République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université SAAD DAHLAB BLIDA -1-

Institut d'aéronautique et des Etudes Spatiales -IAES-

Département de la Navigation Aérienne

Option : **CNS/ATM**

Projet de fin d'études

En vue de l'obtention du diplôme de Master en aéronautique option CNS/ATM

Thème :

Etude et simulation des techniques de Leurrage et Anti-Leurrage du signal GPS par contrôle du C/N_0

Présenté par :

Mr. **AGGAB** Sami

Mlle. **TOUCHI** Damia

Encadré par :

Dr. **DEHOUCHE.** S

Pr. **HAMADOUCHE.** M

Année

2019

Abstract

This work is dedicated to the development of a GPS spoofer, realized by combining Matlab software programming, GNU Radio and emission by HackRF device. In this context, a complete GPS signal simulator was realized. In the second stage, we were interested in spoofing counter measures where *CNR* control was presented and analyzed. Several methods for estimating this parameter have been also presented.

Key-words : GPS system, Spoofing, Anti-Spoofing, *CNR*, ….

Résumé

Ce projet est consacré au développement d'un spoufeur GPS, réalisé en combinant la programmation sous Matlab, GNU Radio puis l'émission par HackRF. Dans ce contexte, un simulateur complet de signal GPS était réalisé. En deuxième étape on s'est intéressé aux techniques d'anti-leurrage où une variante était étudiée, analysée puis simulé, il s'agit du contrôle du *CNR*, où des méthodes d'estimation de ce paramètre ont été présentées.

M**ots clés :** Système GPS, Leurrage, Anti-leurrage, *CNR*, ….

ملخص

يتناول هذا المشروع دراسة حول نظام GPS في الارسال ثم في الاستقبال، بغرض الخداع ومكافحة الخداع. لذلك يستند عملنا على محورين. أولاً، قمنا بمحاكاة إشارة GPS تسمى محاكي GPS لهجوم سرقة الهوية من خلال برنامج GNU Radio وأرضية RF تسمى Hack-RF One للبث على الأجهزة المجهزة. بواسطة جهاز استقبال GPS. في الجزء الثاني ، اقترحنا تقنية لمكافحة الغش من أجل الكشف عن المفسد ، تعتمد على تقدير مدة الموجة الحاملة على الكثافة الطيفية للضوضاء *CNR*.

الكلمات المفتاحية : نظام GPS , محاكاة ساخرة ، مكافحة الخداع ، *CNR* ،

Remerciements

Nous tenons avant tout à remercier ALLAH qui nous a aidés et nous a donnés la patience et le courage d'accomplir ce modeste travail.

Nos vifs remerciements s'adressent à notre directrice de recherche Dr. S. DEHOUCHE et Prof. M. HAMADOUCH, à qui nous exprimons notre gratitude et notre respect pour son accompagnement tout au long de ce travail, pour ses précieux conseils, ses encouragements, son entière disponibilité et sa grande responsabilité.

Nous remercions également tous les enseignants qui nous ont pris en charge tout au long de notre cursus universitaire ainsi que toutes les personnes qui nous ont aidés de près ou de loin à la réalisation de ce travail.

Nous remercions tout spécialement notre cher professeur Mr. BENACHENHOU K. qui nous a aidé et soutenu, sans qui la réalisation de ce projet n'aurait pas vu le jour, et grâce à qui nous avons pu accomplir ce travail.

Dédicace

C'est avec un énorme plaisir que je dédie ce modeste travail à

- *mes chers parents qui m'ont soutenu tout au long de ma vie. Que Dieu les préserve.*
- *mon frère Aymen et mes sœurs Ilhem, Hala et Hibet-Errahmane.*
- *tous mes cousins et cousines et en particulier Imen et Doha*
- *tous mes amis et amies.*
- *aux familles AGGAB, GUETTARI, YOUBI, DALI*
- *mon oncle Ayachi Youbi qui m'a toujours soutenu dans mon parcours universitaire.*
- *mon frère dont on partage tout sauf le sang : BOUDJEBIEUR Abd El Majid.*
- *mes compagnons de la cité -06- : BENYAHLOU Sofiane, SAHI Bachir, BENNOUR Ahmed, ADDALA Salah Eddine, BELKHATIR Zohir, AFTIS Fares, MELIANI Ali…*

L'étudient SAMI AGGAB

Dédicace

C'est avec un énorme plaisir que je dédie ce modeste travail à

- *mon trés cher papa Ali, ma maman Nacera, ainsi que ma soeure Manel*
- *Mes professeur de l'institue d'aéronautique :*

  Mr BENACHENHOU.

  Mme Agoune

  Mr Azazen

  Mr Boudani

  Mme Doudou

  Mme Dehouche

  Mr Ainouche
- *Mes trés cheres amis : Zakaria, Nadia, Noriem, Amel, Ichrak.*

L'étudiente TOUCHI DAMIA

TABLE DES MATIERES

CHAPITRE II: ARCHITECTURE D'UN RECEPTEUR GPS

CHAPITRE III: BROUILLAGE ET LEURRAGE DU GPS

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABREVIATIONS

ADC	Analog to Digital Converter
ADS-B	Automatic Dependent Surveillance Broadcast
AFE	Analog Front End
ARNS	Aeronautical Radio Navigation Service
ATC	Air Traffic Control
AWGN	Additive White Gaussian Noise
BL	Beaulieu's estimation method
BPSK	Binary phase shift key
CAG	Contrôle Automatique du Gain
CDMA	Code Division Multiple Acess
CNR	Carrier to Noise Ratio
DBE	Digital Back End
DLL	Delay Locked Loop
DME	Distance Measuring Equipment
DOA	Direction Of Arrival
DS-CDMA	Direct Sequence CDMA
DSP	Densité Spectrale de Puissance
ECEF	Earth Centred Earth Fixed
EGNOS	European Geostationary Navigation Overlay Service
ENU	East North Up
GIOVE	Galileo In Orbit Validation Element
GLONASS	Globalnaïa Navigatsionnaïa Spoutnikovaïa Sistéma
GNSS	Global Navigation Satellite System
GPS	Global Positionning System
HOW	Handover Word
IFF	Identification Friend or Foe
ILS	Instrument Landing System
IODE	Issue Of Data Ephemeris
IODC	Issue Of Data Clock

JTIDS	Joint Tactical Information Distribution System
LADGNSS	Local Area Differential GNSS
Llh	Latitude Longitude Altitude
LNA	Low Noise Amplifier
MIDS	Multifunctional Information Distribution System
MMR	Multi- Mode Receiver
OACI	Orgatnisation de l'Aviation Civile Internationnalle
PANOVA	Phase-only ANalysis Of VAriance
PDA	Personal Digital Assistant
PIER	Puissance Isotropique Equivalente Rayonnée
PLL	Phase Locked Loop
PPP	Precise Point Positioning
PRN	Pseudo Random Noise
PVT	Position Vitesse Temps
RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio Frequency
ROC	Receiver Operation Characteristic
RSCN	Real Signal Complex Noise
RTK	Real Time Kinematic
SA	Selective Avaitabitity
SDR	Software Defined Radio
SNR	Signal to Noise Ratio
SNV	Signal to Noise Variance
SQM	Signal Quality Monitoring
TACAN	TACtical Air Navigation
TCAS	Traffic Collision Avoidance System
TLM	Telemetry
TOC	Time Of Clock
TOE	Time Of Epoch
TOW	Time Of Week
UTC	Temps Universel Coordonné
VOR	VHF Omni Range
WAAS	Wide Area Augmentation System

LISTE DES SYMBOLES ET NOTATIONS

f_0	Fréquence fondamentale
f_{L1}	Frequence porteuse L1
f_{L2}	Frequence porteuse L2
$S_r(t)$	Signal a la reception
$S_r^k(t)$	Signal associé au satellite k
$n(t)$	Bruit thermique
τ^k	Décalage sur le code du satellite k
f_d^k	Frequence Doppler du satellite k
$r^i_{(\tilde{t},\tilde{f})}(t)$	Replique du signal a la reception
$(\tilde{\tau},\tilde{f})$	Espace de recherche temps/frequence
T_{acq}	Temps d'acquisition
$AQ_i(\tilde{t},\tilde{f})$	Fonction de correlation a l'acquisition
$(\widehat{\tau^i},\widehat{f_d^i})$	Estimation du decalage et du Doppler du satellite i
ρ^i	Pseudo distance du satellite i
c	Célérité de la lumière
δ_d	Distance du discriminateur
δ_{τ^i}	Erreur d'estimation du décalage
d^i	Distance géométrique satellite i / récepteur
δh_r	Biais d'horloge du récepteur
δh_s^i	Biais d'horloge du satellite
ΔI_c^i	Erreur induite des perturbations ionosphériques
ΔT_c^i	Erreur induite des perturbations troposphériques
m_c^i	Erreur de multi-trajets
$\in_c^i$	Bruit de mesure
λ	Longueur d'onde de la porteuse
Φ^i	Déphasage du satellite i
$\widehat{\Phi}^i$	Observation de phase
N^i	Ambiguïté entière
f_p^i	Frequence de la porteuse

ΔI_{Φ}^{i}	Erreur de phase induite par les perturbations ionosphériques
ΔT_{Φ}^{i}	Erreur de phase induite par les perturbations troposphériques
m_{Φ}^{i}	Erreur de phase due au multi-trajets
$\in_{\Phi}^{i}$	Bruit de mesure sur la phase
$\hat{\tau}$	Estimation du décalage sur le code
T_{corr}	Temps de corrélation
(x_i, y_i, z_i)	Coordonnées du satellite i en ECEF
(X, Y, Z)	Coordonnées du récepteur en ECEF
J/S	Rapport de puissance interférence au signal
Q	Facteur d'ajustement
P_i	Puissance du signal du satellite i
G_{ei}	Gain à l'émission du satellite i
G_r	Gain a la réception
L	Les pertes
C_{rc}	Correction de l'amplitude de la cosinus harmonique à la radial de l'orbite
C_{rs}	Correction de l'amplitude de la sinus harmonique à la radial de l'orbite
C_{uc}	Correction de l'amplitude de la cosinus harmonique à l'argument de latitude
C_{us}	Correction de l'amplitude de la sinus harmonique à l'argument de latitude
C_{ic}	Correction de l'amplitude de la cosinus harmonique à l'angle d'inclinaison
C_{is}	Correction de l'amplitude de la sinus harmonique à l'angle d'inclinaison
Δn	Variation moyenne de mouvement
M_0	Anomalie moyenne
e	Excentricité
a	Demi grand axe
i_0	Angle d'inclinaison
i	Variation de l'angle d'inclinaison
Ω	Argument du périgée
Ω_0	Longitude du nœud ascendant
$\dot{\Omega}$	Variation de l'ascension du nœud ascendant

$r[n]$	Signal échantillonné
$r_q[n]$	Signal quantifié
r_{RF}	Signal reçu au niveau de l'antenne du récepteur
$E[I_p(\hat{\tau}, \hat{f}_d)]$	Esperance du signal en voie en phase I
$E[Q_p(\hat{\tau}, \hat{f}_d)]$	Esperance du bruit en voie en quadrature de phase Q
$Var[I_p(\hat{\tau}, \hat{f}_d)]$	Variance du signal en voie en phase I
$Var[Q_p(\hat{\tau}, \hat{f}_d)]$	Variance du signal en voie en quadrature de phase Q
$\widehat{CNR}$	Estimation du CNR
p_e^k	Puissance d'émission à l'antenne du satellite k

Introduction générale

Depuis l'antiquité, l'homme a toujours eu besoin de se positionner et de localiser les objets dans l'environnement. Au début de l'humanité, il pensait à utiliser les pierres, les arbres comme référence pour se repérer et les étoiles pour l'orientation dans la nuit et le soleil dans le jour, puis l'invention de la boussole et le loch à bateau ont été utilisé afin de trouver un chemin.

En XX siècle, l'être humain s'est rapidement vu assisté des capteurs lui permettant d'affiner l'estimation de sa localisation, ce problème de localisation s'est posé de manière plus explicite pour la navigation. D'une manière générale, la localisation d'un mobile consiste à déterminer sa position et sa vitesse.

Les progrès technologiques qui sont introduits dans la société et leurs utilisations se répandent rapidement parmi la population, et de plus en plus des applications sont trouvées pour chaque technologie et domaine. Le système de navigation par satellites *GPS* est un exemple clair de ce phénomène. Depuis que le système de positionnement global *GPS* est devenu opérationnel, ses applications et son utilisation ont considérablement augmenté. De nos jours, presque chaque personne possède un appareil capable de le localiser et le faire guider au moyen du signal *GPS*, ce système utilisé dans de nombreux domaines militaires et civils a pris une place importante dans la vie humaine.

La technologie évolue et se répand et les problèmes de sécurité de tous les systèmes électroniques et de télécommunication augmentent également. Cette préoccupation s'applique à de nombreux secteurs de la société actuelle, dont le GPS fait partie. Comme on peut le constater, la société moderne s'appuie fortement sur ce système, pour un grand nombre d'applications et de services. Cependant, les problèmes liés à la sécurité de tels systèmes sont parfois sous-estimés. C'est le cas de certains services utilisant le signal GPS civil. En fait, la menace des interférences intentionnelles de fréquences radio, telles que des attaques par brouillage ou par leurrage, prend de l'ampleur et des recherches sont en cours pour tenter de trouver des moyens de protéger les utilisateurs civils du *GPS* de ces attaques.

De nos jours, les effets de ces interférences intentionnelles susceptibles de compromettre le bon fonctionnement des récepteurs GPS sont bien connus et la nécessité d'améliorer la sécurité du récepteur a été démontrée, notamment dans le cas des applications dont le dysfonctionnement compromettrait la sécurité des personnes.

Parmi les différentes attaques qui peuvent affecter le GPS, et l'une des plus dangereuses est l'attaque par leurrage. Elle consiste à la transmission de signaux similaires de type *GPS*, alignés sur les signaux des satellites, dans le but de prendre le contrôle de la solution position-vitesse-temps (PVT) calculée par le récepteur. De cette façon, l'attaquant est capable de simuler la position cible sans se faire remarquer et peut causer de graves dommages aux applications reposant sur le signal GPS.

Plusieurs techniques d'Anti-Leurrage ont été proposées dans la littérature, et peuvent être généralement divisées en deux catégories principales, à savoir la détection de Leurrage et la réduction de leurs effets. Les algorithmes de détection visent principalement à détecter la présence d'un dispositif de leurrage, tandis que les techniques d'atténuation visent à neutraliser la menace et à aider le récepteur GPS cible à récupérer sa capacité de positionnement. Des contre-mesures peuvent avoir lieu au niveau de n'importe quel étage opérationnel d'un récepteur GPS, notamment au niveau du traitement du signal, c'est le cas de notre projet, du traitement de données et/ou de la solution de position et du niveau de navigation. D'où vient l'idée de notre travail présenté dans ce mémoire.

On s'intéresse dans ce projet, aux leurrage et Anti-Leurrage du système GPS, notre mémoire est structuré en quatre chapitres comme suit :

- Le premier chapitre est consacré à la description globale des systèmes de positionnement par satellites, en présentant leurs avantages et limitations, ainsi à la présentation d'autres systèmes de navigation ;

- Dans le deuxième chapitre nous présenterons les caractéristiques du signal *GPS* en émission et réception, ainsi nous décrivons l'architecteur simplifiée du récepteur avec ses étages, en donnant les différentes notions nécessaires pour le traitement du signal *GPS* ;

- Nous présentons dans le troisième chapitre les vulnérabilités des signaux *GPS* et les différents types d'attaques de leurrage qui existent dans la littérature, ensuite

nous présentons les outils software et hardware utilisés dans la réalisation de notre projet. Finalement nous décrierons la procédure élaborée pour réaliser une attaque de leurrage via un simulateur du signal GPS civil que nous avons développé ;

- Le dernier chapitre est consacré aux techniques de détection du leurrage. Ainsi, une technique était analysée, elle est basée sur l'estimation du rapport de la puissance porteuse à la densité spectrale de bruit *CNR*.

Nous clôturons notre mémoire par une conclusion générale dans laquelle nous proposons des perspectives pour des travaux futurs.

Chapitre I

Introduction Au Système De Positionnement Par Satellites GPS

- Introduction
- Le principe de positionnement par satellites
- Description du système GPS
- Le signal GPS
- Transmission par spectre étalé
- Poursuite des signaux GPS
- Conclusion

I.1. Introduction :

Le GPS (Global Positionning System) est un système de géo localisation qui assure la fonction de la navigation et de positionnement, en utilisant une constellation de satellites en orbite autour du globe terrestre ainsi que des récepteurs pour les utilisateurs, capables de recevoir, décoder et utiliser les signaux GPS, civils qu'ils soient ou militaires.

La navigation par satellites est le moyen de navigation le plus utilisé et le plus commercialisé au temps actuel, grâce à son efficacité. Dans le domaine de la navigation aérienne, la navigation par satellites permet une autonomie pour les aéronefs. Le GPS est considéré comme un moyen secondaire de navigation aérienne en aéronautique à cause de son manque d'intégrité, de précision et de continuité de service, il n'est pas certifié pour l'atterrissage par I'OACI.

Le GPS fut le premier système conçu pour répondre aux besoins de la navigation et de positionnement, et est actuellement le seul système mondial de positionnement, néanmoins au bout de ces dernières années, il se voit limité. Avec le temps, l'évolution continue de la technologie, la dégradation volontaire du signal, la précision limitée, sont des facteurs poussant à sa modernisation. De plus, l'ère de la monopolisation du monde de la navigation par satellites par le GPS est sur le point de disparaitre, puisque d'autres pays sont en phases de développement de leurs propres systèmes. La Russie dispose déjà de son système GLONASS, l'Inde se propose de développer son système régional IRNSS et la Chine bénéficie des services du système régional BEIDOU et l'Europe a développé le système Galileo. Face à ces facteurs, la modernisation restera l'unique issue pour les américains, pour pouvoir garder leur système dans le monde du positionnement et de la navigation par satellites.

La modernisation portera essentiellement sur de nouveaux signaux plus robustes et fiables. La stratégie de modernisation est constituée de plusieurs éléments, pour les utilisateurs civils la première étape vers la modernisation a eu lieu le 1o Mai 2000 par la désactivation de la source d'erreur intentionnelle nommée < Selective availability >, ceci a optimisé la précision cinq fois pour les utilisateurs civils. La modernisation touchera aussi les signaux du GPS, des signaux civiles supplémentaires sont ajoutés, à savoir; le signal L2C dans la bande de fréquence L2 et un nouveau signal appelé L5. Pour les militaires, un nouveau code militaire (M'code) sera transmis sur les deux fréquences Ll etL2.

Les satellites GPS sont aussi une partie importante dans la stratégie de modernisation. Une nouvelle génération de satellites (block III) a été développée pour répondre aux exigences des utilisateurs militaires et civils jusqu'à 2025. Le dernier élément dans le plan de

la modernisation est de mettre à jour le segment de contrôle de système GPS et ses installations.

La modernisation du GPS offrira alors plusieurs solutions pour les problèmes proposés de la première conception, que ce soit au niveau du segment spatial, les nouveaux signaux proposés ou bien le segment des utilisateurs. Cette modernisation a commencé à porter ses fruits avec le signal L5, en effet, depuis le 28 juin 2010 le premier satellite du block IIF transmet le nouveau signal L5. Ce signal a été conçu pour améliorer la performance du GPS pour les utilisateurs civils, en offrant à la navigation aérienne une solution pour les limites du GPS dans les premiers signaux.

Le signal L5 est un signal conçu pour fournir plus de précision aux utilisateurs civils du GPS. Sa structure se caractérise par plusieurs point intéressants, la cadence de ses codes qui est dix fois plus que celle de l'ancien code C/A. Le signal L5 fait partie de la famille des nouveaux signaux GNSS (Global Navigation Satellite System) , il se compose de deux voix, la première en phase qui contient les données de navigation nommé canal de données, et la deuxième en quadrature de phase appelé le canal pilote dépourvu de données. L'avantage d'avoir cette structure de double canal, se voit essentiellement au niveau de l'étage d'acquisition. En effet, le fait d'avoir les canaux pilote et données laisse le champ de développer des techniques d'acquisition très vaste, des techniques inexistantes sur l'ancienne structure du GPS.

I.2. Le principe du positionnement par satellites :

Pour qu'un système de positionnement par satellites fonctionne correctement, il faut qu'il y'ait une constellation de satellites en orbites autour de la terre, chaque satellite doit diffuser en permanence un signal vers les zones visibles de la terre tout en donnant sa position précise dans l'espace qui sera reçu au niveau des récepteurs des utilisateurs. Le récepteur doit recevoir les signaux provenant des satellites et mesurer la distance qui les sépare pour pouvoir calculer sa position en combinant ces dernières mesures avec les informations de position de chaque satellite qui sont diffusées dans le signal. La figure I.1 illustre ce principe de fonctionnement. [01] [07]

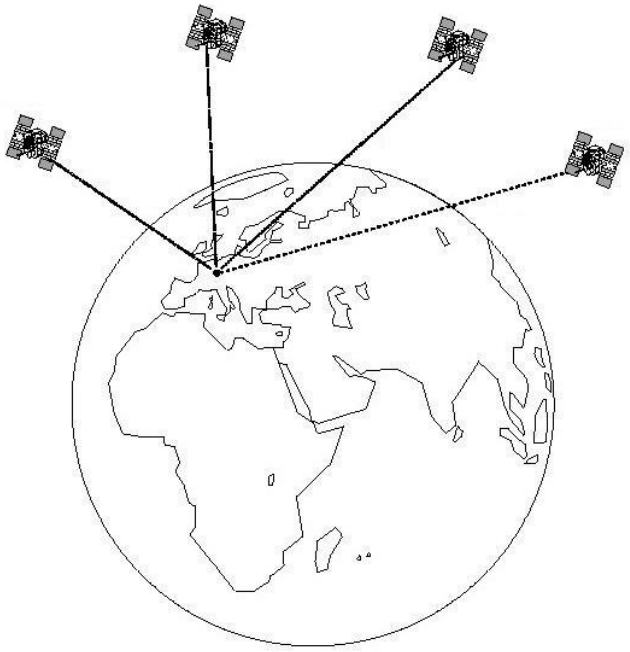

Figure I.1 : Principe de positionnement par satellites.

I.3. Description du système GPS :

I.3.1. Le segment spatial :

Le segment spatial est constitué actuellement d'une constellation de 31 satellites NAVSTAR, répartis sur six plans orbitaux et ayant une inclinaison de 55^{o} sur le plan équatorial ils suivent une orbite quasi circulaire, à une altitude nominale de 20 200 km qu'ils parcourent en 1l heures 56 minutes 02 secondes, soit un demi jour sidéral. Chaque satellite est équipé de panneaux solaires, fournissant l'énergie nécessaire pour alimenter l'équipement électronique installé à bord. L'équipement électronique est composé d'un émetteur-récepteur, d'horloge atomique, d'unité de calcul et de commande destiné à piloter un système de fusées d'appoint permettant de réajuster la position du satellite sur son orbite et d'en contrôler sa stabilité.[16]

Pour assurer la constellation complète de vingt-quatre satellites et sa permanence, plusieurs types de satellites ont été lancés. On distingue plusieurs classes qui correspondent chacune à une étape spécifique dans la constitution du système.

- Satellites du bloc I

Lancés entre 1978 et 1985, les satellites du bloc I ont contribué à la constitution de la phase initiale du système. Leur mission principale était de valider les différents concepts du système GPS. Sur onze du bloc I, à ce jour tous sont en fin de vie.

- Satellites du bloc II

Lancés à partir de 1989, ces satellites contribuent à la phase opérationnelle du système. Des améliorations ont été apportées à ces satellites par rapport à la version précédente, contrairement à ceux du bloc I, ces satellites possèdent un système permettant d'activer ou désactiver de la SA (Selective Avaitabitity) restreignant les possibilités d'utilisation du signal pour le service civil. Il ne reste plus aujourd'hui aucun satellite du Bloc II actif.

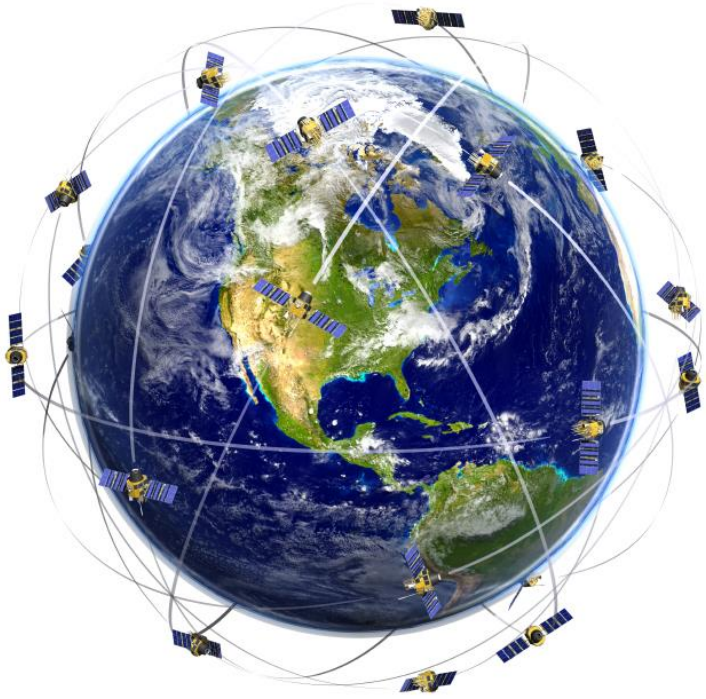

Figure I.2 : La constellation du système GPS.

- Satellites du bloc IIR

Lancés à partir de 1997, dotés d'une meilleure autonomie, ces satellites sont appelés à remplacer petit à petit les satellites du bloc II. Leur durée de vie nominale est augmentée et portée à 10 ans et des horloges atomiques de type Maser à hydrogène remplacent les horloges de césium ou rubidium antérieurement utilisées. Les satellites du bloc IIR possèdent un système de communication inter satellites original. Ainsi, les stations de contrôle et de commandes du segment sol sont capables d'intervenir et d'agir au niveau d'un satellite, même

si celui-ci n'est pas en visibilité, par reliage des ordres de commandes via les autres satellites. Dix-sept satellites du Bloc IIR ont été lancés, le dernier le 20 Décembre2007.

- Satellites du bloc IIF

Les satellites IIF (Foilow-on) construits par Boeing ont été lancés à partir de 2010, ces satellites comportent les modifications rendues nécessaires par la modélisation du système et auront une capacité d'auto-navigation (c'est-à-dire qu'ils seront capables d'être actifs indépendamment du segment sol) pendant une durée de plusieurs mois. Le programme vise à atteindre une constellation de 33 satellites.

- Satellites du bloc III

Les satellites du Bloc III sont encore en phase de développement et ont pour but de faire perdurer le GPS jusqu'en 2030 et plus.

(a) (b)

Figure I.3 : Prototypes des nouveaux satellites (a) Satellites GPS: BtockIIR-M (b) Satellites GPS : BlockIIF

Block I Block II Block IIR

Figure I.4 : Prototypes des anciens satellites GPS

I.3.2. Le Segment sol (de contrôle) :

Le segment sol est composé de tous les équipements installés sur terre constituant d'infrastructure du système et permettant de suivre, contrôler et piloter les satellites en orbite. Cinq stations sont réparties à travers le monde, proche de la ceinture équatoriale. Ce sont Hawai, Colorado Springs, Ascension, Diego Garcia et Kwajalein (archipel des îlesMarshal). La localisation de ces stations est connue avec une très haute précision. Ce segment de contrôle suit tous les satellites, veille à ce qu'ils fonctionnent adéquatement et calcule leurs positions dans l'espace. C'est à ce niveau que les paramètres décrivant l'orbite des satellites et la qualité des horloges embarquées sont estimés, la vérification de l'état des satellites et la détermination d'un repositionnement éventuel sont contrôlés. [07]

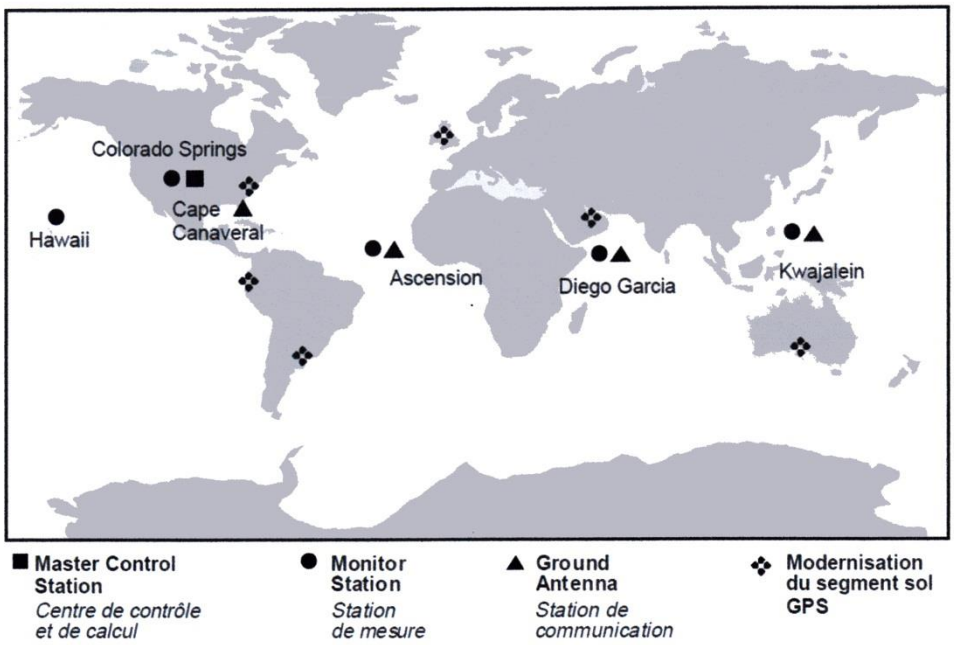

Figure I. 5 : Stations de commande et contrôle du système GPS.

