Spread spectrum ou Étalement de spectre

Introduction

Il existe plusieurs techniques d'étalement de spectre en usage aujourd'hui. Ce document vise à présenter les principales, d'une façon pragmatique sans s'aventurer dans des concepts trop mathématiques. Il examinera les avantages et inconvénients des différentes techniques utilisées. Des exemples simples illustrerons la théorie, puis nous finirons par mentionner les utilisations les plus fréquentes de ces technique pour les communications modernes.

Invention

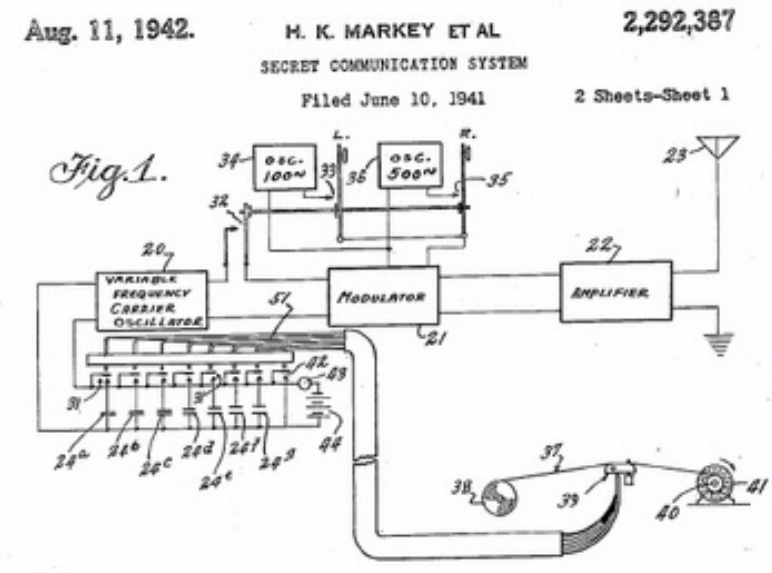
Le premier brevet pour une technique d'étalement de spectre fut accordé en 1942 à une actrice hollywoodienne et un compositeur de ses connaissances.

En effet, Hedy Lamarr (1914 - 2000) actrice américaine d'origine autrichienne et George Antheil (1900 - 1959), compositeur avant gardiste pour son époque, tous deux dotés d'un esprit inventif obtinrent un brevet pour un système intitulé : *Secret communication system* - system de communication secret.

L'invention était initialement proposée pour le guidage à distance d'engins télécommandés tels des torpilles.

La figure ci-dessous représente l'une des illustrations du brevet, celle de l'émetteur. La partie la plus intéressante est tout à gauche, : c'est le *Variable Frequency Carrier Oscillator.*

L'idée de base est de modifier la fréquence de l'oscillateur par pas discrets en commutant différents condensateurs, un par fréquence de sortie. Il est intéressant de constater que les différentes valeurs des condensateur est symbolisée par l'écartement relatif de leurs lames.



Ces condensateurs sont mis en service par des commutateurs commandés par le système représenté en bas vers la droite au moyen d'une transmission pneumatique.

Une bande perforée, telle celle utilisée pour commander des pianos mécaniques, défile à une vitesse contrôlée et actionne ainsi les commutateurs qui enclencheront les différents condensateurs.

À la réception, un système similaire est utilisé, la bande perforée, identique à celle de l'émetteur, étant actionnée à la même vitesse, et de plus synchronisée de temps à autre.

Ce brevet comporte encore plusieurs points spécifiques au guidage de torpilles, mais son élément principal est l'idée d'un changement constant et imprévisible, pour un observateur externe, l'ennemi, de la fréquence d'émission. Cependant puisque le récepteur, connaît et suit ces changements de fréquence, le message est transmis sans encombre, dans son entièreté.

Notons que pour des raisons d'encombrement trop important de ce système pour être placé a bord d'une torpille, il ne fut jamais mis en oeuvre tel quel, mais fut finalement utilisé à des fins militaires en 1962.

