
# Rapport de stage de césure

# Octobre 2025


**AGUIRRE Thomas**

**Illinois Institute of Technology Chicago**


**Intégrité des systèmes de navigation par satellites**

# Table des matières



# Mots-clés

Navigation, Kalman, GNSS, Recherche, Modélisation

# Keywords

Navigation, Kalman, GNSS, Research, Modeling

# Résumé

De octobre 2024 à avril 2025, j'ai réalisé un stage dans les laboratoires Navlab de l'IIT Chicago (IL,USA). Sous l'encadrement de Boris Pervan, nous avons réalisé des recherches avancées sur l'intégrité des systèmes de navigation par satellite. Ces recherches présentent des enjeux technologiques d'actualité nécessitant une attention particulière pour la sécurité et la fiabilité des systèmes. Pour arriver au développement de code, une longue phase d'apprentissage en navigation par satellites a été nécessaire. Après cela, un objectif a été défini : d'abord la mise en place d'un moniteur d'innovation en utilisant des équations de mesure GNSS et INS. Ce modèle permet de détecter des attaques de jamming ou spoofing mais demande un réel travail quant à la définition de ses paramètres et du modèle d'erreurs en général. Alliant ainsi les compétences en Kalman et Inertiel déjà acquises aux nouvelles compétences, nous sommes arrivés à notre modèle puis à l'étude de la sensibilité de notre moniteur vis-à-vis des erreurs provenant des mesures GNSS ou de la centrale inertielle. En étudiant différents cas, avec attaque ou sans attaque, ou en changeant l'IMU, nous avons poursuivi avec une fine étude des différents paramètres et de leur influence sur la fiabilité de notre modèle que nous voulons le plus proche possible de la réalité. Nous sommes arrivés à des résultats clairs : certains paramètres ont une réelle influence sur le modèle et un entre-deux est obligatoire afin de maintenir continuité et intégrité de notre système (ne pas déclencher trop d'alarmes inutiles et ne pas en rater).

# Abstract

From October 2024 to April 2025, I completed an internship in the Navlab laboratories at IIT Chicago (IL,USA). Under the guidance of Boris Pervan, we carried out advanced research focusing on the integrity of satellite navigation systems. This research presents current technological challenges requiring particular attention to system safety and reliability. To get to code development, a long learning phase in satellite navigation was necessary. After this, a goal was defined : firstly, to set up an innovation monitor using GNSS and INS measurement equations. This model can be used to detect jamming or spoofing attacks, but requires a great effort to define its parameters and the error model in general. Combining the Kalman and Inertial skills already acquired with new skills, we arrived at our model and then studied the sensitivity of our monitor to errors coming from GNSS or INS measurements. By studying different cases, with or without attack, or by changing the IMU, we went on to make a detailed study of the different parameters and their influence on the reliability of our model, which we wanted to be as close as possible to reality. The results were clear : some parameters have a real influence on the model, and an in-between is required to maintain the continuity and integrity of our system (not triggering too many unnecessary attacks, and not missing any).

# 1 Introduction

Ces dernières années, nous avons vu l'apparition des voitures autonomes dans notre quotidien [1]. La marque de voiture venant à l'esprit est Tesla. En effet, cette dernière propose des voitures au niveau d'automatisation partielle de la conduite donc de niveau 2 (automatisation partielle : niveau 0 étant pas d'automatisation de la conduite et niveau 5 automatisation complète de la conduite). Néanmoins, de nombreuses autres grandes marques sont en plein développement de voitures autonomes avec comme objectif actuel de démocratiser le niveau 3 (automatisation conditionnelle) : BMW, GM, Ford ou Mercedes-Benz. Ainsi, ce secteur présente de nombreux enjeux, d'abord économiques, mais surtout technologiques car la recherche n'y a jamais été aussi poussée. Le concept des systèmes de navigation autonomes est donc en plein développement et pourrait à l'avenir faciliter notre quotidien en augmentant également la sécurité.

Néanmoins, avant d'arriver au stade où ils sont ancrés dans notre vie de tous les jours, du travail reste évidemment à faire. C'est donc avec ces idées-là en tête que j'ai décidé de réaliser mon stage au sein du laboratoire Navlab [2] géré par Boris Pervan, professeur en génie mécanique et aérospatial, de l'Illinois Institute of Technology de Chicago. En rejoignant ce laboratoire, je rejoins un groupe spécialisé dans le domaine de la recherche avancée en systèmes de navigation qui saura dans un premier temps me guider dans mon apprentissage encore incomplet dans le domaine puis m'aider dans le développement de choses concrètes. J'y ai donc développé ma compréhension des systèmes GNSS/INS et me suis familiarisé avec les différentes problématiques du secteur relatif à la fiabilité et l'intégrité de nos systèmes.

L'objectif final de ce stage était alors d'étudier la sensibilité du moniteur d'innovation, modèle que nous aurions développé au préalable à partir d'une base déjà existante, et sa sensibilité à la variation des multiples paramètres des erreurs provenant des GNSS et INS. La finalité est donc de connaître les conditions qui rendraient notre moniteur moins fiable, créant des alertes inutiles ou n'en créant pas quand nécessaire. Dans ce rapport, nous verrons donc à quel point les variations des paramètres définissant les erreurs GNSS et INS affectent notre moniteur d'innovation dans sa fonction de détection d'alertes.

Ainsi, pour pouvoir répondre à cette problématique et compléter l'objectif qui nous a été fixé, nous verrons plusieurs grandes sections. D'abord, nous commencerons par une présentation du contexte du stage et de l'environnement de travail. Puis nous continuerons en évoquant la problématisation détaillée du thème que nous venons tout juste d'introduire, à savoir les objectifs précis (puisqu'il y en avait bien plus que un et l'objectif final que nous avons cité) et les enjeux. Enfin, nous rentrerons dans le cœur du stage avec une description de l'activité et des résultats du stage, en passant par l'apprentissage par lequel j'ai du passer puis par les travaux réalisés, le codage et l'étude du modèle tout juste construit.

# 2 Présentation du contexte

Le stage de césure a donc été réalisé dans une université américaine avec laquelle l'ENSTA (anciennement ENSTA Bretagne au moment de la signature de la convention de stage) a un lien très fort. En effet, il s'agit de l'Illinois Institute of Technology de Chicago autrement dit IIT Chicago qui est l'un des rares partenaires nord-américains de l'ENSTA. Ce partenariat était par ailleurs nouveau et c'est la présentation de l'école de Chicago à Brest qui m'a permis de la découvrir et développer l'envie d'y réaliser un stage, preuve de l'intérêt des partenariats académiques.

Ce stage a en particulier été réalisé au sein du "Department of Mechanical and Aerospace Engineering" ou Département de génie mécanique et aérospatial dans le campus principal de Chicago au Rettaliata Engineering Center. Le laboratoire d'accueil était le laboratoire Navlab de Boris Pervan qui partage ses locaux avec TruNav dont il est le co-fondateur avec Samer Khanafseh, à qui revient la gestion du second groupe. Cette cohabitation facilite la progression dans la recherche et développe la productivité globale des deux groupes permettant des partages de connaissances et de solutions. En effet, mon encadrant principal tout le long de ce stage était Birendra Kujur, spécialisé en Filtres de Kalman et techniques de spoofing, associé au laboratoire Navlab, mais je pouvais également trouver de l'aide auprès de Kana Nagai, expert en systèmes multi-constellations, et dont les travaux concernaient davantage le groupe Trunav. C'était également le cas de Khatib Bahaddi, autre français du laboratoire mais lié à TruNav, avec qui j'ai beaucoup travaillé, que ce soit pour l'aider vis-à-vis de ses travaux ou lorsque j'avais moi-même besoin d'indications. Le groupe Navlab auquel j'étais lié avait donc une très forte spécialisation dans la recherche avancée en positionnement, navigation et synchronisation (PNT) avec une attention particulière que nous retrouverons pour l'intégrité des systèmes de navigation. Notons par ailleurs que les deux groupes réalisent des travaux liés à la défense américaine sous demande du gouvernement américain lui-même, et cela pose d'ailleurs plusieurs problèmes de confidentialité que nous aurons le temps d'évoquer par la suite.

# 3 Problématisation du thème

Connaissant désormais le contexte global du stage et afin de pouvoir rentrer encore plus dans les détails par la suite, commençons par évoquer comment il me l'a été présenté au premier abord. Il faut savoir que les contacts avec Monsieur Boris Pervan avant mon arrivée à Chicago n'ont pas été nombreux. En effet, suite à quelques mails, nous avons eu un cours entretien se focalisant davantage sur mes connaissances et moins sur ce que j'allais devoir faire. Sans doute l'un des éléments les plus importants dans ma sélection pour ce stage a été la connaissance plutôt approfondie de Kalman et des filtres de Kalman, point majeur de mon CV qui avait attiré l'attention de Monsieur Pervan. Et en effet, nous le verrons par la suite, les filtres de Kalman étaient omniprésents dans mon stage, le cœur du code résidant autour d'une boucle utilisant Kalman.

