Systèmes de localisation en milieu contraint et de leurre GNSS

Alexandre Vervisch-Picois

INSTITUT POLYTECHNIQUE DE PARIS

Systèmes de localisation en milieu contraint et de leurre GNSS

Dossier pour l'obtention de l'Habilitation à Diriger des Recherches de l'Institut Polytechnique de Paris

d'Alexandre Vervisch-Picois

Le 20 octobre 2022 devant le jury composé de

Rapporteurs:
Bertrand Merminod, Professeur à l'Ecole Polytechnique Fédérale de Lausanne
Kyle O' Keef, Professeur au Département Géomatique de l'Université de Calgary
Valérie Renaudin, Directrice de recherche à l'Université Gustave Eiffel

Examinateurs:
Aziz Benlarbi Delaï, Professeur des Universités, Directeur L2E Paris Sorbonne
Pascal Chevalier, Professeur titulaire de la chaire électronique au CNAM
René Junior Landry, Professeur au Département Génie Electrique de l'ETS de Montréal

Sommaire

I. Dossier Administratif

1.1 Curriculum Vitae détaillé

Alexandre Vervisch-Picois

Né le 26 Février 1978 à Rouen

98 Boulevard de la Reine

78000 Versailles

Portable : 06 14 40 65 67

Alexandre.vervisch-picois@telecom-sudparis.eu

1.1.1 Études

09/2007-07/2010	Doctorat de l'Institut National des Télécommunications, Ecole doctorale de l'Université Pierre et Marie Curie. Spécialité : Electronique, Informatique, Télécommunications. "Etude de systèmes de positionnement en intérieur utilisant des mesures de phase du code ou de phase de la porteuse de signaux de navigation par satellites."
09/1999-06/2004	Institut National des Télécommunications, école d'ingénieur, EVRY.
03/2002	First Certificate of Cambridge. Mention B.
09/1998-06/1999	Classes préparatoires de PC* au lycée Charlemagne, PARIS.
09/1996-06/1998	Classes préparatoires de PCSI puis PC* au lycée Masséna, NICE.
06/1996	Baccalauréat S. Mention Bien

1.1.2 Expérience professionnelle

1/01/2013	Intégration au laboratoire UMR5157 SAMOVAR du CNRS
Depuis 10/2012	Maître de Conférences à l'Institut Mines-Télécom/Télécom SudParis dans le département Electronique et Physique, au sein du Groupe Navigation et Radio Hyperfréquences.

1/2011-10/2012 Autoentrepreneur, Paris. Activité de conseils et création de logiciels scientifiques. Consultant en télécom, informatique et électronique.

03/2005-12/2010 Ingénieur de recherche. Institut National des Télécommunications, Evry. Dans le cadre de divers projets, poursuite des études sur les systèmes de positionnement en intérieur en tant qu'ingénieur de recherche. Les différents points traités furent dans la continuité du projet précédent:

Poursuite de l'élaboration du système des répéteurs avec amélioration de la sélection des données.

Développement logiciel en langage C d'un récepteur numérique.

Validation expérimentale de la boucle numérique réductrice d'échos (SMICL).

Participation aux campagnes de mesures et exploitation des données pour le Centre National d'Etude Spatial (CNES) dans le cadre d'actions partenariales.

Participation aux campagnes de mesures et exploitation des données pour Telecom Italia dans le cadre du projet "Indoor positioning system based on GPS repeaters"

A partir de 2007, élaboration d'un système de positionnement en intérieur de type pseudolites.

Etude théorique du problème de l'éblouissement.

Validation expérimentales des concepts de réduction de l'effet en question.

Mise au point de systèmes de filtrage des mesures pour une précision de positionnement inférieure au mètre.

Activités d'enseignement (voir le détail dans la section suivante).

03/2004-12/2004 Ingénieur de recherche. Institut National des Télécommunications, Evry. Dans le cadre du projet « Géoloc », mise en œuvre et étude d'un système de

positionnement à base de répéteurs GPS. Les différents points traités furent les suivants:

Prise en main des récepteurs professionnels, développement logiciel pour la capture de données de positionnement, déploiement du système de répéteurs dans plusieurs environnements et validations expérimentales de la théorie des répéteurs cyclés, participation à la campagne de validation expérimentale de la méthode de mesure d'angles d'arrivée en collaboration avec Télécom Paris.

09/2003-02/2004 Stage de fin d'étude. Laboratoire LACIME de Montréal (CANADA). Elaboration sous Matlab SIMULINK de chaînes de réception complète GPS-GALILEO pour le développement de récepteurs hybrides. Incluant :

Simulateur de constellation de satellites

Numérisation du signal

Boucles numériques de traitement

Calcul de la position

Effet des sources d'erreurs (bruit thermique, échos)

07/2002-09/2002 Assistant commercial dans la société INTESYS activités de Websourcing, e-learning, gestion du temps, Paris. Détermination de la stratégie commerciale, étude de la concurrence, réalisation de supports promotionnels.

1.1.3 Enseignements

Electronique :

Depuis 2012 :

- Electronique numérique : bureau d'étude et travaux pratiques sur le microcontrôleur (48 heures par an) pour la première année des ingénieurs de Télécom Sud-Paris.
- Electronique analogique : travaux pratiques sur la modulation de fréquence (24 heures par an) pour la première année des ingénieurs de Télécom Sud-Paris.
- Projet de fin d'étude pour l'option « Systèmes embarqués » de troisième année des ingénieurs de Télécom Sud-Paris.

De 2012 à 2015 :

- Electronique analogique : travaux pratiques sur la boucle à verrouillage de phase (24 heures par an) pour la première année des ingénieurs de Télécom Sud-Paris.

Depuis 2016 :

- Electronique numérique : cours sur la chaîne de réception d'un récepteur GPS numérique (3 heures par an) pour la deuxième année des ingénieurs de Télécom Sud-Paris.

Radio, hyperfréquences :

Depuis 2012 :

- Cours intégrés pour le domaine "Antennes et Rayonnement" (9 heures) pour la première année des ingénieurs de Télécom Sud-Paris. Diagramme de rayonnement, notion de champ lointain, antennes réseaux, rayonnement du dipôle, polarisation, bilan de liaisons.
- Cours intégrés dans le domaine " Circuits Hyperfréquences" (18-30 heures variable selon les années) pour la première année des ingénieurs de Télécom Sud-Paris. Notions d'impédance caractéristique, notion d'onde stationnaire, guide d'onde, vecteur de Poynting, paramètres S, notion de bruit, notion de non linéarité, application au RADAR.

Depuis 2016 :

- Cours magistraux sur les systèmes sans fil pour toute la promotion en deuxième année des ingénieurs de Télécom Sud-Paris. Cours sur les normes et cours d'introduction et de conclusion (6 heures).
- Cours intégrés sur l'application des normes, notion de brouilleur électromagnétique, faisceau hertzien, dégagement de l'ellipsoïde de Fresnel.

Géolocalisation :

Depuis 2012 :

- Cours sur la géolocalisation (environ 45 heures) pour les options d'ouverture de deuxième année de Télécom Sud-Paris. Notion de précision, méthode de projection plane, cartographie, systèmes GNSS, système de positionnement bluetooth/wifi, données inertielles, fusion de données de positionnement, filtrage de Kalman étendu.
- Cours sur la géolocalisation indoor (environ 30 heures) pour le Master of Sciences Electrical and Optical Engineering (M1 E3A de Paris Saclay depuis 2017 et M1 E3A de l'Institut Polytechnique de Paris à partir de septembre 2020).

Enseignements antérieurs à 2012 :

Enseignements hyperfréquences de Telecom Sud-Paris en deuxième et troisième année :

- INS22, ISM22 : Option de deuxième année orientée navigation par satellites (cours, TD, TP volume horaire : 50 heures) en 2005/2006.
- PHY4502 : Intervenant dans le module « Navigation par Satellite » (Etudiants 2ème année - Niveau M1) de TSP à raison de 18 heures dont 12 heures de Travaux dirigés et 6 heures de cours magistral (les répartitions ayant varié d'une année sur l'autre) pour un total de 20 à 30 élèves. Ces cours incluant de forts aspects d'électronique numérique relative à la réception (et l'émission) GPS, de 2006 à 2011.

- IIO40, IIO35 : TP hyperfréquences, bruit et non linéarité, troisième année (21 heures) en 2005/2006.
- Encadrement de Projet de fin d'étude en troisième année de l'Institut National des Télécom en 2005 et 2006 (6 heures).
- Cours de Master en anglais, présentation des systèmes de navigation par satellite PHY5013 en 2008 et 2009 (6 heures de cours) et TP (3 heures).
- Participation à un jury et encadrement pour le module capteur du master : Traitement de l'Information et Exploitation des Données (Université de Versailles) TRIED de 2005 à 2010 (6 heures).
- Cours de présentation des systèmes de navigation par satellite pour les ingénieurs de deuxième année de l'Ecole Central d'Electronique de Paris en 2005 (3h de cours 3h de TD).
- Cours de présentation des systèmes de navigation par satellite pour les étudiants en DEA de l'Ecole Central d'Electronique de Paris en 2005 (3h de cours)
- Cours de présentation des systèmes de navigation par satellite pour le mastère spécialisé sur "les Systèmes de Navigation et GPS" de l'Ecole Central d'Electronique de Paris en 2006 (3h30).
- Cours de présentation des systèmes de navigation par satellites pour l'unité "Transmission et localisation par satellite" de troisième année de l'Ecole Supérieure d'Ingénieurs en Electrotechnique et Electronique de Paris (ESIEE Paris) 2005 à 2010 (3-5 heures selon les années).

1.1.4 Responsabilités administratives en enseignement

Depuis 2021 :

- Responsable des masters de Télécom Sud-Paris

Depuis 2020 :

- Membre du Comité d'Enseignement de Télécom Sud-Paris.
    - La principale mission du Comité d'enseignement consiste à valider la scolarité et la diplomation des étudiants suivant les formations de Telecom Sud-Paris (Ingénieur, Master of Science, Apprentissage). Il gère les cas particuliers des étudiants en difficulté et rend un avis qui est ensuite validé par le Conseil d'Ecole.

Depuis 2019 :

- Responsable de la mention E3A de l'Institut Polytechnique de Paris

- Elaboration de l'offre de master en coordination avec les enseignants-chercheurs, les laboratoires et les écoles.
- Organisation des comités de mention.
- Gestion de l'évolution des parcours de la mention en harmonie avec la représentation du Département (Communauté) ICE.
- Suivi des inscriptions administratives des étudiants, soutien à la Graduate School de l'IP Paris.

➢ Responsable des PhD track de la mention E3A de l'Institut Polytechnique de Paris

- Organisation des jurys d'admissibilité et d'admission des PhD track.
- Suivi des étudiants admis dans leur choix de parcours master personnalisé.

➢ Responsable du M1 de la mention E3A de l'Institut Polytechnique de Paris

- Elaboration des programmes en coordination avec les enseignants-chercheurs.
- Présidence des jurys d'admission.
- Présentation et soutien des dossiers de bourse.
- Réalisation des emplois du temps.
- Soutien aux étudiants.

De 2017 à 2019 :

➢ Responsable du M1 International de la mention E3A de l'Université Paris-Saclay

- Elaboration des programmes en coordination avec les enseignants-chercheurs.
- Présidence des jurys d'admissions.
- Présentation et soutien des dossiers de bourse.
- Réalisation des emplois du temps.
- Soutien aux étudiants.

Depuis 2016 :

➢ Responsable des Enseignements du Domaine Physique à Télécom Sud-Paris
(le domaine physique intègre plusieurs aspects en lien plus ou moins direct avec le support physique du transport de l'information : optique, radio, électronique).

- Consiste à coordonner l'ensemble des enseignements dispensés dans le domaine de la physique pour l'école d'ingénieur et les masters de l'Université Paris Saclay puis de l'IP Paris.
- Soutien de la cohérence de l'ensemble en lien direct avec les enseignants-chercheurs.
- Interaction et représentation auprès de la direction des formations de l'école.
- Organisation du Conseil de domaine, regroupant enseignant-chercheur et industriels des secteurs.
- Contribution à la constitution du dossier d'accréditation CTI de l'école.
- Accompagnement et organisation de la réforme des enseignements (démarche compétence) pour le domaine physique.

1.1.5 Projets de recherche : contributions et responsabilités

2022-2023 : **Projet PROCOPE** : SMART SECURITY FOR SMART CITIES: ADVANCED E-TICKETING *(Projet Collaboratif France/Allemagne)*

En qualité de : Contributeur aux études techniques

Sujet : Comment garantir la légitimité des données de localisation dans des environnements complexes tels que les SMART CITIES avec des parties "indoor" et "outdoor". On étudie d'une part, l'analyse du comportement du biais de l'horloge du récepteur GNSS en présence d'un leurre et d'autre part, on analyse les capteurs tels que les accéléromètres, les gyroscopes et les magnétomètres pour identifier les incohérences par rapport au signal GNSS reçu. La combinaison et la synergie des différentes technologies et approches innovantes pour assurer la localisation des personnes à l'aide du smartphone pourraient contribuer à la mise en place et au développement de la billetterie électronique.

Partenariat : Télécom Sud-Paris (Evry). German Aerospace Centre. The German Institute for Communications and Navigation (DLR).

2022-2023 : **Projet LOCI** : Localisation Indoor *(Projet Prématuration Institut Polytechnique de Paris)*

En qualité de : Contributeur aux études techniques

Sujet : Développement sur une plateforme SDR de la solution de positionnement Grad-Diff basé sur les mesures de différence de phase.

Partenariat : Télécom Sud-Paris (Evry). Institut Polytechnique de Paris.

2017-2020 : **Projet DIGUE** : Détection d'Interférences GNSS pour UAV autonomE *(Projet Industriel THALES)*

En qualité de : Responsable/Contributeur aux études techniques

Sujet : Projet sur la détection du leurrage de systèmes de navigation d'un drone, suite du projet ANGELAS. Il s'agit de développer des techniques de détection d'un leurrage. Les approches proposées mettent à profit notre compétence sur le fonctionnement des horloges des récepteurs GNSS pour proposer une approche tout à fait inédite.

Partenariat : Télécom Sud-Paris (Evry). THALES SIX GTS (Gennevilliers)

2016-2019 : **Projet PMU** (Projet Industriel PMU)

En qualité de : Contributeur aux études techniques

Sujet : Support au PMU dans la sélection et le test de solutions de tracking pour les chevaux en course (trot et galop). Expertise de la Direction des grands projets du PMU pour l'aide au choix des trois parmi une quinzaine de soumissionnaires à l'appel d'offre du PMU pour un système de tracking. Assistance à l'analyse des solutions proposées, à la mise en œuvre des « pilotes », à l'évaluation et à l'interprétation des résultats. Aide à la décision du consortium retenu pour l'implémentation en course.

Partenariat : Télécom Sud-Paris, Pari Mutuel Urbain

2016-2019 : **Projet PHC-UTIQUE** *(Projet Recherche)*

En qualité de : Contributeur aux études techniques

Sujet : Le projet vise la conception d'une nouvelle architecture, à reconfiguration dynamique, de récepteurs de signaux GNSS quadrimode GPS /GLONASS /GALILEO /COMPASS intégrable, à faible consommation et haute précision capable d'assurer la continuité du positionnement entre l'intérieur et l'extérieur. Dans le cadre de ce projet, il est également proposé d'intégrer des techniques de localisation en intérieur utilisant les signaux GNSS afin d'assurer la continuité du service de positionnement.

Partenariat : Ecole supérieure des communications de Tunis, SupCom (Tunis), Télécom Sud-Paris.

2015-2017 : **Projet AAP Flash sur protection des zones sensibles vis-à-vis des drones aériens, projet ANGELAS** *(projet ANR).*

En qualité de : Responsable à Telecom Sud-Paris, partenaire du projet.

Sujet : Dans le cadre des applications civiles de lutte contre les «drones aériens» (UAS) non-coopératifs, il combine une étude de performances de plusieurs senseurs de technologies différentes, les traitements individuels et de corrélation qui leur sont associés et une analyse de pertinence des réponses à apporter en regard des besoins des différents acteurs et de leurs capacités d'action. Une étude des moyens de neutralisation des drones par le biais de système de « leurrage » a également été menée.

Partenariat : Office National d'Etudes et de Recherches Aérospatiales (Toulouse), Commissariat à l'Energie Atomique et aux énergies alternatives LETI, (Grenoble), Electricité de France, Exavision (Milhaud), Télécom Sud-Paris, THALES communications & Security SAS (Gennevilliers), Institut de Criminologie et de droit pénal de Paris (Paris).

2009-2011 : **I-GNSS,** (projet industriel CNES).

En qualité de : Ingénieur de recherche, responsable des expérimentations

Sujet : Valorisation et applications aval CNES. Retour avec le CNES sur nos nouvelles approches théoriques incluant en particulier les traitements innovants sur la gestion des trajets multiples. Expérimentations en vraies grandeurs sur le site du CNES à Toulouse.

2009-2010 : **Indoor positioning system based on GPS repeaters** *(projet industriel Telecom Italia).*

En qualité de : Ingénieur de recherche, responsable des expérimentations

Sujet : Adaptation de notre approche et déploiement de la solution dans les locaux de Telecom Italia à Turin.

Partenariat : Institut National des Télécommunications, Telecom Italia (Turin)

2006-2008 : **Action R-S06/LN-002-005** *(projet industriel CNES).*

En qualité de : Ingénieur de recherche, responsable des expérimentations

Sujet : Système de localisation universelle à base de répéteurs GPS. Développement et conception d'un prototype de système d'émetteurs. Intégration et conception d'algorithmes de réduction des erreurs liées aux trajets indirects. Validation expérimentale du système.

Partenariat : Institut National des Télécommunications, Centre National d'Etudes Spatiales (Toulouse)

2005-2006 : **AGILE : Application of Galileo In the LBS Environment Projet FP6 Galileo, GJU/05/2407/CTR/AGILE** *(projet européen).*

En qualité de : Contributeur aux études techniques

Sujet : Projet au spectre très large, des solutions techniques à l'étude de marché, intégrant recherche, développement d'applications du système Galiléo aux services géolocalisés. Définition de la feuille de route de l'évolution du système d'augmentation EGNOS et de Galiléo.

Partenariat : Multiples partenaires de l'ensemble des pays d'Europe, pour un budget total de 5 millions d'Euros (Thales, Telecom Italia, Navteq, CNES, Telefonica, etc.)

2005 : **SOPHA: Integration of Software Receiver with Enhanced Integrity Concept on PDA for Safety Critical Handheld Applications Projet FP6 Galileo, GJU/05/2423/CTR/SOPHA** *(projet européen).*

En qualité de : Ingénieur de recherche, expérimentation.

Sujet : Intégration sur PDA d'un récepteur logiciel incluant des concepts d'intégrité adaptés à des applications critiques.

Partenariat : Institut National des Télécommunications, NordNav Technologies (Suède), Teleconsult Austria (Autriche), OECON Ingenieurgesellschaft für Industrieberatung und Projektmanagement mbH (Allemagne).

2005 : **Action R-S05/CM-001-020** *(projet industriel CNES Toulouse).*

En qualité de : Ingénieur de recherche, conception et implémentation des algorithmes, définition des expériences.

Sujet : Le positionnement en intérieur à l'aide de répéteurs GPS. Continuité et développement des méthodes précédentes.

Partenariat : Institut National des Télécommunications, Centre National d'Etudes Spatiales (Toulouse).

2004 : **La localisation en zone de non-couverture des systèmes de navigation par satellites – Cas des répéteurs GNSS** *(projet industriel CNES Toulouse).*

En qualité de : Ingénieur de recherche, conception et implémentation des algorithmes.

Sujet : Localisation en zone de non-couverture des systèmes de navigation par satellites utilisant des répéteurs de signaux.

Partenariat : Institut National des Télécommunications, Centre National d'Etudes Spatiales (Toulouse).

2004 : **GEOLOC** *(Projets incitatifs Groupe des Ecoles des Télécommunications).*

En qualité de : Ingénieur de recherche, expérimentateur.

Sujet : Conception de système de localisation en intérieur hybride basé sur des mesures de temps de propagation de signaux GPS et de mesures d'angles d'arrivée.

Partenariat : Institut National des Télécommunications, Ecole Nationale Supérieure des Télécommunications.

1.1.6 Recherche : encadrement de thèses et stages de fin d'études

Encadrement de thèses :

[th1] **Delphine Isambert** (2020-2023)
Sujet : Algorithme d'Hybridation pour du positionnement précis GNSS.
Thèse en CIFRE avec la société Exagone.
Ma contribution principale consiste à soutenir la doctorante dans l'acquisition de solides bases théoriques nécessaires pour proposer des algorithmes innovants.

[th2] **Victor Truong** (2017-2020) :
Sujet : Détection d'Interférence GNSS pour UAV autonome.

[th3] **Alexandre Patarot** (2012-2015) :

Sujet : Géo-localisation de cibles mobiles en environnement contraint par approches hybrides : inertielle et radio.

Thèse en partenariat avec le CEA.

[th4] **Ye Lu** (2012-2015) :
Sujet : Approches GNSS Indoor pour du positionnement décimétrique.

Contribution à l'encadrement de thèses :

[th5] **Hanen Mehre**z (2016-2019) :
Sujet : Interface Radio SDR pour récepteur GNSS multi-constellation.

[th6] **Iklhas Selmi** (2010-013) :
Sujet : Optimisation des codes et de la génération des signaux de navigation Indoor à l'aide de signaux GNSS.

Stage de fin d'études :

Raphaël Roman (2017) **:**

Sujet : « Caractérisations techniques du comportement d'un drone en présence d'un leurre GNSS.»

Encadrement de stagiaires à TSP (3 mois en 2008) pour un projet d'élaboration d'un récepteur logiciel en C (niveau M2).

1.1.7 Visibilité nationale et internationale

Comité technique/chairman :

Membre du Technical Program Comitee pour la conférence internationale IEEE Indoor Positioning and Indoor Navigation (IPIN).

Chairman pour la conférence international IEEE Indoor Positioning and Indoor Navigation (IPIN)

Travaux de relecture :

Revues (papier et en ligne) :

Relecteur pour la revue IEEE Transaction on Aerospace and Electronic Systems.

Relecteur pour la revue IEEE Journal of Specific Topics in Signal Processing.

Relecteur pour la revue Annals of Telecommunications.

Relecteur pour le journal IEEE : Institution on Engineering and Techonologie (IET) Radar, Sonar & Navigation.

Relecteur pour la revue « Wireless Networks : The Journal of Mobile Communication, Computation and Information ».

Relecteur pour la revue Sensors du journal academic Open access publishing MDPI.

Relecteur pour IEEE Access.

Conférences :

Relecteur pour la conférence internationale : IEEE Indoor Positioning and Indoor Navigation (IPIN)

Relecteur pour : the IEEE International Symposium on Industrial Electronics(ISIE)

Relecteur pour la conférence : International Conference on Intelligent Human Computer Interaction (IHCI)

Relecteur pour la Journée d'Etude sur la TéléSANté (JETSAN).

Commission universitaire :

Membre extérieur de la Commission Consultative de Spécialistes de l'Université Paris-Saclay, section 63 : Electronique, Optronique et Systèmes.

1.1.8 **Brevets**

Un brevet a été déposé en 2008. Il porte sur une nouvelle architecture de récepteur, et en particulier des boucles de poursuite. En copropriété avec le CNES, il se concentre sur des mécanismes de réduction de l'effet du bruit.

Deux nouveaux brevets sont ensuite déposés en 2010 portant sur une technique de réduction de l'effet d'éblouissement (Near-Far effect) dans les systèmes à base de pseudolites.

Deux autres brevets portant sur le positionnement indoor à base de mesures de différences de phase, en mouvement ou statique (triangulation et interférométrie) ont été déposés en France en 2016 avec une extension aux États-Unis, Allemagne et Grande Bretagne.

Un sixième brevet avec THALES Six GTS sur la localisation de leurre GNSS vient d'être déposé fin 2020.

Références :

[BR1] FR0856488 - Procédé de positionnement en intérieur à l'aide de signaux GNSS (Boucle ouverte). Extension PCT.

[BR2] FR1055302 - Procédé de réduction de l'éblouissement d'un récepteur recevant des signaux depuis des émetteurs (DTT-1).

[BR3] FR1055313 - Procédé de réduction de l'éblouissement d'un récepteur au sein d'un système, notamment de géo-localisation (DTT-2).

[BR4] FR3038067 - Procédé de localisation d'un récepteur au sein d'un système de positionnement (GradMouv). Ext US, Allemagne, GB

[BR5] FR3038064 - Procédé de localisation d'un récepteur au sein d'un système de positionnement (GradDiff). Ext US, Allemagne, GB

[BR6] FR2014241 - Procédé pour la détermination de la position d'un leurre à partir d'au moins un récepteur.

1.1.9 Liste des publications

Revues à comité de lecture (ACL) :

[1] Victor Truong, Alexandre Vervisch-Picois, Jose Rubio Hernan, Nel Samama : "Using Clock Bias Behaviour to Detect Spoofing Low Cost GNSS Receivers". Annals of Telecommunications (En cours de review) 2021.

[2] Céline Blache, Geneviève Baudoin, Marc Somson, Thierry Taillandier-Loize, Alexandre Vervisch-Picois, and Nel Samama. An evaluation methodology to access the accuracy of a tracking system in the case of horse races description and experimental validation. Annals of Telecommunications, 74(5-6): 287 – 298, June 2019.

[3] Vervisch-Picois, A.; Samama, N., "Near-far interference mitigation for pseudolites using double transmission," in Aerospace and Electronic Systems, IEEE Transactions on , vol.50, no.4, pp.2929-2941, October 2014.

[4] Nabil Jardak, Alexandre Vervisch-Picois, Nel Samama, "Multipath Insensitive Delay Lock Loop", IEEE Trans. on Aerospace and Electronic Systems, Octobre 2011, Vol. 47, PP.2590-2609.

[5] A. Vervisch-Picois, N. Samama, "Interference Mitigation In A Repeater And Pseudolite Indoor Positioning System", IEEE Journal of Specific Topics on Signal Processing, October 2009, Vol. 3, N°5, PP.810-820.

Conférences internationales à comité de lecture (ACTI)

[6] Thierry Taillandier-Loize, Alexandre Vervisch-Picois and Nel Samama, "A Single Image Based Method To Assess The Accuracy Of A RTK Based Horse Tracking System", ENC2020, 22-25 November 2020, Dresden, Germany.

[7] Alexandre Versvisch-Picois and Nel Samama, "An Approach To Estimate The Absolute Geographical Coordinates Of A Pixel Within A Single Image", ENC2020, 22-25 November 2020, Dresden, Germany.

[8] Alexandre Vervisch-Picois and Nel Samama, "Delta Range Positioning Assisted With Satellites", IPIN 2019: international conference on Indoor Positioning and Indoor navigation, pages 1 – 8, Pise, Italy, September 2019. IEEE Computer Society.

[9] Hanen Mehrez, Rim BARRAK, Adel Ghazel, Muriel Muller, Ghalid Idir Abib, Alexandre Vervisch-Picois, and Nel Samama. Performance analysis assessment for sub-sampling technique: case study reconfigurable GNSS receiver. In SmartNets 2018: International Conference on Smart Applications, Communications and Networking, pages 1–5, Yasmine Hamammet, Tunisia, November 2018c. IEEE Computer Society.

[10] Nel Samama, Alexandre Vervisch-Picois, and Thierry Taillandier-Loize. Indoor positioning: signals of opportunity or local infrastructure? In Journées scientifiques URSI,

”Géolocalisation et navigation”, pages 107–114, Meudon, France, March 2018. Comité national français de radioélectricité scientifique.

[11] Victor, Le Hoang Truong, Nel Samama, Alexandre Vervisch-Picois. “Effects of GNSS spoofing on the clock of a GNSS receiver”,In IPIN 2018 : Indoor Positioning and Indoor navigation, pp.1 - 4, Nantes, France, September 2018. IEEE Computer Society.

[12] Alexandre Vervisch-Picois and Nel Samama. “Specific study of delta range positioning: indoor positioning algorithm with difference of distance measurements.” In IPIN 2018: international conference on Indoor Positioning and Indoor navigation, pages 1 – 7, Nantes, France, September 2018. IEEE Computer Society.

[13] Alexandre Vervisch-Picois, Nel Samama, Thierry Taillandier-Loize. “Influence of GNSS spoofing on drone in automatic flight mode” ITSNT 2017 : 4th International Symposium of Navigation and Timing, Nov 2017, Toulouse, France. pp.1 – 9

[14] Nel Samama, Alexandre Vervisch-Picois, and Thierry Taillandier-Loize. “A GNSS-like indoor positioning system implementing an inverted radar approach: simulation results with a 6/7-antenna single transmitter.” In IPIN 2016: 7th International Conference on Indoor Positioning and Indoor Navigation, Alcala De Henares (IEEE)., pages 1 – 8, October 2016a, Spain.

