Analyse d'un brouilleur GPS

J.-M Friedt, 7 février 2020

KiCAD a récemment été illustré sur le NE555, le composant réputé comme le plus commercialisé dans l'histoire de l'électronique [1]. Nous pouvons nous interroger sur l'utilisation actuelle de ce composant analogique aux fonctionnalités réduites.

Dans le cadre d'une étude sur la robustesse des systèmes de navigation par satellite, nous avons acquis un "bloqueur" GPS. Le budget que nous nous étions alloué pour un tel achat était de 10 euros : l'analyse du système acquis s'avère centré sur le vénérable NE555. Analysons son fonctionnement, et surtout les conséquences de son utilisation.

1 Introduction

Les systèmes de navigation par satellites sont devenus omniprésents dans notre quotidien, de la localisation à la synchronisation d'horloges pour la génération distribuée d'énergie, les communications ou le bon fonctionnement des flottes aériennes [2], avec un coût estimé de la perte de ce service à 1 milliards de livres pour le Royaume-Unis uniquement [3, 4, 5].

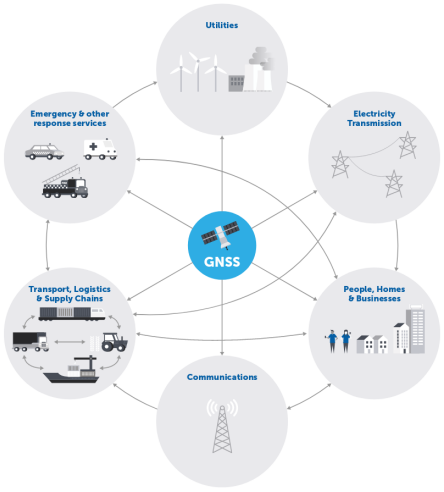


FIGURE 1: Illustration des domaines d'application des systèmes de transfert de temps et de position (PNT) dans l'économie anglaise – extrait de [4]

Cependant, les signaux des satellites de transfert de temps servant au positionnement (*Positioning, Navigation, and Timing* – PNT) en orbite moyenne (MEO, *Medium Earth Orbit*) parcourent 20000 km avant de nous atteindre : les 50 W émis sont dilués sur l'angle solide couvrant la surface de la Terre et une puissance infime atteint le sol, tel que nous l'établirons dans ce document selon le calcul classique de l'équation de Friis [11] de conservation de l'énergie. Il est par conséquent excessivement aisé de saturer le récepteur de tels signaux par un signal émis depuis le sol, même moins puissant, compte tenu du rapport des distances : il s'agit de brouillage, dont nous notons dès le début de ce document qu'il est **illégal**.

Mentionnons par ailleurs que le brouillage de signaux radiofréquences ne démontrent aucune compétence technique : comme toute attaque de déni de service, il s'agit d'une façon stupide et facilement détectable par la perte du service d'handicaper son adversaire en criant suffisamment fort pour l'empêcher d'entendre le signal authentique. Compte tenu du peu d'intérêt technique de l'activité de brouillage, nous nous sommes imposé un budget de 10 euros pour l'investissement matériel nécessaire à cet article.

Le brouillage à large échelle n'est pas un fantasme de spécialistes en sécurité : il a été pratiqué et démontré à grande [6, 7] et petite échelle [8, 9]. Quoique nommé bloqueur GPS, un brouilleur est disponible pour 9 euros sur Amazon [10] (Fig. 2) : notre objectif dans cette présentation est de démontrer l'impact sur une vaste zone de l'utilisation de ce "bloqueur" et de sensibiliser le lecteur aux conséquences de la mise sous tension de ce circuit électronique.

2 Bloqueur v.s brouilleur : analyse du circuit

Le terme "bloqueur" de la publicité du circuit que nous avons acheté pourrait laisser imaginer le client naïf et sans compétence technique que le signal radiofréquence issu de la constellation de GPS

