الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم السعالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

En Télécommunication
Spécialité : Réseaux & Télécommunications

Présenté par

MEZIANE Amina

&

ZAIR Rania

Sécurisation des transmissions des drones face aux interférences par l'étalement du spectre DSSS

Proposé par : Mr. ANOU Abderrahmane

Année Universitaire 2023-2024

Remerciements

Avant toute chose, nous remercions Dieu tout Puissant, miséricordieux et clément, pour nous avoir donné santé, patience, volonté et courage.

Nous sommes reconnaissants envers Mr. ANOU Abderrahmane pour son encadrement attentif, ses conseils judicieux et son dévouement à l'avancement de nos travaux de recherche. Sa passion pour le domaine a été une source d'inspiration constante.

Nous adressons nos sincères remerciements aux membres du jury Mme REGUIEG F.Zohra et Mme AIT MASSAOUD Lisa pour avoir pris le temps d'examiner et évaluer ce travail.

Nous tenons à exprimer notre profonde gratitude envers toutes les personnes qui ont contribué à la réalisation de ce mémoire, directement ou indirectement.

Dédicaces

Nous dédions ce modeste travail : À nos parents, aucun hommage ne pourrait être à la hauteur du soutien qu'ils nous ont donné. À nos frères et sœurs, source de joie et de bonheur. À nos amis, pour leur soutien inébranlable, leurs encouragements et les moments de détente qui ont équilibré les rigueurs académiques. Enfin, nous dédions ce mémoire à tous ceux qui croient en l'importance de la recherche et de l'éducation, car c'est grâce à ces valeurs que nous façonnons un avenir meilleur.

Nous vous disons merci.

ملخص

أثار الاستخدام المتزايد للطائرات بدون طيار في مختلف القطاعات، سواء كانت مدنية أو عسكرية، مخاوف بشأن أمن نقل البيانات. في بحثنا، تم اقتراح تقنية مبتكرة : انتشار طيف التسلسل المباشر (DSSS). تتضمن هذه الطريقة توزيع إشارة الإرسال على نطاق تردد واسع، مما يجعل الاتصالات أقل عرضة للتداخل والتداخل المتعمدين. في عمليات محاكاة DSSS الخاصة بنا، استخدمنا نوعين من التعديل: تعديل سعة التربيع (QAM) وتعديل تحول الطور التربيعي (QPSK). يسمح تعديل QAM بإرسال المزيد من البيانات باستخدام مستويات السعة والطور المتعددة، مما يوفر نطاقاً ترددياً أعلى. يستخدم تعديل QPSK أربع مراحل متميزة لتمثيل البيانات، وهي فعالة من حيث عرض النطاق الترددي والمتانة ضد التداخل. تم اختبار تقنيتي التعديل هاتين لتقييم أدائهما من حيث مقاومة التداخل وكفاءة النقل في بيئات مختلفة. يمثل اعتماد DSSS في أنظمة اتصالات الطائرات بدون طيار خطوة مهمة إلى الأمام لحماية البيانات والموثوقية التشغيلية، خاصة في البيئات المعادية.

الكلمات المفتاحية: الأمن، الإرسال، التشويش، DSSS، الطائرات بدون طيار، QPSK، QAM .

Abstract

The increasing use of drones in various sectors, whether civil or military, has raised concerns about the security of data transmissions. In our research, an innovative technique was proposed : direct sequence spread spectrum (DSSS). This method involves spreading the transmission signal over a wide frequency band, making communications less vulnerable to intentional jamming and interference. In our DSSS simulations, In our DSSS simulations, we used two types of modulation: quadrature amplitude modulation (QAM) and quadrature phase shift modulation (QPSK). QAM modulation allows more data to be transmitted using multiple amplitude and phase levels, providing higher bandwidth. QPSK modulation uses four distinct phases to represent the data, which is efficient in terms of bandwidth and robustness against interference. These two modulation techniques have been tested to evaluate their performance in terms of interference resistance and transmission efficiency in various environments. The adoption of DSSS in drone communication systems represents a significant step forward for data protection and operational reliability, particularly in hostile environments.

Keywords: security, transmissions, jamming, DSSS, drones, QPSK, QAM.

Résumé

L'utilisation croissante des drones dans divers secteurs, qu'ils soient civils ou militaires, a soulevé des préoccupations quant à la sécurité des transmissions de données. Dans notre recherche, une technique innovant a été proposée : l'étalement de spectre à séquence directe (DSSS). Cette méthode consiste à répartir le signal de transmission sur une large bande de fréquences, rendant les communications moins vulnérables au brouillage intentionnel et aux interférences. Dans le cadre de nos simulations DSSS, nous avons utilisé deux types de modulation : la modulation d'amplitude en quadrature (QAM) et la modulation de déphasage en quadrature (QPSK). QAM permet une transmission accrue de données en utilisant plusieurs niveaux d'amplitude et de phase, offrant ainsi une bande passante plus élevée. QPSK utilise quatre phases distinctes pour la représentation des données, ce qui le rend plus efficace en termes de bande passante et de robustesse contre les interférences. Les deux techniques de modulation ont été testées pour leur résistance à l'enfouissement et leur efficacité de transmission dans divers environnements. L'adoption du DSSS dans les systèmes de communication des drones représente une avancée significative pour la protection des données et la fiabilité des opérations, notamment dans des environnements hostiles.

Mots Clée : sécurité, transmissions, brouillage, DSSS, drones, QPSK, QAM.

Table des matières

Introduction Générale **1**

1 Analyse et Applications des Drones **3**

1.1 Introduction . . . 3
1.2 Historique des Drones . . . 3
1.3 Classification des drones . . . 5
1.4 Types des drones . . . 6
1.4.1 Les drones aériens (UAV) . . . 6
1.4.2 Les drones terrestre (UGV) . . . 9
1.4.3 Les drones sous marins (UUV) . . . 9
1.4.4 Comparaison des différents types de drones . . . 10
1.5 Les applications des drones . . . 11
1.5.1 Applications civiles . . . 11
1.5.2 Applications militaires . . . 12
1.6 Principe de fonctionement et composants standard . . . 13
1.6.1 Système de propulsion . . . 14
1.6.2 Châssis . . . 15
1.6.3 Source et gestion de l'énergie . . . 15
1.6.4 Système nerveux central . . . 16
1.6.5 Charge utile . . . 16
1.6.6 Système de communication . . . 16
1.7 Sécurité de la transmission des données . . . 17
1.7.1 Technologie de communication utilisée dans les drones . . . 17
1.7.2 Protocoles de communication utilisé dans les drones . . . 20
1.7.3 Menaces et attaques liés à la transmission des données dans les drones . . . 25
1.7.4 Solutions pour renforcer la sécurité de la transmission des données . . . 25
1.8 Conclusion . . . 26

2 L'étalement de spectre à séquence directe DSSS **27**
2.1 Introduction . . . 27
2.2 Chaîne de transmission . . . 27
2.2.1 Bloc de codage source . . . 28
2.2.2 Bloc de codage canal . . . 28
2.2.3 Bloc d'étalement de spectre . . . 28
2.2.4 Bloc de modulation . . . 29
2.3 Principe de l'étalement de spectre . . . 32
2.4 Les techniques d'étalement de spectre . . . 35
2.5 Le systèmes DS-CDMA . . . 35
2.5.1 Les technique d'accès multiples . . . 35
2.5.2 Critère de choix sur les techniques d'accès . . . 36
2.5.3 Accès Multiple à Répartition de Code (CDMA) . . . 36
2.5.4 Caractéristique du CDMA . . . 37
2.5.5 Description de la technique CDMA . . . 38
2.5.6 L'étalement de spectre par séquence directe(DS-CDMA) . . . 39
2.5.7 Modulateur et Démodulateur DSSS . . . 41
2.5.8 Les canaux de transmission . . . 43
2.6 Avantages et inconvients du DS-CDMA . . . 44
2.7 Les codes d'étalement . . . 46
2.8 Caractéristiques de la séquence PN . . . 46
2.8.1 Propriété d'équilibre . . . 46
2.8.2 Distribution des longueurs d'exécution . . . 47
2.8.3 Autocorrélation . . . 47
2.8.4 Inter-correlation . . . 47
2.9 Les types des séquences d'étalement . . . 48
2.9.1 Les séquences à longueur maximale . . . 48
2.9.2 Séquences de Gold . . . 49
2.9.3 Séquence de kasami . . . 50
2.9.4 Séquence de walsh hadamard . . . 51
2.10 Synchronisation du code . . . 52
2.10.1 Acquisition initiale . . . 52
2.10.2 Poursuite du Code . . . 53
2.11 Conclusion . . . 54

3 Simulations et discussion des résultats **55**
3.1 Introduction . . . 55

3.2 Algorithme 55
3.3 Paramètre de simulation 56
3.4 L'implémentation du protocole TCP 57
3.4.1 Connexion TCP 57
3.4.2 Données Transmises 57
3.5 Résultats de Simulation 58
3.5.1 L'étalement de spectre à séquence directe 58
3.5.2 Signal modulé en QAM 61
3.5.3 Signal modulé en QPSK 64
3.5.4 Le bruit ajouté aux signal modulé 65
3.5.5 Le signal reçu avec bruit modulé en 128-QAM 65
3.5.6 Le signal reçu avec bruit modulé en QPSK 67
3.5.7 Signal démodulée à partir d'un signal QAM 67
3.5.8 Signal démodulée à partir d'un signal QPSK 69
3.5.9 Désétalement de spectre à séquence directe 69
3.6 Comparaison de BER en fonction de SNR 71
3.6.1 Le BER de 128 QAM et la QPSK 71
3.6.2 Le BER des différents M valeurs de QAM 72
3.6.3 Le BER des différents vitesses de déplacement 73
3.7 La reconstruction de l'image 74
3.8 Conclusion 75

Conclusion Générale **76**

Bibliographie **77**

Liste des Figures

1.1 Le Kettering Bug 4
1.2 Le DH 82B Queen Bee 5
1.3 Drone aile volante 6
1.4 L'hélicoptère est un sous-type de drone à voilure tournante 7
1.5 Configurations fréquentes des hélices des multicoptères. 7
1.6 Les drones multirotors (Quatre, six et huit hélices) 8
1.7 Un véhicule terrestre sans pilote tactique Gladiator 9
1.8 Le véhicule sous-marin sans pilote est sur le point de décoller 10
1.9 Schéma simplifié du fonctionnement d'un quadricoptère [1]. 14
1.10 Hélices horaires en carbone (noires), hêtre (beiges) ou nylon (grises) 14
1.11 Châssis d'un drone 15
1.12 Quelques batteries standards embarquées dans des drones 15
1.13 Format de paquet MAVLink V1 (8-263 octets) 21
1.14 Format de paquet MAVLink V2 (12-280 octets) 21
1.15 En-tête UDP 23
1.16 En-tête TCP 24

2.1 Schéma d'une chaîne de transmission 28
2.2 Schéma d'une Modulation 30
2.3 Schéma de constellation de la modulation QPSK 31
2.4 Les constellations 4, 16, 64 et 256 QAM [21]. 32
2.5 Processus d'étalement de spectre 33
2.6 Densité spectrale d'un signal avant, et après l'étalement de spectre 34
2.7 Accès Multiple à répartition de code 37
2.8 Liaison CDMA 38
2.9 Schéma général d'un système à étalement de spectre par séquence directe . . . 40
2.10 Principe d'étalement du spectre par séquence directe 41
2.11 Schéma d'un Modulateur DSSS 42

2.12 Schéma d'un Démodulateur DSSS 43
2.13 Les différents types des séquences d'étalement 48
2.14 Un générateur m-séquence 48
2.15 Un générateur de la séquence Gold 49
2.16 Circuit générique d'acquisition 53

3.1 Algorithme de la simulation 56
3.2 L'établissement de connexion tcp entre client et serveur 57
3.3 L'image transmis pour la simulation DSSS 58
3.4 L'étalement de spetre DSSS 59
3.5 La densité spectrale de puissance (PSD) d'un signal de données 60
3.6 La densité spectrale de puissance (PSD) d'un d'un signal encodé 61
3.7 La table de correspondance des symboles pour la modulation 128-QAM 61
3.8 constellation d'un signal transmis d'une modulation QAM 62
3.9 Signal modulé par 128-QAM 63
3.10 La densité spectrale de puissance du signal modulé en QAM 63
3.11 Signal modulé par la QPSK 64
3.12 La densité spectrale de puissance d'un signal modulé en QPSK 64
3.13 Le signal d'un bruit blanc Gaussien additif 65
3.14 La constellation d'un signal reçu avec bruit 65
3.15 Le signal reçu modulé en 128-QAM 66
3.16 La densité spectrale de puissance d'un signal reçu modulé en 128-QAM 66
3.17 Un signal reçu modulé en QPSK 67
3.18 La densité spectrale de puissance d'un signal reçu modulé en QPSK 67
3.19 Signal démodulé 68
3.20 La densité spectrale de puissance du signal démodulé 68
3.21 Signal demodulé 69
3.22 La densité spectrale de puissance du signal démodulé 69
3.23 Signal decodé 70
3.24 La densité spectrale de puissance d'un signal décodé 70
3.25 Le BER en fonction SNR pour les modulations 128 QAM et QPSK 71
3.26 Le BER en fonction SNR pour les modulations M-QAM 72
3.27 Comparaison de BER pour différents vitesses de déplacement 73
3.28 Les images reconstruites pour différentes résolutions 74

Liste des tableaux

1.1 Comparaison des différents types de drones 10
1.2 Technologies de communication sans fil utilisée dans les drones 17
1.3 Expliquation de chaque en-tête de protocole MAVLink 22

2.1 Caractéristiques de quelques standards de télécommunication 39

3.1 Les paramètre de simulation 56
3.2 Valeurs de BER pour les M-QAM modulations 73
3.3 Valeurs de BER pour les différents vitesses 74

Liste des abréviations

AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CAN	Convertisseur Analogique Numérique
CDMA	Code-Division Multiple Access
DS-CDMA	Direct-Sequence Code Division Multiple Access
DSP	Digital Signal Processing
DSSS	Direct Sequence Spread Spectrum
FDMA	Frequency-Division Multiple Access
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency Shift Keying
GPS	Global Positioning System
MAI	Multiple Access Interface
MAVLINK	Micro Air Vehicle Link
NRZ	Non Return to Zero
PAM	Pulse Amplitude Modulation
PN	Pseudo Noise
PSD	Power Spectral Density
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
SNR	Signal-to-Noise Ratio
TCP	Transmission Control Protocol
TDMA	Time-Division Multiple Access
THSS	Time Hopping Spread Spectrum
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UGV	Unmanned Ground Vehicle
UUV	Unmanned Underwater Vehicles
Wi-Fi	Wireless Fidelity

Introduction Générale

De nos jours, les drones ou UAV jouent un rôle essentiel dans la collecte d'informations à distance, même dans des endroits difficiles ou dangereux. Par exemple, la collecte d'informations est essentielle pour gérer les catastrophes naturelles, organiser les secours et améliorer l'évaluation d'un contexte de crise. Les drones modernes renforcent particulièrement les compétences des équipes de secours dans les opérations de collecte de données dans des situations complexes. Il est possible de déployer des drones pour explorer certaines zones d'inondation et trouver un chemin accessible pour rejoindre les personnes touchées. Ainsi, ils accroissent les capacités d'exploration des équipes de secours, mettant ainsi en danger leur propre sécurité. De plus, dans ce domaine, la mise en place de fonctions de détection de plus en plus avancées, ainsi que l'arrivée de mécanismes autonomes, permettront naturellement aux prochaines générations de drones d'être intégrés aux opérations de recherche, déchargeant ainsi les secouristes de ces tâches.

Afin de réaliser ces perspectives, il est nécessaire de relever deux défis. L'objectif principal est d'obtenir une autonomie adéquate pour ces véhicules, à la fois en ce qui concerne la navigation et l'interprétation des données détectées. Le deuxième point concerne la fiabilité de l'appareil et sa résistance aux agressions accidentelles ou criminelles. Les victimes et les sauveteurs sont confrontés à de nombreuses contraintes juridiques et éthiques en raison des risques potentiels liés à l'utilisation d'un drone, face à ces deux défis.

Les drones sont exposés à des attaques et des risques d'interférence, de brouillage, d'espionnage ou de piratage de leurs signaux radio notamment l'injection de fausses commandes afin de prendre le contrôle de l'UAV, l'accès frauduleux aux données de télémétrie et le piratage des données de télédétection, l'injection de données fabriquées dans le système afin de modifier le cours des opérations de recherche et de sauvetage, et par exemple d'en réduire l'efficacité et de les désorganiser et Le déni de service afin de nuire à ces mêmes opérations, notamment en réduisant les possibilités de communication avec le drone, Ces menaces peuvent compromettre la confidentialité, l'intégrité et la disponibilité des données transmises par les drones. Il faut donc trouver une technique robuste et efficace pour renforcer la sécurité de transmission dans les drones.

Afin de contrer les menaces liées à la transmission des données dans les drones, il est indispensable d'adopter une approche globale qui intègre des mesures techniques, réglementaires et éducatives pour garantir la sécurité des drones et de leurs opérations. Tel que :

- Le cryptage des communications
- Authentification et identification
- Détection des intrusions
- Les techniques de létalement de spectre La DSSS (direct sequence spread spectrum) et la FHSS (Frequency hopping spread spectrum)

Plusieurs techniques ont été proposé pour résoudre le problème de la sécurité des transmissions des données dans les drones. Dans notre travail actuel, nous intéressons à la technique d'étalement de spectre à séquence directe (DSSS) pour renforcer la sécurité des transmissions des drones contre le brouillage. Nous avons effectué une simulation de la technique DSSS à l'aide du langage de programmation Python, en utilisant un protocole serveur-client TCP pour transmettre une image dans un réseaux sans fil et nous ajoutons un bruit blanc gaussien additif, nous avons fait une étude comparative sur les deux types de modulations numériques (QAM & QPSK) utilisé dans la technique DSSS en termes de canal de transmission et le taux d'erreurs sur les bits (BER) en fonction de rapport signal sur bruit(SNR).

Le travail est compose de trois chapitre organisés comme suite :

— Chapitre 1 : Ce chapitre présente un aperçu complet des drones, de leur historique, des différents types, des applications, ainsi que de leurs opérations détaillées et des problèmes de sécurité liés à la transmission de données.

— Chapitre 2 : Le deuxiéme chapitre et dédié au principe de l'étalement de spectre, en particulier l'étalement de spectre par séquence directe qui est l'objet du notre travail.

— Chapitre 3 : Le troisiéme chapitre présente Les résultats de simulation de la technique d'étalement de spectre DSSS pour la sécurisation des transmission des drones.

Chapitre 1

Analyse et Applications des Drones

1.1 Introduction

Un drone, aussi connu sous le nom d'UAV (Unmanned Aerial Vehicle), est un véhicule aérien sans pilote qui peut être contrôlé à distance ou voler de façon autonome. Ces appareils sont équipés de systèmes de navigation et de capteurs, leur permettant d'effectuer diverses tâches [1]. Le mot « drone » est une extrapolation d'un terme anglais qui signifie « faux-bourdon ». En français, le terme est employé pour désigner des véhicules aériens, terrestres, de surface ou sous-marins, alors que la classification anglo-saxonne distingue chaque type d'appareil [2].

1.2 Historique des Drones

Les drones semblent être le produit des avancées technologiques contemporaines. En réalité, leur histoire s'étend sur plusieurs décennies, à l'instar de nombreuses autres avancées. En outre, le développement se poursuit afin de fournir au marché des drones toujours meilleurs et plus avancés qui sont facilement abordables pour les utilisateurs individuels [3].
Les drones proviennent de l'industrie militaire, comme c'est le cas de la majorité des découvertes techniques. L'idée de créer une machine volante sans pilote assis à l'intérieur a d'abord émergé vers la fin des années 1800. Bien qu'il n'y ait qu'une version très basique à l'époque (1849), les variations de vent et les conditions météorologiques les ont fait s'éloigner de leur cible prévue. Cela a été noté dans la première note enregistrée à ce sujet. Les premiers drones, des véhicules aériens sans pilote, ont été utilisés par les troupes autrichiennes pour attaquer Venise en 1849. Une minuterie a été utilisée pour faire exploser les explosifs dans les wagons de montgolfières. Le dispositif a été lancé au-dessus de la zone cible par la force du vent après que des réglages d'étalonnage basés sur des estimations préliminaires aient été effectués. Ces véhicules ne sont pas qualifiés de véhicules aériens sans pilote (UAV) car ils ne répondaient pas aux normes des

drones contemporains, tout en étant des aéronefs sans pilote qui n'étaient pas sous contrôle humain [3].

Le Kettering Bug (Figure 1.1), qui a été développé pendant la Première Guerre mondiale mais pas vraiment utilisé au combat, a été le prochain outil important. Bien qu'il ait l'apparence d'un avion à deux étages, c'était en fait une automobile à quatre roues fonctionnant sur des rails [3].

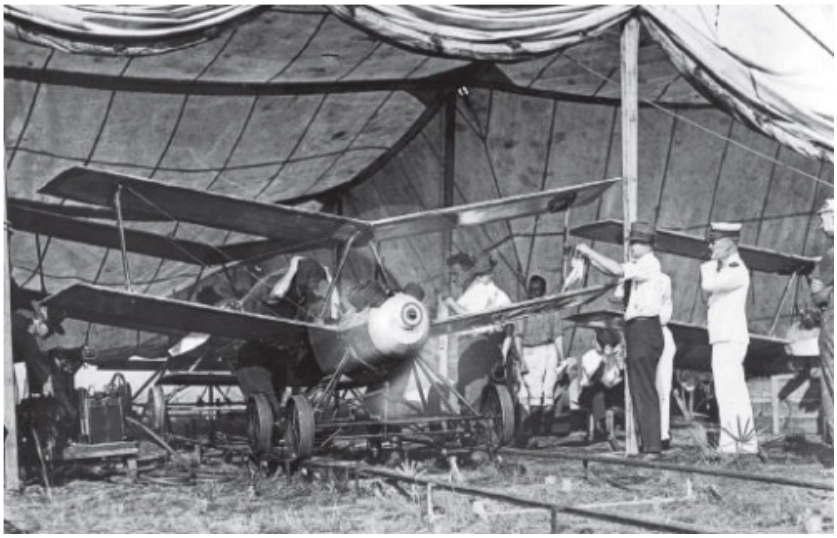


Figure 1.1: Le Kettering Bug

Dès qu'il s'est approché de la destination prévue, le moteur s'est coupé, les ailes se sont détachées du fuselage et le fuselage explosif s'est écrasé sur la terre comme une torpille. Bien qu'il n'ait pas pu atterrir, il n'était pas tenu de le faire comme prévu. Même s'il était incontrôlable, il avait des parties cruciales qui composaient le cadre des dispositifs télécommandés qui sont encore utilisés aujourd'hui. Un baromètre contrôlait l'altitude, tandis qu'un gyroscope contrôlait le cap [3].

Le DH 82B Queen Bee (Figure 1.2), le premier drone existant, a été utilisé par la Royal Navy britannique pour la pratique de la cible en 1935. C'était un gadget réutilisable qui pouvait atterrir, décoller et être contrôlé à distance, à condition qu'il ne soit pas gravement endommagé pendant l'exercice. En outre, le terme "drone" tel qu'il est utilisé aujourd'hui a également ses racines dans cet appareil,le commandant de la marine américaine Delmer Fahrney a été chargé de créer un gadget qui ressemblerait à la reine britannique Bee. Fahrney a appelé sa propre invention "drone", qui signifie abeille mâle, en hommage au nom de l'appareil original. Le terme est resté dans l'usage courant depuis [3].

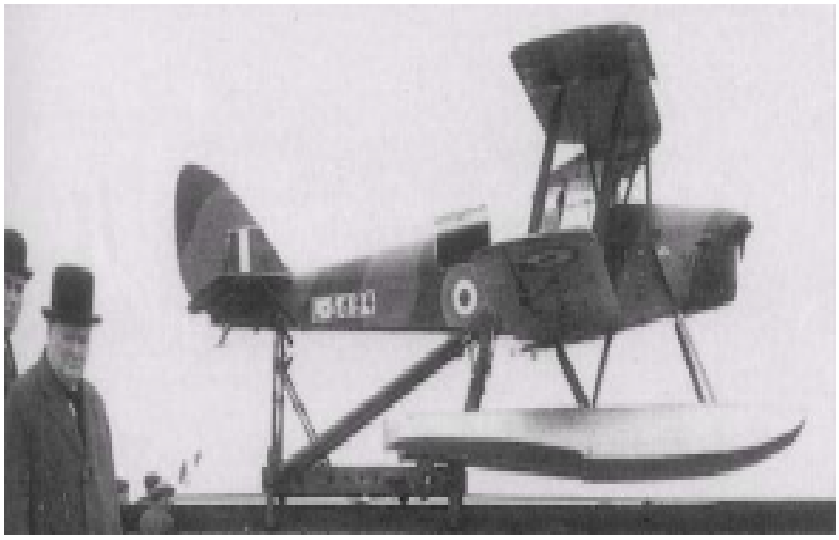


Figure 1.2: Le DH 82B Queen Bee

Les applications militaires pour les véhicules aériens sans pilote remontent au début du 20ème siècle. Depuis le tournant du 20ème siècle, ils ont été utilisés, même si l'armée en possédait déjà des milliers pour les utiliser dans des opérations d'espionnage et de reconnaissance ainsi que pour monter des armes et des explosifs sur eux pour des objectifs offensifs [3].
Les années 1950 ont vu l'adoption générale de la technologie des véhicules aériens sans pilote, qui à l'époque était principalement utilisée dans l'aviation militaire pour éduquer les unités de défense aérienne en utilisant des drones comme cibles mobiles. L'innovation dans les premières décennies du nouveau siècle était nécessaire pour permettre le déploiement de drones pour des applications tactiques directes et des missions de reconnaissance. Sous l'administration Obama, l'idée d'utiliser des drones à des fins tactiques de masse a été examinée plus sérieusement pour la première fois dans l'histoire des États-Unis. L'automatisation, la robotique et la communication machine à machine ont toutes considérablement progressé, ce qui a donné aux drones un nouveau rôle à cet égard [3].

1.3 Classification des drones

La classification des drones est un exercice très complexe, car elle varie en fonction des pays. Toutefois, il est possible de classer les drones aériens selon trois critères : l'altitude de croisière, l'endurance en termes de temps de vol et leurs dimensions principales [4].

- **L'altitude** en fonction de l'altitude de croisière à laquelle l'aéronef évolue, on peut les catégoriser en :
  — Aéronefs évoluent à moyen altitude 5 000 m <h< 15.000 m.
  — Aéronefs évoluent à haute altitude h> 20.000 m.

- **L'endurance** est en fait l'autonomie, c'est le temps que l'aéronef peut passer en vol. L'aéronef est qualifié de longue endurance lorsqu'il atteint 20 à 40 heures.
- **Le rayon d'action** c'est la portée maximale que peut réaliser l'aéronef plein carburant en altitude et vitesse de croisière.

1.4 Types des drones

1.4.1 Les drones aériens (UAV)

1.4.1.1 Voilure fixe

Pour les drones à voilure fixe, la capacité à contrecarrer la gravité est assurée par la présence d'une ou plusieurs ailes ennuyeux. Les contours spécifiques des ailes créent de la portance lorsqu'un avion est soumis à des vents relatifs.Les drones en forme d'avions standards entrent dans cette catégorie, ainsi que toute une gamme d'appareils aux formes plus originales. Lorsque les ailes ne peuvent pas être distinguées du fuselage de l'avion, elles sont souvent appelées «ailes volantes» (figure 1.3) [1].

Figure 1.3: Drone aile volante

Les drones à voilure fixe sont capables de voler sur de longues distances, ce qui les rend idéaux pour les missions d'arpentage et de cartographie. La nécessité de maintenir une vitesse de déplacement minimale et un contrôle limité des mouvements les empêche de manœuvrer avec précision autour des objets. De plus, leur décollage nécessite une vitesse horizontale initiale : ils doivent donc décoller pour commencer leur vol [1].

1.4.1.2 Voilure tournane

Pour les drones à voilure tournante, un ou plusieurs rotors assurent le maintien de l'appareil en l'air. Le corps de chaque hélice est parallèle au sol et exerce une force verticale sur l'air lors de sa rotation. Dans cette catégorie on retrouve des appareils similaires aux hélicoptères, mais aussi des drones aux formes plus spécifiques. Le principal avantage d'un drone à voilure

tournante est sa capacité à maintenir un vol stationnaire, ce qui permet de prendre des photos avec une meilleure stabilité et ainsi d'augmenter la perspective de l'objet d'intérêt [1].

Les hélicoptères sont bien connus dans les cercles traditionnels de l'aviation. Dans ce type d'appareil, un seul rotor maintient l'appareil en l'air. Empêcher l'appareil de s'allumer tout seul Lorsque le rotor principal tourne, selon le principe de la force d'action et de réaction, il est indispensable de prévoir un rotor de queue (ou rotor 'anticouple', figure 1.4) [1].

Figure 1.4: L'hélicoptère est un sous-type de drone à voilure tournante

Les drones multirotors, également appelés « multirotors » ou « multicopters » en anglais, sont extrêmement populaires. Ils sont équipés de plusieurs bras avec des hélices identiques aux extrémités. Le nombre d'hélices et leur configuration peuvent varier. La figure (Figure 1.5) montre également qu'il y a toujours une alternance du sens de rotation de l'hélice. En effet, si toutes les hélices tournent dans le même sens et à la même vitesse, l'appareil tournera naturellement autour de son centre de masse [1].

