

Extraction des paramètres de navigation par signaux d’opportunité

[Hugo BOURGOIN](#)¹

¹ DEMR ONERA, Université de Toulouse, 31000, Toulouse, France

Résumé – Cet article présente une solution d’extraction opportuniste de paramètres de navigation basée sur les signaux 4G (protocole LTE). Des expérimentations concluantes ont été réalisées afin de vérifier la faisabilité de la solution proposée.

Abstract – This article presents an opportunistic extraction solution for navigation parameters based on 4G signals (LTE protocol). Successful experiments have been conducted to verify the feasibility of the proposed solution.

1 Introduction

Avec une utilisation de plus en plus massive de drones, à la fois dans le domaine civil comme dans le domaine militaire, la question de solution de navigation alternative se pose, le service GNSS (*Global Navigation Satellite System*) ne pouvant pas garantir une disponibilité spatiale et temporelle totale. En effet, les canyons urbains et/ou des interférences radiofréquences peuvent perturber la réception des signaux satellitaires.

Le réseau cellulaire (4G/5G) semble être une solution alternative pertinente. Il offre une diversité d’antennes importante, plusieurs bandes de fréquences, et des signaux haut débit (largeur de bande importante) permettant d’obtenir une résolution spatiale précise pour un positionnement.

Cet article présente dans un premier temps différents signaux de synchronisation prévus par le standard, puis une méthode permettant d’extraire des paramètres de navigation, ici les distances relatives entre le récepteur et les balises 4G environnantes. Enfin, la méthode proposée sera validée par expérimentations.

2 Standard LTE

Le signal 4G, utilisé dans les réseaux LTE (*Long Term Evolution*), est complexe et repose sur plusieurs technologies avancées pour offrir des débits de données élevés, une faible latence et une grande capacité de réseau. L’OFDM (*Orthogonal Frequency Division Multiplexing*) est la technologie de multiplexage utilisée pour diviser le spectre disponible en plusieurs sous-porteuses orthogonales. Cela permet une transmission efficace et robuste des données contre les interférences et les multi-trajets.

Chaque sous-porteuse est modulée individuellement avec des schémas de modulation comme QPSK (*Quadrature Phase Shift Keying*), 16-QAM (*Quadrature Amplitude Modulation*), ou 64-QAM, en fonction des conditions du canal de propagation. Leur largeur de bande est de 15 kHz.

Une trame LTE dure 10 ms et est divisée en 10 sous-trames de 1 ms chacune. Chaque sous-trame est à son tour divisée en deux slots de 0.5 ms.

Le spectre est divisé en unités appelées *Resource Block* (RB), chacun comprenant 12 sous-porteuses et 1 slot en temps. Les RB sont les plus petites unités d’allocation de ressources pour les données utilisateurs et les signaux de contrôle.

Le signal 4G opère sur plusieurs bandes de fréquences, et supporte une variété de largeurs de bande (1.4, 3, 5, 10, 15, et 20 MHz) pour s’adapter à différentes conditions.

2.1 Signaux de synchronisation LTE

Il existe plusieurs signaux de synchronisation prévus par le standard LTE. Les signaux PSS (*Primary Synchronization Signal*) et SSS (*Secondary Synchronization Signal*) sont répétés toutes les 5 ms, pour une durée de 1 ms. Nous considérerons que les signaux PRS (*Positioning Reference Signal*) sont répétés toutes les 10 ms, pour une durée de 10 ms (hypothèses vérifiées par expérimentation). Chaque antenne 4G, ou BTS (*Base Transceiver Station*), émet ces signaux de synchronisation, référencés par un ‘*Physical*’ *Cell ID* compris entre 0 et 504, leur répartition étant maillée sur le territoire pour éviter les interférences entre BTS.

2.2 PSS/SSS

Les signaux PSS/SSS permettent aux UE (*User Equipment*) de détecter et déterminer quelle BTS offre la meilleure liaison avec une complexité calculatoire moindre.

