DIGUE : Détection d'Interférences Gnss pour U.a.v autonomE

Victor Truong

INSTITUT POLYTECHNIQUE DE PARIS

NNT : 2020IPPAS018

Thèse de doctorat

DIGUE : Détection d'Interférences Gnss pour Uav autonomE

Thèse de doctorat de l'Institut Polytechnique de Paris
préparée à Télécom SudParis

École doctorale n°626 Ecole Doctorale de l'Institut Polytechnique de Paris (ED IP Paris)
Spécialité de doctorat : Signal, Images, Automatique et robotique

Thèse présentée et soutenue à Palaiseau, le 3 novembre 2020, par

Victor Truong

Composition du Jury :

Geneviève Baudoin Professeur émérite, ESIEE	Examinatrice
Serge Reboul Professeur, Université du Littoral	Rapporteur
Julien Sarrazin Maître de conférences, UPMC	Rapporteur
Dominique Heurguier Ingénieur, Thales	Examinateur
Alain Sibille Professeur, Télécom Paris	Président
Alexandre Vervisch-Picois Maître de conférences, Télécom SudParis	Co-encadrant de thèse
Nel Samama Professeur, Télécom SudParis	Directeur de thèse
José Manuel Rubio Hernan Maître de conférences, Télécom SudParis	Invité

Remerciements

Je souhaite tout d'abord à remercier mes directeurs de thèse, Nel Samama, Alexandre Vervisch-Picois et José Manuel Rubio Hernan, pour m'avoir guidé durant ces trois années de thèse. Vos conseils, votre aide, votre disponibilité, votre suivi ainsi que votre bienveillance ont été des éléments précieux sans lesquels mes travaux n'auraient pas été ce qu'ils sont aujourd'hui. Votre tempérament et votre soutien m'ont permis de traverser cette épreuve presque sans accroc.

Je remercie également l'ensemble des membres du département EPH de Télécom SudParis pour leur accueil chaleureux et pour m'avoir offert un cadre de travail confortable pendant ces trois années. Je remercie particulièrement Ghalid Abib pour toute l'aide matérielle qu'il m'a apporté.

Je tiens également à remercier Thales SIX GTS, et plus particulièrement Dominique Heurguier, sans qui cette thèse n'aurait peut-être pas pu arriver à son terme. Son opinion et ses conseils ont été d'une grande aide pour mes travaux.

J'adresse aussi mes remerciements à Julien Sarrazin, Serge Reboul, Geneviève Baudoin et Alain Sibille pour avoir accepté de faire partie du jury de ma thèse.

Je souhaite aussi "remercier" la SNCF ainsi que la RATP, dont les lignes D et B se sont succédées pour repousser toujours plus loin les limites de ma patience. Je garde une mention honorable pour les bus de la ligne 103 qui m'ont montré que le côté obscur avait parfois de bons côtés, car comme l'a dis un grand sage "par deux toujours ils vont".

Enfin, je remercie vivement ma famille et mes amis. Tout d'abord mes amis, avec qui j'ai partagé les hauts et les bas de la vie de thésard, toujours avec humour. Puis ma famille, pour leur soutien sans faille, leurs encouragements et leur bienveillance durant ces trois années.

Résumé

La présente étude s'inscrit dans le domaine des interférences GNSS, en particulier les interférences de leurrage. Le leurrage consiste à induire une fausse position à un récepteur, c'est-à-dire une position différente de celle où il localisé. Cette étude consiste à proposer une approche de détection d'interférences de leurrage pour drone autonome utilisant les données directement issues des récepteurs. En réalisant un état de l'art des méthodes de détection de leurrage, le contrôle du biais d'horloge est apparu comme une approche potentielle. Une modélisation numérique d'une attaque de leurrage sur un récepteur a mis en évidence que le biais d'horloge présente des sauts lorsqu'il passe de la constellation GNSS à la constellation du leurre. En reproduisant cette attaque sur des récepteurs commerciaux utilisant de vrais signaux, le biais d'horloge présente des sauts plus importants que prévus par le modèle, et dans certains cas sur la dérive du biais également. Ces sauts ont été observés sur différents scénarios d'attaque plus ou moins subtiles, cependant l'amplitude de ces sauts semble aléatoire.

Pour aller plus loin que la simple détection de leurrage, une approche utilisant une formation de drones communicants a été proposée dans le but de faire une estimation de la localisation du leurre. Cette méthode est basée sur un protocole de déplacement permettant à la formation de délimiter une zone de l'espace où le leurre est supposé être localisé. Le protocole actuel n'est pas encore complètement abouti mais il offre déjà une base prometteuse.

L'étude du comportement du biais d'horloge a permis de mettre en évidence son intérêt dans une stratégie de détection de leurrage GNSS. A partir de ce constat, de futurs travaux pourront être menés sur le développement et l'implémentation sur un drone volant d'un algorithme de détection basé sur le contrôle du biais d'horloge. L'étude de l'utilisation d'une formation de drones pour la localisation d'un leurre a permis de poser les bases d'une solution prometteuse. De futurs travaux peuvent être menés afin de compléter le protocole de déplacement et de valider son efficacité face à différents types de leurres.

Mots clés : interférences, drones, leurrage, GNSS, biais d'horloge, GPS

Abstract

This study is part of the field of GNSS interference detection, in particular spoofing interferences. Spoofing consist in inducing a false position to a receiver, i.e a position different from the receiver's true position. The study's aim is to propose an approach for detecting spoofing interferences on an autonomous UAV using data directly available on the receivers. With the study of the state of the art of spoofing detection methods, the monitoring of the clock bias seemed like a potential method. A numerical modeling of a spoofing attack on a receiver showed that the clock bias undergoes jumps when it switch from the GNSS constellation to the spoofing constellation. By replicating this attack on a commercial receivers using real signals, the clock bias shows higher jumps than expected by the model and in some cases the clock drift also show some jumps. These jumps have been observed on different more or less subtle attack scenarios, however the amplitude of the jumps seems random.

To go further than the simple spoofing detection, an approach using a communicating drone formation has been proposed. This method is based on a movement protocol allowing to delimit a space area where the spoofer is supposed to be located. The current protocol is not yet fully completed but it offers a promising basis.

The study of the behavior of the clock bias highlighted its interest in a GNSS spoofing detection strategy. Based on this observation, further work could be carried out on the development and implementation on a UAV of a detection algorithm based on the monitoring of the clock bias. The study of the use of a drone formation for the localization of a spoofer led to the basis of a promising solution. Further work could be carried out in order to complete the movement protocol and to validate its efficiency against different types of spoofers.

Keywords : interferences, UAV, spoofing, GNSS, clock bias, GPS

Table des matières

Table des figures

Liste des tableaux

Liste des acronymes

AGC	*Automatic Gain Control*
C/A	*Coarse/Acquisition*
C/No	*Carrier to Noise*
CAN	Convertisseur Analogique-Numérique
CAV	*Central Authenticity Verification*
COTS	*Commercial Off-The-Shelf*
CRPA	*Controlled Reception Pattern Antenna*
DSP	*Digital Signal Processor*
ECDF	*Empirical Cumulative Distribution Function*
ECEF	*Earth-Centered-Earth-Fixed*
GLONASS	*GLObal NAvigation Satellite System*
GLRT	*Generalized Likelihood Ratio Test*
GNSS	*Global Navigation Satellite System*
GPS	*Global Positioning System*
LASP	*Localisation Assurance Service Provider*
NMA	*Navigation Message Authentication*
NMEA	*National Marine Electronics Association*
PRN	*PseudoRandom Noise*
PSDA	*Power Spectral Density Analysis*
PVT	Position-Vélocité-Temps
RAIM	*Receiver Autonomous Integrity Monitoring*
RF	Radio Fréquence
RPM	*Received Power Monitoring*
SCER	*Security Code Estimation and Replay*
SoS	*Sum-of-Squares*
SPCA	*Structural Power Content Analysis*
SQM	*Signal Quality Monitoring*
SSSC	*Spread Spectrum Security Code*
SSV	*Spatial Signature Vector*
SVM	*Support Vector Machine*
TCXO	*Temperature Compensated X Oscillator*
UAV	*Unmaned Aerial Vehicle*
UTC	*Universal Time Coordonated*
UWB	*Ultra WideBand*

Introduction

Les travaux présentés dans ce document s'inscrivent dans le cadre d'une thèse en coopération avec Thales. Son objectif est de proposer une approche de détection d'interférences de leurrage utilisant des données issues des récepteurs, sans passer par les approches matériels ou de traitement de signal, afin d'avoir une solution peu coûteuse et relativement facile à utiliser en "masse".

Les systèmes de localisation par satellites, plus connus sous le terme GNSS (pour Global Navigation Satellite System ou Géolocalisation et Navigation par un Système de Satellites en français), sont les solutions privilégiées pour les systèmes ayant besoin de se géolocaliser. Les acteurs principaux des GNSS comme le GPS (pour Global Positioning System) ou GLONASS (pour GLObal NAvigation Satellite System) sont extrêmement populaires de part leur accessibilité et leur ouverture. Même si les acteurs du domaine sont conscients qu'il est nécessaire de développer des alternatives aux seuls GNSS, ceux-ci restent au coeur de la géolocalisation. Les drones volants, aussi appelé UAV (pour Unmaned Aerial Vehicle en anglais), se sont largement démocratisés dans le domaine civil depuis quelques années grâce à la réduction des coûts et la miniaturisation de l'électronique. De tels systèmes sont très fortement dépendants des GNSS pour pouvoir fonctionner en vol automatisé. Lors d'un tel mode de fonctionnement, il est important de pouvoir connaître sa position avec fiabilité, les fonctions de géolocalisation et de navigation sont donc essentielles. Cette forte dépendance peut être problématique pour les drones en vol autonome. En effet, il n'est pas rare que les signaux GNSS subissent des interférences, en particulier en milieu urbain. Ces interférences peuvent être intentionnelles et néfastes pour le bon fonctionnement de la géolocalisation d'un drone volant. On peut citer les interférences de brouillage qui peuvent complètement priver un drone de son positionnement ou encore les interférences de leurrage qui constituent un type d'interférences plus subtiles. Le leurrage GNSS n'annule pas les capacités de géolocalisation mais induisent en erreur le positionnement du drone. Une fois que le récepteur du drone calcule une position erronée, les résultats de ses algorithmes de navigation vont être faussés ce qui peut conduire à sa capture ou sa destruction. Ceci peut donc conduire à la capture ou la destruction d'un drone. Voilà pourquoi il est nécessaire de détecter la présence de telles interférences afin, éventuellement, de s'y soustraire.

Il existe déjà de nombreuses méthodes de détection de leurrage qui ont été proposées dans la littérature. Elles se distinguent les unes des autres par les métriques de détections mises en jeu dans leur stratégie de détection et qui seront détaillées dans le Chapitre I . On peut citer les travaux de Jafarnia-Jahromi et al. dans [1] Dans leur étude ils ont implémenté sur un récepteur GNSS un processus de traitement de signaux composé d'une série d'opérations de filtrage permettant d'éliminer les effets Doppler et le bruit présents sur les signaux reçus. On obtient en sortie de ces opérations un spectre permettant une analyse structurelle des signaux reçus. Jafarnia-Jahromi et al. ont alors développé un algorithme de décision statistique basé sur une approche GLRT (pour Generalized Likelihood Ratio Test ou test généralisé du rapport de vraisemblance en français) et permettant de détecter la présence de signaux de leurrage dans les signaux reçus. Cet algorithme de détection a ensuite été testé dans un premier temps en simulation puis sur des jeux de données collectées en situations réelles. Cela a permis de montrer qu'une analyse structurelle de la puissance des signaux est une bonne méthode dans la détection d'interférences GNSS. Cependant cette méthode ne permet pas de faire la distinction entre le leurrage et d'autres types d'interférences GNSS.

Sur un autre type de stratégie, O'Hanlon et al. dans [2] ont étudié les modèles des signaux GNSS civils et militaires, ainsi que celui des codes PseudoRandom Noise (PRN) afin de mettre en évidence la quadrature de phase entre les codes civil et militaire. Un algorithme de détection basé sur l'inter-corrélation entre les signaux civils et militaires a été implémenté sur deux récepteurs et testé en temps réel. Cela a permis de

montrer l'efficacité de l'algorithme de détection exploitant les relations entre les signaux civils et militaires. Cependant cette méthode nécessite qu'un des récepteurs soit totalement sécurisé de toute source d'interférence et elle nécessite aussi l'utilisation d'un canal de transmission de données suffisamment fiable entre les deux récepteurs.

On peut également citer une autre approche proposée par Borio et al. dans [3]. A partir d'une modélisation des signaux GNSS et de la simple différence de déphasage entre deux récepteurs GNSS, il est possible d'isoler des termes géométriques relatifs à la direction d'arrivée des signaux GNSS. Suite à cela un détecteur de type somme des carrés pondérés a été développé afin de déterminer si l'angle d'arrivée est commun à tous les signaux reçus. Cet algorithme de détection a été testé sur une plateforme utilisant deux récepteurs en environnement contrôlé. Cette étude a permis de montrer l'intérêt et la relative facilité de mise en place d'une stratégie basée sur le calcul de la différence de déphasage entre deux récepteurs GNSS. Néanmoins cette méthode est limitée lorsque l'ensemble des signaux pris en compte par le récepteur comprend à la fois des signaux de leurrage et des signaux authentiques Dans cette situation, l'algorithme peut conduire à des faux positifs ou des faux négatifs.

Une autre approche possible est proposée par Marnach et al. dans [4]. Dans cet article, ils ont étudié le calcul du biais d'horloge d'un récepteur GNSS et son implication dans le positionnement par satellite. Un algorithme a ensuite été développé et testé sur une plateforme appelée LASP (pour Localisation Assurance Service Provider) et qui a pour fonction de déterminer si les signaux reçus par un récepteur GNSS sont fiables. L'algorithme exploite le biais d'horloge pour détecter des attaques de *meaconing* (le meaconing est la répétition de signaux GNSS décalés dans le temps, on peut considérer ce type d'interférence comme du leurrage simplifié). A partir d'un historique de mesure du biais d'horloge et d'une régression linéaire, l'algorithme calcule l'erreur du biais d'horloge et observe son comportement pour détecter l'attaque de meaconing. Ceci a permis de montrer que le meaconing provoque des variations abruptes sur l'erreur du biais. Cependant les tests ont été réalisés en environnement contrôlé où la dérive de l'horloge était bien stabilisée, ce qui n'est pas forcément le cas lors d'une utilisation "normale" d'un récepteur. De plus cette étude se limite à du meaconing et ne s'intéresse pas au cas du leurrage. Par ailleurs, l'influence des différents paramètres de l'algorithme sur sa fiabilité n'a pas été étudiée. De même, la possibilité d'appliquer cet algorithme avec des récepteurs COTS (Commercial Off-The-Shelf) n'a pas été étudiée.

Panice et al. dans [5] exploitent la fusion de données sur un drone. Ils ont mis en place sur un drone la fusion de données entre les données GPS et les données des capteurs inertiels. Ils ont ensuite implémenté un algorithme d'apprentissage de type SVM (Support Vector Machine). L'algorithme de SVM est utilisé pour analyser les données issues de la fusion de données GPS/inertielles. Il s'intéresse en particulier aux erreurs entre ces deux sources de données qui ont un comportement prévisible en l'absence de leurrage. La méthode proposée par Panice et al. a été testée en simulation. Les simulations ont permis de montrer qu'il est possible d'exploiter la fusion de données pour détecter le leurrage GNSS avec des performances équivalentes aux algorithmes de contrôle d'intégrité RAIM (Receiver Autonomous Integrity Monitoring). Cependant les performances de l'algorithme se détériorent rapidement lorsque l'attaque de leurrage est une attaque longue durée.

Les études précédentes dans le domaine de la détection de leurrage mettent en évidence le fonctionnement et la dangerosité des interférences de leurrage sur les récepteurs GNSS. Elles proposent différentes méthodes de détection d'interférences de leurrage. Ces méthodes peuvent être classées en fonction des métriques de détection mises en jeu dans leur stratégie. Les méthodes les plus exploitées sont celles qui se reposent principalement sur des phases de traitement de signaux permettant une étude des différentes caractéristiques des signaux reçus par le récepteur. Certaines ont envisagé le chiffrement des signaux comme outil de détection. D'autres méthodes exploitent la direction d'arrivée des signaux pour déterminer s'ils sont authentiques ou issus d'un leurre . Une autre catégorie de méthodes de détection cherchent à combiner ces différentes méthodes entre elles ou avec d'autres composants, comme les centrales inertielles par exemple, pour réaliser de la fusion de données. La majeure partie de ces techniques peuvent impliquer un coût matériel supplémentaire ou une puissance de calcul supplémentaire. D'un autre côté, une autre catégorie de méthodes de détection s'intéressent aux dérives anormale des positions ou de l'horloge. C'est à ces dernières que nous allons nous intéresser. En effet ces méthodes peuvent être utilisées sans gros ajout de matériel car elles exploitent du matériel déjà présent sur les drones, ce qui en fait des solutions bas coût. Ces méthodes sont par ailleurs peu

répandues dans la littérature alors qu'elles sont essentiellement basées sur l'exploitation directe des données de navigation du récepteur embarqué sur le drone.

C'est ce qui justifie la présente étude. Elle consiste à élaborer une méthode de détection de leurrage GNSS à bas coût en exploitant les données de navigation fournies par le récepteur GNSS d'un drone. Une partie de l'étude s'intéresse également à la mise en oeuvre d'un réseau de récepteurs sous forme d'une formation de drones dans l'optique de localiser le leurre attaquant.

L'objectif du chapitre I a été de réaliser un état de l'art sur la détection des interférences de leurrage GNSS. Pour cela, après un rappel sur le fonctionnement de la géolocalisation par satellites, on s'est intéressé au fonctionnement du leurrage GNSS afin d'identifier quels sont les types d'attaques de leurrage les plus susceptibles de toucher un récepteur GNSS. L'idée a ensuite été de faire l'inventaire des différentes techniques de détection de leurrage étudiées dans la littérature afin de déterminer sur quel type de stratégie de détection notre étude se focaliserait.

Le chapitre II a pour objectif d'étudier les effets d'une attaque de leurrage sur l'horloge d'un récepteur GNSS. Pour cela on a développé un modèle numérique afin mettre en évidence l'action d'un leurre sur le biais d'horloge d'un récepteur GNSS. L'idée a ensuite été de mettre en place une attaque de leurrage sur un récepteur commercial, utilisant de vrais signaux, dans le cas où le leurre utilise la même horloge que la constellation satellite afin de valider les résultats obtenus avec le modèle numérique. Puis l'idée a ensuite été d'étudier la cas où le leurre utilise sa propre horloge pour générer ses signaux afin de valider les résultats précédents dans un cas plus réaliste. Les différences d'ordre de grandeur sur les résultats observés ont ensuite été étudiées avant d'étudier un cas où le récepteur est en mouvement.

L'objectif du chapitre III a été de proposer une méthode exploitant un réseau de récepteurs sous forme d'une formation de drones. Pour cela on a réalisé un état de l'art sur les solutions exploitants des réseaux d'antennes et/ou de récepteurs afin de déterminer les possibilités offertes par ce type de structure. L'idée a ensuite été de proposer une base de stratégie d'estimation de la direction du leurre utilisant une formation de drones. Cette base de stratégie a ensuite été testée par le développement d'un code de simulation afin de mettre en évidence les avantages et les limites de cette stratégie et les points d'améliorations possibles.

Enfin, l'objectif du chapitre IV est de faire une analyse critique des travaux présentés dans ce document.

Chapitre I

Etat de l'art

Cet état de l'art se compose de trois thématiques. La première se focalise sur la géolocalisation par satellites et les systèmes GNSS. La deuxième partie détaille le fonctionnement du leurrage GNSS et la dernière partie fait un inventaire des différentes techniques de détection de leurrage que l'on peut trouver dans la littérature.

I.1 Géolocalisation par satellites

I.1.1 Présentation des systèmes GNSS

Les systèmes de positionnement par satellites, désignés par le terme GNSS, ont commencé à se développer lors des années 70 avec en figure de proue les américains avec le GPS suivis par les soviétiques avec le GLONASS quelques années plus tard et, plus récemment, les européens avec GALILEO et les chinois avec BEIDOU. Ces systèmes sont constitués de constellations de satellites en orbites autour de la Terre. Ces satellites émettent des signaux radio-fréquence contenant des informations qui vont permettre à un utilisateur les recevant de se géolocaliser. Les principales composantes des signaux GNSS sont le code PRN propre à chaque satellite, la porteuse sur laquelle le code est modulé, et le message de navigation [6]. Le message de navigation contient ce qu'on appelle les éphémérides du satellite qui permettent de connaître, en particulier, la position du satellite à un instant donné. Dans le cas du GPS on distingue deux types de codes PRN utilisés pour générer deux types de signaux GPS :

— le signal militaire potentiellement crypté, associé au code P(Y) (P pour Precision en anglais) et le code M (pour Military) plus récemment,

— le signal civil, associé au code C/A (pour Coarse/Acquisition en anglais) ouvert à tous les utilisateurs.

La diffusion de ces codes de transmission et des données se faisait à l'origine sur deux fréquences porteuses par le biais d'une technique d'accès de type CDMA (Code Division Multiple Access) :

— la fréquence L1 de 1575.42 MHz qui transmet les code C/A et P,

— la fréquence L2 de 1227.6 MHz qui transmet le code P(Y)

Puis à la fin des années 90 le GPS s'est "modernisé" par l'ajout de deux nouveaux signaux civils : L2C (à la même fréquence que L2) et L5 à 1176.45 MHz.

Les systèmes GNSS tels que le GPS ont une portée universelle. L'utilisation des GNSS est possible pour tout utilisateur pouvant recevoir ces signaux. Ceci est possible grâce à la transparence des GNSS. Le signal GPS civil a une "composition" connue de tous les systèmes utilisateurs possibles. Le code C/A est prévisible étant donné que tous les récepteurs y ont accès. C'est ce qui a répandu l'utilisation des GNSS de façon très large dans le domaine de la navigation, mais c'est aussi ce qui les rend vulnérables car ils ne disposent pas tous de système de sécurité. Cette faiblesse fait que les signaux GNSS sont susceptibles de souffrir d'interférences.

Ces interférences peuvent être dues à l'environnement local, par exemple une zone urbaine où évoluerait un drone volant. Cependant il arrive aussi que ces interférences soient intentionnelles et malveillantes. Le brouillage et le leurrage sont deux types d'interférences intentionnelles et c'est à ce dernier type que notre étude s'intéresse.

I.1.2 Calcul de position

La géolocalisation par satellites est basée sur la mesure du temps d'arrivée d'un signal effectuant le trajet {émetteur-récepteur}. Ce temps d'arrivée permet, à partir de la vitesse de propagation du signal de déduire la distance entre l'émetteur (le satellite) et le récepteur (l'utilisateur). En effectuant cette mesure à partir de plusieurs satellites on peut en déduire la position de l'utilisateur.

Cependant les horloges des satellites et des récepteurs GNSS ne sont pas synchronisées. Lorsqu'un récepteur GNSS reçoit un signal d'un satellite, il mesure en réalité ce qu'on appelle la pseudo-distance entre lui et le satellite émetteur, notée ρ. Cette mesure représente non seulement la distance entre le satellite et le récepteur mais aussi la différence temporelle entre les horloges des satellites et du récepteur. Cette différence temporelle, notée t_u, est communément appelée le biais d'horloge.

Pour déterminer la position du récepteur il faut résoudre un système d'équations obtenu à partir des pseudo-distances (on désignera par la suite ces équations par le terme "équations de navigation"). Les inconnues du système sont les coordonnées de l'utilisateur (x_j, y_j, z_j), exprimées dans un repère centré sur la Terre et suivant sa rotation (ce repère est appelé ECEF pour Earth-Centered Earth-Fixed), et t_u le biais d'horloge. Pour un satellite j du système, on a donc l'équation suivant :

$$\rho_j = \sqrt{(x_j - x_u)^2 + (y_j - y_u)^2 + (z_j - z_u)^2} + ct_u \tag{I.1}$$

avec c la célérité de la lumière et l'indice j faisant référence aux satellites. Ce système d'équations ayant quatre inconnues, trois d'espace et une de temps, il faut au moins 4 satellites pour pouvoir résoudre le système et donc obtenir la position de l'utilisateur (d'où j variant de 1 à au moins 4).

Comme expliqué dans [6] une manière courante de résoudre ce système d'équations non linéaires est d'utiliser des techniques itératives basées sur la linéarisation. Pour cela on définit la position et le biais d'horloge du récepteur comme la somme d'une composante estimée $(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u})$ et d'une composante de décalage $(\Delta x_u, \Delta y_u, \Delta z_u, \Delta x_u)$, on a donc :

$$\begin{cases} x_u = \hat{x_u} + \Delta x_u \\ y_u = \hat{y_u} + \Delta y_u \\ z_u = \hat{z_u} + \Delta z_u \\ t_u = \hat{t_u} + \Delta t_u \end{cases} \tag{I.2}$$

Partant de ça on peut exprimer une estimation de la pseudo-distance $\hat{\rho}$ de façon similaire à l'équation (I.1). Ceci permet de linéariser l'équation (I.1) avec un développement en série de Taylor. On obtient alors l'équation suivante :

$$\rho_j = \hat{\rho_j} - a_{x_j}\Delta x_u - a_{y_j}\Delta y_u - a_{z_j}\Delta z_u + c\Delta t_u \tag{I.3}$$

où :
$$\begin{cases} a_{x_j} = \dfrac{x_j - \hat{x_u}}{\hat{r_j}} \\ a_{y_j} = \dfrac{y_j - \hat{y_u}}{\hat{r_j}} \\ a_{z_j} = \dfrac{z_j - \hat{z_u}}{\hat{r_j}} \\ \hat{r_j} = \sqrt{(x_j - \hat{x_u})^2 + (y_j - \hat{y_u})^2 + (z_j - \hat{z_u})^2} \end{cases}$$

Pour résoudre cette forme linéaire on peut utiliser une forme matricielle du système. Le système d'équation (I.3) s'écrit alors

$$\boldsymbol{\Delta}\rho = \mathbf{H}\boldsymbol{\Delta}\mathbf{X} \tag{I.4}$$

où $\mathbf{H}$ est la matrice du système d'équations linéarisées. Dans le cas de 4 équations (4 satellites) on a les termes suivants :

$$\boldsymbol{\Delta}\rho = \begin{bmatrix} \Delta\rho_1 \\ \Delta\rho_2 \\ \Delta\rho_3 \\ \Delta\rho_4 \end{bmatrix}, \mathbf{H} = \begin{bmatrix} a_{x_1} & a_{y_1} & a_{z_1} & 1 \\ a_{x_2} & a_{y_2} & a_{z_2} & 1 \\ a_{x_3} & a_{y_3} & a_{z_3} & 1 \\ a_{x_4} & a_{y_4} & a_{z_4} & 1 \end{bmatrix}, \boldsymbol{\Delta}\mathbf{x} = \begin{bmatrix} \Delta x_u \\ \Delta y_u \\ \Delta z_u \\ -c\Delta t_u \end{bmatrix}$$

La solution du système est alors

$$\boldsymbol{\Delta}\mathbf{x} = \mathbf{H}^{-1}\boldsymbol{\Delta}\rho \tag{I.5}$$

Dans le cas où plus de satellites sont disponibles (et donc plus d'équations), le système d'équation est surdéterminé. Il existe plusieurs méthodes permettant de résoudre le système dans ce cas là. La méthode standard est la méthode des moindres carrés [6]. Si on note $\boldsymbol{\Delta}\tilde{\mathbf{x}}$ l'approximation de la solution on a alors

$$\boldsymbol{\Delta}\tilde{\mathbf{x}} = \left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T\boldsymbol{\Delta}\rho \tag{I.6}$$

I.2 Leurrage GNSS

I.2.1 Principe général et fonctionnement

Le principe d'un leurrage GNSS est de faire croire à un récepteur GNSS qu'il est positionné à une fausse position, c'est-à-dire une position différente de celle où il est réellement [7]. Pour ce faire il faut répliquer le signal GNSS reçu par le récepteur mais avec quelques altérations adéquates. En faisant cela sur un drone en navigation autonome on peut alors forcer un changement de trajectoire par le biais de cette fausse position. Ainsi en utilisant plusieurs fausses positions successives, on peut contrôler indirectement la trajectoire d'un drone en vol autonome pour l'amener à une certaine position ce qui permet par exemple de le capturer ou de le faire percuter un obstacle pour le détruire. Comme expliqué dans [8], les leurres GNSS peuvent être classés en trois catégories au niveau matériel :

— les simulateurs de signaux GNSS "simples",

— les leurres-récepteurs,

— les leurres "sophistiqués".

La première catégorie regroupe les simples générateurs de signaux pouvant émettre des signaux imitant d'authentiques signaux GNSS. Lorsqu'un récepteur en mode poursuite reçoit ces signaux il les assimile à du bruit. Ceci est déjà suffisant pour perturber un récepteur GNSS commercial.

La deuxième catégorie regroupe des leurres qui combinent générateur et récepteur de signaux GNSS. La partie récepteur permet au leurre de se synchroniser avec d'authentiques signaux GNSS afin d'obtenir une position, le temps et les éphémérides des satellites de la constellation GNSS. Ces informations permettent au leurre de configurer les faux signaux qu'il souhaite émettre.

La dernière catégorie rassemble tous les leurres plus avancés que ceux des catégories précédentes. Ce sont par exemple des leurres qui sont capables de parfaitement synchroniser leurs signaux avec ceux de la constellation GNSS. On range aussi dans cette catégorie les leurres qui tirent avantage de l'utilisation de plusieurs antennes pour émettre depuis différentes directions, imitant la répartition géométrique d'une vraie constellation de satellites.

I.2.2 Fonctionnement détaillé du leurrage

Pour comprendre comment un leurre peut induire en erreur un récepteur GNSS il est nécessaire de s'intéresser au modèle des signaux GNSS. Comme expliqué dans [9], on peut exprimer le signal reçu $y(t)$ par un récepteur GNSS de la façon suivante :

$$y(t) = Re\left\{\sum_{i=1}^{N} A_i D_i[t-\tau_i(t)] C_i[t-\tau_i(t)] e^{j[\omega_c t - \phi_i(t)]}\right\} \tag{I.7}$$

avec :

- N le nombre de signaux,
- A_i l'amplitude de la porteuse du signal i,
- $D_i(t)$ le flux de données du signal i,
- $C_i(t)$ le code PRN d'étalement du signal i,
- τ_i la phase du code du signal i,
- ω_c la fréquence de la porteuse,
- $\phi_i(t)$ la phase de la porteuse.

Comme expliqué précédemment, un leurre doit répliquer de faux signaux similaires aux vrais signaux GNSS que le récepteur reçoit afin que ce dernier n'identifie pas les signaux du leurre comme non pertinents. Avec ce modèle de signal on peut délimiter trois métriques sur lesquelles le leurre peut agir pour que le récepteur suive les signaux du leurre à la place des signaux des satellites de la constellation. Broumandan et al. les explicitent en détail dans [10]. Ces métriques sont :

- la puissance relative (A_i),
- le délai relatif (τ_i),
- la phase relative (ϕ_i).

La façon dont le leurre va paramétrer ces métriques va définir le type d'attaque de leurrage effectué. Ainsi, un leurre va produire des signaux similaires qu'on peut formuler de cette façon :

$$y_s(t) = Re\left\{\sum_{i=1}^{N_s} A_{si}\hat{D}_i[t-\tau_{si}(t)]C_i[t-\tau_{si}(t)]e^{j[\omega_c t-\phi_{si}(t)]}\right\}$$

avec :

— $N_s = N$ pour avoir une fausse constellation de même configuration que la vraie constellation,

— $C_i(t)$ qui doit rester inchangé par rapport aux vrais signaux,

— la meilleure estimation du flux de données $\hat{D}_i(t)$ qui va permettre de définir la fausse position envoyée par le leurre,

— A_{si}, $\tau_{si}(t)$ et $\phi_{si}(t)$ propres aux signaux du leurre.

Lors de l'attaque, le récepteur de la victime reçoit à la fois les signaux des satellites mais aussi les signaux du leurre, auxquels s'ajoute du bruit. Le signal total reçu par le récepteur de la victime est donc le suivant :

$$y_{tot}(t) = y(t) + y_s(t) + \nu(t)$$

où $\nu(t)$ est le bruit reçu. Ce dernier peut être soit naturellement généré, soit une contribution additionnelle du leurre. Partant de ce principe on peut envisager plusieurs types de leurres.

I.2.3 Principaux types de leurre

I.2.3.1 Leurre cohérent

Les leurres qu'on appelle "cohérents" sont des leurres qui arrivent à utiliser les métriques définies précédemment sans répercutions significatives sur les résidus de pseudo-distance. Cette dernière caractéristique fait de ces leurres de bons candidats pour contrer les stratégies de défense exploitant le RAIM. Le RAIM est un type d'algorithme de vérification de l'intégrité de la solution de navigation GNSS. Ce type d'algorithme va donc comparer les mesures des pseudo-distances, en particuliers leur résidus, afin de déterminer la présence ou non de redondance. Un leurre basique attaquant un récepteur rajoute des mesures de pesudo-distances incohérentes avec les autres mesures issues des vrais signaux. Ceci se répercute sur les résidus des pseudo-distances, ce que le RAIM peut détecter.

Pour contrer les RAIM, les leurres cohérents synthétisent la phase de leur code $\tau_{si}(t)$ de telle sorte à avoir une fausse position tout en n'ayant que de faibles résidus de pseudo-distance. De plus le déphasage des porteuses est choisi pour varier de telle sorte que

$$\forall i,\, \forall t_a,\, \forall t_b,\, \omega_c[\tau_{si}(t_b) - \tau_{si}(t_a)] = \phi_{si}(t_b) - \phi_{si}(t_a) \tag{I.8}$$

N'importe quel bon simulateur de signaux GNSS peut faire office de leurre cohérent. Un des défis auxquels doit faire face un leurre est de faire en sorte que le récepteur "s'accroche" sur les faux signaux pour calculer sa position. On peut distinguer deux façons d'y parvenir :

— on commence par brouiller la victime qui perd le suivi des vrais signaux. Le récepteur passe alors en mode acquisition. Ce brouillage peut se faire de façon subtile afin de déjouer les algorithmes de détection d'attaque. Puis on induit la ré-acquisition sur les faux signaux en s'assurant que la puissance des signaux du leurre soit plus élevée que celle des vrais signaux ($\forall i = 1, ..., N,\, A_{si} \gg A_i$).

— On transmet de faux signaux dont les phases du code et de la porteuse du leurre s'alignent sur celles des signaux des satellites ($\tau_{si} \approx \tau_i$). On commence à faible puissance ($A_{si} \approx 0$), puis on augmente A_{si} progressivement jusqu'à dépasser la puissance des vrais signaux ($A_{si} > A_i$) pour capturer la cible avant de l'entrainer vers une autre position en modifiant τ_{si}.

Cette dernière méthode requiert de connaître les vrais valeurs de A_i et $\tau_i(t)$. Pour cela le leurre doit donc également être un récepteur. De plus il est également nécessaire de connaître la relation géométrique entre le leurre et la victime.

La Figure 1 représente la fonction d'auto-corrélation d'un signal GNSS (plus précisément du code qui module la porteuse de ce signal [6]) vue du récepteur lors d'une attaque "cohérente" : les points rouges sont les points de suivi du récepteur, la ligne noire discontinue représente le leurre et la ligne bleue représente la somme leurre + vrai signal. Les trois premières lignes représentent l'initialisation A_{si} et τ_{si} et l'augmentation de A_{si}. Les deux dernières lignes représentent la modification de τ_{si} vers une autre position.

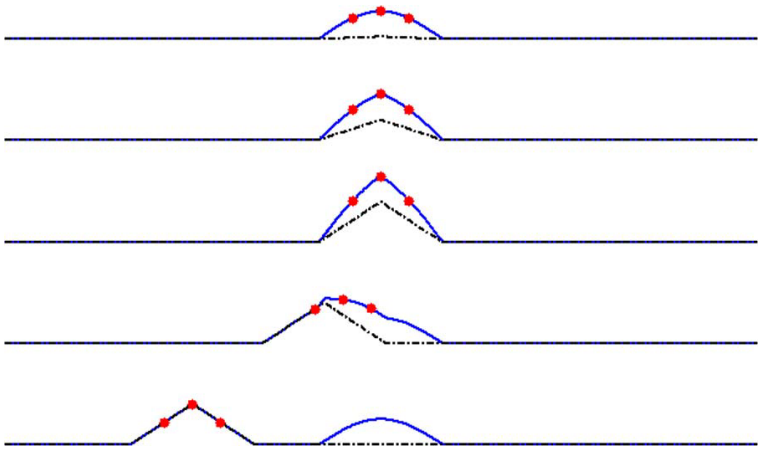

FIGURE 1 – Illustration de la méthode faible puissance de [9]

Un autre défi dans la conception de tels leurres vient des essais en situation réelle. La législation actuelle n'autorise en effet pas la diffusion de signaux sur les bandes de fréquence GNSS, ce qui rend les tests de leurrage en situation réelle légalement impossibles. Tenter de réaliser des expériences de leurrage sans autorisation peut amener de lourdes sanctions. Les essais de techniques de détection se heurtent par ailleurs au même problème.

I.2.3.2 Attaques par répétition

Les leurres cohérents sont très efficaces sur les signaux civils comme le GPS C/A. La transparence des signaux civils les rends prévisibles. Cette prévisibilité facilite la synthèse des codes PRN et des données par le leurre. Cependant dans le cas de signaux cryptés, par exemple les signaux GPS militaires ou des signaux auxquelles des clés d'authentification ont été ajoutées aux données, cette tâche se révèle plus ardue pour les leurres cohérents. Un leurre qui s'attaque à un signal crypté doit pouvoir reproduire correctement les parties non prévisibles du vrai signal.

Une solution possible pour leurrer un récepteur utilisant des signaux cryptés est d'utiliser ce qu'on appelle le meaconing (en anglais). Le meaconing consiste à enregistrer le signal reçu par le récepteur $y(t)$ puis de le rediffuser avec un gain suffisamment grand pour recouvrir le vrai signal au niveau de l'antenne de réception de la victime. Le temps de traitement nécessaire à la rediffusion des vrais signaux ajoute un retard temporel qui se répercute sur la phase du code PRN. Le récepteur va donc lire dans les données reçues un temps qui précède le vrai temps, ce qui altère la position calculée. Avec cette définition on peut considérer le meaconing comme une version simplifiée du leurrage. Une version plus sophistiquée de meaconing serait d'utiliser plusieurs antennes pour réaliser chaque enregistrement et chaque rediffusion sur chaque canal GNSS de façon indépendante les uns des autres.

Une autre méthode pour contrer le cryptage lorsqu'il n'est appliqué que sur le flux de données est l'attaque Security Code Estimation and Replay (SCER). Humphreys détaille plus précisément cette technique dans [11]. Une attaque SCER réalise une estimation des bits $D_i(t)$ imprévisibles et les diffuse dés qu'une estimée

fiable est trouvée. Ce type d'attaque est assez limité car il est très difficile à appliquer sur des signaux complètement cryptés au niveau de leur code PRN. Une attaque SCER efficace a besoin de bons matériels pouvant assurer le processus d'estimation des bits.

I.2.3.3 Techniques de leurrage avancées

Avec les avancées en matière de détection de leurrage, des techniques de leurrage plus avancées ont émergé. Une de ces techniques est celle de l'annulation (nulling en anglais). Le nulling consiste à annuler les vrais signaux pour que ne subsistent que les faux signaux du leurre. Pour cela le leurre doit produire deux signaux par signal de leurrage :

— le premier est le faux signal de leurrage,

— le deuxième est le signal d'annulation.

Le signal d'annulation est tout simplement le vrai signal mais déphasé de π radian, ce qui permet d'effacer complètement toute trace du vrai signal d'origine. Reproduire un signal d'annulation efficace est très difficile car il faut être capable de reproduire de nombreux paramètres physiques, comme par exemple le gain d'antenne ou le diagramme d'antenne, via calibration. Cette phase de calibration rend la mise en place d'une attaque de nulling très contraignante.

Il existe une variante du nulling qui ne diffuse que des signaux d'annulation dont l'amplitude est deux fois plus élevée que les vrais signaux. Ces signaux d'annulation ne sont utilisés que sur certains canaux ce qui permet de jouer sur les éphémérides des satellites au lieu des pseudo-distances.

Dans le cas d'un récepteur utilisant plusieurs antennes, un leurre peut utiliser plusieurs antennes indépendantes, chacune étant "reliée" à une antenne du récepteur ciblé. En exploitant la connaissance des relations géométriques de chaque paire d'antennes leurre-victime et en posant les hypothèses suivantes :

— le leurre est proche de sa cible,

— les diagrammes de chaque antenne sont suffisamment étroits pour que chaque antenne de la cible reçoive des signaux provenant uniquement de l'antenne du leurre associée.

il est alors possible de leurrer un récepteur GNSS à plusieurs antennes en contrôlant la phase de chaque porteuse $\phi_{si}(t)$. Ce type de leurre multi-antennes peut également être utilisé pour contrer les techniques de détection de leurrage basées sur la direction d'arrivée de signaux. Cependant ce type de leurre requiert de bien disposer les antennes autour de la cible.

On constate donc quand on regarde les travaux présents dans la littérature que la plupart des techniques de leurrage avancées sont très coûteuses que ce soit en terme de matériel, de mise en place ou de complexité.

De façon générale, toutes les techniques de leurrage GNSS doivent faire attention à la cohérence physique de leurs altérations. En effet, pour rester discrets les leurres doivent provoquer des changements vraisemblables vis à vis du système qui est attaqué. Par exemple induire un changement de vitesse beaucoup trop élevé et brutal pour un drone est clairement suspicieux et peut facilement être "réfuté" par le biais d'autres appareils présents sur le drone comme les capteurs inertiels par exemple.

I.2.3.4 Coopération de l'utilisateur

Il existe une dernière catégorie d'attaque de leurrage. Cette catégorie regroupe les cas où la victime facilite le travail du leurre en provoquant elle-même le leurrage. Ce sont souvent des utilisateurs qui ont besoin de cacher leur véritable position pour contourner des lois ou des réglementations. On peut citer l'exemple de camionneurs ou de pêcheurs qui leurrent leurs propres récepteurs pour cacher leur passage dans une zone non autorisée par un quelconque règlement.

Avec une victime coopérative il est évidemment plus facile d'appliquer une attaque de leurrage. Les défenses face à ce type de cas ne sont envisageable que par l'utilisation de sécurités physiques.

I.2.4 Historique et mise en évidence des risques

Comme expliqué dans [12] un rapport du département des transports des Etats-Unis, connus sous le nom de rapport Volpe et publié en 2001, soulève la vulnérabilité du système GPS et met en garde contre le risque potentiel des interférences de leurrage. En 2008, Humphreys et al. dans [12] ont réussi à développer un leurre cohérent logiciel de type "leurre-récepteur". Ce leurre a ensuite été implémenté sur une plateforme récepteur GNSS, la Cornell GRID (Figure 2) afin d'en faire un leurre portatif. Il a ensuite été testé avec succès sur un autre récepteur Cornell via des essais en transmission câblée.

FIGURE 2 – Plateforme Cornell GRID

Cette étude démontre qu'il est relativement facile de mettre en place, à partir de composants de type COTS, un leurre GPS capable d'aligner précisément les codes PRN et les données de navigation des faux signaux avec ceux des vrais signaux GPS, permettant ainsi la mise en place d'attaques assez sophistiquées sans que la victime ne s'en rende compte.

En 2011, un drone de surveillance de la CIA a été capturé par l'Iran par ce qu'on pense être une attaque de leurrage. Bien qu'on ne sache pas exactement comment s'y est pris l'Iran, il semblerait que le drone a d'abord été brouillé pour perdre le suivi des signaux militaires ce qui l'a fait basculer sur le suivi des signaux civils pour reprendre sa navigation. Puis le leurre aurait envoyé des faux signaux civils pour leurrer le drone. Cet événement a soulevé beaucoup d'interrogations sur les possibilités de leurrage de drones, en particuliers ceux utilisant le GPS civil pour le positionnement et la navigation.

C'est ainsi que des travaux menés par Shepard et al. on été réalisés en 2012 afin de mettre en évidence, par le biais de tests de leurrage en conditions réelles, la vulnérabilité des systèmes GPS face aux attaques de leurrage dont les résultats sont reportés dans l'article [7]. Contrairement à l'étude de Humphreys et al [12], les essais de leurrage ont été réalisés sur des récepteurs disponibles dans le commerce et ceci en condition de fonctionnement réel. Dans cet article des attaques de leurrage on été réalisées sur deux systèmes dépendants du GPS civil :

— le Hornet Mini, un drone commercial utilisant le GPS pour la navigation,

— un récepteur GPS utilisé dans les appareils de mesure de type "smart grid" (ici un synchrophaseur).

Afin de réduire significativement la complexité de la mise en place d'une attaque de leurrage GPS, il faut que le leurre soit placé le plus proche possible (seulement quelques mètres) de sa cible. Ceci permet de considérer

la distance entre le leurre et la cible comme négligeable. On désigne généralement ce type de situation comme une attaque de proximité. Etant donné la nature de la cible une attaque de proximité n'est pas envisageable. Le leurre doit donc prendre en compte la distance le séparant du récepteur lors de la configuration des messages de navigation de ses signaux. Avec cette contrainte, la précision de la fausse position émise par le leurre ne peut être que de l'ordre du mètre. Le leurre utilisé pour ces tests est une version améliorée du leurre proposé par Humphreys et al. dans [12]. Le leurre est implémenté sur une plate-forme radio portable construite autour d'un DSP (Digital Signal Processor). Le schéma bloc de ce leurre est présenté Figure 3. La partie "récepteur couplé" se charge de récupérer les signaux des satellites. Le module de contrôle va alors modifier les informations issues des signaux des satellites pour configurer les signaux de leurrage pour obtenir une nouvelle solution Position-Vélocité-Temps (PVT).

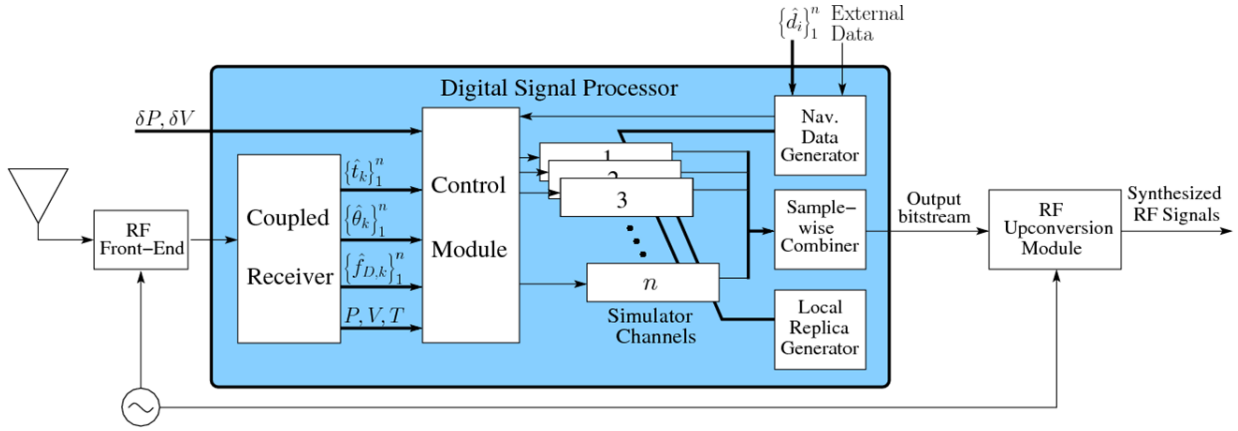

FIGURE 3 – Schéma bloc du leurre utilisé dans [7]

Ce leurre fait partie de la catégorie des leurres-récepteurs cohérents, présentés précédemment en sections I.2.1 et I.2.3.1. Sa stratégie suit celle utilisant des signaux de faible puissance avec augmentation progressive de celle-ci jusqu'à capture de la victime. Dans [7], on considère que le récepteur est complètement capturé si :

— chaque signal de leurrage est décalé de 2 μs par rapport aux vrais signaux,

— chaque signal de leurrage est au moins 10 dB plus puissant que les vrais signaux correspondants.