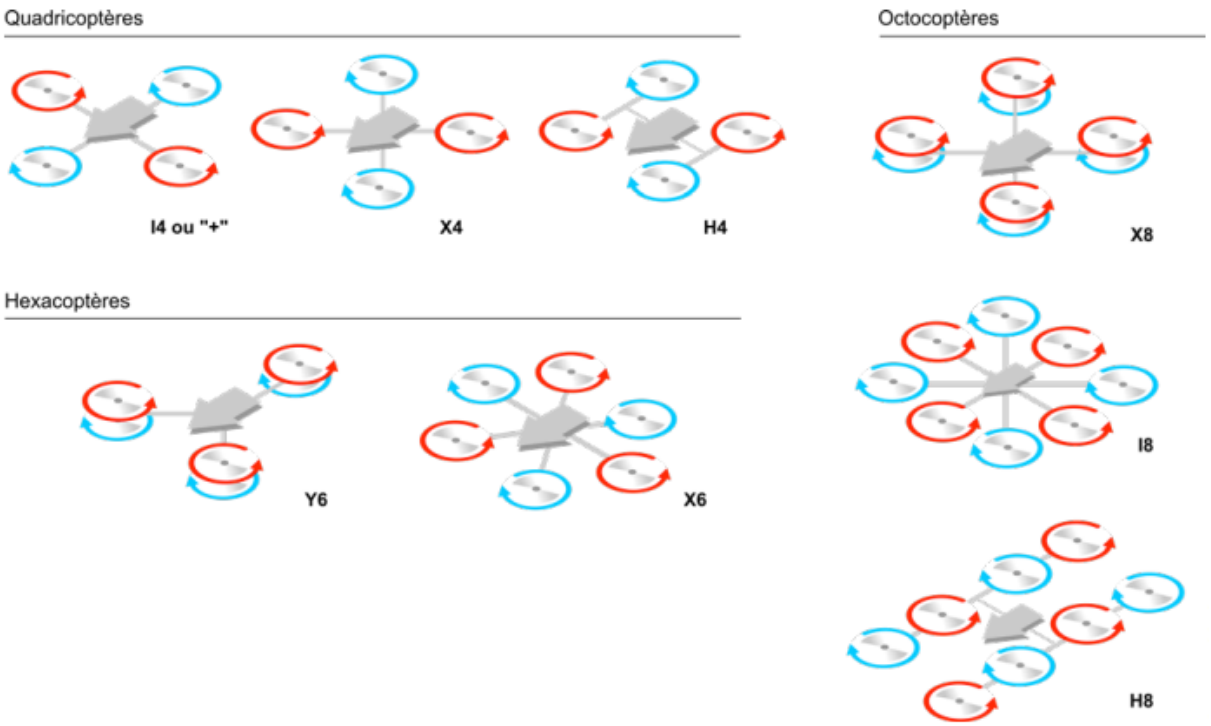


Figure 1.5: Configurations fréquentes des hélices des multicoptères.

Le nombre et la configuration des hélices ont une influence sur la stabilité de vol, l'autonomie et la sécurité. Les multicoptères à quatre hélices, ou 'quadricoptères' (Figure 1.6) connaissent un franc succès, en raison de leur bon rapport coût/performance.

Ils sont de conception simple, mais ne peuvent pas continuer à voler de manière stable si un de leur rotor s'arrête ou est endommagé. On comprendra donc que leur utilisation pour des missions impliquant de voler à proximité ou au-dessus des personnes n'est pas souhaitable. Les hélices sont parfois dédoublées sur chaque bras du drone (modèle Y6 ou X8, par exemple)(Figure 1.6), ce qui permet d'augmenter la sécurité de vol : en cas de défaillance d'un des rotors coaxiaux, l'appareil pourra continuer à voler de manière stable [1].

Figure 1.6: Les drones multirotors (Quatre, six et huit hélices)

1.4.1.3 Plus légers que l'air drone

Les UAV plus légers que l'air sont des aéronefs tels que les dirigeables et les ballons. Ces véhicules bénéficient d'un fonctionnement silencieux et d'une endurance. Avec leur capacité de vol à longue endurance, ces véhicules peuvent être utilisés pour la surveillance et la photographie aérienne.le véhicule [3].

1.4.1.4 Aile battante

L'ornithoptère ou "aile battante" utilise la mécanique de vol des oiseaux comme source d'énergie de l'UAV. Cette technologie a été utilisée par l'armée pour développer un petit UAV "semblable à un oiseau" capable de surveillance [5].

1.4.2 Les drones terrestre (UGV)

Ces dernières années, avec le développement rapide de techniques intelligentes, de techniques de capteurs et de techniques de contrôle des véhicules, les drones terrestre ou les véhicules terrestres sans pilote (UGV) (Figure 1.7) se développent rapidement pour les applications militaires et civiles. La principale caractéristique d'un drones terrestre est qu'il fonctionne sans présence humaine à bord.
Par conséquent, les UGV sont généralement développés pour des applications spéciales. Grâce à des modes de fonctionnement à distance ou autonomes, les UAV peuvent remplacer les humains pour diverses applications, telles que l'irrigation agricole, la logistique ou la livraison express dans des applications civiles, et la reconnaissance, le sauvetage, la recherche ou le combat dans des applications militaires [6].

Figure 1.7: Un véhicule terrestre sans pilote tactique Gladiator

1.4.3 Les drones sous marins (UUV)

Les véhicules sous-marins (UUVs) (figure 1.8) sont tous les types de robots sous-marins qui sont exploités avec un minimum ou sans intervention de l'opérateur humain. Dans les littératures, l'expression est utilisée pour décrire à la fois un véhicule télécommandé (ROV) et un véhicule sous-marin autonome (AUV). Dans le domaine de l'installation, de l'inspection et de la réparation sous l'eau, les robots téléguidés (ROV) sont principalement utilisés. Ils ont été largement utilisés dans les industries offshore en raison de leurs avantages par rapport aux plongeurs humains en termes de sécurité plus élevée, de plus grandes profondeurs, d'endurance plus longue et de moins de demande d'équipement de soutien. Dans son fonctionnement, le ROV

reçoit des instructions d'un opérateur à bord d'un navire de surface (ou d'une autre plate-forme d'amarrage) via un câble attaché ou une liaison acoustique. Les UAV, quant à eux, fonctionnent sans surveillance et supervision constantes de la part d'un opérateur humain. En tant que tel, les véhicules n'ont pas le facteur limitant dans leur plage de fonctionnement du câble ombilical généralement associé aux ROV. Cela permet d'utiliser des UAV pour certains types de missions, comme la collecte de données océanographiques à grande distance lorsque l'utilisation de ROVS est peu pratique [7].

Figure 1.8: Le véhicule sous-marin sans pilote est sur le point de décoller

1.4.4 Comparaison des différents types de drones

Ce tableau (Tableau 1.1) couvre les principales caractéristiques des différents types de drones :

Caractéristiques	**Drones terrestres**	**Drones aériens**	**Drones sous-marins**
Milieu d'opération	Sol	Air	Sous l'eau
Utilisations typiques	Surveillance, livraison agriculture	Surveillance, cartographie, livraison, loisirs	Recherche océanographique, inspection des infrastructures sous-marines, exploration
Avantages	Facilité d'accès et de contrôle, robustesse	Vitesse et couverture étendue, accès à des zones difficiles d'accès	Exploration en profondeur et capacité à fonctionner dans des environnements hostiles
Inconvénients	Limités par les obstacles physiques, dépendants des routes	Dépendants des conditions météorologiques, autonomie limitée par la batterie	Limités par la profondeur de plongée, communication et récupération complexes

Tableau 1.1: Comparaison des différents types de drones

1.5 Les applications des drones

Les drones sont utilisés dans de nombreux domaines civiles et militaires.

1.5.1 Applications civiles

1.5.1.1 Photographie

La photographie aérienne est l'une des utilisations les plus intéressantes des drones. Cette technologie est équipée d'un matériel de prise de vue robuste qui permet aux passionnés de fournir facilement des images aériennes des zones désignées. La photographie aérienne par drone peut produire des images claires et nettes. Outre la possibilité de transmettre des images en direct par Wi-Fi, vous avez également le droit d'exiger une observation de première main des mouvements des drones. Les drones les plus efficaces pour la photographie cinématographique évoluent grâce à la transmission en direct de vidéos aériennes [8].

1.5.1.2 Transport et livraison

L'utilisation de drones pour le transport et la livraison permet de réduire les délais de livraison, d'améliorer l'efficacité du système et d'éliminer le travail humain pour des tâches telles que la livraison de pizzas, de lettres et de petits colis [8].

1.5.1.3 La gestion des catastrophes

La gestion des catastrophes est l'une des principales utilisations des drones. Après une catastrophe, on constate généralement un chaos total dans l'acheminement des ressources en un instant. L'équipe d'intervention dans la région touchée a besoin d'être secourue, et les drones sont un élément clé de cet effort. Ces drones sont équipés de caméras puissantes et uniques qui leur permettent de filmer les personnes et les biens touchés et de sauver ainsi des vies [8].

1.5.1.4 Cartographie géographique

Le domaine de la cartographie géographique en 3D a grandement bénéficié de l'utilisation des drones. Dans le monde entier, de nombreux endroits sont inaccessibles à l'homme. Il peut s'agir d'un littoral dangereux ou de sommets alpins inaccessibles. À l'exception de la création de cartes en 3D prêtes à l'emploi et de l'intention d'acquérir des connaissances sur une parcelle. L'utilisation de drones pour la cartographie géographique est essentielle pour s'assurer que les emplacements et les sites nécessaires sont capturés pour les procédures de cartographie. Grâce aux drones, les géologues peuvent désormais obtenir plus facilement des informations vitales [8].

1.5.1.5 Prévisions météorologiques

Les drones sont utilisés pour les prévisions météorologiques, ou la prévision des conditions atmosphériques. Ces véhicules aériens sans pilote (UAV) ont la capacité d'enregistrer des séquences pendant les tempêtes et les tornades, ainsi que de tester les tendances et les occurrences. D'autre part, les drones constituent un moyen rentable d'effectuer des tâches de prévision météorologique. Les drones supplémentaires peuvent être lancés lorsque les drones détectent une tempête en approche ou, à l'inverse, une perturbation potentiellement dangereuse. Pour ce faire, un essaim de véhicules aériens sans pilote (UAV) peut communiquer entre eux afin de déterminer la meilleure façon d'examiner cette région de l'environnement, en recueillant des données supplémentaires et en utilisant divers modèles de mobilité en fonction des besoins [8].

1.5.1.6 Agriculture

Les drones sont de plus en plus utilisés dans l'agriculture en raison de leur facilité et de leur rapidité à arpenter de grandes parcelles ouvertes, ce qui peut prendre du temps et être encombrant à pied. Les drones peuvent effectuer diverses activités agricoles, telles que la pulvérisation de nutriments et de pesticides sur les plantes, la réalisation d'études préventives et l'évaluation de l'état de développement des plantes et des niveaux d'infection. Les données obtenues à partir de ces études peuvent être utilisées pour le traitement et l'intervention. L'évaluation de l'état des plantes est cruciale car elle permet au drone programmé d'émettre du matériel supplémentaire dans les zones où il est nécessaire, assurant ainsi un soin et une protection efficaces des plantes. Cette méthode garantit également une récolte de qualité uniforme pendant la période de culture‘ [3].

1.5.2 Applications militaires

1.5.2.1 Reconnaissance des bombes

La petite taille des drones pénètre parfois dans les zones restreintes. Les caméras efficaces étant élevées permettent aux UAV d'effectuer la fonctionnalité appropriée de reconnaissance de bombe. Les États-Unis ont développé ces drones pour alerter les gens sur les bombes souschargées et sauver leurs vies [8].

1.5.2.2 Surveillance

La plupart des enquêtes sont menées aux endroits choisis pour vérifier la sécurité dans la région. À l'ère du numérique, les méthodes traditionnelles pour assurer la sécurité sont inappropriées. Les drones, en revanche, sont cruciaux pour la surveillance, ce qui est une option

potentiellement remarquable. Ils vont non seulement réduire les efforts et vous fournir un champ de vision plus large, mais ils vous permettront également d'obtenir plus d'informations dans un laps de temps plus court. Il s'agit d'une approche simple et abordable qui n'a pas d'impact négatif sur la vie des gens [8].

1.5.2.3 Frappe aérienne

L'utilisation des drones pour les frappes aériennes est courante. Une agence gouvernementale a déclaré qu'ils attaquaient souvent les insurgés dans les pays asiatiques avec ces véhicules aériens sans pilote. Contrôlé par les responsables de la défense, il s'attarde autour des sites suspects indiqués. Pour répondre aux exigences militaires ou obtenir des connaissances sur des sujets spécifiques, il peut être envoyé à une zone spécifique [8].

1.5.2.4 Sécurité

Les drones doivent être déployés dès que possible pour des raisons de sécurité. En outre, du point de vue de la protection de la vie privée, les drones sont utilisés par les voyeurs et les paparazzi pour prendre des photos de groupes de résidents à leur domicile ou dans d'autres lieux qui étaient auparavant considérés comme privés. L'essaim de drones peut être déployé dans des endroits considérés comme très probablement dangereux, tels que les zones métropolitaines et les aéroports proches du terrain d'atterrissage. Néanmoins, les drones sont essentiels pour assurer la sécurité. Il s'agit d'un domaine important [8].

1.6 Principe de fonctionement et composants standard

Un drone est un appareil volant qui utilise un système de propulsion. Un drone classique possède plusieurs rotors, habituellement quatre, qu'on désigne sous le nom de quadricoptère. L'action de ces rotors est assurée par des moteurs électriques, fournissent la force requise pour s'élever et se déplacer dans l'espace. En ajustant la vitesse de rotation de ces rotors, le drone a la possibilité de changer de direction, de faire demi-tour ou de tourner sur lui-même.
La figure (Figure 1.9) montre le schéma simplifié du fonctionnement d'un drones, il est équipé de capteurs intégrés, comme des gyroscopes et des accéléromètres, qui lui permettent de maintenir son équilibre et de modifier sa position. Le contrôleur de vol exploite les informations collectées par ces capteurs afin de maintenir son appareil en vol. Le GPS, la détection des obstacles et la prévention des collisions, les caméras et les logiciels sont d'autres caractéristiques essentielles qui améliorent le fonctionnement d'un drone, La figure 1.9 représente schéma de fonctionnement d'un drone.

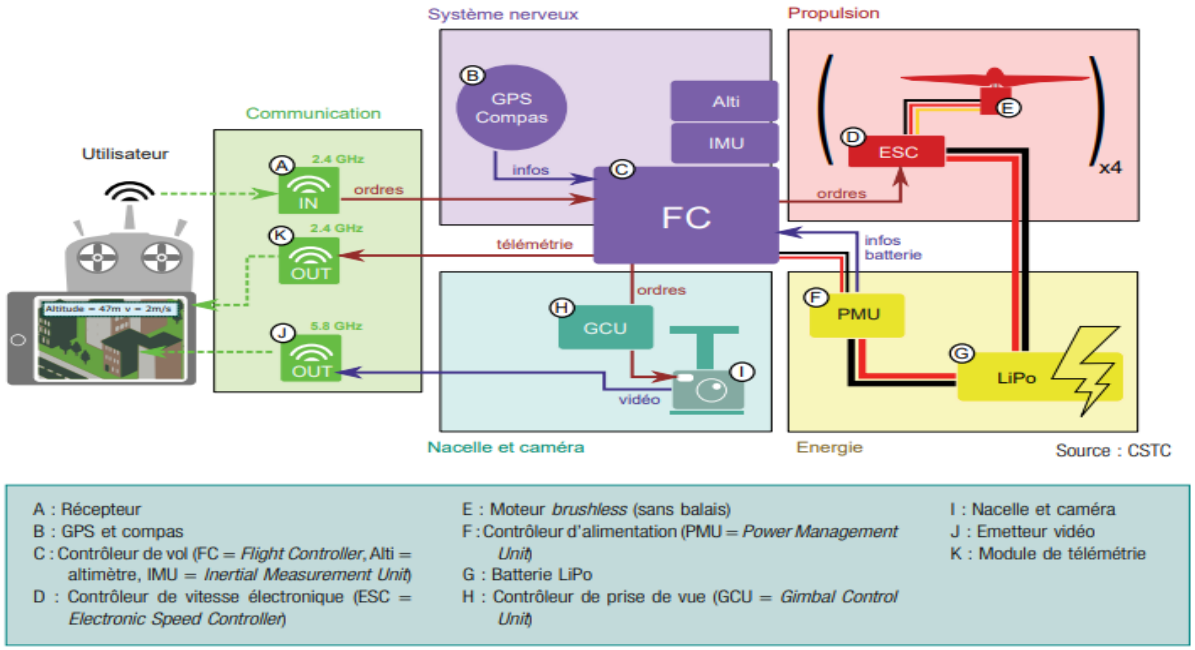


Figure 1.9: Schéma simplifié du fonctionnement d'un quadricoptère [1].

1.6.1 Système de propulsion

Toutes les hélices (Figure 1.10) du multicoptère sont reliées à un moteur qui convertit l'énergie électrique des batteries en énergie mécanique de rotation. Les moteurs à courant continu sans balais, également connus sous le nom de « moteurs brushless », sont actuellement les principaux acteurs du marché des drones professionnels. Un petit circuit électrique nommé « Electronic Speed Controller » (ESC) transforme le courant continu issu de la batterie en un signal approprié au moteur. Chaque ESC a la possibilité de réguler la vitesse de rotation du moteur qui lui est lié. Ainsi, les ESC jouent un rôle essentiel dans la maîtrise des mouvements d'un drone : ils offrent la possibilité d'agir de manière autonome sur chaque moteur et donc sur chaque hélice [9].

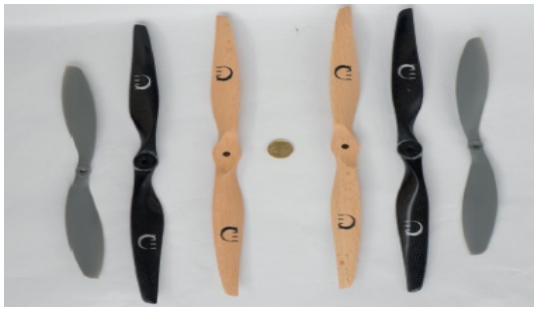


Figure 1.10: Hélices horaires en carbone (noires), hêtre (beiges) ou nylon (grises)

1.6.2 Châssis

Le châssis (Figure 1.11) représente la structure du drone sur laquelle tous les autres éléments, tels que les pièces électroniques, les moteurs et les divers capteurs, sont fixés. La forme de cette structure peut varier considérablement en fonction du type de drone. En termes de puissance, un drone composé de composants plus légers sera capable de supporter une charge plus élevée. Cela justifie la quête constante de matériaux légers et solides pour la construction du châssis.quelle que soit la configuration de chaque moteur et donc de chaque hélice [1].

Figure 1.11: Châssis d'un drone

1.6.3 Source et gestion de l'énergie

Les batteries utilisées dans la plupart des multicoptères électriques sont de type lithium-ion-polymer ou LiPo (Figure 1.12). Ces types de batteries offrent une capacité d'emmagasinage adéquate et leur poids est inférieur à celui des batteries lithium-ion, même à une capacité similaire. Autrement dit, elles ont le rapport puissance/masse le plus élevé. Par ailleurs, leur capacité à décharger rapidement, grâce à leur faible résistance interne, s'avère extrêmement bénéfique. Ce genre de batterie présente cependant un risque élevé d'incendie, et il est donc primordial de prendre en considération ce risque lors de leur utilisation, de leur chargement et de leur stockage [1].

Figure 1.12: Quelques batteries standards embarquées dans des drones

Les pilotes de drones doivent connaître le niveau de la batterie du drone pour anticiper les

atterrissages. Si la batterie est faible, une séquence d'atterrissage d'urgence peut se produire. Les drones modernes sont équipés de systèmes de surveillance continue de la batterie afin d'accroître la sécurité. Certains drones utilisent un microcontrôleur appelé unité de gestion de l'énergie (PMU) pour gérer l'énergie [1].

1.6.4 Système nerveux central

Le contrôleur de vol, également connu sous le nom d'autopilote et parfois appelé MCU (pour 'Microcontroller Unit') ou FC (pour 'Flight Controller'), convertit les ordres coordonnés de la télécommande en ordres coordonnés qu'il envoie aux ESC. Il passe du mode « télécommande » (pousser le manche de contrôle gauche vers le haut, par exemple) au mode « mouvements » (effectuer une translation vers le haut) [1].
Les drones récents sont équipés d'un large éventail de systèmes électroniques et peuvent être ajustés en permanence. Les corrections reposent sur des mesures concrètes effectuées à l'aide de capteurs de vol, qui permettent au drone d'évaluer sa situation : magnétomètre, gyroscopes, accéléromètres ou encore capteurs de pression. La mesure inertielle, également connue sous le nom d'IMU 'Inertial Measurement Unit', est le système électronique qui regroupe les informations de mouvement et les envoie au contrôleur de vol. En cas d'utilisation d'un GPS, le drone pourra même évaluer sa position géographique et éventuellement suivre un itinéraire préétabli. La géolocalisation permet également d'identifier les informations recueillies pendant le vol [1].

1.6.5 Charge utile

Le poids du passager à transporter pour effectuer la mission est connu sous le nom de charge utile. Il est possible que cela implique des capteurs tels qu'un appareil photo, une caméra thermique, une caméra Lidar multispectrale, un capteur de radiation ; ou encore un produit à pulvériser ou à transporter. Tout est possible d'emporter dans un drone, à condition que ce soit de petite taille, léger (au maximum 20 % de la masse totale du drone) et bien protégé [5].

1.6.6 Système de communication

Le système de communication radio assure l'interface entre l'humain et le drone, permettant au télépilote d'envoyer des commandes via une radio-commande vers un récepteur installé sur le drone. Ce dernier peut transmettre des informations telles que l'altitude, la vitesse et le pourcentage de batterie disponible, un processus appelé télémétrie. Les bandes de fréquences de 2,4 GHz et 5,8 GHz sont couramment utilisées pour ces communications. Les radio-commandes, souvent à six canaux comme celles du modélisme, comportent deux manches de contrôle et divers boutons ou commutateurs, ainsi qu'un écran LCD pour la programmation et l'affichage

des paramètres de vol. Un retour vidéo en temps réel depuis la caméra embarquée est souvent essentiel pour le télépilote, permettant de surveiller le vol et de cadrer les images à filmer. La qualité des équipements vidéo varie selon les besoins, un investissement dans une haute qualité étant justifié pour des missions nécessitant des décisions rapides [1].

1.7 Sécurité de la transmission des données

La protection des informations dans les drones revêt une importance capitale pour diverses raisons. En premier lieu, les drones rassemblent et envoient une grande quantité de données sensibles, telles que des images, des vidéos et des informations télémétriques, qui peuvent être exploitées dans des domaines essentiels tels que la surveillance, la cartographie et les inspections industrielles. Il est crucial de garantir la protection de ces données afin d'éviter toute interception, manipulation ou vol par des tiers non autorisés, ce qui pourrait mettre en péril la confidentialité et l'intégrité des données.
Par la suite, il est possible d'utiliser des drones dans des environnements sensibles tels que les infrastructures critiques, les sites militaires ou les espaces aériens restrictifs. Dans ces situations, une atteinte à la sécurité des données pourrait engendrer des dangers importants pour la sécurité nationale ou publique.

1.7.1 Technologie de communication utilisée dans les drones

Les technologies de communication sans fil jouent un rôle crucial en facilitant la transmission de données pour les drones. Avec la capacité de communiquer des données sans fil, les drones peuvent désormais être contrôlés à distance, ce qui permet une plus grande flexibilité et une meilleure efficacité opérationnelles. Le tableau 1.2 présente les technologies de communication sans fil les plus récentes utilisées dans les drones et les paramètres correspondants [10].

Technologie Sans Fil	Portée	Utilisation d'Énergie	Fréquence/Bande Passante
Bluetooth	10m	Faible	2.4 GHz
Bluetooth Faible Énergie	8-10m	Très faible	2.4 GHz
Wi-Fi	100m	Moyenne	2.4 GHz, 5 GHz
ZigBee	100-1500m	Faible	868 MHz, 915 MHz, 2.4 GHZ
LoRaWAN	30km	Faible	500 MHz, 868 MHz, 900 MHz
Narrow Band-IoT	10km	Faible	450 MHz, 3.5 GHz
Réseau 5G	30km	Faible-Haute	200 KHz, 900 KHz

Tableau 1.2: Technologies de communication sans fil utilisée dans les drones

1.7.1.1 Bluetooth

La technologie sans fil Bluetooth vise à remplacer les fils traditionnels entre les gadgets personnels comme les ordinateurs portables, les téléphones portables et les appareils photo numériques. Il fournit un connecteur de câble flexible avec des configurations de broches personnalisables, permettant à plusieurs appareils portables de communiquer entre eux. Bluetooth utilise la norme IEEE 802.15.1 et dispose de quatre paramètres de débit de données pour différentes distances de transmission : 2 Mbps, 1 Mbps, 500 kbps et 125 kbps [10].
Les drones Bluetooth sont conviviaux et abordables. Ils sont équipés de capteurs avancés pour la navigation sur divers terrains et environnements. Les drones Bluetooth sont également portables en raison de leur taille plus petite et plus légère. Cependant, Bluetooth UAS (Unmanned Aerial Systems) ont quelques inconvénients, y compris l'interférence potentielle d'autres dispositifs électroniques, faible puissance du signal sur de longues distances, capacité de charge utile limitée pour des applications plus lourdes, et des dommages potentiels dans des conditions venteuses en raison de leur petite taille.
La technologie sans fil Bluetooth offre flexibilité et commodité aux utilisateurs de drones, mais elle présente également des inconvénients. Il ne convient pas aux applications à longue distance en raison de la faible force du signal, et sa petite taille le rend inadapté à certaines applications [10].

1.7.1.2 Bluetooth Faible Énergie (BLE)

La technologie Bluetooth Faible Énergie (BLE) est utilisée pour le contrôle sans fil et la transmission de données des drones, offrant une latence et une efficacité énergétique moindres. Les drones BLE peuvent communiquer avec d'autres appareils, permettant un transfert de données efficace et une gestion à distance. Ils sont idéaux pour la surveillance, la cartographie, la reconnaissance aérienne et les applications de surveillance des actifs. BLE UAS peut être facilement intégré à d'autres systèmes d'entreprise, permettant un échange de données transparent et une prise de décision plus rapide. Cependant, ils ont des limites telles qu'une autonomie limitée, une durée de vie plus courte et des coûts plus élevés. Pour surmonter ces inconvénients, des protocoles de communication fiables, des considérations de conception pour les interférences et des tests et une maintenance approfondis sont essentiels. En abordant ces questions, les systèmes BLE UAS peuvent fournir des solutions fiables et rentables pour diverses applications [10].

1.7.1.3 Wi-Fi

Wi-Fi (Wireless Fidelity) est une technologie sans fil qui connecte les appareils électroniques via des réseaux sans fil (WAN), permettant la transmission de données sur le réseau. Il est idéal

pour la diffusion en direct et les applications de collecte de données en temps réel dans les drones. Les cartes d'extension internes ou les périphériques USB ou PCI externes permettent la communication sans fil via la technologie Wi-Fi ou Bluetooth. Ils jouent un rôle crucial dans le contrôle des drones, permettant le contrôle à distance ou le vol en formation, mais l'interférence peut causer des difficultés de contrôle. Les progrès technologiques dans les technologies radar, GPS et de suivi peuvent aider à détecter et à éviter les avions à proximité [10].

1.7.1.4 Zigbee

Zigbee est une technologie sans fil populaire en raison de sa faible consommation d'énergie, ce qui le rend idéal pour des applications comme les UAS. Cependant, il est confronté à des défis tels que les interférences potentielles des appareils et les problèmes de latence potentiels. Pour résoudre ces problèmes, les organisations devraient se concentrer sur le développement de technologies qui minimisent la latence et l'interférence, améliorent la portée et la précision de la transmission des données et établissent des protocoles de cybersécurité pour protéger les données et les réseaux UAS contre les menaces malveillantes. En investissant dans ces domaines, les organisations peuvent réduire efficacement les impacts et améliorer les capacités globales de la technologie Zigbee [10].

1.7.1.5 LoRaWAN

LoRaWAN est une technologie sans fil développée pour les applications de l'Internet des objets (IoT), offrant efficacité énergétique, abordabilité, dynamique, fiabilité et communication duplex. Il est souvent utilisé dans les drones pour couvrir des zones tout en conservant la puissance. Cependant, LoRaWAN a des limites, comme une portée de 10 km avant d'exiger la proximité d'une passerelle, ce qui limite son applicabilité dans les scénarios à longue distance. En outre, il a une vitesse maximale d'environ 20 km / h. Pour remédier à ces limites, des mesures sont prises pour assurer une utilisation efficace des systèmes UAS LoRaWAN. Dans l'ensemble, LoRaWAN offre une solution prometteuse pour un réseau sans fil économe en autonomie et à faible consommation [10].

1.7.1.6 Narrow Band-IoT

NB IoT, ou Internet des objets de nouvelle génération (IoT), est une technologie de radiofréquence conçue pour les applications à faible bande passante et longue durée de vie des batteries dans les zones à couverture limitée, telles que les sous-sols ou les régions rurales. Développé par 3GPP, il est idéal pour les appareils comme les moniteurs cardiaques et les capteurs de sécurité. NB IoT fonctionne sur un spectre, assurant la qualité de service et la sécurité. Il trouve des

applications dans les compteurs intelligents, les systèmes de suivi des actifs, les configurations de sécurité et les solutions de surveillance environnementale [10].
NB IoT améliore la consommation d'énergie et l'efficacité spectrale tout en offrant des avantages de couverture et de capacité. Cependant, il présente des inconvénients tels que des débits de données limités, une portée limitée et une durée de vie de la batterie plus courte par rapport aux UAS. Pour remédier à ces limitations, une bande passante plus large pourrait être utilisée, ce qui permettrait de recevoir plus de données et d'améliorer la qualité des données [10].