Un premier ID compris entre 0 et 2 est donné par le PSS, tandis qu’un second, compris entre 0 et 167, est donnée par le SSS ($504=3 \times 168$). En pratique, le *Cell ID* est estimé en évaluant pour chacun d’eux, quel ID possède la corrélation maximale avec le signal reçu (ce qui donne 171 ($168 + 3$) corrélations sur 5 ms). Le *Cell ID* estimé est donné ensuite par :

$$Cell ID = ID_{PSS} + 3ID_{SSS}.$$

2.3 PRS

Les signaux de synchronisation PRS permettent aux UE d'obtenir une localisation plus ou moins précise (*Observed Time Difference Of Arrival*, OTDOA [1]).

Il est possible d'utiliser ces signaux pour détecter les BTS environnantes, qui offrent de meilleures propriétés d'intercorrélation que les signaux PSS et SSS, mais la complexité calculatoire est alors décuplée (511 corrélations sur $T = 10$ ms).

Sa fonction d'autocorrélation présente des lobes secondaires importants, mais suffisamment éloignés pour ne pas provoquer d'ambiguïtés (Figure 1) :

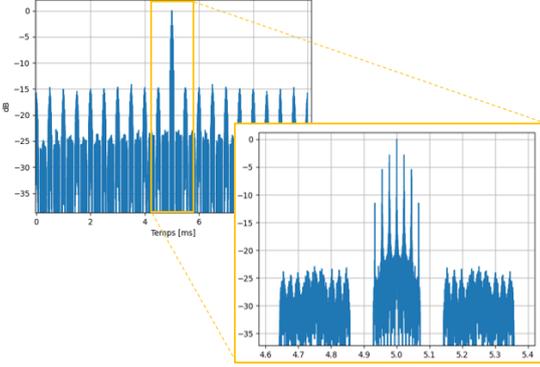


Figure 1 : Autocorrélation d'un signal PRS

3 Description du traitement implémenté

3.1. Réception du signal

Le protocole LTE prévoit d'échantillonner le signal 4G avec une fréquence égale à sa largeur de bande b_w . Les fréquences et largeurs de bande associées sont accessibles publiquement. Le signal est ensuite suréchantillonné avec une fréquence f_s permettant d'être synchronisé avec les RB et de bénéficier des propriétés de corrélation des signaux PRS.

Tableau 1 : Fréquences d'échantillonnage LTE

b_w [MHz]	1.4	3	5	10	15	20
f_s [MHz]	1.92	3.84	7.68	15.36	23.04	30.72

3.2. Acquisition

L'acquisition est une recherche temps-fréquence qui consiste à calculer la corrélation entre le signal reçu et une réplique locale affectée par un délai et une fréquence. Le but de cette opération est double :

- détecter la présence d'une BTS dans l'ensemble des signaux captés par l'antenne du récepteur ;
- déterminer, pour une BTS détectée, le retard et la déviation fréquentielle du signal par rapport à une réplique locale afin d'initialiser les boucles de poursuite.

Plus précisément, le signal $s_r(t)$ à la réception peut être écrit de la manière suivante :

$$s_r(t) = \sum_{k=1}^{n_{BTS}} s_k(t) + n(t),$$

avec $n(t)$ le bruit thermique et n_{BTS} le nombre de BTS présentes. Le signal reçu $s_k(t)$ associé à la BTS k peut s'écrire :

$$s_k(t) = \sqrt{p_k} c_k(t - \tau_k) e^{j2\pi f_k t} e^{j\varphi_k},$$

avec c_k le signal PRS émis par la BTS k et respectivement p_k, τ_k, f_k et φ_k la puissance et le décalage en temps/fréquence/phase du signal induit par sa propagation, qui sont considérés constants sur le temps de corrélation.