I.3.3. Segment utilisateur :

Le segment utilisateur est composé de l'ensemble des utilisateurs (civils et militaires) du système GPS. Il est constitué de récepteurs qui ont été conçus afin de décoder le signal transmis par les satellites pour déterminer la position, la vitesse et le temps de l'utilisateur.[02]

I.4. Le signal GPS:

Les satellites GPS émettent des signaux générés à partir de leurs émetteurs embarqués [10]. Chaque satellite GPS transmet deux signaux différents dans la bande L utilisant deux bandes de fréquences centrées sur les valeurs suivantes :

$$L_1 = 1575{,}42 \text{ MHz}$$

$$L_2 = 1227{,}60 \text{ MHz}$$

Toutes les composantes du signal émis sont cohérentes et générées à partir d'une horloge embarquée de grande stabilité fouissant une fréquence fondamentale à f_0=10,23MHZ. Les deux fréquences porteuse sont générées tel que :

f_{L1}: 154 f_0

f_{L2} : l20 f_0

Ces porteuses sont modulées en phase (BPSK), ce qui permet aux satellites d'envoyer :

- Un message de navigation : il comporte les éphémérides des satellites et leur variations en fonction du temps, des coefficients de modèle ionosphérique, l'état de santé des satellites, les paramètres des horloges ainsi que le raccordement au temps UTC (Universal Time Coordinat).
- Des codes pseudo-aléatoires dits PRN (Pseudo Random Noise) représentant le numéro de code pseudo-aléatoire généré par le satellite sont considérés. Il existe deux types de codes : Le code C/A (Coarse Acquisition): c'est un code d'une longueur de 1023 chips sur chaque 1 ms ce qui donne une fréquence de 1.023 Mbits/s, en accès libre et accessible à tout utilisateur. Un code C/A différent et assigné à chaque satellite. La porteuse L1 est modulée par le code C/A. Le code P(Y) (Precision Code): réservé aux forces armées américaines, qui permet d'accéder aux meilleures performances du GPS. Émis à une fréquence dix fois plus élevée que le code C/A, il nécessite une semaine pour la transmission de la séquence complète du code.

I.4.1. Code pseudo-aléatoire (PRN) :

Le code PRN (Pseudo Random Noise) ou le code pseudo-aléatoire est un signal semblable au bruit qui satisfait un ou plusieurs des tests standard de la statistique aléatoire. Le code pseudo-aléatoire se compose d'une séquence déterministe d'impulsions qui se répéteront après une période donnée. Pour générer une séquence pseudo-aléatoire on utilise un registre à décalage. Ce registre peut avoir un nombre quelconque d'étages qui dépend de la longueur

maximale de la séquence désirée, la sortie d'un registre à décalage se fait généralement sur le dernier étage. La valeur de chaque chip se présentant à la sortie est parfaitement déterministe mais semble suivre une loi aléatoire. Dans un code à longueur maximale. Si l'on additionne, par exemple, modulo 2 deux séquences chip à chip, on obtient une nouvelle séquence ayant des propriétés de corrélations différentes. C'est ce qu'on appelle un code de GOLD.

I.4.2. Code C/A :

Le GPS utilise les codes de GOLD. Ces codes, basés sur la combinaison de deux séquences binaires générés par deux registres à décalage, présentent des caractéristiques intéressantes. Ils sont relativement faciles à calculer, et possèdent des périodes appropriées. Le point fort des codes de GOLD est leur excellente réponse au critère de corrélation. Le code C/A est généré à partir de deux registres à décalage de dix étages appelés LFSR (LinearFeedback shifi Register). Ces deux registres produisent deux polynômes générateurs :

$G_1=x3+x10$ $G_2= x2 +x3 +x6 +x8+ x9 +x10$

Où le vecteur d'initialisation des registres G_1et G_2 est : 1111111111

La sortie du deuxième registre G_2 provient d'un jeu de deux étages de ce registre, qui additionnés avec la sortie du premier registre G_1 produit l'un des trente-six codes possibles. Le schéma de la figure I.6 résume le processus de génération du code C/A.

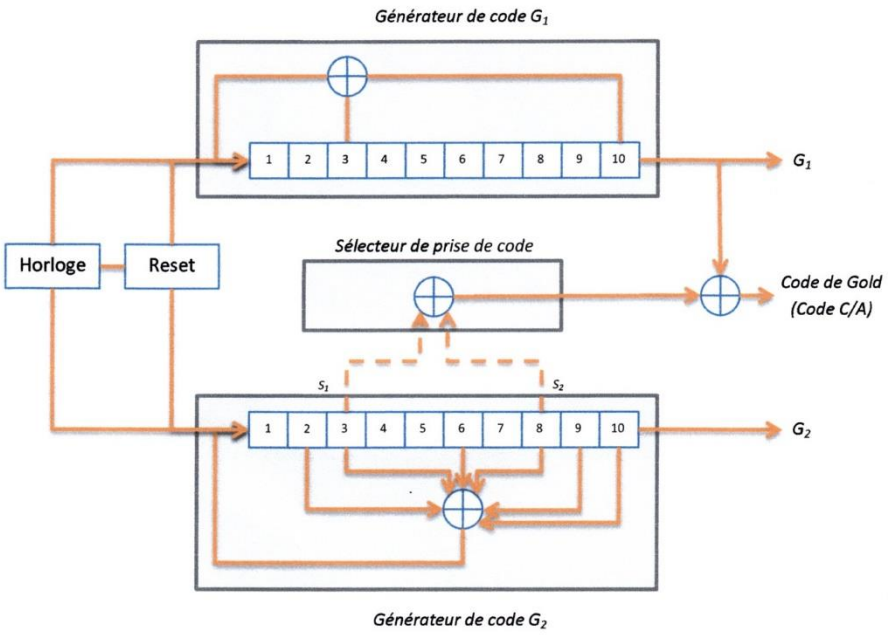

Figure I.6 : Générateur du code C/A

C'est le choix de la combinaison des deux étages de sortie du registre G_2 qui produit l'ensemble de la famille des 37 codes C/A possibles. Un sous-ensemble des 32 premiers codes PRN est affecté et réutilisé quand les vieux satellites sont en fin de vie. Les codes 33 à 37 sont réservés pour les émissions au sol. Le tableau I.1 donne l'assignation des codes C/A pour l'ensemble des satellites GPS. [04]

Tableau I.1 : Assignation des codes C/A pour les satellites GPS.

Numéro du satellite	Numéro du code PRN	Sélecteur de prise de code
1	1	2 ⊕ 6
2	2	3 ⊕ 7
3	3	4 ⊕ 8
4	4	5 ⊕ 9
5	5	1 ⊕ 9
6	6	2 ⊕ 10
7	7	1 ⊕ 8
8	8	2 ⊕ 9
9	9	3 ⊕ 10
10	10	2 ⊕ 3
11	11	3 ⊕ 4
12	12	5 ⊕ 6
13	13	6 ⊕ 7
14	14	7 ⊕ 8
15	15	8 ⊕ 9
16	16	9 ⊕ 10
17	17	1 ⊕ 4
18	18	2 ⊕ 5
19	19	3 ⊕ 6
20	20	4 ⊕ 7
21	21	5 ⊕ 8
22	22	6 ⊕ 9
23	23	1 ⊕ 3
24	24	4 ⊕ 6
25	25	5 ⊕ 7
26	26	6 ⊕ 8
27	27	7 ⊕ 9
28	28	8 ⊕ 10
29	29	1 ⊕ 6
30	30	2 ⊕ 7
31	31	3 ⊕ 8
32	32	4 ⊕ 9
-	33	5 ⊕ 10
-	34	4 ⊕ 10
-	35	1 ⊕ 7
-	36	2 ⊕ 8
-	37	4 ⊕ 10

I.5. Transmission par spectre étalé :

Puisque chaque récepteur reçoit en même temps, sur une même fréquence, plusieurs signaux provenant de plusieurs satellites, il lui faut un moyen pour reconnaître et différencier chaque signal. La technique utilisée pour cela par le GPS est appelée CDMA (Code Division Multiple Access), ou accès multiple par division de code. Cette faculté d'accès multiple est très importante. [16]

Dans le système GPS, plusieurs émissions simultanées correspondant aux satellites de la constellation sont prévues pour cohabiter sans qu'il y ait interférence entre les signaux. Le type de transmission utilisé dans le GPS est une transmission à spectre étalé. Cela signifie que, contrairement aux systèmes dans lesquels la sélection d'une émission par le récepteur est basée sur le filtrage fréquentiel de la porteuse, la sélection s'effectue, ici, en corrélant le signal reçu avec une réplique de cette séquence générée au niveau du récepteur. L'étalement de spectre en séquence directe se fait par la multiplication de l'information à transmettre par le code pseudo-aléatoire, d'où le nom de DS-CDMA c'est-à-dire technique CDMA à séquence directe.

Cette technique d'étalement, rejetant le bruit et facilitant les transmissions numériques dans les cas d'interférences par trajets multiples, est d'autant plus efficace quand la séquence du code pseudo-aléatoire est longue. C'est la raison pour laquelle le code p(y) procuré par rapport au code C/A, une protection naturelle contre les brouilleurs bien supérieure. C'est d'ailleurs, avec l'augmentation de précision liée à sa fréquence 10 fois plus élevée que celle du code C/A, que se trouve le second intérêt du code P(Y).

L'étalement de bande est réalisé, avant transmission, grâce à l'utilisation des codes pseudo-aléatoires qui modulent la séquence d'information. Pour un observateur non averti, la porteuse ainsi étalée par la modulation du code pseudo-aléatoire présente toutes les caractéristiques d'un bruit. A l'inverse, on utilise le même code en réception, l'émetteur et le récepteur étant synchronisés, pour dés-étaler ou restituer le signal dans sa bande étroite d'origine et récupérer les données d'information. On passe ainsi d'un signal à bande étroite vers un signal à large bande.

Dans le CDMA chaque satellite se voit attribuer un code particulier, qu'il utilise pour moduler son signal. Ces codes sont générés de façon prédéterminée et indépendante par les satellites et par chaque récepteur. Les récepteurs, qui connaissent également ces codes,

peuvent les identifier et séparer les différents signaux arrivant sur la même bande de fréquences. Les signaux à spectre étalé présentent les avantages suivants:

- Résistance au brouillage : le spectre du signal portant l'information étant dupliquée sur une large bande, l'interférence d'un signal brouilleur n'affectera qu'une partie des répliques, les autres restants exploitables pour récupérer les données.
- Confidentialité: pour une puissance du signal d'information donné, l'étalement de spectre permet de répartir cette puissance sur les différentes répliques ce qui abaisse le niveau global du spectre. Ainsi, celui-ci peut passer en dessous du niveau du bruit.
- Cryptage : l'étalement de spectre constitue un moyen de cryptage : en effet, le signal étant déjà codé et en dessous du bruit, le seul moyen de le retrouver est de trouver le bon code utilisé à l'émission. Capacité de mesure du retard de propagation: les fonctions d'auto corrélation permettent la synchronisation entre le code local et le code entrant et donc de déterminer le retard et la pseudo-distance. Pour une transmission n'utilisant pas l'étalement de spectre, seule la boucle à verrouillage de phase fonctionne ce qui ne permet pas une telle mesure.
- Partage du canal d'émission: les signaux des différents satellites sont émis simultanément dans une même bande de fréquence. Chaque signal ayant son propre code, il n'y a pas d'interférences avec les autres.

I.6. Poursuite des signaux GPS :

Dans les récepteurs GPS, un processus d'acquisition fait une première recherche pour trouver le code phase et la fréquence du signal reçu pour un satellite spécifié ces deux paramètres changent d'une façon continue, et pour pouvoir continuer à avoir les données de navigation il faut poursuivre ce changement d'une façon continue, pour cela un étage de poursuite a été conçu.

Ces deux problèmes (variation de la fréquence porteuse et changement de phase) doivent être corrigés à la réception, ce qui exige deux modules en plus de celui de l'acquisition, la poursuite de code et celui de la phase lors de la conception des boucles de poursuites.

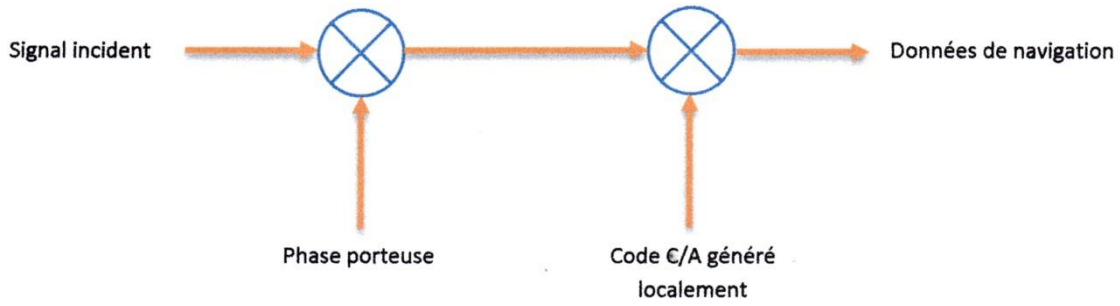

Figure I.7 : Schéma du principe de la démodulation des données

Le signal complet émis par le satellite k est donc de la forme :

$$S^k(t) = \sqrt{2P_c}C^k(t)D^k(t)\cos(2\pi f_{L1}t) + \sqrt{2P_{L1}}P^k(t)D^k(t)\sin(2\pi f_{L1}t) + \sqrt{2P_{L2}}P^k(t)D^k(t)\sin(2\pi f_{L2}t) \quad \text{I.1}$$

I.7. Conclusion :

Dans ce chapitre nous avons expliqué la génération du signal GPS, les propriétés de corrélation de son code, puis l'acquisition et la poursuite de ce dernier pour pouvoir extraire le signal utile qui contient le message de navigation.

Cependant, le code C/A est limité et pas suffisamment précis pour assurer le fonctionnement voulu de la géo localisation. Pour cela le signal L5 a été conçu dans le but de surmonter les faiblesses du code C/A et soutenir les applications (Safety Of Life) tel que la navigation aérienne.

Chapitre II

Architecture D'un Récepteur GPS

- Introduction
- Architecture d'un récepteur GPS
- Les catégories des récepteurs GPS
- Les opérations réalisées par le récepteur GPS
- Conclusion

II.1. Introduction :

C'est à travers des récepteurs que les utilisateurs des systèmes GNSS accèdent aux services de positionnement et de datation et aux applications dérivées. Les caractéristiques de ces récepteurs, seuls équipements visibles de l'utilisateur, sont essentielles pour le type d'utilisation recherchée.

Il existe une très grande variété de récepteurs, adaptés à des besoins spécifiques. Certains privilégient la miniaturisation, pour s'intégrer, par exemple, dans des téléphones mobiles, les engins volant légers ou les animaux surveillés. D'autres mettent en avant telle ou telle performance particulière, comme la robustesse, par exemple pour la navigation maritime ou aérienne ou certaines applications militaires, le coût de production, etc.

Le présent chapitre détaille les principes de fonctionnement et l'architecture des récepteurs et décrit leurs principales caractéristiques ainsi que les grandes catégories d'équipements.

II.2. Architecture d'un récepteur GPS :

Le principe de positionnement par trilatération est très simple a priori, mais la difficulté réside dans la mesure des distances séparant le récepteur des satellites visibles. Pour que cette mesure puisse être réalisée, les signaux GNSS ont été conçus avec des propriétés particulières permettant au récepteur d'estimer leur temps de vol, c'est à dire le temps qu'ils auront mis à parcourir la distance satellite/récepteur. Le récepteur lui-même se décompose en plusieurs « étages » aux missions spécifiques permettant d'aboutir au calcul de la position. [08]

Les récepteurs implémentent quatre fonctions principales : la réception des signaux, où des opérations d'amplification et de filtrage sont effectuées. Le traitement des signaux via des canaux de réception. En passant par les opérations d'acquisition et de poursuite afin de déterminer les retards temporel et fréquentiel liés au signal reçu ; qui seront utilisés pour la démodulation du signal afin de récupérer les données de navigation pour l'évaluation de la position du récepteur. Le schéma de fonctionnement est illustré à la figure II.1.

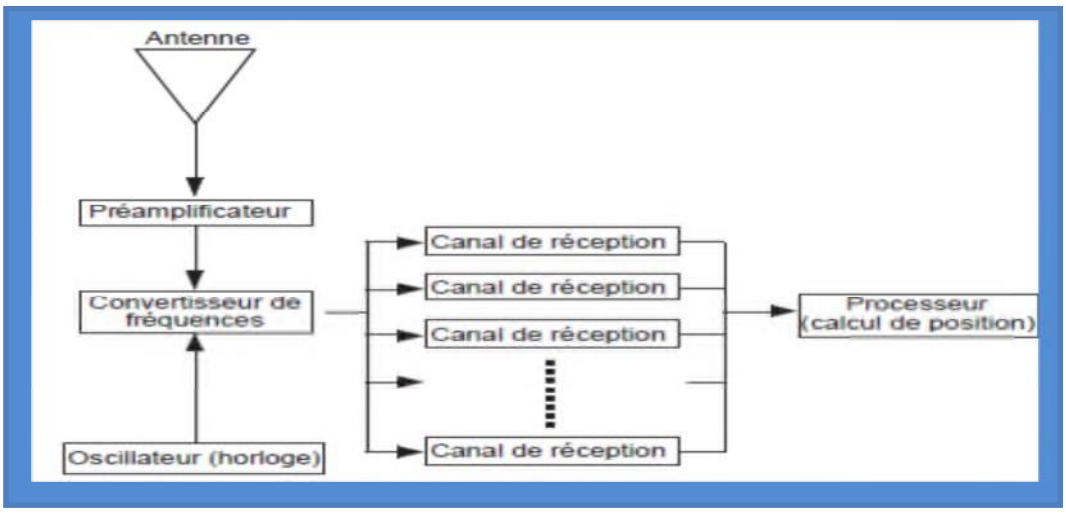

Figure II.1: Schéma de fonctionnement des récepteurs GPS.

II.3. Les catégories des récepteurs GPS :

Les constructeurs de récepteurs ont développé une vaste gamme d'équipements, dont les caractéristiques sont adaptées à de nombreux domaines d'application (récepteurs grand public, récepteurs certifiés pour les transports, récepteurs de qualité géodésique et récepteurs militaires). D'autres types de récepteurs sont en outre dédiés à des usages spécifiques, comme les récepteurs embarqués à bord des satellites, qui échappent à ces catégories. [03]

II.3.1. Les récepteurs grand public :

Les récepteurs grand public ont été développés à l'origine pour utiliser la constellation GPS seule et la fréquence L1 uniquement (code C/A). Ils sont généralement conçus pour apporter une précision horizontale de l'ordre d'une dizaine de mètres, qui est atteinte en utilisant une douzaine de canaux (permettant de recevoir tous les satellites GPS en vue).

La taille de ces récepteurs s'est sensiblement réduite depuis quelques années, du fait de la miniaturisation des puces électroniques, où se trouvent les fonctions de traitement numérique du signal et de calcul de la position, qui atteignent aujourd'hui des tailles inférieures au centimètre.

Au-delà de la précision, les performances recherchées sont la robustesse du service dans des environnements où les satellites sont susceptibles d'être masqués (zones urbaines, indoor) et la rapidité de fourniture du positionnement.

Selon leur usage, on distingue plusieurs types de récepteurs commercialisés, dont les plus courants sont les suivants :

- Récepteurs embarqués
- Récepteurs portables autonomes
- Récepteurs associés à un PDA ou à un Smartphone

La (figure II.2) donne des exemples de récepteurs GPS grand public, avec, de gauche à droite, un récepteur destiné à être embarqué dans une voiture, un récepteur portable autonome et un récepteur prêt à être intégré, par exemple dans un téléphone mobile, dont les dimensions sont inférieures à 3 cm.

Figure II.2 : Exemples de récepteur GPS grand public.

II.3.2. Les récepteurs certifiés pour les transports :

On parle généralement de récepteur « embarqué » dans le cas des applications de transport. Ces récepteurs sont soumis à de fortes contraintes de sûreté de fonctionnement et ne sont proposés qu'après certification par une autorité de contrôle.

Chaque domaine de transport est ainsi contrôlé par une autorité de certification, qui assure que les équipements et services de navigation sont conformes aux normes de sécurité en vigueur. Par exemple, dans le domaine du transport aérien, ce rôle est rempli par les autorités nationales de l'aviation civile.

Les récepteurs ne sont certifiés conformes que pour une utilisation donnée. Par exemple, certains récepteurs peuvent être certifiés pour la navigation aérienne en zone océanique, mais pas pour des phases d'approche, d'atterrissage ou de déplacements au sol.

La (figure II.3) illustre un récepteur Topstar 2020 intégré dans un MMR (Multi- Mode Receiver) utilisé sur Airbus et Boeing.

Figure II.3 : Récepteur Topstar 2020

Au-delà du récepteur lui-même, il s'agit de certifier un service de positionnement utilisant non seulement un récepteur, mais l'ensemble du système de navigation par satellite permettant au récepteur de se positionner. C'est la raison pour laquelle des services dits d'intégrité doivent garantir la précision du positionnement. Par exemple, les systèmes EGNOS (European Geostationary Navigation Overlay Service) ou WAAS (Wide Area Augmentation System) contrôlent en permanence les satellites GPS et avertissent en temps réel l'ensemble des récepteurs de type EGNOS ou WAAS en cas de défaillance ou de dégradation du système GPS. C'est également le cas du service SoL (Safety of Life) de Galileo.

Les différents types de récepteurs certifiés pour les applications de transport sont les suivants :

- **Récepteurs avec intégrité autonome (RAIM) :**

Ces récepteurs sont utilisés pour des phases de transport ne nécessitant pas une précision très importante, comme la navigation en phase océanique, pour laquelle une précision de 100m est largement suffisante, et dont les conditions de visibilité des satellites sont très bonnes. Une technique telle que le RAIM (Receiver Autonomous Integrity Monitoring) permet aux récepteurs de détecter de façon autonome l'apparition d'un dysfonctionnement ou d'une forte dégradation de performance d'un satellite défectueux.

Ces récepteurs peuvent être plus ou moins complexes et performants. Les plus simples sont conçus pour recevoir une seule fréquence en provenance des satellites GPS (signalL1 C/A) ou Galileo (signal E5a ou L1) et sont équipés d'une dizaine de canaux de réception pour acquérir l'ensemble des satellites GPS ou Galileo en visibilité. Les plus complexes peuvent être conçus pour recevoir deux fréquences (récepteurs *bi fréquence*) en provenance de chaque satellite des deux constellations (récepteurs *combinés* GPS/Galileo).

Dans la mesure où l'utilisation combinée des constellations indépendantes GPS et Galileo renforce considérablement la fiabilité du positionnement, les récepteurs combinés

GPS/Galileo utilisant le RAIM pourront être utilisés dans des phases de navigation plus exigeantes.

Le RAIM est une technique de calcul implémentée dans le calculateur du récepteur afin de détecter l'apparition d'une dégradation de la précision de la mesure de distance en provenance d'un satellite parmi tous les satellites visibles. Il s'appuie sur la disponibilité d'un excédent de mesures en provenance des satellites du fait que les constellations GPS ou Galileo offrent de façon quasi permanente un nombre de satellites en visibilité supérieur à quatre. Le récepteur peut dès lors établir plusieurs solutions de positionnement, avec plusieurs combinaisons de satellites comptant au moins quatre satellites. En comparant les résultats fournis, il peut identifier la présence de mesures de distance défectueuses en provenance d'un satellite. Ce principe est illustré à la (figure II.4) :

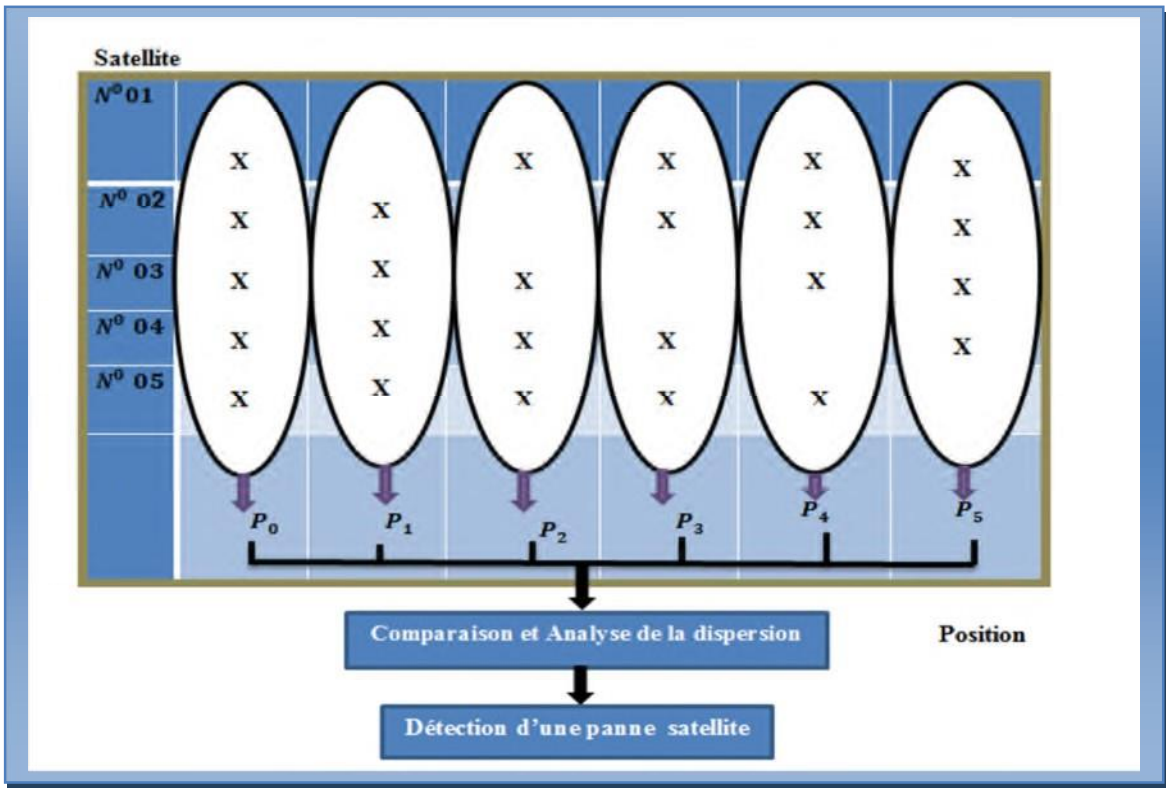

Figure II.4 : Principe de fonctionnement du RAIM.

- **Récepteurs utilisant une augmentation régionale ou locale :**

Ces récepteurs sont utilisés pour des phases de vol pour lesquelles la précision et l'intégrité exigées sont très importantes. C'est le cas des phases d'approche et d'atterrissage dans la navigation aérienne. Ces récepteurs utilisent, en plus des signaux GPS ou Galileo, une source indépendante d'information garantissant les performances du service.

Ces informations sont élaborées et diffusées sur une base régionale, à l'échelle d'un continent, dans le cas des systèmes d'augmentation régionaux comme EGNOS ou WAAS, ou locale, comme un aéroport, dans le cas des systèmes d'augmentation locaux LADGNSS (Local Area Differential GNSS).

- **Récepteurs Galileo Sol :**

Le système Galileo est conçu pour fournir un service, appelé SoL (Safety of Life), dont les performances sont contrôlées en temps réel et garanties par des moyens de mesurent dépendants. Les récepteurs associés sont bi-fréquence (les signaux L1 et E5b) et sont typiquement équipés de 12 canaux, permettant de recevoir tous les satellites Galileo en visibilité. Ils fournissent une alerte en moins de 6 s en cas de dégradation inacceptable des performances de positionnement. Le système GPS prévoit également, dans une version modernisée en cours de définition, de mettre en place un tel service, utilisant les fréquences L1 et L5.

II.3.3. Les récepteurs de qualité géodésique :

Certaines applications nécessitent une précision de positionnement très importante, typiquement de l'ordre du centimètre. C'est le cas en particulier des applications géodésiques, qui visent à établir des cartes terrestres d'une grande précision ou à étudier des mouvements lents et faibles, comme les dérives des continents ou les mouvements le long de failles à haut risque d'activités sismiques. C'est le cas également des applications associées aux transferts de temps afin d'obtenir des synchronisations très précises entre des lieux éloignés.

Ce type d'application s'appuie sur des récepteurs essentiellement statiques, qui mettent en œuvre un ensemble de techniques permettant de réduire le plus possible les erreurs résiduelles. On trouve des récepteurs de ce type dans les systèmes GPS et Galileo eux-mêmes. En effet, comme nous l'avons vu, les systèmes GPS ou Galileo doivent déterminer à quelques centimètres près la position des satellites, ce qui exige le déploiement de récepteurs de qualité « géodésique » sur l'ensemble du globe. Ces récepteurs permettent de mettre en œuvre des

techniques élaborées de mesures de distance et de positionnement, notamment les mesures de phase et les techniques différentielles.

La (figure II.5) donne un schéma de récepteur géodésique qui sera déployé dans le système sol de Galileo. Il a la particularité d'être équipé d'une horloge atomique ultrastable afin d'améliorer la précision de calcul des positions et de la synchronisation des satellites Galileo.

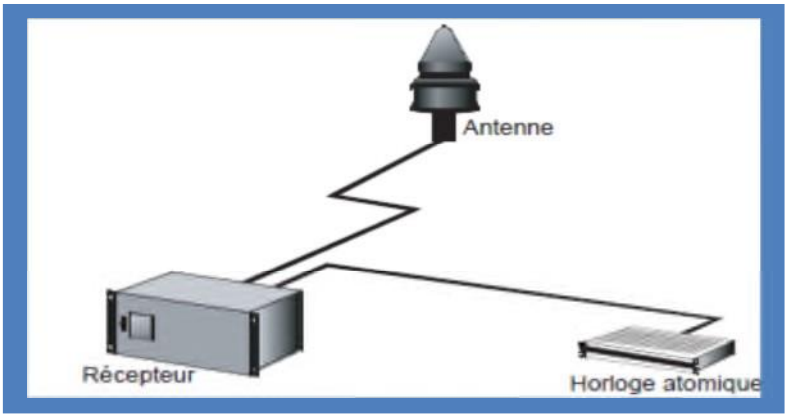

Figure II.5 : Schéma de récepteur géodésique du segment sol de Galileo

II.3.3.1. Mesures de phase :

Les mesures de distance sont réalisées à partir de la mesure du temps de propagation des codes GPS ou Galileo entre le satellite et le récepteur. Pour cela, le récepteur effectue une opération de corrélation consistant à faire coïncider dans le temps le code reçu depuis le satellite et le code généré au niveau du récepteur.

Le signal GPS ou Galileo permet également de mesurer un écart entre les ondulations de la porteuse du signal reçu (la phase du signal reçu) et les ondulations de la porteuse du signal générée au niveau du récepteur. Le grand avantage de cette mesure d'écart de phase est sa précision, qui est de l'ordre de quelques millimètres, à comparer à la précision de corrélation du code, qui est de l'ordre de quelques dizaines de centimètres. Cette mesure de phase est toutefois ambiguë, puisqu'elle ne permet pas de connaître le nombre entier d'ondulations entre le satellite et le récepteur, qui est nécessaire pour déterminer la distance entre le satellite et le récepteur.

Il est possible de lever cette ambiguïté de la mesure de phase grâce à l'accumulation de mesures de code et de phase. Cela permet à un récepteur doté de cette technique d'obtenir des précisions de mesures de distance (hors erreurs de propagation atmosphérique et de positions des satellites) largement inférieures au centimètre.

La (figure II.6) illustre l'amélioration de la précision des mesures de distance apportée par les mesures de phase.