1.7.1.7 Réseau 5G

Le réseau 5G est une innovation technologique qui utilise les ondes radio pour fournir une plus grande capacité de données et des vitesses plus élevées tout en maintenant la vitesse et la fiabilité. Cependant, des technologies supplémentaires telles que le beamforming et le MIMO sont nécessaires pour optimiser la direction et la transmission du signal en raison de sa portée limitée et de sa sensibilité aux interférences.
Les véhicules aériens sans pilote (UAV) peuvent bénéficier de la 5G en ayant une connectivité haute vitesse sans latence, ce qui facilite les opérations en essaim et les missions plus sûres. En outre, il facilite le transfert rapide des données et la diffusion vidéo en temps réel pour une utilisation dans la cartographie, les services de livraison, la surveillance et les activités de recherche et sauvetage. Cela s'accompagne de dépenses de déploiement et de difficultés d'infrastructure qui peuvent être évitées en travaillant avec des fournisseurs de services spécialisés dans la 5G pour les drones et en utilisant les ressources d'infrastructure déjà existantes [10].

1.7.2 Protocoles de communication utilisé dans les drones

1.7.2.1 Le protocole Mavlink (Micro Air Vehicle Link)

Le protocole de communication open source le plus populaire et le plus léger pour les véhicules aériens sans pilote s'appelle Mavlink (Micro Air Vehicle Link). Il permet la communication bidirectionnelle entre l'UAV et la station de contrôle au sol et est pris en charge par plusieurs UAV et systèmes de pilote automatique. Des détails essentiels concernant l'état de l'UAV et les commandes de contrôle fondamentales transmises entre l'UAV et le GCS sont inclus dans les communications [11].
Lorenz Meier a rendu MAVLink 1.0 disponible sous licence LGPL début 2009. La version la plus récente suggérée du protocole MAVLink est la version 2.0, qui a été publiée au début de 2017. Il a diverses améliorations par rapport à MAVLink 1.0 et est également rétrocompatible avec cette version [12].
Le protocole MAVLink spécifie comment les messages sont sérialisés à la couche d'application

et leur structure. Les couches les plus basses du réseau (la couche de transport et la couche physique, par exemple) sont alors informées de ces messages. En raison de sa conception légère, le protocole MAVLink a l'avantage de prendre en charge une variété de couches de transport et de supports. Il peut être envoyé par Ethernet (c.-à-d., réseaux TCP/IP), WiFi ou fréquences sub-GHz, telles que 433 MHz, 868 MHz, ou 915 MHz, canaux série de faible bande passante de télémétrie. Les fréquences sub-GHz permettent la communication longue distance et le contrôle à distance du système sans pilote [13].
Mavlink ne crypte pas les communications afin de maximiser l'efficacité et la vitesse des transferts. Par conséquent, le protocole est sensible à une gamme de menaces de sécurité, y compris DDoS, spoofing GPS, et l'écoute clandestine [11].

— **structure de paquet**

Caque message MAVLink a un en-tête qui est ajouté à la charge utile de données du message. Alors que les données effectuées par le message sont contenues dans la charge utile, l'en-tête contient des informations sur le message lui-même. Le but de la somme de contrôle est de confirmer que le message est intact et ne doit pas être modifié pendant la transmission [12].

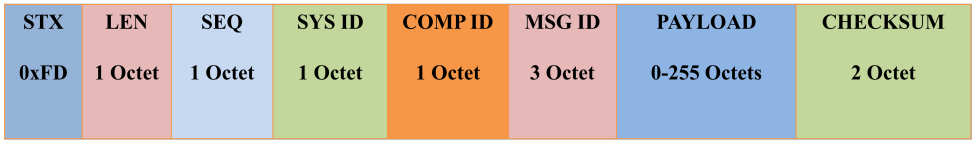


Figure 1.13: Format de paquet MAVLink V1 (8-263 octets)

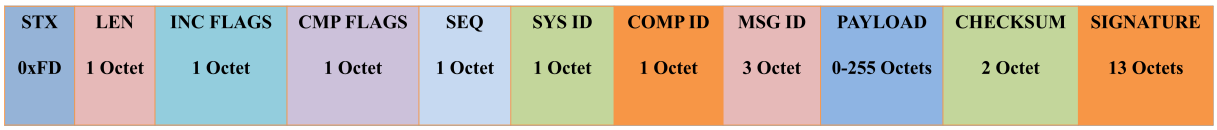


Figure 1.14: Format de paquet MAVLink V2 (12-280 octets)

Le tableau 1.3 explique chaque en-tête MAVLink 1.0 et 2.0 [13].

Acronyme	Contenu	Description
STX	0xFE	Indique le début de la trame
LEN	1 octet	Taille du message en octets
INC FLAGS	1 octet	Indicateurs d'incomptabilité
CMP FLAGS	1 octet	Indicateurs de comptabilité
SEQ	1 octet	Numéro de séquence pour la détection des pertes
SYS	1 octet	Identifiant du système émetteur
COMP	1 octet	Identifiant du type de message
MSG ID	3 octet	Identifiant du type de message
PAYLOAD	0 à 255	Données du message.
Checksum	2 octet	Check-sum du paquet entier
SIG	13 octets	Signature pour l'authentification du message.

Tableau 1.3: Expliquation de chaque en-tête de protocole MAVLink

1.7.2.2 Les protocoles TCP/UDP

Dans les réseaux informatiques, les deux protocoles IP TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) sont le plus souvent utilisés. Alors que UDP est un protocole sans connexion qui échange des datagrammes, la perte de paquets peut se produire et les données reçues avec UDP ne sont pas ordonnées. TCP est un protocole orienté vers la connexion qui nécessite une poignée de main à trois voies [14].
En raison de sa stabilité grâce aux reconnaissances et aux techniques de gestion de la congestion, le TCP semble être un bon choix pour la majorité du trafic C&C (Command and Control) dans le contexte des protocoles utilisés dans les UAV pour la communication serveur sur un réseau mobile. UDP peut être utilisé pour la direction directe du stick en C&C car il a moins de latence et peut fonctionner en temps réel. En outre, en raison de l'absence de procédures de poignée de main et de retransmission, l'UDP convient au trafic de données d'application qui n'est pas pertinent pour la sécurité, comme la transmission vidéo. D'autre part, TCP a d'abord été créé pour les réseaux avec de faibles taux d'erreur binaire [14].

Le protocole UDP

UDP est un protocole de transport qui transforme la livraison de paquets d'hôte à hôte en une communication de processus à processus. Il nécessite un démultiplexage pour permettre à plusieurs processus d'application sur chaque hôte de partager le réseau. Le principal problème de l'UDP est l'adresse utilisée pour identifier un processus. Bien qu'il soit possible d'identifier directement un processus avec un identifiant attribué par le système d'exploitation (pid), cela n'est pratique que dans un système distribué proche, avec un système d'exploitation attribuant des identifiants uniques à tous les processus. Au lieu de cela, un processus est indirectement identifié à l'aide d'un localisateur abstrait, appelé port. L'en-tête UDP contient un numéro de port de 16 bits pour l'expéditeur et le destinataire [15].

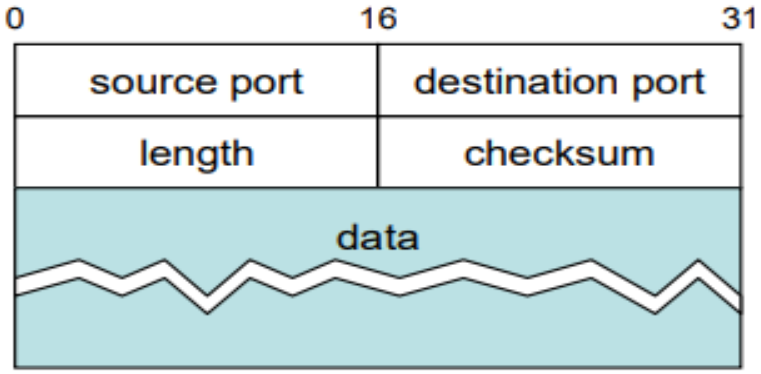


Figure 1.15: En-tête UDP

- port source : numéro de port 16 bits de la source
- port de destination : numéro de port 16 bits de la destination
- longueur : nombre de 16 bits représentant la longueur en octets du datagramme UDP (y compris l'en-tête)
- checksum : 16 bit checksum utilisé pour la détection d'erreur (plus tard)
- data : le message

Le protocole TCP

Le Transmission Control Protocol (TCP) d'Internet est un protocole de transport sophistiqué qui offre une communication fiable. C'est un protocole full duplex, supportant une paire de flux dans chaque direction, et inclut un mécanisme de contrôle de flux pour chaque flux. TCP prend en charge le mécanisme de démultiplication de l'UDP, permettant à plusieurs programmes d'application sur un hôte donné de communiquer simultanément sur Internet. La clé de démultiplication utilisée par TCP est le 4-tuple < port source, hôte source, port de destination, hôte de destination > pour identifier la connexion TCP particulière. Ce protocole est largement utilisé pour la livraison fiable et ordonnée des messages [15]. .

Le protocole TCP est un protocole orienté vers les octets. Une connexion TCP est créée par l'expéditeur, qui y transmet des octets, et est lue par le destinataire. En soi, TCP n'envoie pas d'octets individuels. Ce serait trop lourd. Comme alternative, l'expéditeur génère des octets dans la mémoire tampon de TCP (fenêtre coulissante), à partir de laquelle TCP rassemble suffisamment d'octets pour remplir un segment ou un paquet d'une taille acceptable pour le réseau actuel afin d'éviter une segmentation supplémentaire au niveau de la couche réseau [15].

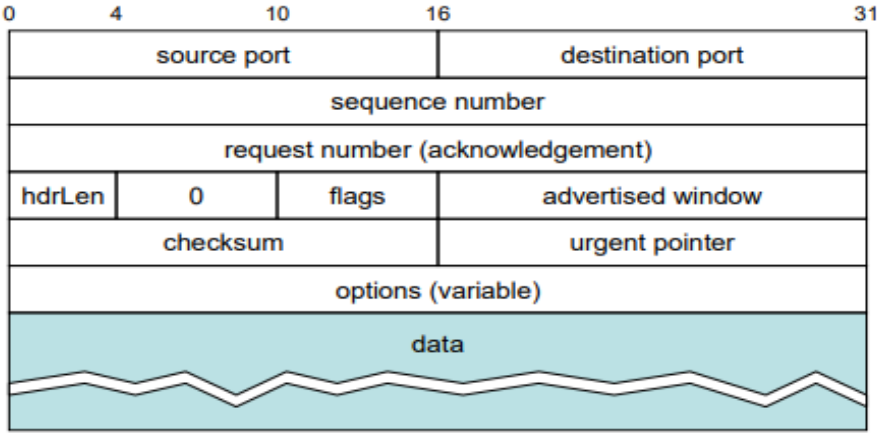


Figure 1.16: En-tête TCP

- Port source : Numéro de port 16 bits de la source
- Port de destination : numéro de port 16 bits de la destination
- Numéro de séquence : 32 bits SN
- Numéro de requête : 32 bits RN
- HdrLen : longueur de l'en-tête en mots de 32 bits, nécessaire en raison des options, également connue sous le nom de champ d'offset
- Drapeaux : 6 bits pour SYN, FIN, RESET, PUSH, URG et ACK
  - SYN et FIN sont utilisés pour établir et terminer une connexion TCP.
  - RESET est activé par le récepteur pour interrompre la connexion, par exemple lorsque le récepteur est troublé par la réception d'un segment inattendu.
  - ACK est activé par le récepteur lorsqu'un accusé de réception doit être lu.
  - PUSH est défini par l'expéditeur pour demander à TCP de vider le tampon d'envoi ; il est également utilisé par le récepteur pour diviser le flux d'octets TCP en enregistrements (non pris en charge par l'API des sockets).
  - URG est défini par l'expéditeur pour signifier que le segment contient des données urgentes.
- Fenêtre annoncée : nombre de 16 bits utilisé pour le contrôle de flux (plus tard)
- Somme de contrôle : somme de contrôle de 16 bits calculée sur l'en-tête TCP, les données TCP et le pseudo-en-tête (même algorithme que pour UDP)
- Urgent pointer : lorsque le drapeau URG est activé, le pointeur urgent indique où se terminent les données urgentes (il commence au premier octet de données)
- Option : variable
- Données : le message

1.7.3 Menaces et attaques liés à la transmission des données dans les drones

Nous considérons les types d'attaques possibles suivant [16] :

- **Attaques d'usurpation GPS (GPS Spoofing Attack) :** Il s'agit d'une forme d'agression où un émetteur radio proche est employé afin d'interférer avec les signaux GPS authentiques. Il est possible que le pirate ne transmette aucune information ou des coordonnées erronées.
- **Attaque d'interception de données (Data Interception Attack) :** Il est réalisé en utilisant un logiciel de reniflage de paquets, qui analyse les paquets de données pendant leur voyage sur le réseau. Les informations collectées sont envoyées au pirate.
- **Attaque par déni de service (Denial of Service Attack) :** Il s'agit d'envoyer un grand nombre de demandes que le drone ne peut pas gérer. Le drone devient occupé, ce qui interdit l'accès aux utilisateurs autorisés. En cas d'agression, un drone pourrait perdre le contact avec son propriétaire et ne pas pouvoir accomplir la tâche à accomplir.
- **Attaque d'infection par un logiciel malveillant (Malware Infection Attack) :** Ce genre d'attaque de sécurité consiste à prendre le contrôle du drone de la victime par un logiciel malveillant et à réaliser des opérations illégales.
  Les logiciels malveillants englobent une variété d'attaques, telles que les logiciels espions, les rançongiciels, les logiciels de contrôle et de commande, et bien d'autres encore.
- **Attaque de l'homme au milieu (Man In The Middle Attack) :** Il arrive lorsqu'un pirate se positionne au cœur d'une conversation entre un utilisateur et un système, soit pour espionner, soit pour imiter l'un des participants, ce qui donne l'impression qu'il y a un flux d'informations en cours.
- **Attaque du trou de ver (Wormhole Attack) :**Une des attaques les plus fréquentes consiste à piéger des paquets à partir d'un seul point du réseau et à les rediriger vers un autre nœud malveillant situé à un emplacement éloigné.
- **Attaque de brouillage (Jamming Attack) :** Il s'agit d'une forme d'attaque par déni de service où un nœud empêche les autres nœuds d'interagir en occupant la communication sur le canal [16].

1.7.4 Solutions pour renforcer la sécurité de la transmission des données

Pour résoudre le probléme de Menaces liés à la transmission des données dans les drones, il est essentiel d'adopter une approche globale qui combine des mesures techniques, réglementaires et éducatives pour assurer la sécurité des drones et de leurs opérations. Tel que :

- **Cryptage des communications :** Le cryptage des communications entre le drone et la station de contrôle est crucial pour protéger les données contre les interceptions non autorisées. L'utilisation d'algorithmes de cryptage robustes, tels que l'AES (Advanced Encryption Standard), assure que les données transmises restent confidentielles et intégrales [17].
- **Authentification et identification :** La mise en œuvre de mécanismes d'authentification permet de vérifier l'identité des entités communiquant avec le drone. Les protocoles comme les certificats numériques et les systèmes basés sur la biométrie peuvent être utilisés pour cette fin [18].
- **Détection des intrusions :** Les systèmes de détection des intrusions (IDS) surveillent le trafic réseau pour identifier les activités suspectes ou malveillantes. Ces systèmes peuvent être basés sur des signatures ou des anomalies, et permettent de détecter rapidement les tentatives d'intrusion [19].
- **Techniques d'étalement de spectre DSSS et FHSS :** Les techniques d'étalement de spectre, telles que le Direct Sequence Spread Spectrum (DSSS) et le Frequency Hopping Spread Spectrum (FHSS), sont utilisées pour améliorer
  la sécurité et la robustesse des communications contre le brouillage et les interférences. Le DSSS étale le signal sur une large bande de fréquences, tandis que le FHSS change fréquemment la fréquence porteuse selon une séquence pseudo-aléatoire [20].

1.8 Conclusion

Dans ce chapitre nous avons fournit un aperçu complet des drones, de leur historique, des différents types, des applications, ainsi que de leurs opérations détaillées et des problèmes de sécurité liés à la transmission de données. Les drones jouent un rôle croissant dans divers secteurs, des applications civiles aux missions militaires stratégiques. Pourtant, leur mise en œuvre pose de graves problèmes de sécurité en raison des risques liés à la transmission et à la réception d'informations sensibles.
Le prochain chapitre examinera la technique d'étalement de spectre à séquence directe pour améliorer la sécurité de la transmission des données dans les drones, prévenir les interceptions illégales et protéger les informations stratégiques pendant les missions critiques.

Chapitre 2

L'étalement de spectre à séquence directe DSSS

2.1 Introduction

L'étalement du spectre est une méthode qui consiste à étendre la gamme de fréquences d'un signal au-delà de ce qui est nécessaire à sa transmission. Cette technique est utilisée à diverses fins, notamment :

- Contrer l'impact néfaste des interférences provoquées par d'autres utilisateurs partageant le canal ou la propagation par trajets multiples.
- Dissimulation du signal grâce à l'utilisation d'une puissance de transmission minimale, ce qui rend difficile son interception par des personnes non autorisées.
- Assurer une répartition équitable des ressources radio.

2.2 Chaîne de transmission

Sur une chaîne de transmission numérique, le bloc "étalement de spectre" se situe entre le bloc "codage canal" et le bloc "modulation", comme illustré dans la figure 2.1. L'élément "reconstruction signal" correspond à l'élément "désétalement de spectre". Le signal large bande est converti en signal bande étroite et en sortie, il fournit les bits probablement émis.

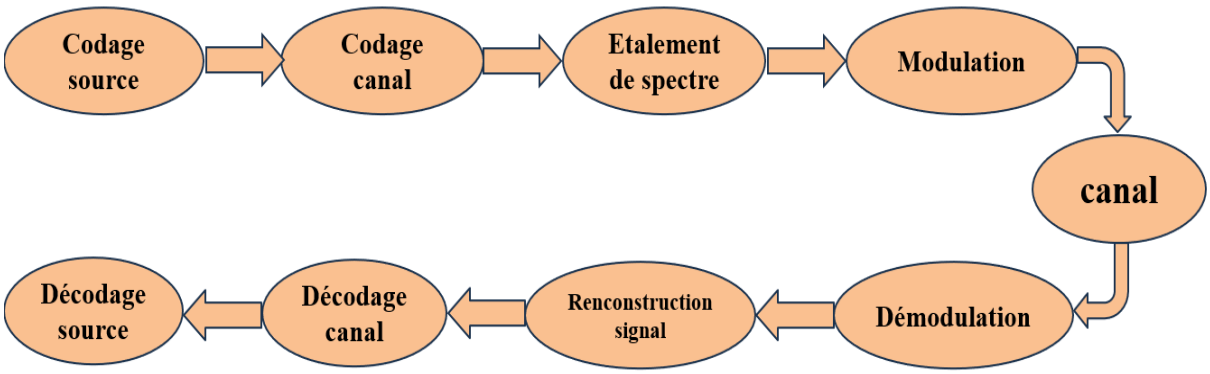


Figure 2.1: Schéma d'une chaîne de transmission

De nos jours, les réseaux numériques utilisent des méthodes de codage de source et de codage canal de plus en plus efficaces, visant à augmenter le débit et à lutter contre les erreurs de transmission [21].

2.2.1 Bloc de codage source

La transformation du signal analogique en signal numérique (en Bits) est effectuée par le codage source. L'objectif de cette opération est d'une part, de minimiser les redondances présentes dans les informations afin de réduire au minimum la quantité de données à transmettre et ainsi augmenter le débit de transmission. De plus, elle vise également à protéger l'information contre toute récupération non autorisée [21].

2.2.2 Bloc de codage canal

En codage canal, le principe fondamental est de substituer le message à transmettre par un message plus long qui inclut de la redondance. Sans répétition, chaque information du message est essentielle pour comprendre l'ensemble du message. Il est donc possible que toute erreur dans une partie du message modifie la signification du message. La redondance vise à éviter que les erreurs ne compromettent la compréhension globale du message. Les symboles sont utilisés pour désigner les données générées par le codeur [21].

2.2.3 Bloc d'étalement de spectre

L'objectif de l'étalement de spectre est d'augmenter la portée du signal tout en maintenant la puissance moyenne, mais en réduisant le niveau spectral. Dans les situations où l'on cherche la discrétion, cela entraîne une intégration totale du spectre du signal utile dans le bruit ambiant [22].

L'information à transmettre est codée par une séquence pseudoaléatoire (Pseudo Noise–code, PN code) connue uniquement par des utilisateurs.

Ces séquences pseudo-aléatoires ont des propriétés particulières :

- Elles sont faiblement auto-corrélées :

$$R_c(\tau) = \int_{-\infty}^{\infty} c(u) \cdot c(u-\tau)du, \quad \forall\tau \neq 0 \tag{2.1}$$

  où $R_c(\tau)$ est la fonction d'auto-corrélation de $c(t)$, le code pseudo-aléatoire. Cela permet de ne pas modifier les propriétés statistiques du signal émis.

- Elles sont faiblement intercorrélées entre elles :

$$R_{cicj}(\tau) = \int_{-\infty}^{\infty} c_i(u) \cdot c_j(u-\tau)du = 0, \quad \forall\tau \tag{2.2}$$

  où $R_{cicj}(\tau)$ est la fonction d'intercorrélation de deux codes pseudo-aléatoires différents $c_i(t)$ et $c_j(t)$. Cela assure la sécurité des données transmises et évite le brouillage des sources entre elles [21].

2.2.4 Bloc de modulation

La modulation consiste à ajouter des informations audio, vidéo, image ou textuelles à un signal porteur électrique ou optique afin de le transmettre sur un support de télécommunication ou électronique. La modulation facilite le transfert d'informations d'un signal électrique à un dispositif de réception qui démodule le signal pour extraire l'information mixte [23]. La modulation numérique implique de modifier l'un des paramètres d'une onde porteuse en fonction du signal à transmettre (signal modulant). En fonction de ce paramètre, on mettra en place le type de modulation. L'onde porteuse peut être ajustée en modifiant les paramètres suivants : l'amplitude, la phase ou la fréquence, ou une combinaison des trois caractéristiques du signal. Dans cette situation, on distingue trois types de modulations : la modulation d'amplitude (Pulse Amplitude Modulation (PAM)), la modulation de phase (Phase Shift Keying (PSK)) et la modulation de fréquence (Frequency Shift Keying (FSK)). D'autres types de modulations peuvent être créés à partir de ces modulations de base. La Modulation d'amplitude en Quadrature (MAQ) est un exemple. En raison de sa mise en œuvre relativement simple et de son caractère quasi optimal, cette modulation est particulièrement intéressante. Elle est largement utilisée dans le domaine des communications numériques, comme la téléphonie mobile ou la Télévision Numérique Terrestre (TNT) [24].

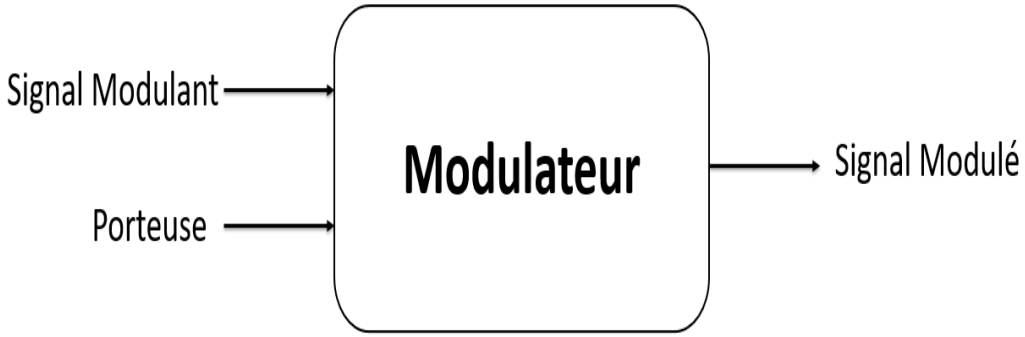


Figure 2.2: Schéma d'une Modulation

2.2.4.1 La modulation QPSK

L'objectif de la modulation est d'ajuster au support de transmission un signal numérique constitué d'éléments binaires. En règle générale, un signal modulé se présente sous la forme suivante :

$$S(t) = A(t) \cdot \cos(2\pi f_c(t) + \phi(t)) \tag{2.3}$$

Si les informations utiles sont transmises par l'amplitude A(t) ou la phase f(t) du signal modulé, on parle alors de modulation d'amplitude ou de modulation de phase.

La modulation QPSK (Keying Phase Shift Quadrature) est une famille de modulations de phase. Un modulateur QPSK simplifié est constitué de deux branches appelées "en quadrature", car elles sont modulées par des fréquences porteuses déphasées de $\pi/2$.

On répartit les bits modulés NRZ sur les branches I et Q d'un modulateur, puis on les module finalement par une porteuse de fréquence f_c. La fréquence porteuse multipliée par les symboles NRZ entraîne une déphase de 180° à chaque fois que les symboles alternent. La sortie du modulateur produit le signal obtenu en combinant les porteuses modulées des branches I et Q, qui sont en réalité des porteuses de fréquence fc avec des sauts de phase de $n\pi/4$.

Le schéma 2.3 illustre le schéma de constellation de la modulation QPSK. Chaque QPSK portant 2 bits présente quatre états dans le diagramme, ce qui correspond à quatre déphasages par rapport à une porteuse de référence non modulée. Pour effectuer une démodulation cohérente du signal reçu, il est nécessaire de créer des porteuses synchrones $(\cos 2pif_ct)$ et $(\sin 2pif_ct)$ dans le récepteur [25].

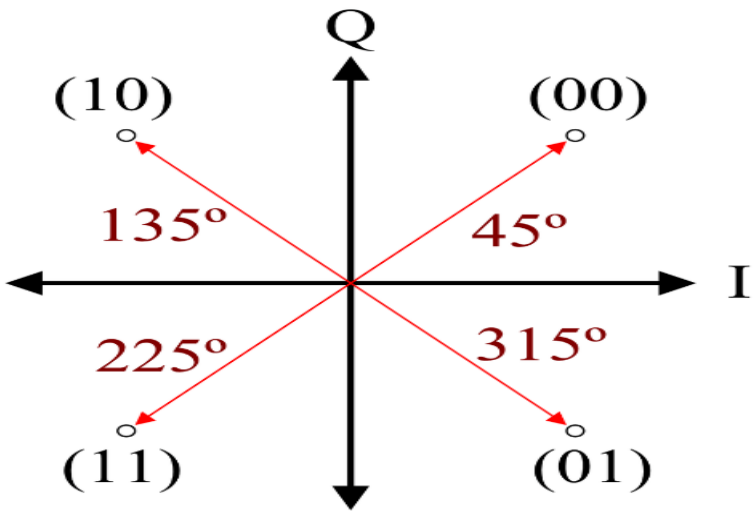


Figure 2.3: Schéma de constellation de la modulation QPSK

2.2.4.2 La modulation QAM

Les modulations d'amplitude sur deux porteuses en quadrature (MAQ) sont également connues sous le nom de QAM, qui signifie "Quadrature Amplitude modulation". Il s'agit d'une modulation qui est appelée bidimensionnelle.

L'association d'une modulation d'amplitude et d'une modulation de phase est appelée modulation QAM. Deux porteuses de fréquence identique sont en décalage de 90°. Il y a deux niveaux de modulation d'amplitude (par exemple 1 et 0,5). Le déphasage de chaque porteuse peut varier entre 0° et 180°. Par cellule, chaque porteuse a la capacité de transporter 4 informations distinctes (soit 2 bits). Les deux porteuses ont la capacité de transporter 4 bits (16 informations distinctes) par cellule, ce qui explique le nom de QAM 16(Il existe également QAM 64, QAM 128...) [26].

Pour ce faire, on écrit le signal modulé s(t) sous la forme suivante :

$$S(t) = a(t) \cdot \cos(2\pi f_0 t + \phi_0) - b(t) \cdot \sin(2\pi f_0 t + \phi_0) \tag{2.4}$$

Où les deux signaux a(t) et b(t) ont pour expression :

$$a(t) = \sum_k a_k g(t - kT) \tag{2.5}$$

$$b(t) = \sum_k b_k g(t - kT) \tag{2.6}$$

Le signal modulé s(t) correspond donc à la somme de deux porteuses en quadrature, que les deux signaux a(t) et b(t) modulées en amplitude.

Les symboles $a_k$et b_k sont généralement considérés comme prenant leurs valeurs respectivement dans les mêmes alphabets à M éléments, ce qui donne lieu à une modulation avec $E = M^2$ états. On peut donc représenter chaque état avec un couple (a_k), ou ce qui est similaire avec un symbole complexe $c_k = a_k + jb_k$. Dans une situation spécifique mais très courante où M peut être écrit $M = 2^n$, les a_k représentent un mot de n bits et les b_k représentent également un mot de n bits. Le symbole complexe $c_k = a_k + jb_k$ peut donc symboliser un mot de 2^n bits.

Cette modulation est généralement appelée modulation d'amplitude en quadrature (MAQ) et si sa constellation comprend E états, elle est connue sous le nom de MAQ-E [26].
La Figure 2.4 présente les constellations 4, 16, 64 et 256 QAM.

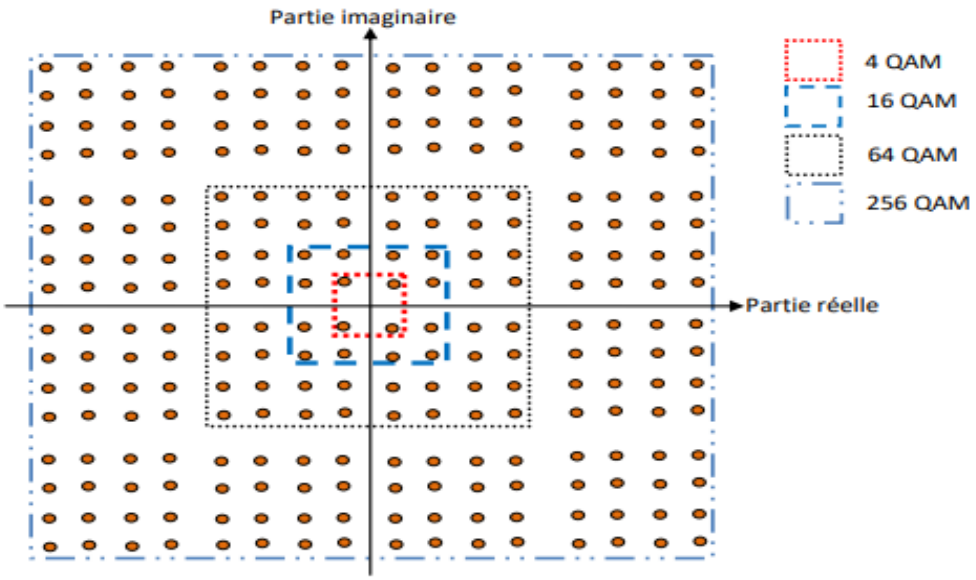


Figure 2.4: Les constellations 4, 16, 64 et 256 QAM [21].

