LES JEUNES IHEDN

[RECHERCHE]

COMMUNICATIONS FURTIVES

ATTAQUE & DÉFENSE

Par Olivier Broyer
Groupe d'Études Scientifiques et Techniques

Ce texte n'engage que la responsabilité de l'auteur. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle de l'association Les Jeunes IHEDN.

SOMMAIRE

À PROPOS DE L'ARTICLE

La multiplication des satellites, en particulier en orbite basse (LEO), rendue possible par la baisse drastique des coûts grâce à l'utilisation de composants sur étagère et à l'optimisation des capacités de lancement ouvre un champ de possibilités inédit.

Mais à mesure que ces opportunités se déploient, de nouvelles menaces émergent. Dans un environnement saturé de capteurs spatiaux et terrestres, une question se dessine : comment transmettre de l'information de furtivement, à l'abri du regard indiscret de satellites ou de stations sol opérés par des puissances étrangères ?

À PROPOS DE L'AUTEUR

Olivier Broyer est ingénieur diplômé d'IMT Atlantique, spécialisé en télécom & automatique. Il est intéressé par l'aérospatiale.

Dans le domaine des communications spatiales, la maîtrise de la sécurité des transmissions constitue un enjeu stratégique majeur. Les conflits récents ont mis en évidence la vulnérabilité des infrastructures spatiales : dans le contexte de la guerre en Ukraine, plusieurs satellites russes ont notamment été observés à proximité de satellites tels qu'Eutelsat, suggérant des activités potentielles d'espionnage, ou de brouillage, en particulier des signaux de navigation comme le GPS.

Face à des menaces d'interception bien réelles, il devient essentiel d'étudier les différentes approches permettant de protéger une transmission contre un agent adverse. Les communications dites furtives s'inscrivent précisément dans cette logique, en cherchant à réduire, voire à éliminer, les capacités de détection, d'identification et d'exploitation d'un signal par un acteur non autorisé.

Dans ce contexte, il convient de distinguer trois étapes fondamentales dans le processus d'interception d'une communication : la détection, l'identification et l'exploitation du contenu. Chacune de ces étapes représente une barrière sécurisant la transmission, un agent ennemi se doit de briser les trois étapes afin d'accéder aux données.

LPD – *Low Probability of Detection*

Ce cas représente l'idéal en matière de communications furtives. La transmission n'est pas détectée par un agent extérieur, lequel n'a même pas conscience qu'un échange a eu lieu. Le signal se confond avec le bruit ambiant ou demeure en dessous des seuils de détection.

LPI – *Low Probability of Intercept / Identification*

Dans cette situation, l'agent adversaire parvient à détecter l'existence d'une transmission, mais il est incapable d'en identifier la nature ou le protocole de

communication. La communication est perçue, mais ne peut être correctement caractérisée.

LPE – *Low Probability of Exploitation*

Ici, le message est détecté et correctement intercepté. Toutefois, il demeure inexploitable, notamment grâce à des mécanismes de chiffrement ou de protection du contenu, empêchant toute compréhension ou utilisation des informations transmises.

Dans la suite de cette partie, seront développées différentes méthodes permettant de rendre une transmission LPD et quelles sont les limites de ces méthodes, ainsi que du côté de l'attaquant comment s'y prendre pour détecter un signal.

Mise en situation :

On considère donc un satellite allié (bleu sur la figure 1) souhaitant communiquer avec la Terre et un satellite ennemi (rouge sur la figure 1) veut tenter **d'intercepter** ou de **brouiller** la communication en se plaçant à proximité du 1er satellite, dans le cône de diffusion du signal. A noter que l'interception peut aussi se faire au sol idem pour le brouillage (ce qui est par ailleurs privilégié dans le cas du brouillage).

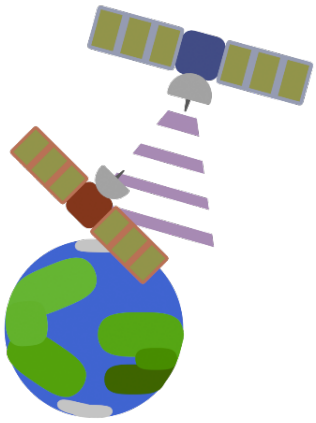

Figure 1 : Mise en situation

Notions de bases en traitement du signal

Cette section développe les bases et notions préalables pour comprendre du traitement du signal, cette section tâchera de rester loin des équations et plus des concepts de bases.

Glossaire

SNR : *signal to noise ratio*, c'est le rapport en décibel entre le niveau d'énergie du signal et du bruit thermique. Si le ratio vaut **0 dB** il y a une puissance équivalente de bruit et d'information.

SCF : *Spectral Correlation Function,* fonction qui permet de repérer des patterns ou ressemblance dans un signal comme la durée symbole par exemple.

CAF : *Cyclic Autocorrelation Function*, il s'agit d'une SCF fait pour une fréquence de retard fixé, elle montre la périodicité d'un signal.

CNA : Convertisseur numérique analogique

HF : Haute fréquence

dB : décibel unité de puissance logarithmique

Symbole : nombre complexe en amplitude et phase contenant plusieurs bits d'informations. Un symbole est émis dans le temps avec une durée symbole associée.

Limite de propagation d'un canal

Les communications à faible probabilité de détection (LPD) impliquent généralement un rapport signal sur bruit (SNR) relativement faible de **0dB** ou moins. Le gain en furtivité se fait ainsi au détriment du débit de communication. Le théorème de Shannon–Hartley permet de déterminer la capacité maximale théorique **sans erreur** d'un canal de communication :

$$C = B.log_2(1 + SNR)$$

Figure 2 : Formule de Shannon-Hartley

Ou **B** est la largeur de bande en Hz et **C** la capacité du canal.

