****

**I**nstitut **S**upérieur d’**I**nformatique

**M**odélisation et de leurs **A**pplications

1, Rue de la Chebarde

TSA 60125

CS 60026

63178 Aubière Cedex

France

*Rapport de Projet*

*3ème année d’élève ingénieur*

*Filière 5 – Réseaux et Sécurité Informatique*

2015/2016

Création d’une radio pirate à l’aide de la radio logicielle



Présenté par : HOANG Jimmy

JOUGLA Benoit

Tuteur de projet : TILMANT Christophe

Enseignant Référent : CHEMINAT Miche

Remerciments

Table Figure et Illustrations

Résumé

Abstract

Table des matières

Glossaire

Introduction

**Réalisation d'une application radio logicielle**

**Qu'es ce que la radio logicielle ?**

La radio classique est un assemblage complexe de composant électronique dont le but est de traiter un signal, aussi bien à la réception qu'à l'émission, afin de transmettre et de recevoir des informations. Le système radio est spécifique à un signal.

Une radio logicielle, au contraire, fonctionne de façon numérique à l'aide d'un processeur classique d'ordinateur. Un convertisseur analogique-numérique, lié à une antenne, permet de recevoir ou d'émettre sur une large bande de fréquences. Les signaux reçues seront ensuite traiter selon le type d'application. Il est donc possible d'utiliser le même équipement pour traiter une multitude de signaux, sous différentes formes et fréquences, en ne changeant que la partie logicielle.

La radio logicielle est beaucoup plus adaptable que la radio classique.

**Quelques exemples d'application :**

Les applications sont nombreuses et variées. Il est possible à l'aide d'un antenne adaptée de récupérer des informations de satellites, d'avions, de bateaux, … Il est possible de récupérer les signaux de n'importe quelle application qui émet des ondes.

Exemple :

Récupérer les messages envoyés par les smartphones, messages envoyés par les services publiques comme la police, les pompiers, informations des avions, ...

Pour émettre des ondes, cela est plus compliqué car les ondes sont protégées et réglementées. Il n'est pas possible de faire tout ce qu'on veut sous peine de sanction. Les fréquences radioélectriques appartiennent au domaine public de l'Etat. L'ANFR, l'Agence Nationale des Fréquences, gère et contrôle l'utilisation de ces fréquences.

Exemple :

Contrôle d'un drone avec un PC via une interface radio, ouvrir fermer une porte de garage, …

**Gnu radio :**

Afin de réaliser des applications de radio logicielle, nous avons utilisé une suite logicielle dédiée à leurs implémentations, Gnu Radio. L'utilisation du logiciel s'articule autour de blocs qu'il suffit d'interconnecter les uns aux autres. Les blocs comprennent des sources (récepteur radio, fichier, …), des blocs de traitements de signal, de l'affichage graphique, ainsi que des blocs de sorties (audio, graphique, …).

Pour réaliser une chaîne de traitement du signal, il est possible de le réaliser en le codant dans un des nombreux langages pris en charge par le logiciel, c++, python, … ou en utilisant une interface graphique, Gnu Radio Companion, qui permet d'assembler les modules graphiquement.

**HackRF One :**

Le HackRF One est un émetteur-récepteur pour la radio logicielle. Il couvre avec les antennes adaptées les fréquences de 1MHz à 6GHz.

**Problématique :** L'objectif de ce projet est de développer une application afin de montrer les failles de sécurités liées aux radios fréquences.

**Radio "pirate" :**

Dans le cadre de ce projet, nous avons décider de développer une radio "pirate". L'application permet de diffuser de la musique et de diffuser des messages.

Chaine de diffusion:

* Diffusion de la musique :  
    
  Dans les émissions en stéréo
* Envoie des messages :