{\gamma_m}(\tau)$ dépend du terme cyclique de la forme du pulse $g(t)$. Il est encore noté que dans le cas où le préfixe cyclique n'est pas utilisé ($T_{cp} = 0$), $\mathcal{R}_s^{\gamma_m}(\tau)$ est nul pour tout $\gamma \neq 0$.

En détectant les pics dans $\mathcal{R}_s^{\gamma}(\tau)$, il devient possible d'estimer la différence entre deux pics et donner ainsi une estimation de T après avoir utilisé un algorithme approprié de détection de pics.

2.3 Méthodes de détection de la cyclostationnarité

La cyclostationnarité d'ordre supérieur (où cyclostationnarité d'ordre n) est la forme la plus générale de la théorie de cyclostationnarité. Dans la littérature, les travaux se limitent généralement à l'utilisation du second ordre (n = 2) et ce afin de réduire la complexité d'implémentation ainsi que le temps de calcul. Pour les mêmes raisons, le présent travail traite la cyclostationnarité de second ordre des signaux OFDM et se base, dans son analyse, sur des outils mathématiques associés aux statistiques de second ordre [2, sec. 4].

Afin de détecter et analyser les caractéristiques cyclostationnaires de second ordre du signal OFDM, nous exposons trois outils mathématiques: la fonction d'autocorrélation cyclique (FAC), la fonction de densité spectrale cyclique (DSC) et la densité spectrale de puissance de la transformée au carré du signal.

2.3.1 Fonction d'Autocorrélation Cyclique (FAC)

Étant donné un processus $x(t)$ à temps discret, sa fonction d'autocorrélation est donnée par :

$$\mathcal{R}_x(t,\tau) = \langle x(t)x^*(t-\tau)\rangle\,, \tag{2.10}$$

avec,

$$\langle . \rangle \triangleq \lim_{T\to+\infty} \frac{1}{2T+1} \sum_{t=-T}^{T} (.)\,, \tag{2.11}$$

$x(t)$ est dit cyclostationnaire si $\mathcal{R}_x(t,\tau)$est périodique. Dans ce cas, un développement en série de Fourier de $R_x(t,\tau)$ est possible. Le coefficient de Fourier $\mathcal{R}_x^{\gamma}(\tau)$ résultant s'écrit ainsi :

$$\mathcal{R}_x^{\gamma}(\tau) = \langle x(t)x^*(t-\tau)e^{-j2\pi\gamma t}\rangle e^{j\pi\gamma\tau}. \quad (2.12)$$

Le terme $e^{j\pi\gamma\tau}$ est introduit afin d'établir la correspondance entre le domaine discret et le domaine continu [14]. Une deuxième représentation de l'équation (2.12) est exprimée après avoir factorisé le terme $e^{j\pi\gamma\tau}$ à l'intérieurde $\langle x(t)x^*(t)e^{-j2\pi\gamma t}\rangle$:

$$\mathcal{R}_x^{\gamma}(\tau) = \langle \{x(t)e^{-j\pi\gamma\tau}\}\{x(t-\tau)e^{j\pi\gamma(t-\tau)}\}^*\rangle. \quad (2.13)$$

La transformation quadratique de l'équation (2.13) est appelée Fonction d'Autocorrélaiton Cyclique (FAC) et reflète la contribution des composantes sinusoïdales (cycliques) de fréquence γ à la fonction d'autocorrélation. Dans ce qui suit, différents types de processus cyclostationnaires sont définis :

Processus purement stationnaire

Un processus est dit purement stationnaire si sa fonction $\mathcal{R}_x^{\gamma}(\tau) = 0$ pour toute fréquence cyclique $\gamma \neq 0$.

Processus purement cyclostationnaire de second ordre

Un processus est dit purement cyclostationnaire si sa fonction d'autocorrélation cyclique $\mathcal{R}_x^{\gamma}(\tau)$ est nulle partout sauf pour γ multiple d'une seule fréquence fondamentale $\frac{1}{T}$ (T est la durée symbole).

Processus cyclostationnaire de second ordre dans le sens général

Un processus est dit cyclostationnaire de second ordre dans le sens général si sa fonction d'autocorrélation cyclique $\mathcal{R}_x^{\gamma}(\tau)$ est non-nulle, pour certaines fréquences cycliques γ multiples d'une seule fréquence fondamentale $\frac{1}{T}$.

Processus polycyclostationnaire de second ordre

Un processus est dit polycyclostationnaire de second ordre si sa fonction d'autocorrélation cyclique possède plusieurs fréquences fondamentales pour lesquelles $\mathcal{R}_x^{\gamma}(\tau)$ est non nulle.

En général, la cyclostationnarité est liée à certains paramètres tels que le taux de symbole, la fréquence symbole, la fréquence d'échantillonnage, etc [14].

2.3.2 Fonction de Densité Spectrale Cyclique (DSC)

Après avoir exprimé la fonction d'autocorrélation cyclique (FAC), il est possible d'en déduire la densité spectrale cyclique(DSC), notée $S_x^{\gamma}(f)$, en utilisant le théorème de Wiener-Khintchine [15]:

$$S_x^{\gamma}(f) = \sum_{\tau=-\infty}^{+\infty} R_x^{\gamma}(\tau) e^{-j2\pi f\tau}. \tag{2.14}$$

Une estimation de cette fonction est possible en utilisant l'équation suivante :

$$\tilde{S}_x^{\gamma}(f) = \frac{1}{N}\frac{1}{T}\sum_{n=-N/2}^{N/2} X_T(n, f-\frac{\gamma}{2}) X_T^*(n, f+\frac{\gamma}{2}). \tag{2.15}$$

avec,

$$X_T(n,f) = \int_{n-T/2}^{n+T/2} x(u) e^{-j2\pi fu} du\,. \tag{2.16}$$

où N représente le nombre d'échantillons. Selon l'équation (2.15), la fonction DSC n'est autre que l'autocorrélation de $X_T(n,f)$ translatée aux fréquences $f-\frac{\gamma}{2}$ et $f+\frac{\gamma}{2}$. La densité spectrale de puissance est un cas particulier de la DSC lorsque $\gamma = 0$.

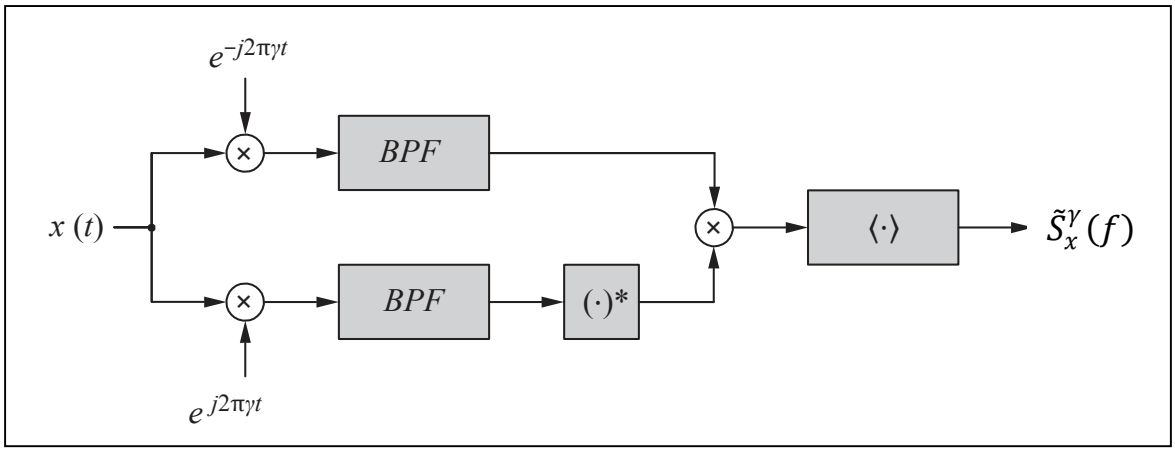


Figure 2.1 Implémentation de la DSC
Adaptée de Gardner (2006, p. 657)

2.3.3 Densité spectrale de puissance de la transformée au carré du signal

La transformation quadratique du signal génère des propriétés cyclostationnaires et permet d'en extraire divers paramètres tels que le débit symbole et la fréquence porteuse en utilisant les raies spectrales une fois que le signal reçu est élevé au carré (*Voir* Figure 2.2). Une telle transformation est utilisée dans divers algorithmes de synchronisation tels que ceux dans [1, 16]. Des transformations non-linéaires d'ordre supérieur sont utilisées dans d'autres schémas de synchronisation et d'estimation de paramètres [17, 18].

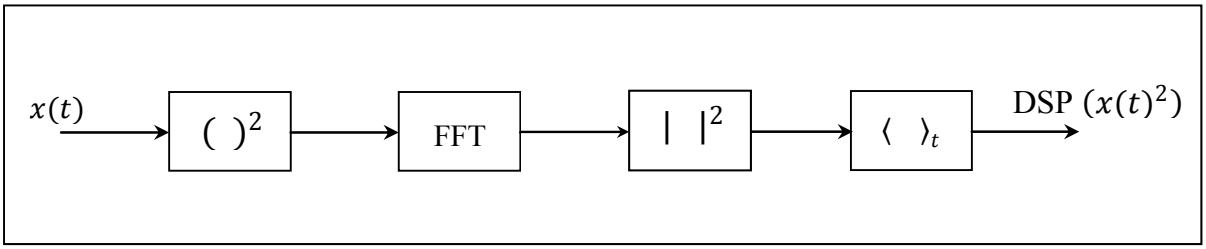


Figure 2.2 Densité spectrale de puissance de la transformée au carré du signal

2.4 Revue de la littérature des méthodes de suppression de la cyclostationnarité pour les systèmes OFDM

2.4.1 Méthodes classiques de suppression de la cyclostationnarité

De nombreuses solutions ont été proposées afin de réduire la cyclostationnarité et ce en modifiant le signal OFDM pour le rendre stationnaire. Dans [19], on propose d'ajouter un signal bruité Ultra-Large Bande synthétisé à l'émetteur, aux symboles OFDM. Cette technique est utilisée pour concevoir un système de radar sécurisé spectralement indétectable. Cependant, une dégradation des performances en termes du taux d'erreur binaire (TEB) est remarquée à cause de l'ajout du bruit. Dans [20], l'élimination complète du PC a permis d'éradiquer les caractéristiques cycliques du signal OFDM. Dans ce dernier design, une complexité supplémentaire a été introduite à cause de l'utilisation d'un égaliseur DFE ("Decision Feedback Equaliser") dont l'objectif est d'éliminer l'interférence inter-symboles. Finalement, [21] propose de remplacer le PC dans chaque symbole OFDM par un signal aléatoire (*Voir* Figure 2.3).

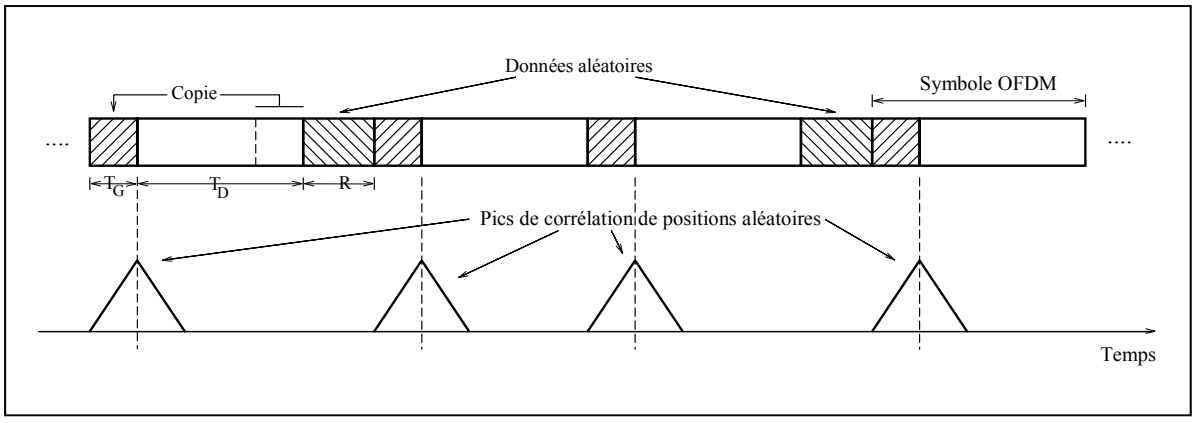


Figure 2.3 Insertion de signaux aléatoires en tant que préfixes cycliques
Adaptée de Yucek (2007, p.4)

2.4.2 Revue de la littérature des méthodes à insertion d'aléa

Divers travaux de la littérature ont proposé d'introduire de l'aléa sur les différents paramètres OFDM.L'insertion de l'aléa sur la phase des signaux modulés a été introduite dans [22] afin d'affaiblir les caractéristiques cyclostationnaires du signal OFDM. De plus, les auteurs de [19] ont proposé de changer les emplacements des pilotes OFDM d'une manière pseudo-aléatoire afin de réduire la probabilité d'interception. Dans une tentative de réduire les propriétés cycliques du signal émis, des séquences pseudo-aléatoires sont utilisées au lieu des préambules dans [20]. Ensuite, une gigue de fréquence a été également introduite pour masquer la signature spectrale du signal. Deux autres techniques sont présentées dans [20] : d'abord, une première technique proposée consiste à faire varier la taille du préfixe cyclique en concaténant des signaux aléatoires au début de certains symboles OFDM. D'autre part, une deuxième technique propose de changer la taille du préfixe cyclique d'une manière adaptative en fonction des conditions du canal. Cette dernière technique présente cependant quelques faiblesses: une estimation continue de l'étalement temporel du canal est nécessaire en vue d'adapter la taille du préfixe cyclique à chaque symbole OFDM. Ceci entraine une complexité d'implémentation supplémentaire. De plus, dans le cas où le canal est à évanouissement lent, l'étalement temporel du canal peut ne pas changer pendant de longues périodes. Ceci permet aux intercepteurs de moyenner la métrique de synchronisation sur un certain nombre de symboles. L'intercepteur peut ainsi se synchroniser au signal après avoir extrait des paramètres OFDM.

2.4.3 Effet de l'évanouissement du canal sur l'insertion d'aléa au préfixe cyclique

L'extraction aveugle des paramètres de synchronisation à l'aide du PC à partir d'un seul symbole est extrêmement difficile dans la pratique en raison de la nature multi-trajet et bruyante du canal [21]. Dans ces conditions, une moyenne de la métrique de corrélation sur un certain nombre de symboles s'impose avant d'appliquer des algorithmes de synchronisation dans [23, 24]. Pour éviter le risque d'émerger indésirablement des informations de synchronisation à partir de plusieurs symboles, [21] propose de modifier la taille du PC adaptativement en fonction des conditions du canal. En fait, la taille du PC est

ajustée à l'étalement temporel maximal du canal dans chaque symbole, ce qui permet d'empêcher les intercepteurs d'effectuer le calcul de la moyenne. Cependant, une telle technique n'est pas bien adaptée aux canaux à évanouissements lents. En effet, dans ces conditions, la réponse impulsionnelle du canal est essentiellement invariante (*Voir* Figure 2.4) pendant le temps de cohérence du canal T_c définie dans [25] par :

$$T_c = \sqrt{\frac{9}{16\pi f_m^2}}, \tag{2.17}$$

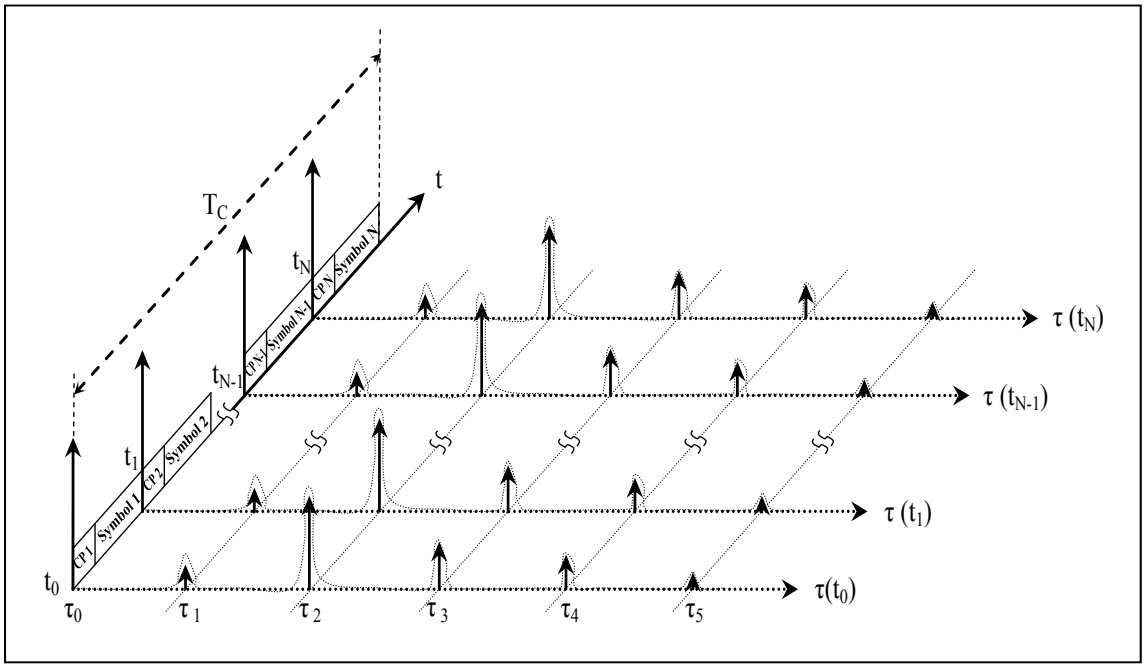


Figure 2.4 Réponse impulsionnelle discrète d'un canal invariant à évanouissement lent

où f_m présente l'étalement Doppler maximal exprimé par $f_m = \upsilon/\lambda$. υ et λ représentent la vélocité et la longueur d'onde, respectivement. À titre d'exemple, considérons un mobile se déplaçant à une vitesse υ = 45 Km/h et recevant un signal OFDM à 5 GHz à partir d'une source distante S. De (2.17), le temps de cohérence est approximée à $T_c \simeq$ 1,8 ms. T_c couvre ainsi environ 500 symboles OFDM chacun de durée $T_s \simeq 4$ µs (802.11a). L'application de la taille adaptative du PC tel que présenté dans [21] ne permet pas de faire varier la taille du PC

pendant T_c. Par conséquent, 500 symboles OFDM sont suffisants pour effectuer la moyenne et combiner les informations afin d'en extraire les paramètres de synchronisation, puisque la taille de PC demeure invariable. Cette technique présente donc une faiblesse d'interception dans les canaux à évanouissement lent. Dans le chapitre suivant, nous proposons une technique qui permet d'éviter cette difficulté en assurant une variation continue de la taille du PC.

2.5 Conclusion

Dans ce chapitre, la cyclostationnarité des systèmes OFDM a été abordée. Il a été démontré que les propriétés cyclostationnaires d'un signal OFDM peuvent être exploitées dans des algorithmes de synchronisation aveugles appropriés. De plus, des outils de détection de la cyclostationnarité ont été exposés. Finalement, une revue critique de la littérature des méthodes de suppréssion de la cyclostationnarité a été présentée.

CHAPITRE 3

SYSTÈME OFDM À FAIBLE PROBABILITÉ D'INTERCEPTION

3.1 Introduction

Dans ce chapitre, nous proposons une combinaison innovante de deux techniques permettant la conception d'un système OFDM sécurisé. D'abord, nous nous concentrons principalement sur l'atténuation des propriétés cyclostationnaires présentes dans les signaux OFDM, puis, nous rajoutons un deuxième niveau de sécurité en introduisant de l'aléa à la fréquence porteuse du signal. À cette fin, nous proposons de 1) faire varier aléatoirement la taille du PC dans chaque symbole OFDM indépendamment du canal, et 2) introduire une gigue de fréquence aléatoire afin de réduire les raies spectrales correspondantes aux sous-porteuses et rendre ainsi difficile la démodulation du signal OFDM.