Dans un cas défavorable, le SNR est de l'ordre de **0dB** (soit 1 en linéaire), et la bande passante est de **10 MHz**. On obtient alors une capacité maximale théorique de **10 Mbit/s**. En pratique, le débit réellement atteignable est inférieur à cette valeur en raison des interférences, du bruit et des pertes introduites par le canal de propagation.

Plus la durée de la transmission est longue plus les chances de se faire détecter augmentent il faut donc trouver des compromis entre SNR et temps de diffusion du message, s'il faut téléverser par exemple des images satellites hautes résolutions de plusieurs Gigabits.

Codage Correcteur d'erreur

Afin de pallier les pertes dans le canal de propagation dû au bruit thermique ou aux interférences il est possible d'utiliser un Codage correcteur d'erreur. Cela permet de renforcer la fiabilité de la transmission, de **détecter** voire **corriger certains bits** qui seraient erronés lors de la transmission, la rendre **plus dur à déchiffrer** si un adversaire ne dispose pas de l'architecture du message et des

clefs de déchiffrement. En contrepartie, cela **diminue le débit** d'information car une partie des données est utilisée pour renforcer la transmission et n'est donc pas rigoureusement de l'information utile.

Un exemple simple d'un codage correcteur d'erreur est l'ajout d'un bit de parité à la fin il faut faire la somme binaire des bits d'un message et en réception si pendant le transport, un bit s'est changé, la somme des bits ne fera plus la même valeur qu'à l'envoie l'erreur est détecté.

Il s'agit là d'un exemple simple et pas forcément optimal il est possible de faire des codages correcteurs d'erreur plus complexe pour des messages plus longs.

Par exemple ici, en transmission Tx, la somme des bits vaut 3 (donc 1 modulo 2) pendant la propagation dans le canal un bit est erroné la somme ne fait plus que 2 (donc 0 modulo 2) en réception Rx le bit de parité est faux l'erreur est détectée.

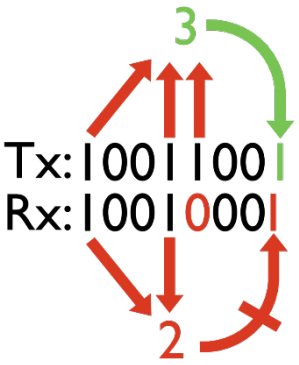

Figure 3 : exemple de codage correcteur d'erreur

Chaîne Montante de communication

Pour transmettre de l'information sur un canal de communication, on suit plusieurs étapes.

Au départ, l'information est représentée sous forme de bits (0 et 1). Pour rendre la transmission plus fiable, on peut ajouter un codage correcteur d'erreurs, qui permet de détecter et parfois de corriger les erreurs dues au bruit.

Ces bits sont ensuite transformés en symboles. Un symbole est une valeur (souvent complexe) qui dépend du type de modulation utilisé, par exemple PSK, QAM ou OFDM. La modulation consiste à représenter l'information sous une forme adaptée à la transmission.

Le signal modulé est ensuite transposé sur une porteuse (une onde de fréquence plus élevée) afin de pouvoir être transmis dans le canal de communication. Cela consiste à multiplier le signal modulé par une sinusoïde de la fréquence désirée.

Pendant sa propagation dans le canal, le signal peut être perturbé par du **bruit**, des **interférences** ou des **pertes** de puissance avec la distance par exemple.

Enfin, le récepteur capte le signal et effectue les opérations inverses : il enlève la porteuse, démodule le signal, convertit les symboles en bits et applique éventuellement le décodage d'erreurs pour retrouver l'information initiale.

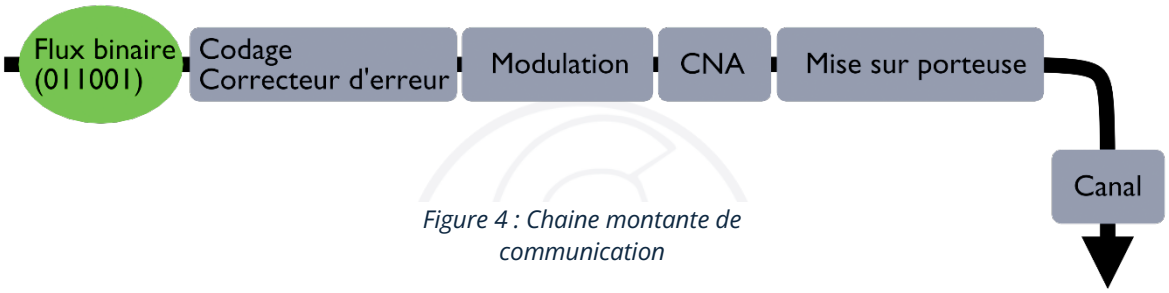

Figure 4 : Chaine montante de communication

Méthodes de détection d'un signal, côté de l'attaquant

Détection par densité énergétique[1]

Il s'agit certainement de la méthode la plus simple en termes d'installation. un observateur externe étudie dans le domaine des fréquences, le spectre, il cherche des zones de fortes énergies spectrales correspondant à une communication. Il peut donc avoir un algorithme fonctionnant avec un **niveau de seuil**, il considère qu'un signal se distingue du bruit omniprésent. Toutefois il est important de garder à l'esprit que plus l'agent regardera un spectre large plus et **devra balayer**

[1] WANG, Tongxiang & YU, Zhang. « Research on Technology of LPI / LPD Communication ». *International Conference on Logistics Engineering*, Management and Computer Science (LEMCS 2014), 2014.

les fréquences en regardant des spectres étroits pour améliorer la visibilité du signal et limiter l'impact du bruit thermique.

