Rapport de laboratoire

Huitième laboratoire : Analyse de signaux radio FM

Roumache Grégoire
Sénéchal Julien
Robert Alexandre
Wallemme Maxime
Kenmeugne Lionel
Didion Charles

Laboratoire de sciences appliquées à l'informatique
Sécurité des systèmes, technologie de l'informatique
Hénallux
Première année, groupe H
Année académique 2019-2020

30 Avril 2020

1 Introduction

Dans ce rapport, nous allons parler un peu des fréquences radios. Comment se fait-il qu'une radio sois capable de monter le son lors des annonces trafic ? Et comment la sécurité des communications radio peut-elle être assurée ? RSD, WFM, FFT, des abréviations qui à première vue n'ont pas beaucoup de sens. Mais qui, pourtant, assure la base de toute les communications radio actuelle.

2 Rappels théoriques

2.1 Qu'est-ce que RDS ?

Qu'est-ce que le Radio Data System ? "RDS" = service de transmission de données numériques qui est également une norme européenne. Développé en 1974 par plusieurs entreprises de radiodiffusions et basé sur son prédécesseur l'ARI (Autofahrer-Rundfunk-Informationssystem).

Il est composé de plusieurs fonctionnalités toute lié à des sous programmes internes :

— Programme service (PS)
— Alternative Frequencies (AF)
— Clock time (CT)
— Traffic programme (TP)
— Traffic annoncement (TA)

1. Le programme service (PS) : fonctionnalité qui permet d'afficher le nom de la station radio active. À la base 8 caractères alphanumérique maximum par après détourner de la norme pour avoir accès au nom du titre de la musique jouer au moment de l'écoute.
2. Alternative Frequencies (AF) : partie logicielle qui se calibre automatiquement sur la meilleure fréquence possible d'écoute (évite les coupures radios quand le véhicule est en mouvement.
3. Le Clock Time (CT) : service qui calibre l'heure de l'appareil de manière automatique prenant en compte les changements d'heures.
4. Trafic Programme (TP) : l'icône qui indique s'il y a des annonces concernant le trafic routier sur cette station.
5. Traffic annoncement (TA) : annonce quand une information sur le trafic a lieu et augmente le volume pour qu'elle soit facilement audible.

2.2 Que veux dire WFM ?

Il existe 3 types de bandes FM :

— *FM* : Frequency Modulation
— *WFM* : Wide Frequency Modulation
— *NFM* : Narrowband Frequency Modulation

WFM signifie *Wide FM*, autrement dit *FM à bande large*. C'est ce qui est utilisé pour la diffusion de la radio en *FM* (88 - 108 Mhz). Le *FM*, lui, est une modulation a bande étroite. Etant donné que le *WFM* a une bande plus large, il y a moyen de faire du Stereo.

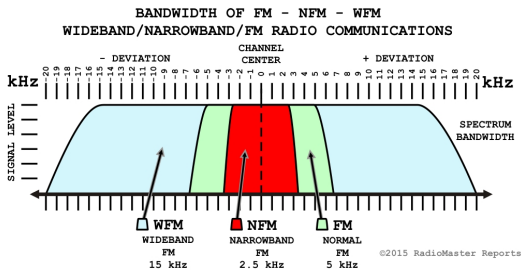

Figure 1 – Différence de bande passante entre *FM*, *WFM*, et *NFM*

2.3 Que représente le paramètre FFT ?

FFT est l'acronyme de *Fast Fourier Transform*. La transformation de Fourier rapide est un algorithme qui sert à calculer la transformation de Fourier discrète. L'utilisation de cet algorithme est beaucoup plus rapide que l'utitilisation d'un algorithme naïf :

- complexité du FFT : $O(n \log n)$;
- complexité de l'algorithme naïf : $O(n^2)$.

Modifier le paramètre *FFT size* (taille de la transformation rapide de Fourier) peut aider à mieux visualiser la fréquence ou le domaine temporel.

2.4 Quel moyen mettriez-vous en œuvre pour vous protéger contre une usurpation de bande de fréquence ?

L'usurpation de bande de fréquence est un type d'attaque parmi d'autres sur les fréquences radio. Le terme généralement utilisé pour l'usurpation est le "spoofing". Deux autres types d'attaques comme le "brouillage" ou "l'écoute passive" peuvent être utilisés. Le brouillage consiste à émettre un bruit sur la fréquence radio à l'aide d'un amplificateur.

L'écoute passive quant à elle, consiste pour l'attaquant à prendre connaissances de données transmises entre l'émetteur et le récepteur de la fréquence radio. Concernant le spoofing (usurpation de bande de fréquences), cela va consister à modifier les valeurs, ou données transmises afin d'atteindre la disponibilité du système. Pour contrer cette attaque, on peut protéger la bande de fréquence radio à l'aide d'une authentification par challenge-réponse.

Cette méthode est bien connue dans le milieu de la sécurité informatique, elle consiste à ce qu'une partie pose un challenge et l'autre partie doit y répondre à l'aide d'un algorithme ou autres et de manière correcte afin de valider l'authentification.

Exemple : Algorithme utilisé : $a \times b - 1$
Challenge :

1	5	6	9	7
a	b	c	d	e

Réponse :

$$1 \times 5 - 1 = 4$$

Le système ou la personne qui envoie le challenge change évidemment à chaque demande d'authentification, les chiffres envoyés. Ainsi, l'attaquant ne possédant pas l'algorithme, il ne pourra pas pénétrer dans le système.

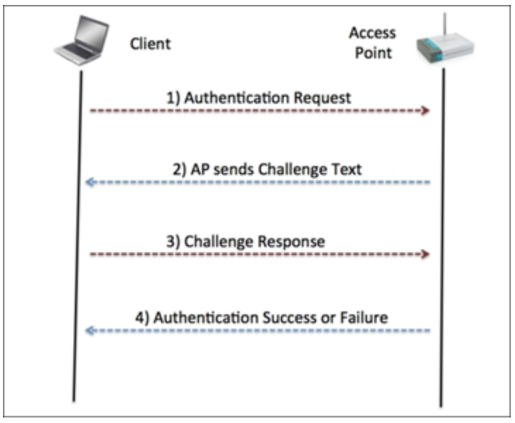

FIGURE 2 – Schéma du dialogue entre le client et le point d'accès

3 Conclusion

Le **Radio Data System** (RDS) est un service de transmission de données numériques en parallèle des signaux audio et **la gestion de la main-d'œuvre** (WFM) est un processus institutionnel qui maximise les niveaux de performance et les compétences d'une organisation. La **transformation de Fourier rapide** (**FFT**) quant à lui est un algorithme de

calcul de la transformation de Fourier discrète (TFD). Toutes ces notions nous ont amenées à nous poser des questions sur les risques ou attaques affectant les fréquences radio. D'où l'usurpation de bande de fréquence (spoofing), le brouillage ou l'écoute passive que nous avons développés mais qui sont des types d'attaques parmi d'autres.

Table des matières

Table des figures

Références

[1] https ://www.forumatena.org/files/livresblancs/L%27environnement%20sans%20fil.pdf

[2] https ://www.youtube.com/watch ?v=19CE1yeKzjU

[3] https ://searchsecurity.techtarget.com/definition/challenge-response-system

[4] https ://www.ornikar.com/code/cours/mecanique-vehicule/technologie-assistance/radio-data-system

[5] https ://www.elttam.com/blog/intro-sdr-and-rf-analysis/

[6] https ://fr.wikipedia.org/wiki/Transformation_de_Fourier_rapide

[7] https ://radiofreeq.wordpress.com/2016/06/21/fm-versus-nfm-for-best-radio-communications/