3.2 Suppression des caractéristiques cyclostationnaires de l'onde OFDM

3.2.1 Préfixe cyclique de taille pseudo-aléatoire

Dans ce paragraphe, nous proposons de réduire les caractéristiques OFDM cycliques tout en conservant les avantages du PC. En effet, la taille de PC est modifiée pseudo-aléatoirement à chaque symbole OFDM. Une fois l'étalement temporel maximal du canal estimé, la variation du PC est déclenchée tout en suivant une distribution uniforme dans un ensemble fini de valeurs possibles.

Ce travail fait l'objet d'une publication dans la conférence MILCOM 2012, soutenu en partie par Ultra Electronics TCS et le Conseil de Recherches en Sciences Naturelles et en Génie du Canada dans le cadre de la Chaire de recherche industrielle en communications sans fil tactiques et d'urgence de haute performance à l'École de technologie supérieure.

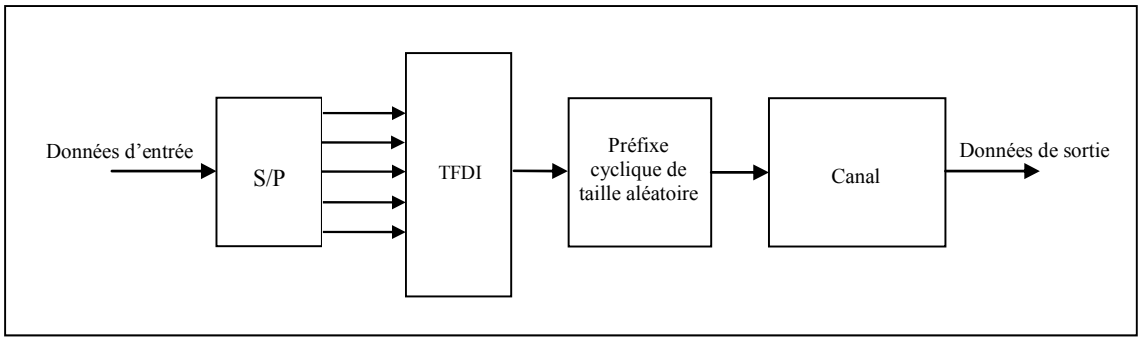


Figure 3.1 Schéma en block de l'émetteur OFDM proposé avec préfixe cyclique aléatoire

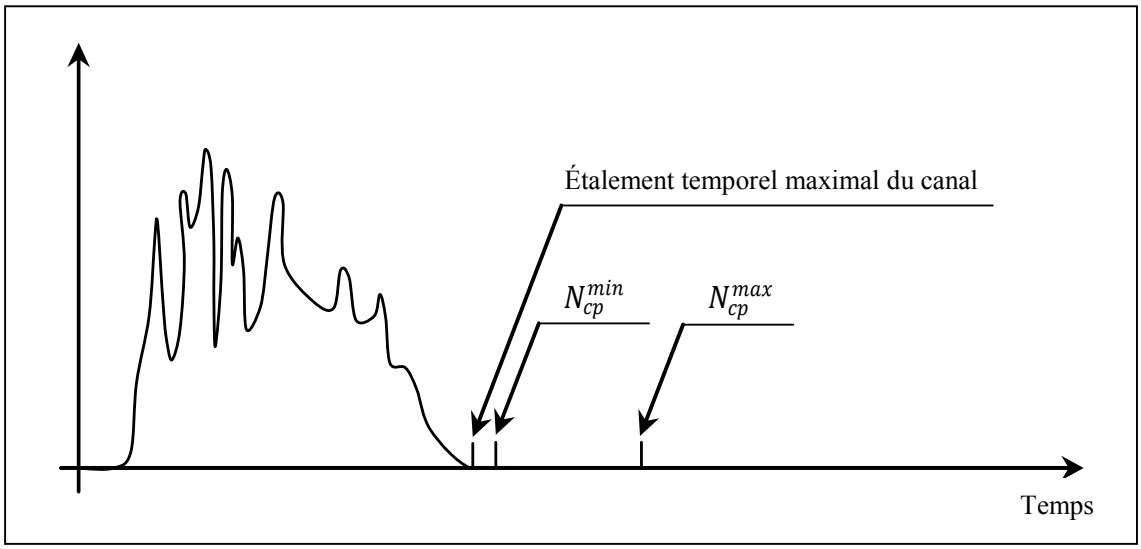


Figure 3.2 Calcul de l'intervalle du préfixe cyclique aléatoire à partir de la réponse impulsionnelle du canal

La valeur minimale N_{cp}^{min} de cet ensemble est choisie de telle manière qu'elle dépasse légèrement l'étalement temporel maximal que le canal peut éprouver (Ex: IEEE 802.11a). La limite supérieure N_{cp}^{max} est choisie de sorte qu'elle assure une marge confortable dans laquelle la taille du PC peut varier. En outre, la fonction pseudo-aléatoire, qui décrit l'évolution de la taille PC, est connue à la fois au niveau de l'émetteur et du récepteur. Par conséquent, sans connaître la durée de chaque symbole, les intercepteurs indésirables sont incapables de se synchroniser au signal transmis.

Afin d'estimer l'étalement temporel maximal du canal, différents algorithmes proposés dans la littérature peuvent être utilisés, tels que [26] et [27]. En outre, il peut arriver que l'étalement temporel maximal du canal devienne légèrement plus long que la taille minimale N_{cp}^{min}du PC. Dans ce cas, une dégradation des performances peut être remarquée à cause de l'IIS. Par conséquent, un gain de codage additionnel peut être utilisé pour compenser la perte de performance.

Afin d'observer l'effet de la technique proposée sur les caractéristiques cycliques, nous évaluons la fonction FAC. Soit $s(n)$ un signal OFDM discret à préfixe cyclique de taille aléatoire :

$$s(n) = \frac{1}{N}\sum_{m=-\infty}^{+\infty}\sum_{k=0}^{N-1} x_{k,m} e^{\frac{j2\pi k\left(n-N_{cp}^{m}-\alpha_m\right)}{N}} g_m(n-\alpha_m)\,, \tag{3.1}$$

où$\{x_{k,m}\}$ sont des symboles i.i.d, centrés, de varianceσ^2, N le nombre de sous-porteuses et $\{g_m(n)\}$ une séquence d'impulsions de durée spseudo-aléatoires N_m avec $N_m = N_u + N_{cp}^m$ où N_u est la durée utile et N_{cp}^m la taille pseudo-aléatoire de l'intervalle de garde. Nous supposons que N_{cp}^m varie entre N_{cp}^{min} et N_{cp}^{max}. Par conséquent, N_m varie également entre N_m^{min} et N_m^{max}, α_m est une époque temporelle à partir de l'origine des temps qui satisfait $\alpha_{m+1} - \alpha_m = N_m$. La fonction d'autocorrélation s'écrit donc comme suit :

$$\begin{aligned}\mathcal{R}_s(n,\tau) &= E\{s(n)s^*(n-\tau)\} \\ &= \frac{1}{N^2}\sum_m\sum_p\sum_{k=0}^{N-1}\sum_{l=0}^{N-1} E\left\{x_{k,m}x_{l,p}^*\right\} \\ &\quad \times E\left\{g_m(n-\alpha_m)g_p^*(n-\tau-\alpha_p)\right\} e^{j2\pi k\frac{(n-N_{cp}^m-\alpha_m)}{N}} e^{-j2\pi l\frac{(n-\tau-N_{cp}^p-\alpha_p)}{N}}\,.\end{aligned} \tag{3.2}$$

Étant donné que les symboles $x_{k,m}$ sont i.i.d de moyenne nulle, $E\{x_{k,m}x_{l,p}^{*}\} = 0$ pour $m \neq p$ et $k \neq l$, on peut écrire donc :

$$\mathcal{R}_s(n,\tau) = A.\sum_{m}\sum_{k=0}^{N-1} E\{g_m(n-\alpha_m)g_m^{*}(n-\tau-\alpha_m)\}\, e^{j2\pi k\frac{\tau}{N}} \tag{3.3}$$

$$= A.\sum_{m} E\{g_m(n-\alpha_m)g_m^{*}(n-\tau-\alpha_m)\}\sum_{k=0}^{N-1} e^{j2\pi k\frac{\tau}{N}}\ ,$$

où $A = \sigma^2/N^2$. Le terme $\sum_{k=0}^{N-1} e^{2i\pi k\frac{\tau}{N}}$ est une série géométrique de raison $e^{j2\pi\frac{\tau}{N}}$, ainsi :

$$\sum_{k=0}^{N-1} e^{j2\pi k\frac{\tau}{N}} = \frac{sin(\pi\tau)}{sin(\frac{\pi\tau}{N})}\, e^{j\pi\left(\frac{N-1}{N}\right)\tau}. \tag{3.4}$$

D'où,

$$\mathcal{R}_s(n,\tau) = A\frac{sin(\pi\tau)}{sin(\frac{\pi\tau}{N})} e^{j\pi\left(\frac{N-1}{N}\right)\tau} \times E\left\{\sum_{m} g_m(n-\alpha_m)g_m^{*}(n-\tau-\alpha_m)\right\}. \tag{3.5}$$

Pour un décalage fixe τ, $\mathcal{R}_s(n,\tau)$ possède les coefficients de Fourier $\mathcal{R}_s^{\gamma}(\tau)$ suivants :

$$\mathcal{R}_s^{\gamma}(\tau) = \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1} R_s(n,\tau)e^{-j2\pi\gamma n}. \tag{3.6}$$

Par conséquent,

$$\mathcal{R}_s^{\gamma}(\tau) = A\frac{sin(\pi\tau)}{sin(\frac{\pi\tau}{N})} e^{j\pi\left(\frac{N-1}{N}\right)\tau} \times\left(\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1} E\left\{\sum_{m} g_m(n-\alpha_m)g_m^{*}(n-\tau-\alpha_m)\right\}e^{-j2\pi\gamma n}\right). \tag{3.7}$$

Cette équation est semblable à celle du signal OFDM classique exprimée dans l'équation (2.8). Cependant, la moyenne statistique qui y est appliquée dans le terme $\left(\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1}E\{\sum_m g_m(n-\alpha_m)g_m^*(n-\tau-\alpha_m)\}\,e^{-j2\pi\gamma n}\right)$, est responsable de la réduction significative des caractéristiques cyclostationnaires du signal OFDM.

3.2.2 Gigue fréquentielle pseudo-aléatoire

Faire passer l'onde OFDM conçue à travers un récepteur non linéaire, génère des raies spectrales qui peuvent être utilisées pour démoduler le signal OFDM [16]. Élever le signal OFDM au carré, constitue un exemple simple de récepteur non linéaire détectant les périodicités. Considérons une constellation BPSK, $x_{k,0} = \pm 1$. Pour le premier symbole OFDM d'indice 0 (ceci peut être généralisé pour tout $k^{ième}$symbole), nous avons :

$$\left(\sum_{k=0}^{N-1} x_{k,0}e^{\frac{j2\pi kn}{N}}\right)^2 = \underbrace{\sum_{k=0}^{N-1} e^{\frac{j4\pi kn}{N}}}_{❶} + \sum_{k=0}^{N-1}\sum_{p=0}^{N-1} x_{k,0}\,x_{p,0}e^{\frac{j2\pi kn}{N}}e^{\frac{j2\pi pn}{N}}, \qquad k \neq p. \qquad (3.8)$$

Le spectre du signal carré génère des raies spectrales à deux fois la fréquence des sous-porteuses (terme ❶de l'équation (3.8)). Afin de réduire au maximum cette signature spectrale, un deuxième niveau de sécurité est ajouté à ce système en insérant de l'aléa à la fréquence porteusef_0, une fois la taille du PC est rendue pseudo-aléatoire conformément au paragraphe précédent. Comme le montre la Figure 3.3, l'insertion de l'aléa est réalisée en ajoutant une nouvelle perturbation prédéfinie ε_m à la fréquence de la porteuse f_0 à chaque symbole OFDM (après chaque opération IFFT). Cette perturbation est générée par l'intermédiaire d'un générateur de nombres pseudo-aléatoires alors que la condition initiale (la clé) est connue au récepteur et à l'émetteur. En utilisant cette clé, l'oscillateur local au niveau du récepteur est capable de régénérer la fréquence porteuse correspondante (f_0+ ε_m). Sans aucune connaissance de cette perturbation, la démodulation reste impossible. Le choix

du générateur de nombres pseudo-aléatoires relève du niveau de sécurité requis et la simplicité d'implémentation dans le récepteur et l'émetteur. Son implémentation au niveau de l'émetteur et du récepteur peut inclure, mais sans s'y limiter, l'utilisation d'une unité de chiffrement, un registre à décalage à rétroaction linéaire (LFSR), des méthodes linéaires et non-linéaires ainsi que des générateurs de séquences chaotiques. Une représentation générale de l'ensemble du système OFDM est illustrée dans la Figure 3.3.

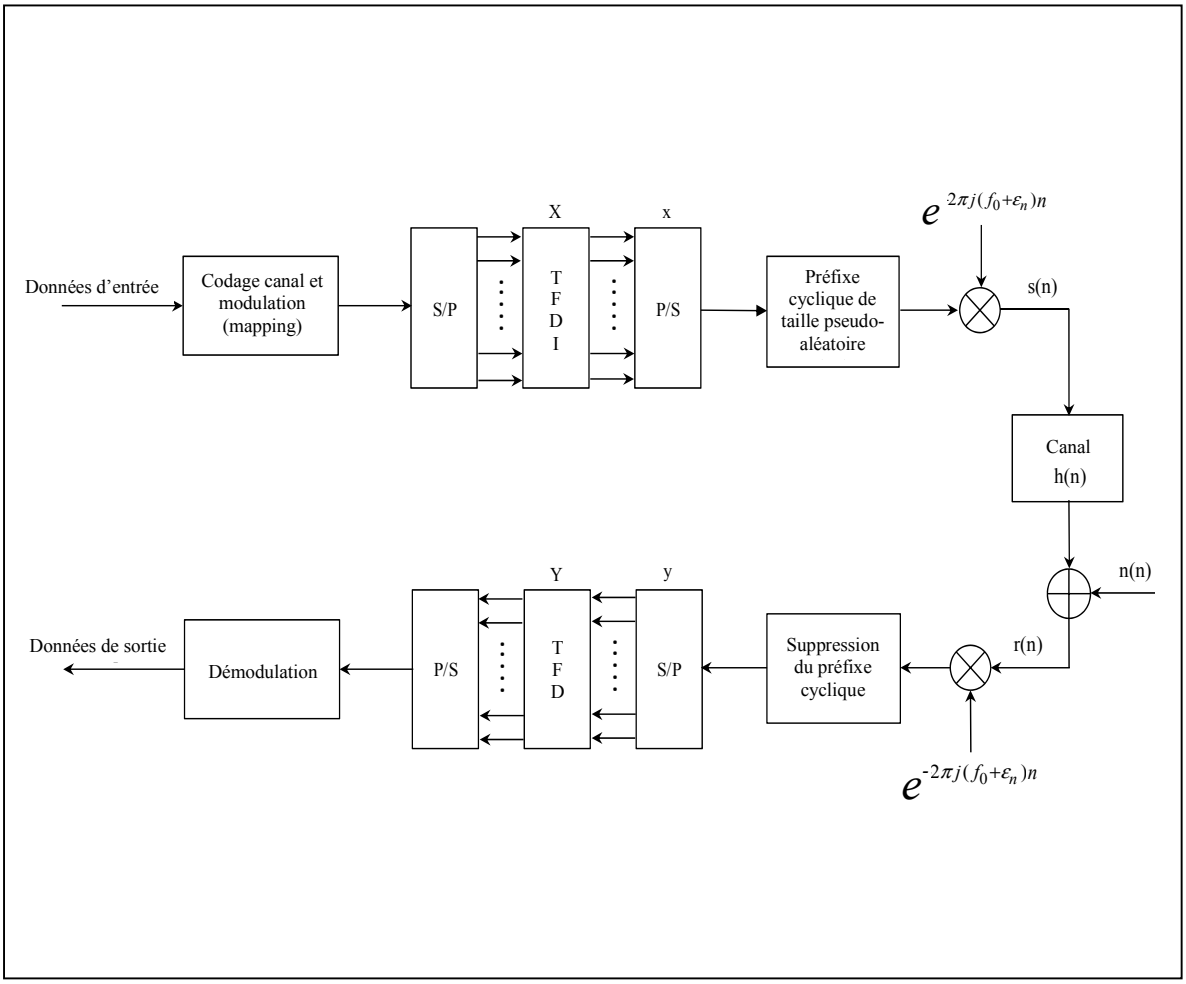


Figure 3.3 Implémentation numérique du système OFDM proposé en bande de base

3.2.3 Analyse des performances sur les canaux sélectifs en fréquence

Dans cette section, la probabilité d'erreur par symbole (PES) du système proposé est évaluée, et ce en présence d'un canal Rayleigh sélectif en fréquence et un bruit blanc gaussien additif. Pour cela, nous utilisons le modèle en bande de base du signal OFDM proposé, donné par :

$$s(n) = \frac{1}{N} \sum_{m=-\infty}^{+\infty} e^{\frac{j2\pi\varepsilon_m n}{N}} \sum_{k=0}^{N-1} x_{k,m} e^{\frac{j2\pi k\left(n-N_{cp}^{m}-\alpha_m\right)}{N}} g_m(n-\alpha_m). \quad (3.9)$$

Il est supposé que l'émetteur et le récepteur sont parfaitement synchronisés. Le canal est aussi suffisamment lent pour être considéré constant sur un symbole OFDM. En outre, aucune interférence inter-symbole, IIS, n'est subite telle que le coefficient canal $h(\eta)$ soit nul pour $\eta < 0$ et $\eta > N_{cp}^{min}$. Sur la base de ces hypothèses, il est possible d'écrire :

$$r(n) = \sum_{\eta=0}^{N_{cp}^{min}-1} h(\eta)s(n-\eta) + n(n)\,, \quad (3.10)$$

où $h(\eta)$ et $n(n)$ sont des variables aléatoires complexes gaussiennes i.i.d, de moyennes nulles et de variances σ_h^2 et N_0, respectivement. Après avoir enlevé les préfixes cycliques du côté récepteur, les signaux résultants peuvent être interprétés comme étant des vecteurs ayant la structure suivante :

$$\mathbf{r_m} = \left[r(\alpha_m + N_{cp}^{m}) \quad r(\alpha_m + N_{cp}^{m} + 1) \quad \ldots \quad r(\alpha_m + N_{cp}^{m} + N - 1)\right]^T. \quad (3.11)$$

Après avoir effectué une transformée de Fourier discrète DFT à N points sur le vecteur $\mathbf{r_m}$ duquel la fréquence de perturbation a été soustraite, le symbole reçu $y_{k,m}$ peut être exprimé tel que :

$$y_{k,m} = \sum_{n=0}^{N-1} r\left(\alpha_m + N_{cp}^m + n\right) e^{-\frac{j2\pi(k+\varepsilon_m)n}{N}} + \sum_{n=0}^{N-1} n(\alpha_m + N_{cp}^m + n)\, e^{-\frac{j2\pi(k+\varepsilon_m)n}{N}}. \quad (3.12)$$

En injectant l'expression (3.10) de $r(n)$ dans l'équation (3.12), nous obtenons l'expression suivante :

$$y_{k,m} = \left(\sum_{n=0}^{N-1} \sum_{k=0}^{N_{cp}^{min}-1} h(\eta) \frac{1}{N} \sum_{\eta=0}^{N-1} x_{k,m} e^{j2\pi(k+\varepsilon_m)\frac{(n-\eta)}{N}}\right) e^{-\frac{j2\pi(k+\varepsilon_m)n}{N}} + n_{k,m}, \quad (3.13)$$

où $n_{k,m} = \sum_{n=0}^{N_{cp}^{min}-1} n\left(\alpha_m + N_{cp}^m + n\right) e^{-\frac{j2\pi(k+\varepsilon_m)n}{N}}$, est le $k^{\text{ième}}$ échantillon de la DFT de $n(\alpha_m + N_{cp}^m + n)e^{-j2\pi\varepsilon_m\frac{n}{N}}$. Étant donné que $n(n)$ est un bruit blanc gaussien, $n_{k,m}$ est également un bruit blanc gaussien. Puisque$h(\eta) = 0$ pour $> N_{cp}^{min}$, il est possible d'étendre son support de [0 N_{cp}^{min}] à [0 N]. Par ailleurs, en simplifiant les termes $e^{\frac{j2\pi\varepsilon_m n}{N}}$ et $e^{-\frac{j2\pi\varepsilon_m n}{N}}$ dans les deux sommes extérieures dans (3.13), nous pouvons obtenir :

$$y_{k,m} = \underbrace{\sum_{n=0}^{N-1} \underbrace{\left(\frac{1}{N} \sum_{k=0}^{N-1} \left(\sum_{\eta=0}^{N-1} \left(h(\eta) e^{-\frac{j2\pi\varepsilon_m\eta}{N}}\right) e^{-\frac{j2\pi k\eta}{N}}\right) x_{k,m} e^{\frac{j2\pi kn}{N}}\right)}_{\text{TFDI}} e^{-\frac{j2\pi kn}{N}}}_{\text{TFD}} + n_{k,m}. \quad (3.14)$$

La première partie de cette expression consiste en une opération TFDI imbriquée dans une opération de TFD. Toutefois, la somme intérieure présente le $k^{\text{ième}}$ échantillon $h_k^{\varepsilon_m}$ d'une TFD à N points du terme $h(\eta)e^{-\frac{j2\pi\varepsilon_m\eta}{N}}$. Ainsi, l'équation (3.14) peut être simplifiée :

$$y_{k,m} = h_k^{\varepsilon_m} x_{k,m} + n_{k,m} . \tag{3.15}$$

Les symboles émis sont ensuite estimés en utilisant un égaliseur. L'égaliseur divise le symbole reçu $y_{k,m}$ par son coefficient de canal correspondant$h_k^{\varepsilon_m}$. L'équation (3.15) montre que le système OFDM proposé est équivalent à une transmission de données sur un ensemble de canaux parallèles semblablement aux systèmes OFDM classiques. Par conséquent, en termes de PES, le système proposé est équivalent à une modulation *M*-QAM sur un canal Rayleigh à évanouissement plat. Dans [28], la PES est donnée par

$$P_s = 2\left(1 - \frac{1}{\sqrt{M}}\right)\left(1 - \sqrt{\frac{g\,\gamma}{1+g\,\gamma}}\right) + \left(1 - \frac{1}{\sqrt{M}}\right)^2 \times \left[\frac{4}{\pi}\sqrt{\frac{g\,\gamma}{1+g\,\gamma}}\,arctan\left(\frac{g\,\gamma}{1+g\,\gamma}\right) - 1\right], \tag{3.16}$$

où $g = \frac{3}{2}(M-1)$ et γ est le rapport signal à bruit.