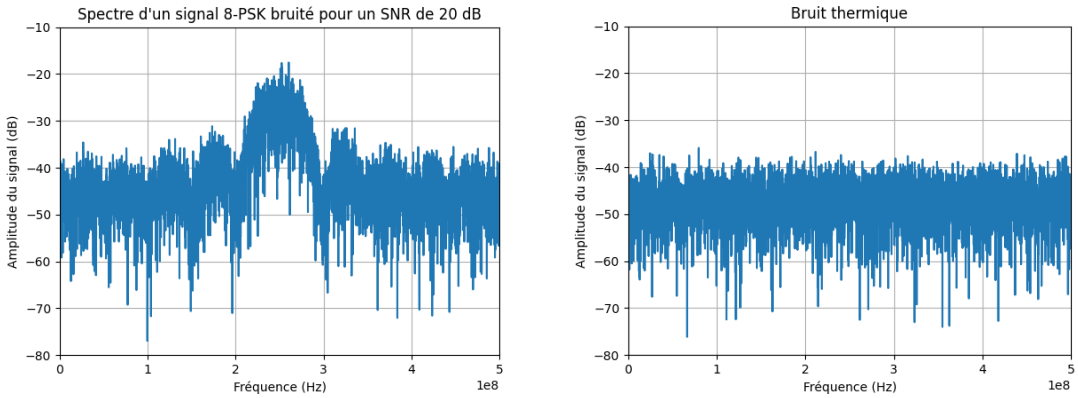

Figure 5 : SPECTRE AVEC SIGNAL PSK OU QUE DU BRUIT THERMIQUE

Dans le cas d'un bon SNR la présence d'un signal se voit distinctement.

Détection par corrélation[2]

Une autre approche consiste à analyser la **structure du signal** à l'aide de la corrélation. Cette méthode permet notamment de mettre en **la présence d'un préambule** (séquence connue par l'émission et la réception pour faciliter la détection d'un signal et l'estimation du canal de propagation), révélatrices d'une communication. Cette approche nécessite toutefois la connaissance de certains paramètres, tels que la fréquence centrale de la porteuse ou la durée symbole ainsi que la forme du préambule.

En présence exclusive de **bruit thermique**, l'autocorrélation d'un signal devrait **rester proche de zéro**, à l'exception du pic central. Le bruit étant aléatoire, sa moyenne est centrée autour de zéro sa corrélation est la somme d'un produit de moyenne nulle qui est de moyenne nulle, aucune structure périodique ou motif

[2] *Ibid.*

récurrent ne se dégage dans le temps. Seul le pic central (à retard nul) reflète l'énergie instantanée du signal.

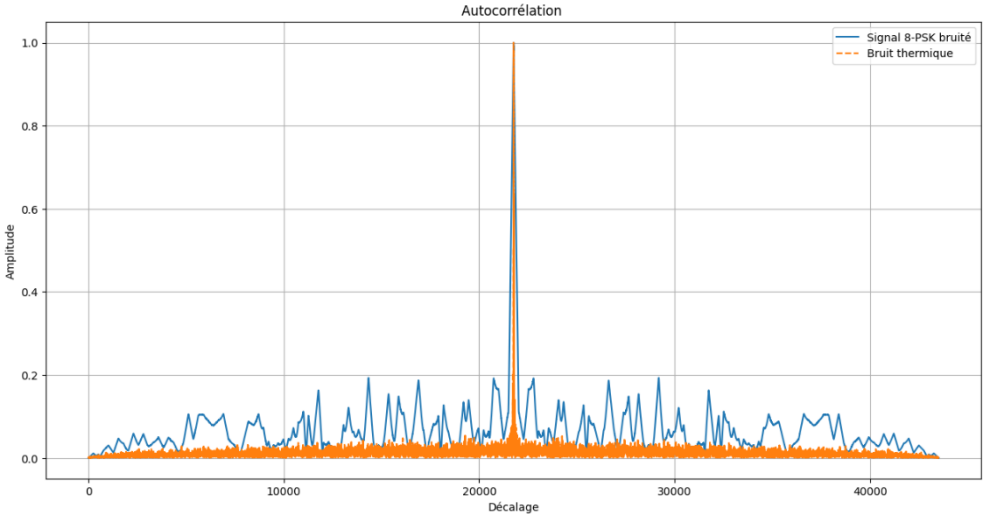

Figure 6 : Autocorrélation d'un signal d'information et de bruit thermique

Dans le cas d'un signal contenant de l'information, des motifs et des éléments de corrélation sont visibles. Il convient de noter que dans cet exemple, le signal a été généré de manière particulièrement favorable et que l'analyse bénéficie de la connaissance préalable de certaines informations sur le signal. Le but est de mettre en évidence le phénomène ; dans la pratique, il peut être beaucoup plus difficile d'obtenir un résultat aussi net.

Par ailleurs, si l'attaquant dispose d'informations supplémentaires, notamment sur le type de modulation employé ou le préambule du message, il peut aller plus loin en réalisant une **corrélation avec un signal de référence** connu et le signal reçu, plutôt qu'une simple autocorrélation, ce qui permet d'améliorer significativement les performances de détection dans le cas d'un préambule.

