**N° d'ordre :**


الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de L'enseignement Supérieur et de La Recherche Scientifique

المركز الجامعي بلحاج بوشعيب عين تموشنت

Centre Universitaire Belhadj Bouchaib-Ain Témouchent

Institut : Technologie
Departement : Génie Electrique
Laboratoire : Structures Intelligentes


# THESE

Présentée pour l'obtention du **diplôme de DOCTORAT LMD**

**Domaine :** Science et Technologie
**Filière** : Télécommunication
**Spécialité** : Télécommunication


**Par** : YAGOUB Réda


## Intitulé

# Développement d'un procédé SDR hybride pour différentes générations de Télécommunications mobiles

Soutenue publiquement, le 23 / 06 / 2019 , devant le jury composé de :

| Nom & Prénom(s) | Grade | Qualité | Etablissement de rattachement |
|---|---|---|---|
| Mr. BENCHERIF Kaddour | MCA | Président | CUBBAT – Aïn Témouchent |
| Mr. BENAISSA Mohamed | MCA | Directeur de thèse | CUBBAT – Aïn Témouchent |
| Mr. BENADDA Belkacem | Pr | Co-Directeur de thèse | Université Abou Bekr Belkaid-Tlemcen |
| Mr. ABRI Mehadji | Pr | Examinateur | Université Abou Bekr Belkaid-Tlemcen |
| Mme. SLIMANE Zohra | MCA | Examinateur | CUBBAT – Aïn Témouchent |

Année Universitaire : 2018/2019

***A** mon défunt père*

***A** ma très chère maman*

***A** ma chère sœur*

***A** mes frères*

***A** ma nièce*

***A** mes amis*

***A** tous ceux qui me sont chers*

# REMERCIEMENTS

A l'issue de ce travail, j'exprime mes vifs remerciements et toute ma gratitude à mon Directeur de thèse Monsieur **Mohamed BENAISSA**, Maître de Conférences Classe A au Centre Universitaire de BELHADJ Bouchaib, d'Aïn Témouchent, pour la qualité de son encadrement, pour sa totale disponibilité et pour le soutien qu'il n'a cessé de m'apporter durant la période de ma thèse.

Mes vifs remerciements vont aussi à mon Co-encadrant Monsieur **Belkacem BENADDA**, Professeur à l'Université de Tlemcen, pour sa disponibilité et son aide, les échanges d'idées, et pour son attention.

Je remercie Monsieur Kaddour BENCHERIF, Maître de Conférences Classe A au Centre Universitaire de BELHADJ Bouchaib, d'Aïn Témouchent, qui m'a fait l'honneur de présider ce jury de thèse.

Je remercie tout particulièrement, Monsieur Mehadji ABRI Professeur à la faculté de Technologie de l'université Abou Bekr Belkaïd de Tlemcen, Madame Zohra SLIMANE Maître de Conférences Classe A au Centre Universitaire de BELHADJ Bouchaib, d'Aïn Témouchent, qui ont acceptés de juger ce travail et d'en être rapporteurs.

Mes sincères remerciements vont également au Dr. Souheyla FEROUANI, Pr. Choukria AYACHE et le Dr. Abdelhafid MERADI, enseignants-chercheurs au Centre Universitaire BELHADJ Bouchaib d'Aïn Témouchent.

*Merci à tous ….*

# Résumé

L’avancement de la technologie numérique a permis de remplacer une partie analogique des systèmes de radiocommunications par des composants numériques, où l'exploitation des équipements peut être réalisée par un logiciel centralisé et de remplacer des contraintes matérielles en contraintes logicielles, on parle de la radio logicielle. Cette technologie permet d’implémenter la majorité des traitements du signal dans le domaine numérique, ceci permet de gagner en souplesse de configuration et de réduire considérablement le coût du développement et de déploiement des systèmes radio avec les normes de communication radio en constante évolution. Ce travail est scindé en deux parties principales:

La première partie est consacrée à la technologie radio logicielle, le concept, l’architecture de la radio logicielle idéale et restreinte et les plateformes à faible coût disponibles permettant aux chercheurs la mise en œuvre des systèmes radios logiciels. Une étude détaillée de la plateforme RTL-SDR a été présentée.

Dans la deuxième partie, nous nous sommes intéressés la réalisation de différentes applications en utilisant la clé RTL-SDR. Dans un premier temps, nous avons présenté des approches utilisées pour la démodulation des signaux de la bande radio FM, l’analyse spectrale et la détection des activités spectrales. Dans un second temps, une application embarquée en combinant la plateforme RTL-SDR et la carte Raspberry Pi version 3 pour la localisation à base du réseau GSM a été présentée.

**Mots clés :**

Radio logicielle; SDR; Analyse spectrale; Détection spectrale; Localisation avec RTL-SDR; Traitement du signal numérique.

# Abstract

The advance made in digital technology has introduced the opportunities to replace analog parts of the radio communication systems with digital components. All improvements provide the opportunity to build reconfigurable radio platform with only software constraints. Based on this context the software-defined radio (SDR) appeared. This emergent technology makes it possible to implement wide range of signal processing algorithms used in the digital domain. Indeed, this will allows greater configuration, flexibility and reduces considerably the costs of developing and deploying radio systems. Moreover, it will allow rapid changing and free of charge to higher or different radio communication standards. This work is divided into two main parts:

The first part is dedicated to the SDR technology, the concept, the different architectures and the low cost platforms available allowing researchers to implement SDR solutions. A detailed study of the RTL-SDR platform is presented.

In the second part, we are interested in the implementation of different applications using the RTL-SDR Dongle. First, we presented approaches used for the demodulation of FM signals, spectral analysis and spectral activity detection. Finally, an embedded positioning application combining the RTL-SDR platform and the Raspberry Pi version 3 based on GSM signals is presented.



**Keywords:**

Software defined radio; SDR; Spectral analysis; Spectral detection; RTL-SDR based localization; Digital signal processing.

# ملخص

أتاح تقدم التكنولوجيا الرقمية استحداث أنظمة اتصالات لاسلكية بمكونات رقمية. حيث يمكن استغلال هذه المعدات بواسطة برامج بسيطة. في هذا السياق ظهر ما يسمى بالراديو المعرف برمجيا. تتيح هذه التكنولوجيا تنفيذ غالبية معالجة الإشارات في المجال الرقمي، مما يعطي مرونة أكبر للأنظمة اللاسلكية ويقلل إلى حد كبير تكلفة تطوير هذه الانظمة بمعايير الاتصالات المتغيرة باستمرار. ينقسم هذا العمل إلى قسمين رئيسيين:

الجزء الأول من هذا العمل مكرس للراديو المعرف برمجيا، المفهوم، والتصميمات المختلفة والمنصات منخفضة التكلفة المتاحة التي تسمح للباحثين بإنشاء أنظمة الراديو المعرف برمجيا. تم تقديم دراسة مفصلة لمنصة RTL-SDR.

في الجزء الثاني من العمل، نهتم بإنشاء تطبيقات مختلفة باستخدام منصة RTL-SDR. أولاً، قدمنا الأساليب المستخدمة في استخلاص إشارات الراديو من نوع FM، ثم تطبيقات للتحليل الطيفي و الكشف عن أنشطته. في الاخير، تم تقديم تطبيق مضمن يجمع بين منصة RTL-SDR وبطاقة الراسبيري الإصدار3 يهتم بتحديد المواقع بالاعتماد على اشارات شبكة GSM.

**كلمات مفتاحية :**

الراديو المعرف برمجيا; SDR; التحليل الطيفي; الكشف عن النشاط الطيفي; تحديد المواقع اعتمادا على RTL-SDR ;معالجة الاشارة الرقمية.

# Table des Matières

**Chapitre 3: Applications pour la radio logicielle restreinte**

**Chapitre 4 : Système embarqué pour la localisation à l'aide du réseau GSM à base de la clé RTL-SDR et Raspberry Pi.**

# Liste des Figures

# Liste des Tableaux

# Acronymes et Abréviations

**ADC** : Analog Digital Converter
**ADS-B** : Automatic dependent surveillance broadcast
**AGCH** : Access Grant Channel
**AIS** : Automatic Identification System
**AM** : Amplitude Modulation
**AOA** : Angle of Arrival
**API** : Application Programming Interface
**APRS** : Automatic Packet Reporting System
**ARFCN** : Absolute Radio Frequency Channel Number
**ASIC** : Application Specific Integrated Circuits
**ASIP** : Application-Specific Instruction-set Processor
**Auc** : Authentication Center
**BCCH** : Broadcast Control Channel
**BCH** : Broadcast Channel
**BPSK** : Binary Phase Shift Keying
**BSC** : Base Station Controler
**BSS** : Base Station Subsystem
**BTS** : Base Transceiver Station
**CAN** : Convertisseur Analogique/Numérique
**CBCH** : Cell Broadcast Channel
**CCCH** : Common Control Channel
**Cell ID** : Cell Identity
**CMOS** : Complementary Metal-Oxide-Semiconductor
**CNA** : Convertisseur Numérique/Analogique
**CPH** : Control processor host
**DAB** : Digital Audio Broadcasting
**DC** : Direct Current
**DRM** : Digital Radio Mondiale
**DSP** : Digital Signal Processor
**DSP** : Digital Signal Processig
**DVB** : Digital Video Broadcast
**DVB-T** : Digital Video Broadcast Terrestrial
**E-CIDTA** : Enhanced Cell-ID + Time Advance
**EEPROM** : Electrically Erasable Programmable Read Only Memory
**EIR** : Equipement Indentity Register
**ETSI** : European Telecommunications Standards Institute
**FACCH** : Fast Associated Control
**FCC** : Federal Communications Commission
**FCCH** : Frequency Correction Channel
**FDMA** : Frequency Division Multiple Access
**FFT** : Fast Fourier Transform
**FI** : Fréquence Intermédiaire

**FM** : Frequency Modulation
**FPGA** : Field Prorammable Gate Arrays
**GCI** : Global Cell Identity
**GIPS** : Giga Instructions Per Second
**GMSK** : Gaussian Minimum Shift Keying
**GPIO** : General Purpose Input/Output pins
**GPP** : General Purpose Processors
**GPS** : Global Positioning System
**GSM** : Globale System for Mobile Communication
**HLR** : Home Location Register
**I/Q** : In-Pahse/Quadrature
**I2C** : Inter Integrated Circuit
**IEEE** : Institute of Electrical and Electronics Engineers
**IMEI** : International Mobile Equipment Identity
**IMSI** : International Mobile Subscriber Identity
**IR** : Infrarouge
**ISS** : International Space Station
**JTRS** : Joint Tactical Radio System
**LabVIEW** : Laboratory Virtual Instrument Engineering Workbench
**LAC** : Location Area Code
**LAI** : Location Area Identity
**LMU** : Location Measurment Units
**LNA** : Low Noise Amplifier
**LTE** : Long Term Evolution
**MCC** : Mobile Country Code
**MCX** : Micro Coaxial Connector
**ME** : Mobile Equipment
**MMITS Forum** : Modular Multifunctional Information Transfer System Forum
**MNC** : Mobile Network Code
**MPEG** : Moving Picture Experts Group
**MSC** : Mobile Switching Center
**MSISDN** : Mobile Subscriber Integrated Services Digital Network
**MSPS** : Mega sample per Second
**NCO** : Numerically Controlled Oscillator
**NOAA** : National Oceanic and Atmospheric Administration
**NSS** : Network Subsystem
**OL** : Oscillateur Local
**OMG** : Object Management Group
**OSS** : Operating Sub-System
**PAL** : Belling-Lee Connector
**PC** : Personal Computer
**PCH** : Paging Channel
**PCI** : Peripheral Component Interconnect
**PI** : Programme Identification
**PLMN** : Public Land Mobile Network

**PPM** : Parts Per Million
**PS** : Programme Service Name
**PTS** : Processeurs de Traitement de Signal
**QoS** : Quality of service
**QPSK** : Quadrature Phase Shift Keying
**RACH** : Random Access Channel
**RDS** : Radio Data System
**RF** : Radio Fréquence
**RLR** : Radio Logicielle Restreinte
**RT** : RadioText
**RTL-SDR** : Realtek Software Defined Radio
**SACCH** : Slow Associated Control Channel
**SCA** : Software Communications Architecture
**SCH** : Synchronisation Channel
**SDCCH** : Standalone Dedicated Channel
**SDR** : Software Defined Radio
**SDRAM** : Synchronous Dynamic Random Access Memory
**SFF** : Small Form Factor
**SIM** : SubscriberIdentity Module
**SMA** : Sub Miniature version A
**SNR** : Signal to Noise Ratio
**SRAM** : Static Random Access Memory
**SWR** : Software Radio
**TCH** : Traffic Channel
**TCXO** : Temperature compensated crystal oscillator
**TDMA** : Time Division Multiple Access
**TDOA** : Time Difference Of Arrival
**ToA** : Time of Arrival
**UHD** : USRP Hardware Driver
**UHF** : Ultra High Frequency
**UMTS** : Universal Mobile Telecommunications Service
**USB** : Universal Serial Bus
**USRP** : Universal Software Radio Peripheral
**VCO** : Voltage-Controlled Oscillator
**VCTCXO** : Voltage Controlled Temperature Compensated Crystal Oscillators
**VGA** : Variable Gain Amplifier
**VGA** : Video Graphics Array
**VHF** : Very High Frequency
**VLR** : Visitor Location Register
**WIF** : Wireless Innovation Forum
**WLAN** : Wireless Local Area Network

# Introduction Générale

De nos jours, les normes de télécommunications sans fil évoluent rapidement. En outre, les utilisateurs doivent constamment opérer simultanément dans différents services sans fil, qui varient en fonction des bandes de fréquences, des modulations, du codage et d'un ensemble de paramètres propres à chacun d'eux. Les équipements radio communication doivent répondre à des besoins croissants en termes de flexibilité et d'adaptabilité aux différents standards. La radio logicielle (SDR- Software Defined Radio) se présente comme une alternative à cette demande technologique. En effet, les dispositifs SDR se présentent comme une solution qui permet de rendre les systèmes de communication flexibles, reconfigurable, moins coûteux et conviviaux.

Le terme de radio logicielle a été inventé par Joe Mitola en 1991 pour désigner la classe de radios reprogrammables ou reconfigurables [1]. En d'autre terme, il s'agit d'une architecture souple et polyvalente qui peut être programmée ou configurée par logiciel. Comparé aux architectures traditionnelles réalisées en technologie analogique, la plupart de ces équipements radios sont définis par matériel avec peu ou pas de logiciel et chaque équipement était conçu pour un usage particulier car chaque norme possédait une architecture spécifique [2].

Dans un avenir proche, les technologies de transmission radio pourraient devenir entièrement numériques, avec une architecture dite idéale [3], dans laquelle la numérisation est effectuée directement après l'antenne par des convertisseurs analogiques numériques à haute fréquence d'échantillonnage et une forte résolution. La plupart des traitements du signal sont effectués par un processeur de signal numérique à grande vitesse.

La radio logicielle utilise des dispositifs numériques programmables pour effectuer le traitement du signal nécessaire pour transmettre et recevoir des informations. Des dispositifs tels que les DSP (Digital Signal Processor) et les FPGA utilisent un logiciel pour leur fournir les fonctionnalités requises pour le traitement du signal. Ces composants numériques sont différents en termes de consommation d'énergie, de puissance de calcul, de souplesse de configuration et d'autres caractéristiques. Des caractéristiques qui influencent la nature de l'application (spatiale, station radio, …), les coûts de revient et les performances.

Ces dernières années, la technologie de la radio logicielle a été considérablement améliorée. La réalisation de plateformes à faibles coûts, permettent aux chercheurs de créer des systèmes radios logiciels diversifiés. En effet, les plateformes actuellement disponibles, sont distinctes en termes de: flexibilité, rapidité de calcul, bande passante, etc.

L'une des plateformes qui a eu un grand succès ces dernières années, est celle à base des dongles RTL-SDR. En effet, cette plateforme qui se présente sous la forme d'une simple clé USB, offre de nombreuses possibilités pour explorer les algorithmes dédiés aux

développements des récepteurs de communications sans fils et les problèmes liés aux implémentations DSP. Il est par exemple envisageable d'utiliser cette plateforme SDR en réception uniquement pour scanner, analyser et démoduler les signaux de la bande spectrale de sensibilité de son tuner.

Cependant, les performances des clés RTL-SDR ne s'apparentent pas à un SDR professionnel, ces clés à faibles coûts et répandus possèdent des faiblesses qui peuvent être résumées dans les points suivants:

- Une bande passante limitée à 3.2Msps au maximum.
- L'utilisation de la fréquence d'échantillonnage maximale de 3.2Msps, engendre une perte des échantillons. Pour éviter ce problème, il est recommandé d'utiliser une fréquence d'échantillonnage inferieure à la fréquence maximale.
- Une gamme des clés USB RTL-SDR est commercialisée avec des oscillateurs local de faible qualité, qui peuvent introduire des décalages sur la fréquence de l'ordre de ± 150 ppm.
- Elle n'est pas bien adaptée pour détecter les signaux faibles puissances (sensibilité médiocre).
- Les nombreuses sources de bruit telles que : le bruit de l'USB, les fuites radio fréquence, un bruit de fond élevé.
- La difficulté à recevoir simultanément les signaux forts et faibles en même temps affectée par la plage dynamique du convertisseur analogique numérique [4].
- Initialement conçus pour la réception de la télévision numérique [5], elles ont, pour le connecteur d'antenne, une impédance d'entrée d'environ 75 Ohms, alors que les équipements radio amateur et professionnel utilisent pour l'antenne une impédance d'entrée de 50 Ohms [6].

L'objectif de ce travail de recherche est le développement des solutions logicielles associées avec les plateformes SDR disponibles au sein du centre universitaire BELHADJI Bouchaïb d'Aïn Témouchent. Des solutions qui visent l'intégration simultanée d'une multitude de services de télécommunications sans fils. Nous avons eu le privilège de manipuler plusieurs plateformes RTL-SDR, où nous nous sommes intéressés au développement de solutions logicielles qui surmontent celles existantes et qui corrigent les limites imposées avec l'utilisation de ces dongles. En effet, dans cette thèse nous présentons les travaux réalisés pour réduire le bruit et surmonter les contraintes de l'imperfection matérielle de ces clés. Dans les solutions que nous présentons, nous avons fait usage des méthodes numériques pour le traitement du signal sans aucune amélioration matérielle.

La présentation de notre thèse se décompose en quatre chapitres.

Le premier chapitre aborde l'état de l'art des technologies radios logicielles. Dans une première partie de ce chapitre, un court historique de la radio logicielle est rappelé, ainsi que le concept et les avantages de cette technologie. Ensuite, dans une seconde partie nous présentons un aperçu de la radio logicielle idéale et la radio logicielle restreinte avec les différentes architectures dédiées à la réception qui coexistent et leurs caractéristiques.

Le second chapitre est consacré à la présentation des plateformes radio logicielle avec leurs principales caractéristiques. La première section de ce chapitre présente des plateformes commerciales actuellement largement disponibles, conçues pour l'émission et la réception. La deuxième section se focalise principalement sur le récepteur à faible coût RTL-SDR, où un aperçu plus détaillés est donné. Dans cette partie, nous avons effectué un travail pour surmonter l'erreur introduite par l'imperfection de l'oscillateur local.

Le troisième chapitre présente les applications réalisées en utilisant la clé RTL-SDR pour une analyse temps réelle de l'activité spectrale. Nous avons également présenté les approches utilisées pour la démodulation. Les signaux de la bande radio FM et AM sont pris comme exemples. Les performances des applications réalisées sont évaluées en termes des signaux disponibles en Algérie. Les développements ont été réalisés sous l'environnement Matlab.