3.3 Résultats de simulation

Dans ce paragraphe, nous montrons que l'onde OFDM conçue possède une faible probabilité d'interception grâce à l'utilisation des deux techniques proposées. En outre, nous fournissons des résultats de simulation démontrant la performance du système en termes de taux d'erreur binaire (TEB). A cet effet, nous considérons la norme IEEE 802.11a pour l'établissement des résultats de simulation. Dans ce système, 64 sous-porteuses sont utilisées, 11 d'entre elles sont utilisées comme sous-porteuses de garde, la sous-porteuse centrale est de type DC, alors que les 52 restantes sont dédiées au transport des données. Le spectre de transmission alloué

est de 20 MHz. Une modulation BPSK est utilisée pour chaque sous-porteuse. Le taux d'erreur binaire et la probabilité d'erreur symbole sont ainsi identiques.

3.3.1 Suppression des propriétés cyclique et spectrale

Dans un scénario non-bruité, nous traçons le spectre du signal OFDM élevé au carré afin de montrer que la signature spectrale est masquée. En outre, la FAC est établie pour illustrer la suppression des caractéristiques cycliques.

La première technique présentée dans le paragraphe 3.2.1 est simulée en changeant la taille de préfixe cyclique d'une manière pseudo-aléatoire parmi l'ensemble des dimensions suivantes {8, 10, 12, 14, 16 échantillons}. Ces dernières valeurs sont considérées comme équiprobables. La Figure 3.5 montre que les pics des fréquences cycliques sont clairement atténués en comparaison avec ceux obtenus dans les systèmes OFDM classiques dans la Figure 3.4. Par conséquent, la probabilité d'interception de la forme d'onde OFDM proposée est faible étant donné que l'extraction des paramètres de transmission demeure difficile.

Après avoir appliqué la technique d'insertion d'aléa au PC, une perturbation pseudo-aléatoire ε_m est rajoutée à la fréquence porteuse. Dans ce cas, ε_m appartient à {-15/64, -30/64, 0, 15/64, 30/64}. La Figure 3.6 trace les caractéristiques spectrales d'un système OFDM classique. Les raies spectrales pourraient facilement être exploitées afin de se synchroniser au signal OFDM. Cependant, une fois la perturbation de fréquence aléatoire est introduite, les raies spectrales sont affaiblies (*Voir* Figure 3.7).

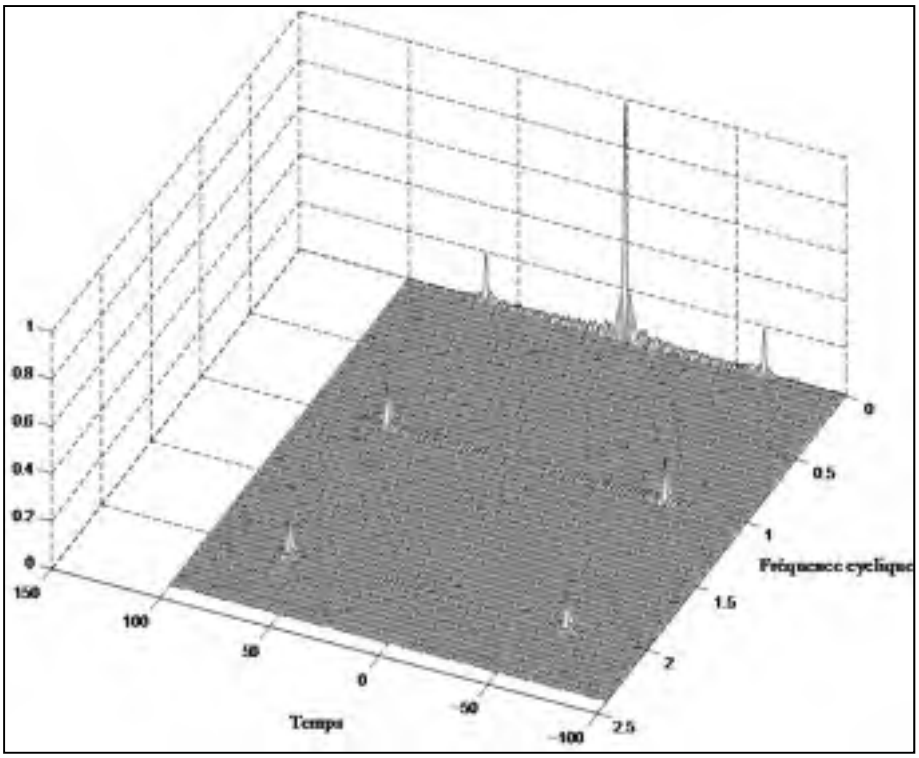


Figure 3.4 Fonction d'autocorrélation d'un système OFDM classique (IEEE 802.11)

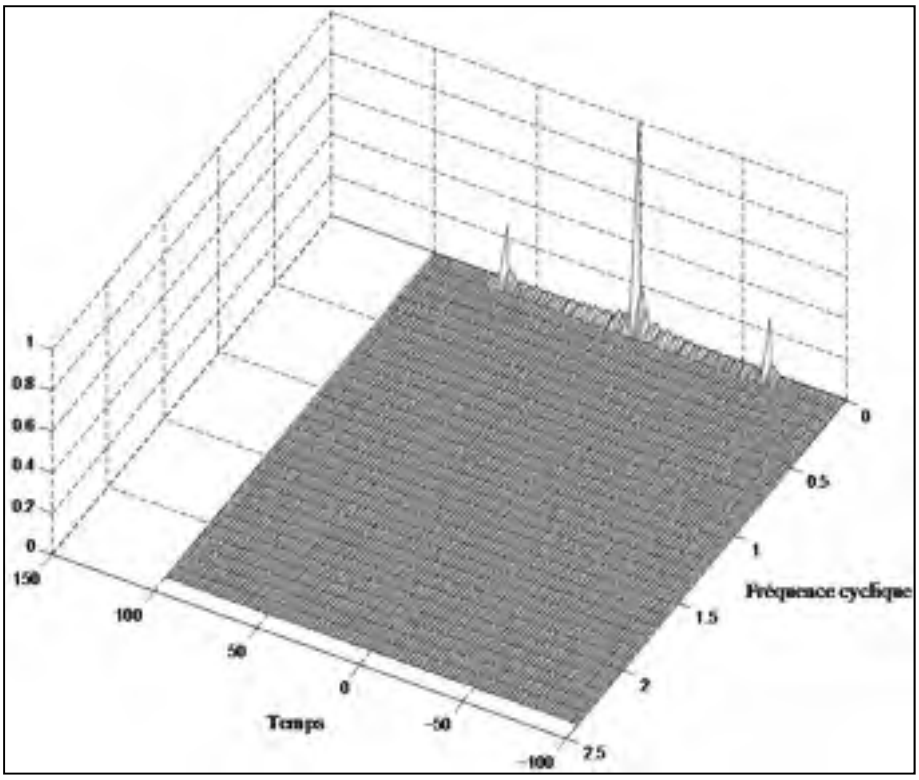


Figure 3.5 Fonction d'autocorrélation du système OFDM proposé

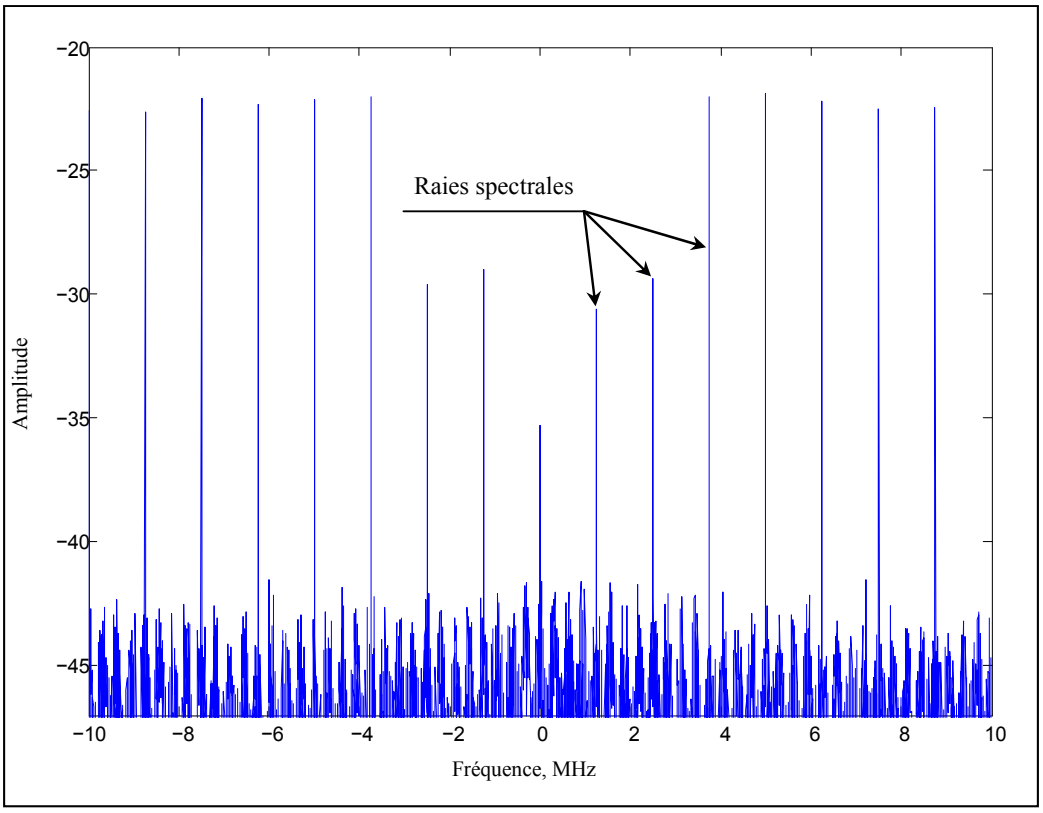


Figure 3.6 Spectre d'un signal OFDM classique élevé au carré

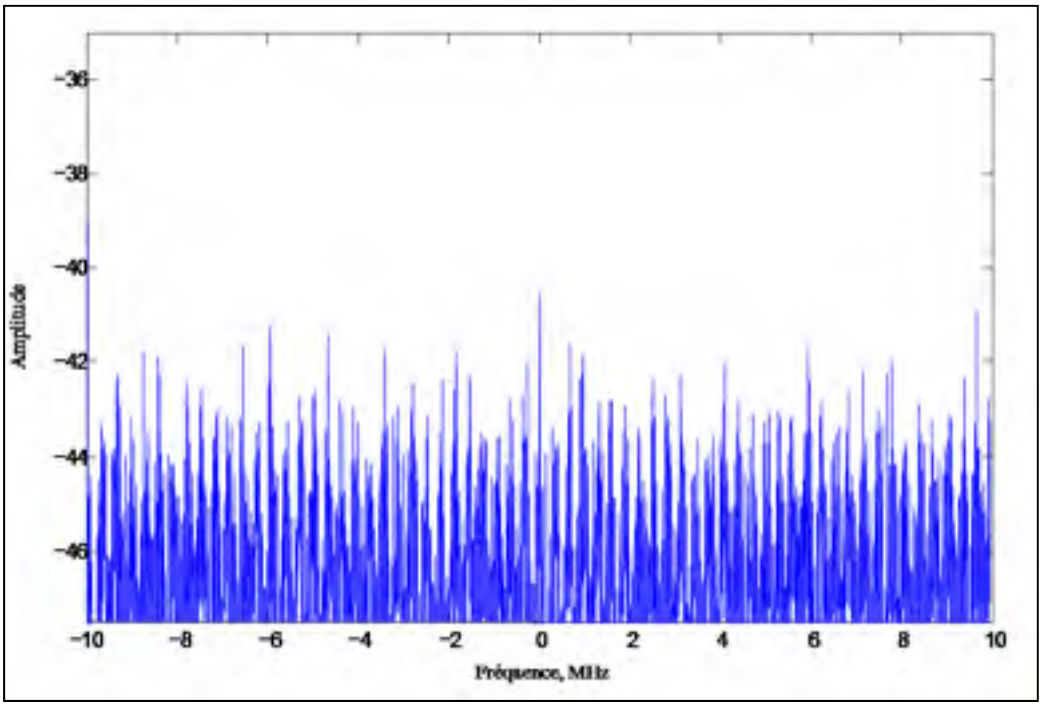


Figure 3.7 Spectre du signal OFDM proposé élevé au carré

3.3.2 Taux d'erreur binaire

Dans ce paragraphe, nous considérons un canal Rayleigh à trajets multiples avec un nombre de trajets N_{tap} variant entre $N_{cp}^{min} = 8$ et $N_{cp}^{max} = 16$ selon différents scénarios de simulation. Nous évaluons la robustesse du système proposé contre l'IIS causée par le fait que l'étalement temporel du canal soit supérieur à la taille minimale du préfixe cyclique N_{cp}^{min}. Dans la Figure 3.8, nous traçons le TEB pour $N_{tap} = 8$. Ce cas ne présente aucun IIS et une bonne concordance entre les courbes théoriques et celles de simulation est constatée. Dans la même figure, pour des longueurs de réponse impulsionnelle du canal qui dépassent N_{cp}^{min}, avec $N_{tap} = 12$ et $N_{tap} = 14$, une dégradation des performances en termes de TEB est remarquée en raison de la présence de l'IIS. Cependant, pour un nombre de trajets $N_{tap} = 12$ à titre d'exemple, le système proposé surpasse les systèmes OFDM classique (avec la taille du PC fixée à 8) en termes de TEB. Cela est dû au fait que le nombre d'occurrences d'IIS dans notre système est faible puisque le PC est de taille variable. En revanche, si la taille du PC est fixe, l'IIS se produit en permanence dans chaque symbole OFDM, ce qui explique une dégradation des performances du système OFDM classique en termes de TEB.

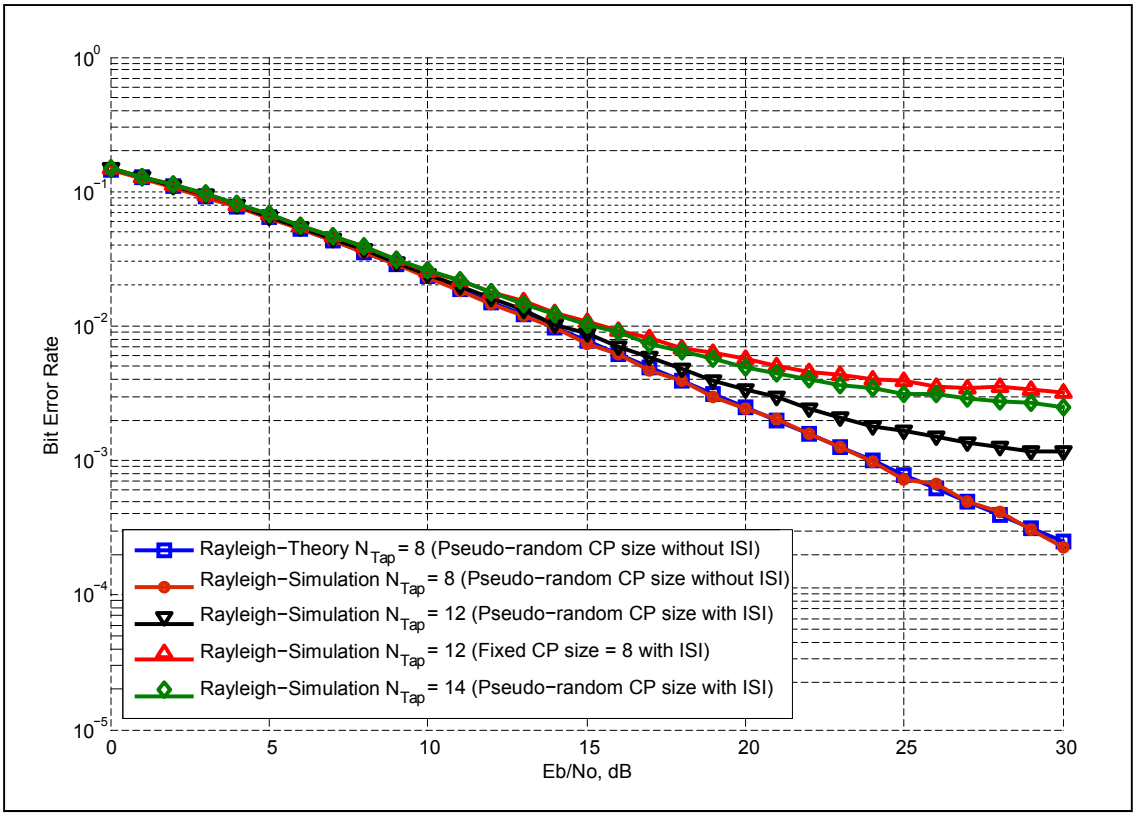


Figure 3.8 Courbes de BER en fonction de la longueur de l'étalement temporel du canal

3.4 Conclusion

Dans ce chapitre, nous avons présenté un nouveau design d'un système OFDM sécurisé. Dans le système proposé, le symbole OFDM utilise une taille pseudo-aléatoire du préfixe cyclique pour réduire les propriétés cyclostationnaires. Afin d'ajouter un niveau de sécurité supplémentaire, une nouvelle perturbation aléatoire est ajoutée à la fréquence porteuse de chaque symbole OFDM. Les fonctions génératrices du préfixe cyclique et de la perturbation fréquentielle aléatoires sont connues à la fois au niveau de l'émetteur ainsi que le récepteur. Enfin, ce nouveau système proposé augmente la sécurité de la couche physique en réduisant considérablement la probabilité d'interception du signal OFDM avec un impact limité sur l'efficacité spectrale qui sont affectés par la taille variable du préfixe cyclique. Cependant, de bonnes performances de l'onde OFDM conçue sont assurées sur les canaux Rayleigh à trajets multiples.

