Anti-leurrage et anti-brouillage de GPS par réseau d'antennes

J.-M Friedt[1], W. Feng[2]
[1] FEMTO-ST, département temps-fréquence, Besançon, France
[2] Xidian University, National Laboratory of Radar Signal Processing, Xi'an, Chine

La localisation, la navigation et le transfert de temps (PNT) par constellation de satellites, et notamment le Système de Positionnement Global (GPS), sont devenus omniprésents dans notre quotidien. Le brouillage – volontaire ou non – et le leurrage de ces signaux très faibles sont désormais accessibles à tout le monde, mais les subir n'est pas une fatalité : nous allons aborder les méthodes pour se protéger de tels désagréments afin de retrouver les services d'origine en annulant ces interférants par une approche multi-antennes.

1 Introduction

Diverses constellations de satellites embarquant des horloges atomiques pour fournir une datation précise du temps de vol du signal reçu au sol sont actuellement en orbite : GPS américain, GLONASS russe, Galileo européen et Beidou/COMPASS chinois pour les constellations en orbite intermédiaire (MEO à une altitude de 20000 km) à portée planétaire. La disponibilité de ces signaux horaires ultra-stables apporte une multitude d'applications dans des domaines aussi variés que le transport, la génération distribuée d'énergie, les communications numériques longues-portée ou les transactions boursières. L'importance de ces applications implique un intérêt évident pour le brouillage – perte de service – mais aussi le leurrage dans lequel un signal erroné est injecté pour fournir un service faussé. Compte tenu de la très grande distance des satellites et la puissance modeste émise d'une cinquantaine de watts, nous avions démontré dans ces pages [1] la capacité à leurrer GPS à moindre coût par une source de radio logicielle [2] – dans notre cas la plateforme PlutoSDR de Analog Devices – pour positionner des téléphones portables, automobiles ou récepteurs avec sortie de datation 1-PPS à l'autre bout de la France. Pour ce faire, nous avions pris soin de fournir une horloge de stabilité court terme – <1000 s, intervalle de temps en deçà duquel seul l'oscillateur à quartz détermine la stabilité globale de l'horloge et l'information des atomes n'a pas d'impact tel que nous l'observons sur la variance d'Allan d'une horloge césium [1, Fig.7] – représentative de celle d'une horloge atomique. Cet intervalle de temps détermine aussi la durée de l'attaque pendant laquelle le récepteur sera incapable d'identifier une incohérence dans les propriétés physiques des signaux reçus. Nous avions identifié qu'un leurrage efficace en espace libre (i.e. sur un récepteur exposé aux vrais signaux GPS) nécessite d'émettre un signal de leurrage comportant les codes des mêmes satellites que ceux actuellement visibles, impliquant une géométrie de constellation qui ne soit pas trop différente de la géométrie actuelle. Cette condition est réalisée en sélectionnant une distance de quelques centaines de kilomètres au plus entre le point réel et le point leurré, et un écart de temps inférieur à quelques heures entre la date leurrée et la vraie date, imposée par le retard entre l'acquisition et la publication des éphémérides par l'*International Global Navigation Satellite System (GNSS) Service* IGS. Nous avions conclu cette discussion en faisant l'hypothèse qu'un signal suffisamment bien leurré – en puissance, en caractéristiques spectrales et en contenu de messages – était indistinguable d'un vrai signal s'il était acquis par une antenne unique, et que seule l'utilisation de plusieurs antennes permettrait d'identifier une incohérence sur la direction d'arrivée des signaux.

Nous allons développer ce dernier principe ici, en démontrant non seulement une méthode efficace en ressources de calcul de détection de leurrage par l'analyse de signaux acquis simultanément par deux antennes, mais aussi la capacité à restituer le signal original en annulant, par interférence destructive, le signal de leurrage. Nous conclurons en étendant la méthode à l'annulation de signaux de brouillage, plus complexe car ne pouvant exploiter les spécificités des signaux transmis par GPS. Toutes ces affirmations s'appuient sur des démonstrations expérimentales.

2 Détection efficace du leurrage

Une constellation GNSS est nécessairement distribuée dans l'espace, alors que nous faisons l'hypothèse d'une source unique de leurrage ou de brouillage. Une analyse de la phase entre plusieurs (dans notre cas deux) antennes réceptrices détectera la même différence de phase entre les deux antennes pour tous les satellites, un cas physiquement impossible pour une vraie constellation (Fig. 1). Nous avions conclu [1] en proposant l'analyse du signal acquis par plusieurs antennes pour établir la direction d'arrivée des signaux issus des divers satellites pour détecter le leurrage, et avions redécouvert par mégarde le CRPA (*Controlled Radiation Pattern Antenna*) [3, 4] habituellement utilisé dans la sécurisation du signal GPS. Alors que cette méthode est classiquement mise en œuvre par des méthodes complexes en termes de calculs, impliquant notamment des inversions de matrices, nous proposons ici une approche intuitive à faibles ressources de calcul issue des premières méthodes d'analyse de GPS que sont le *codeless decoding*. Dans cette approche, largement utilisée à l'époque où les systèmes embarqués ne proposaient pas la puissance de calcul quasi-infinie actuellement disponibles et en particulier par les sondes Vaisala RS80-15G, les caractéristiques du signal physique transmis par les satellites sont analysées sans se soucier d'effectuer un décodage complet [5], permettant par exemple de trouver la vitesse du récepteur par analyse du décalage Doppler sans se soucier de décoder la position. Cette méthode s'appuie sur le fait que la modulation de GPS est une modulation en phase binaire (BPSK [6]) – chaque bit du satellite i est encodé par une phase $\varphi_{PRN,i}$ à 0 ou π – et que la modulation BPSK s'annule en mettant le signal au carré. En effet, la mise au carré du signal fournit le double de l'argument qui est donc 0 ou 2π soit $0[2\pi]$ et l'étalement spectral induit par le modulation disparaît. De ce fait, le signal GPS qui était initialement sous le bruit thermique est rehaussé de la longueur du code, soit 1023 bits ou environ 30 dB, suffisant pour ramener le signal une dizaine de dB au-dessus du bruit thermique et donc de l'analyser. Comme le récepteur n'a aucune raison d'être exactement à la fréquence des horloges atomiques embarquées dans les satellites GPS, l'argument contient par ailleurs un terme de décalage de fréquence $\delta\omega_i$ pour le satellite i, ne serait-ce qu'à cause du décalage Doppler induit par le mouvement du satellite. Comme ce décalage Doppler dépend de la position dans le ciel du satellite (azimut et élévation définissent la projection du vecteur vitesse tangentielle le long de l'orbite vers le récepteur au sol), il sera unique pour chaque satellite de la constellation.