La configuration expérimentale mise en place pour la réalisation de ces attaques de leurrage est présentée Figure 4. Le drone Hornet reste en vol stationnaire à une position fixe maintenue par sa fonction d'auto-pilotage. Lorsque le drone est leurré, son récepteur lit une fausse vélocité correspondant à un changement de position, celle ci étant différente de celle où il est sensé stationner. Pour compenser ce changement le système de commande du drone modifie sa réponse en allant dans la direction opposée.

Ces essais de leurrage de drone civil ont été un succès, le leurre utilisé par Shepard et al. a pu leurrer avec succès le drone Hornet. Ceci met en évidence la vulnérabilité des systèmes dépendant du positionnement par satellites face aux attaques de leurrage, en particulier les systèmes civils qui représentent la majeure partie d'entre eux. Ceci soulève des inquiétudes quant à la sécurité de ce type de système.

Créer à partir de zéro un leurre GPS comme celui présenté dans [7] n'est pas à la portée de tout le monde. Cependant, l'évolution du marché de l'électronique tend vers l'augmentation de la disponibilité de composants COTS pouvant être mis à profit dans la réalisation d'un leurre GNSS. De par la popularité des GNSS, il existe aujourd'hui une large variété de cibles potentielles, qu'elles soient militaires ou civils : drones de surveillance, drones civiles, tours cellulaires utilisant le temps du PVT, contrôleurs électriques, etc... De ce fait, il est nécessaire de développer une défense face au leurrage. Ainsi la première étape dans la mise en place d'une défense contre les attaques de leurrage est la conception d'une technique efficace de détection de ces attaques. C'est ce sujet qui nous intéresse ici.

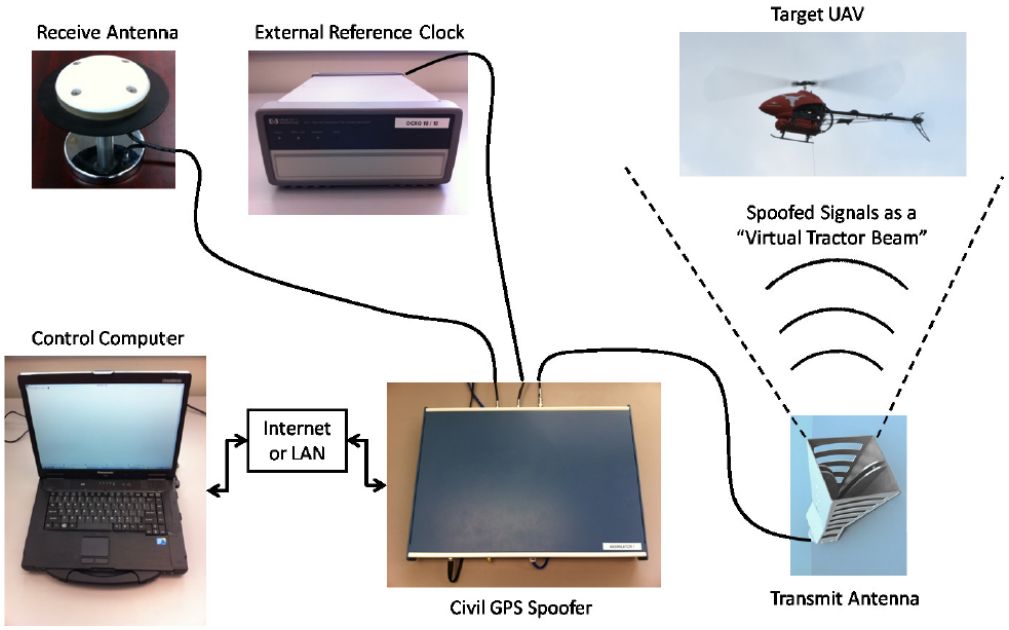

FIGURE 4 – Configuration expérimentale du leurrage du drone Hornet dans [7]

I.3 Méthodes de détection du leurrage GNSS

Une des premières méthodes de détection envisagée a été d'utiliser le RAIM pour détecter les incohérences dans les pseudo-distances calculées par le récepteur. Cependant, nous avons vu précédemment que cette technique ne marche que pour les leurres les plus basiques et l'expansion de COTS abordables et performants tend vers une augmentation du nombre de leurres cohérents. L'intérêt pour la détection des attaques de leurres cohérents est donc vite arrivée dans la littérature. Cette dernière s'est étoffée au cours des années avec de nombreuses techniques diverses et variées. A l'heure actuelle, la plupart des techniques de détection de leurrage repose sur une des deux stratégies d'action suivantes (voire parfois les deux dans certains cas) :

— la première consiste à chercher des différences entre les signaux leurrés et les vrais signaux, ces différences devant pouvoir être détectées par le récepteur de la victime,

— la deuxième va quant à elle s'intéresser aux potentielles interactions entre les signaux de leurrage et les vrais signaux, ces interactions étant quasiment inévitables (sauf pour les attaques d'annulation ou les attaques de signaux à très forte puissance).

Quand on regarde attentivement la littérature, on remarque que les techniques de détection de leurrage considérées comme les plus efficaces sont celles qui vont combiner ces deux stratégies. C'est-à-dire contrôler des différences dans les signaux, comme par exemple la puissance reçue, tout en contrôlant aussi les interactions entre leurre et vrais signaux.

Si on fait une vue d'ensemble sur les techniques de détection étudiées comme l'ont fait Psiaki et al. dans [9], on peut classer les techniques de détection de leurrage en cinq catégories :

— techniques de traitement du signal avancé pour des récepteurs à une seule antenne,

— techniques basées sur le chiffrement de signaux,

— techniques basées sur la géométrie,

— techniques basées sur le contrôle des dérives,

— techniques mixtes

I.3.1 Traitement du signal avancé pour récepteurs à une antenne

Il existe de nombreuses techniques de détection reposant entièrement sur des algorithmes de traitement du signal avancé pouvant être utilisés sur un récepteur GNSS standard. Ces méthodes reposent typiquement sur la recherche de distorsions ou de perturbations dans les caractéristiques des signaux reçus comme la puissance ou la fonction de corrélation par exemple. Afin d'élaborer une stratégie de détection de leurrage, il convient de définir quelles sont les métriques de détection qui seront utilisées. Broumadan et al. ont répertorié les indicateurs de détection les plus courants dans [10] et [13].

On peut classer ces métriques en deux types selon le stade où elles interviennent dans le processus de traitement du signal reçu par le récepteur. On parle alors de pre-désétalement lorsque c'est une métrique qui intervient avant les opérations de corrélation du récepteur et post-désétalement quand elle intervient après.

I.3.1.1 Pre-désétalement

Les méthodes en pre-désétalement "travaillent" sur le signal juste après la démodulation de la porteuse. Elles sont basées sur le contrôle de la puissance globale du signal reçu par le récepteur et font l'hypothèse que les signaux d'interférences sont plus puissants que les vrais signaux. Il s'agit donc d'une analyse globale de la puissance, il n'y a pas d'analyse séparée des différents codes PRN constituant le signal reçu. On désigne aussi ces techniques par le terme Received Power Monitoring (RPM). L'objectif est de trouver des variations anormales dans la puissance des signaux reçus. On peut délimiter trois métriques :

— l'analyse de la variance en bande de base,

— l'analyse de la densité spectrale de puissance (ou PSDA pour Power Spectral Density Analysis),

— l'analyse structurelle du contenu de la puissance (ou SPCA pour Structural Power Content Analysis).

Analyse de la variance

Ces techniques contrôlent en permanence la variance des signaux pour détecter des ajouts de puissance en provenance de signaux de leurrage. Un exemple très connu de ce type de technique de détection est présenté par Akos et al. dans [14]. La majorité des récepteurs GNSS disposent d'un module Automatic Gain Control (AGC) situé au niveau de l'étage d'entrée (front-end). L'AGC permet d'optimiser le gain appliqué sur les signaux reçus en amont du Convertisseur Analogique-Numérique (CAN). Ce gain permet d'avoir des signaux avec des niveaux de puissance adéquats en entrée du CAN. Un schéma de l'architecture d'un récepteur avec un module AGC est présenté Figure 5.

Le gain est souvent variable et une boucle de contrôle permet de réguler sa valeur en fonction des signaux d'entrée. Ceci permet d'assurer une stabilité des signaux de sortie pour en améliorer le traitement, particulièrement la numérisation. En considérant que les signaux du leurre ajoutent de la puissance sur le signal total reçu par le récepteur de la victime, Akos et al ont émis l'hypothèse que cet apport de puissance allait influencer la valeur du gain de la boucle AGC. Pour prouver cette hypothèse, deux tests de leurrage ont été mis en place sur un véhicule équipé d'un récepteur GPS. L'objectif était de déterminer l'influence d'une attaque de leurrage sur la valeur du gain de l'AGC. Le type de leurre utilisé ici est un leurre de type répéteur simple. La Figure 6 présente les données d'intérêt recueillies lors de ces tests :

— la valeur du gain de l'AGC,

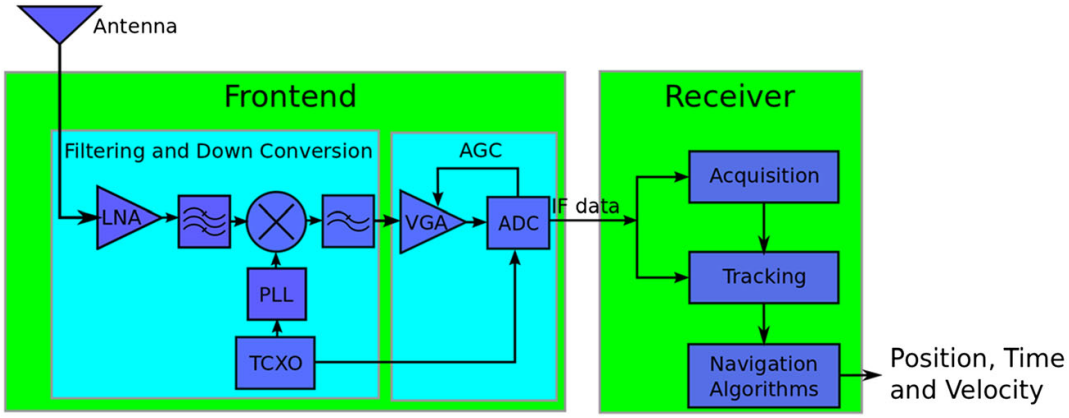

FIGURE 5 – Architecture d'un récepteur GPS avec un module AGC présenté dans [14]

— les coordonnées calculées par le récepteur GPS.

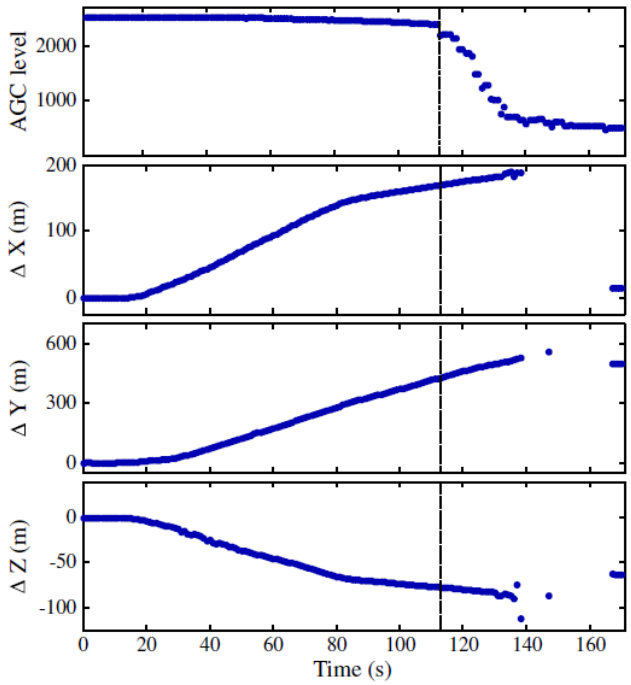

FIGURE 6 – Mesures effectuées lors d'un test de leurrage dans [14]

L'instant correspondant au passage du récepteur GPS du suivi des vrais signaux aux signaux du leurre est mis en évidence par la perte des coordonnées calculées par le récepteur GPS. Lors de ce changement de boucle de suivi on peut constater un changement drastique de la valeur du gain de l'AGC provoqué par la puissance apportée par les signaux du leurre. La puissance apportée par le leurre répéteur est donc assez forte pour faire fluctuer de manière significative le gain du module AGC.

Cependant le leurre répéteur utilisé est assez simple et utilise des puissances directement supérieures aux puissances des signaux GPS perçus localement. Dans le cas d'une attaque plus subtile comme celle exploitant des signaux de faible puissance et utilisée avec succès dans [12] et [7], le gain de l'AGC risque de ne pas varier autant que dans le cas du leurre répéteur simple. Par ailleurs, l'étude d'Akos et al. montre également que le gain de l'AGC varie également selon la température et selon la présence ou non d'obstacles bloquant les

signaux GPS. Ceci suggère que les variations de gain de l'AGC peuvent être un bon indicateur de la "qualité opérationnelle" de l'environnement où se trouve le récepteur GPS mais sans présumer que les variations éventuelles sont liées à un leurre ou un phénomène naturel.

Analyse de la densité spectrale de puissance

Une autre approche en pre-désétalement s'intéresse à la densité spectrale de puissance. Les signaux en bande étroite sont plus faciles à étudier dans le domaine fréquentiel. On définit alors un critère statistique permettant de détecter la présence d'interférence de type leurrage. Ce critère peut être formulé comme suit [15] :

$$\Gamma_{PSD} = \max_{k} \left\{ \left| \sum_{n=0}^{N_s-1} r[n] e^{-j\frac{2\pi nk}{N_s}} \right|^2 \right\} \tag{I.9}$$

avec :

— N_s le nombre d'échantillons sur lesquels la transformée de Fourier discrète a été calculée,

— k allant de 0 à $N_s - 1$,

— $r[n]$ l'échantillon n du signal reçu après conversion analogique/numérique

On considère avoir détecté un signal d'interférence si Γ_{PSD} dépasse un seuil de détection prédéfini. On suppose que ce seuil a été choisi sur la base d'un ensemble de données "propres" et d'une probabilité de fausse alarme arbitraire.

Analyse du contenu structurel de la puissance (SPCA)

La SPCA, introduite par Jafarnia-Jahromi et al. [1], est une approche de faible complexité qui tire parti du caractère cyclo-stationnaire des signaux GNSS pour détecter parmi les échantillons reçus une quantité excessive de puissance issue de signaux "structurés". Par le biais d'un ensemble d'opérations et de filtrage il est possible "d'éliminer" le bruit et l'effet Doppler du spectre du signal reçu. Un test statistique, détaillé dans [1] est alors utilisé sur le spectre obtenu après ces filtrages. Ce test détermine si le signal reçu présente ou non des signaux de leurrage.

I.3.1.2 Post-désétalement

Les méthodes en post-désétalement agissent après les opérations de corrélation du récepteur. Les métriques de détection sont :

— l'analyse du rapport Carrier-to-Noise (C/No), qui est le rapport signal à bruit après désétalement et ramené à une bande de 1 Hz,

— le contrôle de la qualité du signal (Signal Quality Monitoring ou SQM).

Analyse du rapport C/No

Trois termes peuvent affecter le rapport C/No :

— la composante du bruit,

— l'inter-corrélation entre les signaux du leurre et les vrais signaux,

— l'inter-corrélation avec d'autres signaux authentiques.

L'inter-corrélation causée par les signaux du leurre est proportionnelle à la puissance de ces derniers. Des signaux de leurrage de forte puissance peuvent alors réduire considérablement la contribution des codes PRN des vrais signaux sur le rapport C/No et en parallèle faire saturer la valeur perçue du C/No. Etant donné que la puissance maximale que peut recevoir un récepteur GNSS est a priori connue, on peut définir une valeur seuil que peut atteindre le rapport C/No. Ainsi, des valeurs anormalement élevées du rapport C/No peuvent indiquer la présence de signaux de leurrage.

Cependant, un leurre dont les signaux ont une puissance proche des signaux authentiques risque de ne pas se faire détecter avec cette méthode [16]. Ce problème peut être contourné si le récepteur est suffisamment précis dans sa mesure du C/No, mais un tel récepteur demande un coût assez important.

Contrôle de la qualité du signal (SQM)

Ces techniques se focalisent sur la fonction de corrélation du signal reçu. L'interaction de signaux de leurrage avec les vrais signaux provoque des distorsions sur la forme de cette fonction. Les techniques SQM cherchent en particulier une asymétrie, forme anormale, ou un pic de corrélation trop élevé causés par la présence de signaux parasites. A l'origine utilisées pour traiter les trajets multiples, les techniques de SQM ont vu leur intérêt s'étendre à la détection de leurrage GNSS [17]. En supposant que le récepteur soit déjà en train de suivre de vrais signaux on peut mettre en place un test de rapport de symétrie formulé de cette façon :

$$SQM = \frac{(I_{-d} - I_{+d})}{I_0} \tag{I.10}$$

où I_d est la valeur du déphasage en sortie du corrélateur espacée de d chips. Si le SQM dépasse un certain seuil on considère alors qu'il y a une attaque de leurrage. L'avantage du SQM est qu'il n'est pas nécessaire d'avoir de l'information a priori (données propres, valeurs standards d'un paramètre, etc...). En tant que technique de détection de leurrage les résultats des études dans la littérature, comme celles de Manfredini et al. [18] et Huang et al. [19], ont montré de bons résultats.

Bilan

Globalement les techniques pre-désétalement ont une vitesse de traitement plus grande que les techniques post-désétalement et elles sont plus efficaces et plus rapides à détecter les interférences [15]. Cependant, ces méthodes présentent quelques désavantages. Dans leur article, Broumadan et al. montrent que ces métriques de détection, à elles seules, ne sont pas exclusives aux interférences de type leurrage. En effet, des interférences comme les interférences de chemin multiple (diffraction/réflexion) ou les chirp (onde sinusoïdale dont la fréquence balaie sa bande passante de façon répétée) peuvent avoir la même influence que les interférences de type leurrage sur certains ces indicateurs de détection. Ainsi, pour pouvoir discriminer le leurrage des autres interférences, il est nécessaire de combiner ces techniques en utilisant les métriques adéquates (c'est-à-dire qui permettent de réduire les interférences possibles).

De plus, dans le cas des techniques qui s'intéressent à la fonction de corrélation, un autre inconvénient est leur faiblesse face à des signaux de leurrage beaucoup trop puissants. Si un leurre utilise des signaux avec une puissance suffisamment forte pour "noyer" les vrais signaux on ne peut détecter les signaux du leurre que dans la phase où ils sont faibles ce qui diminue les performances de ces techniques.

Par ailleurs, un autre problème avec ces techniques est la nature éphémère de leur application. Une fois le passage du récepteur des vrais signaux aux signaux de leurrage, les distorsions et les variations recherchées sont moins évidentes à trouver car elles ont souvent lieu lors de la transition entre les vrais signaux et les faux signaux. En effet, une fois que le récepteur est accroché au leurre, ce dernier peut se permettre de réduire sa puissance et de ce fait perdre tout aspect suspicieux. Cela nécessite donc de garder une historicité des valeurs des métriques de détection.

I.3.2 Chiffrement des signaux

La meilleure solution pour contrer les interférences de type leurrage est de passer par le cryptage des signaux en cryptant l'entièreté du code d'étalement $C_i(t)$ par une clé de chiffrement. Bien que ce soit déjà le cas avec le GPS militaire, crypter les signaux du GPS/GNSS civils n'est pas envisageable et ce pour deux raisons :

— cela irait à l'encontre du principe de transparence et d'ouverture des GNSS,

— cela nécessiterait de reconfigurer la totalité des satellites des constellations GNSS ce qui représente un coût extrêmement élevé en plus de rendre obsolète tous les récepteurs GPS mis sur le marché depuis 1991.

Malgré ces inconvénients, il existe dans la littérature quelques techniques basées sur le chiffrement des signaux. Ce sont principalement des techniques reposant sur un système d'authentification. On peut citer l'utilisation de clés symétriques Spread Spectrum Security Code (SSSC) sur de courts segments intercalés entre de longs segments de codes PRN C_i qui sont eux prévisibles. Les portions connues servent au suivi des signaux GNSS et les portions inconnues sont enregistrées par le récepteur. Après la diffusion du SSSC, une clé signée arrive dans les données $D_i(t)$. Une fois la clé vérifiée, cette dernière est utilisée pour synthétiser le code PRN inconnu qui est corrélé avec les portions inconnues pour vérifier l'authenticité du signal. Cette méthode génère beaucoup de latence (de l'ordre de quelques secondes voire plusieurs minutes).

Une autre technique utilisant une approche de clé asymétriques privée/publique existe. il s'agit de la méthode Navigation Message Authentication (NMA) détaillée dans [20] et [21]. Cette technique consiste à inclure dans les données une signature numérique imprévisible générée à partir d'une clé privée par le segment de contrôle GNSS. Le récepteur sait où se trouve cette signature dans le flux de données et la vérifie à l'aide d'une clé publique.

Ces deux techniques présentent néanmoins de gros inconvénients. Premièrement, les utiliser va engendrer de la latence dans le fonctionnement du récepteur. Cette latence va de pair avec la longueur des clés d'authentification. Enfin ces méthodes n'enlèvent pas le problème évoqué précédemment qui est la nécessité de modifier les signaux GNSS à la source, c'est-à-dire au niveau des satellites, ce qui n'est pas très pratique.

Il existe cependant une technique qui ne nécessite pas de modifier les signaux. Cette technique, étudiée par Psiaki et al. en 2013 dans [22] et O'Hanlon et al. dans [2], exploite la relation entre le signal civil et le signal militaire. Dans le système GPS, les codes C/A (civil) et P(Y) (militaire) sont modulés en quadrature de phase sur la même porteuse. Un leurre n'a a priori pas connaissance du code militaire, il ne peut donc pas le reproduire dans ses signaux. En comparant des portions identiques de ce qui doit être le code P(Y) on peut savoir si un leurre envoie des signaux au récepteur. Pour cela on doit utiliser deux récepteurs GNSS le premier est la victime potentielle d'une attaque de leurrage tandis que le deuxième est un récepteur protégé afin de s'assurer qu'il ne subit aucun leurrage. Les deux récepteurs doivent pouvoir communiquer par le biais d'un tiers chargé des opérations de corrélation. La Figure 7 représente l'architecture utilisée par O'Hanlon et al. dans [2] pour l'étude de cette technique

La Figure 8 représente les codes PRN reçus par les deux récepteurs (le récepteur sécurisé à gauche et le récepteur potentiellement attaqué à droite).

Le code C/A est représenté en bleu et le code P(Y) en rouge et vert. A l'aide du code C/A des deux récepteurs on extrait une portion du code P(Y) sur les deux récepteurs. Cette portion extraite est trop bruitée pour en connaître le contenu exact. Néanmoins, on peut quand même inter-corréler ces portions bruitées pour détecter la présence du code P(Y) dans le récepteur susceptible d'être leurré. Si le pic de corrélation est élevé alors le signal reçu est déclaré authentique, sinon il s'agit d'un leurre. Cette méthode a l'avantage de fonctionner quasiment en temps réel à condition d'avoir un canal de communication entre les deux récepteurs, ce qui limite grandement la mise en place d'une telle technique. Par ailleurs si un leurre adopte la même stratégie, à savoir rajouter la signature du signal P(Y) sur ses signaux de leurrage alors le leurre restera non détecté.

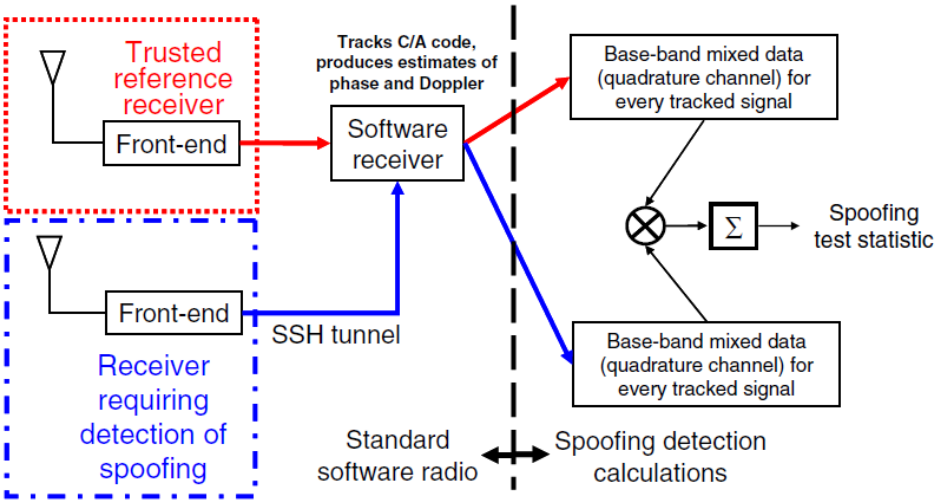

FIGURE 7 – Architecture nécessaire à la mise en place de la stratégie de [2]

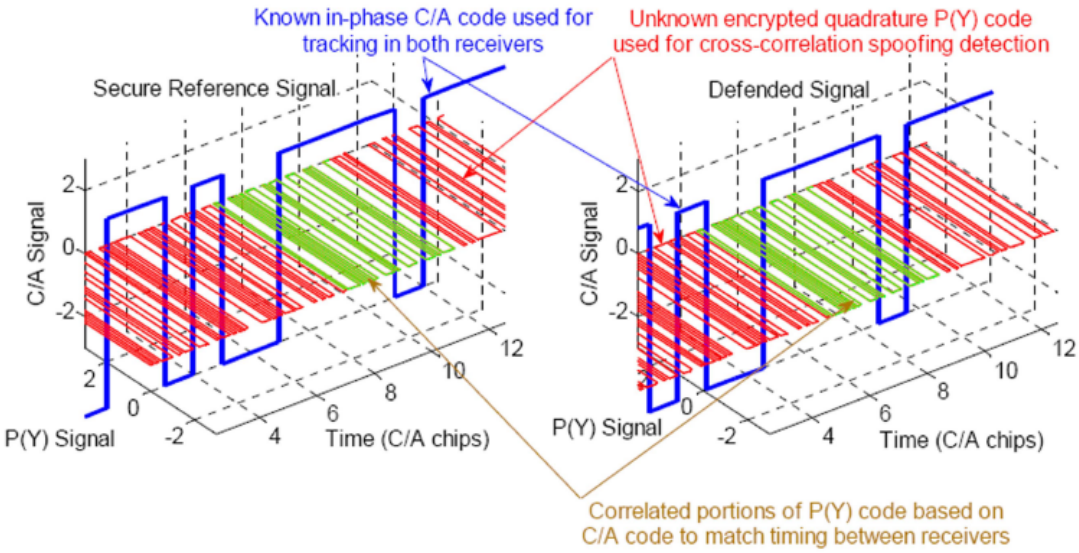

FIGURE 8 – Représentation des codes reçus sur les deux récepteurs dans [22]

I.3.3 Géométrie des signaux

Ce type de techniques va s'intéresser à la direction d'arrivée des signaux GNSS. Il existe de nombreuses "variantes" dans cette catégorie de méthodes de détection et on trouve donc beaucoup d'articles traitant de ce sujet dans la littérature comme l'étude de Montgomery et al. dans [23] ou celle de Psiaki et al. dans [24]. La plupart de ces techniques sont basées sur l'utilisation d'un minimum de deux antennes de réception, parfois avec un seul récepteur, parfois avec plusieurs récepteurs. On se retrouve alors typiquement avec une configuration similaire à celle présentée par [24] et répertoriée ici Figure 9.

Pour déterminer les directions d'arrivée, on utilise le déphasage de la porteuse qui peut être modélisée par :

$$\frac{\lambda\phi_i}{2\pi} = \rho_0^i + (\hat{\boldsymbol{\rho}}^i)^T \Delta\boldsymbol{d} + c(\delta_r - \delta^i) + \frac{\lambda\beta^i}{2\pi} \tag{I.11}$$

avec :

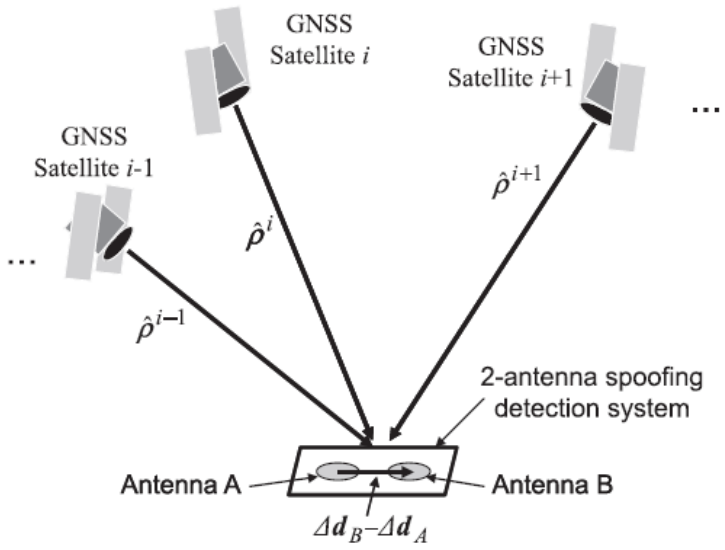

FIGURE 9 – Configuration usuelle pour les techniques géométriques à 2 antennes

— λ : longueur d'onde de la porteuse,

— ρ_0^i : la distance nominale du satellite i,

— $\hat{\boldsymbol{\rho}}^i$: le vecteur unité satellite $i \rightarrow$ récepteur,

— $\Delta \boldsymbol{d}$ le déplacement de l'antenne de réception par rapport à la localisation nominale du récepteur,

— δ_r et δ^i le biais des horloges du récepteur et du satellite i,

— β^i : le biais du déphasage de la porteuse inconnu.

Un récepteur peut se servir de l'interférométrie pour mesurer la direction d'arrivée du vecteur $\hat{\boldsymbol{\rho}}^i$ à partir de trois antennes ou plus avec des décalages de $\Delta \boldsymbol{d}$ différents. Si on souhaite n'utiliser qu'une seule antenne, comme dans [24], on peut mettre en mouvement l'antenne selon un profil spécifique $\Delta d(t)$. Par contre si on n'utilise que deux antennes ou un profil une dimension pour d alors on ne peut pas estimer les trois composantes du vecteur $\hat{\boldsymbol{\rho}}^i$ mais au moins une composante. Un bon récepteur GNSS permet d'atteindre de bonnes mesures pour le vecteur $\hat{\boldsymbol{\rho}}^i$ (environ 3° pour un $\Delta \boldsymbol{d}$ de 0.1 mètre).

Dans le cas où le récepteur n'est pas victime de leurrage, les vecteurs $\hat{\boldsymbol{\rho}}^i$ sont distribués autour du récepteur et viennent du ciel comme sur la Figure 9. Si un leurre effectue une attaque simple, les vecteurs $\hat{\boldsymbol{\rho}}^i$ et donc les signaux reçus proviendraient de la même source et pointeraient donc vers la même direction. Un système de détection de leurrage basé sur la géométrie des signaux va tester si les déphasages ϕ_i reçus aux différentes antennes du récepteur sont plus cohérentes avec la diversité de directions $\hat{\boldsymbol{\rho}}^i$ attendue sur des signaux authentiques ou avec l'uniformité de directions donnée par un simple leurre. La décision sur la présence ou non de leurrage se fait souvent de manière statistique. Par exemple Borio et al. dans [3] et [25] utilisent un détecteur de type Sum-of-Squares (SoS) pour déterminer si toutes les directions d'arrivée des signaux sont communes.

Certaines méthodes n'estiment pas directement $\hat{\boldsymbol{\rho}}^i$ mais vont plutôt exploiter la présence de capteurs inertiels présents sur le système. Les mouvements imposés par le contrôle d'un drone et le vent permettent d'obtenir un historique temporel de $\Delta \boldsymbol{d}$ qu'une centrale inertielle peut sentir. Ceci est difficile à prévoir pour un leurre.

Donc si on remarque que les variations hautes fréquences cohérentes avec chaque vecteur $\hat{\boldsymbol{\rho}}^i$ sont absentes de chaque $\phi_i(t)$ alors une attaque de leurrage a sûrement lieu.

Ces techniques de détection ont le désavantage d'être inefficaces sur un leurre sophistiqué qui transmet ses faux signaux depuis plusieurs directions différentes. Ce type de leurre étant plutôt difficile à mettre en place, les méthodes géométriques gardent tout de même un fort intérêt.

I.3.4 Techniques mixtes

I.3.4.1 Combinaison de techniques

Toutes les techniques présentées jusqu'ici ne sont pas parfaites. Elles possèdent toutes leurs lots d'avantages et d'inconvénients. En effet toutes les techniques de détection ne sont pas efficaces contre tous les modes d'attaque possibles et inversement. Ces inconvénients peuvent être des faiblesses exploitables par des leurres sophistiqués afin de rester indétectables par le système victime de l'attaque de leurrage.

Fort heureusement, les faiblesses d'une méthode de détection peuvent être compensées par une autre technique de détection complémentaire. Par exemple un leurre peut volontairement utiliser des signaux de forte puissance pour éviter les distorsions sur la fonction de corrélation complexe et donc être non détecté par une méthode qui analyse la fonction de corrélation. Si on complète cette analyse de la fonction de corrélation par une technique de type RPM, le récepteur va très certainement détecter l'attaque de leurrage. Inversement, un leurre peut employer une technique d'accrochage lente pour contrer un contrôle de dérives. Dans ce cas là, rajouter une analyse de la fonction de corrélation serait judicieux étant donné que le leurre, par son approche lente, donne une plus grande marge temporelle pour détecter des distorsions anormales de la fonction de corrélation. Par exemple Wesson et al. et Gross et al. dans [26] et [27] ont développé une technique de détection de leurrage basée à la fois sur le contrôle de la puissance reçue et sur la recherche de distorsion de la fonction de corrélation.

I.3.4.2 Combinaison avec "l'extérieur"

Par ailleurs, une autre approche possible pour pallier les faiblesses des techniques énumérées précédemment est de s'aider d'éléments extérieurs pouvant fournir de l'information en rapport avec le positionnement et/ou la navigation. Cette approche s'applique très bien aux systèmes mobiles comme les véhicules, les bateaux ou plus particulièrement les drones volants. De tels systèmes sont tous susceptibles d'embarquer, en plus d'un récepteur GNSS, de nombreux capteurs inertiels. Ces capteurs sont très utiles pour évaluer le comportement du système lors de la navigation. L'idée qui nous intéresse ici serait donc de combiner les techniques de traitement d'information au niveau récepteur avec les informations issues des autres capteurs présents sur le système. Ce type d'approches est souvent utilisé sur les drones car ils sont tous équipés avec un minimum de capteurs inertiels.

On retrouve donc dans la littérature quelques techniques basées sur la combinaison du récepteurs GNSS avec un ou plusieurs autres capteurs. Les différentes techniques se distinguent les unes des autres par la manière dont l'association GNSS-inertiel est exploitée pour la détection d'attaque de leurrage. On peut citer par exemple les travaux de Zou et al. dans [28]. Cet article présente une méthode de détection d'attaque de leurrage sur un drone quadrotor. Cette méthode est basée sur l'estimation du comportement du drone à partir d'un modèle. Pour appliquer cette technique il faut dans un premier temps modéliser le comportement du drone par un modèle physique. Ce modèle est établi par le biais des différentes équations mathématiques issues des équations de la dynamique et de la mécanique des solides. Ce modèle d'estimation est "nourri" par les données GPS, les données inertielles et les commandes initiales que l'utilisateur a définies pour un vol autonome (c'est-à-dire la trajectoire désirée). A partir de ces informations à un instant t, le modèle va prédire le comportement et l'état du drone à l'instant suivant.

La partie détection a lieu juste après. On va définir l'erreur ϵ comme étant la différence entre l'estimation et le comportement réel du drone. On va ensuite définir un seuil de détection sur cette erreur qui va nous indiquer si le drone est en sécurité ou attaqué par un leurre. Les essais réalisés pour cette technique n'ont été fait qu'en simulation sur Matlab et montrent des résultats encourageants. Tout d'abord on constate que l'attaque

de leurrage appliquée a été un succès, comme le montre la Figure 10. Cette Figure montre la position selon l'axe x au cours du temps et on remarque que le leurre a bien décalé la trajectoire du drone.

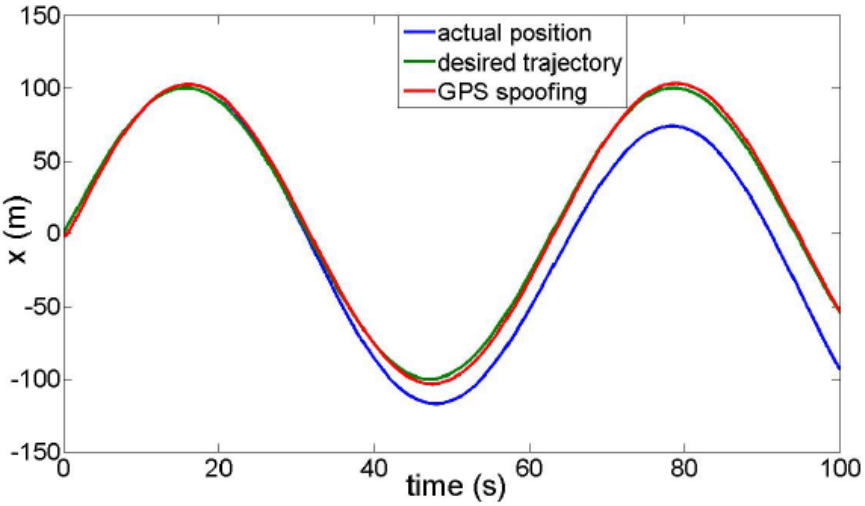

FIGURE 10 – Trajectoire du drone selon l'axe x dans [28]

Ensuite quand on regarde l'erreur ϵ sur l'axe x on obtient la courbe présentée Figure 11.

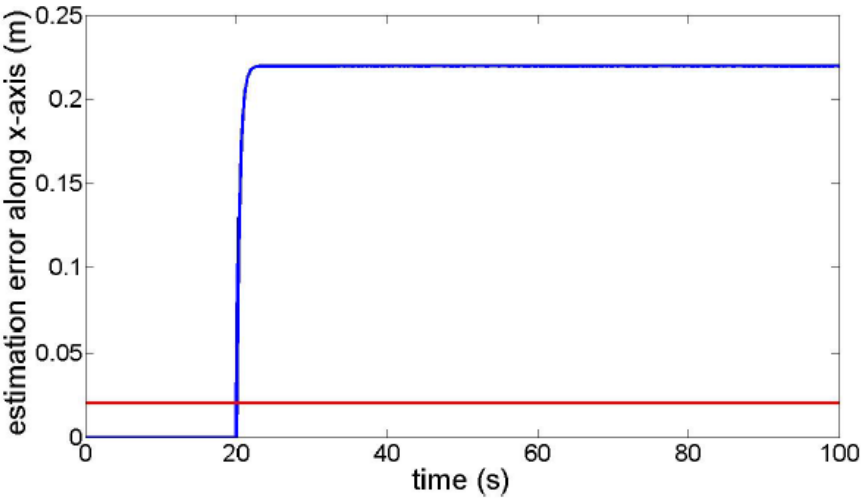

FIGURE 11 – Erreur d'estimation selon l'axe x dans [28]

On constate que l'erreur (en bleu sur la courbe) présente un saut de valeur significatif après le lancement des signaux du leurre. Ce saut dépasse largement le seuil de détection prédéfini (en rouge sur la courbe). Ceci confirme la bonne détection de l'attaque de leurrage de cette technique.

On peut trouver dans la littérature des techniques exploitant la fusion de données entre les capteurs inertiels et le récepteur GNSS. Par exemple on peut citer l'article de Panice et al. [5]. Cet article présente une technique de détection des attaques de leurrage par l'utilisation d'un algorithme SVM sur un drone. Cette méthode exploite la fusion de données entre le GPS et les capteurs inertiels pour déterminer la position du drone. Les

résultats de cette fusion de données sont alors donnés à un algorithme SVM qui va classifier les données pour déterminer si le drone est en situation normale ou en situation d'attaque de leurrage. Dans le même type d'approches Tanil et al. dans [29] exploitent également la fusion de données inertiels/GNSS par le biais de filtres de Kalman qui restent efficaces même contre des leurres sophistiqués capables de suivre leur victime.

I.3.5 Contrôle de dérives

Il reste une dernière catégorie de méthode de détection de leurrage qui nous intéresse plus particulièrement. Il s'agit de la catégorie du contrôle de dérives. Ce type de défense va s'intéresser à la recherche de changements non usuels dans la position du récepteur GNSS ou son horloge au cours de sa navigation. Par exemple si un leurre provoque un changement trop rapide de l'erreur de l'horloge du récepteur, alors la victime peut être capable de détecter ce changement par le biais de la dérive de l'horloge qui présenterait des valeurs trop élevées pour sa classe d'oscillateur.

De même, une centrale inertielle ou tout autre capteur de mouvement peut être utilisé de la même manière. Si on constate des dérives sur la position, la vitesse ou l'accélération qui semblent irréalisables pour le système considéré, alors on peut considérer cela comme une alerte de leurrage.

Il peut cependant arriver que certains leurres prennent leur temps dans la capture de leur cible. Cette capture lente n'engendrerait pas de changement brusque ce qui permet de passer les contrôles de dérives sans être détecté. Cependant cette progression soutenue dans l'attaque rend le leurre vulnérable à d'autres techniques de détection.

Les techniques de détection basées sur le contrôle de dérives peuvent s'avérer très utiles sur des attaques de type meaconing ou SCER. Un exemple probant de ces techniques est l'article de Marnach et al. [4]. Dans cet article, Marnach et al. cherchent à détecter une attaque de meaconing par l'analyse du biais d'horloge d'un récepteur GNSS. En effet, le biais d'horloge et sa dérive ont un comportement prévisible au cours du temps. Le comportement "normal" du biais d'horloge et de sa dérive est représenté sur la Figure 12

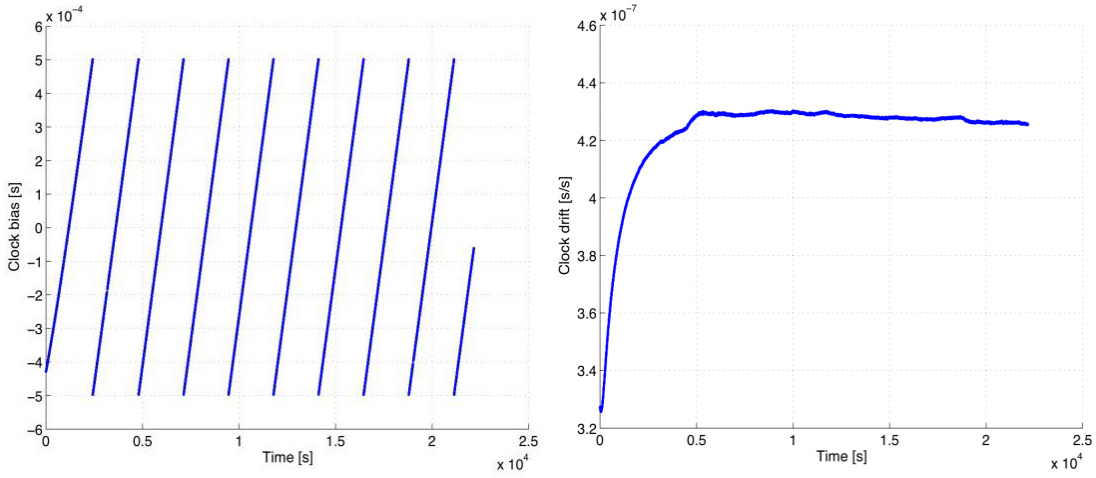

FIGURE 12 – Biais d'horloge (à gauche) et sa dérive (à droite) en situation normale présentés dans [4]

Un récepteur GNSS calcule le biais d'horloge et sa dérive à partir des pseudo-distances qu'il reçoit des satellites. Ces pseudo-distances sont altérées lors d'une attaque de meaconing ce qui devrait logiquement avoir un influence sur le biais d'horloge. L'objectif des tests réalisés dans [4] était donc de détecter à la fois le début et la fin d'une attaque de meaconing. Ces tests ont été réalisés avec des COTS en environnement contrôlé. Afin de mieux visualiser les effets du meaconing sur le biais d'horloge, il a été décidé de réduire l'échelle d'observation en observant non pas directement le biais d'horloge mais plutôt son erreur. Pour cela, à partir d'un ensemble de points S on calcule une estimée du biais d'horloge sur ce ensemble de point S

par régression linéaire $b^{(S)}(t)$. On définit ensuite l'erreur de biais d'horloge e à l'instant t selon S comme la différence entre le biais d'horloge b à l'instant t et l'estimation du biais à l'instant t :

$$e_t^{(S)} = b_t - b^{(S)}(t) \tag{I.12}$$

La courbe de l'évolution de l'erreur du biais d'horloge qu'ils ont obtenu lors de leurs tests est donnée Figure 13

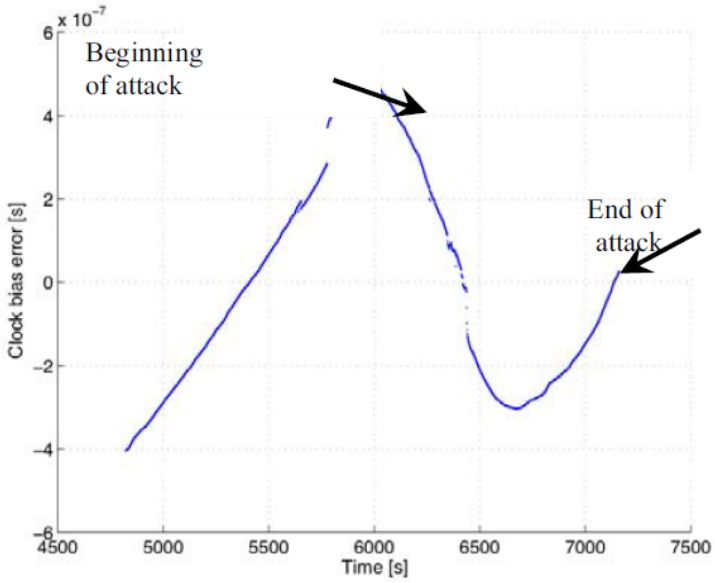

FIGURE 13 – Erreur du biais d'horloge au cours d'une attaque de leurrage dans [4]

Sur cette courbe on constate nettement des changements brusques et inattendus sur l'erreur du biais d'horloge qui ont lieu au début et à la fin de l'attaque de meaconing. Ces changements brusques peuvent donc être utilisés comme indicateurs d'une attaque de meaconing. Le meaconing étant une "sous-version" du leurrage, on peut supposer par intuition qu'un leurrage aurait les mêmes effets sur le biais d'horloge d'un récepteur GNSS et sa dérive.

Une approche similaire peut être adoptée avec les pseudo-distances. Lui et al. se sont penchés sur cette possibilité dans [30] dans le cas d'une attaque de leurrage. Contrairement à Marnach et al, des tests matériels en environnement contrôlé n'ont pas été réalisés. Cependant des simulations sur Matlab ont pu être menées en utilisant un ensemble de données collectées par un récepteur NovAtel en 2012. Ces simulations donnent des résultats encourageants, similaires à ce que Marnach et al. ont pu constater lors de leurs essais de meaconing.