CHAPITRE 4

ANALYSE SPECTRALE DE L'ONDE OFDM À PRÉFIXE CYCLIQUE ALÉATOIRE

4.1 Introduction

La modulation OFDM classique a été largement étudiée dans la littérature. Dans ce contexte, des analyses théoriques complètes ont été accomplies et les expressions exactes des moments du second ordre statistiques ont été développées. Toutefois, de récentes recherches ont proposé de nouvelles variantes de modulation OFDM. Dans le but d'établir une communication sécurisée, le chapitre précédent propose une technique faisant varier aléatoirement la taille du préfixe cyclique à chaque symbole OFDM afin d'atténuer la signature cyclostationnaire du signal OFDM transmis. Cette approche vise essentiellement à empêcher le processus de synchronisation aux utilisateurs indésirables.

La technique de modulation OFDM à préfixe cyclique pseudo-aléatoire souffre d'une faible base théorique de sorte que, au meilleur de nos connaissances, aucune expression de la Fonction du Moment de Second Ordre (FMSO) [29, chap.3] et de la Densité Spectrale de Puissance (DSP), n'a été développée jusqu'à présent. Le présent chapitre expose les expressions exactes de la FMSO et la DSP du signal OFDM à préfixe cyclique aléatoire. Les expressions dérivées sont valables pour n'importe quelle forme d'impulsion et n'importe quelle distribution aléatoire de la taille du préfixe cyclique. À titre d'exemple, une forme d'impulsion rectangulaire est envisagée afin de valider les expressions dérivées. Dans ce cadre, nous sommes tout d'abord menés à étudier les signaux numériques QAM et PSK à durée d'impulsion aléatoire.

4.2 Moments de second ordre des signaux QAM et PSK à durée d'impulsion aléatoire

Afin de dériver les nouvelles expressions FMSO et DSP des signaux QAM et PSK à durées d'impulsions aléatoires, nous procédons d'une manière similaire à [29, sec. 4.4] où un train de pulses réels de durées aléatoires a été envisagé. Dans le présent chapitre, une généralisation du travail [29, sec. 4.4] est effectuée en traitant des signaux modulés complexes ayant des constellations de type QAM et PSK.

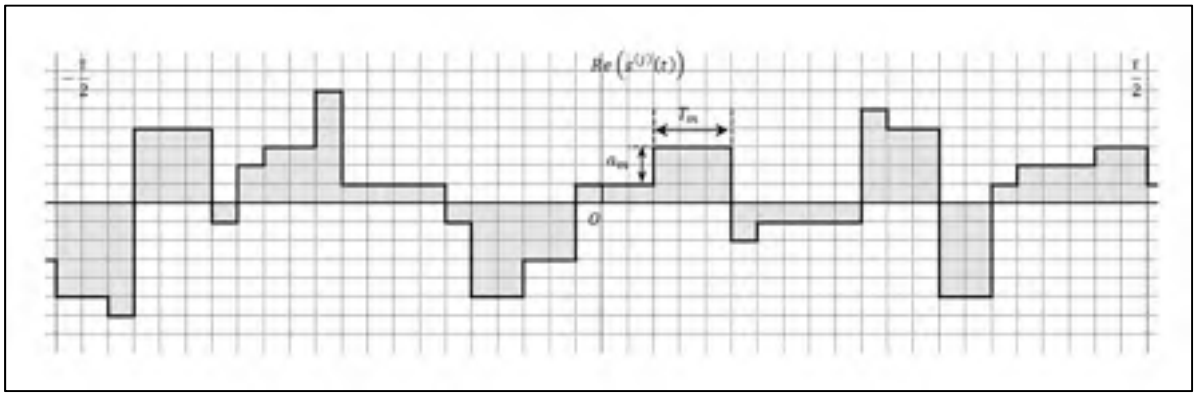


Figure 4.1 Signal à modulation d'amplitude à durée d'impulsion aléatoire

Considérons un signal *M*-aire en bande de base$s(t)$où$M \geq 2$. $s(t)$ peut être considéré comme un processus aléatoire constitué d'un ensemble de fonctions de temps $s^{(j)}(t),\ j \in N,$ appelées représentations statistiques. Soits$_N^{(j)}(t)$ une représentation tronquée de $s(t)$ (*Voir* Figure 4.1), dans l'intervalle $[-\frac{\tau^{(j)}}{2}, \frac{\tau^{(j)}}{2}]$, donnée par

$$s_N^{(j)}(t) = \sum_{m=-N}^{N} c_m^{(j)} g\left(t - \alpha_m^{(j)}\ ;\ T_m^{(j)}\right), \tag{4.1}$$

contenant exactement $2N + 1$ impulsions, où $g(t - \alpha_m\ ;\ T_m)$ est la forme caractéristique de l'impulsion avec $g_{max} = 1$, $\left\{c_m^{(j)}\right\}$ une séquence de symboles appartenant à une constellation QAM ou PSK, $T_m^{(j)}$ la durée de l'impulsion et $\alpha_m^{(j)}$ une époque qui marque le début de

l'impulsion. $T_m^{(j)}$, $\alpha_m^{(j)}$ appartiennent à des suites aléatoires réels. De plus, nous supposons que $T_m^{(j)}$et$c_m^{(j)}$ sont stationnaires. Soit :

$$g\left(t-\alpha_m^{(j)}\,;\,T_m^{(j)}\right)=\mathcal{F}^{-1}\left\{S_g^{(j)}\right\} \tag{4.2}$$
$$=\int_{-\infty}^{+\infty}S_g^{(j)}\left(f,T_m^{(j)}\right)e^{j2\pi f\left(t-\alpha_m^{(j)}\right)}df$$
$$=\begin{cases} g\left(t\,;\,T_m^{(j)}\right), & \alpha_m^{(j)}<t<\alpha_{m+1}^{(j)} \\ 0,\text{ailleurs.} \end{cases}$$

où $S_g^{(j)}$est la densité spectrale de l'impulsion $g(t)$. $\mathcal{F}(.)$ représente la fonction transformée de Fourier et $\mathcal{F}^{-1}(.)$ sa fonction inverse. Les durées$T_m$sont liées aux époques aléatoires par $T_m=\alpha_{m+1}-\alpha_m$. En outre, $T_m$est caractérisée par la densité de probabilité $w_\tau(T_m)$ pour tous les intervalles de durée moyenne $[-\frac{\tau}{2},\frac{\tau}{2}]$ à l'extérieur desquelles w_τ disparaît et contenant exactement $2N+1$ pulses. La fonction d'autocorrélation du signal de $s_N^{(j)}(t)$ est alors donnée par :

$$\mathcal{R}_{s^{(j)}}(t)=\lim_{\tau\to+\infty}\frac{1}{2\,\tau}\int_{-\tau/2}^{+\tau/2}s_N^{(j)}(t_0)s_N^{(j)^*}(t_0+t)dt_0 \tag{4.3}$$
$$=\lim_{\tau\to+\infty}\frac{1}{2\,\tau}\int_{-\infty}^{+\infty}s_N^{(j)}(t_0)s_N^{(j)^*}(t_0+t)dt_0.$$

L'opération d'intégration dans (4.3) a été étendue sur $[-\infty,+\infty]$ étant donné que $s_N^{(j)}(t)$ est nulle en dehors de $[-\tau/2\,,\tau/2]$. Une autre expression de $\mathcal{R}_{s^{(j)}}(t)$ peut être représentée en exprimant la période moyenne τ en fonction de la durée d'impulsion moyenne $\overline{T}$: une durée infinitésimale du signal tronqué $s_N^{(j)}(t)$ entre T et $T+dT$, contient $(2N+1)w_\tau(T)$ impulsions. Par conséquent, la contribution de toutes les impulsions entre T et $T+dT$ en termes de longueur est $(2N+1)Tw_\tau(T)$. La durée moyenne τ peut alors être exprimée par :

$$\tau=(2N+1)\int_0^{+\infty}Tw_\tau(T)dT \tag{4.4}$$
$$=\ (2N+1)\overline{T_\tau}=(2N+1)\overline{T}+0\left(\overline{T}\right),$$

où $\overline{T} = \lim_{\tau \to +\infty} \overline{T_\tau}$,$\mathrm{O}(\overline{T})$ est un reste et $\overline{(.)}$ désigne l'opérateur de moyenne statistique. Nous supposons aussi que $\lim_{\tau^{(j)} \to +\infty} \tau^{(j)} = \lim_{\tau \to +\infty} \tau = \lim_{N \to +\infty} (2N+1)\overline{T}$. Par conséquent, en remplaçant τ par son expression et en injectant l'équation de $s_N^{(j)}(t)$ dans (4.3), il en résulte que :

$$\mathcal{R}_{s^{(j)}}(t) = \lim_{N \to +\infty} \left\{ \frac{1}{(2N+1)2\overline{T}} \sum_{m,n=-N}^{N} c_m^{(j)} \, c_n^{(j)^*} \times \int_{-\infty}^{+\infty} g\left(t_0 - \alpha_m^{(j)} \, ; \, T_m^{(j)}\right) g\left(t_0 + t - \alpha_n^{(j)} \, ; \, T_n^{(j)}\right) dt \; + \; \mathrm{O}\left(\frac{1}{N}\right) \right\}. \tag{4.5}$$

En utilisant le théorème de convolution, énonçant que la transformée de Fourier d'une convolution est le produit des transformées de Fourier, $\mathcal{R}_{s^{(j)}}(t)$ peut être donné par :

$$\mathcal{R}_{s^{(j)}}(t) = \lim_{N \to +\infty} \left\{ \frac{1}{(2N+1)2\overline{T}} \sum_{m,n=-N}^{N} \int_{-\infty}^{+\infty} c_m^{(j)} c_n^{(j)^*} e^{j2\pi f(\alpha_n^{(j)} - \alpha_m^{(j)})} \times S_g^{(j)}\left(f, T_m^{(j)}\right) S_g^{(j)}\left(f, T_n^{(j)}\right)^* e^{-j2\pi f t} df \right\}. \tag{4.6}$$

Soit $n - m = k$. Étant donné que $c_{m,n}^{(j)} = 0$ pour $|m|, |n| > N$, la double série de (4.6) peut être ainsi reformulée comme :

$$\sum_{k=-\infty}^{+\infty} \sum_{m=-N}^{N} \int_{-\infty}^{+\infty} \left\{ c_m^{(j)} {c_{m+k}^{(j)}}^* e^{j2\pi f(\alpha_{m+k}^{(j)} - \alpha_m^{(j)})} S_g^{(j)}\left(f, T_m^{(j)}\right) S_g^{(j)}\left(f, T_{m+k}^{(j)}\right)^* e^{-j2\pi f t} df \right\}. \tag{4.7}$$

La fonction d'autocorrélation d'une représentation particulière *j* est alors donnée par :

$$\mathcal{R}_{s^{(j)}}(t) = \frac{1}{2\overline{T}} \sum_{k=-\infty}^{\infty} \int_{-\infty}^{+\infty} \mathcal{R}_c^{(j)}(k, f) e^{-j2\pi f t} df \, , \tag{4.8}$$

où le coefficient d'autocorrélation $\mathcal{R}_c^{(j)}(k,f)$ est donné par :

$$\mathcal{R}_c^{(j)}(k,f) = \lim_{N\to+\infty} \frac{1}{2(2N+1)} \times \sum_{m=-N}^{N} c_m^{(j)} {c_{m+k}^{(j)}}^{*} S_g^{(j)}\left(f, T_m^{(j)}\right) S_g^{(j)}\left(f, T_{m+k}^{(j)}\right)^{*} e^{j2\pi f(\alpha_{m+k}^{(j)} - \alpha_m^{(j)})}. \quad (4.9)$$

Soit $\mathcal{M}_s(t)$ la fonction du moment de second ordre défini dans le cas des processus stationnaires comme $\mathcal{M}_S(t) = \mathcal{M}_S(t_1,t_2) \triangleq E\{s(t_1)s(t_2)^*\} = \overline{s(t_1)s(t_2)^*}$ où$t = t_1 - t_2$. En appliquant la moyenne statistique des deux côtés de (4.9) et en rappelant l'hypothèse de stationnarité du $T_m^{(j)}$et $c_m^{(j)}$ de telle sorte que $\overline{\mathcal{R}_{s^{(j)}}}(t) = \mathcal{M}_s(t)$ démontré à l'annexe I, il est possible d'écrire :

$$\mathcal{M}_s(t) = \frac{1}{2\overline{T}} \times \sum_{-\infty}^{\infty} \int_{-\infty}^{+\infty} E\left\{c_1 {c_2}^{*} S_g(f,T_1) S_g(f,T_2)^{*} e^{j2\pi f(\alpha_2-\alpha_1)}\right\}_k e^{j2\pi ft} df\,, \quad (4.10)$$

où les indices 1 et 2 se rapportent aux temps$t_1$andt_2 séparés par *k* impulsions successives de durées aléatoires et $E\{.\}_k = E\{.\}_{-k}$. Prenons le cas où T_m et c_m sont statistiquement indépendantes d'une impulsion à l'autre. Pour $c_m = a_m + jb_m$, où a_m et b_m sont deux processus aléatoires conjointement stationnaires, on peut écrire que :

$$\mathcal{M}_s(t) = \frac{1}{2}\left\{\mathcal{M}_a(t) + \mathcal{M}_b(t) + j\left(\mathcal{M}_{ba}(t) - \mathcal{M}_{ab}(t)\right)\right\}, \quad (4.11)$$

où

$$\mathcal{M}_a(t) \triangleq \frac{1}{2\overline{T}} \sum_{-\infty}^{\infty} \int_{-\infty}^{+\infty} E\left\{a_1 a_2 S_g(f,T_1) S_g(f,T_2)^{*} e^{j2\pi f(\alpha_2-\alpha_1)}\right\}_k e^{j2\pi ft} df, \quad (4.12)$$

$$\mathcal{M}_b(t) \triangleq \frac{1}{2\overline{T}} \sum_{-\infty}^{\infty} \int_{-\infty}^{+\infty} E\left\{b_1 b_2 S_g(f,T_1) S_g(f,T_2)^{*} e^{j2\pi f(\alpha_2-\alpha_1)}\right\}_k e^{j2\pi ft} df\,, \quad (4.13)$$

$$\mathcal{M}_{ba}(t) \triangleq \frac{1}{2\overline{\overline{T}}} \sum_{-\infty}^{\infty} \int_{-\infty}^{+\infty} E\left\{b_1 a_2 S_g(f,T_1) S_g(f,T_2)^* e^{j2\pi f(\alpha_2-\alpha_1)}\right\}_k e^{j2\pi ft} df, \quad (4.14)$$

$$\mathcal{M}_{ab}(t) \triangleq \frac{1}{2\overline{\overline{T}}} \sum_{-\infty}^{\infty} \int_{-\infty}^{+\infty} E\left\{a_1 b_2 S_g(f,T_1) S_g(f,T_2)^* e^{j2\pi f(\alpha_2-\alpha_1)}\right\}_k e^{j2\pi ft} df, \quad (4.15)$$

$\mathcal{M}_{ba}(t)$ et $\mathcal{M}_{ab}(t)$ sont les FMSO conjointes des composantes en quadrature a_m et b_m. En supposant que a_m et b_m sont statistiquement indépendants, nous pouvons dériver que $\mathcal{M}_{ba}(t) = \mathcal{M}_{ab}(t)$. En outre, si a_m et b_m appartiennent au même alphabet, alors $\mathcal{M}_a(t) = \mathcal{M}_b(t)$. Par conséquent :

$$\mathcal{M}_s(t) = \mathcal{M}_a(t). \quad (4.16)$$

De (4.16), le problème est ainsi équivalent au calcul des statistiques de second ordre d'un signal réel. En utilisant le théorème de Wiener-Khintchine [15], l'expression de la DSP est alors donnée par :

$$\begin{aligned} \mathcal{W}_s(f) &\triangleq \mathcal{F}\{\mathcal{M}_s(t)\} = \mathcal{F}\{\mathcal{M}_a(t)\} \\ &= \frac{1}{\overline{\overline{T}}} \sum_{k=-\infty}^{\infty} E\left\{a_1 a_2 S_g(f,T_1) S_g(f,T_2)^* e^{j2\pi f(\alpha_2-\alpha_1)}\right\}_k. \end{aligned} \quad (4.17)$$

D'autre part, soit :

$$\begin{cases} \gamma_m(f) = S_g(f,T_m) e^{j2\pi f T_m}, \\ \beta_{m+k}(f) = S_g(f,T_{m+k}), \\ \mathcal{Z}(f) = e^{j2\pi f T}. \end{cases} \quad (4.18)$$

En exprimant la différence des époques $(\alpha_2 - \alpha_1)_k$ en fonction de la durée de pulse T, nous obtenons :

$$(\alpha_2 - \alpha_1)_k = \alpha_{m+k} - \alpha_m = T_m + \Delta_{m,k}(T), \text{ où } \quad \Delta_{m,k}(\tau) = \begin{cases} \sum_{T=m}^{m+k-1} T_\lambda \ , & k \geq 2 \\ 0 \ , & k = 1 \\ -T_m \ , & k = 0 \\ -\sum_{T=m}^{m+k} T_\lambda \ , & k \leq -1 \end{cases} \tag{4.19}$$

Alors, mis à part le cas particulier $k = 0$, l'espérance mathématique dans (4.17) peut être factorisée en un produit de moyennes statistiques. Par conséquent:

$$\begin{aligned} \mathcal{M}_{S_{k\geq 1}}(t) &= \frac{m^2}{\overline{T}} \sum_{k=1}^{\infty} \int_{-\infty}^{+\infty} \left\{ \overline{\gamma(f)\beta(f)^* \mathcal{Z}(f)}^{k-1} \right\} e^{j2\pi ft} \, df, \\ \mathcal{M}_{S_{k=0}}(t) &= \frac{\overline{a^2}}{\overline{T}} \int_{-\infty}^{+\infty} \left\{ \overline{\gamma(f)\beta(f)^* \mathcal{Z}(f)^{-1}} \right\} e^{j2\pi ft} \, df, \\ \mathcal{M}_{S_{k\leq -1}}(t) &= \frac{m^2}{\overline{T}} \sum_{k=1}^{\infty} \int_{-\infty}^{+\infty} \left\{ \overline{\gamma(f)^* \beta(f) \mathcal{Z}(f)^*}^{k-1} \right\} e^{j2\pi ft} df, \end{aligned} \tag{4.20}$$

où $(.)^*$ désigne le conjugué complexe et $m = \overline{a} = \overline{b}$. En constatant que le cas $\overline{\mathcal{Z}(f)} = 1$ peut contribuer par un terme continu possible pour $f = 0$, la fonction de covariance $\mathcal{K}_s(t)$ de $s(t)$ peut être explicitement donnée après avoir calculé la somme en série géométrique dans (4.20), ainsi :

$$\mathcal{K}_s(t) = \mathcal{M}_s(t) - m^2 \tag{4.21}$$

$$= \frac{m^2}{\overline{T}} \int_{-\infty}^{+\infty} \left\{ \overline{\gamma \beta^* \mathcal{Z}^{-1}} + 2 \, \Re\mathrm{e}\left(\frac{\overline{\gamma}\overline{\beta^*}}{1 - \overline{\mathcal{Z}}} \right) \right\} e^{j2\pi ft} \, df. \tag{4.22}$$

Toutefois, la partie continue de la densité spectrale de puissance est exprimée par :

$$\mathcal{W}_{s-m}(f) = \frac{m^2}{\overline{\tau}}\left\{\overline{\gamma\beta^* Z^{-1}} + 2\,\Re\mathrm{e}\left(\frac{\overline{\gamma}\overline{\beta^*}}{1-\overline{\mathcal{Z}}}\right)\right\}. \tag{4.23}$$

où $\Re\mathrm{e}(.)$ désigne la partie réelle d'un nombre complexe. L'expression de $\mathcal{M}_s(t)$ peut être déduite en rappelant que $\mathcal{M}_s(t) = \mathcal{K}_s(t) + m^2$, alors que l'expression de la DSP, notée $\mathcal{W}_s(f)$, de $s(t)$ peut être conclue en ajoutant le terme $\overline{m}^2\delta(f)$à$\mathcal{W}_{s-m}(f)$. À titre d'exemple, considérons des impulsions de formes rectangulaires tels que $S_g(f, T_m) = \frac{1-e^{-j2\pi fT}}{j2\pi f}$. Ainsi, nous dérivons de (4.23) que :

$$\mathcal{W}_s(f) = \frac{\sigma^2}{\overline{T}}\overline{\{T sinc(fT)\}^2} + m^2\delta(f) \tag{4.24}$$

et

$$\mathcal{M}_s(t) = \frac{\sigma^2}{\overline{T}}\int_{-\infty}^{+\infty}\overline{\{T\, sinc(fT)\}^2}e^{j2\pi ft}\,dt + m^2 \tag{4.25}$$

où $sinc(x)$ représente la fonction $sin(\pi x)/\pi x$ et $\sigma^2 \triangleq \overline{a^2} - m^2 = \overline{b^2} - m^2$. Les équations (4.24) et (4.25) représentent les nouvelles expressions de la DSP et la FMSO du signal QAM, PSK à durée d'impulsions aléatoires, respectivement. Contrairement à [29, Sec. 4.4] où les signaux sont supposés être réels, les expressions proposées traitent plus généralement des signaux QAM, PSK complexes. De (4.24), il est clairement visible que l'expression du spectre du signal à durée d'impulsion aléatoire est constituée de :

- Une partie continue qui est égale au spectre continu classique des signaux modulés PSK et QAM, dans laquelle une moyenne statistique sur la durée de l'impulsion T a été effectuée. Ce terme dépend du spectre de la forme d'impulsion qui est supposé être de forme rectangulaire et de la variance des symboles QAM et PSK.