Détection par cyclostationnarité[3]

La cyclostationnarité est une étape qui suit l'autocorrélation. Elle consiste à **analyser les fréquences présentes dans l'autocorrélation** d'un signal afin de mettre en évidence ses harmoniques périodiques. C'est un outil très puissant, mais qui nécessite des calculs numériques importants.

Le principe de cette méthode est d'étudier les autocorrélations en fonction du **rythme de changement des symboles**, en itérant sur différentes fréquences cycliques pour détecter les structures périodiques du signal.

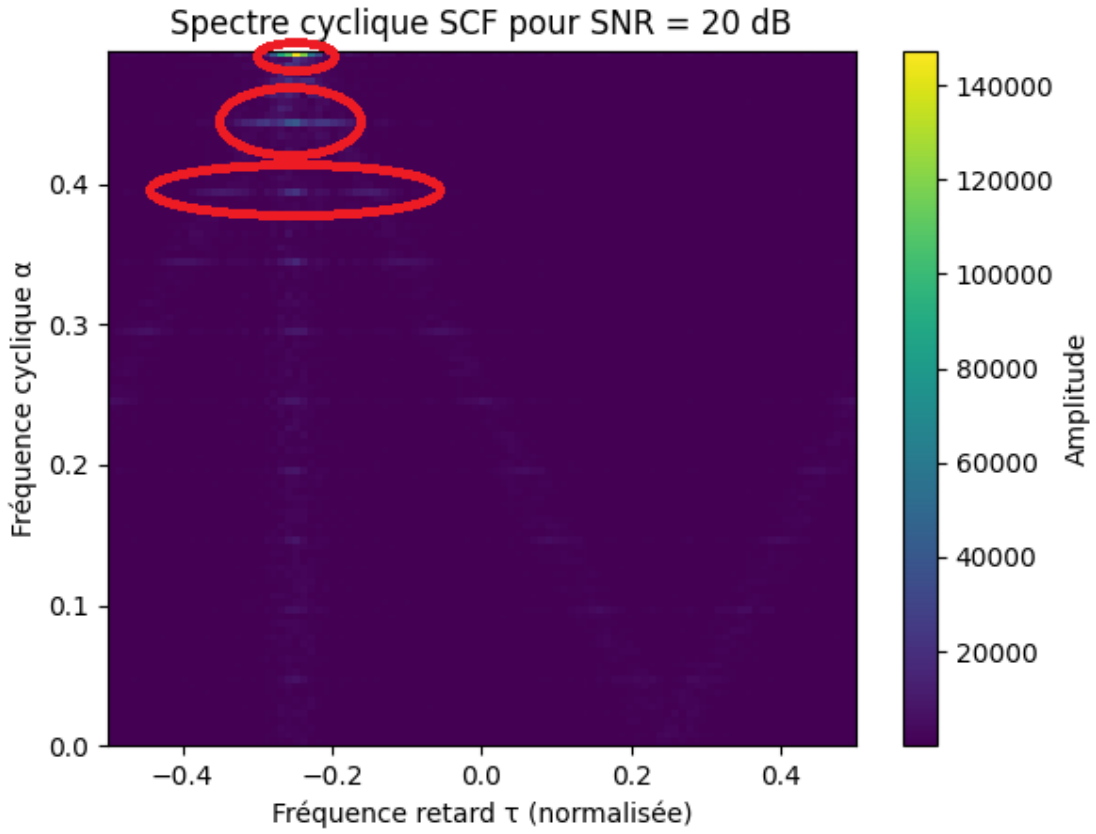

Figure 7 : Analyse de cyclostationnarité

[3] BROWN, Sam. « Cyclostationarit Processing ». PySDR [en ligne], s.d. [consulté le 12/01/2026]. Disponible sur : https://pysdr.org/content/cyclostationary.html.

Dans cet exemple, le signal est détecté dans des conditions de SNR très favorable. La fréquence cyclique correspond à l'intervalle de temps entre deux changements de symbole, c'est-à-dire les instants où le signal modifie sa structure. Dans cet exemple, la durée d'un symbole est de 0,05 s, ce qui se reflète sur le graphe par les traits horizontaux espacés de 0,05 s. Non seulement le signal est détecté, mais cette analyse permet également de mettre en évidence certaines informations sur la structure du signal. Le décalage de la fréquence retard est simplement un biais dû à la modulation[4].

Cette méthode est particulièrement puissante car elle fonctionne avec des SNR assez bas là où les deux autres méthodes ne le permettaient pas !

Dans l'exemple suivant le SNR est de 0 le niveau de bruit est confondu au niveau du signal la méthode de l'autocorrélation ne marche plus et ne permet pas de distinguer des patterns dans le signal. La méthode de la cyclostationnarité quant à elle bien que difficile à analyser détecte toujours un élément malgré le SNR très bas !