I.3.6 Bilan

Cet état de l'art met en évidence que les leurres GNSS sont une menace non négligeable. Les recherches sur des techniques de détection de leurrage GNSS sont très nombreuses et variées. Une bonne partie d'entre elles se focalise sur le traitement de signal avancé et les propriétés géométriques des signaux. Cependant ce type de techniques peut nécessiter l'ajout de matériels ou une puissance de calcul supplémentaire.

D'un autre côté les techniques basées sur le contrôle de dérives peuvent être utilisées sur certains systèmes sans changement ou ajout de matériel. Cela peut être le cas pour les drones par example. Pourtant ce type de techniques n'est pas couramment développé dans la littérature. Marnach et al. [4] ont traité le cas du biais d'horloge face à une attaque de meaconing, mais ce n'est pas aussi complexe ou aussi trompeur qu'une attaque de leurrage. Lui et al. [30] ont adopté une approche similaire avec du leurrage mais en se concentrant sur les pseudo-distances des satellites et non sur le biais d'horloge. Or le biais d'horloge possède l'avantage d'être

plus prévisible, que ce soit sur son comportement ou ses valeurs possibles. Il convient donc de se demander si des formes de leurrage plus avancées que le meaconing ont une influence notable sur le biais d'horloge. C'est sur cette problématique que le chapitre suivant va porter.

Chapitre II

Etude de l'influence du leurrage sur l'horloge d'un récepteur GNSS

II.1 Etude de l'influence du leurrage sur le biais d'horloge par modélisation numérique

L'objectif de cette partie est de caractériser l'action des signaux de leurrage sur l'horloge d'un récepteur GNSS, en particulier son biais et sa dérive. La présentation du fonctionnement d'une attaque de leurrage de la partie I.2.1 se focalise principalement sur les caractéristiques des signaux du leurre. Etant donné qu'on s'intéresse au biais d'horloge, qui est obtenu grâce aux données fournies par les GNSS, notre étude des effets du leurrage sur le biais d'horloge se focalise sur cet aspect (et pas sur une approche signal ou matériel).

La métrique de détection étudiée ici est le biais de l'horloge, cette étude s'apparente donc à la catégorie des contrôles de dérives détaillé au chapitre précédent à la partie I.3.5. Pour cela, la méthode de calcul du biais d'horloge par le récepteur a été étudiée afin de déterminer comment les signaux du leurre impactent le résultat du calcul du biais.

II.1.1 Calcul du biais d'horloge et comportement en condition normale d'utilisation

Comme expliqué précédemment dans l'état de l'art, le biais d'horloge représente la différence temporelle entre les horloges des satellites d'une constellation GNSS [1] et l'horloge du récepteur GNSS.

Les satellites embarquent des horloges atomiques qui ont une dérive plutôt stable, tandis que les récepteurs GNSS utilisent un cristal de quartz parfois compensé en température (désignés par le terme TCXO pour Temperature Compensated X Oscillator) dont la stabilité n'égale pas celle des horloges atomiques. Les problèmes de synchronisation des satellites et des récepteurs avec le temps du système GNSS sont différents. La synchronisation des satellites est traitée par le segment de contrôle du système GNSS à l'aide d'algorithmes spécifiques comme le filtrage de Kalman par exemple.

Le biais d'horloge est calculé en même temps que les coordonnées du récepteur en résolvant le système d'équations de navigation (I.1) décrit précédemment (en I.1.2). On utilise ici la méthode de résolution standard qui est celle des moindres carrées. Pour rappel, la solution du système est

$$\begin{cases} \mathbf{\Delta x} = \mathbf{H}^{-1}\mathbf{\Delta}\rho & \text{si N=4} \\ \mathbf{\Delta \tilde{x}} = \left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{\Delta}\rho & \text{si N>4} \end{cases}$$

1. Les satellites d'une constellation sont synchronisés sur le temps de référence du système GNSS, à savoir GPS Time (GPST) pour GPS, GLONASS Time (GLONASST) pour Glonass, Galileo System Time (GST) pour Galileo, Beidou Time (BDT) pour Beidou

avec N le nombre de satellites visibles de la constellation. Posons $h_{4,j}$ le j^{me} terme de la dernière ligne de la matrice de résolution du système (donc $\mathbf{H^{-1}}$ ou $(\mathbf{H^T H})^{-1}\mathbf{H^T}$). On peut alors exprimer le biais d'horloge par l'expression suivante :

$$\Delta t_u = -\frac{1}{c}\sum_{j=1}^{N} h_{4,j}\Delta\rho_j \tag{II.1}$$

Pour comprendre comment le biais d'horloge se comporte dans des conditions normales, c'est-à-dire sans interférence, un enregistrement de ce dernier a été réalisé sur un récepteur GNSS commercial. Ce récepteur est le u-blox EVK-6T (nommé u-blox 6 par la suite) et il s'agit plus précisément d'un récepteur GPS. Même s'il s'agit d'un récepteur GPS, les résultats obtenus avec ce dernier restent globalement valides pour n'importe quelle constellation GNSS.

Cet enregistrement a été réalisé dans le cas où le récepteur reste à une position fixe sur une durée d'un peu moins de trois heures. Les Figures 14 et 15 montrent le biais d'horloge et la dérive du biais calculés par le récepteur durant cet enregistrement.

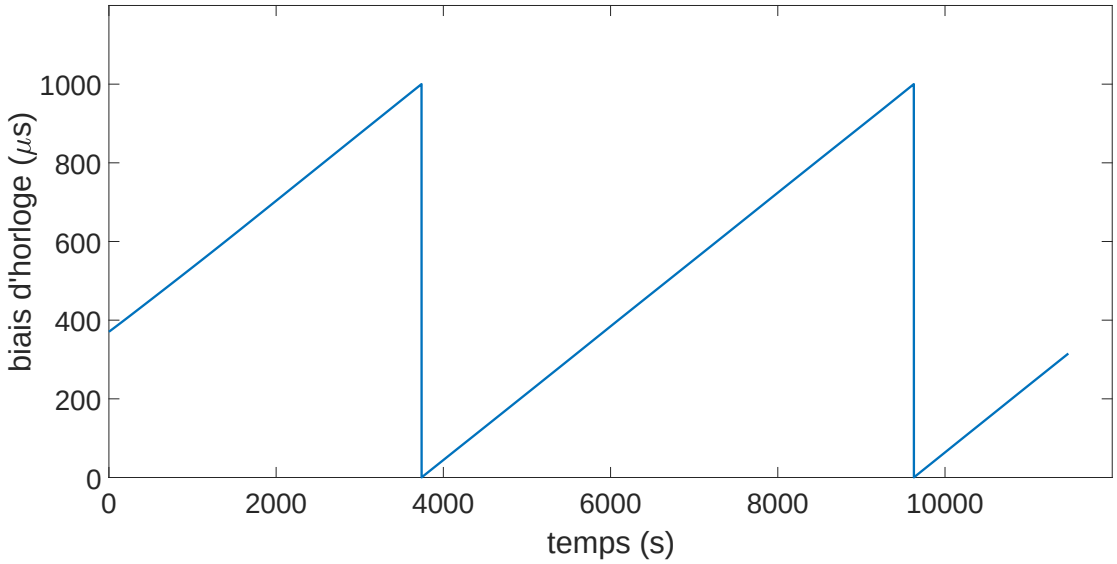

FIGURE 14 – Biais d'horloge calculé par un récepteur GNSS commercial

Cette Figure 14 montre que le biais d'horloge a une variation stable au cours du temps. Son évolution est similaire à un signal en *dents de scie*, avec une partie linéaire qui peut être croissante ou décroissante. Cette forme vient du fait que le récepteur remet à zéro le biais d'horloge lorsque celui-ci atteint ± 1 ms.

Par ailleurs, il y a un autre phénomène important qui influence la synchronisation temporelle : la dérive du biais d'horloge. Il s'agit de la première dérivée temporelle du biais d'horloge et le récepteur GNSS la calcule en même temps que le biais d'horloge, par l'intermédiaire des mesures Doppler. La Figure 14 montre une évolution linéaire du biais d'horloge, ce qui laisse penser que la dérive est constante. Or la Figure 15 montre que ce n'est pas le cas. La dérive de biais présente de faibles variations au cours du temps (de l'ordre de la ns/s).

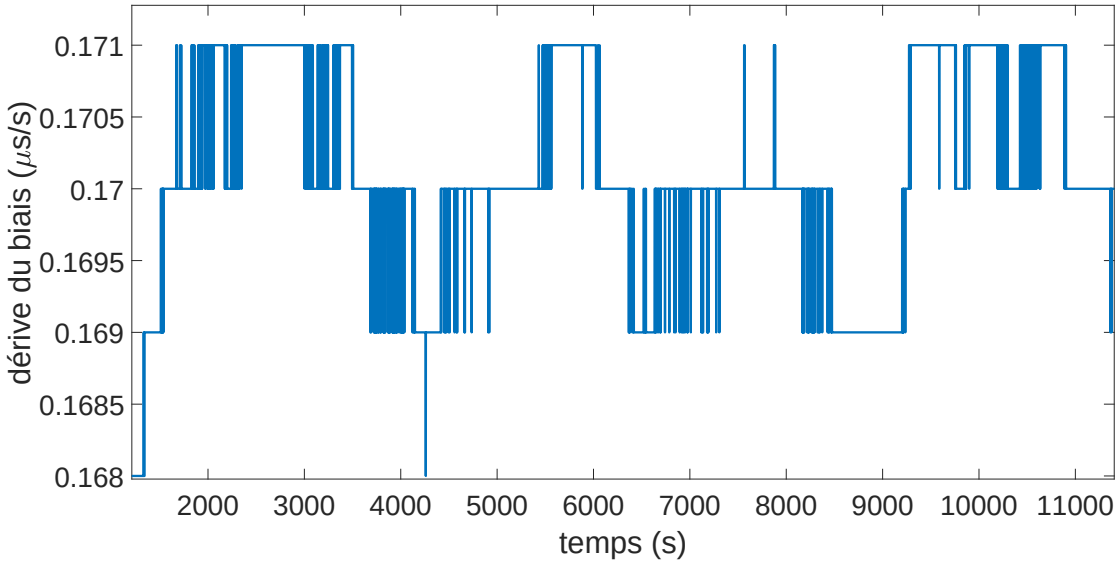

FIGURE 15 – Dérive du biais calculée par un récepteur GNSS commercial

II.1.2 Calcul du biais d'horloge et comportement lors d'une attaque de leurrage

L'objectif d'un leurre est de modifier la solution PVT obtenue en résolvant le système d'équations de navigation. Il peut donc agir sur deux éléments, les positions des satellites et les pseudo-distances, en leur ajoutant des termes "d'erreurs". Notons respectivement $\epsilon_{\rho j}$, ϵ_{xj}, ϵ_{yj}, et ϵ_{zj} les termes d'erreurs des pseudo-distances et des coordonnées des satellites dans le repère ECEF. L'équation (I.1) peut alors s'écrire, pour un satellite j :

$$\rho'_j = \sqrt{(x'_j - x_u)^2 + (y'_j - y_u)^2 + (z'_j - z_u)^2} + ct_u \tag{II.2}$$

avec : $\begin{cases} \rho'_j &= \rho_j + \epsilon_{\rho j} \\ x'_j &= x_j + \epsilon_{xj} \\ y'_j &= y_j + \epsilon_{yj} \\ z'_j &= z_j + \epsilon_{zj} \end{cases}$

La forme linéarisée de (II.2) est donc :

$$\Delta\rho'_j = a'_{x_j}\Delta x_u + a'_{y_j}\Delta y_u + a'_{z_j}\Delta z_u - c\Delta t_u$$

où : $\begin{cases} a'_{x_j} = \dfrac{x'_j - \hat{x_u}}{\hat{r_j}},\ a'_{y_j} = \dfrac{y'_j - \hat{y_u}}{\hat{r_j}},\ a'_{z_j} = \dfrac{z'_j - \hat{z_u}}{\hat{r_j}} \\ \hat{r_j} = \sqrt{(x'_j - \hat{x_u})^2 + (y'_j - \hat{y_u})^2 + (z'_j - \hat{z_u})^2} \\ \Delta x_u = x_u - \hat{x_u},\ \Delta y_u = y_u - \hat{y_u},\ \Delta z_u = z_u - \hat{z_u} \\ \Delta t_u = t_u - \hat{t_u},\ \Delta\rho'_j = \hat{\rho'_j} - \rho'_j \end{cases}$

Le système linéarisé peut alors s'exprimer de manière similaire à ce qui a été décrit précédemment en I.1.2 mais avec les nouveau termes définis ici, soit $\mathbf{\Delta\rho'} = \mathbf{H'\Delta X}$ avec :

$$\mathbf{\Delta}\rho' = \begin{bmatrix} \Delta\rho'_1 \\ \vdots \\ \Delta\rho'_j \\ \vdots \\ \Delta\rho'_N \end{bmatrix}, \mathbf{H'} = \begin{bmatrix} a'_{x_1} & a'_{y_1} & a'_{z_1} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ a'_{x_j} & a'_{y_j} & a'_{z_j} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ a'_{x_N} & a'_{y_N} & a'_{z_N} & 1 \end{bmatrix}, \text{ et } \mathbf{\Delta X} = \begin{bmatrix} \Delta x_u \\ \Delta y_u \\ \Delta z_u \\ -c\Delta t_u \end{bmatrix}$$

On remarque alors qu'après la linéarisation du système, les termes d'erreurs restent présents dans la matrice H. L'équation (II.1) peut s'appliquer avec $h'_{4,j}$ étant les termes de la dernière ligne de la matrice de résolution du système ($\mathbf{H'^{-1}}$ ou $(\mathbf{H'^T H'})^{-1}\mathbf{H'^T}$).

Vu la taille de la matrice $\mathbf{H'}$ et de sa composition il n'est pas facile de donner une expression analytique complète du biais d'horloge mettant en évidence l'impact des termes d'erreurs sur ce dernier. C'est pourquoi un modèle numérique a été développé sur Matlab afin de caractériser l'influence du leurre sur le biais d'horloge du récepteur.

II.1.2.1 Modèle Matlab

Mise en place

Afin de montrer l'influence d'une attaque de leurrage sur le biais d'horloge, un modèle numérique Matlab a été développé pour émuler une attaque d'un leurre cohérent.

Le modèle émule l'attaque de leurrage seulement sur l'aspect calculatoire du traitement des données des signaux reçus par le récepteur. Cela signifie que seules les équations utilisées pour la géolocalisation sont prises en compte et pas le modèle des signaux ou leur niveau de puissance. L'attaque de leurrage choisie pour ce modèle numérique est assez simple, on désignera par la suite cette attaque comme un leurrage fixe. Le terme "fixe" désigne ici un leurrage où la victime est à une position fixe et la fausse position diffusée par le leurre est aussi une position fixe.

La Figure 16 indique la position du récepteur (icône Maison) et la fausse position que le leurre transmet (l'icône étoile). La fausse position est située 240 m au nord de la position du récepteur et elle correspond à la position du leurre.

Pour modéliser cette attaque de leurrage, il est nécessaire de modéliser trois parties :

— les constellations de satellites, via leurs coordonnées dans le repère ECEF,

— le calcul de pseudo-distances,

— le calcul des coordonnées et du biais d'horloge par le récepteur

Pour émuler les satellites, on utilise des données d'éphémérides d'une constellation GNSS. Les données d'éphémérides contiennent des informations relatives aux orbites des satellites. Ces informations, valides sur une période de quelques heures, permettent de calculer les coordonnées des satellites de la constellation dans le repère ECEF pour chaque seconde de l'intervalle de validité [6].

On considère ici un cas purement théorique où le leurre utilise une attaque parfaite, c'est-à-dire que la constellation du leurre est identique à la constellation GNSS que le récepteur ciblé reçoit : mêmes satellites, mêmes positions et mêmes temps GNSS (synchronisation parfaite). On utilise donc les mêmes éphémérides pour émuler la constellation GNSS et la constellation du leurre. De plus, comme les constellations sont identiques, le leurre ne va introduire des termes d'erreurs que sur les pseudo-distances (soit $\epsilon_{xj} = \epsilon_{yj} = \epsilon_{zj} = 0$ et $\epsilon_{\rho j} \neq 0$). Les positions des satellites étant maintenant connues, il faut avoir la valeur du biais d'horloge pour

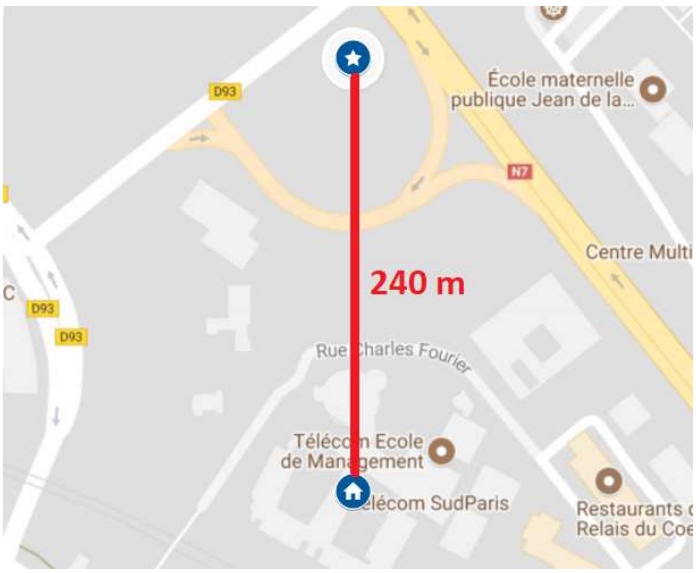

FIGURE 16 – Positions utilisés pour les essais

calculer les pseudo-distances.

Le biais d'horloge du récepteur est émulé par le code sur une durée arbitraire en utilisant une boucle temporelle. Il se comporte de la même manière que sur la Figure 14 en définissant une valeur initiale de biais et une valeur de dérive. Un terme de bruit blanc gaussien est aussi utilisé pour émuler le bruit naturellement présent sur les données de pseudo-distances. En utilisant les pseudo-distances et les positions des satellites, le récepteur peut calculer sa position et son biais d'horloge via une fonction permettant la résolution des équations de navigation décrites précédemment.

Déroulé des événements

Le modèle commence par une initialisation de la position du récepteur, du biais d'horloge et de la position des satellites. Cette première initialisation permet d'avoir les termes estimés nécessaires à la résolution du système d'équations (c'est à dire les termes $\hat{x_u}$, $\hat{y_u}$, $\hat{z_u}$, $\hat{t_u}$). Pour la suite, ces termes estimés pour l'instant t seront les termes de la solution à $(t-1)$.

Chaque seconde, les positions des satellites sont mises à jour et le processus de calcul de position basé sur les équations de navigation est appliqué pour obtenir les coordonnées du récepteur et son biais d'horloge. A un instant arbitraire de la boucle, le récepteur est forcé de passer de la constellation GNSS à la constellation du leurre. Appelons t_s cet instant arbitraire. Quand $t < t_s$ les vraies pseudo-distances (ρ_j) sont utilisées par le processus de calcul de position. Le système d'équations qui doit être résolu est donc le système "classique" :

$$\rho_j(t) = \sqrt{(x_j(t) - x_u(t))^2 + (y_j(t) - y_u(t))^2 + (z_j(t) - z_u(t))^2} + ct_u(t) \tag{II.3}$$

avec $j = \{1, ..., N\}$ et N le nombre de satellites visibles de la constellation (pour notre modèle, $N = 7$).

Quand $t \geq t_s$ les "fausses" pseudo-distances (ρ'_j) sont alors utilisées. Pour déterminer ces fausses pseudo-distances $\rho'_j(t)$, on commence par calculer les pseudo-distances entre les satellites de la constellation et le faux point. Puis on ajoute la distance entre l'antenne du leurre et le récepteur afin de prendre en compte le trajet parcouru par les signaux émis par le leurre pour atteindre le récepteur. Si on note $(x_f(t), y_f(t), z_f(t))$,

$t_e(t)$ et d_{lu} respectivement les coordonnées du faux point, la valeur du biais émulé par le modèle à l'instant t, et la distance entre l'antenne du leurre et le récepteur, on a alors :

$$\rho'_j(t) = \sqrt{(x_j(t) - x_f(t))^2 + (y_j(t) - y_f(t))^2 + (z_j(t) - z_f(t))^2} + ct_e(t) + d_{lu}(t) \tag{II.4}$$

Connaissant maintenant $\rho'_j(t)$, le système d'équations que le récepteur doit résoudre devient :

$$\rho'_j(t) = \sqrt{(x_j(t) - x_u(t))^2 + (y_j(t) - y_u(t))^2 + (z_j(t) - z_u(t))^2} + ct_u(t) \tag{II.5}$$

Résultats

Les Figures 17 et 18 montrent le biais d'horloge et la dérive du biais calculés par le récepteur du modèle Matlab. Dans le cas présent, $t_s = 3600\ s$. Cet instant est représenté par la ligne verticale en pointillé rouge sur les Figures 17 et 18.

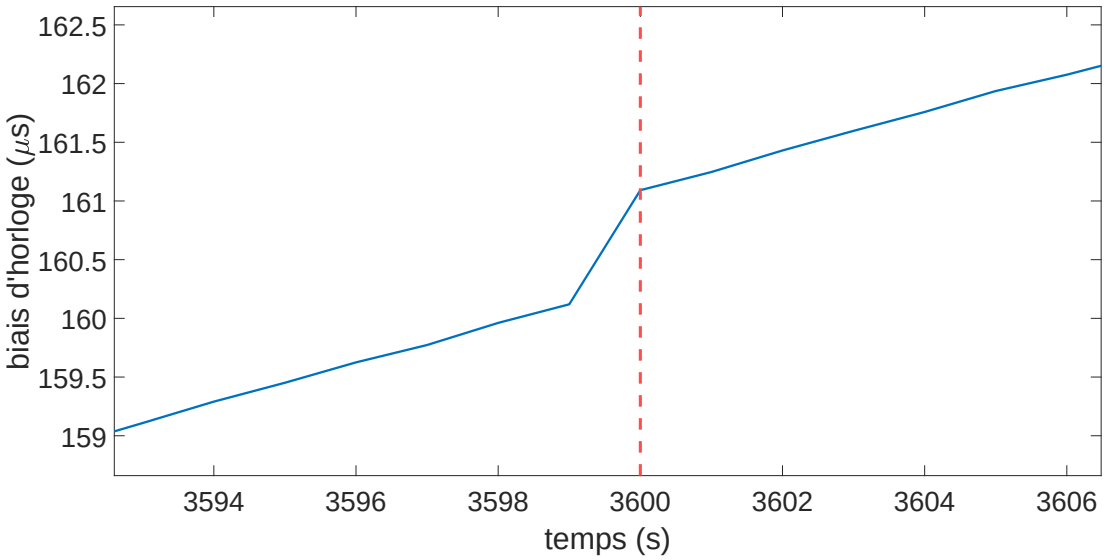

FIGURE 17 – Biais d'horloge au cours du temps sur le modèle

La Figure 17 montre que lorsque le récepteur passe de la constellation GNSS à la constellation du leurre, le biais d'horloge présente un saut de valeur. Ce saut de valeur se traduit sur la dérive du biais par un pic au même instant, comme le montre la Figure 18. La présence d'un terme de bruit aléatoire fait que les amplitudes du saut de biais et du pic de la dérive ne sont pas constants sur plusieurs itérations. Globalement, le saut de biais d'horloge est de l'ordre de 1 μs. Pour ce qui est du pic de la dérive, il est de l'ordre de 0.9 $\mu s/s$.

Ce modèle numérique montre donc qu'une attaque de leurrage sur un récepteur GNSS va causer un saut de valeur sur le biais d'horloge du récepteur. Ceci se reflète par un pic de valeur sur la dérive du biais d'horloge. Dans les conditions de notre modèle, l'attaque de leurrage utilisée est représentative d'un cas idéal (du point de vue du leurre) au niveau de la complexité de configuration des signaux. Malgré cette situation, le saut de biais est suffisamment grand pour être remarquable. Il convient donc de se demander quels paramètres peuvent permettre au leurre de réduire l'amplitude du saut de biais. C'est ce qui est étudié dans la partie suivante.

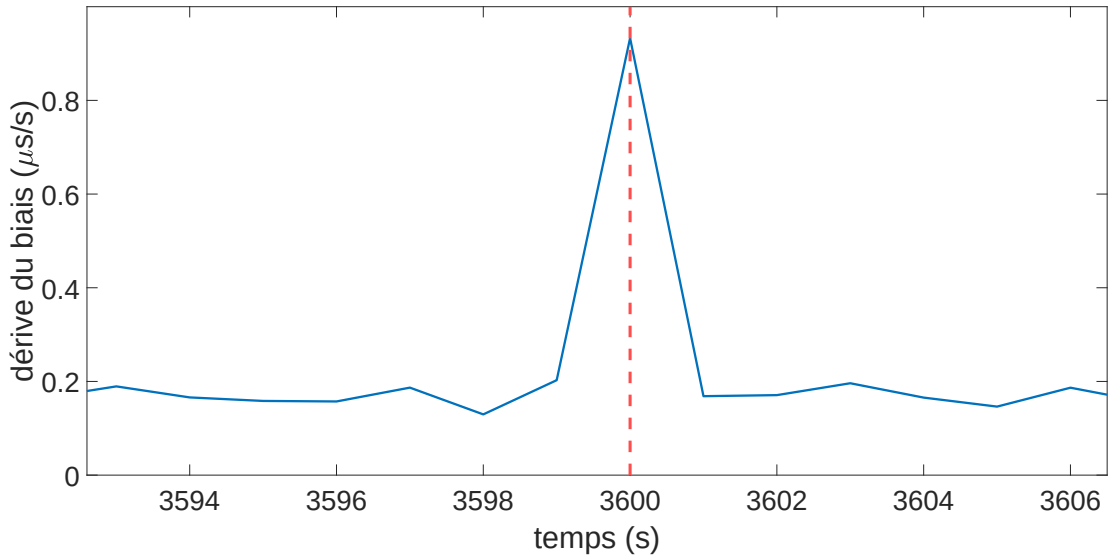

FIGURE 18 – Dérive du biais au cours du temps sur le modèle

II.1.2.2 Etude de l'influence de différents paramètres sur l'amplitude du saut de biais et de la dérive

Pour comprendre quels paramètres ont un impact sur l'amplitude du saut de biais, la variation de quatre paramètres a été testée. Ces paramètres sont :

— le nombre de satellites utilisés par le récepteur pour le calcul de position : ce paramètre permet d'illustrer les cas où des satellites disparaissent de la vue du récepteur, soit par évolution naturelle de leur trajectoire, soit par l'action d'un leurre capable de supprimer des signaux satellites,

— la dérive initiale du modèle du biais d'horloge : les récepteurs ont tendance à avoir une dérive qui leur est propre, ce paramètre permet donc d'illustrer l'influence du choix du récepteur utilisé,

— la distance entre l'antenne du leurre et le récepteur d_{lu},

— la désynchronisation temporelle entre la constellation GNSS et la constellation du leurre : pour tester cette désynchronisation, on introduit un délai temporel entre elles. Ce délai intervient lors de la lecture des éphémérides, où on va récupérer les positions des satellites à des temps GNSS différents pour les deux constellations.

Pour montrer leur influence, les fonctions de répartition empiriques (ou ECDF pour Empirical Cumulative Distribution Function) de l'amplitude du saut de biais d'horloge et du pic de la dérive ont été calculées et leur courbes tracées. Une courbe ECDF s'obtient avec un jeu de données constitué de valeurs d'amplitude de saut de biais et de pic de dérive mesurées sur un grand nombre d'itérations du modèle Matlab. Ce jeu de données s'obtient en faisant tourner le modèle un grand nombre de fois (dans notre cas 100 itérations) tout en mesurant à chaque itération le saut de biais et le pic de la dérive.

La Figure 19 montre un exemple de courbe ECDF. Dans cet exemple, l'abscisse x représente l'amplitude du saut de biais. L'ordonnée de la courbe, $F(x)$, est le pourcentage de données du jeu de données dont la valeur est inférieure ou égale à la valeur en abscisse x. Dans le cas de la Figure 19 on peut donc lire que 68% des itérations réalisées ont un saut de biais d'horloge inférieur ou égal à 0.97 μs.

A elle seule, la courbe ECDF ne nous aide pas trop dans notre étude de l'influence de différents paramètres sur l'amplitude du saut de bais d'horloge et du pic de la dérive. Par contre, si on trace successivement les courbes ECDF pour différentes valeurs d'un paramètre donné et qu'on les compare les unes aux autres, leur

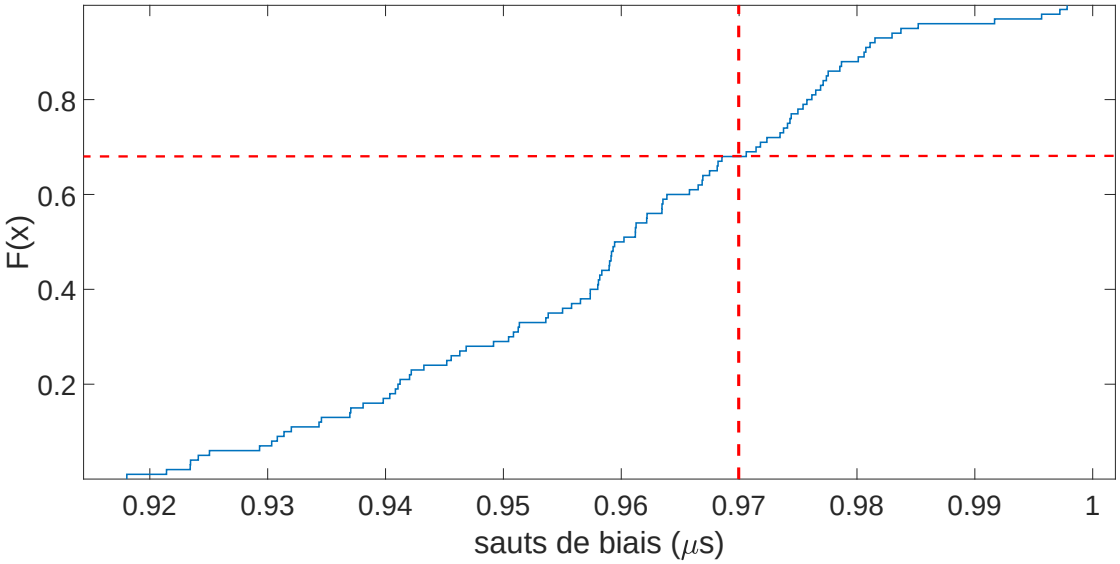

FIGURE 19 – Exemple de courbe ECDF

"dispositions" peuvent être révélatrices d'informations.

La Figure 20 montre les courbes ECDF pour différentes valeurs de distances entre l'antenne du leurre et le récepteur d_{lu}. On constate que les courbes ECDF pour chaque distance testée sont bien séparées. Les courbes ECDF des plus petites distances sont celles qui présentent les sauts de biais les plus faibles tandis que les courbes ECDF des plus grandes distances sont celles qui présentent les sauts de biais les plus grands. Il en est de même pour le pic de la dérive du biais d'horloge, comme le montre la Figure 21.

Ceci montre que la distance entre le leurre et le récepteur a bien un impact sur l'amplitude du saut de biais d'horloge et le pic de sa dérive causés par l'attaque de leurrage.

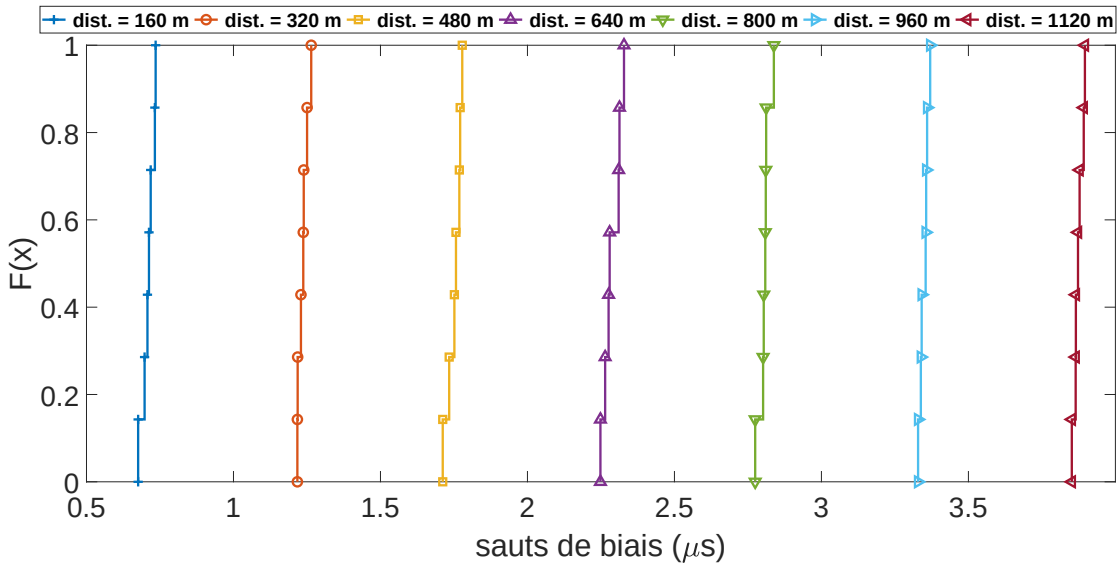

FIGURE 20 – Courbes ECDF du saut de biais d'horloge pour différentes distances

Pour ce qui est de la dérive initiale, le même résultat est observé pour l'amplitude du saut de biais mais pas pour l'amplitude du pic de la dérive. La Figure 22 montre les courbes ECDF du pic de la dérive de biais

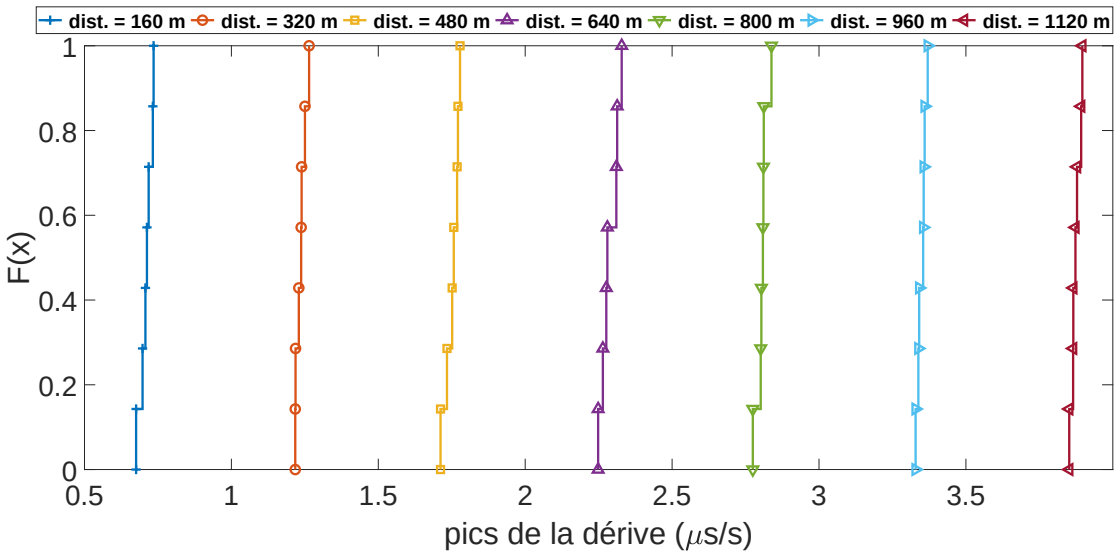

FIGURE 21 – Courbes ECDF du saut de biais d'horloge pour différentes distances

pour différentes valeurs de dérive initiale. On constate que les courbes ECDF sont "mélangées entre elles", ce qui indique que la dérive initiale n'a pas d'impact réel sur l'amplitude du pic de la dérive qui a lieu lors de l'attaque de leurrage.

Concernant le nombre de satellites utilisés pour le calcul de position, les courbes ECDF montrent que ce paramètre n'a pas d'impact sur l'amplitude du biais d'horloge et l'amplitude du pic de la dérive du biais.

Pour ce qui est de la désynchronisation entre les deux constellations, au vu des courbes ECDF présentées Figure 23, il semble que cela n'a pas non plus d'influence sur l'amplitude du biais d'horloge et de l'amplitude du pic de la dérive.

Ainsi, sur l'ensemble des paramètres testés, la distance entre le leurre et le récepteur est le paramètre qui a le plus d'impact sur l'amplitude du saut de biais d'horloge et du pic de la dérive. Cette observation est quelque chose qu'on peu pressentir assez naturellement mais l'expérience le confirme ici. Ainsi, si un leurre souhaite minimiser son impact sur le biais d'horloge du récepteur il doit faire en sorte d'être le plus proche possible de sa cible.

Le modèle numérique développé sur Matlab émulant une attaque de leurrage relativement simple nous confirme qu'une attaque de leurrage a bien une influence sur l'horloge d'un récepteur. Cette influence se manifeste par un saut de valeur inattendu du biais d'horloge, ce qui se répercute comme un pic sur la dérive du biais. Maintenant que ce phénomène a été mis en évidence par notre modèle, il convient de se demander si le même phénomène est présent sur un récepteur GNSS commercial utilisant de vrais signaux et s'il se manifeste avec la même amplitude que sur notre modèle.

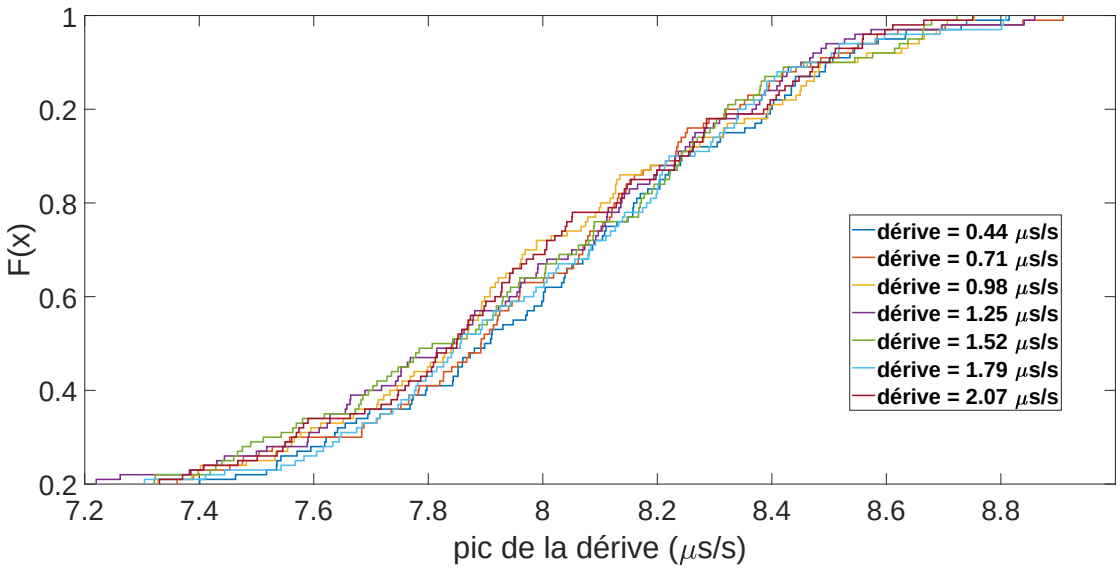

FIGURE 22 – Courbes ECDF du pic de la dérive du biais pour différentes dérives initiales

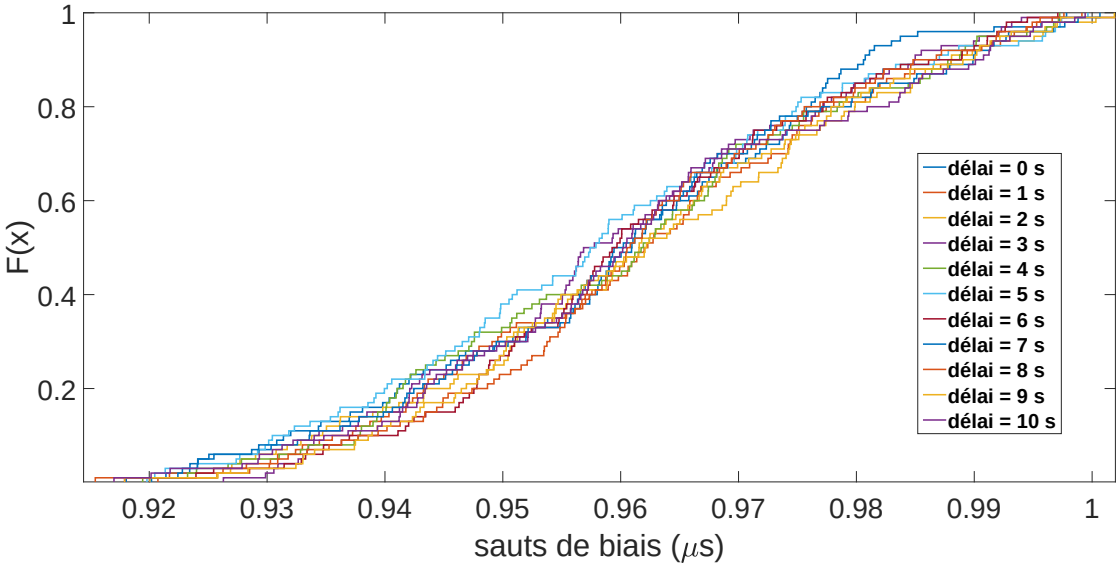

FIGURE 23 – Courbes ECDF du saut de biais d'horloge pour différents délais temporels entre les constellations

II.2 Etude de l'effet d'un leurrage fixe sur le biais d'horloge d'un récepteur GNSS commercial dans le cas d'une seule horloge

L'objectif de cette partie et des suivantes est d'étudier les effets d'une attaque de leurrage sur un récepteur GNSS commercial. Pour faire cela, il est nécessaire de réaliser une telle attaque par le biais d'un générateur de signaux GNSS émettant des signaux de leurage à destination de l'antenne du récepteur.

Cependant, à cause de contraintes législatives, il n'est pas possible de mettre en place une telle expérience en espace libre. L'émission de signaux dans les bandes GNSS est interdite par la loi sans autorisation spéciale (Articles L39 et L41 du code des postes de communications électronique). C'est pourquoi tous nos essais de leurrage ont été réalisés de façon câblée. Deux simulateurs de signaux on été utilisés au cours de nos expérimentations :

— le Labsat 2, qui est un simulateur de signaux pouvant enregistrer et répéter des signaux GPS/GLONASS,

— le Spirent GSS6560, qui est un simulateur capable de générer une constellation GPS complète sur un maximum de 12 canaux (12 satellites) et offre un grand choix de paramètres de configuration sur son logiciel SimGen

Afin de s'assurer que les résultats observés ne sont pas spécifiques à un seul récepteur deux récepteurs GNSS ont été utilisés : le u-blox EVK-6T et le u-blox EVK-M8T (nommés u-blox 6 et u-blox 8 par la suite). L'annexe A présente et explique de façon plus détaillée le fonctionnement du matériel utilisé dans cette partie et dans les parties suivantes.

II.2.1 Mise en place et déroulé des événements

L'objectif de nos premières expérimentations est de répliquer le même type d'attaque de leurrage que celle utilisée sur le modèle Matlab vu en II.1.2.1.

II.2.1.1 Mise en place

L'idée est de simuler deux ensembles de signaux GNSS (les signaux de la constellation GNSS et les signaux de leurrage) avec un seul générateur de signaux. En utilisant un seul générateur pour les deux ensembles de signaux, on s'assure que les signaux sont générés par la même horloge, ce qui permet d'avoir une synchronisation parfaite entre les deux constellations de satellites. L'inconvénient du Spirent et du Labsat est qu'ils ne disposent que d'une seule sortie Radio-Fréquence (RF), ce qui signifie qu'il n'est pas possible d'émettre simultanément deux constellations GNSS. Cependant, il est possible de contourner ce problème avec le Spirent en utilisant les différentes options de paramétrage offertes par ce dernier.

En effet, le Spirent permet de simuler des interférences de type "trajets indirects" (multipath en anglais). Les interférences de trajets indirects sont issues de signaux réfléchis par un ou plusieurs obstacles (le sol ou des immeubles par exemple). Ceci se traduit principalement par un délai sur les pseudo-distances. En configurant correctement le délai introduit par la réflexion des signaux, il est possible d'obtenir des pseudo-distances correspondant à la fausse position souhaitée. Le Spirent disposant de 12 canaux, on peut allouer les six premiers canaux aux satellites de la vraie constellation GNSS et les six derniers canaux à des signaux de trajets indirects tirés des vrais signaux. Cette "astuce" permet alors de reproduire la même attaque de leurrage que sur le modèle Matlab. La constellation "leurre" et la constellation "réelle" ont alors le même oscillateur et la même base de temps. Cela permet de simuler ce que serait une sorte de leurre idéal. La méthode de configuration des trajets indirects sur le Spirent est détaillée en Annexe B .

II.2.1.2 Déroulé des événements

Les différents essais de leurrage présentés ici et dans les parties suivantes sont grandement inspirés des travaux effectués lors d'un projet ANR appelé ANGELAS auquel Telecom SudParis et THALES ont participé. Ce projet avait pour but de développer une variété de technologies anti-drones afin de protéger des zones sensibles (comme une centrale nucléaire ou un site militaire par exemple) de la présence de drones suspects. Une des technologies présentées dans ce projet est le leurrage GNSS. Certains résultats de cette étude sont présentés dans [31]. Un récepteur GPS possède deux modes de fonctionnement :

— le mode acquisition,

— le mode poursuite

Le mode acquisition est le mode dans lequel le récepteur recherche les satellites d'une constellation afin de pouvoir lancer un calcul de position. Durant cette recherche, les boucles du récepteur ne sont accrochées à aucun signal. C'est pour cette raison que le mode acquisition est le mode où le récepteur est le plus vulnérable aux attaques de leurre. Fort heureusement ce n'est pas le mode dans lequel se trouve le plus souvent le

récepteur.

Le mode poursuite suit le mode acquisition. Dans ce mode, le récepteur a trouvé des satellites sur lesquels accrocher ses boucles de suivi et suit donc les signaux issus des satellites auxquels il s'est accroché. C'est pendant ce mode que le récepteur calcule sa position à partir des informations reçues des satellites.

Le biais d'horloge et sa dérive ont été étudiés dans ces deux modes. Pour cela, trois scénarios d'attaques de leurrage inspirés du projet ANGELAS ont été sélectionnés : un en mode acquisition et deux en mode poursuite. Les deux scénarios en mode poursuite sont les suivants :

— attaque douce : le leurre commence par diffuser de faux signaux à faible puissance avant d'augmenter petit à petit cette puissance jusqu'à être légèrement supérieure à la puissance des vrais signaux,

— attaque forte : le leurre envoie directement des signaux de puissance relativement forte.

Le mode acquisition peut être forcé en appliquant un *warm start* sur le u-blox. Le *warm start* est un état particulier d'initialisation du récepteur. Dans celui-ci le récepteur n'a gardé en mémoire que les almanachs, la dernière position connue et le temps UTC (Universal Time Coordonated, soit le temps universel). Le récepteur va donc remettre à zéro son biais d'horloge à chaque *warm start*. Les deux scénarios précédents ne diffèrent pas dans le mode acquisition. C'est pourquoi il a été décidé de ne tester que l'attaque douce en mode acquisition : à chaque augmentation de puissance, un *warm start* est appliqué sur le u-blox.

La constellation simulée est une constellation GPS utilisant des éphémérides datées au 25 janvier 2018 à 11h00. Comme décrit précédemment, les six premiers canaux sont dédiés à la vraie constellation GNSS tandis que les six derniers canaux sont dédiés au leurre. Les signaux de la constellation sont initialement réglés sur une puissance de $-58\ dBm$, afin d'avoir un rapport C/No de $43 - 45\ dBHz$, tandis que les canaux du leurre sont laissés fermés. Au bout de $1'00''$ les canaux du leurre sont configurés en tant que trajets indirects des canaux des vrais signaux tout en restant fermés. La suite des événements pour chaque scénario est donné Tableau 1.