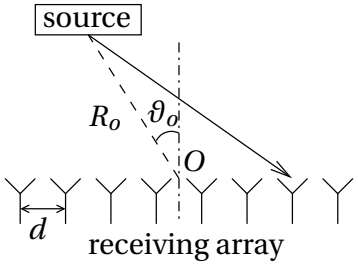


FIGURE 1: Différence de phase entre les signaux acquis par un réseau d'antennes, ici une géométrie linéaire uniformément distribuée qui facilite l'analyse de la relation entre la phase φ, la distance entre antennes d et la direction d'arrivée ϑ_0 sous hypothèse que la distance source-réseau d'antennes R_0 est "grande" ($R_0 \gg 2(Kd)^2/\lambda$ pour K antennes séparées de d) pour vérifier la condition d'onde plane incidente de longueur d'onde λ : $\varphi = 2\pi n d\vartheta_0/\lambda$ au $n$ième élément.

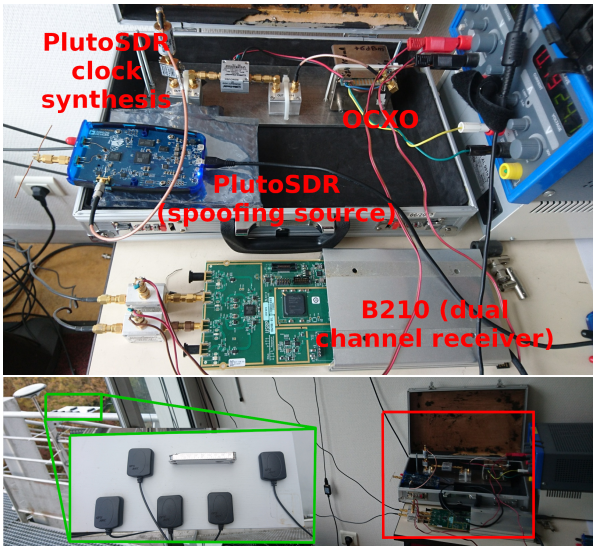


FIGURE 2 – Photo (haut) représentant le matériel utilisé pour le leurrage (PlutoSDR associé à l'oscillateur OCXO) ainsi que le récepteur GPS (B210) connecté aux deux antennes (bas) espacées de la longueur d'onde de la porteuse à la fréquence L1 (1575,42 MHz) divisée par deux, soit 10 cm.

Si le signal GPS est acquis par deux antennes spatialement distinctes (Fig. 2), alors une phase géométrique additionnelle $\varphi_{a,i}$ est introduite par la différence de chemin parcouru par l'onde atteignant l'une puis l'autre antenne a. Cette différence de phase dépend elle aussi de la position du satellite dans le ciel et la projection de la direction d'arrivée du signal sur le vecteur définissant la base le long de laquelle les deux antennes sont placées. Ici encore, si tous les satellites sont dans des positions différentes dans le ciel, la différence des phases géométriques doit être différente pour tous les satellites. Au contraire dans le cas d'un leurrage par une source unique, toutes les directions d'arrivées seront les mêmes pour tous les satellites supposés à des azimuts et élévations différentes, un cas physiquement impossible.

Pour mettre ces concepts en équation : le signal reçu est de la forme

$$s_a(t) = A_a(t)\exp(j\delta\omega_i + \varphi_{PRN,i} + \varphi_{a,i})$$

$$\Rightarrow s_a^2(t) = A_a^2(t)\exp(j2\delta\omega_i + 2\varphi_{a,i})$$

$$\Rightarrow \frac{s_1^2(t)}{s_2^2(t)} = \frac{A_1^2(t)}{A_2^2(t)}\exp(2j(\varphi_{1,i} - \varphi_{2,i}))$$

Ainsi, la transformée de Fourier de $s_a^2(t)$ permet de trouver à l'abscisse $2\delta\omega_i$ le décalage Doppler du satellite i, et l'analyse de l'argument de $\frac{s_1^2(t)}{s_2^2(t)}$ à ces abscisses permet de trouver la direction d'arrivée du signal comme différence des phases géométriques $\varphi_{1,i} - \varphi_{2,i}$. Une valeur identique de phase pour tous les satellites est signature de leurrage, puisqu'une vraie constellation induit des directions d'arrivées différentes des signaux des divers satellites i compte tenu de la diversité spatiale de la constellation.

Nous avions mis en œuvre la détection de leurrage par l'acquisition des signaux reçus par deux antennes connectées à deux voies cohérentes (cadencées par le même oscillateur local) du récepteur de radio logicielle Ettus Research B210 et le post-traitement permettant d'identifier la phase géométrique du signal induite par l'écart de position entre les deux antennes, après avoir éliminé les termes de décalage Doppler et de modulation de phase portant le signal numérique (*codeless decoding*).

La figure 3 présente le résultat de cette analyse pour des puissances de leurrage croissantes de gauche à droite, de 60 dB à 45 dB d'atténuation du signal émis par la PlutoSDR (observée comme une onde continue de 0 dBm si aucune atténuation n'est appliquée). Nous constatons que des atténuations de 60 et 50 dB ne permettent pas un leurrage efficace (diversité des phases observées pour les divers satellites) tandis que 45 ou 40 dB d'atténuation permettent un leurrage efficace (unicité de la phase géométrique pour tous les satellites). En effet, dans le cas des puissances émises les plus faibles, le signal d'origine émis par la vraie constellation, avec sa diversité spatiale, domine le signal de leurrage, expliquant la diversité des phases observées sur Fig. 3 (deux graphiques de gauche) et l'inefficacité du leurrage.

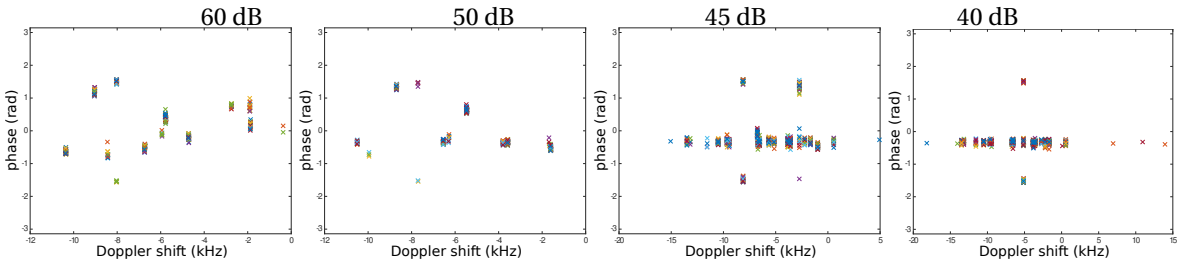


FIGURE 3 – Différence de phase géométrique (ordonnée) représentative de la direction d'arrivée du signal, en fonction du décalage Doppler (abscisse) représentatif du satellite émetteur. Alors qu'une constellation GPS distribuée dans l'espace induit des directions d'arrivée différentes pour chaque satellite (deux figures de gauche), un système de leurrage, même s'il prend soin d'introduire le décalage Doppler cohérent avec la position supposée de chaque satellite, introduit nécessairement la même phase géométrique représentative de la direction d'arrivée du signal venant de l'émetteur unique (deux figures de droite). Ces figures sont obtenues pour des puissances de leurrage croissantes, de 60 dB, 50 dB, 45 dB et 40 dB d'atténuation du signal émis par la PlutoSDR par pas de 5 dB.