Le quatrième chapitre de cette thèse présente une application embarquée en combinant le dongle RTL-SDR et la carte Raspberry Pi version 3. Dans ce cas, l'application développée se présente à l'image d'un système de localisation en exploitant uniquement les stations de base du réseau GSM. La difficulté se résume dans le décodage des signaux GSM simultanément pour toutes les BTSs à la portée du dongle RTL-SDR de tous les opérateurs, ceci sans avoir recours à un abonnement ou l'acquisition d'une carte SIM. L'algorithme proposé exploite les informations relatives au Cell ID. La carte développée n'est pas détectable par les opérateurs du réseau. Les tests présentés ont été effectués dans les trois villes algériennes, Aïn Témouchent, Oran et Sidi Bel Abbes.

# Chapitre 1

# La technologie de la radio logicielle: Etat de l'art

## 1.1 Introduction

Les progrès de la technologie de traitement du signal ont permis l'émergence d'une nouvelle approche d'implémentation des plates-formes de communications sans fil, où la majorité des traitements du signal sont implémentés dans le domaine numérique. Basé sur cette approche, des systèmes radio logicielle (en anglais Software Radios) sont apparus [7].

La radio logicielle est une technologie émergente qui change profondément l'ingénierie liée à la conception des systèmes radio. Dans les communications sans fil traditionnelles, des dispositifs sans fil différents ne peuvent pas communiquer entre eux en raison de leurs différents systèmes radio. Dans le paradigme radio logicielle, de nombreux composants du système radio sont implémentés avec logiciel, et peuvent être reconfigurés, permettant ainsi un seul dispositif radio pour les systèmes sans fil multistandard, multi-bandes [8].Cette technologie offre un large éventail d'avantages, notamment la flexibilité, la reconfigurabilité et la multifonctionnalité, etc. La radio logicielle idéale (SWR : Software Radio) représente le point de flexibilité maximal où les traitements analogiques du signal se font juste au niveau de l'antenne [3]. Par exemple, lors de la réception, le signal radio reçu est directement échantillonné au niveau de la sortie de l'antenne comme illustré dans la figure 1.1 et tous les autres traitements du signal restants (transformée de Fourier, modulation, démodulation, sélection de canaux, établissement de protocoles, égalisation, etc) sont réalisés dans le domaine numérique.

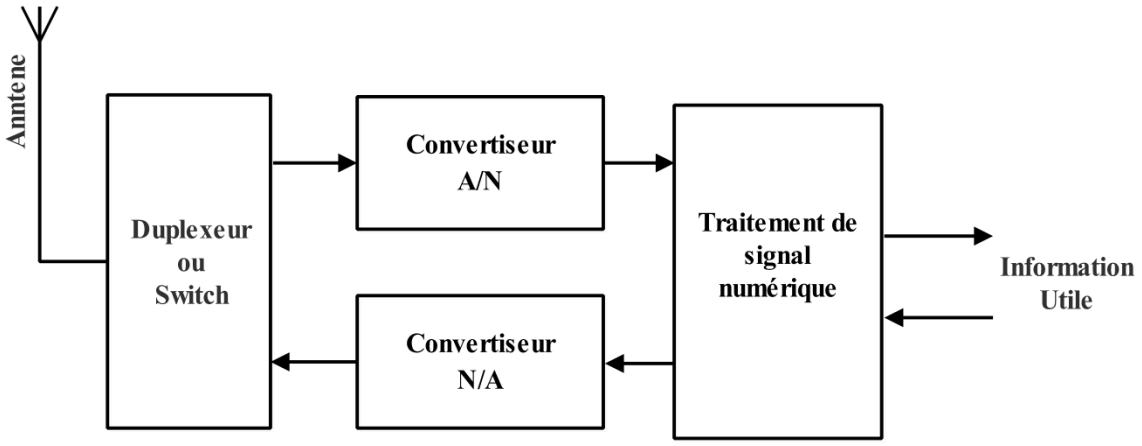



Figure 1.1:Radio logicielle idéale.

Un duplexeur permet de faire fonctionner l'antenne en mode émission ou réception. Les convertisseurs Analogique numériques A/N et numérique analogique N/A font office de passerelle entre les deux types de traitement. La plus grande partie du récepteur ainsi que l'exploitation des données est implémentée sous forme d'algorithmes.

Cependant, la SWR soulève un nombre important de défis du point de vue de la conception, qui implique l'émergence du système radio logicielle restreinte (Software Defined Radio,

SDR), la version réalisable de la SWR. Dans ce chapitre, nous présentons les principaux aspects de la technologie radio logicielle, son concept, les besoins et les avantages de cette technologie émergente en détaillant les différentes architectures existantes.

## 1.2 De la radio matérielle à la radio logicielle

Depuis des décennies, les radiocommunications et leurs équipements sont réalisées en technologie analogique, la plupart de ces équipements radios sont définis par matériel avec peu ou pas de logiciel et chaque équipement était conçu pour un usage particulier car chaque norme possédait une architecture spécifique [2]. La modification du comportement d'un équipement était donc impossible à moins de remplacer certains composants. La figure 1.2 représente l'architecture de la radio matérielle traditionnelle pour un émetteur-récepteur superhétérodyne.

Le principe de la réception superhétérodyne repose sur un changement de fréquence consistant à transposer le spectre d'un signal Radio Fréquence (RF) capté par l'antenne autour d'une fréquence fixe appelée Fréquence Intermédiaire (FI, généralement beaucoup plus basse que celle de la porteuse RF). Ce changement de fréquence est réalisé à l'aide d'un mélangeur et d'un oscillateur local (OL).Après la transposition, le signal FI passe par un étage de filtrage, puis le signal modulé en bande de base est démodulé pour produire l'information analogique de réception.

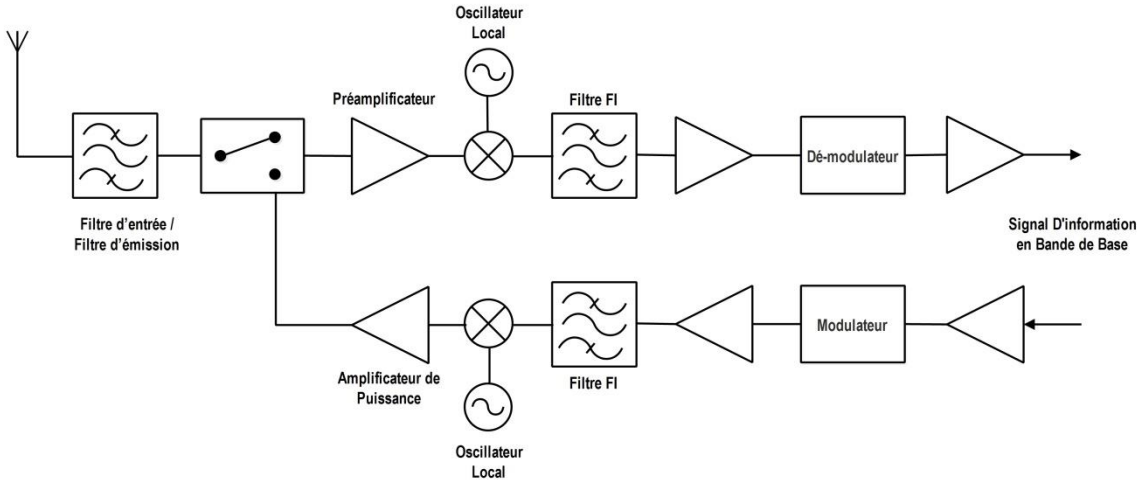



Figure 1. 2: Architecture des systèmes de transmission radio conventionnels.

L'avancement de la technologie numérique a permis de remplacer une partie analogique des systèmes de transmission radiofréquence par une composante numérique et logicielle. Aujourd'hui, l'exploitation des équipements peut être réalisée par un logiciel centralisé, on

parle ainsi de la radio logicielle. Un système radio logicielle est divisé en deux parties : une partie analogique et une partie numérique. La figure 1.3 représente la répartition des opérations réalisées dans la partie analogique et la partie numérique.

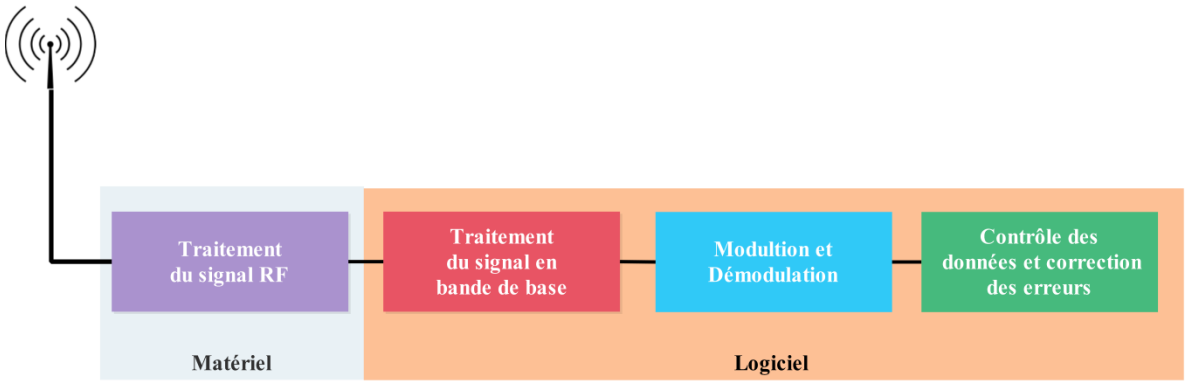



Figure 1. 3: Répartition analogique/numérique dans une plateforme radio logicielle

L'intention fondamentale est donc de passer d'un système traditionnel axé sur le matériel, à un système qui utilise une application logicielle pour effectuer les tâches radio sur une plate-forme informatique.

## 1.3 Approche théorique du concept

### 1.3.1 Bref historique

L'histoire de la radio logicielle a commencé au milieu des années 1980.Le terme «radio logicielle» a été utilisé pour la première fois en 1984 par E-Systemsinc (maintenant Raytheon) pour décrire un récepteur numérique en bande de base [9]. L'un des premiers développements majeurs pour la radio logicielle a été le projet militaire américain appelé SPEAKeasy, une plate-forme émetteur-récepteur conçue par Hazeltine et Motorola qui était basée sur la technologie radio logicielle. Le projet SPEAKeasy a été conçu pour fournir des communications militaires tactiques à des fréquences comprises entre 2 MHz à 2 GHz et assurer l'interopérabilité entre les différentes interfaces radios pour les normes des branches des forces armées [10]. Pour atteindre cet objectif, le SPEAKeasy a utilisé de nombreuses techniques pour fournir un système multi-bandes et multi-modes pouvant fonctionner sur deux bandes ou plus, séquentiellement ou simultanément. Ce projet a permis de traiter plusieurs types de normes qui a procuré des avantages aux militaires tels que l'interopérabilité, la flexibilité, la réactivité, la mobilité et la réduction du coût.

En 1992, le chercheur Joseph Mitola a décrit les principes de l'architecture radio logicielle dans l'article «Software Radio: Survey, Critical Analysis and Future Directions» [11], qui

est devenu la première publication IEEE à utiliser le terme «Software Radio».Il a définit la radio logicielle comme un système radio dont la majorité du traitement du signal est implantée sous forme logicielle, sur les signaux en bande de base.

En 1996, la première association dédiée à la radio logicielle sous le nom «Modular Multi functional Information Transfer System Forum (MMITS Forum)» a été fondée. En 1998, elle a été renommée «Software Defined Radio Forum (SDR Forum)», puis en 2009, en Wireless Innovation Forum [12]. Ce Forum était composé de personnes et d'organisations du gouvernement, de l'industrie et des instituts de recherche dont l'objectif était de promouvoir et de développer les technologies liées à la radio logicielles. Il a formé plusieurs groupes de travail et comités pour stimuler et orienter l'innovation et les normes.

En 1997, le département américain de la défense a créé le programme JTRS (Joint Tactical Radio System) [13]. Le JTRS est destiné à inter-opérer avec les systèmes radio existants et à fournir aux militaires des moyens de communication supplémentaires pour accéder aux cartes géographiques et autres données visuelles et de communiquer par voix et vidéo avec d'autres unités.

### 1.3.2 Concept de la radio logicielle

Le concept de radio logicielle est considéré comme l'avenir des systèmes de radiocommunications. Le nombre de standards de radiocommunication augmente rapidement pour offrir de nouveaux services aux utilisateurs. Les systèmes de radiocommunications multistandards conventionnels utilisent une architecture spécifique pour chaque standard afin de supporter plusieurs normes comme le montre l'exemple d'une architecture tri-standards de la figure 1.4, ce qui engendre une complexité accrue des terminaux à considérer. Les architectures classiques sont difficiles à modifier et leurs fonctionnalités ne peuvent pas supporter de modifications matérielles (reconfiguration par échange de composant) et ne peuvent supporter qu'un certain nombre de standards [13].

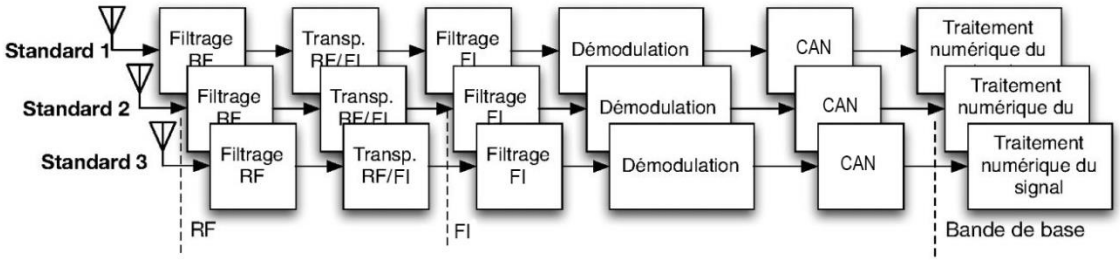



Figure 1. 4: Architecture classique d'un récepteur tri-standard [14].

L'un des objectifs de réalisation d'une radio logicielle est de remplacer des contraintes matérielles en contraintes logicielles. Une radio logicielle est un système radio où les composants sont implémentés en utilisant un logiciel au lieu du matériel. En réalisant les principaux composants en logiciel, une radio logicielle offre un support pour plusieurs standards et plusieurs bandes fréquentielles et des transitions de mode/bande transparentes par la mise à jour logicielle plutôt que le remplacement du matérielle. Ceci permet de gagner en souplesse de configuration et de contrôle sur la partie matérielle restante et de réduire considérablement le coût de développement et de déploiement des systèmes radio avec les normes de communication radio en constante évolution. Cette technologie promet d'apporter la flexibilité, la rentabilité et de la puissance pour faire progresser les communications vers l'avant. La figure 1.5 représente l'architecture générique d'un émetteur-récepteur radio logicielle.

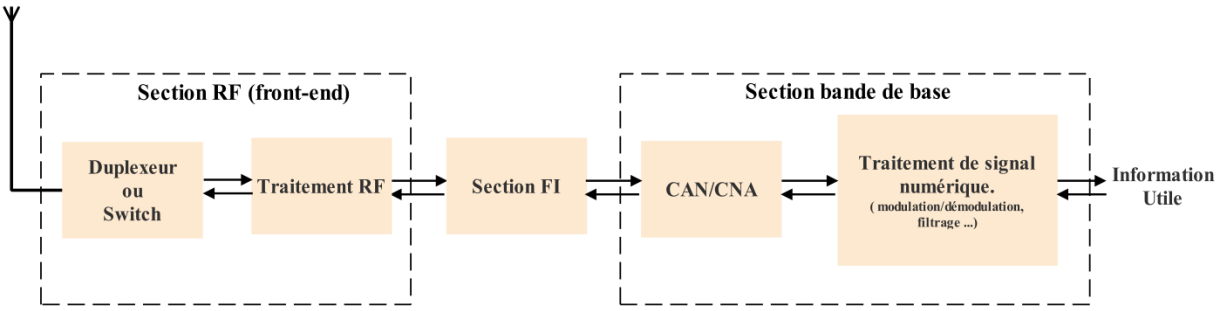



Figure 1. 5: Architecture simplifiée d'une radio logicielle.

Une architecture radio logicielle typique comprend un sous-système numérique et un sous-système analogique. Le sous-système analogique est constitué d'une antenne, d'un duplexeur qui permet d'utiliser la même antenne durant l'émission et la réception du signal, d'un filtre RF, d'un préamplificateur en réception, d'un amplificateur de puissance en émission et d'un oscillateur local OL pour la génération de la fréquence de référence pour la conversion du signal RF en fréquence intermédiaire FI pour la réception et l'inverse pour l'émission et d'un filtrage passe bande autour de la FI. Le sous-système numérique consiste en une conversion de la FI en un signal en bande de base pour la réception (la fonction inverse est réalisée pour l'émission), d'un filtrage numérique, des fonctions de modulation/démodulation, de codage/décodage, etc.

La Wireless Innovation Forum (WIF) définit les différents types de radio logicielle énumérés dans le tableau 1.1 en fonction du positionnement analogique-numérique et du degré de configuration.

| Catégorie | Dénomination | Degré de reconfiguration |
|---|---|---|
| **0** | Radio matérielle | Radio qui ne peut être modifiée par logiciel, reconfiguration par échange de composant |
| **I** | Radio contrôlée par logiciel | Reconfiguration logicielle limitée à un jeu prédéfini de paramètres (niveaux de puissance, interconnexions,…) |
| **II** | Radio définie par logiciel | Contrôle logiciel et reconfiguration des formes d'ondes, fréquence, bande passante,(dé)modulation, détection du signal, paramètre de sécurité, etc. |
| **III** | Radio logicielle idéale | Conversion analogique au niveau de l'antenne, tout le reste du système est reconfigurable. |
| **IV** | Radio logicielle ultime | Toute la radio est reprogrammable. Supporte simultanément plusieurs types de fonctions et différentes fréquences. |

Tableau 1. 1: Catégorisation des systèmes radio logicielle selon la Wireless Innovation Forum [15].

Une SWR consiste à réaliser tous les traitements du signal dans le domaine numérique et éliminer la transposition du signal RF en fréquence intermédiaire, où la numérisation du signal s'effectue juste après l'antenne et tous les traitements requis pour la radio sont effectués par logiciel. L'ajout dans une radio logicielle d'une certaine intelligence, produit une radio logiciel ultime, également nommée "Radio Cognitive" ou "Radio Intelligente" dans laquelle la radio a la capacité de s'adapter à l'environnement opérationnel [16]. Une radio logicielle ultime peut par exemple ajuster sa fréquence de fonctionnement pour profiter du spectre inutilisé et/ou adapter sa puissance d'émission, sa modulation, etc, pour atteindre un compromis acceptable entre la qualité de service (QoS) et les exigences spectrales.

Les opérations de traitement du signal numérique en bande de base de tout système radio est responsable de la transformation numérique des flux de données brutes dans le format correct, prêts à être transmis sur un canal sans fil. Dans un émetteur, cela consiste simplement à moduler le signal d'information et à introduire toute redondance nécessaire pour améliorer la réception. Au niveau du récepteur, les informations provenant du front-end radiofréquence (responsable du traitement du signal analogique) doivent être soigneusement analysées afin d'extraire correctement les données destinées à la réception. Cela nécessite une synchronisation, une démodulation, un décodage, etc. L'ensemble de ces traitements numérique du signal sont assurées par des algorithmes, implémentés dans les composants numériques suivants :

- Digital Signal Processor (DSP),
- General Purpose Processors (GPP),
- Field Programmable Gate Array (FPGA),

- Application-Specific Integrated Circuit (ASIC),
- Application-Specific Instruction-set Processor (ASIP),

Ces composants numériques sont différents en termes de consommation d'énergie, de puissance de calcul, de souplesse de configuration, etc. Le choix du type de composant utilisé dépend de la fonction à réaliser. La figure 1.6 illustre une comparaison entre les différents types de composants numériques en termes de flexibilité/performances. Les circuits comme le FPGA et l'ASIP combinent entre la puissance de calcul élevé et la souplesse de configuration ce qui permet un bon compromis flexibilité/performance.