De nos jours, les techniques d'étalement de fréquence sont partout : GPS, *Bluetooth*, WiFi, téléphone cellulaire, communications militaires, etc.

Quelques notions de physique et mathématiques

Aléatoire (*random*) : se dit d'une séquence (par exemple de nombres) imprévisible. De plus, le tirage d'un nombre n'affecte en aucune façon le tirage du nombre suivant. Il n'est pas non plus possible de tirer des conclusions basées sur l'historique des nombres tirés précédemment.

Exemple 10 nombres entre 0 et 10 : 2 ; 6 ; 1 ; 7 ; 9 ; 8 ; 10 ; 3 ; 4 ; 5.

Il n'est pas possible de déterminer quel pourrait être le onzième nombre, si ce n'est qu'il sera entre 0 et 10. Ici la moyenne est de 5,5. Cette séquence est relativement courte, une plus longue séquence, peut être de longueur infinie, aurait une moyenne de 5,0.

Pseudo-aléatoire (*pseudo random*) : se dit d'une séquence en apparence aléatoire, c'est-à-dire qui se comporte comme une séquence vraiment aléatoire, mais qui peut être répétée, étant produite par un algorithme déterministique. Une telle séquence dépend généralement d'une graine (*seed*) pour sa génération. Une même graine fournit toujours la même séquence. Sans connaissance de l'algorithme et de la graine il est très difficile (mais pas impossible) de duplifier une telle séquence. Une séquence pseudo-aléatoire a une longueur finie et se répète une fois sa longueur maximale atteinte.

Corrélation : opération qui permet de déterminer si deux séquences coïncident. Deux séquences pseudo-aléatoires identiques sont en corrélation (si elles défilent en même temps). Deux séquences aléatoires ou pseudo-aléatoires différentes auront une faible ou aucune corrélation.

Bruit (*noise*) : le bruit est un phénomène aléatoire naturel. En effet, il est impossible de prédire le niveau instantané de bruit à un instant donné en sortie d'un circuit par exemple. On peut en revanche prédire quel sera le niveau de bruit moyen et le mesurer. La nature totalement aléatoire du bruit instantané fait que l'on s'en sert souvent comme graine dans un générateur pseudo-aléatoire, qui fournira ainsi une séquence différente à chaque redémarrage, mais cela n'en fait pas pour autant un vrai générateur de nombres aléatoires.

Notons qu'une séquence pseudo-aléatoire a beaucoup de points communs avec le bruit. Tout comme le bruit, il est impossible de prédire son niveau (sa valeur) au temps suivant, les deux ont (typiquement) un large spectre, la principale différence est qu'une séquence pseudo-aléatoire est reproductible si l'on connaît l'algorithme qui la génère et la graine de départ.