- Une partie discrète qui consiste en une ligne spectrale unique dont l'intensité est déterminée par m^2.

En outre, on sait que :

$$\mathcal{F}^{-1}\left(T\ sinc^2(\pi fT)\right) = \Lambda\left(\frac{t}{T}\right) \triangleq \begin{cases} 1 - \dfrac{|t|}{T}\ , & |t| \leq T \\ 0 \qquad\ , & |t| > T \end{cases} \tag{4.26}$$

où $\Lambda(.)$ est la fonction triangulaire. Ainsi, pour une forme d'impulsion rectangulaire, l'expression finale de la FMSO des signaux QAM, PSK à durée d'impulsion aléatoire, est donnée par :

$$\mathcal{M}_s(t) = \frac{\sigma^2}{\overline{T}}\overline{T\Lambda(\frac{t}{T})} \ + \ m^2\ . \tag{4.27}$$

À partir de l'équation (4.26), $\mathcal{M}_s(t)$ est constituée d'une fonction triangulaire moyennée à laquelle la quantité constante m^2 est rajoutée.

4.3 Moments de second ordre des signaux OFDM à préfixe cyclique aléatoire

Dans cette section, de nouvelles expressions de la FMSO et la DSP de la modulation OFDM à préfixe cyclique de taille aléatoires ont dérivées. Considérons un signal OFDM $v(t)$ à préfixe cyclique de taille aléatoire tel que présenté dans le chapitre précédent :

$$v(t) = \sqrt{\frac{\mathcal{P}}{\mathcal{N}}} \sum_{m=-\infty}^{+\infty} \sum_{k=0}^{N-1} c_{k,m} e^{\frac{j2\pi k(t - Tcp_m - \alpha_m)}{T_u}} g(t - \alpha_m\ ;\ T_m)\ , \tag{4.28}$$

où $\{c_{k,m}\}$ sont des symboles i.i.d de moyenne nulle et de variance σ_c^2. $\mathcal{N}$ est le nombre de sous-porteuses, $\mathcal{P}$ la puissance par symbole et $g(t - \alpha_m\ ;\ T_m)$ la forme d'impulsion caractéristique ($g_{max} = 1$) d'une durée aléatoire $T_m = T_u + Tcp_m$, appartenant à l'ensemble de durées $\mathcal{D} = \{T_{s_1}, T_{s_2}, \dots, T_{s_\mathcal{L}}\}$ de moyenne $\overline{T_s}$. T_u est la longueur utile du symbole et Tcp_m est la taille aléatoire du préfixe cyclique.

Il est supposé que T_m varie entre T_{s_1} et $T_{s_{\mathcal{L}}}$. De plus, α_m est une époque de temps qui marque le début de la $m^{ième}$ impulsion. La fonction d'autocorrélation de la forme d'onde OFDM est donnée par :

$$\begin{aligned}\mathcal{R}_v(t) &= \lim_{\tau\to+\infty}\frac{1}{\tau}\int_{-\tau/2}^{\tau/2} v(t_0)v^*(t_0+t)dt_0 \\ &= \lim_{\tau\to+\infty}\frac{\mathcal{A}}{\tau}\int_{-\tau/2}^{\tau/2}\sum_m\sum_p\sum_{k=0}^{\mathcal{N}-1}\sum_{l=0}^{\mathcal{N}-1} c_{k,m}c_{l,p}^* \times \\ &\quad g(t_0-\alpha_m\,;\,T_m)g^*\big(t_0+t-\alpha_p\,;\,T_p\big)e^{j2\pi k\frac{(t_0-\alpha_m)}{T_u}}e^{-j2\pi l\frac{(t_0+t-\alpha_p)}{T_u}}dt_0\,,\end{aligned} \tag{4.29}$$

où $\mathcal{A}=\mathcal{P}/\mathcal{N}$. En supposant que T_m and c_m sont des processus stationnaires et en appliquant la moyenne statistique aux deux côtés de l'équation (4.29), on obtient la FMSO du signal OFDM à préfixe cyclique de taille aléatoire :

$$\begin{aligned}\mathcal{M}_v(t) = \lim_{\tau\to+\infty}\frac{\mathcal{A}}{\tau}\int_{-\tau/2}^{\tau/2}\sum_m\sum_p\sum_{k=0}^{\mathcal{N}-1}\sum_{l=0}^{\mathcal{N}-1} E\{c_{k,m}c_{l,p}^*\}\times \\ E\left\{g(t_0-\alpha_m\,;\,T_m)g^*\big(t_0+t-\alpha_p\,;\,T_p\big)e^{j2\pi k\frac{(t_0-\alpha_m)}{T_u}}e^{-j2\pi l\frac{(t_0+t-\alpha_p)}{T_u}}\right\}dt_0.\end{aligned} \tag{4.30}$$

Par ailleurs, supposons que $c_{k,m}$ sont décorrélées de telle sorte que $E\{c_{k,m}c_{l,p}^*\}=0$ pour $m\neq p$ et $k\neq l$, il est possible d'écrire que :

$$\mathcal{M}_v(t) = \tag{4.31}$$

$$\lim_{\tau\to+\infty}\frac{\mathcal{A}}{\tau}\int_{-\tau/2}^{\tau/2}\left(\sum_m\sum_{k=0}^{\mathcal{N}-1}E\{g(t_0-\alpha_m\,;\,T_m)g^*\big(t_0+t-\alpha_p\,;\,T_p\big)\}\,e^{j2\pi k\frac{t}{T_u}}\right)dt_0$$

$$\begin{aligned}&= \lim_{\tau\to+\infty}\frac{\mathcal{A}}{\tau}\times \\ &\quad\sum_{k=0}^{N-1}e^{j2\pi k\frac{t}{T_u}}\int_{-\tau/2}^{\tau/2}\sum_m\sigma_c^2\,E\{g(t_0-\alpha_m\,;\,T_m)g^*(t_0+t-\alpha_m\,;\,T_m)\}\,dt_0\end{aligned} \tag{4.32}$$

Après avoir calculé la série géométrique $\sum_{k=0}^{N-1}e^{j2\pi k\frac{t}{T_u}}$, nous obtenons :

$$\mathcal{M}_v(t) = \mathcal{A}\frac{sin(\frac{\pi\mathcal{N}\tau}{T_u})}{sin(\frac{\pi\tau}{T_u})}e^{j\pi\frac{(\mathcal{N}-1)t}{T_u}} \times \lim_{\tau\to+\infty}\frac{1}{\tau}\int_{-\tau/2}^{\tau/2}\sum_m \sigma_c^2\, E\{g(t_0-\alpha_m\,;\,T_m)g^*(t_0+t-\alpha_m\,;\,T_m)\}\,dt_0 \quad \textbf{(E)} \tag{4.33}$$

Le terme **(E)** dans l'équation (4.33) n'est autre que la FMSO du signal QAM, PSK à durée d'impulsion aléatoire étudié dans la section précédente (*Voir* l'annexe II pour la démonstration). Par conséquent, la FMSO des signaux OFDM à préfixe cyclique de taille aléatoire, est donnée explicitement par :

$$\mathcal{M}_v(t) = \frac{\mathcal{A}\,\sigma_c^2}{\overline{T_s}}\frac{sin(\frac{\pi\mathcal{N}t}{T_u})}{sin(\frac{\pi t}{T_u})}\overline{T\Lambda(\frac{t}{T})}e^{j\pi\frac{(\mathcal{N}-1)t}{T_u}} \tag{4.34}$$

où $\overline{T\Lambda(t/T)}$ peut être considérée comme étant l'enveloppe de la FMSO. En appliquant la transformée de Fourier de (4.34), la fonction DSP peut être exprimée par :

$$\mathcal{W}_v(f) = \mathcal{W}_s(f) \otimes \mathcal{F}\left(\sum_{k=0}^{\mathcal{N}-1} e^{j2\pi k\frac{t}{T_u}}\right) \tag{4.35}$$

Par conséquent,

$$\mathcal{W}_v(f) = \sum_{k=0}^{\mathcal{N}-1} W_s\left(f-\frac{k}{T_u}\right) \tag{4.36}$$

où $\otimes$ désigne l'opérateur de convolution. Une autre expression de la DSP peut être présentée par l'introduction de la fonction $sinc$, de sorte que :

$$\mathcal{W}_v(f) = \frac{\mathcal{A}\,\sigma_c^2}{\overline{T_s}}\sum_{k=0}^{\mathcal{N}-1}\overline{\left\{T\,sinc\left(\left(f-\frac{k}{T_u}\right)T\right)\right\}^2} \tag{4.37}$$

Cette dernière expression de la DSP du signal OFDM à préfixe cyclique de taille aléatoire dans (4.37) consiste en une forme moyennée de la DSP d'un signal OFDM classique établie dans [30].

Considérons maintenant que le la durée symbole T_m obéit à une loi uniforme discrète $\mathcal{P}r(T_m) = 1/\mathcal{L}$, où $\mathcal{L}$ désigne la taille de l'ensemble $\mathcal{D}$. Par conséquent, les expressions finales des moments de second ordre du signal OFDM à préfixe cyclique de taille aléatoire s'écrivent comme suit :

$$\mathcal{M}_v(t) = \frac{\mathcal{A}\ \sigma_c^2}{\mathcal{L}\ \overline{T_s}} \frac{sin(\frac{\pi \mathcal{N} t}{T_u})}{sin(\frac{\pi t}{T_u})} \left\{ \sum_{l=1}^{\mathcal{L}} T_{s_l}\ \Lambda(\frac{t}{T_{s_l}}) \right\} e^{j\pi \frac{(\mathcal{N}-1)t}{T_u}} \tag{4.38}$$

et

$$\mathcal{W}_v(f) = \frac{\mathcal{A}\ \sigma_c^2}{\mathcal{L}\ \overline{T_s}} \sum_{l=1}^{\mathcal{L}} \sum_{k=0}^{\mathcal{N}-1} \left\{ T_{s_l}\ sinc\left(\left(f - \frac{k}{T_u} \right) T_{s_l} \right) \right\}^2 \tag{4.39}$$

4.4 Validation des expressions de FMSO et DSP des signaux OFDM à préfixe cyclique aléatoire

Dans cette section, les nouvelles expressions dérivées de la FMSO et la DSP du signal OFDM à préfixe cyclique de taille aléatoire, sont validées. À cet effet, nous considérons les paramètres de la norme IEEE 802.11a [31] pour l'élaboration des résultats d'analyse et de simulation. Ce système présente $\mathcal{N}$= 64 sous-porteuses. Le spectre de transmission alloué est de 20 MHz et une modulation 16-QAM est utilisée sur chaque sous-porteuse. La taille du préfixe cyclique varie d'une façon aléatoire dans l'ensemble suivant $\mathcal{D} =$ {8, 11, 13, 16 échantillons} à chaque symbole OFDM.

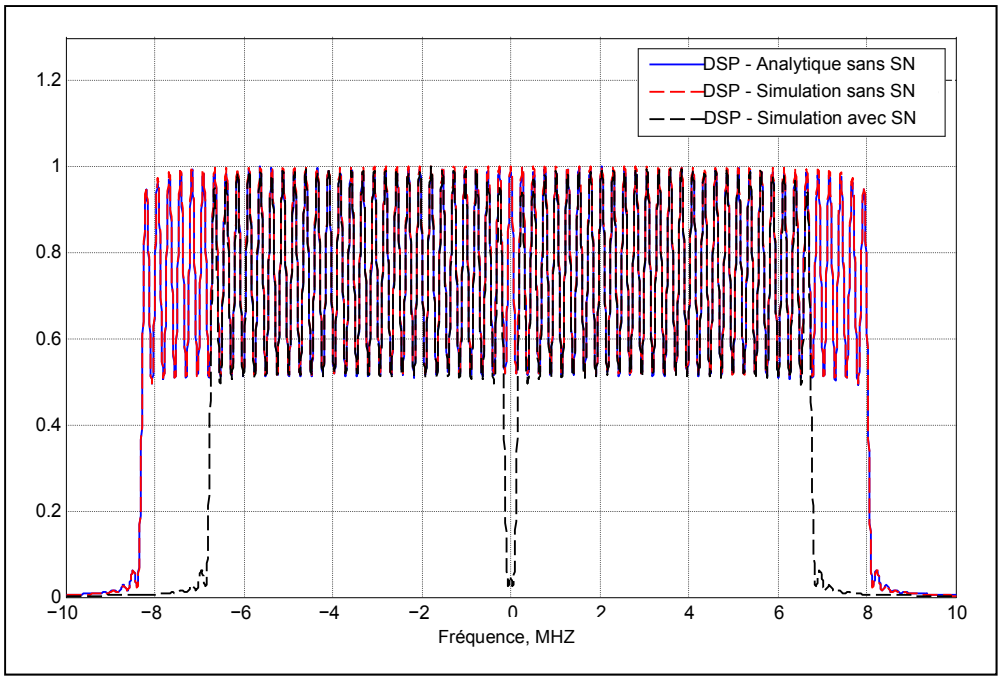


Figure 4.2 Courbes de DSP selon la norme IEEE 802.11 avec et sans SN (SN : Sous-porteuse nulles)

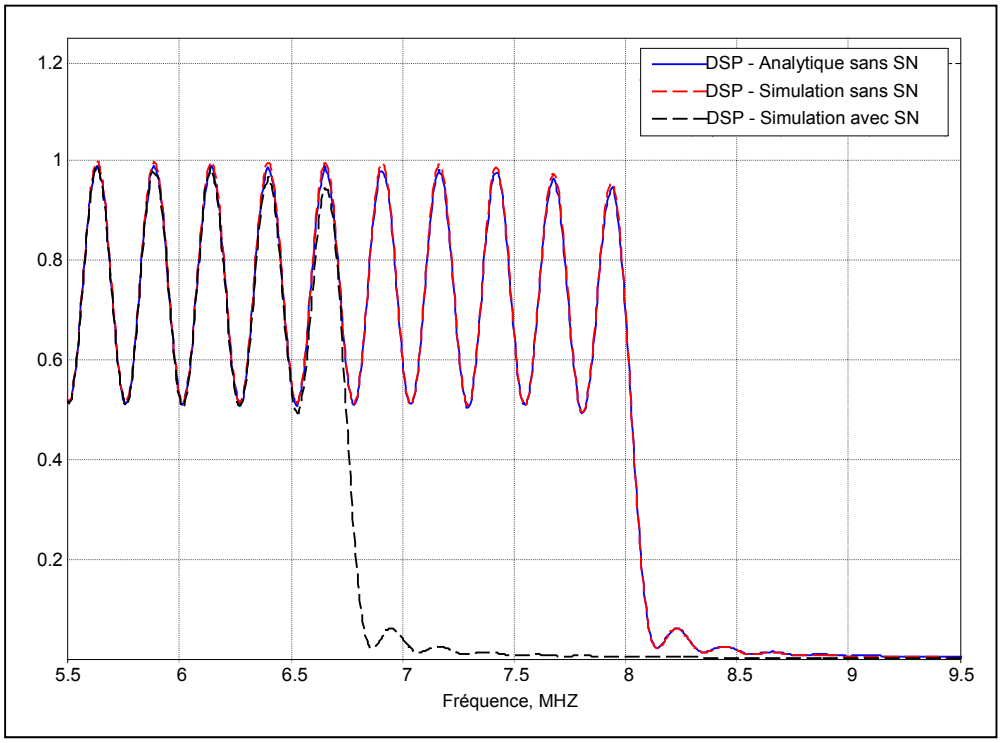


Figure 4.3 Courbes de la DSP agrandies (SN : Sous-porteuse nulles)

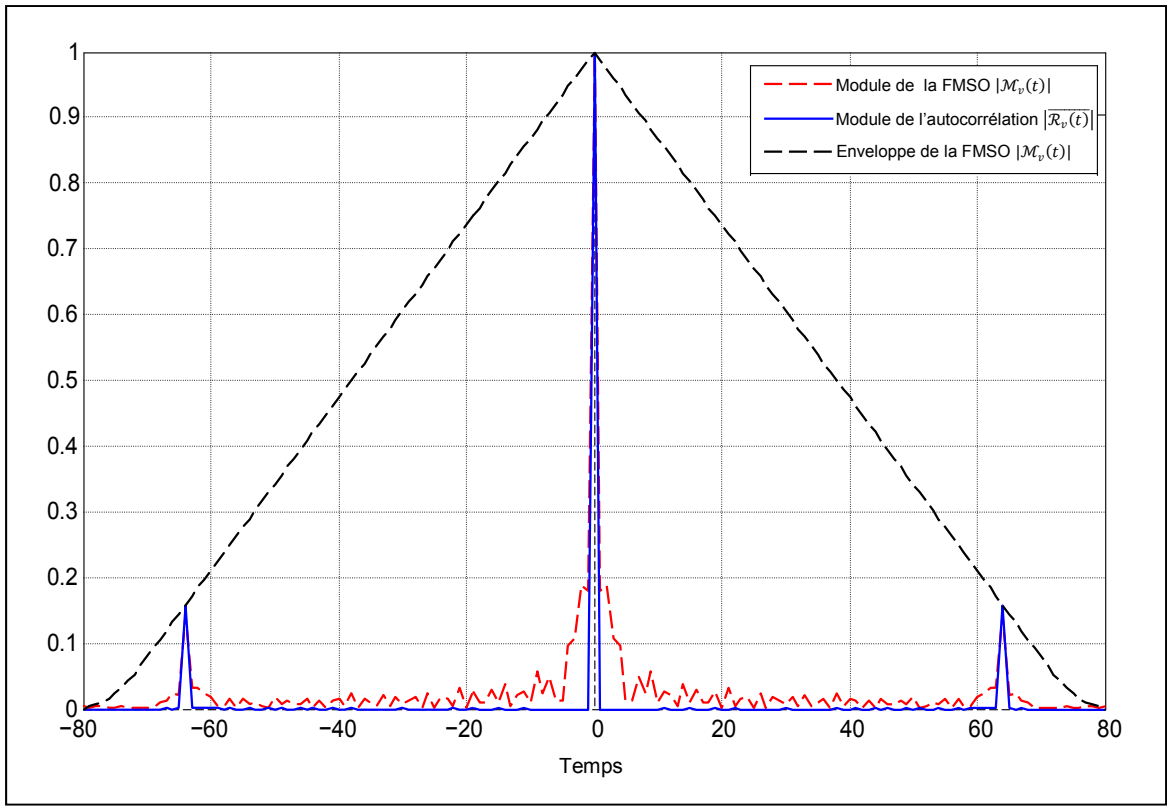


Figure 4.4 Module de la FMSO du signal OFDM à préfixe cyclique de taille aléatoire

4.4.1 Validation des expressions de DSP

Dans la partie simulation, deux signaux sont considérés: un premier signal OFDM utilisant toutes les $\mathcal{N}$ sous-porteuses, et un deuxième signal ayant 11 sous-porteuses de garde nulles et une sous-porteuse DC nulle. Les 52 autres sous-porteuses sont dédiées à la transmission des données. La DSP de ces signaux a été estimée en utilisant la méthode du périodogramme moyenné où une moyenne sur 1000 symboles OFDM est effectuée. En suivant les spécifications de la norme IEEE 802.11, la courbe de simulation ainsi que la courbe analytique de la DSP issue de (4.39) sont tracées dans la Figure 4.2. Une superposition des courbes susmentionnées est notée, particulièrement dans la Figure 4.3 lorsque un agrandissement est effectué. Dans la même figure, une bonne concordance peut également

être observée entre la courbe analytique et la courbe de simulation avec sous-porteuses nulles, surtout dans la région centrale du spectre.