2.3 Principe de l'étalement de spectre

Les techniques d'étalement du spectre, que nous allons étudier maintenant, sont des techniques par lesquelles un signal numérique généré avec une largeur de bande particulière est délibérément étalé dans le domaine des fréquences, ce qui donne ce nom à l'ensemble des techniques.

L'objectif principal de l'utilisation de ces méthodes est de créer une méthode de communication fiable. Initialement utilisées par les militaires pour répondre à leurs besoins de communication, ces techniques génèrent un signal doté d'une résilience accumulée contre les perturbations naturelles, ainsi que contre le bruit et les interférences. Actuellement, ces techniques sont également appliquées dans diverses applications civiles, notamment dans le domaine des communications mobiles [27].

Au moment de la transmission, le concept fondamental de l'étalement du spectre implique la multiplication du signal d'information par des séquences pseudo-aléatoires, également appelées codes PN, qui lui servent de codage essentiel. Lors de la réception du signal, le récepteur doit générer une séquence de codes identiques à celle utilisée lors de la transmission afin d'inverser le processus d'étalement et de récupérer les informations transmises [28].

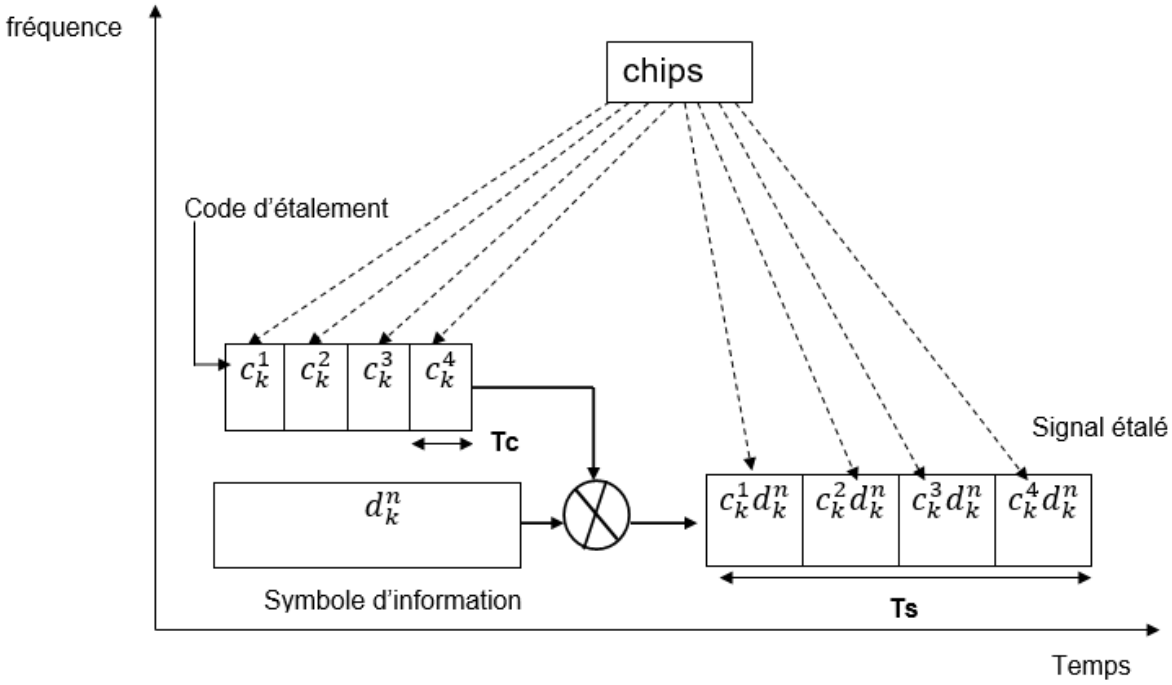


Figure 2.5: Processus d'étalement de spectre

Sur la figure 2.1, représente le processus d'étalement, illustrant la séquence d'éléments $C_k^{(p)}$, où p = 1, 2,...M ,qui représente le code d'étalement du k^{ème} utilisateur .La longueur du code, notée M, est égale à 4 dans cet exemple particulier. Chaque fragment de la séquence a une durée de Tc et une amplitude. On appelle débit chip (Chip rate) le débit avec lequel l'information est échangée, et on le note Bspr. Il s'agit d'un débit de 1/Tc, exprimé en chip par seconde (cps). Par ailleurs, le symbole $d_k^{(n)}$ est utilisé pour le message d'information du k^{ème} utilisateur , où $n = 1, 2, \ldots$. De la même manière, nous pouvons également mesurer la durée de chaque symbole en utilisant T_s, à partir de laquelle nous pouvons également calculer le débit symbole $B_s = \frac{1}{T_s}$, exprimé en symboles par seconde (sps).

Le facteur d'étalement SF (Spreading Factor) est le rapport entre le débit du signal étalé et le signal non étalé [29].

$$SF = \frac{B_{spr}}{B_s} = \frac{T_s}{T_c}$$

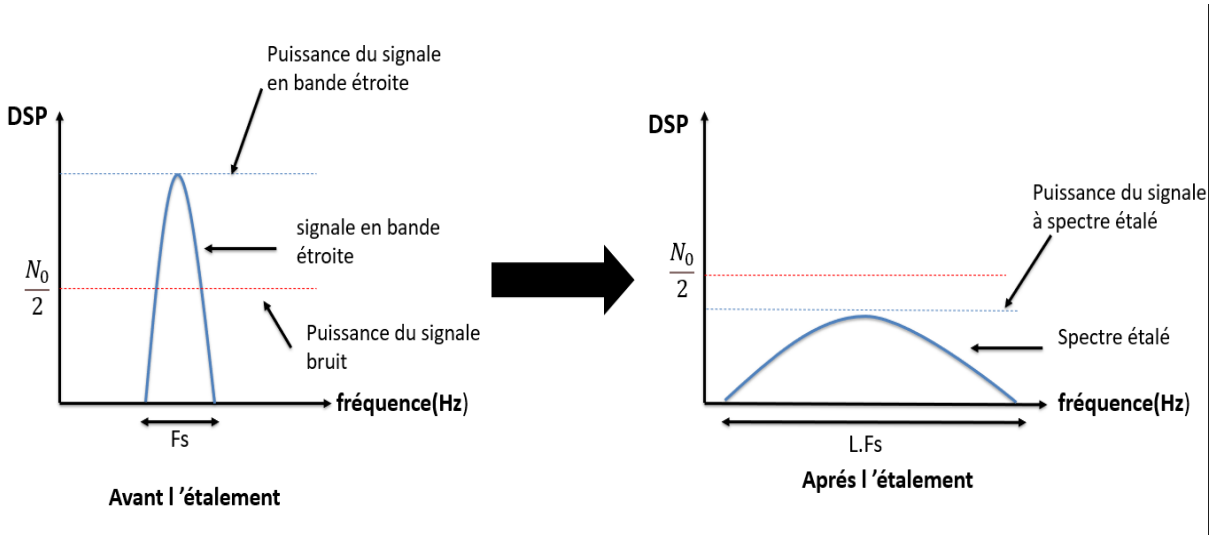


Figure 2.6: Densité spectrale d'un signal avant, et après l'étalement de spectre

Le concept d'étalement du spectre, quelle que soit la technique spécifique utilisée, repose sur le codage des informations à transmettre à l'aide d'une séquence pseudo-aléatoire (PN) connue uniquement de l'émetteur et du récepteur. Ce processus de codage a un effet direct sur la densité spectrale de puissance (DSP), la faisant se propager sur une bande passante plus large. Ceci est visible sur la figure 2.6, où Fs représente la fréquence du symbole, $N_0/2$ représente la densité spectrale de puissance du bruit, L représente le facteur d'étalement (longueur de la séquence utilisée). En conséquence, il est donc possible d'élargir le spectre du signal original en bande de base de largeur Fs au spectre du signal étalé de largeur Fc = L*Fs. La transmission du signal se présente alors comme un bruit à l'égard des autres utilisateurs qui travaillent en bande étroite ou de ceux qui ne disposent pas du code [22]. Devenant ainsi indétectable pour tout individu hostile. Ainsi, il devient indéchiffrable pour toute personne hostile. L'un des objectifs visés, c'est la confidentialité de la transmission. Le signal étalé offre une grande résistance aux interférences qui se situent dans une largeur spectrale beaucoup plus restreinte. Il est important de souligner qu'il s'agit ici d'une source d'interférence ponctuelle qui ne serait présente que sur une bande étroite. Cette solidité découle tout simplement du fait que l'information est dispersée sur une plage de fréquences assez étendue et bénéficie d'une certaine variabilité en fréquence. Seule une partie du spectre du signal utile étalé est perturbée [30].

2.4 Les techniques d'étalement de spectre

Il existe essentiellement deux principaux types de système à étalement de spectre(les plus couramment utilisées) :

- Étalement par saut de fréquence (FHSS) : est une variation de la fréquence de transmission par des sauts discrets pseudo-aléatoires, comme son nom l'indique.
- Étalement par séquence directe (DSSS) : est réalisée en utilisant un signal ou une séquence pseudo-aléatoire dont le débit numérique est supérieur à celui du signal contenant l'information.DSSS est la plus utilisée dans les transmissions de type CDMA[6].
- D'autres méthodes sont plus subtiles, comme le saut en temps (time hopping spread spectrum), où le signal est transmis de manière discontinue, en rafale, à des instants spécifiés par le code, ou encore le chirp spread spectrum, qui est utilisé exclusivement pour l'instant dans les radars [31].

Dans notre travail , nous intéressons sur la technique d'étalement de spectre la plus répandue, l'étalement de spectre par séquence directe décrite en détail par la suite.

2.5 Le systèmes DS-CDMA

Il y a différentes façons de partager une ressource radio entre différents utilisateurs. Nous exposons brièvement les caractéristiques de deux d'entre elles avant de nous pencher sur le CDMA, en particulier le DS-CDMA.

2.5.1 Les technique d'accès multiples

Pour qu'un groupe d'usagers mobiles puisse accéder au réseau en même temps, il faut partager d'une façon ou d'une autre les ressources radio produites par l'opérateur. Il existe trois grandes méthodes de partage des ressources (on parle également d'accès multiples) :

- Le multiplexage temporel (TDMA : Time Division Multiple Access) : où chaque utilisateur émet dans la même bande de fréquence mais à des moments différents.
- Le multiplexage fréquentiel (FDMA : Frequency Division Multiple Access) : Dans cette situation, les utilisateurs envoient en même temps, mais dans des bandes de fréquence différentes.
- Le multiplexage par code (CDMA : Code Division Multiple Access) : Cette méthode implique que "tout le monde communique en même temps et au même endroit, mais chacun dans sa propre langue" [32].

2.5.2 Critère de choix sur les techniques d'accès

Le mode TDMA semble être plus efficace que le mode FDMA en ce qui concerne le débit et la souplesse, mais il semble que le CDMA soit la méthode d'accès la plus appropriée pour les milieux clos car elle répond aux exigences suivantes :

- Protection de l'information grâce à la signature par code.
- Flexibilité car elle peut être facilement superposée à un système existant (peu perturbatrice et immunité aux perturbations grâce à l'étalement de spectre).
- Souplesse en ce qui concerne le nombre d'utilisateurs et les débits grâce au code d'étalement, accès parfaitement aléatoire [29].

Nous nous sommes intéressés à cette dernière catégorie de système car elle est la plus captivante parmi les trois mentionnées en raison de son absence de contraintes de temps et de fréquence. Effectivement, la première catégorie entraîne une limitation de temps : une seule bande de fréquence est employée et chaque utilisateur dispose d'un temps restreint pour communiquer. Le nombre de bandes de fréquences utilisables est limité dans la seconde catégorie : les utilisateurs ont un temps illimité pour communiquer, mais chaque utilisateur utilise une bande de fréquence différente. Cependant, la bande de fréquence n'est pas illimitée et est coûteuse, ce système a un nombre limité d'utilisateurs. Dans la catégorie qui nous intéresse, tous les utilisateurs envoient dans la même fréquence et sans limitation de temps [32].

2.5.3 Accès Multiple à Répartition de Code (CDMA)

Le CDMA est une nouvelle méthode de multiplexage par rapport au TDMA et au FDMA. Dans cette méthode d'accès multiple, les utilisateurs utilisent la même fréquence et communiquent à des intervalles temporels identiques. Les militaires l'utilisent d'abord en raison de sa résistance aux interférences et de son niveau de sécurité.

Chaque émetteur reçoit un code, également connu sous le nom de signature ou de séquence de code, qui lui permet de transmettre des informations sans interférer avec les messages d'autres utilisateurs. Pour réduire les MAI, il est essentiel que les séquences de codes soient strictement orthogonaux [33].

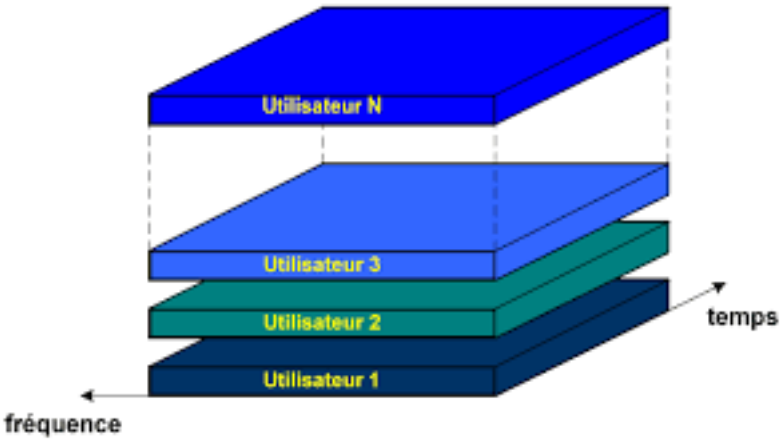


Figure 2.7: Accès Multiple à répartition de code

La méthode CDMA offre aux utilisateurs la possibilité de transmettre leurs données à n'importe quelle fréquence sans nécessiter de synchronisation entre eux. Effectivement, à la différence des techniques TDMA et FDMA, le CDMA n'est pas restreint par des paramètres physiques (temps disponible ou fréquences utilisables), mais par la capacité de générer un nombre maximal de codes. Ainsi, le nombre d'utilisateurs est proportionnel au nombre de séquences d'étalement générées, ces dernières étant sélectionnées de manière à réduire au minimum les interférences d'accès Multiples [33].

Le CDMA implique donc d'étendre le signal sur une bande passante très étendue, de manière à le rendre invisible pour les autres utilisateurs qui utilisent la même bande passante. Lors de la réception, on répète l'opération d'étalement effectuée lors de l'émission. Dans le but de réduire le signal en bande de base, les autres signaux transmis (interférences) sont perçus par le récepteur comme du bruit.

Cette méthode offre un accès à plusieurs ressources et un partage flexible, reconfigurable et sécurisé. L'un des désavantages de cette méthode réside dans la réduction du débit réel, car chaque bit de données sera codé par un mot de longueur plus courte et variable [33].

2.5.4 Caractéristique du CDMA

Ce type de système présente les caractéristiques suivantes [34] :

- La fréquence utilisée est élevée : 7 à 10 fois, tout comme l'analogique actuel et le TDMA/FDMA.
- Plus grande zone de couverture : rayon allant jusqu'à 30 km.
- Réutilisation de la fréquence universelle :Utilisation commune d'une seule bande de fréquence par tous les sites de cellule.
- Minimisation des perturbations : résistance aux bruits élevée, transmission par paquets .

2.5.5 Description de la technique CDMA

La figure 2.8 illustre le schéma général d'une liaison CDMA.Elle est constituée de trois grandes sections :

- **L'émission :** pour chaque utilisateur, la donnée à envoyer est codée par le code de l'utilisateur. Ensuite,les donnée étalées de tous les utilisateurs sont sommées.
- **La transmission :** implique l'émission des données étalées sur le support de transmission, qui peut être un câble (optique ou électrique) ou un canal hertzien.
- **La réception :** le signal reçu est reparti entre tous les récepteurs destinataires. Chaque récepteur extrait du signal reçu le message qui lui a été envoyé, en comparant le signal reçu au code utilisateur à détecter. Les données transmises sont estimées à partir du degré de similitude entre le signal reçu et le code utilisateur souhaité.

Le principe fondamental du CDMA consiste à moduler directement le message à transmettre en utilisant une séquence de code spécifique à un utilisateur spécifique. Ce système a été créé grâce à cette méthode, qui est couramment connue sous le nom de CDMA à étalement de spectre à Séquence Directe ou Direct-Séquence CDMA (DS-CDMA) [35].

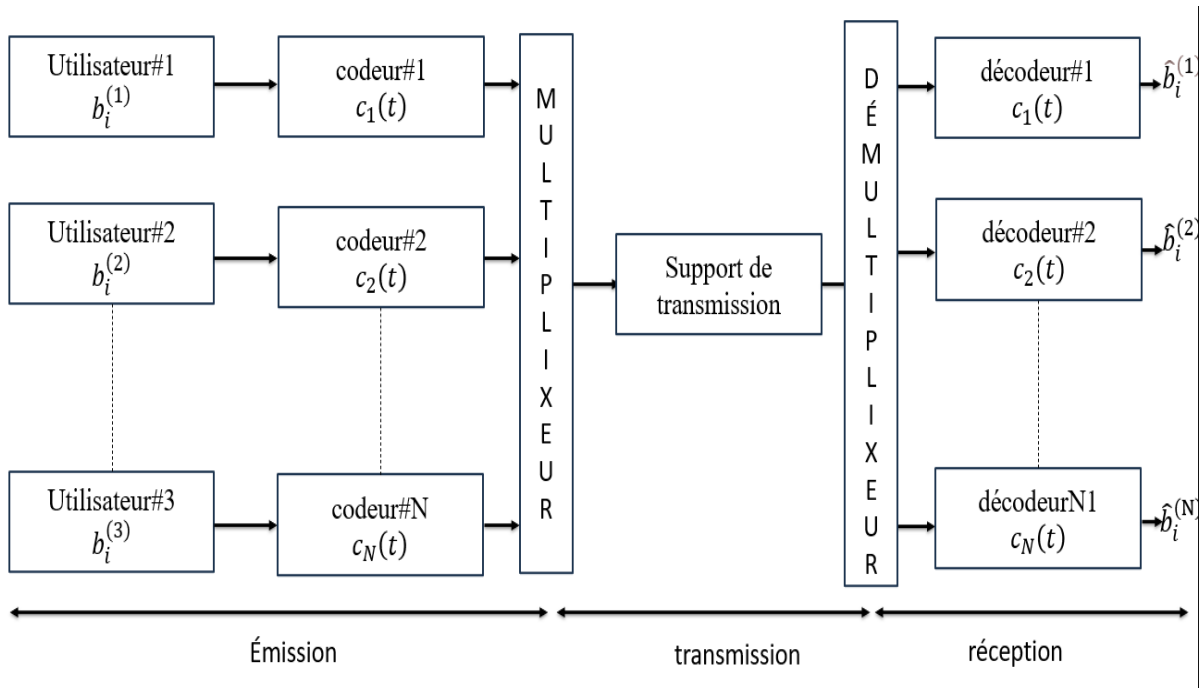


Figure 2.8: Liaison CDMA

2.5.6 L'étalement de spectre par séquence directe(DS-CDMA)

De plus nouvelle génération, ce procédé est destiné aux applications civiles de radio mobile cellulaire pour communications personnelles, associé à une interface radioélectrique de type CDMA (systèmes DSSS-CDMA). En principe, les techniques DSSS ont pour objectif de réduire la densité spectrale de puissance du signal à émettre en l'étalant sur une large bande de fréquence. Le procédé DSSS de modulation à étalement de spectre est une technique d'accès particulièrement flexible, permettant, entre autres :

- Dans la même bande de fréquence, il est possible de transmettre simultanément des signaux à bande étroite émis par différents utilisateurs, sans nécessiter de coordination.
- Concevoir un dispositif de communication à accès multiples à répartition par code (CDMA). Toutes les personnes communiquent à travers une signature (code personnel) qui permet de différencier leur signal de ceux des autres.
- Éviter l'interférence intensionnelle (brouillage) en parlant.
- De diminuer la capacité de repérer le signal en le dissimulant dans le bruit ambiant.
- Garantir, grâce à un traitement unique, une protection contre les perturbations aléatoires causées par les multiples trajets causés par la propagation. Ce dernier aspect suscite un intérêt particulier dans le secteur de la radio mobile [36].

Il convient de noter que cette dernière est la plus couramment employée dans les transmissions de type CDMA. Il s'agit ici de la transmission DS-CDMA.

A partir des spécifications techniques de certains standards, nous pouvons résumer dans le tableau 2.1 leurs spécificités et leurs similitudes :

Standard	Bande de fréquence(MHZ)	Débit(bps)	Technique d'accès	Facteur d'étalement
IS-95	824-849 869-894	1.2288M	DS-CDMA	256
BLEUTOOTH	2400-2483.5	1M	FH-CDMA	79
UMTS	1900-2025 2110-2200	3.84M	DS-CDMA	4, 8, . . . , 256
CDMA2000	824-849 869-894	1.22883M 3.6864M	DS-CDMA	4, 8, . . . , 128 4, 8, . . . , 256
WLAN	2400-2484	11M	DS-CDMA	13
ZIGBEE	868-868.6 902-928 2400-2483.5	20k 40k 250k	DS-CDMA	1 10 16

Tableau 2.1: Caractéristiques de quelques standards de télécommunication

Le tableau 2.1 montre aussi gue la DS-CDMA est la technique dominante dans presque tous les systèmes de 3G [37].

L'étalement de spectre par séquence directe implique la modulation de la trame de symbole à transmettre d(t) grâce à une séquence d'étalement pseudo-aléatoire c(t) (code d'étalement ou pseudo-noise). Le PN-CODE va donc séparer le code à transmettre en unités appelées "chips" avec une période beaucoup plus petite que celle du bit à transmettre (la période du bit à transmettre étant le temps symbole)[14]. Schéma général d'un système à étalement de spectre par séquence directe est illustrée par la figure 2.9.

La technique DSSS à trois fonctions principales à accomplir : la création des codes d'étalement (PN-Code), la corrélation à l'émission qui permet d'étendre la donnée à transmettre et la dé-corrélation à la réception qui permet de récupérer la donnée transmise en remontant le signal au-dessus du bruit [38].

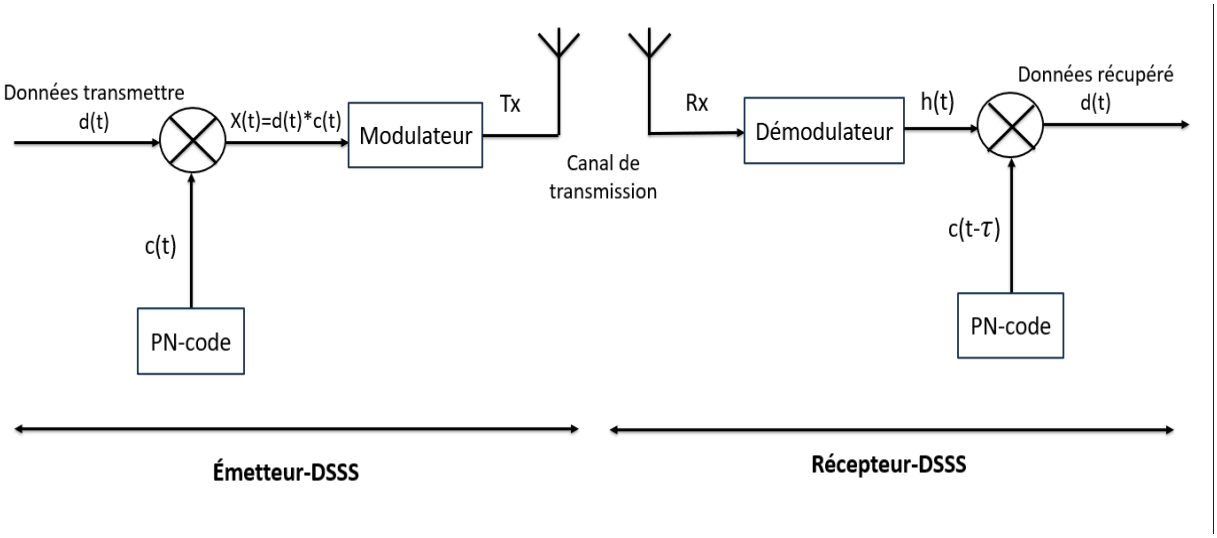


Figure 2.9: Schéma général d'un système à étalement de spectre par séquence directe

Pour bien comprendre le principe d'étalement du spectre par séquence directe, Nous montrons dans la figure 2.10 un exemple qui illustre cette technique.

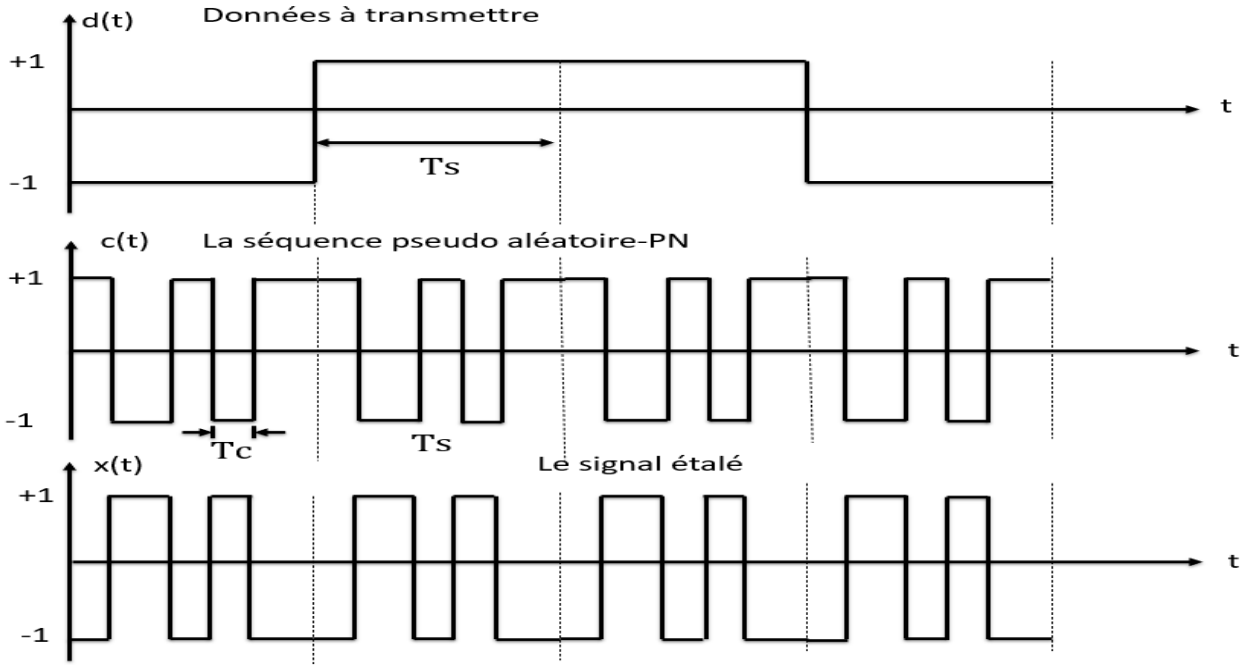


Figure 2.10: Principe d'étalement du spectre par séquence directe

Tous les utilisateurs sont identifiés par un code qui lui est propre. Les bits sont utilisés pour représenter les données d(t) en utilisant une suite de (-1) et de 1. Le code c(t) qui permet de distinguer les utilisateurs est aussi composé de (-1) et de 1, qui sont connus sous le nom de chips. La fréquence des chips est supérieure à celle des bits.à la transmission,l'étalement consiste à multiplier chaque bit de données par un code d'étalement(pseudo-aléatoire), donc on obtient un signal étalé x(t). Après, ce signal est modulé sur son porteur avant qu'il soit transmis.

Lors de la réception, un code localement généré $c(t-\tau)$ où τ est le retard de propagation au récepteur est employé afin de désétaler le signal reçu (Rx) et de récupérer l'information initiale. Afin de garantir le succès de cette opération, il est essentiel que le code local soit identique à celui utilisé à l'émetteur, et que les deux codes soient parfaitement synchronisés. Un simple décalage d'un seul chiffre empêche la récupération de l'information initiale [39].

2.5.7 Modulateur et Démodulateur DSSS

En général, un modulateur DSSS (Fig.2.11) est composé de [40] :

- D'un codeur « Non-Retour à Zéro » (NRZ) qui transforme le signal de données numérique en signal analogique.
- D'un générateur de code aléatoire.
- D'un autre codeur NRZ qui transforme le code d'étalement produit en signal analogique.
- D'un mélangeur qui permet de modifier le signal de données en utilisant le code d'éta-

lement pour obtenir la version étalée du signal de données.

- Par un autre mélangeur, la porteuse est influencée par la version étalée du signal de données.