[15] Alexandre Vervisch-Picois and Nel Samama. “Delta Carrier Range algorithm for indoor positioning: application to pseudolite-like transmitters.” In IPIN 2016: 7th International Conference on Indoor Positioning and Indoor Navigation, Alcala De Henares (IEEE)., pages 1 – 8, October 2016a, Spain.

[16] Ye Lu; Vervisch-Picois, A.; Samama, N., "Cycle slips detection and repair for high accuracy GNSS-based indoor positioning," in Indoor Positioning and Indoor Navigation (IPIN), 2014 International Conference on Indoor Positioning and Indoor Navigation, Busan (IEEE), vol., no., pp.481-490, 27-30 Oct. 2014, Korea.

[17] Samama, N.; Vervisch-Picois, A.; Ye Lu, "Localization by analysis of the geometrical deformation of a network of communicating entities," in Indoor Positioning and Indoor Navigation (IPIN), 2014 International Conference on Indoor Positioning and Indoor Navigation, Busan (IEEE), vol., no., pp.473-480, 27-30 Oct. 2014, Korea.

[18] Patarot Alexandre, Boukallel Mehdi, Lamy Sylvie, Vervisch-Picois Alexandre, “A Belt Mounted IMU With Enhanced Distance Estimation For Pedestrian Indoor Positioning”, The 4th International Conference on Indoor Positioning and Indoor Navigation, Montbéliard (IEEE), October 2013, France.

[19] Vervisch Alexandre, Selmi Ikhlas, Samama Nel, Lu Ye, “A New Approach for Decimeter Accurate GNSS Indoor Positioning Using Carrier Phase Measurements”, The 4th International Conference on Indoor Positioning and Indoor Navigation, Montbéliard (IEEE), October 2013, France.

[20] Selmi Ikhlas, Vervisch-Picois Alexandre, Gottesman Yaneck, Samama Nel, “GNSS-Based Calibration of the Infrastructure of the Repealite Indoor Positioning System” , The 4th International Conference on Indoor Positioning and Indoor Navigation, Montbéliard (IEEE), October 2013, France.

[21] Lu Ye, Vervisch-Picois Alexandre, Samama Nel “First Theoretical Aspects of a Cmaccuracy GNSS-based Indoor Positioning System”, The 4th International Conference on Indoor Positioning and Indoor Navigation, Montbéliard (IEEE), October 2013, France.

[22] Alexandre Vervisch-Picois, Iklhas Selmi, “Positoning Results of the Repealite Based Indoor Positioning System in a Small Room”, JETSAN, Fontainebleau, mai 2013.
[23] Iklhas Selmi, Alexandre Vervisch-Picois, Yaneck Gottesman, Nel Samama, "Optical and Radio Calibration of the repealite Based Indoor Positioning System", The 3rd International Conference on Indoor Positioning and Indoor Navigation (IEEE), Sydney, November 2012, Australia.
[24] Alexandre Vervisch-Picois, Iklhas Selmi, François Delavault, Yaneck Gottesman, Nel Samama, "Experimental Positioning Results of the Repealite Based Indoor Positioning System - Preliminary 2D results ", The 3rd International Conference on Indoor Positioning and Indoor Navigation, Sydney (IEEE), November 2012, Australia.
[25] Alexandre Vervisch-Picois, Nel Samama, "First Experimental Performances of the Repealite Based Indoor Positioning System", The Ninth International Symposium on Wireless Communication Systems (IEEE), Paris, August, 2012, France.
[26] Alexandre Vervisch-Picois, Anca Fluerasu, Nel Samama, "A Brief History of the Evolution of Local Infrastructure Based GNSS Indoor Positioning Systems - From Pseudolites to Repealites, through Repeaters ", ENC-GNSS2011, Londres, Novembre 2011, UK.
[27] Anca Fluerasu, Alexandre Vervisch-Picois, Nel Samama, "Repeater based Indoor Positioning - Summary of experimental campaigns of measurements", ENC-GNSS2011, Londres, Novembre 2011, UK.
[28] Iklhas Selmi, François Delavault, Yaneck Gottesman, Alexandre Vervisch-Picois, Nel Samama, "Time delayed transmitter based indoor positioning system - A simple electronic and optical architecture for signal generation", ENC-GNSS2011, Londres, Novembre 2011, UK.
[29] Iklhas Selmi, Alexandre Vervisch-Picois, Nel Samama, "Optimal Codes for GNSS-like Signals for Indoor Positioning", ENC-GNSS2011, Londres, Novembre 2011, UK.
[30] Alexandre Vervisch-Picois, Ikhlas Selmi, Yaneck Gottesman, Nel Samama, "Current Status of the Repealite Based Approach - A Sub-Meter Indoor Positioning System ", IEEE-NAVITEC 2010, 8-10 December 2010, Noordwijk, The Netherlands.
[31] Alexandre Vervisch-Picois, Nel Samama, "Indoor carrier phase measurements through GNSS transmitters - Theory and first experimental results ", 13th IAIN World Congress, 27-30 October 2009, Stockholm, Sweden.
[32] Anca Fluerasu, Nabil Jardak, Alexandre Vervisch-Picois, Nel Samama, " GNSS Repeater Based Approach for Indoor Positioning: Current Status ", ENC-GNSS2009, Naples, Mai 2009, Italie.
[33] Anca Fluerasu, Nabil Jardak, Alexandre Vervisch-Picois, Marco Boschetti, Nel Samama, " Multipath effects on the GNSS repeater based approach. Tracking loop discriminator impact on multipath mitigation ", ENC-GNSS2009, Naples, Mai 2009, Italie.
[34] A. Vervisch-Picois, N. Samama, "Systemic Interference Mitigation with a Combined Repeater/Pseudolite Approach for Indoor Positioning", ION 2009 ITM, Anaheim, January 2009, USA.
[35] N. Jardak, A. Vervisch-Picois, N. Samama, "Pseudorange Multipath Mitigation Technique Based on a Subcarrier x PRN Code Replica", ION 2009 ITM, Anaheim, January 2009, USA.
[36] A. Vervisch-Picois, A. Fluerasu, N. Jardak, N. Samama G. Artaud, L. Ries, M. Jeannot, "Real Implementation of an Optimised Tracking Loop for Multipath Mitigation Case of the Repeater Based Indoor Positioning System", ION 2009 ITM, Anaheim, January 2009, USA.

[37] Nabil Jardak, Anca Fluerasu, Alexandre Vervisch-Picois, Marc Jeannot, Nel Samama, " Optimized Tracking Loop for Multipath Mitigation Case of Repeater Based Indoor Positioning System", ENC-GNSS2008, Toulouse, Avril 2008, France.

[38] Alexandre Vervisch-Picois, Marc Jeannot, Nel Samama, " Analysis Of Receivers' Intrinsic Performances To a Code Phase Jump ", GNSS 2007, Genève, Mai 2007, Suisse.

[39] Nabil Jardak, Alexandre Vervisch-Picois, Marc Jeannot, Anca Fluerasu, Nel Samama, "Implementation of an Optimized Code Loop for Indoor Positioning", ION GNSS 2007, Forth Worth, Septembre 2007, USA.

[40] Anca Fluerasu, Nabil Jardak, Alexandre Vervisch-Picois, Marc Jeannot, Marco Boschetti, Nel Samama, "Study of Multipath Effects for the GNSS Repeater Based Indoor Positioning Technique", ION GNSS 2007, Forth Worth, Septembre 2007, USA.

[41] Alexandre Vervisch-Picois, Andre Bideau, Marc Jeannot, Nel Samama, "2D Indoor Dynamic Positioning Using GNSS Based Repeaters ", ION GNSS 2006, Forth Worth, Septembre 2006, USA.

[42] Nabil Jardak, Nel Samama, Alexandre Vervisch-Picois, " Futurs GNSS et Continuité Intérieur-Extérieur de la Fonction Localisation ", UbiMob 2006, Paris, Septembre 2006, France.

[43] Alexandre Vervisch-Picois, Nel Samama, "Analysis of 3D Repeater Based Indoor Positioning System – Specific Case of Indoor DOP ", ENC-GNSS 2006, Manchester, Mai 2006, UK.

[44] Nel Samama, Alexandre Vervisch-Picois, "3D Indoor Velocity Vector Determination Using GNSS Based Repeaters ", ION GNSS 2005, Long Beach, September 2005, USA.

[45] Jean-Christophe Cousin, Nel Samama, Alexandre Vervisch-Picois, "An Indoor Positioning System Using GPS Repeaters and AOA Measurements ", ION GNSS 2005, Long Beach, September 2005, USA.

[46] Nel Samama, Alexandre Vervisch-Picois, "Current Status of GNSS Indoor Positioning Using GNSS Repeaters ", ENC-GNSS 2005, Munich, July 2005, Germany.

[47] Julien Caratori, Marc François, Nel Samama, Alexandre Vervisch-Picois, "UPGRADE RnS Indoor Positioning System in an Office Building", ION GNSS 2004, Long Beach, September 2004, USA.

[48] Julien Caratori, Marc François, Nel Samama, Alexandre Vervisch-Picois, " UPGRADE: 2D Experimental Results for the RnS Approach", EURAN2004, June 2004, Munich, Germany

II. Travaux sur les systèmes de navigation

Liste des acronymes

AOA : Angle Of Arrival

AGC : Automatic Gain Control

C/A : Coarse Acquisition

CEA : Commissariat à l'Energie Atomique

CORS : Continously Operating Reference Stations

DSP : Densité Sprectrale de Puissance (SPD en anglais)

EDF : Electricité de France

GNSS : Global Navigation Satellite Systems

GPS : Global Positioning System

ICD : Interface Control Document

ION : Institute Of Navigation

IOT : Internet Of Things

IPIN : Indoor Positioning and Indoor Navigation

I/Q : In phase and Quadrature components

LBS : Location Based Services

ONERA : Office National d'Etudes et de Recherches Aérospatiales

OSI : Open Systems Interconnection

PMU : Pari Mutuel Urbain

PPP : Precise Point Positioning

PRN : Pseudo Random Noise

RAIM : Receiver Autonomous Integrity Monitoring

RF : Radio Fréquence

ROC : Receiver Operating Characteristics

RSSI : Receiver Signal Strength Indication

RTK : Real Time Kinematic

SA : Selective Availability

SDR : Software Defined Radio

TDOA : Time Difference Of Arrival

TOA : Time Of Arrival

TRP : Time Relative Positioning

TTFF : Time To First Fixed

UWB : Ultra WideBand

Avant-propos

Nani gigantum humeris insidentes[1] *(Bertrand de Chartres)*

Cela fait un peu plus d'une quinzaine d'années que je travaille sur les systèmes de positionnement. Mes premiers travaux consistaient à extraire des mesures de distances des données GPS. Je m'aperçois bien des années plus tard que j'ai parcouru beaucoup de chemin, compris beaucoup de mécaniques dont j'ignorais l'existence. Pourtant, avec la douce ironie que le temps qui passe donne au regard que l'on porte à toutes choses, je m'aperçois que les travaux que je mène aujourd'hui sont toujours inspirés par ces débuts. Un peu comme Marcel Proust dont on[2] dit qu'il savait qu'on écrit toujours le même livre, un chercheur regarde la réalité avec les yeux qui l'ont formé et même si ceux-ci évoluent, la filiation et les traits communs sont patents entre ses premières études et celles qu'il entreprend plus tard. On se tromperait en y voyant un aspect réducteur du travail de recherche, c'est précisément l'inverse qui est ici affirmé : on enrichit un sujet qui évolue et qui s'avère inépuisable. Certaines approches qu'on a abandonnées en leur temps deviennent applicables, d'autres qu'on a pensées pour un tout autre usage se révèlent plus pertinentes encore pour une problématique naissante. La recherche n'est pas qu'une marche en avant tête baissée, c'est un cheminement sinueux fait d'embranchements et qui ne perd pas l'œil qu'il porte sur le passé. On s'y trouve comme sur un chemin de montagne où les pics nous apparaissent à chaque détour sous un aspect différent.

Aussi j'affirme que si nos métiers consistent à alimenter ce qu'on appelle aujourd'hui l'innovation, dont la société contemporaine a un besoin organique et vital, on ne doit ni négliger, ni mépriser ce qui a été fait, par soi ou nos prédécesseurs, même très anciens. On leur doit grand merci et plus encore à ceux qui nous ont édifiés, et nous édifient encore. Ils restent toujours une grande source d'inspiration. Je porte à l'intelligence humaine un respect et une admiration qui ne connaissent ni l'espace, ni le temps. Notre époque n'est ni plus, ni moins intelligente que celles du passé. Elle a ses clairvoyances et ses œillères, ses ouvertures et ses obstacles. C'est à nous qu'il revient, chacun au niveau qui nous est assigné, d'explorer les premières et de surmonter les derniers.

Animé de cet esprit et fort de ces expériences, je pense avoir quelque chose à apporter au monde de la recherche. A tout le moins, je vais tenter de le montrer dans le présent mémoire.

[1] « Des nains sur des épaules de géants. »
[2] Bernard de Fallois préface de *Contre Sainte Beuve.*

2.1 Introduction : contexte et enjeux

Je vais commencer en m'autorisant une forme, modeste, de transgression. Je vais contextualiser mais de manière très large, peut-être trop large. Pourtant il me semble indispensable de le faire dès à présent pour ensuite resserrer mon propos sur mes travaux.

Les sujets de ma recherche sont centrés sur la géolocalisation. Question très vaste en elle-même et qui préoccupe l'humanité depuis qu'elle a besoin de se déplacer. Avant les années 1990, et le déploiement du Global Positioning System, elle relevait surtout d'affaires de marins sur mer, de géomètres sur terre, de géographes et de militaires sur les deux. Il m'est en effet difficile de débuter ce manuscrit en n'évoquant pas le GPS, mais avant cela je voudrais faire part au lecteur d'une réflexion plus générale sur la place de celui-ci. La planète sur laquelle nous vivons a connu des bouleversements d'une nature particulière ces dernières années. Les changements rapides à l'échelle de l'évolution - les Homo Sapiens que nous sommes ont peu évolué génétiquement depuis 100 000 ans [49] - sont le propre des sociétés humaines. Aussi, sans nécessairement invoquer de grandes références historiques, on peut considérer comme acquis que nous vivons depuis la dernière grande guerre dans le mouvement de ce que les historiens appellent la troisième mondialisation. Celle-ci se caractérise par des transformations dans les relations politiques et économiques entre les pays du monde. Tout particulièrement à travers une intensification, dans le temps et dans l'espace, des échanges des biens et de la circulation des hommes. Pour ne pas se gripper, une dynamique de cet ordre et de cette ampleur, dont les causes ne sont pas notre sujet, doit fatalement se doter d'outils efficaces. C'est une mécanique bien connue de l'histoire : Philippe de Macédoine a inventé la phalange pour conquérir la Perse, les empereurs chinois ont suscité l'invention du papier pour l'administration et la Caravelle a été conçue par les Portugais lorsqu'ils ont voulu prendre le large depuis leur étroite bande de terre du bord de l'Europe. On pourrait multiplier les exemples de cette sorte. Cependant, cette vision des choses ne manque pas de susciter des objections. Une vision plus techno-centrée aura tendance à attribuer aux découvertes scientifiques la cause des transformations, ce qui ne semble pas à priori moins juste. Cette dialectique, j'y songe pratiquement tous les jours, pas seulement au sujet des GNSS : mais qui influence qui ? L'interaction à travers des influences réciproques me semble incontestable, mais tout bien compté, selon moi, la primauté reste au mouvement, même s'il est difficile de contester que l'outil influence nécessairement celui qui le manie. L'ancien président des Etats-Unis Barack Obama a eu une formule très juste au sujet de l'outil militaire américain : « Ce n'est pas parce qu'on a le plus beau marteau que tous les problèmes sont des clous. » Même si l'outil militaire a un caractère très particulier, et que les catégories habituelles y sont complexes à appliquer, on peut quand même en retenir une maxime simple qui est qu'un bel outil donne une furieuse envie de s'en servir. En s'en servant il est inévitable que celui-ci influence son utilisateur, comme le bras du forgeron se déforme à force de frapper le métal.

En considération de tout ceci, il me semblerait naïf de ne pas reconnaître le caractère éminemment politique des Global Navigation Satellite Systems (GNSS) et de la géolocalisation dans la mesure où ils sont un outil du mouvement de la mondialisation dans laquelle s'inscrit, de bon ou mauvais

gré, l'ensemble des nations du monde. Ce n'est d'ailleurs pas un hasard si, parmi ces nations, celles qui possèdent et gèrent des constellations de satellites montrent, ou ont montré, des ambitions mondiales. Les Etats-Unis et l'URSS (redevenue la Russie) vainqueurs de la dernière guerre mondiale, chefs des deux blocs de la guerre froide, en tant que géants géopolitiques furent tout naturellement portés à développer de tels systèmes. L'Union Européenne, conglomérat plus ou moins bien défini de nations partageant une civilisation commune, s'est également lancée dans de tels développements sous une forte impulsion de la France, suivant une tradition gaullienne qui est en fait une tradition historique. L'héritage colonial, ainsi que le rôle de la France dans les deux précédentes mondialisations et sa tradition spatiale (programme Ariane), incitent notre pays à pousser ces initiatives au sein de l'Union Européenne, allant parfois jusqu'à les sauver de l'abandon pur et simple. Bien entendu, on se doit également de mentionner la puissance chinoise de retour au premier plan. Aujourd'hui, les premiers objectifs de déploiement de sa constellation Beidou concernent, et ce n'est pas un choix fortuit, ce qu'elle considère comme sa zone d'influence d'Asie-Pacifique. On peut presque lire la géopolitique à travers l'histoire présente et future du déploiement des constellations GNSS. Cela ne doit pas nous surprendre. Tout a commencé avec cette révolution qu'a constitué l'ouverture de la période des grandes découvertes et des grands voyages maritimes des XV^{ième}, XVI^{ième} siècles. L'élargissement aux espaces fluides, que sont les océans, de l'espace géographique sillonné et sillonnable s'est accompagné d'une indispensable mathématisation de la représentation du monde physique. En effet, pour inclure à cet espace les étendues maritimes, auxquelles les représentations des espaces solides sous forme de terroir ne peuvent s'appliquer, il a fallu les redéfinir en termes d'espace fluide et réticulé. Les mathématiques l'ont permis. En effet, comment définir une position au milieu de la mer ? Rien ne ressemble plus à un carré de mer qu'un autre carré de mer. Il faut donc faire appel à une abstraction mathématique issue d'un calcul que l'on va relier à une représentation sur une carte. Cette position « virtuelle » correspond bien à une position réelle, mais il n'y a aucun autre moyen que cette abstraction pour l'identifier, ce qui n'est pas le cas sur terre (exception faite du désert de sable). Cela a son importance car en plus, du point de vue d'un être humain, on doit garder à l'esprit qu'on ne peut vivre que sur la terre ferme, donc sur un espace solide. Dans les espaces fluides (la mer, le ciel et désormais l'espace, voire le cyberespace), il lui faut un « vaisseau » pour se transporter et des repères pour se guider entre deux points de l'espace solide. Un homme n'a jamais pour destination un point de l'espace fluide car il ne peut pas y vivre [50]. On peut dire que les réseaux des espaces fluides relient les points de l'espace solide. Les conséquences de ce changement de paradigme furent considérables pour l'humanité. Pour bien saisir la mesure de ce bouleversement, on peut se souvenir que les Romains antiques ne se représentaient pas leur domination comme essentiellement géographique, malgré certaines expressions parvenues jusqu'à nous comme « Mare Nostrum » (« notre mer » pour désigner la Méditerranée). Ils ne dominaient pas un espace, ils dominaient les peuples qui occupaient un espace [51]. Les rois de France, jusqu'à la révolution française, parlaient encore de « leurs peuples », la référence à l'espace géographique ne commence véritablement qu'au XVII^{ième} siècle. Ainsi, à partir du XV^{ième} siècle, la politique s'est progressivement faite « géo » politique, par cette connexion des lieux terrestres à travers les espaces fluides, pour lesquels la mise en réseau est indispensable pour s'y mouvoir. Pour une puissance, dominer signifie désormais tenir le réseau qui permet l'interconnexion des espaces solides. Les GNSS s'inscrivent comme une phase de cette dynamique amorcée il y a six siècles et qui nous gouverne toujours. Voilà qui explique, anthropologiquement, voire même philosophiquement, pourquoi certaines nations se lancent dans le déploiement de constellations GNSS. Aujourd'hui, celui qui domine le réseau, impose son « la »

au « là », autrement dit à la planète. Je ne vais pas rester plus longtemps sur la philosophie et la politique, j'y reviendrai par petites touches dans la partie de ce mémoire qui concerne les systèmes de leurre. J'ai simplement fait ce paragraphe pour contredire, un peu, Raymond Aaron et montrer que parfois l'on comprend, un petit peu, l'histoire que l'on fait [52][3].

La référence au GPS[4] est devenue un lieu commun. Dans le langage courant, le GPS ne désigne pas seulement le système, mais l'appareil électronique, ou le logiciel, délivrant le calcul de position, voire les informations de navigation, que celui-ci utilise des satellites ou pas du tout ! En résumé, selon un processus métonymique classique, la partie désigne le tout. Bien que spécialiste du sujet, ce serait une faute de ma part de mépriser la perception commune, car elle a une signification. Cela ne concerne pas seulement l'utilisateur, mais également les industriels. Dès lors que l'on veut parler de géolocalisation, le GPS et ses concepts exercent un tropisme très puissant. Depuis son déploiement et la généralisation de son utilisation, on peut mesurer cette influence à travers des exemples simples : une personne non spécialiste ne parle pas de coordonnées géographiques mais de coordonnées GPS, pas toujours de manière très appropriée d'ailleurs. Est-ce si problématique que cela ? Comme souvent, il y a des bons et des mauvais aspects. L'avantage est qu'en généralisant la géolocalisation, le public et les industriels intègrent ces problématiques à leurs produits et leurs besoins, ce qui est stimulant du point de vue de la recherche. Le gros inconvénient est que, certes ils pensent géolocalisation, mais ils la pensent avec les catégories des GNSS à l'extérieur et en attendent les mêmes performances et la même disponibilité, et ce, quelles que soient les conditions d'utilisation. Cela conduit à certaines incompréhensions. Je me souviens d'un échange avec un responsable technique d'une entreprise de matériels destinés aux géomètres qui m'avait demandé pourquoi on n'arrivait pas à l'intérieur à faire aussi précis qu'à l'extérieur. Question pertinente s'il en est, pour laquelle j'ai improvisé une réponse impliquant le mouvement des satellites et l'environnement de trajets indirects. Mais la question elle-même illustre bien la vision du praticien qui applique naturellement les catégories du GPS à toutes les approches de géolocalisation. Je crois peu à nos capacités à transformer ces perceptions bien ancrées. Il faut faire avec et s'il doit y avoir une évolution, elle ne peut s'envisager que sur le temps long. A notre niveau, nous ne pouvons au mieux qu'émettre des réserves vis-à-vis de l'enthousiasme et des déceptions que ces confusions engendrent et replacer la problématique sur le plan scientifique, ce que nous entendons faire dans ce mémoire.

Il ne me semble pas utile en introduction de rappeler les principes fondamentaux des GNSS, j'aurais l'impression de paraphraser le début de ma thèse de doctorat. On lira néanmoins avec grand profit le chapitre consacré à l'historique de l'excellent ouvrage de mon collègue et mentor Monsieur Nel Samama sur le sujet [53]. En revanche je vais faire deux mentions spéciales sur ce que je considère comme les deux piliers de mes travaux ces dernières années et que je vais développer : le positionnement en milieu contraint (ou indoor), dont j'ai commencé à parler, et les attaques de leurre sur les systèmes de navigation. L'articulation de l'un vers l'autre peut sembler a priori curieuse. Comment passe-t-on du positionnement indoor aux attaques de leurre GNSS ? Nous verrons que cela procède d'une dynamique où se mêle approfondissement d'expertise scientifique et opportunité. Commençons par évoquer le positionnement indoor.

[3] « Les hommes font l'histoire mais ne savent pas l'histoire qu'ils font. »
[4] L'acronyme GNSS peine à s'imposer au-delà du strict cadre des professionnels du secteur.

2.1.1 Positionnement Indoor : une gageure ?

En matière de géolocalisation dans les environnements où le ciel est ouvert, et il y en a beaucoup, les GNSS sont devenus rois, détrônant les étoiles de leur empire plurimillénaire de repères célestes de l'espace et du temps. La décennie 2000 a été marquée par l'émergence de systèmes de géolocalisation, impulsée par l'intégration du GPS dans les systèmes grand public, comme les voitures individuelles par exemple. A partir d'un simple terminal, il devenait possible d'obtenir la position de l'antenne à laquelle celui-ci est relié. En s'imaginant pouvoir étendre cette possibilité à toutes sortes d'applications (agriculture, navigations maritime et fluviale, sécurité civile, localisation du téléphone du piéton pour les services géolocalisés, etc.), le potentiel économique, industriel, même sociétal (santé) de la géolocalisation a été très rapidement identifié. Il fallut cependant le courant de la décennie 2000 pour que l'on comprenne que géolocalisation, néologisme apparu à cette époque, ne signifiait pas, techniquement parlant, uniquement extension de l'usage du GPS. Le principe de fonctionnement du GPS, dont le calcul de la position à partir des mesures de temps de propagation constitue l'essentiel, n'est en effet pas applicable directement à tous les environnements, y compris l'intérieur des bâtiments, ou milieux dits « contraints » [54]. Les causes principales de cette limitation sont d'abord la faible puissance des signaux issus des satellites à la réception dans un tel environnement, mais aussi leurs multiples déformations, causées par la présence des trajets indirects (ou échos) [55]. Comme nous le disions en introduction, le GPS et ses attraits ont néanmoins longtemps exercé un tropisme puissant sur l'ensemble des solutions proposées pour pallier ces insuffisances. Quoi de plus séduisant que de pouvoir utiliser les satellites en tous lieux ? Les satellites sont gratuits (enfin pour être plus précis, leur coût est déjà réglé de manière incompressible par les impôts), de plus le récepteur existe et est déjà intégré au terminal. A partir de cela, on a vu émerger deux grandes problématiques de recherche que les études sur le terrain ont inspiré [56]. La première consiste à fournir une assistance au GPS lorsque celui-ci ne fonctionne qu'imparfaitement, typiquement dans les rues ou le dernier étage des bâtiments. Le terme de « light indoor » a été proposé pour décrire ces environnements. L'« Assisted GNSS », dans son expression la plus primaire, consiste à relier un récepteur GNSS à un réseau d'échange de données quelconque (le réseau de téléphonie mobile par exemple) et de récupérer via celui-ci des informations à un débit plus élevé permettant de réduire le temps d'obtention de la première position (le Time To First Fixed). Les performances sont cependant limitées pour ce qui concerne la précision et la fiabilité. On entend par là la capacité à assurer un positionnement de manière continue avec des performances identiques pour un terminal GNSS statique ou dynamique. Une alternative, mais qui peut aussi avoir pour but la complémentarité, a consisté à améliorer la sensibilité des récepteurs GNSS [57]. On maintient la même logique de n'utiliser que les satellites pour le calcul effectif du point. Cette augmentation de la sensibilité pouvant s'appuyer sur du traitement du signal plus avancé, l'augmentation du temps d'intégration [58], ou l'amélioration des composants.

Vers la fin des années 2000, il est apparu clairement que cette approche, principalement centrée sur le terminal et les signaux GNSS, ne suffirait pas à assurer la géolocalisation dans l'ensemble des environnements. Dans la majorité de ceux-ci, les signaux GNSS peuvent être totalement absents ou inutilisables car trop faibles ou trop déformés. Or le besoin est incontestablement présent. On a vu le développement des applications industrielles (mines, usines, entrepôts, etc.) et mobiles à

destination du public (SmartPhone), ensemble d'applications qu'on désigne sous l'appellation « Location Based Services » (LBS). Les LBS sont l'ensemble des services « logiciels » qui utilisent des informations de données géographiques. Il faut donc alimenter ces services pour qu'ils soient exploitables. Les GNSS, bien sûr, sont au premier rang de ces pourvoyeurs d'information, mais les difficultés rencontrées dans certains environnements ont amené à une prise de conscience que l'approche GNSS seule ne suffisait pas. Notons avec une certaine ironie qu'il en fut de même autrefois des méthodes de positionnement sur mer. En pleine mer, avant les GNSS, il était très difficile de connaître sa position en plein jour, il fallait attendre la nuit et ces petites ancres optiques que sont les étoiles pour calculer sa latitude. Le calcul de la latitude était plus facile dans l'hémisphère nord que dans l'hémisphère sud, privé d'étoile polaire. L'indoor est un peu notre hémisphère sud. Cette prise de conscience a abouti en 2010 à la création d'une conférence scientifique spécialement dédiée à ces problématiques l'«International conference on indoor Positioning and Indoor Navigation » (IPIN) qui se tient toujours. Nul besoin de plus insister : s'il y a une conférence de référence sur le sujet, c'est parce que c'est un sujet. Auparavant ces questions étaient principalement intégrées aux conférences sur la navigation comme la conférence annuelle d'Institute Of Navigation des Etats-Unis (ION). La problématique du positionnement et de la navigation en milieu contraint est toujours d'actualité car aucune solution définitive n'y a été apportée. Pour ma part, je me suis intéressé aux approches basées sur des émetteurs locaux qui reproduisent la constellation qu'on peut résumer sous le qualificatif pseudolites/répéteurs. A partir de ces travaux, j'ai développé des approches originales qui m'ont amené vers des développements qui peuvent aller au-delà des problématiques de l'indoor, vers le positionnement précis. J'y reviendrai plus en détails dans le prochain chapitre. Mais ceci pour souligner qu'à travers ces travaux j'ai acquis une connaissance certaine du comportement d'un récepteur en présence d'un signal de type GNSS mais qui n'est pas issu des satellites. Ceci m'a amené à sillonner un autre champ d'étude : le leurrage GNSS.