4.4.2 Validation des expressions de FMSO

Dans ce paragraphe, nous utilisons le signal de simulation OFDM occupant toute la bande allouée. La Figure 4.4 montre que la courbe d'autocorrélation moyennée correspond bien à la courbe analytique de la FSMO en particulier pour les pics correspondants aux indices -64, 64 (correspondants à la durée utile du symbole OFDM) et 0. Contrairement aux signaux OFDM classiques, un léger arrondissement est aussi noté au niveau des extrémités de la courbe de l'enveloppe de la FMSO. Ceci est dû à la taille aléatoire du préfixe cyclique.

4.5 Conclusion

Dans ce chapitre, les expressions exactes de la fonction du moment de second ordre (FSMO) et de la densité spectrale de puissance (DSP) des signaux PSK et QAM en bande de base dont les durées d'impulsions sont aléatoires, ont été dérivés pour la première fois. En outre, les mêmes expressions ont été obtenues pour des signaux OFDM à préfixe cyclique de taille aléatoire. Il a été démontré que ces expressions dérivées ne sont autres que des formes moyennées des DSP et FMSO des signaux classiques numériquement modulés. Les expressions dérivées présentent une base théorique pour les anciens et futurs travaux permettant de valider les résultats de simulation qui y sont établis.

CHAPITRE 5

IMPLÉMENTATION D'UN ÉMETTEUR OFDM À PRÉFIXE CYCLIQUE ALÉATOIRE

5.1 Introduction

Dans ce chapitre, une implémentation d'un émetteur OFDM à préfixe cyclique pseudo-aléatoire sur la plateforme GNU Radio est présentée. Ensuite, les performances en termes de cyclostationnarité de l'onde OFDM générée sont évaluées. Ces performances sont comparées aux performances basées sur le modèle théorique de la technique à préfixe cyclique pseudo-aléatoire présentée dans le chapitre 3.

5.2 Radio logicielle SDR

La radio logicielle ("Software Defined Radio", SDR) a été introduite dans le but de concevoir des appareils configurables pouvant implémenter différents systèmes de communication sans fil et fonctionnant à différentes fréquences [36,38].

5.2.1 Principe de la SDR

La radio logicielle consiste à réduire au maximum la partie matérielle dans un appareil de communication sans fil, au prix d'une dominante partie logicielle exécutable sur des ordinateurs personnels [37, 38]. Cette partie logicielle est responsable de générer un flux fini ou infini de signal numérique qui passera par d'éventuels blocs de traitement numérique du signal. La partie matérielle prend ensuite la relève en convertissant le signal numérique à la sortie de la partie logicielle, en un signal analogique en bande de base. Celui-ci sera par la suite translaté à la fréquence porteuse et finalement transmis à travers l'antenne radiofréquence. Ce concept de la SDR, illustré dans la Figure 5.1, est différent de celui des radios traditionnelles d'un point de vue structurel. Les radios

traditionnels implémentent ses fonctions de communication sur des parties matérielles dédiées ou programmables.

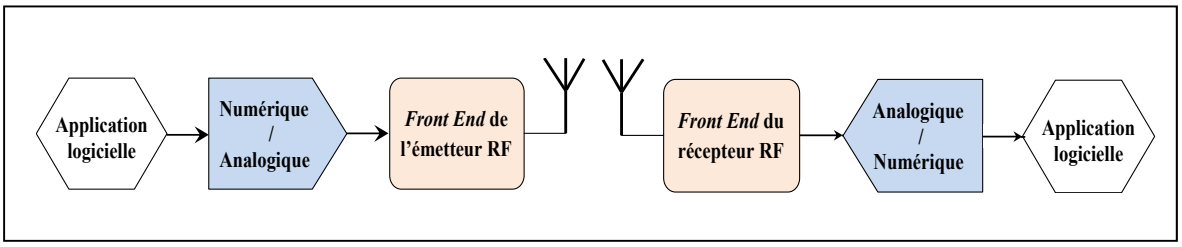


Figure 5.1 Diagramme en block d'un émetteur et un récepteur de type SDR

La technologie SDR exige l'utilisation d'une partie matérielle minimale. Celle-ci est constituée d'un convertisseur analogique-numérique (CAN), d'un convertisseur numérique-analogique (CNA) ainsi d'un module RF responsable de la modulation du signal à la fréquence d'émission ou de réception [37, p. 364]. L'utilisation combinée de tels éléments matériels ainsi qu'un ordinateur doté d'une puissance de calcul suffisante pour l'exécution de la partie logicielle constituent l'essentiel de la technologie SDR.

La reconfigurabilité constitue un avantage majeur de la SDR. Tous les paramètres qui sont définis dans la partie logicielle sont susceptibles d'être reconfigurés d'une façon flexible [37, p. 373][38]. Ceci permet le développement facile et non-coûteux de nouvelles techniques et algorithmes de communications en utilisant le concept de prototypage à base de la technologie SDR. Cependant, la radio logicielle possède quelques inconvénients qui ont restreint le champ d'application d'une telle technologie. D'après [38], l'un des inconvénients est la taille importante des ordinateurs dont le rôle consiste à effectuer le traitement du signal. Ces ordinateurs sont beaucoup plus volumineux que les systèmes matériels dédiés ou programmables, utilisés dans les radios traditionnelles. Pour cette raison, l'idée d'utiliser la SDR dans un appareil portatif implémentant plusieurs radios, a été peu envisagée. L'utilisation de la SDR a été ainsi habituellement limitée à des applications de recherche ainsi que des applications implémentées dans les stations de base ("Base Station", BS). L'inconvénient le plus important de la radio logicielle est la

consommation élevée en termes de puissance des appareils SDR [38]. En effet, la partie logicielle dans un système SDR peut nécessiter de gourmandes capacités de calcul. Ceci exige beaucoup de puissance dont la génération est généralement difficile dans un appareil portable de taille limitée.

5.2.2 Revue de la littérature des projets SDR

Les projets SDR dans la littérature sont constitués d'une partie logicielle gratuite le plus souvent libre ("Free software") qui subit continuellement des améliorations, et d'une partie matérielle commercialisée dotée d'une antenne radiofréquence. Ce matériel est généralement développé indépendamment de la partie logicielle, comme c'est le cas du projet GNU Radio [32]. Dans un autre type de projet, connu dans la littérature sous le nom HPSDR ("High Performance Software Defined Radio") [33], des cartes électroniques dotées d'un certain nombre de puces FPGA("Field-Programmable Gate Array") sont utilisées, en plus des ordinateurs, pour effectuer des opérations de traitement numérique du signal.

Le présent mémoire s'intéresse au projet GNU Radio, dont la philosophie est principalement basée sur le logiciel. Le projet GNU Radio vise à concevoir une partie logicielle modulaire qui soit capable de générer et traiter le signal en bande de base à transmettre. Ensuite, une partie matérielle translate la fréquence du signal à la fréquence porteuse désirée. Dans ce projet GNU Radio, l'utilisateur a la possibilité d'adapter le code source libre déjà existant aux exigences de son système de communication, en y effectuant les modifications nécessaires. Quant à la partie matérielle, elle est généralement accompagnée de logiciels pilotes, permettant la compatibilité entre la partie logicielle et le matériel. Ettus Research LLC est la compagnie qui fournit la partie matérielle ainsi que ses logiciels pilotes pour le projet GNU Radio [34]. Le projet GNU Radio est considéré comme étant le plus populaire parmi la liste des radios logicielles, ce qui justifie son choix dans le présent travail.

5.3 Plateforme de développement

Cette section présente la plateforme GNU Radio qui a été choisie pour l'implémentation de l'émetteur OFDM à préfixe cyclique pseudo-aléatoire. Cette plateforme, introduite en 2001 par Eric Blossom et John Gillmore, est libre et est distribuée sous la licence GNU General Public Licence. Elle a pour objectif le développement des applications SDR. Depuis lors, une large communauté de développeurs a manifesté un intérêt croissant pour cette plateforme en développant le code source de plusieurs applications SDR.

5.3.1 Plateforme GNU Radio

La GNU Radio est une plateforme logicielle conçue pour permettre le développement des applications SDR. Elle fournit des moyens qui permettent de générer le code source de modules pouvant être utilisés dans l'implémentation des prototypes des applications de communication.

L'architecture de la partie logicielle de la plateforme GNU Radio est composée de modules qui peuvent être divisés en deux types. Le premier type inclut les modules implémentant des blocs de traitement de signal tels que la TFD, des filtres, etc. Ces modules sont développés à base du langage de programmation C++.Le deuxième type représente les modules assurant l'interconnexion des modules de traitement de signal susmentionnés. Ces modules d'interconnexion permettent de rassembler les modules C++ et sont développés à l'aide du langage Python. Une fois les modules C++ compilés, leurs paramètres sont susceptibles à être reconfigurés à travers le langage Python.

Figure 5.2 Graphe d'une application GNU Radio

Une application GNU Radio est basée sur l'interconnexion de plusieurs modules formant un graphe (*Voir* Figure 5.2). Cette représentation de graphe offre au concepteur la possibilité d'avoir une vision modulaire du système permettant de faciliter la tâche de développement. De plus, toutes les applications GNU Radio sont basées sur une classe principale qui, construit le graphe en établissant les interconnexions requises après avoir instancié les modules implémentés. Au moment de la mise en marche de l'application, le code source de cette classe est exécuté d'une façon séquentielle conformément au graphe. La liaison des modules C++ est effectuée par l'intermédiaire d'une méthode Python appelée *connect*.

5.3.2 Périphérique USRP N210

Les applications GNU Radio jouissant d'une faible complexité d'implémentation (Exemple : applications audio), requièrent des caractéristiques matérielles ordinaires disponibles dans les ordinateurs actuels [38]. En revanche, l'application que nous implémentons dans le présent travail est caractérisée par une haute complexité puisqu'elle implémente un nombre considérable d'opérations qui doivent être exécutées en temps réel. De plus, ce projet implémente une application large bande dont le signal résultant doit être transmis à hautes fréquences. Du matériel sophistiqué est ainsi requis afin de répondre à ces exigences. Dans ce contexte, la plateforme GNU Radio utilise un appareil appelé USRP ("Universal Software Radio Peripheral") développé par la compagnie Ettus Research. Cet appareil est responsable de la conversion du signal numérique en bande de base traité au sein

de l'ordinateur, en un signal analogique RF de quelques GHz. L'USRP est aussi responsable de la démodulation du signal RF reçu à travers l'interface sans fil [35]. Dans ce qui suit, nous nous concentrerons sur l'une des plus récentes versions des appareils USRP connu sous le nom USRP N210.

Figure 5.3 Vue de face du périphérique USRP N210

L'appareil USRP N210 est composé d'une carte mère qui contient :

- un FPGA dédié aux calculs à vitesse élevée ;
- un CAN (bande passante : 25 MHz) ;
- un CNA (bande passante : 25 MHz).

La puce FPGA a pour rôle la conversion du signal à fréquence intermédiaire ("Intermediate Frequency", IF) en un signal en bande de base, et inversement. La carte mère est connectée à une carte fille permettant l'émission et la réception du signal analogique RF. Dans le présent travail, la carte fille utilisée est la RFX2400 opérant dans la bande de fréquence 2.3–2.9 GHz. De plus, l'USRP N210 est connecté à l'ordinateur à travers son interface Gigabit Ethernet.

5.3.3 Interface graphique GNU radio

La plateforme GNU Radio offre une interface graphique ("GNU Radio Companion", GRC) permettant la création des applications GNU Radio. Les modules y sont insérés et connectés pour former le graphe de l'application. L'interface GRC est dotée d'une liste de modules qui sont prêts à être utilisés dans les applications GNU Radio. L'utilisateur peut aussi ajouter ses propres modules personnalisés, comme c'est le cas dans le présent travail (*Voir* Figure 5.4). Les paramètres de chaque module sont définis dans un fichier XML que l'interface GRC utilise pour évaluer la validité des paramètres de configuration dans le graphe. De plus, l'interface GRC permet de générer le code Python nécessaire pour exécuter l'application conçue.

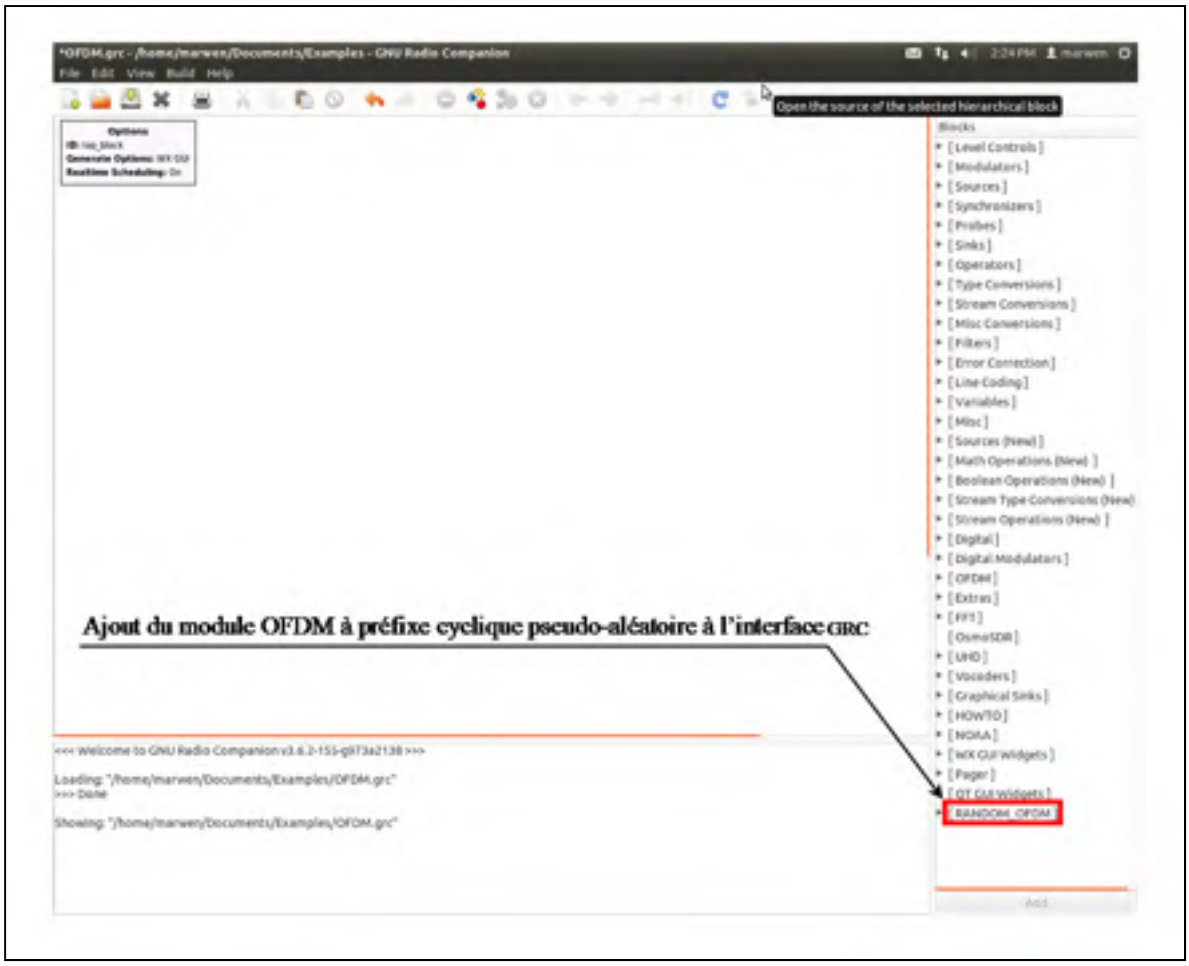


Figure 5.4 Interface graphique GRC de la plateforme GNU Radio

5.4 Stratégie d'implémentation

L'émetteur OFDM à préfixe cyclique aléatoire est codé dans le fichier exécutable random_ofdm_application.py. Ce fichier englobe les paramètres généraux de l'application tel que la taille des données à transmettre, et fait appel à plusieurs fichiers de code source en instanciant les classes qui y sont définies. Le code source de l'application est organisé hiérarchiquement en deux niveaux d'abstraction. La classe random_ofdm_application.py représente le niveau d'abstraction le plus élevé dans cette hiérarchie (*Voir* Figure 5.5). Le deuxième niveau englobe des classes qui définissent des paramètres relatifs à la modulation et au périphérique USRP. Les blocs gris clair représentent les fichiers code source codés en Python. D'autre part, les blocs en gris foncé sont des fichiers codés en C++. Les blocs blancs représentent les modules instanciés dans les fichiers Python.

Le fichier random_ofdm_application.py instancie les modules suivants :

Source aléatoire : Ce module constitue le générateur du flux de données à traiter dans le module suivant. Ne nécessitant pas une puissance de calcul avancée, ce module est codé en Python ;

Modulateur OFDM à préfixe cyclique aléatoire : Ce module est détaillé dans le paragraphe « Modulateur OFDM » ci-dessous ;

Contrôleur ("Throttle") : Ce module contrôle la vitesse de transmission en définissant un débit maximal ;

Émetteur USRPN210: Ce module est dédié à la transmission de l'onde OFDM générée à travers l'appareil USRP.

