

Situation d'Apprentissage et d'Évaluation n°31 : Mettre en œuvre un système de transmission

Destinataire : Alain ROUX

Étudiants : Pierre CHAVEROUX - Daniel HALIDI

Sommaire

Introduction.....	1
1. Principe du brouilleur radio FM et Schéma Synoptique.....	2
1.1. Qu'est-ce qu'un brouilleur radio ?.....	2
1.1. Quelles sont les différences entre un brouilleur AM et FM ?.....	3
1.2. Schéma synoptique d'un brouilleur radio en fréquences (FM).....	5
1.3. Applications possibles et responsabilités légales.....	6
2. GNU Radio : Frequency Jammer.....	8
2.1. Généralités.....	8
2.2. Flowchart N°1 : montage simple.....	9
2.3. Flowchart N°2 : montage d'application.....	16
3. Frequency Jammer ~ Adalm Pluto.....	18
3.1. Configuration hardware.....	18
3.2. Brouillage d'une connexion à une Access Point Wi-Fi - 2.437 GHz.....	19
Conclusion.....	22
Annexes - Sources.....	23

Introduction

La SAE31, pour ‘Situation d’Apprentissage et d’Évaluation n°31’, est le premier projet en autonomie du troisième semestre. Cet exercice, centré sur le module RT2 : Connecter les entreprises et les usagers, aura pour objectif de traiter des brouilleurs radio en fréquence. Ce rapport aura donc pour objectif de venir compléter la présentation technique orale qui aura lieu en fin de semestre.

Les brouilleurs radios sont des appareils passionnantes utilisés de manière très réglementée en France, et plutôt à destination du corps des armées que pour le corps civil. De ce fait, il ne sera difficilement possible de tester le fonctionnement d'un brouilleur ailleurs qu'en laboratoire. Pour pallier l'aspect pratique de cet exercice, nous utiliserons le logiciel GNU Radio pour simuler le fonctionnement d'un brouilleur radio.

Dans un premier temps, nous tâcherons de comprendre le principe général d'un brouilleur radio, en faisant la distinction entre un brouilleur en fréquence et un brouilleur en amplitude. Une fois fait, nous créerons un schéma synoptique du fonctionnement de ce frequency jammer. Ensuite, nous aborderons l'aspect juridique du domaine et des responsabilités légales qui s'appliquent à l'étude de ce sujet. Enfin, nous verrons les différentes utilisations possibles d'un brouilleur en fréquence, qu' elles soient militaires ou civiles.

Dans un second temps, nous nous intéresserons en détail aux manipulations effectuées dans le logiciel de simulation GNU Radio afin de pouvoir simuler le fonctionnement d'un brouilleur radio en fréquence. Nous détaillerons dans cette dernière partie le rôle de chaque bloc qui compose notre flowchart, et nous tâcherons d'établir un lien chronologique de l'évolution des caractéristiques du signal transmis sur le médium, entre l'émetteur et le récepteur.

Dans un troisième et dernier temps, nous mettrons en pratique les compétences acquises grâce à la carte Adalm Pluto et un test de brouillage d'un Access Point Wi-Fi 2,437 GHz.

Nous conclurons ensuite ce rapport par une analyse rétrospective de l'étude effectuée sur les brouilleurs radios en fréquence et de cette SAE.



1. Principe du brouilleur radio FM et Schéma Synoptique

Dans cette première partie, nous allons chercher à comprendre ce qu'est un brouilleur radio en fréquence. Pour ce faire, nous aborderons ses principales caractéristiques techniques, et nous détaillerons son fonctionnement en s'appuyant sur un schéma synoptique.

1.1. Qu'est-ce qu'un brouilleur radio ?

Un brouilleur radio est un appareil électronique qui a pour but d'émettre des signaux radiofréquences pour empêcher ou limiter la communication sans fil entre deux machines (l'émetteur et le récepteur) dans une zone donnée.

Les brouilleurs radios (Radio Jammer en anglais) émettent délibérément des signaux électromagnétiques sur les mêmes fréquences que les signaux cibles à brouiller. Lorsque l'appareil est en fonctionnement, les signaux d'origine sont noyés ou brouillés par les signaux pirates du brouilleur, ce qui perturbe ou empêche la communication normale.

La composition physique (Hardware) d'un brouilleur radio est amenée à différer en fonction de sa complexité ou de son milieu d'utilisation, mais nous allons ici chercher à en cerner les principaux. Ainsi, on retrouve dans cet appareil les modules suivants :

- Un oscillateur local : c'est le cœur du brouilleur, cet élément a pour rôle de générer le signal de brouillage à la fréquence souhaitée.
- Un amplificateur en puissance : pour pouvoir brouiller des signaux lointains dans l'espace, le signal émis par l'oscillateur local a besoin d'être amplifié. Ce rôle est rempli par l'amplificateur qui permet d'augmenter l'amplitude du signal de brouillage.
- Une unité de contrôle : cet élément est le cerveau du brouilleur, il a pour objectif de permettre à l'utilisateur de configurer l'appareil et de sélectionner la fréquence de brouillage, la puissance de sortie ou encore la modulation du signal.
- Une ou plusieurs antennes : évident, mais essentiel, les antennes ont pour rôles d'émettre et de propager le signal de brouillage en direction de la cible.
- Autres composants électroniques d'un brouilleur : pour fonctionner, le brouilleur a besoin de composants standards tels qu'une alimentation électrique, un boîtier (étanche ou non), un système de refroidissement (pour les plus gros appareils), etc.

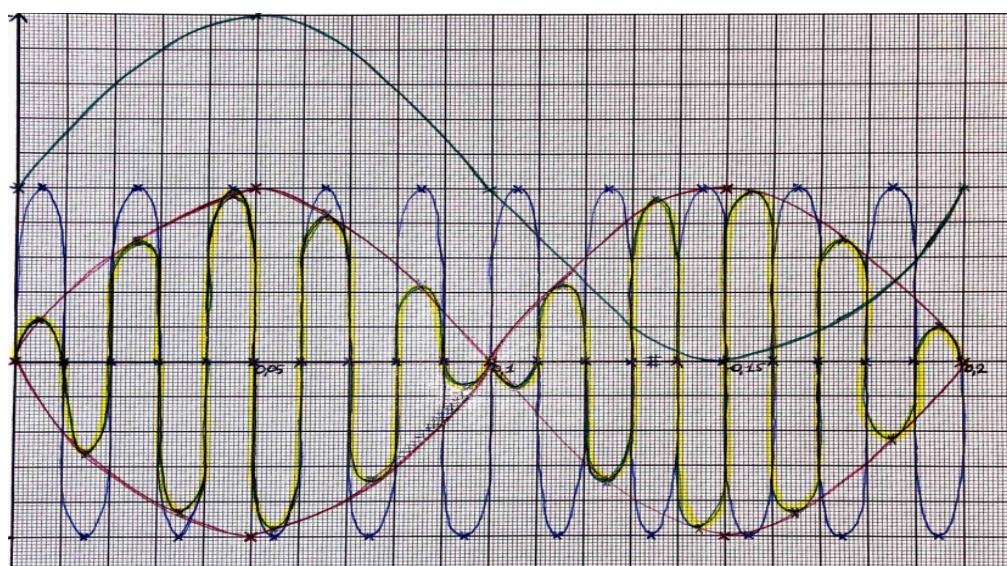
Les brouilleurs radios peuvent prendre des apparences différentes :



1.1. Quelles sont les différences entre un brouilleur AM et FM ?

Les brouilleurs en amplitudes (AM) et les brouilleurs en fréquences (FM) sont tous les deux des appareils remplissant les caractéristiques de la partie précédente. Cependant, on distingue ces deux types de 'Jammers' par la façon dont ils vont brouiller les signaux de communications cibles. L'objectif de cette partie est donc de comprendre la technologie utilisée dans chacun des deux cas.

Avant de rentrer dans le détail, il est nécessaire de faire un arrêt sur le vocabulaire utilisé pour décrire un signal radio. Le graphique effectué lors du TD d'introduction à cette SAE nous permettra aisément de faire ce travail de rappel :



On tire des sinusoïdes ci-dessus le vocabulaire suivant :

- La fréquence porteuse : cette fréquence sert de base pour transmettre la donnée. Elle est utilisée comme support de l'information. La fréquence de la porteuse est donc la même que la fréquence du signal émis en sortie. C'est la sinusoïde bleue.
- Le signal modulant : le signal modulant est le signal qui porte l'information que l'on souhaite transmettre (qui peut être de la voix, de la vidéo, etc). C'est la sinusoïde rouge.
- Le signal modulé : c'est le résultat de la combinaison du signal modulant et de la fréquence porteuse. Ce signal est celui qui est modulé puis émis par l'émetteur et qui sera capté et démodulé par le récepteur. C'est la sinusoïde surlignée.

Moduler un signal, c'est donc de transmettre une information issue d'un signal modulant sur (ou en fonction d') une porteuse. La modulation superpose alors les caractéristiques du signal modulant (telles que son amplitude, sa fréquence et sa phase) sur la fréquence porteuse.

Maintenant que nous avons rappelé les différents acteurs d'un signal modulé, abordons la différence entre un brouilleur radio en modulation de fréquence et un brouilleur radio en modulation d'amplitude.

- Le brouilleur radio par modulation d'amplitude

Les brouilleurs en amplitudes, à la différence de leurs concurrents, cherchent à perturber les communications en modifiant l'amplitude du signal porteur de la cible. Ces signaux sont moins discrets que ceux issus des brouilleurs FM, mais permettent des applications plus larges. L'amplitude du signal de la porteuse est modulée pour ajouter du bruit et perturber la communication, le rendant plus difficile à décoder.