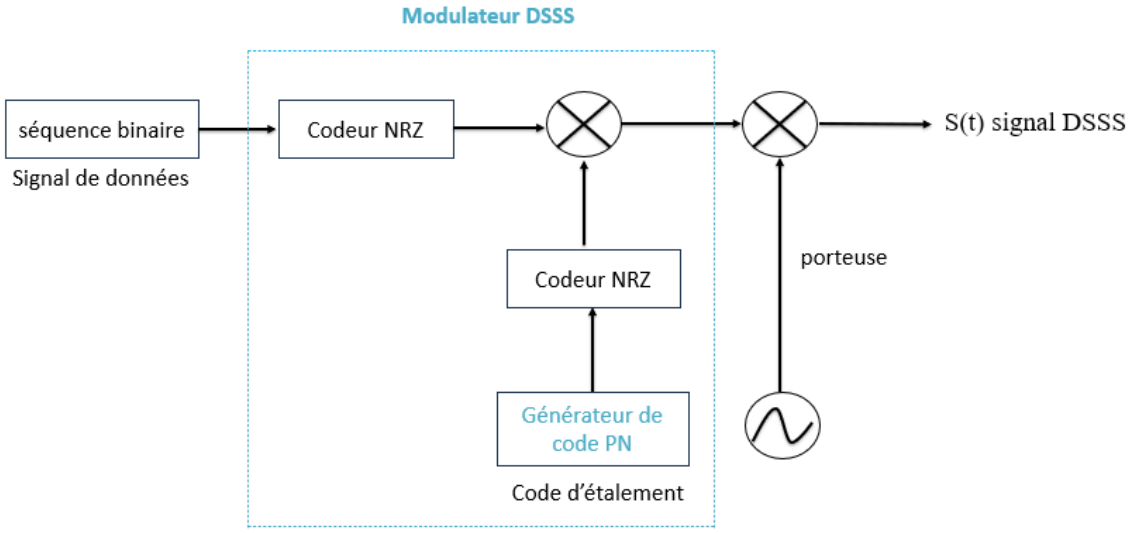


Figure 2.11: Schéma d'un Modulateur DSSS

Le générateur de code pseudo-aléatoire permet de produire la séquence binaire pseudo-aléatoire périodique de longueur N qui est utilisée comme code d'étalement. Il est essentiel de sélectionner ou de concevoir l'algorithme utilisé dans le générateur en respectant les deux règles suivantes [40] :

- Le code d'étalement doit avoir une fonction d'autocorrélation semblable à celle d'un bruit blanc.
- La fonction d'intercorrélation entre deux codes d'étalement différents doit être aussi proche que possible de 0 (conformité des codes pour l'orthogonalité).

Ces propriétés sont vérifiées par plusieurs codes connus, tels que les codes Gold utilisés par le système GPS et les codes Walsh . Comme représenté dans la figure 2.12, la démodulation d'un signal DSSS débute par la suppression de la porteuse à l'aide d'un oscillateur local qui produit une copie de la porteuse, d'un mélangeur qui module le signal reçu avec la copie de la porteuse et d'un filtre passe-bas. Ensuite, le signal ramené en bande de base est désétalé en utilisant un démodulateur composé d'un générateur de code PN et d'un codeur NRZ, qui créent une réplique analogique du code d'étalement utilisé. Ensuite, un mélangeur et un intégrateur sont utilisés pour ajuster la période d'intégration à la durée T_s d'un bit du signal de données initial. Par la suite, le signal obtenu est normalisé avant d'être converti en une séquence binaire à l'aide d'un convertisseur analogique numérique (CAN) [40].

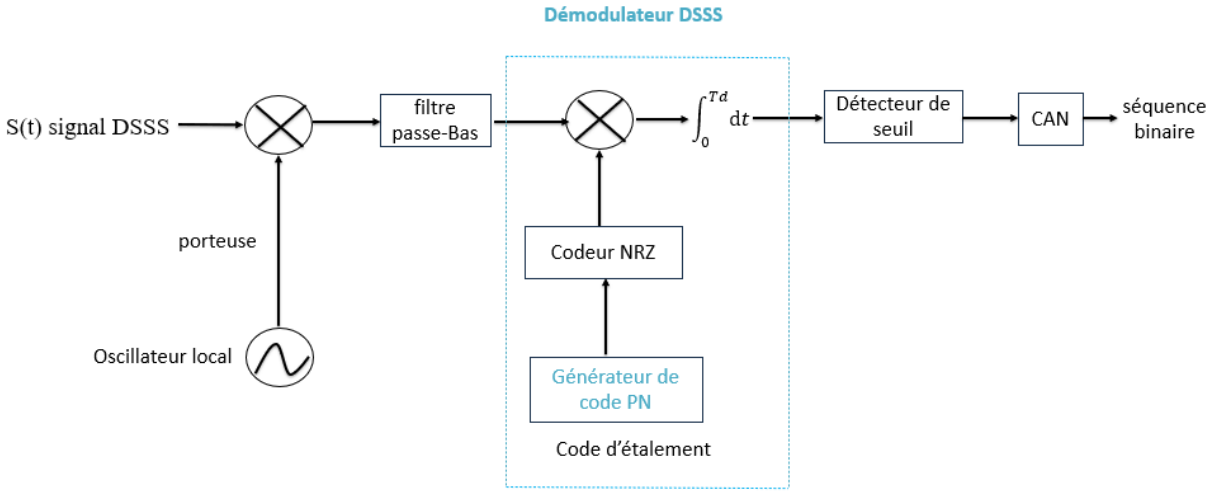


Figure 2.12: Schéma d'un Démodulateur DSSS

2.5.8 Les canaux de transmission

2.5.8.1 Canal de Rayleigh

Le canal de Rayleigh est, par définition, un canal à multiples trajets, avec une multitude de trajets indéterminables. En effet, il n'y a pas de contact direct entre l'émetteur et le destinataire, et plusieurs versions d'un même signal peuvent lui parvenir décalées de quelques instants après avoir réfléchi à des obstacles. La distribution de Rayleigh permet de représenter à petite échelle les fluctuations de l'amplitude du signal reçu. En considérant qu'une sinusoïde $s(t) = \sin(2\pi f_0 t)$ est transmise dans un canal à multiples trajets. À chaque trajets, on introduira un déphasage c et une atténuation $a_i(t)$ sur le signal transmis. La somme des différents trajets donnera le signal reçu (sans prendre en compte le bruit additif gaussien) [24] :

$$r(t) = \sum_i \alpha_i(t) \cos(2\pi f_0 t - \theta_i(t)) = a_0(t) \cos(2\pi f_0 t) + a_1(t) \sin(2\pi f_0 t) \tag{2.7}$$

Avec :

$$\theta(t) = 2\pi f_0 \tau_i(t)$$

$$a_0(t) = \sum_i a_i(t) \cos(\theta_i(t))$$

$$a_1(t) = \sum_i a_i(t) \sin(\theta_i(t))$$

Il est supposé que les échantillons du processus aléatoire $\alpha_i(t)$ soient indépendants et identiques partagés. Donc, on suppose que les échantillons du processus aléatoire $\theta_i(t)$ sont des

variables aléatoires uniformes sur $[0, 2\pi]$. Dans cette situation, les éléments de phase et de quadrature $a_0(t)$ et $a_1(t)$ sont deux processus aléatoires Gaussiens distincts [24].

La définition de l'enveloppe d'évanouissement se fera selon :

$$a = \sqrt{a_1^2 + a_0^2} \tag{2.8}$$

2.5.8.2 Canal à bruit additif blanc Gaussien

Le canal à bruit blanc additif gaussien est le modèle de canal le plus utilisé dans les transmissions numériques, et il est également l'un des plus simples à générer et à analyser. Ce son reflète les bruits internes (bruit thermique causé par les défauts des équipements...) et les bruits externes (bruit d'antenne...). Ce type de transmission est cependant plutôt lié à une transmission filaire, car il constitue une transmission quasi-parfaite de l'émetteur au récepteur. Le message reçu est alors écrit :

$$r(t) = s(t) + n(t) \tag{2.9}$$

Le bruit est représenté par n(t), un processus aléatoire gaussien de moyenne nulle, de variance σ^2, et de densité spectrale de puissance bilatérale $\Phi = \frac{N_0}{2}$ [36].

2.6 Avantages et inconvients du DS-CDMA

En raison de leur étalement et de leur spectre élargi, les signaux DS-CDMA présentent plusieurs caractéristiques qui les distinguent des signaux à bande étroite :

- **Possibilité d'accès multiple :** si plusieurs utilisateurs envoient en même temps des signaux à spectre étalé, le récepteur peut néanmoins identifier les utilisateurs à condition que les codes utilisés aient des intercorrélations assez faibles. L'utilisation d'un code spécifique pour désétaler le signal global ne fera en réalité apparaître que le signal étalé avec ce code. Si les utilisateurs ne sont pas nombreux en même temps, la puissance du signal d'intérêt dans la bande utile est alors bien supérieure à celle des interférences dans cette même bande [31].
- **Une excellente résistance aux perturbations de bande étroite :** lorsque des perturbations de bande étroite sont émises, elles peuvent être ajoutées au signal étalé. Le récepteur effectue l'inverse de l'étalement. De cette manière, le signal étalé est converti en signal bande étroite tandis que les perturbations sont en bande étroite est étendue. Ainsi, la force des perturbations devient insignifiante par rapport à celle du signal utile reconstitué.
- **Faible brouillage des émissions classiques à bande étroite :**les signaux à bande étroite peuvent coexister sur la même bande de fréquence que ceux générés par un système à étalement de spectre, sans causer de perturbations significatives entre les deux systèmes.

Ces signaux ont une puissance qui s'étend sur une large plage de fréquences, ce qui entraîne une densité spectrale de puissance très faible par rapport à celle des signaux à bande étroite.

- **Contrairement aux transmissions en bande étroite :** l'étalement de spectre permet de lutter de manière efficace contre les effets des trajets multiples de propagation. Les trous de Fading causés par ces multiples trajets peuvent absorber. Tout le spectre d'une bande étroite de modulation. Si la bande de modulation large est supérieure à la bande de cohérence du canal radio, seule une partie du signal disparaît [41].
- **Faible probabilité d'interception :** La communication est difficilement détectée lorsque le signal présente les caractéristiques d'un bruit aléatoire dont le niveau peut être inférieur à celui du bruit thermique. En outre, en cas de détection du signal, seuls les récepteurs qui ont les paramètres de La séquence d'extension pourront accéder aux informations.
- **Le multiplexage et l'adressage sélectif :** permettent la coexistence de plusieurs émissions dans la même bande de fréquence lorsque les codes d'étalement associés à chacun des signaux sont orthogonaux, c'est-à-dire qu'ils présentent une inter-corrélation proche de zéro. La clé de codage de chaque signal est la séquence d'étalement qui lui est attribuée.Seule la clé de codage du récepteur permet d'exploiter ce signal, ce qui est appelé l'Accès Multiple à Répartition par les séquences d'étalement.
- La principale caractéristique du DS-CDMA par rapport aux systèmes traditionnels réside dans sa capacité à réutiliser l'intégralité du spectre à travers toutes les cellules, car il n'existe pas de concept d'allocation de fréquence dans ce système. Cela accroît considérablement la capacité du système DS-CDMA (en raison de la diminution du facteur de réutilisation des fréquences).
- La sectorisation est utilisée dans les systèmes AMRT et AMRF afin de réduire l'interférence entre les canaux. Mais l'efficacité globale de ces systèmes diminue (car les fréquences ne peuvent pas être utilisées pour les secteurs d'une cellule). D'un autre côté, la sectorisation augmente la capacité des systèmes DS-CDMA. Il est possible de réaliser cette sectorisation en introduisant simplement trois équipements radio similaires dans les trois secteurs. Ainsi, la réduction de l'interférence mutuelle se traduit par une augmentation de la capacité (environ de 3 facteurs) [41].

Parmi les inconvénients de systéme DS-CDMA sont [18] :

- L'encombrement spectral considérable rend souvent difficile l'attribution de fréquences, car le signal possède toujours la même puissance mais celle-ci est répartie de manière différente. Il est donc nécessaire d'utiliser un sous-système pour contrôler la puissance.
- L'augmentation de la complexité des systèmes entraîne une augmentation de leur coût par rapport aux systèmes à bande étroite.
- Dans un environnement perturbé par les autres utilisateurs, il est nécessaire de synchro-

niser la séquence d'étalement de l'utilisateur concerné dans le récepteur avec celle de l'émetteur pour démoduler correctement les données utiles. Selon la méthode employée pour résoudre cette synchronisation, la complexité du récepteur varie.

L'utilisation de ce genre d'émetteur-récepteur, qui utilise l'étalement de spectre, est principalement répandue dans les systèmes CDMA, c'est-à-dire dans un environnement multi-émetteur [41].

2.7 Les codes d'étalement

Les séquences de codage de pseudo-bruit (PN) sont utilisées pour disperser en bande l'énergie du signal en agissant comme des porteuses déterministes, semblables à du bruit. Le choix d'un code approprié est crucial car sa longueur et son type imposent des restrictions sur les capacités du système. La séquence de code PN se compose de 1 et de -1 et est soit un pseudo-bruit ou un pseudo-aléatoire, ce n'est pas une véritable séquence aléatoire en raison de sa nature périodique. Il est impossible de prévoir les signaux aléatoires.

L'autocorrélation d'un code PN a des propriétés similaires à celles du bruit blanc.

— **Pseudo-aléatoire :**
  - Pas aléatoire, mais il semble aléatoire pour l'utilisateur qui ne connaît pas le code.
  - Signal périodique, déterministe, connu de l'émetteur et du récepteur. Il sera plus difficile de détecter le signal envoyé et plus proche d'une onde binaire véritablement aléatoire plus la période du code d'étalement PN est longue.
  - Caractéristiques statistiques de l'échantillon de bruit blanc .

— **longueur :**
  - Code court : $N_c.T_c$=T_s, la même séquence PN pour chaque symbole de données.
  - Code long : des motifs de puce distincts sont attribués à chaque symbole ($N_c.T_c$ »T_s) car la période de la séquence PN est nettement plus longue que celle du symbole de données [42].

2.8 Caractéristiques de la séquence PN

2.8.1 Propriété d'équilibre

Le nombre de uns et de zéros binaires dans chaque phase de la séquence ne diffère pas de plus d'un chiffre.

$$pn = +1 + 1 + 1 - 1 + 1 - 1 - 1 \rightarrow \sum = +1$$

L'équilibre d'un-zéro (composante continue) peut limiter le degré de la suppression de la porteuse qui peut être obtenue lors de la modulation d'une porteuse avec une séquence de codage PN, étant donné que la suppression de la porteuse dépend de la symétrie du signal de modulation [42].

2.8.2 Distribution des longueurs d'exécution

Une série consiste en une séquence unique de chiffres binaires. Parmi les séries de uns et les zéros de chaque période aient une longueur de 1 pour environ la moitié de leurs séries, une longueur de 2 pour environ 1/4, une longueur de 3 pour un huitième, et ainsi de suite [42].

2.8.3 Autocorrélation

La fonction d'autocorrélation du signal numérique est impulsive, un peu comme un signal de bruit blanc, d'où l'origine du terme « pseudo-bruit ».
La fonction d'autocorrélation pour la séquence périodique pn est définie comme le nombre d'accords moins le nombre de désaccords dans une comparaison terme à terme d'une période complète de la séquence avec un décalage cyclique (position tau) de la séquence elle-même :

$$Ra(\tau) = \int_{-\frac{NcTc}{2}}^{\frac{NcTc}{2}} pn(t) \cdot pn(t+\tau)dt \tag{2.10}$$

Il est préférable que $Ra(\tau)$ ne soit pas plus grand qu'un compte si non synchronisé ($\tau = 0$). Pour les séquences PN, l'autocorrélation présente un maximum important (uniquement) pour une synchronisation parfaite de deux séquences identiques (comme le bruit blanc). la synchronisation du récepteur est basée sur cette propriété [42].

2.8.4 Inter-correlation

Le concept de l'inter-correlation décrit l'interférence entre les codes pn_i et pn_j :

$$Rc(\tau) = \int_{-\frac{NcTc}{2}}^{\frac{NcTc}{2}} pn_i(t) \cdot pn_j(t+\tau)dt \tag{2.11}$$

Lorsque le coefficient de corrélation $Rc(\tau)$ est nul pour tous les τ, les codes sont appelés orthogonals. Dans le cadre du cdma, plusieurs utilisateurs utilisent la même bande RF et envoient simultanément. Lorsque les codes d'utilisateur sont orthogonaux, il n'y a pas d'interférences entre les utilisateurs après décodage, et la confidentialité de la communication de chaque utilisateur est protégée.

En réalité, les codes ne sont pas parfaitement orthogonaux, donc la corrélation entre les codes d'utilisateur entraîne une détérioration des performances (une augmentation de la puissance sonore après despreading), ce qui restreint le nombre maximal de personnes simultanément [42].

2.9 Les types des séquences d'étalement

Les séquences habituellement utilisées sont donné dans la figure :

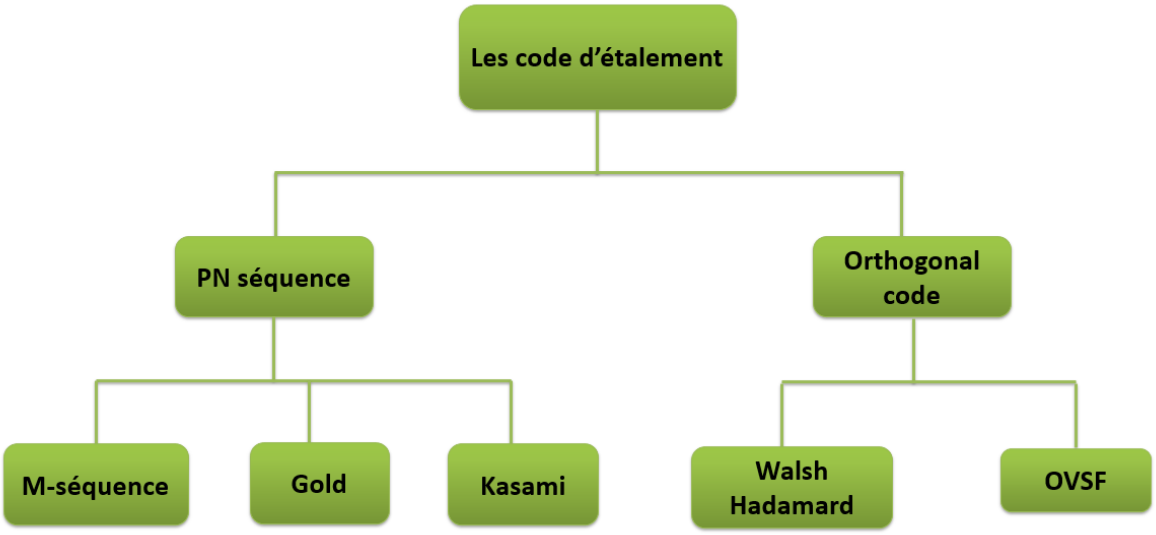


Figure 2.13: Les différents types des séquences d'étalement

2.9.1 Les séquences à longueur maximale

Typiquement, un générateur m-séquence est composé de n bascules en cascade (circuit à décalage), dont certaines sont reconnectées par un ou exclusif. Un simple exemple de trois étages est illustré dans la figure 2.14 [38].

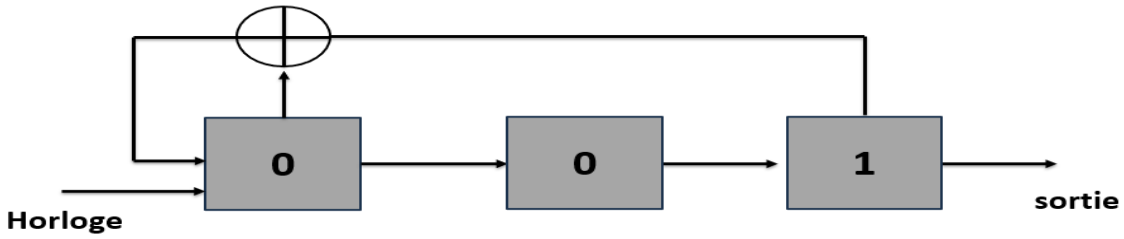


Figure 2.14: Un générateur m-séquence

Le registre contient les différents états suivants : 001,100,110,111,011,101,010, puis à nouveau 001. Les sequences pseudo-aleatoires peuvent avoir une longueur maximale de $N = 2^n - 1$ (les m-sequences) avec n etages. L'auto-entretien est interdit dans l'état tout à zéro. Le rebouclage est le résultat de calculs mathématiques provenant de l'algebre des polynômes : le générateur est basé sur le polynôme caractéristique (approche mathématique), par exemple : $x^{15} + x^{13} + x^9 + x^8 + x^7 + x^5 + 1$ indique des bouclages sur les étapes 5,7,8,9,13 et 15.

La fonction d'auto-corrélation de ces m-séquences est maximale pour un décalage nul à $2^n - 1$, et négligeable(-1) pour toute autre valeur de decalage.

On appelle ces code quasi-orthogonaux des codex linéaires et ils ne présentent pas une protection (cryptage) très élevée : il est possible de les déchiffrer en utilisant une connaissance partielle de la séquence [39].

2.9.2 Séquences de Gold

La famille de séquences PN connues sous le nom de séquences Gold est particulièrement appréciée pour les systèmes CDMA non orthogonaux. Au fur et à mesure que la longueur du code augmente, l'importance des trois pics de corrélation croisée dans les séquences Gold commence à diminuer.

Après avoir ajouté deux séquences de longueur maximale modulo-2, on obtient des codes Gold. Les séquences de code sont ajoutées puce par puce, via une horloge synchrone. Les deux générateurs de code conservent la même relation de phase puisque les m-séquences ont la même longueur. Les codes créés (voir figure 2.15) sont de longueur non maximale et ont la même longueur que les deux codes de base lorsqu'ils sont combinés ensemble [43].

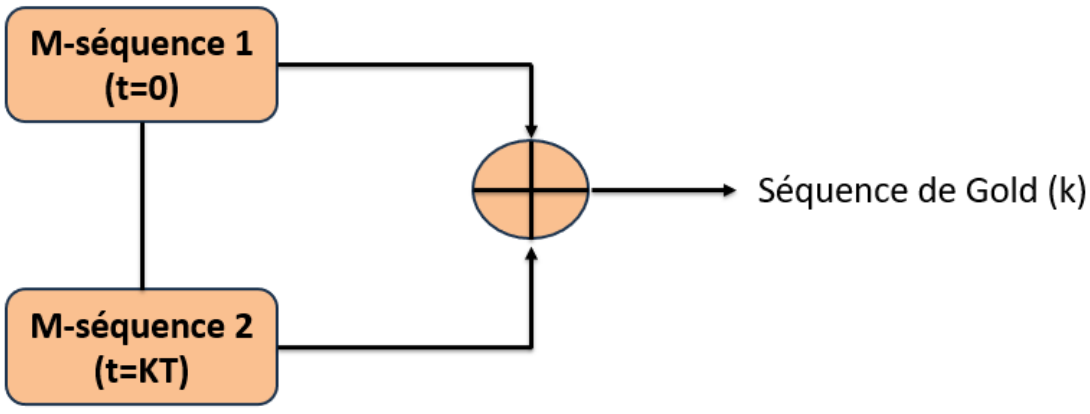


Figure 2.15: Un générateur de la séquence Gold

La fonction d'autocorrélation sera donc moins bonne que celle des m-séquences. Chaque changement de position de phase entre deux m-séquences générées entraîne la génération d'une nouvelle séquence.

Outre l'avantage de pouvoir générer un grand nombre de codes, les codes Gold peuvent être sélectionnés de manière à ce que, sur un ensemble de codes disponibles à partir d'un générateur donné, l'autocorrélation et l'inter-corrélation soient les plus faibles possibles. D'un générateur donné, l'autocorrélation et linter-corrélation entre les codes soient uniformes et limitées. Lorsque des m-séquences spécialement sélectionnées, appelées m-séquences préférées, sont utilisées, les codes Gold générés ont une inter-corrélation à trois valeurs [43].

2.9.3 Séquence de kasami

Les séquences de Kasami sont un autre ensemble majeur de séquences aléatoires utilisées dans certains systèmes de troisième génération. Elles sont établies en utilisant une méthode similaire à celle employée pour les codes de Gold .
Il existe des petits et des grands ensembles de Kasami :

- **Les petits ensembles de Kasami :** Pour chaque pair de n, il est possible de créer un petit ensemble comprenant $M = 2^{n/2}$ séquences distinctes chacune de période $N = 2^n - 1$. Pour définir un ensemble, en commençant par une ML-séquence (a) de période N et en effectuant une décimation avec $=2^{n/2} + 1$, nous obtenons une séquence (a') avec une période de $2^{n/2} - 1$. Nous répliquons ensuite une seule période de (a'q) fois pour produire une séquence de longueur $N = (2^{n/2} + 1)(2^{n/2} - 1)$. Finalement, nous produisons l'ensemble de kasami en combinant par XOR N bits de a et N bits a', ainsi que tous les résultats des $2^{n/2} - 1$ étapes de décalage des bits de (a') [44].
- **Les grands ensembles de Kasami :**
  Un grand ensemble de kasami comprend des séquences de Gold ainsi que le petit ensemble de kasami en tant que sous-ensemble. Un tel ensemble est défini en commençant par la génération d'une ML-séquence (a) de période N, puis sa décimation avec $q = 2^{n/2} + 1$ pour former (a') et une autre décimation avec $q = 2^{n/2} + 1$ pour former (a''). Par la suite, on forme l'ensemble en combinant par XOR (a), (a') et (a'') avec des décalages différents de (a') et (a'') .

Remarque : Les séquences de Kasami ont une valeur d'intercorrélation maximale plus faible que les séquences de Gold. Pour le petit ensemble de Kasami, cette valeur est de$2^{n/2} - 1$ et elle est de $2^{n/2} + 1$pour le grand ensemble [44] .

2.9.4 Séquence de walsh hadamard

Les codes orthogonaux de Walsh sont les plus couramment employés dans les applications de CDMA. Il s'agit des lignes d'une matrice carrée particulière appelée matrice de Hadamard. Pour un code de Walsh de longueur n, il faut donc n lignes pour créer une matrice carrée de(n*n) de code de Walsh. Chacune de ces lignes est orthogonale. Une fois mis en application avec le système de CDMA, chaque utilisateur nomade utilise une des n ligne de la matrice comme code de propagation, fournissant la corrélation croisée [35]. La transformée de Walsh-Hadamard définie par :

$$H_{2^n} = (1) \qquad \text{pour } n = 0$$

$$H_{2^n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

Dont n est une puissance de 2 qui indique la dimension de la matrice. L'exemple suivant illustre la construction de la matrice d'Hadamard d'ordre $N = 2^3 = 8$ [44] :

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Les codes binaires d'étalement sont les lignes de la matrice H. Les codes de WalshHadamard pour le facteur d'étalement SF = 8 sont ainsi les suivants :

$$S1 = [+1 \quad +1 \quad +1 \quad +1 \quad +1 \quad +1 \quad +1 \quad +1]$$

$$S2 = [+1 \quad -1 \quad +1 \quad -1 \quad +1 \quad -1 \quad +1 \quad -1]$$

$$S3 = [+1 \quad +1 \quad -1 \quad -1 \quad +1 \quad +1 \quad -1 \quad -1]$$

$$S4 = [+1 \quad -1 \quad -1 \quad +1 \quad +1 \quad -1 \quad -1 \quad +1]$$

$$S5 = [+1 \quad +1 \quad +1 \quad +1 \quad -1 \quad -1 \quad -1 \quad -1]$$

$$S6 = [+1 \quad -1 \quad +1 \quad -1 \quad -1 \quad +1 \quad -1 \quad +1]$$

$$S7 = [+1 \quad +1 \quad -1 \quad -1 \quad -1 \quad -1 \quad +1 \quad +1]$$

$$S8 = [+1 \quad -1 \quad -1 \quad +1 \quad -1 \quad +1 \quad +1 \quad -1]$$

Nous démontrons que les codes de la matrices H_8 sont orthogonaux.
$(S[1].S[2]) = [+1+1+1+1+1+1+1+1].[+1-1+1-1+1-1+1-1] = +1-1+1-1+1-1+1-1 = 0$
(S[3].S[4]) = [+1 +1 -1 -1 +1 +1 -1 -1].[+1 -1 -1 +1 +1 -1 -1 +1] = +1 -1 +1 -1 +1 -1 +1 -1 =0

Donc les code sont orthogonaux, De la même manière on peut démontrer les autres codes.

2.10 Synchronisation du code

La réception du signal informatif nécessite une synchronisation parfaite du récepteur avec l'émetteur, ce qui implique que le code dans le récepteur est parfaitement aligné sur celui de l'émetteur. On effectue cette opération en deux étapes :

- L'acquisition, également appelée synchronisation grossière, permet de synchroniser le récepteur avec l'émetteur avec une incertitude de $\pm 0.5 T_c$..
- Le suivi du code (code tracking) assure l'exécution et la synchronisation précise entre l'émetteur et le récepteur [45].

2.10.1 Acquisition initiale

L'acquisition de code PN est l'une des tâches les plus difficiles dans la conception d'un récepteur à étalement de spectre à séquence directe. La synchronisation grossière entre le signal reçu et le code généré localement par le récepteur est l'objectif de l'acquisition initiale de code. L'acquisition initiale dans le système DS-SS est similaire à l'ajustement de la phase du signal

d'étalement (du code) de référence à celle du signal reçu. Différentes méthodes d'acquisition permettent d'ajuster les phases, toutes reposant sur le principe de fonctionnement fondamental illustré dans la figure 2.16.

La phase de la séquence d'étalement est supposée par le récepteur, qui essaie de dés-étaler le signal reçu en utilisant la phase hypothétique. En cas de concordance avec la séquence du signal reçu, le signal étalé à large bande sera correctement dés-étalé afin de produire un signal de données à bande étroite.
Puis, un filtre passe-bande (BPF), dont la bande passante est proche de celle du signal de données à bande étroite, sera employé afin de recueillir la puissance du signal dés-étalé. Comme la phase hypothétique est le signal reçu, le BPF collectera l'intégralité de la puissance du signal dés-étalé. Ainsi, le récepteur estime qu'une synchronisation grossière a été effectuée et lance la boucle de poursuite afin d'effectuer une synchronisation fine.