Tableau 1 – Tableau des actions pour chaque scénario

Scénario	Actions
Acquisition	- A $2'00''$ ouvrir les canaux du Spirent à $-64\ dBm$ et appliquer un *warm start* sur le u-blox. - Chaque $1'0''$, augmenter la puissance sur le Spirent de $2\ dB$ et appliquer un *warm start* sur le u-blox. - Répéter l'étape précédente jusqu'à ce que le u-blox s'accroche sur la fausse position.
Attaque douce	- A $2'00''$ ouvrir les canaux du Spirent à $-63\ dBm$. - Chaque $1'30''$, augmenter la puissance sur le Spirent de $5\ dB$. - Répéter l'étape précédente jusqu'à ce que le u-blox s'accroche sur la fausse position.
Attaque forte	- A $3'00''$ ouvrir les canaux du Spirent à $-38\ dBm$. - Attendre que le u-blox s'accroche sur la fausse position.

II.2.2 Résultats et premières conclusions

Le premier u-blox qui a été testé est le u-blox 6. Pour tester la reproductibilité de nos attaques, chaque scénario a été testé plusieurs fois. Les courbes présentées par la suite sont celles obtenues sur une de ces itérations. Le contrôle du déroulé de l'attaque a lieu sur le logiciel u-center qui est le logiciel dédié du u-blox servant a récupérer en temps réel les données du récepteur. En vérifiant "l'état" des satellites vus par le récepteur et la position calculée on peut déterminer l'instant où le récepteur passe de la vraie constellation GPS à la fausse constellation du leurre.

II.2.2.1 Acquisition

Le premier scénario testé est le mode acquisition. Dans ce mode le leurre a pu capturer le récepteur avec des signaux plus puissants de 2 dB par rapport à la puissance des signaux de la vraie constellation. Les Figures 24 et 25 montrent respectivement le biais d'horloge et la dérive du biais lors du scénario d'acquisition. Les lignes en pointillé rouge numérotées indiquent les instants où un *warm start* est appliqué, la ligne en pointillé vert indique le moment où le récepteur passe sur la fausse position. A chaque *warm start* le récepteur remet à zéro son biais d'horloge.

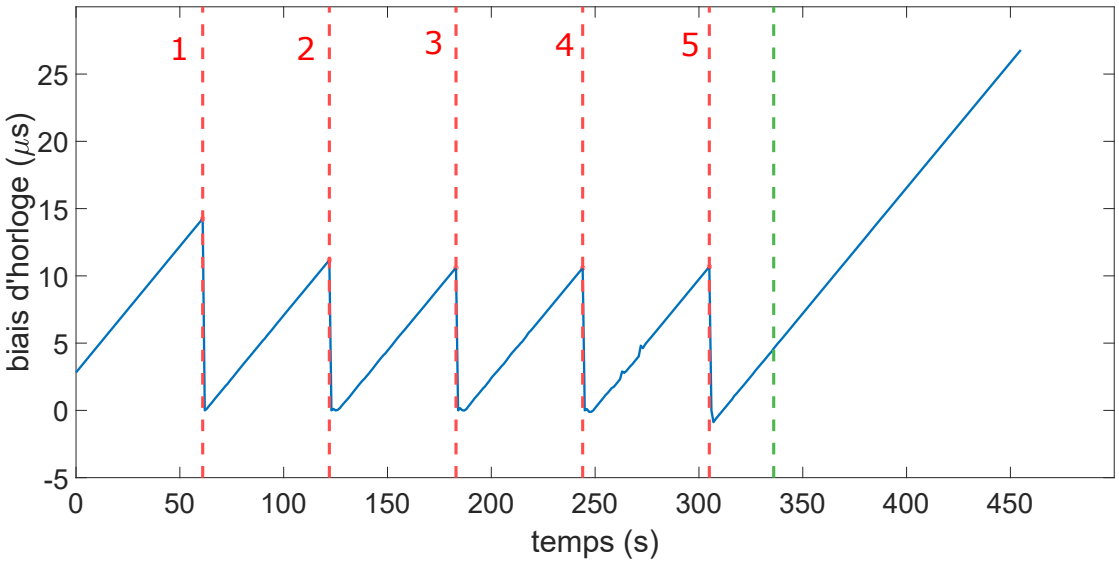

FIGURE 24 – Biais d'horloge durant le scénario d'acquisition dans le cas à une horloge

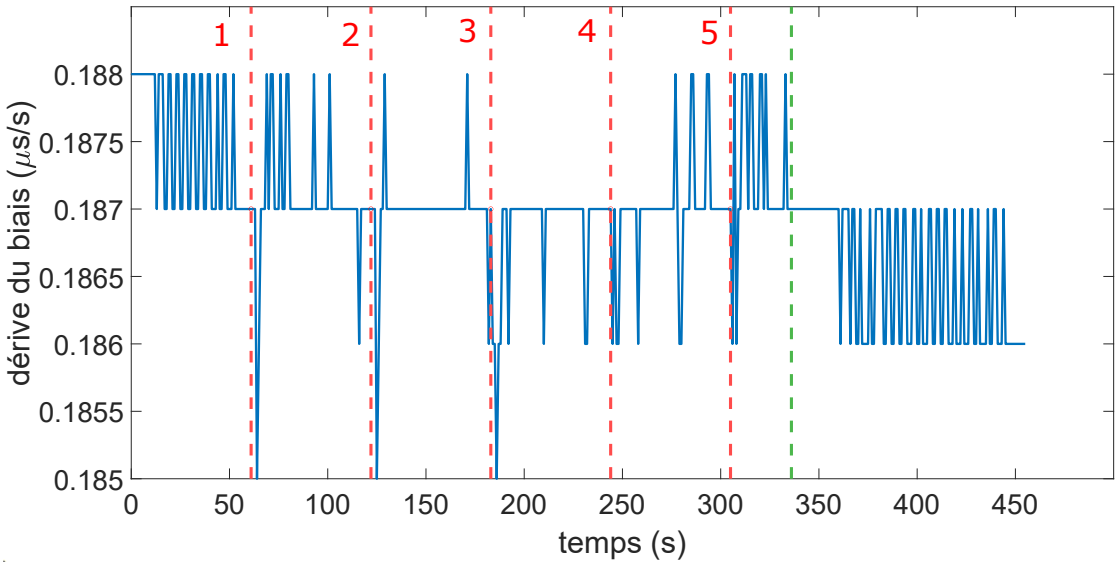

FIGURE 25 – Dérive du biais durant le scénario d'acquisition dans le cas à une horloge

Sur les itérations de ce scénario, suite au *warm start* appliqué après que les puissances des signaux de leurrage soient égales à celles des vrais signaux (le numéro 4 sur la Figure 24), le récepteur a des difficultés à se raccrocher à des signaux, ce qui peut expliquer les quelques faibles pics que le biais d'horloge présente entre le *warm start* 4 et le *warm start* 5 sur la Figure 24.

Lorsqu'on s'intéresse au passage du récepteur sur la fausse position, on constate un bref saut sur le biais d'horloge. Malgré ce saut, on constate Figure 25 que la dérive du biais ne présente pas de pic lors du saut de biais et ne semble donc pas perturbée par les signaux du leurre. La Figure 26 montre un zoom sur l'instant où le récepteur passe sur le faux point. La ligne en pointillé vert représente l'instant où le récepteur passe sur la fausse position et la ligne en pointillé rouge représente un prolongement du biais d'horloge avant cet instant.

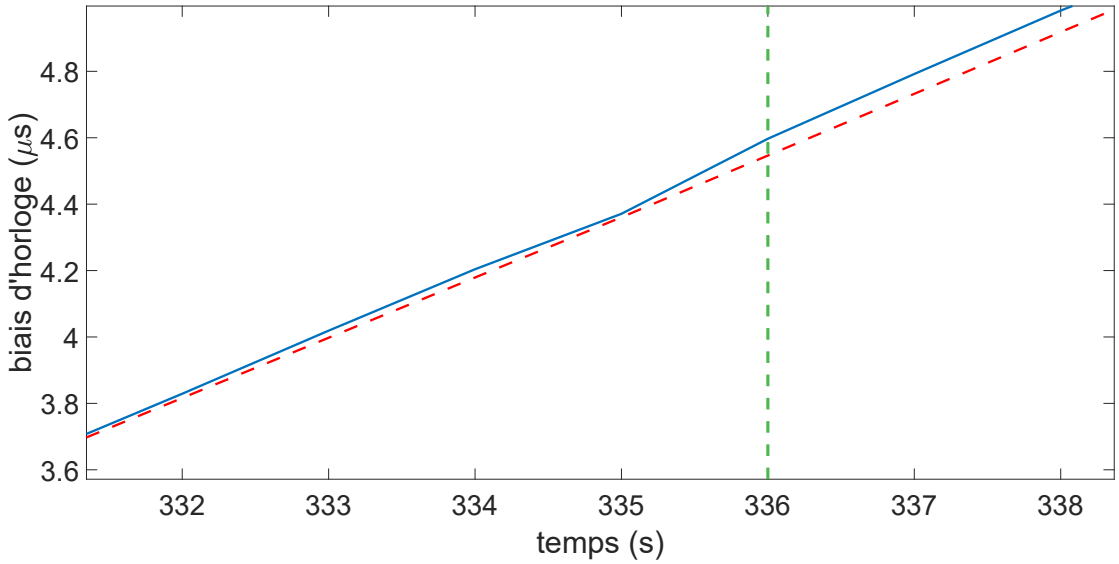

FIGURE 26 – Zoom sur le biais d'horloge durant le scénario d'acquisition dans le cas à une horloge

II.2.2.2 Attaque douce et attaque forte

Dans le cas d'une attaque douce le leurre a pu capturer le récepteur avec des signaux plus puissants de 5 dB par rapport à la puissance des signaux de la vraie constellation. Dans quelques cas, des puissances égales à celles de la vraie constellation ont suffi. La Figure 27 montre le biais d'horloge durant une attaque douce. Les lignes en pointillé rouge indiquent les moments où la puissance des signaux du leurre sont augmentées et la ligne en pointillé vert indique l'instant où le récepteur passe sur le faux point. La Figure 28 est un zoom de cet instant avec la ligne en pointillé rouge représentant une prolongation du biais d'horloge avant le passage sur le faux point.

Sur cette dernière Figure on constate également un saut de biais d'horloge lors du passage sur la constellation du leurre. Une fois encore ce saut de biais ne se répercute pas sur la dérive du biais.

Le scénario d'attaque forte a également été un succès. Les mêmes phénomènes sur le biais d'horloge et la dérive du biais ont pu être observés.

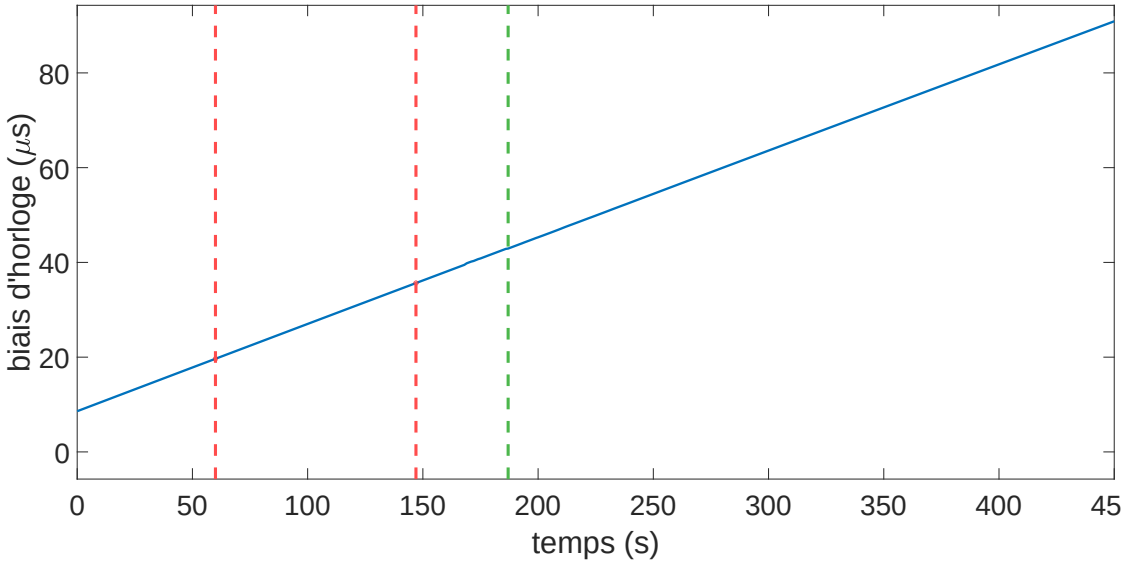

FIGURE 27 – Biais d'horloge lors d'une attaque douce dans le cas à une horloge

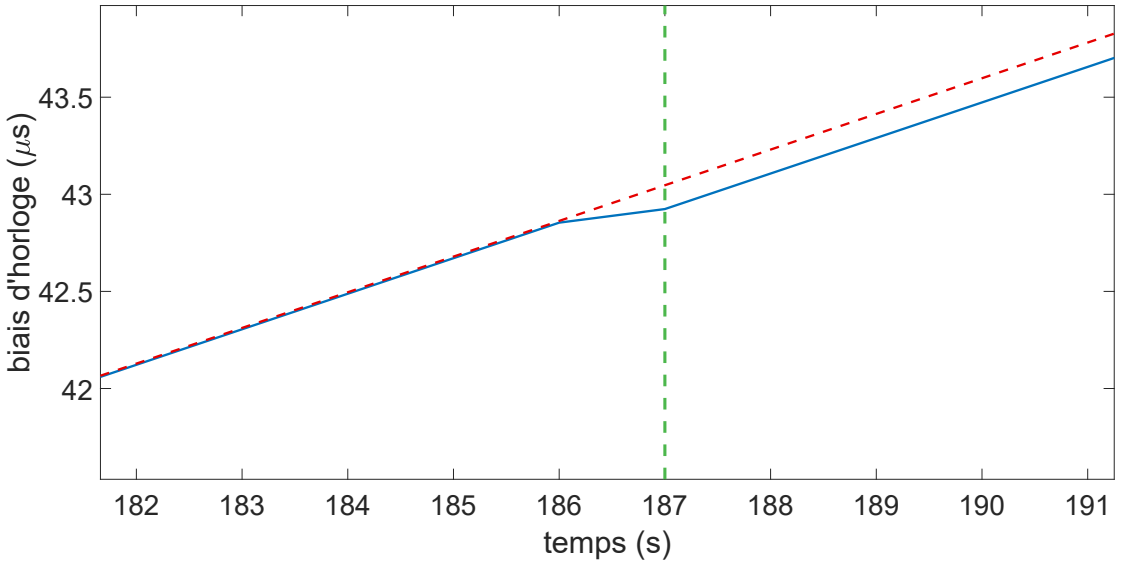

FIGURE 28 – Zoom sur le biais d'horloge lors d'une attaque douce dans le cas à une horloge

II.2.2.3 Résultats sur le u-blox 8 et comparaison avec le u-blox 6

Pour le u-blox 8, les différents scénarios de leurrage ont également été un succès. Par exemple, la Figure 29 montre le biais d'horloge durant une attaque de leurrage forte contre le u-blox 8. La ligne en pointillé rouge est une courbe servant de prolongement de la courbe de biais précédent l'attaque de leurrage, la ligne verticale en pointillé vert indique le moment où le récepteur passe sur la fausse position.

Les moyennes des sauts de biais observés sur l'ensemble des itérations de chaque scénario pour chaque u-blox sont répertoriées Tableau 2.

Avec le u-blox 8 on peut remarquer quelques différences, que ce soit sur le saut de biais ou sur le comportement global du récepteur lors d'une attaque de leurrage. Sur le scénario d'acquisition on constate que le u-blox 8 a plus de facilité que le u-blox 6 à retrouver des signaux après un *warm start*. De plus, le u-blox 6 prenait en compte dans ses calculs de moins en moins de satellites à mesure que la puissance des signaux du

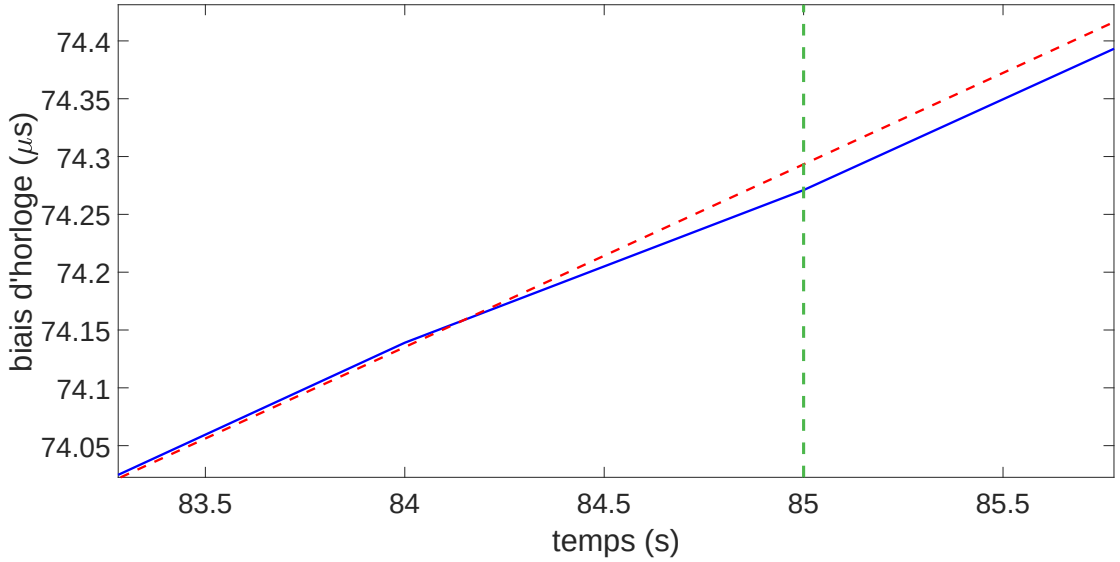

FIGURE 29 – Biais d'horloge lors d'une attaque forte dans le cas à une horloge (u-blox 8)

Tableau 2 – Moyennes des sauts sur le biais sur les u-blox 6 et 8 dans le cas d'une seule horloge

	u-blox 6	u-blox 8
Scénario	saut de biais (μs)	saut de biais (μs)
Acquisition	0.179	0.807
Attaque douce	0.177	0.307
Attaque forte	0.172	0.343

leurre augmentait, ce qui n'a pas été le cas avec le u-blox 8.

Sur le scénario d'attaque douce, la puissance des signaux du leurre a du dépasser de 10 dB la puissance des vrais signaux pour capturer le récepteur. Par ailleurs, lors des attaques douce et forte, le u-blox 6 passait par des phases de perte de suivi de signaux précédent le passage sur la constellation du leurre. Ces phases de perte n'ont pas été observées sur le u-blox 8.

Concernant les sauts, on constate qu'ils sont en moyenne de plus grande amplitude avec le u-blox 8.

II.2.2.4 Bilan

Ces expérimentations mettent en évidence les mêmes observations issues du modèle Matlab de la partie II.1.2.1. L'attaque de leurrage va provoquer un saut de valeur sur le biais d'horloge du récepteur quand la boucle de suivi de celui-ci va "s'accrocher" sur les signaux du leurre. Cependant, les amplitudes de ces sauts sont plus faibles que celles calculées avec le modèle (en moyenne 0.176 μs pour le u-blox 6 et 0.485 μs pour le u-blox 8), mais cela reste suffisamment élevé pour être détecté.

Concernant la dérive du biais d'horloge, elle ne semble pas perturbée par les signaux de leurrage, malgré le saut observé sur le biais. Ceci peut provenir d'une part de la façon dont le récepteur calcule la dérive du biais et d'autre part de l'amplitude du saut de valeur du biais d'horloge. Un effet de lissage due au processus de calcul a pu "effacer" le pic de la dérive. L'amplitude du pic aurait pu être trop faible, au vu de l'amplitude du saut du biais, pour que le processus de calcul prenne en compte ce pic.

Ces expérimentations de leurrage GNSS confirment les observations issues du modèle Matlab concernant le biais d'horloge. Cependant, il est aussi possible que ce saut de valeur sur le biais puisse avoir une autre origine. De part sa méthode d'attaque, un leurre va altérer la constellation satellite qu'un récepteur perçoit à travers

les différents signaux reçus. Il convient donc de se demander si une simple modification de la constellation GNSS perçue par le récepteur peut conduire à des effets notables sur le comportement du biais d'horloge. C'est ce qui est étudié par la suite.

II.2.3 Effets des modifications sur la constellation GNSS vue par le récepteur

Cette partie s'intéresse à l'influence que peut avoir une modification de la constellation GNSS vue par le récepteur sur son horloge. Comme expliqué partie II.1.1, le biais d'horloge résulte de la solution d'un système d'équations. En réalité l'horloge d'un récepteur a plusieurs biais : un pour chaque satellite de la constellation. Le biais d'horloge que le récepteur calcule est en réalité une moyenne de ces différents biais. Si plusieurs satellites de la constellation disparaissent brutalement, leurs biais ne sont plus disponibles pour le récepteur ce qui a de forte chance de modifier la solution calculée.

Ainsi, plusieurs essais de suppression de satellites de la constellation ont été testés sur notre récepteur. Le Spirent a été configuré pour générer des signaux d'une constellation GPS de 10 satellites. Au bout de 30 minutes, k satellites sont coupés en fermant leurs canaux sur le Spirent et au bout d'une heure les satellites sont réactivés. Ce test a été réalisé avec $k = \{1, 2, 3, 4, 5\}$. Les Figures 30 et 31 montrent le biais d'horloge et la dérive du biais sur un essai avec $k = 5$, la ligne en pointillé rouge indique l'instant où les satellites sont coupés et la ligne en pointillé vert indique l'instant où les satellites sont rallumés.

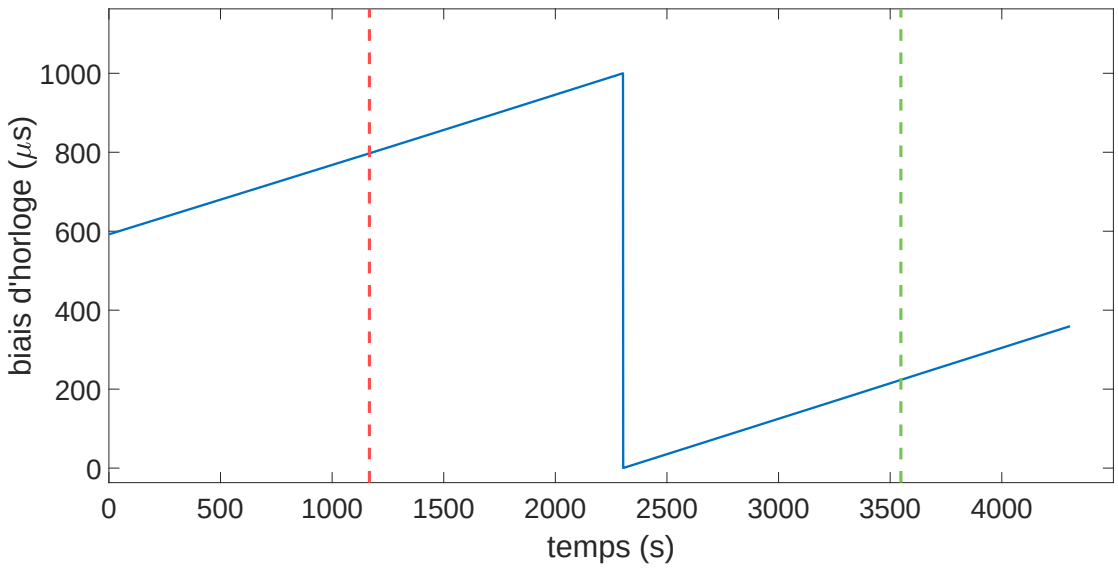

FIGURE 30 – Biais d'horloge lors d'un essai de coupure de satellites

Au cours de ces essais, il a été constaté que la perte de satellites n'a pas d'effet notable sur les biais d'horloge et sa dérive. Ce qui confirme que le saut de valeur du biais d'horloge et le pic de la dérive du biais ont bien pour origine les signaux de leurrage. Cependant, le cas étudié dans le modèle et dans cette partie expérimentale est un cas idéal du point de vue du leurre. En effet, il est peu probable que le leurre utilise exactement la même horloge que le récepteur ciblé. L'horloge du leurre a probablement des spécifications techniques différentes de l'horloge du récepteur. Il est également peu probable que l'horloge du leurre puisse se synchroniser de façon très précise avec l'horloge du récepteur. Il convient donc d'étudier une situation plus réaliste, où le leurre utilise une horloge distincte de celle du récepteur.

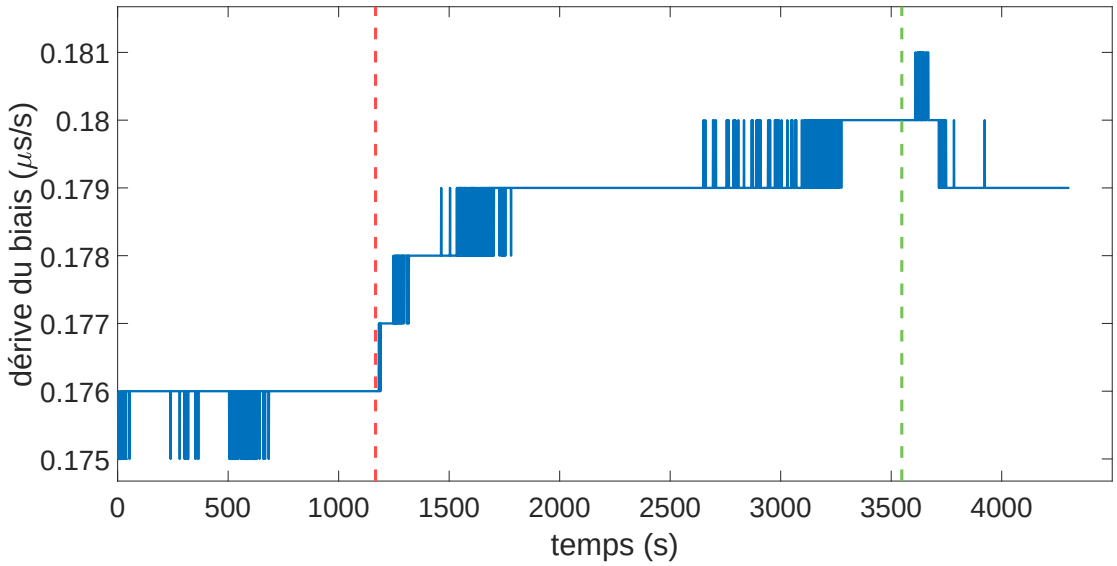

FIGURE 31 – Dérive du biais lors d'un essai de coupure de satellites

II.3 Etude de l'effet d'un leurrage fixe sur le biais d'horloge d'un récepteur GNSS commercial dans le cas de deux horloges

L'objectif de cette partie est d'étudier le cas où le leurrage est réalisé en utilisant un simulateur de signaux GNSS différent de celui utilisé pour simuler la vraie constellation.

II.3.1 Mise en place

En plus du Spirent, le Labsat a été utilisé pour réaliser cette étude. Dans un premier temps le Spirent est utilisé pour générer la vraie constellation GNSS sans aucune perturbation. Il s'agit de la même constellation que celle utilisée en partie II.2. Le Spirent émet ses signaux vers le Labsat qui les enregistre pendant 15 minutes. Avec cet enregistrement le Labsat peut jouer le rôle de la vraie constellation GNSS, tandis que le Spirent joue le rôle du leurre.

Les signaux du leurre reprennent les paramètres de configuration du Spirent utilisés lors de l'enregistrement précédent mais avec cette fois-ci la fausse position comme position à calculer (soit un faux point 240 m au nord de la vraie position). Un atténuateur réglé à -23 dB a été ajouté en sortie du Spirent afin de disposer d'une bande de puissance à utiliser sur le Spirent plus large. Les vrais signaux (Labsat) et les faux signaux (Spirent) se rejoignent au niveau d'un séparateur de signal utilisé en tant que sommateur. Le signal de sortie de ce dernier est alors envoyé sur le récepteur GNSS u-blox. Le montage expérimental est présenté Figure 32.

Comme lors de la partie II.2, le biais d'horloge et sa dérive ont été étudiés dans les deux modes de fonctionnement du récepteur (acquisition et poursuite), on reprend donc les scénarios définis précédemment.

A ces trois scénarios, un quatrième scénario a été testé. Ce scénario est désigné par la suite comme l'attaque de brouillage. Dans ce scénario on utilise une fonctionnalité du Labsat pour émettre un bruit de forte puissance pour perturber le drone ciblé, puis le leurre envoie ses signaux avant d'arrêter la diffusion du bruit.

II.3.2 Procédure expérimentale

Quand le Spirent génère sa constellation, il génère aussi un bruit thermique fixe quelque soit le niveau de puissance réglé sur son logiciel SimGen. Le Labsat enregistre l'ensemble {signaux-bruit} du Spirent et en mode replay le Labsat émet les signaux et le bruit avec la même amplification. Afin de s'assurer que les signaux du Spirent et du Labsat sont émis à des niveaux de puissance équivalents, il est donc nécessaire de

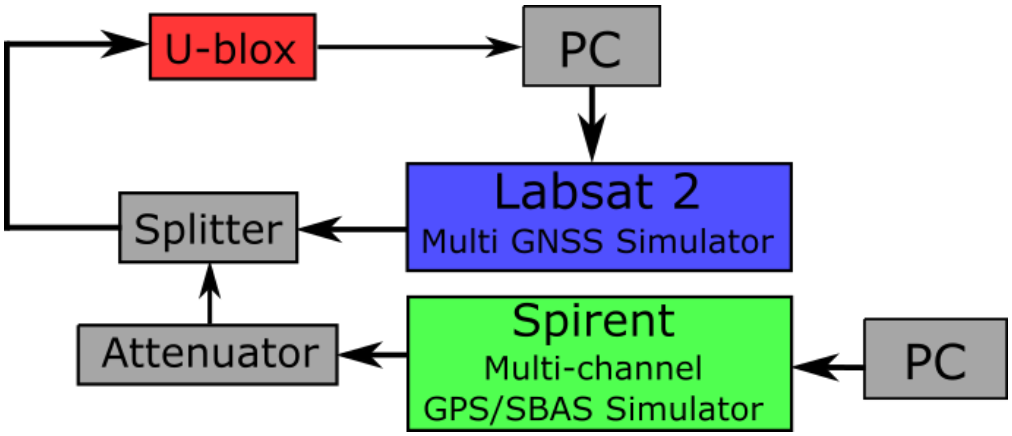

FIGURE 32 – Montage expérimental

"calibrer" le Spirent avant de se lancer dans les tests des différents scénarios de leurrage. Cela permet d'avoir un comportement du récepteur analogue entre le Spirent et le Labsat.

Le principe de cette calibration est de déterminer quel réglage de puissance sur SimGen permet d'avoir au niveau du récepteur un rapport C/No équivalent au Labsat seul lorsque le Spirent est actif. Pour cela on réalise un enregistrement du Spirent à vide, c'est à dire le Spirent avec ses canaux fermés, afin de n'avoir que le bruit thermique du Spirent. Puis on joue cet enregistrement avec le Labsat en même temps que le Spirent avec ses canaux ouverts et on règle la puissance des canaux du Spirent pour que le récepteur reçoive des signaux avec des rapports C/No équivalents au cas où seul le Labsat est présent.

La répétition des vrais signaux par le Labsat nous donne au niveau du u-blox des signaux de rapport C/No entre 39 et 41 $dBHz$ avec le Labsat seul. Après ajout des signaux du Spirent, la sortie du Spirent a dû être réglée à -66 dBm pour obtenir les mêmes rapports C/No.

Une fois cette étape réalisée, on peut commencer les différents tests d'attaque de leurrage. La procédure pour lancer un test d'attaque de leurrage est la suivante :

— paramétrer le Spirent et fermer les canaux de sortie,

— lancer le Spirent et immédiatement après, lancer le Labsat de tel sorte qu'ils soient quasiment simultanés,

— attendre que le récepteur u-blox s'accroche sur la constellation du Labsat et donc la vraie position et laisser le u-blox se stabiliser dessus (environ 2 minutes après le début),

— appliquer les actions du scénario testé.

Les actions des différents scénarios sont listées dans le Tableau 3.

II.3.3 Résultats

Le premier u-blox qui a été testé est le u-blox 6. De même que précédemment, chaque scénario a été testé plusieurs fois. Les courbes suivantes sont celles obtenues sur une de ces itérations.

II.3.3.1 Acquisition

Le premier scénario testé est le mode acquisition. Dans ce mode, l'attaque de leurrage a été un succès à partir d'une puissance de -64 dBm sur le Spirent, ce qui fait avec l'atténuateur une puissance totale de -87 dBm.

Tableau 3 – Tableau des actions pour chaque scénario

Scénario	Actions
Acquisition	- A $3'30''$ ouvrir les canaux du Spirent à -68 dBm et appliquer un *warm start* sur le u-blox. - Chaque $1'30''$, augmenter la puissance sur le Spirent de 2 dB et appliquer un *warm start* sur le u-blox. - Répéter l'étape précédente jusqu'à ce que le u-blox s'accroche sur la fausse position.
Attaque douce	- A $4'00''$ ouvrir les canaux du Spirent à -65 dBm. - Chaque $1'30''$, augmenter la puissance sur le Spirent de 5 dB. - Répéter l'étape précédente jusqu'à ce que le u-blox s'accroche sur la fausse position.
Attaque forte	- A $5'00''$ ouvrir les canaux du Spirent à -40 dBm. - Attendre que le u-blox s'accroche sur la fausse position.
Attaque de brouillage	- A $5'00''$ lancer le bruit numérique sur le Labsat à 100%. - A $5'10''$ ouvrir les canaux sur le Spirent à -65 dBm. - A $5'20''$ régler le bruit numérique sur le Labsat à 0%. - Attendre sur le u-blox s'accroche sur la fausse position.

Le u-blox ne voit alors que des signaux avec un rapport C/No de $48 - 50$ $dBHz$.

Les Figure 33 et 34 montrent respectivement le biais d'horloge et sa dérive calculés par le u-blox. Les lignes en pointillé rouge indiquent les moments où un *warm start* a été appliqué. Les lignes en pointillé vert montrent les instants où le récepteur se raccroche sur des satellites. Les chiffres en rouge indiquent le numéro du *warm start* correspondant.

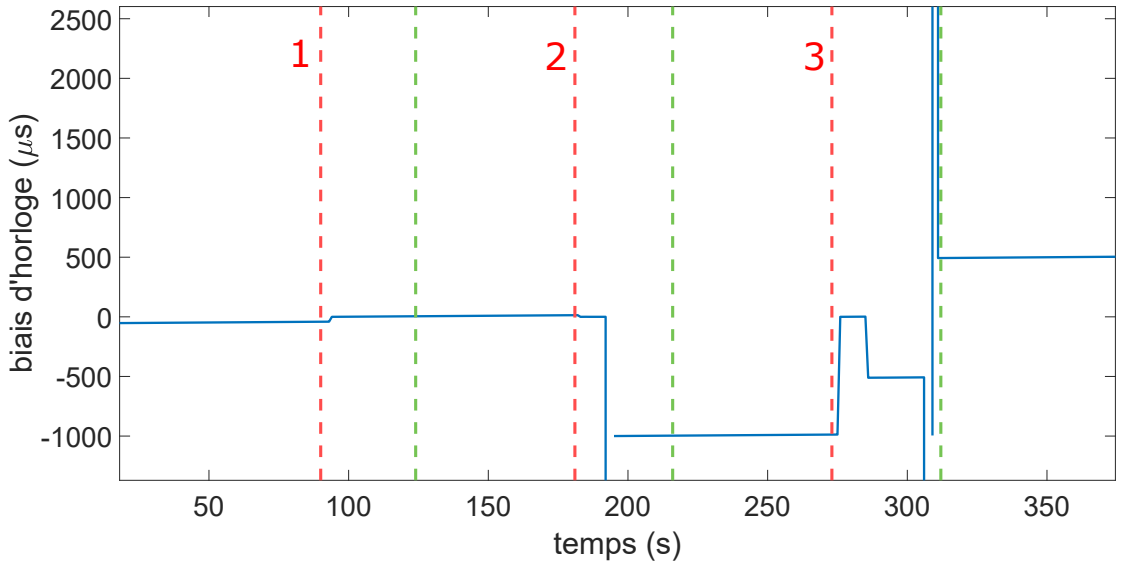

FIGURE 33 – Biais de l'horloge durant le scénario d'acquisition

On peut constater que pour le deuxième *warm start*, après la remise à zéro du biais d'horloge on constate un premier saut de biais de 1010.23 μs. Lorsque le récepteur se raccroche sur une constellation, la position calculée est toujours sa vraie position. Pour le troisième *warm start*, on constate un nouveau saut de biais (de 1480.5 μs) qui a lieu après la remise à zéro du biais. C'est après ce troisième *warm start* que le récepteur finit par s'accrocher à la constellation du leurre et calcule donc le faux point.

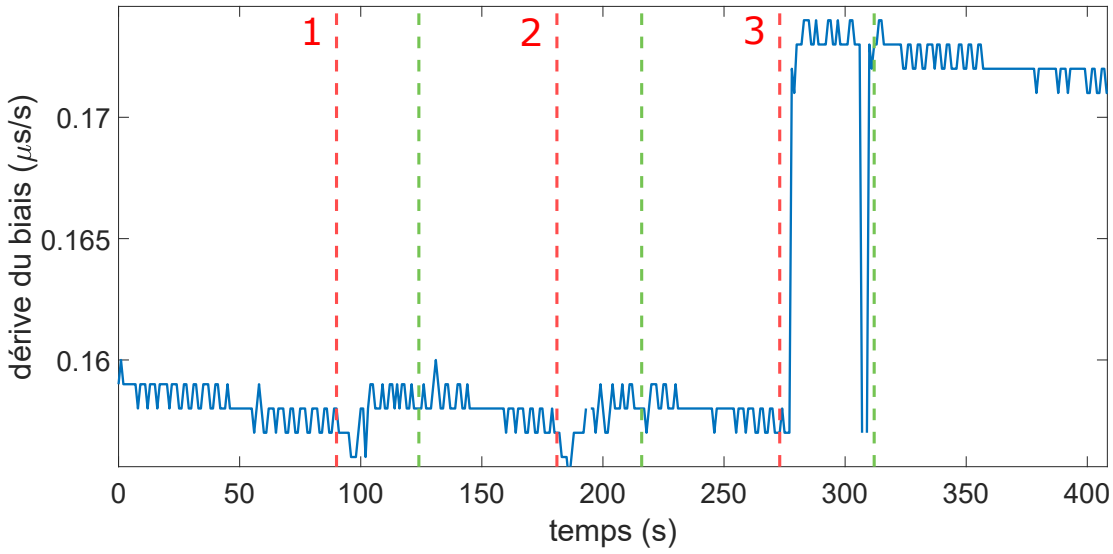

FIGURE 34 – Dérive du biais de l'horloge durant le scénario d'acquisition

Concernant la dérive du biais, elle n'est pas vraiment impactée par les premiers *warm starts*. Par contre, après le dernier *warm start* la dérive du biais présente un saut de 0.016 $\mu s/s$ ce qui est bien plus grand que les variations usuelles de la dérive qui sont habituellement de l'ordre de 0.001 $\mu s/s$. Contrairement aux tests de leurrage de la partie II.2, la dérive est perturbée par l'attaque de leurrage. De plus, contrairement au modèle de la partie II.1.2.1, la dérive ne présente pas qu'un simple pic mais un saut de valeur qui "modifie" la valeur autour de laquelle la dérive va varier après l'attaque (par exemple, sur la Figure 34 on est passé d'un peu moins de 0.16 $\mu s/s$ à un peu plus de 0.17 $\mu s/s$).

II.3.3.2 Attaque douce

Le scénario testé en deuxième est l'attaque douce. Ce scénario s'est aussi soldé sur un succès de l'attaque de leurrage. Le leurre a réussi à capturer le récepteur u-blox à partir d'une puissance de -45 dBm sur le Spirent, soit une puissance totale de -68 dBm. Cependant ceci s'est fait sur un temps d'action relativement long. Le passage des vrais signaux aux faux signaux peut prendre jusque 3 minutes pour être effectif. Après avoir augmenté la puissance du Spirent à -42 dBm, soit un total de -65 dBm (C/No de $49-51$ $dBHz$ vu par le u-blox), ce passage se fait en moins d'une minute.

Les Figures 35 et 36 montrent le biais de l'horloge et sa dérive dans ce cas. Les lignes en pointillé indiquent les instants où la puissance a été augmentée. La flèche 1 indique l'instant où le récepteur perd le suivi des vrais signaux. La flèche 2 indique le moment où le récepteur s'accroche aux faux signaux du leurre.

On remarque sur ces courbes que le biais de l'horloge et la dérive du biais présentent également un saut de valeur assez important. Ici on mesure un saut de 687 μs pour le biais et de 0.015 $\mu s/s$ pour la dérive.

II.3.3.3 Attaque forte et brouillage

Avec l'attaque forte, l'attaque s'est avérée être un succès à partir de -40 dBm sur le Spirent, soit une puissance totale de -63 dBm. Les tracés des courbes du biais d'horloge et de la dérive du biais montrent que ces dernières présentent le même comportement face aux attaques de leurrage que dans l'attaque douce et le mode acquisition. Quand le récepteur u-blox passe des vrais signaux aux faux signaux on a un saut dans le biais et sa dérive.

Pour le scénario d'attaque de brouillage, le Spirent réglé à -65 dBm (soit une puissance totale de -88 dBm) a permis un leurrage réussi. Ici aussi les courbes du biais de l'horloge et de sa dérive présentent un saut de

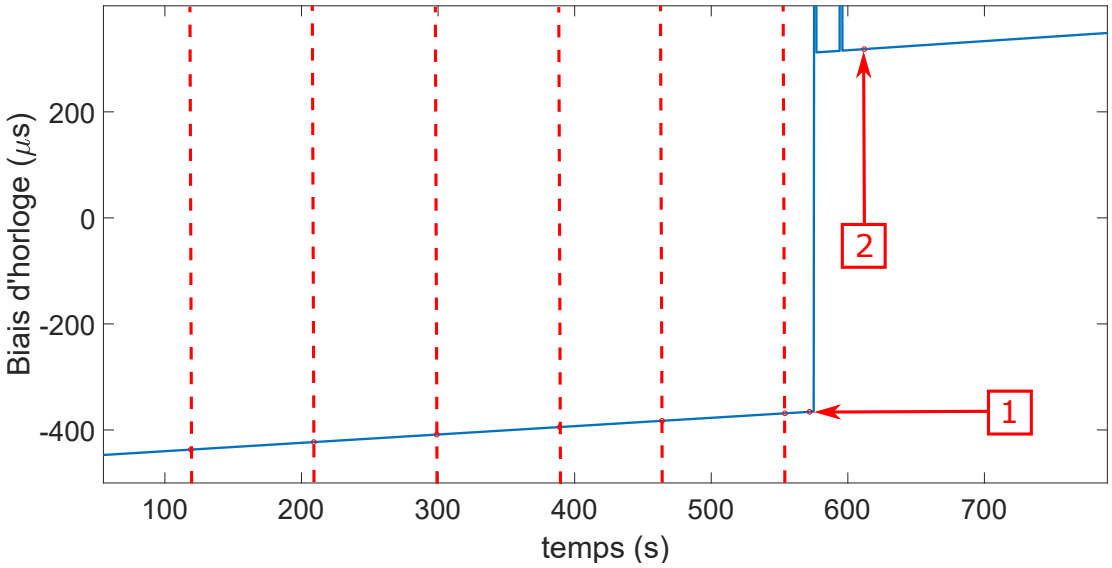

FIGURE 35 – Biais d'horloge lors d'une attaque douce

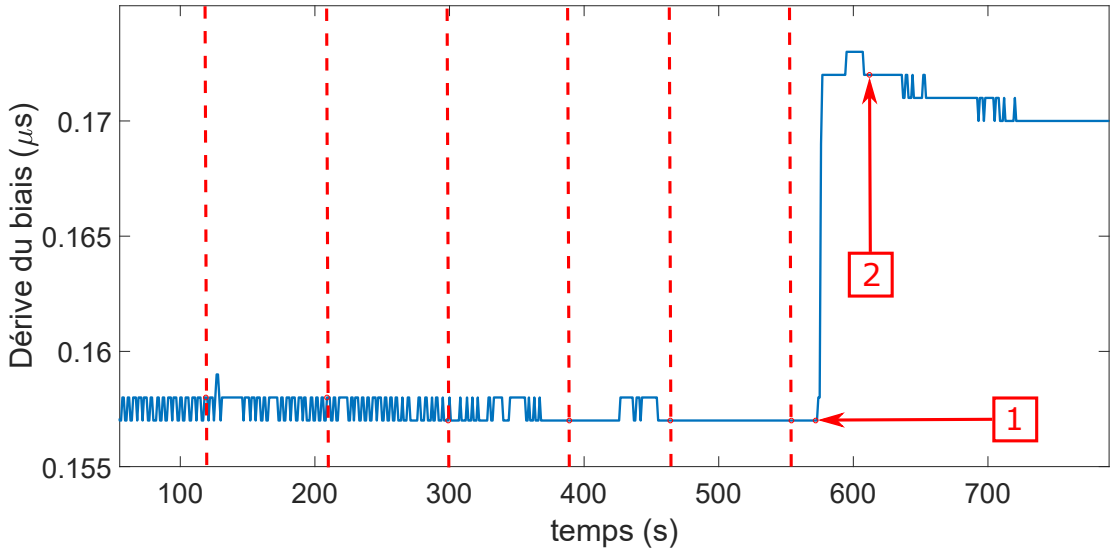

FIGURE 36 – Dérive du biais lors d'une attaque douce

valeur sur ces derniers quand le récepteur passe sur les signaux du leurre.

Les courbes tracées du biais d'horloge et de la dérive du biais sont données Figures 37 et 38. La ligne en pointillé rouge désigne l'instant où le Labsat envoie son bruit numérique de forte puissance, la flèche rouge indique le moment où le bruit est coupé et la flèche verte indique l'instant où le récepteur s'accroche à la fausse position. On constate ici un saut de 318.9 μs pour le biais et de 0.018 $\mu s/s$ pour la dérive.

Comme précisé précédemment, ces différents scénarios ont été testés sur plusieurs itérations. Les moyennes des valeurs de sauts mesurées est répertoriée dans le Tableau 4.