Une première étape consiste en la synchronisation fréquentielle du signal reçu. La déviation fréquentielle est calculée par corrélation avec son préfixe cyclique. Afin de réaliser l'étape d'acquisition pour la BTS k , le récepteur va créer une réplique du signal PRS correspondant $c_k(t)$:

$$r_k(\hat{f})(t) = c_k(t) e^{j2\pi \hat{f}_k t},$$

l'espace de recherche temps, puis effectuer la corrélation avec le signal reçu :

$$AQ_k(\tilde{\tau}) = \frac{1}{T_{acq}} \left| \int_0^{T_{acq}} s_r(t) r_k^*(\hat{f})(t - \tilde{\tau}) dt \right|,$$

où * désigne le conjugué complexe et avec $\tilde{\tau} \in [0, T_{acq}]$

Ainsi, une BTS de *Cell ID* k sera détectée si la valeur maximale de la corrélation AQ_k excède un seuil. Le retard $\tilde{\tau}$ correspondant à ce maximum permettra d'initier la poursuite en générant une réplique locale du signal PRS de *Cell ID* k retardée de la même manière.

3.3. Poursuite

L'étape de poursuite permet de suivre l'évolution du retard, de la fréquence et de la phase porteuse engendrée par les mouvements relatifs du récepteur par rapport à une BTS, et ainsi de mettre à jour une éventuelle localisation au cours du temps. Cette étape est réalisée grâce à des structures (boucles à verrouillage) qui vont suivre les variations des paramètres nécessaires au calcul de la position grâce à la corrélation du signal reçu par des répliques locales générées par le récepteur.

Dès que l'étape d'acquisition détecte une BTS, une poursuite est initialisée en corrélant le signal reçu avec une réplique retardée du signal PRS correspondant. L'ensemble des boucles fonctionnent en parallèle avec un temps d'intégration ajustable en fonction du rapport signal à bruit. Elles fournissent des estimations des

paramètres de navigation avec une période égale à ce temps d'intégration, comme le montre la Figure 2 :

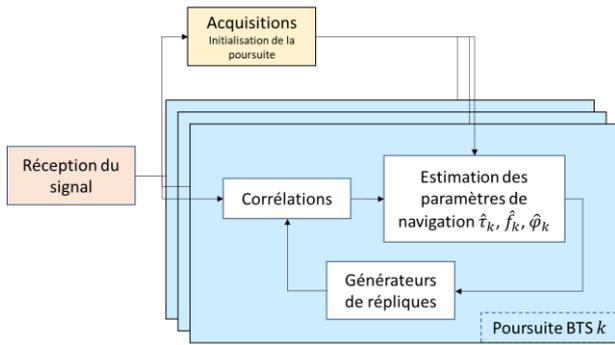


Figure 2 : Synoptique du traitement réalisé

3.3.1. Poursuite du retard

Pour pouvoir mesurer l'erreur d'estimation du retard, le récepteur calcule 3 points de corrélation réalisés avec 3 répliques locales. La poursuite du retard implémentée utilise une boucle à verrouillage d'ordre 2, et est décrit dans [2, Figure 5.13, page 173].

Plus précisément, si le signal associé à la BTS k est reçu avec un retard τ_k et que le récepteur a une connaissance à priori de ce retard $\hat{\tau}_k$ (i.e. le retard précédemment estimé par la boucle), trois répliques sont alors créées en choisissant δ_d la distance du discriminateur de retard telle que $0 < \delta_d < T_c$, où T_c est la largeur du pic principal d'autocorrélation :

- une réplique décalée du retard $\hat{\tau}_k$ (point de corrélation *Prompt*),
- une réplique décalée du retard $\hat{\tau}_k + \delta_d/2$ (point de corrélation *Late*),
- une réplique décalée du retard $\hat{\tau}_k - \delta_d/2$ (point de corrélation *Early*).