En revanche, si la phase hypothétique ne correspond pas au signal reçu, l'opération de dés-étalement produira un signal à large bande et le BPF ne pourra capter qu'une petite partie de la puissance du signal dés-étalé. Ainsi, le récepteur estime que cette phase hypothétique est erronée et tente donc de tester d'autres phases [45].

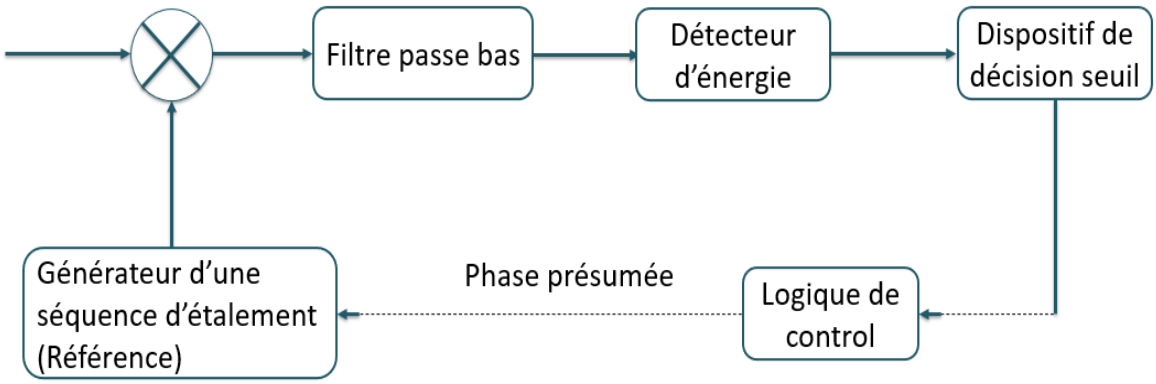


Figure 2.16: Circuit générique d'acquisition

2.10.2 Poursuite du Code

L'objectif de la poursuite de code est d'obtenir et de maintenir une synchronisation précise tout au long de la communication. Une boucle de poursuite de code ne commence son fonctionnement qu'après avoir atteint l'acquisition initiale. Une approche courante de synchronisation fine implique la création d'un circuit de suivi de code capable de suivre la phase de code en cas d'une légère erreur de fréquence [46].

Le rôle de la poursuite est de perfectionner et de maintenir le code d'étalement en accord avec la trame reçue afin de réaliser l'opération de désétalement de manière adéquate.

2.11 Conclusion

Dans ce chapitre, nous avons présenté le principe de l'étalement de spectre, en particulier l'étalement de spectre par séquence directe qui est l'objet du projet, en décrivant ces principaux avantages et inconvénients. Nous avons présenté une technique d'accès multiple connue sous le nom "Accès Multiple à Répartition par les Codes" (AMRC) ou CDMA. Cette méthode est basée sur la technique de l'étalement de spectre à séquence directe(DS-CDMA). Nous avons ainsi cité les principaux codes d'étalement (m-séquences, walsh hadamard, de Gold et de Kasami). Au niveau du récepteur, l'extraction du signal informatif nécessite une synchronisation entre les codes reçus et ceux générés localement. Pour obtenir cette dernière, deux étapes sont exigées : l'acquisition des codes et la poursuite des codes. Ensuite nous avons introduit le principe de l'acquisition initiale et de la poursuite de la séquence PN.

Dans le chapitre suivant, nous allons présenter Les résultats et l'interprétation de simulation sous phython pour la sécurisation des transmission des drones, nous ont permis de vérifier l'effet de l'étalement de spectre par séquence directe comme il a été étudié dans la partie théorique.

Chapitre 3

Simulations et discussion des résultats

3.1 Introduction

Les drones sont de plus en plus utilisés dans divers domaines tels que la surveillance, la livraison, l'agriculture et la cartographie. la sécurité des transmissions devient un enjeu crucial. Les drones en tant que systèmes sans fil, sont particulièrement vulnérables aux attaques de brouillage, pouvant entraîner la perte de contrôle, la capture de données sensibles ou la neutralisation des appareils. Par conséquent, le renforcement de la sécurité des communications entre les drones et leurs stations de contrôle est une priorité pour garantir leur fiabilité et efficacité.

Ce chapitre se concentre sur la simulation et l'implémentation de la technique DSSS avec la modulation QAM et QPSK entre le drone est le GCS pour renforcer la sécurité des transmissions des données, intégrée avec le protocole TCP, et mise en œuvre à l'aide du langage de programmation Python. Le protocole TCP (Transmission Control Protocol), réputé pour sa fiabilité et son contrôle de flux, se combine ici avec DSSS pour offrir une solution robuste contre le brouillage.

3.2 Algorithme

Comme mentionné dans l'introduction de ce chapitre, cette simulation va constituer une représentation de tous ceux qui ont été déjà mentionnés. Pour commencer de manière efficace, nous avons suivi un algorithme que nous allons expliquer étape par étape dans les sections suivantes. Le schéma illustrée dans la figure 3.1 résume les principales étapes de la simulation.

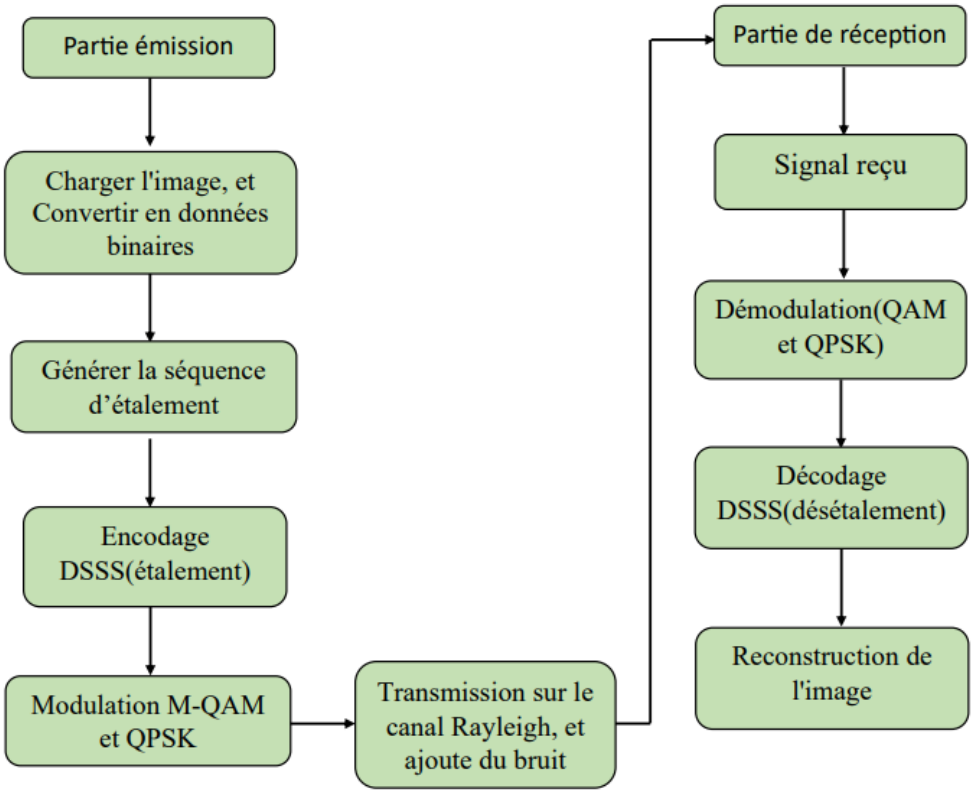


Figure 3.1: Algorithme de la simulation

3.3 Paramètre de simulation

Le tableau 3.1 résume les différents paramètre utilisés pour la simulation :

Paramètre	**Signification**	**Valeur**
(width,height)	La taille de l'image	(// 40, // 40)
Channel	Type de canal	Rayleigh
M	Ordre de modulation	128
snr	Le rapport signal sur bruit	20
$snr - range$	Plage de snr	[0,30,0.1]
f_c	Fréquence porteuse	1000 hz
v	Vitesses de déplacement	40 m/s
Velocities	Plage de vitesse	[0,50,150,200,250,300]
N	Longueur de la séquence d'étalement	16
Sampling-rate	Taux d'échantillonnage	8000

Tableau 3.1: Les paramètre de simulation

3.4 L'implémentation du protocole TCP

En utilisant un système d'accusé de réception, TCP garantit un transfert de données fiable. En émission d'un segment, il est lié à un numéro d'ordre (ou numéro de séquence). Lorsque l'information est reçue, la machine affiche un segment d'information avec un drapeau d'identification de réception. Lorsqu'un segment est perdu, il est réexpédié à l'aide d'un chronomètre. Afin de synchroniser les séquences entre les machines en communication, on utilise le mécanisme de "three-way handshake" lors de la mise en place d'une connexion. Cela offre aux applications cliente et serveur la possibilité de se mettre d'accord sur les numéros de commande initiales.

3.4.1 Connexion TCP

Pour établit une connexion TCP entre le client et le serveur nous avons met en place un serveur TCP qui écoute sur une adresse IP "192.168.16.42" et un port spécifique "12345" pour envoie des données (sérialisées) au client.
Lorsqu'une connexion est établie, un paquet SYN est envoyé par le client, suivi d'un paquet SYN-ACK par le serveur, puis un paquet ACK par le client.
Cela établit une connexion TCP (Figure 3.2) en utilisant le "three-way handshake"

```
In [6]: runfile('C:/Users/Dell/Documents/serveur tcp.py',
TCP Server is listening on 192.168.137.7:12345
Connected to GCS by ('192.168.137.1', 54873)
```

(a) Le serveur est connecté au client

```
In [14]: runfile('C:/Users/Crash/Desktop/jupyter/clie.py',
wdir='C:/Users/Crash/Desktop/jupyter')
Connected to Drone at 192.168.137.7:12345
```

(b) Le client est connecté au serveur

Figure 3.2: L'établissement de connexion tcp entre client et serveur

3.4.2 Données Transmises

Dans notre travail, nous avons utilisé une image montré dans la figure 3.3 comme un signal d'information pour le DSSS. Le format des données DSSS suit un signal d'information numérique sous forme des bits (0 et 1). L'image est une représentation complexe bidimensionnelle de pixels en niveaux de gris, ce qui ne correspond pas directement au format de données attendu par le DSSS. Il faut convertir les données de l'image en un flux de bits binaires approprié pour le DSSS. Pour facilite la manipulation et l'encodage, nous avons redimensionné l'image originale en une version plus petite (`width` // 40, `height` // 40).

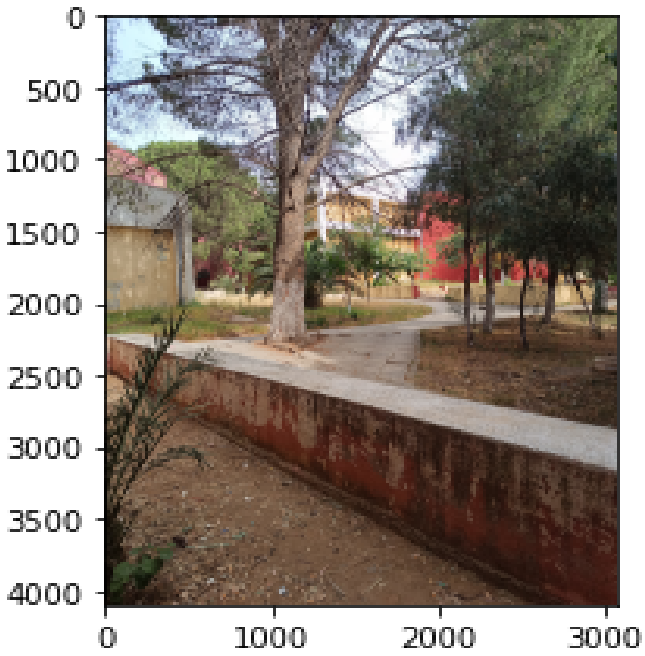


Figure 3.3: L'image transmis pour la simulation DSSS

Après la modulation DSSS ces bits binaires deviennent des symboles complexes (partie réelle et imaginaire), ces symboles vont être convertis en un format binaire adapté à l'envoi via TCP. Chaque symbole complexe est sérialisé en deux nombres flottants (float), représentant la partie réelle et la partie imaginaire.
Les données sérialisées est envoyés au client afin qu'il puisse les reconvertir en symboles complexes et effectuer la démodulation DSSS et finalement la reconstruction de l'image originale.

3.5 Résultats de Simulation

3.5.1 L'étalement de spectre à séquence directe

La figure 3.4 présente trois graphiques qui illustrent les différentes étapes du processus d'encodage DSSS (Direct Sequence Spread Spectrum) pour la transmission de données.

Le graphe de bits de données (data bits) montre la séquence des bits de données d'origine aprés la conversion de l'image en une représentation binaire. Chaque pixel de l'image est transformé en une séquence binaire de 8 bits par canal de couleur, et Les données binaires de l'image sont ensuite converties en une séquence de bits représenté par 1 et -1.

Le graphe de Chip Sequence Duplicated montre la séquence de chips utilisée pour l'encodage DSSS, dupliquée pour correspondre à la longueur des bits de données. Pour génère une séquence d'étalement, nous avons utilisé la transformée de Hadamard pour créer une matrice de walsh-

Hadamard. Une ligne aléatoire de cette matrice est sélectionnée pour être utilisée comme séquence d'étalement.

Le graphe de Données encodées (encoded Data) montre le résultat de l'application de la séquence de chips aux bits de données, produisant le signal encodé. Chaque bit de données est multiplié par la séquence de chips. Si le bit de données est 1, la séquence de chips est utilisée telle quelle. Si le bit de données est -1, la séquence de chips est inversée (multipliée par -1). Le résultat est une séquence de valeurs qui représente le signal étalé prêt pour la transmission.

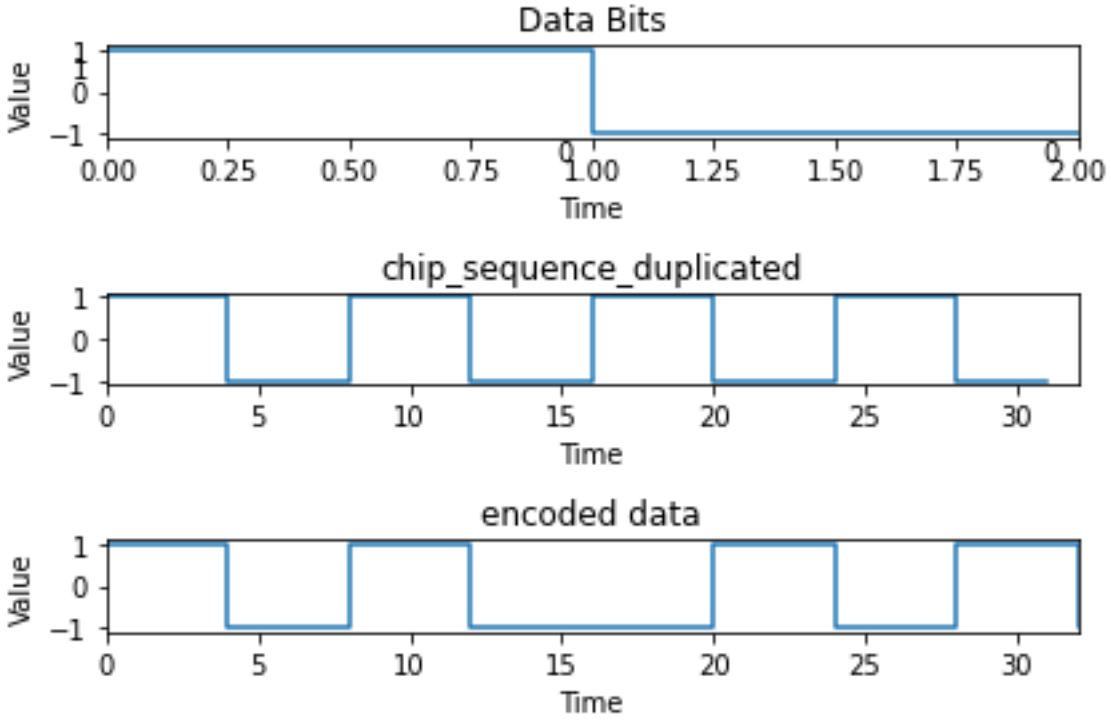


Figure 3.4: L'étalement de spetre DSSS

La figure 3.5 montre la densité spectrale de puissance (PSD) d'un signal de données. La PSD est une mesure qui montre comment la puissance du signal est distribuée en fonction de la fréquence.

Les pics présents dans la figure indiquent les fréquences dominantes dans le signal de données. Dans ce cas, on observe des pics importants à des fréquences spécifiques, par exemple à environ 1000 Hz, 2000 Hz, et 3000 Hz. Ces pics montrent où la majorité de la puissance du signal est concentrée. La densité spectrale de puissance plus faible entre les pics indique que le signal contient moins de puissance à ces fréquences intermédiaires.

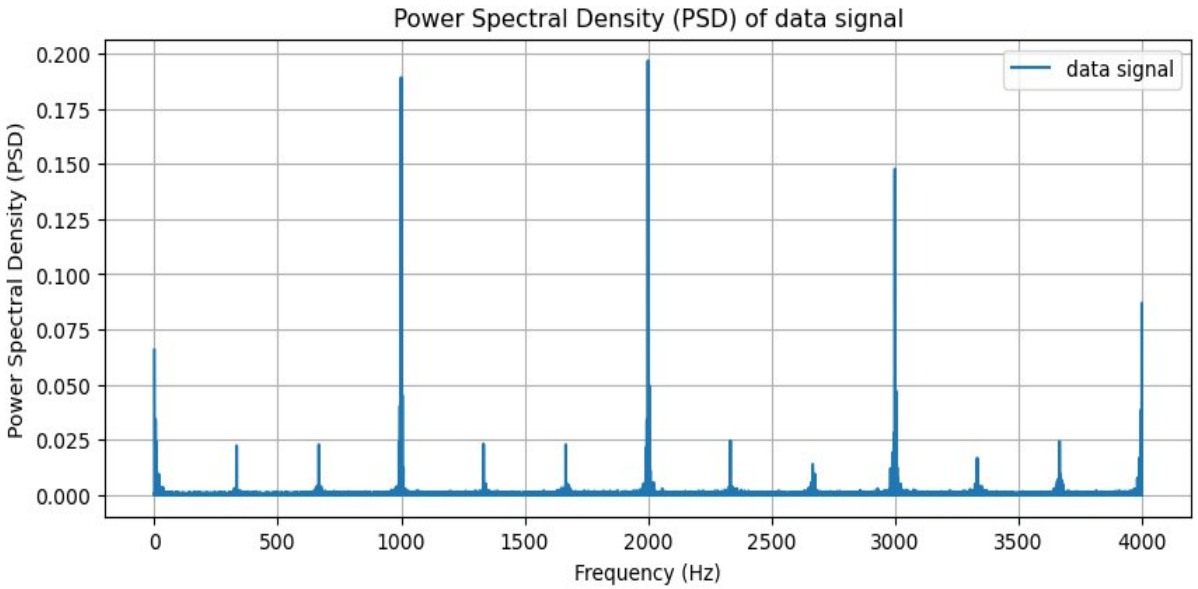


Figure 3.5: La densité spectrale de puissance (PSD) d'un signal de données

La figure 3.6 représente la densité spectrale de puissance du signal après l'encodage (étalement de spectre). Contrairement à la PSD du signal de données non encodé, qui montrait des pics étroits et bien définis à des fréquences spécifiques, cette figure montre une répartition plus étendue de la puissance sur une gamme plus large de fréquences, ce qui est une caractéristique typique de l'encodage DSSS.

Bien que des pics de puissance soient toujours présents, ils sont plus nombreux et moins marqués, indiquant que le signal a été étalé sur une plus large bande de fréquences. Les pics principaux semblent être centrés autour de fréquences spécifiques, mais ils sont entourés de nombreux autres pics plus petits, ce qui indique une distribution plus uniforme de la puissance.

- **Avant Encodage :** La densité spectrale de puissance montrait des pics distincts à des fréquences spécifiques, indiquant que la puissance du signal était concentrée dans ces fréquences.
- **Après Encodage (Figure Actuelle) :** La PSD montre que la puissance est étalée sur une gamme plus large de fréquences. Cela correspond à l'effet du codage DSSS, où une séquence pseudo-aléatoire est utilisée pour étaler le spectre du signal.

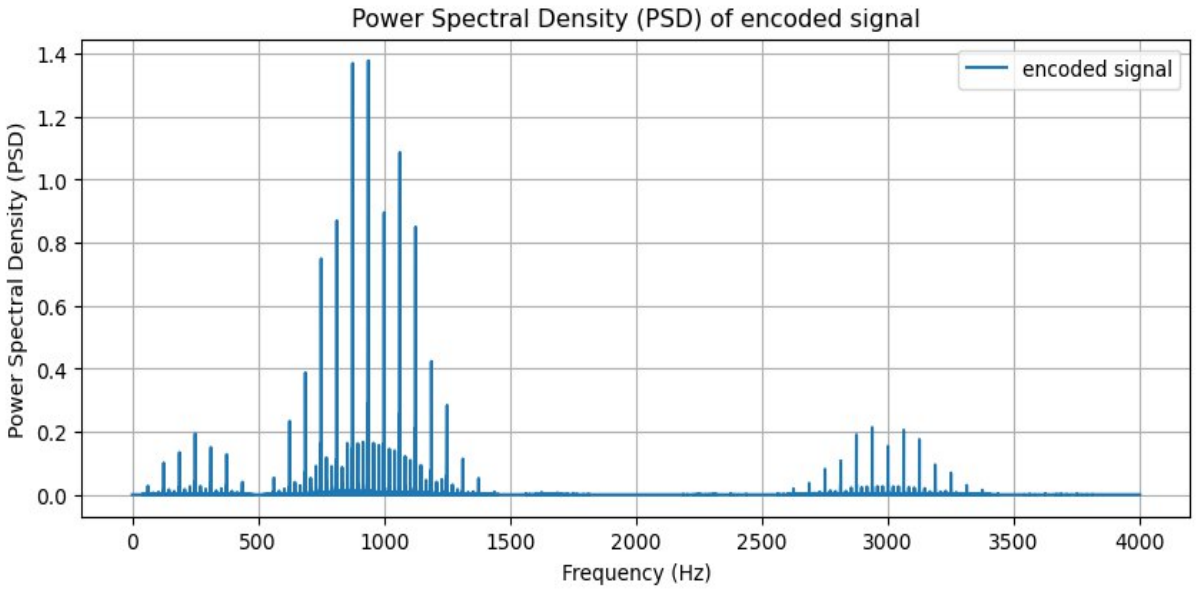


Figure 3.6: La densité spectrale de puissance (PSD) d'un d'un signal encodé

3.5.2 Signal modulé en QAM

La figure 3.7 montre une table de correspondance des symboles pour la modulation 128-QAM (Quadrature Amplitude Modulation). En modulation QAM, chaque symbole est représenté par un point dans un plan bidimensionnel, où l'axe des x représente la composante en phase (I) et l'axe des y représente la composante en quadrature (Q). Cette modulation utilise 128 points de constellation, ce qui permet de transmettre 7 bits par symbole (car 2^7=128).

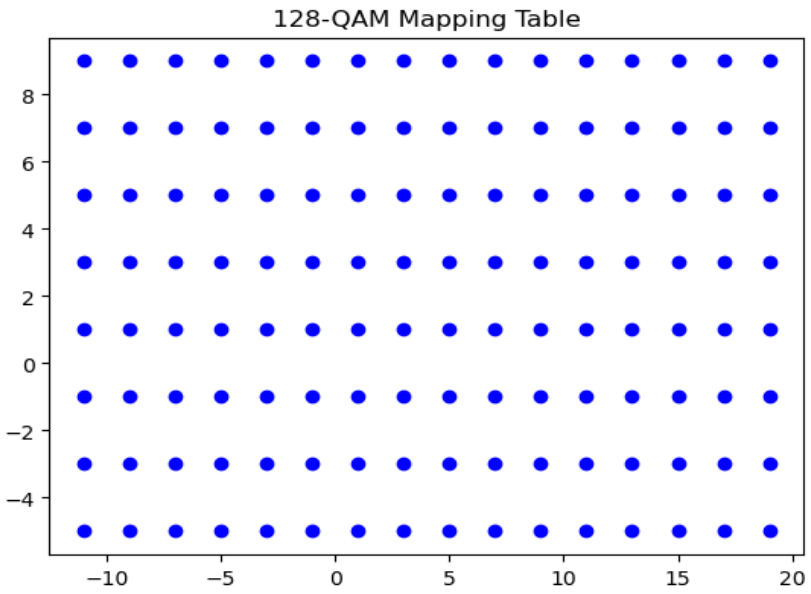


Figure 3.7: La table de correspondance des symboles pour la modulation 128-QAM

Une constellation d'un signal transmis à l'aide d'une modulation QAM est illustrée dans la figure 3.8. Dans le plan IQ, les symboles modulés sont symbolisés par des points bleus, où la composante en phase est située sur l'axe des x et la composante en quadrature sur l'axe des y. Les points se situent dans des positions qui montrent les diverses combinaisons d'amplitude et de phase employées pour transmettre les données. Une constellation QAM efficace doit comporter des points bien rapprochés et alignés afin de réduire au minimum les erreurs de transmission.

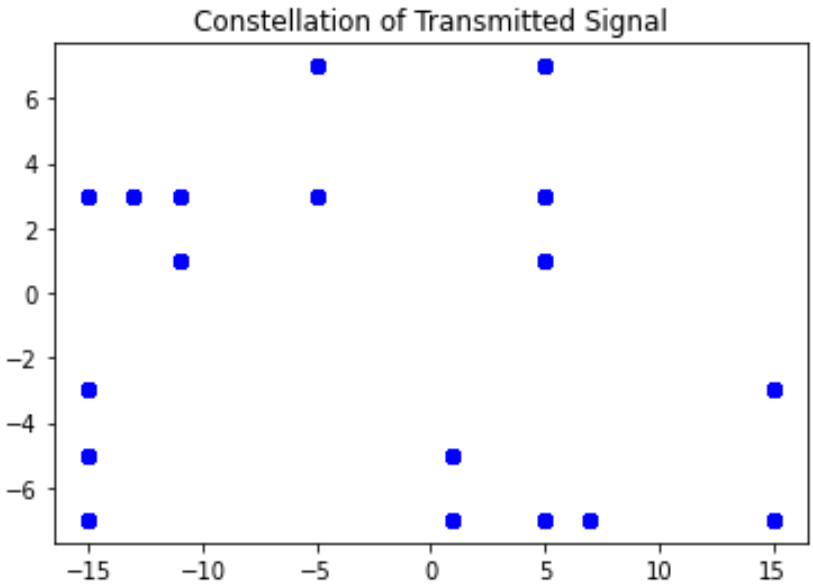


Figure 3.8: constellation d'un signal transmis d'une modulation QAM

Dans notre travail, nous avons utilisé deux modulations QAM(128-QAM) et QPSK pour comparer entre les deux. La figure 3.9 montre un signal modulé utilisant la modulation d'amplitude en quadrature (QAM) à 128 états (128-QAM). Dans une modulation 128-QAM, il y a 128 états possibles de la combinaison des amplitudes des deux porteuses, ce qui permet de transmettre une grande quantité d'informations par unité de temps.

Dans le domaine des communications, un signal modulé en QAM peut être représenté par une composante réelle (I pour "In-phase") et une composante imaginaire (Q pour "Quadrature"). Ces composantes sont modulées indépendamment et combinées pour former le signal final.

- La courbe bleue (partie réelle) et la courbe orange (partie imaginaire) fluctuent de manière complexe, reflétant les variations rapides des amplitudes dues à la modulation 128-QAM.
- Les variations des amplitudes dans les deux courbes représentent les informations encodées dans le signal.

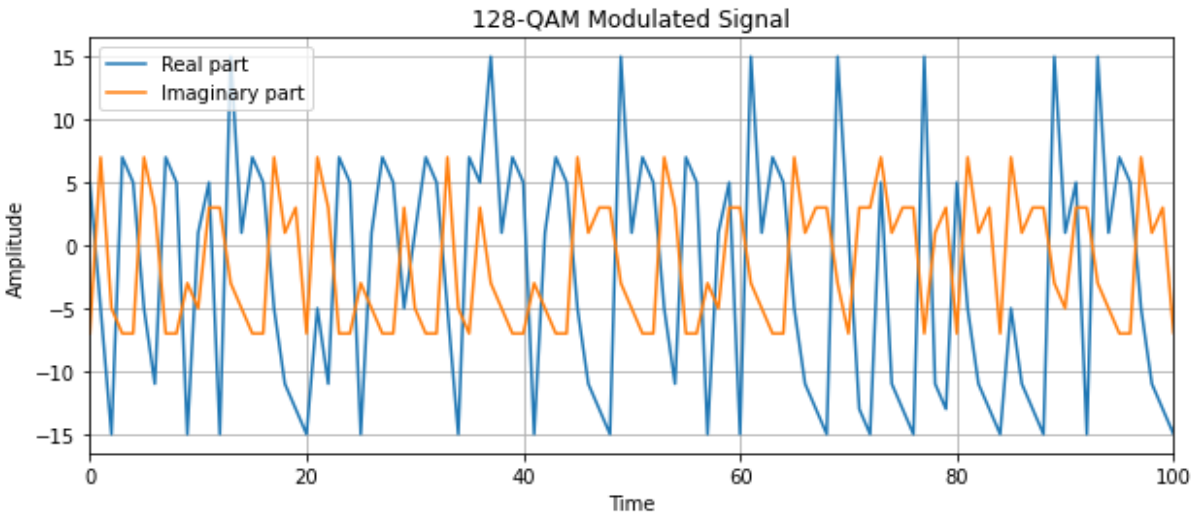


Figure 3.9: Signal modulé par 128-QAM

La figure 3.10 montre la densité spectrale de puissance (DSP ou PSD pour Power Spectral Density) d'un signal modulé en fonction de fréquence, nous avons observés :

- Des pics importants à certaines fréquences particulières, comme près de 0 Hz, à environ 2000 Hz et près de 4000 Hz, qui suggèrent que le signal contient des composantes de forte puissance à ces fréquences.
- Le pic près de 0 Hz est souvent la composante continue ou la composante moyenne du signal, tandis que les pics à 2000 Hz et 4000 Hz suggèrent la présence de composantes périodiques ou harmoniques à ces fréquences, souvent liées à la modulation du signal.
- Les petites variations de la PSD entre les pics principaux peuvent représenter des composantes harmoniques mineures ou du bruit dans le signal.