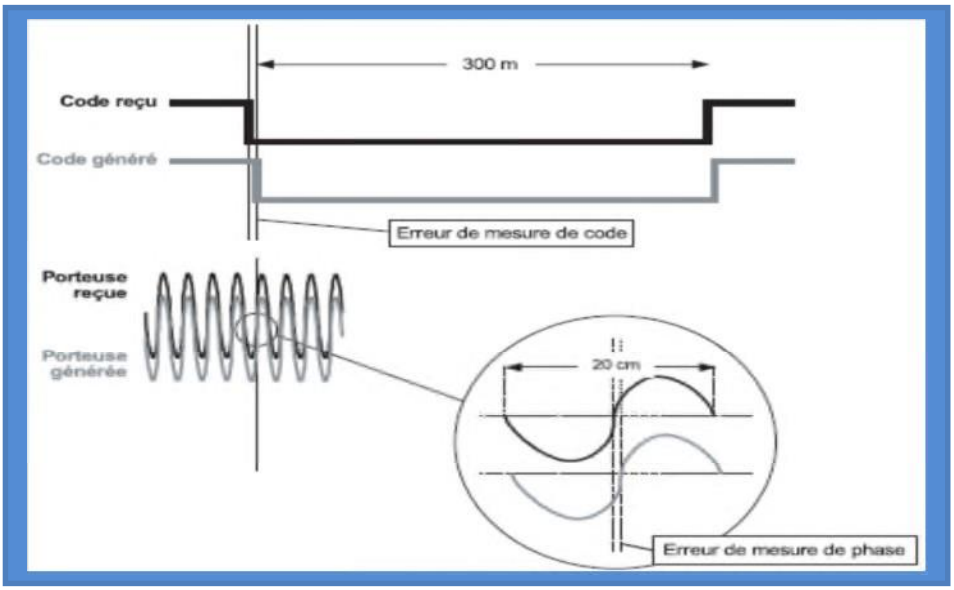

Figure II.6: La mesure de phase.

II.3.3.2. Techniques différentielles :

Ces techniques permettent d'éliminer une grande part des sources d'erreur de mesure grâce à l'utilisation de plusieurs récepteurs et à la combinaison de leurs mesures. Il est de la sorte possible de positionner les récepteurs les uns par rapport aux autres avec une précision centimétrique, voire millimétrique. Ces techniques sont utilisées en géodésie afin d'établir des positions de points de référence avec une très grande précision. Il est possible, par exemple, de déterminer les mouvements tectoniques le long des failles pour mieux anticiper des séismes potentiels ou bien de surveiller les déformations de grandes structures, comme les ponts ou barrages.

La technique différentielle dite des « simples différences » consiste à combiner les mesures de deux récepteurs par rapport à un même satellite, comme l'illustre la (figure II.7). La différence de ces deux mesures de distance permet d'éliminer les sources d'erreurs en provenance du satellite. L'erreur due à l'écart de synchronisation du satellite par rapport au temps système est annulée puisqu'elle s'applique de la même façon sur les deux mesures. L'erreur de positionnement du satellite est également annulée dans le cas où les deux récepteurs sont proches (l'effet de l'erreur dans la direction satellite-récepteur est le même) ou à tout le moins fortement diminuée dans le cas où les récepteurs sont éloignés. Les erreurs de

propagation atmosphérique sont également compensées dans le cas où les deux récepteurs sont proches et soumis aux mêmes erreurs de propagation. Cependant, les erreurs liées au récepteur lui-même, et en particulier à l'instabilité de son horloge, ne sont pas annulées.

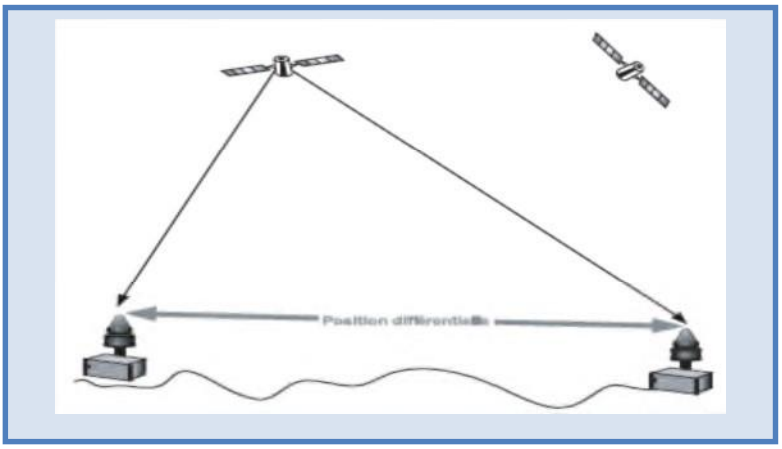

Figure II.7 : Technique différentielle simple différence.

La technique dite des « doubles différences » permet de s'affranchir des erreurs liées aux horloges des récepteurs. Avec cette technique, ce sont les mesures entre deux récepteurs et deux satellites qui sont soustraites les unes des autres, comme l'illustre la (figure II.8), supprimant les erreurs provenant des satellites et des horloges récepteur.

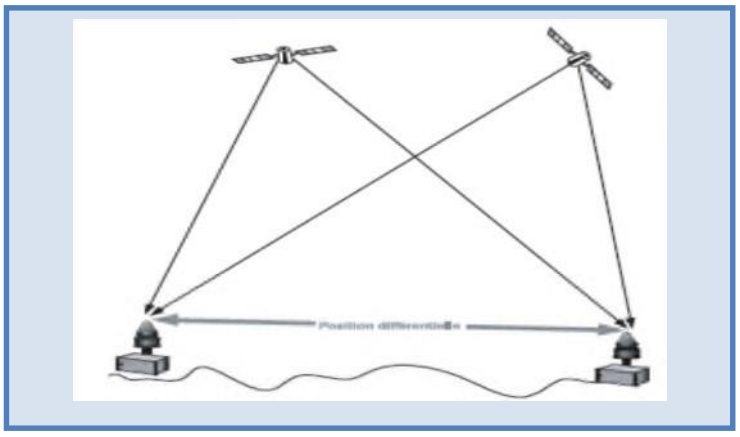

Figure II.8 : Technique différentielle dite des doubles différences.

II.3.4. Les récepteurs militaires :

À l'origine, le système GPS a été conçu pour répondre aux besoins des armées américaines de disposer d'un positionnement de l'ensemble des équipements, troupes ou armes déployées sur des terrains d'opération. Ce besoin concerne aussi bien les armées de terre, la marine ou l'aviation. Il existe une grande variété de récepteurs GPS développés pour de tels besoins et contraintes spécifiques des applications militaires. La (figure II.9) illustre un exemple d'un récepteur GPS militaire.

Figure II.9 : Un récepteur GPS militaire

Ces récepteurs doivent opérer dans des environnements extrêmement hostiles, qui induisent des caractéristiques spécifiques, notamment les suivantes :

- Ces équipements faisant partie du système d'arme, leur accès doit être contrôlé.
- Afin de faire face à la « guerre électronique » sur un théâtre d'opération, ces récepteurs doivent être extrêmement résistants au brouillage. Les codes des signaux dédiés à ces applications ont été spécialement conçus pour apporter une résistance accrue au brouillage et aux mauvaises conditions de réception.
- Afin d'assurer une continuité précise du positionnement en cas de masquage ou de brouillage, les récepteurs peuvent être « aidés », c'est-à-dire couplés à d'autres équipements de navigation leur permettant de réacquérir très rapidement les signaux de satellites perdus. Dans l'aviation, le couplage des récepteurs GPS avec des centrales à inertie, fournissant une position continue mais dont la précision se dégrade avec le temps, permet d'améliorer sensiblement les performances de robustesse et de précision de chacun de ces systèmes lorsqu'ils sont utilisés de façon isolée.

II.4. Opérations réalisées par un récepteur GPS :

Entre la réception du signal et le calcul de la position de l'utilisateur, le récepteur doit effectuer plusieurs étapes pour extraire les informations nécessaires à l'obtention d'une solution pour l'utilisateur. [15]

Le schéma bloc classique d'un récepteur est donné à la (figure II.10). Le bloc "Réception" se réfère au bloc de traitement classique du signal à la réception (i.e., numérisation du signal, séparation des voies I et Q, etc.). S'en suit alors deux étapes qui ont pour but de synchroniser le récepteur avec les signaux de navigation : l'acquisition (qui est réalisée en parallèle sur chacun des canaux de réception) et la poursuite (qui peut être ou non réalisée en parallèle selon le choix de l'architecture de poursuite). Ces deux étapes du processus de navigation sont détaillées dans les sections 4.1 et 4.2.

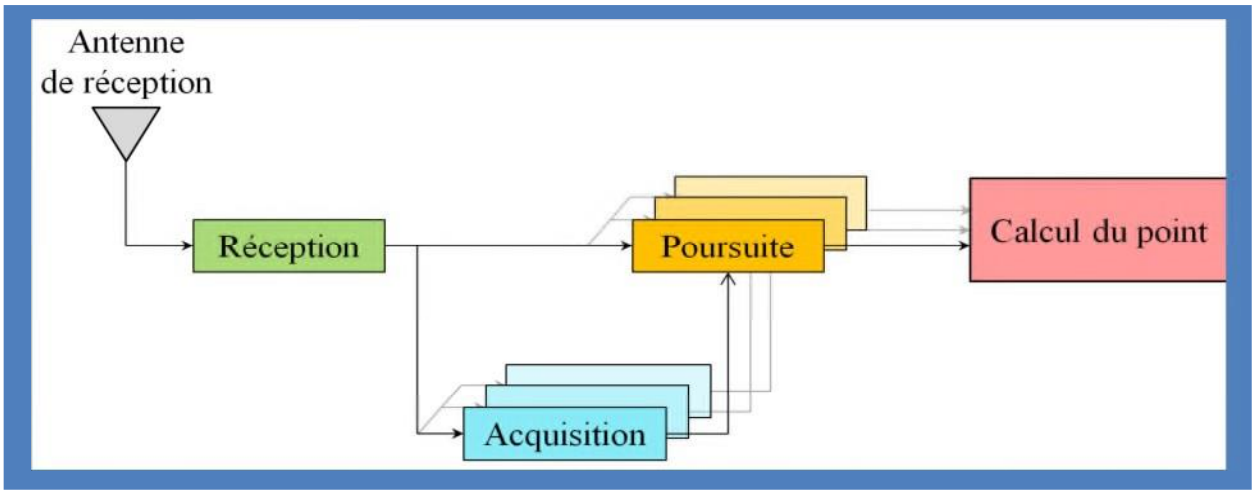

Figure II.10 : Schéma bloc des opérations réalisées par le récepteur.

II.4.1. Acquisition du signal GPS :

Afin de lancer le processus de poursuite du signal de navigation, le récepteur effectue une étape d'acquisition. Cette opération primordiale a pour but de détecter la présence du signal d'un satellite dans l'ensemble des signaux reçus par l'antenne du récepteur. L'acquisition permet également de déterminer le décalage du code et l'écart de fréquence provoqués par la propagation du signal et l'effet Doppler [05]. Ces informations serviront par la suite d'initialisation pour les boucles de poursuite. De manière générale, l'acquisition est une recherche temps-fréquence qui consiste à calculer, sur un ensemble de délais temps/fréquence, les différentes corrélations entre le signal reçu et une réplique locale affectée par un délai et un Doppler fixe, les buts de cette opération sont :

- Détecter la présence d'un satellite dans l'ensemble des signaux captés par l'antenne du récepteur ;
- Déterminer, pour un satellite dont la présence a été détectée, le retard sur le code et la fréquence Doppler à la réception du signal associé afin d'initialiser les boucles de poursuite.

Plus précisément, le signal à la réception est donné par :

$$S_r(t) = \sum_{k=0}^{N_{sat}} S_r^k(t) + n(t) \qquad \text{(II.1)}$$

Avec $n(t)$ le bruit thermique et $S_r^k(t)$ le signal associé au satellite k qui peut s'écrire simplement sous la forme :

$$S_r^t(t) = \sqrt{p_e^k}\, C_k(t - \tau^k) e^{i2t\pi f_d^k} \qquad \text{(II.2)}$$

Avec respectivement τ^k et f_d^k le décalage sur le code et la fréquence Doppler du signal à la réception associé au satellite k qui sont considérés constants sur le temps de corrélation. Pour réaliser l'étape d'acquisition pour le satellite i, le récepteur va créer une réplique

$$r^i_{(\tilde{t},\tilde{f})}(t) = C_i(t - \tilde{\tau}) e^{i2t\pi\tilde{f}} \qquad \text{(II.3)}$$

Avec $(\tilde{\tau}, \tilde{f}) \in E = [\tau min, \tau max] * [fmin, fmax]$ l'espace de recherche temps/fréquence.

Le récepteur va alors calculer l'ensemble des points de corrélation suivants :

$$AQ_i(\tilde{t}, \tilde{f}) = \frac{1}{T_{acq}} \int_0^{T_{acq}} S_r(t)\, \overline{r^i_{(\tilde{t},\tilde{f})}(t)} dt = \Gamma^{r^i}_{S_r}(\tilde{t}, \tilde{f}) \qquad \text{(II.4)}$$

Avec T_{acq} le temps d'acquisition. Or, on sait d'après les propriétés de l'étape de corrélation, que les valeurs $AQ_i(\tilde{\tau}, \tilde{f})$ sont quasi nulles si le signal associé au satellite i ne fait pas partie des signaux reçus. Dans le cas contraire, la recherche temps -fréquence est maximale lorsque la réplique est synchronisée en temps et en fréquence avec le signal reçu, lorsque $\tilde{\tau} = \tau^i$ et $\tilde{f} = f_d^i$ pour pouvoir alors détecter la présence d'un satellite dans l'ensemble des signaux reçus, des techniques de détection sont mises en place après les recherche temps/fréquence pour

déterminer si le maximum obtenu sur une recherche est suffisamment important pour confirmer la présence du satellite en question. Si la présence du satellite *i* est confirmée, l'estimation de τ^i et de f_d^i peut se faire par la recherche du maximum suivante :

$$\left(\widehat{\tau^i}, \widehat{f_d^i}\right) = max_{(\tilde{t},\tilde{f})\in E}\left|AQ_i\left(\tilde{t},\tilde{f}\right)\right| \qquad \text{(II.5)}$$

La précision de ces estimations est logiquement liée à la finesse de la grille de recherche.

II.4.2. Poursuite du signal GPS :

Après l'étape d'acquisition détaillée dans la section précédente qui a pour but de détecter la présence d'un satellite et d'estimer le retard et la fréquence Doppler initiaux du signal à la réception, le récepteur bascule en mode poursuite. [05]

L'étape de poursuite permet de suivre l'évolution du retard sur le code, de la fréquence et de la phase porteuse engendrée par les mouvements relatifs entre le satellite et l'utilisateur et ainsi de mettre à jour le calcul du point. Cette étape est réalisée grâce à des structures qui vont suivre les variations des paramètres nécessaires au calcul de la position grâce à la corrélation du signal reçu par des répliques locales générées par le récepteur. Le schéma bloc de l'étape de poursuite est donné à la (figure II.11).

Différentes mesures peuvent être réalisées par le récepteur lors de la poursuite pour estimer les différentes distances utilisateur/satellite. Les mesures du retard sur le code, de la phasage porteuse ainsi que le suivi de la fréquence Doppler du signal de navigation, elles seront brièvement détaillées dans la section suivante.

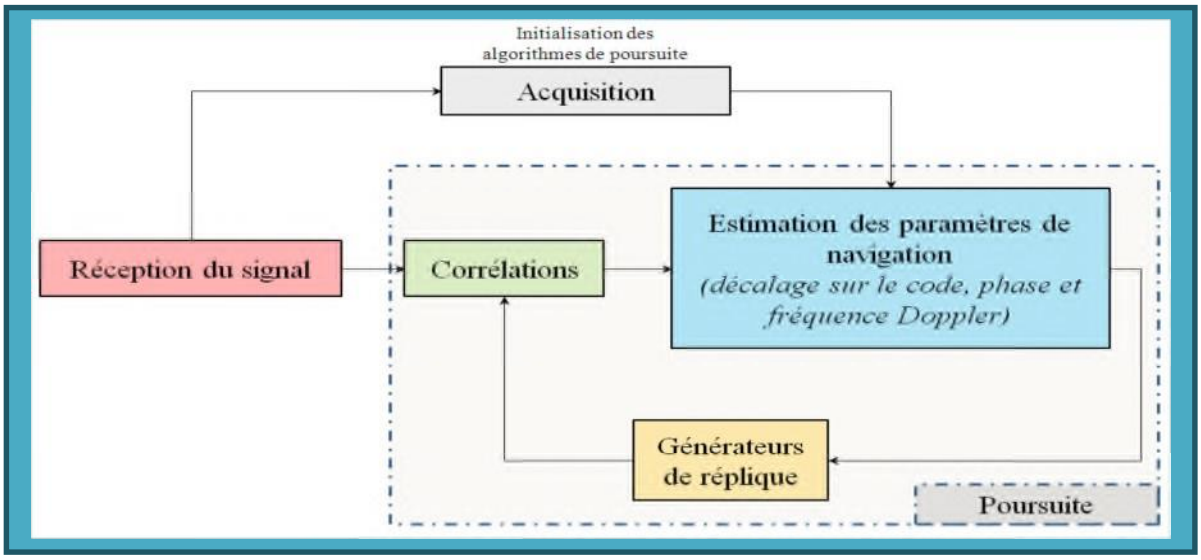

Figure II.11 : Schéma bloc de l'étape de poursuite.

II.4.2.1.Poursuite et observation du retard sur le code :

Pour pouvoir calculer sa position, le récepteur doit estimer la distance qui le sépare des satellites de navigation. L'estimation de distance associée à un satellite peut être réalisée à partir du retard induit par le temps de propagation sur le code du signal de navigation. En effet, si τ^i est l'estimation du retard sur le code associé au satellite i, l'estimation de distance ρ^i, aussi appelée "pseudo-distance", associée au même satellite est alors déduite par :

$$\rho^i = c\tau^i \qquad \text{(II.6)}$$

Le retard sur le code est généralement en perpétuelle évolution du fait des mouvements relatifs entre le satellite et l'utilisateur au cours du temps. Pour pouvoir estimer la distance qui le sépare du satellite, le récepteur doit donc continuellement mettre à jour l'estimation du retard sur le code que l'étape d'acquisition lui a fourni initialement. Cette mesure de temps est effectuée au sein d'une architecture de poursuite qui met à jour le décalage temporel qu'il existe entre le code pseudo-aléatoire du signal reçu, et le même code généré en local au niveau du récepteur afin de les synchroniser (la génération du code local étant synchronisée avec la génération du code au niveau du satellite). [15] [08]

La (figure II.12) illustre schématiquement la détermination du temps de propagation par estimation du décalage sur le code.

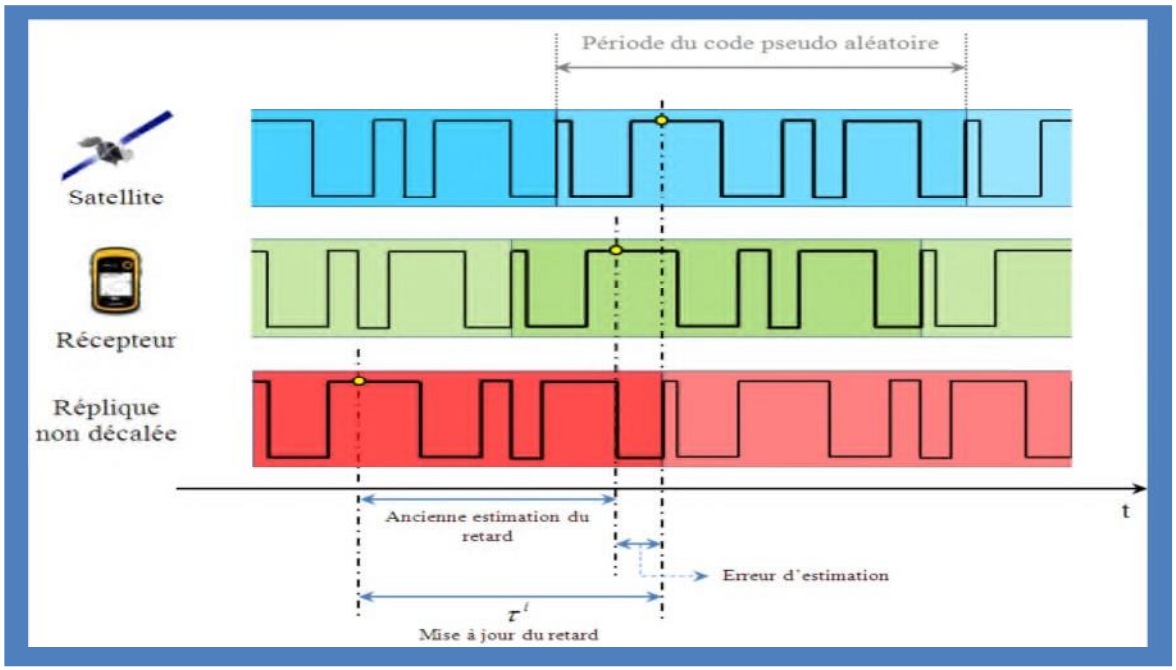

Figure II.12 : Principe de l'estimation du décalage sur le code pseudo-aléatoire.

Un exemple de structure de poursuite du retard sur le code est donné à la (figure II.13). Cette architecture correspond à celle des boucles à verrouillage aussi appelées DLL *(Delay Locked Loop)* lorsqu'elles poursuivent le retard sur le code. La boucle fonctionne en cinq étapes qui visent à comparer le signal reçu avec la réplique locale grâce à une étape de corrélation, à estimer l'erreur d'estimation du retard grâce à un discriminateur qui va extraire cette erreur du produit de corrélation, à filtrer cette erreur et mettre à jour l'estimation du retard, et à générer une nouvelle réplique pour la prochaine étape de corrélation.

Pour pouvoir mesurer l'erreur d'estimation du retard, le récepteur calcule trois points de corrélation réalisés avec trois répliques locales différentes : c'est le principe du calcul *Early/Late*.

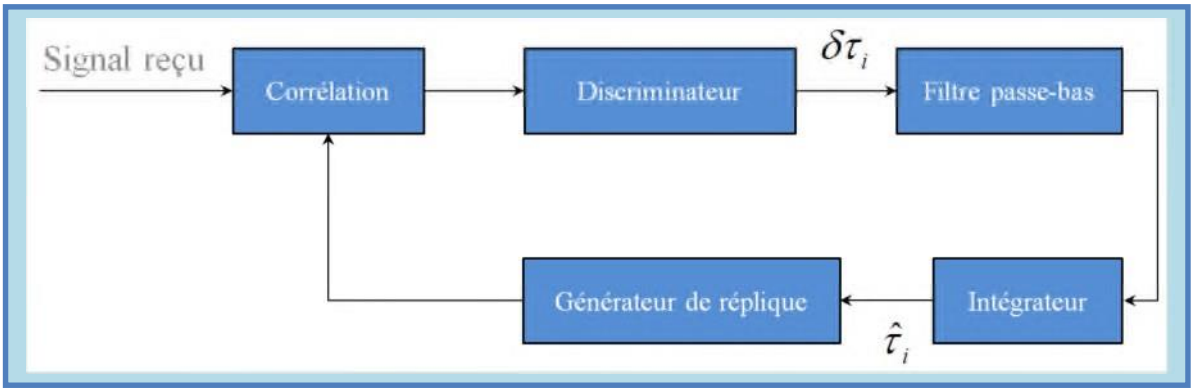

Figure II.13 : Exemple de structure de poursuite du retard sur le code

Plus précisément, si le signal associé au satellite i est reçu avec un retard τ^i et que le récepteur à une connaissance a priori de ce retard $\tilde{\tau}^i$ (i.e., le retard précédemment estimé par la boucle), trois répliques locales sont alors créées :

- une réplique décalée du retard $\tilde{\tau}^i$ (point de corrélation *Prompt*),
- une réplique décalée du retard $\tilde{\tau}^i + \frac{\delta_d}{2}$ (point de corrélation *Late*),
- une réplique décalée du retard $\tilde{\tau}^i - \frac{\delta_d}{2}$ (point de corrélation *Early*), avec δ_d la distance du discriminateur choisie telle que $0 < \delta_d < T_c$.

La (figure II.14) illustre les différents points de corrélation associés aux trois répliques ainsi créées. Il existe différents discriminateurs permettant de mesurer l'erreur d'estimation du décalage sur le code via les différents points de corrélation calculés. Par exemple, il est possible d'estimer l'erreur par la combinaison suivante :

$$\frac{|E|^2 - |L|^2}{|E|^2 + |L|^2} = \frac{4}{2T_c - \delta_d} \qquad \text{(II.7)}$$

Avec $\delta_{\tau^i} = \tau^i - \hat{\tau}^i$ l'erreur d'estimation du décalage temporel.

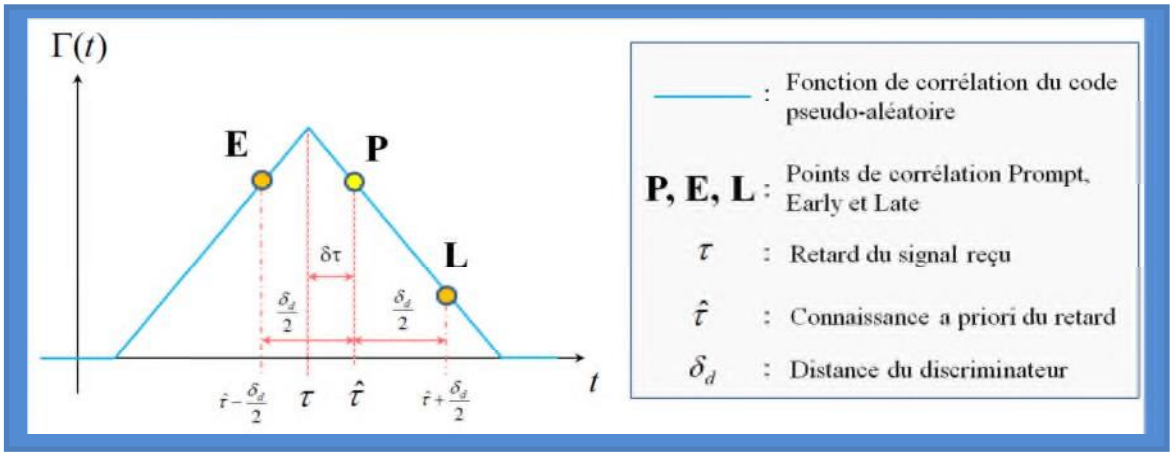

Figure II.14 : Points de corrélation Early, Late et Prompt.

L'estimation de la pseudo-distance donnée par la boucle de poursuite, aussi appelée observation de pseudo-distance, peut être décomposée en plusieurs composantes liées à la distance satellite/récepteur et aux diverses perturbations rencontrées lors de la propagation du signal. L'observation de pseudo-distance peut se modéliser de la sorte:

$$\rho^i = d^i + c\left(\delta h_r - \delta h_s^i\right) + \Delta I_c^i + \Delta T_c^i + m_c^i + \in_c^i \qquad \text{(II.8)}$$

Avec

– d^ila distance géométrique satellite/récepteur,

– δh_r le biais d'horloge du récepteur,

– δh_s^i le biais d'horloge du satellite *i*,

– ΔI_c^i l'erreur induite par les perturbations ionosphériques sur le code,

– ΔT_c^i l'erreur induite par les perturbations troposphériques sur le code,

– m_c^i l'erreur due à la présence de multitrajets sur le code,

– $\in_c^i$ le bruit de mesure sur le code.

L'équation (II.8) montre que l'observation de pseudo-distance contient, en plus de l'information de distance *di*, des termes de perturbations qui, s'ils ne sont pas estimés par les

algorithmes de calcul du point ou divers modèles mathématiques, entrainent des erreurs de positionnement non négligeables.

II.4.2.2. Poursuite et observation de la phase porteuse :

En plus de pouvoir utiliser les mesures de pseudo-distance, il est possible pour le récepteur de calculer sa position en utilisant également la phase de l'onde porteuse (à noter que l'estimation de phase n'est pas exclusivement utilisée pour calculer la position de l'utilisateur).

En effet, le temps de propagation du signal va entraîner un déphasage au niveau de la porteuse entre le signal reçu et les répliques générées par le récepteur (comme pour le code, la génération de la réplique locale est synchronisée en temps avec la génération au niveau du satellite). Tout comme le retard induit sur le code, ce déphasage est lié à la distance satellite/utilisateur.

En effet, le déphasage théorique lié au temps de propagation utilisateur/satellite *i* est donné par :

$$\Delta\Phi^i = 2\pi \frac{d^i}{\lambda} \qquad \text{(II.9)}$$

Avec : λ la longueur d'onde de la porteuse.

L'utilisation de l'information de phase permet théoriquement d'obtenir un positionnement plus précis que l'utilisation des pseudo-distances.

Cependant, l'estimation du déphasage pose un problème d'ambiguïté. Comme pour le retard sur le code, l'estimation de la phase s'effectue avec des structures de poursuite qui comparent le signal reçu avec une réplique locale. Lors de la poursuite, l'estimation de phase $\widehat{\Phi}^i$ (aussi appelée observation de phase) ne correspondra pas au déphasage théorique sera donnée par :

$$\widehat{\Phi}^i = \Delta\Phi^i - N^i \qquad \text{(II.10)}$$

Avec : N^i la phase inconnue du récepteur aussi appelé terme "d'ambiguïté entière".

Ce terme d'ambiguïté résulte du fait qu'il n'est possible d'estimer ponctuellement une phase qu'à π ou 2π près selon l'estimateur de phase utilisé. Ainsi, au moment où la poursuite de phase est lancée, le récepteur va synchroniser la phase de la réplique locale avec la phase du signal reçu en estimant un retard qui n'excède pas un cycle de phase comme l'illustre la (figure II.15). Lorsque la poursuite est enclenchée, l'estimation de phase au cours du temps peut également subir des pertes de cycles dues à cette incapacité à estimer la phase au-delà d'un cycle ; ce problème est appelé "phénomène de sauts de cycle". [09]

A ces problèmes d'ambiguïté et de sauts de cycle s'ajoutent également toutes les perturbations liées à la propagation du signal.

