Reverse engineering de télécommandes radio

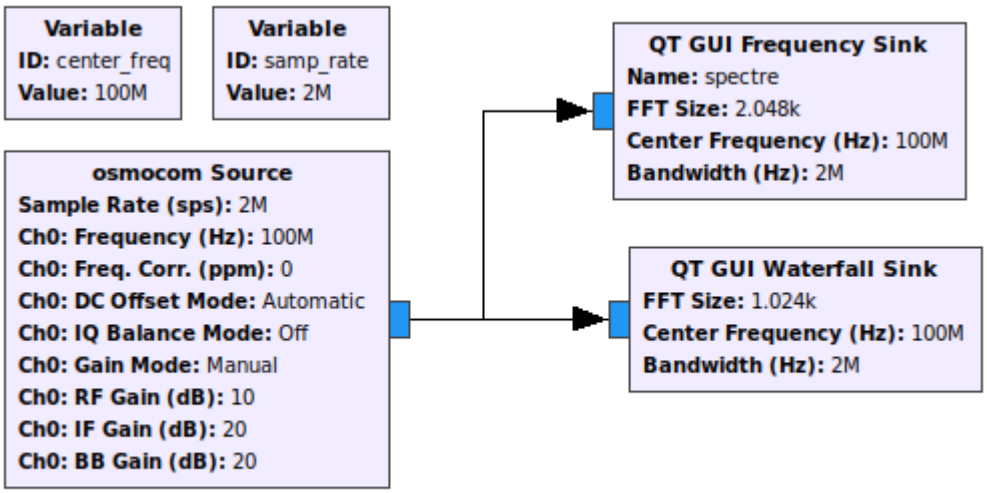
Introduction

Les télécommandes de portails, sonnettes sans fils, capteurs de température sans fils, etc, fonctionnement généralement dans les bandes ISM 433 ou 868 MHz.
Dans ce tp nous allons étudier le fonctionnement (fréquence, modulation, protocole) de deux carillon sans fils. Ces objets très basiques n'offrent aucune sécurité. Il est très facile de reproduire le signal de l'émetteur et ainsi faire sonner le carillon sans disposer de la télécommande originale.

Objet n° 1 : carillon sans fil EXTEL LOOBS
Objet n°2 : carillon sans fil HONEYWELL SERIES 3 (Honeywell ActivLink®)

1/ Mise en évidence de la fréquence d'émission et du type de modulation

Rechercher la fréquence centrale et la bande passante utilisée par les deux objets :
- avec l'analyseur de spectre (utilisez la fonction "Max Hold" car l'émission n'est pas permanente).
- avec le HackRF ou une clé RTL-SDR et le programme GQRX.
- avec le HackRF et un programme gnuradio :



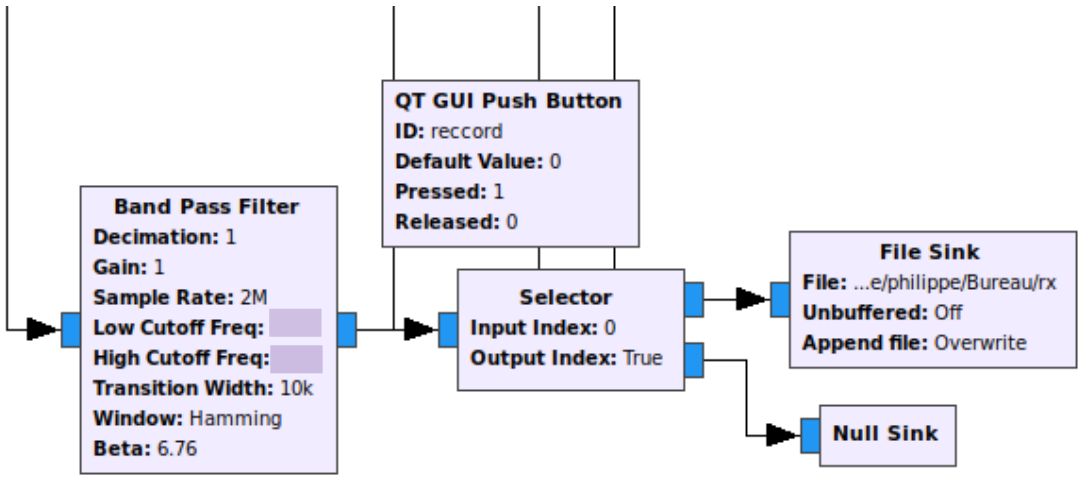
- Faire des images des spectres et des warterfall obtenus.
- Conjecturer le type de modulation utilisé par chaque objet.

2/ Replay attack

L'attaque par rejeu consiste simplement à enregistrer le signal de la télécommande et à ré-émettre un signal identique. Tout les objets qui émettent toujours le même code sont vulnérable à ce type d'attaque.

2.1/ Enregistrement du signal

- Ajouter à votre programme précédent un filtre passe bande centré sur la fréquence d'émission et de bande passante légèrement supérieure à la bande utilisée.
Vérifier avec le waterfall et la vue spectrale que le signal en sortie du filtre est correct.