Fort de ce constat et de cet équipement (Fig. 2), nous désirons améliorer la détection du leurrage par la restitution du signal d'origine, selon la technique classique du *beamforming* consistant à diriger le faisceau

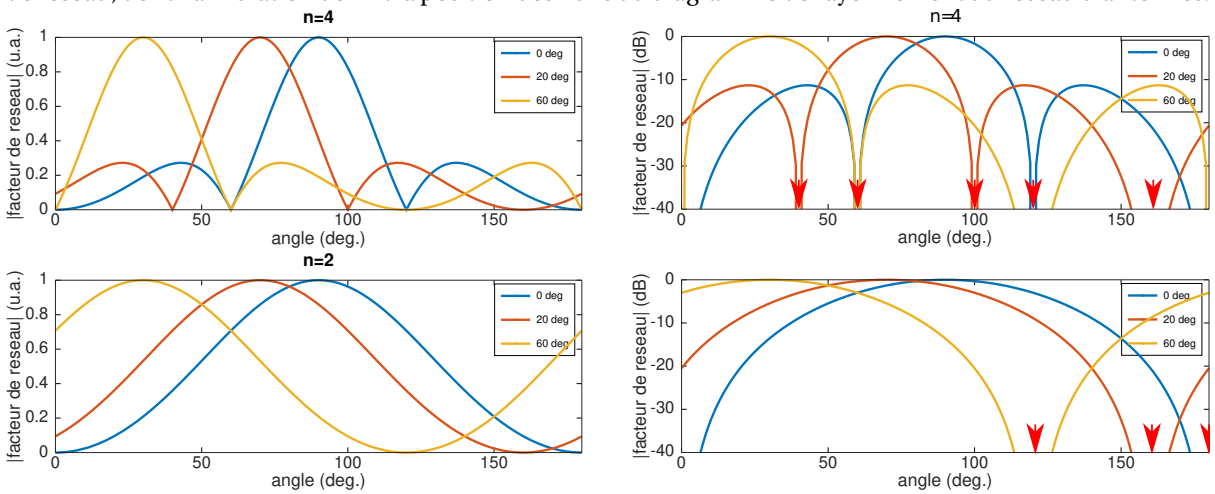
électromagnétique émis par un réseau d'antennes vers une cible donnée par l'introduction d'une phase judicieusement choisie entre un émetteur et chaque antenne. Cette méthode, bien connue de tous les émetteurs-récepteurs numériques multi-antennes (MIMO pour *Multiple Inputs Multiple Outputs*), s'extrapole vers le *nullsteering* qui consiste à orienter non pas le maximum du faisceau mais un null (minimum de puissance reçue) de rayonnement obtenu par interférence destructive vers la source d'un brouillage par exemple [7, 8]. Cette méthode est notamment utilisée par les radioamateurs de la sécurité civile lors de la recherche de balise (*fox hunt*) puisqu'un null (interférence destructive) est plus fin qu'un maximum (interférence constructive) de faisceau, permettant donc de plus finement ajuster la direction à la cible en vue de l'interférence destructive du signal qu'elle émet.

Annulation d'interférants par réseau d'antennes

Il est classique [9] de considérer que si une antenne présente un diagramme de rayonnement $R(\phi,\theta)$ selon l'azimuth ϕ et l'élévation θ, alors un réseau de telles antennes, distribuées de façon linéaire et équidistante de séparation d pour faciliter la mise en équation, présente un diagramme de rayonnement (Fig. 1) de la forme $R(\phi,\theta)\left(1+\exp(j\varphi)+\exp(j2\varphi)+...+\exp(jn\varphi)\right)$ avec $n+1$ le nombre d'antennes. Cette phase φ introduite entre chaque antenne est la projection du vecteur d'onde $\vec{k}=2\pi/\lambda\,\vec{u}_o$ de l'onde plane incidente sur le vecteur définissant la base du réseau d'antennes $d\,\vec{u}_a$, avec $|\vec{u}_a|=1$. Puisque d'aprés Fig. 1, $\vec{u}_o\cdot\vec{u}_a=\cos(\vartheta_0)$, alors $\varphi=2\pi\cos(\vartheta_0)\cdot d/\lambda$. Nous nous retrouvons donc avec le diagramme de rayonnement unitaire R multiplié par le facteur de réseau $\sum_{m=0}^{n}\exp(mj2\pi\cos(\vartheta_0)\cdot d/\lambda)$. Il s'agit de la somme des termes d'une suite géométrique $\sum_{m=0}^{n}p^m$ puisque l'indice m dans l'argument de l'exponentielle complexe peut sortir pour passer en exposant, et la somme de cette suite est explicitée comme $(p^n-1)/(p-1)$ qui dans notre cas particulier vaut

$$\frac{\exp(nj2\pi\cos(\vartheta_0)\cdot d/\lambda)-1}{\exp(2j\pi\cos(\vartheta_0)\cdot d/\lambda)-1}$$

(noter le n au numérateur qui a disparu du dénominateur) qui se réarrange en $\exp(j(n-1)\pi\cos(\vartheta_0)\cdot d/\lambda)\frac{\sin(n\pi\cos(\vartheta_0)\cdot d/\lambda)}{\sin(\pi\cos(\vartheta_0)\cdot d/\lambda)}$. Le premier terme est imaginaire pur et s'élimine donc lors du tracé du module du facteur de réseau, dont l'annulation définit la position des nulls du diagramme de rayonnement du réseau d'antennes.



Gauche : module normalisé du facteur de réseau en échelle linéaire, en haut pour 4 antennes et en bas pour 2 antennes, avec une phase introduite entre éléments de 0, 20 et 60° illustrant le balayage électronique de faisceau avec le null qui se déplace le long de l'azimuth en abscisse. Nous supposons ici un réseau d'antennes isotropes donc $R=1$. Droite : idem, en échelle logarithmique, mettant en évidence la finesse du null devant la largeur du lobe de rayonnement. Les flèches rouges sur le diagramme en dB attire l'œil sur quelques nulls remarquables en fonction de la phase introduite électroniquement ou numériquement entre les éléments successifs du réseau d'antennes tel que indiqué en légende.

Dans notre cas, nous désirons annuler la source de leurrage – voire de brouillage – qui a été identifiée au préalable par le traitement des signaux acquis par radio logicielle [10]. Ayant sauvé les signaux de deux voies de mesures cohérentes, nous désirons appliquer un post-traitement permettant de retrouver le signal d'origine caché sous le signal de leurrage par élimination de celui-ci.