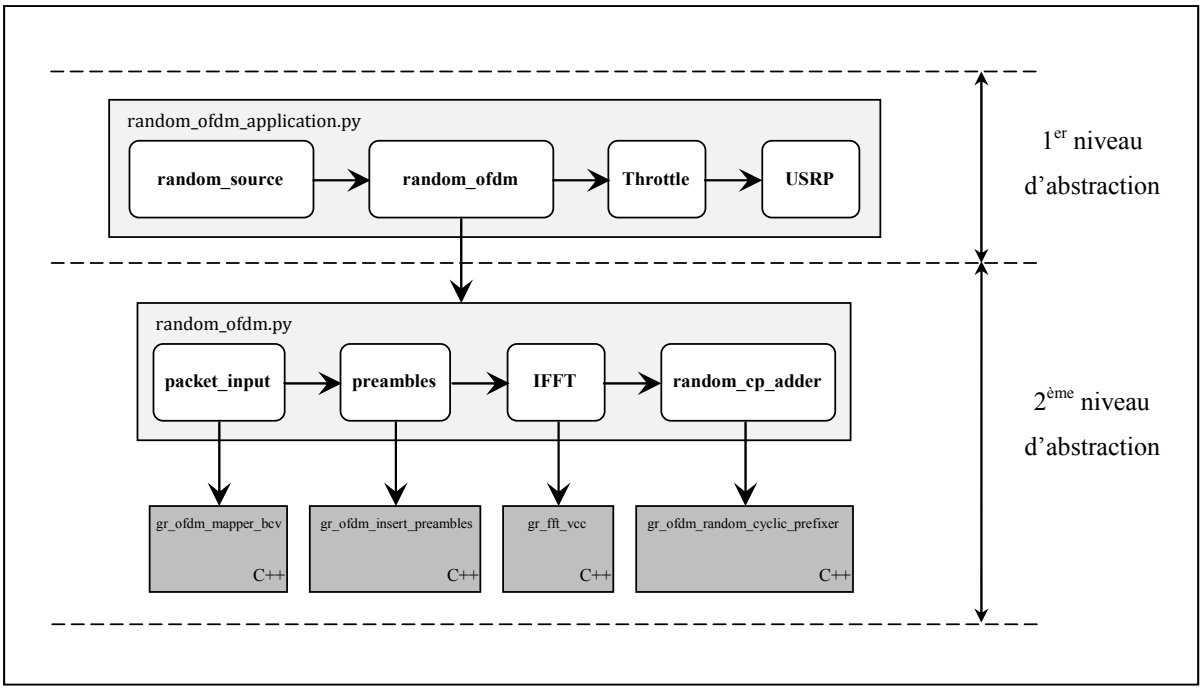


Figure 5.5 Hiérarchie modulaire de l'application GNU Radio implémentée

Modulateur OFDM

La classe relative au modulateur OFDM est développée dans le fichier random_ofdm.py. Tel qu'illustré à la Figure 5.5, les modules qui y sont instanciés sont développés en C++. Le modulateur OFDM est doté d'une fonction d'envoi qui prend comme entrée la charge de données ("payload") et l'envoie au premier module *pkt_input*. Cette fonction d'envoi a pour mission la construction du paquet en utilisant la fonction *ofdm_packet_utilis.make_packet*. Celle-ci ajoute un suffixe de contrôle basée sur le code détecteur d'erreur CRC ("Contrôle de Redondance Cyclique") à la charge de données. Ensuite, une fonction *insert_tail* est utilisée afin d'acheminer les données à la sortie de la fonction d'envoi vers le module *pkt_input*, en les stockant dans une file d'attente appropriée.

Le premier module du modulateur OFDM à préfixe cyclique aléatoire est appelé *pkt_input*. Ce module est développé sous forme d'une classe C++ codée dans le fichier gr_ofdm_mapper_bcv.cc. Cette classe convertit le flux de données provenant de la méthode *insert_tail* en des vecteurs de symboles complexes selon le paramétrage défini dans le

premier niveau d'abstraction. Dans une étape ultérieure, ces symboles complexes attaqueront le module TFDI du modulateur OFDM. Par ailleurs, le fichier random_ofdm.py instancie le module *preambles* codé en C++ dans le fichier gr_ofdm_insert_preambles.cc. Ce module ajoute un préambule à chaque paquet OFDM à transmettre.

Les données à la sortie du module *preambles* seront par la suite traitées dans le module TFDI codé en C++ au fichier gr_fft_vcc.cc. Ce module calcule la TFDI du vecteur entrant constitué de symboles complexes. La taille de la transformée de Fourier inverse est un paramètre qui peut être spécifié au niveau de l'interface GRC. La prochaine étape consiste à insérer un préfixe cyclique de taille aléatoire au début de chaque symbole OFDM. Cette technique est effectuée au sein du module *random_cp_adder* définie dans le fichier gr_ofdm_random_cyclic_prefixer.cc. L'intervalle dans lequel le préfixe cyclique varie peut être défini à partir de l'interface graphique GRC (*Voir* Figure 5.6).

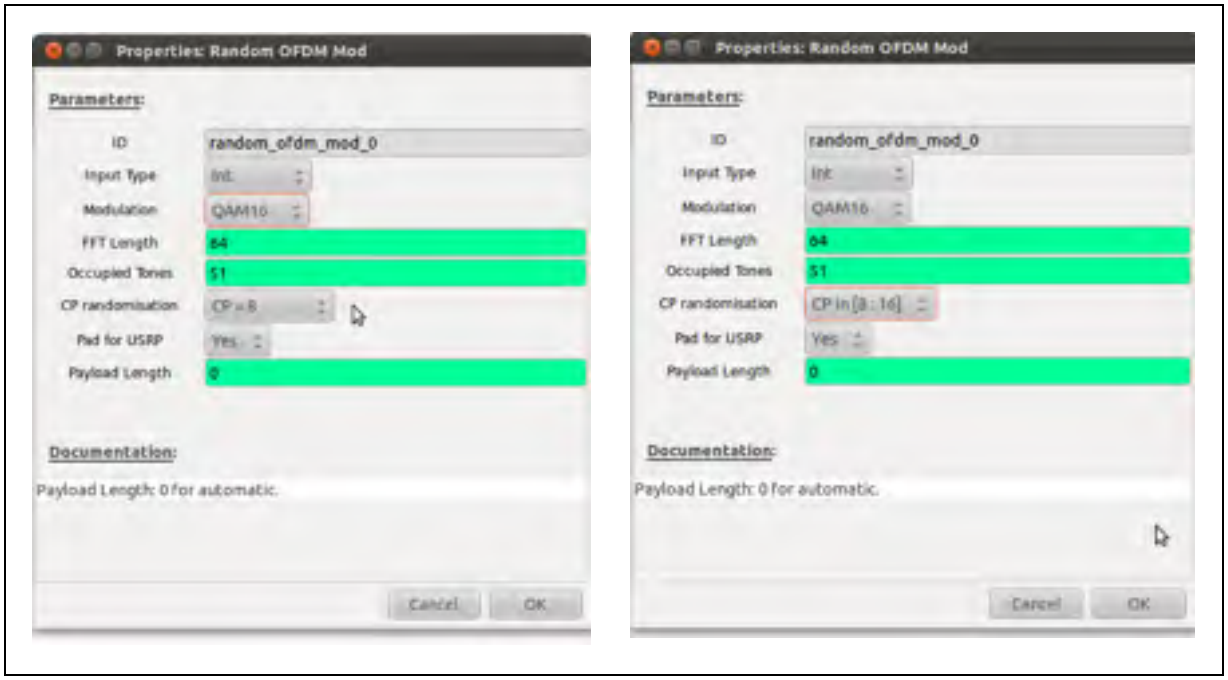


Figure 5.6 Configuration de la taille du préfixe cyclique à partir de l'interface GRC

5.5 Mesure de performances

Une fois l'émetteur OFDM à préfixe cyclique pseudo-aléatoire implémenté sur la plateforme GNU Radio, un scénario de test est mis en œuvre afin de mesurer les performances de l'émetteur en termes de cyclostationnarité. Les caractéristiques de l'onde OFDM implémentée sont définies au Tableau 5.1.

Tableau 5.1 Paramètres du système OFDM implémenté

Paramètre	Valeur
Taille de la TFD	64
Sous-porteuses de données	52
Taille discrète du préfixe cyclique, N_{cp}	{8, 11, 13, 16}
Fréquence RF porteuse	2.49 GHz
Fréquence d'échantillonnage TFD	10MHz
Espace inter-canal Δf	156.25 kHz
Indices des sous-porteuses de données	{-26 to -1, +1 to +26}
Durée du PC, T_{cp}	{0.8, 1.1, 1.3, 1.6 µs}
Durée utile de symbole,T_s	6.4 µs

5.5.1 Scénario de test

Les Figures 5.7et5.8illustrent le scénario de test ainsi que le graphe correspondant, respectivement. Un émetteur GNU Radio noté « A » est supposé transmettre une onde sans fil OFDM à préfixe cyclique aléatoire, à un récepteur « B ». Un utilisateur malicieux « C » essaie, entre-temps, d'intercepter le signal transmis OFDM en effectuant certaines opérations de traitement de signal afin d'en extraire les paramètres de transmission. Ces paramètres sont généralement utilisés pour permettre la synchronisation au signal OFDM transmis.

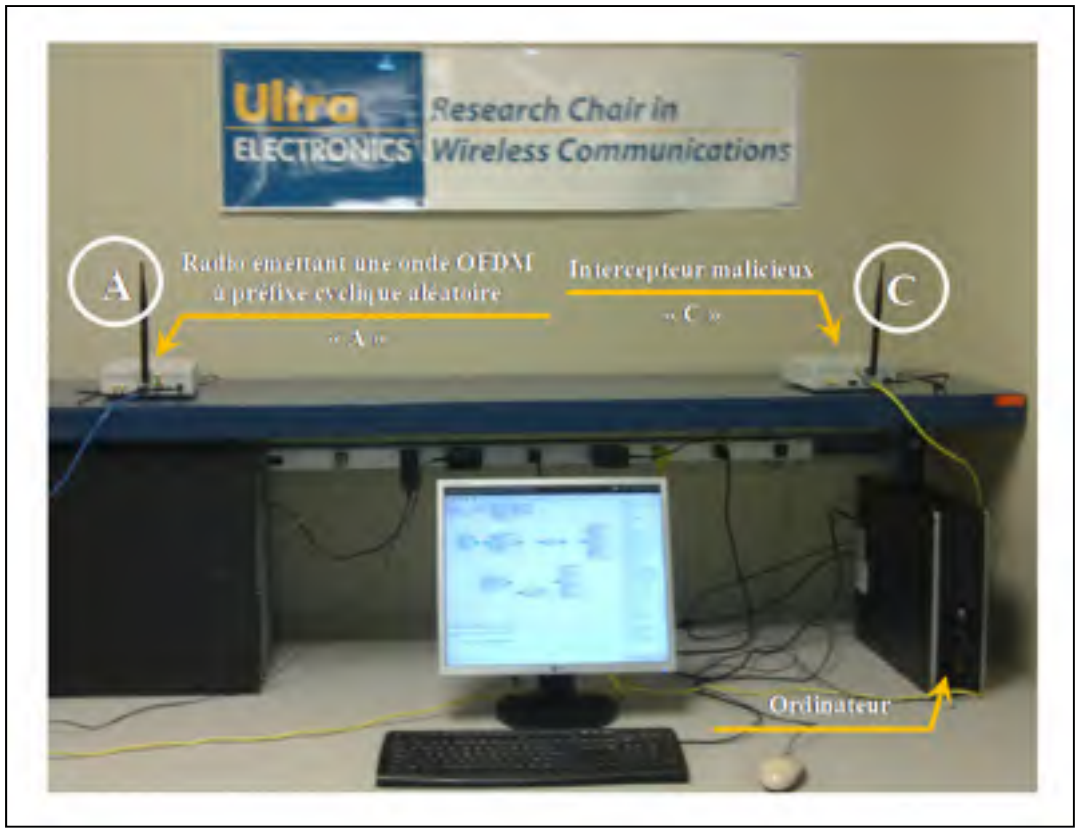


Figure 5.7 Scénario de test de l'onde OFDM à préfixe cyclique aléatoire.

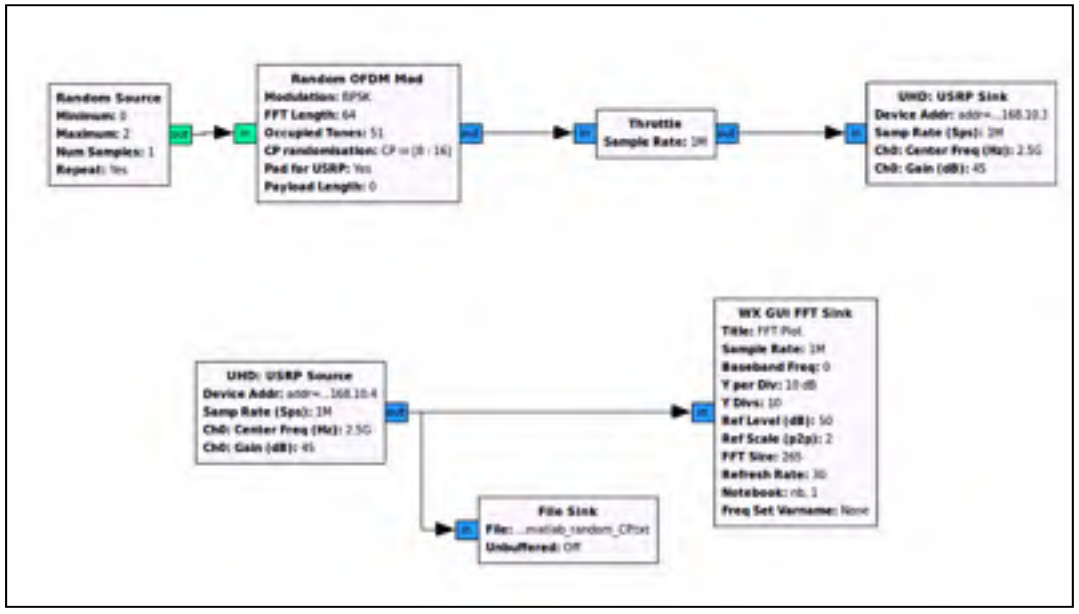


Figure 5.8 Graphe correspondant au scénario de test de l'onde OFDM à préfixe cyclique de taille pseudo-aléatoire

Le traitement de signal effectué par la radio « C » est simulé en utilisant le logiciel MATLAB. Cette radio enregistre l'onde OFDM reçue dans un fichier binaire qui sera, par la suite, assujetti à une analyse complète de cyclostationnarité.

5.5.2 Analyse de cyclostationnarité

Les transformations exposées dans ce paragraphe représente un échantillon des transformations de second ordre non-linéaires que peut effectuer un intercepteur malicieux afin d'intercepter un signal OFDM. Ainsi, les performances en termes de cyclostationnarité du signal OFDM à préfixe cyclique aléatoire sont mises en relief. Dans un premier lieu, la courbe de la CAF de l'onde interceptée au niveau de la radio « C » est tracée à la Figure 5.9.Il est clair que la cyclostationnarité du signal OFDM émis est considérablement réduite une fois comparée à la courbe de la fonction d'autocorrélation cyclique de l'onde OFDM classique tracée à la Figure 5.10.

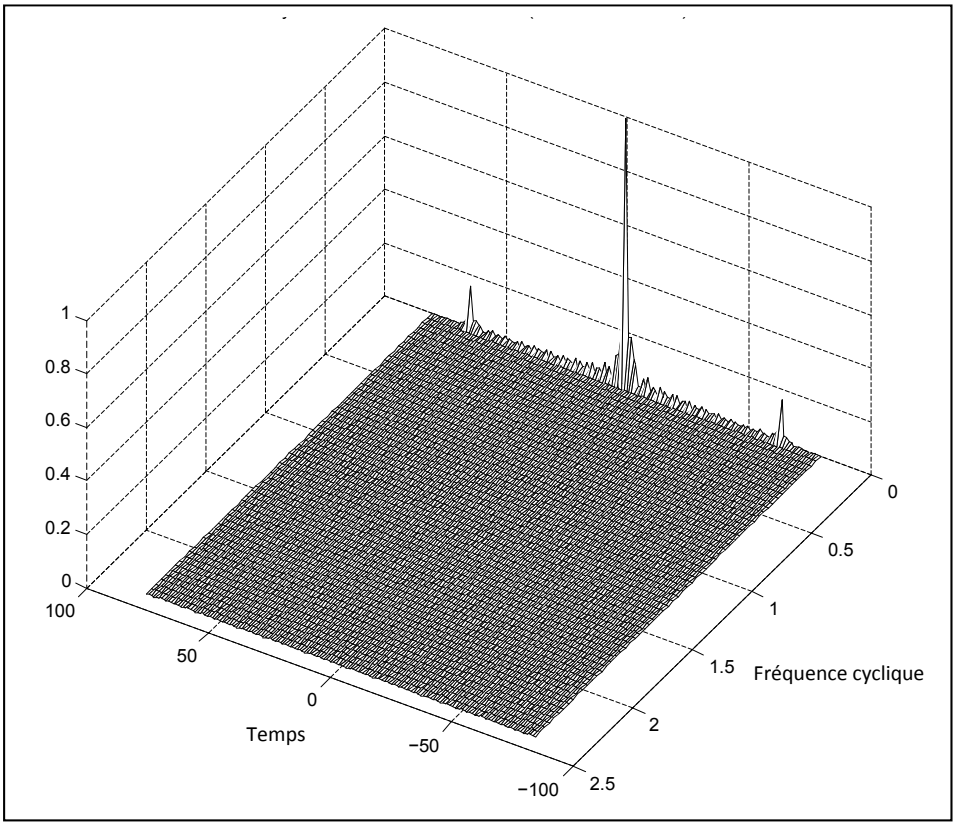


Figure 5.9 Fonction d'autocorrélation cyclique du signal OFDM à préfixe cyclique de taille pseudo-aléatoire reçu par la radio « C »

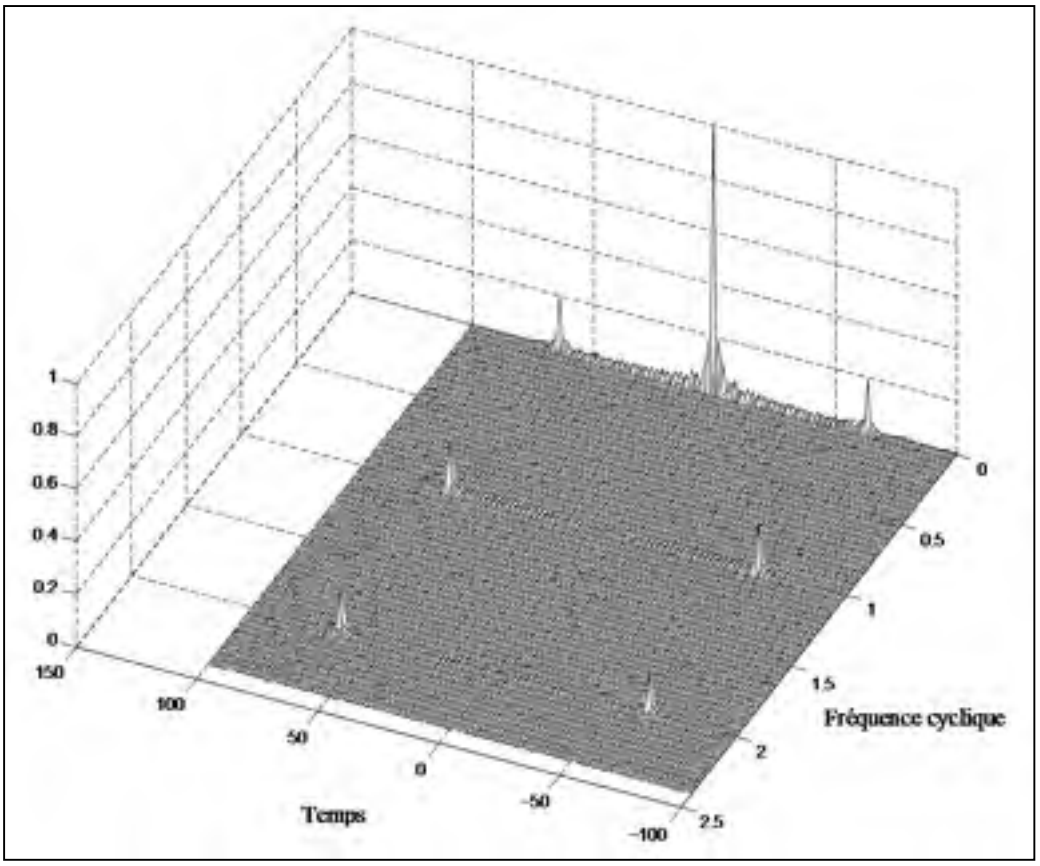


Figure 5.10 Fonction d'autocorrélation cyclique du signal OFDM classique à préfixe cyclique de taille fixe

La Figure 5.11 trace le spectre du signal élevé au carré. Il est possible d'y constater que, contrairement à la Figure 5.12 où le préfixe cyclique est fixe, les raies spectrales sont atténuées grâce à la technique à insertion d'aléa, conformément aux courbes théoriques du spectre du signal OFDM classique élevé au carré illustrées dans les Figures 3.6 et 3.7.