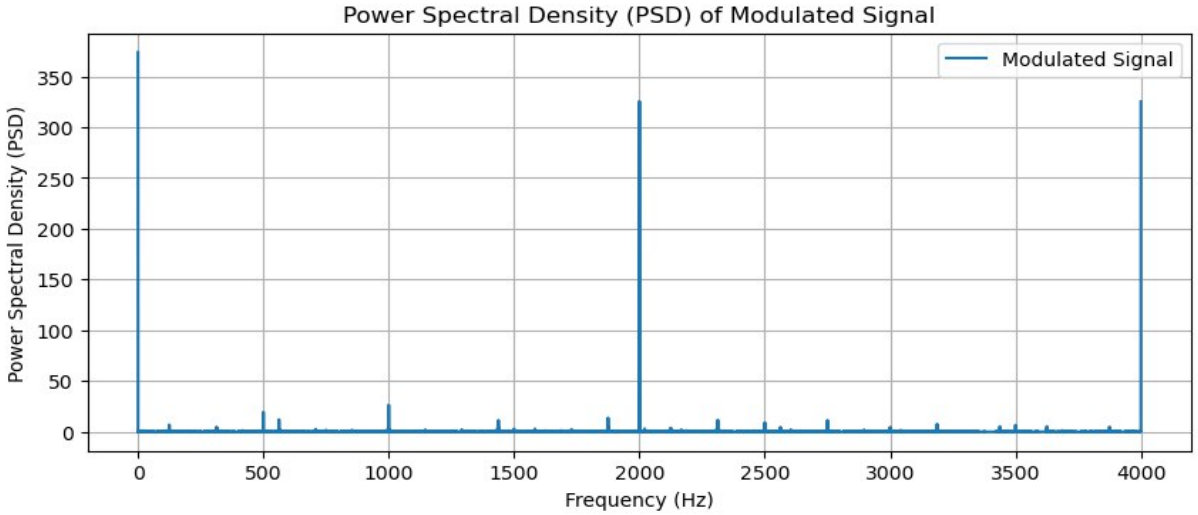


Figure 3.10: La densité spectrale de puissance du signal modulé en QAM

3.5.3 Signal modulé en QPSK

La figure 3.11 montre un signal modulé en utilisant la modulation par déphasage en quadrature (QPSK, Quadrature Phase Shift Keying). la courbe orange (partie imaginaire) montrent des transitions entre les niveaux d'amplitude.

La modulation QPSK encode deux bits par symbole, avec chaque symbole représentant une combinaison spécifique des phases de la composante réelle et imaginaire. Les transitions régulières et les niveaux d'amplitude discrets reflètent les changements de phase du signal modulé, permettant ainsi de transmettre des données de manière efficace.

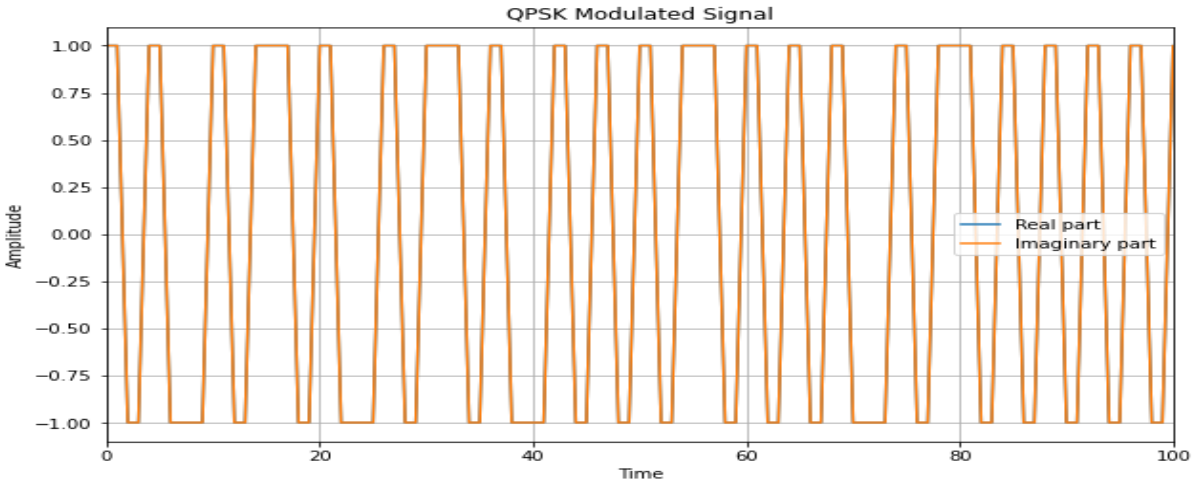


Figure 3.11: Signal modulé par la QPSK

La figure 3.12 représente la densité spectrale de puissance (PSD) d'un signal modulé. Le pic principal à environ 2000 Hz indique la fréquence porteuse, et la largeur de bande autour de ce pic montre la bande passante du signal modulé.

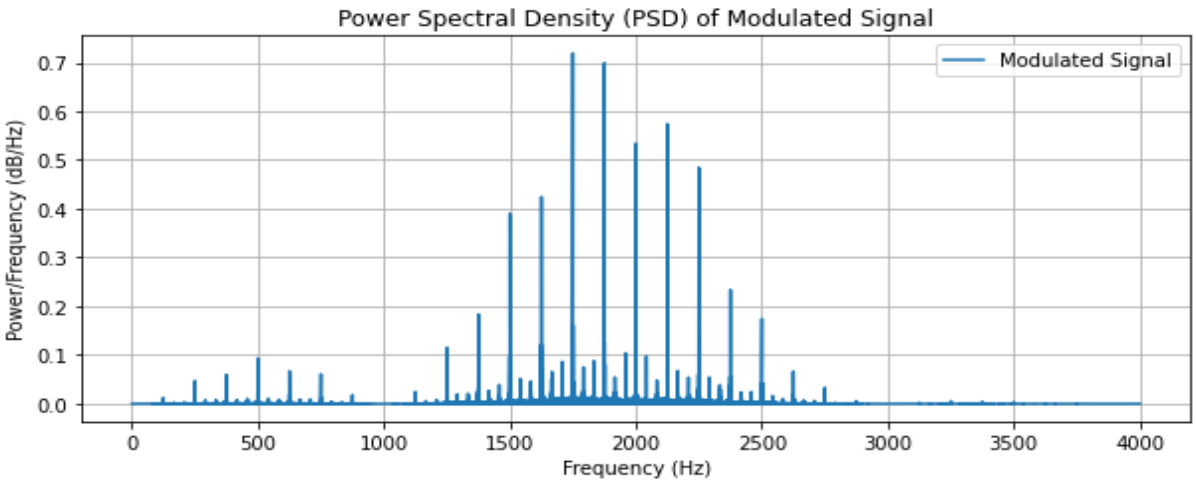


Figure 3.12: La densité spectrale de puissance d'un signal modulé en QPSK

3.5.4 Le bruit ajouté aux signal modulé

La figure 3.13 montre les parties réelle et imaginaire d'un signal de bruit (bruit blanc gaussien additif) en fonction du temps, ce bruit ajouté aux signal modulé.

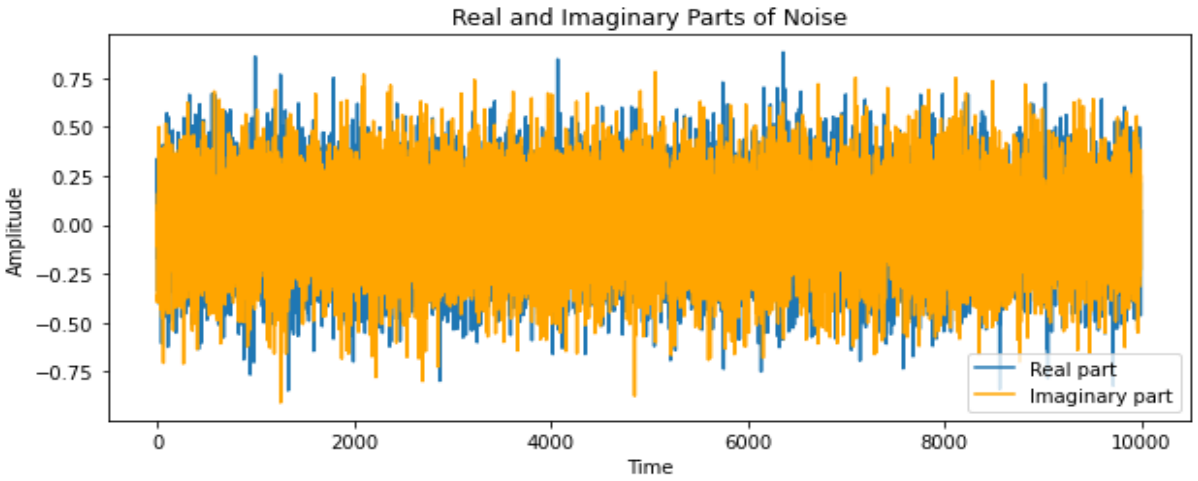


Figure 3.13: Le signal d'un bruit blanc Gaussien additif

3.5.5 Le signal reçu avec bruit modulé en 128-QAM

La figure 3.14 montre la constellation d'un signal reçu avec bruit, affecté par un canal de Rayleigh avec un effet Doppler. Les points de constellation sont dispersés largement, avec des points éparpillés loin de l'origine. Cela indique des variations importantes dues au canal de Rayleigh et à l'effet Doppler.

L'effet Doppler, causé par la vitesse élevée, entraîne un décalage de fréquence du signal reçu. Ce décalage varie en fonction du mouvement relatif entre l'émetteur et le récepteur.

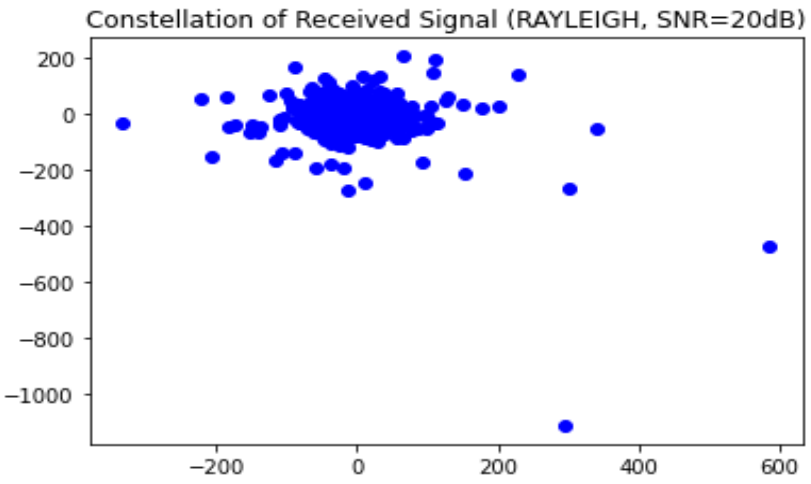


Figure 3.14: La constellation d'un signal reçu avec bruit

La figure 3.15 montre les parties réelle et imaginaire d'un signal reçu modulé en 128-QAM (Quadrature Amplitude Modulation). Les variations observées dans les courbes des parties réelle et imaginaire du signal reçu montrent les fluctuations dues au canal de transmission et aux effets Doppler. Ces fluctuations peuvent être dues à des interférences, du bruit.

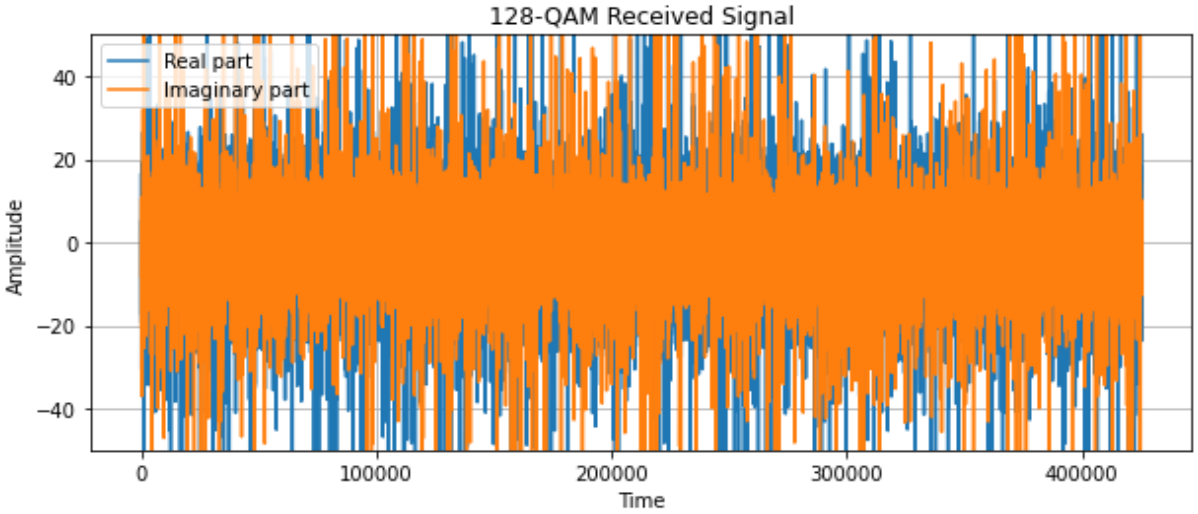


Figure 3.15: Le signal reçu modulé en 128-QAM

La figure 3.16 montre la densité spectrale de puissance (Power Spectral Density, PSD) d'un signal reçu modulé en 128-QAM.

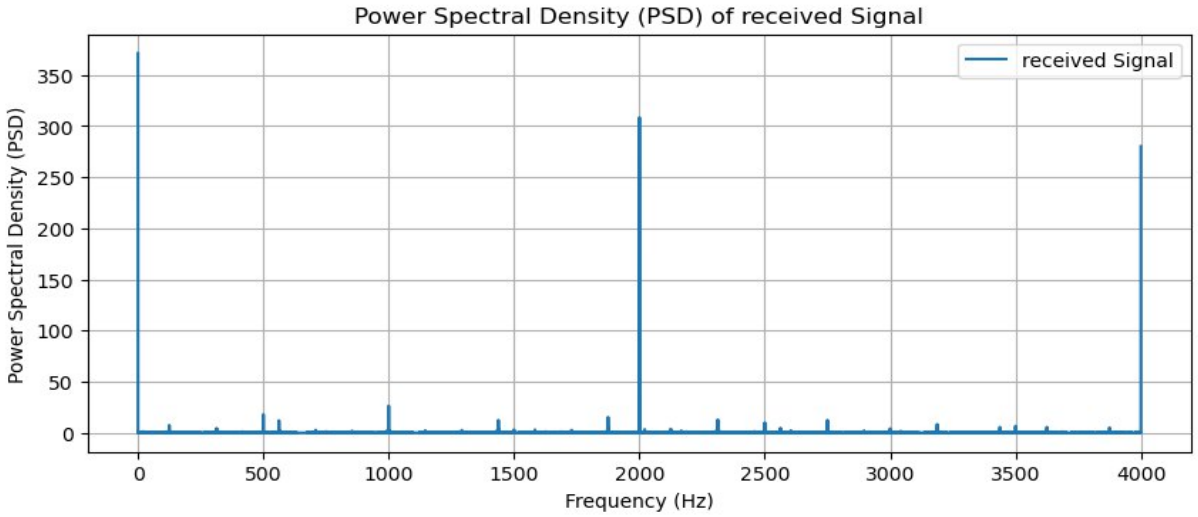


Figure 3.16: La densité spectrale de puissance d'un signal reçu modulé en 128-QAM

3.5.6 Le signal reçu avec bruit modulé en QPSK

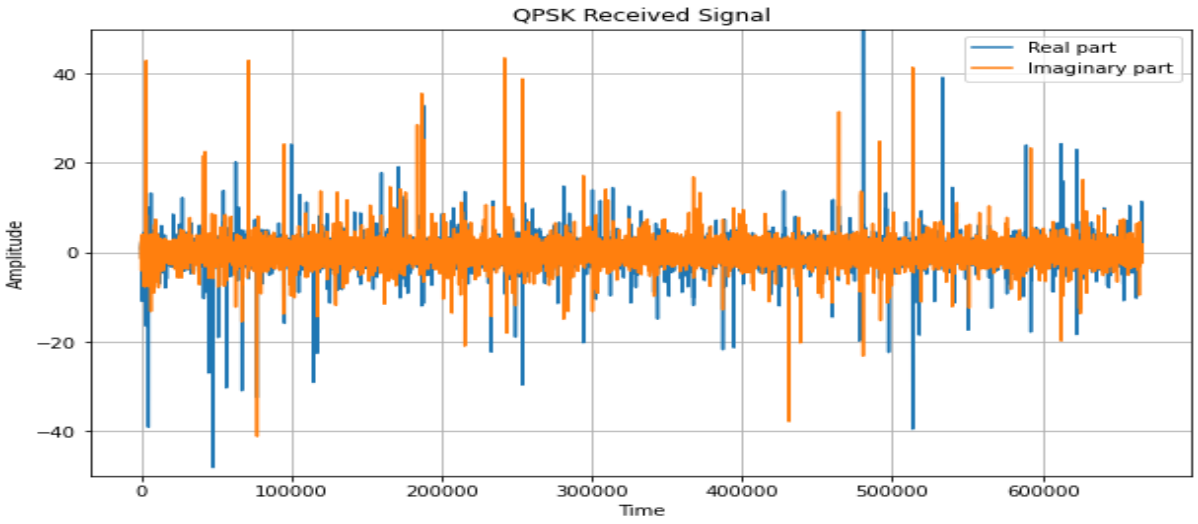


Figure 3.17: Un signal reçu modulé en QPSK

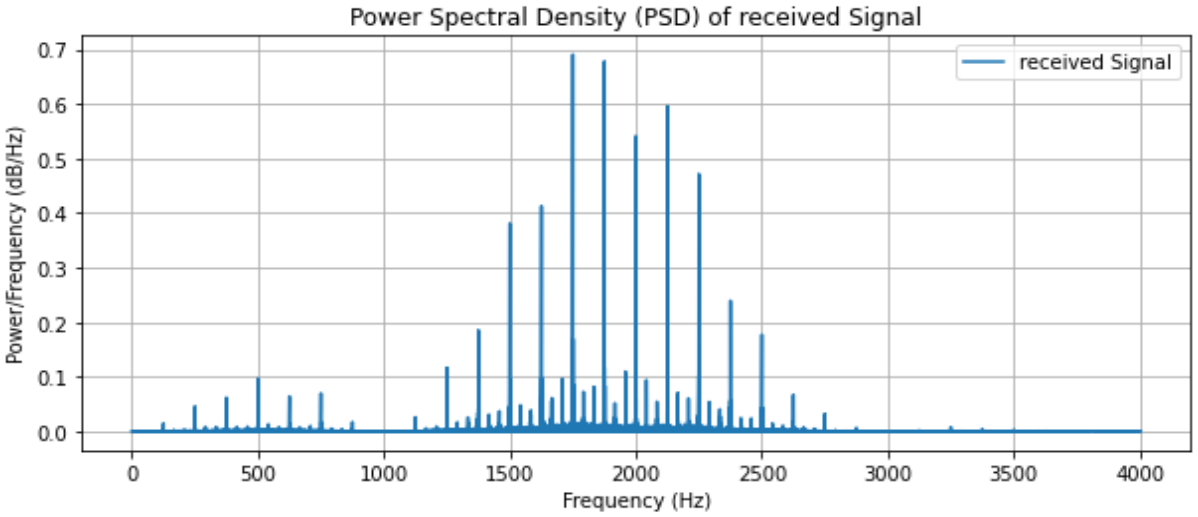


Figure 3.18: La densité spectrale de puissance d'un signal reçu modulé en QPSK

3.5.7 Signal démodulée à partir d'un signal QAM

Pendant la modulation, les données numériques sont converties en un signal analogique qui peut être transmis sur un canal de communication. Pendant la démodulation, ce signal analogique est converti de nouveau en données numériques. La figure 3.19 montre le comportement temporel de la partie réelle d'un signal démodulé à partir d'un signal QAM(128-QAM), avec la partie imaginaire étant constante à zéro.

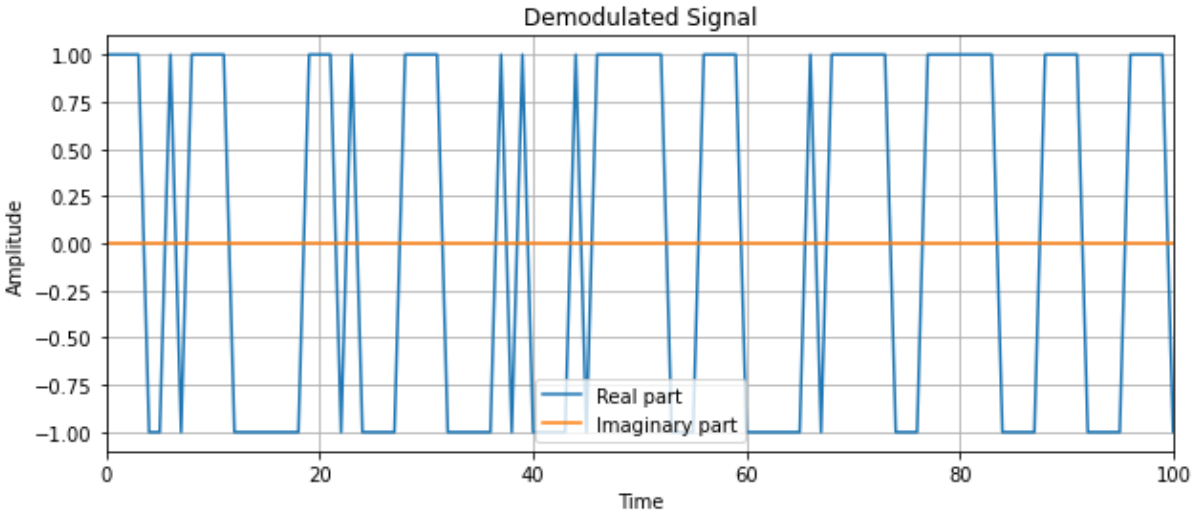


Figure 3.19: Signal démodulé

La densité spectrale de puissance (PSD) du signal démodulé est illustré dans la figure 3.20. le signal démodulé est constitué d'une composante principale à la fréquence du signal porteur et de plusieurs composantes secondaires à des fréquences plus basses. Cela est dû au processus de démodulation, qui permet de récupérer le signal original à partir du signal modulé.

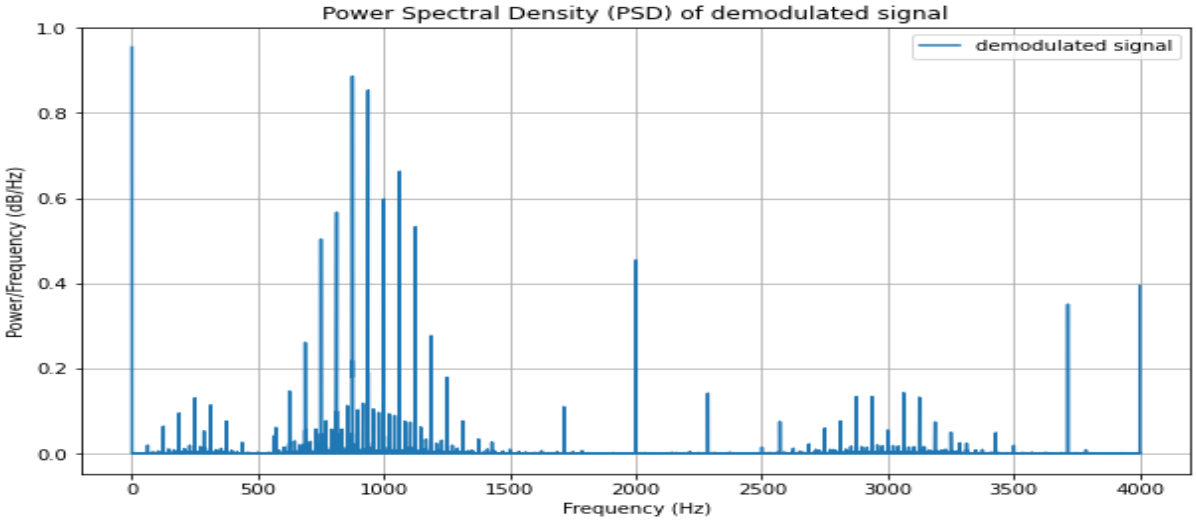


Figure 3.20: La densité spectrale de puissance du signal démodulé

3.5.8 Signal démodulée à partir d'un signal QPSK

La figure 3.21 montre le signal démodulé en QPSK, où les transitions de niveaux d'amplitude représentent les changements de phase correspondant aux symboles QPSK.

La figure 3.22 montre la densité spectrale de puissance de ce signal, mettant en évidence les fréquences dominantes et leurs puissances associées.

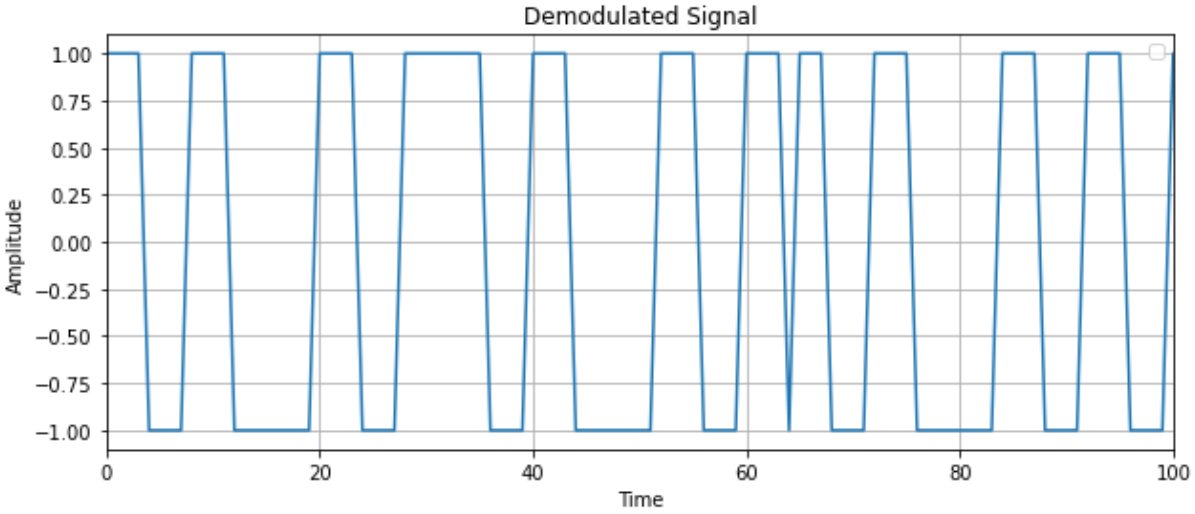


Figure 3.21: Signal demodulé

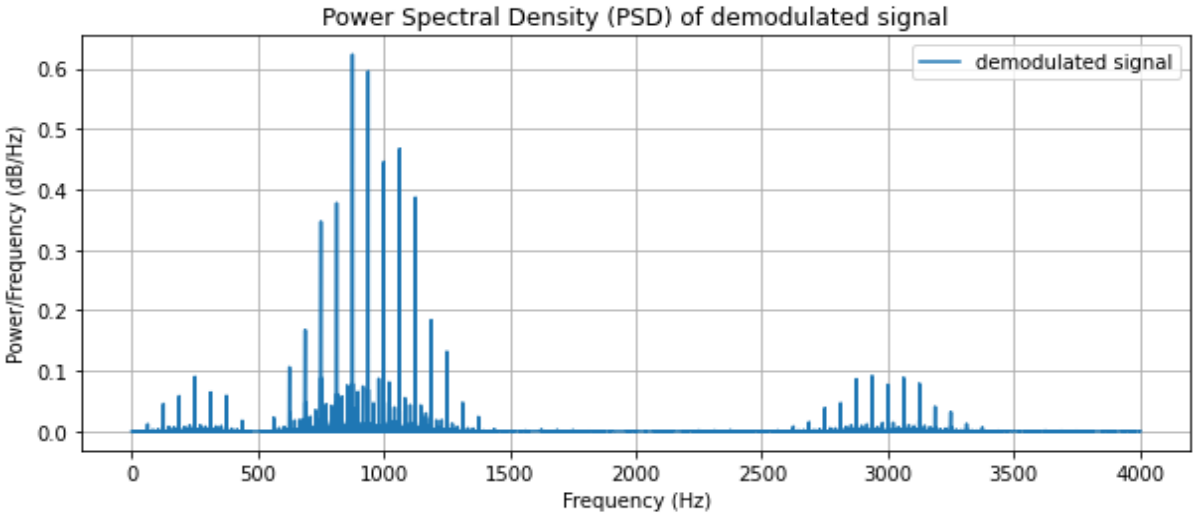


Figure 3.22: La densité spectrale de puissance du signal démodulé

3.5.9 Désétalement de spectre à séquence directe

Le récepteur utilise la même séquence d'étalement pour corréler le signal reçu et récupérer les bits de données originaux. Le processus inverse du DSSS est appliqué pour obtenir le signal

décodé.