3 Annulation du leurrage

Le problème que nous nous posons consiste donc à identifier la pondération du signal de leurrage détecté par une antenne afin de le soustraire du signal acquis par la seconde antenne. Lorsque la structure du signal de leurrage est connue, nous venons de voir que nous obtenons par le ratio des transformées de Fourier des carrés des signaux acquis par chaque antenne une contribution en amplitude $\sqrt{\frac{A_1^2}{A_2^2}}$ dont nous avons pris la racine carrée pour avoir directement le ratio des pondérations, et un déphasage $\varphi_1 - \varphi_2$ (l'indice représente l'antenne réceptrice) constant pour tous les satellites i dans le cas d'un leurrage. Nous pourrons donc déjà commencer par appliquer cette pondération sur le signal d'une antenne pour soustraire le leurrage du signal acquis par la seconde antenne et ainsi espérer retrouver le signal d'origine.

Dans le cas du brouillage, le problème d'identification de la pondération est plus complexe car nous ne profitons pas de la structure spécifique de la modulation BPSK du signal de leurrage. L'identification de la pondération du signal de brouillage détecté par une antenne sur le signal acquis par la seconde antenne est un problème très proche de celui que nous avions abordé dans le contexte du RADAR passif [11] dans lequel le signal direct entre une source non-coopérative illuminant une cible et un récepteur est bien plus puissant que le signal réfléchi par cette cible. En effet, le signal direct décroît comme le carré de la distance (conservation de l'énergie dans l'équation de Friis) alors que la puissance du signal rétrodiffusé par la cible décroît comme la puissance quatrième de la distance en supposant la cible comme une source ponctuelle. Nous avions à l'époque développé la solution minimisant l'erreur quadratique qu'est le pseudo-inverse, un calcul matriciel permettant d'inverser une matrice qui n'est pas carrée. Ce pseudo-inverse d'une matrice contenant plus de lignes que de colonnes peut se voir comme la solution à un problème sur-contraint puisque trop d'observations (échantillons dans le temps que sont les lignes) imposent une solution sur les pondérations (les colonnes représentant les mesures par chaque antenne) en fournissant plus d'équations que de variables. Ce domaine, quand le nombre d'antennes croît pour rendre le problème de plus en plus difficile, se généralise par le domaine intitulé STAP pour *Space-Time Adaptive Processing*, la diversité spatiale étant représentée par les antennes distribuées et l'aspect temporel par les mesures acquises en fonction du temps sur chaque antenne. Ce domaine a été largement appliqué au domaine de l'annulation du leurrage de GPS [12, 13, 14]. Comme souvent, il est utile d'apprendre le jargon d'un domaine pour en découvrir la littérature, jargon qui n'est appris qu'en fin de projet et non au début lorsque l'étude bibliographique devrait orienter les recherches !

Le traitement nécessite d'identifier la pondération du signal interférent détecté par une antenne dans le signal reçu par la seconde antenne. Une fois cette pondération α (complexe, i.e. en amplitude et en phase) identifiée, il est possible de retrancher le signal interférent détecté par la première antenne $s_1(t)$ sur le signal reçu par la seconde antenne $s_2(t)$. La difficulté porte donc sur l'identification efficace de cette pondération. Nous utilisons le pseudo-inverse pour rechercher ces poids :

$$\alpha = pinv(s_2) \times s_1$$

où

$$pinv(X) = (X^t \cdot X)^{-1} \cdot X^t$$

Le signal véritable s est alors retrouvé par :

$$s = (s_1 - \alpha \times s_2)$$

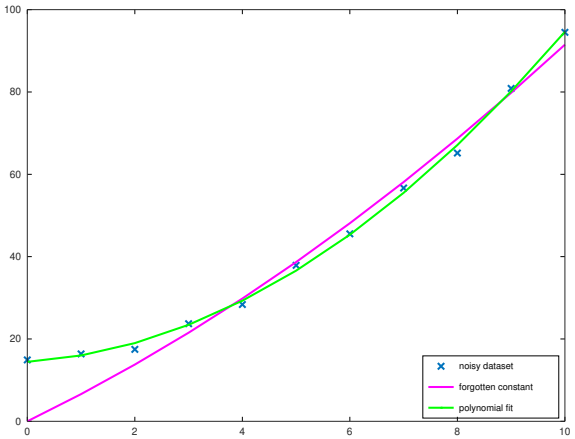
Démonstration de la solution au moindre carré du problème surdimensionné, i.e. avec plus de lignes que de colonnes : $y = Mx \not\Rightarrow x = M^{-1}y$
y est une combinaison linéaire des colonnes de M pondérées par les coefficients x : x doit donc minimiser

$$\varepsilon = ||y - Mx||_2 = (y - Mx)^H \cdot (y - Mx) \in \mathbb{R}$$
$$= (y^H y - y^H Mx - \underbrace{x^H M^H y}_{(y^H Mx)^H} + \underbrace{x^H M^H Mx}_{\partial/\partial x = 2M^H Mx})$$

$$\Rightarrow \frac{\partial \varepsilon}{\partial x} = \frac{\partial}{\partial x}\left(-2\ \underbrace{y^H Mx}_{\partial/\partial x = M^H y} + x^H\ \underbrace{M^H M}_{inversible}\ x\right) = 0 \Leftrightarrow M^H y = M^H Mx \text{ et}$$

$$x = (M^H M)^{-1} M^H y = \texttt{pinv}(M) \times y$$

On note que $(y^H Mx)^H = y^H Mx$ car il s'agit de scalaires.
À titre d'illustration, nous fabriquons un signal bruité y que nous désirons ajuster par un modèle parabolique. Le premier modèle (a) est incorrect car la matrice fournie en argument de `pinv` ne contient que des termes linéaires et quadratiques et pas de terme constant. Le second essai (b) contient bien un terme constant en dernière colonne, qui s'ajuste donc bien aux données expérimentales. GNU/Octave (ou Matlab) fournit cette fonction `pinv` sous la forme de l'opérateur anti-slash (cas c).




```
x=[0:10]'
y=2*x+0.6*x.^2+13+(5*rand(11,1)-2.5)
a=pinv([x x.^2])*y        %oops no cst
plot(x,a(2)*x.*x+a(1)*x,'m')
b=pinv([x x.^2 ones(11,1)])*y
%    1.86 0.62    13.4 (vs 2 0.6 13)
plot(x,b(2)*x.*x+b(1)*x+b(3),'g')
c=([x x.^2 ones(11,1)])\y % same res.
```

P.J. Dhrymes, *Mathematics for Econometrics*, Springer-Verlag (2013), pp.149–169
R. Penrose, *A generalized inverse for matrices*, Proc. Cambridge Philosophical Society **51** (3) 5406-–413 (1955)

Afin de fournir une solution générique à l'annulation des signaux interférant avec la réception de GPS, nous traitons des deux cas dans le cas particulier du leurrage, à savoir identification de la pondération par traitement des ratios des carrés des signaux, ou par pseudo-inverse.