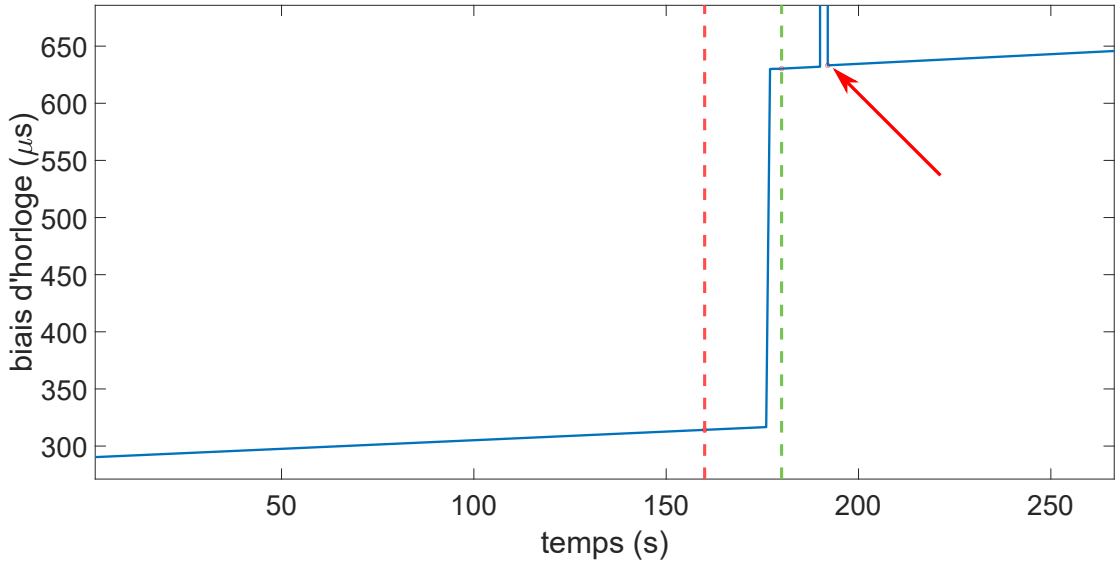

FIGURE 37 – Biais d'horloge lors d'une attaque par brouillage

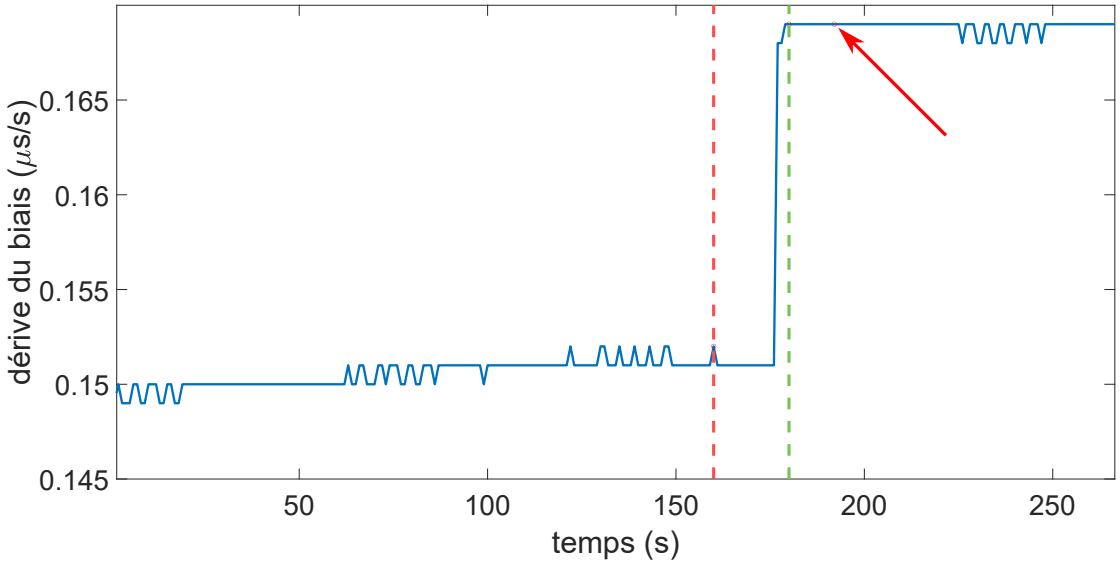

FIGURE 38 – Dérive du biais d'horloge lors d'une attaque par brouillage

Tableau 4 – Moyennes des sauts sur la dérive et le biais avec les rapports C/No mesurés sur le u-blox 6

Scénario	Dérive (μs/s)	Biais (μs)	C/No (dBHz)
Acquisition	0.016	1317.3	48-50
Attaque douce	0.0153	666.13	49-51
Attaque forte	0.0118	776.32	50-52
Attaque de brouillage	0.0133	393.4	41-43

II.3.3.4 Quelques remarques

Parmi les itérations de ces différentes attaques, certaines d'entre elles ont donné des résultats moins notables. En effet sur quelques itérations, malgré un leurrage réussi et malgré la présence d'un saut de valeur sur le biais, la dérive du biais ne présente donc pas de saut de valeurs importants modifiant la valeur autour de laquelle la dérive va varier après l'attaque.

Les Figures 39 et 40 montrent le biais d'horloge et sa dérive dans un de ces rares cas durant une attaque forte. La ligne verticale indique l'ouverture des canaux du Spirent, la flèche 1 indique le moment où le récepteur perd les vrais signaux et la flèche 2 indique l'instant où le récepteur se localise à la fausse position. On voit bien Figure 39 que le biais présente un saut de valeur alors que la Figure 40 montre que la dérive subit une variation légère après la perte des signaux de la vraie constellation avant de "revenir" à la même valeur moyenne après avoir récupéré les signaux du leurre.

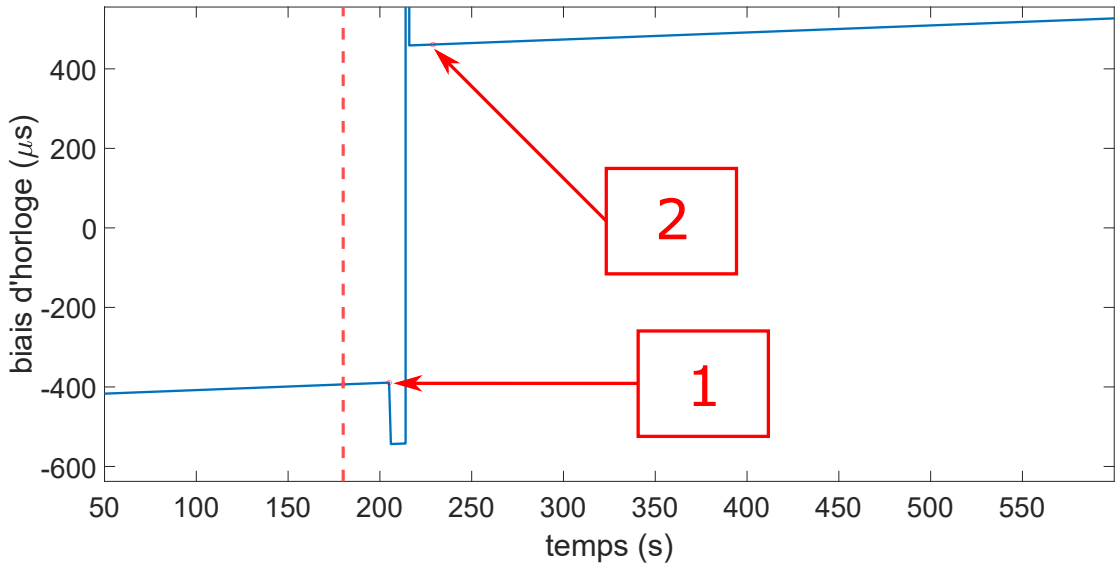

FIGURE 39 – Biais durant une attaque de poursuite présentant un saut important

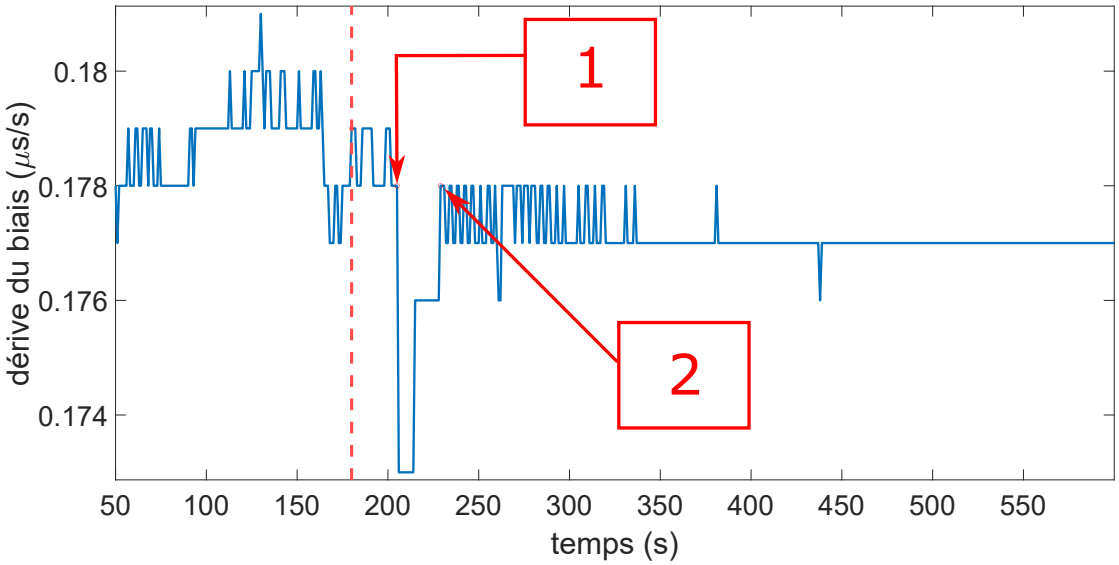

FIGURE 40 – Dérive durant une attaque de poursuite ne présentant pas de saut important

Une hypothèse pouvant expliquer ces cas particuliers est qu'il s'agirait d'une synchronisation fortuite des horloges des satellites et du récepteur.

II.3.3.5 Résultats du u-blox 8 et comparaison avec le u-blox 6

Les Figures 41 et 42 montrent le biais d'horloge et la dérive du biais durant une attaque forte sur le u-blox 8. La ligne en pointillé verticale indique l'ouverture des canaux du Spirent, la flèche 1 indique l'instant où le récepteur perd les vrais signaux et la flèche 2 indique l'instant où il se localise sur la fausse position.

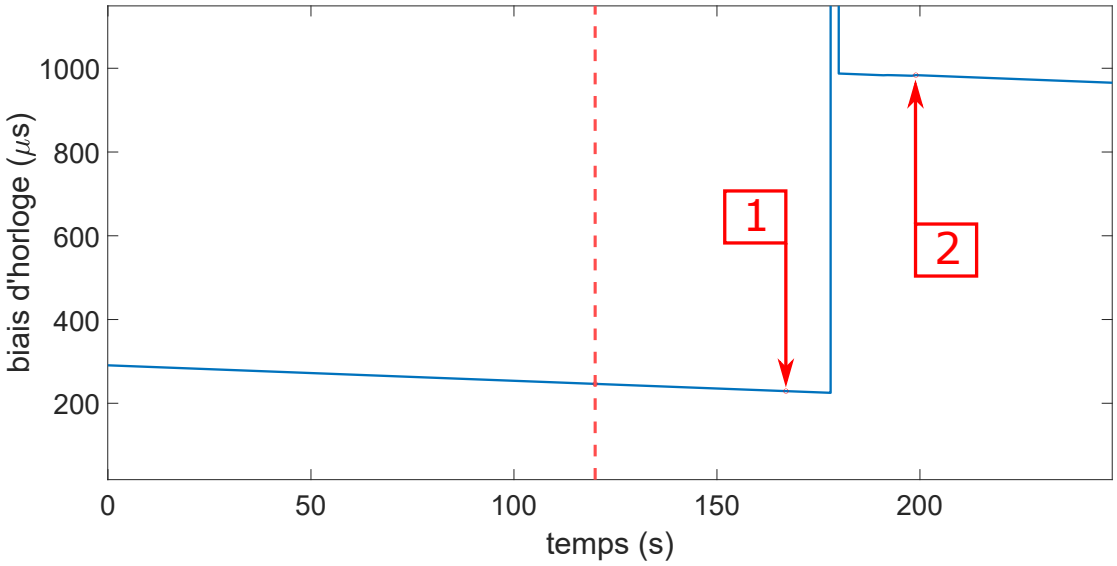

FIGURE 41 – Biais d'horloge lors d'une attaque forte sur le u-blox 8

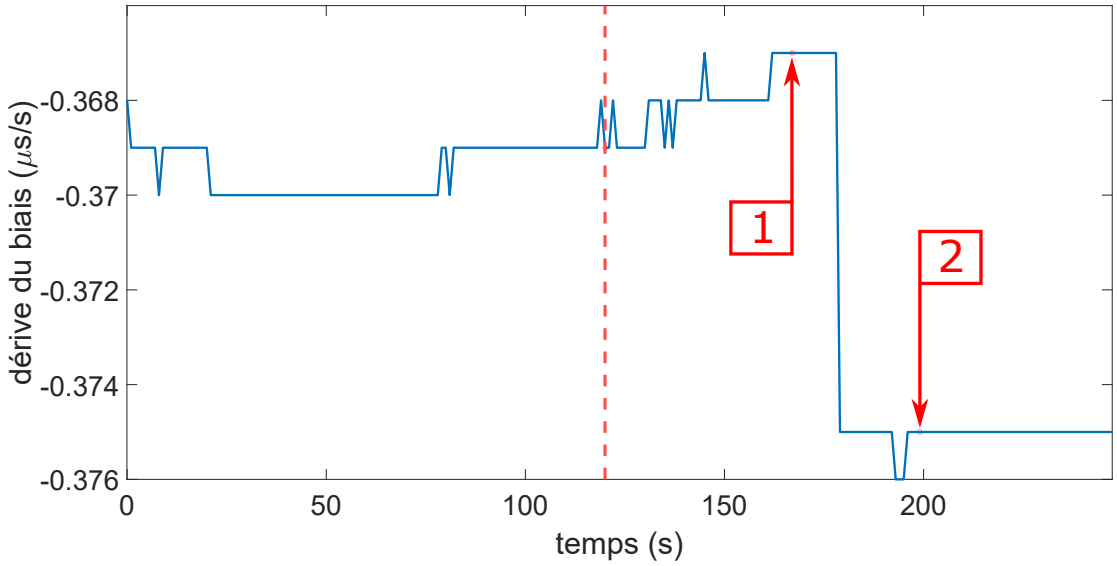

FIGURE 42 – Biais d'horloge lors d'une attaque forte sur le u-blox 8

Les résultats obtenus présentent les mêmes observations pour ce scénario et les autres que pour le u-blox 6. Quand une attaque de leurrage survient et réussit à capturer le récepteur ciblé, le biais d'horloge et la dérive du biais présentent un saut de valeur lors du passage du récepteur des vrais signaux aux faux signaux. Le Tableau 5 résume les résultats obtenus sur le u-blox 8.

Il est intéressant de noter que quelques différences apparaissent entre les deux u-blox. Dans le mode acquisition, la puissance nécessaire pour réussir à leurrer le u-blox est plus grande pour le u-blox 8. Cette différence

Tableau 5 – Moyennes des sauts sur la dérive et le biais avec les rapports C/No mesurés sur le u-blox 8

Scénario	Dérive (μs/s)	Bias (μs)	C/No (dBHz)
Acquisition	0,0165	498,1	48-50
Attaque douce	0.0163	774.53	49-51
Attaque forte	0.0178	936.02	50-52
Attaque de brouillage	0.018	986.2	41-43

est de l'ordre de 10 dB. Pour les autres scénarios la puissance nécessaire pour leurrer assez rapidement la cible présente de très faibles différences (de l'ordre du dB) entre le u-blox 6 et le u-blox 8. Par ailleurs, les essais sur le u-blox 8 ne présentent pas les quelques cas où la dérive du biais n'a pas de saut de valeurs significatifs évoqués sur le u-blox 6.

II.3.3.6 Conclusions sur ces essais

Ces quatre scénarios de leurrage confirment les conclusions obtenues avec le modèle Matlab (partie II.1.2) et les essais de leurrage avec le Spirent seul (partie II.2). En effet une attaque de leurrage va provoquer des sauts sur le biais de l'horloge mais également sur la dérive de l'horloge. Cependant on constate deux grandes différences au niveau de l'amplitude de ces sauts par rapport au modèle et aux essais à une horloge.

La première différence concerne la plage de valeurs de l'amplitude des sauts sur divers itérations d'un même essais. Sur le modèle, l'amplitude du saut de biais ne varie que très peu selon les itérations (de l'ordre de 1.0 ± 0.1 μs) et lors des essais à une horloge cette variation est légèrement supérieure (de l'ordre de 0.22 ± 0.5 μs). En revanche, sur l'ensemble des essais à deux horloges l'amplitude des sauts présente de plus grandes variations entre les différentes itérations. Les valeurs mesurées allant de la dizaine de μs jusqu'à un peu plus de 1 ms.

L'autre différence qui en découle est donc l'ordre de grandeur de ces sauts, avec les sauts de 10 à 1000 fois plus élevés dans le cas à deux horloges.

Ces différences peuvent provenir du fait que la vraie constellation GNSS et la constellation du leurre sont générées avec deux générateurs de signaux GNSS indépendants, ce qui signifie qu'ils ne sont pas synchronisés et lancés séparément "à la main". Ceci amène donc un décalage temporelle entre les horloges des deux simulateurs, et donc entre les deux constellations.

Il faut également prendre en compte les différences de spécification techniques entre les deux appareils (précision, stabilité par exemple) qui peuvent influencer ce délai. On peut alors se demander si ce décalage temporelle est vraiment prépondérant dans la différence d'ordre de grandeur observés sur les sauts de valeurs. On peut alors envisager deux hypothèses.

La première est que le délai entre les deux horloges va accroître l'amplitude des sauts de biais et de la dérive, ce qui contredirait la partie II.1.2.2 de l'étude.

L'autre hypothèse est que cette différence d'ordre de grandeur ne vient pas du délai en lui même mais plutôt de l'utilisation de deux horloges distinctes et du passage de la boucle de suivi du récepteur d'une horloge a une autre. Par ailleurs il est également possible que les différences entre les horloges peuvent causent un phénomène aléatoire affectant l'amplitude des sauts. Il convient donc d'étudier si au cours d'un grand nombre d'itérations, l'amplitude des sauts de biais et de dérive sont aléatoires ou semblent suivre une certaine régularité. La partie suivante se focalise donc sur l'étude de ces différentes hypothèses.

II.4 Etude des différences d'ordre de grandeur des sauts de biais

II.4.1 Etude de l'influence du délai entre le Spirent et le Labsat

Pour cette première étude, le scénario d'attaque forte a été testé avec un décalage de l'ordre de la minute entre le Spirent et le Labsat. Ce décalage est "créé" à la main en allumant le Spirent après le Labsat, c'est donc le Spirent qui est en retard par rapport au Labsat. Les délais testés vont de zéro minutes à dix minutes. Le Tableau 6 présente les sauts de la dérive et du biais d'horloge mesurés au cours de ces essais.

Tableau 6 – Sauts de biais et de dérive mesurés lors des essais de délai

Délai (min)	Saut de dérive du biais (μs/s)	Saut de biais d'horloge (μs)
0	0.008	1246.3
1	0.008	754.6
2	0.001	654.12
3	0.008	627.2
5	0.011	659.3
10	0.008	1639.7

On constate alors que comme lors de l'étude de la partie II.1.2.2 l'importance du délai entre les constellations n'a pas d'influence notable sur l'amplitude des sauts de biais. Ce n'est donc pas la cause des différences d'ordre de grandeur entre le modèle, le cas à une horloge et le cas à deux horloges. On en déduit donc que le facteur prépondérant de ces différences est l'utilisation de deux horloges pour simuler les signaux. Cependant cela ne nous indique toujours pas la large plage de valeurs d'amplitude de sauts de biais mesurée précédemment. La partie suivante s'intéresse donc à ceci, ainsi qu'à l'éventuel côté aléatoire de l'amplitude des sauts.

II.4.2 Etude de l'aléatoire de l'amplitude des sauts des valeurs du biais et de la dérive

Afin d'étudier le caractère aléatoire de l'amplitude des sauts de valeur du biais d'horloge et de la dérive, il est nécessaire de mesurer les sauts sur un grand nombre d'itérations. Le Labsat et le Spirent permettent de répéter en boucle des émissions de signaux GNSS, il est donc possible d'automatiser les itérations d'attaque de leurrage. Cependant, l'attaque de brouillage et le scénario du mode acquisition requièrent obligatoirement l'action de l'utilisateur pour les *warm starts* et l'activation du bruit sur le Labsat. C'est pourquoi ces deux scénarios ne peuvent pas être étudiés ici. Par ailleurs, étant donné la nécessité d'avoir un grand nombre d'itérations, la durée de toute la procédure itérative risque d'être très longue. Des deux scénarios restant, c'est à dire l'attaque douce et l'attaque forte, c'est l'attaque forte qui prend le moins de temps à réaliser. C'est pourquoi le scénario d'attaque forte est le seul à avoir été étudié pour cette partie.

En mode répétition, le Labsat permet de régler un délai (à la seconde près) entre chaque répétition. Le Spirent ne propose pas une telle option et dispose d'un délai qui lui est propre entre chaque répétition. Il faut donc bien régler le délai du Labsat afin de coïncider avec celui du Spirent. Cependant, l'impossibilité de synchroniser le démarrage du Spirent et du Labsat implique un décalage temporel qu'il faut également prendre en compte dans le réglage du délai de répétition du Labsat. La délai entre les répétitions du Spirent et le décalage dû à la non simultanéité du lancement du Labsat et du Spirent sont deux facteurs qu'on ne peut pas totalement maîtriser. Ainsi, au vu de la précision du réglage du délai de répétition du Labsat, on ne peut pas compenser efficacement le délai entre les deux appareils. Au fil des itérations le décalage va petit à petit augmenter, il faut donc essayer le plus possible de minimiser ce décalage et son augmentation avec le délai de répétition du Labsat et le lancement des appareils.

Trois séries de mesures de différentes longueurs (en nombre d'itérations et donc en temps de réalisation) ont été réalisées. Ces séries sont respectivement de 170, 192 et 256 itérations et seront nommés par la suite série 1, 2 et 3 respectivement. Au vu de la difficulté de la synchronisation du lancement des deux simulateurs de signaux, le décalage, et plus particulièrement son accroissement au cours du temps, n'est pas le même sur les trois séries. Sur la série 1 le décalage atteint $1'30''$ à la dernière itération, sur la série 2 il atteint $1'15''$,

et sur la série 3 il atteint $1'30''$. La Figure 43 montre les valeurs mesurées de sauts de biais d'horloge lors de la série 3. Sur l'ensemble des trois séries, les amplitudes des sauts de biais mesurées varient de 0.04 μs à 1.63 ms avec une forte proportion d'entre elles étant assez élevées (95% d'entre elles sont supérieures à 25 μs). De plus, on peut constater que sur les trois séries les amplitudes mesurées des sauts de biais ne suivent pas une certaine régularité au cours des itérations mais semblent plutôt soumises à un phénomène aléatoire. Notre modèle Matlab ne tiens pas compte de ce côté aléatoire, c'est pourquoi les amplitudes des sauts de biais calculés sur le modèle sont plus faibles et ont une plage de valeurs moins large. On peut donc en déduire que l'attaque de leurrage, plus précisément le passage à une autre constellation présente à cause du leurre, provoque un saut de biais dont l'amplitude n'est pas prévisible due à un phénomène aléatoire affectant cette dernière.

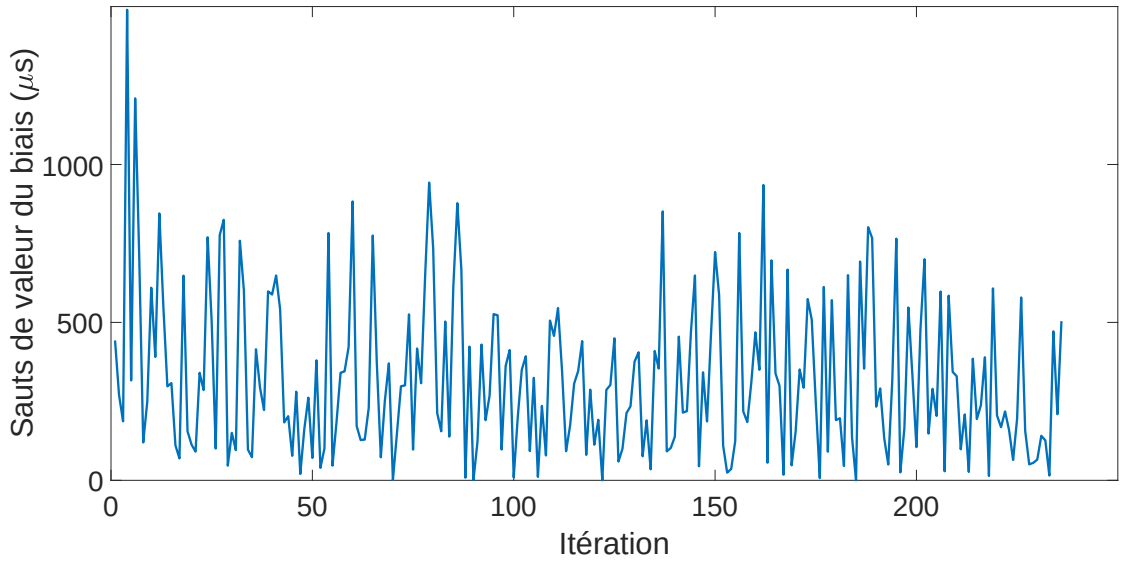

FIGURE 43 – Saut de biais d'horloge mesuré à chaque itération (série 3)

Concernant la dérive du biais, son comportement diffère selon les séries. La Figure 44 montre les sauts de valeurs de la dérive du biais lors des trois séries d'itérations.

Sur la série 1 l'amplitude du saut de la dérive du biais augmente graduellement au fil des itérations alors que sur les autres séries les amplitudes sont globalement plus constantes avec de faibles variations. A part leur longueur, la principale différence entre les trois séries est la rapidité d'augmentation du délai entre le Labsat et le Spirent. La série 1 est celle dont le décalage a augmenté le plus rapidement et c'est également la série dont les sauts de biais varient le plus. Cela peut aussi être lié au comportement relatif des oscillateurs des deux simulateurs respectifs. On constate donc que de manière globale, l'amplitude des sauts de valeurs de la dérive est, à l'instar des sauts de valeurs du biais, non prévisible.

Tous les résultats précédents ont été obtenus dans le cas d'un leurrage fixe (c'est-à-dire un leurrage d'un récepteur à une position fixe). Or les systèmes dépendant des GNSS tels que les drones ou les véhicules sont des systèmes qui se déplacent. Il convient donc de se demander si les conclusions précédentes sont valables dans le cas d'un récepteur en mouvement.

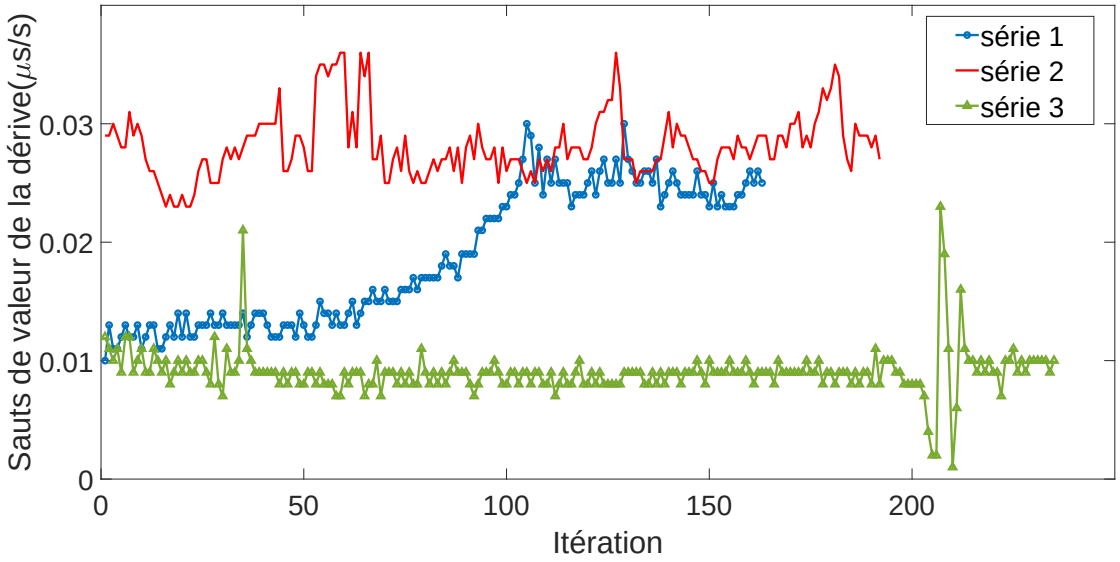

FIGURE 44 – Sauts de la dérive du biais mesurés à chaque itération des 3 séries

II.5 Etude dans le cas d'un récepteur en déplacement

L'objectif de cette partie est d'étudier si les résultats obtenus dans les parties précédentes sont toujours valables lorsque le récepteur ciblé est en mouvement, ce qui est une situation plus vraisemblable dans le cas des drones autonomes. Nous allons donc nous intéresser à des essais de leurrage mobiles. Le terme "mobile" désigne ici un leurrage où la victime suit une trajectoire pré-définie. Le leurre va agir selon deux cas possibles :

— cas 1 : le leurre va induire une fausse position fixe,

— cas 2 : le leurre va induire une fausse trajectoire qui commence comme la trajectoire du récepteur avant de diverger vers une fausse position.

II.5.1 Scénarios

La trajectoire du récepteur part de la vraie position utilisée lors des essais de leurrage fixe et couvre un périmètre de 2.8 km. Cette fausse trajectoire constituée de quatre Waypoints a été simulée sur le Spirent par l'utilisation d'un fichier de scénario sur le logiciel SimGEN. La vitesse du récepteur a été fixée à 14 m/s ce qui est à peu près équivalent à la vitesse maximale du drone Anafi de la société Parrot [32] . Cette trajectoire simulée a ensuite été enregistrée sur le Labsat, de la même manière que les vrais signaux du leurrage fixe.

La fausse position du cas 1 est celle utilisée dans les essais de leurrage fixe. La fausse trajectoire du cas 2 est une trajectoire à trois *Waypoints* qui reprend le point de départ (*Waypoint 1*) et le Waypoint 2 de la trajectoire du récepteur. Le troisième et dernier Waypoint de la fausse trajectoire est situé à 630 m du Waypoint 3 de la trajectoire du récepteur, dans le prolongement de l'axe {*Waypoint* 2 - *Waypoint* 3} de la trajectoire du récepteur. La Figure 45 montre la trajectoire du récepteur (en bleu, parcourue dans le sens des aiguilles d'une montre) et la fausse trajectoire (en pointillé rouge) sur une carte.

FIGURE 45 – Cartographie des trajectoires pour le leurrage mobile

II.5.2 Procédure expérimentale

Les puissances appliquées sur les signaux simulés sont les mêmes que dans les essais du leurrage fixe. Concernant les scénarios d'attaque, compte tenu de la vitesse du drone, seule l'attaque forte a été testée sur les tests de leurrage mobile. Les actions à réaliser sur ce scénario sont les mêmes que celles décrites précédemment dans le Tableau 1. La différence ici est que les canaux du Spirent sont ouverts à $4'00''$ au lieu de $5'00''$.

II.5.3 Résultats sur le u-blox 8

Le premier récepteur testé est cette fois le u-blox 8.

II.5.3.1 Cas 1 : fausse position fixe

Les tests réalisés dans ce cas ont été un succès. On remarque cependant quelques différences vis à vis du leurrage fixe. En effet on constate qu'à puissance égale la rapidité de capture du leurre dépend du moment où on lance le leurre. Autrement dit, cela dépend de la distance séparant le faux point de la position actuelle du récepteur.

Concernant le biais d'horloge et la dérive, les courbes tracées sur une itération de ce test sont données Figure 46 et 47. La ligne en pointillé rouge représente l'instant où les canaux du Spirent ont été ouverts, la flèche 1 indique le moment où le récepteur perd le suivi de la vraie constellation et la flèche 2 indique la reprise du suivi de position sur le leurre.

On remarque ici que le biais d'horloge présente le même comportement face aux attaques de leurrage que sur le leurrage fixe : un saut de valeur a lieu dans la phase de transition du suivi des vrais signaux aux faux signaux. Sur l'itération de la Figure 46 il s'agit d'un saut de 1008.4 μs.

Concernant la dérive du biais, on a des observations différentes de ce qui était attendu. En effet, on constate sur toutes les itérations réalisées, la dérive ne présente pas du tout de saut de valeur important, ce qui est contraire aux observations faites sur la dérive lors du leurrage fixe.

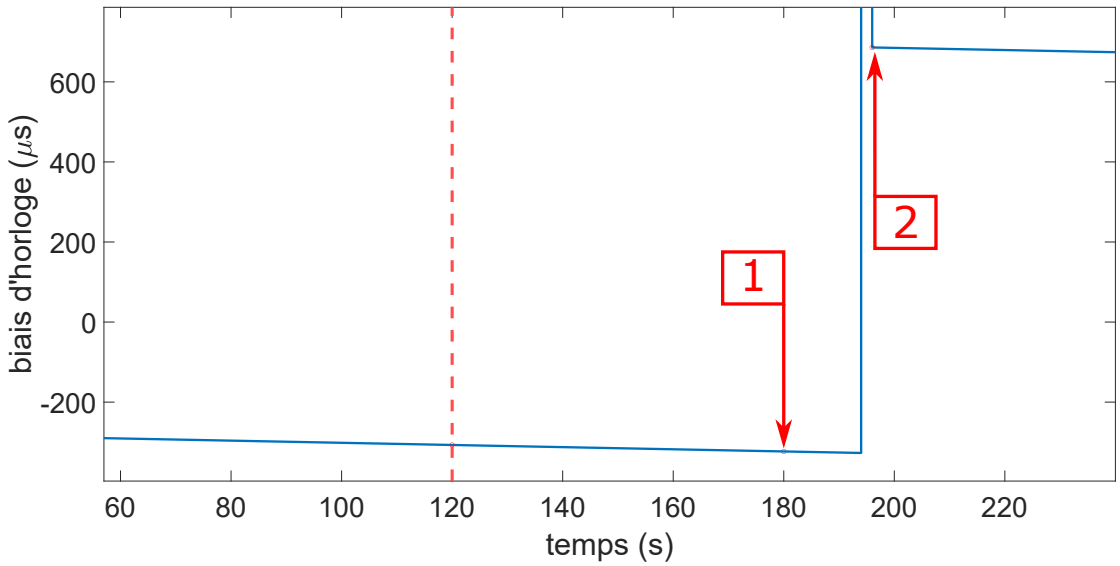

FIGURE 46 – Biais d'horloge pour un leurrage mobile sur fausse position fixe (u-blox 8)

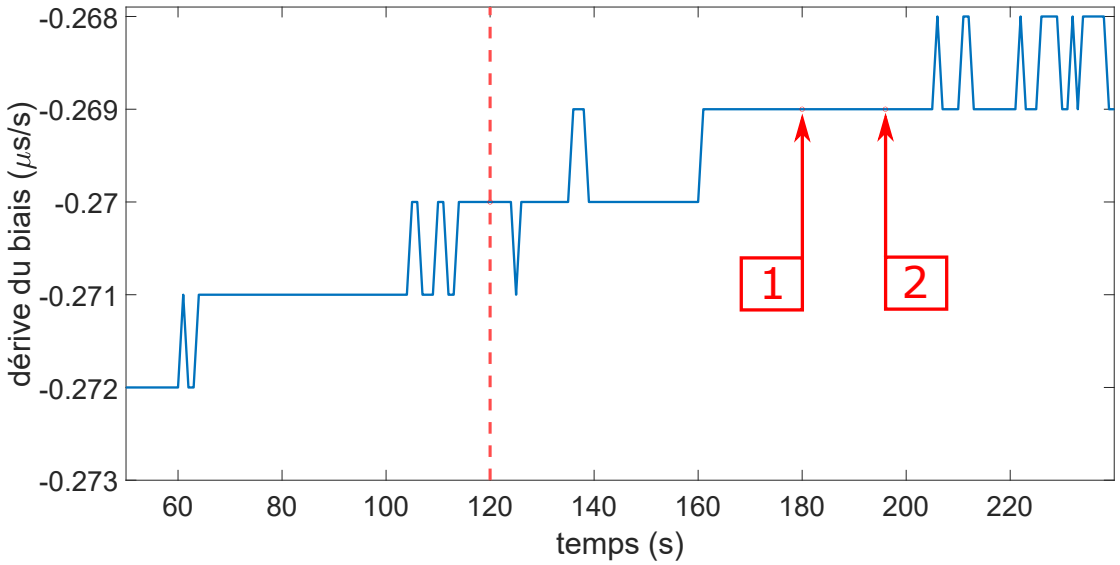

FIGURE 47 – Dérive du biais pour un leurrage mobile sur fausse position fixe (u-blox 8)

II.5.3.2 Cas 2 : fausse trajectoire

Dans ce cas de fausse trajectoire, le leurrage du récepteur u-blox a également été un succès. On constate que sur l'ensemble des itérations réalisées, le temps de capture est plutôt court (de l'ordre de la trentaine de secondes en moyenne). Les courbes tracées du biais d'horloge et de sa dérive sur une itération arbitraire sont représentées Figures 48 et 49. Les lignes en pointillé rouge montrent l'instant où les canaux du Spirent sont ouverts, la flèche 1 indique le moment où le récepteur perd le suivi des vrais signaux et la flèche 2 indique l'instant où le récepteur récupère un suivi de positionnement sur le leurre.

De même que dans le cas 1, on constate sur l'ensemble des itérations réalisées que le biais d'horloge présente un saut de valeur significatif causé par l'attaque de leurrage (dans le cas de la Figure 48 on est à un saut de 101,2 μs). Malheureusement il n'en est toujours pas de même pour la dérive du biais où force est de constater que les sauts de valeur significatifs sont absents lors de l'attaque de leurrage.

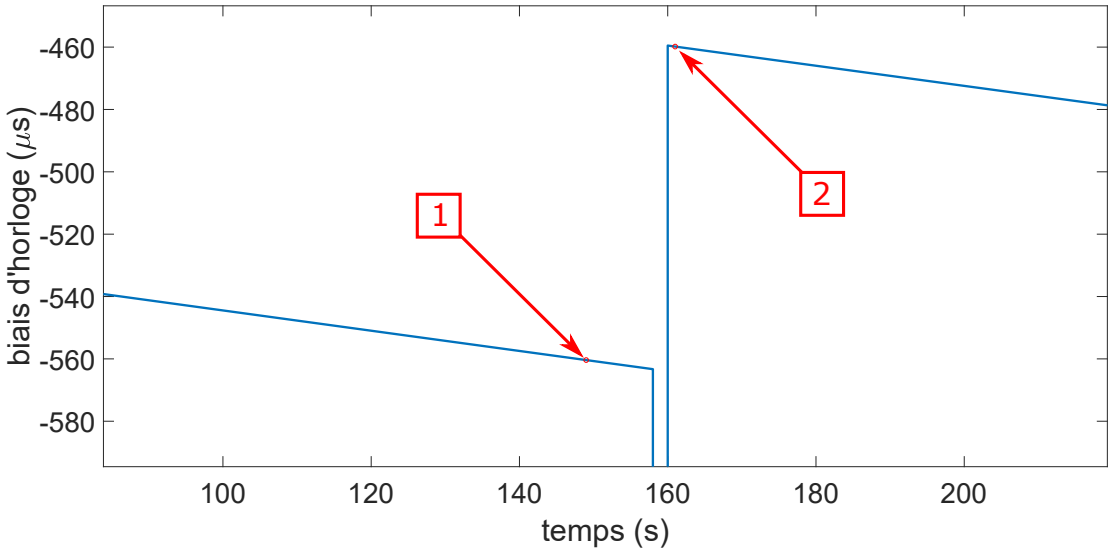

FIGURE 48 – Biais d'horloge durant un leurrage sur fausse trajectoire (u-blox 8)

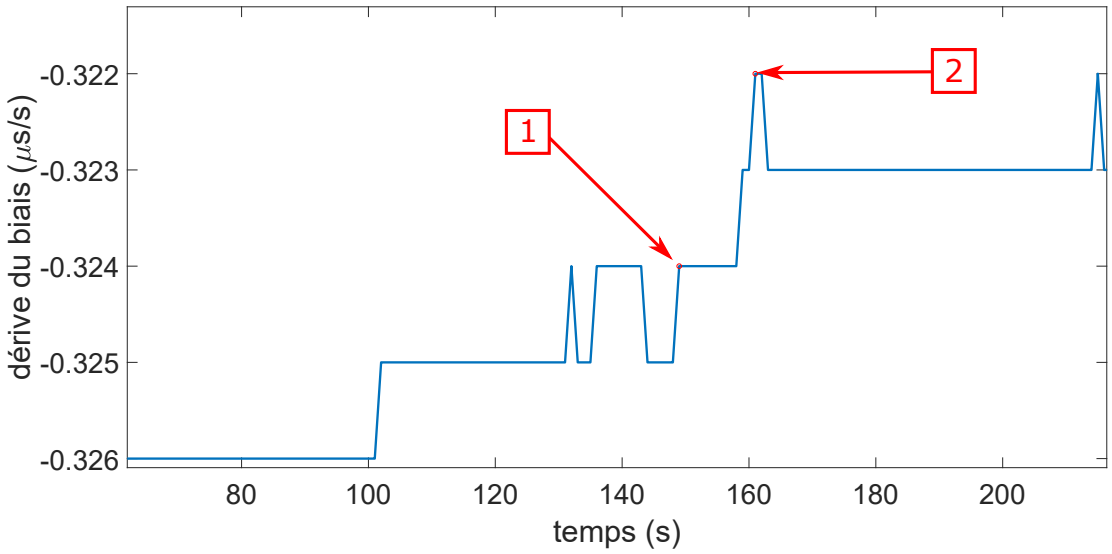

FIGURE 49 – Dérive du biais durant un leurrage sur fausse trajectoire (u-blox 8)

II.5.4 Résultats sur le u-blox 6

Le u-blox 6 a ensuite été testé. Le leurre a eu plus de difficultés à capturer sa cible avec le u-blox 6 comparé au u-blox 8 ou aux scénarios de leurrage fixe. Il a fallu plusieurs essais avant de pouvoir réussir à aller au bout des scénarios de leurrage mobile. Durant les tentatives où l'attaque a échoué, le récepteur ne se raccrochait à aucuns signaux dans certains cas ou restait sur les signaux de la vraie constellation.

Les Figures 50 et 51 représentent respectivement le biais d'horloge et la dérive du biais pour un leurrage mobile sur fausse position fixe avec le u-blox 6. La ligne en pointillé rouge indique l'ouverture des canaux du leurre, les flèches 1 et 2 indiquent respectivement la perte de suivi des vrais signaux et l'accrochage sur les signaux On constate que le biais d'horloge présente bien un saut lorsque le récepteur passe sur les signaux du leurre, mais ce saut n'est pas aussi direct que sur les essais précédents.

En effet, on peut observer des sauts intermédiaires assez significatifs entre la perte de suivi des vrais signaux et

l'accrochage sur les faux signaux (environ 70 μs et 10 μs). Contrairement au u-blox 8 on constate que la dérive du biais est perturbée lors de l'attaque. Comme le biais d'horloge, la dérive présente un saut intermédiaire entre la perte des vrais signaux et l'accrochage sur les signaux du leurre. Ces sauts intermédiaires interviennent dans des phases où le récepteur a bien identifié la présence des signaux des deux constellations mais ne sait pas lesquels il doit suivre. Ces sauts peuvent donc provenir d'une tentative du récepteur à s'accrocher à une des deux constellations.

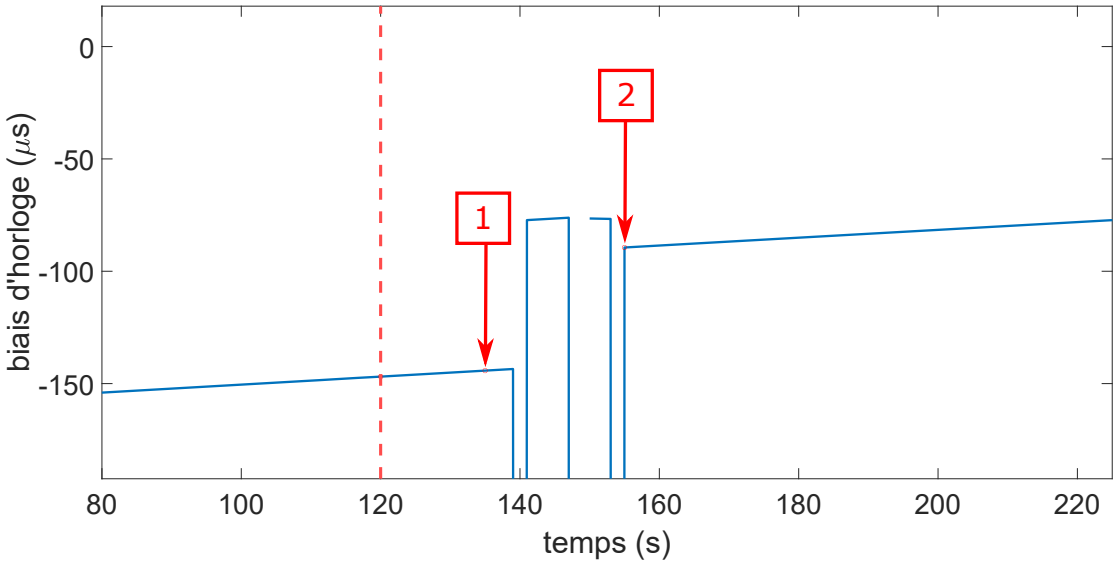

FIGURE 50 – Biais d'horloge pour un leurrage mobile sur fausse position fixe (u-blox 6)

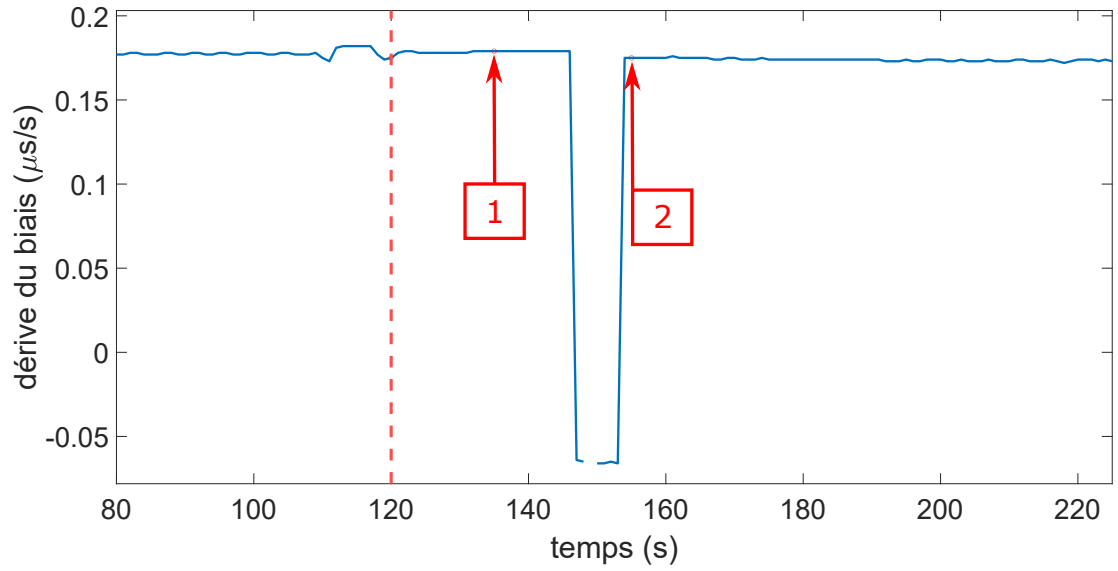

FIGURE 51 – Dérive du biais pour un leurrage mobile sur fausse position fixe (u-blox 6)

II.5.5 Conclusions sur ces essais de leurrage mobile

Il semble donc clair que les attaques de leurrage ont une influence sur le biais de l'horloge. En effet, même lorsque le récepteur ciblé est en mouvement, l'attaque de leurrage va provoquer au niveau du biais de l'horloge un saut de valeur plus important que les variations "naturelles" de cette dernière. La dérive du biais est également impactée dans le cas du u-blox 6 mais pour ce qui est du u-blox 8, on constate qu'elle reste impassible lors d'une attaque de leurrage dans le cas d'une victime en mouvement.