Enfin, après l'entretien, il m'était difficile de savoir exactement ce que j'allais y faire, quels étaient les enjeux et les objectifs. Mes recherches personnelles m'avaient au préalable amenées à la conclusion que je travaillerais de près ou de loin sur les voitures autonomes guidées par satellite. La mise en place de la convention de stage avec l'ENSTA Bretagne a alors effacé les doutes. Les objectifs étaient alors les suivants : étudier de nouvelles améliorations aux systèmes de navigation par satellite avec utilisation potentielle de centrales inertielles, de signaux de satellites basses orbites (LEO pour Low Earth Orbiting) et de télémétrie laser afin de garantir la fiabilité des systèmes de positionnement, navigation et synchronisation (PNT) dans des lieux d'applications à sécurité cruciale. On comprend alors déjà les enjeux du stage vis-à-vis du laboratoire puisque on est directement dans le domaine des voitures ou véhicules autonomes contrôlés par satellite. En particulier, ce dernier point était lié aux travaux de Birendra Kujur. Trois objectifs bien spécifiques ont alors été définis pour la première fois par le laboratoire, à savoir :

— Établir une base solide de connaissance sur la théorie et le fonctionnement du GNSS
— Comprendre les menaces cyber-physiques externes affectant le PNT
— Concevoir, mettre en œuvre et tester des mesures d'atténuation pour au moins un élément de menace.

Le stage et ses objectifs ont donc été définis ici pour la première fois. Ces objectifs semblent alors cohérents vis-à-vis des multiples recherches que j'avais pu réaliser. En effet, mes connaissances en Kalman faciliteraient la partie codage une fois un approfondissement dans le domaine des systèmes de navigation par satellites réalisé tout en apportant par ailleurs un point de vue différent au vu de la filière dont je proviens. Les deux premiers objectifs ont donc assez logiquement été respectés et une bonne partie de mon temps après mon arrivée à Chicago a été dédiée à rattraper mon retard dans le domaine avec des cours à propos de la navigation par satellite et aux menaces d'attaques. Néanmoins, le troisième point a légèrement changé et c'est en ce sens que l'on peut dire qu'il y a une modification de la définition du stage durant celui-ci. En effet, dans les faits, il s'agissait davantage de la continuité du développement d'un code déjà existant afin d'établir un modèle capable de détecter des attaques et fidèle aux comportements effectifs que l'on

aurait avec des systèmes de navigation existant. Les deux objectifs restent tout de même relativement proches dans leur définition.

Rappelons par ailleurs que certains travaux sont liés à la défense américaine. Aucun détail ne m'a cependant été communiqué par soucis de confidentialité mais on devine donc un lien fort et de nombreux enjeux vis-à-vis des technologies américaines et de leur développement au niveau des armées. On peut supposer que ces travaux serviront pour des véhicules terrestres en milieu de guerre. Un exemple de véhicule correspondant pourrait être les différents véhicules qui avaient été présentés par Arquus lors du parrainage de la promotion Fise 2025 de l'ENSTA Bretagne.

Les différents laboratoires Navlab et Trunav fonctionnent donc par des financements, parfois gouvernementaux comme nous venons de le dire, il y a alors une certaine pression avec des rendus mensuels à faire selon le projet et de nombreuses dates limites à respecter. Certaines absences prolongées notamment de l'encadrant délégué ont pu créer certains ralentissements pour mon collègue Khatib et moi, créant des périodes de travail plus intensives pour essayer de rattraper et respecter les dates limites.

# 4 Description de l'activité et des résultats du stage

## 4.1 Premiers pas et apprentissage

Comme indiqué précédemment avec les deux premiers points des objectifs, il a été important au début du stage de rattraper certains points en navigation par satellite et construire une base de connaissance suffisamment solide pour pouvoir travailler sur ce thème. Ainsi, il m'a d'abord été demandé de suivre des cours à la fois en ligne, mais aussi en présentiel ou même lire des livres pour essayer de combler mon retard. Un compte rendu a donc été nécessaire ainsi qu'un entretien avec mon encadrant afin de revoir les points qui avaient mal été compris. Beaucoup d'aspects ont été vus à commencer par les fondamentaux de la navigation par satellite et ses équations parfois indigestes, survolant également de nombreux concepts déjà vus en cours d'inertiel en deuxième année à l'ENSTA Bretagne ou bien même des concepts de traitement du signal, tout en m'introduisant au concept des sources d'erreurs qui ont été au cœur de mon travail par la suite. J'ai également pu survoler des concepts de signaux avec lesquels j'étais déjà familier, détaillant au passage l'architecture d'un receveur de signal et le facteur de bruit à travers la formule de Friis ou encore le GPS assisté permettant de réduire le temps de positionnement et la précision en utilisant par exemple une tour GPS fixe receveuse. Notons néanmoins qu'une bonne partie de l'apprentissage s'est faite au fur à mesure par des recherches en parallèle du code et des travaux réalisés.

Dans cette première sous-section, je présenterai quelques concepts que je juge importants pour la compréhension des problématiques qui vont suivre. Commençons d'abord par le schéma suivant (Fig. 1) [3] :

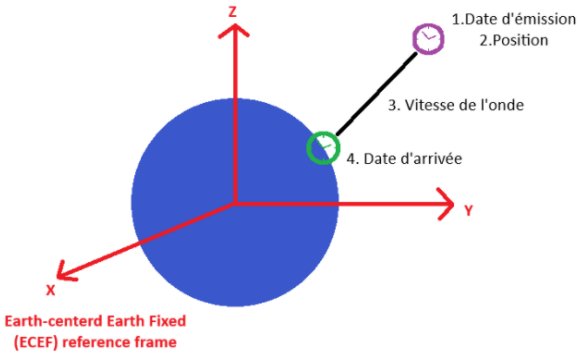


FIGURE 1 – Représentation du fonctionnement d'un GPS

A ce schéma, on associe les équations suivantes :

$$\tau_C(t) = \left( \frac{d_u^{(k)}}{c} + b_u - \delta B^{(k)} \right) + \delta I_u^{(k)} + \delta T_u^{(k)} + v_u^{(k)} \tag{1}$$

Avec :

- $d_u^{(k)} = \sqrt{(x_u - x^{(k)})^2 + (y_u - y^{(k)})^2 + (z_u - z^{(k)})^2}$ la vraie distance entre le satellite k et l'utilisateur
- $(x_u, y_u, z_u)$ la position de l'utilisateur
- $(x^{(k)}, y^{(k)}, z^{(k)})$ la position du satellite k
- $c$ la vitesse de la lumière
- $b_u$ le biais de l'horloge de l'utilisateur et $\delta B^{(k)}$ l'erreur d'horloge du satellite k
- $\delta I_u^{(k)}$, $\delta T_u^{(k)}$,$v_u^{(k)}$ les délais ionosphériques, troposphériques et d'autres incertitudes

Afin de pouvoir procéder aux calculs, on a donc besoin des 4 points donnés dans le schéma. On notera par ailleurs que c'est déjà ici que se crée les biais d'horloge qui ne peuvent pas avoir une précision absolue. L'équation (1) est la pseudo-durée qu'on a entre le satellite k et l'utilisateur. Les différentes erreurs apparaissent déjà et on comprend donc mieux l'influence et l'intérêt qu'elles vont avoir par la suite. A partir de ce schéma et de ces équations, on construit les pseudo-distances et on trouve la position de l'utilisateur $(x_u, y_u, z_u)$ et le biais de l'horloge de l'utilisateur $b_u$ en résolvant généralement le système à plusieurs inconnus avec plusieurs équations obtenues à partir des multiples satellites. Une longue étape de linéarisation, que nous ne détaillerons pas ici, est à faire puis quelques calculs matriciels interviennent.

Autre élément important que nous rencontrerons par la suite et qui est lié à la télécommunication, il s'agit de la structure du signal puisque nous allons en servir par la suite. D'abord, introduisons un schéma de la structure du signal (Fig., 2) [3].

Ainsi, à chaque fois qu'un GPS envoie un signal, cela ressemble au schéma ci-dessus. On y retrouve d'abord la porteuse ou "Carrier", dont la fréquence dépend de la bande de fréquence choisie (L1 à 1.57542 GHz ou L2 à 1.22760GHz)). En effet, certaines fréquences

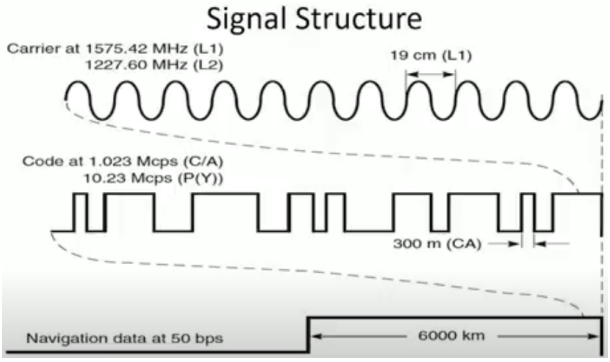


FIGURE 2 – Structure du signal

sont bloquées/atténuées par l'atmosphère donc celle du signal doit être bien choisie. Puis, au milieu le code pseudo-aléatoire PRN, code binaire pour les informations nécessaires.