L'efficacité de l'annulation du signal interférant est démontrée en traçant la carte des maxima de corrélation en fonction du décalage Doppler et de l'indice du satellite dont le code est corrélé. Ensuite, un traitement de radio logicielle de décodage de GNSS sera appliqué sur les signaux bruts (pour valider l'efficacité du leurrage et du brouillage) et sur les signaux nettoyés (pour valider l'efficacité de l'annulation de l'interférent). En effet, seul un décodage efficace du signal original valide l'efficacité de l'algorithme.

Dans un premier temps, nous avons évalué la capacité à identifier le poids α de la contribution du signal de leurrage sur une antenne par rapport à l'autre par des séquences courtes (10 secondes) de leurrage entrecoupées de la mesure du "vrai" signal L1 de la constellation GPS (Figs. 4 et 5).

La séquence d'acquisitions de données visant à démontrer l'annulation du signal de leurrage en affichant la carte Doppler-code est :

1. 10 s véritable constellation avec les antennes orientées vers le ciel
2. 10 s leurrage à X dB en exploitant les éphémérides de l'IGS acquises une paire de mois avant l'expérience (i.e. géométrie de la constellation incohérente avec celle de la date d'acquisition)
3. 10 s véritable constellation avec les antennes orientées vers le ciel
4. 10 s leurrage à X dB en exploitant les éphémérides de l'IGS acquises une heure avant l'expérience (i.e. géométrie de la constellation cohérente avec celle de la date d'acquisition)
5. 10 s véritable constellation avec les antennes orientées vers le ciel

Cette séquence est répétée pour X compris entre -60 et -30 dB émis par pas de 5 dB. Les atténuations réfèrent à la configuration de la PlutoSDR, qui émet une porteuse à 0 dBm en l'absence d'atténuation.

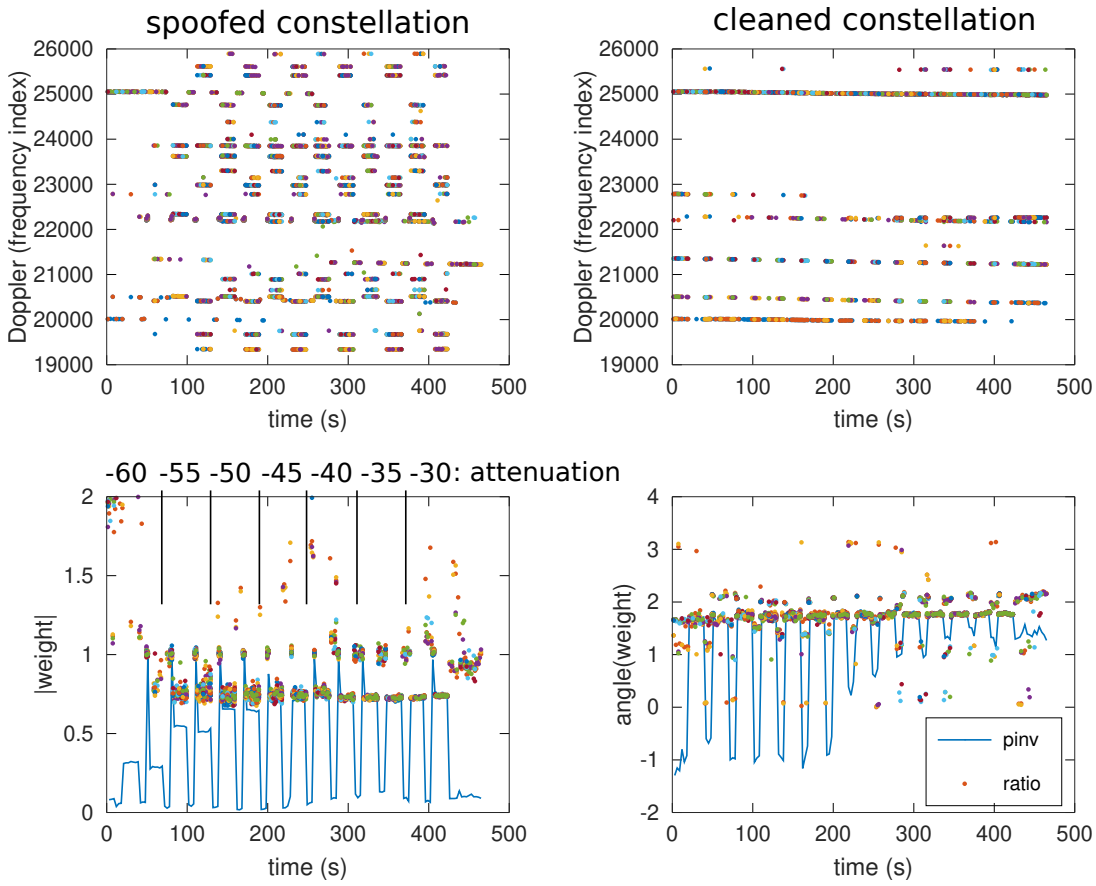


FIGURE 4 – Démonstration du leurrage (haut-gauche) et de l'annulation du leurrage par calcul du pseudo-inverse (haut-droite). Sur chaque figure, en ordonnée le décalage Doppler est représentatif de la vitesse du satellite, avec la constellation de leurrage présentant des incohérences avec la "vraie" constellation dont les caractéristiques sont visibles en haut à droite. Cette élimination de la source de leurrage est validée par l'analyse du module et de la phase de la pondération du leurrage entre les deux antennes (bas-gauche) en comparaison de la mise au carré du signal pour annuler la modulation et retrouver le double de la phase géométrique (bas-droite).

En bas à droite de la figure 4, la phase du poids identifié par pseudo-inverse (ligne bleue) se stabilise à chaque phase de leurrage à 1,6 rad, pour être au contraire aléatoire en l'absence de leurrage. Cette valeur de phase est cohérente avec l'analyse sans décodage décrite précédemment [1] de la séquence pseudo-aléatoire (points dans la figure bas, droite de 4) obtenue par le ratio des transformées de Fourier du carré du signal acquis par chaque antenne qui fournit. En bas à gauche de la Fig. 4, le module du poids calculé par pseudo-inverse diffère du poids calculé comme rapport des transformées de Fourier du carré du signal acquis par chaque antenne. En effet, à faible puissance de leurrage, le pseudo-inverse ne bénéficie pas du gain de compression obtenu par l'annulation de la modulation BPSK en mettant le signal au carré : le rapport des puissances reçues par les deux antennes n'a pas de raison de varier avec la puissance incidente, et le pseudo-inverse ne semble donc pas converger vers une valeur réaliste à faible puissance de leurrage.