La figure 3.23 montre le signal décodé après avoir traversé le processus d'encodage et de décodage DSSS. Le signal récupéré présente des valeurs discrètes oscillant entre 1 et -1, représentant les bits de données originaux. Cela démontre que le processus de DSSS a permis de transmettre et de récupérer les bits de données de manière efficace, même en présence de bruit et d'interférences dans le canal de communication.

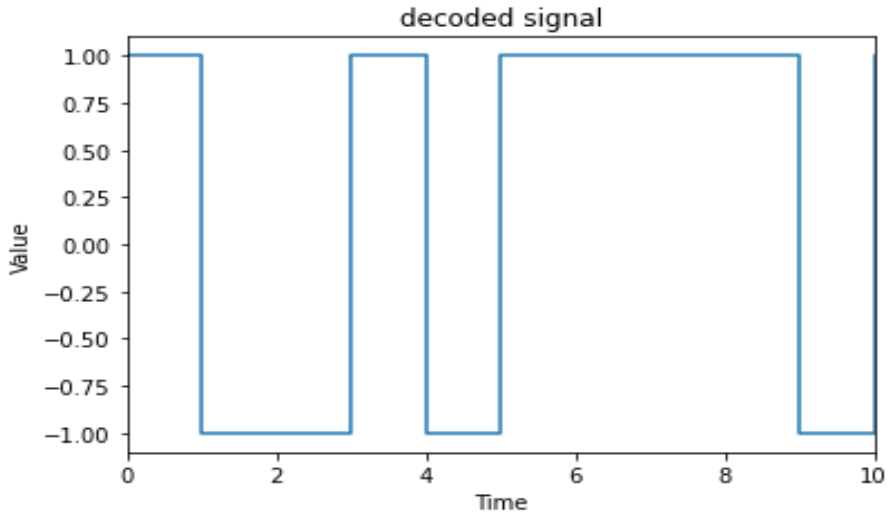


Figure 3.23: Signal decodé

La figure 3.24 montre la densité spectrale de puissance d'un signal décodé. La PSD du signal décodé ressemble plus à la PSD du signal original non encodé, avec des pics bien définis aux mêmes fréquences. Cela montre que le processus de décodage a réussi à récupérer les fréquences dominantes du signal d'origine.

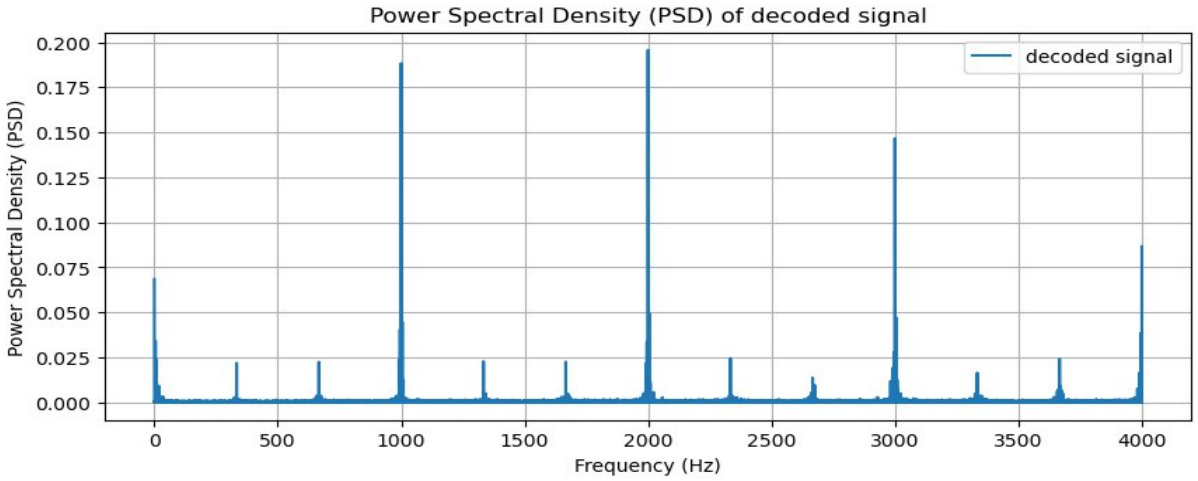


Figure 3.24: La densité spectrale de puissance d'un signal décodé

3.6 Comparaison de BER en fonction de SNR

3.6.1 Le BER de 128 QAM et la QPSK

Pour réaliser une étude comparative, nous devons analyser les performances des modulations 128 QAM et QPSK sur deux types de canaux : AWGN (Additive White Gaussian Noise) et Rayleigh. Nous considérerons également l'effet Doppler avec une vitesse de 40 m/s et une fréquence de 1kHz. La figure 3.25 montre le taux d'erreur binaire (BER) en fonction du rapport signal sur bruit (SNR) pour les modulations 128 QAM et QPSK.

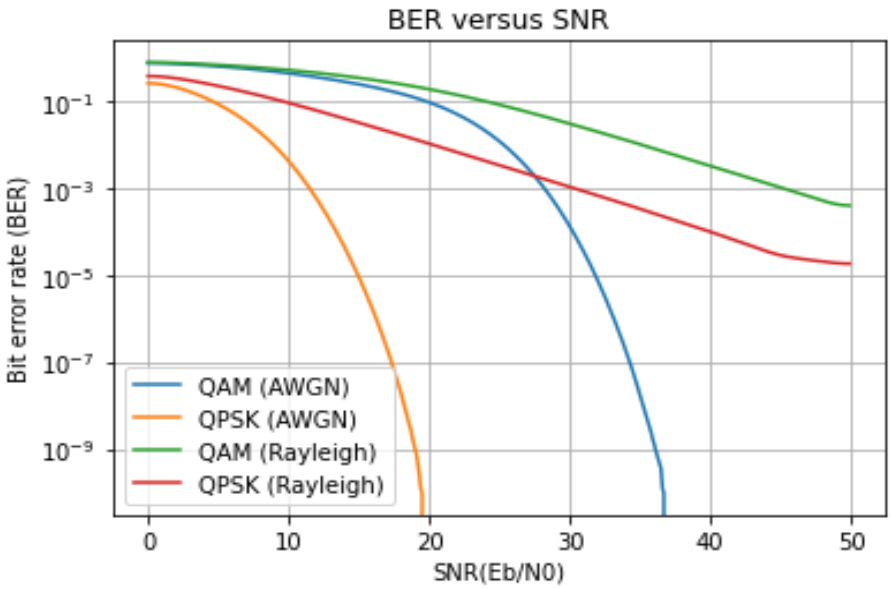


Figure 3.25: Le BER en fonction SNR pour les modulations 128 QAM et QPSK

- **128 QAM (AWGN) :**
  - Le taux d'erreur binaire diminue à mesure que le SNR augmente jusqu'à ce qu'il devienne nul.
  - La modulation 128 QAM offre une meilleure efficacité spectrale que QPSK.
  - La courbe BER-QAM est plus proche de la capacité théorique du canal AWGN.
- **QPSK (AWGN) :**
  - Le taux d'erreur binaire est également réduit avec l'augmentation du SNR jusqu'à ce qu'il devienne nul.
  - QPSK est moins efficace que QAM en termes de bande passante.
  - La courbe BER-QPSK suit la même tendance que QAM.
- **128 QAM (Rayleigh) :**
  - Dans un canal Rayleigh, la performance se dégrade en raison de l'effet Doppler de vitesse 40 m/s et fréquence de 1khz et le BER devient BER = 0,0007.

— La courbe BER-QAM est plus élevée que celle dans le canal AWGN.

- **QPSK (Rayleigh) :**
  — Le canal Rayleigh affecte davantage QPSK que QAM.
  — La courbe BER-QPSK est significativement plus élevée dans le canal Rayleigh, mais le BER reste toujours nul.

Nous avons remarqué que la modulation 128 QAM est plus efficace en termes de bande passante, mais elle est plus sensible au l'effet d'oppler dans le canal Rayleigh. D'un autre côté, QPSK présente une meilleure résistance dans ce canal, mais une faible efficacité en termes de bande passante.

3.6.2 Le BER des différents M valeurs de QAM

Les courbes de la figure 3.26 montrent les performances des différentes modulations M-QAM (4-QAM, 8-QAM, 16-QAM, 32-QAM, 64-QAM, 128-QAM, 256-QAM) en termes de BER en fonction du SNR.
Plus le SNR est élevé, plus le taux d'erreur binaire est faible, les modulations à plus haute densité (comme 128-QAM 256-QAM) ont des BER plus élevés, mais offrent un débit de données plus élevé.

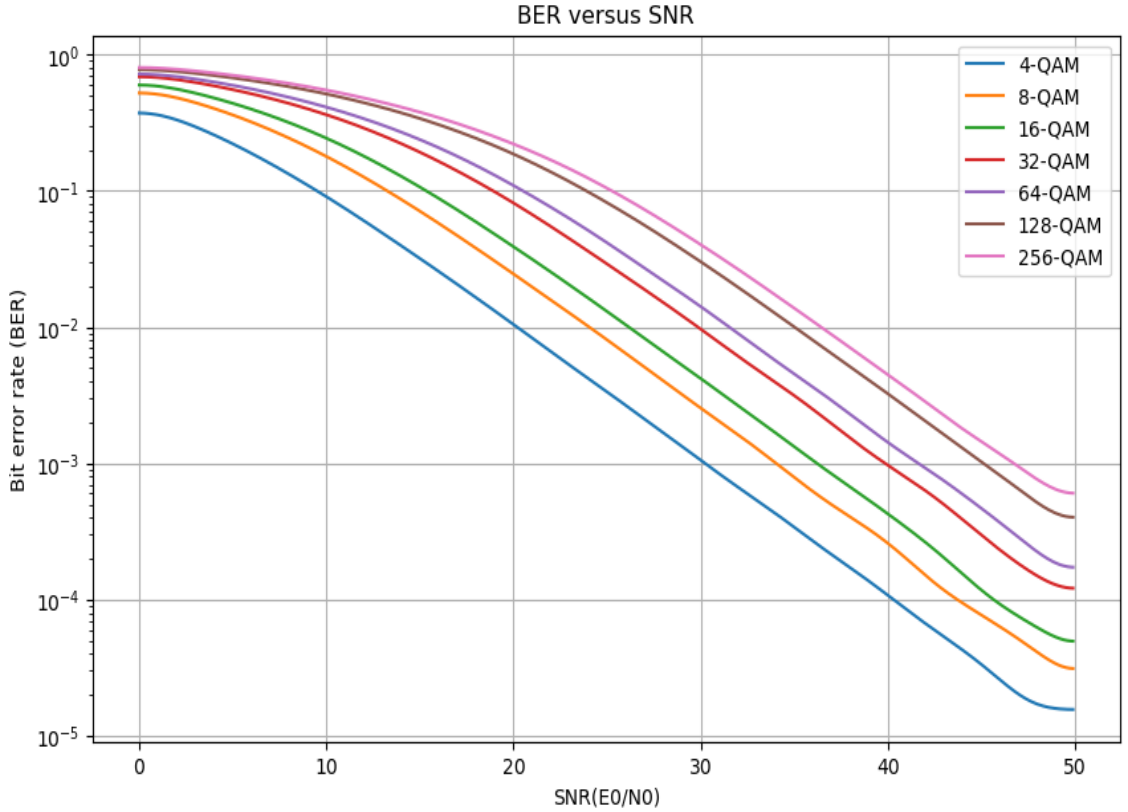


Figure 3.26: Le BER en fonction SNR pour les modulations M-QAM

Le tableau 3.2 présente la valeur de BER pour chaque modulation M-QAM.

Type de modulation	taux d'erreur binaire
4-QAM	0.0
8-QAM	0.0
16-QAM	0.0
32-QAM	2.1499×10^{-5}
64-QAM	1.3974×10^{-4}
128-QAM	7.4174×10^{-4}
256-QAM	1.6769×10^{-3}

Tableau 3.2: Valeurs de BER pour les M-QAM modulations

Le choix de la modulation sera déterminé par les conditions du canal et les exigences en matière de taux d'erreur pour une application pratique. Dans des environnements bruyants, les modulations plus simples telles que 4-QAM ou 16-QAM sont plus résistantes, tandis que des modulations plus complexes telles que 128-QAM ou 256-QAM offrent des débits de données plus élevés, mais nécessitent des conditions de canal meilleures (SNR plus élevés).

3.6.3 Le BER des différents vitesses de déplacement

La figure 3.27 présente le taux d'erreur binaire (BER) en fonction du rapport signal sur bruit (SNR) de modulation 128 QAM sur le canal Rayleigh avec des différents vitesses de déplacement.

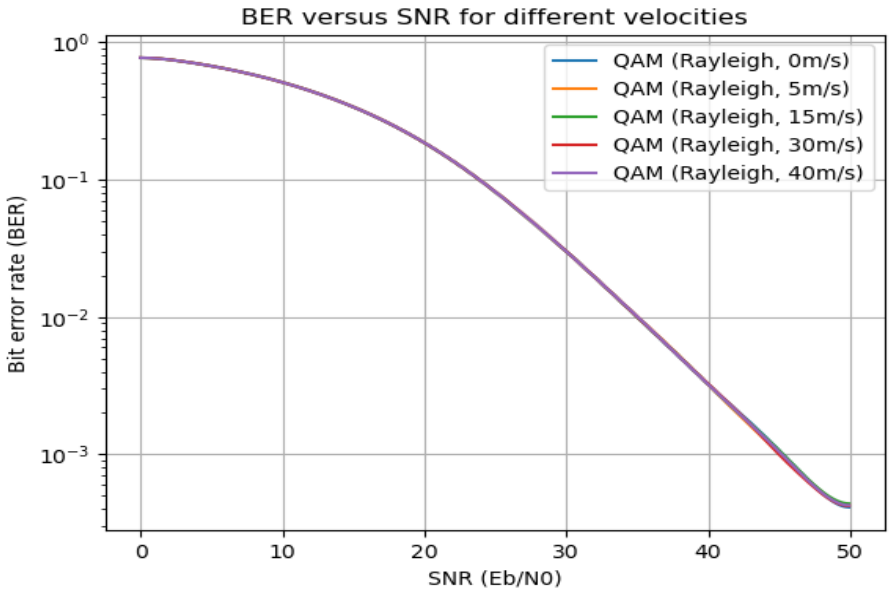


Figure 3.27: Comparaison de BER pour différents vitesses de déplacement

Le tableau 3.3 présente la valeur de BER pour chaque vitesse de déplacement.

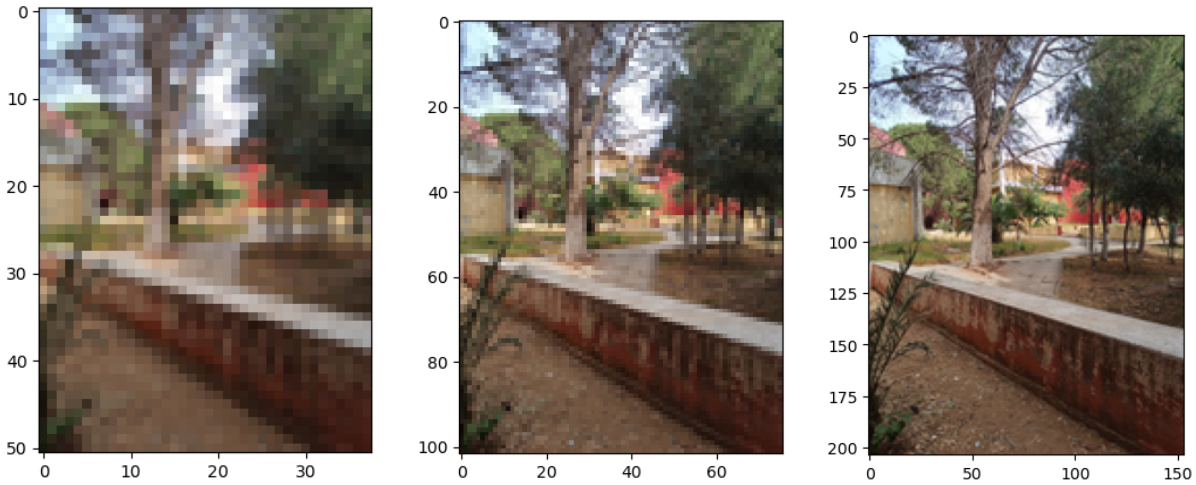
Vitesses m/s	Taux d'erreur binaire
0	7×10^{-4}
5	8×10^{-4}
15	8×10^{-4}
20	7×10^{-4}
40	8×10^{-4}

Tableau 3.3: Valeurs de BER pour les différents vitesses

Nous constatons que le BER ne varie pas de façon linéaire en fonction de la vitesse. Les variations des valeurs de BER indiquent que d'autres éléments environnementaux ou techniques peuvent avoir un impact sur le taux d'erreur, en dehors de la vitesse de l'objet.

3.7 La reconstruction de l'image

À la fin de notre travail, nous avons tenté de reconstruire l'image originale que le serveur envoie au client à partir des bits de 1 et de 0 vers une image. Pour ce faire, nous avons utilisé différentes résolutions de l'image originale. Plus la résolution est élevée, plus il faut de bits à transmettre, ce qui entraîne des temps de récupération plus longs de l'image originale.
La figure 3.28 montre les images reconstruites pour différentes résolutions de l'image originale utilisée dans la simulation de notre code.



(a) largeur//80, hauteur//80 **(b)** largeur//40, hauteur//40 **(c)** largeur//20, hauteur//20

Figure 3.28: Les images reconstruites pour différentes résolutions

3.8 Conclusion

Nous avons effectué dans ce chapitre une simulation de la technique DSSS à l'aide du langage de programmation Python, en utilisant un protocole serveur-client TCP pour transmettre une image dans un réseaux sans fil et nous ajoutons un bruit blanc gaussien additif dans le but de renforcer la sécurité des transmissions dans les drones, nous avons fait une étude comparative sur les deux types de modulations numériques (QAM & QPSK) utilisé dans la technique DSSS, Nous avons remarqué que la QPSK donne de meilleur résultats en termes de taux d'erreurs binaire, tandis que la 128 QAM offrent un débit de données plus élevé.

Conclusion Générale

Dans ce mémoire nous explorons en détail l'importance croissante de l'étalement de spectre à séquence directe (DSSS) dans le renforcement de la fiabilité et de la sécurité des systèmes de communication, en particulier dans les environnements confrontés à des interférences et à des brouillages importants. Les applications des drones en constituent un exemple concret, où la stabilité et la sécurité des communications sont primordiales pour des missions critiques.
Le DSSS se distingue par sa capacité à répartir le signal de transmission sur une large bande de fréquences, plutôt que de se concentrer sur une seule fréquence fixe. Cette approche ingénieuse permet de minimiser considérablement l'impact des interférences et du brouillage, qui peuvent perturber et même interrompre les communications traditionnelles. En effet, en utilisant une séquence pseudo-aléatoire pour étaler le signal, le DSSS réduit la probabilité qu'un signal soit affecté par des interférences à un moment donné.
L'efficacité du DSSS repose sur l'optimisation de paramètres clés tels que le choix de la séquence d'étalement et le rapport signal sur bruit (SNR). La séquence d'étalement détermine comment le signal est réparti sur le spectre, tandis que le SNR mesure la qualité du signal par rapport au bruit. En ajustant ces paramètres en fonction des exigences spécifiques de l'application, il est possible de maximiser le débit, d'améliorer la qualité de la transmission et de minimiser le taux d'erreur de bit.
Les simulations montrent que la DSSS est efficace pour atténuer les effets du brouillage et des interférences, et améliorer la fiabilité des transmissions des données dans les drones. En répartissant le signal sur une large bande de fréquences grâce à une séquence pseudo-aléatoire, le DSSS réduit la probabilité qu'un signal soit affecté par des interférences à un moment donné. Nos recherches ont également utilisé deux types de modulation, le QAM et le QPSK, pour optimiser les performances du DSSS. Les résultats indiquent une amélioration notable du rapport signal sur bruit (SNR) et une diminution de taux d'erreur de bit (BER), contribuant ainsi à une communication plus stable et sécurisée, essentielle pour les applications critiques des drones.
L'intégration de la modulation OFDM (Orthogonal Frequency Division Multiplexing) est proposée comme prochaine étape pour renforcer encore la robustesse et l'efficacité des communications par drone.

Bibliographie

[1] Yves Vanhellemont Samuel Dubois, Michael de Bouw. Les drones au service de la construction : Technologies, enjeux et perspectives. *Innovation Paper / CSTC*, 2019.

[2] Abderrezzag ZIOU. Réalisation d'un système de suivi d'objets basé sur les drones. Mémoire de MASTER, Université de 8 Mai 1945 Guelma, Octobre 2020.

[3] Márton Bálint. History, types, application and control of drones. *Security Science Review*, 2022.

[4] hasni Mhamed Sanah nabil. Simulation numerique et etude dynamique du drone shadow 200. Mémoire de MASTER, Université Saad Dahleb Blida 1, 2010/2011.

[5] Rodolphe Jobard. *Les Drones : fonctionnement, télépilotage, applications, réglementation 3e éd.* Editions Eyrolles, 2017.

[6] Jun Ni, Jibin Hu, and Changle Xiang. Unmanned Ground Vehicles : An Introduction. In Jun Ni, Jibin Hu, and Changle Xiang, editors, *Design and Advanced Robust Chassis Dynamics Control for X-by-Wire Unmanned Ground Vehicle*, pages 1–19. Springer International Publishing, 2018.

[7] Hongfei Yao, Hongjian Wang, Yiming Li, Ying Wang, and Chunsong Han. Research on Unmanned Underwater Vehicle Threat Assessment. *IEEE Access*, 2019.

[8] Haque Nawaz, Husnain Mansoor Ali, and Shafiq-ur-Rehman Massan. Applications of unmanned aerial vehicles : A review. *3C Tecnología*, pages 85–105, 2019-11-06.

[9] Birmingham. *Building Multicopter Video Drones - Build and Fly Multicopter Drones To Gather Breathtaking Video Footage*. Packt Publishing, 2014.

[10] Thi VO, Chia-Nan Wang, Fu-Chiang Yang, Tien Nguyen, and Mandeep SINGH. Internet of Things (IoT) : Wireless Communications for Unmanned Aircraft System. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, 23 :388–399, 2023-10-16.

[11] Navid Khan, N. Jhanjhi, Sarfraz Brohi, Abdulwahab Almazroi, and Abdulaleem Almazroi. A Secure Communication Protocol for Unmanned Aerial Vehicles. *Computers, Materials & Continua*, 2021.

[12] Azza Allouch, Omar Cheikhrouhou, Anis Koubâa, Mohamed Khalgui, and Tarek Abbes. Mavsec : Securing the mavlink protocol for ardupilot/px4 unmanned aerial systems. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 621–628. IEEE, 2019.

[13] Anis Koubâa, Azza Allouch, Maram Alajlan, Yasir Javed, Abdelfettah Belghith, and Mohamed Khalgui. Micro air vehicle link (mavlink) in a nutshell : A survey. *IEEE Access*, 7 :87658–87680, 2019.

[14] Patrick Purucker, Josef Schmid, Alfred Hob, and Bjorn W. Schuller. System requirements specificationfor unmanned aerial vehicle uav to server communication. In *2021 International Conference on Unmanned Aircraft Systems ICUAS*, pages 1499–1508. IEEE, 2021-06-15.

[15] Saad Mneimneh. Computernetworks udp and tcp. *Hunter College of CUNY. New York*, 2008.

[16] Moez Krichen. Défis de sécurité pour les communications par drones : Menaces, attaques et contre-mesures possibles. 2022-09.

[17] Yih-Chun Hu, Adrian Perrig, and David B Johnson. Ariadne : A secure on-demand routing protocol for ad hoc networks. In *Proceedings of the 8th annual international conference on Mobile computing and networking*, pages 12–23, 2002.

[18] Kuan Zhang, Xiaohui Liang, Rongxing Lu, and Xuemin Shen. Sybil Attacks and Their Defenses in the Internet of Things. *IEEE Internet of Things Journal*, 2014-10.

[19] Robert Mitchell and Ing-Ray Chen. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys*, 2014-03-01.

[20] Mathias Payer, Awais Rashid, and Jose M. Such, editors. *Engineering Secure Software and Systems : 10th International Symposium, ESSoS 2018, Paris, France, June 26-27, 2018, Proceedings*. Lecture Notes in Computer Science. Springer International Publishing, 2018.

[21] Melal Khireddine. *Analyse des méthodes d'égalisation des techniques CDMA*. Mémoire de Master, présenté à l'Université De Batna, 2008.

[22] Crépin Nsiala-Nzéza. Récepteur adaptatif multi-standards pour les signaux à étalement de spectre en contexte non coopératif. Thése de Doctorat présentée devant l'Université de Bretagne Occidentale, Juillet 2006.

[23] TADJ EDDINE Mohamed Amine Yassine. BENZORGAT Mustapha Nour Eddine. Le data mining pour l'étude des performances des systèmes multiporteuses à accès multiple. Mémoire de MASTER, UNIVERSITÉ DR MOULAY TAHAR – SAIDA,Septembre 2020.

[24] Ahmed Hadji. Systèmes de modulations codées à haute efficacité. Thése de Doctorat, Université Dr Moulay Tahar, Saïda (Algérie), novembre 2021.

[25] Mr. MOHAMED CHERIF Merzouk. Mr. RAMDANE Rafik. Etude du dimensionnement d'un réseau 3g(umts), application pour la ville de tizi-ouzou. Mémoire de MASTER, UNIVERSITÉ DR MOULOUD MAMMERI TIZI-OUZOU, 2008/2009.

[26] BOUDJEMA Ilyas. Etudes des formats de modulations et de démodulations : Dpsk et qam. Mémoire de MASTER, Université Aboubakr Belkaïd – Tlemcen – , juin 2019.

[27] Sunil Bhooshan. *Fundamentals of Analogue and Digital Communication Systems*, volume 785 of *Lecture Notes in Electrical Engineering*. Springer Singapore, 2022.

[28] M. SAAD AMMAR M.TEKFI REZKI. *Etude des techniques à étalement de spectre Application à la CDMA et simulation sous Matlab*. Mémoire de fin d'études, UNIVERSITé MOULOUD MAMMERI, TIZI-OUZOU, 2008/2009.

[29] Zine el Abidine REGAI. *EGALISATION AVEUGLE MULTIUTILISATEURS POUR LES SYSTEMES DS-CDMA DANS LES RESEAUX DES TELEPHONES MOBILES*. Mémoire de magister, Université de Biskra, Mars 2010.

[30] SAIDANI Samir. Contribution à l'evaluation des performances des systèmes de communications mobiles. Mémoire de Master, Université 8 mai 1945 – Guelma, 2012.

[31] Eric Batut. Etude du bloc de réception dans un terminal umts-fdd et développement d'une méthodologie de codesign en vue du fonctionnement en temps réel. Thése, INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE, juin 2002.

[32] Laurent DUBREUIL. Amélioration de l'étalement de spectre par l'utilisation de codes correcteurs d'erreurs. Thése de Doctorat, UNIVERSITé DE LIMOGES école doctorale Science, 11 octobre 2005.

[33] M. FASSI Benattou. Contribution à l'étude des codes zcz (zero correlation zone) :application au système cdma. THESE DE DOCTORAT, Université Djillali Liabès de Sidi-Bel-Abbes, 2014.

[34] Saïd OUGGAD and Yacine BENNOUR. *Automatique CMLD-CFAR basé sur les réseaux de neurones artificiels : Application à l'acquisition dans les systèmes DS/CDMA*. Mémoire de MASTER, UNIVERSITE KASDI MERBAH OUARGLA, 2019/2020.

[35] BOUCHAM Maamar. *Amélioration des performances d'une liaison DS-CDMA avec récepteur Rake*. Mémoire de MASTER, UNIVERSITE SAAD DAHLAB DE BLIDA, 2008/2009.

[36] Melal Khireddine. Analyse des méthodes d'égalisation des techniques cdma. Mémoire de MASTER, Université De Batna, Novembre 2008.

[37] Melle.Kibeche Houda. *Contréle de puissance dans un systéme de communication CDMA dans les véseaux GSM*. Mémoire de MASTER, Université de jijel, juin/2012.

[38] M DIONY Nouhoun Bakary. Synchronisation d'une transmission par étalement de spectre simulation sous simulink. Mémoire de fin d'étude,université de saad dahlab de blida,2006/2007.

[39] BERBRA Kamel. Performances de détection des communications radios mobiles avec des antennes intelligentes.Thése de Doctorat, université de saad dahlab de Blida, 17 octobre 2018.

[40] AINA HERITIANA RASOLOMBOAHANGINJATOVO. Application du dsss À un systÈme d'identification par radiofrÉquence reconfigurable pour l'amÉlioration de la sensibilitÉ du lecteur et de la portÉe. THÈSE de Doctorat, L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES, mai 2018.

[41] Mme. BELAL Samira. Transmission sécurisée des images médicales par ds-cdma. Mémoire de Master, UNIVERSITÉ MOHAMMED SEDDIK BENYAHIA – JIJEL, 2020/2021.

[42] ir.J.Meel. *Spread Spectrum (SS)*. vlaams instituut voor de bevordering van het wetenschappelijk technologisch onderzoek.

[43] Vijay Kumar.Garg. *Wireless Communications and Networking*. The Morgan Kaufmann Series in Networking. Morgan Kaufmann, 1. ed edition, 2007.

[44] Karim Ouertani. Détection multi-utilisateurs pour un réseau de modems acoustiques sous-marins. Thése de Doctorat, L'ECOLE NATIONALE D'INGENIEURS DE TUNIS En habilitation conjointe avec l'Université de Bretagne Sud, decembre 2013.

[45] Amel AISsAOUI. Synchronisation adaptative du code pn dans les systemes de communication ds/ss. Thése de Doctorat, Université MENTOURI Constantine,Juin 2008.

[46] Imane MAHMOUDI.Kaoutar MOSBAH. Amélioration de l'acquisition adaptative des séquences pn dans les systèmes ds-cdma en utilisant la technique d'optimisation des essaims de particules. Mémoire de MASTER, UNIVERSITE KASDI MERBAH OUARGLA, Juin/2018.