Pour compenser cela, il serait intéressant de regarder le comportement des Doppler des différents satellites de la constellation GNSS durant ces tests de leurrage. En effet, les Doppler ont généralement le même comportement que la dérive de l'horloge, à laquelle s'ajoute la variation naturelle liée au mouvement relatif du satellite et du récepteur. Contrairement à la dérive de l'horloge, les Doppler sont des mesures directes issues des données des satellites et ne sont donc pas altérés par un quelconque calcul effectué par le récepteur. Ainsi leur comportement peut différer vis à vis de la dérive lors d'une attaque de leurrage et donc éventuellement présenter des sauts. Avec le u-blox 8 la mesure des Doppler de chaque satellite de la constellation peut être consultée en direct à l'instant t dans la liste des messages NMEA (National Marine Electronics Association) sur le logiciel u-center. Cependant, il n'est pas possible de stocker cette mesure automatiquement à chaque instant dans un tableau de données continues comme avec le biais d'horloge ou la dérive.

Chapitre III

Etude d'une approche de localisation de leurre par l'utilisation d'une formation de drones

L'étude menée dans le chapitre précédent a mis en évidence les effets d'une attaque de leurrage sur l'horloge d'un récepteur GNSS. Le biais d'horloge subit un saut lorsque le récepteur passe de la vraie constellation GNSS à la constellation du leurre. Ceci peut dans certains cas se répercuter par des sauts sur la dérive du biais de celui-ci. Les résultats obtenus peuvent être utilisés dans une stratégie de défense contre le leurrage applicable sur un récepteur de type COTS.

Ce chapitre va plutôt s'intéresser à une autre stratégie de défense contre le leurrage. Cette stratégie a pour point central la collaboration entre plusieurs drones, et donc plusieurs récepteurs. C'est dans cette optique qu'un bref état de l'art des méthodes utilisant plusieurs antennes et/ou plusieurs récepteurs a été réalisé.

III.1 Etat de l'art sur les réseaux d'antennes/récepteurs

Comme expliqué dans [33], les techniques de défense contre le leurrage utilisant plusieurs éléments (antennes et/ou récepteurs) sont généralement désignées par le terme de méthodes "spatiales". Ce terme est utilisé car ces méthodes ont pour objectif d'analyser la signature spatiale des signaux reçus pour identifier les interférences de leurrage. Ces méthodes font donc l'hypothèse que le leurre émet ses signaux par le biais d'une unique antenne. On peut intégrer ces méthodes à la catégorie des techniques basées sur la géométrie décrite précédemment en I.3.3. On peut distinguer deux groupes parmi les techniques spatiales :

— les techniques à base d'antennes en réseau,

— les techniques à base de récepteurs en réseau

La plupart de ces techniques font l'hypothèse que le leurre émet ses signaux à partir d'une seule antenne. Ceci implique donc que les signaux de leurrage reçus par le système GNSS ciblé proviennent de la même direction.

III.1.1 Réseau d'antennes

Les réseaux d'antennes se présentent sous la forme d'une structure rassemblant un ensemble d'antennes reliées à un unique récepteur. Chaque antenne est connectée à son propre canal de conversion RF. Ces ensembles {antenne - étage de conversion} sont connectés à une unité de classification qui va envoyer les données nécessaires à l'unité de calcul de solution PVT d'un récepteur [33]. Ce type de structure a été pensé à la base pour contrer les interférences de brouillage ce qui a donné naissance à la technologie CRPA (pour Controlled

Reception Pattern Antenna)[6].

Les Figures 52 et 53 représentent respectivement une photo d'une antenne CRPA et le schéma bloc d'une antenne de ce type.

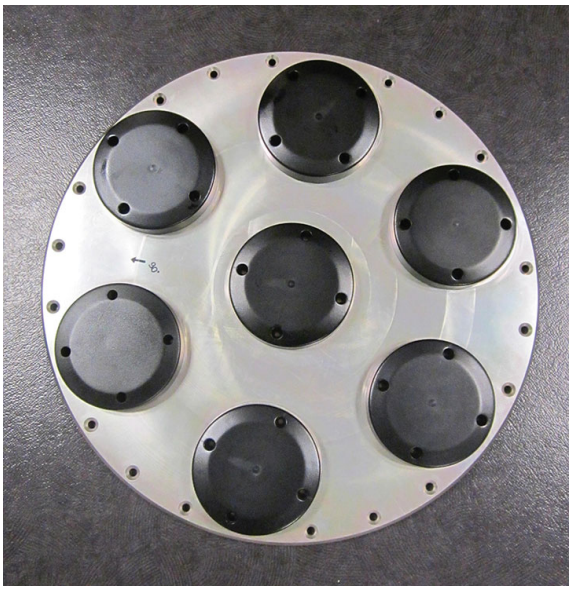

FIGURE 52 – Antenne CRPA

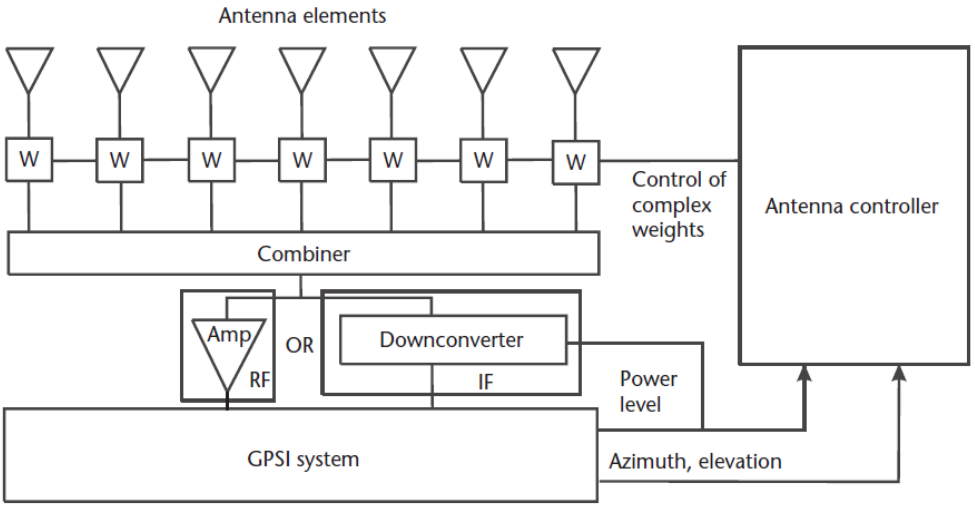

FIGURE 53 – Schéma bloc d'une antenne CRPA présenté dans [6]

Comme le montre le schéma bloc, les antennes du réseau sont chacune associées à un terme de pondération, représenté par le bloc W de la Figure 53. La pondération des signaux reçus par les antennes et la répartition spatiale des antennes du réseau permettent de contrôler la forme du diagramme de réception global de l'antenne CRPA en réduisant le poids des zones touchées par les interférences (on appelle ce processus le *null steering*) et amplifier les autres (on appelle ce processus le *beam steering*).

Dans la littérature de nombreux travaux de recherche ont été lancés pour adapter ce type de structure pour la défense contre les interférences de leurrage. Ces techniques ont pour objectif d'aller plus loin que la simple

détection de leurrage en ajoutant la possibilité de classifier les signaux reçus en signaux de leurrage ou en signaux authentiques, mais aussi en ajoutant la possibilité d'atténuer l'impact des signaux de leurrage.

De la même manière que pour les techniques de traitement du signal avancé évoquées partie I.3.1, les techniques par réseau d'antennes peuvent être appliquées en pre-désétalement ou en post-désétalement.

III.1.1.1 Pre-désétalement

Pour les techniques en pre-désétalement, comme celle proposée par Daneshmand et al. dans [34] et [35], une matrice de corrélation spatiale est formée en calculant l'intercorrélation entre les signaux reçus par les antennes. Etant donné que les signaux du leurre viennent d'une même source, la puissance de ces signaux s'additionne. Ceci se reflète par une zone spatiale présentant des densités de puissance plus forte que pour les vrais signaux. Cette matrice permet d'identifier les vecteurs de signature spatiale (ou SSV pour Spatial Signature Vector) des signaux de leurrage pour les atténuer.

La Figure 54 présente le schéma bloc du module anti-leurrage développé par Daneshmand et al. dans [34].

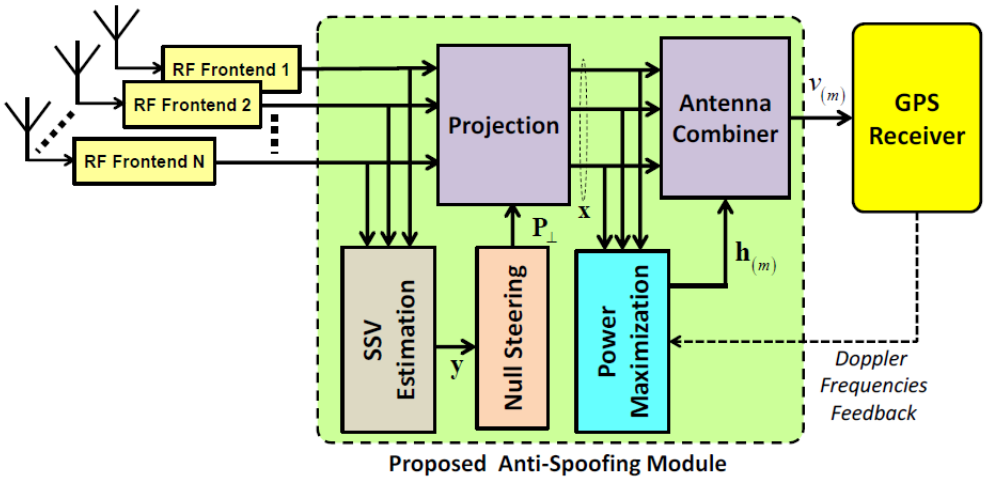

FIGURE 54 – Schéma bloc du module anti-leurrage de [34]

Ces techniques en pre-désétalement présentent l'avantage de demander relativement peu de puissance de calcul. Par ailleurs, le signal de sortie du module anti-leurrage peut être transmis sur un unique canal de transmission. Il est donc possible d'utiliser ce module sur n'importe quel récepteur.

Cependant pour être efficace il faut que la puissance des signaux du leurre soit suffisamment forte pour pouvoir se démarquer des vrais signaux.

III.1.1.2 Post-désétalement

Pour les techniques post-désétalement le principe général reste le même mais l'estimation des vecteurs de signature spatiale se fait sur les signaux démodulés. Comme expliqué dans [36] plutôt que de s'intéresser à la puissance des signaux du leurre, on s'intéresse directement à leur angle d'arrivée. Par le biais d'une intercorrélation il est possible de déterminer les vecteurs de signature spatiale correspondant au leurre.

Ces méthodes restent efficaces contre les leurres à faible puissance mais la puissance de calcul nécessaire est plus importante. Par ailleurs, il est nécessaire de modifier les modules d'acquisition et de suivi du récepteur GNSS pour pouvoir démoduler l'ensemble des signaux reçus de chaque antenne du réseau.

Quelques travaux visant à réduire la charge de calcul de ces méthodes ont donné des résultats encourageants. Rossouw et al. [37] proposent d'utiliser un *récepteur instantané* (ou *snapshot receiver* en anglais) qui est un

type de récepteur n'utilisant que les signaux reçus sur un bref intervalle de temps (pouvant aller de 2 ms à plus de 100 ms). Cette portion de données est envoyée à un serveur pour le traitement. Ceci permet d'alléger la charge de calcul que le récepteur doit réaliser.

III.1.2 Réseau de récepteurs

Comme expliqué dans [33] les techniques à base de réseau de récepteurs se présentent sous la forme d'en ensemble de récepteurs répartis sur un voisinage plus ou moins proche. Chaque récepteur du réseau opère de façon indépendante et n'est connecté physiquement à aucun autre récepteur du réseau. Il y a cependant un canal de communication entre les membres du réseau et/ou vers une station en cloud pour échanger leurs mesures. A partir de cette architecture, plusieurs techniques peuvent être mises en place.

III.1.2.1 Utilisation des positions

Une première possibilité est d'utiliser les positions des récepteurs du réseau. Jansen et al. dans [38] se sert de la distance entre les récepteurs du réseau par le biais des positions GPS. La Figure 55 montre la formation de récepteurs GPS utilisée dans [38]. Il s'agit d'une formation de quatre récepteurs (notés $R_1, ..., R_4$) répartis sur un carré de côté d, qui correspond à la distance entre les plus proches voisins. Chaque récepteur calcul à partir des coordonnées GPS la distance des ses plus proches voisins.

Comme illustré Figure 55, lorsque la formation est attaquée par le leurre, les signaux de leurrage proviennent de la même source et pointent vers la même fausse position. La position calculée par les récepteurs touchés est alors la même, la distance entre voisins calculée par les récepteurs touchés ne sera plus d mais une valeur tendant vers 0. En surveillant les distances entre voisins calculées par les récepteurs on peut alors identifier si le réseau de récepteurs est attaqué par un leurre.

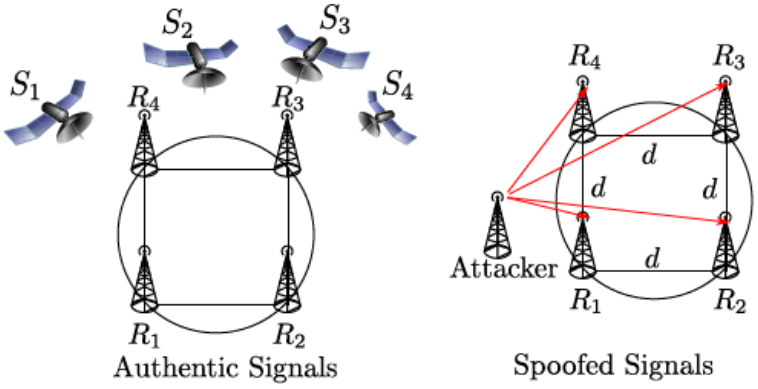

FIGURE 55 – Réseau de récepteurs utilisé par Jansen et al. dans [38]

III.1.2.2 Angle d'arrivée et déphasage de la porteuse

On peut citer dans un premier temps les techniques calculant directement l'angle d'arrivée des signaux. L'hypothèse de l'unicité de l'antenne du leurre implique que les signaux arrivant sur les récepteurs du réseau présentent le même angle d'arrivée. A partir de deux récepteurs il est possible de calculer l'angle d'arrivée des signaux. Des travaux comme ceux de Borio et al. dans [3] et [25] (déjà évoqués brièvement en I.3.3) présentent de bons résultats. La Figure 56 illustre le problème de calcul d'angle d'arrivée présenté dans [3]. R_x1 et R_x2 désignent les deux récepteurs, d_i^j $(j = \{1, 2\})$ est la distance entre le récepteur j et le satellite i, D est la distance entre les récepteurs et α_i est l'angle d'arrivé des signaux du satellite i.

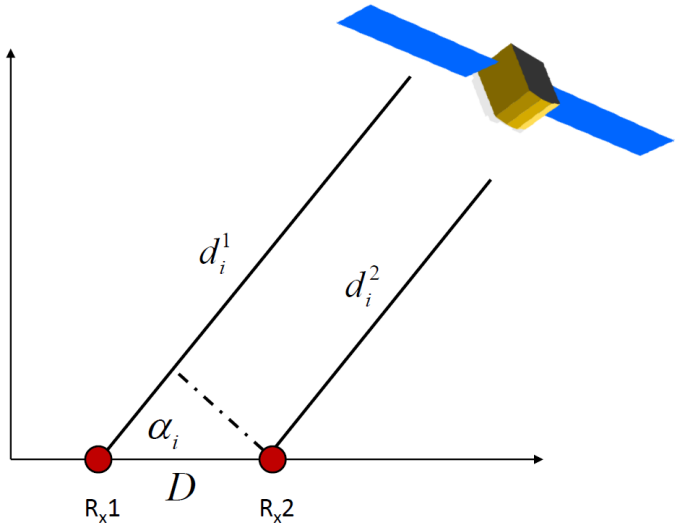

FIGURE 56 – Modélisation du problème de calcul d'angle d'arrivée dans [3]

Vu l'ordre de grandeur de la distance entre les satellites et les récepteurs, on peut faire l'approximation que les signaux reçus d'un satellite i au niveau des récepteurs sont parallèles. On peut alors exprimer la différence des distances comme

$$d_i^1 - d_i^2 = Dcos(\alpha_i) \tag{III.1}$$

L'expression mathématique de la simple différence de déphasage de la porteuse $\Delta\phi_i$ fait intervenir ce terme géométrique. La simple différence est la différence du déphasage d'un signal d'un satellite entre les deux récepteurs, soit

$$\Delta\phi_i = \phi_i^1 - \phi_i^2 \tag{III.2}$$

En utilisant la simple différence de déphasage de la porteuse, on peut vérifier si le terme géométrique est le même pour tous les signaux reçus, ce qui indique si les signaux sont authentiques ou issus d'un leurre. Pour réaliser cette classification une utilise une approche de type GLRT pour discriminer le cas avec leurrage du cas sans leurrage. Le terme de décision statistique utilisé est une somme des carrés pondérée des simples différences de déphasage (d'où le nom de "Sum-of-Squares detector" affilié à cette méthode dans [3]). Si le terme est supérieur à un certain seuil, alors les récepteurs sont leurrés.

Un inconvénient de cette technique est qu'il n'est possible de détecter correctement l'attaque de leurrage que lorsque tous les signaux suivis par les récepteurs sont des signaux de leurrage. Dans le cas où les récepteurs suivent à la fois des signaux de leurrage et des signaux authentiques, le détecteur Sum-of-Squares peut donner des faux positifs ou des faux négatifs. Nguyen et al. dans [39] ont montré qu'utiliser la double différence de déphasage de la porteuse $\nabla\Delta\phi_i$ permet de corriger ce défaut. La double différence est la différence de la simple différence entre le signal de deux satellites, soit

$$\nabla\Delta\phi_i = \Delta\phi_i^1 - \Delta\phi_i^2 \tag{III.3}$$

Une autre façon d'exploiter le déphasage de la porteuse est de regarder sa variation au cours du temps. Jahromi et al. ont démontré dans [40] et [41] que dans le cas des signaux du leurre, la double différence du déphasage de la porteuse est invariante au cours du temps, ce qui n'est pas du tout le cas avec les signaux

des satellites. On peut donc utiliser la variation de la double différence du déphasage de la porteuse pour classifier les signaux reçus.

Il est possible d'appliquer ces techniques avec une station cloud intégrée au réseau. Broumandan et al. dans [42] utilisent une architecture de réseau où les récepteurs sont connectés à une station cloud nommée centrale de vérification d'authenticité (ou CAV pour Central Authenticity Verification en anglais). La Figure 57 présente un schéma bloc de cette structure de réseau.

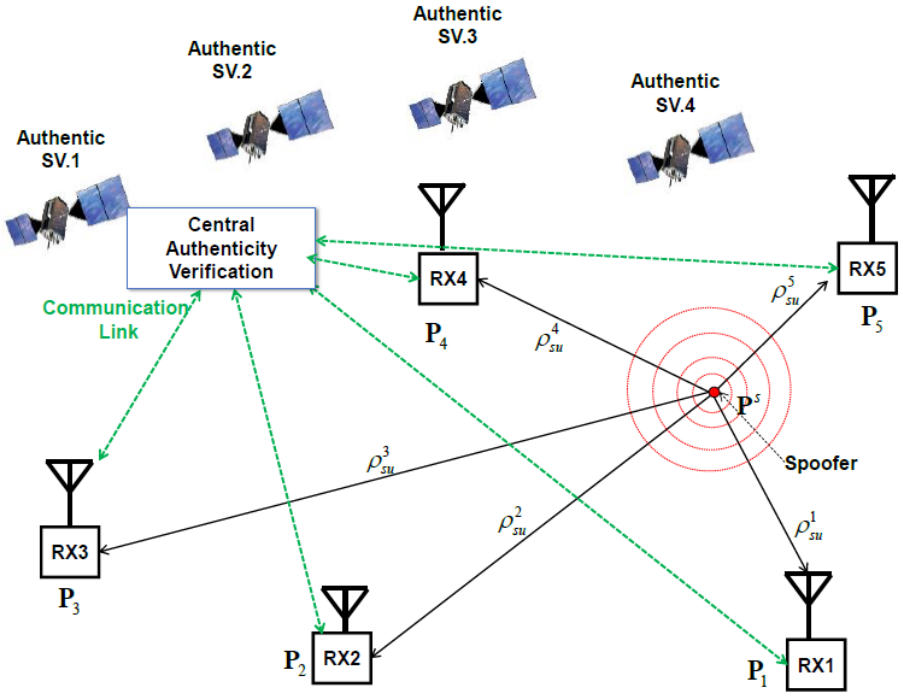

FIGURE 57 – Schéma bloc du réseau proposé dans [42]

La CAV sert principalement à gérer l'état du réseau et traiter les données envoyées par les récepteurs. La détection et la classification des signaux de leurrage se fait donc sur la CAV, mais il est aussi possible de laisser les récepteurs s'occuper de la détection du leurrage par le biais de méthodes mono-récepteur comme le contrôle du gain de l'AGC par exemple. Par ailleurs, la CAV peut aussi exploiter les solutions PVT calculées par les récepteurs, en particulier le biais d'horloge, pour localiser le leurre.

L'inconvénient de ce type de technique est qu'il est nécessaire de disposer d'une capacité de calcul suffisamment grande pour traiter l'ensemble des données échangées par les récepteurs. Il faut également s'assurer d'avoir un bon transfert des données entre les différents membres du réseau.

Cet état de l'art montre qu'en utilisant des structures à "éléments multiples" telles que les réseaux d'antennes ou les réseaux de drones, il est possible de mettre en place des défenses anti-leurrage plus avancées que la simple détection d'interférence. L'ajout principal de ces techniques vis à vis des techniques "mono-élément" est la capacité de classification des signaux reçus. Un autre ajout que peuvent apporter ces techniques multi-éléments est la capacité de localisation de la source d'interférence. La suite de notre étude vise à proposer une idée de stratégie exploitant un réseau de récepteurs pour estimer la direction d'un leurre GNSS.

III.2 Proposition d'une stratégie anti-leurrage basée sur l'utilisation de drones en formation

La stratégie développée dans ce chapitre a pour objectif de réaliser une estimation de la direction où se trouve le leurre par l'utilisation d'un réseau de récepteurs. Ce réseau prend la forme de plusieurs drones répartis selon une formation géométrique spécifique.

L'estimation de la direction du leurre est réalisée par le biais de ce qu'on appelle un protocole de déplacement. Le protocole de déplacement définit un ensemble de mouvements réalisés par la formation de drones dans l'optique de délimiter une zone de l'espace dans laquelle le leurre est localisé.

III.2.1 Hypothèses de départ et mise en place de la stratégie

Afin de pouvoir fixer les modalités de mise en place de cette stratégie, il convient de se fixer quelques hypothèses de départ :

— La première hypothèse est que le leurre est localisé à une position fixe et n'émet pas ses signaux dans une direction spécifique. On considèrera par la suite que le leurre utilise une antenne de type Cassegain ou Yagi-uda.

— La deuxième hypothèse est qu'au moins un des drones de la formation n'est pas touché par les signaux du leurre.

— Enfin, les drones de la formation naviguent tous à la même altitude, on travaillera donc principalement en deux dimensions dans le plan horizontal.

La formation de drones est composée d'au moins trois drones, et dans le cas de notre étude développée par la suite, ce nombre est monté jusque cinq drones. Les drones de la formation sont répartis les uns par rapport aux autres selon une forme géométrique fixe. La Figure 58 montre la répartitions des drones dans le cas d'une formation à trois, quatre et cinq drones (représentés en bleu sur le Figure) vue dans le plan horizontal. Les flèches vertes N et E sont les axes Nord et Est d'un repère du plan horizontal centré sur un des drones de la formation. Par la suite on appellera ce repère le *repère local*.

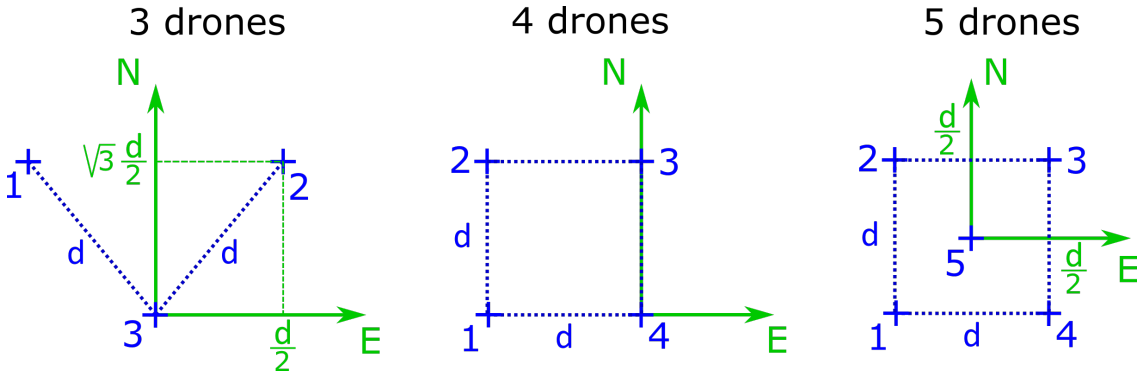

FIGURE 58 – Formations de drones étudiées par la suite

Chaque drone de la formation est capable de détecter s'il subit une attaque de leurrage grâce à une technique de détection de leurrage mono-récepteur au choix. Les drones sont donc capables de transmettre leur statut (leurré ou non leurré) aux autres drones. Dans notre cas on considèrera que la détection du leurrage se fait par le contrôle du comportement du biais d'horloge du récepteur.

Au sein de la formation, on attribue à un drone le rôle de *drone de contrôle*. Ce drone de contrôle est responsable de la gestion de la formation. C'est donc lui qui gère les déplacements des drones de la formation. Il

est aussi responsable du contrôle des distances entre chaque drone voisin et le statut non leurré / leurré des drones de la formation, ces deux informations étant envoyées par les autres drones.

L'échange d'information et le calcul de distance entre drones voisins peut être réalisé en utilisant la technologie Ultra Large Bande(ULB ou UWB pour Ultra WideBand en anglais). Par ailleurs, le drone de contrôle est celui sur lequel on va centrer le repère local.

Malgré l'hypothèse fixée plus tôt stipulant qu'au moins un drone n'est pas touché par les signaux du leurre, il est toujours possible que le drone de contrôle ne soit pas ce drone chanceux. La formation de drones doit alors être capable de changer dynamiquement l'identité du drone de contrôle. Par défaut le drone de contrôle est le drone représenté au centre du repère Nord-Est sur la Figure 58.

III.2.2 Protocole de déplacement

La stratégie d'estimation de la direction du leurre peut être découpée en quatre étapes. Elles sont illustrées dans le cas d'une formation à trois drones sur les Figures 59 à 62 : les drones sont représentés par les croix bleues, le drone de contrôle est annoté par la lettre C, le repère local est représenté en vert, le leurre est représenté par le carré rouge S tandis que son champs d'action est représenté en pointillés rouges. Les quatre étapes de la stratégie sont les suivantes :

— Etape 1 : on "initialise" la formation de drones en définissant le drone de contrôle et les coordonnées des drones de la formation. Les drones sont en mode navigation et se déplacent de façon autonome en conservant bien la géométrie de la formation. Lorsqu'un drone arrive dans le champs d'action du leurre et se fait leurrer (par exemple le drone 1 sur le Figure 59), un saut du biais d'horloge est détecté sur l'horloge du récepteur et l'information est envoyée au drone de contrôle qui stoppe le déplacement de la formation pour lancer le protocole de déplacement.

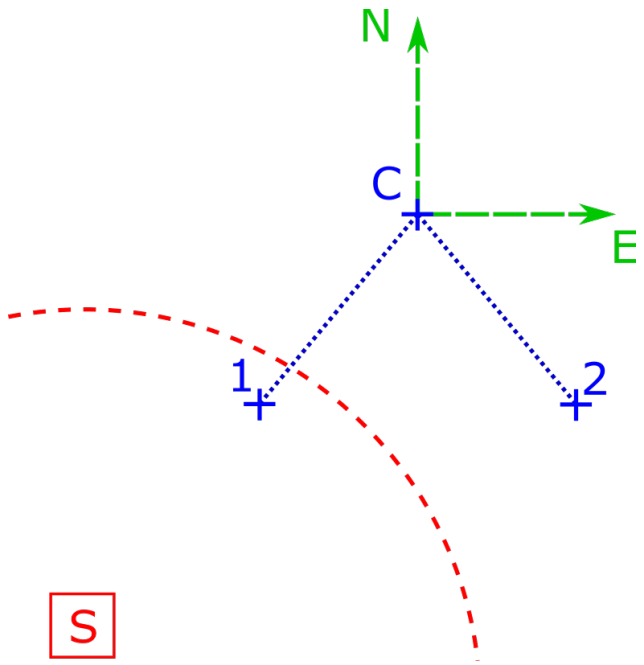

FIGURE 59 – Etape 1

— Etape 2 : les drones de la formation se mettent en rotation autour du drone central, tout en conservant la forme géométrique initiale de la formation. Au cours de la rotation, le drone de contrôle inspecte le statut leurré/non leurré des drones de la formation. L'observation des statuts des drones permet de déterminer si un drone sort ou rentre dans le champs d'action du leurre. Lorsqu'un drone de la

formation change de statut, on garde en mémoire sa position et l'angle correspondant dans le repère local. Cela correspond à la position $1'$ et l'angle β sur la Figure 60.

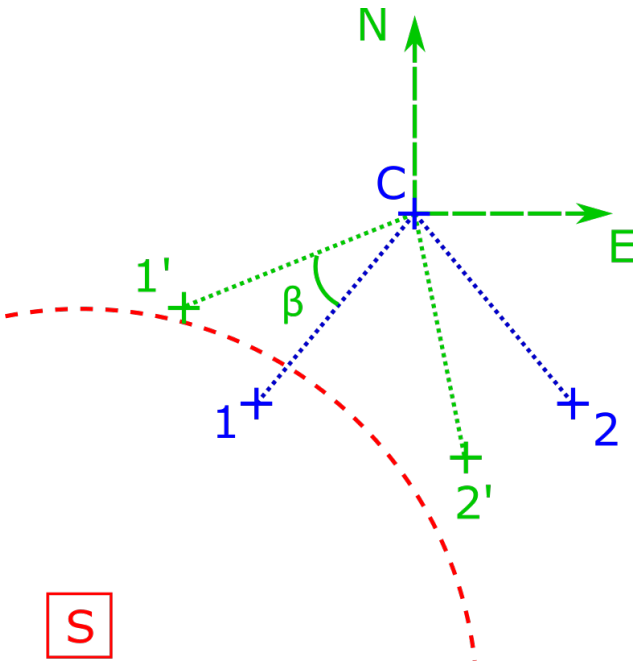

FIGURE 60 – Etape 2

— Etape 3 : la rotation de la formation de drones continue jusqu'à ce qu'un nouveau changement d'état d'un drone de la formation arrive. Encore une fois on enregistre la position et l'angle de rotation correspondants. Par exemple, sur la Figure 61 cela correspond à la position $2''$ et l'angle α.

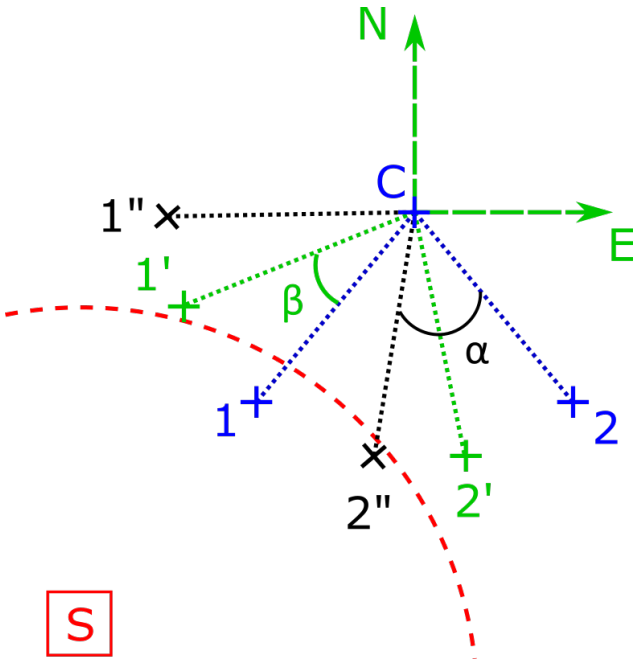

FIGURE 61 – Etape 3

— Etape 4 : A l'aide des angles obtenus lors des changements de statut des drones de la formation on peut définir une zone angulaire dans le repère local où le leurre est susceptible de se trouver. Le drone de contrôle peut alors définir une nouvelle direction de déplacement pour s'éloigner du leurre. Sur la Figure 62 la zone angulaire correspond à la zone délimitée par les lignes en pointillés jaunes.

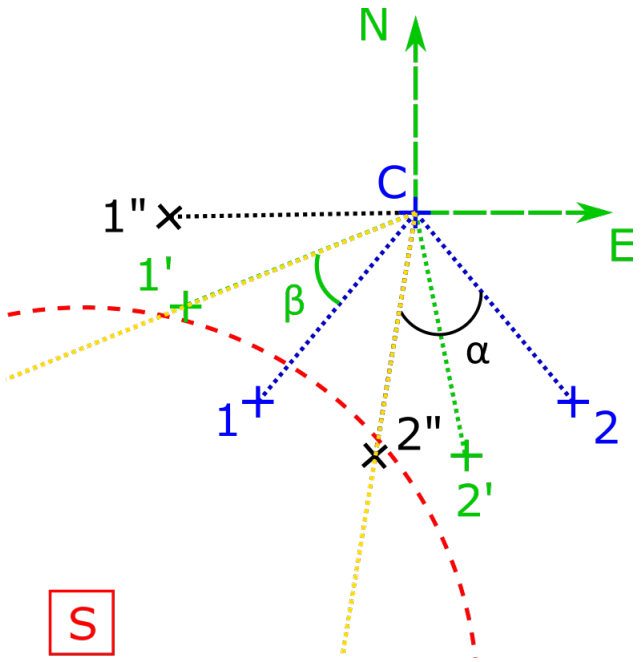

FIGURE 62 – Etape 4

Un protocole comme celui-ci est ici illustré dans un cas idéal où le leurre dispose d'une antenne isotrope lui permettant d'émettre uniformément dans toutes les directions. En pratique ce n'est pas le cas et il est donc nécessaire de prendre en compte le comportement des différents types d'antennes qu'un leurre peut utiliser. On peut néanmoins envisager que ce protocole de déplacement constitue une base de travail pour une stratégie anti-leurrage qu'il conviendra d'enrichir par la suite.

La suite de notre étude consiste donc à tester cette base de stratégie afin de mettre en évidence ses limites et les points pouvant être améliorés.

III.3 Développement d'un code de simulation

Afin de tester les bases de notre stratégie de défense anti-leurrage par réseau de récepteurs, un code de simulation a été développé. Ce code a pour objectif de reproduire le protocole de déplacement décrit en partie III.2.2.

Le code de simulation utilise une boucle itérative pour gérer le contrôle des statuts des drones, de leurs positions et des commandes de déplacement. On considère que chaque itération de la boucle représente l'ensemble des opérations de détection de leurrage, contrôle du statut des drones de la formation et calcul des nouvelles positions pour l'itération suivante. Cela implique donc qu'on ne modélise pas les capacités techniques des récepteurs GNSS pour le traitement des métriques de détection de leurrage ainsi que le traitement de tous les calculs relatifs aux déplacements.

Pour pouvoir simuler différents scénarios de tests pour le protocole de déplacement, il est nécessaire de bien modéliser la formation de drones et ses déplacements mais également l'action du leurre.

III.3.1 Mise en place d'un repère local

Le premier bloc important de ce code de simulation est la mise en place du repère local. Ce repère local est important car c'est dans celui-ci que le drone de contrôle va travailler pour gérer l'ensemble des déplacements de la formation. C'est aussi dans ce repère que la zone angulaire où peut se trouver le leurre est estimée. Même si les raisonnements décrits dans ce chapitre sont dans un cadre deux dimensions, le repère local est en réalité défini comme un repère trois dimensions dans le code de simulation. Comme expliqué précédemment, le repère local est toujours centré sur le drone central et ses axes sont orientés vers la direction Est, la direction Nord et la direction verticale. Les drones de la formation étant à la même altitude, on ne travaillera qu'avec les coordonnées du plan (Nord-Est) du repère local.

Pour obtenir le repère local, il est nécessaire d'effectuer un changement de repère à partir des coordonnées du drone de contrôle exprimées dans le repère ECEF. Ces dernières sont également obtenues par une conversion des coordonnées GNSS (à savoir latitude, longitude et altitude). Les détails des opérations de changement de repère sont donnés en Annexe C.

La Figure 63 illustre le changement de repère opéré pour obtenir les coordonnées d'un drone dans le repère local. Sur cette figure, le repère ECEF est le repère $(O, \overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z})$ tandis que le repère local est le repère $(P, \overrightarrow{h}, \overrightarrow{e}, \overrightarrow{n})$.

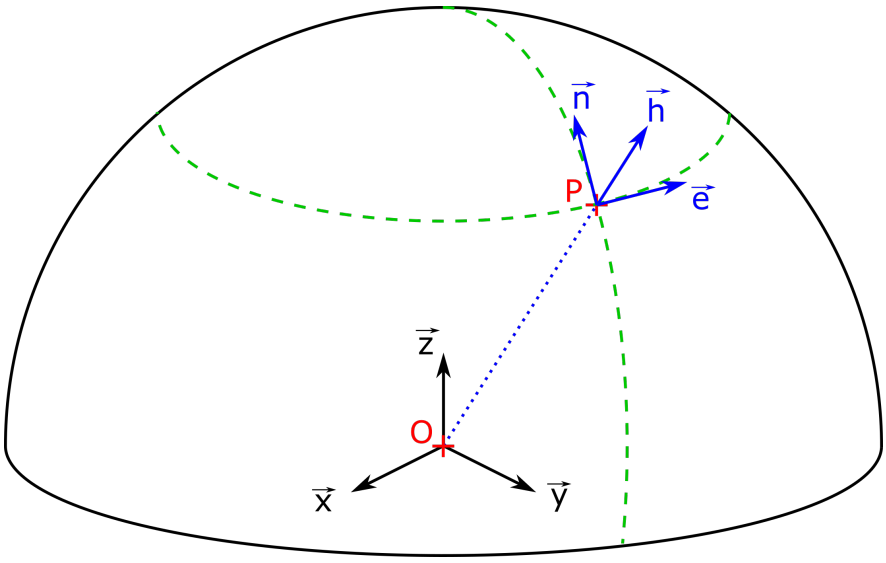

FIGURE 63 – Changement de repère

Le repère local étant centré sur le drone de contrôle de la formation, son orientation et sa position relative au repère ECEF sont dépendants de la position du drone de contrôle. Il est donc mis à jour à chaque déplacement du drone de contrôle. Comme la répartition géométrique des drones de la formation est fixe, les coordonnées de chaque drone dans le repère local restent constant. Par ailleurs, vu que le drone de contrôle n'est pas immunisé face aux attaques de leurrage, son rôle peut être attribué à n'importe quel drone non leurré de la formation et cela de façon dynamique. Ainsi, chaque drone D_i connait les coordonnées des autres drones de la formation exprimées dans le repère local centré sur D_i. Par exemple dans le cas d'une formation à quatre drones on a :

L'utilisation de ce repère local permet donc de faciliter le positionnement des drones de la formation par une représentation plus intuitive de l'espace qu'avec le repère ECEF. Les détails des calculs pour passer du repère local au repère ECEF (et inversement) est décrit en Annexe 3.

Tableau 7 – Coordonnées des drones dans le repère local

Drone de contrôle	Coordonnées			
	D1	D2	D3	D4
D1	$(0,0)$	$(0,d)$	(d,d)	$(d,0)$
D2	$(0,-d)$	$(0,0)$	$(d,0)$	$(0,-d)$
D3	$(-d,-d)$	$(-d,0)$	$(0,0)$	$(0,-d)$
D4	$(-d,0)$	$(-d,d)$	$(0,d)$	$(0,0)$

III.3.2 Modélisation du diagramme de rayonnement des antennes

Le deuxième bloc important du code de simulation est la modélisation du diagramme de rayonnement des antennes. On considère que le leurre est immobile et utilise une antenne émettant ses signaux autour d'elle. Le statut d'un drone est décidé à partir du niveau de puissance des signaux reçus par le drone. En regardant si la puissance des signaux du leurre dépasse la puissance des signaux des satellites d'un certain seuil, on décide si le drone est leurré ou non.

En pratique les antennes RF n'émettent pas leurs signaux uniformément dans toutes les directions. Ainsi, pour savoir dans quelles directions une antenne va rayonner le plus de puissance, et donc en déduire la puissance reçue par un drone à un point donné, on doit s'intéresser au diagramme de rayonnement. Ce diagramme représente le gain de l'antenne dans une direction spécifique de l'espace. Il s'agit d'une représentation en trois dimensions mais les documentations techniques des antennes utilisent souvent une représentation en deux dimension de ce diagramme (plan horizontal ou plan vertical).

La forme de ce diagramme est une source potentielle de problème dans l'application de la stratégie d'estimation de la direction du leurre présentée partie III.2.2. Afin de déterminer les limites de cette stratégie vis à vis du type de diagramme de rayonnement de l'antenne du leurre, il a été décidé de tester deux types d'antennes communes :

— une antenne de type parabolique, aussi appelée Cassegrain,

— une antenne de type Yagi-Uda.

A l'aide de la toolbox *Antenna* de Matlab il est possible de concevoir des antennes RF personnalisées. Les Figures 64 et 65 montrent le diagramme de rayonnement 3D des antennes Cassegrain et Yagi-Uda utilisés par la suite. Etant donné que la formation de drone travaille dans le plan horizontal, les diagrammes utilisés pour le leurre du code de simulation seront des diagrammes en deux dimensions.

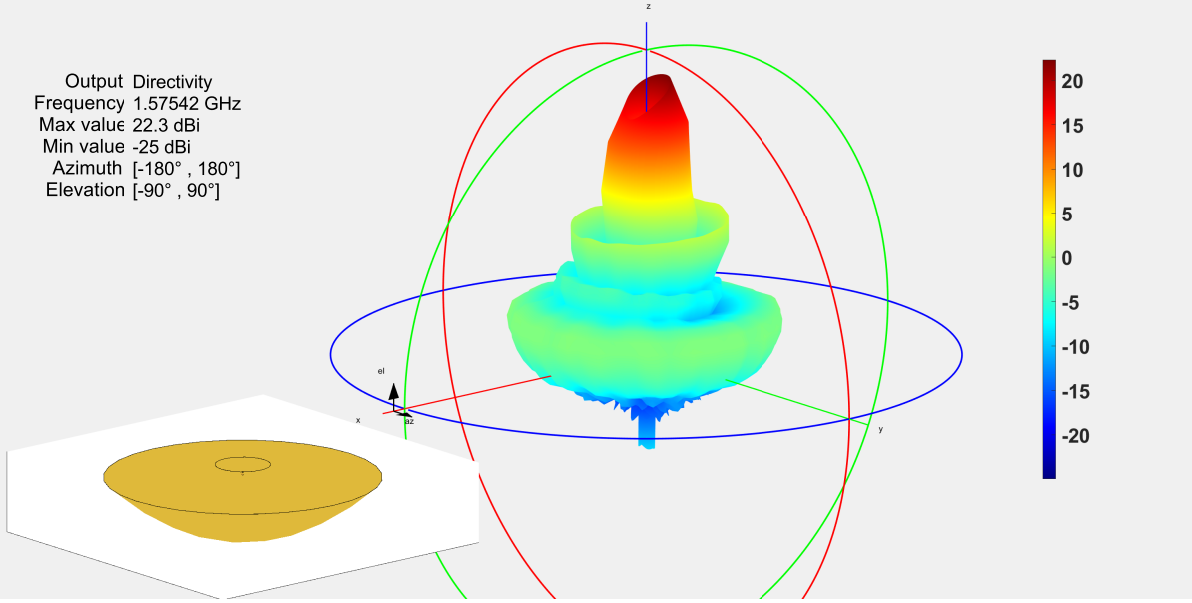

FIGURE 64 – Diagramme de rayonnement 3D de l'antenne Cassegrain

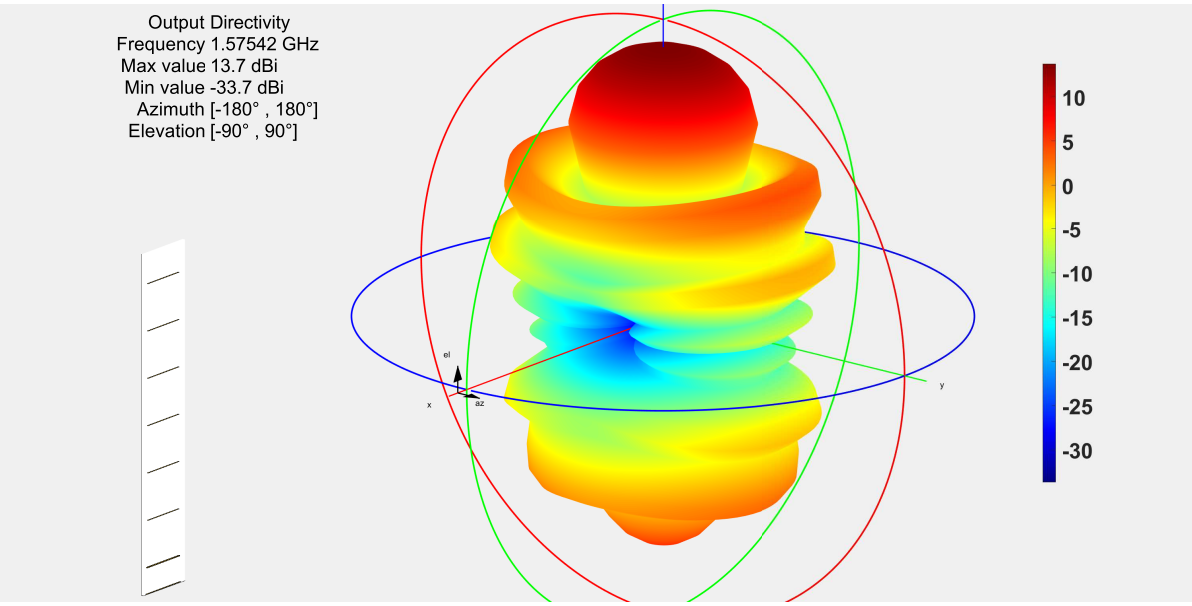

FIGURE 65 – Diagramme de rayonnement 3D de l'antenne YagiUda

Pour calculer la puissance des signaux du leurre reçus par un drone, on utilise l'équation des télécommunications (aussi appelée équation de Friis) :

$$P_r = P_t + G_t + G_r - P_{propagation} \tag{III.4}$$

avec P_r la puissance reçue par le récepteur (en dBm), P_t la puissance délivrée par l'antenne du leurre (en dBm), G_t et G_r respectivement les gains de l'antenne du leurre et du récepteur, et $P_{propagation}$ les pertes de propagation. Les pertes de propagation peuvent s'exprimer comme suit :

$$P_{propagation} = -20 \times \log\left(\frac{\lambda}{4\pi d}\right) = -20 \times \log\left(\frac{c}{4\pi f d}\right)$$

avec c la célérité de la lumière, f la fréquence des signaux (en MHz) et d la distance entre les deux antennes (en km). Avec ces unités pour f et d, on a alors :

$$P_{propagation} = 32.45 + 20\log(f) + 20\log(d)$$

D'où la puissance reçue exprimée par :

$$P_r = P_t + G_t + G_r - 32.45 - 20\log(f) - 20\log(d) \tag{III.5}$$

Les diagrammes de rayonnement nous permettent de calculer les gains d'antenne correspondant à la direction du drone étudié vis à vis du leurre. Dans le cadre de notre étude, les plans horizontaux des diagrammes de rayonnement ont été utilisés. Ces derniers sont représentés Figure 66 pour l'antenne Cassegrain et Figure 67 pour l'antenne Yagi-Uda.