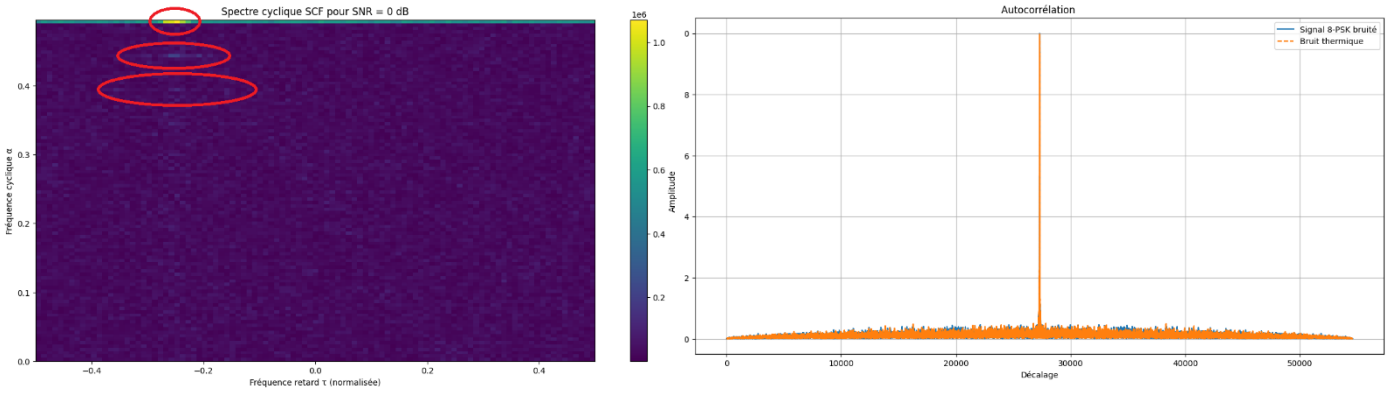

Figure 8 : Cyclostationnarite et autocorrelation

[4] Pour aller plus loin : BROWN, Sam. « Cyclostationarit Processing ». PySDR [en ligne], s.d. [consulté le 12/01/2026]. Disponible sur : https://pysdr.org/content/cyclostationary.html.

Ici l'autocorrélation ne permet pas de déceler le signal pour un SNR de 0dB pour la cyclostationnarité, les paternes restent visibles !

À l'issue de cette partie, différentes méthodes d'interception ou de détection de transmission ont été développées. Il est possible de mettre en œuvre des méthodes plus élaborées non détaillé ici ; cela permet toutefois d'avoir une vision d'ensemble des méthodes disponibles. Ci-dessous se trouve un tableau récapitulatif des trois méthodes proposées.

	densité énergétique	corrélation	cyclostationnarité
Complexité calculatoire	faible	moyenne	élevé
Robuste à faible SNR	faible	moyenne	élevé
Connaissance préalable du signal	Non	Oui	Non

Figure 9 : Tableau récapitulatif des méthodes de détection

Méthodes de communications furtives

Afin de passer inaperçue il existe plusieurs méthodes pour dissimuler les signaux, et faire des signaux **LPD ou LPI** afin d'éviter les interceptions par des agents extérieurs.

Frequency-hopping spread spectrum (FHSS)[5]

Le principe de cette méthode consiste à changer périodiquement la fréquence de la porteuse au cours du temps selon une séquence prédéfinie, connue uniquement de l'émetteur et du récepteur. Ainsi, un attaquant ne connaissant pas cette séquence ne pourra pas ajuster correctement son système afin d'intercepter ou de déchiffrer le signal de manière fiable. De plus, s'il n'a pas accès à l'intégralité du signal, il lui sera impossible de l'exploiter correctement. Dans le cas d'un brouilleur, celui-ci devra soit bruiter une très large bande de fréquences, ce qui est coûteux en énergie, soit tenter de suivre les sauts de fréquence, ce qui s'avère particulièrement complexe sans connaissance préalable de la séquence.

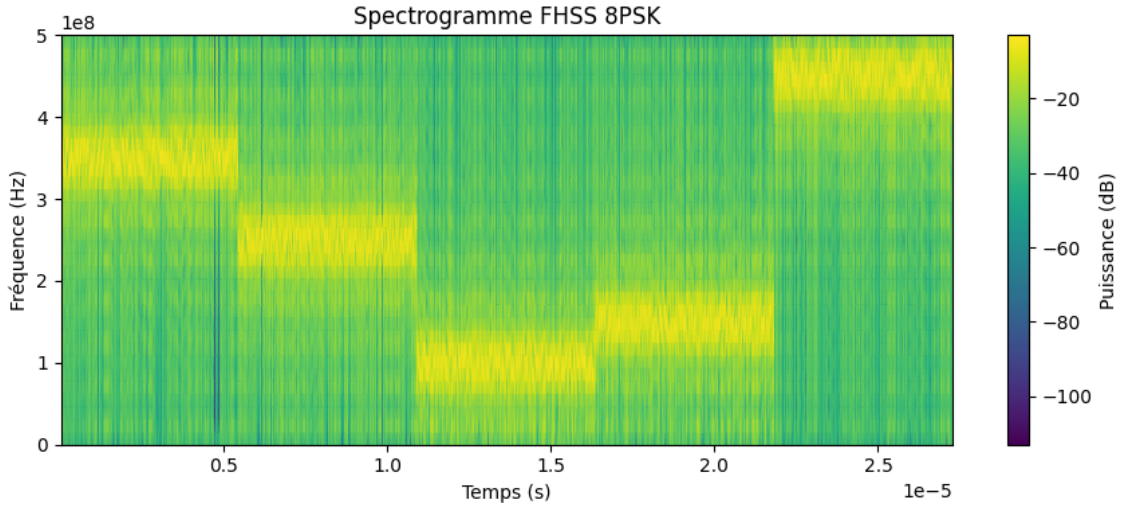

Figure 10 : Diagramme temps fréquence avec une modulation FHSS

Ci-dessus est représenté un spectrogramme temps fréquence, il permet de montrer ou se situe l'énergie du signal fréquentiellement au cours du temps. Les sauts de fréquences sont alors bien visibles. Sans connaître le pattern des sauts de fréquence, il devient difficile pour un attaquant de regarder le spectre à la bonne gamme de fréquence au bon moment.