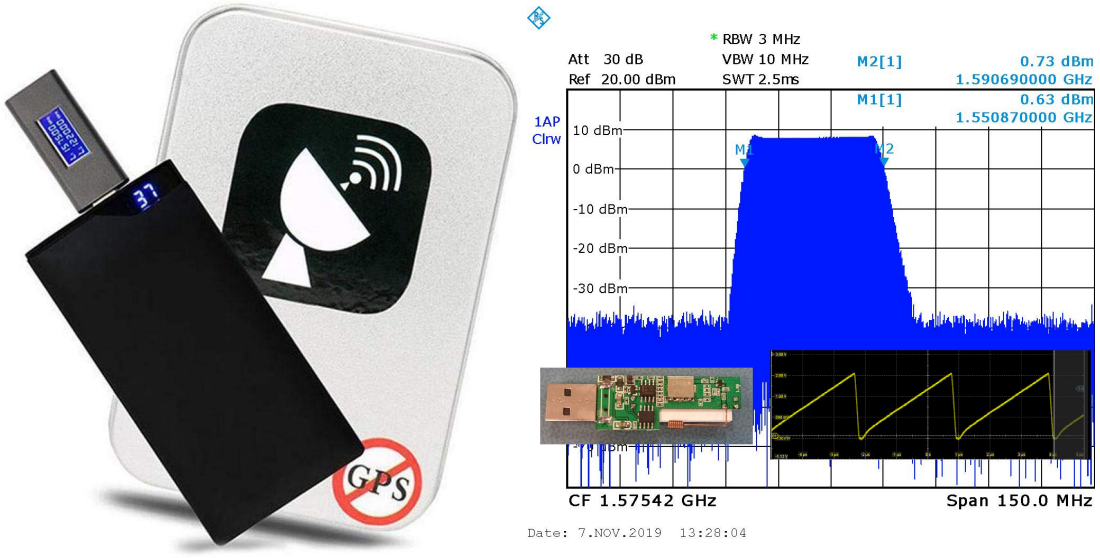


FIGURE 2 – Gauche : publicité du “bloqueur” GPS. Droite : spectre émis par le “bloqueur” qui fonctionne comme un brouilleur émettant 10 mW dans la bande de communication de GPS (et bien plus). En insert, une photographie du circuit et le signal généré par le NE555 pour polariser l’oscillateur micro-onde commandé en tension.

est miraculeusement annulé à proximité du récepteur. Même une solution d’interférence destructive ne serait que locale, excessivement complexe à ajuster, et difficile à mettre en œuvre sur le signal CDMA large bande de GPS. En pratique, nous avons acheté le brouilleur le plus ignoble qui puisse être imaginé : un générateur de signal en forme de dent de scie (le vénérable NE555, Fig. 3) polarise la tension d’ajustement d’un oscillateur micro-onde autour de 1,575 GHz (Fig. 2, droite).

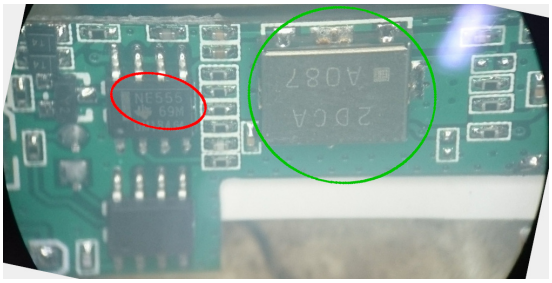


FIGURE 3 – Le circuit du brouilleur GPS : un NE555 (rouge) polarise la tension de commande de l’oscillateur (vert) qui, suivi d’un amplificateur monolithique, émet 10 dBm. Le circuit intégré en bas d’image, non identifié, polarise les cristaux liquides d’un afficheur qui ne sert à rien d’autre que faire croire à l’utilisateur qu’il “bloque” (brouille) la bande L2, mais il n’en est rien puisque l’excursion de la source micro-onde est (heureusement) insuffisante.

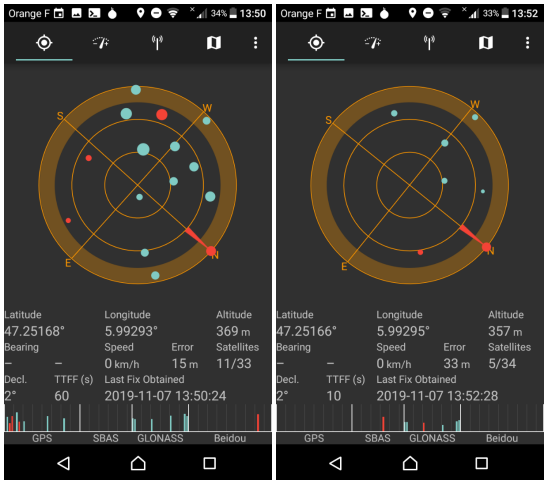
Comme tous ces composants dérivent terriblement avec les conditions environnementales, et en particulier la température, en l’absence d’un quartz ou d’un contrôle de la fréquence, la plage de fréquences balayée est largement supérieure aux 2 MHz de bande passante de GPS : le signal triangulaire

issu du NE555 induit un balayage de l'oscillateur micro-onde sur la gamme 1,55 à 1,59 GHz. Hasard ou proximité de la Russie, la bande 1,6 GHz de GLONASS (1602.0-–1615.5 MHz) est en limite de bande de brouillage et n'est pas trop affectée par le brouilleur. On notera la publicité mensongère sur le site d'Amazon et sur l'écran du brouilleur qui mentionne la bande L2 (militaire) de GPS : aucun signal n'est émis dans cette bande, qui nécessiterait sûrement une excursion excessive de l'oscillateur ou tout au moins d'un circuit un peu plus complexe de polarisation pour ne pas polluer toute la bande entre 1,227 GHz et 1,5754 GHz.