Par ailleurs, les cartes Doppler-PRN (Fig. 5) présentent des aberrations en présence du signal de leurrage (plusieurs satellites de mêmes PRN à des décalages Doppler différents : lignes du haut et milieu) qui disparaissent lors de l'annulation du signal de leurrage (ligne du bas).

Néanmoins, seule une démonstration de l'obtention de la "vraie" position en présence d'un signal de leurrage validera le bon fonctionnement de l'algorithme. Pour ce faire, le logiciel libre `gnss-sdr` s'appuyant sur la bibliothèque de traitement numérique de signaux radiofréquences GNU Radio est utilisé pour traiter les

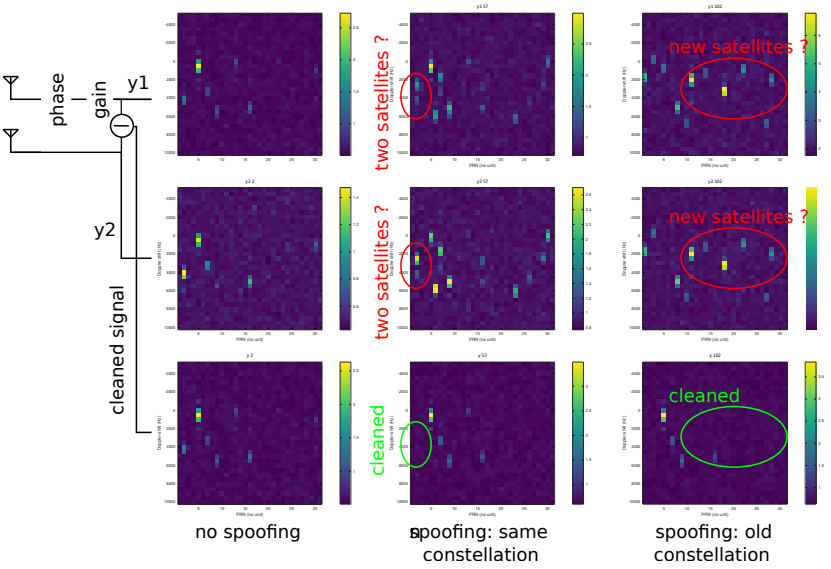


FIGURE 5 – Cartes Doppler-PRN acquises par les deux antennes (haut et milieu) lors du leurrage puis après annulation du signal de leurrage (bas) tel qu'expliqué dans la Fig. 4.

signaux nettoyés des interférents. Cette approche a été mise en œuvre en post-traitement sur des enregistrements de deux minutes pour garantir la réception des trames de navigation permettant un positionnement.

Un exemple de traitement exploitable de `gnss-sdr` sur un fichier de signaux nettoyé du leurrage est fourni ci-dessous :

```
New GPS NAV message received in channel 15: subframe 5 from satellite GPS PRN 04 (Block Unknown)
New GPS NAV message received in channel 13: subframe 5 from satellite GPS PRN 02 (Block IIR)
New GPS NAV message received in channel 3: subframe 5 from satellite GPS PRN 23 (Block IIR)
New GPS NAV message received in channel 6: subframe 5 from satellite GPS PRN 26 (Block IIF)
Position at 2019-Nov-30 10:59:42.000000 UTC using 4 observations is
Lat = 47.251759020 [deg], Long = 5.993861290 [deg], Height = 687.019 [m]
Velocity: East: -0.092 [m/s], North: -0.091 [m/s], Up = -0.207 [m/s]
```

avec une estimation correcte de la position, proche de l'Observatoire de Besançon tandis que la position erronée a été choisie au large de Brest.

Nous savons que `gnss-sdr` initialise de façon aléatoire les constantes de ses boucles d'asservissement et de ce fait, de multiples exécutions du même logiciel ne convergent pas toujours vers la même solution. Ainsi, nous avons procédé à une analyse statistique de l'efficacité de l'algorithme de nettoyage des signaux. Pour cela, chaque analyse a été itérée 100 fois afin d'obtenir un résultat en %.

La puissance radiofréquence émise par le PlutoSDR a été mesurée à 0 dBm sur une porteuse pure (onde continue) en l'absence d'atténuation, et à -30 dBm lors de la modulation BPSK du C/A code de GPS sur L1 [1]. Lors de nos tests, la puissance émise a été atténuée de 30 à 60 dB. À la distance d'environ 3 m qui séparaient l'émetteur du récepteur, les pertes de propagation en espace libre (équation de Friis) à 1575,42 MHz sont de 46 dB : en négligeant tout gain d'antennes supposées omnidirectionnelles en réception (patch) et en émission (dipôle), la puissance reçue est de l'ordre de -111 à -136 dBm dans nos conditions de tests.

Les résultats de cette analyse sont fournis dans le tableau 1, dont nous concluons que

— lorsque le signal de leurrage est puissant (-35 et -40 dB), sa structure est aisément identifiée et l'algorithme d'annulation est efficace puisque la soustraction de la source de leurrage est suffisamment bonne pour que le vrai signal redevienne plus puissant que le signal de leurrage, se traduisant par aucun leurrage (soit la bonne position est retrouvée soit aucune solution n'est trouvée),

— un signal plus faible de leurrage (-45, -50 dB) est en compétition avec le vrai signal, induisant une identification erronée de position/date avant annulation, mais la procédure de nettoyage du signal est incapable de retrouver le signal original et par conséquent l'échec d'un positionnement est le résultat le plus probable du traitement,

— à faible puissance de leurrage (-60 dB), le leurrage est inefficace et la bonne position est toujours identifiée.
— Le choix de la géométrie actuelle de la constellation ou une géométrie très différente des satellites (par exemple en choisissant les éphémérides obtenues 6 h avant le leurrage) n'impacte pas significativement le résultat d'annulation de leurrage bien qu'il rende le leurrage lui même plus complexe, mettant en compétition les signaux de navigation de la vraie constellation contre ceux du leurrage.

TABLE 1 – Capacité d'annulation du signal de leurrage en fonction de sa puissance. Chaque ligne fournit le résultat sous forme de pourcentage "avant correction"/"après correction par poids issu du pseudo-inverse"/"après correction par poids issu du ratio des carrés des signaux". Les deux colonnes de gauche représentent la configuration utilisée, puissance émise et constellation utilisée, les trois colonnes de droite représentent le résultat obtenu par le récepteur, soit une position correcte, une position erronée (position de leurrage) et pas de position déterminée.

atténuation TX (dB)	Constellation	Pos. correcte (%)	Pos. erronée (%)	Pas de solution (%)
35	actuelle	0/90/100	57/0/0	43/10/0
40	actuelle	0/93/100	96/0/0	4/7/0
45	actuelle	0/2/100	61/1/0	39/97/0
50	actuelle	0/3/100	31/7/0	69/90/0
55	actuelle	52/23/100	0/0/0	48/77/0
60	actuelle	88/64/100	0/0/0	12/36/0
40	-6 h	7/100/100	44/0/0	49/0/0
50	-6 h	6/4/100	90/96/0	4/0/0

Les spectres des signaux de leurrage sont présentés en Fig. 6 (a), mettant en évidence le plancher de bruit et des signaux de leurrage jusqu'à 30 dB plus puissants que la ligne de base du plancher de bruit thermique autour de 2 dB sur ce graphique, avec un spectre s'étalant sur une largeur de ±1 MHz. Cette structure sera significativement différente de celle observée lors du brouillage (Fig. 6 – b), sujet abordé dans la section suivante.