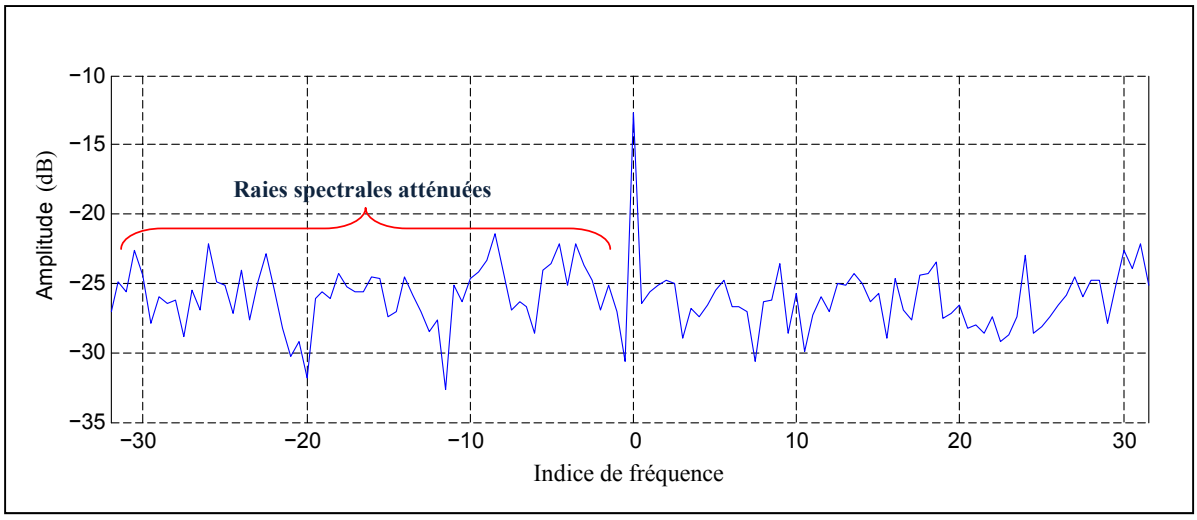


Figure 5.11 Spectre du signal OFDM à préfixe cyclique aléatoire élevé au carré

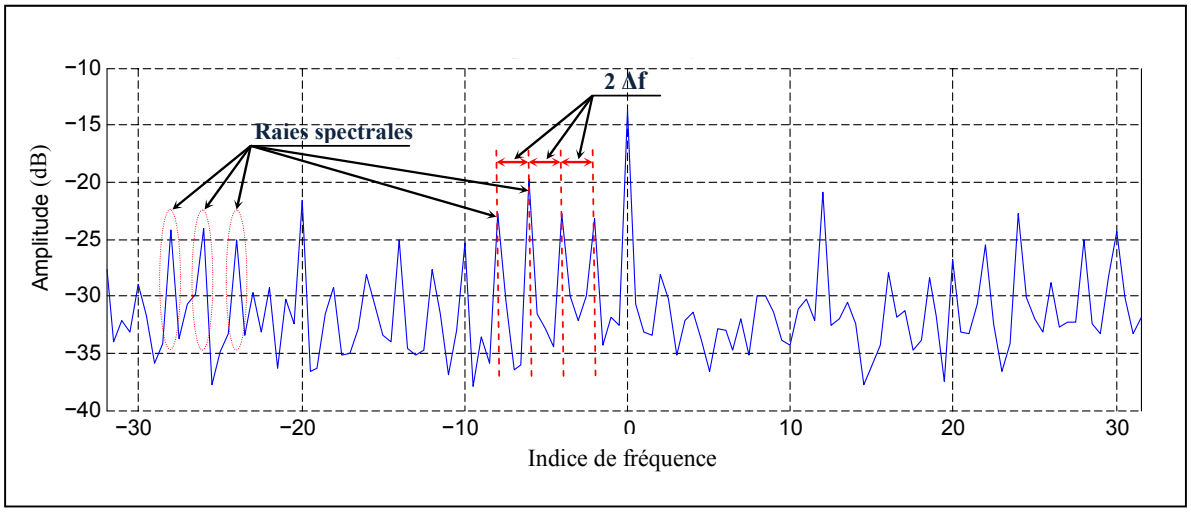


Figure 5.12 Spectre du signal OFDM classique élevé au carré
(Δf : Espacement inter-canal)

Finalement, il est attendu, dans de futurs travaux, qu'une meilleure atténuation des caractéristiques cyclostationnaires et spectrales de l'onde OFDM pourrait être réalisée, une fois que la technique de gigue de fréquence sera implémentée en tant que deuxième niveau de sécurité conformément à la description du chapitre 3.

5.6 Conclusion

L'implémentation d'un émetteur OFDM à préfixe cyclique de taille pseudo-aléatoire sur la plateforme GNU Radio a été exposée dans ce chapitre. Une revue de littérature concernant le concept de la radio logicielle a été présentée dans un premier lieu. Ensuite, la plateforme d'implémentation GNU Radio a été abordée et une attention particulière a été accordée aux radios USRP N210. Une section entière a été dédiée à la stratégie d'implémentation basée sur l'utilisation combinée des deux langages de programmation C++ et Python. De plus, une analyse de la cyclostationnarité a été proposée dans le cadre d'un scénario de test de l'émetteur OFDM. Finalement, une validation des courbes de cyclostationnarité obtenues a été effectuée en les comparant aux courbes théoriques produites dans le chapitre 3. Cette analyse a permis de conclure que l'onde OFDM à préfixe cyclique pseudo-aléatoire est caractérisée par une faible probabilité d'interception.

CONCLUSION

Dans ce mémoire, un système OFDM à faible probabilité d'interception a été proposé. Ce système est basé sur l'insertion d'aléa aux paramètres de l'onde OFDM classique. En effet, plusieurs contributions y sont identifiées : La première contribution porte sur la conception d'un système de communication OFDM implémentant un préfixe cyclique de taille pseudo-aléatoire ainsi qu'une gigue de fréquence pseudo-aléatoire. La deuxième contribution porte sur l'analyse des performances du système proposé sur un canal de Rayleigh sélectif en fréquences. Ensuite, une analyse spectrale de l'onde OFDM à préfixe cyclique de taille pseudo-aléatoire a été effectuée. La dernière contribution porte sur la démonstration de faisabilité de l'émetteur du système proposé en implémentant la technique à insertion d'aléa au préfixe cyclique sur la plateforme GNU Radio.

L'insertion d'aléa à la taille du préfixe cyclique ainsi qu'à la fréquence porteuse ont permis de réduire considérablement les propriétés cyclostationnaires du signal OFDM. Ces deux techniques empêchent des utilisateurs malicieux d'utiliser les algorithmes aveugles de synchronisation et d'estimation de paramètres OFDM [1]. En outre, l'analyse spectrale de l'onde OFDM à préfixe cyclique de taille pseudo-aléatoire a donné naissance aux nouvelles expressions du moment de second ordre ainsi que la densité spectrale de puissance. Cette analyse présente alors une base théorique pour la validation de plusieurs travaux de la littérature.

Finalement, une implémentation d'un émetteur OFDM à préfixe cyclique aléatoire sur la plateforme GNU Radio a été réalisée. Les performances de l'émetteur implémenté en termes de cyclostationnarité ont été évaluées en établissant un scénario de test de l'onde OFDM implémentée. Dans ce scénario, un émetteur OFDM à préfixe cyclique pseudo-aléatoire est implémenté sur une radio de type GNU Radio. D'autre part, une radio malicieuse de type GNU Radio essaie d'intercepter le signal transmis en effectuant des transformations non-linéaires adéquates. Après avoir appliqué ces transformations, une atténuation des caractéristiques cyclostationnaires et spectrales a été démontrée une fois que les courbes de la fonction d'autocorrélation cyclique ainsi que le spectre du signal OFDM élevé au carré sont

tracées. De plus, une bonne concordance avec les courbes théoriques a été aussi notée. Ceci valide la faible probabilité d'interception de l'onde OFDM implémentée.

RECOMMANDATIONS

Les futurs travaux pourraient porter sur l'étude de cyclostationnarité d'ordre supérieur afin d'élaborer une description totale du signal OFDM à préfixe cyclique aléatoire. De plus, une élaboration des expressions de la fonction d'autocorrélation cyclique (FAC) ainsi que la densité spectrale cyclique (DSC) du signal OFDM à préfixe cyclique aléatoire, pourrait être envisagée. Une implémentation de la technique de gigue de fréquence sur la plateforme GNU Radio pourrait être considérée afin de consolider la sécurité à la couche physique du système OFDM implémenté. Finalement, une étude concernant le choix des nombres aléatoires et leur impact sur l'atténuation des caractéristiques cyclostationnaires pourrait faire l'objet de travaux futurs.

.

ANNEXE I

Démonstration mathématique (1)

Dans cette annexe, nous démontrons que $\overline{\mathcal{R}_{s^{(j)}}(t)} = \mathcal{M}_s(t)$. On sait que :

$$\overline{\mathcal{R}_{s^{(j)}}(t)} = \lim_{\tau \to +\infty} \frac{1}{\tau} \int_{-\tau/2}^{+\tau/2} \overline{s^{(j)}(t_0) s^{(j)^*}(t_0 + t)} dt_0, \qquad \text{(A I-1)}$$

Sachant que $s^{(j)}(t)$ est stationnaire, il en résulte que

$$\overline{\mathcal{R}_{s^{(j)}}(t)} = \left(\lim_{\tau \to +\infty} \frac{1}{\tau} \int_{-\tau/2}^{+\tau/2} dt_0 \right) \mathcal{M}_s(t) = \mathcal{M}_s(t), \qquad \text{(A I-2)}$$

ANNEXE II

Démonstration mathématique (2)

Dans cette annexe, nous démontrons que le terme (**E**) dans (4.33) représente la FMSO des signaux QAM et PSK à durée d'impulsion aléatoire. D'après la section 4.1, un signal PSK et QAM à durée d'impulsion aléatoire est donnée par :

$$s^{(j)}(t) = \sum_{m=-\infty}^{+\infty} c_m^{(j)} g\left(t - \alpha_m^{(j)} ; T_m^{(j)}\right), \tag{A II-1}$$

tandis que sa fonction d'autocorrélation, est exprimée par :

$$\begin{aligned} \mathcal{R}_{s^{(j)}}(t) &= \lim_{\tau \to +\infty} \frac{1}{\tau} \int_{-\tau/2}^{+\tau/2} s^{(j)}(t_0) {s^{(j)}}^*(t_0 + t) dt_0 \qquad \text{(A II-2)} \\ &= \lim_{\tau \to +\infty} \frac{1}{\tau} \int_{-\infty}^{+\infty} \sum_{m=-\infty}^{+\infty} \sum_{n=-\infty}^{+\infty} \left\{ c_m^{(j)} {c_n^{(j)}}^* g\left(t_0 - \alpha_m^{(j)} ; T_m^{(j)}\right) g\left(t_0 + t - \alpha_m^{(j)} ; T_m^{(j)}\right) dt_0 \right\}. \end{aligned}$$

En appliquant la moyenne statistique des deux côtés de (A II-2), il en résulte que :

$$\begin{aligned} \overline{\mathcal{R}_{s^{(j)}}(t)} = \lim_{\tau \to +\infty} \frac{1}{\tau} \int_{-\tau/2}^{+\tau/2} \sum_{m=-\infty}^{+\infty} \sum_{n=-\infty}^{+\infty} \Big\{ & E\left(c_m^{(j)} {c_n^{(j)}}^* \right) \times \qquad \text{(A II-3)} \\ & E\left(g\left(t_0 - \alpha_m^{(j)} ; T_m^{(j)}\right) g\left(t_0 + t - \alpha_n^{(j)} ; T_n^{(j)}\right) \right) dt_0 \Big\} \end{aligned}$$

En supposant que c_m sont i.i.d de moyenne nulle et en rappelant que $\overline{\mathcal{R}_{s(j)}}(t) = \mathcal{M}_s(t)$, on peut obtenir :

$$\mathcal{M}_s(t) = \lim_{\tau \to +\infty} \frac{1}{\tau} \sum_{m=-\infty}^{+\infty} \int_{-\tau/2}^{+\tau/2} \sigma^2 E\left\{ g\left(t_0 - \alpha_m^{(j)} ; T_m^{(j)}\right) g\left(t_0 + t - \alpha_m^{(j)} ; T_m^{(j)}\right) dt_0 \right\} \tag{A II-4}$$

Par conséquent, nous montrons que l'expression (**E**) dans (4.33) correspond exactement à la FMSO d'un signal QAM, PSK à durée d'impulsion aléatoire.

BIBLIOGRAPHIE

[1] Marwen Bouanen, Francois Gagnon, Georges Kaddoum, Denis Couillard, and Claude Thibeault."An LPI design for secure OFDM systems. "In *MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012*, pp. 1-6.IEEE, 2012.

[2] Gardner, William A., Antonio Napolitano, and Luigi Paura. "Cyclostationarity: Half a century of research." *Signal processing* 86, no. 4 (2006): 639-697.

[3] Chang, R. W., and R. Gibby. "A theoretical study of performance of an orthogonal multiplexing data transmission scheme." *Communication Technology, IEEE Transactions on* 16, no. 4 (1968): 529-540.

[4] Engels, Marc, ed. *Wireless OFDM Systems: How to make them work ?*. Springer, 2002.

[5] Weinstein, S., and Paul Ebert. "Data transmission by frequency-division multiplexing using the discrete Fourier transform." *Communication Technology, IEEE Transactions on* 19, no. 5 (1971): 628-634.

[6] Shen, Yushi, and Ed Martinez. "Channel estimation in OFDM systems. "*Application note, Freescale semiconductor* (2006).

[7] Van De Beek, J-J., Magnus Sandell, Mikael Isaksson, and P. Ola Borjesson. "Low-complex frame synchronization in OFDM systems."In *Universal Personal Communications.1995. Record., 1995 Fourth IEEE International Conference on*, pp. 982-986. IEEE, 1995.

[8] Sandell, Magnus, Jan-Jaap van de Beek, and Per Ola Börjesson. "Timing and frequency synchronization in OFDM systems using the cyclic prefix."In *Proc. Int. Symp. Synchronization*, pp. 14-15. 1995.

[9] Van de Beek, Jan-Jaap, Magnus Sandell, and Per Ola Borjesson."ML estimation of time and frequency offset in OFDM systems." *Signal Processing, IEEE Transactions on* 45, no. 7 (1997): 1800-1805.

[10] Speth, Michael, Ferdinand Classen, and Heinrich Meyr. "Frame synchronization of OFDM systems in frequency selective fading channels." In *Vehicular Technology Conference, 1997, IEEE 47th*, vol. 3, pp. 1807-1811. IEEE, 1997.

[11] Keller, Thomas, Lorenzo Piazzo, Paolo Mandarini, and Lajos Hanzo. "Orthogonal frequency division multiplex synchronization techniques for frequency-selective fading channels." *Selected Areas in Communications, IEEE Journal on* 19, no. 6 (2001): 999-1008.

[12] Bolcskei, Helmut. "Blind estimation of symbol timing and carrier frequency offset in wireless OFDM systems." *Communications, IEEE Transactions on* 49, no. 6 (2001): 988-999.

[13] Karygiannis, Tom, and Les Owens. "Wireless network security." *NIST special publication* 800 (2002): 48.

[14] Gardner, William A., "Cyclostationarity in Communications and Signal Processing." *IEEE Press*, New York (1994).

[15] Iniewski, Krzysztof, ed. *Wireless technologies: circuits, systems, and devices*. CRC, 2007.

[16] Meyer, R. R., and M. N. Newhouse. "OFDM waveform feature suppression." In *MILCOM 2002. Proceedings*, vol. 1, pp. 582-586. IEEE, 2002.

[17] Gelli, Giacinto, DavideMattera, and Luigi Paura. "Blind wideband spatio-temporal filtering based on higher-order cyclostationarity properties." *Signal Processing, IEEE Transactions on* 53, no. 4 (2005): 1282-1290.

[18] Morelande, Mark R., and Abdelhak M. Zoubir. "On the performance of cyclic moments-based parameter estimators of amplitude modulated polynomial phase signals." *Signal Processing, IEEE Transactions on* 50, no. 3 (2002): 590-606.

[19] Surender, Shrawan C., and Ram M. Narayanan. "Synchronization for wireless multi-radar covert communication networks." In *Proceedings of SPIE, the International Society for Optical Engineering*, pp. 65780U-1. Society of Photo-Optical Instrumentation Engineers, 2007.

[20] Wang, Xianbin, Paul Ho, and Yiyan Wu. "Robust channel estimation and ISI cancellation for OFDM systems with suppressed features." *Selected Areas in Communications, IEEE Journal on* 23, no. 5 (2005): 963-972.

[21] Yucek, Tevfik, and HuseyinArslan. "Feature suppression for physical-layer security in ofdm systems." In *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pp. 1-5. IEEE, 2007.

[22] Hurd, H. L. "Stationarizing properties of random shifts." *SIAM Journal on Applied Mathematics* 26, no. 1 (1974): 203-212.

[23] Van De Beek, J-J., Magnus Sandell, Mikael Isaksson, and P. Ola Borjesson."Low-complex frame synchronization in OFDM systems."In *Universal Personal Communications.1995. Record., 1995 Fourth IEEE International Conference on*, pp. 982-986. IEEE, 1995.

[24] Sandell, Magnus, Jan-Jaap van de Beek, and Per Ola Börjesson. "Timing and frequency synchronization in OFDM systems using the cyclic prefix."In *Proc. Int. Symp. Synchronization*, pp. 14-15. 1995.

[25] Rappaport, Theodore S. *Wireless communications: principles and practice*. IEEE press, 1996.

[26] Witrisal, Klaus, Yong-Ho Kim, and Ramjee Prasad. "A new method to measure parameters of frequency-selective radio channels using power measurements. "*Communications, IEEE Transactions on* 49, no. 10 (2001): 1788 1800.

[27] Schober, Henrik, Friedrich Jondral, R. Stirling-Gallacher, and Zhaocheng Wang. "Delay spread estimation for OFDM based mobile communication systems." In *Proceedings of the European Wireless Conference*. 2002.

[28] Alouini, M-S., and Andrea J. Goldsmith. "A unified approach for calculating error rates of linearly modulated signals over generalized fading channels."*Communications, IEEE Transactions on* 47, no. 9 (1999): 1324-1334.

[29] Middleton, David. *An introduction to statistical communication theory*. Vol. 960. New York: McGraw-Hill, 1960.

[30] Liu, Chunming, and Fu Li. "On spectrum modeling of OFDM signals for digital broadcasting." In *Signal Processing, 2004.Proceedings.ICSP'04. 2004 7th International Conference on*, vol. 3, pp. 1886-1889. IEEE, 2004.

[31] IEEE 802.11 Working Group. "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications." (1997).

[32] Blossom, Eric."GNU software radio."*http://gnuradio.org*.

[33] "High Performance Defined Radio." *http://openhpsdr.org*.

[34] Ettus, Matt. "Universal software radio peripheral (USRP)." *Ettus Research LLC http://www.ettus.com*.

[35] Ettus, M. (2005). USRP User'sand Developer's Guide. *Ettus Research LL.*

[36] Mitola, Joe. "The software radio architecture." *Communications Magazine, IEEE* 33, no. 5 (1995): 26-38.

[37] Dillinger, Markus, Kambiz Madani, and Nancy Alonistioti. *Software defined radio: architectures, systems, and functions*. Wiley, 2003.

[38] Majo Boter, Marcos. "Design and implementation of an OFDM-based communication system for the GNU Radio platform." (2011).