2.1.2 La menace des leurres GNSS

Commençons par une question : qu'est-ce que le « leurrage » GNSS ? Le « leurrage », autre néologisme issu du terme anglais « spoofing », consiste à diffuser un signal de type GNSS, dont l'objectif est de se substituer aux signaux issus des satellites, au niveau des modules de traitement des récepteurs qui sont à sa portée. Le signal leurre oblige ainsi le récepteur à calculer, non plus sa véritable position, mais celle définie par l'émetteur du signal leurre. Il existe plusieurs types de leurrage, nous y reviendrons, mais je focalise mon attention sur les leurres de type dit « cohérent », dont l'action n'a pas de répercussion sur les résidus de calcul [59] et donc peu sensibles aux stratégies d'intégrité classiques de type Receiver Autonomous Integrity Monitoring (RAIM) [60]. On ne doit pas confondre le leurrage avec le brouillage. Le brouillage consiste à faire perdre la solution de navigation à un récepteur, le leurrage tente de lui substituer une autre solution de navigation. Ainsi, si le brouillage n'est pas nécessairement intentionnel, le leurrage l'est dans l'écrasante majorité des cas. On a donc affaire à une attaque intentionnelle, qui peut être plus ou moins sophistiquée. Mais dans quel contexte cela peut-il se rencontrer ? Pour le comprendre, revenons quelques années en arrière.

Le système GPS, même s'il n'est pas une arme à proprement parler, a été conçu pour les applications militaires. Il a donc des caractéristiques adaptées à celles-ci :

- Il n'est pas saturable, théoriquement un nombre de récepteurs infini peut l'utiliser simultanément.
- Il nécessite la connaissance de codes pour récupérer les données transmises et calculer sa position.
- Il est émis de telle sorte que la puissance à la réception est très faible (quelques dixièmes de femto Watt).

A l'origine il y avait deux services, deux signaux sur deux fréquences distinctes, un civil et un exclusivement militaire. Cependant, les applications civiles n'utilisant que le signal C/A « Coarse Acquisition », ont connu l'expansion phénoménale dont nous avons parlé précédemment. Le signal militaire, plus performant et plus robuste, a été globalement délaissé par les applications civiles pour plusieurs raisons. D'abord, il nécessite une électronique plus complexe et plus coûteuse (sa bande passante est plus large), mais surtout, il faut connaître le code, donc être en lien direct avec l'armée américaine, pour l'exploiter à pleine performance. Le code dit « civil », est plus vulnérable au brouillage et aux attaques de leurrage [61], mais il est disponible et caractérisé intégralement dans la documentation officielle des ICD (Interface Control Document) [62]. Les récepteurs se développant et s'étendant en nombre et en applications, la vulnérabilité de ces signaux civils, pourtant identifiée dès les origines [63], a été longtemps négligée. Il faut attendre les travaux de Shepard, Bhatti, Humphreys et Fansler sur les déroutages de drones [64] et de navires [65] et l'incident de la récupération d'un drone de la CIA par l'Iran [66] pour qu'une prise de conscience dépassant le cercle des spécialistes, s'amorce. Pour filer le raisonnement jusqu'au bout, je pense que c'est cette extension des applications civiles du GPS qui a retardé cette prise de conscience pendant toutes ces années. Elle a sorti les GNSS de la catégorie des problématiques exclusivement militaires. Ce faisant, le leurrage l'a été par corollaire. Tâchons tout de même de ne pas en rester à une explication trop systémique. La menace des leurres n'est en effet pas seulement causée par la diffusion des GNSS et de leur usage, elle relève également du développement technique. Un leurre peut être un simple répéteur constitué d'une antenne de réception, d'un amplificateur et d'une antenne de réémission. Mais il peut également être plus sophistiqué s'il est en capacité de récréer des signaux GNSS, ce que font les générateurs de signaux destinés à la recherche et à l'industrie. Des constructeurs comme le britannique SPIRENT sont spécialisés dans la fabrication de tels matériels. La nouveauté de ces dix dernières années est le développement des Software Defined Radio (SDR). Ce sont des cartes électroniques reprogrammables, aux coûts relativement modestes, qui permettent de reconstituer des signaux sources dans des gammes de fréquences qui incluent très confortablement celles des GNSS. S'il serait plus qu'abusif de dire que c'est à la portée de tout le monde, on peut tout de même affirmer que le coût et la complexité d'un leurre sont désormais suffisamment réduits pour qu'ils représentent une menace non négligeable pour tout type d'application. Ainsi, on arrive à une situation pour laquelle notre grande dépendance aux GNSS (navigation de drone, génie civil, synchronisation, etc.) nous a rendu plus vulnérables aux attaques, dans le cadre de conflits conventionnels ou anarchiques. On s'aperçoit, y compris dans les sphères militaires, que ces GNSS sont finalement fragiles. Si vous organisez tout votre système tactique autour d'une information à la fiabilité douteuse, on imagine aisément les problèmes qui peuvent en découler pour la sécurité des personnels, voire pour l'objectif de la campagne. On peut étendre

cette remarque à des cas de figures plus pacifiques. On pourrait imaginer quelqu'un qui « s'amuserait » à leurrer les récepteurs des géomètres ou des ingénieurs du génie civil, pour fausser les calculs et engendrer des surcoûts de construction. Ce qui ne constitue qu'un exemple parmi une multitude d'autres qui relève de cette inévitable tendance anarchique à laquelle toute société se trouve confrontée.

Revenons un instant sur le caractère tardif de la prise de conscience de la menace des leurres et profitons-en pour relever un paradoxe. Cette apparente désinvolture vis-à-vis de ces problèmes de leurre n'a cependant pas concerné les solutions alternatives pour l'indoor, ou ce qu'on appelle « les systèmes d'augmentation terrestres » comme les pseudolites ou les répéteurs, dont la plupart des législations restreint fortement l'usage [67]. Le réflexe de défense des régulateurs, finalement sain, de protéger des interférences, n'a pas prévenu, ou de manière très superficielle, la menace des leurres. En ce qui nous concerne, nous nous sommes glissés dans ce paradoxe qui nous a au final plutôt profité. En effet, nos travaux de thèses et ceux qui les ont précédés ont été consacrés aux méthodes de type répéteurs et pseudolites, qui ont sur un récepteur GNSS des effets analogues à ceux d'un leurre. Les répéteurs et les pseudolites sont en quelque sorte des leurres pleins de bonnes intentions. Ainsi, au milieu des années 2010, lorsque des survols de zones interdites par des drones ont commencé en France, nous avons été sollicités pour nous intéresser aux problématiques des leurres, à l'époque en tant qu'attaquant du récepteur GNSS, pour perturber les systèmes de navigation de ces drones afin de les détourner de leurs objectifs. Nos travaux dans ce domaine se sont ensuite poursuivis, mais du point de vue de la détection des attaques, puis de la localisation des leurres sur lesquels je travaille aujourd'hui.

On pourrait dire que je porte deux fers au feu : les leurres GNSS et le positionnement indoor. J'espère, dans ce court chapitre introductif, avoir mis en avant la manière dont les ramifications se sont mises en place, d'une façon qui me semble assez cohérente. Voyons maintenant ce qu'il en est plus précisément de la question du positionnement indoor.

2.2 Système de positionnement en milieu contraint

Il serait vain de vouloir dresser en quelques paragraphes un état de l'art exhaustif des propositions permettant de résoudre les problèmes que pose le positionnement indoor. C'est une question dont la complexité ne se trouve pas uniquement dans les réponses qu'on y apporte, mais également dans la manière dont on la pose. Ainsi, je vais dans un premier temps brosser rapidement le tableau général pour me focaliser sur les approches que j'ai privilégiées, en justifiant ce choix. Je vais m'intéresser essentiellement aux aspects techniques du problème, laissant de côté les approches systémiques. Celles-ci faisant entrer en jeu des problématiques de standardisation et de cartographie, elles entraîneraient le propos dans des digressions qui feraient sortir ce travail de son objectif principal.

2.2.1 La question de la géolocalisation indoor : solutions générales

Il est à peu près clair et acquis qu'il n'est pas raisonnable de projeter simplement ce qui se fait à l'extérieur avec les GNSS pour la géolocalisation à l'intérieur[5]. De nombreuses approches ont été développées depuis plus d'une dizaine d'années (ce qui correspond à la date de mon doctorat). Un des exercices les plus délicats consiste à classifier ces approches, à définir les critères qui permettent de les classifier. Le problème a tellement de variables possibles que la discussion est rendue pratiquement infinie. On pourra toujours trouver argument pour contredire l'interprétation de quelqu'un en citant une multitude de cas particuliers qui deviennent des généralités par la force du nombre. Ce qui m'intéresse ici est de présenter ma vision du problème et les travaux qui en découlent. Il faudra donc pardonner les impasses que je vais fatalement faire. Formation scientifique oblige, je vais agir ici comme lorsque l'on veut résoudre une équation à plusieurs variables (ou un système à multiples contraintes) : je vais commencer par tenter de dresser une liste de ces variables les plus importantes en les définissant puis je m'intéresserais à des cas de figure particuliers.

Complexité du terminal

C'est la grande force des GNSS. Il faut comprendre non une complexité subjective, ce qui est complexe pour quelqu'un pouvant être simple pour un autre et inversement, mais plus en termes de coût de mise en œuvre. Ce coût ne doit pas être vu comme exclusivement pécuniaire, même si ce critère est dimensionnant. Il peut s'agir d'un algorithme qu'on ajoute à un terminal existant (comme le SmartPhone). Si on a besoin de développer une antenne particulière, ce n'est pas pareil que si on utilise des fonctions hardwares déjà existantes ou de coût rendu faible par la standardisation et les économies d'échelle (comme c'est le cas des puces GNSS).

Complexité de l'infrastructure

Faut-il déployer une infrastructure spécifique ou utilise-t-on une infrastructure existante ? Il s'agit un peu ici de la question miroir de celle du terminal. Pour les GNSS comme nous l'avons évoqué,

[5] On utilisera les mots « intérieur » ou « indoor » pour désigner la localisation dans les « milieux contraints »

l'infrastructure existe déjà. Un cas de figure que l'on rencontre pour d'autres méthodes, comme celles basées sur les réseaux sans fil (Wi-Fi, Zigbee, Bluetooth). D'autres, telles l'Ultra Wide Band (UWB) ou les pseudolites, nécessitent une infrastructure dédiée. D'autres encore n'en nécessitent aucune, comme les systèmes inertiels ou certains systèmes optiques.

Précision/performance

Difficile de ne pas évoquer la précision lorsqu'on parle de géolocalisation. Je l'accole au terme performance tout à fait à dessein, pour en quelque sorte en diluer la trop violente évidence. En effet, la notion de précision est sujette à discussion. Déjà parce que le français courant ne nuance pas comme l'anglais la différence entre « precision » et « accuracy » (on a le terme exactitude comme équivalent de ce dernier, mais on l'emploie assez peu). Dans son usage le plus commun, et on doit tenir compte du commun, on comprend la précision comme l'erreur que l'on obtient sur le calcul final de la position dans le système de référence utilisé. Le système de référence pouvant être mathématisé par un repère cartésien ou une indication plus globale (par exemple symbolique, comme la pièce où on se trouve). En tout état de cause, la précision ne peut pas être détachée du système de représentation dans lequel on place la solution. La cartographie indoor apparaît alors comme une problématique majeure pour exploiter toute solution de positionnement indoor.

Disponibilité/continuité

Toujours par comparaison avec les GNSS, dès qu'on a un bout de ciel au-dessus de l'antenne de réception, on récupère des signaux GNSS. Cela ne signifie pas forcément que la position sera calculée avec précision, ni même qu'elle sera calculée, mais les satellites sont disponibles. La question est identique pour le cas de l'indoor. Si on déploie une solution : dans quelle mesure sera-t-elle disponible et assurera la continuité du calcul de la position ? Immédiatement vient la question de la couverture et de la transition entre différents modes de positionnement. Par exemple si on passe de l'indoor à l'outdoor, ou entre deux environnements indoor de natures différentes qui contraignent à basculer d'une technologie ou d'une approche à l'autre. On voit que le problème de la disponibilité/continuité peut rapidement devenir complexe

Intégrité

Cette question est un des grands points faibles des systèmes de géolocalisation. On peut tenter de la définir ainsi : comment s'assurer que le calcul final obtenu possède la « qualité » qu'il est censé avoir ? Dans ce domaine, les GNSS ont les systèmes d'augmentation (comme EGNOS) pour le garantir, mais cela peut ne pas suffire pour un récepteur simplement autonome, comme on le verra dans la troisième partie sur la question du leurrage GNSS. L'indoor a la même préoccupation et au-delà de l'intégrité à proprement parler, la capacité à donner une estimation de la fiabilité de son calcul.

Nous allons nous limiter à ces cinq aspects pour décrire un certain nombre d'approches qui nous semblent les plus représentatives de ce qui s'est fait ces dix dernières années. Cela nous permettra ensuite d'aborder nos propres approches faisant l'objet de travaux de recherche.

Voyons donc les solutions et classons-les en fonction des critères que nous venons de voir.

Techniques et Technologies

Nous distinguons ici les techniques des technologies. On peut définir les secondes comme la mise en pratique des premières, qui regroupent elles-mêmes l'ensemble des algorithmes et principes d'estimation de la position. La figure suivante, issue de [68], illustre assez convenablement l'ensemble des techniques et technologies ayant cours pour résoudre les problématiques du positionnement indoor.

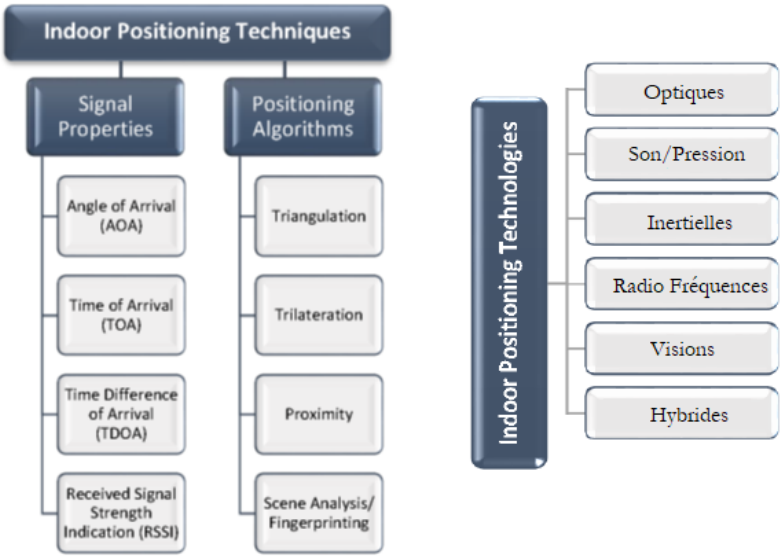

Figure 1

Explicitons un peu le contenu des différentes technologies.

Optiques : incluent toutes les approches qui utilisent des capteurs reposant sur les ondes électromagnétiques dans les fréquences visibles et l'infrarouge [69] [70].

Son/pression : tout ce qui peut correspondre à la mesure d'une variation de pression de l'air, dans les fréquences ultrasons, donc avec [71] ou sans aspect ondulatoire (baromètre) [72].

Inertielles : les grandeurs inertielles correspondent aux mesures des contraintes mécaniques liées au mouvement [73]. J'y ajoute les mesures de champs magnétique car on les associe de façon courante à travers les approches magnéto-inertielle. [74].

Radio Fréquences : cette catégorie inclut toutes les approches radio qui sont très nombreuses : GNSS, UWB, Wifi, Radar, RFID, etc. [75]

Visions : j'associe à vision tout ce qui relève du traitement de l'image et ses dérivés [76].

Hybrides est une catégorie spéciale qui consiste à associer une partie ou l'ensemble des approches précédentes, simultanément ou séquentiellement, pour réaliser le positionnement dans les meilleures conditions possibles.

Avant de dresser les comparaisons, évoquons les techniques de la figure :

AOA : mesure d'angle d'arrivée. Elle peut se baser sur des principes d'interférométries, en diversifiant les sources ou les récepteurs (radio, sonar, voire optique) ou des approches goniométriques. Elle permet de mettre en œuvre les algorithmes de triangulation.

TOA : mesures de temps d'arrivée. Permet de mesurer des distances grâce à la mesure du temps de parcours (Time of Flight) et la connaissance de la vitesse de propagation dans le milieu. Beaucoup de technologies s'y rapportent (optique, acoustique, radio), elles permettent le calcul par trilatération (comme les GNSS) ou en association avec une mesure d'angle (comme certains radars).

TDOA : une version dérivée de la précédente pour laquelle on ne mesure plus des temps d'arrivée, mais les différences de temps d'arrivée entre les signaux. La solution obtenue est souvent équivalente à la précédente, sauf si la synchronisation des signaux est gérée avec moins de précision.

RSSI : mesure de puissance du signal et tout ce qu'on peut en faire pour l'exploiter, avec une cartographie ou un algorithme de proximité. Le principe étant d'associer une position à des valeurs de puissances de signaux reçus depuis plusieurs émetteurs. En somme, cela consiste à lier des grandeurs physiques à des positions, en espérant qu'en en prenant suffisamment on finisse par obtenir une relation bijective entre les deux.

Arrivés à ce stade, nous pouvons noter les différentes technologies pour chacun des critères précédents. Chaque technologie pouvant utiliser l'une, l'autre, voire plusieurs des techniques précédemment citées. On attribue une note entre 1 et 3 à chaque technologie, 3 étant la meilleure et 1 la plus faible. Le tableau suivant montre les résultats.

Table 1

	CX Term	CX infras	Preci/perf	Disp/Cont	Intégrité	Total
Optique	2	2	3	1	2	10
Acoustique	3	1	2	2	2	10
Inertielle	3	3	2	2	2	12
Vision	2	3	2	1	2	10
RF	3	1	2	2	2	10

En allant directement au résultat, on conclurait que globalement toutes les méthodes se valent, sauf l'inertielle qui semble un peu meilleure. On pourrait trouver des arguments pour justifier les notes attribuées à chaque ligne du tableau. Par exemple pourquoi mettre 1 en infrastructures à l'acoustique ? Parce qu'on sait qu'on doit déployer un très grand nombre d'émetteurs/récepteurs avec certaines approches à cause de leur portée courte [77]. Pourquoi dans ce cas ne mettre que 2 à la précision/performance, alors que les performances attendues peuvent aller jusqu'au centimètre ? Parce que les mêmes émetteurs peuvent perdre en qualité par les obstructions. Pourquoi mettre 2 en intégrité à toutes les technologies ? Parce qu'elles ont toutes des possibilités de vérifier la cohérence de leur résultat de positionnement, mais sans garantie absolue. Enfin, on pourrait fortement discuter l'approche inertielle, puisque celle-ci ne fournit pas une estimation de la position mais plutôt du déplacement du terminal (ou du nombre de pas [78]). Pour obtenir un positionnement à rigoureusement parler, il faut l'assistance d'un point de référence ou de recalage, quelle que soit la mesure considérée (champ magnétique ou accélération). Les travaux que nous

avons co-encadrés avec le CEA sur le sujet [th3] montraient cette nécessité d'une autre référence plus absolue pour améliorer la calibration des composants inertiels.

La conclusion est que ce tableau peut être tout à fait défendable, mais également fortement contestable. Il faudrait descendre à un niveau de détails bien plus élevé pour qu'il commence à avoir une signification un tant soit peu objective. J'en conclus qu'une analyse générale de la question du positionnement indoor relève de la tautologie : quels que soient la valeur des arguments que l'on présente, ils peuvent toujours être considérés comme pertinents.

Partant de ce constat, pour se sortir de ce qu'on peut considérer comme une impasse, il y a plusieurs approches possibles. L'une d'elle est l'hybridation (ou la fusion), dont l'objectif est de minimiser les désavantages de certaines approches en exploitant les avantages des autres. Les approches hybrides sont très séduisantes. Elles sont efficaces pour des scénarios donnés, qui ne sont ni simples, ni évidents, comme le montre les résultats de la compétition organisée par la conférence IPIN [79]. Les différents scénarii et les approches proposées par les équipes en compétition est une excellente synthèse illustrant les avantages et limites des approches hybrides (et pas uniquement hybrides). Cela met également en avant une problématique que je n'aborde pas du tout ici mais pourtant essentielle qui est la cartographie indoor. Cependant les approches ont souvent les faiblesses de leurs forces : en mêlant des données de différentes natures, on mêle également des incertitudes de différentes natures.

Une autre approche consiste à se focaliser sur une technique particulière et, à mesure que les embûches s'accumulent, et qu'on réfléchit aux moyens de les contourner, c'est alors que le travail du chercheur prend, selon moi, tout son sens. Nous l'allons montrer par ce qui suit.

2.2.2 Nos travaux : approches type pseudolites, Grad Diff et Grad Mouv

L'essentiel de ma contribution à la recherche dans le domaine de la géolocalisation indoor s'appuie sur des techniques dérivées des pseudolites. A ce stade il n'est pas inutile de rappeler en quoi cela consiste.

Principe des pseudolites

Un pseudolite est un émetteur terrestre transmettant des signaux ayant la même structure que les signaux envoyés par un satellite, d'où leur nom résultant de la contraction du terme de « pseudo-satellite ». Le principe est simple : une constellation (certains préfèrent parler d'un réseau) de pseudolites est déployée dans la zone de non couverture des GNSS, qui peut être par exemple un bâtiment. Les émetteurs jouent alors localement le rôle des satellites et la position peut théoriquement être calculée de la même façon que lorsque les signaux proviennent des satellites. La figure 2 illustre schématiquement ce qui se passe. On dispose les « pseudolites » dans l'environnement où on veut réaliser le positionnement, on synchronise leur émission et les récepteurs peuvent calculer leur position comme lors de la navigation autonome du GNSS à l'extérieur.

L'intérêt majeur de cette approche est qu'on garde le même terminal, ce qui présente l'avantage de ne pas changer de technologie entre milieu intérieur et extérieur. Ainsi, l'essentiel de l'effort

d'adaptation réside dans le traitement des signaux et les mesures associées à ceux-ci. On peut également souligner que les améliorations apportées par les travaux de recherche sur les terminaux GNSS fonctionnant à l'extérieur, et l'effort est substantiel, bénéficient pour partie aux approches pseudolites.

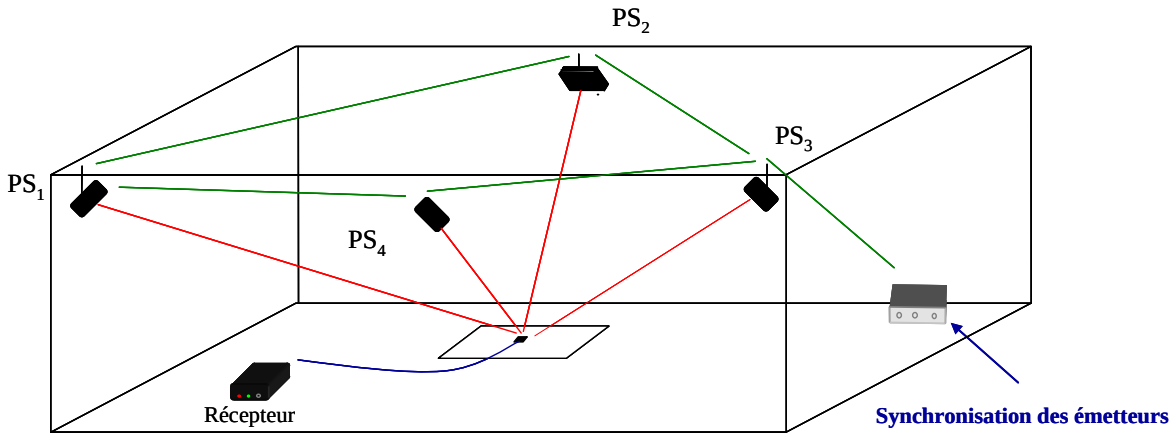

Figure 2

Toutefois, le « canal » de propagation dans le milieu intérieur a des spécificités par rapport à celui de l'extérieur qui regroupe des avantages et des inconvénients. Citons quelques avantages :

- Les positions des émetteurs sont fixes, donc peuvent être connues précisément plus aisément que celles des satellites.
- Les signaux transitent dans l'atmosphère sur quelques dizaines de mètres et ne traversent qu'une couche atmosphérique, contrairement aux signaux provenant des satellites (troposphère et ionosphère).
- Pas d'erreur relativiste entre les horloges récepteur et émetteur (champ de gravité et de vitesse identique).

Parmi les inconvénients, on peut relever :

- La présence plus importante de trajets indirects et d'obstacles qui dégradent ou font perdre la mesure.
- Un effet d'éblouissement (near-far effect) lié à la nature des signaux (CDMA) permettant le contrôle d'accès. Il est bien connu dans la téléphonie mobile de troisième génération mais pour les GNSS il peut survenir également si une partie des signaux satellites est atténuée à la réception (par la traversée d'un obstacle). Les signaux les plus « puissants » éblouissent le récepteur qui ne peut plus traiter les plus faibles.
- La synchronisation des émetteurs qu'il faut réaliser au moindre coût possible.

Pour ce qui nous concerne, nos travaux de ces dix dernières années ont été réalisés avec ce que nous avons baptisé les répélites. Rappelons brièvement leur principe.

Principe des répélites

Les signaux des satellites sont récupérés au niveau d'une antenne placée à l'extérieur dans une zone de bonne couverture, comme pour un répéteur. En réalité le signal d'un seul satellite suffit. Il est donc possible, voire souhaitable pour réduire le bruit à la réception, de substituer un générateur de signaux à cette antenne. Les signaux sont alors, comme pour les répéteurs, distribués vers les antennes de réémission, à la différence près que, cette fois-ci, ils sont retardés avant l'émission sur chaque antenne de telle sorte qu'ils n'interfèrent pas les uns avec les autres. La figure 3 donne la représentation schématique de ces émetteurs.

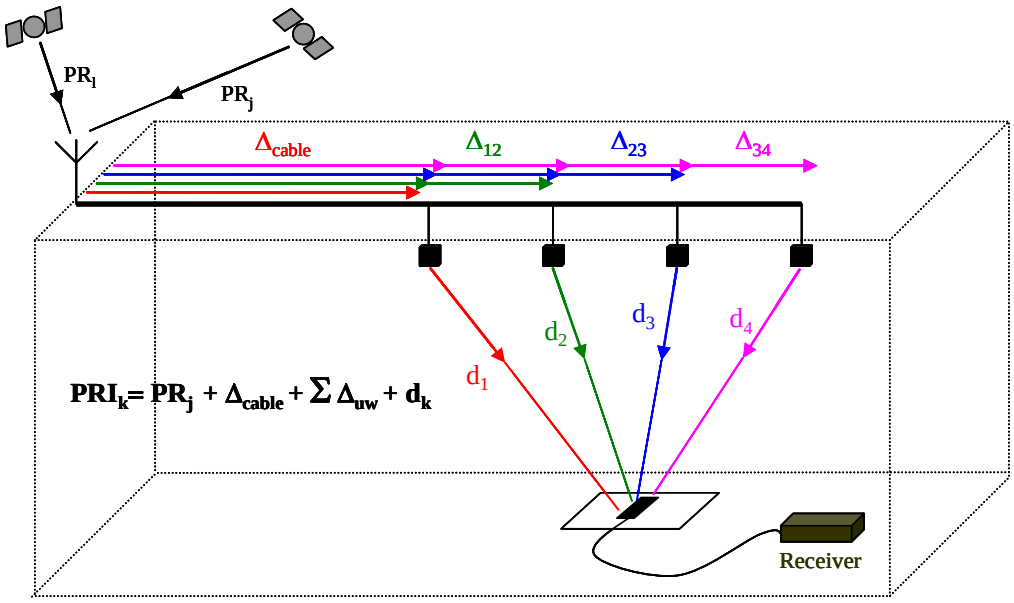

Figure 3

Les PR_j désignent les pseudodistances séparant les satellites de l'antenne extérieure. On parle bien de pseudodistances car elles incluent le biais d'horloge du récepteur. Δ_{cable} représente le retard commun correspondant au passage à travers les câbles menant vers les antennes et $\Delta_{i,i+1}$ correspond au retard volontairement induit entre deux antennes successives indexées i et i + 1. Les distances d_i sont les distances séparant les antennes de réémission de celle du récepteur.