4 Annulation du brouillage

Nous voilà capables de rejeter efficacement un leurrage, l'attaque la plus subtile qui ne saurait être involontaire, et donc la plus dangereuse car faisant croire qu'un signal authentique est disponible. Dans la pratique, le cas le plus commun est le brouillage puisque techniquement trivial et sans intérêt, qu'il soit volontaire ou involontaire. Nous désirons donc nous assurer que notre traitement est efficace contre ce genre de perturbation ou d'attaque, et avons pour celà acquis un brouilleur GPS. Compte tenu de la stupidité de l'objectif, le budget limité que nous nous sommes imposé de 10 euros est atteint avec un "bloqueur de signaux GPS" [1] dont le fonctionnement et l'impact sont décrits en détail dans [15]. On notera que la trivialité de la méthode de brouillage induite par le coût réduit du circuit de balayage d'un oscillateur micro-onde réduit notablement la portée de l'attaque face à une approche plus subtile d'exploiter une source de leurrage comme source de brouillage telle que nous décrivons en fin de [15] : dans un tel cas, notre approche de protection revient au cas de la section précédente en bénéficiant à nouveau de la structure BPSK de la modulation annulée par mise au carré du signal.

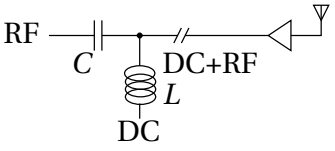
Les résultats de l'annulation d'un brouilleur sont résumés au Tab. 2 et sont cohérents avec les résultats d'annulation du leurrage :

— un signal puissant à courte portée sature le traitement analogique radiofréquence, interdisant l'annulation du brouillage par traitement numérique ultérieur (4,5 à 6,0 m)
— à portée intermédiaire (6,0 à 7,5 m), alors que le brouillage fonctionne bien sur les signaux bruts du récepteur, l'annulation du brouillage fonctionne et permet de retrouver la vraie solution avec un taux de succès croissant avec la distance au récepteur,
— à longue portée (distance du brouilleur au récepteur de 8,0 à 10 m), le brouillage est inefficace et l'annulation du brouillage est inutile pour obtenir la bonne position.

1. disponible auprès de `https://www.amazon.fr/IrahdBowen-Bloqueur-Bouclier-Brouilleur-Disjoncteur/dp/B07KSC5LLD`

Pour résumer les résultats fournis dans le tableau 2, l'efficacité de l'annulation au brouillage est d'autant plus efficace que la source est intense, dans la limite de fonctionnement des amplificateurs inclus dans les antennes actives GPS. Cette conclusion, à première vue étrange, se comprend bien en analysant le principe de pseudo-inverse : plus le brouillage sort du bruit qui pollue le signal acquis par les deux antennes, plus son identification et donc son rejet sont aisés. Au contraire l'identification d'un brouillage à la limite du bruit thermique est le cas le plus contraignant car l'identification de ses propriétés est entachée d'erreur par le bruit. Une fois la pondération du bruit identifiée, son rejet est très efficace et permet de retrouver le signal d'origine. Ici encore l'analyse se fait en post-traitement sur des données acquises par une plateforme de radio logicielle Ettus Research B210 munie de deux antennes patch faible coût pour recevoir la bande L1, polarisées par un montage en T implémenté sous forme du circuit MiniCircuits ZFBT-4R2GW+ (voir encadré).

Note sur le T de polarisation
ou comment en réaliser un soi-même



Architecture d'un T de polarisation permettant de porter sur un même câble (droite) le signal d'alimentation continu (DC, bas) et le signal radiofréquence (RF, gauche) vers le récepteur

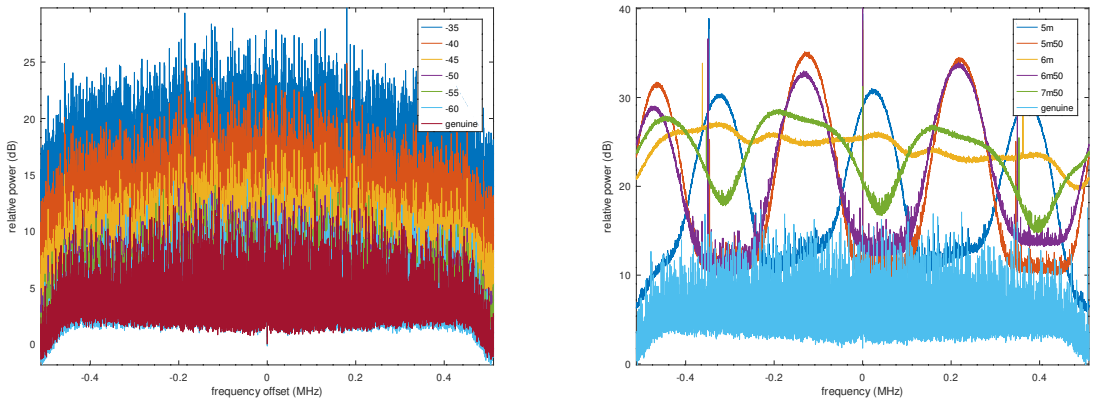
Le T de polarisation commercial est utilisé par paresse de connecter une inductance L de quelques microhenrys et un condensateur C de quelques nanofarads sur un montage en T (Fig. gauche) pour d'une part alimenter par une polarisation continue (DC) l'amplificateur présent dans l'antenne active, et d'autre part laisser le signal radiofréquence passer vers le récepteur sans en endommager l'étage de réception par une polarisation DC. Le choix des composants s'obtient en considérant que l'inductance L d'impédance $L\omega$ avec $\omega = 2\pi \cdot f$ la pulsation angulaire à la fréquence $f = 1575,42$ MHz doit présenter une valeur grande devant l'impédance du condensateur C de valeur $1/(C\omega)$ afin de favoriser le passage du signal radiofréquence vers le récepteur plutôt que vers l'alimentation. Une application numérique nous informe qu'un condensateur de 1 nF présente une impédance de 0,1 Ω, petit devant les 50 Ω de l'impédance d'entrée du récepteur et devant l'impédance de 10 kΩ d'une inductance (de bonne qualité tout de même) de 1 μH. Ces deux composants, condensateur et inductance, se comportent idéalement face à la composante DC de l'alimentation pour la bloquer afin d'éviter d'endommager le récepteur RF, tout en passant l'inductance comme un fil pour alimenter l'amplificateur de l'antenne active.