Ainsi, en utilisant les équations (8) que nous détaillerons par la suite, nous utilisons ce que nous voyons avec la figure 2 pour pouvoir estimer la pseudo-distance et la phase porteuse en utilisant donc la structure que nous venons de définir. Une des deux équations de (8) (l'équation supérieure) correspond à la mesure de la pseudo-distance en utilisant la code de la figure, possédant une résolution de seulement quelques mètres avec une résistance au bruit plus importante. L'autre équation de (8) (l'équation inférieure) correspond à la mesure de phase de la porteuse avec l'apparition de $N_\phi$ à estimer, possédant une précision plus importante (moins d'un centimètre) mais moins robuste.

Enfin, définissons rapidement Jamming et Spoofing pour ne plus avoir à le faire puisque nous traiterons principalement de spoofing par la suite [5] :

— Jamming : type d'interférences intentionnelles qui corrompt un signal cible afin d'en réduire les performances en transmettant des signaux parasites

— Spoofing : type d'interférences intentionnelles qui corrompt un signal cible en reproduisant le signal GNSS authentique falsifiant alors ce signal. Le spoofer peut alors entraîner l'utilisateur sur une trajectoire différente.

## 4.2 Aide sur d'autres projets

Comme j'ai déjà pu l'évoquer. Mon stage ne s'est pas limité aux différents objectifs et travaux que j'ai pu lister. J'ai déjà évoqué avoir pu participer à du débuggage important sur mes codes mais aussi souvent sur des codes en lien avec les travaux de mon collègue Khatib Bahaddi. Un travail relativement important qui m'a été donné que nous allons essayer de détailler (sans trop détailler tout de même par souci de volume) et encore une fois sans pouvoir rentrer dans le détail et divulguer des morceaux du code.

Ce petit travail consistait à calculer un ensemble de positions de satellites, cela en considérant le récepteur statique avec position connue afin de vérifier le bon fonctionnement du code à la fin. Le code principal lisait alors d'abord les pseudo-distances et éphémérides à partir de données collectées puis il y avait un tri pour ne garder que les sa-

tellites utilisables vis-à-vis du récepteur (donc que l'on considère visible). Puis, à partir de fonctions Matlab déjà existantes, on procédait aux calculs de des positions de ces mêmes satellites pour les stocker dans la grosse matrice qui sera le résultat final à analyser.

Pour détailler légèrement, il y avait deux fichiers à lire : un premier était le fichier d'observation du récepteur avec les dates des observations, les satellites visibles avec les pseudo-distances ainsi que leur constellation et des informations sur le récepteur lui-même ; le deuxième fichier contenait les éphémérides détaillés pour chaque satellite avec les semi-grands axes, excentricité, inclinaisons (que nous pouvons voir sur la figure suivante Fig. 3 [3]) et autres corrections ou temps de référence.

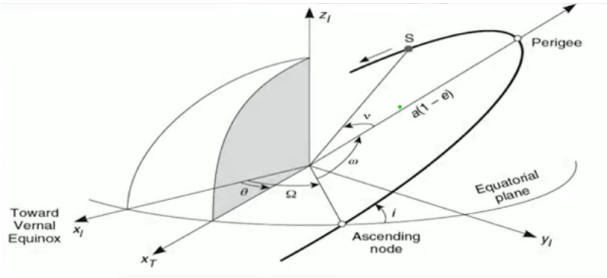


FIGURE 3 – Détails géométrie et calcul position satellite

Il a donc fallu travailler sur plusieurs petites fonctions : la première permettait assez simplement de sélectionner des satellites selon leur constellation (GPS, Galileo...), la deuxième permettait (comme nous avons pu le dire juste avant) de sélectionner les satellites pertinents pour le récepteur et même de sélectionner les $n$ meilleurs satellites, la troisième permettait enfin de calculer les positions ECEF précises des satellites à partir des pseudo-ranges et des éphémérides.

Mon collègue récupérait donc finalement un code capable d'extraire et traiter des données GPS et il s'en servait donc pour son déplacement de véhicules. Il obtenait alors des résultats tels que le suivant permettant de calculer approximativement la position d'un véhicule en mouvement (Fig. 4).

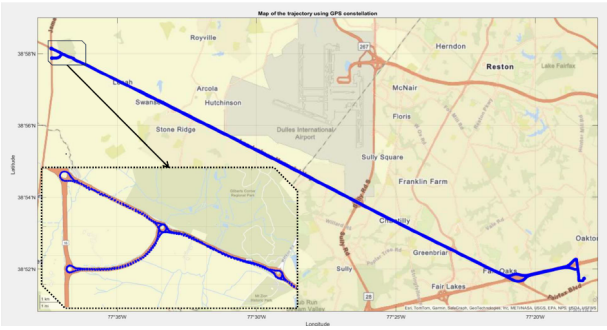


FIGURE 4 – Résultats obtenus par mon collègue en utilisant la fonction définie

## 4.3 Travaux finaux

### 4.3.1 Code et plus de théorie

Maintenant, intéressons-nous à ce qui a été réalisé durant ce stage. Il faut savoir que la majeure partie de mon temps était consacré à du codage, que ce soit par le développement du code lui-même pour mettre en place de nouveaux concepts ou par la résolution de bugs par exemple. Cependant, comme évoqué plus tôt, les travaux réalisés au sein du laboratoire sont liés de près ou de loin au gouvernement américain et à la défense américaine , un accord a donc été fait afin de ne pas divulguer le code ou des parties du code, en code brut ou en pseudo-code. Je m'efforcerai donc dans ce qui va suivre de détailler au maximum le travail fait, les équations, les concepts mis en place et même le modèle, tout en respectant cet accord. Notez par ailleurs que aucun accord n'a été fait vis-à-vis des résultats obtenus.

Tout d'abord, avant de rentrer en détails dans le travail fait, il est nécessaire d'expliquer encore quelques concepts simples (Je les explique maintenant et non dans la partie 4.1 puisqu'ils contiennent des équations que nous utilisons directement dans le code, cela permet d'expliquer mon travail sur le code). Il faut donc savoir que dans le cadre des systèmes de navigation par satellites, on utilise la combinaison GNSS/INS afin d'estimer au mieux la position de notre appareil. GNSS ou Global Navigation Satellite System permet le positionnement par satellite. Il en existe plusieurs, GPS pour les États-Unis, QZSS pour le Japon, Beidou pour la Chine, Galileo pour l'Union Européenne, GLONASS pour la Russie. Cependant, cela a ses limites notamment vis-à-vis de l'environnement et particulièrement en ville (qui est d'ailleurs un enjeu majeur au sein du laboratoire : l'étude et l'utilisation des systèmes de navigation dans des milieux à gratte-ciels comme le centre-ville de Chicago) ou encore par rapport à sa sensibilité aux attaques de Spoofing et Jamming que nous expliquerons sous peu. On utilise alors des centrales inertielles pour également estimer les paramètres de déplacement d'où l'intérêt de la combinaison.

Ce code nous permet de détecter les attaques de spoofing à l'aide d'un "innovation monitor" ou moniteur d'innovation. On compare nos mesures GNSS avec les prédictions du Filtre de Kalman, puis, à l'aide d'un Chi-squared monitor, on établit un test statistique cumulatif afin de détecter les anomalies. Ce test est lui-même comparé à un seuil, créant une alarme si dépassé. Il est donc important d'avoir un modèle d'erreur bien établi afin de ne pas créer de fausses alarmes ou d'en manquer des réelles.

Ainsi, nous pouvons alors détailler le code sur lequel j'ai travaillé. Il y a alors plusieurs étapes :

1. Initialisation des données et paramètres
2. Chargement et création de données
3. Estimation de position, vitesse et attitude
4. Combinaison GNSS et INS et correction d'erreurs
5. Simulation des erreurs
6. Détection d'anomalies

Pour mieux comprendre, nous allons donc parcourir ces différentes étapes en essayant encore et toujours de respecter l'accord de confidentialité et ne pas rentrer réellement dans le code :

(1) : On initialise l'aléatoire et les générateurs d'aléatoire, les paramètres définissant certains biais ou les erreurs comme par exemple $sig\_val$ définissant les écart-types du bruit résiduel, ainsi que les variables globales qui nous permettront de stocker les résultats comme la variable des probabilités de non-détection. On définit également la classe d'IMU utilisée (on en verra les détails plus tard), le temps d'initialisation de l'INS et de réaction après le début de l'attaque de spoofing (si attaque il y a) et le scénario de manière générale. On initialise également certaines fréquences d'échantillonnage, les horloges et les détails pour les satellites. Enfin, on donne les valeurs voulues aux différents flags, on définit notre moniteur d'innovation, la position initiale et le système de coordonnées.

(2) : On appelle de multiples scripts pour charger des données, générer les erreurs ou les données INS ou GNSS ou même initialiser certaines matrices de covariance.