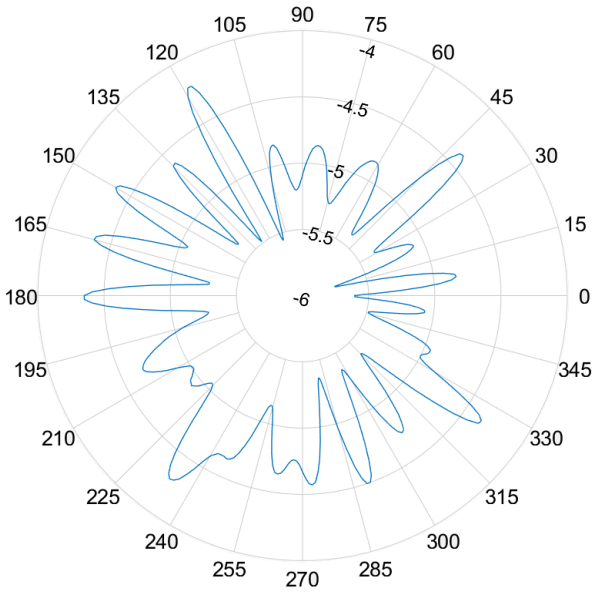

FIGURE 66 – Diagramme horizontal en polaire de l'antenne Cassegrain

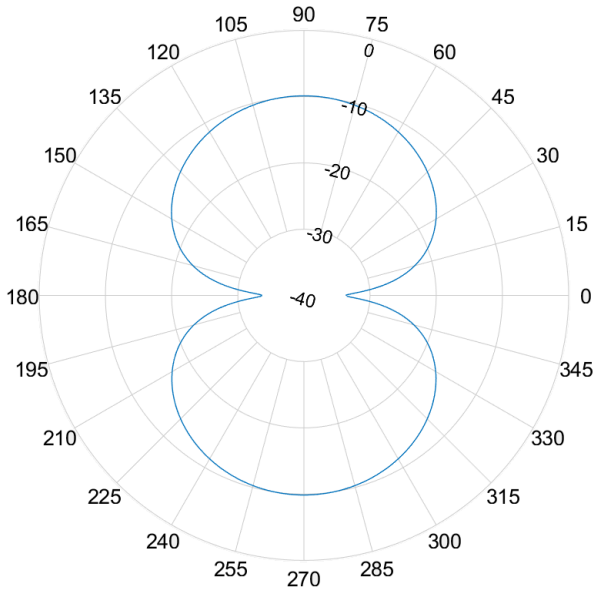

FIGURE 67 – Diagramme horizontal en polaire de l'antenne Yagi-Uda

Il est aussi possible d'utiliser l'équation de Friss pour déterminer le rayon d'action du leurre, c'est à dire déterminer pour chaque angle autour du leurre la distance telle que la puissance reçue soit égale à une certaine valeur. Par exemple, pour une puissance reçue de $-130\ dBm$ et une puissance de transmission de $-55\ dBm$, on obtient les rayons d'actions représentés sur la Figure 68 pour l'antenne Cassegrain et la Figure 69 pour l'antenne Yagi-Uda. Tracer ce rayon d'action est très utile pour contrôler le déroulé des simulations de notre stratégie.

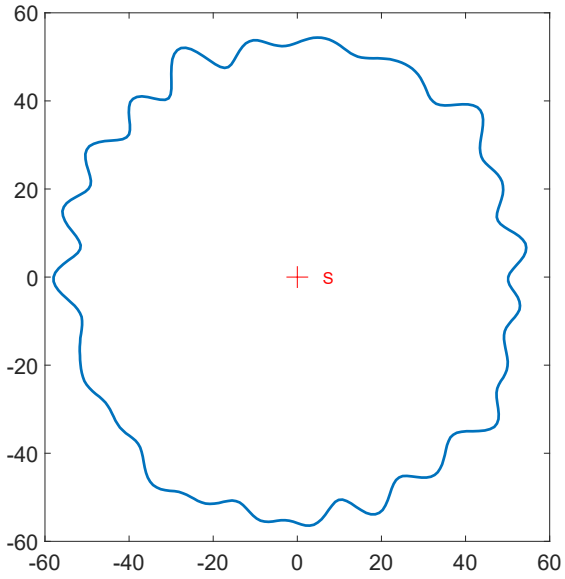

FIGURE 68 – Rayon d'action en m de l'antenne Cassegrain pour une réception de -130 dBm

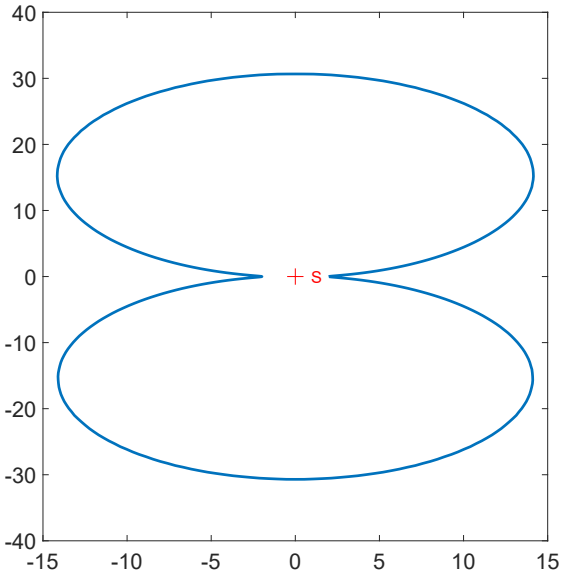

FIGURE 69 – Rayon d'action en m de l'antenne Yagi-Uda pour une réception de -130 dBm

Ces blocs importants étant maintenant en place, on peut se lancer dans des simulations de quelques scénarios afin de tester la validité de notre stratégie d'estimation de la direction du leurre GNSS.

III.4 Etude de quelques scénarios par simulation

Le code de simulation nous permet de simuler une formation de drones se déplaçant en direction d'un leurre GNSS immobile. Comme précisé précédemment, deux cas de figure sont envisagés :

— le leurre utilise une antenne Cassegrain et donc le diagramme de rayonnement utilisé en simulation est celui présenté Figure 66 et a l'allure d'un cercle présentant des lobes irréguliers,

— le leurre utilise une antenne Yagi-Uda et donc le diagramme de rayonnement utilisé en simulation est celui présenté Figure 67 et a l'allure d'un 8 formé de deux lobes se joignant sur une partie centrale présentant une inflexion.

L'objectif est de vérifier si la zone déterminée par le protocole de déplacement correspond bien à la direction du leurre lorsque la formation entre dans son champ d'action.

III.4.1 Protocole de test

A partir de ces deux diagramme d'antennes, il est possible de s'intéresser à plusieurs zones particulières des diagrammes où le ou les premiers drones de la formation vont se faire leurrer. Sur ces zones spécifiques on s'intéressera aussi à l'influence de quelques paramètres sur l'estimation de la direction du leurre et la précision de la zone délimitée par le protocole de déplacement. Ces paramètres sont :

— la distance entre les drones de la formation d,

— le nombre de drones dans la formation.

III.4.1.1 Définition des zones d'intérêts pour les simulations

Les zones d'intérêts sélectionnés pour les simulations sont présentés Figure 70 pour l'antenne Cassegrain et Figure 71 pour l'antenne Yagi-Uda. Elles sont représentées par les carrés rouges et numérotées, les flèches rouges indiquent la direction d'arrivée de la formation de drones.

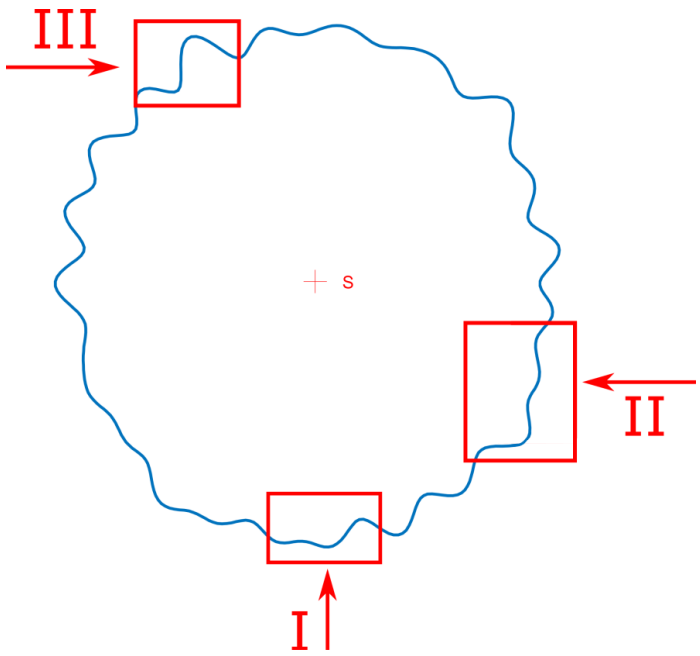

FIGURE 70 – Zones d'intérêt sélectionnées pour l'antenne Cassegrain

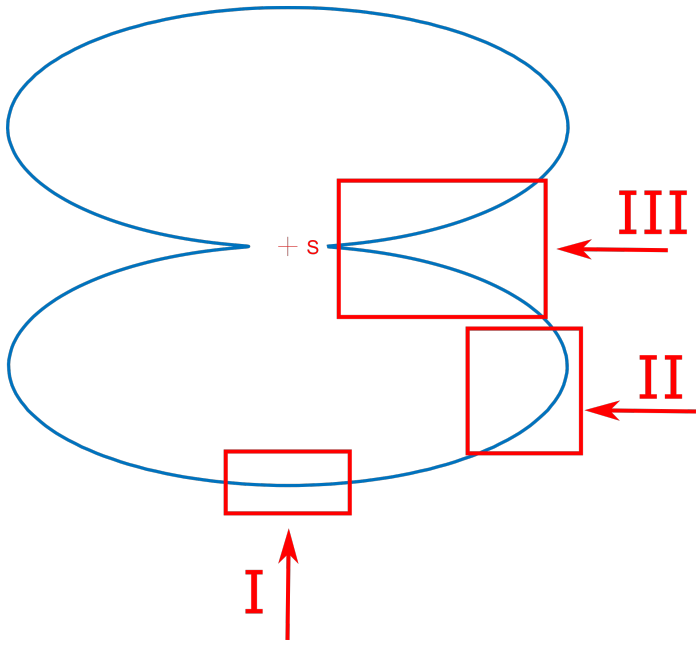

FIGURE 71 – Zones d'intérêt sélectionnées pour l'antenne Yagi-Uda

Les zones I pour les deux antennes n'ont pas vraiment de particularités et servent de référence pour tester le protocole de déplacement dans un cas simple. La zones II et III ont été sélectionnées car elles présentent

certaines particularités susceptibles de mettre en échec le protocole de déplacement des drones. La zone II de l'antenne Cassegrain présente de faibles lobes, le rayon d'action est presque "plat" sur la zone avant de présenter un "creux", et la direction d'arrivée de la formation ne pointe pas vers le leurre. De même la zone II de l'antenne Yagi-Uda couvre l'extrémité du lobe inférieur du rayon d'action et la direction d'arrivée de la formation ne pointe pas vers le leurre. La zone III de l'antenne Cassegrain présente un lobe relativement important proche de lobes "secondaires" successifs. La zone III de l'antenne Yagi-Uda correspond à la jointure des deux lobes du diagrammes de rayonnement et peut potentiellement mener à une mauvaise estimation.

III.4.1.2 Déroulement des simulations

Pour tous les paramètres, la simulation suit le déroulé des étapes décrites plus tôt dans la partie III.2.2. La formation part d'une position éloignée d'un maximum de 120 m du leurre. Elle se déplace en mouvement linéaire vers la zone d'action du leurre, suivant les directions décrites Figures 70 et 71, jusqu'à ce qu'au moins un drone soit leurré. A ce moment là, les drones se mettent à tourner autour du drone de contrôle (rotation dans le sens trigonométrique) jusqu'à un changement de statut d'un drone de la formation. La position du drone qui a changé d'état est conservée et son angle dans le repère local est calculé. La rotation des drones continue dans le même sens jusqu'à un nouveau changement de statut d'un drone de la formation.

Pour les cas de notre étude, la vitesse linéaire des drones est fixée à 15 m/s (ce qui est à peu près équivalent à la vitesse maximale d'un drone de la marque Parrot [32]) tandis que la vitesse angulaire est de $\frac{\pi}{20}$ rad/s. Pour les paramètres testés, les valeurs choisies sont les suivantes :

— nombre de drones N_d : 3, 4 et 5 drones (avec comme drone de contrôle respectivement 3, 4 et 5),

— distance entre les drones d : 10, 20 et 30 mètres.

Pour valider le succès du protocole de déplacement, on calcul θ_L qui est l'angle entre le drone de contrôle à l'instant où on commence les rotations et le leurre. Puis, une fois la zone angulaire obtenue par les rotations, notée E_L, on regarde si l'angle entre le drone de contrôle et le leurre est bien dans la zone angulaire.

On s'intéresse aussi à l'amplitude de la zone angulaire ΔE_L qui sert d'indicateur de la précision du protocole de déplacement. On regarde aussi le temps, en nombre d'itération de la boucle et noté t_p, que va mettre la formation pour estimer la zone angulaire du leurre (c'est à dire entre le début des rotations et l'obtention du dernier angle d'estimation de la zone).

III.4.2 Résultats

Le protocole de déplacement a été testé avec toutes les combinaisons de paramètres décrits précédemment, ce qui représente 54 cas différents. Pour illustrer le fonctionnement du code de simulation, prenons l'exemple du cas avec une formation de cinq drones, avec la distance $d = 20$ m avec une arrivée dans la zone II d'un leurre avec une antenne Yagi-Uda.

La Figure 72 montre l'étape 1 du protocole de déplacement. La formation est initialisée à une centaine de mètres du leurre. Les positions initiales des drones sont représentées par des croix bleues. Le drone de contrôle est ici le drone 5 qui se trouve au centre de la formation. La formation déplace alors sur l'axe Est dans la direction représentée par la flèche verte, la formation après déplacement est représentée par des croix vertes. Lorsqu'un drone entre dans le rayon d'action du leurre, représenté par une croix rouge pour le leurre et les lignes bleues pour le rayon d'action, la formation stoppe son mouvement linéaire. Le drone leurré est ici le drone 2.

Un drone étant leurré, on passe alors à l'étape 2 représentée Figure 73. Les drones de la formation se mettent en rotation autour du drone de contrôle dans le sens trigonométrique jusqu'à ce que le statut d'un drone de la formation change. Ici c'est le drone 3 qui change de statut lorsqu'il entre dans le rayon d'action du leurre. Sa position est enregistrée et on en déduit une première borne de la zone angulaire où se trouve le leurre. Cette première borne est représentée en pointillés jaunes sur la Figure 73. Dans cette exemple l'angle

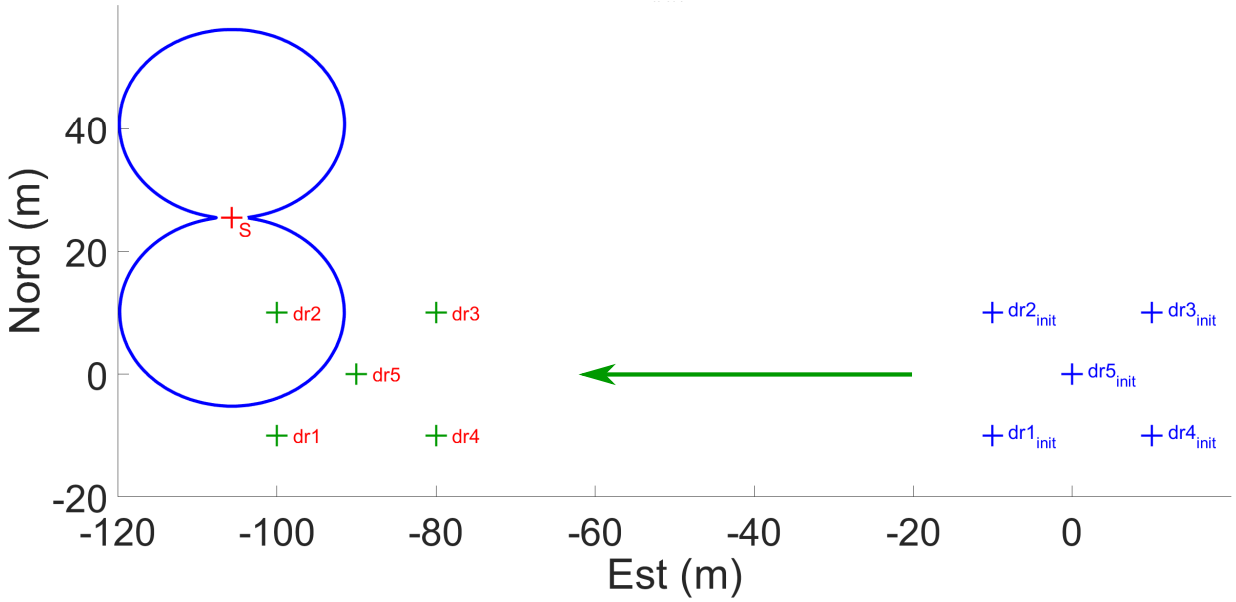

FIGURE 72 – Etape 1 du protocole de déplacement sur le simulateur

correspondant est de 108°.

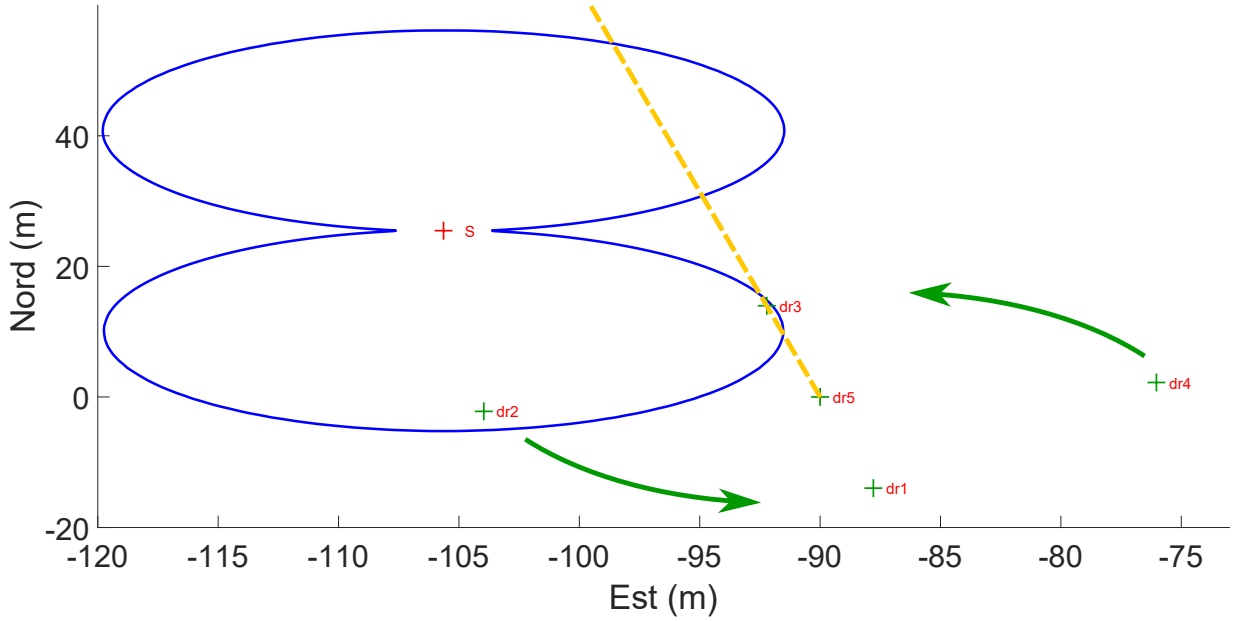

FIGURE 73 – Etape 2 du protocole de déplacement sur le simulateur

Une fois cette borne acquise, les rotations reprennent dans le même sens jusqu'à ce qu'un deuxième drone change de statut, ici il s'agit du drone 2 qui sort du rayon d'action du leurre. On enregistre sa position et détermine la deuxième borne de la zone angulaire qui est également représentée en pointillées jaunes sur la Figure 74. Ici cela correspond à un angle de 225°, on a donc $E_L = [108°, 225°]$. L'angle du leurre dans le repère local centré sur le drone 5 à cet instant là est $\theta_L = 154.45°$. On a donc $\theta_L \in E_L$, on considère donc que l'estimation est un succès.

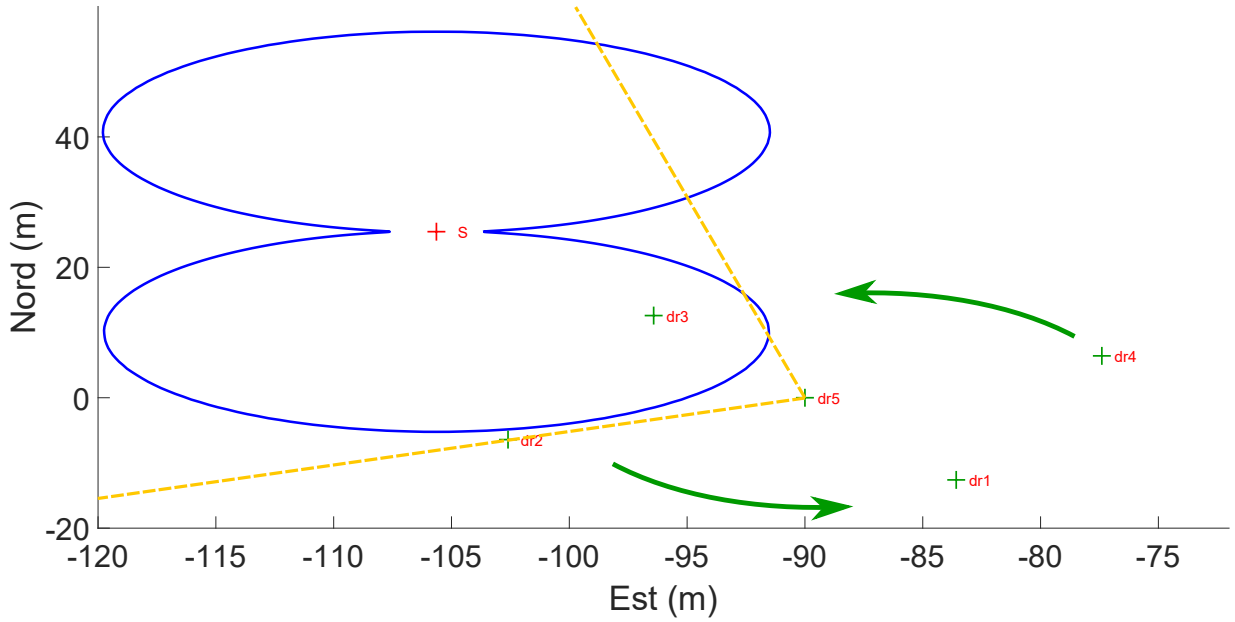

FIGURE 74 – Etapes 3 et 4 du protocole de déplacement sur le simulateur

Ce processus a été lancé sur les 54 combinaisons de paramètres possibles. Les mesures de θ_L, E_L, ΔE_L, et t_p sont regroupés dans le Tableau 6 pour l'antenne Cassegrain et le Tableau 7 pour l'antenne Yagi-Uda. Les zones colorées en jaune sur les deux tableaux indiquent les cas où le protocole de déplacement a échoué, c'est à dire les cas où $\theta_L \notin E_L$.

Sur les 54 cas simulés, on dénombre 16 cas d'échec, soit environ 30% d'échec. Plusieurs raisons peuvent expliquer ces quelques échecs.

Une bonne partie de ces échecs sont des cas où deux drones sont leurrés à la fin de l'étape 1 du protocole. Etant donné que le sens de rotation est conservé entre les étapes 2 et 3 du protocole, il y a de forte chance qu'à l'étape 2 un des deux drones leurrés sorte du champ d'action du leurre tandis qu'à l'étape 3 le deuxième drone leurré sorte en donnant le même angle. C'est une situation qui s'est le plus produite lors des simulations en zone I sur les deux types d'antenne. Une solution envisageable pour contourner ce problème serait d'utiliser plus de drones dans la formation.

Ces drones supplémentaires permettent un changement de statut de la formation ayant lieu avant que le deuxième drone leurré au début des rotations n'ait le temps de sortir suivant la trajectoire du premier. Cela se remarque déjà avec les simulations de formation à cinq drones qui n'ont pas eu d'échec sur les zones I. Une alternative possible si on ne souhaite pas ajouter de drones serait d'inverser le sens de rotation à l'étape 3.

Tableau 6. Récapitulatif des simulations sur l'antenne Cassegrain

Zone		I			II		
Distance d (m)		10	20	30	10	20	30
N_d	Mesure						
3	θ_L (°)	90	90	90	154.45	154.45	154.45
	E_L (°)	[156, 159]	[156, 159]	[129, 132]	[114, 237]	[96, 219]	[96, 228]
	ΔE_L (°)	3	3	3	123	123	132
	t_p (itération)	11	11	8	13	11	12
4	θ_L (°)	90	90	90	154.45	159.54	162.99
	E_L (°)	[153, 153]	[99, 81]	[144, 135]	[117, 234]	[207, 162]	[198, 135]
	ΔE_L (°)	0	18	9	117	45	63
	t_p (itération)	7	29	5	6	8	40
5	θ_L (°)	90	90	90	154.45	154.45	154.45
	E_L (°)	[144, 45]	[153, 45]	[162, 27]	[216, 126]	[108, 225]	[99, 216]
	ΔE_L (°)	99	108	135	90	117	117
	t_p (itération)	10	10	8	9	10	9

Zone		III		
d (m)		10	20	30
N_d	Mesure			
3	θ_L (°)	274	274	274
	E_L (°)	[252, 312]	[294, 252]	[285, 252]
	ΔE_L (°)	60	42	33
	t_p (itération)	8	8	8
4	θ_L (°)	274	274	274
	E_L (°)	[234, 288]	[234, 288]	[243, 288]
	ΔE_L (°)	54	54	45
	t_p (itération)	2	2	2
5	θ_L (°)	302.72	302.72	312
	E_L (°)	[0, 315]	[252, 351]	[0, 279]
	ΔE_L (°)	315	99	279
	t_p (itération)	10	4	6

D'autres cas d'échec observés sont dus à des particularités géométriques des rayons d'actions du leurre. C'est notamment le cas avec l'antenne Yagi-Uda où la formation à quatre drones semble être la plus sensible à ce type de problème. Les zones problématique sont la zone II et la zone III qui correspondent respectivement à l'extrémité du lobe inférieur et la zone d'inflexion où se joignent les deux lobes du "8". La formation à quatre drones semble être la plus sensible à ce type de problème.

Tableau 7. Récapitulatif des simulations sur l'antenne Yagi-Uda

Zone		I			II		
Distance d (m)		10	20	30	10	20	30
N_d	Mesure						
3	θ_L (°)	90	90	90	121.56	125.56	172.12
	E_L (°)	[156, 159]	[138, 141]	[0, 354]	[105, 201]	[105, 201]	[174, 114]
	ΔE_L (°)	3	3	354	96	96	60
	t_p (itération)	11	9	6	9	9	6
4	θ_L (°)	90	90	90	121.56	140.27	140.27
	E_L (°)	[153, 153]	[117, 72]	[117, 72]	[108, 207]	[198, 153]	[198, 180]
	ΔE_L (°)	0	45	45	99	45	18
	t_p (itération)	7	28	28	3	7	5
5	θ_L (°)	90	90	90	121.56	121.56	121.56
	E_L (°)	[162, 36]	[153, 36]	[117, 189]	[198, 108]	[99, 207]	[198, 108]
	ΔE_L (°)	126	117	72	90	108	90
	t_p (itération)	9	9	6	7	8	7

Zone		III		
d (m)		10	20	30
N_d	Mesure			
3	θ_L (°)	168.35	168.35	168.35
	E_L (°)	[156, 174]	[96, 264]	[156, 174]
	ΔE_L (°)	18	168	18
	t_p (itération)	6	16	6
4	θ_L (°)	168.35	173.99	173.99
	E_L (°)	[117, 153]	[189, 216]	[171, 126]
	ΔE_L (°)	36	27	45
	t_p (itération)	7	4	4
5	θ_L (°)	168.35	168.35	168.35
	E_L (°)	[252, 189]	[270, 99]	[261, 171]
	ΔE_L (°)	63	171	90
	t_p (itération)	6	6	4

A titre d'exemple on peut regarder le cas d'une formation à 4 drones distants de 10 m arrivant sur la zone III de l'antenne Yagi-Uda. Les Figures 75 à 77 montrent les étapes du protocole de déplacements dans ce cas.

A l'étape 1 le drone 2 est leurré. Dans une formation à 4 drones le drone 4 est le drone de contrôle, les drones tournent donc autour de ce dernier (Figure 75).

A l'étape 2, le drone 1 change de statut en entrant dans le rayon d'action du leurre au niveau du haut du lobe inférieur. On enregistre donc sa position et l'angle correspondant (Figure 76).

A l'étape 3, le drone 1 ressort du rayon d'action du leurre par l'extrémité du lobe inférieur. La zone angulaire déduite ne contient pas le leurre, on a donc un échec (Figure 77).

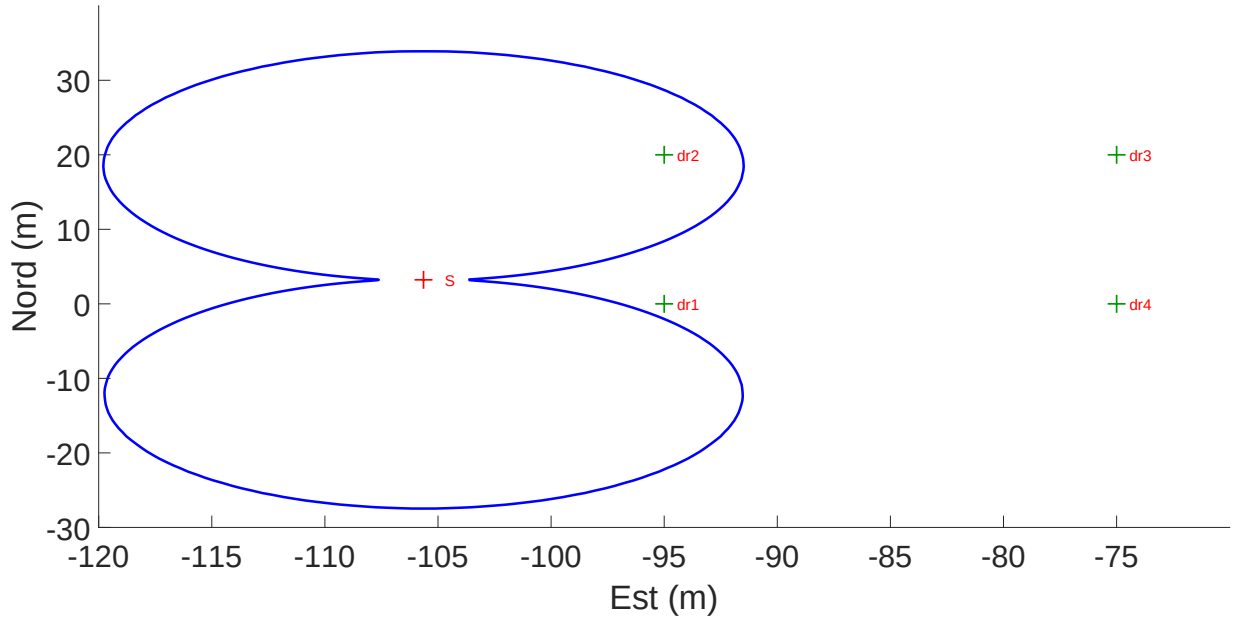

FIGURE 75 – Etape 1 du protocole de déplacement sur un cas d'échec

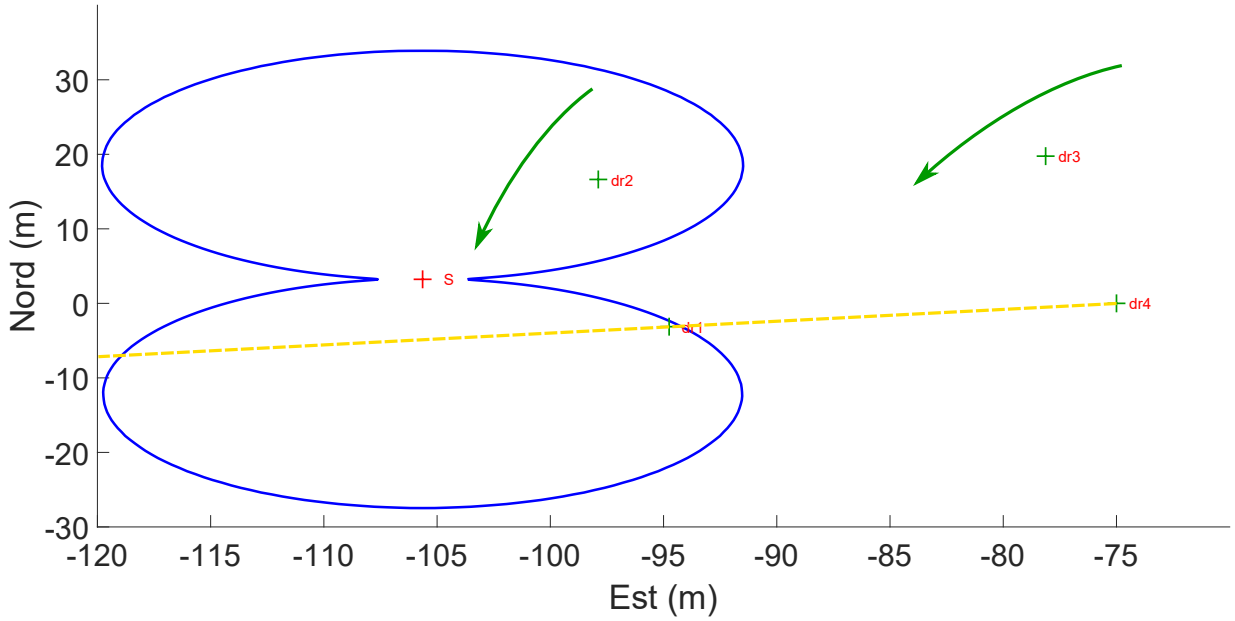

FIGURE 76 – Etape 2 du protocole de déplacement sur un cas d'échec

Contrairement à la formation à quatre drones, les formations à trois et cinq drones s'en sortent mieux. Mise à part le nombre de drones, la principale différence entre la formation à quatre drones et les formations à trois et cinq drones est la distance entre le drone de contrôle et les autres drones de la formation.

En effet, sur les formations à trois et cinq drones le drone de contrôle est équidistant avec chacun des drones de la formation, ce qui n'est pas le cas dans la formation à quatre drones. Utiliser une autre forme géométrique pour la formation à quatre drones peut être une solution possible, avec par exemple une forme en triangle équilatéral avec le drone de contrôle situé au centre du triangle, comme illustré sur la Figure 78.

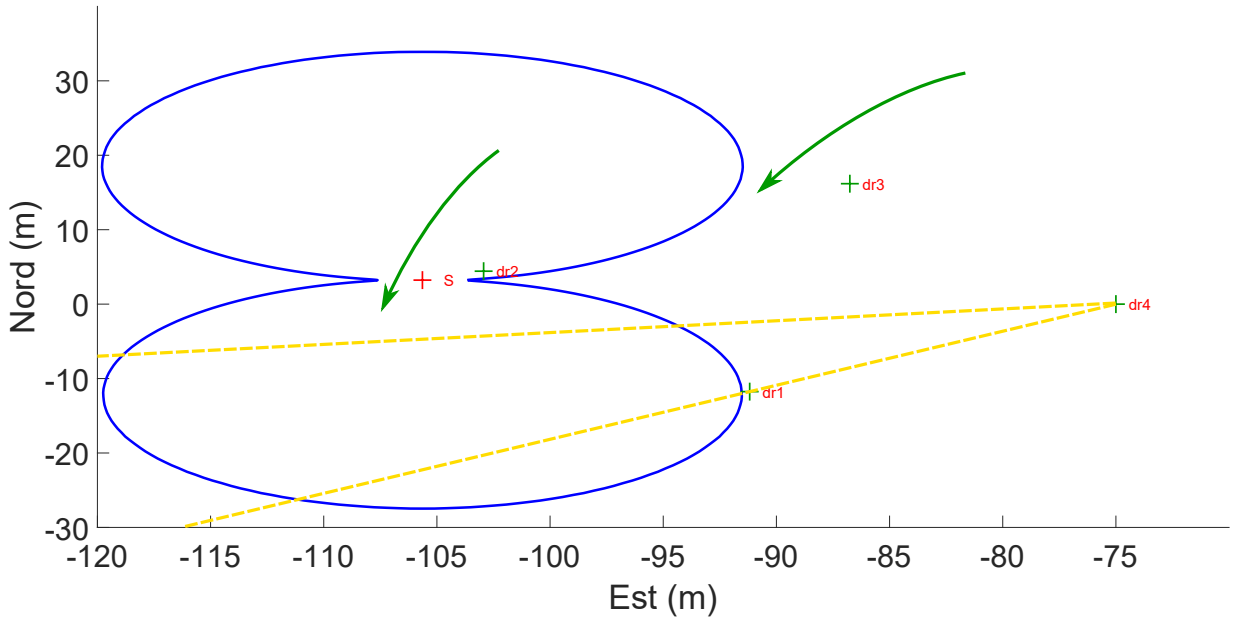

FIGURE 77 – Etapes 3 et 4 du protocole de déplacement sur un cas d'échec

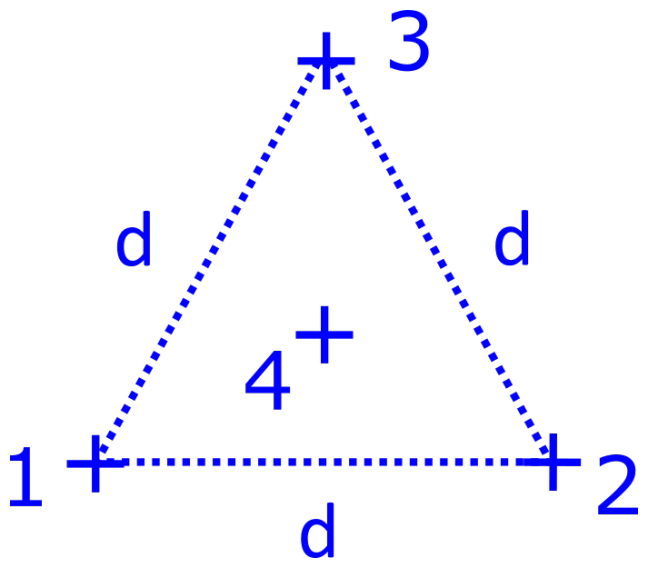

FIGURE 78 – Autre formation à 4 drones possible

Par ailleurs, la distance d entre les drones semble être un paramètre optimisable. Une grande distance peut faciliter l'estimation de la zone dans certains cas mais peut aussi conduire à une mauvaise estimation.

III.4.3 Bilan

Il apparait donc que cette base de stratégie de défense anti-leurrage présente un certain potentiel. Elle reste cependant, dans son état actuel, très perfectible. On peut néanmoins déjà envisager quelques améliorations.

Mettre en place la possibilité de changer le sens de rotation des drones selon le nombre de drones leurrés initialement devrait corriger quelques cas d'échecs rencontrés dans nos simulations. Utiliser des formations suivant une forme géométrique "centrée", c'est à dire où le drone de contrôle et les autres drones sont équi-

distants, est également une amélioration possible.

Il est donc nécessaire de faire davantage de simulations sur cette stratégie avec d'autres diagrammes de rayonnement plus complexes afin d'améliorer le protocole de déplacement. On peut également envisager de s'aider des variations de puissance de signaux reçus pour déterminer si les drones se rapprochent du leurre ou non au cours de leurs mouvements mais cela suppose que la formation est suffisamment proche du leurre pour que les variations de puissance ne soient pas trop faibles.

Par ailleurs, les tests effectués jusqu'à maintenant se limitent à un problème en deux dimensions. Il conviendra donc d'étendre le protocole à un processus en trois dimensions en ajoutant par exemple des rotations dans le plan vertical pour délimiter le rayon d'action du leurre dans ce plan.

Cependant tout ceci est à nuancer avec deux facteurs importants dans un cas pratique, à savoir les vitesses des déplacements des drones (linéaire et angulaire) et surtout la rapidité de détection du leurrage par les drones de la formation. Le protocole de déplacement fonctionnant de manière séquentielle (détection/contrôle de statut $\leftrightarrow$ déplacement), ces deux facteurs vont jouer un rôle important sur la rapidité de cette stratégie à estimer la zone angulaire où le leurre est localisé.

Chapitre IV

Bilan des travaux de la thèse

Après avoir réalisé un état de l'art sur le leurrage GNSS au chapitre I, l'étude menée lors de cette thèse s'est focalisée sur deux aspects de la défense anti-leurrage.

Le premier est la détection d'interférences de leurrage. Celui-ci est traité dans le chapitre II avec l'étude des effets du leurrage sur le biais d'horloge d'un récepteur GNSS. Le second est la localisation du leurre avec pour objectif sa neutralisation. Cet aspect est traité dans le chapitre III avec l'étude d'une stratégie de localisation du leurre par le biais d'une formation de drones.

IV.1 Travaux sur l'horloge des récepteurs

IV.1.1 Résumé des résultats obtenus et comparaisons avec d'autres méthodes

L'étude des effets du leurrage sur le biais d'horloge a commencé par une modélisation numérique sur Matlab.

Ce modèle permet de reproduire un attaque de leurrage plutôt simple sur un récepteur fixe dans un cas idéal et purement théorique où le leurre utilise la même horloge que celle de la constellation GNSS.

Cette modélisation a montré qu'une attaque de leurrage provoque des sauts sur le biais d'horloge du récepteur, ce qui se répercute sur sa dérive. L'amplitude de ces sauts peut être minimisée par le leurre en se rapprochant le plus possible de sa cible.

L'attaque de leurrage a ensuite été reproduite sur deux récepteurs commerciaux utilisant de vrais signaux GPS à l'aide de simulateurs de signaux, d'abord dans le cas idéal décrit plus tôt et utilisé sur le modèle, puis dans un cas plus réaliste où le leurre utilise sa propre horloge.

Sur l'ensemble des différents scénarios testés, des sauts de biais d'horloge ont été observés lorsque le récepteur passe de la constellation satellite à la constellation du leurre, ce qui valide les résultats obtenus avec le modèle. Ces sauts de biais ont pu être observés même dans un scénario "discret" où le leurre utilise de faibles puissances.

Cependant la dérive du biais ne présente pas de pic dans le cas idéal à une horloge (le leurre et la constellation GNSS partagent la même horloge), mais dans le cas, plus réalise, à deux horloges (le leurre a sa propre horloge), la dérive présente également un saut (au lieu d'un "simple" pic). On a également constaté une différence importante sur l'amplitude des sauts de biais entre le cas idéal et le cas plus réaliste.

Différents tests ont montré que cette différence vient principalement de l'utilisation de deux horloges différentes pour générer les deux constellations. Ces tests ont également mis en évidence que l'amplitude des sauts de biais semble soumise à un phénomène aléatoire. On en déduit que l'amplitude des sauts de biais d'horloge lors d'une attaque de leurrage ne sont pas prévisibles. Dans le cas d'un récepteur en mouvement, des sauts

de biais d'horloge ont également pu être observés.

Cette approche de détection basée sur le contrôle du biais d'horloge présente quelques avantages par rapports aux autres approches de la littérature.

Un premier avantage est qu'il s'agit d'une approche peu coûteuse. En effet, le biais d'horloge est une donnée directement accessible sur le récepteur, il n'est pas nécessaire d'ajouter de composants ou d'allouer de la puissance de calcul supplémentaire pour récupérer cette information. On s'affranchit donc des opérations de traitement du signal utilisées dans les méthodes de détection de la catégorie éponyme comme dans [1].

Par ailleurs, les essais de leurrage menés dans notre étude montrent qu'il est possible de détecter un leurrage avec le biais d'horloge même lorsque le leurre utilise des signaux de faible puissance ou de trop forte puissance. Ceci n'est pas le cas de la méthode du contrôle du gain de l'AGC [14] qui échoue face à des signaux de faible puissance ou des stratégies basées sur le SQM qui faiblissent lorsque les signaux du leurre sont trop fort [17].

Par rapport à d'autres méthodes de détection de la catégorie du contrôle de dérives comme celle de Marnach et al dans [4], notre étude confirme les observations faites par Marnach et al sur les attaques de meaconing et les étend aux attaques de leurrage. De plus, Marnach et al. n'utilisent pas directement le biais d'horloge mais l'erreur du biais, qui est calculée à partir d'une régression linéaire sur une fenêtre de données.

Cependant, avec le biais d'horloge, le leurre peut en théorie minimiser son impact en étant très proche de sa cible. De plus, si un récepteur s'accroche directement sur les signaux d'un leurre à son initialisation, le biais d'horloge ne présentera pas de sauts. Par ailleurs, l'approche étudiée ici ne semble pas avoir de capacité de classification des signaux reçus que peuvent avoir les méthodes utilisant plusieurs récepteurs, comme dans [1] ou [3] par exemple.

IV.1.2 Perspectives

Les résultats des expérimentations réalisées dans cette partie ont mis en évidence que le biais d'horloge d'un récepteur GNNS peut être exploité dans une stratégie de détection de leurrage.

Même si les tests de leurrage ont été réalisés sur deux modèles différents de récepteur, ces derniers sont issus du même constructeur. On peut donc se demander si utiliser d'autres récepteurs, ayant des composants de différentes qualités aura un impact sur les phénomènes observés avec les récepteurs u-blox.

Par la suite on pourra envisager le développement d'un algorithme de détection basé sur le contrôle du biais d'horloge et de sa dérive. On pourra ensuite implémenter cet algorithme sur un drone volant et le tester en conditions réelles. Une étude préalable sur le choix du seuil de détection devra également être menée.

IV.2 Travaux sur les drones en formation

IV.2.1 Résumé des résultats obtenus et comparaison avec d'autres méthodes

L'état de l'art des méthodes de défense anti-leurrage utilisant un réseau d'antennes ou de récepteurs montre qu'en utilisant ce type de structure il est possible non seulement faire de la détection de leurrage, mais également de la classification de signaux reçus par les récepteurs.

L'approche proposée dans cette étude est composée de trois éléments principaux : des drones répartis sur une formation géométrique fixe et pouvant échanger des informations, une capacité de détecter une attaque de leurrage avec une méthode au choix présente sur chaque drone de la formation (dans notre cas on suppose utiliser une détection basée sur le contrôle du biais d'horloge), et un protocole de déplacement géré par un drone de contrôle pour estimer la direction du leurre. A ceci s'ajoute l'hypothèse, qui peut être plus ou moins forte selon les situations, qu'au moins un des drones de la formation n'est pas touché par des interférences

de leurrage. L'étude menée sur cette approche s'est focalisée sur le protocole de déplacement.

On attribue un statut leurré ou non leurré à tous les drones de la formation. Le principe du protocole de déplacement est de mettre en rotation les drones de la formation autour du drone de contrôle dès qu'un drone change de statut. En contrôlant le statut des drones lors des phases de rotation, on délimite une zone angulaire dans le plan horizontal autour du drone de contrôle dans laquelle le leurre est supposé être localisé.

Des simulations ont été réalisées afin de tester cette base de stratégie contre deux types d'antennes classiques, la Yagi-Uda et la Cassegrain. Différents scénarios ont été envisagés pour ces simulations afin de tester l'influence du nombre de drones dans la formation, et la distances entre chaque drone, sur les capacités d'estimation de la direction du leurre. Avec ces scénarios, nous avons également testé le protocole de déplacement contre des zones particulières des diagrammes de rayonnement des antennes Yagi-Uda et Crassegrain. Ces zones ont été choisies car pour une grande part, leur forme peut potentiellement mettre en difficulté le protocole et aboutir sur une mauvaise estimation. Les simulations sur ces cas pathologiques ont donné des résultats plutôt encourageants, avec 70% des cas testés aboutissant à une estimation correcte.