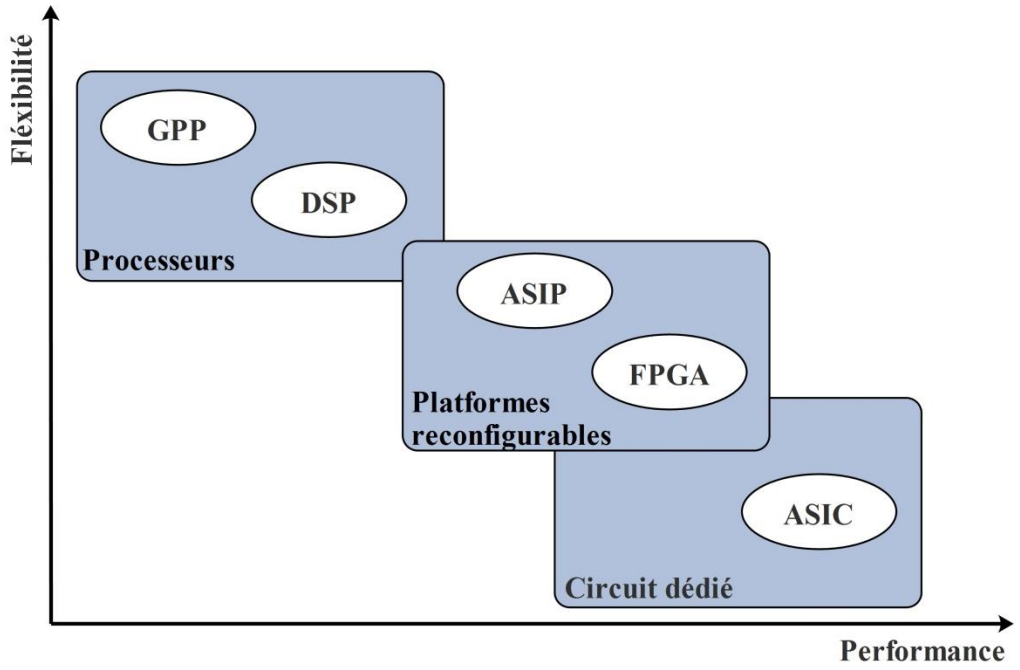



Figure 1. 6: Rapport flexibilité/performance des différentes catégories de composants numériques.

### 1.3.3 Avantages de la radio logicielle

L'évolution de la radio logicielle prend de plus en plus d'ampleur et procure de nombreux avantages pour tous les acteurs du domaine, aussi bien les fabricants, les opérateurs que les utilisateurs. Ces avantages sont les suivants [2,17]:

- Migration de l'analogique au numérique (DSP, FPGA…) ;
- Élimination du matériel analogique et de son coût, ce qui entraîne une simplification des architectures radio et une amélioration des performances;
- Performance des équipements embarqués;
- Augmentation de la vitesse des interfaces de communication ;

- Si la plupart des traitements sont effectuées dans le domaine numérique, la reconfiguration peut être assez simple et les coefficients de filtrage peuvent être modifiés. Dans le domaine analogique, l'espace et les ressources limitent les options de reconfiguration disponibles;
- Dans le domaine analogique, seul un petit nombre de types de modulation/démodulation sont possibles. Cependant, dans le domaine numérique, les possibilités sont illimitées si les fonctions sont configurables par logiciel;
- Une radio logicielle offre une portabilité des formes d'ondes et d'interopérabilité entre différents systèmes de communications.

## 1.4 Architectures de la radio logicielle

### 1.4.1 La radio logicielle idéale

Pour une SWR la numérisation du signal est effectuée directement après l'antenne (ou prés) de l'antenne et tous les traitements du signal sont effectués par logiciel dans le domaine numérique [3]. La figure 1.7 illustre l'architecture d'une SWR. Elle est composée d'une antenne large bande pour supporter une très grande gamme de fréquence, d'un convertisseur analogique/numérique (CAN) et d'un convertisseur numérique/analogique (CNA) avec une forte résolution et une fréquence d'échantillonnage très élevé et des processeurs de traitement de signal (PTS) numérique très performants pour réaliser les opérations complexes en temps réel.

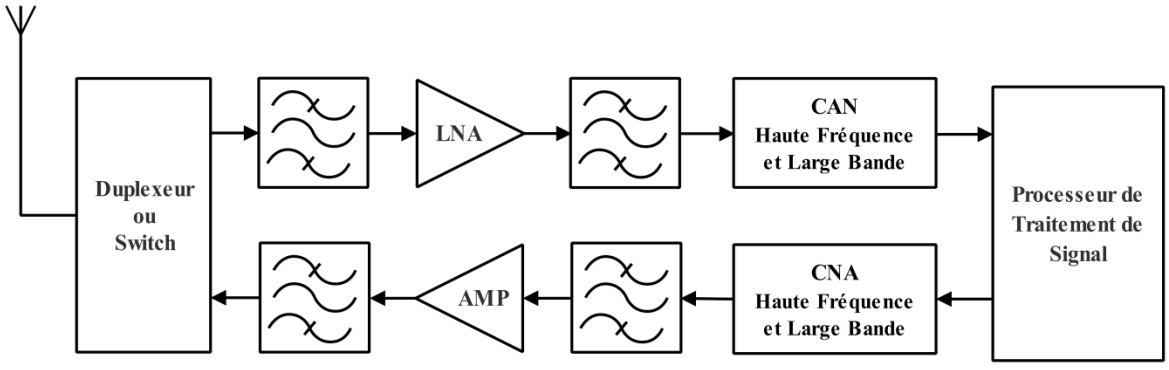



Figure 1.7: Architecture d'une SWR.

Cependant, de nombreux défis doivent être surmontés si l'on désire réaliser une SWR [18] :

- Une SWR ne devrait pas limiter la fréquence porteuse ou la bande passante de la forme d'onde. L'antenne devrait être capable de capturer des ondes électromagnétiques à partir de très basses fréquences (<1 MHz) jusqu'à des

fréquences très élevées (> 60 GHz). La conception d'une telle antenne à large bande, si elle est disponible, impose des exigences élevées au front-end RF et au CAN et CNA ;

- La sélection du signal désiré et le rejet des signaux indésirables (sélection du canal) est une caractéristique clé du front-end RF. Cependant, l'antenne et les filtres nécessaire pour implémenter la sélection du canal sont généralement des structures électromécaniques difficiles à régler de façon dynamique ;
- Le CAN aurait besoin d'un taux d'échantillonnage très élevé pour prendre en charge les signaux large bande, et d'un nombre élevé de bits de quantification pour supporter la grande variation de tension (dynamique d'entrée - écart entre la puissance minimale et la puissance maximale) [19].

Au-delà de ces inconvénients, une SWR a besoin d'une capacité de traitement du signal très élevée pour supporter les opérations de traitement du signal complexes pour différentes normes de communications sans fil, à titre d'exemple, [20] estime une puissance de traitement du signal pour le GSM, qui opère autour de la fréquence 900MHz, de10 GIPS (Giga Instructions Per Second) et jusqu'à 100 GIPS pour l'UMTS. La réalisation d'un tel système qui respecte ces critères sans consommer une quantité excessive de puissance, à prix raisonnable, est impossible avec la technologie actuelle.

Toutes ces contraintes imposent actuellement de passer par une phase intermédiaire combinant les anciennes et les nouvelles techniques : il s'agit de la radio logicielle restreinte (RLR) ou la SDR.

### 1.4.2 La radio logicielle restreinte

La version pratique de la SWR est la RLR (Figure 1.8). Dans une RLR, le signal reçu est échantillonné après un traitement approprié du signal analogique (transposition de fréquence, sélection de canal, rejet d'interférence et amplification).Ce type de récepteur représente le scénario probable où l'utilisateur sélectionne quelques canaux à la fois: par exemple, pendant que l'utilisateur effectue un appel téléphonique (GSM) en utilisant son micro-casque (Bluetooth), il télécharge également un fichier à partir du Web (WLAN : Wireless Local Area Network), la consommation d'énergie devient raisonnable et les réductions des coûts sont toujours possibles. Cependant, un front-end flexible avec une capacité de traiter des signaux à large gamme de fréquences pour différents standards est nécessaire. Ceci a un impact important sur la conception des segments analogiques et numériques du récepteur. Les principaux critères de sélection d'un front-end RF sont la complexité, le coût et la consommation d'énergie [21].

Actuellement, il existe plusieurs types d'architectures front-end RF. Dans la section suivante, nous présentons un bref aperçu des différentes architectures de front-end analogiques pour la mise en œuvre d'une radio logicielle multistandard.

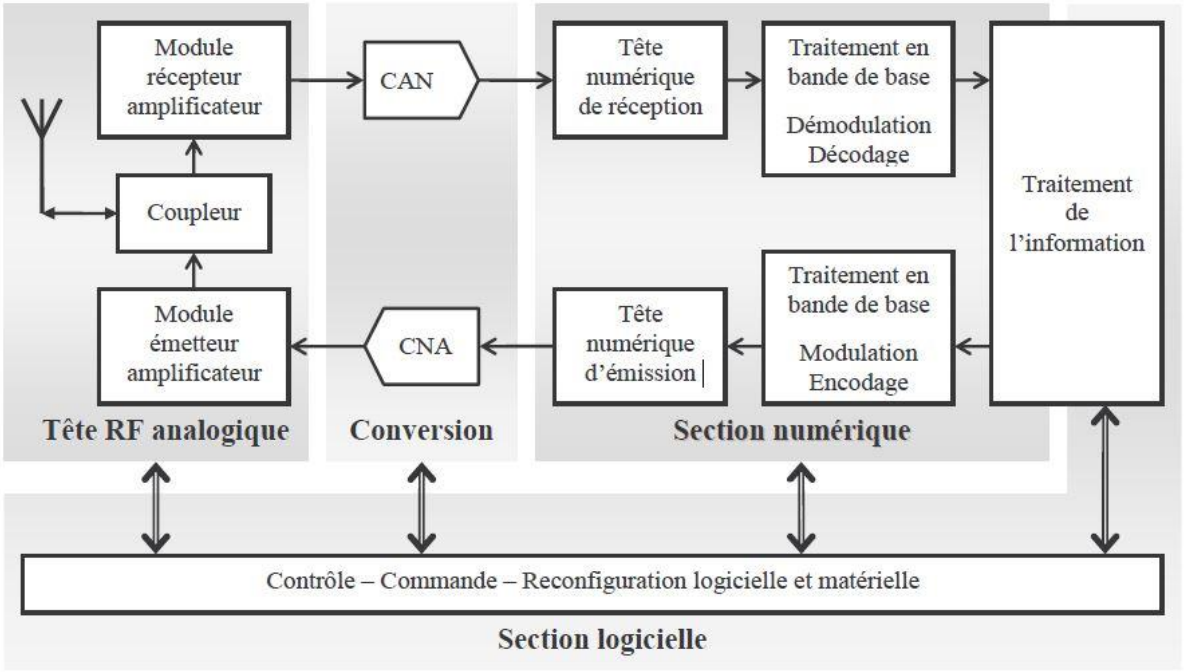



Figure 1.8: Architecture d'une radio logicielle restreinte [22].

### 1.4.2.1 Architectures candidates pour la RLR

#### a. Architecture hétérodyne

Le récepteur hétérodyne transpose le signal reçu à l'antenne en FI inférieure en utilisant un mélangeur. Cette opération permet d'utiliser un filtre moins sélectif pour éliminer les signaux indésirable avant la conversion vers le domaine numérique. La figure 1.9 montre l'architecture du récepteur RF à double changement de fréquence. Elle se base sur l'utilisation de deux mélangeurs, suivi chacun d'un filtre, d'un amplificateur et d'un CAN. La première fréquence intermédiaire $FI_1$ est sélectionnée suffisamment haute pour supprimer efficacement la fréquence image et la deuxième fréquence intermédiaire $FI_2$ est sélectionnée suffisamment basse pour assouplir l'exigence sur le filtre de sélection de canal.

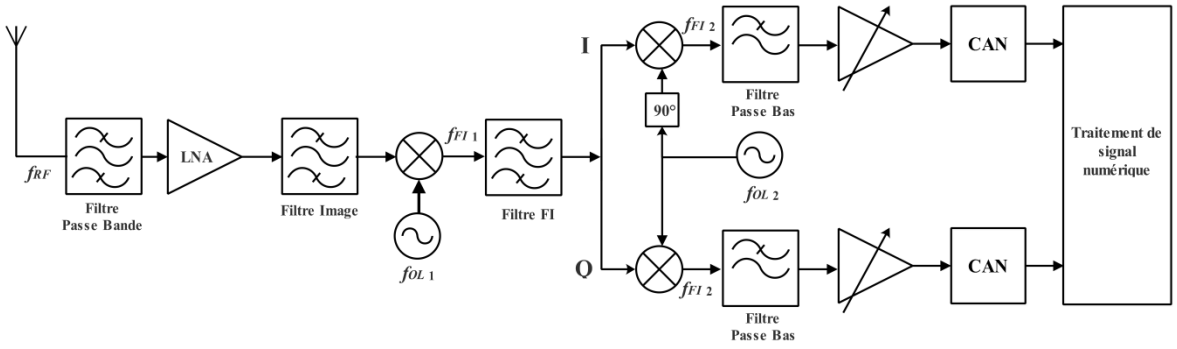



Figure 1.9: Schéma bloc d'un récepteur superhétérodyne à double changement de fréquence.

Cependant, les récepteurs hétérodynes présentent un certain nombre de problèmes substantiels en ce qui concerne leur intégration complète sur puce. Cela contraste avec les tendances actuelles dans la conception des émetteurs-récepteurs pour les appareils alimentés par batterie qui poussent vers l'adoption de radios rentables, évolutives et éco-énergétiques conçues avec les technologies CMOS numériques. Une solution simple pour augmenter le niveau d'intégration du récepteur est de transférer l'échantillonnage du signal de la bande de base aux fréquences plus élevées, et d'utiliser un CAN à haute résolution directement après le filtre passe bande de la première transposition en FI [23], comme le montre la figure 1.10.

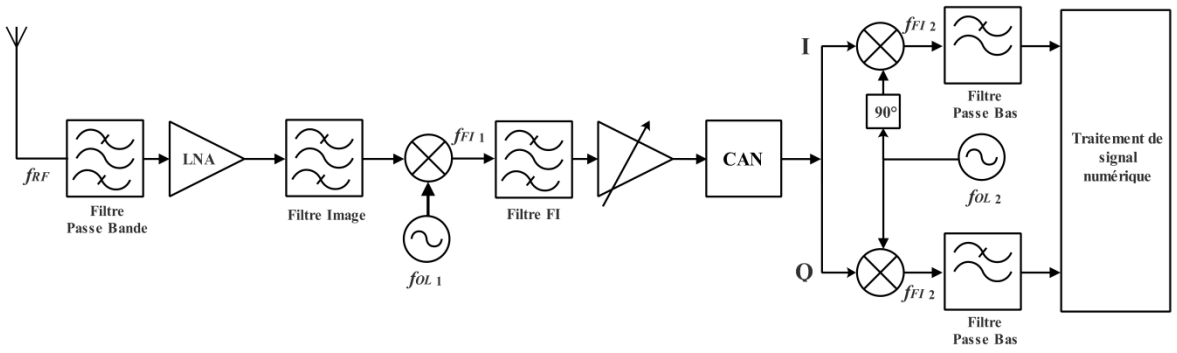



Figure 1. 10: Schéma bloc d'un récepteur superhétérodyne avec une conversion de signal en phase/quadrature dans le domaine numérique.

Le signal RF désiré est reçu à l'entrée de l'antenne avec une fréquence centrale $f_{RF}$. Ce signal passe par un filtre passe bande afin d'isoler la bande de réception pour ensuite l'amplifier par un amplificateur à faible bruit (LNA : Low Noise Amplifier). Un second filtrage du signal, avant le mélangeur, est nécessaire pour éliminer la fréquence image.

La transposition du signal est effectuée à l'aide d'un mélangeur par la multiplication du signal RF avec le signal issu de l'OL ($f_{OL}$).

$$\cos 2\pi f_{RF}t \times \cos 2\pi f_{OL}t = \frac{1}{2}\left[\cos 2\pi(f_{RF} + f_{OL})t + \cos 2\pi f_{FI}t\right] \quad (1.1)$$

Avec : $f_{FI} = f_{RF} - f_{OL}$

A la sortie du mélangeur on obtient deux signaux à fréquence centrale $f_{RF} + f_{OL}$ et $f_{FI}$. Le Filtre FI permet de garder seulement le signal désiré dont la fréquence centrale est égale à $f_{FI}$, comme le montre la figure 1.11.

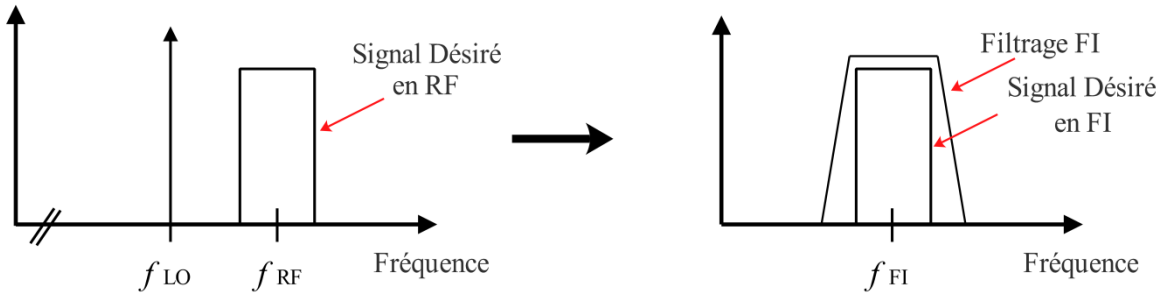



Figure 1. 11: Principe de la conversion en fréquence intermédiaire.

**b. Architecture homodyne (zero-IF)**

Le récepteur homodyne original a été développée en 1932 par une équipe de scientifiques à la recherche d'un moyen pour simplifier l'architecture hétérodyne [24]. Ce récepteur était capable de démoduler les signaux modulés en amplitude (AM) en utilisant un OL synchronisé sur la fréquence porteuse du signal utile. Le signal reçu pouvait être converti directement en bande de base. Tous les signaux indésirables pouvaient être rejetés par un filtre passe-bas. L'architecture résultante avait moins de complexité et une consommation d'énergie plus faible.

Le récepteur homodyne moderne, aussi appelé récepteurs zéro-FI ou à conversion directe en raison de l'absence de la FI ($f_{RF} - f_{LO} = 0$), n'est plus limité à la réception de signaux AM. Il est désormais capable de traiter des types de modulations plus complexes. L'architecture de ce récepteur permet un niveau d'intégration plus élevé avec une dissipation de puissance plus faible. Le synoptique d'un récepteur homodyne est illustré à la figure 1.12. Le signal RF est sélectionné par le filtre RF passe bande, puis amplifié par l'amplificateur (LNA), comme pour l'architecture superhétérodyne. Une fois filtré et amplifié, le signal est transposé directement en bande de base en utilisant un bloc IQ composé de deux mélangeurs montés en quadrature [23]. Comparé à la figure 1.10, il est évident que le nombre de composants analogiques de ce récepteur est réduit.