- Le brouilleur radio par modulation en fréquence

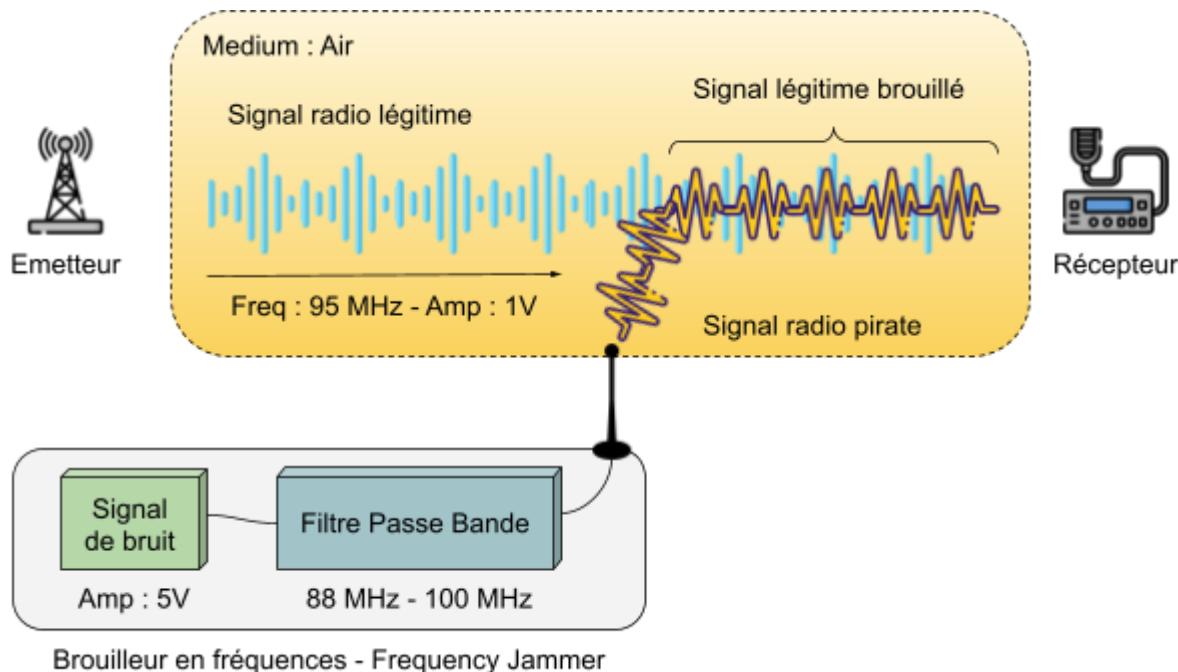
Les brouilleurs en fréquences sont des appareils difficilement détectables, car cherchent à perturber les communications en émettant un signal de brouillage à la même fréquence que la porteuse du signal cible.

Pour utiliser ce type de brouilleur, il est donc nécessaire de régler précisément l'oscillateur que l'appareil intègre sur la fréquence du signal cible (à la fréquence de la porteuse du signal cible).

Lorsque les deux signaux (celui de la cible et celui du brouilleur) partagent le même environnement, l'un interfère avec l'autre. Cette interférence ne modifie pas nécessairement la fréquence de la porteuse du signal cible, mais rend le signal source indiscernable du bruit radio ambiant pour le récepteur. En effet, un récepteur radio est conçu et paramétré pour démoduler des signaux à une fréquence porteuse bien précise. Si le signal qu'il reçoit est perturbé, il n'arrive plus à extraire correctement l'information et rend la communication difficile, voire impossible.

1.2. Schéma synoptique d'un brouilleur radio en fréquences (FM)

Nous tâcherons ici de créer un schéma synoptique fidèle au fonctionnement d'un brouilleur radio en fréquence (Frequency Jammer).



La communication entre l'émetteur et le récepteur est considérée comme fonctionnelle. Cette dernière est fixée pour cet exemple à 95 MHz pour une amplitude de 1V. Le schéma synoptique de notre brouilleur est assez simple puisque ce dernier ne se compose que de deux blocs : le premier qui a pour rôle de générer le signal de bruit à une amplitude donnée (ici 5V) et le deuxième qui permet de ne faire passer qu'une bande de fréquence donnée sur le médium. Pour rappel, ce médium est l'air.

Une fois que le brouilleur a généré son signal de brouillage à la fréquence voulue, le signal est envoyé sur le médium. Le signal radio légitime envoyé par l'émetteur est alors superposé au signal radio pirate. Du point de vue du récepteur qui est configuré pour ne récupérer qu'un certain type de signal à une fréquence donnée, ce dernier n'arrive plus à extraire l'information du médium. L'information transportée par le signal légitime est ainsi confondue dans le bruit ambiant imposé par le brouilleur. Nous détaillerons plus en détail le fonctionnement de l'émetteur du bruit ainsi que du filtre lorsque nous simulerons le fonctionnement du brouilleur avec GNU Radio.

La bande de fréquence que nous utiliserons sera de 88 MHz à 100 MHz, correspond à la bande VHF (Very High Frequency). Très utilisée pour la diffusion de stations de radio FM (fréquence modulée), elle permet par exemple la diffusion de musique.

1.3. Applications possibles et responsabilités légales

L'utilisation d'un brouilleur radio est soumis à une réglementation très stricte, empêchant par exemple de brouiller (volontairement ou non) des communications légitimes telles que les services d'urgence, les communications militaires, les systèmes de transport, etc. En France, l'utilisation de brouilleurs de signaux est illégale, comme le décrit l'article L33-3-1 du Code des postes et des communications électroniques. L'utilisation non autorisée de ces derniers peut entraîner des sanctions sévères, y compris des amendes et des peines de prison. Les seules dérogations concernent les besoins de l'ordre public, de la défense et de la sécurité nationale ou du service public de la justice (notamment dans les établissements pénitentiaires).

On peut citer quelques exemples d'impact de l'utilisation des brouilleurs dans une petite ville comme celle de Blagnac, en particulier dans le cadre de la présence de l'aéroport à proximité de l'IUT :

1. **Retards et congestion du trafic aérien** : Les perturbations des communications peuvent entraîner des retards dans les autorisations de décollage et d'atterrissement, ainsi que des congestions du trafic aérien.
2. **Confusion des instructions orales** : Les brouillages peuvent entraîner une mauvaise compréhension des instructions entre les pilotes et les contrôleurs de la circulation aérienne, augmentant le risque d'incidents.

L'usage de brouilleurs dans les zones militaires est très fréquent afin de perturber ou limiter la capacité de communication de l'ennemi et d'éviter les intrusions par le biais de drones par exemple.

1. **Déception électronique** : Les brouilleurs peuvent être utilisés dans le cadre de la guerre électronique pour induire l'adversaire en erreur. En créant des interférences sur certaines fréquences, les militaires peuvent essayer de tromper l'ennemi sur la position, les intentions ou les mouvements des forces amies.
2. **Contre-mesures électroniques** : Les brouilleurs peuvent être utilisés comme contre-mesures électroniques pour contrer les tentatives d'interception ou de brouillage ennemi. En adaptant rapidement les fréquences et les techniques de brouillage, les forces militaires peuvent maintenir leur avantage en matière de communication et de renseignement.

3. **Protection contre les drones** : Les brouilleurs peuvent être utilisés pour contrer les drones ennemis en perturbant les signaux de contrôle entre le drone et son opérateur. Cela peut aider à neutraliser ou à détourner des drones hostiles.

Voici comment fonctionne généralement le brouillage de drones :

- a. **Brouillage des signaux de contrôle** : Les drones sont généralement pilotés à distance à l'aide de signaux radio entre le drone et la station au sol (télécommande). Les brouilleurs peuvent perturber ces signaux de contrôle en émettant des interférences radioélectriques sur les fréquences utilisées par les drones. Cela peut rendre difficile, voire impossible, la communication entre le drone et son opérateur, le forçant ainsi à perdre le contrôle et à atterrir de manière contrôlée ou à retourner à sa base.
- b. **Brouillage des systèmes de navigation** : Certains drones utilisent des systèmes de navigation par satellite tels que le GPS pour déterminer leur position et suivre des itinéraires préprogrammés. Les brouilleurs peuvent également perturber ces signaux de navigation, induisant des erreurs dans la localisation du drone.
- c. **Détournement du signal** : Dans certains cas, plutôt que de simplement brouiller les signaux, les brouilleurs peuvent être utilisés pour détourner le contrôle du drone. En interceptant le signal de la télécommande du drone, les brouilleurs peuvent prendre le contrôle du drone et le faire voler selon les instructions de l'opérateur du brouilleur.

Enfin, l'utilisation de brouilleurs peut aussi être utile afin de brouiller la connexion Wi-Fi dans certains endroits tels que les centres pénitentiaires où l'accès est censé être entièrement révoqué aux détenus. Les brouilleurs de signaux cellulaires émettent des signaux perturbateurs sur les fréquences des réseaux de téléphonie mobile (GSM, 3G, 4G, etc.) à l'intérieur de la prison. De ce fait, les téléphones mobiles des détenus qui se trouvent dans la zone d'effet du brouilleur, ne peuvent pas se connecter aux réseaux cellulaires à proximité.

Cependant, l'utilisation de brouilleurs de signaux cellulaires dans les prisons est contre-productive, car elle peut également perturber les communications des gardiens, des personnels de sécurité et des services d'urgence dans la région, mettant ainsi en danger la sécurité publique.

En faisant l'étude des utilisations possibles d'un brouilleur FM, on se rend vite compte que ces derniers sont utilisés principalement à des fins d'attaques, souvent couplés avec des mouvements de forces armées ou des attaques cybercriminelles. Si nous avons l'opportunité de tester le fonctionnement d'un brouilleur avec le logiciel Adalm Pluto, nous tâcherons d'émettre notre signal de brouillage à de très faibles puissances pour ne pas être détecté.