3.3.2. Poursuite de la phase

La mesure de la fréquence et de la phase du signal est moins coûteuse en calcul. Elle nécessite seulement les points de corrélations *Prompt*. L'architecture de la poursuite de phase implémentée consiste en une PLL (*Phase Lock Loop*) d'ordre 3 assistée par une FLL (*Frequency Lock Loop*) d'ordre 2, telle que décrit en [2, Figure 5.8, page 165] et plus précisément en [2, Figure 5.21, page 182]. Cette structure fournit une estimation de la fréquence et du déphasage par rapport à la réplique locale.

3.3.3. Extraction des paramètres de navigation

À partir des estimations des paramètres de navigation pour chaque BTS, il est possible de calculer la vitesse radiale relative à chaque BTS grâce à la fréquence mesurée (effet Doppler). Par contre, la distance n'est pas accessible, ne connaissant pas le décalage temporel des signaux PRS. Ayant pour information leur intervalle de répétition (10 ms), ce qui donne une ambiguïté

distance de 300 km, un positionnement par TDOA (*Time Difference of Arrival*) est possible. De la même manière, la phase du signal, qui apporte une information de variation de distance relative, peut être exploitée.

4. Expérimentations

Une campagne de mesures a été effectuée sur le site du Fauga de l'ONERA en mai 2024. Des enregistrements I/Q fixes et mobiles (en voiture) ont été effectués avec le moyen de mesures illustré en Figure 3.



Figure 3 : Moyen de mesure (USRP B210 et antenne LTE)

L'USRP (*Universal Software Radio Peripheral*, Figure 3) est synchronisé par antenne GNSS, et commandé par l'intermédiaire de scripts Python qui appliquent le traitement en temps différé, une fois le signal enregistré.

Le véhicule est équipée d'un récepteur GNSS pour obtenir une vérité terrain. Etant dans un environnement rural, nous avons écouté l'ensemble des opérateurs de la bande 800 MHz, qui offre un bon compromis entre portée des antennes et performances d'acquisition de récepteur. Le signal porté sur la fréquence de 783 MHz, appartenant à l'opérateur Free, présentait le meilleur rapport signal à bruit.

4.1. Acquisition

L'étape d'acquisition a permis de mettre plusieurs BTS en évidence (28, 55, 111 et 454) sur la fréquence de 783 MHz comme le montre la Figure 4 :

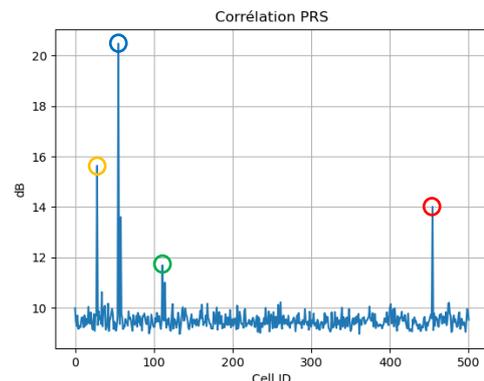


Figure 4 : Acquisition des signaux PRS

Le fait d'acquérir les signaux de plusieurs BTS sur la même fréquence nous affranchit des problèmes de synchronisation et de diversité spatiale des émetteurs.

On note une décorrélation totale entre puissance reçue et distance (ou temps de propagation), comme le montre la Figure 5 présentant les fonctions

d'intercorrélations entre le signal reçu et les répliques des PRS correspondant aux *Cell IDs* détectés. La puissance reçue étant fonction des diagrammes de rayonnement des BTS et de l'antenne utilisées et des conditions de propagation, il paraît difficile d'en extraire des informations de navigation.

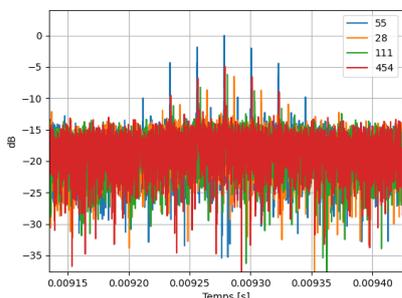


Figure 5 : Corrélations avec les signaux PRS

L'association des *Cell IDs* aux BTS n'est pas une information communiquée par les opérateurs. Pour autant nous avons identifié l'une d'entre elles par corrélation avec nos mesures.