Toutes les autres étapes se regroupent globalement. On démarre la boucle de Kalman [6, 4] en estimant $\overline{x}_k$ à partir de $\hat{x}_{k-1}$, de $\Phi_k$ la matrice de transition d'état et des différentes matrices modélisant le bruit, de même pour la covariance de l'erreur d'estimation d'état $\overline{P}_k$ :

$$\overline{x}_k = \Phi_k \hat{x}_{k-1} + \Gamma_{w_k} w_k \tag{2}$$

$$\overline{P}_k = \Phi_k \hat{P}_{k-1} {\Phi^T}_k + \Gamma_{w_k} w_k \Gamma^T_{w_k} \tag{3}$$

On récupère les mesures GNSS sous le format suivant avec $H_k$ la matrice d'observation et $v_k$ le bruit de mesure :

$$z_k = H_k \overline{x}_k + v_k \tag{4}$$

Alors, on procède à une estimation de l'état $\hat{x}_k$ :

$$\hat{x}_k = \overline{x}_k + K_k \gamma_k \tag{5}$$

Avec le gain de Kalman :

$$K_k = \overline{P}_k \cdot H'_k \cdot \left(H_k \cdot \overline{P}_k \cdot H'_k + V_k\right)^{-1} \tag{6}$$

Et parce que l'innovation au temps k est définie par la différence entre d'abord les mesures réelles avec les pseudodistances GNSS comprenant donc le bruit environnant et donc une éventuelle attaque puis avec les prédictions et estimations du filtre de Kalman :

$$\gamma_k = z_k - H_k \overline{x}_k \tag{7}$$

Enfin, on termine avec le calcul de $\hat{P}_k$ pour la boucle suivante. En bref, tout cela se résume avec la figure 5 [4]

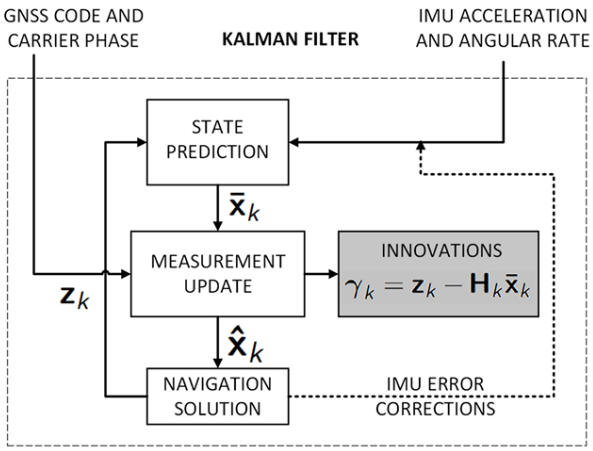


FIGURE 5 – Architecture du filtre de Kalman avec GNSS/INS

En suivant les formules qui suivent (12,13,14), on a enfin le test statistique et la détection d'attaque que nous allons détailler maintenant. Avant cela, il nous faut définir d'autres éléments.

En effet, notre problème majeur dans ce qui va suivre est donc la multiplicité des erreurs externes qui apparaissent dans les équations de mesure GNSS et INS. Les erreurs GNSS qui nous intéressent sont : Ionosphérique (peut faire varier la position de dizaines de mètres dû au passage dans la couche de l'atmosphère), troposphérique (peut faire varier la position de quelques mètres du au passage dans une couche inférieure de l'atmosphère), multi-trajets (du à la réflexion du signal sur les surfaces environnantes comme les bâtiments), horloge satellite (apparaît dans les mesures de pseudo-distance satellite-appareil). Les erreurs INS sont : biais de l'accéléromètre et du gyroscope, bruit de mesure de l'accéléromètre et du gyroscope. Des variations de ces erreurs dans notre modèle pourraient créer des problèmes de fiabilité.

Détaillons alors les équations du modèle que nous venons de décrire. Ces équations apparaissent donc dans le code et on y comprend l'importance de l'étude des erreurs. Commençons par détailler les équations de mesures GNSS. On a d'abord [7] :

$$\begin{bmatrix} \rho \\ \lambda\phi \end{bmatrix} = \begin{bmatrix} p \\ p \end{bmatrix} + \begin{bmatrix} c\,(dt_{rc} - dt_{sv}) \\ c\,(dt_{rc} - dt_{sv}) \end{bmatrix} + \begin{bmatrix} I_\rho \\ -I_\phi \end{bmatrix} + \begin{bmatrix} T_\rho \\ T_\phi \end{bmatrix} + \begin{bmatrix} m_\rho \\ m_\phi \end{bmatrix} + \begin{bmatrix} 0 \\ \lambda N_\phi \end{bmatrix} + \begin{bmatrix} v_{th_{(\rho)}} \\ v_{th_{(\phi)}} \end{bmatrix} \tag{8}$$

Avec :

- $\rho$ pseudo-distance du code (distance apparante satellite-récepteur)
- $\lambda\ \phi$ Phase porteuse (carrier)
- $p$ vraie distance satellite-récepteur
- $c\,(dt_{rc} - dt_{sv})$ Biais d'horloge avec $c$ vitesse de la lumière, $dt_{rc}$ erreur d'horloge du récepteur, $dt_{sv}$ erreur d'horloge du satellite
- $I$ erreur ionosphérique (code $\rho$ et carrier $\phi$)
- $T$ erreur troposphérique (code $\rho$ et carrier $\phi$)
- $m$ erreur multi-trajet (code $\rho$ et carrier $\phi$)
- $\lambda N_\phi$ ambiguïté de phase
- $v$ autres bruits

On précisera cependant que l'erreur de multi-trajets $m$ suit un processus de Gauss-Markov d'Ordre 1 :

$$\dot{m} = -\frac{1}{\tau_m} m + v_m \tag{9}$$

Avec :

- $\dot{m}$ dérivée de l'erreur m
- $\tau_m$ constante de temps que nous réutiliserons par la suite
- $v_m$ bruit blanc gaussien

Enfin, détaillons désormais les équations de mesure IMU :

$$\widetilde{u} = u^* + b_c + b + \eta_u \tag{10}$$

Avec :

- $\widetilde{u}$ la valeur mesurée
- $u^*$ la valeur réelle
- $b_c$ le biais fixe
- $b$ le biais variable
- $\eta_u$ le bruit blanc

Une fois de plus, on précise que le biais variable $b$ suit un processus de Gauss-Markov d'Ordre 1 :

$$\dot{b} = -\frac{1}{\tau_b} b + v_b \tag{11}$$

Avec :

- $\dot{b}$ dérivée de l'erreur b

- $\tau_b$ constante de temps que nous réutiliserons par la suite
- $v_b$ bruit blanc gaussien

C'est donc à partir de ce modèle que le filtre de Kalman est appliqué : il intègre les mesures GNSS brutes pour estimer et corriger les erreurs INS, améliorant ainsi la précision de la navigation.

Après avoir rapidement définis ces termes, il est également nécessaire de se focaliser sur l'élément important du code et du modèle à savoir le test statistique. En effet, c'est à partir de cela que l'on déclenche les alarmes : elles sont activées en utilisant un quotient entre ce test statistique et un seuil. On définit alors dans un premier temps le vecteur d'innovation au temps k selon u [4] :

$$\gamma_k^u = \mathbf{u}^T \mathbf{H}_k^T \mathbf{S}_k^{-1} \gamma_k \tag{12}$$

Avec :

- $\gamma_k = \mathbf{z}_k - \mathbf{H}_k \overline{\mathbf{x}}_k$
- $u$ vecteur de projection unitaire
- $z_k$, $H_k$, $S_k$ et $x_k$ proviennent du filtre de Kalman

En pratique, ce vecteur permet donc de réaliser notre test statistique et de déterminer si les données GNSS/INS sont cohérentes avec le modèle attendu ou si il y a une attaque. On définit justement ce test statistique cumulatif en utilisant $\gamma_k^u$ de la manière suivante :

$$q_N = \sum_{k=1}^{N} \left(\gamma_k^u\right)^T \gamma_k^u \tag{13}$$

Avec $\gamma_k^u$ que nous venons tout juste de définir et $N$ la taille de l'échantillon. Cette méthode permet ainsi de détecter des effets faibles dans le temps comme ce peut être le cas dans le cadre des attaques de Spoofing selon la définition établie plus tôt. Enfin, la définition de l'étape de vérification du déclenchement d'alarme apparaît enfin :

- $q_k > T_k^2$ alors le moniteur d'innovation crée une alerte
- $q_k \leq T_k^2$ alors rien ne se passe

Notons par ailleurs que le seuil a été défini par :

$$T_k = F_\Gamma^{-1}\left(P_{FA} \,\middle|\, \frac{k}{2}, 2\right) \tag{14}$$

Avec :

- $P_{FA}$ la probabilité d'obtenir une fausse alerte
- $k$ l'étape
- $F_\Gamma^{-1}$ l'inverse de la fonction de répartition CDF de la distribution gamma

### 4.3.2 Paramètres GNSS : problèmes et analyses

Une des finalités de mon stage était donc d'analyser individuellement l'influence des variations des paramètres définissant les erreurs extérieures apparaissant dans les équations de mesure GNSS qui ont été définies auparavant. L'idée était donc de se focaliser sur les différentes composantes de temps de ces mêmes erreurs, en particulier celles associés au Processus de Gauss-Markov d'ordre 1, aussi noté GMRP pour "First Order Gauss-Markov Random Process", que l'on retrouve dans notre Gamma Innovation Monitor. En plus de ces composantes de temps, il était aussi pertinent de s'intéresser aux écarts-types de ces erreurs. Une petite précision qui permettra de mieux comprendre les phénomènes et résultats que nous verrons par la suite : les composantes de temps des erreurs modélisent l'évolution des erreurs, comment elles se propagent dans le temps, tandis que les écarts-types modélisent assez logiquement l'amplitude des variations des erreurs.