2. GNU Radio : Frequency Jammer

L'objectif de la deuxième partie de ce rapport est d'aborder en détail le fonctionnement du flowchart GNU Radio que nous avons mis au point. Deux versions de ce dernier ont été produites : l'une permettant de comprendre le fonctionnement d'un brouilleur radio FM en passant en entrée un signal simple, et l'autre plus complexe, mais plus proche de la réalité, permettant de brouiller une entrée audio externe.

2.1. Généralités

GNU Radio est un logiciel de simulation radio libre et open source qui permet de simuler le fonctionnement de diverses applications AM et FM du monde des télécommunications. Ce logiciel conçu à des fins pédagogiques, de recherches et de développements de nouvelles applications nous permet de nous familiariser avec les concepts étudiés à l'IUT au cours des diverses ressources de ces deux premières années de BUT.

GNU Radio est un outil complet qui se distingue entre autres par sa large bibliothèque de blocs de traitements du signal permettant une modularité et flexibilité de l'outil. En utilisant des blocs de traitement préexistants, on facilite la conception et la réutilisation du code nous permettant d'aborder des sujets complets assez facilement. D'autre part, GNU Radio permet de prendre en charge des interfaces matérielles permettant de faire le lien entre le monde de la simulation et l'application réelle des flowcharts créé dans l'outil. C'est par exemple le cas de la carte HackRF One, similaire à l'Adalm Pluto, dont nous ferons bientôt l'acquisition. Cette carte permet de tester ou de pirater les fréquences radios comprises entre 1 mHz et 6 000 mHz. Il est possible de la manipuler à l'aide d'un SDR comme GNU Radio. On peut aussi citer la carte Adalm Pluto que nous utiliserons en dernière partie de cette SAE.

Bien que s'éloignant du sujet originel de cette SAE, un exemple d'application de GNU Radio sur du piratage radio dans le monde réel peut être retrouvé dans la conférence nommé "Dave Rowntree: Hacking the Radio Spectrum with GNU Radio", disponible sur YouTube en suivant l'URL suivante : <https://www.youtube.com/watch?v=hiNcjJEaqO8>.

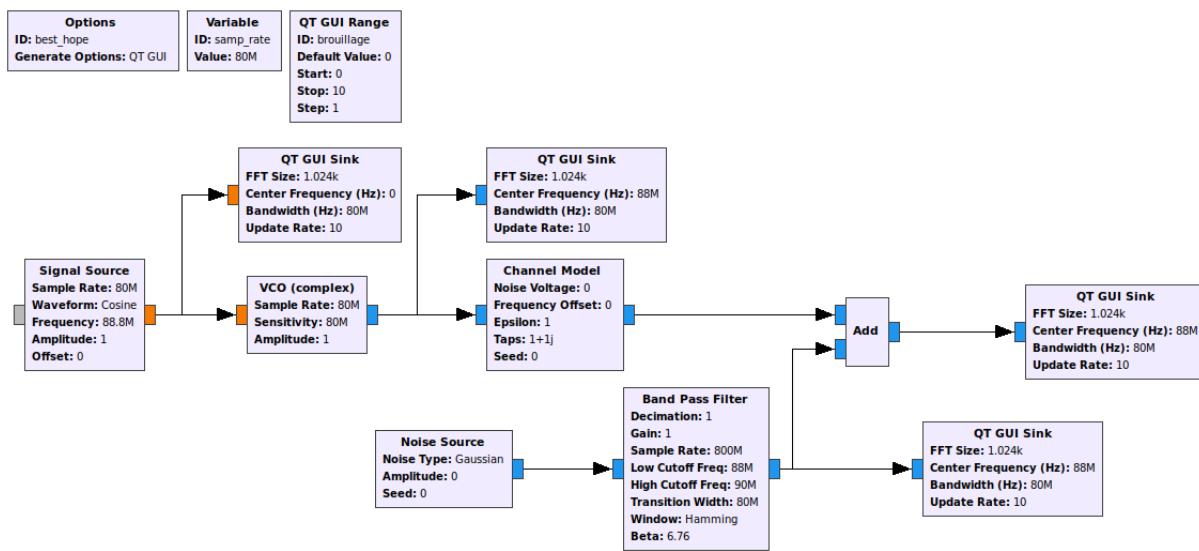
Nous détaillerons donc au cours des prochaines pages de ce rapport le fonctionnement de l'outil et les blocs que nous avons utilisés pour créer les deux types de brouilleur radios proposés.



2.2. Flowchart N°1 : montage simple

Le premier flowchart de brouilleur radio en fréquence que nous avons créé nous aura permis de comprendre le fonctionnement des différents blocs à utiliser dans GNU et aura permis de se familiariser avec leurs options respectives.

Le premier flowchart prenant en entrée un simple signal sinusoïdal modulé en fréquence par un VCO est alors le suivant :



L'objectif de ce dernier est de bien comprendre le fonctionnement du brouilleur que nous avons mis en place, avant de changer la source du signal par un autre plus difficile à interpréter sur les analyseurs de spectre.

Commençons par faire l'étude détaillée de chaque bloc utilisé :

- Généralités

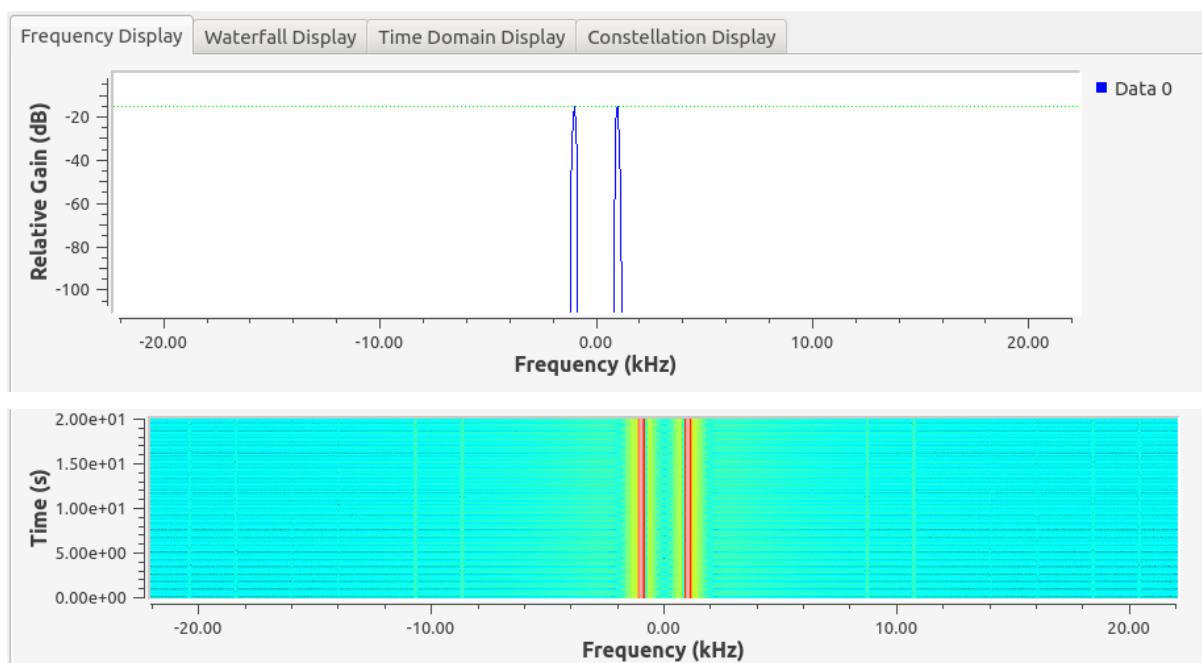
Variables : Le `sample_rate` est le nombre d'échantillons pris par seconde lors de la numérisation d'un signal analogique. On l'exprime en hertz (Hz). Par exemple, un `sample_rate` de 10 000 Hz signifie que 10 000 échantillons sont pris chaque seconde pour représenter le signal. Le choix du `sample_rate` est crucial, car il détermine la fidélité avec laquelle le signal analogique original est représenté dans le domaine numérique. Un `sample_rate` trop bas peut entraîner une perte d'information et une distorsion du signal, tandis qu'un `sample_rate` trop élevé peut nécessiter des ressources de traitement importantes et entraîner une surcharge du système.

- L'Émission d'un signal modulé en fréquence :

Bloc Signal Source : comme son nom l'indique, ce bloc a pour rôle de simuler l'émission d'un signal source. Il est possible de choisir d'émettre des signaux périodiques constants, sinusoïdaux, carrés, triangle ou en dents de scie. On peut alors définir sa fréquence, son amplitude, son offset ou encore son type (float, entier ou complex). Ici, nous choisissons pour l'exemple d'émettre un signal de fréquence 88,8 MHz, d'amplitude 1V et sans offset. Le type du signal est fixé à "Float" pour répondre aux besoins du type de signal en entrée du VCO.