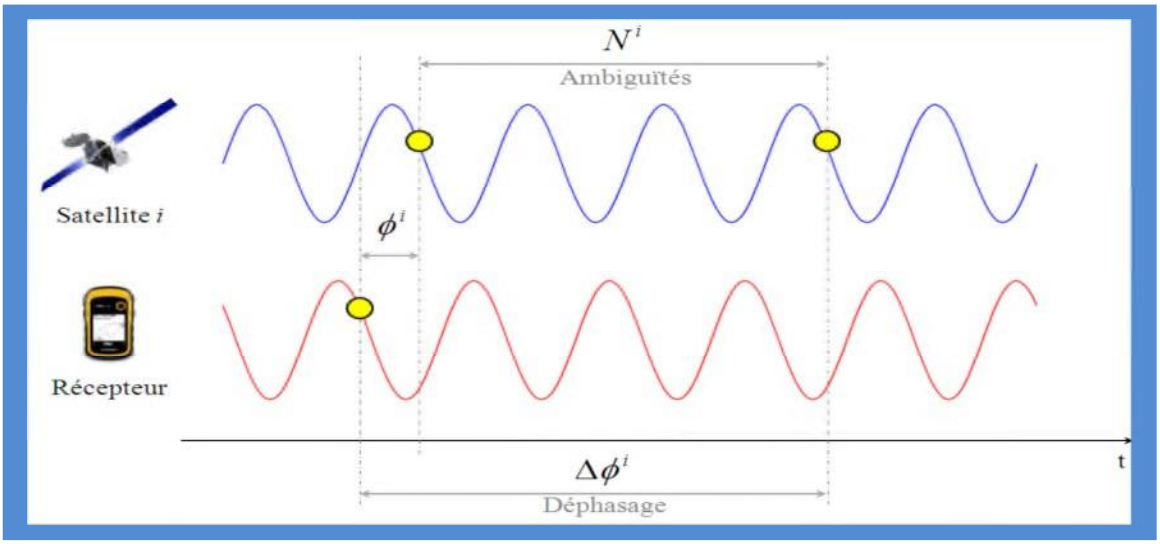

Figure II.15 : Illustration du problème d'ambiguïté entière lors de l'estimation de phase.

Pour un satellite *i* la phase peut se décomposer de la sorte :

$$\widehat{\Phi}^i = \Delta\Phi^i + 2\pi f_p^i\left(\delta h_r - \delta h_s^i\right) + \Delta I_\Phi^i + \Delta T_\Phi^i + m_\Phi^i + \epsilon_\Phi^i + \Delta N^i \qquad \text{(II.11)}$$

Avec

– f_p^i la fréquence porteuse,

– δh_r le biais d'horloge du récepteur,

– δh_s^i le biais d'horloge du satellite *i*,

– ΔI_Φ^i l'erreur de phase induite par les perturbations ionosphériques sur la phase,

– ΔT_Φ^i l'erreur de phase induite par les perturbations troposphériques sur la phase,

– m_{Φ}^{i} l'erreur de phase due à la présence de multi trajets sur la phase,

– $\in_{\Phi}^{i}$ le bruit de mesure sur la phase,

– ΔN^{i} l'erreur de phase due aux ambiguïtés de phase et aux sauts de cycle.

Comme pour l'observation de pseudo-distance, l'observation de phase est entachée de perturbations qui vont induire des erreurs lors du calcul de la position de l'utilisateur.

II.4.2.3. Poursuite de la fréquence Doppler :

La connaissance de la fréquence Doppler du signal reçu ne permet pas d'estimer la position de l'utilisateur. Cependant, il est possible d'estimer la fréquence Doppler au cours du temps afin de synchroniser en fréquence les répliques locales du récepteur au niveau des boucles d'estimation du délai sur le code.

Outre la nécessité de synchroniser en fréquence les répliques du récepteur, la connaissance de la fréquence Doppler permet également d'assister l'estimation du décalage sur le code.

En effet, connaissant la fréquence Doppler f_d du signal à la réception, il est possible de compenser la dynamique satellite/utilisateur au niveau de l'estimation du décalage sur le code $\hat{\tau}$ par :

$$\hat{\tau} = \hat{\tau} - \frac{f_d}{f_p} T_{corr} \qquad \text{(II.12)}$$

Avec : f_p la fréquence porteuse du signal reçu et T_{corr} le temps de corrélation du signal au niveau du récepteur. Le principe de pré-compensation Doppler sur le code est donné à la (figure II.16) :

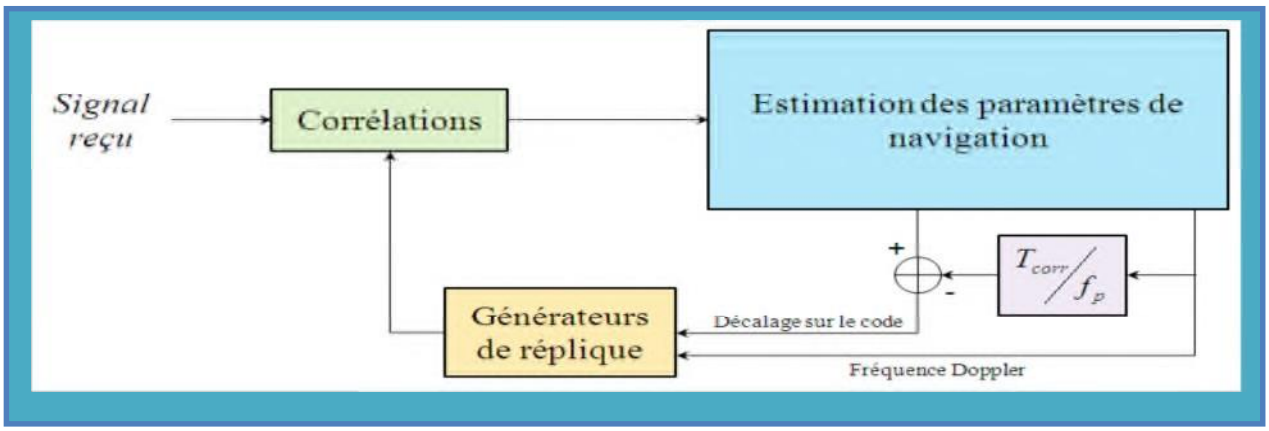

Figure II.16 : Pré-compensation Doppler sur le code

Pour estimer la fréquence Doppler du signal reçu au cours du temps, un système bouclé (basé sur la corrélation du signal reçu avec une réplique locale) est mis en place comme pour le cas de l'estimation du décalage sur le code ou la phase.

Une interaction entre le système de poursuite de la fréquence Doppler et le système de poursuite de phase peut également être instaurée de par la relation de dérivation/intégration qui lie ces deux grandeurs.

II.4.3. Calcul de la position de l'utilisateur :

Pour pouvoir calculer sa position, le récepteur va chercher à mesurer la distance qui le sépare des satellites dont il connaît les positions (grâce aux éphémérides contenues dans le message de navigation) via les différentes observations fournies par les algorithmes de poursuite. Pour ce faire, le récepteur dispose de plusieurs techniques regroupées en deux grandes familles(Les techniques de positionnement standard et les techniques de positionnement précis) :

II.4.3.1. Les techniques de positionnement standard :

Utilisent directement les observations de pseudo-distance. Par exemple, si on ne cherche qu'à corriger le biais d'horloge du récepteur et si on pose :

– (x_i, y_i, z_i) les coordonnées du satellite *i*,

– (X, Y, Z) les coordonnées du récepteur,

– δh_r le biais horloge du récepteur avec les satellites,

– $\in^i$ l'erreur de mesure de pseudo-distance contenant les perturbations atmosphériques, les perturbations liées aux multi-trajets et le bruit de mesure

Alors la pseudo-distance ρ^i entre le récepteur et le satellite *i* peut s'écrire:

$$\rho^i = \sqrt{(x_i - X)^2 + (y_i - Y)^2 + (z_i - Z)^2} + \delta h_r + \epsilon^i \qquad \text{(II.13)}$$

Si le récepteur reçoit les signaux de N_{sat} satellites en vue, alors on obtient le système d'équations suivant :

$$(S_1)\begin{cases} \rho^1 = \sqrt{(x_1 - X)^2 + (y_1 - Y)^2 + (z_1 - Z)^2} + \delta h_r + \epsilon^1 \\ \rho^2 = \sqrt{(x_2 - X)^2 + (y_2 - Y)^2 + (z_2 - Z)^2} + \delta h_r + \epsilon^2 \\ \vdots \\ \rho^{N_{sat}} = \sqrt{\left(x_{N_{sat}} - X\right)^2 + \left(y_{N_{sat}} - Y\right)^2 + \left(z_{N_{sat}} - Z\right)^2} + \delta h_r + \epsilon^{N_{sat}} \end{cases}$$

A partir du système (*S*1) il est possible de déterminer les coordonnées (*X*, *Y*, *Z*) et le biais d'horloge dh_r du récepteur à condition d'avoir estimé suffisamment de pseudo-distances.

Pour calculer la position du récepteur, d'autres techniques peuvent être mises en place comme les techniques d'estimation par les moindres carrés, les moindres carrés récursifs, le filtrage de Kalman étendu, ou la méthode de Bancroft.

II.4.3.2. Les techniques de positionnement précis :

Utilisent, contrairement aux techniques de positionnement standards, les observations de pseudo-distance ainsi que les observations de phase. De plus, les diverses erreurs liées à l'ionosphère ou aux ambiguïtés de phase sont désormais prises en compte et sont compensées par des combinaisons linéaires entres différentes observations obtenues sur une ou plusieurs porteuses.

Le récepteur a deux possibilités pour effectuer ces combinaisons :

–Soit il utilise les observations sur la pseudo-distance et sur la phase qu'il a lui-même estimé. Ce mode de positionnement correspond au mode PPP *(Precise Point Positioning).*

–Soit il utilise, en plus de ces observations, des observations provenant d'un récepteur de référence. Ce mode de positionnement correspond au mode RTK *(Real Time Kinematic).*

Quel que soit le mode de positionnement utilisé, les combinaisons d'observations sont traitées par des filtres de Kalman étendus qui estiment la position et la dynamique de l'utilisateur.

II.5. Conclusion :

Nous avons parcouru les différents types de récepteurs pour la navigation par satellite. Au-delà des techniques de base qui sont communes à tous ces récepteurs, ce sont les types d'applications qui constituent les véritables différences entre tous ces équipements de réception.

On a vu ainsi, les opérations réalisées par le récepteur GPS, dans lequel il doit effectuer plusieurs étapes (Le traitement classique du signal à la réception, l'acquisition et la poursuite) pour extraire les informations nécessaires au calcul du point.

Chapitre III

Brouillage Et Leurrage Du GPS

- Introduction
- Vulnérabilité des signaux GPS
- Brouillage des signaux GPS
- Leurrage des signaux GPS
- Outils, matériels & logiciels
- Brouillage des signaux GPS par HackRF
- Simulateur de signaux GPS
- Interface Sous GNU Radio
- Résultats
- Conclusion

III.1. Introduction :

Les récepteurs GPS civils sont vulnérables à divers types d'attaques dus à la faible puissance du signal et la publication des données du message navigation par l'U.S.A. on note qu'il existe plusieurs types d'attaques, on distingue :

- *Brouillage (Jamming) :* il s'agit de la transmission d'un signal plus puissant dans la même bande de fréquences que le GPS afin de bloquer la réception au niveau récepteur ;
- Leurrage (Spoofing) : Cette technique permet d'émettre des signaux GPS afin de transmettre de fausses informations de localisation. Si le brouillage peut être non intentionnel, le leurrage ou « spoofing » ne peut être qu'intentionnel, sa réalisation est sophistiquée et nécessite des moyens techniques et logistiques importants, souvent difficiles à acquérir sans un soutien étatique. Il s'agit là de mesures offensives pouvant avoir de lourdes conséquences ;
- Leurrage par usurpation (Meaconing) : Il s'agit de la réception des signaux GPS puis les diffuser tout en manipulant les pseudo-distances.

C'est la très faible puissance du signal GPS qui le rend vulnérable au brouillage, qu'il soit intentionnel ou pas. Les interférences fortes sont utilisées lors du brouillage, ce qui entraîne généralement une perte du signal utile et par conséquent l'incapacité de positionnement du récepteur. Cependant, le leurrage est une interférence structurelle et plus ou moins discrète, faite par des spécialistes du traitement de signal GPS de telle manière que les signaux établis puis transmis ressemblent suffisamment aux signaux satellitaires authentiques, par conséquent il sera difficile de les déceler ou les éliminer par des récepteurs conventionnels.

La structure des signaux GPS civils, y compris le type de modulation, les signaux *PRN*, la fréquence d'émission, la largeur de bande du signal, la plage du Doppler, la puissance du signal et de nombreuses autres caractéristiques étant connus et publiés, ce qui offre l'accès au développement de différents types de '*Spoofeur*' et similairement les contre-mesures associées.

Dans ce chapitre, on s'intéresse à la vulnérabilité des signaux GPS et les différents types de brouillage et de leurrage relevés dans la littérature. Par la suite, nous présentons les outils software et hardware que nous utiliserons. Après un court passage sur le brouillage GPS, on présente notre logiciel de leurrage que nous avons développé.

III.2.Vulnérabilité des signaux GPS :

On peut diviser ou classer la vulnérabilité des signaux GPS en deux niveaux de complexité selon la manière de fabriquer les signaux erronés, on distingue :

- La vulnérabilité au niveau de l'étage de traitement de signal ;
- La vulnérabilité au niveau de traitement des données.

III.2.1. Vulnérabilité au niveau traitement du signal :

Les tâches principales du module de traitement du signal sont l'acquisition et la poursuite du signal. Dans la phase d'acquisition du signal, le spoofeur peut transmettre des signaux contrefaits qui sont beaucoup plus puissants que les authentiques ce qui peut amener le récepteur à les acquérir. Dans la phase de suivi du signal, une attaque par spoofing plus élaborée peut avoir lieu. Elle repose sur l'émission d'un signal erroné qui s'approche lentement de l'authentique jusqu'au verrouillage de la DLL sur lui, une fois le récepteur verrouillé il sera contrôlé par le spoofeur. [06]

De nombreuses variantes d'attaques de spoofing peuvent exister, la liste suivante non-exhaustive résume les plus importantes :

- *Délai d'accrochage* : Le spoofeur aborde le signal authentique avec un délai relatif $\Delta\tau_s$ tout en ajustant son amplitude A_s. Il s'initialise, avec un retard relatif avec une faible amplitude, puis il réduit le retard progressivement tout en augmentant l'amplitude. Quand $\Delta\tau_s$ tend vers zéro et A_s soit similaire à l'authentique ; à ce moment, la puissance du signal erroné est augmentée progressivement au même temps que le retard relatif afin de s'éloigner des paramètres de verrouillages authentiques ;
- *Accrochage aligné* : Similaire à la précédente, mais avec le spoofeur aligné sur le signal satellite en visibilité directe, c'est à dire $\Delta\tau_s$ égale zéro dès le début de l'attaque. Cela évite d'être détecté en un point éloigné du corrélateur de la DLL mais nécessite une connaissance précise de la position du récepteur en question ;
- *Brouillage puis leurrage* : Dans ce cas, le spoofeur oblige le récepteur à passer en mode acquisition en raison d'un brouillage excessif qui provoque une perte de verrouillage des signaux GPS authentiques, tout en transmettant des signaux de leurrage. Une fois le brouilleur est désactivé le récepteur acquière les signaux de leurrage.

III.2.2. Vulnérabilité au niveau traitement de données :

Dans le module de traitement de données, les informations sont extraites des messages de données et les *PVT* (*Position, Vitesse* et *Temps*) sont résolus à l'aide des mesures fournies par le module de traitement de signal. Comme la structure de trame du message de données est publiquement connue et que les informations ne changent pas rapidement au cours de certains intervalles de temps, le message de données peut être facilement falsifié, ce qui oblige le récepteur victime à admettre le message altéré de manière fortuite. [12]

III.3. Le brouillage :

Le brouillage consiste à diriger intentionnellement de l'énergie électromagnétique vers un système de navigation afin de perturber ou d'empêcher la transmission du signal. Ainsi, les brouilleurs GPS diffusent leur signal de brouillage dans la bande de fréquence utilisée pour les communications par satellite. Les signaux GNSS est toujours disponible mais ses signaux de diffusion sont totalement noyés par la puissance du brouilleur. [12]

III.3.1. Brouillage non-intentionnel :

Plusieurs sources potentielles de brouillage non-intentionnel du GPS peuvent être répertoriées, on peut les classer en trois classes principales :

- La première concerne le brouillage dit '*Co-canal*' causé par les systèmes continus ou pulsés fonctionnant dans les mêmes bandes que les signaux de navigation ;
- Le second groupe concerne les brouillages dits de '*Canal adjacent*' causés par les systèmes continus ou pulsés fonctionnant dans les bandes adjacentes à celles des signaux de navigation. Ces interférences peuvent être dues à un découplage et une réjection insuffisante du spectre émis par rapport à la bande des signaux de navigation, ou à des produits d'intermodulation résultant notamment des caractéristiques non-linéaires des amplificateurs de forte puissance lorsqu'ils servent à amplifier plusieurs porteuses de fréquences voisines ;
- La troisième classe concerne les brouillages '*hors-bande*' correspondant à des rayonnements de systèmes éloignés des bandes de navigation et peuvent être dus aux harmoniques et aux produits d'intermodulation générés par des systèmes radioélectriques dans l'environnement plus ou moins proche du récepteur, et à des bruits

large bande.

Connaissant ces classes, des exemples de sources de brouillages non intentionnels sont identifiés :

- Les systèmes fonctionnant dans les mêmes bandes que le GPS: systèmes de radionavigation aéronautique DME/TACAN, système de communications militaires JTIDS/MIDS, Radars primaires de contrôle aérien (ATC) ;
- Les systèmes fonctionnant dans les bandes adjacentes: Radars primaires de la surveillance du trafic aérien (ATC), Radars de Défense, services mobiles par satellite, autres systèmes de radionavigation aéronautique (SSR, TCAS, IFF, ADS-B)…Les systèmes fonctionnant dans des bandes éloignées (interférences par harmoniques principalement): émetteurs TV et FM, systèmes de radionavigation aéronautique VOR et ILS ;
- Systèmes de communications VHFCOM, service Radioamateur.

III.3.2. Brouillage intentionnel :

On note que le signal GPS se trouve dans une bande de type ARNS dédiée aux services de radionavigation aéronautique, il s'agit d'une bande règlementée. Emettre dans cette bande peut engendrer de lourdes conséquences liées à la sureté de la vie humaine. Quoique dans notre étude, on utilisera un brouillage de très faible puissance à portée très limitée.

La figure (III.1) illustre un scénario de brouillage intentionnel. A la réception un signal brouilleur constant et de puissance suffisante peut bloquer la réception du signal GPS dans une zone donnée. Le rayon de perturbation centré sur la source de brouilleur est fonction de la puissance d'émission et de la fréquence centrale du brouilleur.

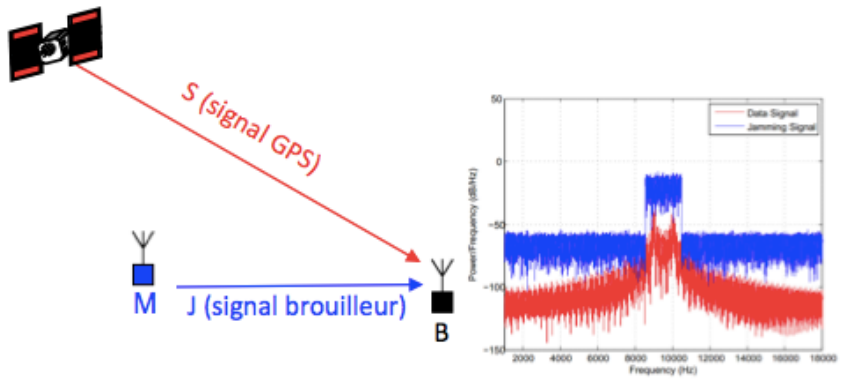

Figure III.1 : Brouillage intentionnel.

A la réception, le brouilleur est quantifié par le rapport signal à interférence *J/S*, C'est le rapport de puissance entre deux signaux reçus au même temps dans la bande du recepteur. En présence d'interférence c'est le *CNR* qui prend une nouvelle forme :

$$\left[\frac{C}{N_0}\right]_{eq} = \frac{C}{N_0 + J} = \frac{1}{1/_{C/N_0} + {}^{J/S}/_{Qf_c}} \qquad \text{(II.1)}$$

Avec :

J/S : Rapport de puissance interférence au signal ;

f_c : fréquence du code GPS 1.023 MHz ;

Q : facteur d'ajustement du gain de traitement

= 1 pour l'interférence à bande étroite ;

= 1.5 pour l'interférence large bande ;

= 2 pour l'interférence Gaussienne à large bande.

Aussi écrite en décibel :

$$\frac{J}{S} = 10.log\left(Q.f.\left(\frac{1}{10^{(-C/N_0)_{eq}/10}} - \frac{1}{10^{-(C/N_0)/10}}\right)\right) \qquad \text{(II.2)}$$

Cette expression est utilisée pour déterminer la performance du GPS fonction de J/S à son seuil de poursuite. A titre d'exemple, si on considère que C/N_0 = 41.9 dB-Hz, $[C/N_0]_{eq}$ = 28 dB-Hz (Seuil de poursuite PLL pour BER<10^{-5}) et pour une interférence à bande étroite donc Q=1, on aura :

AN : J/S = 10*log[1*1.023.10^6*(1/10 $^{-2.8}$-1/10 $^{-4.19}$)] = 39.9 dB

C'est ce rapport qui est utilisé pour quantifier l'influence de l'interférence sur la réception du signal GPS, ceci en utilisant l'équation des télécommunications formulée en fonction du type de l'interférence par le biais d'un facteur Q :

$$D^2 \leq P_i + G_{ei} + G_{ri} - 20.log\left(\frac{4\pi}{\lambda}\right) - L_r - L_d - \left[\frac{J}{S}\right]_{max} - S_r \qquad \text{(II.3)}$$

Cette dernière expression obtenue, permet de tracer des courbes caractéristiques déterminant la puissance nécessaire à émettre pour que le brouilleur soit influent à partir de la distance désirée, ceci pour différents rapports de *J/S*.

Si à titre d'exemple $(J/S)_{max} = 20$ dB, un brouilleur de PIRE '1w' sera influent si sa distance est inférieure de 105Km.

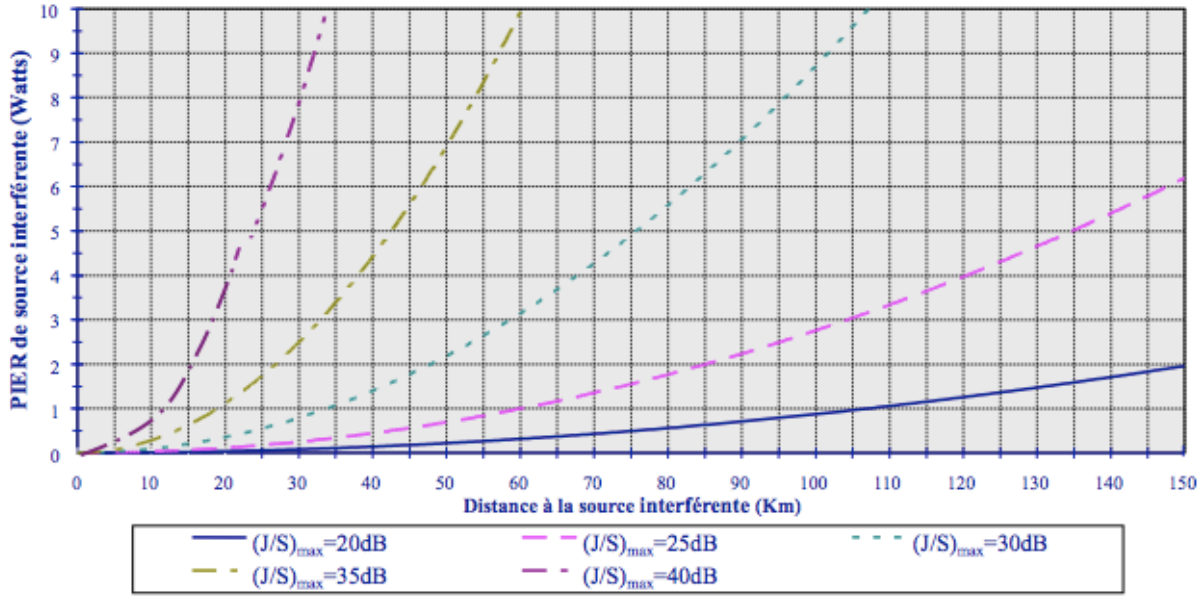

Figure III.2 : Courbes caractéristiques du brouillage intentionnel.

III.4.Le leurrage :

Le leurrage ou 'Spoofing' est une transmission délibérée de signaux GPS erronés dans l'intention de leurrer le récepteur en lui fournissant des fausses informations de position satellite, de vitesse ou de temps. Le but du spoofeur est de forcer discrètement le récepteur à se verrouiller sur les signaux erronés, par conséquent les informations récupérées après décodage sont fausses et par la suite la position aussi. [04] [12]

Le signal transmis par le spoofeur une fois verrouillé avec les signaux authentiques, il sera capable de prendre le contrôle du récepteur. Du point de vue pratique on peut modifier lentement la solution de position sans que le récepteur ne remarque une incohérence ou des discontinuités dans la solution. Bien qu'illégal, les études sur le spoofing se multiplient et deviennent un axe de recherche du domaine. On classe ces études en fonction de la complexité du spoofeur et de la difficulté de le détecter puis de l'éliminer. On différencie :

- *L'attaque simpliste :* Basée sur l'utilisation d'un simulateur du signal GPS pour produire le signal erroné puis le transmettre au récepteur. Ce type d'attaque est le plus facile à réaliser, mais il est également coûteux et facilement détectable, car ce type d'attaque présente généralement des discontinuités, dans les pseudo-distances, les fréquences Doppler, la synchronisation ou dans les calculs PVT. La figure III.3 montre une scène d'une attaque simpliste.
- *L'attaque intermédiaire* : Ce type de spoofeur possède un récepteur intégré qui collecte et suit les paramètres du signal satellitaire, afin de générer un nouveau signal cohérent avec l'authentique puis le transmettre au récepteur cible. Ce type d'attaques est généralement capable de modifier les différents paramètres sans créer de discontinuités. Cette technique est illustrée par la figure III.4.
- *L'attaque sophistiquée* : Son objectif est de surmonter une faiblesse de l'attaque intermédiaire, à savoir qu'elle diffuse depuis une seule antenne et une seule direction. La version sophistiquée utilise plusieurs antennes différentes pour diffuser chaque signal satellite afin de ne pas être détectée grâce à des techniques antispoofing reposant sur une discrimination d'angle d'arrivée. Cependant, ces attaques ont un niveau de complexité beaucoup plus élevé, étant donné le processus de synchronisation et de communication entre chaque émetteur, ce qui le rend très difficile à réaliser et ne convient pas à des exemples de scénarios réels. La figure (III.5) présente un scénario proposé de l'attaque sophistiquée.

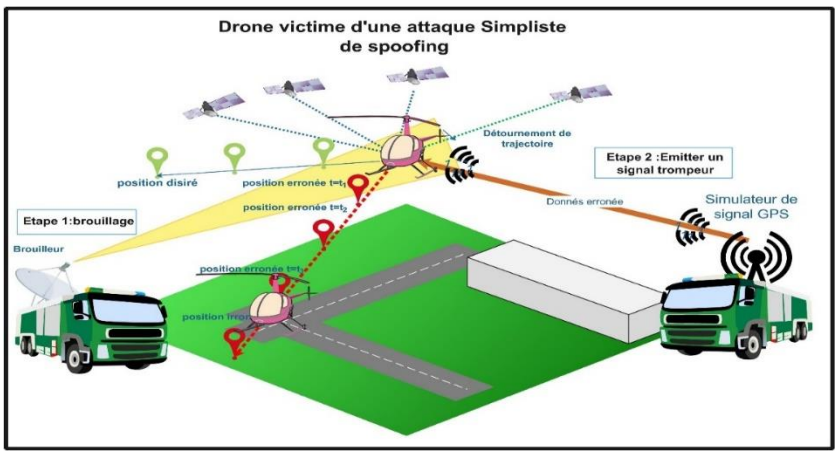

Figure III.3 : Une scène d'une attaque simpliste.

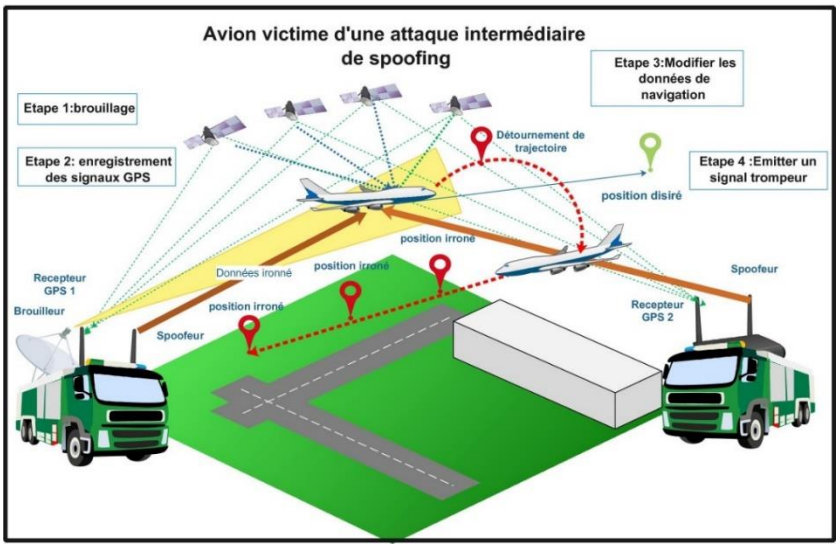

Figure III.4 : Une scène d'une attaque intermédiaire.

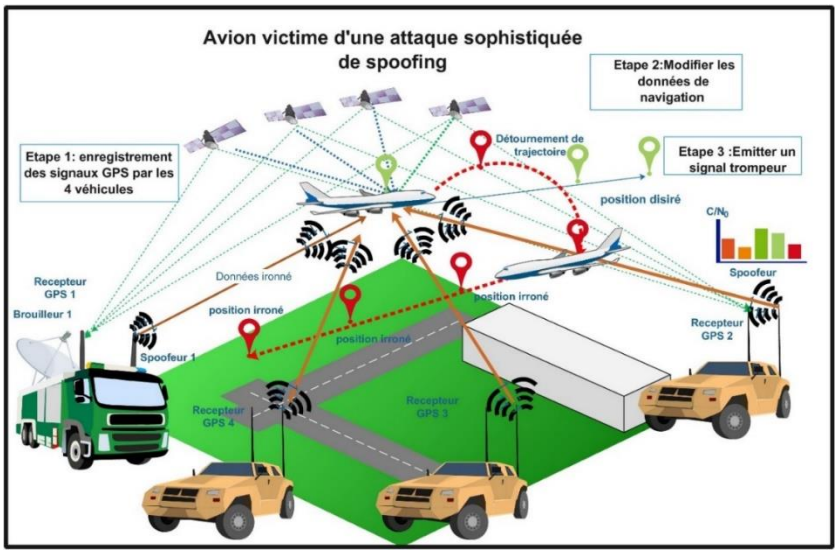

Figure III.5 : Une scène d'une attaque sophistiquée.