Avec des traitements particuliers, le positionnement avec des répélites permet de réduire les deux derniers désavantages cités plus haut. La synchronisation est réglée de façon évidente par le fait qu'on a une source unique de signal. L'éblouissement se résout grâce à des approches que nous avons développées lors de mes travaux de thèse [3] [5]. Nous l'avons mis en œuvre et cela a mis à notre disposition un dispositif expérimental qui nous a permis de tester les répélites dans divers environnements. Nous avons ainsi pu disposer de données exploitables pour tester les traitements mathématiques que nous allons exposer. Il n'aura pas échappé au lecteur qu'il reste un problème qui n'a pas encore été abordé, le premier point de la liste des désavantages qui est : les trajets indirects.

La mère des batailles : les trajets indirects

Toutes les approches reposant sur la mesure de temps de propagation avec des technologies radio ont le même problème avec les trajets indirects, aussi appelés échos. En présence de ces échos, le signal récupéré au niveau du centre de phase de l'antenne de réception peut être modélisé mathématiquement comme une somme composite de signaux directs (le plus court chemin que l'on veut mesurer) et de signaux retardés pondérés des différences de phase avec les signaux directs. Les signaux indirects, comme ils sont « cohérents » avec le signal direct, agissent comme des interférences dont la nature constructive ou destructive est déterminée par la différence de phase avec le signal direct. En termes de traitement du signal, le résultat obtenu est la déformation de la fonction de corrélation qui provoque une erreur de mesure qu'on ne peut pas caractériser comme le bruit thermique par une distribution gaussienne [80] et qui peut atteindre plusieurs mètres. On est en présence d'une source d'erreur qui mérite donc attention et qui, soit dit en passant, a beaucoup de succès auprès des étudiants (mais pas qu'eux) pour expliquer les défaillances des solutions qu'ils proposent. Quoi qu'il en soit, on ne peut pas ignorer cette source majeure d'erreur. A l'extérieur elle se rencontre dès qu'un environnement présente des obstacles même si les émetteurs satellites sont à vingt mille kilomètres d'altitude. Le milieu intérieur se caractérise par une propagation soumise à beaucoup d'obstacles, statiques ou dynamiques, masquages et horizons obstrués. La gestion en est ainsi encore plus critique qu'à l'extérieur et les conséquences sur l'erreur de calcul, voire sa disponibilité, plus grande encore.

Les trajets indirects sont un sujet qui préoccupe la recherche depuis de nombreuses années. On remarque que les efforts se portent sur toutes les couches du modèle OSI. Antenne, échantillonnage Radio Fréquence, traitement du signal, jusqu'au traitement du calcul de position. Tous les axes stratégiques sont explorés pour réduire leur influence. Nous nous sommes nous-même attaqués à cette question à travers plusieurs approches, relevant plutôt du traitement du signal, ayant pour objectif la réduction de leurs effets sur le signal GNSS [4]. Leur influence est telle qu'on peut sans trop s'avancer affirmer qu'ils ont justifié le développement de la technologie de l'Ultra Wide Band pour la mesure de distance instantanée car celle-ci y est réputée moins sensible que les signaux de type GNSS. A ce stade il semble nécessaire de rappeler la structure d'un signal GNSS. Dans sa version la plus élémentaire, un signal GNSS en fonction du temps t, provenant d'un satellite se présente ainsi :

$$S(t) = A.\sin\left(2\pi f_{L1}.t + \varphi_p(t)\right).c(t + \varphi_c(t))$$

Avec :

A : l'amplitude du signal à la réception (qui en toute rigueur dépend également du temps)

f_{L1} : la fréquence de la porteuse

c(t) : la composante code du signal

$\varphi_P(t)$: la phase de la porteuse

$\varphi_c(t)$: la phase du code

L'information sur la distance se retrouve dans les déphasages du signal que l'on peut relier à son « temps de vol » entre les deux antennes d'émission et de réception. D'après l'équation ci-dessus, il y a donc deux composantes susceptibles de donner la distance : la phase du code et la phase de la porteuse. En pratique elles sont mesurées par le récepteur par rapport à ses propres phases référencées par le temps défini par son oscillateur. La référence de temps pour le récepteur n'étant pas la même que celle de la constellation de satellites, leur différence constitue le fameux biais d'horloge dont on reparlera plus loin. La phase du code est assez sensible aux trajets indirects, mais elle est non ambigüe, c'est-à-dire qu'une mesure permet d'obtenir directement une estimation de la distance émetteur-récepteur. La phase de la porteuse est moins sensible aux trajets indirects et également moins bruitée que le code. On parle d'un bruit de mesure de l'ordre de quelques millimètres alors que celui du code est de l'ordre du mètre. En revanche elle est ambigüe, ce qui signifie qu'on ne mesure instantanément qu'une fraction de longueur d'onde de la distance séparant l'émetteur du récepteur. Mathématiquement, c'est comme si on n'avait accès qu'au reste de la division euclidienne de la distance par la longueur d'onde.

Cependant, cette mesure de phase de la porteuse a un grand avantage : sa mesure instantanée (issue de la boucle de phase) est peu sensible aux trajets indirects. Ce qui constitue une des raisons pour lesquelles on l'utilise avec les satellites pour les applications de positionnement différentiel centimétrique de type RTK [81]. Ce type de positionnement différentiel ayant cette particularité qu'il permet de travailler sous l'hypothèse que les trajets indirects sont, avec le bruit thermique, la seule source d'erreur significative qui reste. Les erreurs liées à la traversée de l'atmosphère, aux erreurs d'horloge récepteur et satellites étant théoriquement supprimées par différence.

Après avoir mis au point l'approche répélites et travaillé quelques temps sur l'amélioration des mesures de codes, nous avons concentré notre réflexion sur l'utilisation des mesures de phase de la porteuse.

Je me permets une petite digression au sujet de ces mesures de phase. Aujourd'hui, on pourrait être tenté d'arguer que la réglementation restreignant fortement les émissions dans la bande GNSS ainsi que le développement depuis ces dix dernières années des approches reposant sur l'Ultra Wide Band, les approches de type pseudolites sont rendues un peu vaines. A cela on peut apporter plusieurs réponses. La première est que, quand on regarde les performances obtenues pour la géolocalisation en milieu contraint, l'UWB ne fait ni mieux, ni moins bien que les pseudolites pour une complexité au moins équivalente [82] et [83]. Comme pour les pseudolites, le moindre obstacle dégrade ou compromet les performances. Disons que les avantages majeurs de l'approche UWB résident dans le droit d'émettre dans sa bande de fréquences dédiée, que n'a pas si aisément les pseudolites, et, ce qui n'est pas peu, la mesure de distance sans ambiguïté. Je cite l'approche UWB car il me semble légitime qu'elle y figure, mais cette comparaison n'est pas au cœur de la démarche que j'ai voulu exposer ici.

D'après ce qui vient d'être dit plus haut, la difficulté principale lorsque l'on veut utiliser les mesures de phase de la porteuse est de lever les ambiguïtés. Cela nous a amenés à développer deux approches s'appuyant sur ces mesures, les approches dites Grad Diff et Grad Mouv. Commençons par expliciter la première.

Grad Diff

Les mesures de phase instantanées étant moins sensibles aux trajets indirects, très influents en indoor, nous avons réfléchi à un dispositif qui permette de les exploiter. En physique de l'électromagnétisme, quelle que soit la fréquence ou les applications considérées, la mesure de phase porte assez naturellement vers les approches interférométriques. A une certaine distance de l'émetteur, en fonction de la longueur d'onde, celles-ci permettent de mesurer l'angle d'arrivée du signal. Comment les appliquer dans un contexte de pseudolites ?

On dispose d'une source de signaux GNSS à deux sorties synchronisées qu'on relie à deux antennes distinctes. On prend soin de séparer ces deux antennes d'une longueur d'onde (19 cm pour le GPS sur L1) ou d'une demie longueur d'onde. Sur chaque antenne, la source émet l'équivalent du signal qu'envoie un satellite. Deux conditions sont alors requises :

1. les codes GNSS envoyés sur chaque antenne doivent être différents
2. ils doivent impérativement être synchronisés.

La figure 4 montre le positionnement avec plusieurs Grin-Loc (qui est le nom du pseudolite de Grad Diff) :

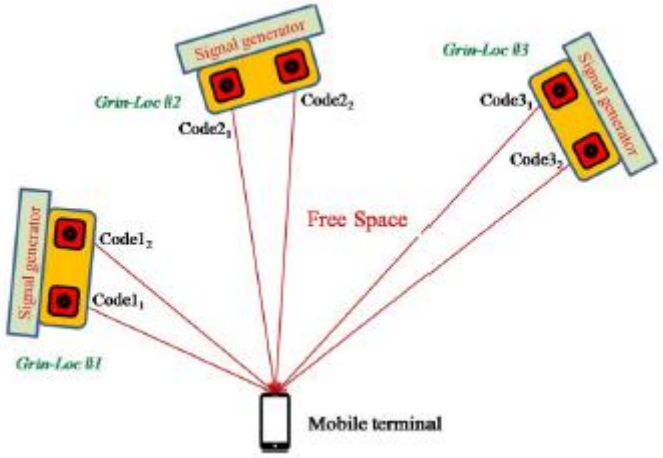

Figure 4

A la réception, on récupère les signaux comme n'importe quel récepteur GNSS et on mesure la phase de la porteuse de chaque signal reçu. On différencie les phases provenant d'un Grin-Loc donné, faciles à identifier avec les codes (n_1 et n_2 pour le Grin-Loc #n), ce qui nous donne une mesure de l'angle d'arrivée pour chaque Grin-Loc. Avec plusieurs Grin-Loc on obtient la position (en 2 ou 3 dimensions) par triangulation. On a également baptisé ce dispositif le radar inversé car usuellement, la différence de marche est obtenue sur deux antennes à la réception, ce qui est l'inverse de ce qui se passe ici. En fait, on applique le théorème de réciprocité de l'électromagnétisme.

Un premier avantage est qu'on a des émetteurs indépendants qui n'ont pas besoin d'être synchronisés, la seule problématique de synchronisation se posant au niveau du générateur de signaux des deux antennes d'un Grin-Loc. La question de l'éblouissement ne se pose pas entre

signaux issus d'un même dispositif Grin-Loc : ils suivent le même chemin à une fraction de phase près. Cependant elle peut se poser entre Grin-Loc, l'un pouvant éblouir le récepteur et masquer les autres. Des stratégies de type répélites peuvent alors être mises en œuvre, mais cela nous fait perdre l'avantage de l'absence de synchronisation. Les premières expériences à partir d'un générateur de signaux et d'un récepteur GPS classique (ublox 6T) donnent ce genre de résultat :

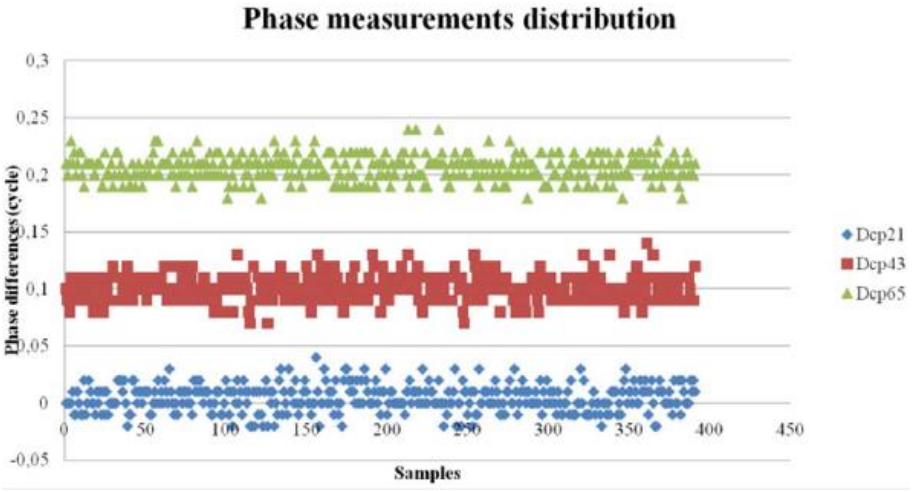

Figure 5

On a bruit de mesure, mais un récepteur classique arrive bien à mesurer la phase attendue (ici 0, 0.1 et 0.2 cycle).

Reste à mener le calcul de position. On peut procéder par triangulation ou par d'autres approches. Nous sommes engagés pour l'année 2022-2023 sur un projet appelé « LOCI » qui va consister à utiliser un Software Defined Radio (SDR) pour la mise en œuvre des Grin-Loc et de calculer la position avec des algorithmes d'optimisation polynomiale (méthodes d'optimisation mathématique avancée). L'intérêt majeur consiste ici à résoudre le système d'équations obtenu sans passer par l'hypothèse du parallélisme des rayons entre les antennes d'émission et l'antenne de réception. On peut partir des équations basiques de la différence de marche dont il est bien connu que la solution est une intersection d'hyperboloïdes :

$$\sqrt{(x-x_{Grn}^{1})^2+(y-y_{Grn}^{1})^2+(z-z_{Grn}^{1})^2}-\sqrt{(x-x_{Grn}^{2})^2+(y-y_{Grn}^{2})^2+(z-z_{Grn}^{2})^2}=\Delta\varphi_{Grn}^{21}$$

Avec : $x_{Grn}^{i}, y_{Grn}^{i}, z_{Grn}^{i}$ les coordonnées des antennes, i={1,2}, du Grin-loc n et $\Delta\varphi_{Grn}^{21}$ la différence de phase mesurée entre les signaux issus des antennes 1 et 2 du Grin-Loc n.

Usuellement on simplifie la résolution en se considérant suffisamment loin pour n'avoir qu'à chercher les intersections des plans asymptotes des hyperboloïdes. Avec l'optimisation polynomiale, on part directement du système d'équations sans hypothèse particulière.

Une contrainte forte de cette approche concerne l'influence de l'erreur de mesure sur le calcul de position. Comme pour toute mesure d'angle, plus la distance entre la source et le récepteur est importante, plus les erreurs de mesure ont d'influence sur le calcul de la position. Cela limite la portée du système à quelques mètres, mais on peut en attendre une mesure de quelques centimètres entre deux points sur une ligne horizontale par exemple.

Nous allons maintenant aborder une autre approche qui peut complémenter celle-ci, ou fonctionner de façon indépendante, pour le cas où l'antenne de réception se déplace.

Grad Mouv

Il s'agit d'une autre manière de résoudre la question des ambiguïtés des mesures de phase (mais sans les résoudre formellement, on aura compris). On considère encore la différence entre deux de ces mesures, mais cette fois-ci au lieu d'avoir deux antennes d'émission en un point et un récepteur, on considère plusieurs antennes d'émission en différents points de l'espace (comme les pseudolites) et un récepteur qui se déplace. On calcule alors la différence entre les mesures de phase pour différentes positions du mouvement, qui correspondent donc à plusieurs instants distincts. La figure 6 illustre ce qui se produit lors du déplacement en termes de mesures de variation de distance.

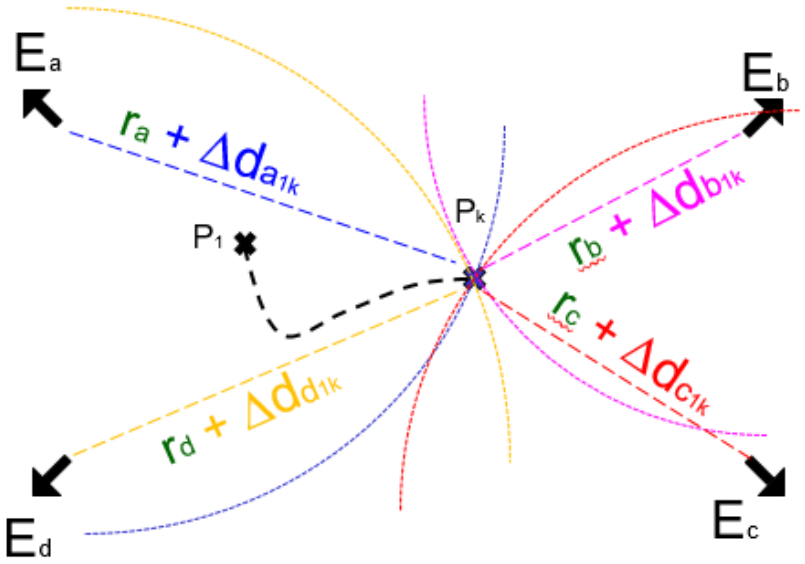

Figure 6

Quelques explications s'imposent : on a quatre émetteurs (E_a, E_b, E_c E_d) et un récepteur qui se déplace entre la position P_1 et la position P_k. La position initiale P_1 est définie par les distances $r_a = E_aP_1$, $r_b = E_bP_1$, $r_c = E_cP_1$, $r_d = E_dP_1$ qui sont inconnues. Entre la position P_1 et la position P_k il peut se passer tout ce que l'on veut, on sait que la position P_k se définit avec les distances $E_aP_k = r_a+\Delta da_{1k}$, $E_bP_1 = r_b+\Delta db_{1k}$, $E_cP_1 = r_c+\Delta dc_{1k}$, $E_dP_1 = r_d+\Delta dd_{1k}$. On connaît les valeurs des Δd grâce aux mesures de phases de porteuse. On a donc ici un jeu de 4 mesures des variations de distances liées au déplacement et ce jeu de variation est unique au déplacement entre P_1 et P_k.

D'expérience, je sais qu'on a un peu de mal à se représenter la réalité de cette situation. Pour s'en convaincre plus aisément, on peut considérer un déplacement sur une dimension (sur une droite) dans différentes configurations, comme sur la figure 7.

Les flèches à côté des variations de distance indiquent les relations avec celles obtenues pour le mouvement 1. Le récepteur s'éloigne de PL1 d'une quantité $\Delta d1_{12}$ et se rapproche de PL2 d'une quantité $\Delta d2_{12}$. Il faut bien penser à considérer les signes de ces variations qui indiquent si le récepteur s'éloigne ou se rapproche des émetteurs. A part dans le cas où la droite serait sur la médiatrice du segment PL1PL2 (auquel cas il faudrait un troisième émetteur), entre les positions P

à l'instant t_1 et P à l'instant t_2, les variations de distance Δd sont uniques. On le voit sur la figure : un même mouvement à un endroit différent sur la droite induit des valeurs de Δd différentes.

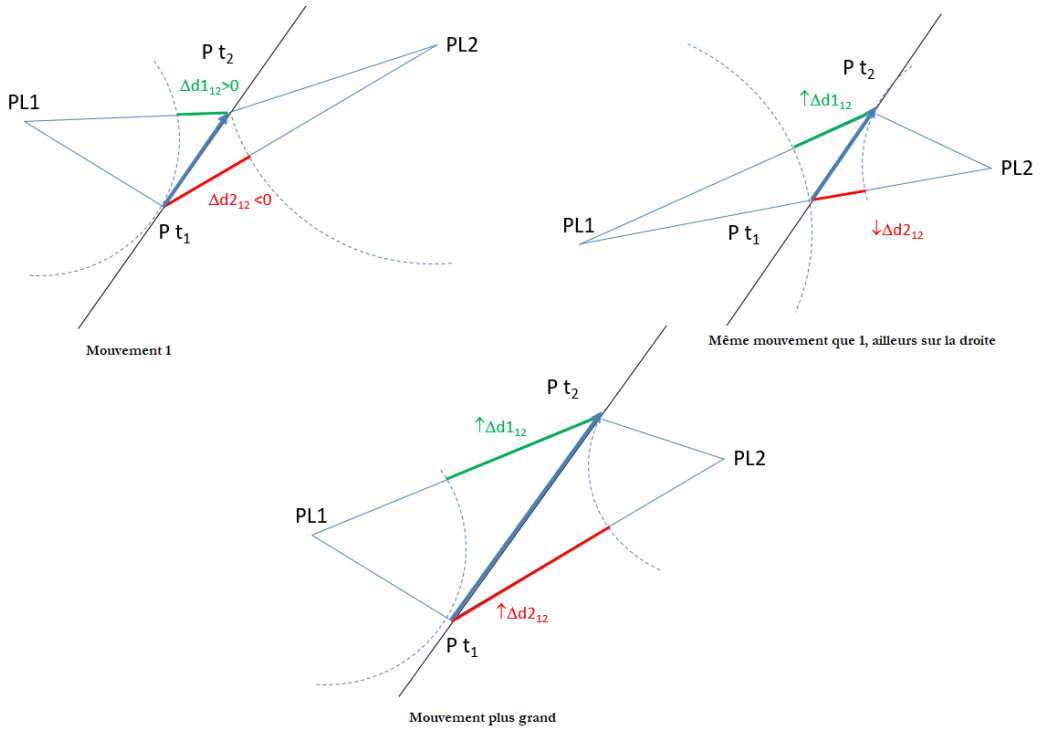

Figure 7

Si le jeu de variations est unique en fonction des positions, qu'on dispose des mesures de ces variations pour k positions successives, alors on doit pouvoir retrouver ces k positions en connaissant simplement la variation des distances pour un nombre suffisant d'émetteurs. La mise en équation est alors la suivante :

$$\sqrt{(x_k - x_{PL}^i)^2 + (y_k - y_{PL}^i)^2 + (z_k - z_{PL}^i)^2} - \sqrt{(x_1 - x_{PL}^i)^2 + (y_1 - y_{PL}^i)^2 + (z_1 - z_{PL}^i)^2} + \Delta b_{k1} = \Delta\varphi_i^{k1}$$

Pour des positions du récepteur allant de k = 2 à n de coordonnées (x_k, y_k, z_k) et les positions des pseudolites allant de i = 1 à N de coordonnées $(x_{PL}^i, y_{PL}^i, z_{PL}^i)$. On a Δb_{k1} la dérive du biais d'horloge entre l'instant 1 et l'instant k (associées aux positions correspondantes, la position initiale étant la position 1). Celle-ci est commune à toutes les mesures indépendamment du pseudolite i considéré. $\Delta\varphi_i^{k1}$ est maintenant la mesure de la différence de phase de la porteuse du signal provenant du pseudolite i entre l'instant 1 et l'instant k.

Ce système d'équations prend en compte l'ensemble du mouvement entre les instants 1 et k. Une condition pour qu'il ne soit pas lié, donc que la solution soit unique, est que chaque position considérée soit différente des autres. Cela correspond, en fait, à la condition du déplacement. On peut ensuite mettre en avant une inégalité afin de savoir combien d'émetteurs et combien de positions sont nécessaires pour déterminer l'ensemble des positions avec cette approche

Grad Mouv. Si on reprend les variables ci-dessus, en appelant m = 1, 2 ou 3, la dimension du positionnement, on trouve l'inégalité suivante :

$$m\left(1+\frac{1}{k}\right)+1 \leq N$$

Un exemple : si on veut calculer une position en 3 dimensions avec 2 positions, il faudra : 3(1+1/2)+1 = 5,5 soit 6 pseudolites. Pour réduire le nombre de pseudolites, on peut augmenter le nombre de positions considérées, 2 étant le minimum. Si on prend k = 3 positions, on tombe à 5 pseudolites et on ne peut pas faire mieux car même pour un nombre de positions k important, la partie gauche de l'inégalité aura toujours un résultat supérieur à 4. Si on a un autre moyen de connaître la dérive du biais d'horloge, le nombre minimum de pseudolites est réduit à 4.

Une fois ces principes posés, vient la question de la résolution du problème. Il n'est pas exclu à l'avenir d'appliquer également des méthodes de type optimisation polynomiale comme pour Grad Diff, mais ce qui a été étudié et mis en œuvre jusqu'à lors est une méthode classique de linéarisation par développement de Taylor, associée à la recherche des moindres carrés du système linéaire obtenu. Le système ressemble à cela :

$$\frac{x_{PL}^i-\hat{x}_k}{\hat{d}_k^i}dx_k+\frac{y_{PL}^i-\hat{y}_k}{\hat{d}_k^i}dy_k+\frac{z_{PL}^i-\hat{z}_k}{\hat{d}_k^i}dz_k-\frac{x_{PL}^i-\hat{x}_1}{\hat{d}_1^i}dx_1-\frac{y_{PL}^i-\hat{y}_1}{\hat{d}_1^i}dy_1-\frac{z_{PL}^i-\hat{z}_1}{\hat{d}_1^i}dz_1+d\Delta b_{k1}=\Delta\varphi_i^{k1}-\Delta\hat{\rho}_i^{k1}$$

Avec $\hat{x}_k, \hat{y}_k, \hat{z}_k$ et $\hat{x}_1, \hat{y}_1, \hat{z}_1$ les coordonnées hypothétiques des positions prises par le récepteur respectivement aux instants k et 1. $\hat{d}_k^i$ et $\hat{d}_1^i$ sont les distances entre le pseudolite i et les points précédents. La grandeur $\Delta\hat{\rho}_i^{k1}$ est la mesure de variation de distance hypothétique correspondant à ces positions. Le calcul des moindres carrés consiste à partir de ces positions hypothétiques, à minimiser les résidus :

$$\|HX-(\Delta\varphi-\Delta\hat{\rho})\|$$

H étant la matrice des cosinus directeurs (correspondant à l'équation précédente), X le vecteur $\{dx_k dy_k, dz_k \ldots dx_1 dy_1, dz_1\}$ et $\Delta\varphi-\Delta\hat{\rho}$ le vecteur des différences entre les mesures réelles et les mesures de variation de distance hypothétique. La norme de ce résidu est minimale si et seulement si [84] :

$$H^t H.X = H^t.(\Delta\varphi-\Delta\hat{\rho})$$

L'algorithme consiste à définir une valeur hypothétique de X, soit $\widehat{X}$, puis de produire une première valeur de X qui nous permet de corriger sa valeur hypothétique : $\widehat{X} \leftarrow \widehat{X}+X$, puis de recalculer X avec la nouvelle matrice H issue de la nouvelle valeur de $\widehat{X}$ en suivant ce processus jusqu'à ce que X ne varie quasiment plus.

Tout ceci correspond à l'adaptation à notre problème d'un procédé très connu, utilisé entre autres pour calculer la position avec des mesures GNSS de type code. Cependant, ici, on va rencontrer une problématique particulière liée à la stabilité de la solution. Dans un cas où « tout se passe bien », minimiser les résidus est assez facile pour une raison simple : il n'y a qu'un seul minimum. Pour le cas qui nous occupe, il peut arriver qu'il y ait plusieurs minimas. On perçoit assez rapidement l'importance de la position hypothétique $\widehat{X}$ dans la résolution car, en fonction de celle que l'on

choisit initialement, l'algorithme peut nous amener à un minima qui correspondra à une position fausse. Nous avons cherché à comprendre quels paramètres du problème influencent la solution, à la fois en termes de stabilité et de précision. Pour cela nous avons mené une étude systématique consistant à étudier deux aspects : d'une part l'influence de la trajectoire en faisant varier la longueur et la forme, droite ou courbe, d'un déplacement en deux dimensions. D'autre part, l'influence de la position hypothétique choisie au départ de l'algorithme, tout ceci dans un espace ayant les dimensions d'une grande pièce (entre 60 et 100 m²). La stabilité se définit par le nombre de minima observés pour un jeu de mesures donné en faisant varier la position hypothétique dans l'espace considéré. Les résultats sont rapportés dans [12] et [15]. Cette étude permet de mettre en avant que la stabilité de l'algorithme est essentiellement influencée par les variations des angles $P_1PL_iP_k$ (comme on les voit sur la figure 7). Plus les angles sont importants, plus l'algorithme est stable et plus sa solution est précise. On retrouve là les effets classiques de l'influence de la géométrie sur le calcul de position, autrement dit, la dilution de précision. Dans un environnement réel comme celui d'une grande pièce de 6 mètres sur 10, on a un algorithme parfaitement stable pour un déplacement de 4 mètres en ligne droite et raisonnablement stable pour un déplacement de 2 mètres. En dessous d'1 mètre, la stabilité est plus compliquée à obtenir même avec la précision des mesures de phase de la porteuse. On a ici un compromis à trouver entre la stabilité de la méthode et la distance entre deux mesures. Si on attend trop longtemps entre deux mesures, l'environnement et les trajets multiples auront plus d'influence que si la durée entre deux mesures est courte. La vitesse de déplacement entre ici en ligne de compte. Si on veut résumer à grand trait : cela marchera d'autant mieux que les émetteurs sont près et qu'on se déplace rapidement au début du mouvement. Un autre intérêt de l'approche réside dans l'absence d'obligation de la mettre en œuvre en permanence. Elle peut servir à déterminer le point initial, comme cela se fait avec les procédures de détermination des ambiguïtés entières du RTK. On peut ensuite calculer la position plus traditionnellement en suivant l'évolution des variations de distances. Cette évolution des mesures de variations de distance accumule cependant les erreurs au fil du temps à cause des trajets indirects. En effet, on a bien vu plus haut que la mesure instantanée de la phase de la porteuse était moins sensible aux trajets indirects. Toutefois, à force d'accumulation, les erreurs peuvent devenir importantes. Visuellement et mathématiquement, cela ressemble au genre de dérives qu'on observe lorsqu'on intègre les sorties d'un accéléromètre ou d'un gyroscope, même si physiquement cela n'a absolument rien à voir. On note simplement une analogie de comportement lié à l'intégration de mesures entachées d'erreur non assimilable à une distribution gaussienne centrée. Aussi, en relançant régulièrement la méthode Grad Mouv entre deux (ou plusieurs) positions ultérieures aux premières, on permet ainsi de borner la dérive du calcul de position.