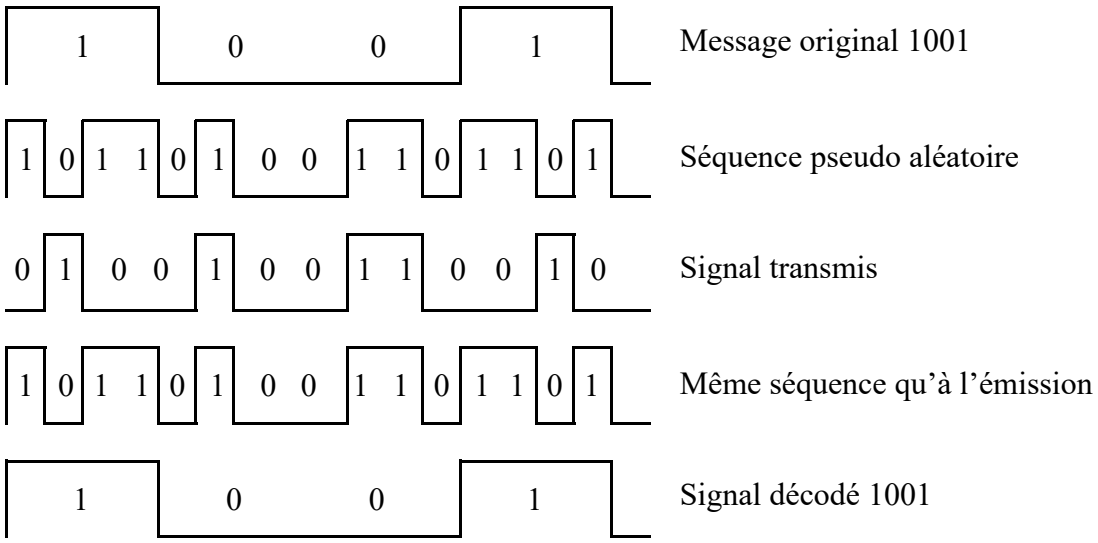
Types d'étalement de spectre

Il y a deux méthodes principales, celle décrite par Hedy Lamarr, appelée **saut de fréquence** (*frequency hopping*) et une seconde qui ne produit que des sauts de modulation, le plus souvent de phase, appelée **séquence directe** (*direct sequence*).

Notons que l'étalement de spectre n'est pas une méthode de modulation

Séquence directe (*direct sequence - DSSS Direct Sequence Spread Spectrum*)

C'est la méthode la plus simple d'étalement de spectre. Le signal à transmettre est combiné avec une séquence pseudo-aléatoire de vitesse plus élevée que le code à transmettre, souvent au moyen d'une fonction ou-exclusif (XOR). La figure ci-dessous illustre cela pour une séquence pseudo-aléatoire 4 fois plus rapide que le code à transmettre. La séquence pseudo-aléatoire utilisée ici est : 1011010001101101. En pratique une telle séquence est beaucoup plus rapide que 4 fois la vitesse des données, comme dans cet exemple.



On peut utiliser plusieurs types de modulation, mais le plus souvent, on utilise le BPSK ou une autre forme de PSK. L'utilisation d'une séquence rapide élargit d'autant le spectre de l'émission tout en n'utilisant qu'une seule porteuse. Cet élargissement du spectre immunise le signal contre des interférences (typiquement à bande étroite) et des écoutes clandestines. En raison de l'étalement du spectre par un signal assimilable à du bruit, l'émission apparaît pour le non initié comme du bruit à large bande, ce qui renforce la sécurité de la liaison. En fait, il peut même devenir invisible car noyé dans le bruit et visible seulement quand désétalé au moyen de la bonne séquence.

Il est aussi possible, en utilisant des séquences pseudo-aléatoires adéquates, non (ou que faiblement) corrélées, d'accommoder plusieurs émissions en DSSS dans une même plage de fré-

quences. Cette technique est utilisée en CDMA (*Code Division Multiple Access*) utilisé entre autres pour les téléphones cellulaires.

Sauts de fréquence (*frequency hopping - FHSS Frequency Hopping Spread Spectrum*)

Dans ce cas on fait usage de plusieurs, voire d'un grand nombre de porteuses séparées.

L'espace disponible pour la transmission est divisé en plusieurs, voire un grand nombre de canaux. Par exemple la bande ISM des 2,4 GHz, utilisée par le *bluetooth*, est divisée en 79 canaux de 1 MHz de large.

Le signal émis change constamment de fréquence parmi les canaux disponibles selon une séquence pseudo-aléatoire. A la réception, la même séquence est utilisée pour que le récepteur écoute le signal la ou il est émis au fur et a mesure de ces sauts de fréquence.