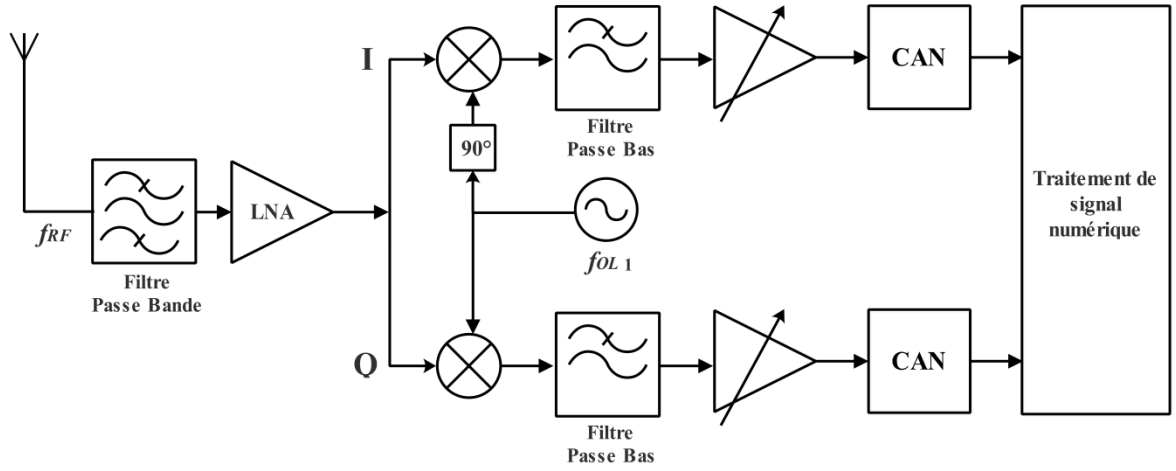



Figure 1. 12: Schéma bloc d'un récepteur à conversion directe.

Le spectre du signal RF avec une transposition directe en bande de base est illustré dans la figure 1.13. Le filtre de réjection de la fréquence image est supprimé (la fréquence image du signal RF n'existe plus) et les contraintes sur les CAN sont réduites [25].

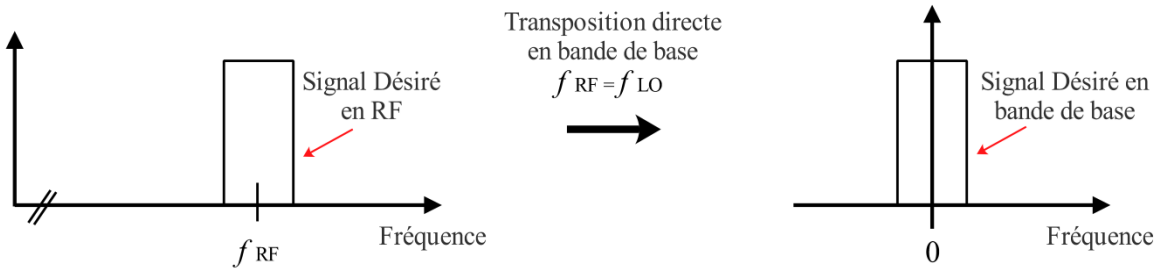



Figure 1. 13: Principe de la conversion directe.

Cependant, cette architecture souffre des problèmes suivants :

- L'isolation de l'OL et du LNA [26,27] : les fuites entres les différentes entrées du mélangeur produisent ce qu'on appelle le *DC offset* (une tension continue de décalage). Ce Problème est due aux fuites entre l'entrée RF et l'entrée de l'OL du mélangeur et vice versa (figure 1.14). Cela peut dégrader la qualité du signal en bande de base et peut saturer les étages suivants du récepteur.

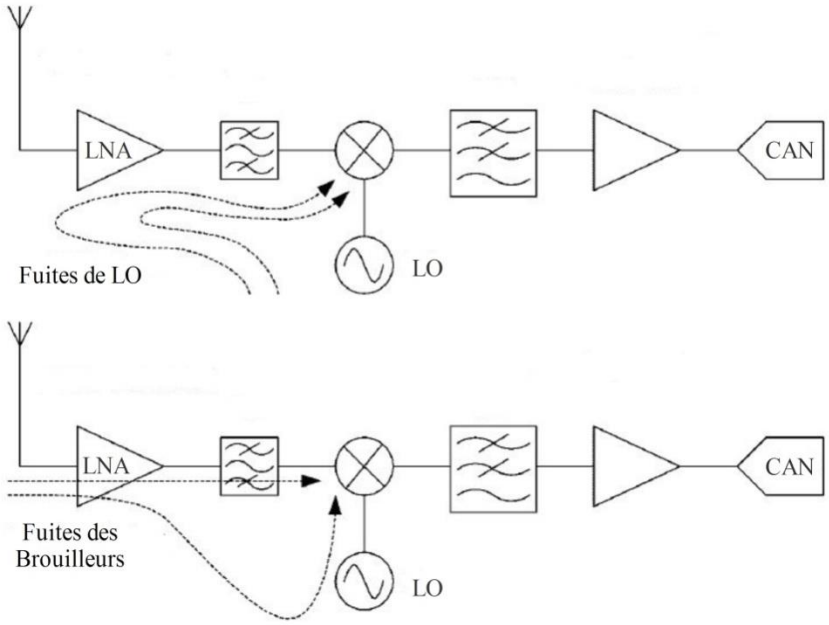



Figure 1. 14: Fuites de l'OL et du LNA [21].

- Le problème d'intermodulation d'ordre deux. En effet, supposons que les deux fréquences brouilleurs$f_1$et $f_2$ soient présentes en entrée de l'amplificateur. En sortie, on retrouve les produits d'intermodulation d'ordre deux suivants : $2f_1, 2f_2, f_1 + f_2, f_1 - f_2$. En raison des fuites entre l'entrée RF et la sortie du mélangeur le terme à la fréquence$f_1 - f_2$va se retrouver en bande de base et peut venir parasiter le signal utile [28]. Ce phénomène est illustré dans la figure 1.15.

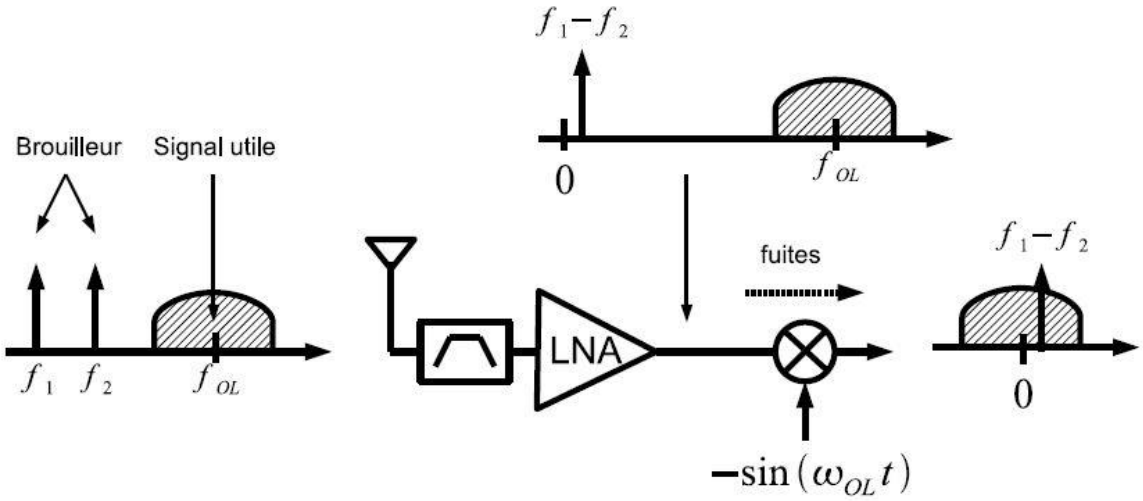



Figure 1. 15 : Effet de l'intermodulation d'ordre deux [29].

- Le problème de déséquilibre IQ. Le non-appariement entre les voies I et Q peut perturber la qualité du signal en bande de base et se traduire en une erreur de gain et de phase qui vont augmenter le taux d'erreur binaire [29]. Afin de pallier ces problèmes, de nombreuses techniques ont été proposées [30,31,32].

La flexibilité dans un récepteur à conversion directe, sa simplicité relative et son nombre minimal de composants en font l'une des architectures les plus populaires pour les récepteurs multistandard [23].

### c. Architecture à sous échantillonnage

Une autre technique de translation en basses fréquences des signaux RF appelée sous-échantillonnage (Bandpass Sampling), peut être réalisée par sous-échantillonnage du signal d'entrée RF sans avoir besoin de mélangeurs (figure 1.17).

Le principe de cette technique est d'échantillonner le signal RF en utilisant une fréquence d'échantillonnage $f_{se}$ (appelée fréquence de sous échantillonnage) plus basse que la fréquence maximale ($f_{max}$) du signal d'entrée (le théorème de Nyquist-Shannon ($f_{se} > 2f_{max}$) n'est pas respecté). La figure 1.16 montre cette technique pour un signal RF borné entre la fréquence minimale $f_L$ et la fréquence maximale $f_H$, échantillonné à une fréquence $f_s$. Dans le domaine des fréquences, le sous-échantillonnage donne plusieurs copies du signal utile non superposées et répétées autour des multiples de $f_{se}$ Parmi ces répliques, seulement celle située en bande de base nous intéresse. Un filtre passe bas permet de récupérer le signal désiré [23,28].

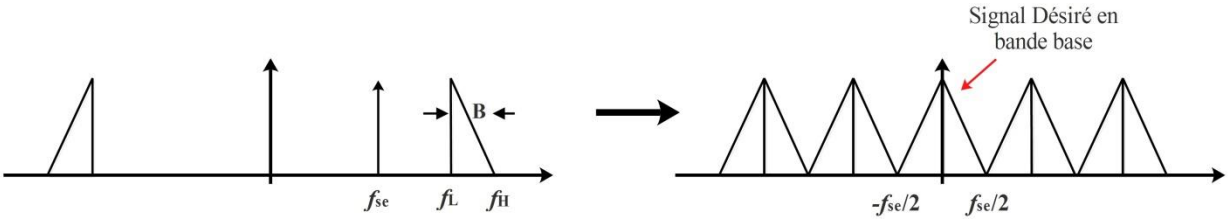



Figure 1. 16: Principe de la technique de sous-échantillonnage.

L'équation 1.2 donne les fréquences auxquelles les copies du signal sont situées dans le spectre [33]:

$$f_{img} = n\, f_{se} \pm f_{RF} \qquad (1.2)$$

Avec

- $f_{img}$ : la fréquence de réplique du signal,
- $n$ : un nombre entier.

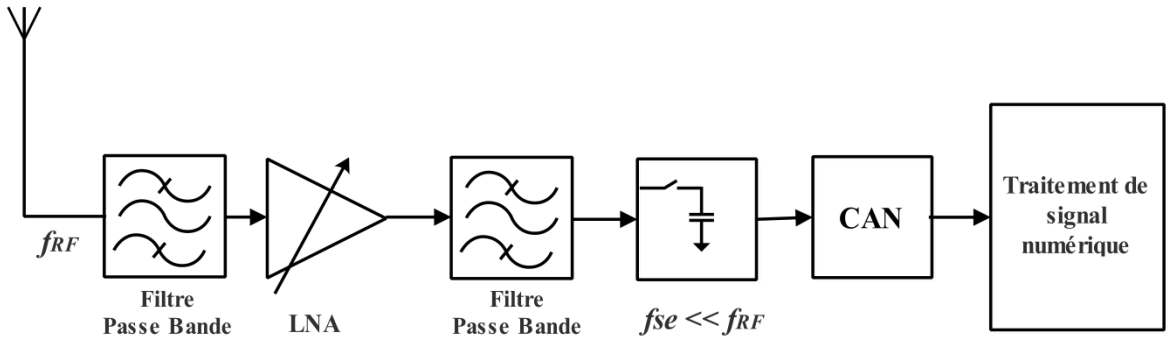



Figure 1.17 : Schéma bloc d'un récepteur à sous-échantillonnage.

L'avantage de cette architecture réside dans sa simplicité. Cependant, cette solution comporte des inconvénients [34]:

- Le filtre analogique doit être très sélectif pour isoler la bande du système et éliminer les brouilleurs éventuels ;
- La dégradation du rapport signal sur bruit (SNR, Signal to noise ratio) à cause d'une faible atténuation des signaux hors bande ;
- Le bruit introduit par la gigue des échantillonneurs.

Dans le domaine de la radio logicielle, cette technique a été de nombreuses fois utilisée [35,36]. C'est la solution la plus proche de la SWR puisqu'elle consiste à numériser le signal le plus proche possible de l'antenne.

## 1.5 Conclusion

Dans ce premier chapitre, un état de l'art des systèmes radio logicielle a été présenté. Nous avons introduit l'émergence et le concept des systèmes radio logicielle, ensuite les défis qui rendent la conception d'une SWR difficile. Et finalement, nous avons présenté les différentes architectures pour RLR. En effet, ces dernières décennies, les réseaux sans fil ont continué à se développer et progressent rapidement et leurs utilisations a considérablement augmenté, avec un nombre important des standards de communication. Remplacer des étages matériels par d'autres étages complètements à base de logiciels permet d'introduire la reconfiguration facile qui permet de combiner différents standards de communications. Nous avons mis le point sur le fait que la radio logicielle permet de mettre en œuvre dans une seule plateforme plusieurs solutions. Les systèmes radio actuels et futurs s'imposent sous une version basée sur le logiciel. Cette migration a permis la création d'une multitude de solutions, nous aborderons quelques-unes d'entre elles dans le chapitre suivant.

# Chapitre 2

# Plateformes Radio Logicielle

## 2.1 Introduction

Récemment, des progrès considérables ont été réalisés dans la recherche et le développement de la radio logicielle. La disponibilité de plates-formes sans fil programmables permettant aux chercheurs de créer des radios logicielles, telles que Universal Software Radio Peripheral (USRP), d'Ettus Research LLC et autres plateformes commerciales actuellement largement disponibles. Certaines de ces plateformes sont conçues uniquement pour la réception. Elles peuvent être à bas prix (environs 2000 DZD), comme pour la clé RTL-SDR (Realtek Software Defined Radio). D'autres sont conçues pour l'émission et la réception avec des prix qui dépassent généralement les 40000 DZD. Le tableau 2.1 présente une liste non exhaustive des plateformes SDR avec leurs principales caractéristiques [37].

| ***Nom*** | ***Fréquence Minimale. (MHz)*** | ***Fréquence Maximale (MHz)*** | ***Bande Passante (MHz)*** | ***Résolution du Convertisseur (Bits)*** | ***Transmission*** | ***Prix (DZD)*** |
|---|---|---|---|---|---|---|
| RTL-SDR | 24 | 1766 | 3.2 | 8 | Non | ~2000 |
| Airspy mini | 24 | 1750 | 6 | 12 | Non | ~ 14000 |
| SDRPlay RSP1A | 0.001 | 2000 | 10 | 14 | Non | ~2700 |
| Funcube Pro+ | 0.15 | 2050 | 0.192 | 16 | Non | ~27000 |
| HackRF One | 1 | 6000 | 20 | 8 | Oui | ~40000 |
| BladeRF | 300 | 3800 | 28 | 12 | Oui | ~56000-88000 |
| USRP B200/B210 | 70 | 6000 | 56 | 12 | Oui | ~220000-260000 |
| MatchStiq | 300 | 3800 | 28 | 12 | Oui | ~600000 |

Tableau 2. 1: Différentes plateformes SDR.

Ces plateformes sont différentes en termes de: flexibilité, rapidité de calcul, bande passante, etc. La clé RTL-SDR a été commercialisée au début de l'année 2013. Elle peut être utilisée comme récepteur, via un PC ce qui permet d'analyser et de démoduler plusieurs types de signaux appartenant à la gamme des fréquences allant de 24MHz à 1.76 GHz. Dans ce chapitre, nous abordons quelques plateformes SDR émettrices et réceptrices utilisée dans le domaine de la recherche, notre intérêt est orienté vers le récepteur RTL-SDR que nous allons traiter en détail.

## 2.2 USRP

L'USRP est la plateforme SDR la plus connue de la communauté des développeurs et chercheurs. Elle permet de concevoir et de mettre en œuvre rapidement des systèmes radio logiciels puissants et flexibles. Cette plateforme est conçue par Ettus Research LLC. Son coût peut atteindre les 1360000DZD [38,39].

Cette plateforme est totalement open source : l'architecture, les schémas, les firmwares, les codes sources FPGA, etc. Elle est combinée avec un logiciel gratuit & open source à l'image de GNU Radio, elle permet alors de travailler comme terminal émetteur récepteur totalement libre. La figure 2.1 illustre le schéma bloc de la plateforme USRP. Son cœur est constitué d'une FPGA communicant avec deux cartes filles émettrices (deux émetteurs : Tx) et deux cartes fille réceptrices (deux récepteurs : Rx) à travers des CAN et CNA, et un port de communication pour l'interfacer avec un PC.

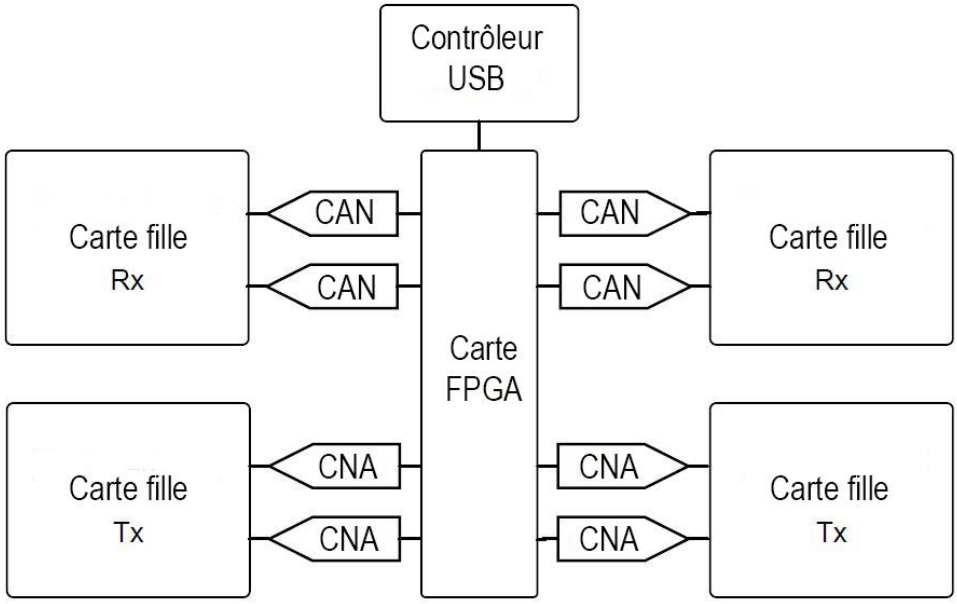



Figure 2. 1: Architecture simplifiée de la carte USRP [4].

Les cartes filles traitent les opérations analogiques telles que le filtrage et les conversions de fréquences. Diverses cartes filles sont vendues séparément par Ettus Research, la gamme de fréquence dépend de la carte fille utilisée et peuvent traiter des applications fonctionnant jusqu'à 6 GHz [41].

La carte FPGA, en fonction de la série USRP, gère quelques opérations liée au traitement du signal et la majorité des opérations sont assurées sur un système hôte par exemple un ordinateur, via une connexion USB ou Gigabit Ethernet. Ces plates-formes peuvent être facilement reconfigurées pour divers utilisations.

L'USRP communique avec l'ordinateur hôte à l'aide du pilote spéciale (USRP Hardware Driver, UHD). En outre, il est supporté par une multitude de systèmes d'exploitation à l'image de Windows, UNIX et Mac OS X. En outre, l'UHD fonctionne avec de nombreux logiciels tiers (Third-party software) telles que GNU Radio, Labview, Simulink et Open BTS.