Dans notre modèle, ainsi que dans tous les modèles sur lesquels j'ai travaillés durant le stage, il y a de nombreuses sources d'erreurs : ionosphérique, troposphérique, ainsi que des erreurs d'horloge des satellites et de multi-trajets. A partir de tout ce qui avait été fait jusqu'à présent, nous pourrons étudier l'influence des composantes associées aux erreurs que nous venons de lister.

Connaissant l'importance de l'intégrité dans le cadre de nos systèmes de navigation, et donc de détecter les attaques extérieures sur notre système, il est alors crucial d'avoir un modèle d'erreur avec une précision optimale. En effet, il nous faut être le plus proche possible d'un système qui nous renvoie le moins de fausses alarmes possibles et qui manque le moins de détections possible. C'est pour ces raisons qu'il nous faut évaluer nos paramètres individuellement.

Pour cela, nous devons alors estimer les limites des différentes composantes que nous avons mentionnées plus tôt, limites qui serviront ainsi de références pour notre modèle d'erreur.

La Table 1 montre les valeurs nominales ainsi que les limites supérieures et inférieures utilisées dans le cadre de notre simulation d'erreurs GNSS. Elles correspondent à 10% et 1000% de nos valeurs nominales. Le résultat est la Table 1 suivante :

| | Paramètres | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | $\tau_{iono}$ $(hr)$ | $\sigma_{iono}$ $(m)$ | $\tau_{mp}$ $(s)$ | $\sigma_{mp}$ $(m)$ | $\tau_{tropo}$ $(hr)$ | $\sigma_{tropo}$ $(m)$ | $\tau_{sat}$ $(hr)$ | $\sigma_{sat}$ $(m)$ |
| Valeurs nominales | 40 | 8.991 | 25 | 4.970 | 20 | 0.09 | 5 | 1.8 |
| Limite d'incertitude inférieure | 4 | 0.8991 | 2.5 | 0.497 | 2 | 0.009 | 0.5 | 0.18 |
| Limite d'incertitude supérieure | 400 | 89.91 | 250 | 49.70 | 200 | 0.9 | 50 | 18 |

TABLE 1 – Constantes de temps et écarts-types pour les différentes erreurs

C'est alors particulièrement intéressant de se focaliser sur la rapport entre le test statistique et le seuil. En effet, comme nous pouvons le voir avec l'illustration des performances du moniteur d'innovation, un rapport du test et du seuil plus grand que 1

nous indiquerait donc qu'il y a une alerte tandis que un rapport plus petit que 1 nous indiquerait au contraire qu'il n'y pas d'attaque détectée et donc pas d'alerte. Ainsi, une composante de temps ou un écart-type mal évalué, trop grand ou trop petit, pourrait mener à de grandes dégradations de la performance. Nous pourrions alors avoir des fausses alertes quand il n'y a pas d'attaque ou des détections d'attaques manquées lorsqu'il y a bien une attaque.

En partant de la courbe paramétrée avec la valeur nominale, nous devrions donc pouvoir assez simplement évaluer l'influence des différentes composantes. Pour cela, nous fixons toutes les composantes à leur valeur nominale, à l'exception d'une, dans l'exemple du dessous il s'agit donc de la composante de temps de l'erreur ionosphérique. Nous la faisons alors varier pour étudier l'influence de la courbe, en particulier son maximum qui nous donne une information direct vis-à-vis du seuil. Les deux figures de la Figure 6 servent d'exemple pour mieux comprendre ce qui nous intéresse et ce que nous analysons.

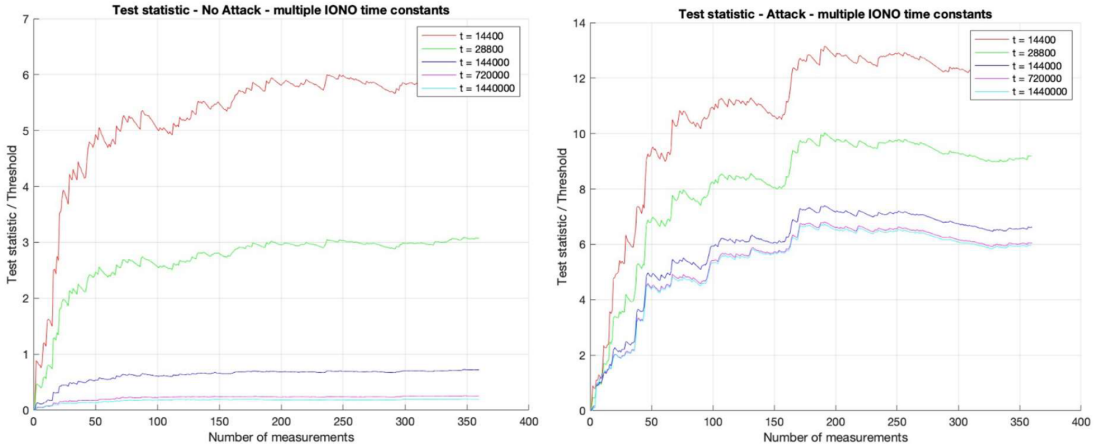


FIGURE 6 – No attack case results

Si l'on se réfère à la figure de gauche dans la Figure 6, la courbe représentant le rapport devrait donc idéalement et assez logiquement se situer en dessous du seuil de 1 et ne certainement pas le dépasser au risque de déclencher une alerte alors que nous sommes bien dans le cas sans attaque. Dans notre cas, la courbe de la valeur nominale correspond au trait bleu foncé associé à la valeur $t = 144000$, tandis que la courbe rouge pour $t = 14400$ est celle de la limite inférieure, puis la courbe cyan pour $t = 1440000$ est celle de la limite supérieure.

On commence donc par faire varier les paramètres GNSS un par un dans un cas sans attaque. D'abord, la composante de temps $\tau_{iono}$ et l'écart-type $\sigma_{iono}$ de l'erreur ionosphérique. On regarde les figures telles que celles obtenues dans la Figure 6, à quel point le maximum augmente ou diminue et surtout, toujours dans le cas sans attaque, s'il passe au dessus du seuil 1. Puis, on réalise donc ce même processus pour toutes les autres composantes listés dans le tableau.

Dans le case d'une composante de temps, quelle qu'elle soit, les observations sont globalement toujours les mêmes. On note que pour une valeur plus petite de la composante,

les courbes vont avoir tendance à excéder en terme de maximum la courbe de référence et souvent même à passer au dessus de 1, toujours avec de nombreuses variations. Cela semble s'expliquer par le fait qu'il y a des plus grandes variations dans les erreurs (cf. GMRP 1), ce qui influence l'innovateur gamma, suggérant une attaque. Au contraire, une plus grande valeur nous donne une courbe dont le maximum sera généralement en dessous de celui de la courbe de référence, s'approchant davantage de 0 lorsque la valeur augmente.

Dans le cas de l'étude des écarts-types, des observations similaires peuvent être faites avec une différence majeure cependant. En effet, dans ce cas, des valeurs plus faibles de l'écart-type donne des valeurs du maximum de la courbe plus faible et inversement. C'est une conséquence directe du modèle théorique que nous avons vu plus tôt et cela était donc attendu. Il doit néanmoins être aussi noté, et nous l'observerons également par la suite, que pour 1000% de la valeur nominale de l'écart-type, les valeurs maximales peuvent être parfois dix fois plus grandes, nous donnant donc uné idée de l'influence des différents paramètres, mais nous reviendrons dessus avec les graphes qui suivent.

Pour mieux comprendre cette influence des paramètres que nous avons déjà tant évoquée, intéressons-nous au pourcentage du changement du rapport entre le test statistique et le seuil, nous l'appellerons $q_k$. Pour cela, on regarde le maximum des courbes lorsque la limite inférieure ou supérieur est utilisée, puis on le compare à celui de la courbe de la valeur nominale et on en déduit le pourcentage. Cela nous donne alors la Figure 7 et la Figure 8.