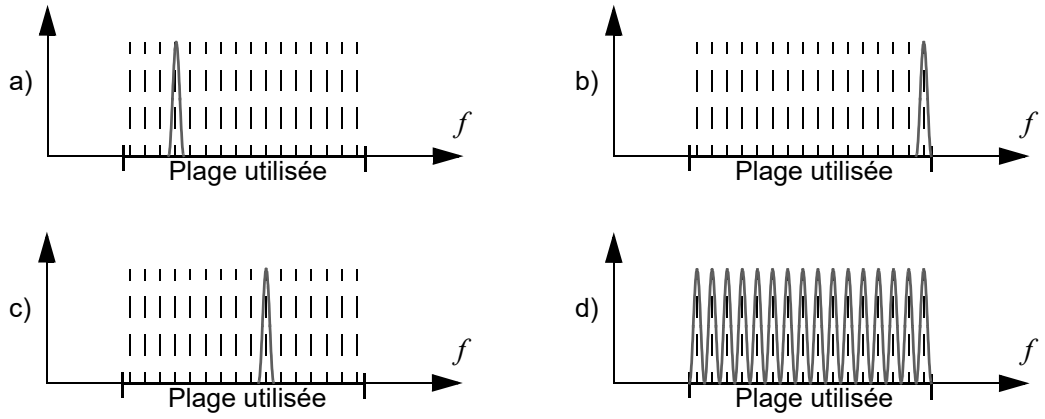
Le résultat est que la transmission est relativement immunisée contre des interférences, qui typiquement n'affectent que l'un ou peu des canaux utilisés. de plus pour les communications sécurisées (militaires), il est difficile d'intercepter le message si l'ennemi ne connaît pas la séquence pseudo-aléatoire utilisée.

Il pourrait sembler que d'utiliser une large plage de fréquences pour la transmission d'un message est un gaspillage de largeur de bande, mais en réalité, il est possible que plusieurs transmissions se passent simultanément en parallèles avec relativement peu d'interférences entres elles par l'utilisation de séquences pseudo-aléatoires non corrélées.

Cette technique est aussi utilisée pour les communication militaires en raison de son immunité au brouillage et de sa résistance aux écoutes clandestines.

Il existe essentiellement deux méthodes de FHSS, soit les saut sont relativement lents et plusieurs bits consécutifs sont transmis par chaque porteuse, soit, les saut sont rapides et dans ce cas, comme dans la DSSS, chaque bits est transmis en plusieurs sauts de fréquence.

Il existe même des techniques de FHSS adaptatives, qui détectent et évitent en temps réel les canaux inutilisables en raison de bruit ou d'interférences.



Exemple de transmission un FHSS. La plage de fréquence utilisée est divisée ici en 16 canaux. En **a**, pendant un bref instant, le canal numéro 4 est utilisé. En **b**, à l'instant suivant, le canal 16 est utilisé. En **c** à l'instant suivant, c'est le canal 10 qui est utilisé, etc. En **d**, le spectre

d’une telle émission après un temps assez long pour que tous les canaux aient été utilisé au moins tous une fois.

Un exemple de technique en FHSS est le *bluetooth*, qui utilise des sauts de fréquence pseudo-aléatoires à 1600 sauts par seconde sur 79 canaux de 1 MHz dans la bande ISM 2,4 GHz.

Cette technique permet des connexions robustes à courte portée pour des périphériques tels que les souris, claviers et casques sans fil. La technique de sauts de fréquence adaptatifs évite la saturation des canaux, améliorant ainsi la coexistence avec d’autres technologies utilisant la bande des 2,4 GHz comme par exemple le WiFi.

Pour les radioamateurs, il y n’y a pas d’applications concrètes des techniques de spread spectrum. En effet, aucun besoin de sécuriser des transmissions ou de lutter contre des brouillages. Cependant, quelques essais ont été tentés, et le FCC autorise des essais sur les fréquences supérieures à 420 MHz, qui doivent ête identifié en télégraphie ou en phonie de façon a pouvoir être reçu sur un récepteur conventionnel.

Références :

https://www.qsl.net/n9zia/ss.qexss.html

https://www.analog.com/en/resources/technical-articles/introduction-to-spreadspectrum-communications--maxim-integrated.html

https://www.geeksforgeeks.org/computer-networks/what-is-spread-spectrum/

https://www.ccs.neu.edu/home/rraj/Courses/6710/S10/Lectures/SpreadSpectrum.pdf

https://sss-mag.com/ss.html

https://www.ausairpower.net/OSR-0597.html

OP 2026-04-06