## 2.3 Kansas University Agile Radio (KUAR)

La plateforme KUAR (Kansas University Agile Radio) est une autre plateforme similaire à l'USRP. Comme illustré dans la figure 2.2, la KUAR se compose de cinq sous-systèmes principaux : une alimentation, processeur de contrôle (Control processor host, CPH), une carte numérique avec un processeur dédié au traitement du signal DSP (Digital Signal Processing), des CAN et CNA. Un front-end RF pour l'émission et la réception et des antennes actives avec des connecteurs SMA (Sub Miniature version A) qui permettent l'utilisation d'une variété d'antennes commerciales et de prototypes. La gamme de fréquence est de 5250 à 5850 MHz et la bande passante de 30 MHz. La plate-forme a été conçue pour être alimentée par batterie, permettant ainsi un fonctionnement sans connexion avec une source d'alimentation externe.

Le CPH du KUAR est un PC intégré qui contient un processeur à usage général (GPP, General Purpose Processor) Pentium à 1,4 GHz, une mémoire vive (SDRAM, Synchronous Dynamic Random Access Memory) à 1 GB et une mémoire de stockage de 8 GB. Il se connecte à la carte de traitement numérique via une connexion PCI Express. Le CPH exécute Linux et fournit des connexions USB 2.0, VGA, PCI Express et Gigabit Ethernet (10/100/1000 Mbps) [42].

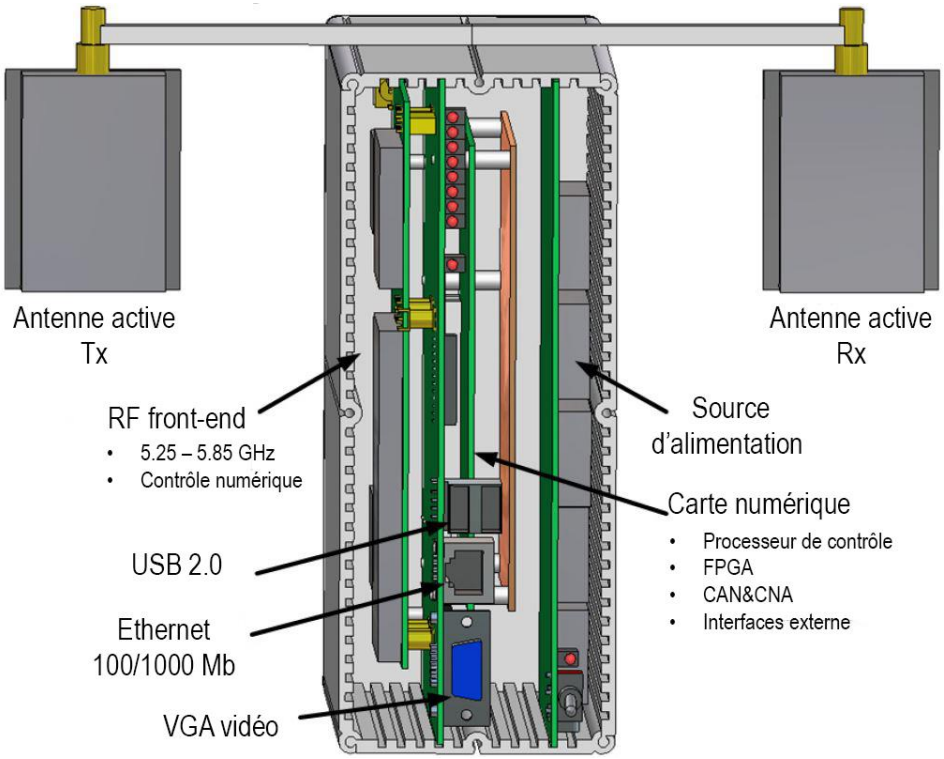



Figure 2. 2: Les composants de la carte KUAR [42].

La majorité des opérations des composants dédiés à la communication numérique et les traitements du signal numérique sont effectuées sur une FPGA (field-programmable gatearray) de type XilinxVirtex II Pro, qui possède 30816 cellules logiques, deux microprocesseurs PowerPC 405 et fonctionne jusqu'à 350 MHz.

Le principal avantage de cette plate-forme est le degré de flexibilité qu'elle offre. Les développeurs ont la possibilité d'implémenter des standards de communication selon trois méthodes différentes :

- Le système de modulation : BPSK, QPSK, etc, est entièrement implémenté dans le FPGA peu de tâches sont attribuées au GPP de l'hôte,
- Une implémentation logicielle complète entièrement mis en œuvre sur le GPP avec une implication minimale du FPGA,
- une implémentation hybride, où le développeur peut partitionner la conception de la manière qui correspond à ses critères. Ici, les deux microprocesseurs PowerPC peuvent être utilisés comme des processeurs à usage général. Ces microprocesseurs peuvent exécuter des logiciels de la même manière que le CPH.

## 2.4 Small Form Factor (SFF SDR)

La plateforme SDR SFF (Small Form Factor**)** était l'une des premières plateformes de développement embarquées pour la radio logiciel. Elle a été conçue autour des dernières technologies DSP (Digital signal processor) et FPGA en tant que solution de développement matériel et logiciel intégrée et moins chère.

Cette plateforme se compose de trois modules comme le montre la figure 2.3:

- Le module de traitement numérique (MTN) est la couche de traitement du signal avec une combinaison GPP / DSP en plus d'un FPGA.
- Le module de conversion de données (MCD) est la couche intermédiaire est équipé d'un FPGA supplémentaire, ainsi que deux CAN et deux CNA. Les CAN ont une fréquence d'échantillonnage maximale de 125 MHz et une résolution de 14 bits. Dans le chemin d'émission les CNA ont une résolution de 16 bits à une fréquence d'émission borné par 500 MHz au maximum [43].
- Le module radiofréquence (MRF) est le front-end RF, ce module constitué de deux étages utilisés conjointement. Un étage RF accordable qui convertit les signaux entre 200 MHz et 1 GHz en une fréquence intermédiaire de 30 MHz, il est équipé de cinq filtres analogiques et de trois oscillateurs locaux. Le second étage implémente la norme WiMAX RF (Worldwide Interoperability for Microwave Access) module avec une gamme de fréquence comprise entre 2,3 GHz et 2,7 GHz [44].

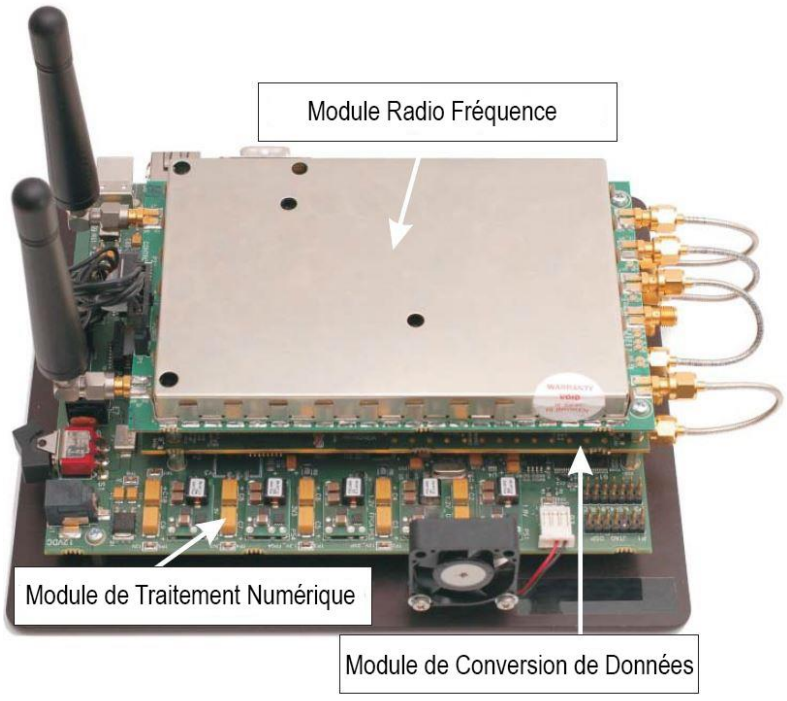



Figure 2. 3: La plate-forme SDR SFF [44].

## 2.5 NUAND BladeRF

La carte NUAND BladeRF est une carte SDR open source avec une interface USB 3.0, la Figure 2.4. Il contient un microprocesseur ARM A-9, un FPGA Altera Cyclone-4 et un émetteur-récepteur RF LMS6002D [45]. Cette carte est capable de fonctionner en mode MIMO (multiple-input and multiple-output). La plate-forme fonctionne sous Linux, Windows, Mac et aussi elle supporte le logiciel GNURadio. Cette carte peut être alimentée par USB et possède une mémoire SRAM (Static random-access memory) intégrée de 512 MB [46].

Le bladeRF peut être configuré pour fonctionner comme un modem RF personnalisé, une picocellule GSM et LTE, un récepteur GPS, etc, sans avoir besoin de cartes d'extension. Avec un prix de ~77000 DZD, il s'agit d'une solution rentable qui contient tous les éléments d'un système de communication radiofréquence.

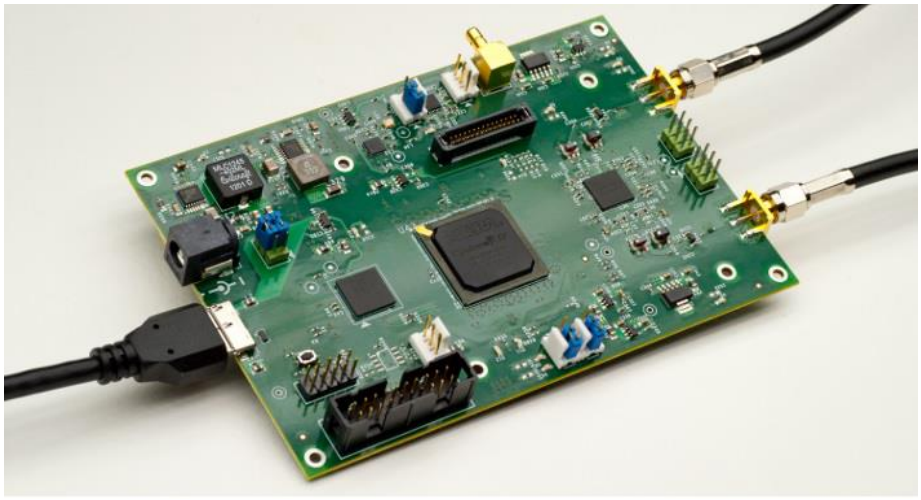


Figure 2. 4 : La plateforme BladeRF [47].

La carte bladeRF possède les caractéristiques suivantes :

- une gamme de fréquence de 300MHz – 3.8GHz,
- CAN et CNA haute performance intégrés avec une fréquence d'échantillonnage de 40MSPS, et une résolution de 12 bits,
- Jusqu'à 28 MHz de bande passante instantanée,
- Oscillateur VCTCXO (Voltage Controlled Temperature Compensated Crystal Oscillators) avec une tolérance de 1 PPM,
- USB 3.0 interface à haute vitesse.

## 2.6 Récepteur SDR à faible coût RTL-SDR

### 2.6.1 Présentation de la clé RTL-SDR

A l'origine, ces appareils étaient conçus pour être utilisés comme des récepteurs DVB-T (Digital Video Broadcast-Terrestrial). Basés sur la puce Realtek RTL2832 dont la fonction principale est la démodulation DVB (Digital Video Broadcast) et d'envoyer les trames vidéo MPEG (The Moving Picture Experts Group) à travers un simple port USB. Le flux ainsi construit peut être affiché facilement sur un PC. Cependant, en 2012, grâce aux efforts combinés de Antti Palosaari, Eric Fry et l'équipe Osmocom, il a été découvert que le RTL-SDR peut être utilisées comme une solution SDR générique, uniquement pour la réception. Le principe consiste à faire basculer le fonctionnement de la puce Realtek RTL2832 dans un mode où elle émettrait des échantillons I/Q vers le port USB. Ceci ouvre les perspectives d'un traitement numérique dans un ordinateur hôte. Ils ont également trouvé des commandes pour ajuster la fréquence centrale utilisée pour la réception, ainsi que la fréquence d'échantillonnage. Par conséquent, contrôler avec précision ce type de périphériques [48]. À partir de là, une communauté s'est formée, pour développer l'infrastructure logicielle dédiée SDR et des fabricants ont commencé à produire des clés (ou Dongles) plus adaptés aux applications SDR, avec le nom RTL-SDR.

Ces clés capables de recevoir des signaux dans la plage sur laquelle leur tuner (RF front-end) fonctionne, comprenant des différentes fréquences de la bande VHF et UHF, sauf que leurs capacité dépasse la bande des signaux de télévision numérique qu'ils étaient conçus pour recevoir initialement. La plage ou la gamme de fréquence de ces clés varie d'une à l'autre en fonction des composants utilisés, mais se situe généralement entre 24 MHz et 1,76 GHz. Bien sûr, les performances de ces clés ne correspondent pas à un SDR professionnel, mais elles fonctionnent extrêmement bien comparativement avec leur prix.


Figure 2. 5: La clé RTL-SDR avec une antenne omnidirectionnelle.

Particulièrement dans ce mode SDR large bande, cette clé USB donnera la possibilité de réaliser de nombreux projets intéressants, parmi ces applications on peut citer [49]:

- L'écoute des conversations non cryptées des ambulances, des pompiers...
- L'écoute des conversations du contrôle de la circulation aérienne.
- Le suivi des positions d'avions comme un radar avec le décodage ADSB.
- Le décodage ACARS des avions.
- Décodage non cryptés des transmissions vocales numériques.
- L'écoute de la radio amateur sur SSB avec une modulation LSB / USB.
- Le suivi de positionnement d'un bateau comme un radar avec le décodage AIS.
- Le suivi et la réception des données météo des ballons d'agences météorologiques.
- Le suivi d'un ballon lancé à haute altitude.
- L'écoute du radioamateur en UHF-VHF.
- Le décodage radioamateurs des signaux APRS.
- Regarder la TV analogique.
- Décoder les signaux GSM.
- Utilisation RTL-SDR avec les appareils Android comme scanner radio portable.
- Recevoir des signaux GPS et les décoder.
- Utilisation RTL-SDR comme un simple analyseur de spectre.

- Recevoir les images NOAA des satellites météorologiques.
- L'écoute de satellites et l'ISS.
- La radioastronomie.
- L'écoute des radios FM, et le décodage des informations RDS.
- Écoute des radios diffusés en DAB.
- Recevoir la Radio Numérique Mondiale (DRM)
- L'écoute de la Radio internationale à ondes courtes.

Depuis sa première apparition, plusieurs générations ont été développées pour la clé RTL-SDR. Les générations se distinguent par le tuner utilisé (Tableau 2.2), et le connecteur d'antenne MCX (Micro Coaxial Connector), PAL (Belling-Lee Connector) ou SMA (Sub Miniature Version A), et aussi le type de l'oscillateur local utilisé [50]. Ces dispositifs, qui exploitent le principe de la radio logicielle restreinte, sont divisés en deux parties. Une partie analogique, il s'agit du tuner ou le front-end pour effectuer les traitements du signal analogique avec la puce Realtek RTL2832U pour numériser et convertir le signal numérique en bande base et l'envoyer au PC hôte pour des traitements de signal additionnel (démodulation, filtrage…). Les clés RTL-SDR les plus communes utilisent le tuner Raphael Micro R820T ou R820T2. Tout au long de cette thèse on va utiliser ce type de clés (combinaison R820T2/RTL2832U), la figure 2.6 montre les principaux composants internes de cette clé.

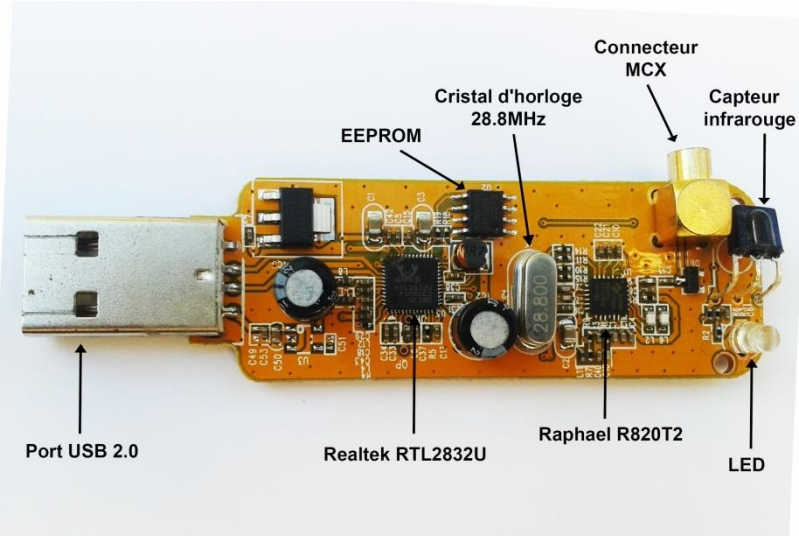



Figure 2. 6: Les composants internes de la clé RTL-SDR (R820T2/ RTL2832U).

- **Capteur infrarouge (IR)**:utilisé pour s'interfacer la clé avec une télécommande.
- **Connecteur MCX** : pour attacher l'antenne avec la clé RTL-SDR.
- **Cristal d'horloge 28.8MHz** : utilisé pour la génération du signal de référence à l'oscillateur local et à l'horloge.
- **La mémoire EEPROM** (mémoire morte effaçable électriquement et programmable): garde les informations de configuration USB pour la clé, cette mémoire est connecté au Realtek RTL2832U via un bus $I^2C$.
- **Raphael R820T2**: le tuner, qui est responsable au traitement analogique du signal.
- **Realtek RTL2832U** : la puce qui est responsable au traitement numérique du signal.
- **Port USB 2.0** (Bus Universel en Série) : utilisé pour transférer les données I/Q à la station de traitement hôte.

### 2.6.2 Les caractéristiques de la clé RTL-SDR

La clé RTL-SDR est basée sur la puce RTL2832 de chez Realtek qui contient un convertisseur analogique-numérique, un USB *datapump* pour transférer les échantillons bruts I (In-phase) et Q (Quadrature) codé sur 8 bits avec une fréquence d'échantillonnage maximale de 3.2Mhz. Néanmoins, la clé RTL-SDR est instable avec la fréquence maximale qui engendre une perte des échantillons. Nous avons trouvé que la meilleure fréquence d'échantillonnage qui permet d'éviter les pertes et assure une stabilité de la clé est de 2.4MHz. Pour la réception, la gamme de fréquence varie et dépond du tuner utilisé. Il en existe plusieurs types, dans le tableau 2.2 les différents tuners avec leur gamme de fréquence sont présentés [51].

Étant donné que les clés RTL-SDR sont conçues pour être utilisées pour la réception des signaux de la télévision, elles ont toutes une impédance d'entrée de 75 Ohms [52]. Cependant, les nouvelles clés RTL-SDR sont fournies avec des connecteurs SMA de 50 ohms.

| *Tuner* | *Game de Fréquence* |
|---|---|
| Elonics E4000 | 52 - 2200 MHz avec un écart de 1100 MHz à 1250 MHz (variable) |
| Rafael Micro R820T | 24 - 1766 MHz |
| Fitipower FC0013 | 22 - 1100 MHz |
| Fitipower FC0012 | 22 - 948.6 MHz |
| FCI FC2580 | 146 - 308 MHz et 438 - 924 MHz |

Tableau 2. 2: Les différents tuners de la clé RTL-SDR.

### 2.6.3 Architecture de la clé RTL-SDR

La clé RTL-SDR comprend une section analogique : antennes, amplificateurs et filtres. La partie analogique est implémentée par le tuner radio Raphael R820T2. La section numérique combinant le convertisseur analogique-numérique, et le port USB par le circuit Realtek RTL2832U. La figure 2.7 montre le schéma block de la clé RTL-SDR, Les processus de traitement du signal sont effectués en deux étapes : la transposition radio fréquence (RF) vers une fréquence intermédiaire (FI) dans l'étage analogique. Par la suite, la conversion de la fréquence intermédiaire en bande de base dans le domaine numérique.