III.5. Outils matériel et logiciel :

III.5.1.Le HackRF One :

III.5.1.1. Description :

Le HackRF One illustré par la figure (III.6) est un équipement permettant d'effectuer des émissions / réceptions sur une large gamme de fréquences allant de 1MHz à 6 GHz avec une puissance de sortie de 1 mW à 30 mW selon la bande. L'unité est livrée avec un port d'antenne SMA, des ports CLKIN / CLKOUT SMA et un port USB 2.0 avec une série d'antennes.

Le matériel a été développé par Michael Ossmann (USA) comme un dispositif 'Open source' pouvant être connecté aux ordinateurs par le biais d'un port USB et qui s'interface avec de nombreux logiciels particulièrement le C++ et le GNURadio.

Figure III.6 : HackRF One.

La carte HackRF One se caractérise par une flexibilité très élevée pour le choix du parcours du signal. Les commutateurs HF situés à tous les points de jonction critiques permettent la sélection de différents composants, en fonction du choix de l'utilisateur. Après l'entrée de l'antenne, deux amplificateurs MMIC MGA-81 Ga-As se suivent, l'un sert à l'entrée, l'autre à la sortie. Les circuits intégrés des amplificateurs peuvent être sélectionnés dans et hors du parcours du signal par des commutateurs HF (SKY13317). Le bloc amplificateur est suivi d'un filtre passe-bas et d'un filtre passe-haut, qui peut être utilisé pour limiter le signal sur n'importe quel parcours (entrée / sortie). Après le filtre, le signal arrive à un mélangeur HF RFFC 5072. Ce mélangeur peut être utilisé jusqu'à 6 GHz. Le signal est mélangé en conversion haute ou basse, au choix de l'utilisateur. Le mélangeur et les filtres peuvent être contournés par d'autres interrupteurs HF, permettant ainsi aux signaux IF d'être orientés directement vers les amplificateurs ou plutôt vers l'antenne.

Le composant principal utilisé est un Maxim MAX2837 qui couvre une plage de fréquences de 2,3 à 2,7 GHz. La puce utilise des filtres monolithiques qui fournissent un signal très linéaire et un faible niveau de bruit. Les données IQ sont transmises à un convertisseur AN/NA Maxim MAX5864. Ce convertisseur dispose d'une résolution de 8 bits avec un taux d'échantillonnage maximal de 20 MS/s.

L'ensemble des circuits est conçu à obtenir une faible consommation d'énergie, l'alimentation se fait par le biais du port USB. La carte dispose d'une prise USB Micro-B, un câble approprié est inclus. Pour synchroniser plusieurs cartes HackRF One, le système offre des connecteurs d'entrée et sortie d'horloge. Ces signaux peuvent être utilisés pour faire fonctionner plusieurs cartes en parallèle, par exemple pour les mesures sur des systèmes MIMO ou des systèmes full duplex. Deux boutons poussoirs et plusieurs LED de diagnostic rendent l'utilisation facile.

III.5.1.2. Caractéristique du HackRF :

Le HackRF est caractérisé par :

- Fréquence de fonctionnement de 1 MHz à 6 GHz ;
- Emetteur-récepteur semi-duplex jusqu'à 20 millions d'échantillons par seconde, ce qui est suffisant même pour les transmissions en bande large telles que WFM, DECT, Wifi et autres ;
- Échantillons en phase et quadrature à 8 bits (I à 8 bits et Q à 8 bits) ;
- Compatible avec GNU Radio, SDR et plus ;
- Filtre de gain et de bande de base RX et TX configurable par logiciel ;
- Alimentation du port d'antenne contrôlée par logiciel (50 mA - 3,3 V) ;
- Connecteur d'antenne femelle SMA ;
- Entrée et sortie d'horloge femelle SMA pour la synchronisation ;
- Boutons pratiques pour la programmation ;
- Têtes à broches internes pour expansion ;
- USB 2.0 haute vitesse ;
- Alimenté par USB ;
- Matériel open source ;
- La puissance d'émission maximale absolue de HackRF One varie en fonction de la fréquence de fonctionnement, le tableau III-1, ci-dessous montre les intervalles des puissances qui correspondent à des fréquences données :

Fréquence (MHz)	Puissance (dBm)
10 à 2150	5 à 15
2150 à 2750	13 à 15
2750 à 4000	0 à 5
4000 à 6000	-10 à 0

Tableau III.1 : La variation de la puissance en fonction de la fréquence.

- La puissance de réception maximale de HackRF One est de -5 dBm. Tout dépassement de -5 dBm peut entraîner des dommages permanents. En théorie, HackRF One peut accepter en toute sécurité jusqu'à 10 dBm avec l'amplificateur RX frontal désactivé. Cependant, une simple erreur logicielle ou utilisateur pourrait activer l'amplificateur, entraînant des dommages irréversibles.

III.5.1.3. Antenne d'émission ANT500 :

L'antenne ANT500 que nous avons utilisé est une antenne télescopique conçue pour fonctionner entre 75 MHz et 1 GHz. Sa longueur totale est configurable de 20 cm à 88 cm. ANT500 est une antenne polyvalente de 50 ohms fabriquée en acier inoxydable et comprend un connecteur mâle SMA, un arbre rotatif et un coude ajustable. Cette antenne sous notre disponibilité est fournie avec HackRF One.

Le diagramme de rayonnement de l'ANT500 selon les deux plans, E et H, est illustré par la figure III.7.

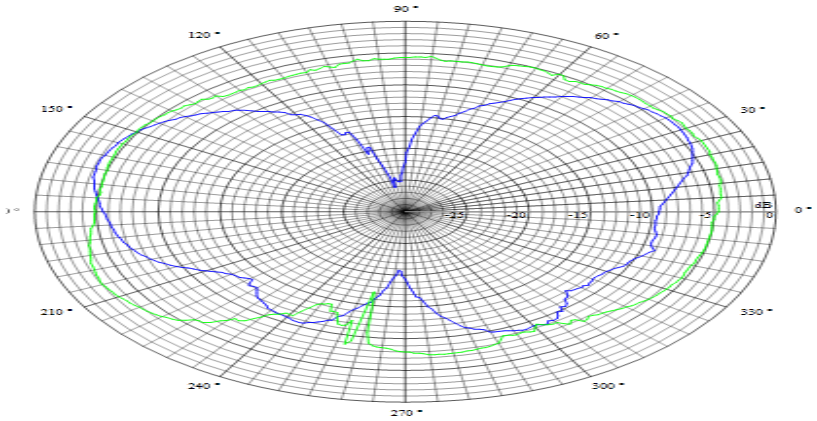

Figure III.7 : Diagramme de rayonnement de l'ANT500.

III.5.1.4. VCO TCXO 0.5 PPM :

Sachant que le Doppler lié aux satellites varie entre -5KHz et +5KHz, ce qui correspond à une déviation de fréquence L1 égale à 3.174 ppm, or que la stabilité en fréquence du HackRF est de l'ordre de 30 ppm, ce qui empêche une simulation correcte du Doppler liée au signal erroné.

Afin de surmonter cette limitation, on a installé sur le HackRF une source d'horloge externe, il s'agit du module VCO TCXO 05. Ce module super-minuscule dote notre HackRF avec une horloge beaucoup plus précise. L'oscillateur à quartz contrôlé par la température de 10MHz est 0.5 PPM (maximum) et a le bruit de phase ultra-bas. Il ne mesure que 0,58"x 0,4", ce qui garantit que les broches de l'en-tête HackRF ne sont pas obstruées par le module. Parfait pour toute expérimentation de haute précision, tel que notre projet GPS.

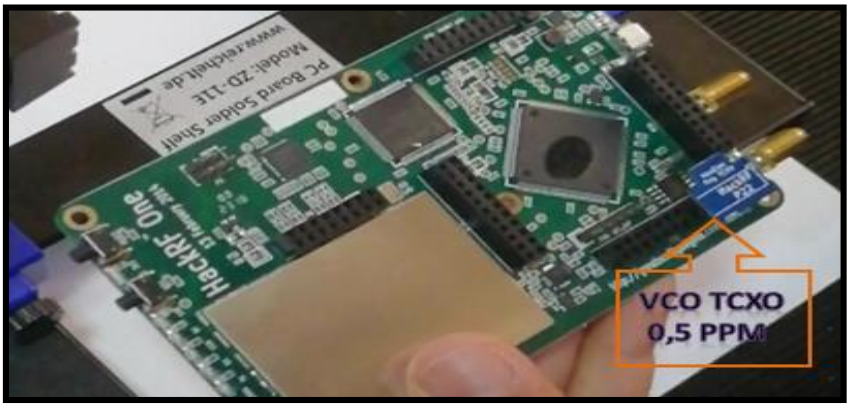

Figure III.8 **:** l'emplacement du VCO TCXO 0.5 ppm sur le HackRF.

III.5.2. GNU Radio :

III.5.2.1. Description :

GNU Radio est une boîte à outils de développement de logiciel libre qui fournit les blocs d'exécution DSP utilisés pour implémenter les SDR (Software Defined Radio) en conjonction avec du matériel RF externe à faible coût et facilement disponible. Il est largement utilisé dans les environnements amateurs, universitaires, commerciaux et militaires pour soutenir la recherche sur les communications sans fil, ainsi que pour mettre en œuvre des systèmes de radio du monde réel. GNU Radio Companion (GRC) est une interface utilisateur graphique qui permet de créer des graphiques de flux GNU Radio dans un environnement d'outil graphique convivial. [13]

GNU Radio fonctionne sous Linux et utilise un modèle de traitement de flux pour traiter de grandes quantités de données en temps réel, par opposition à un environnement de traitement de réseau traditionnel (comme Matlab, par exemple). En pratique, cela signifie que chaque bloc de traitement de signal possède un programmateur indépendant qui s'exécute dans son propre thread d'exécution et que chaque bloc s'exécute aussi rapidement que le permet la CPU, le flux de données et l'espace tampon.

La figure III.9, présente un exemple en utilisant GNU Radio, il s'agit de la génération d'un signal sinusoïdal, de fréquence L_1=15757.42 MHz et échantillonné à 2.6 MHz. Ce signal et son spectre seront affichés. En plus, le module 'osmocomSink' permet de transmettre ce signal sinusoïdal par le biais du HackRF.

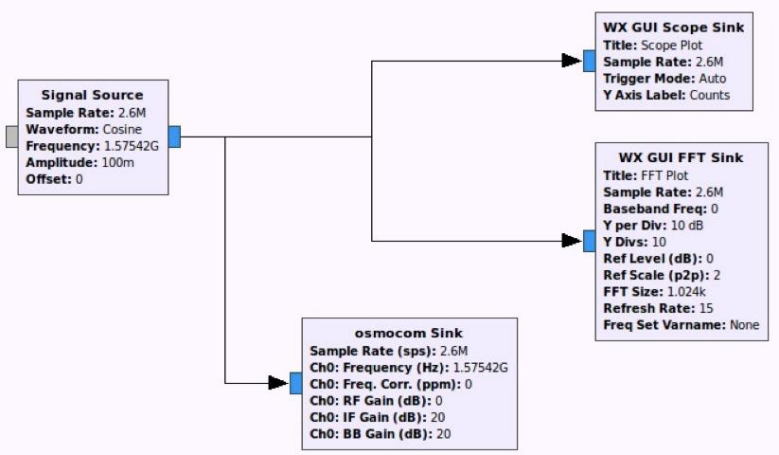

Figure III.9 : Génération d'un 'COS' et affichage de son spectre par GNU Radio.

III.5.2.2. Avantage d'utilisation du GNU radio :

La radio GNU présente plusieurs avantages que nous pouvons résumer comme suit :

- GNU Radio permet au concepteur de traiter en temps réel un flux de données . En outre, le programme radio peut être simulé en boucle ;
- Plus de 100 blocs sont disponibles pour développer facilement de nouvelles normes et applications, ainsi que des réseaux sans fil ;
- Le langage Python est relativement facile à maîtriser. Il décrit les étapes de traitement dans les blocs successifs et liés ;
- Grâce à un script Python, un flux de données peut atteindre une vitesse maximale sous des blocs de traitement ;
- La communauté des concepteurs de GNU Radio est large. La boîte à outils peut être réalisée par un simple ordinateur hôte sous Linux, Windows et Mac ;

- Un graphe de flux (ou une chaîne de communication) peut être reconfiguré même au moment de l'exécution. Plusieurs paramètres du traitement du signal peuvent être modifiés, tels que la fréquence, la puissance et les taux d'échantillonnage.

III.5.2.3. La liaison GNURADIO-HACKRF :

L'utilisation de GNU Radio dans ce projet a facilité l'émission, l'analyse et l'enregistrement des données. HackRF s'interface directement avec GNU Radio grâce aux modules de la bibliothèque 'osmocom' disponible. Néanmoins, des manipulations sont nécessaires afin d'exploiter nos résultats stockés dans des fichiers. On note que notre logiciel est réalisé sous-Matlab. La liaison est montrée par la figure (III-10).

Figure III.10 : La liaison GNURADIO et HACKRF One.

III.5.3. Application « GPS Test » Android :

Afin d'analyser nos émissions de types GPS ou brouillage, on a utilisé l'application Androïde nommée 'GPS test', cette application illustrée par la figure (III-11), elle permet de :

- Afficher les satellites en diagramme de ciel ;
- Afficher le niveau des signaux en barres verticales ;
- Fournir la position en Latitude, Longitude et Altitude ;
- Afficher la position sur une carte world ;
- Afficher la vitesse ;
- Fournir le temps à partir de données GPS.

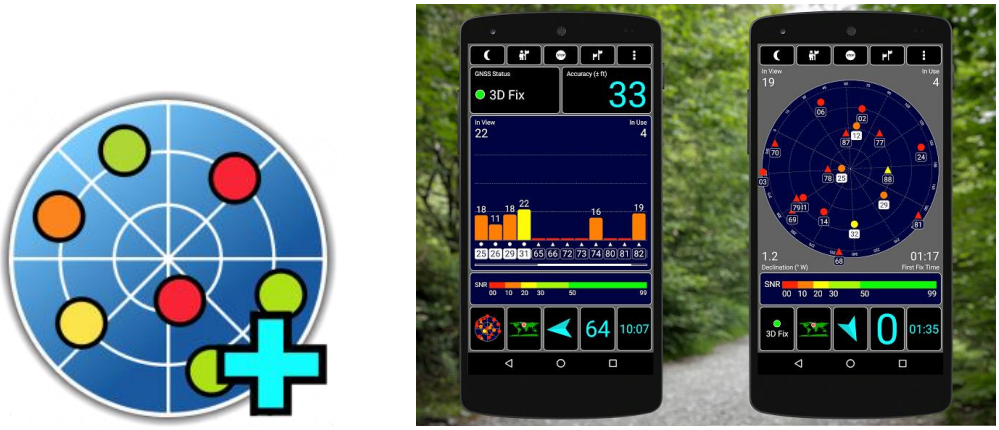

Figure III.11 : L'application GPS Test sur smartphone sous Androïde.

III.6. Brouillage des signaux GPS par HackRF :

Dans cette étape, on s'intéresse au brouillage du récepteur GPS en utilisant une source de bruit Gaussien sous GNU Radio puis l'émettre par le HackRF. Pour ce faire, on a utilisé le schéma GNU Radio illustré par la figure (III-12) avec les caractéristiques affichées sur chaque bloc. La figure (III-13) quant à elle montre la densité spectrale du ce signal émis, où on observe qu'il s'agit d'une bonne approximation du bruit blanc.

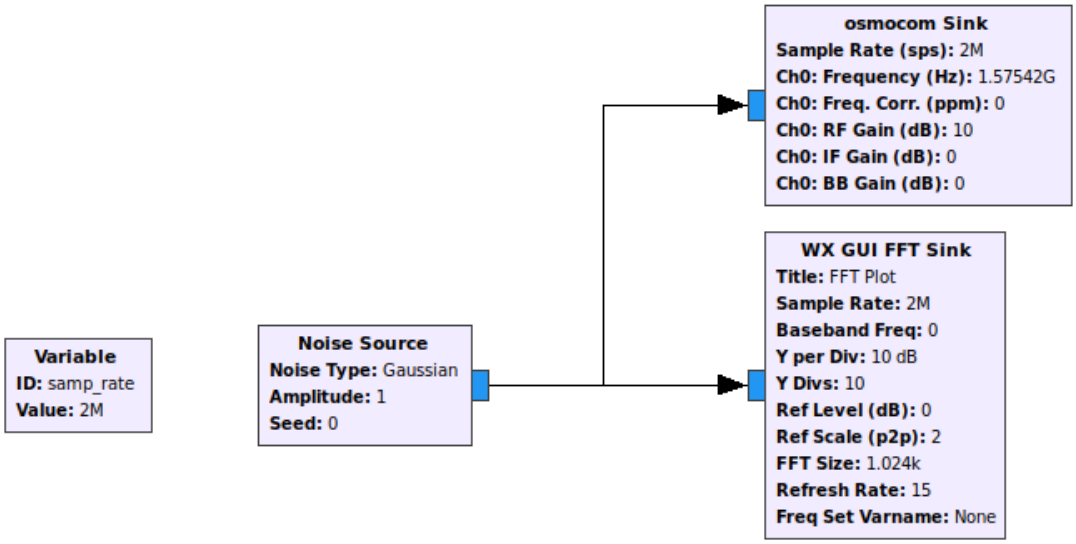

Figure III.12 : Brouilleur Gaussien dans la bande du GPS.

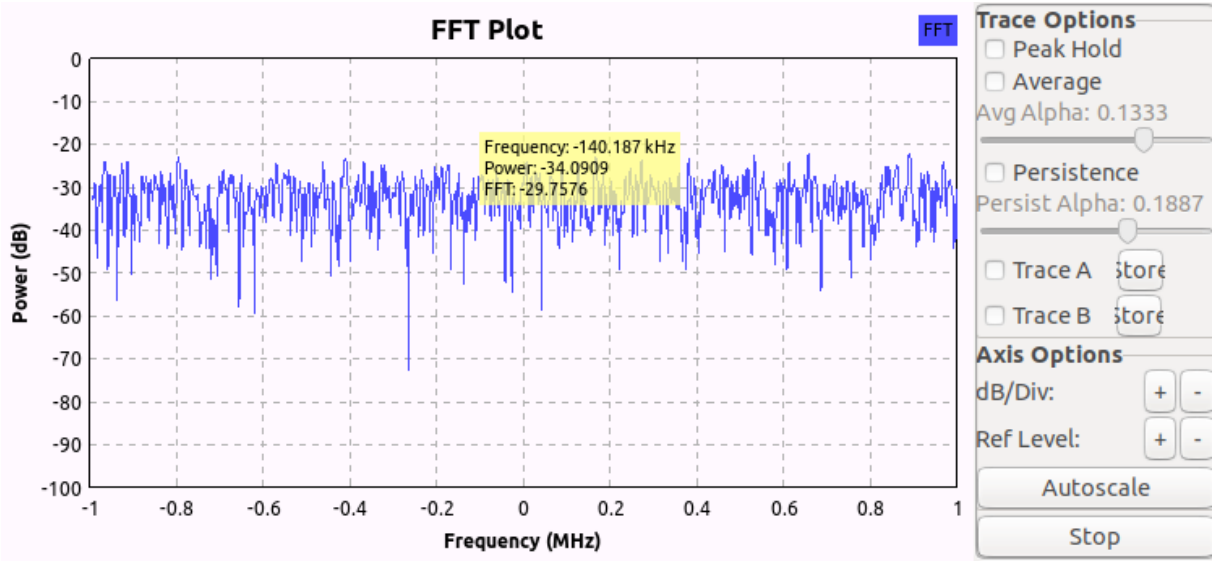

Figure III.13 : Densité spectrale du bruit émis.

Avant de lancer notre brouilleur, on a pris deux imprimes écrans. La première image concerne les niveaux de puissance des signaux GPS reçus, l'autre correspond au diagramme du ciel ou la constellation des satellites par rapport à notre position, ces images sont données par les deux figures (III-14 - a et b), dans ce cas la position est calculée ce qui est noté par le cercle vert en haut à gauche portant l'indication '*3D Fix*'.

Une fois le brouilleur est lancé, on observe d'abord une diminution des niveaux de signaux, tel que montré par la figures (III-14 - c), jusqu'à leur extinction totale après quelques secondes. On observe que cette fois la position n'est pas calculée. Un examen de la carte du ciel montre que les satellites ne sont plus exploitables.

Ce type de simulation, nous a permis de maitriser les puissances mises en jeu entre le HackRf et le téléphone et une bonne maîtrise des réglages des différents gains à l'émission. Il sera bien utile d'étudier l'influence d'autres types de brouilleurs.

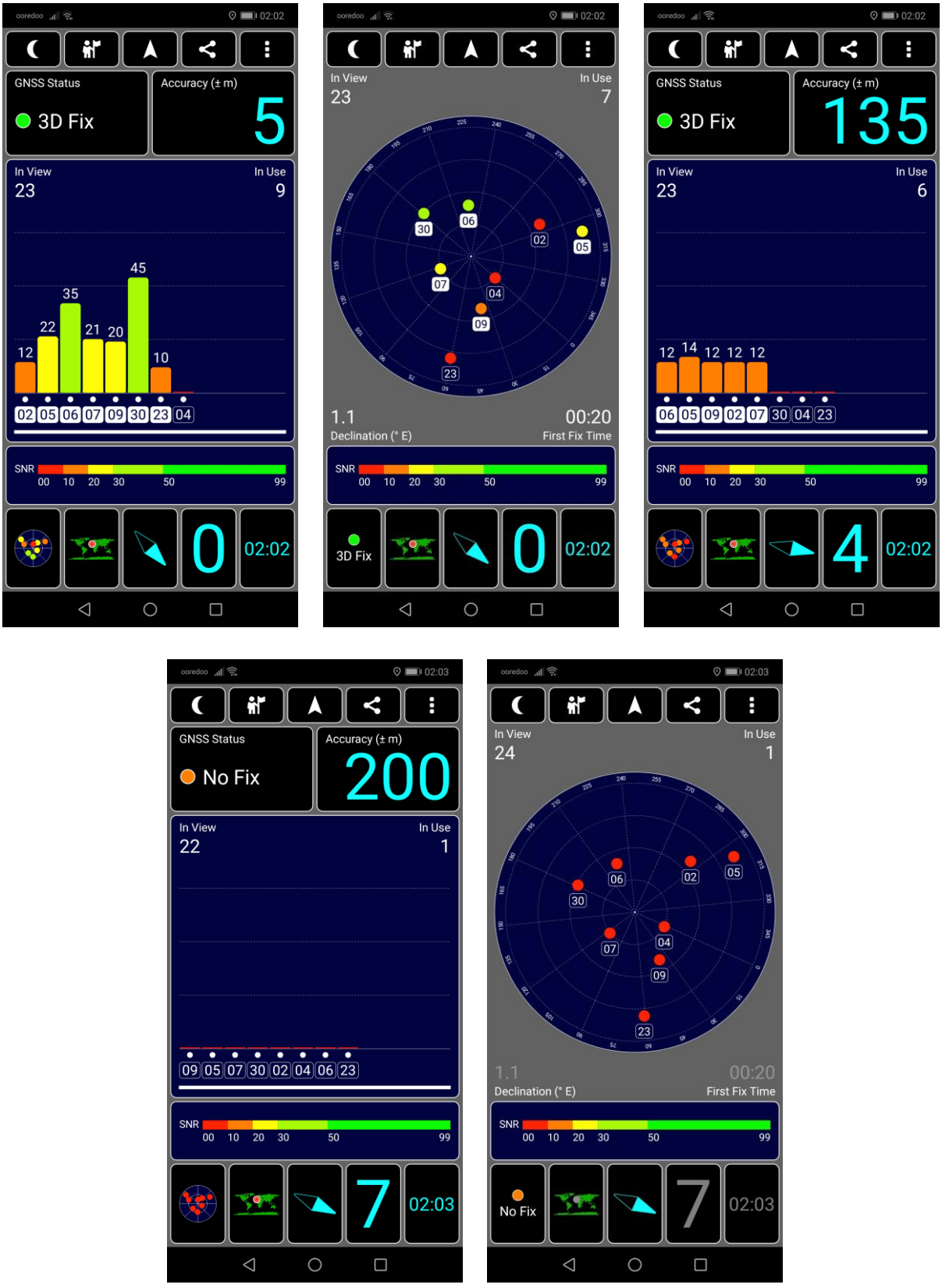

Figure III.14 : (de gauche à droite a-e): Situation avant et après brouillage.

III.7. Simulateur des signaux GPS :

III.7.1. Etapes de réalisation du spoofeur :

Dans cette partie on s'intéresse à développer un simulateur de signaux GPS, dans le but de réaliser un leurrage du récepteur. Pour y arriver, on a utilisé à l'addition des outils logiciels et matériels cités dans les paragraphes précédents, le Logiciel Matlab et des fichiers de types Rinex.

Notre logiciel sous Matlab permet de réaliser les fonctions suivantes :

- Lire le temps UTC ;
- Convertir le temps UTC en temps GPS ;
- Introduire une position erronée, fixe ou mobile en Llh ;
- Transformer la position erronée en ECEF ;
- Adapter puis Lire le fichier IGS, changer les paramètres nécessaires : TOC et TOE, Week number, IODE, IODC ;
- Stocker les données dans un cube ;
- Explorer ce cube selon le temps GPS le plus proche au temps de validité des éphémérides 'Toe' afin de récupérer la matrice d'éphémérides la plus récente ;
- Calculer de la position des satellites 'xyz' et leurs vitesses ;
- Calculer la position des satellites en ENU / par rapport à la position erronée du récepteur ;
- Calcul des angles d'azimut et d'élévation de chaque satellite ;
- Filtrer les satellites selon une élévation supérieure à un angle de masque désiré ;
- Récupérer la matrice résultante, sa première colonne identifie les PRNs des satellites, les autres les données des éphémérides associés ;
- Tracer le diagramme du ciel en 2D ou optionnellement en 3D ;
- Générer le message de navigation de durée désirée avec les conversions et les emplacements nécessaires ;
- Générer les bits de parité et les placer dans leurs positions exactes ;
- Calculer la distance entre la position erronée du récepteur et chaque satellite GPS au temps de réception ;
- Calculer la position des satellites au temps d'émission ;
- Calculer la distance entre position erronée du récepteur et chaque satellite au temps d'émission ;

- Calculer les retards de propagation ;
- Générer le code C/A de chaque satellite avec le retard correspondant ;
- Calculer la vitesse relative satellite / Récepteur afin de calculer le Doppler ;
- Calculer la phase du signal reçu ;
- Réaliser le produit entre le message de données et les codes C/A,
- Introduire les retards entre les signaux simulés, précisément les retards relatifs des 'TLM' ;
- Mettre le signal dans un fichier sous format Binfloat ;

Une fois ces étapes réalisées, on doit :

- Utiliser notre interface réalisée sous GNU Radio pour l'émission par le biais de HackRF ;
- Utiliser HackRF et émettre le signal ;
- Recevoir le signal par le module GPS lié à l'Arduino ou par l'application 'GPS test' ;

Ces étapes sont résumées par la figure (III-15).

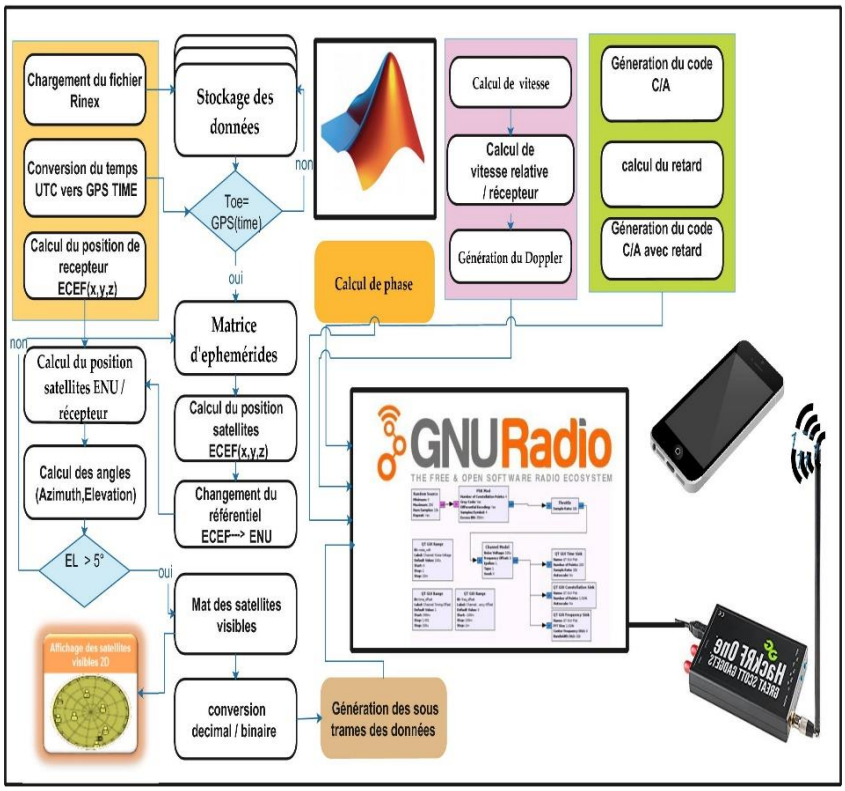

Figure III.15: synoptique du simulateur

Notre programme élaboré dépasse mille lignes de programmation Matlab, dans ce qui suit on présente seulement les étapes essentielles.

III.7.2. Génération du message :

Un fichier Rinex est un fichier qui contient des données de navigation, il s'agit d'éphémérides. Ce type de fichier n'est malheureusement pas disponible en temps réel pour nous. Le site IGS network, fournit ces fichiers pour des dates antérieures et pour un nombre important de stations autour du monde. Celle que nous avons choisie est celle de 'Melilla – Espagne', avec un fichier associé qui date depuis le 30 avril 2019, donc un traitement pour changer un certain nombre d'informations dans ce fichier afin de l'aligner avec le moment de notre émission s'avère nécessaire. Cette station est identifiée selon :

Réseau	Ville	Pays	Agence	Latitude	Longitude
IGS	Melilla	Espagne	IGN-E	35.2812194	-2.9516417

Le fichier Rinex est un format spécifique des données d'éphémérides, il contient des centaines de lignes présentées selon la forme : [04]

```
1 19  4 30  0  0  0.0-5.166977643967D-06-8.526512829121D-12 0.000000000000D+00
   3.800000000000D+01 2.131250000000D+01 4.513759588320D-09 2.304426529963D+00
   9.685754776001D-07 8.721235208213D-03 4.749745130539D-06 5.153652557373D+03
   1.728000000000D+05-1.583248376846D-07-2.477958434287D+00-1.024454832077D-07
   9.752949145022D-01 2.960937500000D+02 6.934654142580D-01-8.059264366977D-09
   2.250093722456D-10 1.000000000000D+00 2.051000000000D+03 0.000000000000D+00
   2.000000000000D+00 0.000000000000D+00 5.587935447693D-09 3.800000000000D+01
   1.728000000000D+05
```

Figure III.16: une trame Rinex.