Grâce au dispositif expérimental de type répélite de notre conception, nous avons pu appliquer la méthode dans deux environnements : une configuration de bâtiment de type « canyon urbain » et une pièce fermée dans laquelle on a fait circuler un petit robot équipé d'une antenne. Voici les résultats :

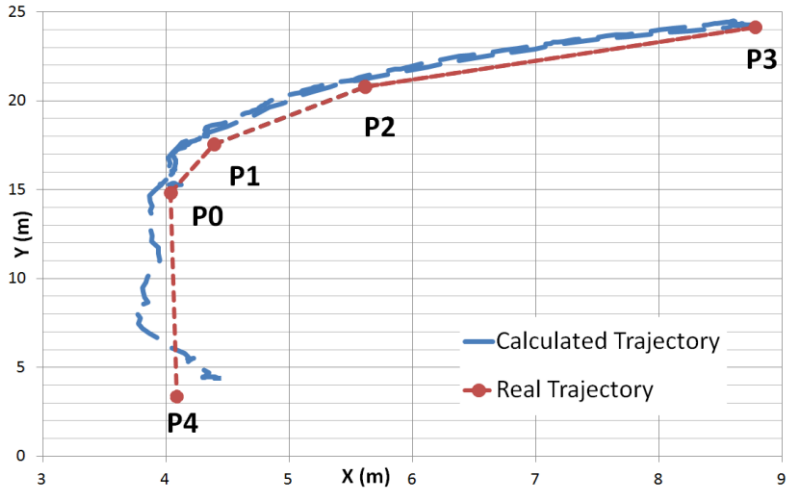

Figure 8

La trajectoire part du point P0 et fait un aller-retour vers le point P3 pour aller ensuite vers le point P4. On applique la méthode Grad Mouv pour déterminer le point initial P0. L'erreur sur cette position initiale est de l'ordre de 40 cm et se maintient à peu près sur toute la trajectoire, sauf au point P4 où on observe une dérive jusqu'à 1 mètre. Si on réapplique Grad Mouv entre P0 et P4, l'erreur retombe à 70 cm. Ceci illustre bien l'effet de bornage de l'erreur dont nous avons parlé. Soulignons que le matériel utilisé ici est très simple : les antennes d'émission et de réception sont des antennes patch classiques et le récepteur utilisé n'est complexe que parce qu'il permet de modifier sa configuration pour suivre les signaux pseudolites.

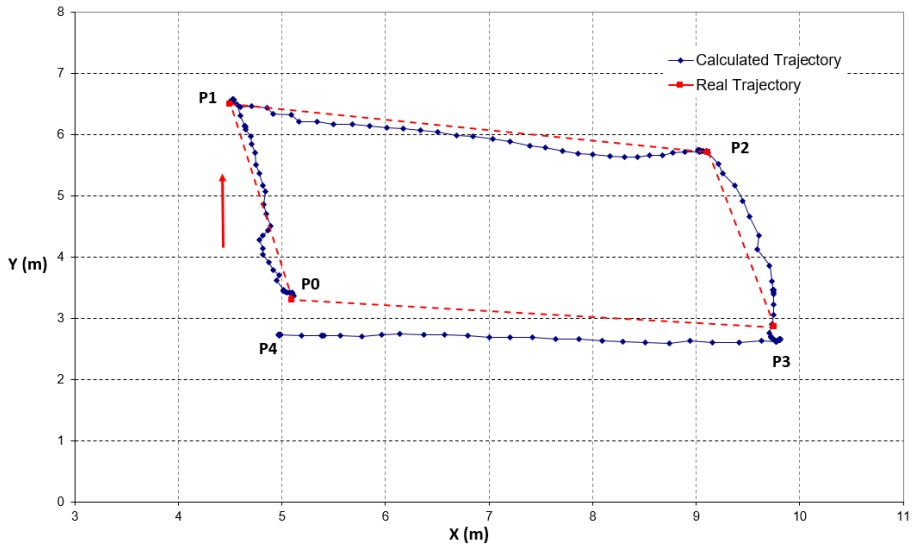

Figure 9

La figure 9 montre les résultats dans un environnement fermé. L'estimation de la position de départ est encore meilleure (14 cm) que le cas précédent et la correction de trajectoire, qu'on ne voit pas ici, fait passer de 70 à 50 cm d'erreur sur la position d'arrivée. Attention aussi à la trajectoire dite réelle sur la figure, en fait seuls les points marqués sont connus de façon précise.

En conclusion sur cette approche, on peut dire qu'elle permet de calculer la position avec les mesures de variation de distances, finalement dans des conditions assez simples d'emploi : il suffit de bouger de quelques mètres pour obtenir une position. Les bonnes conditions de fonctionnement exigent que les angles entre les positions suivies et les émetteurs varient suffisamment au cours du mouvement pour que la position soit obtenue avec une qualité et une stabilité suffisante. Les expériences menées donnent une bonne idée des ordres de grandeur nécessaires et ceux-ci sont tout à fait compatibles avec les applications indoor (quelques mètres suffisent pour des zones de couverture de quelques dizaines de mètres carrés).

A partir de ces travaux, nous avons été amenés à étendre nos réflexions sur divers sujets. Le premier de ceux-ci concerne la localisation d'objets mobiles communicant dans un réseau. Imaginons un tel réseau comme sur la figure 10.

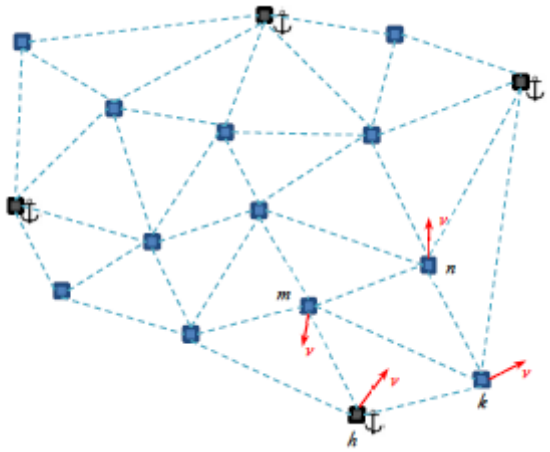

Figure 10

Il y a parmi les éléments du réseau, des ancres (indiquées en noires) qui ne sont pas nécessairement fixes, mais dont on connait toutes les données de géolocalisation (position et vitesse). Les données des autres objets du réseau (en bleu) ne sont connues que de manière fragmentaire, par la variation de leur distance relative (donnée par le doppler) et/ou par leurs distances relatives les uns par rapport aux autres. On se pose alors deux questions : y a-t-il une solution à ce problème ainsi formulé ? Quelle est l'influence de l'erreur des mesures sur la solution ?

Les réponses sont assez complexes : une partie des travaux de thèse menés par Monsieur Yé Lu [th4] permettent d'y répondre partiellement. Pour résumer, très succinctement, on a pris un scénario donné considérant une ancre et plusieurs mobiles. On peut dire qu'on peut trouver une solution, mais on retrouve les conditions géométriques que nous avons énoncées précédemment pour Grad Mouv. Si les mouvements ne sont pas assez marqués (les angles relatifs), on risque de rencontrer des situations pour lesquelles, quel que soit l'algorithme de résolution choisi, il y a plusieurs minima locaux qui peuvent induire de fausses résolutions. Il apparait dans cette étude, outre la géométrie, que ce qui influence le plus le résultat sont surtout, c'est presque une banalité, les erreurs de mesures. Il a été proposé une méthode qui permet d'éliminer 20% des points calculés qui posent problème à partir des caractéristiques mêlant mesures et étapes intermédiaires de calcul de l'algorithme de positionnement.

C'est un sujet qui reste partiellement en friche, la systématisation étant assez délicate à cause du nombre pléthorique de possibilités. L'Intelligence Artificielle pourrait trouver ici des applications intéressantes pour caractériser les situations pour lesquelles le calcul des positions du nuage serait impossible, ou pour détecter quels nœuds du réseau on peut exclure pour améliorer la géolocalisation de l'ensemble. Cette approche peut avoir beaucoup d'applications. On pense à l'Internet des Objets (IOT), en extrayant les Doppler des objets communiquant, mais pas seulement. J'anticipe un peu sur le chapitre suivant, mais on peut imaginer un essaim de drones, que seule relie la connaissance des mesures de distances entre les uns et les autres (ou la variation de celle-ci). Si une partie de l'essaim voit son GNSS brouillé (ou leurré), il pourrait s'appuyer sur la partie « saine », donc les drones qui ne sont pas sous influence du brouillage, qui servirait d'ancre à l'autre partie pour maintenir la géolocalisation de l'ensemble. Les mesures de variation de distances pouvant être extraites de toutes les méthodes possibles (radio, optique, acoustique, image, etc.).

Le second sujet de réflexion concerne la possibilité d'appliquer la méthode Grad Mouv à l'extérieur, non plus avec des émetteurs locaux comme des pseudolites, mais avec des satellites. L'adaptation nécessaire et ses conséquences méritent un chapitre dédié qui sera le suivant.

2.2.3 De Grad Mouv au Time Relative Positioning, le PPP-RTK

Partant d'une réflexion sur la possibilité d'exploiter l'approche Grad Mouv en présence conjointe d'émetteurs au sol comme les pseudolites et de satellites, nous nous sommes demandés comment elle s'appliquerait avec des satellites GNSS seuls. Il a convenu pour cela d'analyser les différences entre les deux situations, pseudolites et satellites. On relève deux différences majeures :

1. Les satellites sont loin, les pseudolites sont en général plus près.
2. Les satellites se déplacent, les pseudolites sont en général fixe.

Autant il est difficile de contester les affirmations précédentes sur les satellites, autant nous sommes bien conscients qu'on peut tout à fait avoir des pseudolites mobiles (montés sur véhicules ou sur drones) qui se trouvent assez loin du récepteur. Mais à ce stade, nous nous bornerons à remarquer que l'éloignement comme le déplacement seront toujours plus importants pour un satellite que pour n'importe quel pseudolite. Ceci pour bien souligner que ce qui compte, ce sont les ampleurs des déplacements relatifs satellite-récepteur. En une seconde, un satellite peut se déplacer jusqu'à 4 km par rapport à un récepteur sur Terre, alors que celui-ci se déplacera de quelques dizaines de mètres par seconde au maximum (pour un bateau par exemple). En termes d'éloignement, les satellites se trouvent à plusieurs milliers de kilomètres, alors qu'un pseudolite se trouvera à quelques kilomètres au maximum (pour les applications outdoor). La figure 11 illustre la situation relativement à la géométrie :

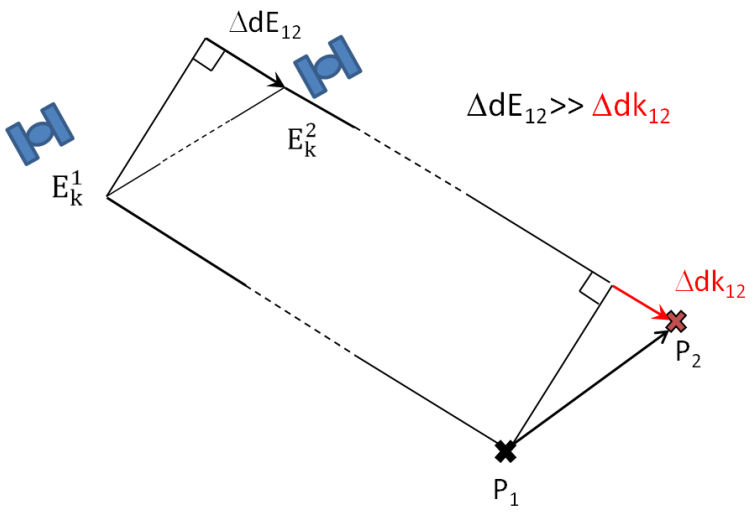

Figure 11

La conséquence de l'éloignement est que les rayons symbolisant les émissions en provenance du satellite sont quasi parallèles. On a vu au chapitre précédent que la stabilité de l'algorithme était influencée par la variation de l'angle $P_1E_k^1P_2$, (l'éloignement permet de confondre en un seul les angles $P_1E_k^1P_2$ et $P_1E_k^2P_2$) or dans ce cas il est toujours égal à 0°. Le système d'équations obtenu avec Grad Mouv, pour un petit mouvement, sera forcément lié, donc impossible à résoudre puisque n'ayant pas une solution unique. Le mouvement du satellite est moins problématique à cet égard, on pourrait même dire que celui-ci est assez favorable puisqu'il lève l'obligation au récepteur de se déplacer, même si quelques secondes de déplacement ne seront pas suffisantes pour que les angles varient significativement.

A partir de ce constat, qui ressemble à une impasse, on peut envisager deux approches. La première consiste à essayer de retrouver les conditions pour appliquer Grad Mouv, nous en parlerons plus loin. La seconde consiste à chercher à calculer non pas la position, mais le déplacement $\overrightarrow{P_1P_2}$ comme sur la figure. Il s'agit d'une technique connue. On appelle la détermination de ce déplacement à partir des mesures de phase de la porteuse le Time Relative Positioning (TRP). Voyons de quoi il s'agit.

Grad Mouv et le Time Relative Positioning (TRP)

Déterminer le déplacement avec précision peut être très intéressant pour des applications scientifiques comme la mesure de la hauteur des vagues [85], le vol des oiseaux [86] ou plus largement maritime, dans des environnements comme l'océan où le calcul différentiel comme le RTK n'est pas possible faute de station à proximité.

Les approches sur ce sujet existent et consistent, entre deux instants 1 et 2 consécutifs, à considérer comme une inconnue le vecteur déplacement. L'équation se formule ainsi (c'est une version adaptée de l'équation de base de [87]):

$$\sqrt{(x_1 + D_x - x_k^2)^2 + (y_1 + D_y - y_k^2)^2 + (z_1 + D_z - z_k^2)^2} - \sqrt{(x_1 - x_k^1)^2 + (y_1 - y_k^1)^2 + (z_1 - z_k^1)^2} + Db^{1,2} = \Delta\varphi_i^{1,2}$$

Les variables D_x, D_y et D_z sont les inconnues qui correspondent au déplacement entre les instants 1 et 2 et $Db^{1,2}$ correspond à la variation du biais d'horloge entre les mêmes instants. x_k^2, y_k^2, z_k^2 et x_k^1, y_k^1, z_k^1 sont les coordonnées du satellite k respectivement aux instants 2 et 1. On a x_1, y_1 et z_1 qui correspondent à la position du récepteur à l'instant 1. Cette position est une estimation « approximative » qui peut venir du calcul avec des mesures de code par exemple. On peut se permettre de partir d'une telle position à cause de la grande distance entre le récepteur et le satellite. Comme l'illustre la figure 12, le même déplacement provoque les mêmes variations de distances entre deux points qui ne sont pas situés au même endroit, à condition que ces points ne soient « pas trop loin », typiquement quelques dizaines de mètres. On y voit une illustration géométrique de pourquoi Grad Mouv ne peut pas fonctionner avec les satellites pour un déplacement de quelques secondes : le parallélisme des rayons.

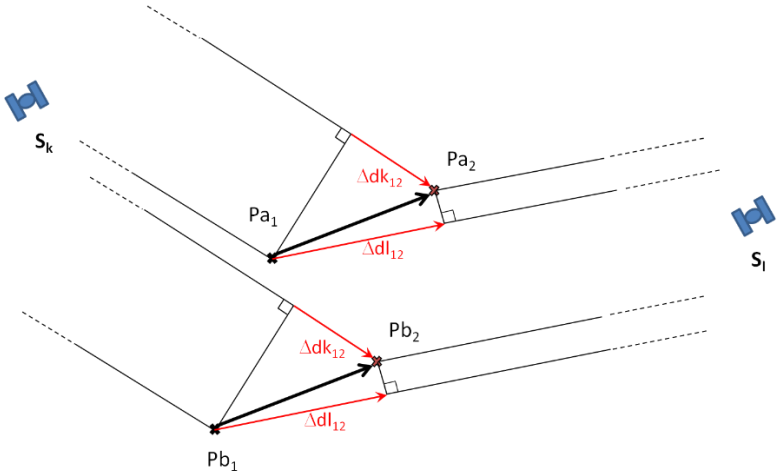

Figure 12

On peut ensuite résoudre le système d'équations obtenu en linéarisant le problème avec un développement de Taylor et une approche itérative de réduction des moindres carrés semblable à celle du calcul de position classique. Celle-ci n'a pas les soucis de stabilité que l'on peut rencontrer avec Grad Mouv car on ne cherche pas la même chose qu'avec ce dernier. L'algorithme est stable car il est très proche des conditions de l'algorithme classique et ses performances obéissent à des conditions très similaires. On pourrait tout à fait, avec des pseudolites, une fois le point initial déterminé avec Grad Mouv, remplacer le calcul de la position par une méthode comme celle-ci. Attention toutefois aux hypothèses : ici le point initial peut être connu de manière approximative, ce qui, dans le cas général, ne se produira pas avec des pseudolites pour lesquels le parallélisme observé sur la figure 12 a peu de chance de se retrouver.

Quelques précisions sur la mesure sont maintenant nécessaires, car il ne s'agit plus de mesurer un signal qui transite entre deux points sur Terre, mais entre un objet dans l'espace et un autre sur Terre. Nous verrons que ceci va progressivement nous amener vers les problématiques du Precise Point Positioning. Décomposons d'abord la mesure de différence de distance de signaux provenant d'un satellite k :

$$\Delta\varphi_k^{1,2} = \varphi_k^2 - \varphi_k^1 + \Delta b^{1,2} + \Delta\delta_k^{iono\ 1,2} + \Delta\delta_k^{tropo\ 1,2} + \delta_k^{paral\ 1,2}$$

La variation de phase que l'on recherche est $\varphi_k^2 - \varphi_k^1 = \Delta dk_{12}$. On voit que s'additionnent trois sources d'erreur (en dehors de la variation du biais d'horloge) : l'ionosphère, la composante humide de la troposphère et le défaut du parallélisme. On fait abstraction ici de toutes les autres sources d'erreur liées à l'antenne, aux éphémérides des satellites, etc. Le but n'est pas de faire de positionnement millimétrique à ce stade.

Pour ces trois sources d'erreur identifiées, la durée entre les instants 1 et 2 est un paramètre déterminant. En effet, plus celle-ci est grande, moins l'hypothèse du parallélisme des rayons issus des satellites aux positions S_k^1et S_k^2 est vérifiée. Autre effet qui perturbe progressivement le calcul : l'ionosphère et la composante humide de la troposphère. On sait que ces couches atmosphériques influent sur la mesure de distance, code comme phase. Toutefois, on sait qu'à part dans des conditions très particulières, les concentrations ioniques dans l'ionosphère ou de gouttelettes d'eau dans la troposphère, responsables des phénomènes physiques entraînant les variations du temps de propagation du signal, ne vont pas changer significativement si on prend comme hypothèse que la durée entre les instants 1 et 2 est de quelques secondes. Ce n'est donc pas cela qui donne de l'importance à ces sources d'erreur, mais le mouvement du satellite. En effet, pour un récepteur sur Terre, la longueur d'ionosphère (et de troposphère) traversées par le signal varie fortement d'une seconde à l'autre à cause du mouvement du satellite, d'autant plus si celui-ci est à une élévation basse.

Quoi qu'il en soit, on a donc intérêt, pour diminuer ces effets, à prendre le plus petit intervalle de temps possible entre les deux instants. C'est bien la conclusion générale à laquelle parviennent les expérimentateurs du Time Relative Positioning [86].

Nous sommes désormais sur un terrain qui nous a, semble-t-il, éloigné de Grad Mouv, mais nous y revenons. Qu'est-ce que Grad Mouv peut apporter au Time Relative Positioning ?

On arrive à démontrer que sous les mêmes hypothèses on peut ramener le problème à un calcul géométrique assez simple, sans passer par la linéarisation. Voyons tout de suite l'idée.

On part de la figure 11, montrant que les deux rayons sont parallèles. On suppose que le point P_2 est connu, ce sera notre point hypothèse (en cela le départ est inversé par rapport au TRP classique). On arrive à montrer facilement que $\Delta dE_{12} \cong E_k^2P_2 - E_k^1P_2$, avec P_2 la position approximative de la fin du mouvement. La démonstration repose aussi sur les grandes distances considérées et sur le parallélisme. On a typiquement une seconde entre les instants 1 et 2. On extrait la valeur de Δdk_{12} en soustrayant de la mesure de variation de phase la valeur de ΔdE_{12} ainsi que la valeur de variation du biais d'horloge obtenue avec les mesures de code et les Doppler (donc la dérive du biais). Les expériences réalisées montrent une précision suffisante dans l'estimation de la dérive du biais par ce moyen là pour ne pas avoir besoin de l'intégrer dans la solution. Autrement dit, une fois ces deux corrections réalisées, on travaille avec une mesure de variation de distance non biaisée.

L'étape suivante consiste, par construction, à définir une position « virtuelle » de satellite S_k' en suivant un vecteur parallèle à la direction P_2S_k, de telle sorte que la distance entre P_2 et S_k soit égale à 2 fois Δdk_{12}. La figure 13 montre ce qui en résulte :

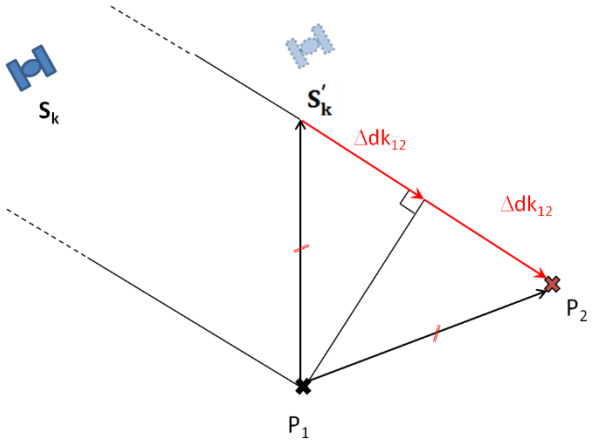

Figure 13

Si on résume en quelques mots, avec une telle construction, on peut dire que pour un satellite donné, l'ensemble des solutions P_1 compatibles avec cette configuration est le plan médiateur du segment S'_kP_2. Pour un nombre minimum de satellites égal à 3, on peut théoriquement déterminer le déplacement par l'intersection des 3 plans ainsi définis. Analytiquement, cela revient à résoudre un système linéaire de trois équations (ou plus) à trois inconnues. La force de cette approche par rapport à la précédente : il n'est pas besoin ici de passer par la linéarisation et un algorithme itératif. On peut faire appel à une méthode de décomposition de type QR ou factorisation de Cholesky, à l'image de ce qu'on rencontre pour certaines approches de levée des ambiguïtés entières pour le RTK [88].

L'idée de cette approche est venue en cherchant à adapter Grad Mouv aux satellites. Elle a permis de bien comprendre les sources d'erreur et les phénomènes physiques et géométriques mis en jeu. A partir de cela, la réflexion est ouverte. Si on tient compte de la problématique liée à l'ionosphère et la troposphère, on a des perspectives de travaux très intéressants. Si on privilégie les satellites à élévations hautes, on sait que les erreurs liées à l'ionosphère et la troposphère sont plus faibles sur le Time Relative Positioning. En utilisant des constellations multiples, on aura la possibilité d'en avoir en nombre suffisant, pour mener plus longtemps un calcul de déplacement de qualité sans avoir recours aux approches bifréquences pour supprimer l'influence de l'ionosphère, fusse au prix d'une dégradation de la dilution de précision. La question de la variation du biais d'horloge pourrait également être réglée d'une autre façon que ce que nous avons présenté : en faisant des différences simples entre satellites et en regardant comment transformer les équations pour se ramener au cas de la figure 13.

Une autre perspective intéressante concernerait, nous l'avons évoqué, l'application directe de Grad Mouv avec les satellites. On a vu que ce qui l'empêchait était le parallélisme des rayons incidents depuis deux positions de satellites. Si on attend suffisamment longtemps entre les deux prises (entre l'instant 1 et l'instant 2), les positions du satellite considéré seront suffisamment éloignées pour lever le parallélisme. Rien n'interdit alors, théoriquement, de mener le calcul avec Grad Mouv, comme cela a été fait pour des pseudolites. En effet, ce qui compte pour que l'algorithme soit stable, encore une fois c'est l'angle du déplacement du récepteur par rapport à l'émetteur. Cet angle peut parfaitement venir du déplacement de l'émetteur (ici le satellite) : la situation sera équivalente. L'important est qu'il y ait un angle significatif, peu importe que ce soit le mouvement du récepteur

ou de l'émetteur qui le crée. La question qui vient naturellement est : combien de temps faut-il attendre pour avoir un angle suffisant ? Nous avons mené quelques tests rapides pour lesquels, avec les seules mesures de phase, on arrive à calculer une position sans aucune correction au bout de 30 secondes. Cette position n'est pas centimétrique, plutôt de l'ordre de la dizaine de mètres, mais on peut reconnaître le caractère encourageant de ces premiers résultats. Les effets de l'ionosphère et de la troposphère n'ont pas été corrigés, or ils dégradent rapidement les mesures selon les résultats de [85]. Il faudrait étudier en détail le comportement de l'algorithme, comme cela a été fait pour les pseudolites. Les relations de dépendances des performances de la méthode vis-à-vis de la position des satellites méritent également une étude. Voilà des perspectives de travaux autour de cette approche, surtout lorsque l'on voit qu'aujourd'hui un fort accent est mis sur la recherche du positionnement précis sans calcul différentiel direct. Ce qui nous amène directement aux travaux de thèse en cours que nous encadrons sur le Precise Point Positioning.

Problématique du Precise Point Positioning, le PPP-RTK

L'expression Precise Point Positioning recouvre plusieurs techniques. La manière la plus aisée de le définir consiste à donner ses objectifs. Le but du PPP est de réaliser un positionnement centimétrique, voire millimétrique, sans faire appel directement aux approches différentielles de type RTK. Elle consiste essentiellement en une approche réseau du problème. Un récepteur GNSS relié à un réseau de stations qui lui envoie des informations permettant de corriger autant que possible les sources d'erreur liées au calcul de la position. Les sources d'erreur principales étant liées aux délais de propagation atmosphériques, aux éphémérides des satellites, à leurs horloges, aux retards liés à l'électronique des satellites mais aussi à des éléments auxquels on ne pense pas forcément, comme la position du centre de phase de l'antenne du satellite par rapport à son centre de masse. Ce dernier est l'objet du calcul des éphémérides, qui dérivent des équations de Kepler, alors que celui qui compte pour la mesure de temps de propagation est le centre de phase. Le reste des erreurs concernent le récepteur : l'antenne, les retards et le bruit propre. Dans sa version dite « conventionnelle », les mesures du récepteur utilisant le PPP sont considérées comme débarrassées de l'influence de l'ionosphère [89]. Cette définition peut varier selon les auteurs, celle-là présuppose l'utilisation d'un récepteur au moins bi-fréquence pour chaque constellation GNSS utilisée, ce qui fait grimper le coût global. En tout état de cause, le principe est de partir d'une position calculée à partir de mesures de code, déjà partiellement purgées d'un certain nombre d'erreurs, et d'améliorer petit à petit la précision en utilisant les mesures de phase de la porteuse.

La grande limitation de l'approche réside dans le temps qu'il faut pour converger vers une position centimétrique. Autant quelques secondes suffisent avec le RTK pour estimer les ambiguïtés entières (on en revient toujours à cette problématique), autant pour le PPP la convergence et donc la détermination en question, selon les méthodes et les conditions de réception peut prendre de plusieurs minutes à plusieurs heures. On résout souvent le problème en le posant de manière paramétrique (les paramètres en question étant les différentes erreurs prises en compte) avec une résolution itérative [90]. On comprend aisément que l'essentiel des travaux dans ce domaine se focalise sur l'amélioration de la vitesse de convergence. Les travaux en cours, réalisés dans le cadre d'une thèse avec la société Exagone, gestionnaire du réseau Teria, consistent à exploiter les CORS (Continously Operating Reference Stations) d'un réseau dédié au NRTK (N pour Network) pour améliorer la vitesse de détermination des ambiguïtés phase. Une approche hybride dite PPP-RTK utilise les données de correction obtenues en appliquant le RTK entre les stations du réseau. On

peut ainsi accélérer le processus de résolution en déterminant les paramètres atmosphériques. Les objectifs des travaux étant de travailler sur plusieurs aspects, entre autres de voir jusqu'à quel point on peut alléger le réseau, c'est-à-dire diminuer le nombre de stations nécessaires pour obtenir des performances acceptables. Les travaux s'orientent actuellement vers l'élaboration d'un estimateur qui permettrait de caractériser les performances d'un réseau en fonction de plusieurs critères, dont sa densité.