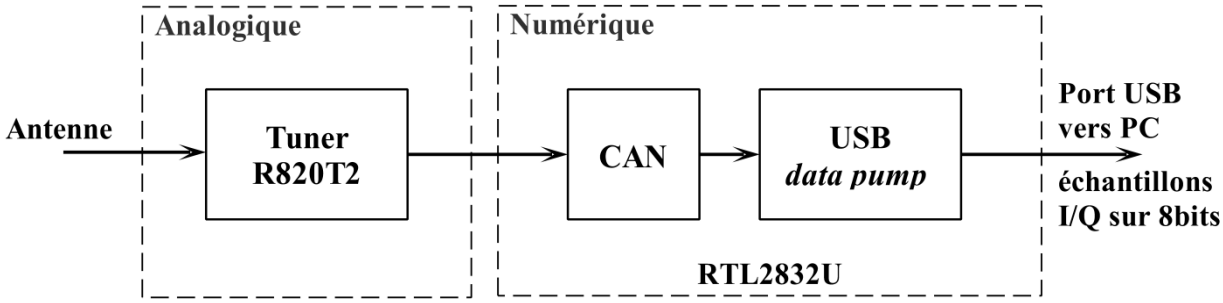



Figure 2. 7: Schéma block de la clé RTL-SDR.

Le circuit radio fréquence Raphael R820T2 est responsable des traitements analogiques. Le signal RF provenant de l'antenne passe par un amplificateur à faible bruit (Low Noise Amplifier LNA) avec un facteur de bruit de <4,5 dB. Par la suite un filtrage de rejection d'image est appliqué. En fin, une transposition de fréquence est réalisée, à l'aide d'un oscillateur commandé en tension (VCO), vers une fréquence intermédiaire de 3.57MHz. Le VCO est contrôlé par le RTL2832U via une interface $I^2C$ (Inter Integrated Circuit). Le signal à la sortie du mélangeur passe par un filtre passe bande FI, pour éliminer les composants en haute fréquences et conserver juste le signal occupant la fréquence intermédiaire. Le contrôle du gain est également fourni pour LNA et l'amplificateur à gain variable (VGA, Variable Gain Amplifier) [53].

Le signal issu de tuner Raphael R820T2 est injecté à l'entrée du Realtek RTL2832U qui contient un convertisseur CAN avec une fréquence d'échantillonnage de 28.8MHz. Le signal FI est numérisé par le CAN et transposé en bande de base à l'aide d'un oscillateur à contrôle numérique (NCO, Numerically Controlled Oscillator), puis un processus de décimation est effectué pour réduire le taux d'échantillonnage à une valeur inférieure, par ex. à 2.4MHz. Des échantillons en phase et en quadrature I/Q sont alors envoyés à la station de traitement à travers le port USB. Le signal que le PC reçoit a une largeur de bande de 2,4 MHz. La figure 2.8 montre l'architecture de la clé RTL-SDR avec les principales étapes de traitement du signal.

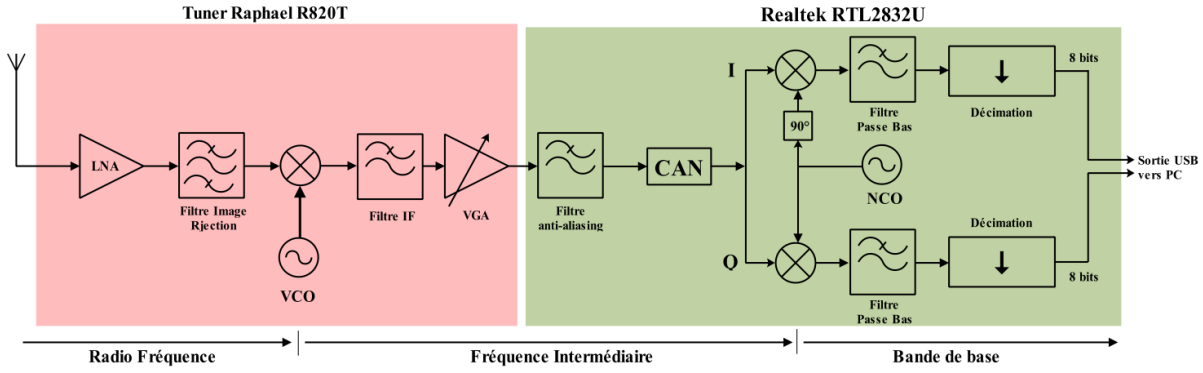



Figure 2. 8: L'architecture interne de la clé RTL-SDR (R820T/RTL2832U).

### 2.6.4 Exemple d'utilisation

Pour comprendre le principe de fonctionnement de la clé RTL-SDR, nous expliquerons comment recevoir la station FM radio Aïn Témouchent centrée autour de la fréquence 95,9MHz. En premier il faut définir la fréquence centrale de la clé RTL-SDR sur 95,9 MHz. Le signal FM serait converti par le tuner R820T2 de RF à la fréquence intermédiaire $f_{IF} = 3.57MHz$, en utilisant un mélangeur et un oscillateur local avec une fréquence $f_{LO} = f_{RF} - f_{IF}$ , Un modèle simple pour le signal FM d'entrée, $(t) = \cos 2\pi f_{RF} t$ , multiplié par le signal de l'oscillateur local $s(t) = \cos 2\pi f_{LO} t$, avec $f_{LO} = 95.9 - 3.57 = 92.33$ MHz . Alors la sortie du mélangeur doit être :

$$r(t) \times s(t) = \frac{1}{2}[\cos 2\pi(f_{RF} + f_{LO})t + \cos 2\pi(f_{RF} - f_{LO})t] \quad (2.1)$$

$$r(t) \times s(t) = \frac{1}{2}[\cos 2\pi(199.23 \cdot 10^6)t + \cos 2\pi(3.57 \cdot 10^6)t] \quad (2.2)$$

Le composant à 199.23MHz est atténué par le filtre FI du R820T2 et seul le signal en fréquence intermédiaire est passé à l'étape suivante, où le signal sera échantillonné à 28,8 MHz par le RTL2832U, et émis en tant que signal I/Q en bande de base vers l'ordinateur. À ce point-là, le signal serait toujours modulé en FM (en bande de base) et devrait être

démodulé afin de récupérer le signal audio. Les processus de démodulation sont effectués au niveau de la station de traitement. La figure 2.9 montre les étapes de transposition de fréquence appliquées sur le signal dans le domaine fréquentiel.

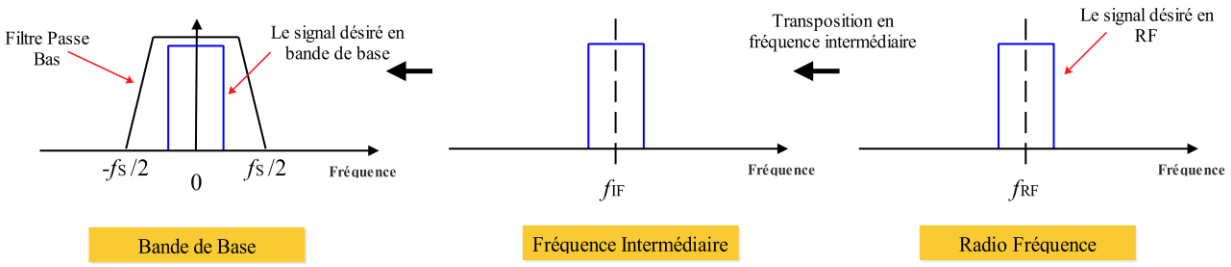



Figure 2. 9: La transposition de fréquence réalisée dans la clé RTL-SDR.

### 2.6.5 L'erreur de fréquence dans la clé RTL-SDR

Comme tous les dispositifs physiques, les émetteurs-récepteurs radios ont un degré d'imprécision. Les oscillateurs à cristal sont souvent construits avec une tolérance mesurable, exprimées en PPM (Parts Per Million), qui peuvent varier d'un appareil à l'autre en raison de l'imprécision de fabrication et / ou de la température.

Une grande tolérance peut signifier que la fréquence reçue peut ne pas correspondre exactement à la fréquence à laquelle vous vous attendez. Vous pouvez constater que la fréquence sera toujours décalée de quelques kilohertz (le canal reçu n'est pas centré sur la fréquence de réception). L'oscillateur local (OL) dans les clés RTL-SDR peut atteindre un décalage en fréquence jusqu'à ± 150 PPM ou plus. Certaines clés RTLSDR sont désormais dotées des oscillateurs améliorés avec des tolérances plus faibles, comme les oscillateurs TCXO (Temperature compensated crystal oscillator). Pour atténuer cette imperfection du matériel, Il existe des outils d'évaluation du décalage de fréquence de OL qui permet aux utilisateurs des clés RTL-SDR de déterminer le décalage de fréquence de leurs dispositifs sans avoir à acquérir du matériel de laboratoire supplémentaire et cher. Les quatre outils populaires qui sont utilisés pour estimer le décalage de fréquence de OL sont : Kalibrate-rtl [54], rtl_test[55], LTE-Cell-Scanner[56], LTESS-track[57].

Nous avons développé notre propre solution sous MATLAB pour estimer l'erreur de fréquence de OL de la clé RTL-SDR, la méthode utilisé est la même de celle utilisé dans l'outil Kalibrate-rtl, est basé sur les signaux GSM, nous expliquons par la suite en détail cette méthode. L'outil rtl_test est basé sur une approche simple consiste à compter les échantillons fournit par la clé RTL-SDR et les comparer avec le taux d'échantillonnage nominal. Les outils LTE-Cell-Scanner et LTESS-track basés sur les signaux LTE comme référence qui ne sont pas disponible en Algérie dans la gamme de fonctionnement de la clé RTL-SDR.

### 2.6.5.1 Description d'algorithme de correction

Dans un système de radiocommunication mobile cellulaire GSM (Globale system for mobile communication), il existe un signal de référence. Ce signal permet au mobile de détecter la présence d'un réseau (services GSM), de choisir la meilleure station de base, de connaître le paramétrage local du système et de se synchroniser dans le temps et la fréquence. Ce signal est appelé la voie balise qui est émise à une puissance maximale constante, vous retrouvez plus d'information sur le système GSM dans l'annexe C.

Les réseaux GSM utilise une combinaison de FDMA et de TDMA. La station mobile doit donc se synchroniser en fréquence et en temps. Pour ce faire, elle utilise le burst de correction de fréquence et le burst de synchronisation respectivement. La station de base transmet le burst de correction de fréquence sur le canal FCCH (Frequency Correction Channel) dans des positions régulières, ce burst est envoyé toutes les 46.15 ms et présente seulement sur le slot 0 de la voie balise dans les trames 0, 10, 20, 30 et 40 d'une multitrame à 51 trames comme le montre dans la figure 2.10 [58].

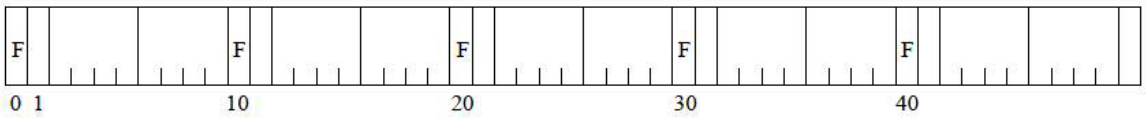
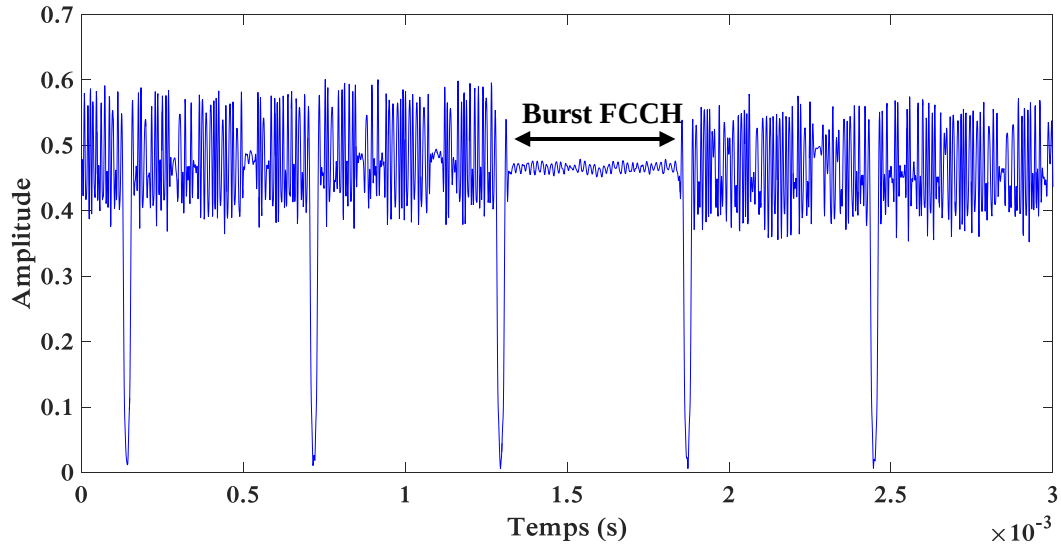


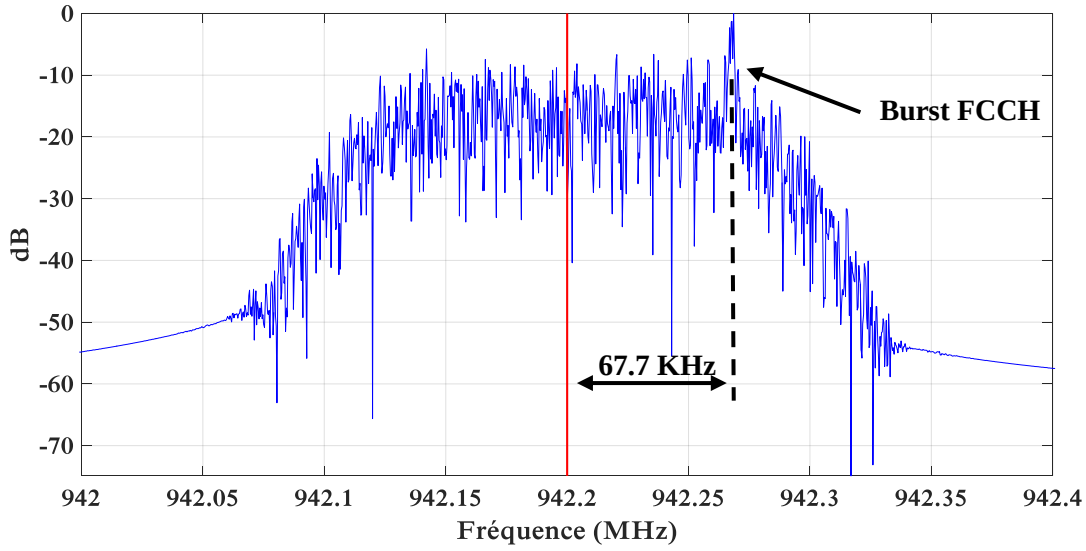

Figure 2. 10: Le burst FCCH dans la multiframe-51.

Le burst FCCH dans le système GSM est composé de 142 zéros consécutifs qui avec la modulation GMSK, produit une onde sinusoïdale continue d'environ 67.7 KHz au-dessus de la fréquence centrale de signal RF. La figure 2.11 représente le burst FCCH dans le signal GSM capté par la clé RTL-SDR dans le domaine temporel et dans le domaine fréquentiel.

$$f_{FCCH} = f_{RF} + 67.7KHz \qquad (2.3)$$




(a)




(b)

Figure 2. 11: Le signal GSM capté par la clé RTL-SDR sur la fréquence 942.2MHz. (a) la représentation temporel, (b) la représentation fréquentiel.

La détection de la position du burst FCCH dans le signal reçu permet de déterminer à quelle fréquence il se trouve, afin de pouvoir calculer le décalage à partir de 67.7 KHz. Le pic le plus élevé dans le spectre de signal reçu correspond à la fréquence détectée de ce burst

comme le montre dans la figure 2.11(b). Ce pic est ensuite utilisé pour déterminer le décalage de fréquence où :

$$\Delta f = 67.7KHz - f_{fd} \quad (2.4)$$

Avec $\Delta f$ est le décalage où la fréquence d'erreur, et $f_{fd}$c'est la fréquence du burst FCCH détecté dans le signal GSM reçu.

Il existe plusieurs méthodes pour détecter le burst FCCH [59]. La méthode utilisé dans notre script MATLAB est de trouver la différence de phase entre chaque paire d'échantillons, et puisque le burst FCCH est une onde sinusoïdale continue, la différence de phase doit être constante [60].

Mathématiquement, nous considérons $N_1$ et $N_2$ , deux échantillons complexes consécutifs :

$$N_1 = A_1 e^{j\theta_1} \quad (2.5)$$

$$N_2 = A_2 e^{j\theta_2} \quad (2.6)$$

Pour calculer la différence de phase entre $N_1$ et $N_2$ , nous multiplions $N_1$ par le conjugué de $N_2$ :

$$N_1 \times \overline{N_2} = A_1 A_2 e^{j(\theta_1 - \theta_2)} \quad (2.7)$$

La figure 2.12 montre la différence de phase du signal GSM capté par la clé RTL-SDR qui contient un burst FCCH.

Pour localiser le début du burst FCCH, nous faisons une boucle pour parcourir tout le vecteur de phase de différence calculé, avec une fenêtre (Window) de langueur de :

$$w = \frac{142\ bit \times fréquence\ d'échantillonage}{Débit\ binaire} \quad (2.8)$$

Avec le débit binaire d'un canal GSM est 270.833 kbps.

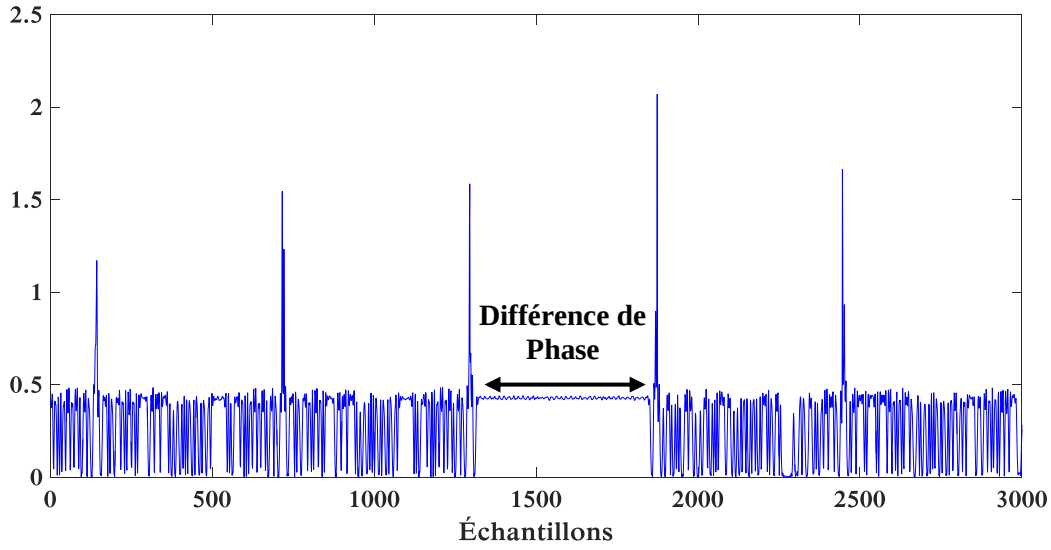



Figure 2. 12: La différence de phase du signal GSM capté par la clé RTL-SDR sur la fréquence 942.2MHz.