Ces lignes contiennent les paramètres d'éphémérides, définies par le tableau III-2 ci-dessous.

Les données de navigation sont fournies par le fichier RINEX sous format décimal, cependant afin de les exploiter dans le message de navigation on doit les convertir en format binaire sur un nombre de bits défini et après multiplication par un facteur d'échelle. Les tableaux suivants indiquent l'emplacement et la taille des données de navigation dans les sous-trames et les facteurs d'échelles correspondants. [04]

Tableau III.2 : Données Rinex.

Bloc des données de navigation				
Numéro du satellite	Époque t_{oc} , temp GPS	a_{f0} (s)	a_{f1} (s/s)	a_{f2} (s/s^2)
	$IODC_{nav}$	C_{rs}	Δn	M_0
	C_{uc}	E	C_{uc}	$\sqrt{a}$
	t_{oe}	C_{ic}	Ω_0	C_{is}
	i_0	C_{rc}	Ω	$d\Omega/dt$
	di/dt	Source de données	Semaine	-
	Précision	Etat du sat.	BGD_{E5aE1}	BGD_{E5bE1}
	Temps de transmission	-	-	-

Tableau III.3 : Les éléments de la première sous-trame.

Paramètre	Emplacement	Nombre de bits	Facteur d'échelle LBS	Unités
Numéro de semaine	61-70	10	1	semaine
Précision du satellite	73-76	4		
Santé du satellite	77-82	6	1	
IODC	83-84	10		
t_{oe}	219-234	16	2^4	seconds
af_2	241-248	8	2^{-55}	Sec/sec^2
af_1	249-264	16	2^{-43}	Sec/sec
af_0	271-292	22	2^{-31}	seconds

Tableau III.4: Les éléments de la deuxième sous-trame.

Paramètre	Emplacement	Nombre de bits	Facteur d'échelle LBS	Unités
C_{ic}	61-76	16	2^{-29}	rad
Ω_e	77-84 91-114	32	2^{-31}	demi-cercles
C_{is}	121-136	16	2^{-29}	rad
i_0	137-144 151-174	32	2^{-31}	demi-cercles
C_{rc}	181-196	16	2^{-5}	mètres
ω	197-204 211-234	32	2^{31}	demi-cercles
Ω	241-264 271-278	24	2^{-43}	demi-cercles /sec

Tableau III.5 : Les éléments de la troisième sous-trame.

Paramètre	Emplacement	Nombre de bits	Facteur d'échelle LBS	Unités
C_{rs}	61-68 69-84	8 16	2^{-5}	mètres
Δn	91-106	16	2^{-43}	demi-cercles /sec
M_0	107-114 121-144	32	2^{-31}	demi-cercles
C_{uc}	151-166	16	2^{-29}	rad
e_s	167-174 181-204	32	2^{-33}	-
C_{us}	211-226	16	2^{-29}	rad
$\sqrt{a_s}$	227-234 241-264	32	2^{-19}	mètres $^{1/2}$
t_{oe}	277-286	16	2^4	seconds

Tableau III.6: Les éléments de la quatrième et la cinquième sous-trame.

Sous trame	**Pages**	**Données**
4	2, 3, 4, 5, 7, 8, 9 et 10	Les almanachs de satellite 25 à 32
	1, 6, 11, 16 et 21	Utilisation future réservée
	12, 19, 20,22, 23 et 24	Utilisation future réservée
	13	Tableau de correction des messages de navigation
	14 et 15	Utilisation réservée du système
	17	Message spécial
	18	Données ionosphériques et UTC
	25	Drapeau anti-spoofing, santé du satellite 25 à 32
5	1 à 24	Les almanachs du satellite
	25	Santé du satellite 1 à 24, temps référence, nombre de semaine

Une fois les paramètres orbitaux convertis et placés dans leurs positions, on ajoute au début de chaque sous-trame 8 bits de préambule '10001011', selon la forme suivante : [04]

TLM

Préambule 1000 1011	Donnée	Parité
8 bits	26 bits	6 bits

Le deuxième mot (Mot : 30 bits) de chaque sous-trame est noté HOW 'Hand over Word', il inclut une version tronquée du temps dans la semaine TOW. Ce nombre est appelé le comptage 'Z'. Le compte Z correspond au nombre de secondes écoulées depuis le dernier début de la semaine GPS en unités de 1,5 s. La valeur maximale du compte Z est de 403 199. La valeur du Z-count dans le HOW est une version tronquée ne contenant que les 17 bits les plus significatifs (MSB). Cette troncature augmente le compte Z par incréments de 6s correspondant au temps qui s'écoule entre la transmission de deux sous-trames de navigation consécutives.

La valeur de Z-count tronqué dans le HOW correspond au temps de transmission de la sous-trame de données de navigation suivante. Pour obtenir l'heure de transmission de la sous-trame en cours, il faut multiplier le Z-count tronqué par 6 et soustraire 6 s du résultat. Le mot HOW est défini comme suit :

HOW

Temps dans la semaine			Numéro de sous-trame			Parité
17 bits			3 bits			6 bits

Le message GPS contient des bits générer par un algorithme détecteur d'erreurs, il s'agit de bits de contrôle de parité, de nombre 6 bits placés à la fin de chaque mot. Si on note d_i, i=1:24 les bits du mot considéré. Les six bits de parité sont définis selon les équations ci-dessous, où les deux bits notés D_{29}^* et D_{30}^* sont les deux derniers bits de parité du mot précédent.

La figure (III-17), présente l'organigramme que nous avons développé afin de générer le message de navigation.

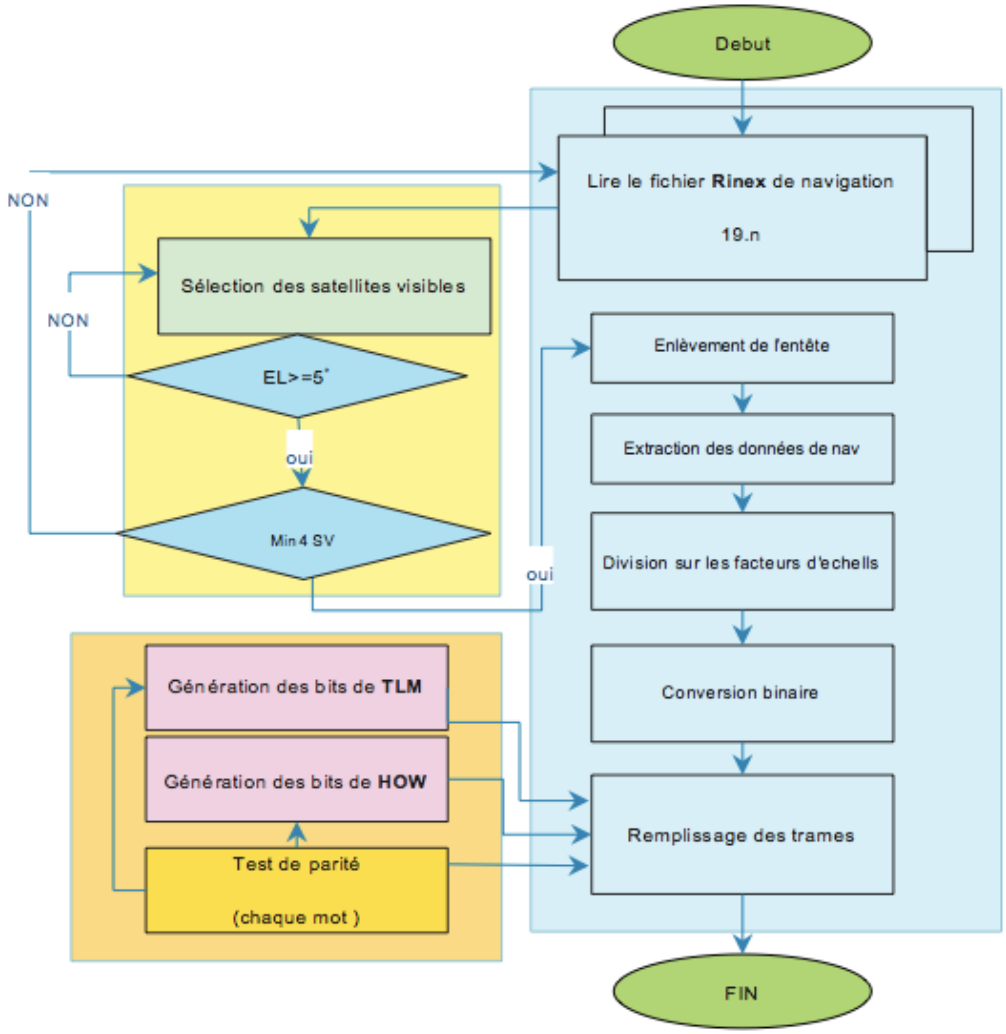

Figure III.17 : Organigramme de la génération du message de navigation.

III.7.3. Interface du logiciel :

Nos fonctions réalisées sont regroupées sous une seule interface conviviale complète et pratique. Elle permet de récupérer les données liées aux satellites GPS à n'importe quel moment et n'importe quel endroit introduit de notre part. Par un simple clic sur un bouton correspondant, on peut afficher, le diagramme du ciel en 2D ou 3D, les PRN's associés sont affichés. On peut avoir :

- La position des satellites ;
- Le Doppler ;
- Le temps GPS au moment de la constellation ;
- La situation future ou antérieure de la constellation ;
- Les retards des codes C/A ;
- Le message de navigation ;

✦ Les signaux GPS associés à la constellation, …

Notre logiciel développé s'est synchronisé correctement avec la constellation GPS. Un exemple tiré de cette interface correspondant à notre position au sein de l'université est illustré par la figure (III-18) ci-dessous. Notre constellation peut être vue en trois dimensions, ceci est illustré par la figure (III-19). Si on désire au même moment évaluer la constellation à Pékin (Chine) à titre d'exemple, il suffit d'introduire les coordonnées (116.39 E, 39.9 N). [06]

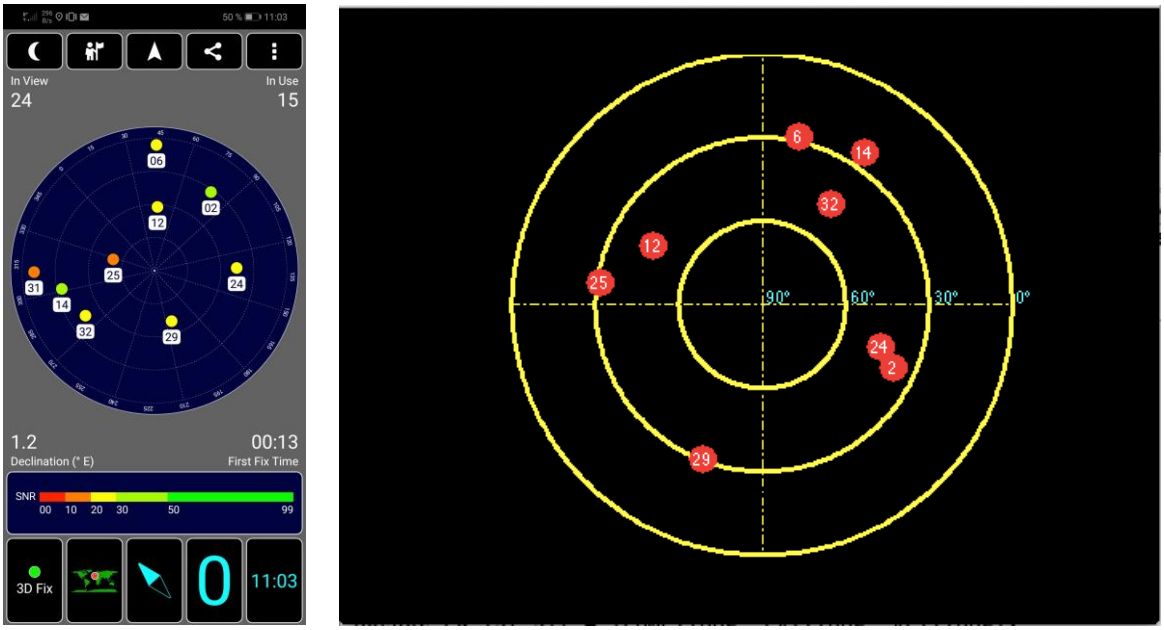

Figure III.18 : Diagramme du ciel 2D & GPStest.

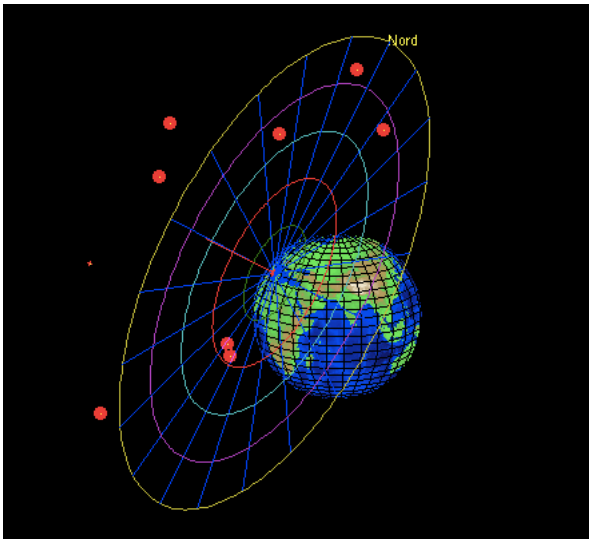

Figure III.19 : Diagramme du ciel 3D.

III.8. Interface du logiciel GNU Radio :

Nous avons développées l'interface GNU Radio illustrée par la figure (III-20) (ci-dessous) afin de transmettre nos signaux simulés.

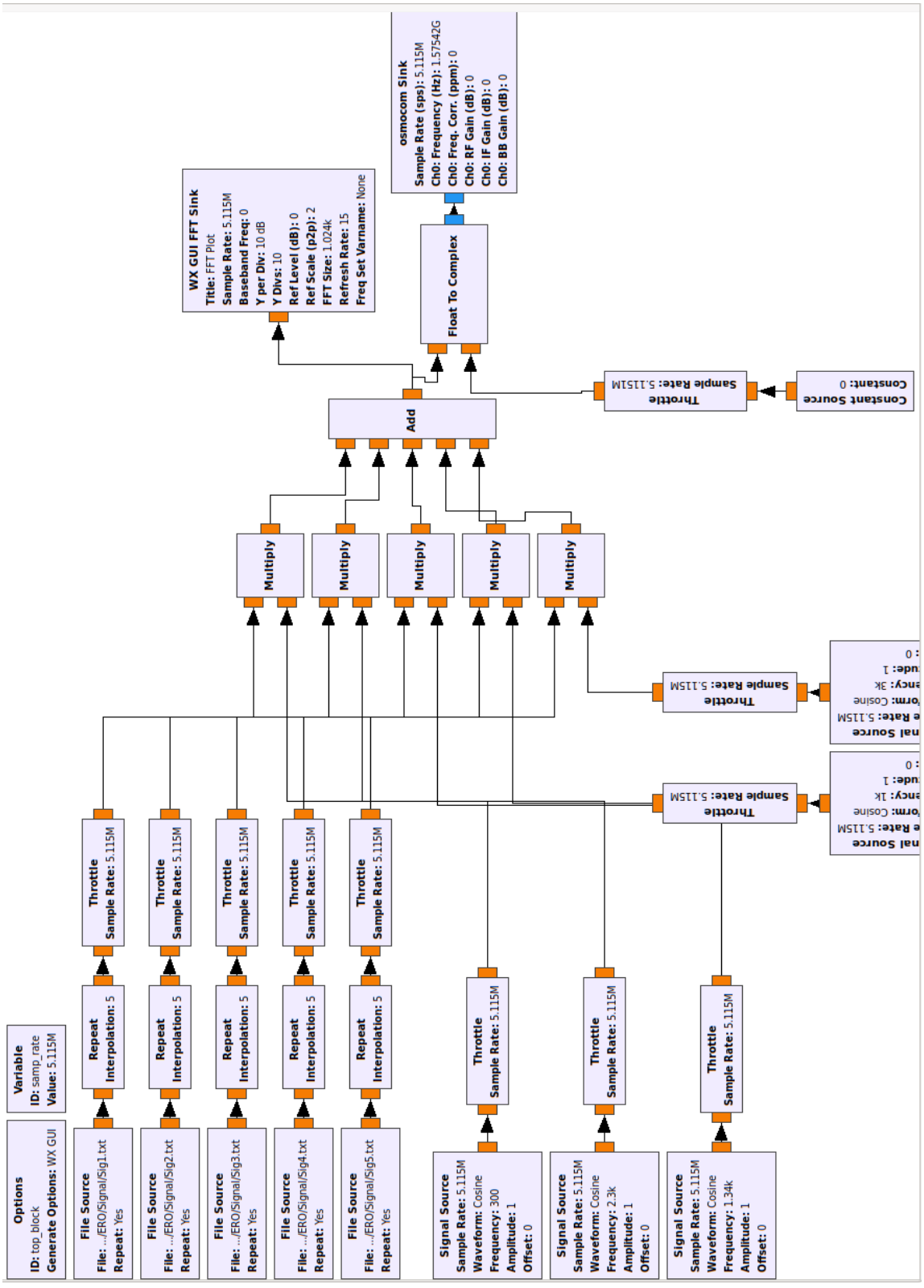

Figure III.20 : Interface du logiciel GNU Radio pour le leurrage.

La figure (III-21) présente le spectre du signal émis, en bande de base, on observe la fréquence de coupure de 1.023 MHz qui correspond bien à un signal GPS.

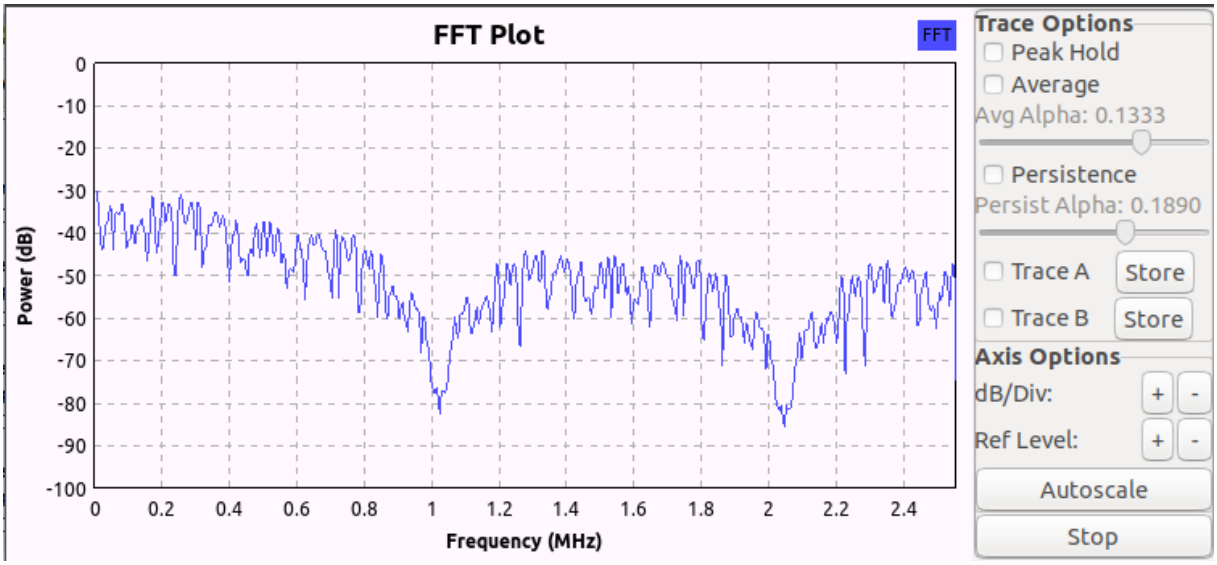

Figure III.21 : Spectre du signal émis.

III.9. Résultats obtenus :

Nos résultats de simulation sous leurrage sont illustrés par la série des figures (III-22), a, b, c, e, d, e, g, h, i. Ces figures prises par des imprimes écrans selon le temps indiqué au-dessus à droite. Sous leurrage avec un signal correspondant à la constellation authentique à l'addition de signaux erronés. La figure (III-22-a) montre que les satellites sont traités, il s'agit des PRN's : 02, 05, 13, 07, 09, 23, 16, 25, 06 et 30 cependant dans le canal d'acquisition on a plus de satellites disponibles, on note les PRN's : 32, 08 et 29. Quelques secondes plus tard, d'autres satellites apparaissent c'est les PRNs : 06, 14 et 03.

Après une minute de leurrage, Sur la figure (III-22-d), tous les satellites sont exploitables sur le diagramme de ciel, leurs niveaux de signal sont acceptables selon la figure (III-22-e). Une fois le spoofeur éteint, les satellites disparaissent progressivement de la carte du ciel ce qui est confirmé par les figures (III-22-f-g-h).

En clair, sans spoofeur le récepteur GPS du téléphone revient à son mode de fonctionnement normal, il fournit le diagramme du ciel présenté par la figure (III-22-i), en comparant avec la figure (III-22-d), on observe l'absence totale des deux satellites 16 et 29, qui existaient dans notre signal spoofeur.

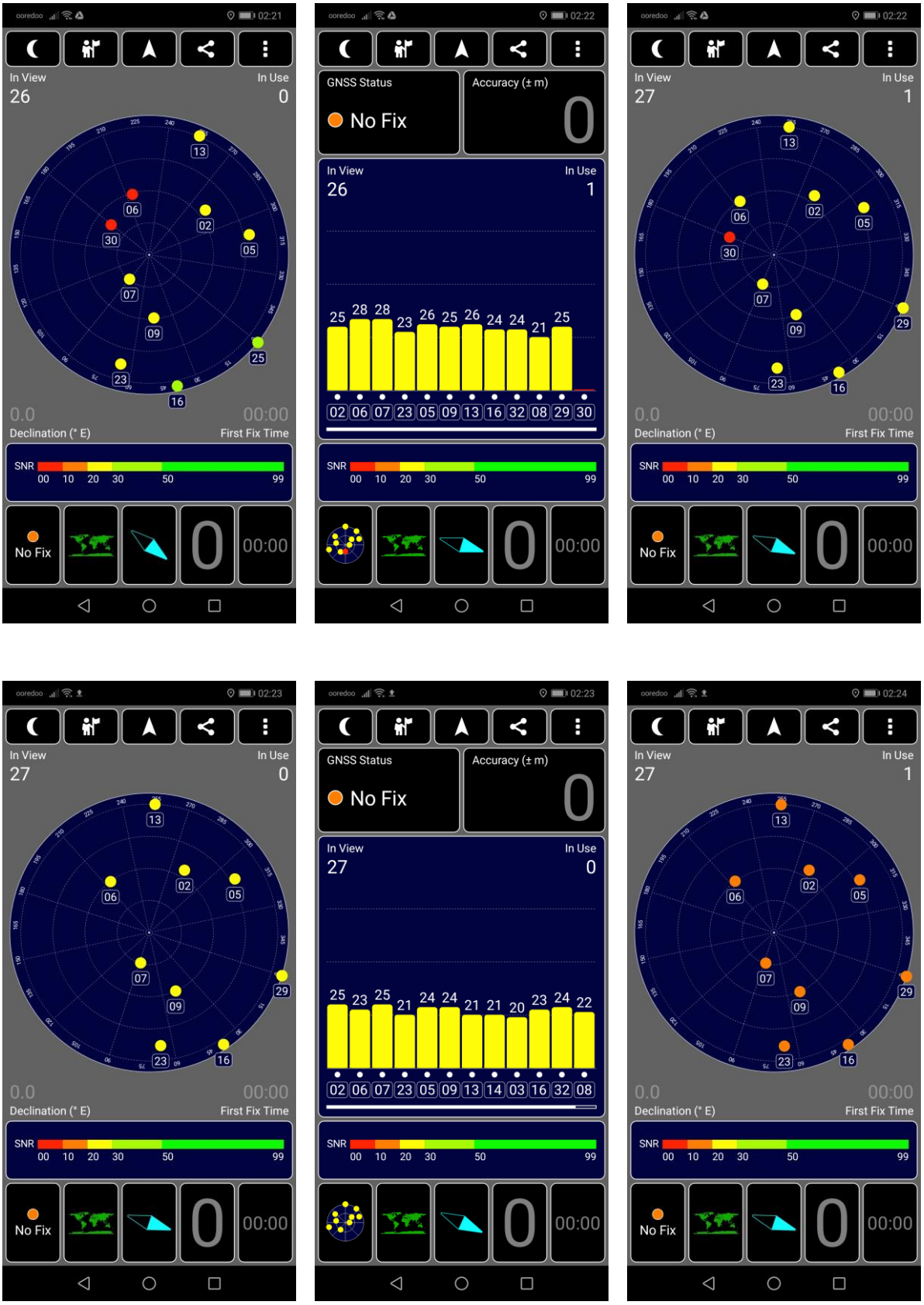

Figure III.22 : (de gauche à droite a-f): Situation sous leurrage.

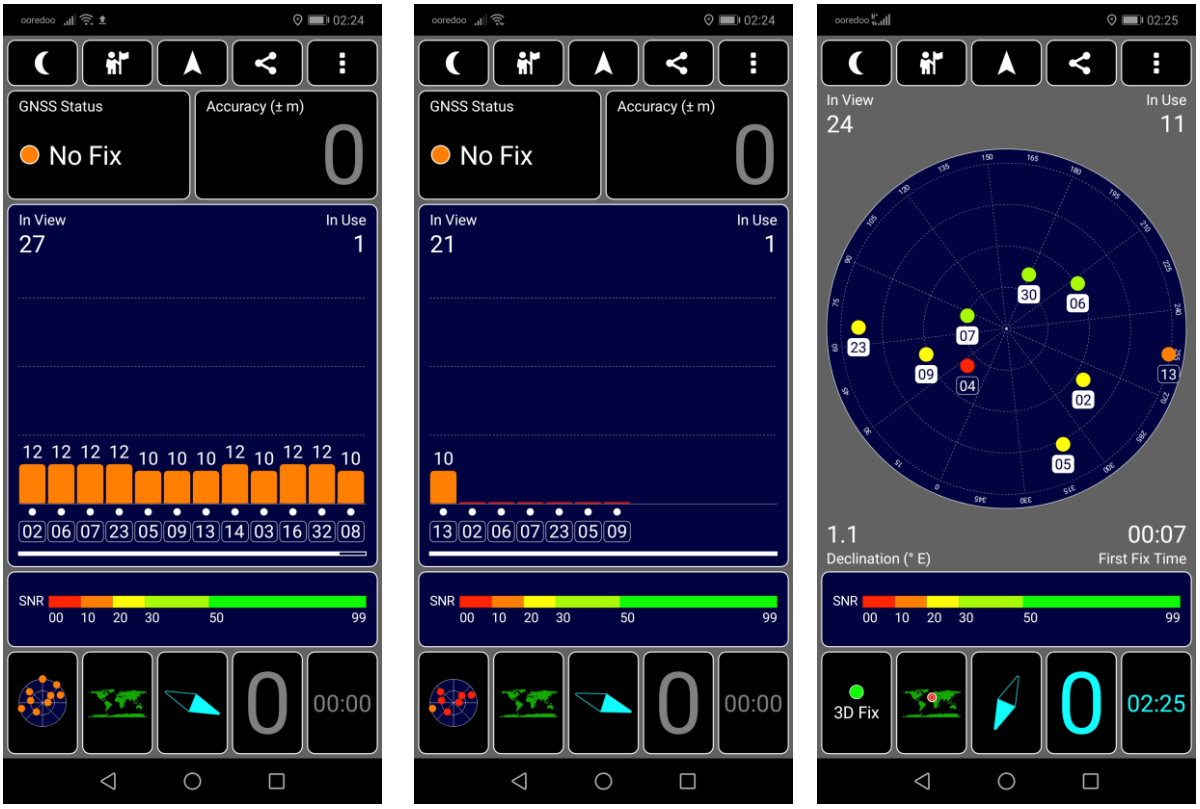

Figure III.22 (de gauche à droite g-h-i): Situation sous leurrage.

Il est à noter, que sous spoofeur, malgré le nombre suffisant des satellites présents, la position n'était pas calculée, l'information 'No fix' était visible contrairement au cas spoofeur absent. Ceci est dû à plusieurs explications, principalement :

- ✦ Des retards non maîtrisés de notre part concernant les 'TLM' ;
- ✦ Notre téléphone est doté d'une mémorisation de sa position GPS ;
- ✦ Un stockage des éphémérides dans la mémoire du téléphone dont il faut initialiser.

III.10. Conclusion :

Le signal GPS est vulnérable aux interférences dans sa bande en raison de sa faible puissance, une très faible interférence peut facilement le bloquer. Le leurrage est une interférence délibérée qui vise à contraindre les récepteurs GPS à générer de solutions de positionnement fausses.

L'attaque par leurrage est potentiellement beaucoup plus menaçante que le brouillage puisque le récepteur ne peut déceler cette menace et il fournit toujours une solution de positionnement qui semble fiable. La structure du signal GPS étant dans le domaine public, la mise en œuvre d'un spoofeur de capacité perturbatrice est possible.

Le simulateur de signal GPS transmet des signaux semblables à ceux du système GPS. Ces signaux ne sont pas essentiellement synchronisés avec la constellation GPS actuelle tandis que les spoofeurs encore plus sophistiqués exploitent des récepteurs qui se synchronisent d'abord avec les signaux authentiques.

L'élaboration d'un spoofeur, se trouve en face de plusieurs techniques d'anti-spoofing. Ces techniques sont plus ou moins complexes, dans le chapitre suivant on s'intéresse au :

- Contrôle du CNR ;

.

Chapitre IV

Techniques D'anti-Leurrage

- 1. Introduction
- 2. Détection et atténuation du leurrage
- 3. Détection du spoofeur par contrôle du *CNR*
- Conclusion

IV.1. Introduction :

De nos jours, diverses applications telles que la navigation et les systèmes d'atterrissage, réseaux de communication numériques, transactions boursières et beaucoup d'autres services dépendent des signaux GPS. Donc la sécurité de ces services devient de plus en plus importante. Cependant, lorsque les signaux deviennent extrêmement faibles lorsqu'ils atteignent la Terre, ils sont vulnérables aux interférences et différents types d'attaques présentées dans le chapitre précédent.