Ceci clôt la partie de ce mémoire consacrée au suite de mes travaux en lien avec le positionnement indoor. On voit que les pistes de réflexion sont encore très ouvertes et gardent de riches potentialités, bien que l'on se soit éloigné du positionnement indoor à strictement parler. Pour se permettre une métaphore, disons que l'arbre s'est ramifié à partir du tronc en trois branches : Grad Diff, qui reste sur l'axe principal, Grad Mouv qui peut s'étendre aux GNSS à l'extérieur, voire aux réseaux d'objets communiquant, puis l'étude du PPP-RTK qui dérive des précédents. Nous allons voir qu'il y a une quatrième branche qui semble un peu à part : le « spoofing » (ou leurrage) GNSS. J'ai été amené à y travailler dans des circonstances que nous allons préciser dans le chapitre suivant.

2.3 L'intégrité des systèmes de navigation

Comme je l'expliquais en introduction, faire des misères au récepteur GNSS est une tradition de mes travaux de recherche. D'habitude, mes intentions sont les meilleures du monde : il s'agit d'assurer la continuité du service de géolocalisation dans les milieux intérieurs. On peut cependant être moins bien intentionné : on parlera alors de leurrage ou spoofing. Le principe d'un leurrage GNSS est de faire croire à un récepteur qu'il est situé à une fausse position, soit une position différente de celle où il se trouve réellement. Les buts de ce genre d'attaque sont divers. Il y a le contexte militaire ou conflictuel pour lequel on cherche à perturber les capacités de géolocalisation de son adversaire pour l'intoxiquer, voire induire chez lui certains comportements pour l'amener dans un piège. Le principe de l'embuscade en fait. Le contexte civil n'est pas en reste. Les objectifs relèvent souvent de la crapulerie. On peut par exemple vouloir mettre en défaut un système de paiement automatisé, violer une zone de pêche interdite ou tricher sur les heures de conduite de ses chauffeurs routiers (la réglementation impose des pauses régulières à ceux-ci), etc. En somme, le leurrage est une action hostile. La question qu'on peut alors se poser : est-ce simple ? Puis viendra une deuxième question : en cas d'attaque, est-il facile de la détecter ?

2.3.1 Problématique technique du leurrage

Pour réaliser un leurrage, il faut répliquer le signal GNSS reçu par le récepteur avec quelques altérations adéquates. Il faut également s'assurer que le signal leurre prenne l'ascendant sur les signaux provenant des satellites au niveau du récepteur. La manière dont ces deux conditions sont remplies définit les catégories des leurres. On retient la classification proposée en [91] qui nous donne trois types de leurres, à laquelle on ajoute une catégorie sur les répéteurs :

1. les leurres répéteurs ou « meaconer »
2. les simulateurs de signaux GNSS "simples"
3. les leurres-récepteurs
4. les leurres "sophistiqués"

La première catégorie correspond à l'approche la plus simple et la plus aisée à mettre en œuvre : récupérer un signal authentique en plaçant une antenne à un endroit donné. Signal que l'on va amplifier et réémettre en direction de la zone où on veut effectivement leurrer les récepteurs GNSS. Le récepteur ainsi leurré calcule la position de l'antenne où le leurre a récupéré les signaux d'origine. C'est une forme particulière de ce qu'on appelle le « meaconing » [92], l'avantage étant ici de pouvoir très facilement leurrer les récepteurs utilisant de multiples constellations. On a en revanche peu d'emprise sur la position calculée par le récepteur, il est ainsi plus difficile de faire du contrôle de trajectoire.

La deuxième catégorie regroupe les simples générateurs pouvant émettre des signaux imitant d'authentiques signaux GNSS. Lorsqu'un récepteur en mode poursuite reçoit ces signaux, il les assimile à du bruit. Mais si ceux-ci sont suffisamment forts, ils peuvent prendre le pas sur les véritables signaux GNSS. Un SDR basique peut générer des signaux qui affectent le calcul de position, comme cela été démontré en 2018 avec un dispositif HackRF et une bibliothèque open

source (Wireless Attack Launch Box) [93]. Le tout associé à une astucieuse stratégie a montré qu'on pouvait leurrer un conducteur qui suit le GPS de sa voiture. La faiblesse de ce type d'attaque réside dans sa trop grande simplicité. En effet, il suffit au récepteur d'avoir un peu de mémoire courte des évènements récents pour s'apercevoir qu'il y a un problème. Les éphémérides et la position qui changent brusquement peuvent alerter le récepteur. Une fois le récepteur alerté, le spoofer devient alors un simple brouilleur rendant inopérant le positionnement.

La troisième 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 afin d'obtenir une position, l'horloge et les éphémérides des satellites des constellations GNSS. Ces informations permettent au leurre de configurer les faux signaux qu'il souhaite émettre. L'intérêt ici est de pouvoir réaliser des attaques plus subtiles et plus difficiles à détecter vu que la référence temps de la fausse constellation est la même que l'authentique. Nous avons déjà cité en introduction les travaux de Shepard en 2012 qui ont montré l'efficacité et l'impunité de telles approches sur un drone et sur un bateau en pilotage automatique en les détournant de leurs trajectoires.

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 véritable constellation de satellites. Une attaque qu'on pourrait qualifier de type « pseudolite ». On peut ainsi fortement compromettre l'efficacité des stratégies de détection utilisant la direction d'arrivée des signaux que nous verrons plus loin. En pratique, les conditions pour qu'un tel cas de figure soit opérant sont loin d'être faciles à mettre en œuvre.

2.3.2 Leurre cohérent : projet Angelas

Le consortium du projet Angelas dans lequel nous avons été impliqués avec l'ONERA, THALES, EDF, le CEA et l'Institut de Criminologie de Paris, consistait à répondre à la menace représentée par les survols de zones interdites, comme des centrales nucléaires, par des drones de petites tailles. Une idée pour les neutraliser consistait à leur envoyer un signal de leurre pour empêcher le survol de la zone en question. En associant le leurre avec les techniques de détection proposées par les partenaires, on pouvait définir une stratégie qui aurait permis, au moins théoriquement, de déterminer son point de récupération (l'endroit où il se pose) à partir du comportement du drone en vol autonome, sous l'influence d'un leurre. Pour réaliser cela, nous avons testé le comportement d'un drone sous l'effet d'un leurre cohérent. Commençons par définir celui-ci.

Leurre cohérent

Les leurres qu'on appelle "cohérents" arrivent à utiliser les métriques correspondant au calcul d'une position sans répercussion significative sur les résidus de pseudo-distances qui sont habituellement exploités par les algorithmes d'intégrité de type RAIM. La solution proposée par le leurre forme ainsi un tout « cohérent » qui rend la fraude difficile à détecter à partir des seules mesures et du calcul position/temps effectué. Il s'agit des leurres les plus simples à réaliser qu'on retrouve dans les trois premières catégories citées précédemment.

Pour être efficace, le leurre doit néanmoins résoudre un premier problème qui consiste à s'imposer sur le signal authentique. Pour cela il y a, en général, deux approches possibles :

1. Augmenter la puissance du signal jusqu'à ce que le signal authentique cède le pas sur celui du leurre.
2. Brouiller temporairement le signal authentique avant d'envoyer le signal leurre.

L'avantage de la première approche est sa simplicité. Il est assez facile d'augmenter la puissance d'un signal RF. Combiné à une antenne directive, les signaux GNSS étant reçus, nous l'avons vu, avec des puissances faibles, le résultat n'est pas compliqué à obtenir. En revanche, il est peu discret. En pratique, les rapports signal à bruit (SNR) des signaux satellites diminuent progressivement à mesure que la puissance reçue des signaux du leurre augmente. Les SNR devenant trop faibles, le récepteur perd les signaux satellites et finit par accrocher les signaux plus puissants. La figure 14, montre ce qui se passe en extrême limite de décrochage au niveau de la fonction d'auto-corrélation pour un signal satellite k :

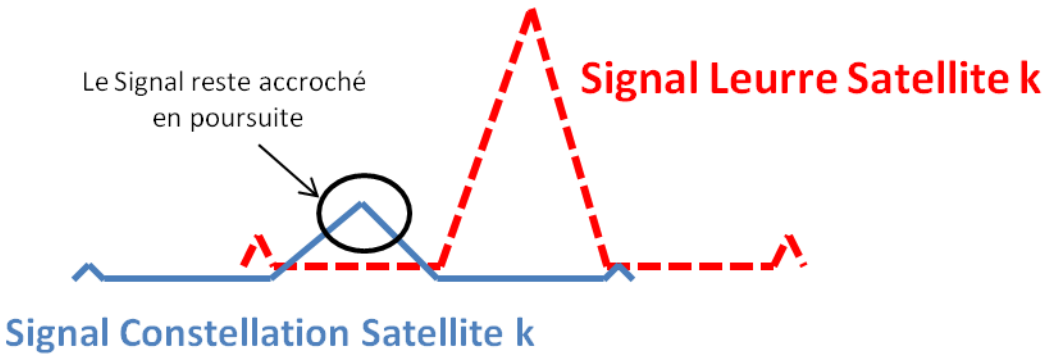

Figure 14

La seconde approche est plus subtile, au sens où, pour produire l'effet de perte du signal, elle fait appel au brouillage direct au lieu d'un effet de saturation qui se produit avec la première. Mais sur le principe, en termes de signal, elle revient au même : perte, suivie d'un accrochage sur le plus puissant. Avantage non négligeable : on n'a pas besoin d'émettre le leurre à une puissance trop élevée. Les expériences que nous avons menées sur un récepteur du type de ceux que l'on trouve dans les drones (µblox 6T-8T), montrent que la différence de puissance nécessaire pour que le récepteur s'accroche au signal du leurre est de 6 à 8 dB pour la seconde approche, alors qu'elle est de 25-30 dB pour la première.

Nous avons testé le comportement des récepteurs en modifiant les caractéristiques du signal leurre pour éprouver les stratégies d'intégrité mises en œuvre par ceux-ci. En complément des conclusions précédentes sur la puissance, on a pu mettre en évidence deux phénomènes liés à la fausse position et au temps :

- En changeant de constellation on réduit considérablement le seuil de 25-30 dB à 10 ou 15 dB selon l'éloignement du point.

- Pour qu'un leurre fonctionne, on doit surveiller le temps associé aux signaux du leurre afin qu'il s'éloigne le moins possible du temps de la constellation sur laquelle le récepteur était accroché.

On pourra objecter que les résultats de ces études concernent le récepteur que nous avons utilisé et que cela ne démontre que peu de choses quant aux réactions de l'ensemble des récepteurs GNSS existant. Cependant, des études postérieures aux nôtres que nous avons déjà citées [93] confirment ce type de comportement et la fragilité des récepteurs face à une attaque de leurre aussi simple que celle que nous avons décrite. Rappelons également que dans le cadre de cette étude, il s'agissait surtout de définir une attaque d'un récepteur GNSS d'un drone de petite taille, donc équipé d'un récepteur assez commun. Nous avons donc borné l'étude et nous maintenons ses conclusions générales pour ce qui concerne la majorité des puces GNSS que l'on trouve dans les applications grand public, comme les téléphones mobiles par exemple.

Il restait à vérifier si le leurre cohérent le plus simple qui soit induit bien le comportement qu'on attend sur le système de navigation d'un drone. Comme il est interdit d'émettre des signaux GNSS puissants, nous avons imaginé un protocole expérimental en liaison « filaire » pour le mettre en évidence. Nous nous sommes contentés de démontrer la capacité d'un leurre à créer une zone d'exclusion, soit une zone dont le drone se détournera automatiquement s'il est sous l'influence du leurre. Pour cela nous avons mis en place le montage suivant :

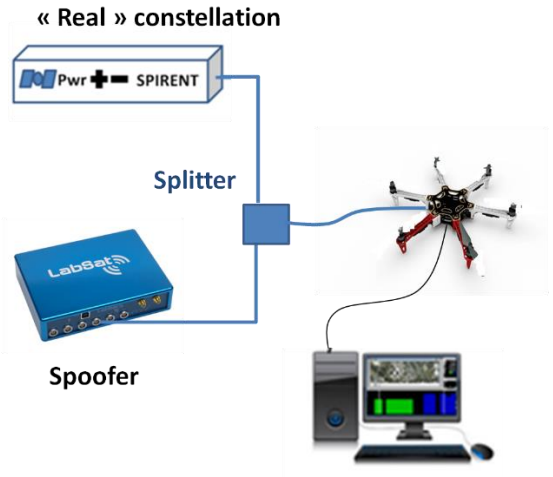

Figure 15

Un générateur de type SPIRENT qui simule ici la véritable constellation. Un simple répéteur de signaux (« spoofer ») qu'on active à un instant donné. Ce leurre consiste en un appareil (LabSat2) qui permet de rejouer un signal enregistré. Dans ces conditions, la configuration de leurre est équivalente à un répéteur qui enverrait son signal avec un retard de plusieurs secondes. Les deux sont reliés à un combineur (« splitter ») dont la sortie reliée au récepteur GNSS du drone (un µ-blox neo M8T) remplace l'antenne de celui-ci. Le contrôleur de vol est une carte Dropix 2 piloté par le firmware ardupilot. Du matériel tout à fait classique pour la communauté des praticiens du drone. Avec cette carte on peut définir un plan de vol. Nous le faisons sous la forme la plus simple qui soit : le déplacement d'un point de départ (Take off) jusqu'à un point défini à l'avance (Waypoint 1). On enlève les hélices du drone qui ne servent à rien, l'observation ne se faisant pas

au niveau du comportement du drone, mais dans les éléments télémétriques. La figure 16 montre en haut la description des scénarios mis en place. Les graphes en dessous indiquent les commandes des six moteurs (grandeurs proportionnelles à une tension électrique) que la carte de navigation leur envoie, respectivement à gauche pour le scénario 1 et à droite pour le scénario 2.

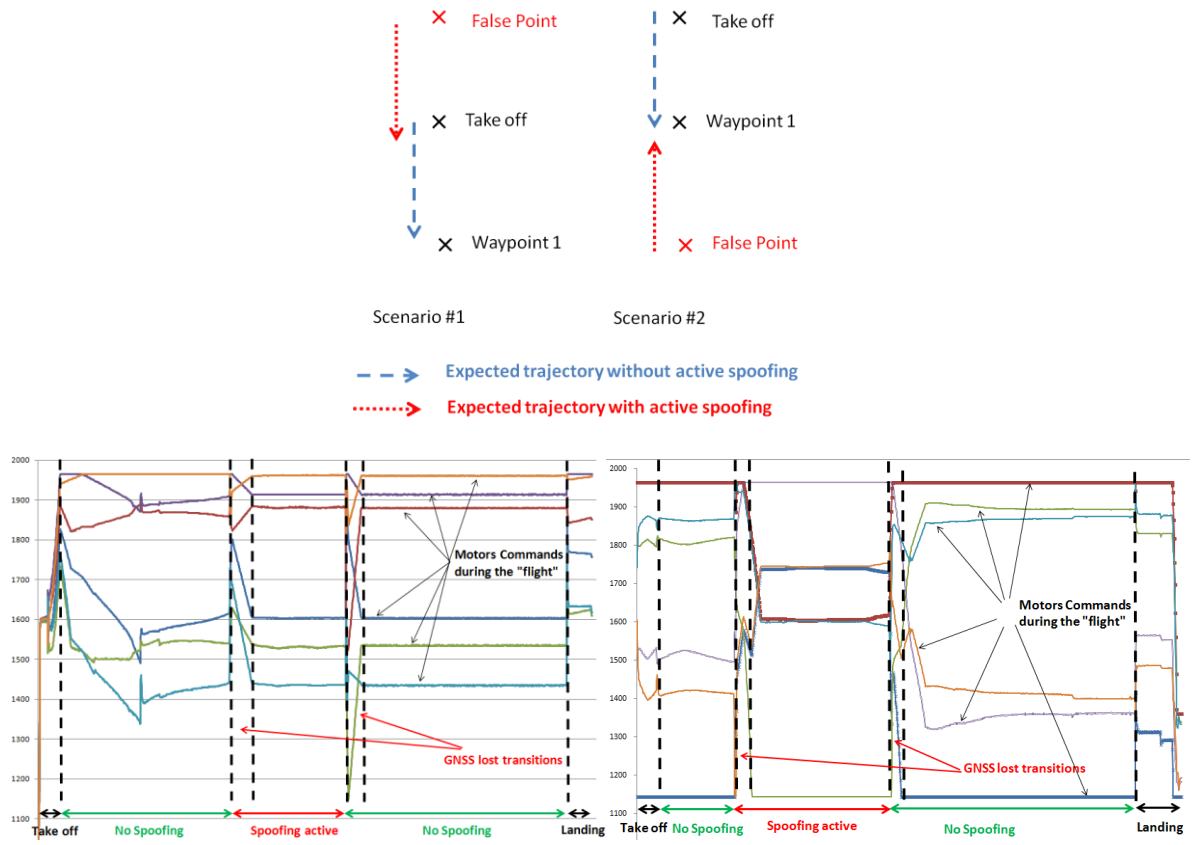

Figure 16

On met clairement en évidence ici que pour le scénario 1, la présence de leurre ou son absence n'entraîne pas de modification des commandes de vol. Le « faux point » est simplement un peu plus loin que le point de décollage. Comme l'indique la figure, on s'attend à la même trajectoire avec ou sans leurre. Pour le scénario 2 en revanche, on s'attend à ce que les commandes s'inversent lorsque le leurre s'active, le drone devant alors opérer une manœuvre de virage à 180 degrés. Si on ne peut pas conclure quant au comportement exact que cela produirait, on note quand même une inversion assez nette des commandes bien en contraste avec le scénario 1, qui semblent globalement se recaler lorsque le leurre n'est plus actif. Ces travaux ont fait l'objet d'un article [13].

Ainsi, on démontre qu'en faisant croire au drone qu'il est à une fausse position, et qu'en connaissant sa position réelle, on peut contrôler indirectement sa trajectoire si celui-ci est en mode de navigation autonome, donc sans pilote et suivant une trajectoire prédéfinie. Cela fonctionne avec un leurre tout à fait basique.

Après cette étude, dans le cadre de travaux avec THALES, nous nous sommes intéressés au problème inverse : comment détecter une attaque de leurre GNSS ? Avec des moyens limités mais potentiellement à grande échelle. Nous allons le voir dans la section suivante.

2.3.3 Détection du leurre

Nous venons de voir que l'attaque de leurre cohérent est assez efficace sur des récepteurs basiques. On entend par « basique » les récepteurs qui n'intègrent pas de stratégie anti-spoofing, c'est-à-dire la quasi-totalité des récepteurs grand-public et une bonne partie des récepteurs professionnels. En quoi consiste une stratégie anti-spoofing ?

Tout d'abord détecter l'attaque, puis enclencher un processus de défense pour échapper à l'influence du leurre, si cela est possible. Nous aborderons peu ce dernier point, sauf lorsque cela est pertinent, mais à ce stade il n'est pas inutile de savoir qu'il est généralement difficile de s'affranchir de l'influence d'un leurre autrement qu'en fuyant sa zone d'effet. Il y a deux grandes classes de stratégies de détection :

- 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).

Ces stratégies se déclinent ensuite avec différentes techniques :

- techniques de traitement du signal avancées 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

Nous allons présenter succinctement différentes approches de détection de leurre relevant de ces techniques avant de présenter la nôtre.

Traitement du signal[6] :

Il existe une série de méthodes qui opèrent avant corrélation, soit entre la numérisation du signal et sa démodulation. On comprend l'intérêt qu'il peut y avoir à surveiller ces étapes car, comme nous l'avons dit plus haut, le leurre cohérent forme un tout. S'il est bien conçu, les mesures falsifiées que le récepteur effectue sont en théorie trop parfaites pour déceler la fraude. Ainsi, en regardant ce qui se passe en amont, on peut espérer déceler des comportements « anormaux » permettant de caractériser une attaque.

La première de ces approches, bien connue, consiste à surveiller la boucle à contrôle automatique de gain (AGC) qui permet d'égaliser la puissance d'entrée avant la numérisation du signal. Considérant la distance entre récepteur et satellites, dans des conditions de fonctionnement « normales », soit une antenne à l'extérieur sous un ciel bien dégagé, les variations de puissance de réception entre les signaux des satellites n'excèdent pas une dizaine de dB. La plage dynamique de puissance d'un récepteur GNSS, qui correspond à la capacité à recevoir des signaux de puissances différentes, est donc en général faible, ainsi que le nombre de bits du numériseur de l'étage de

[6] Pour cette section je m'appuie essentiellement sur le recensement de [94]

conversion Analogique/Numérique. La boucle AGC garantit que les niveaux de puissance d'entrée soient compatibles avec les seuils du numériseur qui conserve ainsi sa capacité à représenter des signaux dans des gammes de puissances différentes, tout en le protégeant des variations brutales de celles-ci.

Lorsqu'un signal leurre s'ajoute brusquement aux signaux satellites authentiques, on observe une variation discontinue à tendance baissière du gain de la boucle AGC. Il baisse car la puissance du signal leurre est généralement plus élevée et nécessite donc moins de gain. L'idée développée par Denis Akos [95] est de détecter ces variations, donc d'analyser la variance en bande de base, pour caractériser une attaque. L'approche a quelques limites : d'abord, s'il y a un brouillage préalable, on verra bien une différence dans le gain de l'AGC, mais subsiste un doute sur la présence d'un leurre ou non vu que le signal leurre n'a besoin que de 6 à 8 dB de plus pour dominer le signal authentique. Il pourrait tout à fait s'agir d'un retour d'une situation de masquage. En somme, la caractérisation pour efficace qu'elle soit, n'est pas suffisamment systématique.

Une autre approche s'intéresse à la structure de la puissance du signal (Structral Power Analysis) [96]. Elle nécessite la manipulation donc l'accès aux échantillons numérisés I/Q. L'objectif est de repérer les anomalies de puissance dans la structure du signal. En effet la Densité Spectrale de Puissance (DSP) d'un signal satellite est un spectre de raies séparées d'1 kHz, de différentes puissances occupant une certaine largeur de bande (2 MHz pour le GPS L1 avec des raies d'une largeur de 50 Hz à cause de la modulation du message de navigation). Le spectre du signal GNSS résulte de la somme de l'ensemble des signaux satellites. En cas de présence d'un signal leurre, des raies vont s'ajouter aux autres sur le spectre et l'ensemble va donc présenter des anomalies de puissance. La méthode consiste à exploiter les propriétés cycliques des codes PRN. En multipliant le signal en bande de base par son conjugué décalé d'un chip du code, on élimine les Doppler de chaque signal tout en créant une nouvelle série de codes cycliques. Le résultat est filtré (numériquement) de deux façons : une pour retirer toutes les parties périodiques et ne laisser que le bruit et l'autre pour filtrer le bruit et ne garder que les composantes périodiques. Ce bruit est comparé à un seuil qui permet de détecter s'il y a présence de signaux leurres ou non.

Autre méthode : refaire l'acquisition du signal régulièrement [97]. L'idée est de rechercher toutes les corrélations avec tous les PRN, tous les décalages codes et tous les Doppler possibles. Avec un calculateur moderne ce n'est pas un problème. On compare alors les résultats au seuil d'acquisition et si le même PRN (satellite) apparaît plusieurs fois au-dessus du seuil d'acquisition, il y a une forte suspicion qu'un leurre soit à l'œuvre (à condition que la constellation leurre soit la même que l'authentique).

Le but de ces techniques est d'obtenir les caractéristiques des signaux (numéro de PRN, décalage code et Doppler) pour pouvoir opérer un tri entre les signaux leurre et les signaux authentiques pour éliminer ensuite les premiers. Une approche nommée Spoofing Detection Classification and Cancelation [97] regroupe les trois approches citées précédemment puis distinguent les signaux leurre des autres grâce à un déplacement mesuré par une centrale inertielle. Les signaux leurre auront tous la même variation Doppler puisqu'ils viennent de la même antenne, ainsi on peut les distinguer des autres. Une méthode de suppression successive des interférences est ensuite appliquée. Notons tout de même que pour être efficace l'approche nécessite de pouvoir distinguer

les signaux et donc, en lien avec ce que nous avons dit plus haut, un convertisseur analogique numérique à plusieurs bits (12 pour les expériences présentées).

Cette approche me rappelle des souvenirs. Une partie de ma thèse a été consacrée à la mise au point d'une méthode anti-éblouissement pour les pseudolites et j'y retrouve les mêmes logiques. Au fond, le leurre, lorsqu'il devient puissant, agit comme l'effet near-far (l'éblouissement) au niveau du récepteur en dominant tous les autres signaux. Retrouver des approches analogues pour supprimer ses effets n'est pas surprenant.

Le traitement du signal recouvre d'autres types de méthodes, comme la projection dans des sous espaces orthogonaux [98], déjà employés contre les trajets indirects et l'éblouissement. On peut également citer l'étude de la qualité de la fonction de corrélation (Signal Quality Monitoring). Le principe est proche de celui de l'analyse de la DSP mais se fait directement sur la corrélation. En effet un signal leurre va déformer la fonction d'autocorrélation. En récupérant les points de cette fonction et en l'étudiant, on peut déterminer si un leurre est présent ou pas sur le signal satellite [99]. L'avantage est qu'on n'a pas besoin des échantillons I/Q, les sorties de corrélateurs suffisent. Cela ressemble beaucoup aux approches pour distinguer les trajets indirects, la méthode s'en inspire d'ailleurs. Elle a les mêmes contraintes : il faut une bande passante suffisante (supérieure à 2 MHz pour le GPS L1 C/A) et une numérisation avec plusieurs bits pour que les indicateurs soient à même de distinguer les effets des faux signaux.

On peut également analyser les variations du Carrier To Noise Ratio (C/N0), information plus facilement accessible sur des récepteurs plus communs, même si la méthode n'est pas forcément compatible avec la précision standard avec laquelle les récepteurs délivrent cette information. L'idée est de proposer un modèle de canal de propagation pour le signal du leurre, en supposant que celui-ci étant en général au sol, la réception de son signal sera plus susceptible de souffrir de la présence d'obstacles. La difficulté est de trouver les seuils et le modèle statistique adéquats [100].

De cette section sur le signal, on peut conclure que les approches ont dans l'ensemble une bonne efficacité. Deux réserves cependant :

- En général elles nécessitent une sophistication de la numérisation et une bande passante qui ne sont pas applicables à la majorité des récepteurs GNSS (ce qui se comprend : pour travailler le signal, il faut que celui-ci soit représenté avec précision).
- Certaines situations naturelles provoquent sur le signal des effets analogues à ceux d'un leurre, on peut rapidement se retrouver avec un taux de fausses alarmes important et voir des leurres quand il n'y en a pas.

Chiffrement :

Je vais très peu parler du chiffrement parce que c'est une solution qui selon moi n'en est pas vraiment une et qui demanderait une transformation complète de la logique des GNSS. Tout d'abord, en quoi cela consiste-t-il ? Afin d'empêcher un leurre d'agir, on pourrait rajouter un étage de codage aux signaux GNSS. Il faudrait dès lors avoir la clé de cryptage du code pour exploiter les signaux et vérifier que ceux-ci ne sont pas faux, en supposant que le leurre ne connaît pas la clé en question. Le principe du chiffrement existe déjà dans les GNSS, depuis quasiment l'origine mais pour les signaux militaires. Le code P(Y) sur L1 et L2 en est l'illustration la plus fameuse. On

pourrait dire dans une certaine mesure que la Selective Availability du GPS, levée en 2000, était aussi une forme de chiffrement, mais c'est bien après sa suppression que la géolocalisation a véritablement explosé.

Je formulerai trois objections sur la pertinence de cette approche :

- Cela transforme complètement la philosophie qui a permis la diffusion des GNSS et leur exploitation en masse en instaurant nécessairement une relation serveur/client.
- Cela ne protège pas vraiment des leurres de type répéteurs.
- Cela rend inutilisables tous les récepteurs manufacturés depuis 1991 et ne peut donc concerner que les signaux modernisés (ce qui est le cas pour certains d'entre eux).

Sinon on peut citer quand même une approche consistant à parier sur le fait que le leurre ne va pas diffuser le code P du GPS (ou autres signaux cryptés des autres constellations). Dans ce cas, même sans connaissance exacte dudit code, on peut utiliser les caractéristiques communes entre celui-ci et le code civil pour détecter une attaque de leurre [101]. Ce n'est pas selon moi une méthode de chiffrement à proprement parler, cela nous ramène plutôt à une approche signal par différentiation.