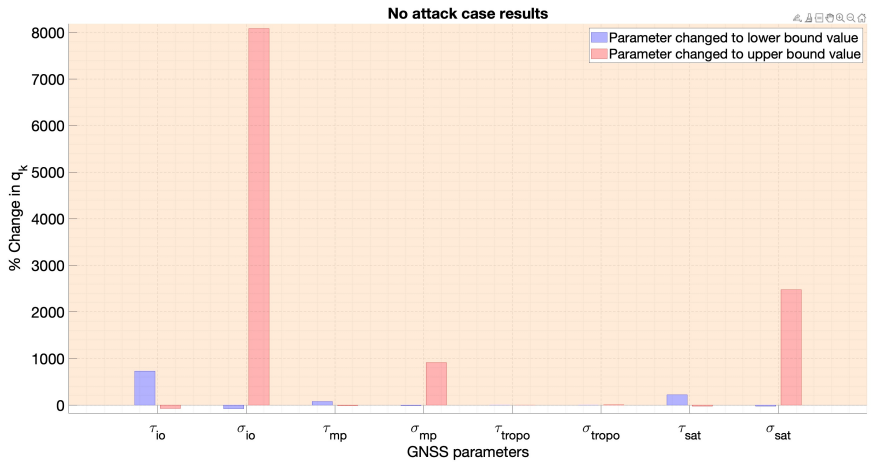


FIGURE 7 – No attack case results

Pour ces deux figures, les limites de la Table 1 ont été utilisées, le rapport $q_k$ évolue donc en comparaison au rapport obtenu avec la valeur nominale. Ces variations ont donc une signification importante que l'on a déjà pu évoquer mais qui prend désormais sens :

— Sans attaque : une augmentation dans la zone orangée pourrait nous donner une fausse alerte

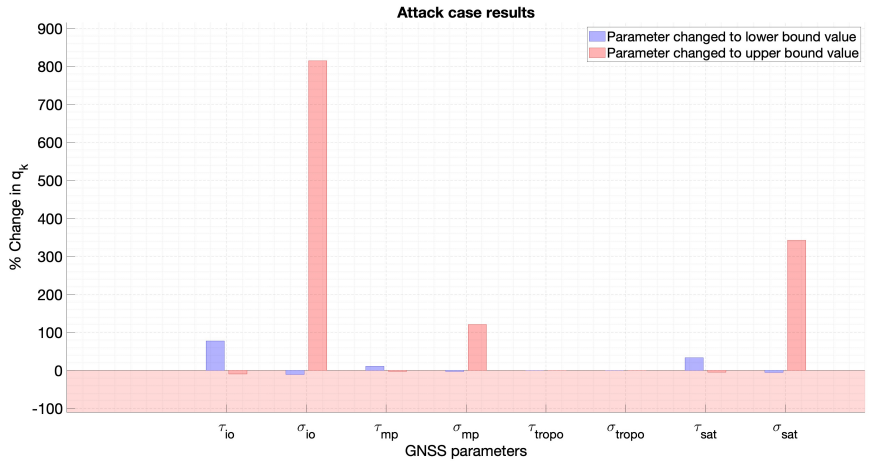


FIGURE 8 – Attack case results

— Avec attaque : une diminution dans la zone rouge pourrait manquer l'alerte en cas d'attaque

Assez logiquement, nous répétons des observations que nous avons déjà pu faire. D'abord, sans attaque, la plus grande influence provient d'une augmentation de l'écart-type $\sigma_{io}$ de l'erreur ionosphérique atteignant 8086% d'augmentation dans le rapport $q_k$ pour la limite supérieure. Pour l'écart-type $\sigma_{mp}$ lié au multi-trajets, on obtient 913%, et 2474% pour $\sigma_{sat}$ de l'erreur d'horloge des satellites. Les autres paramètres qui semblent avoir une influence notable sont lorsque l'on atteint les limites inférieures pour les composantes de temps $\tau_{io}$ de l'erreur ionosphérique avec 731% d'augmentation pour $q_k$ et celle de l'erreur d'horloge du satellite $\tau_{sat}$ avec 219%. Toutes les autres composantes nous donnent des changements inférieurs à 80%.

Avec attaque, les composantes intéressantes semblent être les mêmes et l'allure globale du graphe reste la même. Sans trop détailler, $\sigma_{io}$ donnent 814%, $\sigma_{mp}$ 120%, $\sigma_{sat}$ 342%. Pour les composantes de temps, on obtient 77% pour $\tau_{io}$, 33% pour $\tau_{sat}$ et tout le reste est en dessous de 12%.

Dans ce contexte, il est ainsi important de trouver le bon équilibre entre continuité et intégrité. En effet, selon le cas et donc selon la figure (Fig.7 ou Fig.8), une augmentation ou une diminution pourrait créer une fausse alerte ou rater une détection comme nous l'avons dit à plusieurs reprises. Les figures illustrent désormais parfaitement l'importance de ces phénomènes : l'augmentation de $q_k$ provoquée par une diminution de $\tau_{io}$ ne poserait en apparence pas de problème dans le cas avec attaque de la Figure 8 mais pourrait avoir un impact majeur dans le cas sans attaque de la Figure 7 et pourrait créer ces fameuses fausses alertes.

Ainsi, certains paramètres demandent une attention particulière lorsqu'il s'agit de les estimer et donc, comment mentionné précédemment, un entre-deux est certainement nécessaire pour maintenir continuité et intégrité : ne pas signaler trop d'attaques alors qu'il n'y en a pas tout en ratant le moins possible.

### 4.3.3 Paramètres INS : problèmes et analyses

**Détails des IMU**

Avant de rentrer dans le détail des paramètres INS, il est important de définir exactement comment sont nos IMU (Inertial Measurement Unit ou Unité de Mesure Inertielle). En effet, nos IMU permettent de mesurer des accélérations linéaires à partir des accéléromètres et des vitesses de rotation à partir des gyroscopes. Néanmoins il y a plusieurs paramètres donnés dans le code pour définir un IMU :

- VRW pour Velocity Random Walk : bruit blanc des mesures de l'accéléromètre
- ARW pour Angular Random Walk : bruit blanc des mesures du gyroscope
- ABIS pour Accelerometer Bias Instability : dérive du biais de l'accéléromètre
- GBIS pour Gyroscope Bias Instability : dérive du biais du gyroscope
- ABT pour Accelerometer Bias Time Constant : constante du processus de Gauss-Markov d'ordre 1 (cf plus haut) pour l'accéléromètre. Une grande valeur permet une constance, une petit implique des variations aléatoires.
- GBT pour Gyroscope Bias Time Constant : constante du processus de Gauss-Markov d'ordre 1 (cf plus haut) pour le gyroscope. Une grande valeur permet une constance, une petit implique des variations aléatoires.
- ABR pour Accelerometer Bias Repeatability : biais maximum possible entre deux utilisations de l'accéléromètre
- GBR pour Gyroscope Bias Repeatability : biais maximum possible entre deux utilisations du gyroscope

Les trois IMU que nous allons utiliser par la suite sont HG9900, STIM300 et AUTO-1 dont voici les caractéristiques dans le tableau suivant :

| **Caractéristique** | **HG9900** | **STIM300** | **AUTO-1** |
|---|---|---|---|
| VRW ($m/s/\sqrt{hr}$) | 0.0143 | 0.12 | 0.18 |
| ARW ($deg/\sqrt{hr}$) | 0.001 | 0.5 | 0.2 |
| ABIS (mg) | 0.01 | 0.0643 | 0.04 |
| GBIS (deg/hr) | 0.0035 | 3 | 7 |
| ACCEL_BIAS_TAU (s) | 3600 | 3600 | 3600 |
| GYRO_BIAS_TAU (s) | 3600 | 3600 | 3600 |
| ABR (mg) | 0.025 | 0.75 | 1.5 |
| GBR (deg/hr) | 0.003 | 4 | 120 |

TABLE 2 – Comparaison des IMU

On constate alors déjà les différentes de qualité des IMU. On voit clairement que le HG9900 est le meilleur IMU et nous donnera sans doute les meilleurs résultats. Néanmoins, les deux autres présentent des paramètres meilleurs que l'autre donc on peut s'attendre à des résultats équivalents en certains points.

**HG9900**

Intéressons-nous désormais à l'influence des paramètres INS (Inertial Navigation System ou Système de navigation inertielle). D'abord, il nous faut choisir une "Grade of IMU" ou Classe de centrale inertielle, à savoir HG9900. De la même manière que pour les paramètres GNSS, on fixe les paramètres à l'exception de celui que nous étudions pour analyser les changements dans le rapport test statistique et seuil $q_k$. On peut déjà s'attendre à des changements pour $q_k$ plus faibles avec HG9900 que pour les classes de centrale inertielle suivantes, qui seront de moins bonne qualité.

Les paramètres qui pourraient nous intéresser dans le cadre des paramètres INS sont multiples, nous nous focaliserons sur les suivants : la constante de temps $ab\_tau$ et l'écart-type $ab\_sig$ du biais de l'accéléromètre, la constante de temps $gb\_tau$ et l'écart-type $gb\_sig$ du biais du gyroscope, le bruit de mesure $an$ de l'accéléromètre et $gn$ du gyroscope. Avec la simple même méthode que précédemment, on estime les limites des différentes composantes. La Table 3 montre les valeurs nominales ainsi que les valeurs inférieures et supérieures (10% et 1000%).

| | Parameters | | | | | |
|---|---|---|---|---|---|---|
| | $\tau_{accel\_bias}$ $(s)$ | $\sigma_{accel\_bias}$ $(m)$ | $\tau_{gyro\_bias}$ $(s)$ | $\sigma_{gyro\_bias}$ $(m)$ | $\sigma_{dev\_accel}$ $(m)$ | $\sigma_{dev\_gyro}$ $(m)$ |
| VN | 3600 | $9.8067 \times 10^{-5}$ | 3600 | $1.6968 \times 10^{-8}$ | $2.3833 \times 10^{-4}$ | $2.9089 \times 10^{-7}$ |
| Sup | 360 | $9.8067 \times 10^{-6}$ | 360 | $1.6968 \times 10^{-9}$ | $2.3833 \times 10^{-5}$ | $2.9089 \times 10^{-8}$ |
| Inf | 36000 | $9.8067 \times 10^{-4}$ | 36000 | $1.6968 \times 10^{-7}$ | $2.3833 \times 10^{-3}$ | $2.9089 \times 10^{-6}$ |