Chaque bit GPS occupe 20 ms (transmission à 50 bps) et chaque bit est lui même encodé par 20 répétitions du code pseudo-aléatoire qui représente chaque satellite, code de 1023 bits de longueur émis au rythme de 1,023 Mb/s (donc répétition du code toutes les millisecondes). En cadençant le NE555 à 300 kHz environ, nous sommes dans l'ordre de grandeur du taux de répétition du code identifiant chaque satellite, garantissant que le récepteur sera incapable de retrouver le signal d'origine.

3 Efficacité sur téléphone portable

Est-ce qu'un dispositif aussi trivial marche? Le traitement du signal a beau faire des miracles, si la puissance du brouilleur dépasse la puissance de l'information reçue, la lutte est déloyale entre un satellite à 20000 km et un brouilleur à quelques mètres ou centaines de mètres du récepteur.



Sans brouillage Brouillage

FIGURE 4 – Téléphone portable en vue d'une constellation GPS lui permettant de se positionner (gauche) et lors du brouillage (droite).

Nous constatons (Fig. 4) qu'un téléphone portable voit sa capacité de localisation clairement handicapée par le brouilleur : la constellation GPS disparaît et seule la capacité d'exploiter GLONASS sur ce récepteur multi-constellations permet d'encore obtenir une estimation de la position. Dans cette expérience, l'antenne du brouilleur avait été dessoudée et remplacée par un connecteur SMA (Fig. 5), et malgré l'absence de l'élément rayonnant, le téléphone était brouillé à quelques mètres du brouilleur. À quelle distance cette attaque est-elle efficace si une antenne est fixée à la sortie de l'oscillateur micro-onde?

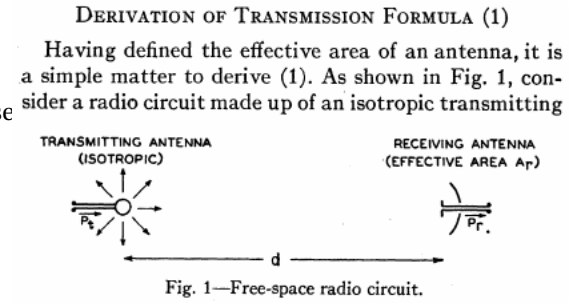
FIGURE 5 – Montage utilisé pour les tests : l'antenne a été remplacée par un connecteur SMA pour les mesures en mode conduit sur analyseur de spectre. Ce connecteur rayonne suffisamment pour démontrer le brouillage de GPS sur un rayon de quelques mètres sans risquer d'affecter les récepteurs à grande distance. Le circuit est alimenté par une batterie fournissant 5 V sur un connecteur USB.

4 Portée du déni de service par brouillage

Nous avons mesuré la puissance émise par l'oscillateur – suivi d'un amplificateur – de 10 mW ou +10 dBm. L'équation de Friis, qui décrit la conservation de la puissance radiofréquence émise P_E sur une sphère de rayon d et donc de surface $4\pi d^2$, indique que la puissance reçue P_R par un récepteur ponctuel à distance d de l'émetteur est, pour une longueur d'onde de λ

$\frac{P_R}{P_E} \propto \left(\frac{\lambda}{4\pi d}\right)^2$

le symbole de proportionnalité indiquant que nous avons omis le facteur de directivité des antennes émettrice ou réceptrice, nous plaçant ici dans le contexte de diagrammes de rayonnement isotropes. En passant sur une échelle logarithmique, et en notant que $20\log_{10}(c/(4\pi)) \simeq 147{,}5$ avec $c = 3 \cdot 10^8$ m/s la célérité de la lumière dans le vide, alors l'équation de Friis devient (puisque $\lambda = c/f$ avec f la fréquence de l'onde transmise)


DERIVATION OF TRANSMISSION FORMULA (1)

Having defined the effective area of an antenna, it is a simple matter to derive (1). As shown in Fig. 1, consider a radio circuit made up of an isotropic transmitting

Fig. 1—Free-space radio circuit.