Géométrie :

Quand on parle de géométrie, il s'agit en fait de s'intéresser à la direction d'arrivée du signal. En effet, pour la plupart des leurres cohérents, nous l'avons vu, le signal leurre est issu d'une seule antenne. Cela signifie que tous les signaux satellites ont la même direction d'arrivée, le leurre n'étant pas capable de falsifier cette information qui relève de la géométrie. La solution pour cela est d'introduire de la diversité spatiale. La solution la plus simple étant d'avoir deux (ou plusieurs) antennes séparées et reliées à deux récepteurs différents extrayant les mesures de phase de la porteuse. On peut ensuite réaliser des calculs d'interférométrie [102]. On obtient un résultat similaire en faisant bouger la même antenne [103], l'hypothèse étant que le leurre est suffisamment loin pour qu'un mouvement n'ait pas d'incidence sur l'angle entre les deux prises. Plusieurs approches existent, mais le principe est toujours le même : utiliser la différence de marche pour montrer que tous les signaux proviennent de la même direction (le même angle d'arrivée) lorsque le signal provient d'un leurre. On retrouve là les mêmes principes que Grad Diff, mais niveau réception. Comme l'objectif ici n'est pas de mesurer la direction d'arrivée, on lève la contrainte de la distance entre les antennes de l'ordre de λ, $\lambda/2$.

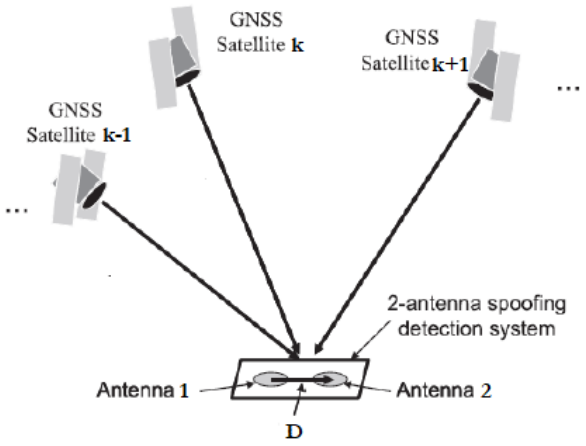

Figure 17

Les nuances entre les approches vont dépendre du matériel que l'on utilise et de la complexité du mouvement effectué. Si on considère le satellite k, pour deux antennes placées à côté l'une de l'autre (ou la même se déplaçant) à une distance D, la différence entre les pseudodistances phase de la porteuse pour chaque récepteur valent :

$$\Delta\varphi_k^{1,2} = \varphi_k^2 - \varphi_k^1 + \lambda.\Delta N_k^{1,2} + \Delta b^{1,2}$$

Avec $\varphi_k^2 - \varphi_k^1$ la différence entre les fractions de phase correspondant à une longueur d'onde pour chaque récepteur et $\lambda.\Delta N_k^{1,2}$ la différence entre les ambiguïtés entières du satellite k des signaux reçus par les récepteurs 1 et 2 et $\Delta b^{1,2}$ la différence entre les biais d'horloge.

Pour un signal provenant d'un leurre, la quantité : $\varphi_k^2 - \varphi_k^1 + \lambda.\Delta N_k^{1,2} = D\cos(\alpha_k)$ (α_k l'angle d'arrivée du signal du satellite k) est la même pour tous les satellites et varient de la même façon.

A partir de ce principe, se posent des problèmes qui sont liés aux paramètres que l'on connaît mal, donc le biais d'horloge et les ambiguïtés. En effet, les pseudodistances phase que l'on mesure ne donnent pas concrètement accès à la valeur de $\Delta\varphi_k^{1,2}$, sauf si on connaît la position du récepteur. Le problème du changement d'attitude des antennes qui fera varier l'angle α_k, en cas de récepteur en mouvement, doit également être géré. Les différentes approches existantes se proposent de résoudre ces problèmes. Le biais d'horloge peut être par exemple supprimé en mettant en commun les oscillateurs des deux récepteurs et une centrale inertielle peut assister le système pour déterminer l'attitude de l'ensemble des antennes. Une autre idée intéressante consiste à considérer les ambiguïtés comme des variables aléatoires qu'on ne cherche pas à déterminer tout en opérant une double différence pour éliminer le biais (on en revient toujours aux mêmes recettes). On estime les variances de ces doubles différences et, à partir d'une caractérisation statistique, on définit un seuil à appliquer à un estimateur qui permet de dire si les doubles différences sont statistiquement les mêmes pour tous les satellites ou si elles sont diversifiées comme en l'absence de leurre [104].

De ces approches dérive une solution pour éliminer l'influence du leurre. Un peu à l'image de ce qui peut se faire pour les trajets indirects, une fois qu'on a déterminé la direction d'arrivée du leurre, on peut former un creux à la réception dans la direction du signal leurre [105]. Cela nécessite d'avoir

une tête RF par élément du réseau d'antennes pour pouvoir faire le traitement d'annulation du signal leurre par orthogonalisation.

La géométrie propose une bonne approche avec quelques contraintes : le déplacement ou l'utilisation de plusieurs antennes. Reste bien sûr la menace d'un leurre de type pseudolite qui met en échec ces approches, mais qui n'est pas le sujet ici.

Contrôle de dérives et des métriques en général :

Ce type de défense va s'intéresser à la recherche de changements non usuels dans la position du récepteur GNSS, de son horloge ou de toutes sortes de calculs/mesures qu'il effectue au cours de sa navigation. L'avantage de ces approches est qu'elles travaillent essentiellement sur des données haut niveau, donc accessibles dans la plupart des récepteurs. Cela les rend plus facilement applicables et généralisables à des plateformes courantes, comme les Smartphones. La structure est toujours plus ou moins la même : on a deux blocs de données, un qui prédit, l'autre qui mesure. Lorsqu'on observe une variation trop importante entre prédiction et mesure, on émet une alarme. On peut s'intéresser aux Doppler satellites et s'attacher à détecter la variation nécessairement commune de par le mouvement relatif récepteur-leurre [106]. Une autre approche consiste à fusionner plusieurs observations (puissance, position, C/N0) pour parvenir au même résultat [107]. Autre 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. Les attaques dites de « meaconing » (par répétition du signal plus ou moins retardé) peuvent être ainsi détectées. C'est l'objet des travaux de [108]. Comme le signal est retardé, il y a des effets assez notables sur la dérive du biais d'horloge. Dans le même ordre d'idée, citons également des travaux sur le biais d'horloge réalisés par le PLAN Group de Calgary en 2012. En faisant bouger un récepteur sous l'influence d'un leurre cohérent, on peut mesurer les variations liées au mouvement sur le biais d'horloge [109].

C'est à ce dernier type d'approches que nous nous sommes intéressés, mais tirant profit de notre expérience des répéteurs, nous avons pris la question de façon plus directe que celle présentée précédemment.

Détection du saut de biais d'horloge

Pour l'avoir expérimenté depuis longtemps et avoir cherché à l'exploiter afin de calculer la position d'un récepteur en indoor, nous savons que la réception de signaux GNSS cohérents, transmis depuis une antenne unique, a une influence sur les pseudodistances mesurées et sur le biais d'horloge calculé. Le passage d'une source d'émission (la constellation de satellites) à une autre source (le leurre) va nécessairement se traduire par une variation dans la mesure des pseudodistances à cause de deux phénomènes : le changement d'horloge de référence et la distance entre le leurre et le récepteur. Revenons rapidement aux équations pour identifier les termes dont nous parlons :

$$\rho_j(t) = \sqrt{(x_j(t) - x_u(t))^2 + (y_j(t) - y_u(t))^2 + (z_j(t) - z_u(t))^2} + c\Delta t_u(t) \quad (1)$$

$$\rho_j^{spo}(t) = \sqrt{(x_j^{spo}(t) - x_{spo}(t))^2 + (y_j^{spo}(t) - y_{spo}(t))^2 + (z_j^{spo}(t) - z_{spo}(t))^2} + c\Delta\mathbf{t_{spo}}(\mathbf{t}) + \mathbf{d_{spo-u}}(\mathbf{t}) \quad (2)$$

(1) représente l'équation pour le satellite j à l'instant t avec la constellation de satellites authentique. On y reconnait la pseudodistance $\rho_j(t)$, les coordonnées des satellites (x_j,y_j,z_j) et les inconnues qui sont la position du récepteur (x_u,y_u,z_u) et le biais d'horloge noté t_u. L'équation (2) donne son équivalent en présence d'un leurre. Le leurre peut falsifier les éphémérides des satellites, mais surtout, indirectement, la position calculée par le récepteur. Il génère un signal dont le récepteur va extraire des mesures falsifiées le conduisant au calcul des coordonnées $(x_{spo},y_{spo},z_{spo})$. Dans certaines situations il peut aussi vouloir leurrer le calcul lié à l'horloge, nous y reviendrons plus loin. Sauf que le leurre ne contrôle pas tout, en tout cas pas dans n'importe quelle condition. La quantité $c.\Delta t_{spo}(t)$ correspond au biais entre l'horloge du récepteur et celle de la constellation du leurre, incluant tous les retards liés à l'électronique. La valeur de $d_{spo\text{-}u}(t)$ représente la distance entre l'antenne d'émission du leurre et celle du récepteur leurré, matérialisée par le temps de propagation du signal leurre jusqu'à celle-ci, que l'on retrouve donc dans la mesure de la pseudodistance. Lors d'une attaque de leurre, lorsqu'un récepteur passe d'une situation « non-leurrée » à une situation « leurrée », le premier terme change car l'horloge change et le second apparaît.

Partant de ce constat, les travaux réalisés dans le cadre de la thèse de Monsieur Victor Truong [th2], que nous avons encadrés, ont démontré qu'on pouvait détecter une attaque de leurre en suivant l'évolution du biais d'horloge et de sa dérive. La figure suivante montre l'effet typique d'une telle attaque sur le biais d'horloge et sa dérive pour un récepteur de type µ-blox 8 :

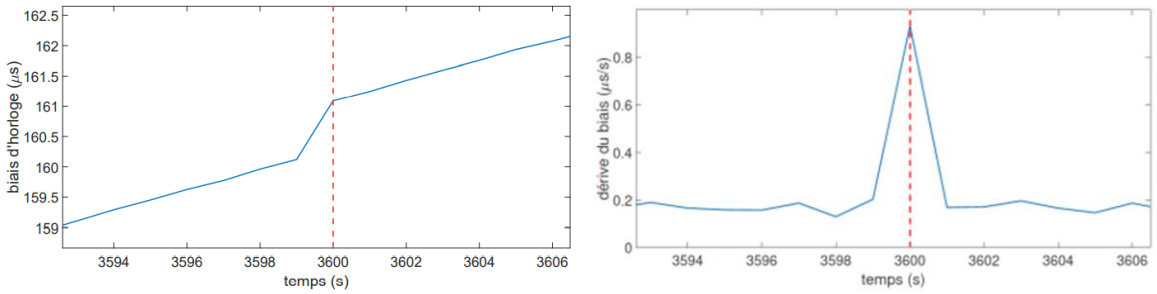

Figure 18

Pour réaliser ces expériences, on place à l'entrée, en filaire, deux générateurs de signaux dont l'un joue le rôle du signal authentique et l'autre celui du signal leurre que l'on active à un instant donné. Une alternative consiste à utiliser le même générateur, ici un SPIRENT GSS 6700, en dédiant la moitié des canaux aux signaux authentiques et l'autre moitié aux signaux leurre, qui sont en pratique des copies retardées dans le temps des canaux authentiques, que l'on peut activer et désactiver grâce à des commandes scriptées. L'avantage est de pouvoir ici contrôler la valeur de la somme des termes $c.\Delta t_{spo}(t) + d_{spo\text{-}u}(t)$ en induisant un retard sur l'ensemble des canaux des signaux leurre. Encore une fois ici, on détourne un outil de sa fonction principale pour faire apparaître et mesurer les phénomènes qui nous intéressent.

On a pu, grâce à ce dernier montage, tracer la courbe Receiver Operating Characteristic (ROC) pour les récepteurs µblox 6T et 8T pour les signaux GPS L1, avec l'approche de la détection de saut pour des valeurs de $c.\Delta t_{spo}(t) + d_{spo\text{-}u}(t)$ entre 0 et 1 µs et entre 0 et 0,5 µs.

Chaque point de la courbe a été obtenu en faisant varier le seuil entre 5 m et 0.3 m (en distance équivalente). On ne le voit pas bien sur la figure mais avec un seuil de 5 m la probabilité de détection

est de 0,73 et 0,87 pour le 8T et de 0,83 et 0,91 pour le 6T. On a des courbes qui sont proches du détecteur idéal, ce qui n'est pas surprenant vu qu'un saut a forcément lieu. Notre capacité à le détecter ne dépend que du bruit sur le calcul de la dérive du biais et donc de la méthode de son calcul que nous ignorons. On aurait un détecteur quasi idéal si on ne regardait que la variation des pseudodistances mesurées. Ici on s'oblige à passer par un résultat du calcul de position : on doit donc tenir compte du comportement lié à l'algorithme. C'est précisément ce qui est caractérisé par ces courbes et diffèrent entre deux versions du récepteur pour le même manufacturier. A première vue, le 6T est un meilleur récepteur pour la détection du saut lié au leurre que le 8T. Notre hypothèse pour l'expliquer se résume ainsi : il y a un filtrage, probablement un filtre de Kalman, dont le réglage est plus sélectif pour le 8T dont la tête RF est de meilleure qualité (les C/N0 des signaux satellites sont 6 à 8 dB meilleurs).

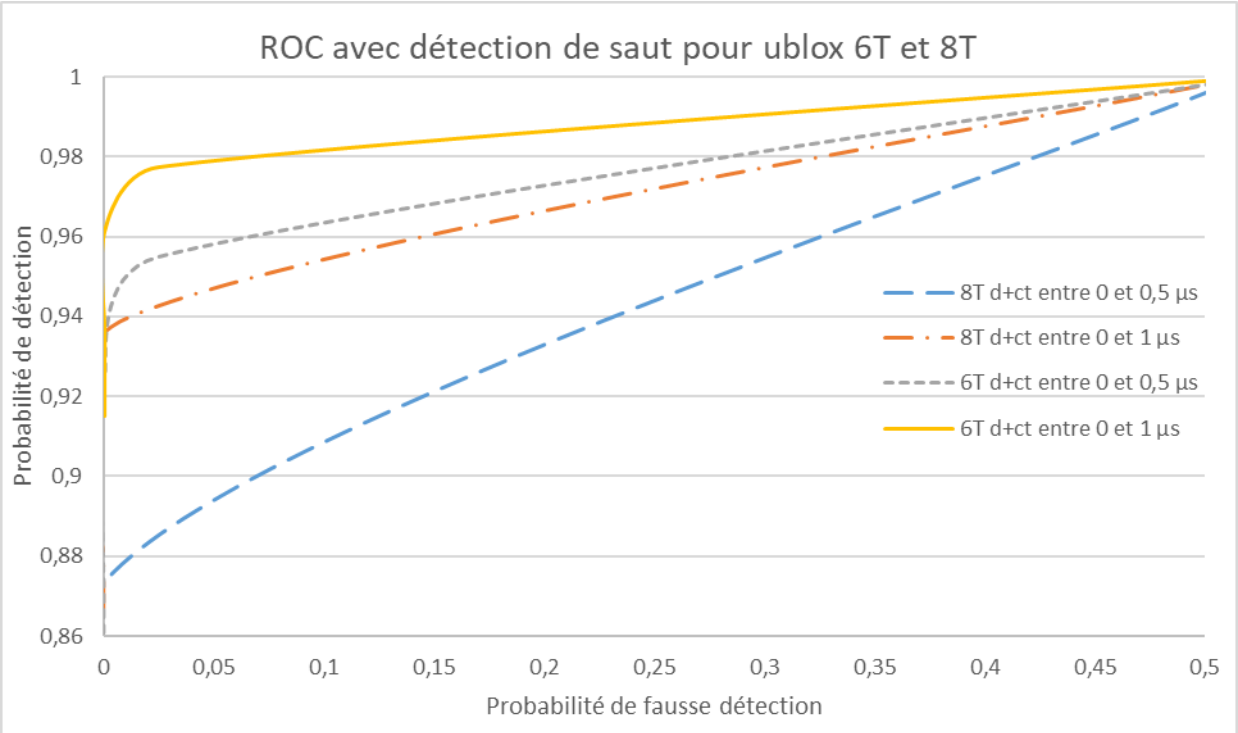

Figure 19

Cependant, il y a des phénomènes que les courbes ne mettent pas en avant mais qui sont propres au fait de travailler avec une donnée « haut niveau » dont on ignore globalement les mécanismes d'obtention. Quand bien même connaîtrions-nous précisément les algorithmes implémentés par le fabricant, il serait difficile d'anticiper leur comportement dans une situation pour laquelle ils n'ont pas été conçus. A titre d'illustration de mon propos, nous avons observé que le biais d'horloge faisait apparaître le saut lorsque le récepteur relançait une acquisition courte après une attaque. Plus cette attaque est forte, soit plus c. $\Delta t_{spo}(t) + d_{spo\text{-}u}(t)$ est grand, plus il a tendance à relancer une acquisition après quelques secondes sans en avoir préalablement tenu compte. Son filtrage élimine dans un premier temps le saut de la solution, mais comme ce saut est bien un offset sur la mesure, et pas un effet du bruit, la solution devient incohérente et l'oblige à relancer une acquisition rapide pour mettre à jour la mesure.

De l'intérêt et des limites de l'empirisme

On pourra légitimement s'étonner de la relative simplicité théorique de l'approche. Il ne s'agit au fond que de détecter un saut sur une donnée dont l'évolution est relativement stable en conditions normales. La complexité vient de sa mise en œuvre sur des plateformes dont on ne dispose que des sorties « haut niveau », ce qui oblige à une approche très empirique. Cela présente des avantages : comme on se situe très en aval du traitement du signal, on exploite des données faciles d'accès pour un coût dérisoire en termes de puissance de calcul comparé à certaines autres méthodes présentées plus haut. On peut aussi généraliser l'approche décrite pour caractériser le comportement de n'importe quel récepteur, quelle que soit leur sophistication. En revanche il y a certaines limites. Les comportements observés relève de l'interprétation, ce qui limite forcément la portée de toute tentative de généralisation, d'autant qu'il est très compliqué d'être exhaustif sur l'ensemble des situations rencontrées. Cela dit on peut formuler la même critique à l'ensemble des approches, simplement le travail à partir de données plus « haut niveau » a forcément un côté plus artificiel que nous assumons.

Bien sûr, cette approche de détection du saut sur le biais est loin de résoudre l'ensemble des cas. Les courbes présentées sont valables pour l'expérience réalisée qui, si elle simule des conditions très favorables pour l'attaquant (mêmes constellations, puissances de signaux suffisantes), ne représente pas un récepteur attaqué en conditions réelles. Surtout, il y a d'autres phénomènes susceptibles de provoquer des sauts sur le biais d'horloge que l'attaque d'un leurre (changement de constellation, apparition/disparition d'un satellite, masquage, etc.), même si les filtres mis en place sur le calcul du biais par le récepteur considéré ont justement un effet bénéfique de lissage sur ces phénomènes courants.

Qu'en-serait-il avec un leurre particulièrement retors ? Si on prend l'exemple du ublox 8T, pour le seuil le plus élevé (5 m), la somme c. $\Delta t_{spo}(t) + d_{spo\text{-}u}(t)$ doit être inférieure à 150 m pour qu'on rate la détection systématiquement. Un leurre désireux de passer inaperçu devrait dans ce cas-là neutraliser, donc annuler les effets de la somme de c. $\Delta t_{spo}(t) + d_{spo\text{-}u}(t)$. Pour cela, il peut commencer par se synchroniser sur la constellation réelle, ce qui est le cas d'un répéteur par exemple. Cependant, il faudrait être plus complexe qu'un répéteur car le temps passé dans le système de réception-amplification-réémission, qui inclut la longueur de câble entre l'antenne de récupération et l'antenne de réémission, ajoute un délai qui peut être de plusieurs centaines de nanosecondes (quelques dizaines de mètres). Ce délai ne peut pas être calibré, pas plus que la distance au récepteur qui s'y ajoute. Il a une chance de fonctionner s'il est suffisamment proche de la zone d'attaque et que les délais supplémentaires ne sont pas trop importants. Sa stratégie pourrait consister à placer antenne de récupération et antenne de réémission très proches pour minimiser le câblage et donc les délais. La contrepartie à ce dispositif : la position du leurre est donnée directement par le calcul de position au niveau du récepteur leurré. Si on a maintenant un leurre plus sophistiqué qui synchronise ses signaux sur ceux de la constellation en annulant le biais de son propre oscillateur (ce qui ne va pas de soi), il faut qu'il ait en plus la capacité d'avancer sa propre horloge pour annuler les effets de la distance entre lui et le récepteur. Un tel contrôle pourra intéresser les attaques sur le temps, qui ne cherchent pas à falsifier tant la position que la synchronisation du récepteur. Ce n'est pas impossible à faire, mais c'est plus compliqué et restreint la zone « furtive » du leurre dont le diamètre (ou la longueur maximale) n'excèdera pas 300 m, sinon les récepteurs 8T seront en mesure de détecter l'attaque. La conclusion est que, bien que l'approche

puisse être mise en échec, elle a quand même la potentialité de fonctionner relativement bien face à une attaque de leurre cohérent.

Que faire une fois l'attaque identifiée ? Si fuir la zone semble une bonne idée, une alternative peut consister à chercher à supprimer les effets du leurre. Plusieurs approches intéressantes existent, mais de notre côté nous nous sommes intéressés à la possibilité de localiser son antenne d'émission.

2.3.4 Localisation du leurre

Nos travaux sur la localisation du leurre ont commencé dans le cadre d'un projet avec THALES SIX. Le contexte du projet était le déploiement de drones à bas coûts, dotés de chipset GNSS standards pour détecter puis localiser un leurre. Le coût de chaque unité étant réduit, on a ainsi la possibilité d'en déployer en grand nombre avec des protocoles de détections peu calculatoires, compatibles donc avec une plateforme de type drone pour laquelle l'énergie disponible est limitée. S'appuyer sur du matériel de qualité standard mais en quantité, un principe qui n'a pas manqué d'attrait pour nous. Principe qui permet des effets de saturation à peu de frais et qui a montré une terrible efficacité dans l'actualité récente lors du court et très intense conflit entre l'Azerbaïdjan et l'Arménie pour le Haut Karabagh en 2020.

L'idée de localiser le leurre vient assez naturellement des observations de la section précédente. Le calcul du biais d'horloge, ainsi que les mesures de pseudodistances, contiennent une information sur la distance entre l'antenne d'émission du leurre et le récepteur leurré, que nous avons appelé $d_{spo\text{-}u}(t)$. On voudrait trouver un moyen de récupérer cette information et l'exploiter pour calculer la position, comme pour les approches répéteurs du positionnement indoor. Nos travaux, qu'on ne peut détailler plus avant ici pour des raisons de confidentialité, reposent sur ce principe. D'autres équipes ont déjà travaillé à cette fin en utilisant le biais d'horloge. En 2015, des expériences ont été menées par les équipes de l'université de Calgary [110]. D'autres travaux sur des récepteurs synchronisés en réseaux ont également montré la faisabilité de la localisation du leurre en utilisant le biais d'horloge [111]. D'autres approches ne s'intéressant pas au biais d'horloge existent également. On peut citer les approches basées sur l'estimation de la direction d'arrivée, par interférométrie étendue avec plusieurs antennes et récepteurs ou avec la diversité spatiale dans la répartition de la puissance. Il s'agit d'une sorte d'extension des approches de détection géométriques que nous avons vues plus haut. On peut également citer d'autres idées plus originales [112], mais également plus restreintes au niveau du type d'attaque considérée. Il s'agit ici d'utiliser des principes de calcul de doubles différences code à des instants différents, ce qui rappelle la section précédente de ce mémoire, pour déterminer la position de l'antenne de récupération du signal d'un leurre de type « meaconer ».

Nous avons déjà travaillé sur le sujet de la localisation de leurre lors de la thèse de Victor Truong [th2]. Il n'était pas alors question d'exploiter la distance contenue dans le biais d'horloge, mais d'utiliser plusieurs drones détectant une attaque et déterminant une direction d'arrivée du signal leurre grâce à leurs évolutions.

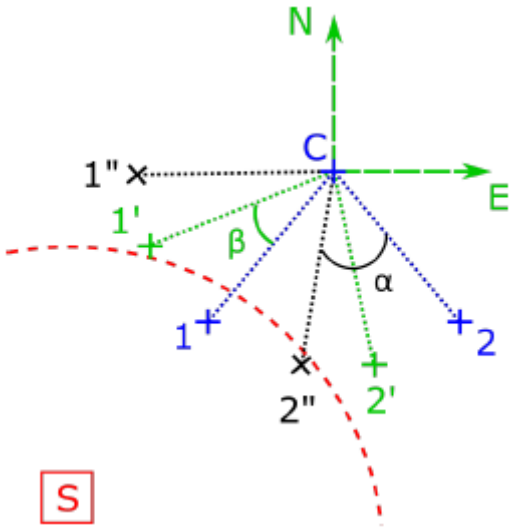

Figure 20

La figure 20 montre les évolutions d'un essaim à trois drones, deux d'entre eux (« 1 » et « 2 ») évoluant respectivement vers les positions « 1' », « 1" » et « 2' », « 2" », autour d'un autre situé en position central (« C »). On cherche à déterminer la direction d'arrivée du signal du leurre « S ». La procédure est la suivante :

1. L'essaim évolue en formation jusqu'à ce qu'au moins l'un des drones détecte une attaque.
2. Une fois l'attaque détectée, on décide quel drone servira de pivot (« C ») et quel(s) drones seront pivotant (« 1 » et « 2 »).
3. On commence à faire pivoter l'un des drones pris dans la zone d'attaque (« 1 ») jusqu'à ce qu'il sorte de la zone (position « 1' »), on note la dernière position calculée hors influence du leurre.
4. On fait tourner l'essaim dans l'autre sens jusqu'à ce que l'autre drone (« 2 ») entre dans la zone d'influence du leurre (« 2" »), on relève la dernière position calculé hors influence du leurre (« 2' »).
5. Une fois ces opérations effectuées, on calcule la direction d'arrivée à partir du point « C », ce qui correspond à la bissectrice de l'angle 1'C2' (on peut le faire avec plus de drones ce qui donnera une valeur moyenne)

La méthode suppose que le drone en « C » reste immobile pendant les opérations, mais c'était bien l'idée derrière ce projet dont l'origine était : utiliser des drones à bas coût en nombre dans des zones où les attaques ne sont pas forcément très sophistiquées. Quant à la mise en œuvre d'une telle approche, elle présuppose une capacité des drones de rester en formation et de faire tourner cette formation. Nous avions pensé à un asservissement qui mêlerait mesures de distance avec des modules UWB et fonction « follow me » basée sur de l'image et l'exploitation des capteurs inertiels. Un prototypage était prévu, mais des difficultés économiques rencontrés par le constructeur de drones ont provoqué l'annulation du projet financé sur Fond Unique Interministériel. THALES SIX a néanmoins soutenu les travaux de la thèse associée en dépit de cette annulation.

D'ailleurs les travaux sur l'ensemble de ces sujets sont toujours en cours et nous poursuivons notre collaboration avec THALES SIX dans ce domaine.

2.4 Conclusion

Dans cette conclusion, je vais résumer brièvement les contributions que j'ai présentées dans mon développement, j'insisterai sur les perspectives puis je terminerai sur quelques réflexions.

Synthèse

Mes travaux de recherche de ces dernières années reposent sur deux piliers, ou marchent sur deux jambes, selon qu'on préfère une métaphore statique ou en mouvement :

1. Le positionnement indoor à partir d'émetteurs locaux de type GNSS
2. L'attaque et la défense avec les leurres GNSS

Le positionnement indoor, qui reste mon expertise première, m'a permis de développer plusieurs approches dans le prolongement de mes travaux de thèse, prenant en considération les limitations physiques liées à la propagation en milieu intérieur. Les principes des systèmes Grad Mouv et Grad Diff ont chacun donné des résultats intéressants dans des registres différents. Grad Diff, basé sur de l'interférométrie, fait toujours l'objet de travaux sur les algorithmes de positionnement. Les développements autour de Grad Mouv ont permis de pousser la compréhension des mécanismes de calcul de positionnement absolu grâce à des mesures de variations de distances. En étendant la possibilité de l'application à l'extérieur avec les satellites, on a abouti à un calcul très simplifié du vecteur déplacement à partir des mesures de phase de la porteuse. Ces approches ont également mené à des travaux sur le positionnement d'objets mobiles dans un réseau à partir de divers degrés d'information sur les déplacements relatifs desdits objets.

Pour ce qui concerne les leurres GNSS, comme je le disais en introduction, c'est notre expertise dans le domaine des répéteurs qui m'a conduit vers ce sujet. J'ai d'abord étudié les effets d'une attaque, mis au point les protocoles pour réussir à prendre le contrôle indirect d'un drone en vol autonome et défini les expérimentations pour le démontrer. Je n'ai pas présenté dans ce mémoire toute l'étude sur le comportement en vol d'un drone attaqué par un leurre en fonction du récepteur et du système de navigation utilisés. J'ai simplement voulu montrer notre capacité à travailler dans un consortium en lien avec des industriels et à répondre aussi pertinemment que nous le pouvions aux attentes. Ce qui constitue à mes yeux une preuve du succès de l'étude est la poursuite de nos travaux dans le domaine à travers notre partenariat prolongé avec THALES, à la fois sur l'utilisation du biais d'horloge pour détecter les attaques et localiser le leurre. Localisation sur laquelle nous travaillons à partir d'autres approches, entre autre l'exploitation de ce même biais d'horloge (et sa variation), avec plusieurs récepteurs ou un même récepteur en mouvement.