Figure 6 : Association des *Cell IDs* aux BTS (Fond cartographique issu de Cartoradio.fr)

4.2. Poursuite et extraction des paramètres de navigation

Les déplacements parcourus consistent en un aller retour sur une ligne droite avec une vitesse maximale de 30 km/h, représentée par une flèche rouge sur la Figure 6. Le véhicule a démarré au bout de quelques secondes afin de faciliter la convergence (et l'analyse des estimations) des boucles de poursuite.

Les résultats présentés par la suite correspondent aux sorties retard $\Delta d_{\tau,k}$ et phase $\Delta d_{\varphi,k}$ des boucles de poursuite ramenées en distance relative exprimées en mètres. Elles sont comparées avec les distance relatives calculées par données GNSS (représentées en tirets noirs sur les Figures 7 et 8) :

- $\Delta d_{\tau,k} = c\hat{\tau}_k$,
- $\Delta d_{\varphi,k} = \frac{\lambda\hat{\varphi}_k}{2\pi}$,

avec c la célérité de la lumière et λ la longueur d'onde du signal reçu.

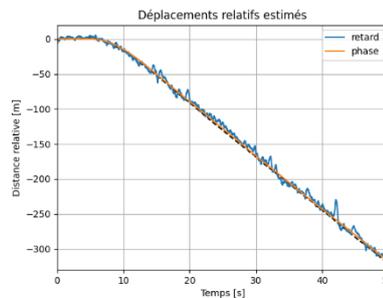


Figure 7 : Aller - Distances relatives estimées

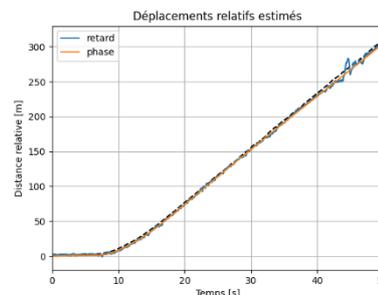


Figure 8 : Retour - Distances relatives estimées

Pour l'aller comme pour le retour, les estimations de distances relatives semblent cohérentes avec celles calculées par l'intermédiaire des données GNSS. Les estimations basées sur la phase sont moins bruitées que celles basées sur le retard, mais peuvent rapidement devenir ambiguës pour des déplacements plus rapides.

5. Conclusion et perspectives

Nous avons mis en œuvre une solution d'extraction opportuniste des paramètres de navigation avec des signaux LTE, à partir de [2]. L'exploitation des paramètres de retard, de fréquence et de phase pour chaque BTS, ou l'exploitation de la phase du signal reçu se sont montrées suffisamment précises pour envisager une solution de positionnement alternative aux GPS. La faisabilité technique n'est plus à démontrer (OTDOA [1]), mais deux verrous technologiques se présentent : les *Cell IDs* des BTS ne sont pas accessibles et leurs coordonnées renseignées publiquement ([3]) ne sont pas toujours précises.

Dans le futur, nous réaliserons une campagne d'expérimentation similaire en milieu urbain pour observer l'impact de multi-trajets, et implémenterons un algorithme de localisation et un filtre de Kalman afin d'estimer les performances de localisation.

Références

- [1] S. Fischer, « Observed Time Difference Of Arrival (OTDOA) Positioning in 3GPP LTE », Qualcomm Technologies, Inc., 2014
- [2] E. D. Kaplan et C. J. Hegarty, Éd., *Understanding GPS: principles and applications*, Second edition. in Artech House mobile communications series. Boston London: Artech House, 2006.
- [3] « Cartoradio - ANFR ». Consulté le: 26 mars 2025. [En ligne]. Disponible sur: <https://www.cartoradio.fr/>