TABLE 2 – Capacité d'annulation d'un signal de brouillage en fonction de sa puissance. Chaque ligne affiche un pourcentage de solution "avant correction"/"après correction". La première colonne indique la distance brouilleur/récepteur, les deux colonnes de droite le résultat du récepteur, soit une position correcte identifiée, soit aucune solution trouvée.

Distance	Pos. correcte (%)	Pas de solution(%)
Sans brouillage	100	0
10m00	100/100	0/0
9m00	100/100	0/0
8m00	100/100	0/0
7m50	0/94	100/6
6m50	0/49	100/51
6m00	0/79	100/21
5m50	0/0	100/100
5m00	0/0	100/100
4m50	0/0	100/100

Nombre de publications et publicités annoncent ce genre de résultat, se gardant bien de décrire leur implémentation ou leurs performances en pratique, se contentant le plus souvent de simulations. À titre d'illustration, cette approche s'apparente au fonctionnement du système dont la publicité décrit "*GAJT protects GPS-based navigation and precise timing receivers from intentional jamming and accidental interference, Novatel said. The unit features a null-forming antenna system, which ensure satellite signals necessary to compute position and time are always available, the company said.*" [2] sans bien sûr en décrire l'implémentation.

2. https://insidegnss.com/canadian-army-tests-novatels-gps-anti-jam-technology/



(a) (b)

FIGURE 6 – Spectres des signaux de leurrage (a) et de brouillage par balayage du signal de commande d'un oscillateur commandé en tension (b).

5 Conclusion

Nous avions présenté diverses sources de perturbations de signaux radiofréquences qui sont devenus indispensables au quotidien de la majorité d'entre nous que sont les signaux de datation (et donc de localisation) des constellations de satellites équipés d'horloges atomiques qualifiés de Global Navigation Satellite Systems (GNSS) et du plus connu d'entre eux, GPS. Nous avons développé ici une stratégie d'identification de leurrage, de réjection de leurrage efficace en puissance de calcul requise et compatible avec une mise en œuvre en temps-réel, et avons étendu cette étude au cas des sources de brouillage. Ces dernières sont plus simples à identifier compte tenu de la perte de service, mais plus complexes à rejeter compte tenu de l'absence de structure connue et prévisible du signal interférant. Alors que nombre de ces études ont été publiées dans les décennies passées, leur intérêt renaît avec le passage de GPS d'un système militaire à un système utilisé au quotidien dans nombre d'applications civiles allant bien au-delà de la navigation ou du positionnement, et surtout avec la facilité d'attaquer ce protocole avec une radio logicielle faible coût localisée à une distance nettement inférieure aux 20000 km du satellite en orbite moyenne.

Remerciements

Cette étude a été motivée par le laboratoire commun FAST-LAB entre l'institut FEMTO-ST de Besançon (Doubs) et la société Gorgy Timing de La Mure (Isère) soutenu financièrement par l'Agence National de la Recherche. J.-Y. Dauvignac et C. Migliaccio (LEAT, Univ. Nice) ont présenté le facteur de réseau à JMF lors d'un cours sur les antennes aux étudiants de Master1 de l'Univesité de Franche-Comté à Besançon. Toutes les références bibliographiques qui ne sont pas librement disponibles sur le web ont été acquises sur Library Genesis (`gen.lib.rus.ec`), une ressource indispensable à notre recherche quotidienne.

Références

[1] G. Goavec-Merou, J.-M Friedt, and F. Meyer. Leurrage du GPS par radio logicielle. *MISC*, HS19 :88–106, Fev. 2019. `https://connect.ed-diamond.com/MISC/MISCHS-019/Leurrage-du-GPS-par-radio-logicielle`.

[2] L. Huang and Q. Yang. Low cost GPS simulator : GPS spoofing by SDR. In *DEFCON*, volume 23, 2015. `media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Lin-Huang-Qing-Yang-GPS-Spoofing.pdf`.

[3] M. Jones. Anti-jam technology : Demystifying the CRPA. *GPS World*, April 2017. `https://www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/`.

[4] I.J. Gupta, I.M. Weiss, and A.W. Morrison. Desired features of adaptive antenna arrays for GNSS receivers. *Proc. IEEE*, 104(6) :1195–1206, June 2016.

[5] D Borio. Squaring and cross-correlation codeless tracking : analysis and generalisation. *IET radar, sonar & navigation*, 5(9) :958–969, 2011.

[6] J.-M Friedt and G. Cabodevila. Exploitation de signaux des satellites GPS reçus par récepteur de télévision numérique terrestre DVB-T. *Opensilicium*, 15, 2015. `https://connect.ed-diamond.com/Open-Silicium/OS-015/Decodage-des-signaux-de-satellites-GPS-recus-par-recepteur-de-television-numerique-terrestre-DVB-T`.

[7] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle. Overview of spatial processing approaches for GNSS structural interference detection and mitigation. *Proc. IEEE*, 104(6) :1246–1257, June 2016.

[8] M.G. Amin, X. Wang, Y.D. Zhang, F. Ahmad, and E. Aboutanios. Sparse arrays and sampling for interference mitigation and DOA estimation in GNSS. *Proc. IEEE*, 104(6) :1302–1317, June 2016.

[9] A.J. Fenn. Adaptive Antennas and Phased Arrays. à `https://ocw.mit.edu/resources/res-ll-002-adaptive-antennas-and-phased-arrays-spring-2010/`

[10] E. Schmidt, Z. Ruble, D. Akopian, and D. J Pack. Software-defined radio GNSS instrumentation for spoofing mitigation : A review and a case study. *IEEE Transactions on Instrumentation and Measurement*, 68(8) :2768–2784, 2018.

[11] J.-M Friedt. Radar passif par intercorrélation de signaux acquis par deux récepteurs de télévision numérique terrestre. *GNU/Linux Magazine France*, 212 :36–, 2018.

[12] T. K. Sarkar, H. Wang, S. Park, R. Adve, J. Koh, K. Kim, Y. Zhang, M. C Wicks, and R. D Brown. A deterministic least-squares approach to space-time adaptive processing (STAP). *IEEE Transactions on Antennas and Propagation*, 49(1) :91–103, 2001.

[13] S.-J. Kim and R. A Iltis. STAP for GPS receiver synchronization. *IEEE Transactions on Aerospace and Electronic Systems*, 40(1) :132–144, 2004.

[14] D. Lu, Q. Feng, and R. Wu. Survey on interference mitigation via adaptive array processing in GPS. *Piers Online*, 2(4) :357–362, 2006.

[15] J.-M Friedt. Analyse d'un brouilleur GPS. *Hackable*, 33 :104–113, 2020.