Une stratégie de défense anti-leurrage comme celle-ci se distingue des autres études présentes dans la littérature sur plusieurs points. L'approche que nous proposons ne requiert pas de modification sur les étages de fonctionnements des récepteurs GNSS, ce qui répond aux demandes initiales. Ce qui n'est pas le cas de la plupart des méthodes post-désétalement, comme celle de Meurer et al. dans [36] par exemple, qui nécessitent de modifier les unités d'acquisition et de suivi des récepteurs utilisés dans le réseau, ce qui va à l'encontre d'un objectif de diffusion massive.

Comparée à des méthodes utilisant des centrales de vérification d'authenticité (CAV) comme celles présentées dans [42], notre approche reprend l'idée d'utiliser un élément jouant le rôle de gestionnaire du réseau mais dans notre cas n'importe quel élément du réseau peut jouer ce rôle. De plus le rôle de gestionnaire, assuré par le drone de contrôle, peut être transféré à un autre élément du réseau s'il est mis en défaut. Par ailleurs, les CAV ont généralement une grande quantité de données à traiter, ce qui n'est, dans l'état actuel, pas le cas du drone de contrôle de notre formation qui n'utilise que le statut des drones de la formation et les positions relatives des autres drones de la formation. Le point commun entre notre approche et les approches basées sur les réseaux de récepteurs est qu'il est nécessaire d'assurer un bon canal de transmission d'informations entre les membres du réseau.

IV.2.2 Perspectives

Le protocole de déplacement, tel que présenté dans cette étude, n'en est encore qu'à ses balbutiements. On peut déjà dégager quelques améliorations permettant de corriger quelques scénarios d'échec observés lors des simulations. Par exemple, dans les cas où deux drones de la formation sont touchés avant le début de la phase de rotation, introduire une inversion du sens de rotation après le premier changement de statut permet de corriger quelques échecs rencontrés. On pourra également penser à rallonger le protocole de déplacement en utilisant une succession de mouvements de rotation et de mouvements linéaires pour délimiter plusieurs zones suspectes.

De plus, il est nécessaire d'étudier l'efficacité de l'estimation de la zone du leurre sur d'autres types d'antennes dont les diagrammes de rayonnements présentent des caractéristiques plus particulières (lobe principal très large et non centré sur le leurre par exemple).

Par ailleurs, l'approche proposée est basée sur un raisonnement en deux dimensions. Il convient donc de transposer et d'enrichir le protocole de déplacement dans une réflexion en trois dimensions de la problématique.

En plus de l'étude des capacités de localisation de cette approche, il sera nécessaire d'étudier ses performances en terme de temps d'exécution et précision de la zone angulaire estimée. Ceci peut se faire en étudiant l'impact de la rapidité de détection de leurrage et des vitesses de déplacement des drones.

Conclusion

Au cours de cette thèse, nous avons proposé, à partir de l'état de l'art, une approche de détection de leurrage d'un récepteur GNSS basée sur l'analyse du comportement de son horloge. Des simulations et des études expérimentales ont montré qu'une attaque de leurrage provoque des sauts identifiables du biais de l'horloge du récepteur et dans certains cas également de la dérive du biais de cette dernière.

Partant de ce constat, on pourra envisager le développement d'un algorithme de détection de leurrage utilisant le biais d'horloge et la dérive du biais de cette dernière comme métrique de détection. Après une étude sur le choix des seuils de détection, cet algorithme pourra être implémenté sur un drone volant afin de le tester en conditions réelles.

Il pourra également être envisagé d'étudier la possibilité de mettre en place une méthode de détection de leurrage de la catégorie des techniques mixtes. Une piste possible consisterait à fusionner les données GNSS avec celles issues des commandes moteurs du drone, qui fournissent une indication sur les mouvements réels du drone que l'on peut comparer au calcul de position obtenu.

Afin d'aller plus loin que la "simple" détection de leurrage, une approche centrée sur l'utilisation de drones disposés selon une formation géométrique fixe a été proposée afin de réaliser une estimation de la direction du leurre. Une première base de stratégie utilisant un protocole de déplacement associé aux capacités de détection du leurrage des drones, a été proposée et testée par le biais de simulations sur quelques cas d'études. Cette stratégie semble prometteuse mais nécessite encore quelques points à étudier afin de l'améliorer.

Tout d'abord il conviendra d'étudier l'efficacité du protocole de déplacement face à d'autres types d'antennes dont le diagramme de rayonnement présente des particularités plus prononcées que l'antenne Yagi-Uda ou Cassegrain. Par la suite on pourra étudier la possibilité de compléter le protocole de déplacement en modifiant les rotations selon le nombre de drones touchés ou en combinant mouvement linéaire et mouvement angulaire.

Il conviendra également d'étendre cette stratégie en trois dimensions, et d'étudier l'impact des vitesses de déplacement sur les performances de cette approche.

Par ailleurs, toujours dans une optique de localisation du leurre, il pourra être envisagé d'essayer de déterminer la distance du drone à partir d'une formation de drone.

Annexe A

Présentation du matériel utilisé

Le matériel utilisé pour réaliser nos essais de leurrage est le suivant :

- des récepteurs GNSS u-blox EVK-6T (nommé u-blox 6 par la suite) et u-blox EVK-M8T (nommé u-blox 8 par la suite),
- un simulateur de signaux GPS Spirent GSS6560,
- un simulateur de signaux GNSS (GPS et GLONASS) Labsat 2.

A.1 Récepteurs u-blox

Les récepteurs utilisés dans nos essais de leurrage sont des récepteurs GNSS du fabricant suisse U-blox. La Figure 79 présente les u-blox 6 et 8, respectivement à gauche et à droite.

FIGURE 79 – Récepteurs u-blox

Ces modèles de récepteur présentent l'avantage de disposer d'un port USB. Ceci permet à un utilisateur de pouvoir se connecter directement avec le récepteur par le biais d'un ordinateur afin de récupérer différentes données fournies par le récepteur. Les récepteurs u-blox sont donc livrés avec un logiciel appelé *u-center* dont l'interface permet de visualiser en temps réel les données reçues par le récepteur. Parmi ces données on peut citer notamment les rapports C/No de chaque canal GNSS donnés en $dBHz$, le temps GNSS, les coordonnées GPS calculées par le récepteur, le biais d'horloge, la dérive du biais, les pseudo-distances de chaque satellite, etc. La plupart des données peuvent être enregistrées dans un tableau qui peut être copié et exporté sur Excel. Il est également possible d'enregistrer dans un fichier log l'ensemble des données reçues durant une acquisition. Ce fichier log peut alors être lu par u-center pour rejouer l'acquisition de données en direct. Par ailleurs, le logiciel u-center permet de "remettre à zéro" le récepteur selon trois états différents :

— *cold start* : le récepteur n'a gardé aucune donnée en mémoire,

— *warm start* : le récepteur n'a gardé en mémoire que les almanachs, la dernière position connue et le temps UTC,

— *hot start* : similaire au *warm start* mais avec l'addition des éphémérides des satellites.

La Figure 80 présente l'interface du logiciel u-center avec la configuration utilisée lors de nos essais de leurrage GNSS.

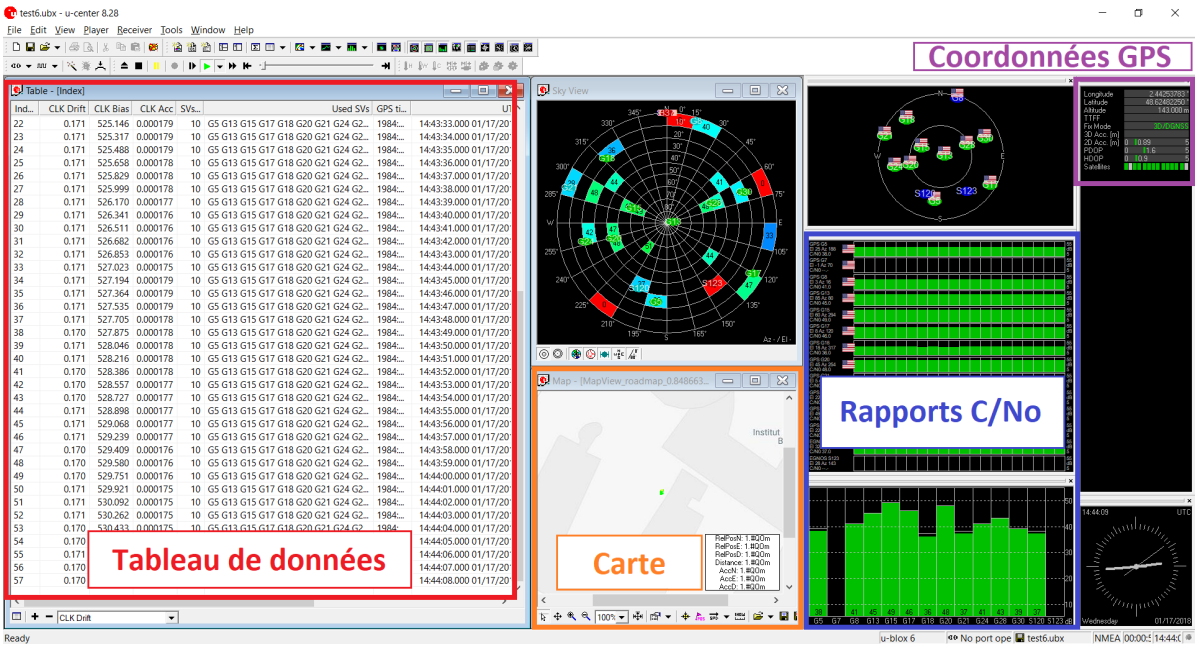

FIGURE 80 – Logiciel u-center

Le cadre rouge indique le tableau de données. Par défaut ce tableau est vide et l'utilisateur choisit quelles données il souhaite afficher. Les coordonnées GPS du récepteur sont affichées au niveau du cadre violet. La position calculée peut être affichée sur une carte, représentée ici dans le cadre orange. Le cadre bleu indique le niveau des rapports C/No de chaque satellite à l'instant t (dans la partie inférieure) mais aussi un historique de ces rapports sur une fenêtre de temps. Cette représentation permet également de connaître quelles satellites le récepteur utilise pour le calcul de position via un code couleur :

— canal vert : le satellite est utilisé pour le calcul,

— canal bleu : le satellite est vu par le récepteur mais non utilisé dans le calcul.

A.2 Simulateur Spirent

Le Spirent GSS6560 est un simulateur de signaux GPS. Avec cet appareil, il est possible de complètement simuler une constellation GPS et de diffuser ses signaux à travers 12 canaux de transmissions maximum. La Figure 81 montre une photo du Spirent.

La sortie RF du Spirent délivre des signaux à une puissance nominale de $-50\ dBm$. L'utilisateur peut ajuster la puissance délivrée sur chaque canal, ce qui permet d'avoir en sortie des signaux pouvant varier de $-100\ dBm$ à $-35\ dBm$. Le Spirent est piloté par un logiciel appelé *SimGEN*, dont une capture d'écran est montrée

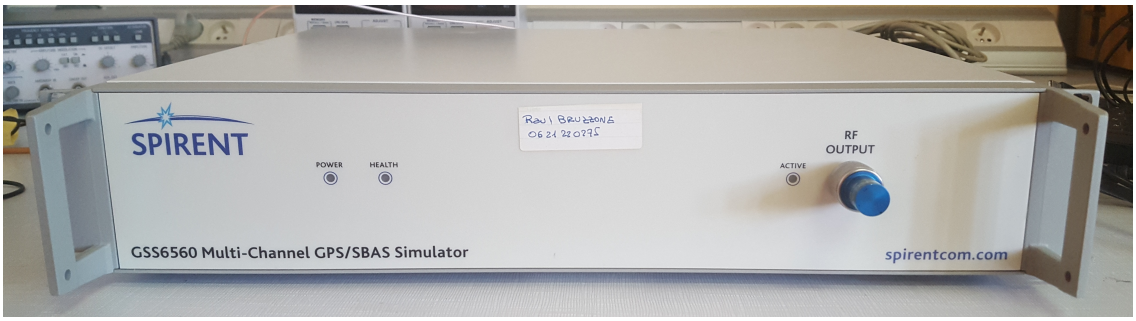

FIGURE 81 – Simulateur Spirent

Figure 82.

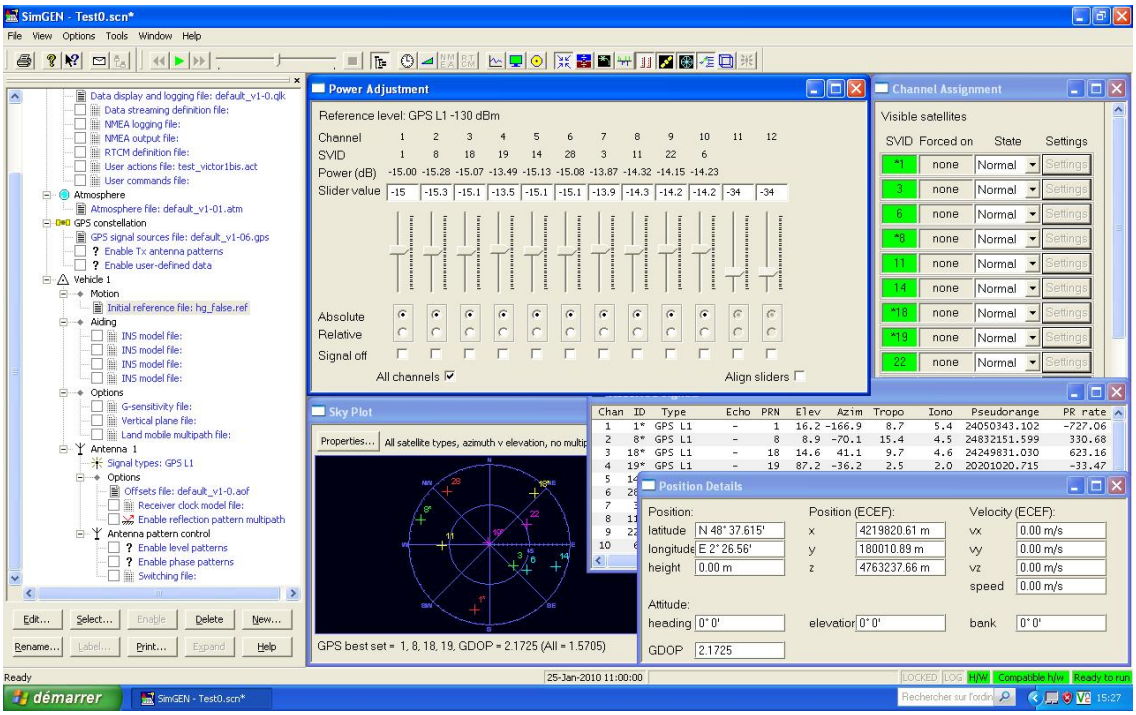

FIGURE 82 – Logiciel SimGEN

Ce logiciel permet de paramétrer le Spirent et tous les signaux qu'il va émettre. Parmi les paramètres réglables on peut citer la puissance des signaux sur chaque canal, la position GPS que le récepteur doit calculer, un déplacement du récepteur, la date et le temps GPS, les éphémérides des satellites, des perturbations comme les trajets indirects et bien d'autres paramètres.

Pour lancer une simulation de signaux, il faut au préalable avoir défini les paramètres de la constellation. Le logiciel dispose de fichiers contenant les éphémérides et les almanachs des constellations GPS. Il suffit alors que l'utilisateur définisse une date et une heure pour que le Spirent en déduise "l'état" de la constellation GPS correspondant. L'utilisateur peut également définir une durée de simulation pour que le Spirent arrête automatiquement l'émission de ses signaux.

Il est également possible de répéter automatiquement un scénario de simulation une fois terminé. Lors d'une simulation certains paramètres peuvent être modifiés à la volée par l'utilisateur, mais SimGEN offre également également la possibilité de mettre en place des scénarios de simulation en amont. Ces scénarios permettent de

définir une chronologie d'évènements afin d'appliquer des changements de paramètres à des temps spécifiés. Les paramètres qui peuvent être modifiés par ce procédé sont les mêmes que ceux qu'un utilisateur peut modifier à la volée durant une simulation. La chronologie des actions du scénario est stockée dans un fichier nommé *User actions file*. Etant donné que la position GPS à calculer ne peut pas être modifiée en cours de simulation, il est nécessaire d'utiliser un *User actions file* pour simuler les changements de position.

Durant une simulation, l'utilisateur peut afficher des fenêtres de contrôle. Cela permet de vérifier notamment la position GPS à calculer, en coordonnées ECEF ou géodésiques, les positions des satellites et les pseudo-distances de chaque satellite de la constellation simulée.

A.3 Simulateur Labsat

FIGURE 83 – Simulateur Labsat

Le Labsat 2 est un générateur de signaux GNSS (GPS et GLONASS), il est représenté sur la Figure 83. Ce générateur GNSS est tout simplement un enregistreur-répéteur de signaux. En effet, avec le Labsat il est possible d'enregistrer des signaux GPS/GLONASS par le biais du logiciel fourni avec le Labsat. Ces enregistrements peuvent être soit continus, soit à durée fixée. L'interface d'enregistrement est présentée Figure 84

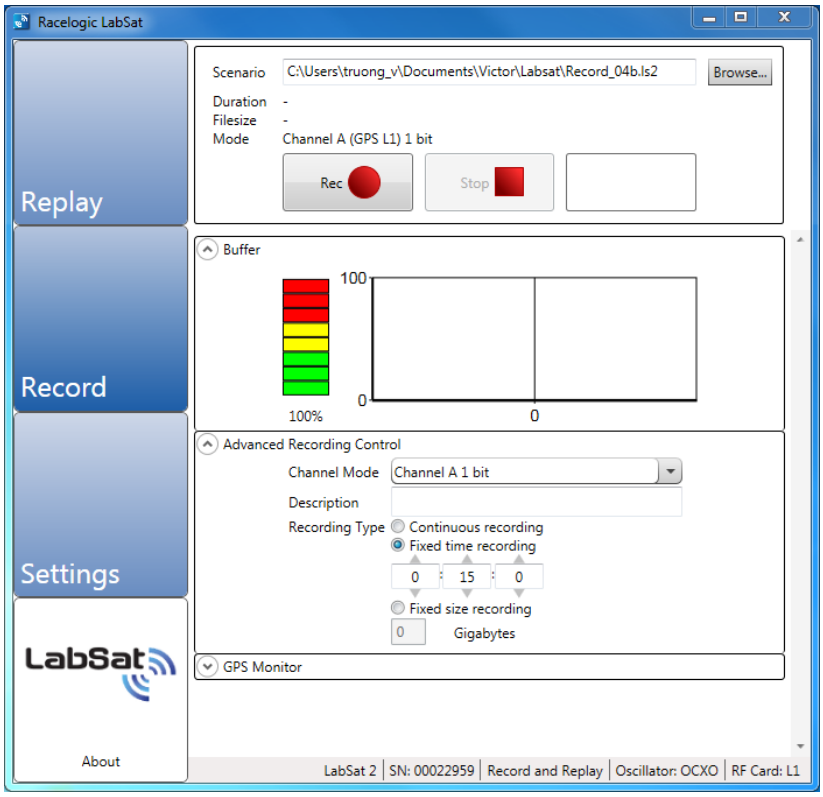

FIGURE 84 – Interface d'enregistrement du Labsat

La répétition de ces signaux passe aussi par le logiciel. Sur l'interface de répétition il est possible d'appliquer une atténuation sur les signaux de sortie.

Il est aussi possible de fixer le temps de départ de l'enregistrement, ou encore de boucler la répétition de l'enregistrement avec un délai entre chaque itération au choix. De plus il est également possible de diffuser un bruit numérique à puissance variable. L'interface de répétition est présentée Figure 85.

La sortie du Labsat délivre une puissance nominale d'environ $-83\ dBm$ sans atténuation. Avec l'atténuation la puissance peut aller jusque $-107\ dBm$ environ.

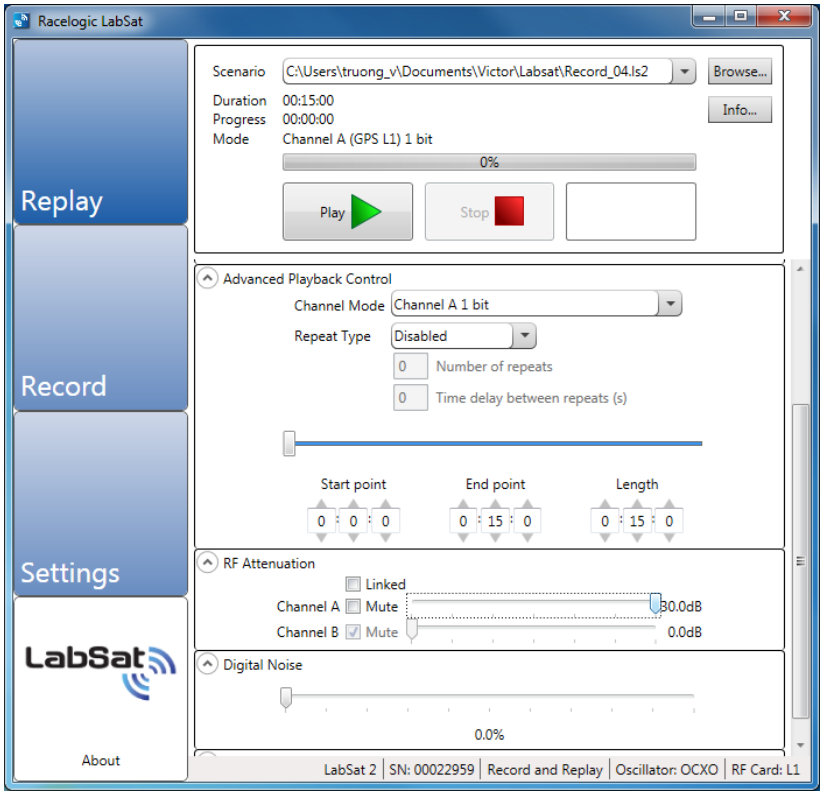

FIGURE 85 – Interface de répétition du Labsat

Annexe B

Utilisation de la fonction trajets indirects du Spirent pour simuler une attaque de leurrage synchronisée

Cette annexe détaille la méthode utilisée pour simuler une attaque de leurrage mettant en jeu une constellation GNSS et des signaux de leurrages calés sur la même horloge que les signaux de la constellation GNSS. Le Spirent ne dispose que d'une seule sortie RF, il n'est donc pas possible de directement générer la constellation GNSS et la constellation du leurre en même temps. Pour contourner ce problème on peut exploiter l'option de simulation de trajets indirects du Spirent.

B.1 Simulation d'un leurrage par l'utilisation des trajets indirects

Les interférences de trajets indirects sont issues de signaux réfléchis par un ou plusieurs obstacles (le sol ou des immeubles par exemple). Les signaux réfléchis subissent donc un délai qui se traduit par des erreurs sur les pseudo-distances. On peut alors exploiter la répercussion de ce délai sur les pseudo-distances pour simuler les signaux du leurre. La Figure 86 illustre le principe des trajets indirects.

On considère un récepteur au point R. Le récepteur va recevoir des signaux directs, c'est-à-dire arrivant directement du satellite SV_j, représentés ici par le signal en noir. Certains signaux peuvent être réfléchis par un réflecteur (en rouge sur la Figure 86) avant d'atteindre le récepteur R, comme celui représenté en bleu sur le Figure 86. Le signal réfléchi va donc avoir une distance de parcourt allongée. Cette distance supplémentaire est ici représentée en pointillé bleu.

L'option de simulation de trajets indirects du Spirent permet de simuler ces signaux réfléchis. Pour ce faire, il ajoute à un signal de base, sous forme d'un délai, la distance supplémentaire causée par la réflexion du signal (la partie du signal en pointillé bleu sur la Figure 86). En exploitant cette option avec les bons paramètres, on peut s'en servir pour générer des signaux de leurrage.

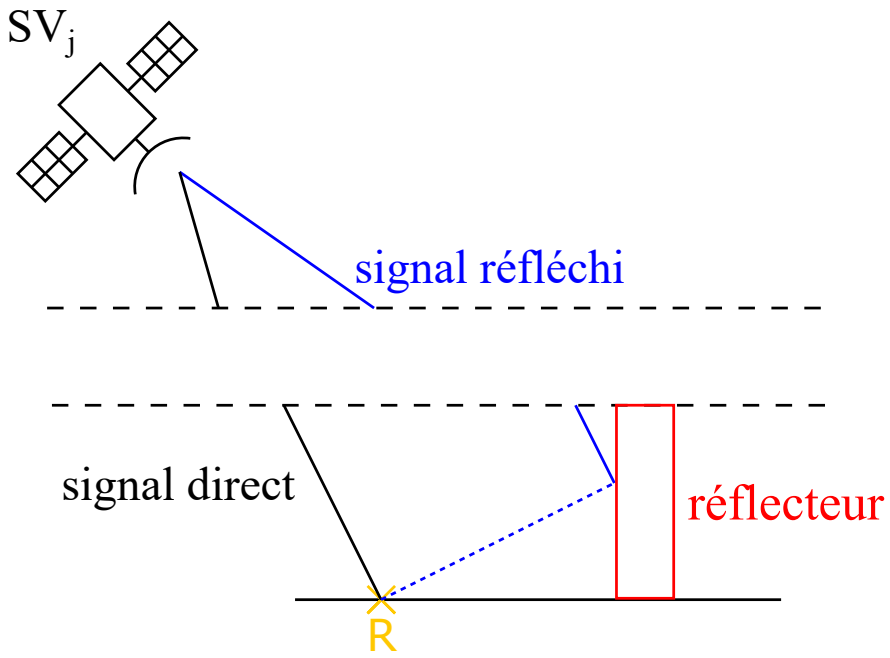

FIGURE 86 – Illustration des trajets indirects

La Figure 87 illustre l'idée derrière l'utilisation des trajets indirects pour simuler une attaque de leurrage. Considérons deux points R et L représentant respectivement la position d'un récepteur GNSS et la fausse position qu'un leurre veut envoyer au récepteur, et un satellite SV_j émettant des signaux GNSS.

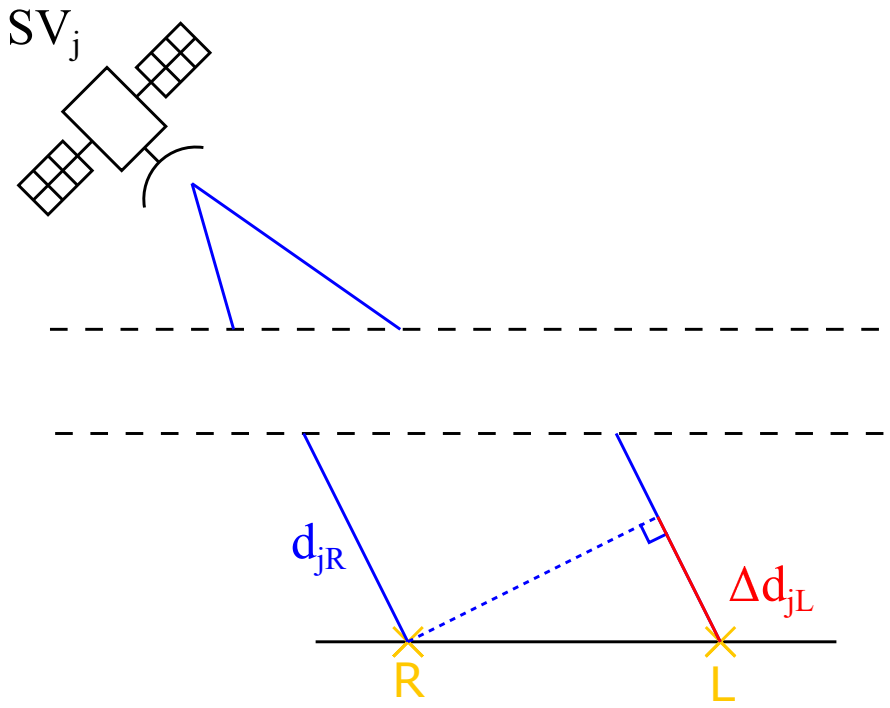

FIGURE 87 – Illustration du détournement de la fonction trajets indirects du Spirent

Vues les altitudes élevées des satellites, on peut faire l'hypothèse que les signaux arrivant au niveau des récepteurs (et donc aux points R et L) sont parallèles. Le signal arrivant au point R correspond à une

distance notée d_{jR}, en bleue sur la Figure 87. Avec l'hypothèse du parallélisme des signaux, le signal arrivant au point L est parallèle au signal arrivant au point R. Ainsi, la distance du signal arrivant au point L, notée d_{jL}, peut s'exprimer comme suit :

$$d_{jL} = d_{jR} + \Delta d_{jL} \tag{B.1}$$

avec Δd_{jL} une distance "intermédiaire" représentée en rouge sur la Figure 87. Cette distance "intermédiaire", et par extension la pseudo-distance correspondante, peut jouer le rôle de délai causé par un trajet indirect. Ainsi, on peut utiliser un trajet indirect avec un délai configuré tel qu'il corresponde à un Δd_{jL} correspondant à la fausse position souhaitée.

B.2 Mise en place sur le Spirent

Les trajets multiples peuvent être simulé sur le Spirent à partir d'un modèle polynomial pour représenter le délai du signal et l'amplitude relative. On peut exprimer ce modèle comme le polynôme suivant :

$$\text{Délai } = d_0 + d_1 t + d_2 t^2 + d_3 t^3 + d_4 t^4 + d_5 t^5 \tag{B.2}$$

Pour pouvoir simuler les signaux du leurre, il faut donc déterminer les coefficients du polynôme B.2 donnant le bon Δd_{jL}.

Pour cela, on réalise à l'aide d'un récepteur u-blox deux acquisitions de données à partir des mêmes paramètres de configuration de constellation GPS du Spirent. Sur la première simulation le point GPS calculé est celui du récepteur, tandis que sur la deuxième simulation le point GPS calculé correspond au faux point souhaité par le leurre. Sur ces deux simulations on enregistre le biais d'horloge du récepteur et les pseudo-distances des satellites de la constellation. A partir de ces deux données on peut calculer les distances $d_{jR}(t)$ pour la première acquisition et $d_{jL}(t)$ pour la deuxième en soustrayant le biais aux pseudo-distances. On calcule alors la différence $(d_{jL}(t) - d_{jR}(t))$ et on réalise une interpolation polynomiale sur cette différence. Les coefficient du polynôme d'interpolation correspondent aux coefficients du polynôme à utiliser pour configurer les signaux de trajets multiples du Spirent. Dans notre cas d'étude un polynôme de degré 1 a suffit à obtenir le faux point souhaité.

Une fois le polynôme de délai déterminé, on alloue les six premiers canaux du Spirent à la constellation GNSS. Les six canaux suivants sont alloués aux signaux de trajets multiples des signaux de la constellation GNSS, les signaux de trajets multiples jouant alors le rôle des signaux d'un leurre GNSS.

Annexe C

Changement de repère

Le changement de repère utilisé dans la partie III.3.1 permet de passer du repère ECEF au repère local. La Figure 88 présente ces deux repères et les éléments géométriques permettant le passage de l'un à l'autre. Ici la Terre est simplifiée sous forme d'une sphère, mais dans les calculs c'est un ellipsoïde.

Le repère ECEF est centré sur le centre de la Terre. Ses axes $\overrightarrow{x}$ et $\overrightarrow{y}$ sont dans le plan horizontal de latitude 0°, avec $\overrightarrow{x}$ orienté suivant la direction de longitude 0° et $\overrightarrow{y}$ orientée suivant la direction de longitude 90°E. L'axe $\overrightarrow{z}$ est orienté vers le pôle Nord.

Le repère local est centré sur un point P de coordonnées ECEF (x_P, y_P, z_P). Ce repère est lié au plan horizontal défini à l'altitude du point P, noté H sur le Figure 88. Ses axes $(\overrightarrow{h}, \overrightarrow{e}, \overrightarrow{n})$ correspondent respectivement à l'axe d'altitude, la direction Est et la direction Nord.

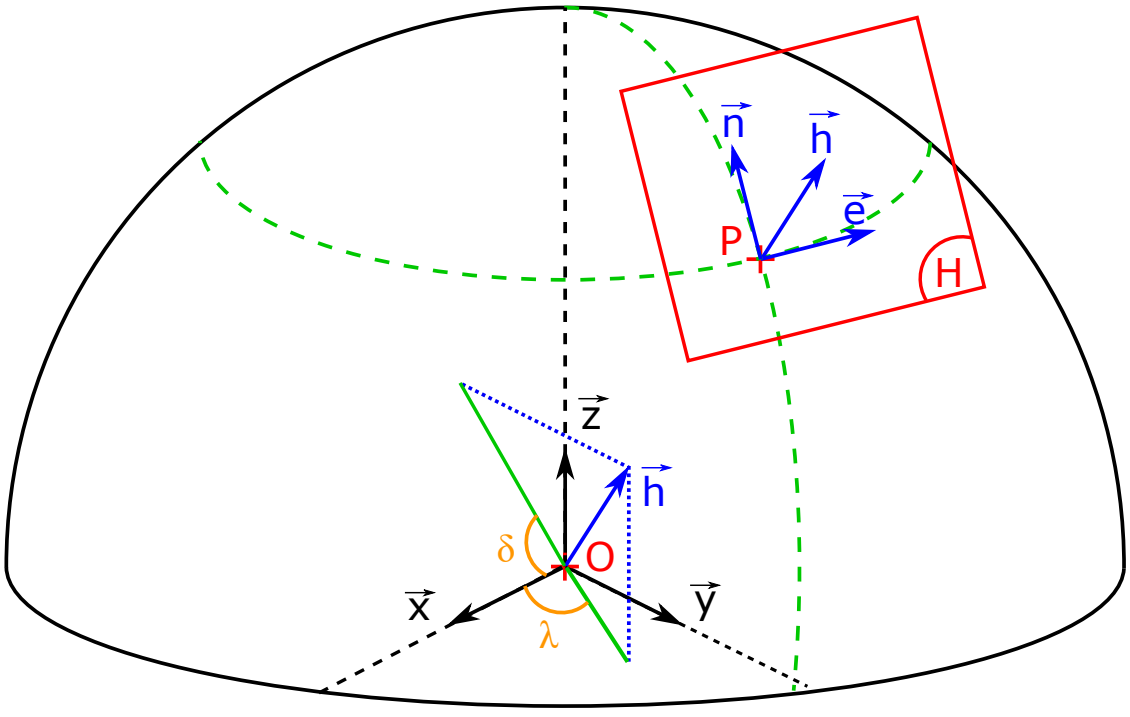

FIGURE 88 – Passage du repère ECEF au repère local

Le changement de repère consiste donc à passer du repère $R_0 = (O, \overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z})$ au repère $R_p = (P, \overrightarrow{h}, \overrightarrow{e}, \overrightarrow{n})$. Pour passer de l'un à l'autre, on calcule la matrice de transformation entre les deux repères en utilisant la

composition de transformations géométriques. Comme illustré Figure 88, à partir du repère ECEF on doit effectuer une rotation d'axe $\overrightarrow{z}$ d'angle λ, puis une rotation d'axe $\overrightarrow{y}$ d'angle $-\delta$, et enfin une translation suivant le vecteur $\overrightarrow{OP}$. L'angle λ correspond à l'angle de longitude du point P. Si on note (x_h, y_h, z_h) les coordonnées du vecteur $\overrightarrow{h}$, alors $\delta = \arctan\left(\frac{z_h}{x_h}\right)$. Pour déterminer les coordonnées de $\overrightarrow{h}$ il suffit de convertir les coordonnées GPS du point P dans le repère ECEF, puis de convertir dans le repère ECEF les coordonnées GPS d'un point ayant la même latitude et longitude que P mais une altitude différente. La différence de ces deux coordonnées nous donne les coordonnées du vecteur $\overrightarrow{h}$.

L'ordre et les modalités des transformations géométriques étant maintenant définis, on peut calculer la matrice de transformation. Notons Rz, R_y les matrices de rotations d'axe $\overrightarrow{z}$ et $\overrightarrow{y}$, T_{OP} la matrice de translation de O à P. On a alors :

$$\mathbf{T_{OP}} = \begin{bmatrix} 1 & 0 & 0 & x_P \\ 0 & 1 & 0 & y_P \\ 0 & 0 & 1 & z_P \\ 0 & 0 & 0 & 1 \end{bmatrix}, \mathbf{R_z} = \begin{bmatrix} \cos(\lambda) & -\sin(\lambda) & 0 & 0 \\ \sin(\lambda) & \cos(\lambda) & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \text{ et } \mathbf{R_y} = \begin{bmatrix} \cos(-\delta) & 0 & \sin(-\delta) & 0 \\ 0 & 1 & 0 & 0 \\ -\sin(-\delta) & 0 & \cos(-\delta) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

La matrice de transformation est donc

$$M_{EL} = T_{OP} \cdot R_z \cdot R_y \tag{C.1}$$

Ainsi si on note $\mathbf{X_e}$ et $\mathbf{X_l}$ respectivement les coordonnées d'un point dans le repère ECEF et dans le repère local on a :

$$\mathbf{X_e} = M_{EL} \cdot \mathbf{X_l} \tag{C.2}$$

Bibliographie

[1] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Pre-Despreading Authenticity Verification for GPS L1 C/A Signals : Pre-Despreading GPS L1 Authentication," *Navigation*, vol. 61, pp. 1–11, Mar. 2014.

[2] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals : Real-Time Codeless GPS Spoofing Detection," *Navigation*, vol. 60, pp. 267–278, Dec. 2013.

[3] D. Borio and C. Gioia, "A Dual-antenna Spoofing Detection System Using GNSS Commercial Receivers," *Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015)*, p. 7, 2015.

[4] D. Marnach, S. Mauw, M. Martins, and C. Harpes, "Detecting Meaconing Attacks by Analysing the Clock Bias of Gnss Receivers," *Artificial Satellites*, vol. 48, Jan. 2013.

[5] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescape, "A SVM-based detection approach for GPS spoofing attacks to UAV," in *2017 23rd International Conference on Automation and Computing (ICAC)*, (Huddersfield, United Kingdom), pp. 1–11, IEEE, Sept. 2017.

[6] E. D. Kaplan and C. Hegarty, eds., *Understanding GPS : principles and applications*. Artech House mobile communications series, Boston : Artech House, 3rd ed ed., 2017. OCLC : ocm62128065.

[7] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," in *Preprint of the 2012 ION GNSS Conference*, (Nashville, USA), p. 15, Sept. 2012.

[8] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," *International Journal of Navigation and Observation*, vol. 2012, pp. 1–16, 2012.

[9] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*, vol. 104, pp. 1258–1270, June 2016.

[10] A. Broumandan, R. Siddakatte, and G. Lachapelle, "An approach to detect GNSS spoofing," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, pp. 64–75, Aug. 2017.

[11] T. E. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, pp. 1073–1090, Apr. 2013.

[12] T. E. Humphreys, B. M. Ledvina, V. Tech, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the Spoofing Threat : Development of a Portable GPS Civilian Spoofer," *Preprint of the 2008 ION GNSS Conference*, p. 12, 2008.

[13] A. Broumandan, A. Jafarnia-Jahromi, G. Lachapelle, and R. T. Ioannides, "An approach to discriminate GNSS spoofing from multipath fading," in *2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, (Noordwijk, Netherlands), pp. 1–10, IEEE, Dec. 2016.

[14] D. M. Akos, "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC) : Spoofing Detection via Automatic Gain Control," *Navigation*, vol. 59, pp. 281–290, Dec. 2012.

[15] A. Jafarnia-Jahromi, N. Fadaei, S. Daneshmand, A. Broumandan, and G. Lachapelle, "A review of pre-despreading GNSS interference detection techniques," in *5th ESA International Colloquium Scientific and Fundamental Aspects of the Galileo Programme*, (Braunschweig, Germany), p. 8, Oct. 2015.

[16] A. Jafarnia Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements," *International Journal of Satellite Communications and Networking*, vol. 30, pp. 181–191, July 2012.

[17] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level," in *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, (Netherlands), pp. 1–6, IEEE, Dec. 2010.

[18] E. G. Manfredini, F. Dovis, and B. Motella, "Validation of a signal quality monitoring technique over a set of spoofed scenarios," in *2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, (Noordwijk, Netherlands), pp. 1–7, IEEE, Dec. 2014.

[19] J. Huang, L. Lo Presti, B. Motella, and M. Pini, "GNSS spoofing detection : Theoretical analysis and performance of the Ratio Test metric in open sky," *ICT Express*, vol. 2, pp. 37–40, Mar. 2016.

[20] C. Günther, "A Survey of Spoofing and Counter-Measures : A Survey of Spoofing and Counter-Measures," *Navigation*, vol. 61, pp. 159–177, Sept. 2014.

[21] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, (Monterey, CA, USA), pp. 262–269, IEEE, May 2014.

[22] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, p. 18, Oct. 2013.

[23] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-Autonomous Spoofing Detection : Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer," in *Proceedings of ION 2009 International Technical Meeting*, p. 7, 2009.

[24] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data," in *Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013)*, p. 43, 2013.

[25] D. Borio and C. Gioia, "A sum-of-squares approach to GNSS spoofing detection," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 52, pp. 1756–1768, Aug. 2016.

[26] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS Signal Authentication Via Power and Distortion Monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, pp. 739–754, Apr. 2018.

[27] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-Likelihood Power-Distortion Monitoring for GNSS-Signal Authentication," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, pp. 469–475, Feb. 2019.

[28] Qiang Zou, Sunan Huang, Feng Lin, and Ming Cong, "Detection of GPS spoofing based on UAV model estimation," in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, (Florence, Italy), pp. 6097–6102, IEEE, Oct. 2016.

[29] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, pp. 131–143, Feb. 2018.

[30] K. Liu, W. Wu, and Z. Wu, "Using the Receiver Clock Offset Abnormal to Prove the Existence of Spoofing Signal," in *2018 37th Chinese Control Conference (CCC)*, (Wuhan), pp. 4592–4596, IEEE, July 2018.

[31] A. Vervisch-Picois, N. Samama, and T. Taillandier Loize, "Influence of GNSS spoofing on drone in automatic flight mode," in *Proceedings of the International Technical Symposium on Navigation and Timing (ITSNT) 2017*, (ENAC, Toulouse, France), p. 9, Nov. 2017.

[32] Parrot, "Parrot Anafi productsheet," 2018.

[33] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of Spatial Processing Approaches for GNSS Structural Interference Detection and Mitigation," *Proceedings of the IEEE*, vol. 104, pp. 1246–1257, June 2016.

[34] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, (Nashville, USA), p. 12, Sept. 2012.

[35] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A GNSS structural interference mitigation technique using antenna array processing," in *2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, (A Coruna, Spain), pp. 109–112, IEEE, June 2014.

[36] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, "Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation using Direction Assisted Multiple Hypotheses RAIM," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, p. 11, Sept. 2012.

[37] J. R. van der Merwe, A. Rugamer, A. F.-D. Goicoechea, and W. Felber, "Blind Spoofing Detection Using a Multi-Antenna Snapshot Receiver," in *2019 International Conference on Localization and GNSS (ICL-GNSS)*, (Nuremberg, Germany), pp. 1–7, IEEE, June 2019.

[38] K. Jansen, N. O. Tippenhauer, and C. Pöpper, "Multi-receiver GPS spoofing detection : error models and realization," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, (Los Angeles California USA), pp. 237–250, ACM, Dec. 2016.

[39] V. H. Nguyen, G. Falco, M. Nicola, and E. Falletti, "A Dual Antenna GNSS Spoofing Detector Based on the Dispersion of Double Difference Measurements," in *2018 9th ESA Workshop on Satellite Navigation-Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, (Noordwijk, Netherlands), pp. 1–8, IEEE, Dec. 2018.

[40] A. J. Jahromi, A. Broumandan, S. Daneshmand, N. Sokhandan, and G. Lachapelle, "A double antenna approach toward detection, classification and mitigation of gnss structural interference," *Proceedings of the NAVITEC 2014 Conference*, pp. 3–5, Dec. 2014.

[41] A. J. Jahromi, A. Broumandan, and G. Lachapelle, "Gnss signal authenticity verification using carrier phase measurements with multiple receivers," in *2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, (Noordwijk, Netherlands), pp. 1–11, IEEE, Dec. 2016.

[42] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "A Network-based GNSS Structural Interference Detection, Classification and Source Localization," in *Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015)*, p. 12, Sept. 2015.

Titre : DIGUE : Détection d'Interférences Gnss pour U.a.v autonomE

Mots clés : interférences, drones, leurrage, GNSS, biais d'horloge, GPS

Résumé : La présente étude s'inscrit dans le domaine des interférences GNSS. Elle consiste à proposer une approche de détection d'interférences de leurrage pour drone autonome utilisant les données directement issues des récepteurs. En réalisant un état de l'art des méthodes de détection de leurrage, le contrôle du biais d'horloge est apparu comme une approche potentielle. Une modélisation numérique d'une attaque de leurrage sur un récepteur a mis en évidence que le biais d'horloge présente des sauts lorsque le récepteur passe de la constellation GNSS à la constellation du leurre. En reproduisant cette attaque sur des récepteurs commerciaux utilisant de vrais signaux, le biais d'horloge présente des sauts plus importants que prévus par le modèle, et dans certains cas sur la dérive du biais également. Ces sauts ont été observés sur différents scénarios d'attaque plus ou moins subtiles, cependant l'amplitude de ces sauts semble aléatoire.

Pour aller plus loin que la simple détection de leurrage, une approche utilisant une formation de drones communicants a été proposée dans le but de faire une estimation de la localisation du leurre. Cette méthode est basée sur un protocole de déplacement permettant à la formation de délimiter une zone de l'espace où le leurre est supposé être localisé. Le protocole actuel n'est pas encore complètement abouti mais a été testé en simulation sur quelques cas avec des résultats prometteurs.

L'étude du comportement du biais d'horloge a permis de mettre en évidence son intérêt dans une stratégie de détection de leurrage GNSS. A partir de ce constat, de futurs travaux pourront être menés sur le développement et l'implémentation sur un drone volant d'un algorithme de détection basé sur le contrôle du biais d'horloge. L'étude de l'utilisation d'une formation de drone pour la localisation d'un leurre a permis de poser les bases d'une solution prometteuse. De futurs travaux peuvent être menés afin de compléter le protocole de déplacement et de valider son efficacité face à différents types de leurres.

Title : GNSS interference detection for autonomous UAV

Keywords : interferences, UAV, spoofing, GNSS, clock bias, GPS

Abstract : This study is part of the field of GNSS interference detection. Its aim is to propose an approach for detecting spoofing interferences on an autonomous UAV using data directly available on the receivers. With the study of the state of the art of spoofing detection methods, the monitoring of the clock bias seemed like a potential method. A numerical modeling of a spoofing attack on a receiver showed that the clock bias undergoes jumps when it switch from the GNSS constellation to the spoofing constellation. By replicating this attack on a commercial receivers using real signals, the clock bias shows higher jumps than expected by the model and in some cases the clock drift also show some jumps. These jumps have been observed on different more or less subtle attack scenarios, however the amplitude of the jumps seems random.

To go further than the simple spoofing detection, an approach using a communicating drone formation has been proposed. This method is based on a movement protocol allowing to delimit a space area where the spoofer is supposed to be located. The current protocol is not yet fully completed but it offers a promising basis.

The study of the behavior of the clock bias highlighted its interest in a GNSS spoofing detection strategy. Based on this observation, further work could be carried out on the development and implementation on a UAV of a detection algorithm based on the monitoring of the clock bias. The study of the use of a drone formation for the localization of a spoofer led to the basis of a promising solution. Further work could be carried out in order to complete the movement protocol and to validate its efficiency against different types of spoofers.

Institut Polytechnique de Paris
91120 Palaiseau, France