Perspectives

On peut ici distinguer les perspectives en cours et les perspectives à moyen terme. Encore une fois je vais développer les deux axes indépendamment.

Pour ce qui concerne le positionnement indoor, la question générale reste ouverte. Il y a toujours de nouvelles méthodes, liées à des technologies ou à des approches émergentes ou réémergentes (comme le Machine Learning) qui sont explorées avec intérêt. Le fruit de ma réflexion sur le sujet m'amène à finalement privilégier les approches locales et décentralisées au détriment d'une

approche globale, séduisante mais trop calquée sur les GNSS. La communauté qui s'intéresse à ces questions suit une logique tout à fait conforme à cette réflexion, il n'y a plus grand monde aujourd'hui qui croit aux « killer applications » et leurs solutions définitives. De mon côté, je compte bien poursuivre ce que je sais faire le mieux, ce sur quoi j'ai capitalisé depuis toutes ces années, parce que les résultats sont fertiles, même s'ils n'avancent pas aussi vite que je le voudrais. Reprenons les exemples des systèmes Grad Div et Grad Mouv. Ont-t-il une vocation à être déployés pour des applications grand-public, industrielles voire militaires ? On doit admettre qu'en eux-mêmes, au stade de leur développement actuel, bien qu'ils fassent encore l'objet de travaux et de projets financés, ce serait un peu compliqué. Cependant, ce qu'on peut dire c'est qu'ils ouvrent des perspectives très intéressantes. On a vu qu'en tirant le fil de Grad Mouv, on parvenait à une estimation peu calculatoire du vecteur de déplacement d'un récepteur GNSS, qu'on pourrait imaginer appliquer à la calibration de la boussole d'un Smartphone par exemple. De même, comme je l'ai évoqué dans mon développement, Grad Mouv appliquée avec quelques adaptations non encore clairement formulées pourrait permettre un positionnement théorique de l'ordre de quelques décimètres avec un récepteur en mode autonome. Associé à des approches PPP ou RTK, il y a là un potentiel intéressant pour raccourcir le temps de convergence de la solution ou la récupération de la position après une perte liée à un masquage. Dans ce registre, Grad Diff n'est pas en reste puisque les premiers essais sur les algorithmes de positionnement par optimisation polynomiale sont surprenants et prometteurs à la fois.

En tous cas, je revendique cette dimension de la recherche pour laquelle, ce que nous faisons trouvera ses applications, même par fragments. Certaines choses resteront dans le domaine de la recherche et d'autres seront effectivement utilisées, même s'il ne s'agit que d'une petite partie de ce que nous aurons exploré. Certaines idées que nous considérons très bonnes aujourd'hui n'auront peut-être aucun avenir, alors qu'un point mineur sera d'un grand profit. Voilà pourquoi on doit poursuivre, je le redis, ce que nous savons faire de mieux : un sujet n'est jamais totalement épuisé et on peut toujours faire fructifier des branches que nous avons délaissées autrefois.

Pour ce qui concerne les leurres, la perspective générale est à peu près bien connue. On sait que la menace existe et qu'il y a un intérêt à développer des stratégies pour les contrer. De l'avis même des plus éminents spécialistes de la question, la réponse se doit d'être adaptée aux récepteurs et aux applications concernées [114]. Pour les récepteurs commerciaux, ceux sur lesquels nous travaillons, la variable « temps », donc le biais d'horloge, est considérée comme la plus pertinente. Nous partageons cette analyse et c'est pour cela que nos travaux vont dans cette direction, avec tous les avantages et inconvénients qui lui correspondent : les données exploitables sont abondantes pour la plupart des récepteurs, la contrepartie étant que ce sont des données issues de processus qui n'ont pas été conçus pour la fonction qu'on cherche à leur faire exercer. Une grande partie des travaux consiste en premier lieu à comprendre puis à adapter les données de sortie que l'on obtient. Une logique analogue à celle du capteur logiciel. Dans la mesure où dépasser ou contourner une contrainte reste à mes yeux un travail passionnant, ce n'est pas un souci majeur. Mon entrée dans ce champ de la recherche, si je n'en nie pas la dimension opportuniste, est à mes yeux assez en cohérence avec le travail sur les répéteurs, nous l'avons déjà mentionné. Simplement, puisqu'il est question de perspectives, je me trouve désormais, sur ce sujet particulier, impliqué dans ce qu'on appelle « la dialectique de l'épée et de la cuirasse ». Nous avons commencé en mettant au point des attaques, puis avons appris à les détecter. Nous allons à présent saisir à nouveau la poignée de l'épée

pour trouver la faiblesse de la nouvelle cuirasse. J'ai déjà évoqué les limites de la détection dans le chapitre consacré à ce sujet, nous devrions donc logiquement y travailler. Je précise qu'il est nouveau pour moi de travailler dans cette logique, nos approches et nos méthodologies sont au départ peu militaires. Mais comme l'a dit Léon Trotsky, qui, en grand praticien, s'y connaissait bien sur le sujet : « Ce n'est pas parce que vous ne vous intéressez pas à la guerre que la guerre ne va pas s'intéresser à vous. » Il avait raison, ou du moins pas tout à fait tort. Le contexte international dans lequel nous nous trouvons à l'heure où j'écris ces lignes rend cette citation particulièrement éloquente. Pour être tout à fait honnête, je dois reconnaître que les questions militaires et géopolitiques m'intéressent depuis bien avant que la problématique des leurres ne devienne un sujet d'études pour moi. Qu'il s'agisse d'une collision opportuniste, ou d'un tropisme inconscient, selon l'interprétation que l'on préfèrera, le résultat est là. Les perspectives à plus long terme sont, en plus de la dialectique sur le sujet des leurres, un élargissement aux questions de positionnement GNSS robuste, déjà largement traitées mais avec des approches originales, liées à l'ensemble de nos travaux.

Réflexion

Je suis bien conscient que la synthèse que je viens de présenter détonne un peu par rapport à l'introduction, aussi je me réserve cette ultime partie pour faire part de réflexions plus personnelles.

Je suis ingénieur de formation et je reste un ingénieur, cela se ressent dans mes travaux de recherche. J'espère être parvenu à le faire comprendre au fil de ces pages. Je suis aujourd'hui considéré comme un « enseignant en radio fréquence et électronique ». Je m'intéresse toujours à ces domaines, mais si le lien existe, le moins que l'on puisse dire est que mes travaux de recherche ont un lien assez indirect avec le cœur de ces domaines. Passionné par les sujets liés aux GNSS, j'ai commencé par faire beaucoup de traitement du signal, mes premières publications en thèse de doctorat en témoignent, et je garde une compétence forte dans ce domaine. Aujourd'hui je m'occupe principalement de géométrie et d'algorithmes de positionnement. Tout ceci s'explique très bien, encore une fois, par ma fibre d'ingénieur. A chaque fois qu'un problème s'est posé à moi, ma méthode d'analyse systématique a été d'identifier les points bloquant et d'approfondir les connaissances et compétences nécessaires pour le résoudre. Prenant également en compte les contraintes matérielles, je garde toujours à l'esprit de valider expérimentalement les avancées sur des données « réelles ». Cela peut sembler d'une grande banalité, il s'agit après tout d'une démarche assez classique, mais il ne me paraît pas absurde de le souligner. Si j'ai fait du signal, c'est parce que les trajets multiples, puis la question du near-far se sont posés à moi en ces termes. De la même façon Grad Mouv est venue d'une intuition que la géométrie imposait une unicité aux positions d'un déplacement.

Mais alors qu'est-ce que c'est que cet ingénieur qui veut diriger des recherches ?

Voilà la question (enfin) posée ! Justement, une fois le problème et ses contraintes définis, le travail de recherche à proprement parler commence. Les implications théoriques se déploient, on peut les retrouver aussi dans des problématiques haut niveau comme les mesures de distances ou plus bas niveau comme le signal. En résumé, l'ingénieur donne le cadre, le chercheur file la réflexion. C'est ainsi que les doctorants, stagiaires ou ingénieurs qui sont amenés à travailler sous ma supervision sont guidés. La première phase de plongée dans le bain est toujours délicate et chronophage, car

les sujets sur lesquels nous travaillons demandent un long temps d'apprentissage. Ce n'est qu'au terme de ce long apprentissage qu'on peut devenir vraiment productif.

J'aimerais à présent faire quelques remarques plus générales, sur les sujets évoqués dans ce mémoire et leurs implications.

On aura compris que nos approches sont assez diverses. Certaines épousent les tendances, d'autres moins. On aura noté qu'il y a peu d'Intelligence Artificielle dans mes perspectives, même si je ne m'interdis pas, on l'a vu, d'explorer les problématiques par cet axe « très tendance ». Mon point de vue, forcément discutable, est que si l'IA ouvre des perspectives énormes de recherche, il m'apparaît moins évident qu'elle ouvre des perspectives aussi énormes de solutions. Mais il en va de même pour chaque nouveauté. Au fond je reste très pragmatique et un peu conservateur, ce qui peut paraître un défaut dans la profession que j'exerce. Je me questionne souvent : est-ce que finalement ce n'est pas la logique du renard de la fable pour qui les raisins sont trop verts ? Est-ce une question de capacités ? Je suis loin d'être le plus brillant dans mon domaine et au fond si je suis parfois réticent à épouser les tendances, cette forme de conservatisme peut être une manière commode de cacher la crainte de ne pas comprendre ce que la modernité apporte. M'interroger sur ce que je fais, et a fortiori sur ce que je ne fais pas, me semble un moyen commode de résister à l'inertie naturelle de mon caractère tout en en tirant partie. Cependant, en contrepoint à ce que je viens d'écrire, je revendique paradoxalement une certaine originalité. Je veux bien questionner cette originalité, admettre qu'elle n'est pas pertinente en tous sujets, qu'elle se cache parfois un peu derrière la misère des moyens disponibles qui est depuis quelques années l'apanage de la recherche française. Toutefois il me semble avoir tenté dans ce mémoire de donner une consistance et une cohérence à cet ensemble. J'espère y être parvenu.

Pour revenir un instant sur la question des moyens. Dans notre beau pays, on est toujours enclin à ne pas se satisfaire de ce qu'on a. Certains pensent qu'il s'agit d'un trait de caractère très français hérité des origines paysannes de notre nation (le laboureur soldat est notre substrat). Ne jamais se satisfaire de ce qu'on possède est une forme de superstition. Je ne déroge pas à la règle et m'inscris dans cette tradition, mais seulement dans une certaine mesure. Je ne dirais pas que les moyens manquent, ce qui manque est plutôt une certaine aisance. J'entends par là une absence de limitation, raisonnable, dans les possibilités d'expérimenter le fruit de nos réflexions. J'ai la chance de travailler dans un domaine, me situant essentiellement au niveau traitement des récepteurs, où on peut avancer sans nécessiter des frais immenses. On pourrait arguer que les SDR, les matériels reconfigurables, ainsi que le développement du logiciel libre offrent des possibilités à peu près illimitées. Je nuancerai toutefois ceci en rappelant que le matériel ne remplace pas le temps de développement. Entre la fin de ma thèse et mon intégration à Télécom Sud-Paris en tant qu'enseignant-chercheur, j'ai fait du développement sur récepteur logiciel. Je sais que cela prend du temps. Le coût n'est pas seulement financier, le temps passé au développement doit être ajouté au compte final. Notre charge administrative personnelle limite forcément le temps que nous pouvons consacrer au développement. Si on se dit que l'on devrait logiquement le confier à des ingénieurs, des étudiants ou des stagiaires, on revient sur la contrainte que j'évoquais plus haut sur le temps qui doit être consacré à l'initiation au sujet.

Lorsque je réfléchis à mon « positionnement » en tant que chercheur, je conclus que je me situe en aval des considérations matérielles, lorsqu'il faut raisonner sur le système. Pour faire un peu de

provocation, gratuite, je dirais qu'au fond un matériel ne vaut pas grand-chose en tant que tel. Il doit s'inscrire dans un système. On peut avoir un bijou technologique doté de toutes les qualités intrinsèques, il ne vaut rien s'il n'est pas l'outil de mise en œuvre d'une doctrine. L'histoire des techniques est une longue litanie… Léonard de Vinci est un technicien de génie dont les inventions fabuleuses, ses machines de guerre dont il était spécialiste, n'ont pas fait la différence lors des guerres d'Italie. On peut être fasciné par la technicité des chars allemands de la seconde guerre mondiale, c'est le fragile Sherman américain et le rustique T34 soviétique qui ont finalement emporté la guerre. Moins martial et plus près de nous l'échec du Concorde ou encore plus près celui de l'A380 en sont des illustrations presque d'école. Il faut parfois privilégier une efficacité moyenne mais dotée d'autres qualités plus utiles lorsqu'elles servent une doctrine d'emploi. A ce jeu, le nombre l'emporte souvent sur la qualité. Ce qui ne signifie pas, d'un point de vue scientifique, qu'il ne faille pas creuser en direction de la qualité. Néanmoins, d'un point de vue macroscopique, et nos métiers ont aussi pour objectif de se mettre au service de la masse, il ne faut pas rejeter ou mépriser ce qui semble à priori moins dans le haut de la gamme. L'exploitation optimale du matériel le moins cher, avec des considérations algorithmiques simples, ont, selon moi, beaucoup d'avenir. Ne serait-ce que pour des aspects énergétiques, amenés à devenir de plus en plus prégnants pour l'avenir. Dans ce contexte, il me semble opportun de développer des approches qu'on peut qualifier d'astucieuses, ou de contournement. Approches qui ne prennent pas de front les défis technologiques par l'amélioration du matériel, dont le passage à l'économie d'échelle prend fatalement du temps, et pose de surcroît des questions pour l'accès à certaines ressources nécessaires, qui deviennent vite des problèmes géopolitiques. On sait ce qu'il en est des métaux rares et de la politique d'expansion chinoise en Afrique par exemple.

Une autre réflexion, corollaire de la précédente, sur la recherche de la rupture technologique. Le discours médiatique se délecte de cette fable que je considère loin de la réalité de la pratique scientifique. Pour compréhensible que cela soit, ce discours pèse sur les décideurs, industriels et politiques, qui sont nos sources de financement. C'est une partie de notre éthique, en tous cas c'est la mienne, de garder un œil critique et distancié qui nous permet de distinguer entre les modes scientifiques et une véritable rupture. Les véritables ruptures sont rares et dépendent des circonstances propices ou non. Je reviens sur les exemples militaires : l'arme à feu portative (le fusil), l'avion, le char d'assaut et le missile incarnent des ruptures au sens où ils ont forcé leurs intégrations dans les doctrines d'emplois existantes, jusqu'à les faire changer. Pourtant les autres armes issues d'héritages plus anciens ne cessent pas brutalement d'exister, ni d'évoluer. Le canon existe toujours, les avions à hélice aussi. La source dont le monde tire l'essentiel de son énergie reste le charbon, dont le destin industriel a commencé au début du XIXème siècle. Il existe même des procédés inventés pendant la première guerre mondiale pour faire de l'essence à partir du charbon… Tout ceci pour illustrer qu'en l'absence de véritable rupture technologique, on peut choisir de s'efforcer à exploiter au mieux les technologies existantes, voire régénérer celles qu'on considère comme dépassées. L'armée de l'air américaine a un temps envisagé d'investir dans les avions à hélices, beaucoup moins coûteux et déployables en grand nombre, pour maintenir la supériorité aérienne une fois celle-ci acquise par ses matériels plus sophistiqués comme le (très) coûteux F-35. Cette idée a semble-t-il été abandonnée, il n'est pas exclu qu'elle fasse son retour d'ici quelques années.

Enfin, je terminerai sur une évocation de l'actualité dramatique qui se déroule à l'est du continent européen. Les leurres GNSS semblent participer à ce conflit. Il y a déjà eu des incidents en Mer Noire au cours de ces dernières années [115] et en Finlande [116] Il faut toujours rester prudent vis-à-vis des informations qui remontent en temps de conflit, mais il semble que depuis le déclenchement de la guerre en février dernier les brouillages/leurrages sont signalés dans la zone [117] et perturbent le trafic aérien.

Un triste rappel que les GNSS, comme la géographie [118], cela sert d'abord à faire la guerre.

2.5 Références

[49] Bernard VANDERMEERSCH, article « Homo Sapiens Sapiens » pour l'Encyclopédia universalis édition en ligne française.
Lien : https://www.universalis.fr/encyclopedie/homo-sapiens-sapiens

[50] Philippe Forget Gilles Polycarpe, (1997) « Le réseau et l'infini. Essai d'anthropologie philosophique et stratégique », Economica.

[51] Paul Veyne, « Y a-t-il eu un impérialisme romain ? » Mélanges de l'école française de Rome. 1975. pp 793-855.

[52] Raymond Aron, « Leçons sur l'histoire: cours du Collège de France », 1972-1974.

[53] Nel Samama, (2019) "Indoor Positioning, Technologies and Performance.", Chap 1, pp 1-15, Wiley-IEEE Press.

[54] Kaplan, E.D. and Hegarty, C. (2017). "Understanding GPS/GNSS: Principles and Applications", chap 14, p 935, 3e Artech House

[55] Puricer P., Kovar P. "Technical Limitations of GNSS Receivers in Indoor Positioning.", the 2007 IEEE 17th International Conference Radioelektronika, Brno, Czech Republic, 24–25 April 2007, pp. 1–5.

[56] Frank Van Diggelen, (2009) "A-GPS: Assisted GPS, GNSS, and SBAS" , Artech.

[57] G. Lachapelle, H. Kuusniemi, D. T. H. Dao, Macgougan G. & Cannon M. E., "HSGPS signal analysis and performance under various indoor conditions", *Proceeding of GPS/GNSS Conference*, pp. 1-14, 2003.

[58] Pany T., Riedl B., Winkel J., Woerz T., Schweikert R., Niedermeier H., Lagrasta S., Lopez-Risueno G., Jiménez-Baños D., "Coherent integration time: The longer, the better.", Inside GNSS 2009, 4, 52–61.

[59] Kaplan, E.D. and Hegarty, C. (2017). "Understanding GPS/GNSS: Principles and Applications", chap 11.4.3 , pp 693-704, 3e Artech House.

[60] Brown R. G., "GPS RAIM: Calculation of Thresholds and Protection Radius Using Chi-Square Methods-A Geometric Approach," ION Red Book Series, Volume 5, Global Positioning System, Papers Published in NAVIGATION, 1998.

[61] Scott L. "Anti-Spoofing and Authenticated Signal Architecture for Civil Navigation Systems", ION GPS 2003, Portland, Oregon USA, 2003.

[62] US Government, "NAVSTAR GPS Space Segment/Navigation User Interfaces", IS-GPS-200D, May 21, 2021.

[63] Warner J.S. and Johnston R.G., "A simple demonstration that the global positioning System (GPS) is vulnerable to spoofing", Journal of Security Administration, 2002.

[64] Shepard D. P., Bhatti J. A., Humphreys T. E. and Fansler A. A., "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," ION GNSS, Nashville, USA September 2012.

[65] University of Texas News, " UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea"
https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

[66] Rawnsley A., "Iran's Alleged Drone Hack: Tough, but Possible," Dec. 2011, http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps/#.

[67] CEPT, ECC "ECC REPORT 183 Regulatory Framework for Outdoor GNSS Pseudolites." February 2013.
[68] Sakpere W., Adeyeye-Oshin M. and Mlitwa N.B.W. "A state-of-the-art survey of indoor positioning and navigation systems and technologies." South African Computer Journal, 2017, 29 (3), 145-197.
[69] Kim B., Choi B., Kim E. and Yang K., "Indoor localization using laser scanner and vision marker for intelligent robot," *2012 12th International Conference on Control, Automation and Systems*, 2012, pp. 1010-1012.
[70] Moreno M. V., Zamora M. A., Santa J. and Skarmeta A. F., "An Indoor Localization Mechanism Based on RFID and IR Data in Ambient Intelligent Environments," 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2012, pp. 805-810.
[71] Medina C., Holm S. and Segura J.C., "Feasibility of ultrasound positioning based on signal strength", Indoor Positioning and Indoor Navigation (IPIN), International Conference on, pp. 1-9, Sydney,Australia, November 2012.
[72] Binghao Li, Harvey B. and Gallagher T., "Using barometers to determine the height for indoor positioning," International Conference on Indoor Positioning and Indoor Navigation, 2013, pp. 1-7.
[73] Hsu C. and Yu C., "An Accelerometer Based Approach for Indoor Localization," 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, 2009, pp. 223-227.
[74] Renaudin V., Afzal M. H. and Lachapelle G., "New method for magnetometers based orientation estimation," IEEE/ION Position, Location and Navigation Symposium, 2010, pp. 348-356.
[75] Nel Samama, (2019) "Indoor Positioning, Technologies and Performance.", Chap 7, pp 145-156, chap 8 pp 180-186, chap 9 pp 191-216, chap 10 pp 223-239, Wiley-IEEE Press.
[76] H. Borstell, S. Pathan, Liu Cao, K. Richter and M. Nykolaychuk, "Vehicle positioning system based on passive planar image markers," International Conference on Indoor Positioning and Indoor Navigation, 2013, pp. 1-9.
[77] Qi J., Liu GP., "A Robust High-Accuracy Ultrasound Indoor Positioning System Based on a Wireless Sensor Network." *Sensors (Basel)*. Published 2017 Nov 6. MDPI.
[78] M. Romanovas, V. Goridko, A. Al-Jawad, M. Schwaab, M. Traechtler, L. Klingbeil, and Y. Manoli. "A study on indoor pedestrian localization algorithms with foot-mounted sensors." In 2012 International Conference on Indoor Positioning and Indoor Navigation (IPIN), pp 1-10, 2012.
[79] V. Renaudin *et al.*, "Evaluating Indoor Positioning Systems in a Shopping Mall: The Lessons Learned From the IPIN 2018 Competition," in *IEEE Access*, vol. 7, pp. 148594-148628, 2019.
[80] Kaplan, E.D. and Hegarty, C. (2017). "Understanding GPS/GNSS: Principles and Applications", chap 9.5 , pp 599-612, 3e Artech House.
[81] A. Leick, L. Rapoport, D. Tatarnikov, "GPS Satellite Surveying", chap 7 pp 401-474,4th Wiley.
[82] H. Perakis and V. Gikas, "Evaluation of Range Error Calibration Models for Indoor UWB Positioning Applications," 2018 International Conference on Indoor Positioning and Indoor Navigation (IPIN), 2018, pp. 206-212.
[83] A. R. Jiménez and F. Seco, "Comparing Decawave and Bespoon UWB location systems: Indoor/outdoor performance analysis," *2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2016, pp. 1-8.

[84] Stark H. and Woods J. W., "Probability, Random Process, and Estimation Theory for Engineers", EngleWood Cliffs, NJ: Prentice-Hall, 1986.
[85] Mohamed ali Chouaer, « Utilisation du Positionnement Relatif Temporel GNSS pour l'auscultation topographique et la mesure des vagues. », Mémoire de Maîtrise en Sciences géomatiques, Université de Laval, Québec, Canada.
[86] Traugott J., Holzapfel F. and Sachs G., "Conceptual Approach for Precise Relative Positioning with Miniaturized GPS Loggers and Experimental Results", march 31st 2010. https://www.sto.nato.int/publications/STO%20Educational%20Notes/RTO-EN-SET-116-2010/EN-SET-116(2010)-04.pdf
[87] Kaplan, E.D. and Hegarty, C. (2017). "Understanding GPS/GNSS: Principles and Applications", chap 2.5 , p 69, 3e Artech House.
[88] Kaplan, E.D. and Hegarty, C. (2017). "Understanding GPS/GNSS: Principles and Applications", chap 12, pp 732-737, 3e Artech House.
[89] Kaplan, E.D. and Hegarty, C. (2017). "Understanding GPS/GNSS: Principles and Applications", chap 12, pp 746-752, 3e Artech House.
[90] Wabbena, Gerhard, Schmitz, Martin, Bagge, Andreas, "PPP-RTK: Precise Point Positioning Using State-Space Representation in RTK Networks," Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005), Long Beach, CA, September 2005, pp. 2584-2594.
[91] 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.
[92] Sait Murat Giray, "Anatomy Of Unmanned Aerial Vehicle Hijacking With Signal Spoofing", 6th International Conference on Recent Advances in Space Technologies (RAST), pages 795 – 800, June 12-14, 2013, Istanbul, Turkey.
[93] Kexiong (Curtis) Zeng & Al.,"All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems" 27th USENIX Security Symposium. August 15–17, 2018, Baltimore, MD, USA.
[94] 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.
[95] D. M. Akos, "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)", Navigation, vol. 59, pp. 281-290, Dec. 2012.
[96] A. Jafarnia, A. Broumandan, J. Nielsen and G. Lachapelle (2014) "Pre-Despreading Authenticity Verification for GPS L1 C/A Signals." Navigation, 61(1): 1-11.
[97] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver," GPS Solutions, vol. 19, no. 3, pp. 475–487, 2015.
[98] S. Han, L. Chen, W. Meng, and C. Li, "Improve the security of GNSS receivers through spoofing mitigation," IEEE Access, vol. 5, pp. 21057–21069, 2017.
[99] E. G. Manfredini, F. Dovis and B. Motella, "Validation of a signal quality monitoring technique over a set of spoofed scenarios," 2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2014, pp. 1-7.
[100] Dehghanian Vahid, Nielsen John, Lachapelle Gérard, "GNSS Spoofing Detection Based on Receiver C/No Estimates," Proceedings of the 25th International Technical Meeting of the

Satellite Division of The Institute of Navigation (ION GNSS 2012), Nashville, TN, September 2012, pp. 2878-2884.

[101] 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.

[102] Montgomery, P. Y., Humphreys, T. E., & Ledvina, B. M. (2009, January). Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In Proceedings of the 2009 International Technical Meeting of The Institute of Navigation (pp. 124-130).

[103] Psiaki, M.L., Powell, S.P., O'Hanlon, B.W., "GNSS Spoofing Detection using High-Frequency Antenna Motion and Carrier-Phase Data," Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2013), Nashville, TN, September 2013, pp. 2949-2991.

[104] D. Borio and C. Gioia, "A sum-of-squares approach to GNSS spoofing detection," in IEEE Transactions on Aerospace and Electronic Systems, vol. 52, no. 4, pp. 1756-1768, August 2016.

[105] Daneshmand, Saeed, Jafarnia-Jahromi, Ali, Broumandon, Ali, Lachapelle, Gérard, "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012), Nashville, TN, September 2012, pp. 1233-1243.

[106] W. Qi, Y. Zhang and X. Liu, "A GNSS anti-spoofing technology based on Doppler shift in vehicle networking," 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), 2016, pp. 725-729.

[107] L. Chiarello, A. V. Guglielmi, N. Laurenti, F. Bernardi, F. Longhi and S. Fantinato, "Detection of GNSS Spoofing by a Receiver in Space via Fusion of Consistency Metrics," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1-6.

[108] D. Marnach, S. Mauw, M. Martins and C. Harpes, "Detecting Meaconing Attacks by Analysing the Clock Bias of GNSS Receivers", Artificial Satellites, vol. 48, no. 2, pp. 63-83, 2013.

[109] A. Jafarnia-Jahromi, S. Daneshmand, A. Broumandan, J. Nielsen, and G. Lachapelle, "PVT solution authentication based on monitoring the clock state for a moving GNSS receiver," in European navigation conference (ENC), vol. 11, 2013.

[110] Broumandan Ali, Jafarnia-Jahromi Ali, Daneshmand Saeed, Lachapelle Gérard, "A Network-based GNSS Structural Interference Detection, Classification and Source Localization," Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2015), Tampa, Florida, September 2015, pp. 3358-3369.

[111] S. Bhamidipati and G. X. Gao, "GPS Multireceiver Joint Direct Time Estimation and Spoofer Localization," in IEEE Transactions on Aerospace and Electronic Systems, vol. 55, no. 4, pp. 1907-1919, Aug. 2019.

[112] S. Shang, H. Li, C. Peng and M. Lu, "A Novel Method for GNSS Meaconer Localization Based on a Space–Time Double-Difference Model," in IEEE Transactions on Aerospace and Electronic Systems, vol. 56, no. 5, pp. 3432-3449, Oct. 2020.

[113] Aumayer, B.M., Petovello, M.G. "Feasibility assessment of MEMS oscillators for GNSS receivers." *GPS Solut* **20,** 385–398 (2016).

[114] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," in *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258-1270, June 2016.
[115] GPS World, Oct. 2017. [Online]. Available: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/
[116] Euronews: https://www.euronews.com/next/2022/03/16/planes-and-smartwatches-near-finland-s-russian-border-had-gps-issues-and-not-for-the-first
[117] MentourPilot.com :https://mentourpilot.com/who-jams-and-spoofs-gps-signals-near-russia-ukraine/
[118] Yves Lacoste (1976) : « La géographie ça sert d'abord à faire la guerre. », Edition La découverte, collection Poche (2014).