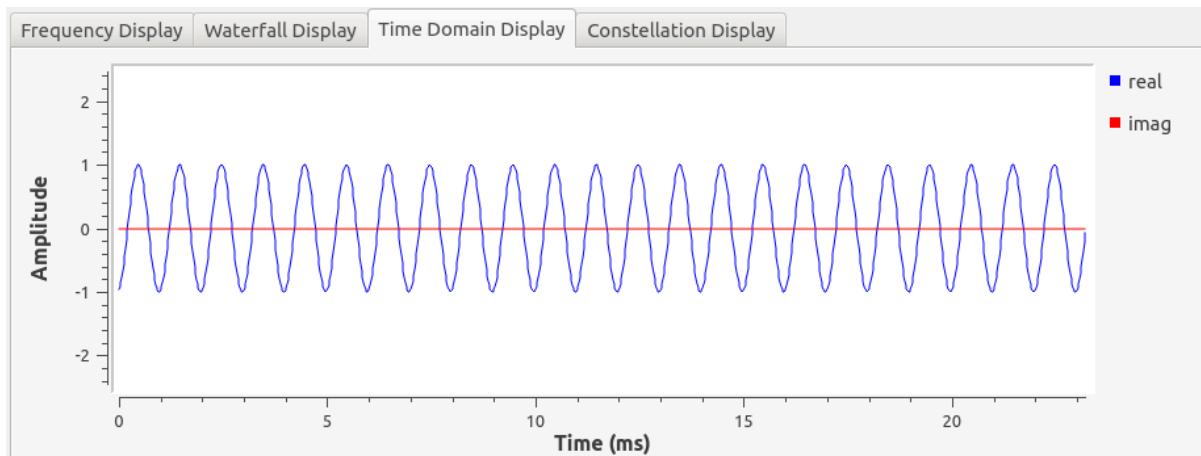
Bloc QT GUI Sink : ce bloc est utilisé à des fins de visualisation du signal qui est transmis au VCO. On donne l'exemple suivant pour un signal à 1 kHz, permettant une meilleure visualisation du signal. Ne nécessitant pas de configurations particulières, il permet l'affichage de la représentation spectrale du signal ainsi que sa représentation temporelle :

- Transformée de Fourier :



Il est important de noter que GNU Radio est un outil de simulation qui cherche à se rapprocher au maximum de la réalité mathématique des signaux qu'il gère plus que purement de l'aspect physique de ces derniers. La composante négative en fréquence sur la représentation spectrale du signal n'est pas à prendre en compte d'un point de vue physique, mais existe bel et bien d'un point de vue mathématique dans la transformée de Fourier du signal.

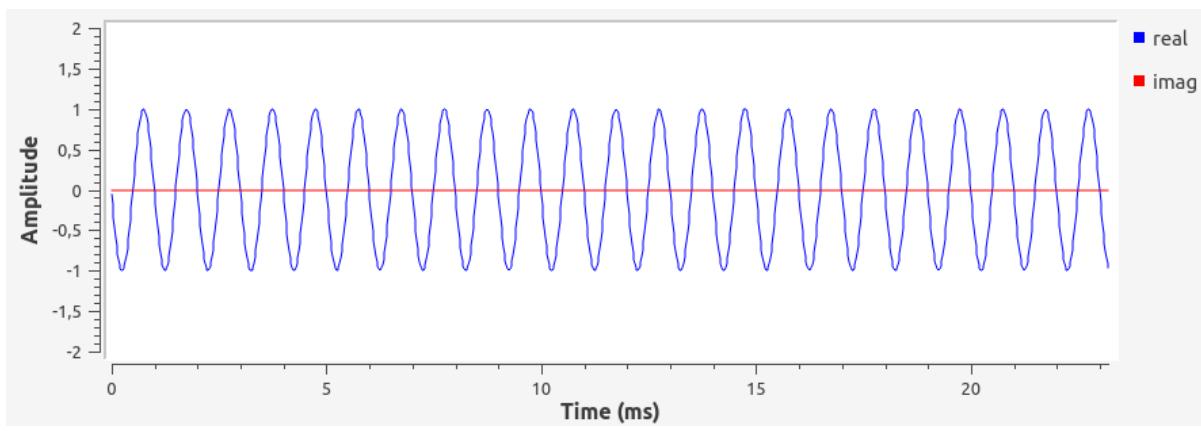
- Représentation temporelle :



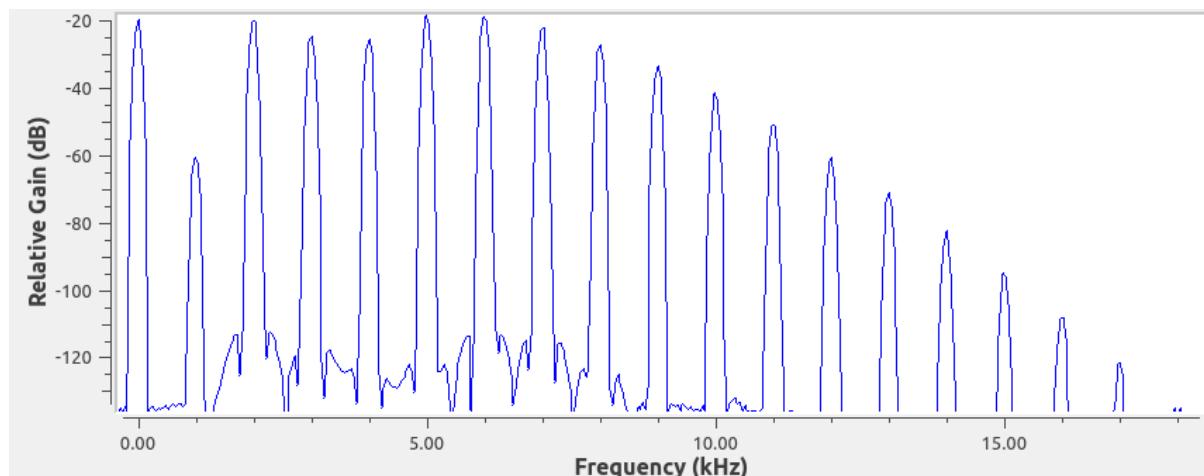
On rappelle ici que le bloc de signal source a été considéré en mode “Float”, donc la composante imaginaire du signal est nulle (ligne rouge sur la visualisation de la sinusoïde).

Bloc VCO (complex) : l’oscillateur commandé en tension (Voltage Controlled Oscillator) a pour rôle de coder en sortie un signal dont la fréquence est fonction de la tension d’entrée. Dans le cas de notre exemple, le signal qui est passé en entrée est un signal sinusoïdal dont son amplitude varie entre -1 V et 1 V. De cette façon, le signal en sortie du VCO sera fonction de l’amplitude à un instant T du signal. Nous utilisons le VCO de type (complex) car celui-ci nous permet de passer en entrée un signal de type “Float” et de récupérer en sortie un signal de type “Complex”. Un autre bloc VCO existe aussi, mais ne permet pas de gérer les signaux possédant une partie imaginaire.

Bloc QT GUI Frequency Sink : ce bloc de visualisation très semblable au bloc QT GUI Sink va nous permettre d’illustrer le fonctionnement du bloc VCO (complex). Pour la sinusoïde en entrée suivante :



On obtient la transcription en fréquence suivante :



- Simulation du médium de transmission :

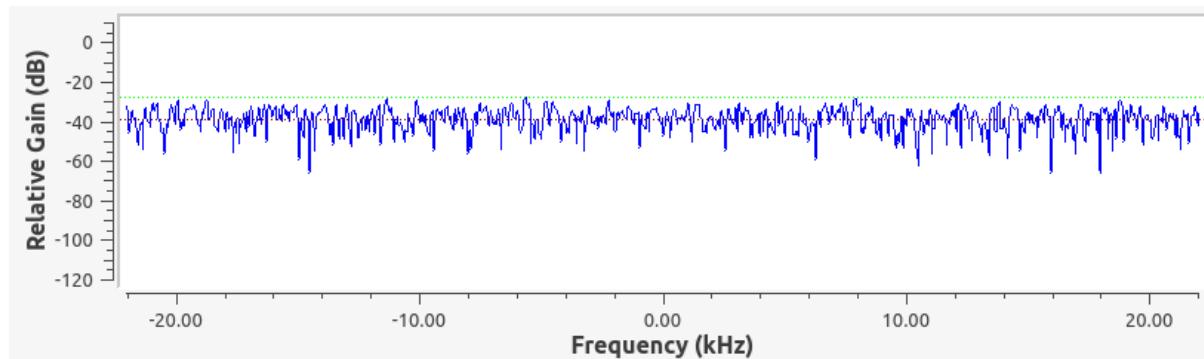
Bloc Channel Model : Nous ajoutons ce bloc non nécessaire au fonctionnement de notre brouilleur pour simuler le bruit qui peut être apporté au signal lors de son passage dans le médium (l'air). En augmentant la valeur de Noise Voltage, on peut faire varier l'intensité du bruit appliquée au médium, simulant par exemple de mauvaises conditions météorologiques.

- L'Émission d'un signal de brouillage :

C'est par l'ajout des blocs suivants que nous allons réussir à brouiller le signal. Pour remettre en perspective l'aspect réel de cet exercice, il est important de considérer le brouilleur comme un appareil pirate qui est ajouté dans l'enceinte de la portée radio partagée par l'émetteur et le récepteur du signal légitime. Son rôle est donc d'interférer entre les deux entités communicantes pour rendre l'information imperceptible au milieu d'un bruit ambiant.

Bloc Noise Source : ce bloc est assez similaire à un bloc démission d'un signal, si tenté que ce dernier émet un bruit sur toutes les fréquences de communication à une amplitude donnée. Il est possible de choisir entre différents types de bruit : gaussien, uniforme, laplacien ou par impulsion. Nous choisirons d'utiliser le type gaussien, car les valeurs du bruit sont centrées autour d'une moyenne avec une dispersion déterminée par l'écart-type. Il est particulièrement adapté à notre application, car possède une distribution uniforme sur l'ensemble de la bande passante fréquentielle. On pourra donc selon le paramétrage du filtre passe bas brouiller la fréquence voulue.