À chaque itération de la boucle, la fenêtre se déplace avec une position dans le vecteur de phase de différence et la différence entre les valeurs maximale et minimale est calculée, cela nous donne un nouveau vecteur, si la valeur minimale de ce vecteur est inférieure au seuil prédéfinit, ce sera donc l'emplacement du burst FCCH. Une fois que nous avons l'emplacement du burst FCCH, nous devons déterminer à quelle fréquence il se trouve afin de pouvoir calculer le décalage à partir de 67.7KHz. Dans notre solution MATLAB la valeur finale de décalage est calculée à partir de la moyenne de plusieurs mesures.

### 2.6.5.2 Evaluation de notre application MATLAB

Nous avons testé notre application MATLAB avec deux modèles populaire des clés RTL-SDR, le premier avec TCXO (figure 2.13(a)) et le deuxième non-TCXO (figures 2.13(b)). Et nous avons également la comparé avec les deux outils de correction de fréquence rtl_test et Kalibrate-rtl. Concernant les deux autres outils (LTE-Cell-Scanner et LTESS-track), ils sont basé sur les signaux LTE qui ne sont pas disponibles en Algérie dans la gamme de fréquence de ces clés.


(a) (b)

Figure 2. 13: (a) La clé RTL-SDR TCXO (Silver), (b) La clé RTL-SDR Non-TCXO (Blue).

L'outil rtl_test outil estime le décalage de fréquence en fonction de la différence entre le nombre d'échantillons I/Q collectés dans chaque intervalle de temps d'une durée déterminé et le nombre attendu basé sur la fréquence d'échantillonnage nominale. L'inconvénient de cette méthode c'est que l'horloge de référence interne de l'ordinateur où les mesures sont effectués doit être très précise [21], Sinon, il y aura des divergences et des imprécisions dans la détermination de décalage de fréquence de la clé comme le montre dans la figure montre 2.14 et 2.15 pour une clé Non-TCXO et TCXO, respectivement. Concernant les mesures effectués par l'outil Kalibrate-rtl c'est presque la même estimation de décalage avec notre application MATLAB, il y a une différence de ~2 PPM pour les mesures effectués sur la clé Non-TCXO, et une différence de ~0.1 PMM pour les clés TCXO. Les avantages de notre application c'est que peut effectuer des mesures fiables dans presque ~8 secondes, comparé par l'outil Kalibrate-rtl qui prend ~1 minute et l'outil rtl_test qui prend plusieurs minutes, et que n'a pas besoin des outils extérieurs pour les utilisateurs de MATLAB, et qu'elle peut utiliser avec n'importe quelle type des appareils SDR supporté par MATLAB avec un simple changement.

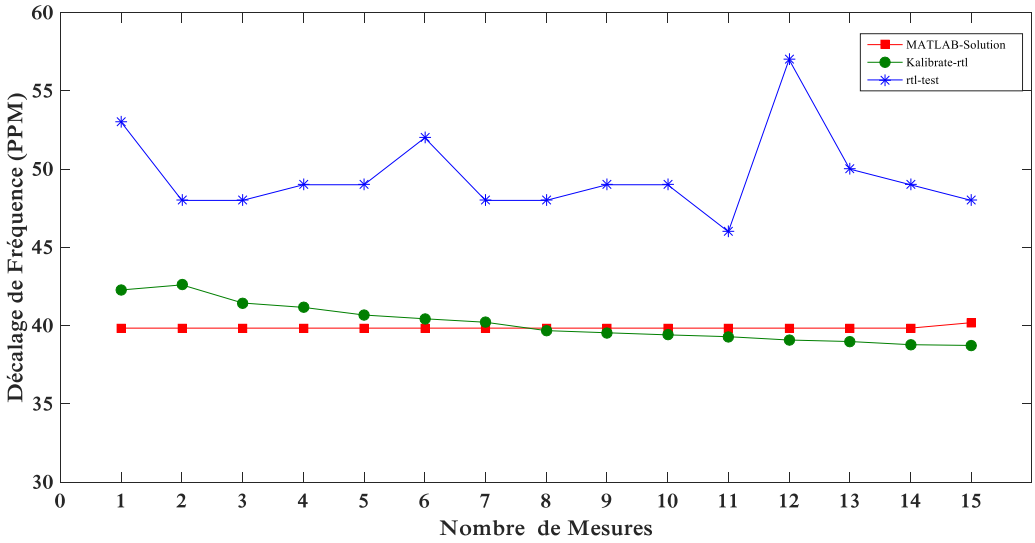



Figure 2. 14: Comparaison de notre application MATLAB avec rtl_test et kalibrate-rtl (Non-TCXO).

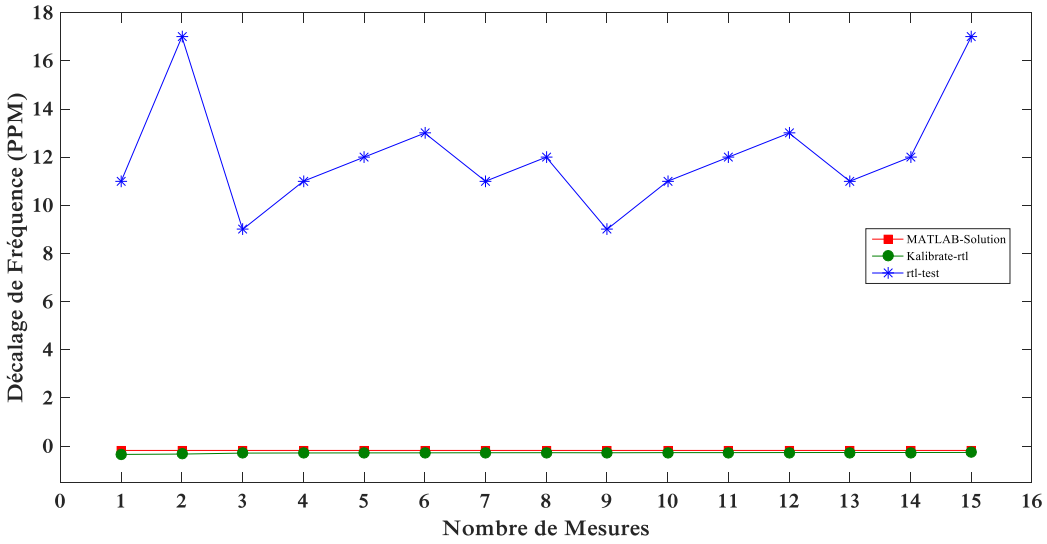



Figure 2. 15: Comparaison de notre application MATLAB avec rtl_test et kalibrate-rtl (TCXO).

On peut constater que les clés avec les oscillateurs TCXO ne nécessiteront normalement aucune correction de fréquence, qui ont généralement une tolérance de ±1 PPM ou moins.

## 2.7 Conclusion

Dans ce chapitre nous avons présenté quelques plateformes émetteur-récepteur disponibles sur le marché adoptées pour les solutions SDR. Ces plateformes se distinguent par la flexibilité qu'elles offrent, la technologie de conception et la bande de fréquence, etc. Etant donné leur coût assez élevé, il n'a pas été possible pour nous de les exploiter. Notre intérêt a été porté vers le récepteur RTL-SDR à faible coût, où nous avons détaillé ses caractéristiques, son architecture et son principe de fonctionnement. C'est sur cette dernière plateforme que nous avons développé nos solutions SDR. En effet, les clés RTL-SDR donnent la possibilité aux chercheurs de concevoir des applications radio logicielle, en réception, pour différentes standard de communication radio fréquence entre 24MHz et 1,75GHz.

# Chapitre3

# Applications pour la radio logicielle restreinte

## 3.1 Introduction

Pour faire fonctionner un périphérique SDR, à partir d'un ordinateur personnel ou d'un FPGA exécutant les algorithmes de traitement numérique du signal, un logiciel est nécessaire pour activer l'interaction et prendre en charge le traitement du signal en bande de base.

Dans ce chapitre, nous présentons quelques applications de la radio logicielle que nous avons réalisés en se basant sur la clé à faible coût RTL-SDR et l'environnement de développement MATLAB. La première application permet d'utiliser la clé RTL-SDR comme un récepteur SDR large bande sous l'environnement MATLAB. Dans la deuxième application, nous proposons un algorithme de détection des signaux captés par la clé RTL-SDR.

## 3.2 Applications à la RLR sous MATLAB

Les échantillons I/Q fournis par la clé RTL-SDR sont envoyé au PC où les traitements du signal numérique sont effectués. Il existe plusieurs logiciels pour différentes plateformes à usage général qui permettent à la clé RTL-SDR un fonctionnement comme un récepteur radio à large bande ou bien pour des applications spécifiques telles que le décodage des signaux ADS-B (Automatic dependent surveillance broadcast) des avions, le décodage des signaux AIS (automatic identification system) des navires, etc [61].Il y a aussi des environnements de développement tel que MATLAB et Simulink qui donnent la possibilité de développer et d'appliquer les différents traitements de signal sur les échantillons I/Q brut. Dans les sections suivantes nous présentons des applications de la RLR en utilisant MATLAB et la clé RTL-SDR.

### 3.2.1 Développement d'une interface graphique pour la clé RTL-SDR

#### 3.2.1.1 Présentation

En 2014, MathWorks a publié un package pour interfacer et contrôler la clé RTL SDR avec MATLAB et Simulink. Avec ce package, les utilisateurs peuvent capturer les échantillons I/Q brut du RTL-SDR et implémenter tout type de traitement de signal numérique.

Dans ce qui suit, nous allons présenter l'implémentation d'une application SDR avec une interface graphique sous Matlab [62], qui permet aux utilisateurs d'utiliser RTL-SDR pour:

- Balayer manuellement la bande spectrale souhaitée dans la gamme de fréquence de la clé RTL-SDR;

- Scanner automatiquement des bandes de fréquence telles que FM, GSM900, etc, avec une sélection simple;
- Visualiser en temps réel le spectre du signal capturé par le RTL-SDR ;
- Démodulation des signaux FM ;
- Démodulation des signaux AM.

Comme le montre la figure 3.1, l'interface de l'application est divisée en trois sections :

**a- La section des opérations** : Elle permet de switcher entre les différents modes; visualisation de spectre en temps réel (*Real Time*), le balayage d'une bande de fréquences manuellement ou bien automatiquement (*ManualScan, Auto Scan*), la réception et la démodulation des signaux FM et AM.

**b- La section des fréquences** : Elle permet de sélectionner la fréquence de début et de fin pour le mode scan, ou alors la fréquence centrale de la clé pour les autres modes.

**c- La section des paramètres** : Elle permet de contrôler et de configurer facilement la clé RTL-SDR. Le Contrôle du gain pour le LNA (amplificateur à faible bruit) et le VGA (amplificateur à gain variable). Le PPM (parties par million) est utilisé pour la correction du décalage de fréquence et le NFFT est utilisé pour définir le nombre de points dans la représentation spectrale FFT (Fast Fourier Transform).

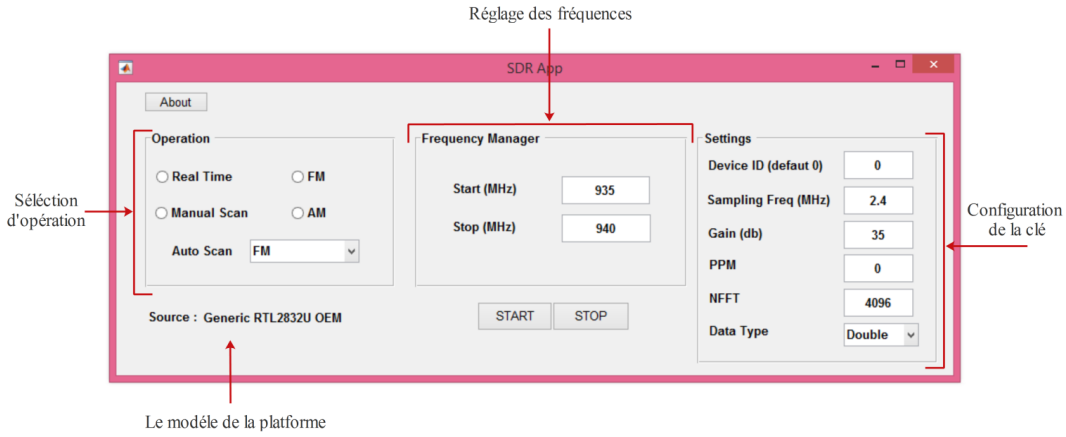



Figure 3. 1: Interface de l'application.

### 3.2.1.2 Visualisation de spectre en temps réel

L'analyse spectrale en mode temps réel, pour la visualisation du spectre et du spectrogramme des signaux reçus par la clé RTL-SDR sont effectués par la fonction MATLAB *dsp.SpectrumAnalyzer*[63].

### a- Canaux FM

La figure 3.2 montre la réception de la station FM d'AIN TEMOUCHENT diffusée sur la fréquence 95,9MHz en temps réel, ainsi que d'autres stations adjacentes.

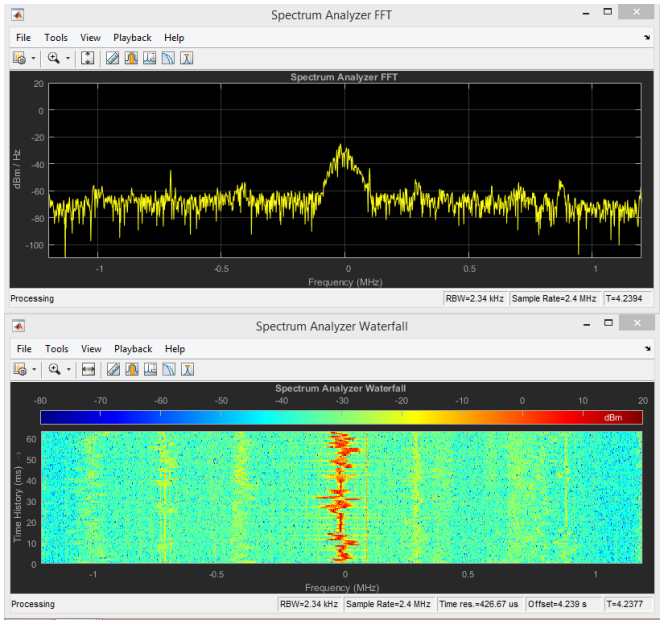
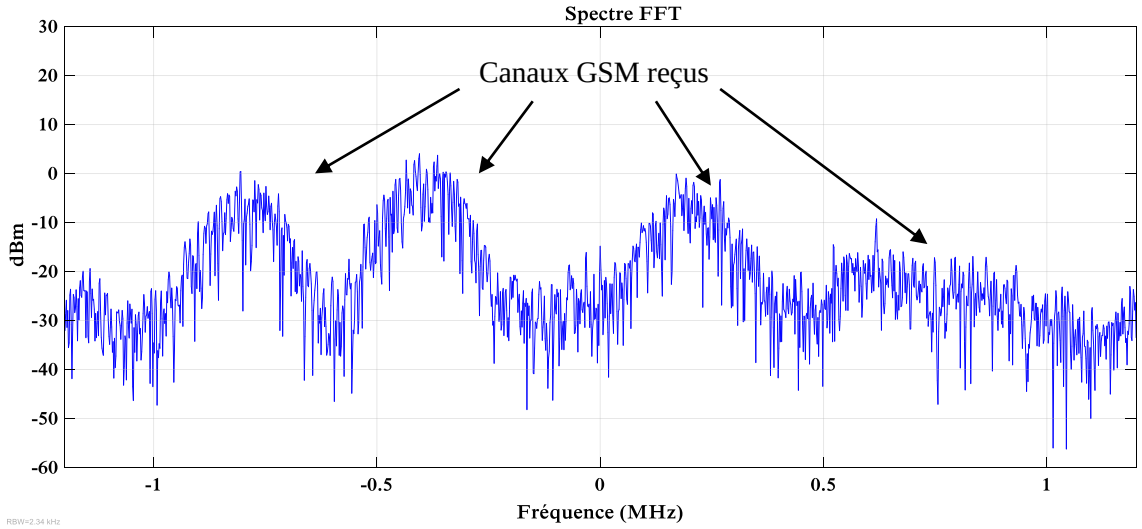



Figure 3. 2: Réception des stations FM en temps.

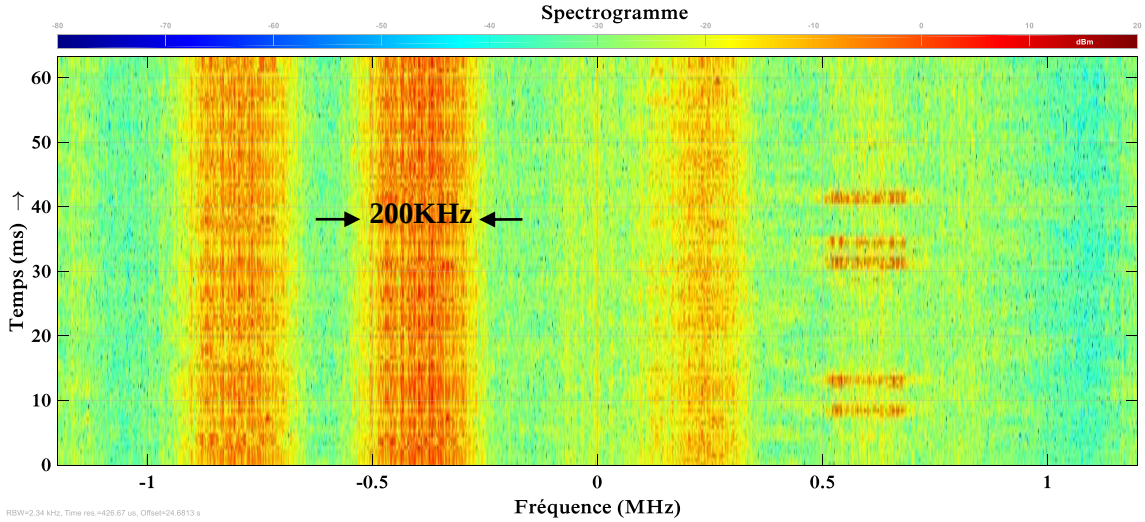
La fréquence d'échantillonnage est fixée à 2,4 MHz, ce qui donne une bande du signal reçu égale à 2,4 MHz (de -1,2 MHz à 1,2 MHz).En bande de base, cela signifie que la fréquence centrale de la clé RTL-SDR est située à 0 Hz. Ainsi, la fréquence 95.9MHz de la station d'AIN TEMOUCEHNT est transposée et centrée en bande de base à la fréquence de 0Hz. Pour cette bande passante de 2,4 MHz, plusieurs stations radio FM adjacentes peuvent être reçues.

### b- Canaux GSM

La figure 3.3 (a) illustre le spectre des canaux GSM reçus en temps réel et la figure 3.3 (b) montre le spectrogramme de ces canaux en fonction du temps. La clé RTL-SDR est réglée sur la fréquence 942,5 MHz. Cette fréquence appartient à la bande de liaison descendante GSM900 [935MHz – 960MHz].




(a)




(b)

Figure 3. 3: Réception des signaux GSM en temps réel. (a) Le spectre FFT. (b) Le spectrogramme.

### 3.2.1.3 Balayage des fréquences

Pour scanner une large gamme de fréquence par exemple 50MHz, un simple réglage de la bande passante de la plateforme SDR tel que l'USRP B210 qui a une bande passante de 56MHz permet d'obtenir l'information spectrale sur la plage désirée. Malheureusement, ce n'est pas le cas avec la clé RTL-SDR qui a une bande passante de 2.4MHz (3.2MHz au max).