Ces signaux contrefaits peuvent induire le destinataire en erreur en lui signalant des résultats incorrects de position ou de temps, ce qui peut avoir des conséquences graves, par exemple, détournement d'un drone ou éloignement d'une frappe d'un missile guidé par GPS , blocage des réseaux de communication numériques…

C'est pour cette raison, ces dernières années, nombreuses techniques d'anti-leurrage ont été développées et des algorithmes pratiques combinent des techniques complémentaires pour générer une protection optimisée.

Dans ce chapitre, nous allons présenter en premier lieu l'architecture radiofréquence d'un récepteur GPS puis on cite les différentes techniques de la détection du leurrage d'une manière générale. En deuxième lieu, on étudie la technique d'antileurrage qui estime le rapport de puissance porteuse sur la densité spectrale de bruit '*CNR*' afin de le contrôler, elle concerne les spoufeur fournissant des signaux qui apparaissent par rapport au récepteur à des distances supérieures à un chip du code C/A utilisé (300 m).

IV.2. Détection et atténuation du leurrage :

Le leurrage est l'une des menaces de la sécurité des systèmes qui utilisent le GPS. Cette dernière décennie plusieurs techniques ont été développées dans le but de détecter ou détecter et réduire les effets du leurrage. [11] Chacune de ces techniques repose sur des caractéristiques spécifiques du signal composite traité, on distingue :

- *Techniques du traitement d'antenne :* Étant donné que la plupart des attaques de spoufeurs sont réalisées à l'aide d'une seule antenne émettrice, les méthodes de traitement d'antennes sont parfaitement adaptées pour détecter et atténuer le spoufeur en utilisant un traitement spatial. À l'aide d'antenne réseau, chaque antenne estime la *'DOA'* d'un satellite GPS. En comparant les informations de position de satellite transmises dans le message GPS à celles estimées, un spoofeur peut facilement être détecté et supprimé par la suite en utilisant des techniques de formation de faisceau.

- *Techniques liées au récepteur :* En tant que méthode de détection de pré-corrélation, la surveillance de l'AGC frontal du récepteur peut être utilisée comme indication d'une attaque par usurpation. Mais contrairement à la détection de brouillage, les méthodes de post-corrélation pour la détection du leurrage sont beaucoup plus adaptées ;

- *Techniques cryptographiques :* La falsification n'est possible que parce que la plupart des signaux GPS n'utilisent aucune protection cryptographique. Il n'y a pas de faiblesse signalée en matière de leurrage des signaux militaires, car ces derniers reposent sur des codes générés de manière cryptographique et des messages chiffrés. L'inconvénient est que le traitement de ces signaux très bien protégés nécessite des modules de sécurité spéciaux et une infrastructure clé.

Un bref résumé des techniques d'anti-leurrage, soulevé de la littérature, est présenté dans le tableau IV.1 suivant. On note que dans notre projet, on s'intéresse à deux méthodes de contrôle du CNR. [11]

Tableau IV.1 : Techniques d'Anti-Spoofing des récepteurs GPS.

Méthodes	Nécessite	Complexité	performance
Contrôle CNR	Estimation CNR	Faible	Alerte
Contrôle CAG	Sortie CAG	Faible	Alerte
Contrôle DOA	Antennes réseau	Haute	Atténuation
PANOVA	Antenne double	Haute	Détection
Réseau synthétique	Récepteur en mouvement	Faible	Atténuation
Contrôle cohérence Code / Phase	---	Faible	Détection
Contrôle éphémérides	---	Faible	Alerte
Contrôle horloge satellite	---	Faible	Alerte
Contrôle cohérence positions/récepteurs	Multi-récepteurs	Moyenne	Détection
Hybridation	Multiple systèmes de navigation	Haute	Détection
SQM	---	Faible	Détection

IV.3. Détection de présence du spoufeur par contrôle du CNR :

IV.3.1. Etage RF :

Le rôle principal du récepteur est de détecter puis délivrer le signal RF reçu au niveau de l'antenne au convertisseur ADC, tout en maintenant une qualité de signal " acceptable ". La sensibilité et la dynamique du récepteur sont les deux principaux paramètres qui définissent la marge de puissance d'entrée perçue par l'antenne. Alors que le taux d'erreur binaire et le taux d'erreur de symboles sont les mesures qui définissent la qualité acceptable du signal reçu. Actuellement, les récepteurs GPS repose sur ce qu'on qualifie de Radio Logicielle.

Le concept de la Radio Logicielle a été introduit par Mitola qui a proposé une architecture radio logicielle dite "idéale". Dans cette architecture, illustrée par la figure (IV.1), la conversion analogique numérique est directement effectuée après l'antenne, le filtre Radio Fréquence (RF) et l'amplification faible bruit du signal (LNA). Un processeur de traitement spécialisé (DSP) réalise alors les traitements numériques du signal. Dans la figure (IV.1), la partie numérique de l'architecture est encadrée en couleur mauve. Cependant, cette architecture exige une antenne à large bande et un convertisseur analogique numérique (ADC) ayant une fréquence d'échantillonnage importante. Dans le domaine du GNSS, ce type d'architecture n'est pas utilisé car la fréquence d'échantillonnage nécessaire est trop importante, d'où la proposition de la Radio Logicielle Restreinte. Il s'agit d'une topologie dérivée, donc c'est une approche au traitement de données radiofréquences déportant un maximum de traitement sur du logiciel au lieu de dépendre du matériel, [13]

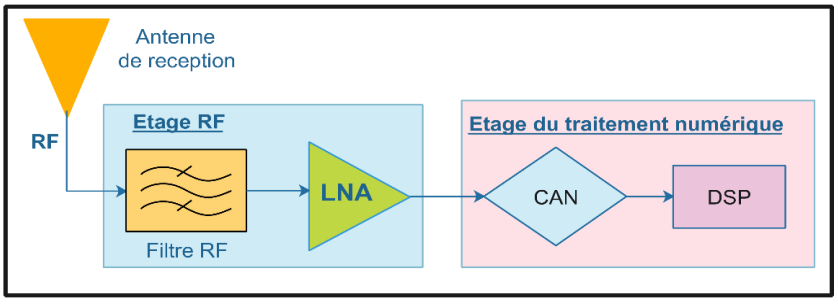

Figure IV.1 : Architecture Radio Logicielle (SR).

La structure de la Radio Logicielle Restreinte est illustrée par la figure (IV.2). Dans cette architecture, on identifie :

- *Le bloc "Analog Front-End"(AFE) :* Est composé de fonctions RF, de nature analogique. On y retrouve les composants nécessaires pour baisser la fréquence de

signal, tels que les filtres RF, amplificateurs et mélangeurs. Cette baisse est réalisée avec un ou plusieurs mélangeurs et des filtres de mise en forme du signal. L'objectif de ce bloc est de baisser la fréquence du signal à bande passante limitée, dans le but de faciliter son échantillonnage ;

- *Le bloc "Digital Back End" (DBE)* : Regroupe les composants qui réalisent les traitements numériques du signal. Selon sa fonction et du degré de flexibilité souhaité, de la vitesse de calcul et des contraintes logicielles, ce bloc peut être réalisé à base d'ASIC, de FPGA, de processeurs ou de processeurs spécialisés DSP ;

- *Le convertisseur ADC (CAN)* : fait le lien entre la partie Analogique et la partie numérique du "Front End".

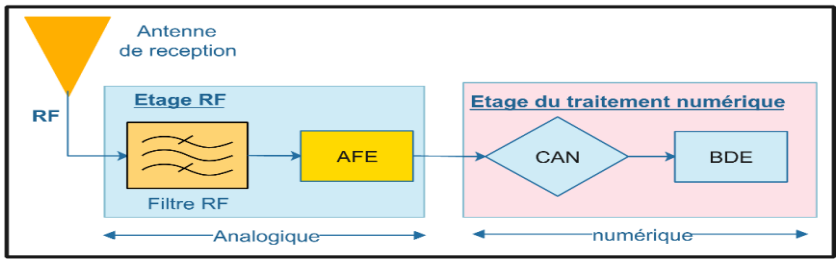

Figure IV.2 : Architecture SDR.

Généralement, la transposition de fréquence se réalise en deux étapes, on parle du traitement superhétérodyne. La figure (IV.3) présente l'architecture "Radio Fréquence" classique d'un récepteur GPS de types superhétérodyne telle quelle est adoptée par le constructeur "Accord Software".

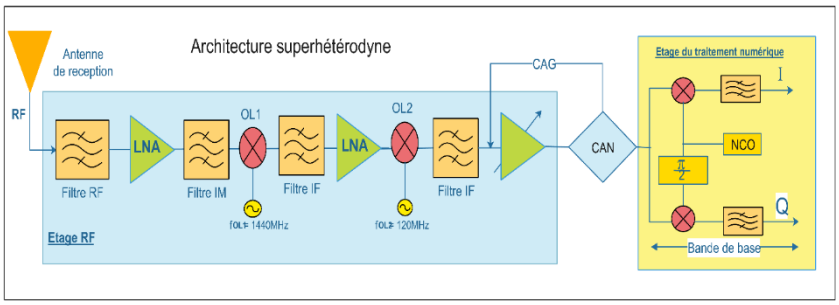

Figure IV.3 : Architecture superhétérodyne d'un récepteur GPS.

Dans cette architecture le signal est transposé deux fois en fréquences intermédiaires :

- Une première fois à la fréquence $f_1 = f_{L1} - f_{OL1} = 135.42$ MHz avec 1440MHz ;
- Une seconde fois à la fréquence $f_2 = f_1 - f_{OL2} = 15.42$ MHz avec $f_{OL2} = 120$MHz.

Le signal est alors sous-échantillonné à la fréquence $f_e = 20$ MHz et se retrouve en bande de base autour de la fréquence centrale $f_c = 4.58$ MHz.

Dans l'architecture illustrée par la figure (IV.3), on remarquera la présence d'un système de correction automatique du gain. L'objectif de ce système d'amplification contrôlée est de maintenir la dynamique du bruit en entrée du convertisseur analogique numérique, dans la plage de tension d'entrée de celui-ci. En effet le signal GPS étalé peut être considéré comme un bruit large bande dont la puissance est utilisée pour piloter la correction automatique de gain.

Dans un récepteur GPS la quantification du signal est réalisée sur un faible nombre d'éléments binaires. En effet l'information que contient le signal est principalement contenue dans les changements de signe du signal. Soit trois informations :

- Le rythme du signal renseigne sur la fréquence porteuse ;
- Les modifications de signe renseignent sur les sauts de π dans le signal ;
- Les transitions du signal binaire sont mélangées à la porteuse.

Dans ce contexte la quantification utilisée dans les récepteurs est souvent sur 1 ou 2 bits et sur un nombre supérieur dans les applications spécifiques nécessitant une analyse fine du signal pour lutter contre le brouillage à titre d'exemple.

IV.3.2. Les rapports *CNR* et *SNR :*

Les récepteurs GPS disposent d'une méthode permettant d'indiquer la puissance du signal des différents satellites qu'ils suivent. Généralement, ces récepteurs affichent l'intensité du signal sous forme de barres verticales, exprimant l'intensité du signal en terme de puissance porteuse sur la densité spectrale de bruit *CNR* ou en terme du rapport signal sur bruit *SNR*. Un exemple de cette présentation est illustré par la figure (IV.4). [13] [12]

Le *SNR* caractérise en général un signal analogique en bande de base, est utilisé pour la conception, l'évaluation et la vérification des performances d'un récepteur *GPS,* il est généralement exprimé en décibel. *SNR* fait référence au rapport entre la puissance du signal et la puissance du bruit dans une bande passante donnée, il est donné par :

$$SNR_{dB} = S - PN \qquad \text{(IV.1)}$$

Où :

S : est la puissance du signal, généralement la puissance porteuse exprimée en unités de décibel / milliwatt (dBm) ou décibel / watts (dBW) ;

PN : est la puissance de bruit dans une bande passante en unités de dBm.

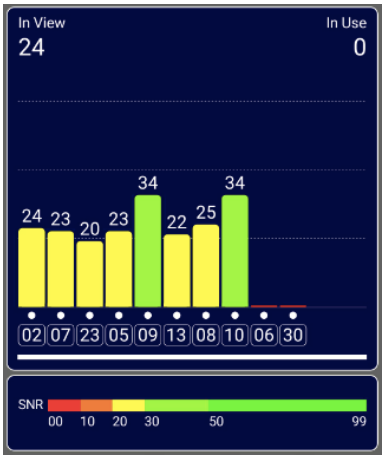

Figure (IV.4) : Intensité du signal (SNR).

Le *CNR* se réfère au rapport de la puissance porteuse au bruit par unités bande passante, il exprimé en décibel-Hertz (dB-Hz). Contrairement au *SNR*, *CNR* fournit une indication sur la puissance du signal reçu indépendamment des algorithmes d'acquisition, de poursuite du signal et de la bande passante de l'étage RF du récepteur. Pour un signal satellitaire et un étage RF d'un récepteur donné, la valeur du *CNR* varie suivant la configuration matérielle. Par exemple, l'utilisation d'un long câble d'antenne aura une incidence sur le rapport *CNR*. Cependant, ce rapport reste constant à travers les différentes étapes de traitement du signal du récepteur, comme la pré-détection (Pré-filtrage + amplification), l'acquisition et la poursuite. C'est pour cette raison que deux récepteurs différents, qui sont connectés à la même antenne et qui poursuivent le même satellite, délivrent la même valeur de *CNR*. Nous pouvons exprimer *CNR* comme suit :

$$\begin{aligned} CNR_{dB-Hz} &= C - (PN - B) \\ &= C - N_0 \end{aligned} \qquad \text{(IV-2)}$$

Par conséquent :

$$SNR = \left(\frac{C}{N_0}\right)/B \qquad \text{(IV-3)}$$

Où :

C : est la puissance de porteuse en dBm ou *dBW* ;

N : est la *puissance de bruit* en dBm ou *dBW* ;

N_0 *:* est la densité de puissance du bruit en *dBm-Hz* ou *dBW-Hz* ;

B : est la bande passante d'observation, qui est généralement la bande passante équivalente au bruit du dernier étage de filtrage dans le récepteur.

Afin de déterminer *CNR*, il faut clairement déterminer la puissance de la porteuse et la densité de bruit à l'entrée au récepteur. En ce qui concerne le bruit, on note qu'il est considéré thermique, Gaussien et blanc, sa densité de puissance N_0 est donnée par :

$$N_0(dBw/Hz) = 10.log_{10}(k.T) \quad \text{(IV-4)}$$

Où :

k : est la constante de Boltzmann $1{,}38.10^{-23}$ J / K ;

T : est la température de bruit en degrés sur l'échelle Kelvin.

La valeur typique N_0 correspond à une température ambiante de 290 °K, elle est donc de -204 dBW / Hz ou -174 dBm / Hz.

En ce qui concerne le signal, sa puissance qui est celle de sa porteuse, elle est donnée par :

$$P_r = P_e + G_e + G_r + 20.log(\lambda/4\pi R) \quad \text{(IV-5)}$$

Où :

P_r : est la puissance de la porteuse reçue ;

P_e : est la puissance de la porteuse émise ;

G_e : est le gain de l'antenne d'émission ;

G_r : est le gain de l'antenne du récepteur ;

λ: est la longueur d'onde ;

R : est la distance séparant l'émetteur du récepteur ;

On note que le dernier terme de l'équation (IV-5) définit les pertes de propagation en espace libre.

Pour le cas d'un récepteur GPS, La puissance porteuse nominale assurée à la réception est autour de -158 dBW, ce qui correspond à une valeur de CNR égale à 45 dB-Hz. Sachant la bande du récepteur qui est généralement de 2 MHz, la valeur du SNR est de -17 dB. Toutefois,

on note que ces valeurs de référence, considérées pour une distance moyenne récepteur-satellite de 20 000 Km, varient entre 35 à 50 dB-Hz pour *CNR* et de -28 à -13 pour *SNR*. Cela est fonction de l'angle d'élévation du satellite et par conséquent sa distance.

Au niveau traitement, la figure IV.5 illustre un exemple typique pour les changements du SNR fonction des différents étages du traitement du signal. Ceci pour une valeur de CNR égale à 45 dB-Hz.

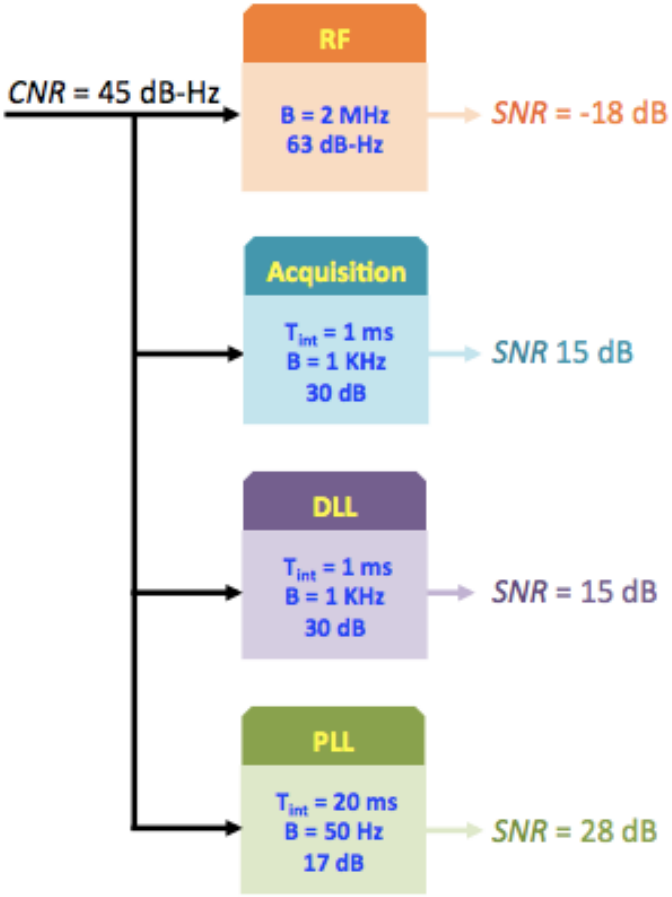

Figure IV.5 : Valeurs de SNR fonction des étages de traitement.

IV.3.3. Evaluation du *CNR :*

Afin de déceler la présence d'un leurrage, les récepteurs GPS exploitent le contrôle du *CNR* comme paramètre indicateur. Dans des conditions normales, la puissance du signal reçu change sans cesse suivant le mouvement du satellite aussi bien que selon le relief terrestre. Cependant, lorsqu'un signal spoofeur qui est généralement de puissance élevée, se présente, le *CNR* peut subir un changement soudain pouvant indiquer la présence d'un spoofeur. De plus, une analyse de cohérence entre le *CNR*, la distance et l'élévation peut être considérée comme indicateur supplémentaire.

On note que *CNR* qui nous intéresse est celui évalué à l'issu du canal corrélateur, c'est à dire pour une plage de valeurs qui adéquate au CAG ou aux étages dotés d'une saturation de puissance.

Pour évaluer *CNR*, nous considérons l'étage corrélateur d'un récepteur *GPS* illustré par la figure IV.6. Le signal reçu au niveau de l'antenne du récepteur est donné par :

$$r_{RF}(t) = \sum_{i=1}^{L} y_i(t) + \eta_{RF}(t) \qquad \text{(IV.6)}$$

L est le nombre de satellites visibles au récepteur, le signal est entaché de bruit Gaussien aditif $\eta_{RF}(t)$.

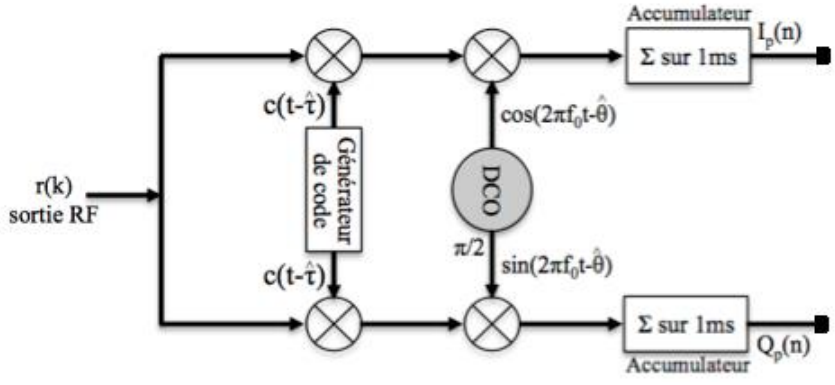

Figure IV. 6 : Corrélateurs pour voie en phase et en quadrature de phase.

Le signal GPS est donnée par la forme suivante :

$$y_i(t) = A_i e_i(t-\tau_i).d_i(t-\tau_i).cos[2\pi(f_{RF}+f_{di})t+\varphi_i] \quad \text{(IV.7)}$$

Où :

f_{RF} est la fréquence du signal GNSS ;

'τ_i' et '$f_{d,i}$' sont le code phase et la fréquence Doppler associés au signal reçu ;

φ_i est la phase du signal ;

e_i(t) contient les codes d'étalement, pour le signal GPS L1 il s'agit des codes *C/A* ;

d_i(t) représente les données de navigation.

On a aussi :

$$C = \frac{A^2}{2} \quad \text{(IV.8)}$$

Où :

C : est la puissance du signal ;

Le signal sera translaté en fréquence intermédiaire, en négligeant les effets du filtrage, le signal à la sortie de l'étage radio fréquence sera alors :

$$r_{RF}(t) = \sum_{i=1}^{L} A_i e_i(t-\tau_i).d_i(t-\tau_i).cos\left[2\pi\left(f_{IF}+f_{di}\right)t+\varphi_i\right]+\eta(t) \quad \text{(IV.9)}$$

Où : f_{IF} est la fréquence intermédiaire du récepteur GNSS, η(t) est le bruit filtré en étage intermédiaire. Le signal est ensuite échantillonné à la fréquence f_e, en négligeant les effets de la quantification, le signal sera de la forme :

$$r(nT_e) = \sum_{i=1}^{L} A_i e_i(nT_e-\tau_i).d_i(nT_e-\tau_i).cos\left[2\pi\left(f_{IF}+f_{di}\right)t+\varphi_i\right]+\eta_{IF}(nT_e) \quad \text{(IV.10)}$$

Pour la simplification, dans ce qui suit, nous adoptons la notation $x[n]=x(nT_e)$, 'T_e' étant la période d'échantillonnage, nous aurons ainsi :

$$r[n] = \sum_{i=1}^{L} A_i e_i \left[n - \frac{\tau_i}{T_e}\right] . d_i \left[n - \frac{\tau_i}{T_e}\right] . cos \left[2\pi \frac{(f_{IF} + f_{di})}{f_e} t + \varphi_i\right] + \eta_{IF}[n] \qquad \text{(IV.11)}$$

Les codes d'étalement des signaux GPS possèdent des propriétés d'orthogonalité, ils peuvent alors être traités individuellement par le récepteur, nous pouvons considérer le signal reçu à partir d'un satellite :

$$r[n] = Ae_i[n - \tau_0] . d_i[n - \tau_0] . cos[2\pi F_D n + \varphi] + \eta_{IF}[n] \qquad \text{(IV.12)}$$

Dans cette équation, $F_D=(f_{IF}+f_{d,i})/fe$ et $\tau_0=\tau_r/T_e$. $\eta_{if}[n]$ est un bruit Gaussien centré discrétisé à la fréquence 'f_e' de densité spectrale de puissance 'N_0' et variance $\sigma_{If}^2 = N_0 B_{IF}$. B_{IF} est la bande passante après l'étage radio fréquence. Il est souvent préférable de choisir la fréquence d'échantillonnage $f_e = B_{IF}$. En normalisant la puissance du bruit, on peut réécrire *r[n]* selon :

$$r[n] = \sqrt{\frac{2C}{N_0 f_e}} e_i[n - \tau_0] . d_i[n - \tau_0] . cos[2\pi F_D n + \varphi] + \eta_{IF.1}[n] \qquad \text{(IV.13)}$$

Les deux composantes I_p et Q_P sont regroupées dans l'expression suivante :

$$R_c(\hat{\tau}_i, \hat{f}_{di}) = \frac{1}{N} \sum_{n=0}^{N-1} r(n) . c_i(n - \hat{\tau}_i) . e^{-j2\pi \hat{f}_{di} n} \qquad \text{(IV.14)}$$

En considérant un canal à bruit additif Gaussien et à la présence du signal utile aligné, le signal composite est de nature aléatoire de densité Gaussienne. Par conséquent après corrélation les deux composantes en phase et en quadrature possèdent les moyennes suivantes :

$$
\begin{aligned}
E\left[I_p\left(\hat{\tau},\hat{f}_D\right)\right] &= E\left[\frac{1}{N}\sum_{n=0}^{N-1} r[n]\,.\,c[n-\hat{\tau}].\cos\left(2\pi\hat{f}_D n\right)\right] \\
&= \frac{1}{N}\sum_{n=0}^{N-1} E\left[y[n]+\eta_{IF}[n]\right].c[n-\hat{\tau}].cos\left(2\pi\hat{f}_D n\right) \\
&= \frac{1}{N}\sum_{n=0}^{N-1}\sqrt{\frac{2C}{N_0 f_e}}e_i[n-\tau_i].c_i[n-\tau_i].cos\left[2\pi f_{i,D} n+\varphi\right].c[n-\hat{\tau}].cos\left(2\pi\hat{f}_{i,D} n\right) \\
&= \sqrt{\frac{C}{2N_0 f_e}}\frac{1}{N}\sum_{n=0}^{N-1}\left[cos(\varphi_i)+cos\left(4\pi\hat{f}_{i,D}+\varphi_i\right)\right] \\
&= \sqrt{\frac{C}{2N_0 f_e}}cos(\varphi_i)
\end{aligned}
\qquad \text{(IV.15)}
$$

De même, on démontre que pour la variable en quadrature :

$$
E\left[Q_p\left(\hat{\tau},\hat{f}_D\right)\right] = \sqrt{\frac{C}{2N_0 f_e}}sin(\varphi_i) \qquad \text{(IV.16)}
$$

Leurs variances sont données comme suit :

$$
\begin{aligned}
Var\left[I_p\left(\hat{\tau},\hat{f}_D\right)\right] &= Var\left[Re\left\{\frac{1}{N}\sum_{n=0}^{N-1} r[n]\,.\,c_i[n-\hat{\tau}_i].\,e^{-j2\pi\hat{f}_D n}\right\}\right] \\
&= Var\left[\frac{1}{N}\sum_{n=0}^{N-1} r[n]\,.\,c_i[n-\hat{\tau}_i].\cos\left(2\pi\hat{f}_D n\right)\right] \\
&= \frac{1}{N^2}\sum_{n=0}^{N-1} Var\left[r(n).c[n-\hat{\tau}_i].\cos\left(2\pi\hat{f}_D n\right)\right] \\
&= \frac{1}{N^2}\sum_{n=0}^{N-1}\frac{\sigma_{IF}^2}{2} = \frac{\sigma_{IF}^2}{2N} = \frac{1}{2N}
\end{aligned}
\qquad \text{(IV.17)}
$$

De même pour la composante en quadrature, nous aurons :

$$Var\left[Q_p(\hat{\tau},\hat{f}_D)\right] = Var\left[I_p(\hat{\tau},\hat{f}_D)\right] = \frac{1}{N^2}\sum_{n=0}^{N-1}\frac{\sigma_{IF}^2}{2} = \frac{\sigma_{IF}^2}{2N} = \frac{1}{2N} \quad \text{(IV.18)}$$

Suite à ces démonstrations, on peut résumer que les deux voies en phase et en quadrature de phase sont distribuées selon :

$$\begin{cases} I_p : N\left(\sqrt{\frac{C}{2N_0 f_e}}cos(\varphi_i), \frac{1}{2N}\right) \\ Q_p : N\left(\sqrt{\frac{C}{2N_0 f_e}}sin(\varphi_i), \frac{1}{2N}\right) \end{cases} \quad \text{(IV.19)}$$

En analysant cette dernière équation (IV .19), on peut exprimer la valeur de *CNR* à partir de la composante I_P comme suit :

$$CNR = \frac{C}{N_0} = \frac{1}{T_{\text{int}}}.\frac{\left(E\left(I_p\right)\right)^2}{V\left(I_p\right)} \quad \text{(IV.20)}$$

Avec : T_{int} est le temps d'intégration cohérente donné par :

$$T_{\text{int}} = \frac{N}{f_e} \quad \text{(IV.21)}$$

Nous pouvons alors conclure que c'est la statique de I_P qui permet d'observer le *CNR*.

IV.3.4. Méthodes d'estimation du *CNR :*

On a démontré que *CNR* peut être estimé d'une manière statistique. Dans ce contexte, plusieurs estimateurs ont été proposés dans la littérature, développés initialement pour servir le domaine des communications numériques puis adaptés au domaine du traitement de signal *GPS*. Parmi ces estimateurs, on peut citer **:**

- La méthode signal réel – bruit complexe (Real Signal-Complex Noise - RSCN) ;
- La méthode variance signal à bruit (Signal-to-Noise Variance - SNV) ;
- La méthode de Beaulieu (Beaulieu's method - BL) ;

Ces méthodes sont proposées en considérant la fonction de corrélation donnée par l'équation (IV.14). On note que cette fonction est complexe car elle est issue de la combinaison des deux voies en phase et en quadrature de phase aux instants *k*.

On définit un estimateur de la puissance totale du signal après corrélation par :

$$\hat{P}_{Tot} = \frac{1}{N}\sum_{k=1}^{N}|R(k)|^2 \qquad \text{(IV.22)}$$

Ou de même :

$$\hat{P}_{Tot} = \frac{1}{N}\sum_{k=1}^{N}|R^{Re}(k)|^2 + \frac{1}{N}\sum_{k=1}^{N}|R^{Im}(k)|^2 \qquad \text{(IV.23)}$$

Et un estimateur de la puissance du bruit tel que :

$$\hat{P}_b = \frac{1}{N}\sum_{k=1}^{N}\left(R^{Im}(k)\right)^2 \qquad \text{(IV.24)}$$

IV.3.4.1. Estimateur *RSCN :*

L'idée principale de cet estimateur est de supposer que la distribution du bruit est identique sur la voie en phase I_p et sur la voie en quadrature de phase Q_p. L'estimateur RSCN utilise la composante imaginaire de la corrélation pour estimer la puissance du bruit.

Cet estimateur tire profit de la ressemblance des distributions du bruit dans les deux voies I_p et Q_p. Par conséquent, l'estimation du bruit peut être réalisée uniquement sur la voie Q_p. L'expression de cet estimateur est donnée par :

$$\widehat{CNR} = \frac{1}{T_{int}}\frac{\hat{P}_{Tot}/_2 - \hat{P}_b}{\hat{P}_b} \qquad \text{(IV.25)}$$

On observe qu'il s'agit d'un estimateur simple, mais très sensible au changement de la phase résiduelle 'j_i'. En effet, dès l'apparition d'une erreur de phase, la puissance du signal se partage entre les deux voies en phase I_p et en quadrature de phase Q_p, ce qui induit une diminution du CNR estimé.