FIGURE 6: Illustration de l'article de Friis [11] sur la conservation de l'énergie lors de la propagation d'une onde

$$\left(\frac{P_R}{P_E}\right)_{dB} = 20\log_{10}(f) + 20\log_{10}(d) - 147{,}55$$

Les satellite GPS émettent 50 W avec des antennes de gain 13 dBi (gain par rapport à une antenne isotrope) vers la surface de la Terre, soit 60 dBm. Une onde électromagnétique à 1,57542 GHz parcourant une distance de 20000 km perd 182 dB soit une puissance au sol de -122 dBm, bien au dessus des -130 dBm requis par la norme imposée par l'US Air Force [12] et de la sensibilité des récepteurs à mieux que -150 dBm. Par compression d'impulsion, le signal émis sur une bande de 1 MHz et comportant un code pseudo-aléatoire connu se répétant toutes les millisecondes [13], le rapport signal à bruit est amélioré par le récepteur de 1000 ou 30 dB, donc un brouilleur doit émettre suffisamment pour que le récepteur soit ébloui au-delà de -92 dBm.

Le brouilleur que nous avons acquis émet 10 mW=10 dBm. Les -92 dBm sont donc atteints pour une atténuation de 102 dB qui est obtenue à une distance de $d = 10^{65{,}6/20} = 1900$ m. En étant un peu conservateur sur le rapport signal à bruit, nous pouvons raisonnablement considérer que nous

brouillons les récepteurs sur un rayon de **1 km autour de l'émetteur.** La mise sous tension de ce dispositif est donc tout sauf anodine : l'École Nationale Supérieure de Mécanique et des Microtechniques (ENSMM) dans laquelle ces mesures ont été faites se trouve à moins de 400 m de la RN47 qui contourne Besançon et 1100 m de la caserne de gendarmerie locale (caserne capitaine Girard), avec les conséquences que l'on peut imaginer si le déni de service affecte ces utilisateurs.

Les 30 dB de compression d'impulsion que nous avons ajouté à notre bilan de liaison viennent du fait que le décodage de GPS profite de la connaissance du code pseudo-aléatoire émis par les satellites avec lequel le bruit est incohérent : la portée de l'attaque devient bien plus intéressante si un signal suivant la même séquence de modulation de phase est émis pour brouiller GPS, tel que le fait la base russe de Khmeimim en Syrie [14] : dans ce cas, un même émetteur porterait à une soixantaine de kilomètres en négligeant la courbure de la Terre sur une telle distance. Israel s'est plaint de ce brouillage efficace [15] dans son voisinage qui affecte ses aéroports, au même titre que la Finlande avec les signaux émis par la Russie depuis Murmansk [7]. On notera sur le spectre des signaux émis par le brouilleur (Fig. 7) une certaine structure, notamment des raies à la fréquence de balayage de l'oscillateur micro-onde induite par le NE555, contrairement aux spectres de signaux de leurrage GPS qui occupent l'ensemble de la bande de 2 MHz de large par étalement du spectre par la génération du code pseudo-aléatoire [16, Fig.3]. Le plancher de bruit (courbe bleue claire sur la Fig. 7) du signal non-brouillé dans la bande GPS est le bruit thermique puisque le signal GPS se trouve une dizaine de dB en dessous de ce niveau [13].

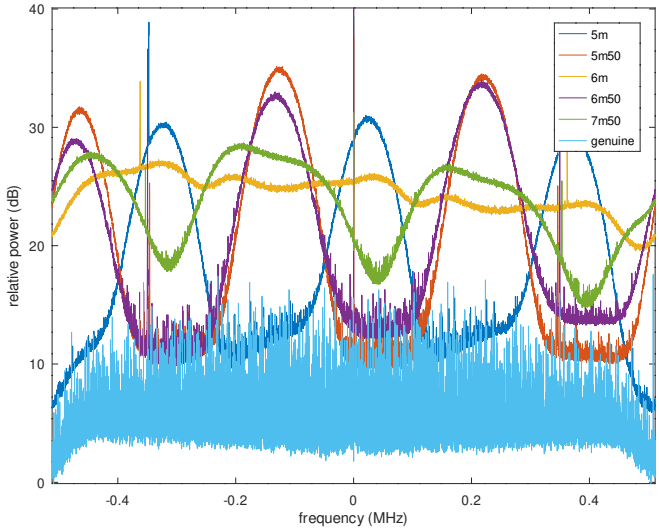


FIGURE 7 – Spectre des signaux de brouillage acquis par récepteur de radio logicielle B210 connectée à une antenne active GPS. Le spectre du signal non-brouillé est visible en bleu clair. La légende indique la distance entre le brouilleur et l'antenne réceptrice, *en l'absence d'antenne sur l'émetteur* puisque lors de cette mesure, seul un connecteur SMA soudé en sortie d'amplificateur radiofréquence rayonne.