[5] CUEVAS, Diego ; GUTIÉRREZ, Mikel ; IBÁÑEZ, Jesús & SANTAMARIA, Ignacio. L*ow Probability of Detection Communication Using Noncoherent Grassmannian Signaling*. Dept. of Communications Engineering Universidad de Cantabria, Spain, 2025.

L'un des autres avantages de ce système réside dans la répartition du signal sur plusieurs sous-bandes. En effet, la transmission sur plusieurs sous-bandes améliore la robustesse du signal face aux effets du canal de propagation, tels que le bruit, les interférences et les évanouissements sélectifs.

Direct Sequence spread spectrum (DSSS)[6]

Cette autre méthode de modulation consiste à multiplier le flux binaire avant de le moduler sur porteuse par un code binaire pseudo-aléatoire (0 ou 1) haute fréquence, connu à la fois du satellite émetteur et du récepteur.

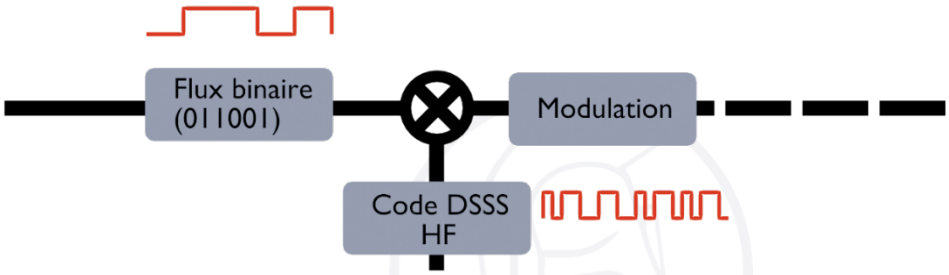

Figure 11: Architecture DSSS

En raison des propriétés temps ↔ fréquence, une modulation à haute fréquence implique une occupation plus large du spectre fréquentiel, conduisant ainsi à un étalement du signal. Celui-ci peut alors être reçu avec un SNR plus faible, tout en restant détectable après desétalement. Le facteur d'étalement du spectre est égal au rapport :

$$Facteur_{etalement} = \frac{F_{DSSS}}{F_{binaire}}$$

Figure 12 : Formule étalement du spectre

[6] *Ibid.*

De plus, l'ajout de ce code rend le déchiffrement du message beaucoup plus difficile pour un attaquant ne disposant pas du code pseudo-aléatoire approprié, ce qui renforce le caractère **LPE** du signal.

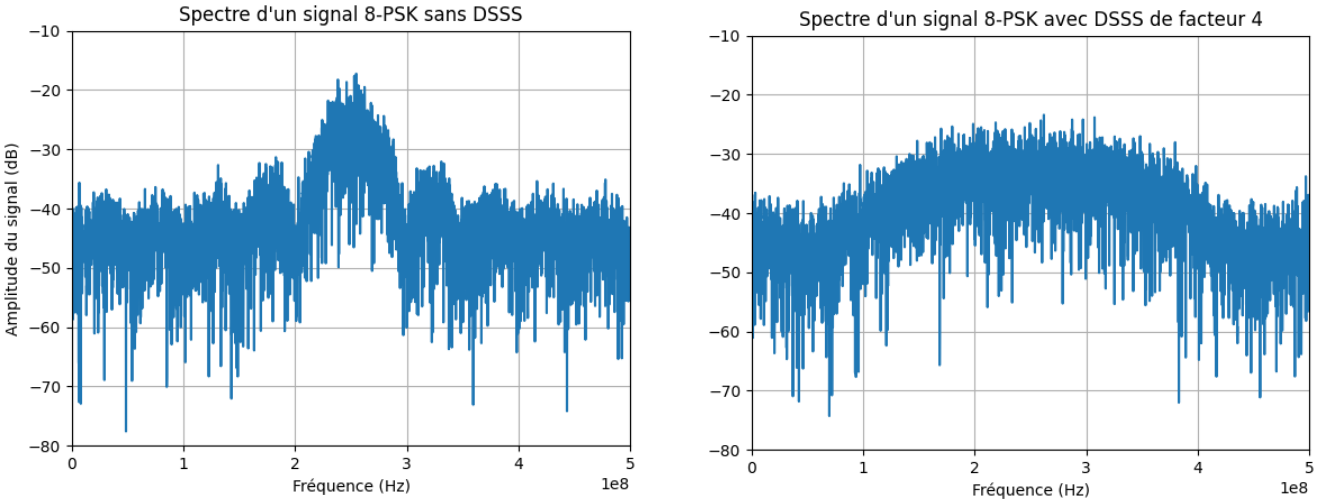

Figure 12 : Signal avec DSSS

Dans cette exemple l'effet de l'étalement du spectre est bien visible l'information est plus répartie en fréquence le SNR à en conséquent diminué. Le lobe principal est passé d'une largeur de bande de **1Mhz** environ à **4 Mhz.** L'énergie maximum du signal est aussi divisée par **4** soit **6db** environ.

Il est par ailleurs possible de combiner les techniques FHSS et DSSS afin de rendre la transmission encore plus robuste et difficile à intercepter. Pour ces deux méthodes, un élément clé est le **synchronisme** entre l'émetteur et le récepteur : ceux-ci connaissent précisément l'instant auquel la transmission a lieu, information inconnue d'un attaquant qui doit alors scruter en permanence l'ensemble du spectre à la recherche d'une éventuelle émission.

De ce fait, puisque ces deux techniques utilisent des séquence de modulation de fréquence pour le FHSS ou code pseudo-aléatoire pour le DSSS, il est indispensable de synchroniser l'émission et la réception, afin que le récepteur

applique le bon code au bon instant et puisse ainsi désétaler et déchiffrer correctement la transmission.