IV.3.4.2. Estimation *SNV :*

Il s'agit d'une méthode pour les modulations BPSK, dérivée de l'estimation par le maximum de vraisemblance (Maximum Likelihood) qui elle est dédiée aux modulations QPSK introduite en 1966 par Gilchriest. Elle est également connue comme la methode de synthèse des variances. La puissance du signal est estimée en utilisant :

$$\hat{P}_s = \left(\frac{1}{N} \sum_{k=1}^{N} R^{Re}(k) \right)^2 \tag{IV.26}$$

Tandis que l'estimation du CNR est donnée par :

$$\widehat{CNR} = \frac{1}{T_{int}} \frac{\hat{P}_s}{\hat{P}_b} = \frac{1}{T_{int}} \frac{\hat{P}_s}{\hat{P}_{Tot} - \hat{P}_s} \tag{IV.27}$$

Encore, il s'agit d'une méthode sensible au changement de la phase résiduelle « φ_i ». Cet estimateur est faible en biais, mais qui existe quand même pour les faibles puissances, celui-ci est lié à l'estimateur quadratique de $\hat{P}_s$.

IV.3.4.3. Estimation *BL :*

Cette methode est motivé par une formulation intuitive des estimateurs de la puissance du signal et celle du bruit

Dans cet estimateur, on utilise uniquement la voie en phase *Ip*. L'estimation de la puissance du signal est donnée par :

$$\hat{P}_s = \frac{1}{2} \left(\left(R^{Re}(k) \right)^2 + \left(R^{Re}(k-1) \right)^2 \right) \tag{IV.28}$$

Cependant, l'estimation de la puissance du bruit est :

$$\hat{P}_b = \left(R^{Re}(k) - R^{Re}(k-1) \right)^2 \tag{IV.29}$$

Où l'estimateur $\hat{P}_s$ donne une meilleure approximation de la puissance du signal P_s quand la puissance du bruit est moins importante et donc l'affecte le moins possible alors que l'estimateur $\hat{P}_b$ approxime la puissance totale du bruit P_b pour une modulation BPSK qui est utilisée dans les données GNSS. Donc, le bruit est présent sur la sortie Q_p alors que l'estimation

de P_s se fait uniquement sur la sortie I_p cela donne que l'effet du bruit pour cet estimateur est significativement inferieur à celle du signal. L'estimateur du *CNR* est donné par :

$$\widehat{CNR} = \frac{1}{T_{int}}\left[\frac{1}{N}\sum_{k=1}^{N}\frac{\hat{P}_b}{\hat{P}_s}\right]^{-1} \quad \text{(IV.30)}$$

IV.3.5. Comparaison des estimateurs :

Afin d'évaluer la performance des différents estimateurs, on a simulé le synoptique illustré par figure (IV.6). Ceci est réalisé en utilisant un code *C/A PRN1* d'une durée de 1ms sous une fréquence d'échantillonnage de 1.023 MHz et pour différentes valeurs de *CNR*.

Nos résultats obtenus pour le cas d'une phase résiduelle « φ_i » nulle sont illustrés par la figure (IV-7) ci-dessous. On observe que les estimateurs présentés convergent vers les vraies valeurs sans aucun biais pour le cas des CNR forts. Cependant, aux faibles CNR, des biais différents apparaissent. Dans cette plage de valeurs du CNR, on constate que l'estimation '*SNV'* présente la meilleure performance, contrairement à l'estimation par la méthode de '*Beaulieu*' qui présente la plus mauvaise.

Les deux figures (IV-8) et (IV-9), sont obtenues pour les cas où « φ_i =30° » et « φ_i =60° » respectivement. On observe que la méthode de '*Beaulieu*' résiste mieux à l'apparition de phase résiduelle en comparant avec les deux autres méthodes.

Finalement, La figure (IV-10) correspond au cas où « φ_i =90° », c'est à dire au cas où le signal se trouve uniquement sur la voie en quadrature de phase. On observe que les méthodes présentées ont échoué à estimer correctement le *CNR*. Un résultat attendu vu les expressions utilisées.

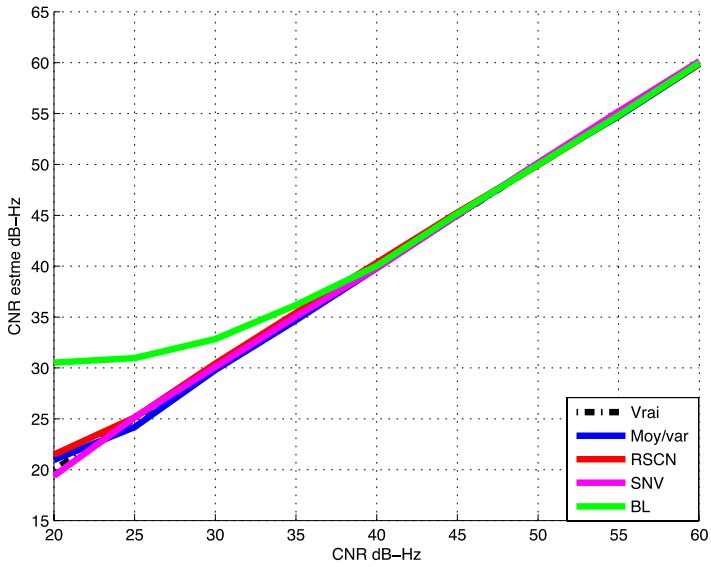

Figure IV.7 : Valeurs du *CNR* obtenues par les différents estimateurs, φ_i =0°.

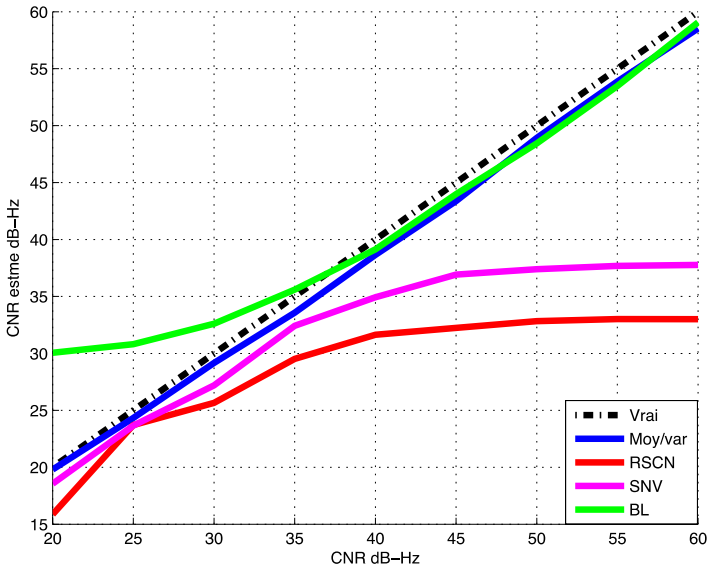

Figure IV.8 : Valeurs du *CNR* obtenues par les différents estimateurs, φ_i =30°.

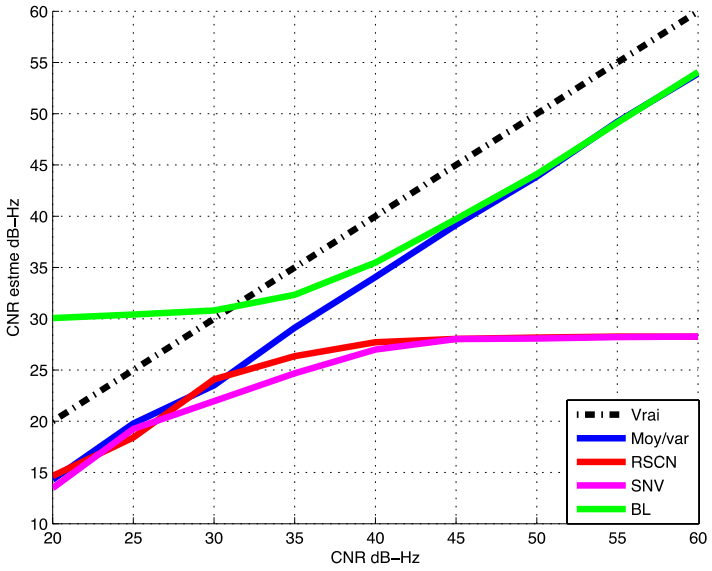

Figure IV.9 : Valeurs du *CNR* obtenues par les différents estimateurs, φ_i =60°.

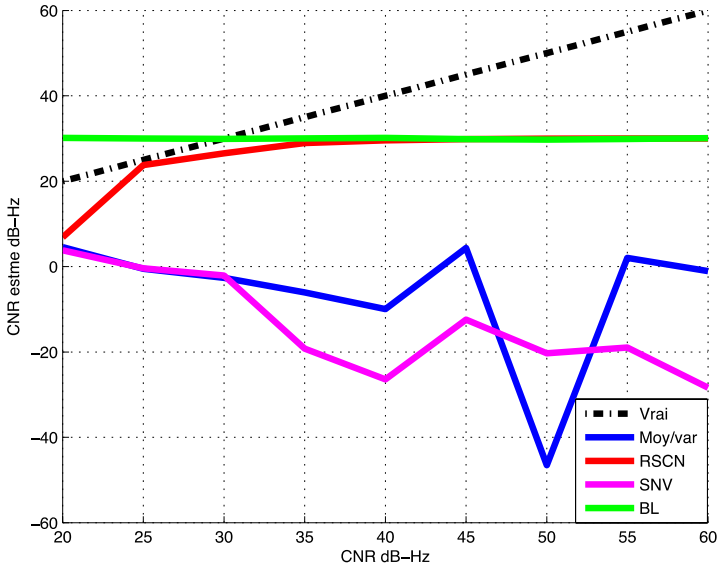

Figure IV.10 : Valeurs du *CNR* obtenues par les différents estimateurs, φ_i =90°

IV.3.6. Vérification de cohérence du *CNR :*

Une fois le *CNR* est estimé, le récepteur GPS peut d'un moment à l'autre vérifier sa cohérence vis-à-vis plusieurs paramètres, on s'intéresse à :

- Les distances satellites – récepteur ;
- L'élévation des satellites.

En utilisant notre simulateur présenté en deuxième chapitre, nous nous sommes intéressés au scénario illustré par la figure (IV-11) et dont les données relatives sont présentées par le tableau (IV-2) ci-dessous.

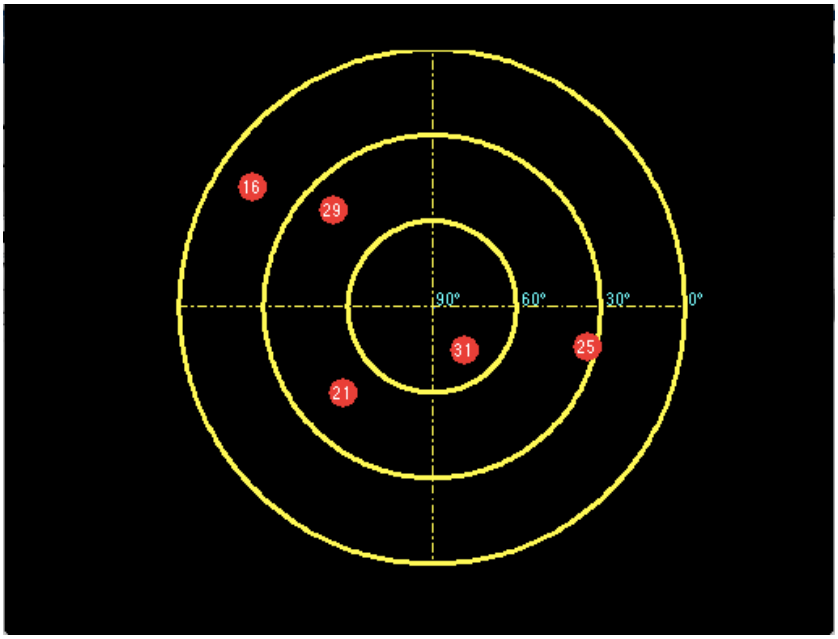

Figure IV.11 : Diagramme du ciel.

Tableau IV.2 : Les paramètres réels du scénario.

PRN	29	25	21	31
Elévation (deg)	41°	32°	46°	71°
Azimute (deg)	315°	104°	222°	156°
Distance (km)	23723	23016	20269	19467
Doppler (kHz)	3.75	-5.10	3.46	-2.51
CNR (dB-Hz)	46	53	59	60

A travers les valeurs présentées dans le tableau et qui sont évaluées au niveau du récepteur à chaque époque, on peut identifier quelques incohérences liées à la présence d'un spoufeur. A titre d'exemple, sachant que *CNR* est inversement proportionnel à la distance, par conséquent en comparant les données issues de deux satellites et on trouve que le plus éloigné possède le plus grand *CNR*, alors dans ce cas on émet une alerte concernant le risque d'avoir un spoufeur. Cette situation s'applique aussi sur le contrôle de l'angle d'élévation du satellite, une valeur qui est proportionnelle au *CNR*.

Dans la figure (IV.12), on a tracé le *CNR* estimé en fonction de la distance pour les quatre satellites considérés, cela pour les deux situations absence et présence du spoufeur. Dans la première situation, il est clair que la courbe décroissante obtenue exprime une relation cohérente entre les distances et les *CNR* correspondants. Cependant le cas avec spoufeur présente une incohérence visible, elle est décelée par un simple détecteur de signe de pente sur cette courbe.

De même, dans la figure (IV.13), on a tracé le *CNR* estimé cette fois en fonction de l'élévation pour les quatre satellites considérés, cela aussi pour les deux situations absence et présence du spoufeur. Pour la première situation, la courbe est croissante ce qui est cohérent contrairement au deuxième cas où la courbe est en partie décroissante, il s'agit d'une indication liée à la présence du spoufeur.

Dans la figure (IV.14), on a présenté les différentes valeurs du *CNR* obtenues pour les quatre satellites en absence du spoufeur. Cependant la figure (IV.15) présente le cas en présence du spoufeur. En analysant cette dernière figure on peut tirer les observations suivantes :

- Le *PRN 21* présente des variations cohérentes du *CNR* ;
- Le *PRN 25 a* subit une diminution du *CNR* alors qu'il est en rapprochement vers le récepteur vu son Doppler négatif ;
- Le *PRN 29* présente aussi une incohérence ;
- Le *PRN 31* présente aussi une incohérence.

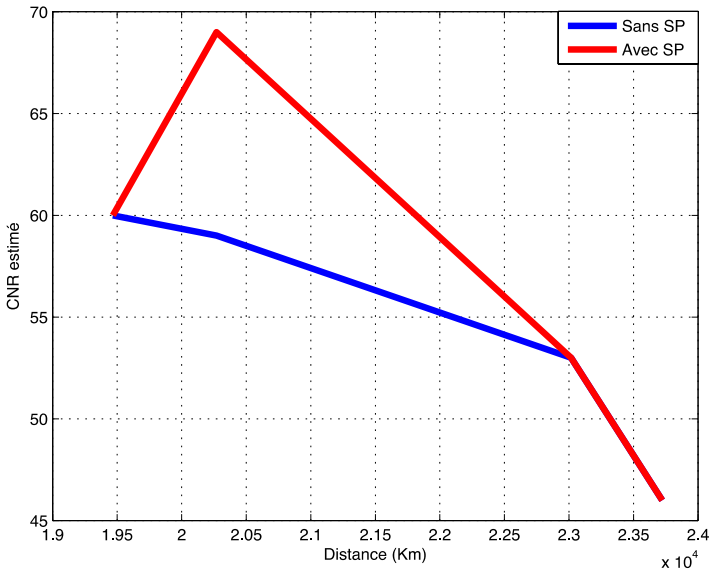

Figure IV.12: Courbe du *CNR* estimé en fonction de la distance.

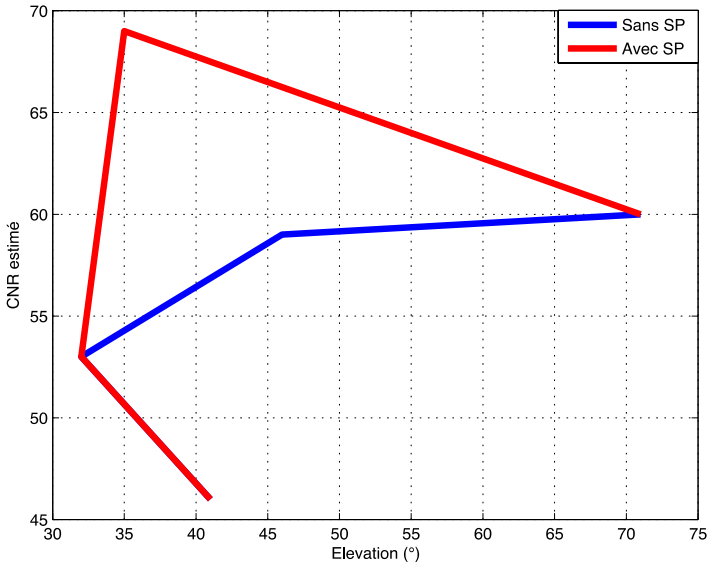

Figure IV.13: Courbe du *CNR* estimé en fonction de l'élévation.

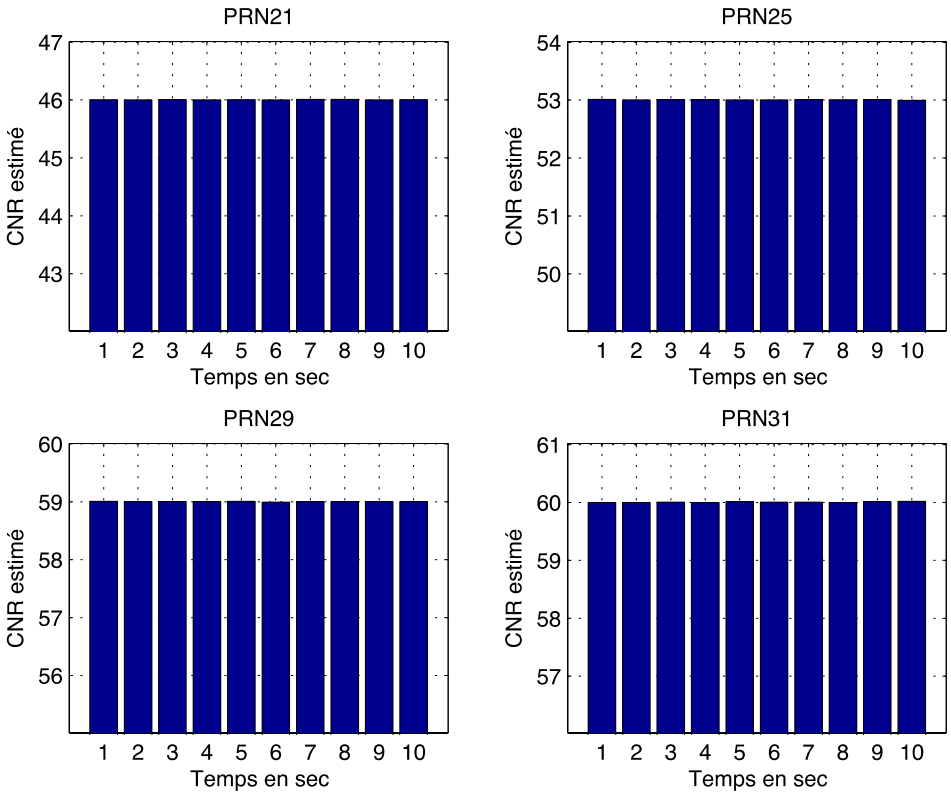

Figure IV.14: *CNR* en absence du spoofeur.

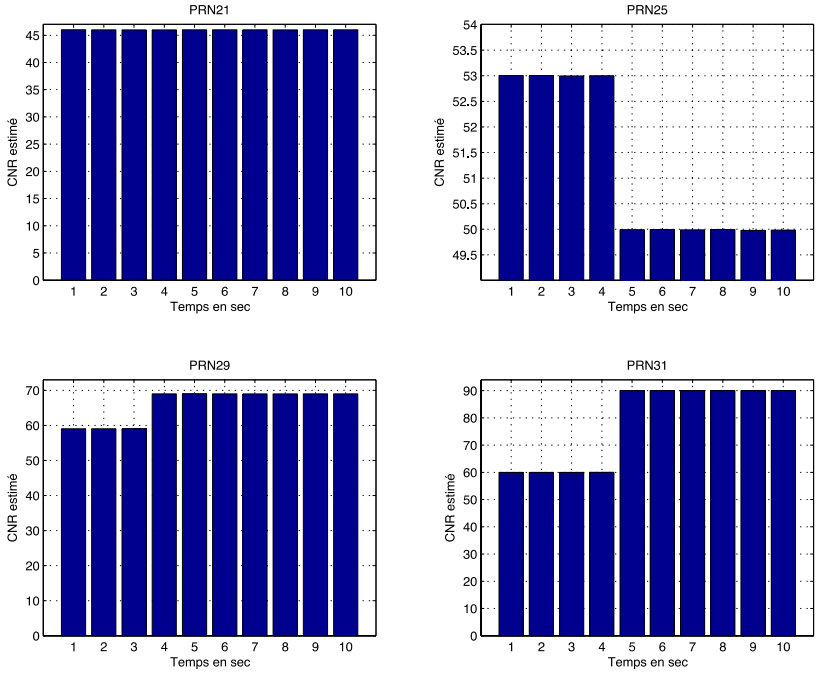

Figure IV.15: *CNR* en présence du spoofeur.

IV.4. Conclusion :

Nous sommes arrivés à un temps où tout est dépendant de notre position est donc inévitablement des signaux GPS. Cette dépendance met en valeur son utilité dans notre vie de tous les jours car sa vulnérabilité aura des conséquences lourdes qui nous affectent. Pour s'en protéger il est impératif de trouver des solutions de sécurité contre les brouilleurs et les spoofeur, dont le développement est très rapide, qui peuvent être utilisés pour nuire aux utilisateurs.

Afin de parvenir à cela, l'élaboration de techniques d'alerte de présence ou non de spoofeur est importante. Parmi ces nombreuses techniques on s'est intéressé dans cette étude à celle du contrôle du CNR.

Pour cela, nous avons étudié les différentes méthodes du contrôle du CNR, à savoir :

- **RSCN :** signal réel bruit complexe
- **SNV :** variance signal/bruit
- **BL :** méthode de Beaulieu

Ces méthodes nous ont permis de faire une estimation du $\widehat{CNR}$ puis comparées entre elles à différents déphasages pour tracer leur différentes courbes de $\widehat{CNR}$ estimé en fonction du CNR réel, afin de déterminer laquelle est la mieux adaptée. On interprète nos résultats du meilleur estimateur pour chaque phase résiduelle dans ce tableau :

déphasage	0°	30°	60°	90°
Estimation la plus proche	SNV	BL	BL	Echec de toutes les techniques

On remarque donc que pour un déphasage de 90° toutes les techniques échouent à estimer le CNR ceci parce que le signal se trouve seulement sur la voie en quadrature de phase alors que les estimateurs utilisés ont été basé uniquement sur la voie en phase.

De ce fait en obtenant la bonne estimation $\widehat{CNR}$ va permettre de vérifier la cohérence du CNR par :

- Analyse de la courbe $\widehat{CNR}$ en fonction de la distance sat/rec qui a une relation inversement proportionnelle (plus la distance augmente plus le CNR diminue) qui mène à dire en cas d'incohérence qu'il y'a un possible spoofeur
- Analyse de la courbe $\widehat{CNR}$ en fonction de l'angle d'élévation des satellites par rapport au récepteur (plus l'angle d'élévation diminue ce qui insinue que la distance sat/rec augmente plus le CNR diminue par conséquence) ce qui aussi laisse à croire à la possible présence d'un spoofeur.

Conclusion générale

En évoluant l'homme a réussi à perfectionner la façon de se positionner dans son environnement, depuis l'utilisation de pierres, arbres et autres reliefs qui l'entourent ainsi que l'orientation par les étoiles et le soleil, ce dont il s'est inspiré pour concevoir le Système de Positionnement Global (GPS). Le GPS est passé par d'innombrables phases de développement qui ont mené à sa version actuelle, celle-ci menacé de jour en jour par l'évolution très rapide de systèmes plus compliqués les uns que les autres tel que les Brouilleurs et les Spoofeurs considérés dans notre étude.

Dans ce projet, nous avons présenté des généralités sur le GPS pour mettre le point sur ses vulnérabilités essentiellement à cause de sa faible puissance ainsi que la connaissance publique des différentes parties de son signal GPS. Les menaces qui touchent la sécurité d'une mesure fournie par le GPS pourraient se produire soit au niveau du traitement de signal soit en traitement de données. Les menaces proviennent généralement des :

- Brouilleurs : la fonction d'un brouilleur consiste à émettre des signaux dans la même bande de fréquence des signaux GPS, vu leur faible puissance, pour les noyer et éviter à l'utilisateur d'en extraire les données désirées.
- spoofeurs : le but d'un spoofeur est de leurrer un récepteur en imitant des signaux GPS connus du point de vue de leurs structures, afin de le mener à calculer les faux paramètres PVT proposés par la personne effectuant le leurrage. Ainsi nous avons injecté nos données erronées puis émis vers le récepteur, selon différents grades de difficultés.

Après avoir pris connaissance de ces techniques, nous avons simulé nos propres signaux pour les deux menaces (brouillage et spoofing), les résultats ont été illustrés dans le chapitre III comme suit :

- Brouillage : avant la simulation le récepteur affichait parfaitement l'apparition des satellites GPS visibles en temps réel. Après simulation nous avons remarqué que les satellites disparaissent un à un et leurs signaux à faible puissance étaient totalement noyés par notre signal de brouillage.

- Leurrage (Spoofing) : le récepteur parvient à détecter les satellites visibles et à calculer les paramètres PVT de façon régulière. Avant d'émettre nos signaux générés à partir des données du fichier Rinex sous MATLAB, nous avons eu recours au brouillage pour éviter que notre spoofeur ne soit détecté (ou choisir un endroit ou la réception GPS est médiocre). En lançant l'émission de notre signal grâce au HackRF One et a l'interface GNU Radio, on remarque l'apparition des satellites dont les codes sont ceux que nous avons utilisé. Par la suite le calcul de PVT se fait sur le récepteur et la position suggérée est affiché. Donc le leurrage a été réalisé avec succès.

En dernière partie, nous avons proposé des techniques pour détecter la présence d'un spoofeur pour s'en protéger, nous avons opté dans ce travail pour la technique de contrôle du CNR elle est basée sur l'estimation des paramètres qui aboutissent au $\widehat{CNR}$. Dans ce cadre, les méthodes d'estimation suivantes ont été employées :

- RSCN : signal réel bruit complexe
- SNV : variance signal/bruit
- BL : la méthode de Beaulieu

Pour chaque méthode, nous avons tracé les courbes du $\widehat{CNR}$ en fonction du vrai CNR pour des déphasages différents ($\varphi = 0°, 30°, 60°, 90°$) pour déterminer l'estimation la plus proche et donc la méthode la plus efficace, dont on s'en-tire avec la conclusion que la méthode SNV donne une estimation sans biais pour un déphasage nul, tandis que la methode de BL se trouve etre la meilleure pour $\varphi_i \neq 0°$ sauf pour un déphasage de 90° toutes les estimations échouent a évaluer le CNR.

L'estimation du $\widehat{CNR}$nous a permis de détecter une éventuelle présence d'un spoofeur, et ce en observant la cohérence du $\widehat{CNR}$ par rapport à :

- La distance : en ayant connaissance que la puissance est atténuée si la distance augmente on a eu à tracer la courbe du $\widehat{CNR}$ en fonction de celle-ci, de laquelle on conclue la possible présence d'un spoofeur si on remarque une pente négative à cette courbe.
- L'angle d'élévation : la diminution de cet angle indique que la distance du satellite est grande, et donc le $\widehat{CNR}$ diminue. On arrive par cela à conclure que la possibilité de présence d'un spoofeur est affectée à une pente négative de cette courbe.

Les résultats obtenus par la technique de contrôle du CNR permettent de détecter la présence d'un spoofeur, cependant, elle permet seulement à la détection du Leurrage (spoofing) et non à l'atténuer.

Nous proposons par ailleurs, pour de futurs travaux, l'étude des techniques permettant d'atténuer ou d'annuler l'influence d'un spoofeur, mentionnées dans le chapitre IV, elles nécessitent une étude plus approfondie et dont la réalisation requière des maitrises, connaissances et matériels bien plus élaborés.

REFERENCES BIBLIOGRAPHIQUES

[01]. El-Rabbany.A, "Introduction to GPS: The Global Positioning System", Artech House, ISBN 1-58053-183-0, 2002.

[02]. Peter J.G.Teunissen, Oliver Montenburk (Eds), " Handbook of Global Navigation Satellite system", Springer, e-ISBN: 978-3-319-42928-1, 2017.

[03]. G.S.Rao, "Global Navigation Satellite System with essentials of satellite communication", Tata McGraw- Hill, ISBN: 978-0-07-070029-1, 2010.

[04]. "The Almanac, Orbit Data and Resources on Active GNSS Satellites", GPS World, August 2015.

[05]. Steven C, Fisher and Kamran Ghassemi, " GPS IIIF- The Next Generation", Proceedings Of The IEEE, Vol. 87, No. 1, January 1999.

[06]. https://www.gps.gov/

[07]. Col Matthew Smitham, "Global Positioning Systems Directorate", GPS Program Update to ION GNSS, 10 September 2014.

[08]. Hofmann-Wellenhof Lichtenegger Wasle, " GNSS, Global Navigation Satellite Systems, GPS, Glonass, Galileo & more", Springer Wien New York, ISBN 978-3-211-73012-6, 2008.

[09]. Galileo Initial Services, European Commission - Fact Sheet, , Brussels, 14 December 2016.

[10]. Global Navigation Satellite System (GNSS) Manual, Second Edition, ICAO Doc 9849, June 2012.

[11]. Joeao Pedro Duque Duarte, "Integrity Monitoring Techniques in GPS/Galileo", Instituto Superior Técnico, Lisboa, Portugal, May 2015.

[12]. James Bao-Yen Tsui, "Fundamentals of Global Positioning System Receivers: A Software Approach", John Wiley & Sons, ISBN 0-471-20054-9, 2000.

[13]. John W.Betz, " Engineering Satellite-Based Navigation and Timing, Global Navigation Satellite Systems, Signals, and Receivers", IEEE Press Editorial Board, ISBN: 978-1-118-61597-3, 2016.

[14]. Fevzi Aytaç Kaya, Müzeyyen Sarıtaş, "A Computer Simulation Of Dilution Of Precision In The Global Positioning System Using Matlab".

[15]. Frank van Diggelen, "A-GPS: Assisted GPS, GNSS, and SBAS", Artech House, ISBN-13: 978-1-59693-374-3, 2009.

[16]. IS-GPS-200J. "Global positioning systems directorate systems engineering & Integration, IS-GPS-200", 25 APR 2018.