TABLE 3 – Valeurs des composantes utilisées pour les paramètres INS

De la même manière que pour les paramètres GNSS, on procède à l'analyse des changements de $q_k$. Les deux cas, attaque ou non, sont représentés par les figures 9 et 10

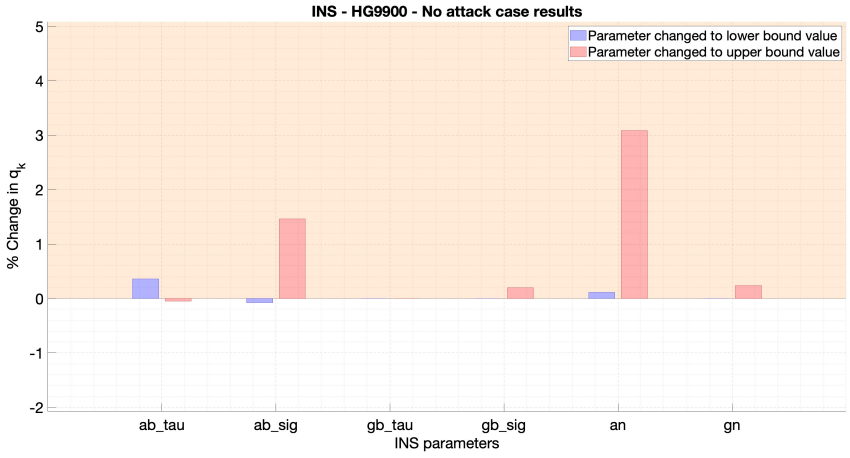


FIGURE 9 – No attack case results - HG9900

La première différence majeure par rapport à la partie précédente est visible rapidement. En effet, on constate que les changements de $q_k$ sont beaucoup plus faibles qu'auparavant. En absence d'attaque, on ne dépasse pas les 5%. Dans le cas d'une attaque, les

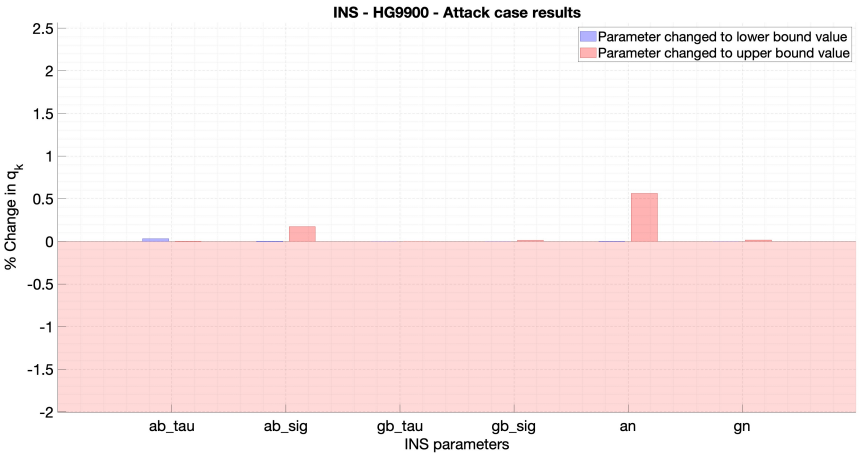


FIGURE 10 – Attack case results - HG9900

changements sont encore plus faibles et on reste en dessous de 1%. Néanmoins, il doit être noté que les deux influences les plus importantes sont provoquées par des augmentations de l'écart-type *ab_sig* du biais de l'accéléromètre et du bruit de mesure de l'accéléromètre *an*. Quand il y a une attaque, les influences observées sont les mêmes mais donc à une échelle plus faible.

### STIM300

Changeons alors l'IMU pour toujours étudier l'influence des paramètres dans différentes conditions techniques. On étudie les variations des mêmes paramètres et on obtient les figures 11 et 12 ci-dessous.

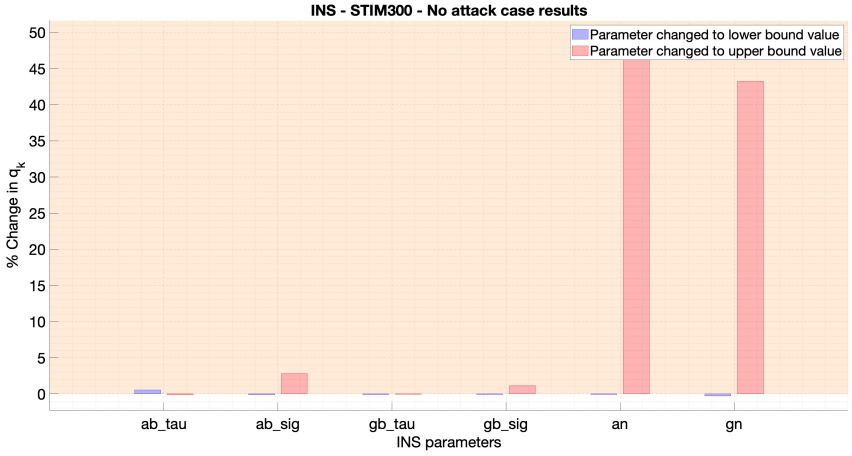


FIGURE 11 – No attack case results - STIM300

On constate alors qu'une augmentation aux valeurs limites supérieures pour le bruit de mesure de l'accéléromètre *an* et du gyroscope *gn* provoquent des changements importants dans le ratio du test statistique, allant jusqu'à 50% en absence d'attaque et 8% avec attaque. Bien supérieur à ce que nous avions avec le grade of IMU précédent HG9900 qui était par ailleurs de bien meilleur qualité.

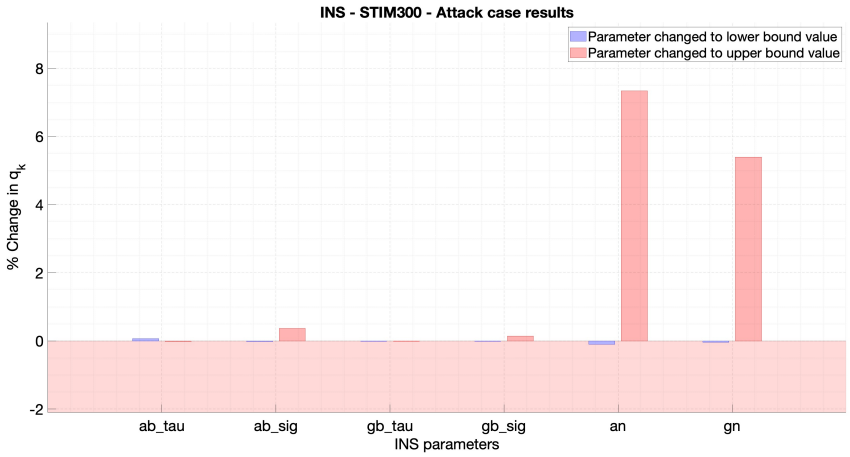


FIGURE 12 – Attack case results - STIM300

## AUTO-1

Dernier IMU et le plus mauvais : AUTO-1. De la même manière que précédemment, on obtient les figures 13 et 14.

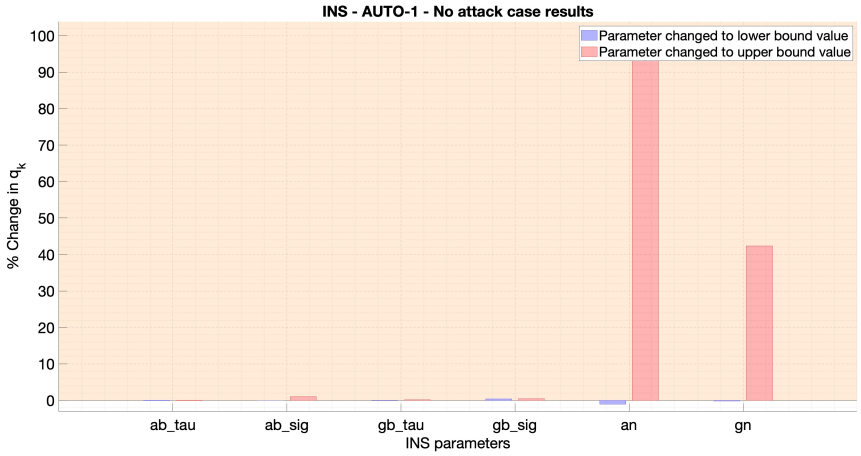


FIGURE 13 – No attack case results - AUTO-1

Les observations sont encore plus flagrantes et surtout similaires à ce que avons pu voir avec STIM300. On obtient, toujours pour les deux mêmes paramètres *an* et *gn* que précédemment, des grandes fluctuations atteignant 100% de la valeur nominale dans le cadre d'une attaque pour *an*, 50% pour *gn*.