Au vues des méthodes des attaquants décrite ci-dessus, en utilisant des méthodes de cyclostationnarité ou de corrélation, même si le signal transmit se fait avec de faible SNR il peut tout de même être détecté par la structure du signal.

Dissimulation dans du bruit[7,8]

Cette méthode consiste à camoufler le signal transmit en le faisant passer pour du bruit. Après avoir été mis sur porteuse le signal est modulé en amplitude et en phase par un bruit pseudo aléatoire une fois encore connus en émission et en réception. En faisant ça le signal transmit aura des propriétés plus proches du bruit et sera difficile à détecter.

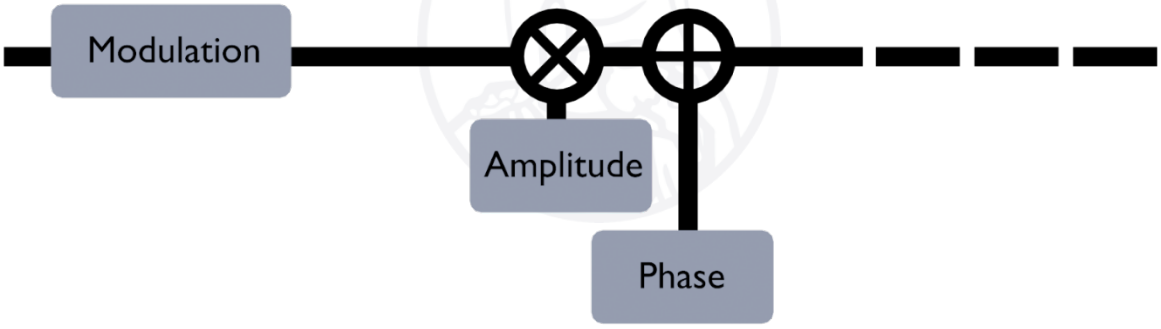

Figure 13 : Architecture dissimulation bruit

Ce masque de Canal permet de rendre moins visible le signal, en effet dans le cas d'une analyse par cyclostationnarité, le signal camouflé reste toujours un peu visible avec la fréquence symbole qui ressort mais l'amplitude est plus faible et les harmoniques décroissent plus rapidement que dans le cas sans masque de canal.

[7] CHOI, Junsung ; Park, Dongryul ; Kim, Suil & Ahn, Seungyoung. « Implementation of Noise-Shaped Signaling System through Software-Defined Radio ». *Appl. Sci.*, 2022, 12(2), 641.
[8] BASH, Boulat A. ; GOECKEL, Dennis ; GUHA, Saikat & TOWSLEY, Don. « Hiding Information in Noise: Fundamental Limits of Covert Wireless Communication ». IEEE, 2015.

Ici un SNR de 10dB a été choisi afin de bien mettre en valeur le phénomène avec un SNR proche de 0 la détection est plus difficile.

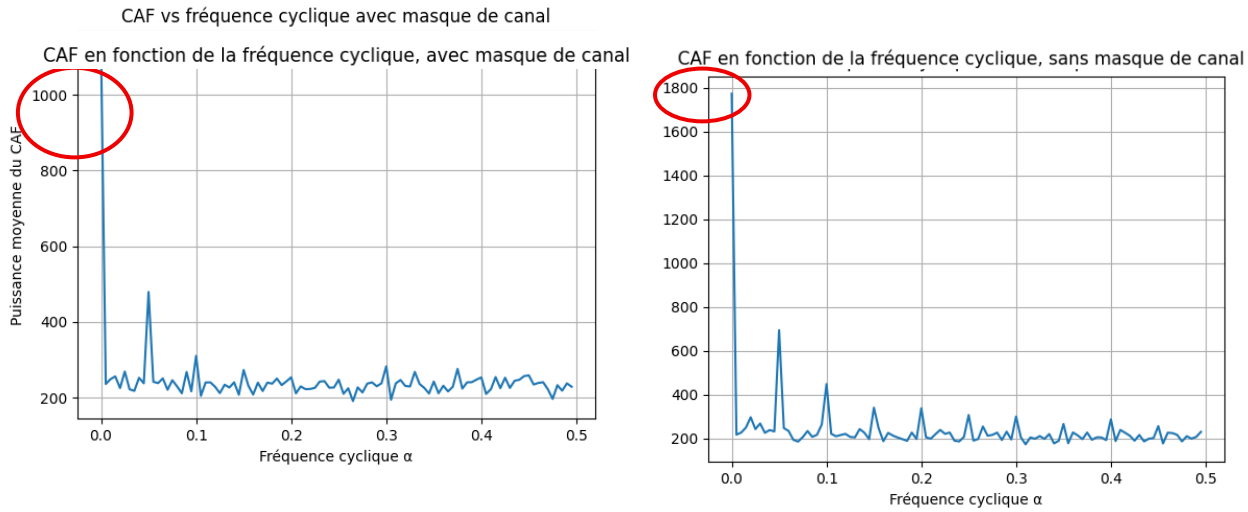

Figure 14 : Analyse par cyclostationnarité avec et sans masque de canal

Plus le signal est furtif, plus la synchronisation de la communication entre l'émetteur et le récepteur est importante, le récepteur pensera qu'il reçoit du bruit autrement !