Notre intérêt pour l'analyse du dispositif de brouillage porte sur l'annulation du signal de brouillage pour retrouver le signal d'origine. Cependant, le signal de brouillage est tellement puissant que la radio logicielle que nous désirons exploiter pour le traitement des signaux acquis est simplement inutilisable. En effet, les antennes actives (modèle grand publique à 25 euros/pièce, mono-bande) que

nous avons utilisé pour la réception des signaux sont équipées d'un pré-amplificateur qui sature probablement face au signal de brouillage, et aucun post-traitement du signal acquis ne saurait retrouver l'information de la "vraie" constellation de satellites si le brouilleur est trop proche du récepteur. À moyenne portée, des solutions de mitigation existent pour éliminer le brouillage et retrouver l'information authentique de la constellation de satellites.

5 Conclusion

Le brouillage – volontaire ou non – des signaux de positionnement transmis par satellite, en particulier GPS, peut impacter des utilisateurs sur une portée dont un utilisateur d'un "bloqueur" ne se doute pas. Nous avons présenté un circuit excessivement simple pour générer un signal de brouillage de GPS dont nous avons démontré l'efficacité, analysé le fonctionnement et estimé la portée. L'objectif a été de sensibiliser le lecteur à l'impact de l'utilisation d'un tel circuit et bien entendu d'en dissuader l'acquisition.

Remerciement

Cette étude est motivée par le laboratoire commun FAST-LAB entre la société Gorgy Timing, l'institut FEMTO-ST et l'OSU Theta de l'Observatoire de Besançon, avec le soutien de l'Agence Nationale de la Recherche.

Références

[1] L. Frenzel, *The 555 : Best IC Ever Or Obsolete Anachronism?* (Dec 11, 2007) à https://www.electronicdesign.com/technologies/boards/article/21764753/the-555-best-ic-ever-or-obsolete-anachronism

[2] hackaday.com/2019/06/09/gps-and-ads-b-problems-cause-cancelled-flights/ ou www.forbes.com/sites/zakdoffman/2019/06/09/hundreds-of-u-s-flights-canceled-as-gps-based-airc

[3] *The economic impact on the UK of a disruption to GNSS* (2017), à assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf

[4] *Satellite-derived Time and Position : A Study of Critical Dependencies* (2018) à assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf

[5] J. Coffed, *The Threat of GPS Jamming* (2014), à www.chronos.co.uk/files/pdfs/cs-an/ThreatOfGPSJamming_V2.0_January2014.pdf

[6] A. Rawnsley, *North Korea Jams GPS in War Game Retaliation*, Wired (2011), à www.wired.com/2011/03/north-korea-jams-gps-in-war-game-retaliation/

[7] T. Nilsen, *Pilots warned of jamming in Finnmark* (2018, à thebarentsobserver.com/en/security/2018/11/pilots-warned-jamming-finnmark indique le déploiement de "Northern Fleet Center of Radio-Electronic Warfare (TsREB) in the Murmansk region", ou jamestown.org/program/russias-new-electronic-warfare-capabilities-in-the-arctic/

[8] *No jam tomorrow* (2011) à www.economist.com/technology-quarterly/2011/03/12/no-jam-tomorrow

[9] *Son brouilleur GPS bloque l'aéroport de Nantes* à paris.maville.com/actu/actudet_-son-brouilleur-gps-bloque-l-aeroport-de-nantes_54028-3258706_actu.Htm

[10] https://www.amazon.fr/IrahdBowen-Bloqueur-Bouclier-Brouilleur-Disjoncteur/dp/B07KSC5LLD

[11] H.T. Friis *A Note on a Simple Transmission Formula*, Proc. I.R.E. 254- (1946)

[12] *Global Positioning System Standard Positioning Service Signal Specificiation*, p.14 (1995)

[13] J.-M Friedt, G. Cabodevila, *Exploitation de signaux des satellites GPS reçus par récepteur de télévision numérique terrestre DVB-T*, OpenSilicium **15** (Juillet-Sept. 2015)

[14] T. Humphreys, *GNSS Radio Frequency Interference Detection from LEO* à https://www.gps.gov/governance/advisory/meetings/2019-06/humphreys.pdf

[15] https://www.c4isrnet.com/global/mideast-africa/2019/07/02/why-cant-israeli-pilots-get-a-gps-signal/

[16] G. Goavec-Merou, J.-M Friedt, F. Meyer, *Leurrage du GPS par radio logicielle*, MISC HS (2019)