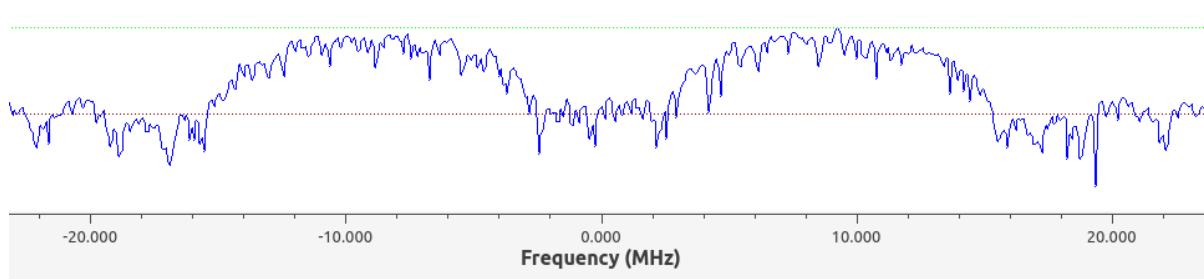
La représentation spectrale du bruit émis avant traitement en sortie du bloc “Noise Source” est la suivante :



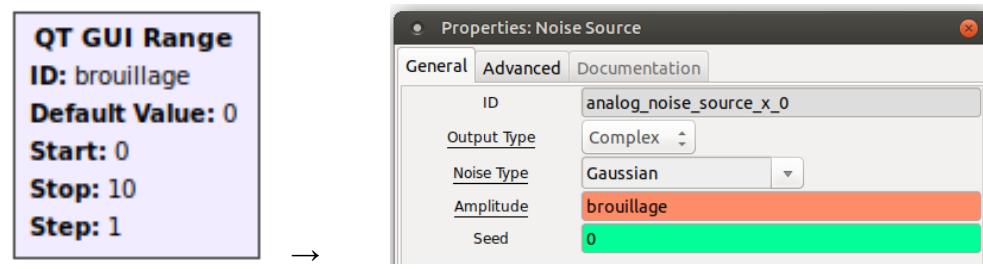
Bloc Band Pass Filter : le filtre passe bande est un filtre particulièrement intéressant dans notre cas puisque va nous permettre de concentrer le brouillage sur une plage de fréquence prédéfinie. En effet, ce filtre étant la concaténation d'un filtre passe bas et d'un filtre passe haut, on peut ajuster les fréquences de coupure de ces deux filtres pour ajuster notre bande de fréquence passante. C'est ce type de filtre qui est utilisé dans les vieilles radios FM, filtre sur lequel on peut ajuster avec une molette pour ne récupérer que la fréquence spécifique d'une chaîne de musique, par exemple NRJ ou SudRadio.

Pour paramétrier ce filtre, il suffit de définir les champs de gain, de sample rate, transmission width et les extremums de la plage de fréquence à laisser passer. Le sample rate est le nombre d'échantillons que prend le bloc pour échantillonner le signal. Avec un sample rate d'entrée de 80 MHz, il est nécessaire d'en prendre un bien plus élevé (au moins huit fois plus élevé) pour le filtre. Le sample rate à appliquer au filtre est donc de 800M. En faisant ainsi, on s'assure que le filtre est précis. On relève deux problèmes avec ce bloc : nécessitant un sample rate élevé, le flowchart nécessite une grande capacité hardware système pour fonctionner. On note que ce sample rate trop élevé a déjà fait planter plusieurs fois note VM. Ensuite, le bloc d'affichage n'arrive pas à suivre pour des fréquences trop élevée, ce qui produit en sortie un affichage correct, mais avec une échelle décalée.

Ce bloc couplé au bloc noise source a pour allure la suivante :



Bloc QT GUI Range : ce bloc va nous permettre de créer une variable que l'on pourra modifier au cours de l'exécution du programme. On appelle ici notre variable "brouillage". Ainsi, on peut modifier l'amplitude de notre signal de brouillage avec le curseur suivant :

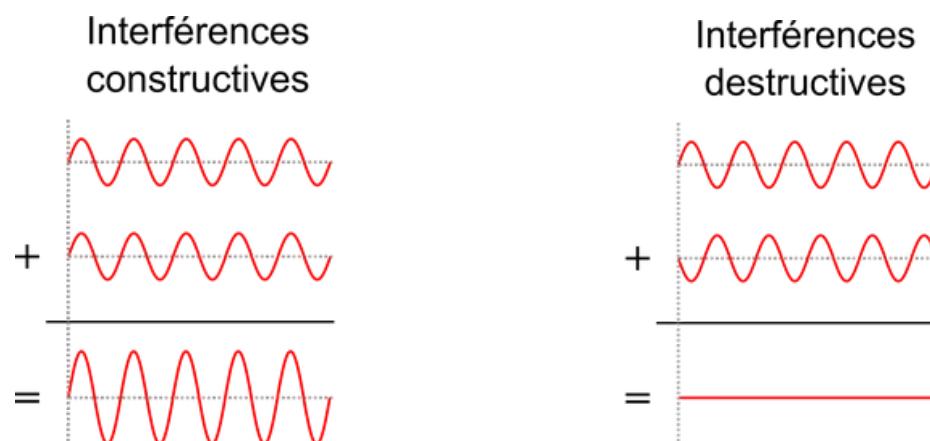


brouillage → 5,0

Bloc Add : ce bloc est le dernier que nous utiliserons dans ce flowchart. Il sert à simuler l'émission du signal de brouillage sur le médium de communication en ajoutant le signal original légitime et le signal brouilleur. En sortie de ce bloc, on se place au niveau du récepteur du signal. Lorsque l'on ajoute deux signaux, il faut considérer les cas suivants :

- Si les deux sinusoïdes ont la même fréquence et des phases similaires, l'addition des signaux peut augmenter l'amplitude du signal résultant. Cela est dû à la sommation constructive des ondes.
- Si les deux sinusoïdes ont la même fréquence, mais des phases opposées, elles peuvent s'annuler lors de l'addition, entraînant une atténuation du signal résultant. Cela est dû à la sommation destructive des ondes. Il pourrait être très intéressant d'utiliser ce phénomène dans le cas de notre brouilleur. En effet, plutôt que de chercher à rendre l'information imperceptible au milieu du bruit radio, il pourrait être intéressant d'annuler l'information en émettant un signal à la même fréquence, mais avec une phase opposée.

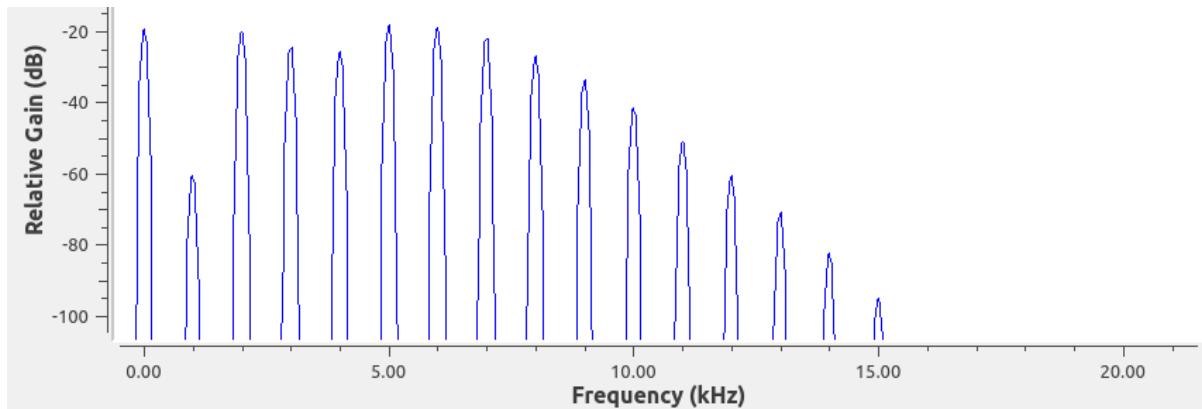
Le schéma suivant résume bien les différents cas possibles lors de l'ajout de deux signaux sur un medium :



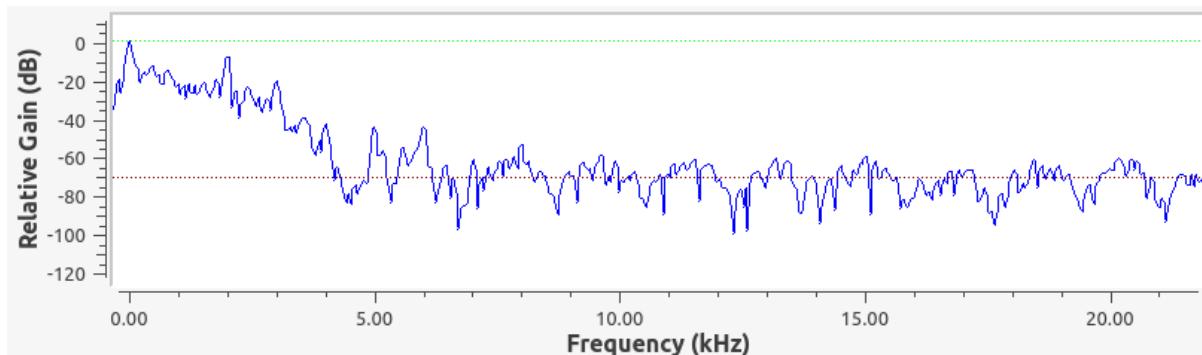
- Réception du signal sur le médium : signal clair ou signal brouillé ?