Modulation des lobes secondaires[9]

Cette dernière méthode est particulièrement intéressante car plus moderne. Aujourd'hui, les antennes sont généralement constituées d'une multitude de petites antennes patch formant un réseau d'antennes. Chaque élément peut être modulé en phase et en amplitude afin de générer un signal parfaitement contrôlé. En réalisant la somme de l'ensemble des signaux émis, on obtient un signal plus puissant et orientable, défini par un diagramme de rayonnement.

Ce diagramme (Figure 15) présente un lobe principal, qui correspond à la direction de communication souhaitée, mais également des lobes secondaires. Ces derniers

[9] ZHAO, Jiahao ; QIAO, Shichen ; BOOSKE, John H. & BEHDAD, Nader. « Low-probability of Intercept/Detect (LPI/LPD) Secure Communications Using Antenna Arrays Employing Rapid Sidelobe Time Modulation ». *Arxiv*, 17 juin 2024.

sont généralement indésirables, car ils constituent une conséquence inhérente à la structure et au fonctionnement des antennes réseau.

La solution de modulation visant à permettre une communication furtive consiste alors à faire varier dynamiquement la phase et l'amplitude des éléments d'antenne périphériques, de manière à modifier le contenu informationnel des lobes secondaires. En faisant osciller rapidement ces paramètres, le signal rayonné en dehors du lobe principal ressemble à du bruit du point de vue d'un ennemi.

Ainsi, un satellite ennemi cherchant à intercepter la communication en se plaçant à proximité n'aura pas nécessairement accès au lobe principal, qui contient l'information utile. Il ne pourra capter que les lobes secondaires, ne transportant qu'un signal assimilable à du bruit, ce qui rend la détection ou le déchiffrement de la transmission impossible ou très difficile.

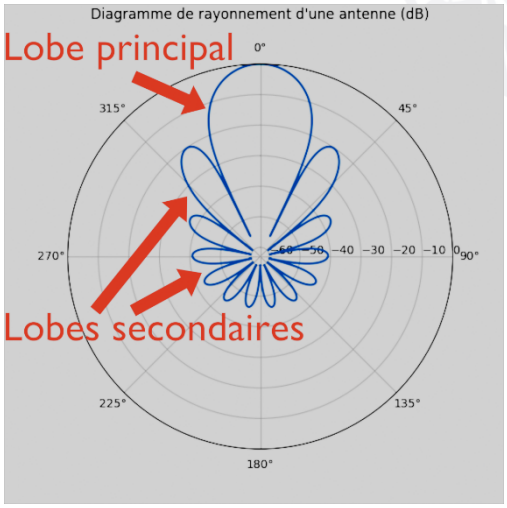

Figure 15 : Exemple de diagramme de rayonnement

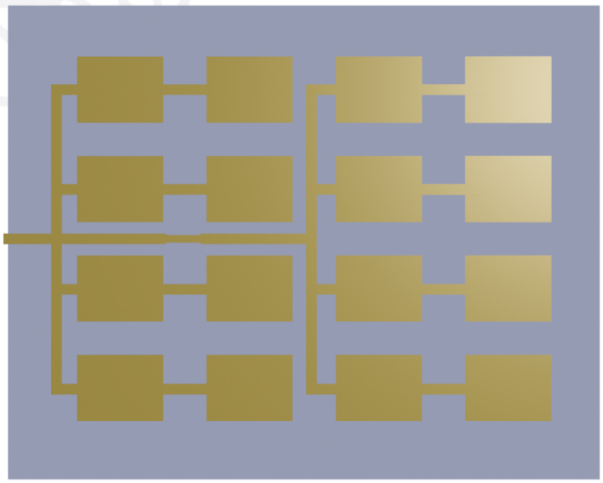

Figure 16 : Réseau d'antenne patch

Conclusion

L'interception des communications constitue une menace majeure dans le contexte spatial. Comme présenté dans cet article, l'accès à une information transmise nécessite de franchir trois étapes clés : la détection, l'identification et l'exploitation du signal. Les méthodes de détection modernes, notamment basées sur la corrélation et la cyclostationnarité, montrent que même des signaux à faible SNR peuvent être révélés par leur structure.

Pour y faire face, différentes techniques de communication furtive ont été étudiées, telles que l'étalement de spectre (FHSS, DSSS), la dissimulation du signal dans le bruit ou encore le contrôle des lobes secondaires via des antennes réseau. Il est possible de combiner toutes ces méthodes et d'être rigoureusement synchronisée en émission et réception pour renforcer encore la sûreté de la transmission.

Du point de vue d'un défenseur l'efficacité des méthodes de transmission est résumée ci-dessous :

	FHSS	DSSS	Dissimulation	Lobes secondaires
Robuste brouillage	+	+	=	=
LPD	=	+	++	+
LPE	+	=	++	++

Toutefois, une perspective particulièrement prometteuse réside dans les communications optiques par laser. Cette technologie est déjà maîtrisée pour les liaisons inter-satellites, facilitées par l'absence d'atmosphère, L'énergie du laser

étant absorbée par l'atmosphère. Elle commence également à se développer pour les communications espace-sol, bien que celles-ci soient plus complexes en raison des phénomènes de diffraction, de diffusion et de turbulence atmosphérique, susceptibles d'engendrer des pertes ou un élargissement du faisceau.

Cette solution réduit de manière drastique les possibilités d'interception : le faisceau laser étant extrêmement directif, un satellite espion devrait se placer quasiment dans l'axe exact de la transmission pour en capter le signal. Par ailleurs, une liaison optique permet d'atteindre un rapport signal sur bruit très élevé, autorisant des débits d'informations nettement supérieurs à ceux des communications radiofréquences, tout en conservant un niveau de furtivité intrinsèquement élevé.






publication@jeunes-ihedn.org