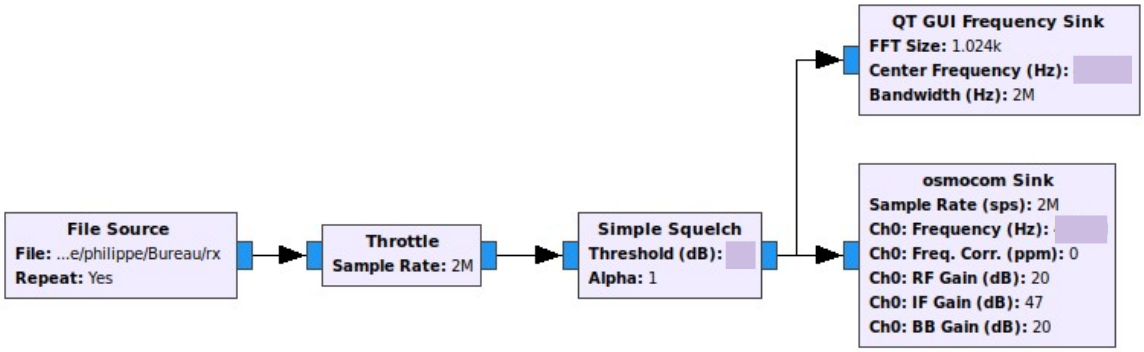


- Ajouter l'enregistrement dans un fichier :

Le fichier produit par l'enregistrement (File Sink) est rapidement volumineux (2M samples par seconde !). On va donc enregistrer uniquement lorsqu'on appuie sur un bouton (QT GUI PushButton). Le reste du temps le calcul est envoyé à la poubelle (Null Sink). Pour qu'un nouvel appui recommence bien un nouvel enregistrement et écrase le précédent, on utilise le mode d'enregistrement "Overwrite".

2.2/ Rejeu du signal

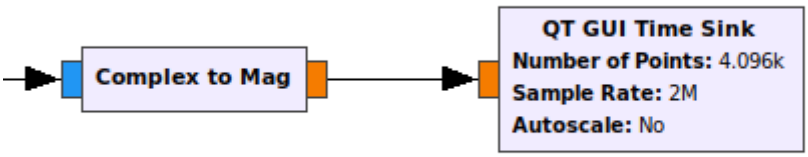
Il suffit de relire le fichier précédent et de l'envoyer sur le hackRF.



3./ Démodulation du signal

3.1/ Démodulation ASK (AM)

Pour démoduler l'ASK, il suffit de prendre le module du signal complexe (I+jQ).



Après la démodulation, il n'est plus nécessaire de garder une fréquence d'échantillonnage élevée. On aura avantage à diminuer la fréquence d'échantillonnage avec un "Rationale Resampler" en respectant le critère de Shanon par rapport au signal modulant.
Sur l'oscilloscope (QT GUI Time Sink) régler la durée de visualisation (X Max) et le déclenchement (trigger normal, level), pour capturer une trame complète.
Comment est encodée l'information ?

3.2/ Démodulation FSK (FM)

Pour démoduler le FSK et donc démoduler la fréquence, il suffit de prendre l'argument du produit du signal complexe par le même signal décalé d'une période d'échantillonnage. En effet le signal complexe I+jQ à la forme générale :

Reverse engineering de télécommandes radio

$$x(t)=A(t).e^{(j\,\omega t+\phi_0)}=A(t).e^{(j\,2\pi f\,t+\phi_0)}$$

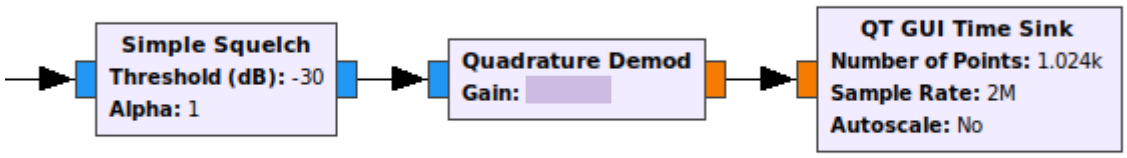
En FSK, l'amplitude reçue est maintenue constante par un très fort gain et on s'intéresse à retrouver la fréquence f émise à chaque instant.

Le signal échantillonné à la fréquence fs peut alors s'exprimer :

$$x(n)=A.e^{(2\pi j(f.\frac{n}{f_s})+\phi_0)} \qquad t=n.T_s=\frac{n}{f_s}$$

- Montrer que l'argument du produit $x(n).\overline{x((n-1))}$ est proportionnel à la fréquence et donner le facteur de proportionnalité (gain du démodulateur).

Le bloc démodulateur en quadrature réalise cette démodulation :



Il est précédé d'un squelch pour éviter de démoduler le bruit.

près la démodulation, il n'est plus nécessaire de garder une fréquence d'échantillonnage élevée. On aura avantage à diminuer la fréquence d'échantillonnage avec un "Rationale Resampler" en respectant le critère de Shanon par rapport au signal modulant.

Ajuster le gain en fonction de la déviation de fréquence que vous avez estimé.