En sortie du bloc Add, on rajoute un second bloc “QT GUI Frequency Sink” afin de regarder l'état du signal sur le médium et de valider le fonctionnement de notre brouilleur. Pour ce faire, reprenons le cheminement du signal sur le médium :

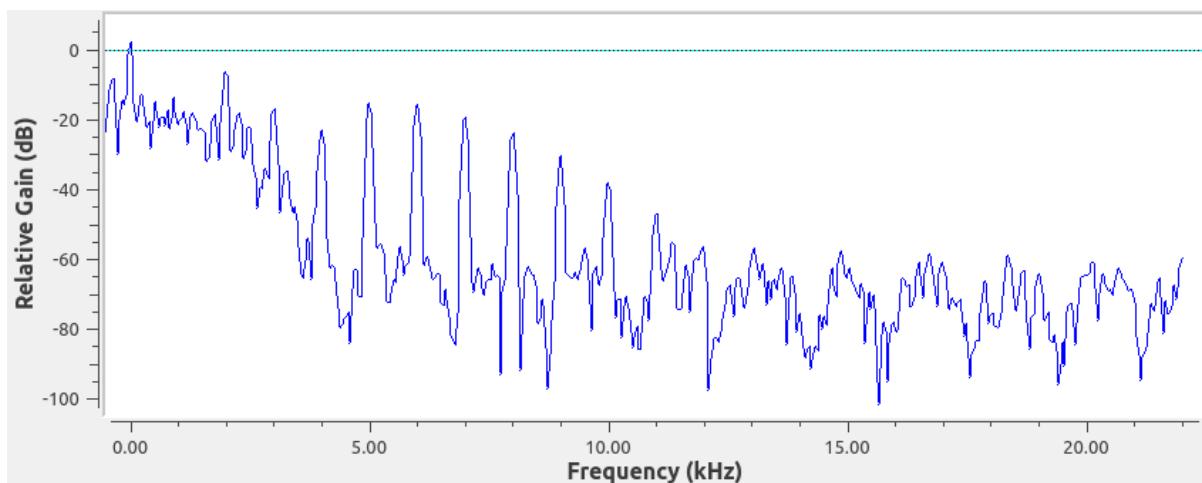
- Signal clair émis sur le médium en sortie du bloc émetteur :



- Émission d'un signal de bruit sur la même plage de fréquence que le signal légitime :



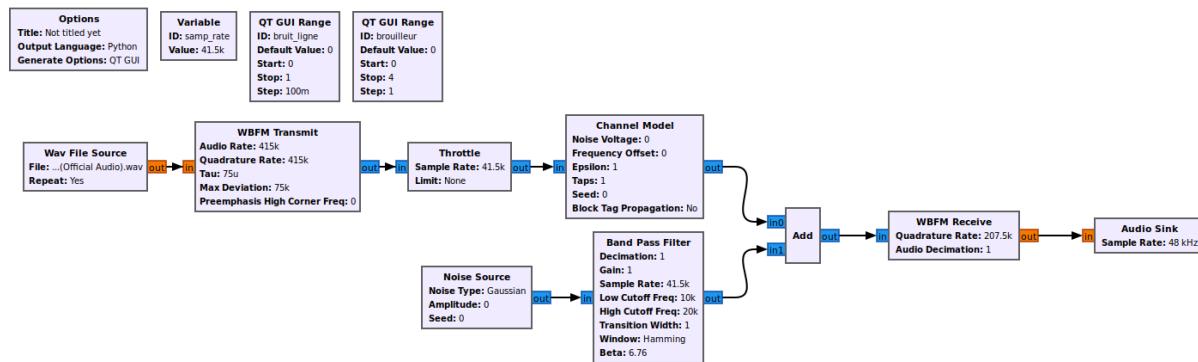
- Signal brouillé récupéré en sortie au niveau du récepteur :



On remarque que le signal de donnée est confondu dans le signal de bruit. On considère donc que notre signal est brouillé. Plus on augmente la puissance du brouilleur avec la variable “brouillage”, plus le signal légitime sera confondu avec celui du brouilleur.

2.3. Flowchart N°2 : montage d'application

Maintenant que nous avons compris le fonctionnement d'un brouilleur et que son fonctionnement est validé pour un signal d'entrée simple, on peut chercher à brouiller un signal plus réaliste : une communication vocale via radio. Pour ce faire, nous réutiliserons en partie le montage GNURadio précédent, tout en rajoutant les blocs nécessaires à l'interprétation du flux audio par le logiciel. Le flowchart est alors le suivant :



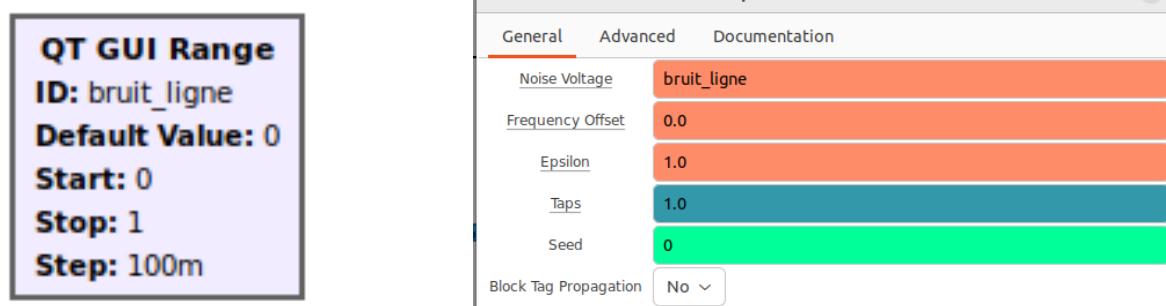
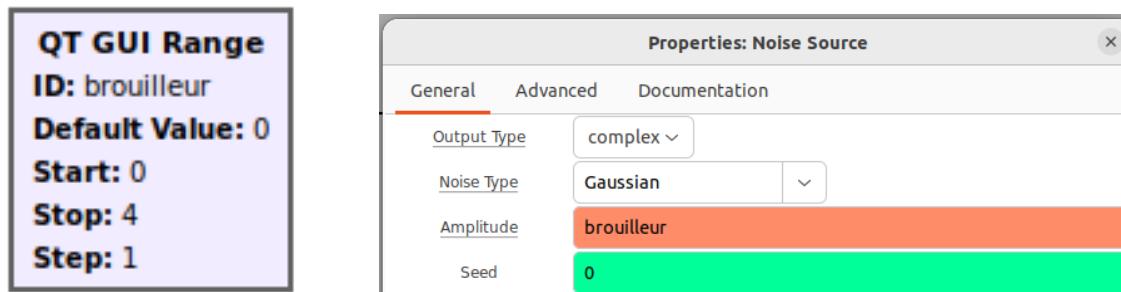
Bloc Wav File Source : ce bloc a pour rôle de lire les fichiers audio au format WAV en tant que source pour les données d'entrée dans GNURadio, fournissant ainsi une manière de traiter des signaux audio enregistrés préalablement. On choisira de jouer à l'aide de ce bloc un fichier d'entrée simulant une communication militaire, pour coller au maximum aux applications réelles d'un jammer en fréquence.

Bloc WBFM Transmit : Ce bloc fonctionne en prenant un signal audio en entrée, donc ici notre fichier wav. Il utilise la modulation de fréquence (FM) à large bande pour transformer ce signal audio en un signal radiofréquence. La modulation de fréquence implique que la fréquence de la porteuse varie proportionnellement au signal audio. On peut donc y voir un fonctionnement assez similaire qu'avec le VCO utilisé précédemment. Ainsi, les variations du signal audio sont représentées par des variations correspondantes dans la fréquence de la porteuse.

Bloc WBFM Receive : Ce bloc opère du côté récepteur de la communication radio, et est la composante inverse du bloc WBFM Transmit. Il prend un signal radiofréquence modulé en fréquence (FM) en entrée, tel que celui généré par le bloc WBFM Transmit. Le bloc WBFM Receive effectue la démodulation, un processus inverse de la modulation, afin d'extraire le signal audio d'origine. La démodulation de fréquence inverse les variations de fréquence introduites lors de la modulation, récupérant ainsi le signal audio de base. Une fois démodulé, le signal audio peut être envoyé au bloc Audio Sink qui s'occupera de rejouer le signal reçu. Ce processus permet la transmission et la réception d'informations audio sur des canaux radio à l'aide de la modulation de fréquence.

Bloc Audio Sink : Ce bloc sert de destination pour les données audio dans notre flowchart GNURadio, permettant de lire le fichier audio en se plaçant du point de vue du récepteur de l'information.

Afin de pouvoir jouer sur le flowchart une fois ce dernier lancé, nous rajoutons deux variables “Slider”. Ces derniers, nous permettront de faire évoluer les valeurs de bruit sur le médium pour l'un et ajuster la puissance du jammer pour l'autre. Ces deux blocs sont les suivants :



Une fois le flowchart lancé, on peut alors avoir accès à deux sliders qui nous permettent de jouer sur ces deux valeurs.

Le slider “medium_noise” va permettre en parallèle du bloc “Channel Model” de simuler le bruitage naturel qu'il peut y avoir entre l'émetteur et le récepteur sur le médium de communication de l'air.

Le slider “jammer_noise” permet de jouer sur l'amplitude du signal de bruit qui est émis sur le médium. On peut donc jouer sur la puissance de brouillage émise.

Les deux sliders ‘bruit_ligne’ et ‘brouilleur’ sont les suivants :



3. Frequency Jammer ~ Adalm Pluto

3.1. Configuration hardware

Après de nombreuses heures de recherches et de tests, nous ne sommes pas parvenus à utiliser l'Adalm Pluto pour brouiller la communication radio entre une station radio FM et une voiture. Nous pensons que cet échec est dû au fait que l'Adalm Pluto ne possède pas la puissance nécessaire pour interférer avec la connectivité radio forte qu'une voiture peut avoir avec une station radio à proximité.

Cependant, et pour utiliser cet outil intéressant qu'est l'Adalm Pluto, nous allons chercher à brouiller une connexion cellulaire 2,4 Wifi entre deux appareils. Pour ce faire, nous connecterons le téléphone de Pierre avec le point d'accès Wifi du téléphone de Daniel.