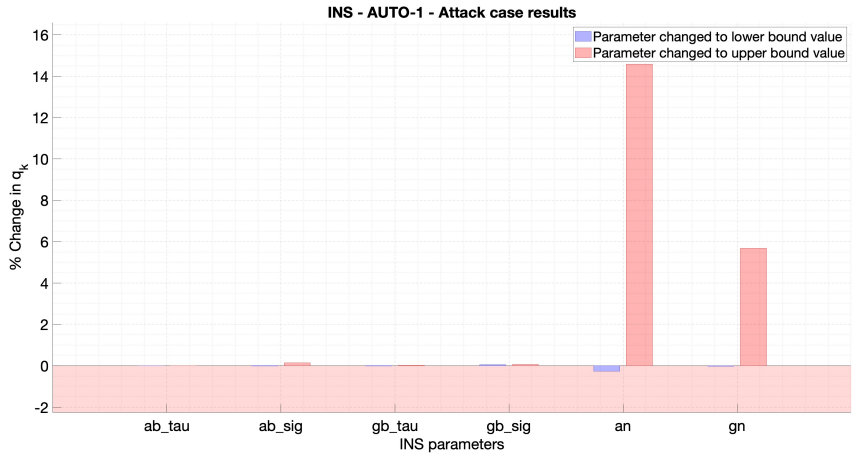


FIGURE 14 – Attack case results - AUTO-1

### Recapitulatif

Ainsi, les différents graphes que l'on a pu voir jusqu'à présent mettent en lumière des résultats particulièrement intéressants : pour les paramètres INS les plus influents, ils provoquent tout de même beaucoup moins de changements pour $q_k$ que pour les paramètres GNSS les plus influents. On constate surtout que les changements sont beaucoup plus importants dans le cas sans attaque, pouvant donc amener à davantage de fausses alertes. L'analyse des différentes IMU mettent aussi en lumière les paramètres qui nécessitent une grande attention à savoir le bruit de mesure *an* de l'accéléromètre et *gn* du gyroscope. Enfin, assez logiquement, un IMU de meilleure qualité nous donne des changements plus faibles, preuve de l'intégrité de la centrale inertielle.

Les figures suivantes (Fig. 15 et 16), faisant la comparaison des différentes classes d'IMU dans la même figure, illustrent parfaitement ce qui a été vu. D'abord sur les paramètres les plus influents, puis sur la classe d'IMU et aussi pour la comparaison attaque et sans attaque.

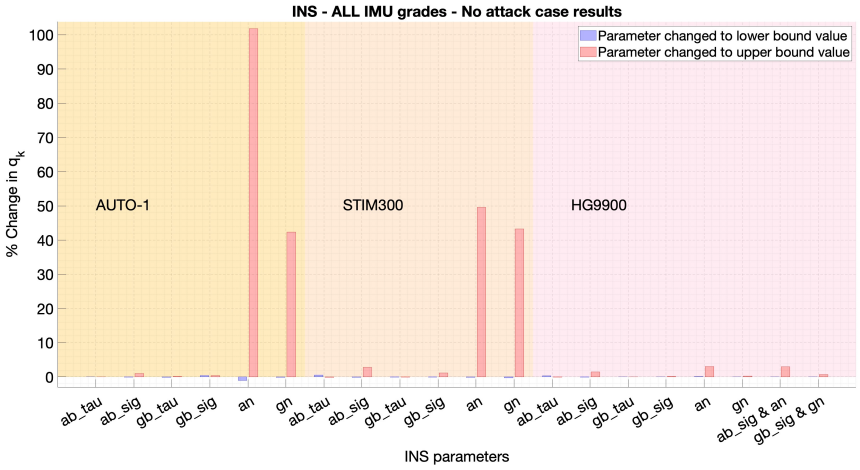


FIGURE 15 – All grades of IMU - No attack case

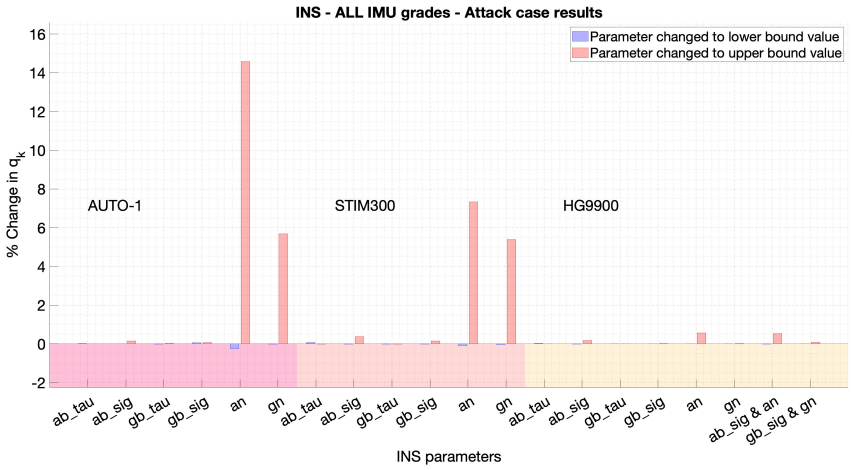


FIGURE 16 – All grades of IMU - Attack case

# 5 Conclusion

Ainsi, à travers ce rapport nous avons donc pu retracer ce qui a été fait durant ce stage à l'Illinois Institute of Technology de Chicago. Tout cela a été fait avec l'aide de Birendra Kujur, délégué encadrant choisi par Boris Pervan. Dans un premier temps, il y a donc eu un apprentissage dont nous avons pu retracer certaines étapes notamment celles des pseudo-durées et pseudo-distances entre un satellite et un receveur mais également des suppléments en télécommunication. Ensuite, nous avons pu évoquer une grande partie de ces 6 mois à savoir le code et la théorie qui l'encadre. Code qui pouvait concerner le modèle que nous avons établi ou même parfois des morceaux pouvant aider mon collègue Khatib dans son travail avec le calcul de position de satellite. Nous sommes alors arrivés à l'étude de notre système de navigation et l'étude des différents paramètres. De cette étude, nous pouvons en tirer l'importance de la fiabilité et de la sécurité surtout lorsqu'il s'agit d'attaques externes comme du jamming ou du spoofing. On connaît désormais les paramètres importants et cette nécessité d'avoir un IMU de bonne qualité ainsi que celle de réaliser un entre-deux pour maintenir continuité et intégrité. Dans une utilisation pratique, il est important de calibrer nos paramètres.

Au-delà de ces aspects techniques, je noterai également en conclusion l'importance de ce stage dans le cadre de ma formation. D'abord, j'ai été plongé dans un environnement complètement différent de celui que j'ai l'habitude de fréquenter. Un environnement américain qui a des attentes différentes et de nombreuses dates limites, imposant une certaine pression pour non seulement travailler mais trouver des solutions parfois dans des délais courts. Évidemment, cela m'a aussi permis de renforcer ma confiance et mon niveau en anglais. L'autre aspect qui selon moi a été important est l'utilisation de Kalman et d'éléments des cours d'Inertiel dans un contexte différent. Si le second cours a moins été utilisé, le premier était au cœur du stage et m'a permis de me renforcer dans un domaine où je me considérais en retard par rapport à d'autres élèves de ma promotion. Enfin, cela m'a aussi amené l'idée que le domaine des voitures autonomes présente des problématiques

beaucoup plus diverses que ce que je pouvais m'imaginer. En effet, en comparaison à la robotique autonome classique que j'ai pu voir jusqu'à présent, l'aspect de la sécurité est davantage mis en avant. Le recul obtenu après le stage me fait conclure que ce n'est pas un domaine prioritaire à l'avenir bien que le stage fut une bonne expérience en soi.

Enfin, je conclurai en remerciant Monsieur Boris Pervan pour sa confiance et l'opportunité qu'il m'a donné, alors même que mon CV ne présentait pas de compétences directes et claires en système de navigation par satellite. Je remercie également Birendra Kujur pour son aide quotidienne. Pour terminer, je remercie Khatib Bahaddi qui m'a guidé lors de mon apprentissage et avec qui j'ai travaillé au quotidien tout au long de ces six mois de stage.

# 6 Annexes

# Références

[1] Voiture-autonome.net, *L'évolution des voitures autonomes en 2025 : progrès, défis et perspectives*, 27 février 2025. `https://www.voiture-autonome.net/constructeurs/voiture-autonome-resume-2025`

[2] Illinois Institute of Technology, *NavLab – Navigation Laboratory*, `http://www.navlab.iit.edu/`

[3] Stanford Center for Position, Navigation and Time, *GPS MOOC (Massive Open Online Course)*, 2014. `https://scpnt.stanford.edu/about-scpnt/gps-mooc-massive-open-online-course`

[4] Kujur, B., *Satellite Spoofing and Fault Detection for Integrated GNSS/INS Systems*, PhD Dissertation, August 2025

[5] Ahmed, S., Khanafseh, S., Pervan, B., *GNSS Spoofing Detection based on Decomposition of the Complex Cross Ambiguity Function*, INSIDE GNSS, Sep–Oct 2022 Edition, Protecting PNT : Mitigating Jamming and Spoofing Threats

[6] Brown, R. G., Hwang, P. Y. C., *Introduction to Random Signals and Applied Kalman Filtering : With MATLAB Exercises*, 4th Edition, Wiley, 2012

[7] Gallon, E., Khanafseh, S., Joerger, M., Pervan, B., *Performance Assessment of Fault Free Recursive ARAIM with High-Integrity Time-Correlated Measurement Error Models*, Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022), Denver, Colorado, September 2022