Pour vérifier si le Adalm Pluto est joignable, on peut effectuer un simple ping :

```
pierre@Pierre-Desktop:~$ ping 192.168.2.1 -c 1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.331 ms

--- 192.168.2.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.331/0.331/0.331/0.000 ms
pierre@Pierre-Desktop:~$
```

On peut alors accéder au système en utilisant le couple user / mdp suivant :

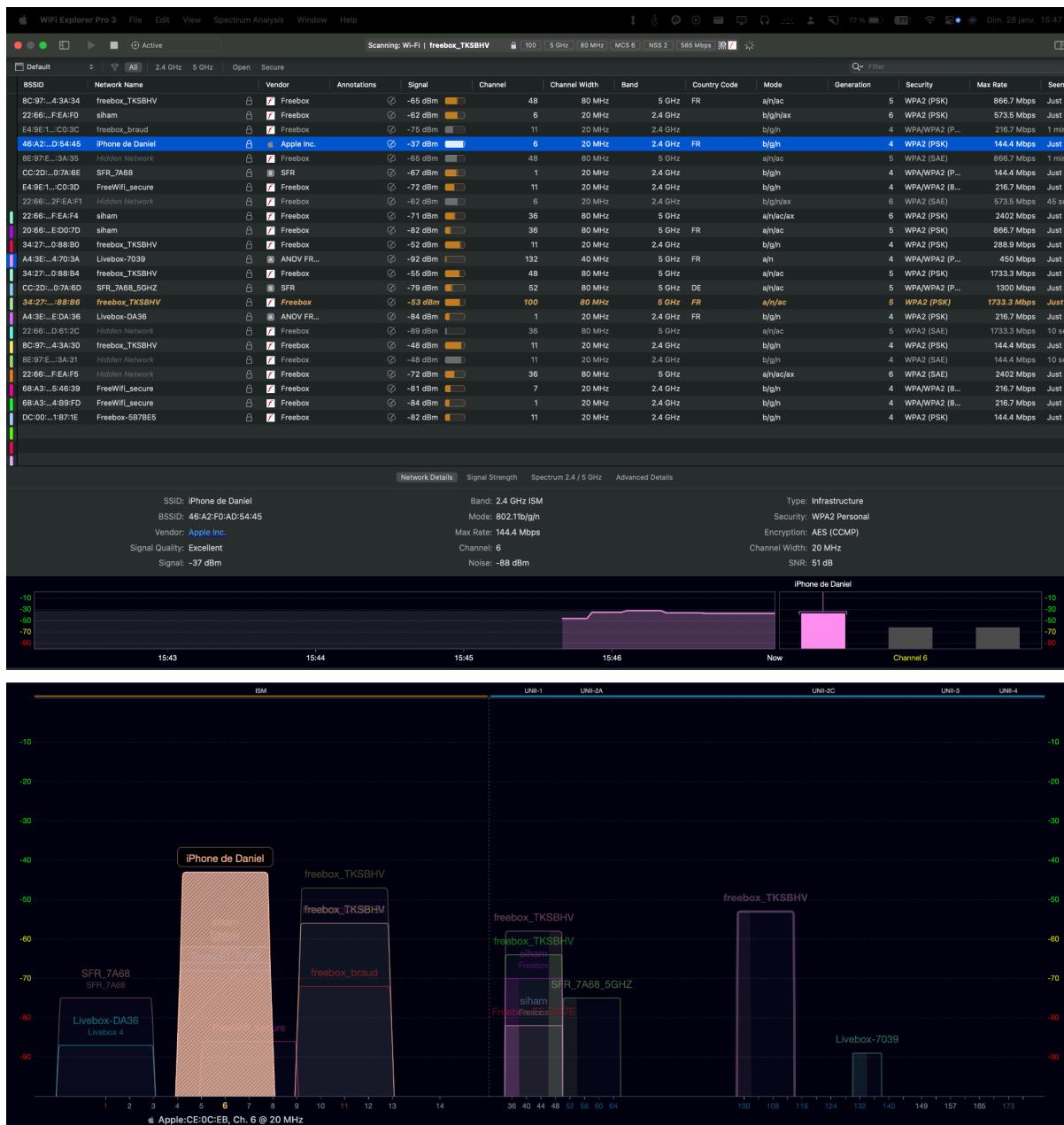
- Login : root
 - Password : analog

Pour atteindre les fréquences que l'on cherche à brouiller, il est nécessaire de "hacker" le Adalm. Nous n'avons pas eu besoin de le faire, car ce denier était déjà "jailbreaké" lorsque nous l'avons récupéré. Pour vérifier que le Adalm est prêt à être utilisé, il faut que les informations systèmes soient identiques aux suivantes :

```
# fw_printenv | grep "attr_name=" # fw_printenv | grep "attr_value="
attr_name=compatible attr_value=ad9364
```

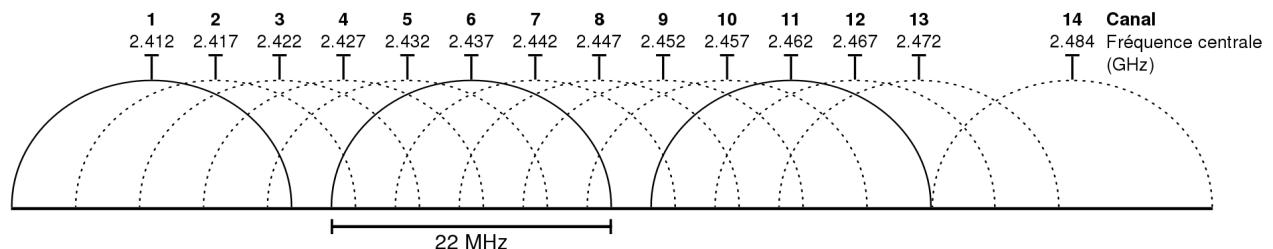
3.2. Brouillage d'une connexion à une Access Point Wi-Fi - 2.437 GHz

Pour ce test, nous avons décidé de brouiller un Wi-Fi créé par un point d'accès mobile. Pour ce faire, nous avons activé le partage de connexion sur un téléphone mobile puis nous avons scanné les réseaux wifi à proximité afin de récupérer le canal utilisé par le point d'accès. On utilise le logiciel Wifi Explorer Pro 3 (Logiciel Mac OS Payant, mais piratable) dans le but de scanner les réseaux à proximité et d'obtenir une multitude d'informations sur ces réseaux (SSID, FAI, atténuation du signal en dBm, canal utilisé, la fréquence du wifi ou encore le débit maximum sur les réseaux).



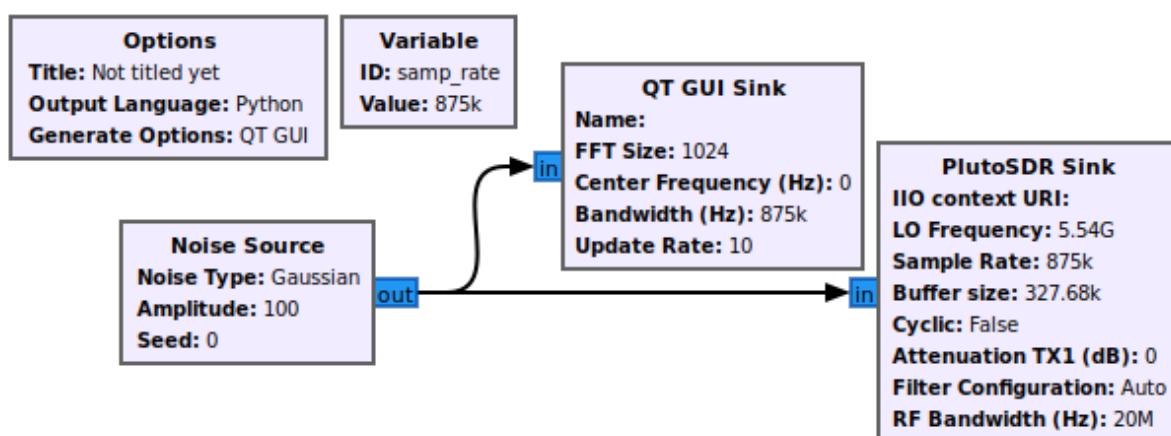
On observe ici que le réseau iPhone de Daniel est entre les fréquences 4 et 8, mais le pic est situé sur le canal 6. En effet, les canaux 4,5,7 et 8 sont ceux qui présentent le plus d'atténuation sur la bande de fréquence.

On note les différents canaux de fréquences suivantes :



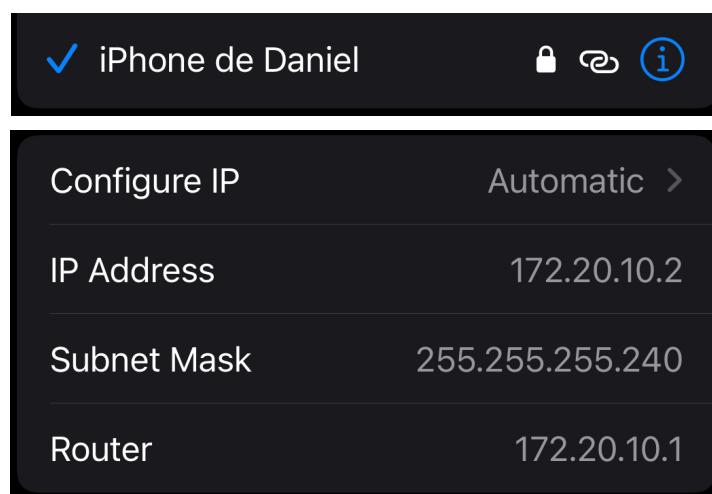
De ce fait, nous allons brouiller la fréquence associée au canal 6 qui est la fréquence centrale sur la plage de fréquence.

Le flowchart que nous avons utilisé est le suivant :

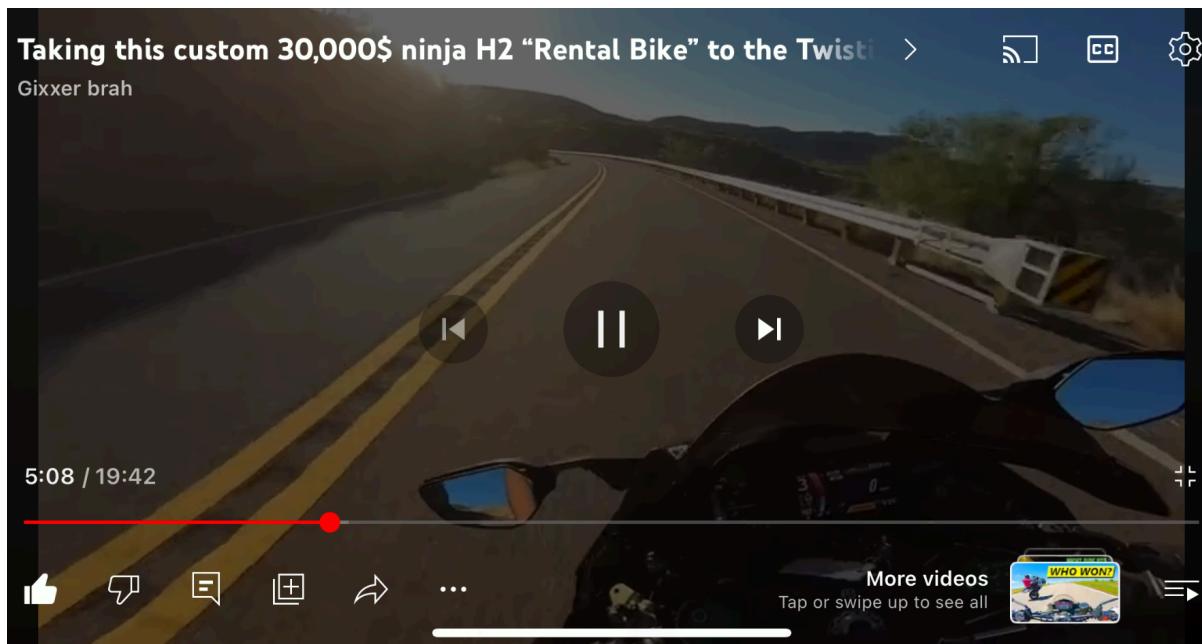


Ce dernier est assez simplifié. En effet, quand notre brouilleur sur les différents flowchart se composait d'un bloc "Noise Source" et d'un bloc "Band Pass Filter", ce dernier bloc ne sera pas utilisé, car le bloc "PlutoSDR Sink" ne peut émettre que sur une fréquence précise. Comme explicité plus haut, la fréquence est fixée à 2.437 GHz après analyse du partage de connexion. L'objectif est donc ici de brouiller la communication entre le téléphone de Pierre et le partage de connexion instancié par Daniel.

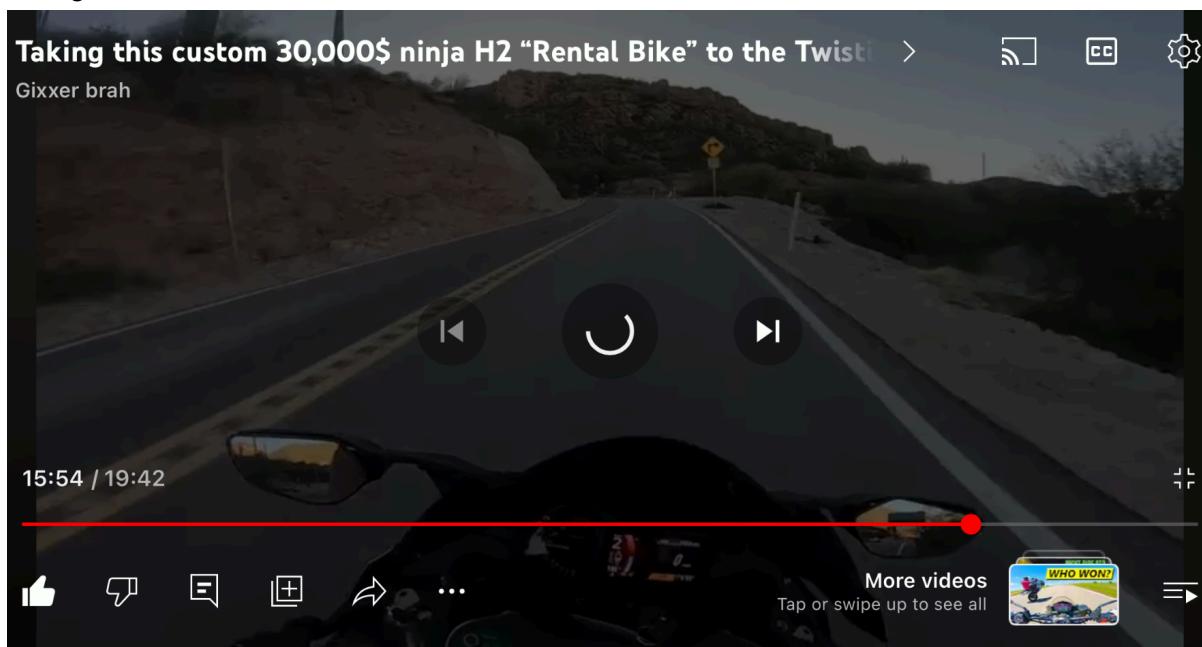
Les paramètres de la connectivité sur le téléphone client sont les suivants :



Lorsque le téléphone de Pierre est bien connecté à l'access point de Daniel et que le brouilleur est désactivé, on peut regarder une vidéo YouTube :



Mais dès lors que le brouilleur est activé, la connectivité est perdue et il devient impossible de regarder notre vidéo.



Notre brouilleur est donc fonctionnel ! On note que tous les réseaux WiFi à proximité appartenant au canal 6 sont aussi brouillé. Il faut donc éviter de pratiquer ce test sur une trop longue durée, avant par exemple que les voisins ne s'aperçoivent du dysfonctionnement de leur Wi-Fi. Une vidéo en live de notre test est disponible sur le lien suivant : <https://youtu.be/irUiQXL5fBM>

Conclusion

En conclusion, cette SAE nous aura permis d'appréhender les notions fondamentales des transmissions modulés en fréquences entre un émetteur et un récepteur, au travers de l'exercice du brouillage de ces communications.

Après avoir abordé le fonctionnement théorique d'un brouilleur en fréquence, nous avons mis en place plusieurs Flowcharts GNU Radio : le premier prenant en entrée un signal sinusoïdal simple et le second permettant de brouiller une communication audio. Finalement, nous avons pu mettre en pratique les notions acquises en utilisant un Adalm Pluto pour brouiller la communication Wi-Fi d'un Accès Point à proximité. La manipulation de GNU Radio nous aura permis de réutiliser les compétences acquises en TP et d'approfondir la compréhension du fonctionnement de certains blocs, en particulier ceux destinés à la modulation du signal en fréquence (VCO et WBFM).

Bien que le cahier des charges de cette SAE nous paraît respecté, nous regrettons d'avoir été limités par les performances de nos VMs et PCs. Nous avons en effet passé de nombreuses heures à observer les Flowchart GNU planter, entre autres lors de l'utilisation d'un sample_rate trop élevé. Pour pouvoir fournir des tests de qualités et valider le fonctionnement de nos FlowChart, il aura été nécessaire de dédier une machine entière à GNU Radio. Ceci explique la différence de version qui a été utilisé entre le premiers montage et les deux suivants. La version 3.10 de GNU Radio nous a paru plus stable que la 3.7. On note aussi que les blocs utilisés sur la version 3.10 sont aussi disponibles sur la version 3.7.

Finalement, il a été très agréable de pouvoir tester notre montage dans des conditions réelles avec l'Adalm Pluto. En effet, nous avons dans un premier temps cherché à brouiller la communication radio entre une voiture et une station de musique FM à proximité. Nous nous sommes alors vite rendu compte que le brouilleur ne possédait pas la puissance nécessaire pour noyer le signal source dans du bruit. Comme solution secondaire et pour proposer un test en position réelle, nous avons choisi de brouiller un access point Wifi. Bien que travaillant à des fréquences bien plus élevées (Ordre du Gigahertz plutôt que du Mégahertz), le brouillage a pu avoir lieu, car la puissance délivrée par le téléphone de Daniel était raisonnable en comparaison avec celle délivrée par l'Adalm Pluto pour le brouillage. Pour rappel, la vidéo de notre test est disponible sur l'URL suivante : <https://youtu.be/irUiQXL5fBM>

Nous tenons par ailleurs à remercier M. Alain Roux pour sa pédagogie et pour son aide dans les moments fastidieux de troubleshooting des différents flowcharts. De plus, le prêt de l'Adam Pluto nous aura permis d'apporter une dimension pratique à ce projet qui a fortement été apprécié par les deux membres du groupe (la théorie c'est bien, la pratique c'est encore mieux !).

Annexes - Sources

- Adalm Pluto

https://community.element14.com/products/roadtest/rv/roadtest_reviews/1698/beginners_guide_to_adalm-pluto

- Logiciel analyseur wifi MacOS

<https://apps.apple.com/fr/app/wifi-explorer-pro-3/id1587083834>

- Comment utiliser un analyseur wifi (tuto android)

<https://www.youtube.com/watch?v=83fx2nmrfhw>

- Autres sources :

<http://www.hb9afo.ch/articles/pluto/default.htm>

<https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html#eb-overview>

https://wiki.analog.com/university/tools/pluto/users/customizing#customizing_the_pluto_configuration

<https://www.youtube.com/watch?v=Yx3RPOtv7x8&list=PL0fsYX5KdLrWcKdrFSL3ZKM65ktJc6Htr>