Afin d'obtenir l'information spectrale sur une large gamme de fréquence (plus de 2.4MHz) avec la clé RTL-SDR, par exemple de $f_1$ jusqu'à $f_2$, un processus répétitif sur le réglage de la fréquence centrale ($f_c$) de la clé est effectuée. L'application récupère les données I/Q pour différentes fréquences centrales dans la plage désirée, ces fréquences centrales ($f_c$) sont données comme suit :

$$f_{c(i+1)} = f_{c(i)} + 2.4\,MHz \quad \text{avec} \quad i = 1,2,3 \ldots, \frac{(f_2 - f_1)}{2.4MHz} \tag{3.1}$$

La figure 3.4 illustre un exemple de huit segments de spectre de 2,4 MHz (bande passante de la RTL-SDR) rassemblés pour augmenter la gamme de balayage totale à 19,2 MHz. Cependant, des atténuations sont introduites par le filtre interne de la clé RTL-SDR aux extrémités de chaque segment [64]. Pour éliminer ces atténuations le pas doit être inférieur à 2,4 MHz. Nous avons alors configuré notre application pour conserver les données de $f_c - 0.6MHz$à $f_c + 0.6MHz$ et avec un pas de 1.2 Mhz, ce traitement permet de ne conserver que la moitié des informations spectrales, d'où l'équation 3.1 devient:

$$f_{c(i+1)} = f_{c(i)} + 1.2MHz \tag{3.2}$$

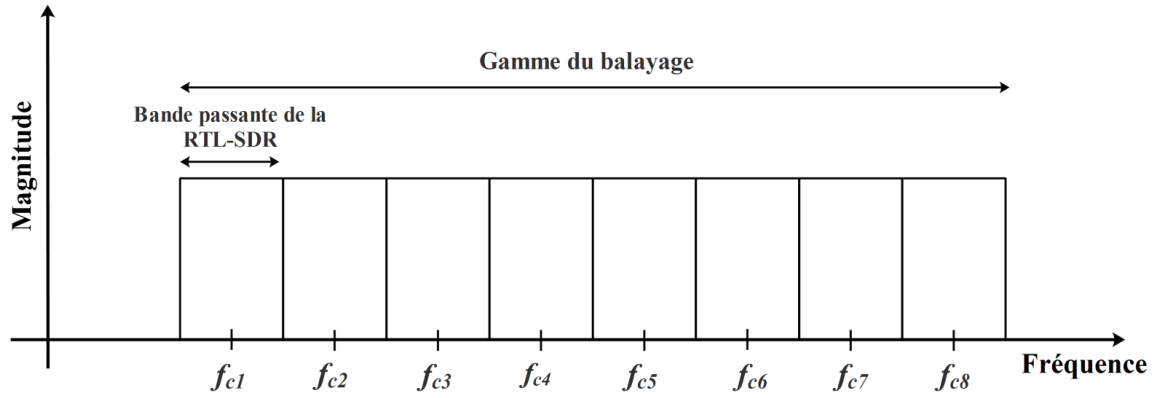



Figure 3. 4: Processus de collecte de données à partir de plusieurs captures de la clé RTL-SDR.

La figure 3.5 montre les fonctions de traitement de signal (DSP) implémentées sur les données I/Q captées par la clé RTL-SDR pour le mode de balayage. Les données I/Q provenant de la clé RTL-SDR sont exploitées pour donner le signal numérique $x_{RTL}[n]$suivant :

$$x_{RTL}[n] = x_I[n] + jx_Q[n] \tag{3.3}$$

La première étape de traitement de signal est de supprimer les pics. Ces pics apparaissent dans le spectre aux différentes fréquences centrales sélectionnées $f_c$ comme le montre la figure 3.6(a). Ces pics sont causés par le convertisseur analogique-numérique ADC ou

l'oscillateur local. Une méthode simple pour supprimer ces pics est de soustraire la moyenne du signal d'origine, ceci est illustré dans la figure 3.6(b) [65,66] :

$$x_{DC}[n] = x_{RTL}[n] - moy(x_{RTL}[n]) \quad (3.4)$$

Avec la valeur moyenne d'un signal $x[n]$ est définit par :

$$x_{moy}[n] = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (3.5)$$

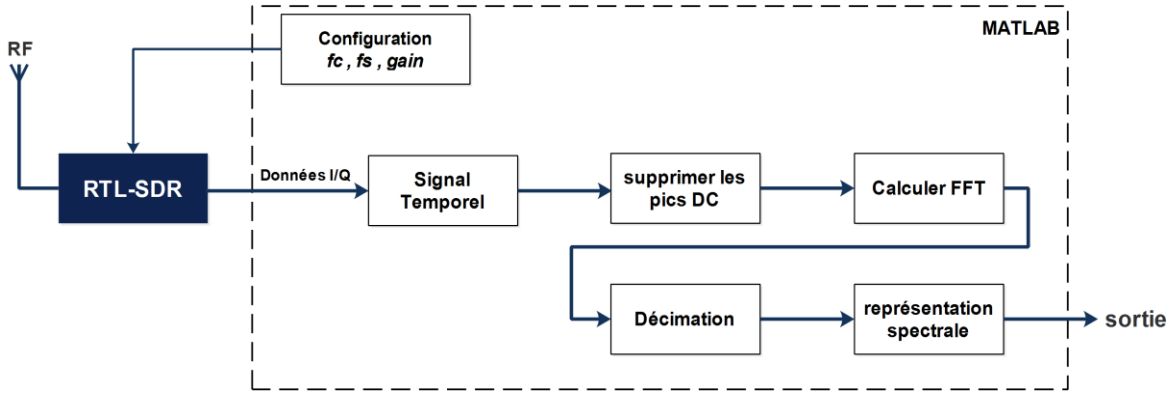
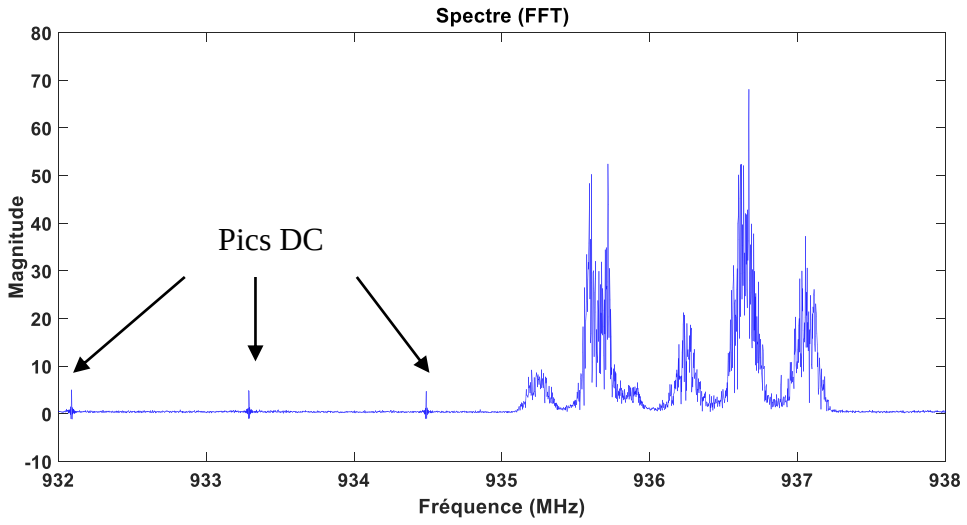
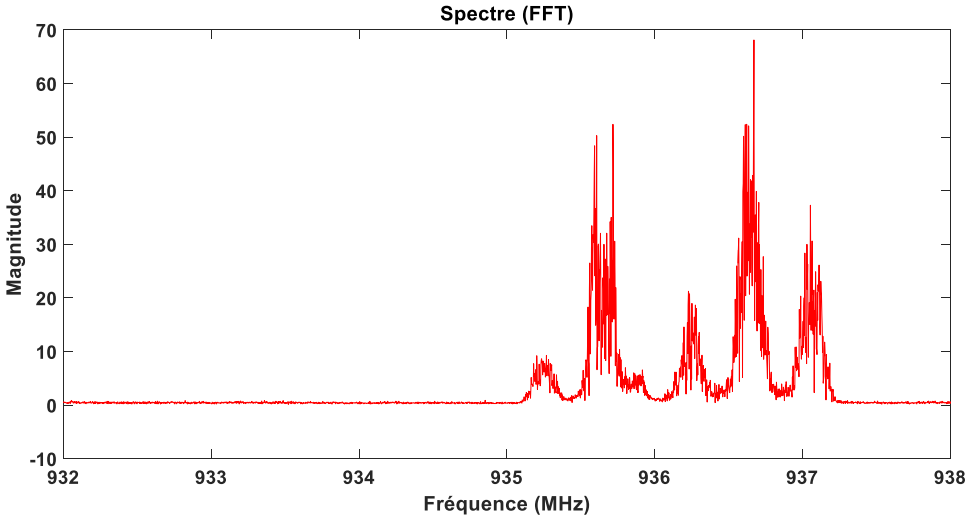



Figure 3. 5: Etapes de traitement du signal numérique pour le mode du balayage.

Ensuite, la transformée de Fourier est implémentée pour transformer le signal du domaine temporel en domaine fréquentiel, et finalement un processus de décimation est effectué pour réduire la résolution pour une bonne représentation spectrale.




(a)




(b)

Figure 3. 6: (a) Signal avec les pics. (b) Signal après suppression des pics.

### a- Balayage GSM

La figure 3.7 illustre le spectre pour un balayage de fréquence de 5 MHz, allant de 950 MHz à 955 MHz dans la bande de liaison descendante GSM. Selon la norme GSM, chaque canal a une largeur de 200 kHz. Nous distinguons sur la figure 3.7 la réception de six canaux GSM.

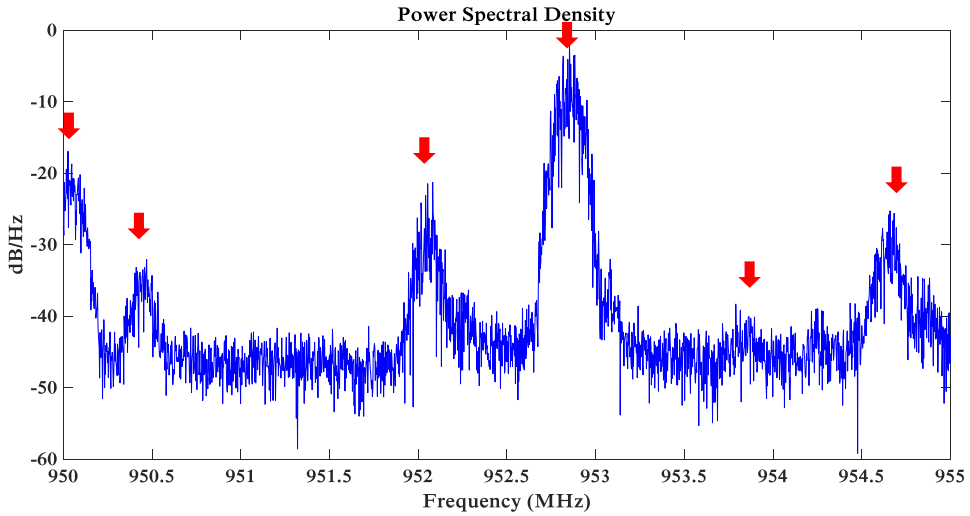



Figure 3. 7: Balayage d'une plage de 5 MHz dans la bande de liaison descendante GSM900.

Certains des canaux GSM semblent contenir des signaux beaucoup plus puissants que les autres, cela peut être dû au fait que les antennes de transmission de ces canaux sont polarisées avec l'antenne du RTL-SDR ou sont des canaux de contrôle de diffusion comprenant des informations de contrôle envoyées en continu à tous les téléphones mobiles présentent dans la cellule. Le tableau 3.1illustre tous les canaux reçus avec leurs numéros ARFCN (numéro de canal de radiofréquence absolu) [58]. Cela peut être calculé en utilisant les équations suivantes :

$$f_{UL} = 890MHz + (0.2MHz \cdot n) \text{pour} \;\; 1 \leq n \geq 124 \quad (3.6)$$

$$f_{DL} = f_{UL} + 45\ MHz \quad (3.7)$$

Avec :

$f_{UL}$ : Fréquence porteuse sur la liaison montante,

$f_{DL}$ : Fréquence porteuse sur la liaison descendante

$n$ : Numéro de canal (ARFCN).

| ***Fréquence du Canal (MHz)*** | ***ARFCN*** |
|---|---|
| 950.0 | 75 |
| 950.4 | 77 |
| 952.0 | 85 |
| 952.8 | 89 |
| 953.8 | 94 |
| 954.6 | 98 |

Tableau 3. 1: Canaux GSM reçus et leur RFCN.

**b- Balayage FM**

Toutes les stations radios FM ont une largeur spectrale de 200 kHz et diffusent dans la bande 87,5 MHz à 108 MHz. La figure 3.8 illustre les résultats de balayage d'une partie de la bande FM ([92 MHz - 98 MHz]). Plusieurs stations FM sont reçues avec des puissances différentes. Le tableau 3.2illustre les noms de certaines stations FM détectées de la plage balayée.

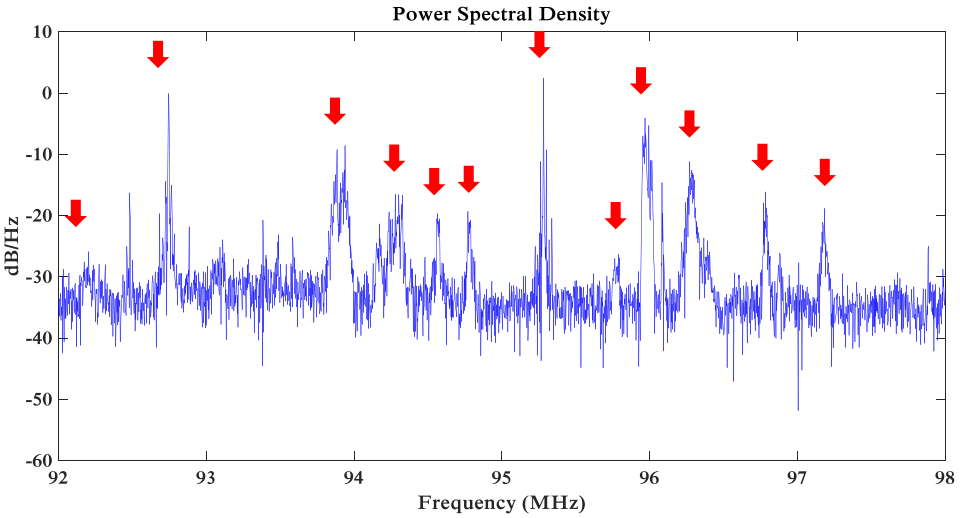



Figure 3. 8: Analyse d'une plage de 6 MHz dans la bande FM.

| ***Station FM*** | ***Fréquence (MHz)*** |
|---|---|
| Radio SINTONIA | 95.2 |
| Radio Oran EL-Bahia | 92.7 |
| Radio Aïn Témouchent | 95.9 |

Tableau 3. 2: Quelques stations FM identifiées.

### 3.2.1.4 Démodulation des signaux FM

Pour démoduler un signal FM, une des méthodes standard utilisées consiste à prendre la dérivée du signal reçu pour transformer le signal FM en un signal AM, puis effectuer une détection d'enveloppe afin de récupérer le signal d'information. Le signal FM reçu par la clé RTL-SDR est transposé en bande de base en quadrature (I/Q), afin de récupérer le signal d'information et un discriminateur de bande de base (Complex Baseband Discriminator) est implémenté.

Nous pouvons écrire le signal FM $x_{FM}(t)$sous la forme suivante :

$$x_{FM}(t) = A\,[\cos(2\pi f_c t + \emptyset(t))] \qquad (3.8)$$

Où : $\emptyset(t) = 2\pi k_m \int_{-\infty}^{t} s_i(t)dt$ (3.9)

Avec :

$\emptyset(t)$ : La phase de signal FM

$s_i(t)$ : Le signal d'information basse fréquence

$k_m$ : Constant de modulation (Gain)

Considérons le signal FM en bande de base, après la multiplication avec la fréquence de l'oscillateur local et un filtrage, le signal à la sortie de la clé RTL-SDR est représenté sous la forme :

$$x_{RTL}(t) = \frac{A}{2}[x_I(t) + jx_Q(t)] \quad (3.10)$$

$$x_{RTL}(t) = \frac{A}{2}[\cos(2\pi\Delta ft + \emptyset(t)) + j\sin(2\pi\Delta ft + \emptyset(t))] \quad (3.11)$$

Où $\emptyset(t)$ contient le signal d'information et $\Delta f$représente la petite erreur de fréquence (entre le signal RF reçu et la fréquence d'oscillateur local) dans la transposition de signal $x_{RTL}(t)$ en bande de base. Le discriminateur de fréquence prend la dérivé du signal FM $x_{RTL}(t)$. En séparant la partie réelle et la partie imaginaire de ce signal nous obtenons :

$$x_I(t) = \Re e\,[x_{RTL}(t)] = \frac{A}{2}\cos(2\pi\Delta ft + \emptyset(t)) \quad (3.12)$$

$$x_Q(t) = \Im m[x_{RTL}(t)] = \frac{A}{2}\sin(2\pi\Delta ft + \emptyset(t)) \quad (3.13)$$

La dérivée de chaque composant donne :

$$\frac{dx_I(t)}{dt} = -\frac{A}{2}[2\pi\Delta f + \emptyset'(t)]\sin(2\pi\Delta ft + \emptyset(t)) \quad (3.14)$$

$$\frac{dx_Q(t)}{dt} = \frac{A}{2}[2\pi\Delta f + \emptyset'(t)]\cos(2\pi\Delta ft + \emptyset(t)) \quad (3.15)$$

Pour extraire l'information utile les étapes suivantes sont appliquées :

$$x_I(t)\frac{dx_Q(t)}{dt} = \frac{A^2}{4}[2\pi\Delta f + \emptyset'(t)]\cos^2(2\pi\Delta ft + \emptyset(t)) \quad (3.16)$$

$$x_Q(t)\frac{dx_I(t)}{dt} = -\frac{A^2}{4}[2\pi\Delta f + \emptyset'(t)]\sin^2(2\pi\Delta ft + \emptyset(t)) \quad (3.17)$$

$$r(t) = \left[x_I(t)\frac{dx_Q(t)}{dt}\right] - \left[x_Q(t)\frac{dx_I(t)}{dt}\right] \quad (3.18)$$

$$r(t) = \frac{A^2}{4}[2\pi\Delta f + \emptyset'(t)]\cos^2(2\pi\Delta f t + \emptyset(t)) + \frac{A^2}{4}[2\pi\Delta f + \emptyset'(t)]\sin^2(2\pi\Delta f t + \emptyset(t))$$

$$r(t) = \frac{A^2}{4}[2\pi\Delta f + \emptyset'(t)][\cos^2(2\pi\Delta f t + \emptyset(t)) + \sin^2(2\pi\Delta f t + \emptyset(t))]$$

Ce qui nous donne

$$r(t) = \frac{A^2}{4}[2\pi\Delta f + \emptyset'(t)]$$

En divisant le signal $r(t)$ par $(x_I^2(t) + x_Q^2(t))$ nous obtenons :

$$s(t) = \frac{\frac{A^2}{4}[2\pi\Delta f + \emptyset'(t)]}{\frac{A^2}{4}[cos^2(w_\Delta t + \emptyset(t)) + sin^2(w_\Delta t + \emptyset(t))]} \quad (3.19)$$

$$s(t) = [2\pi\Delta f + 2\pi k_m s_i(t)] \quad (3.20)$$

Et finalement, un filtrage passe bas est appliqué au signal démodulé $s(t)$pour éliminer tout bruit à des fréquences supérieures à la fréquence maximale du signal utile.

Afin de tester la réception des signaux FM dans des conditions acceptable nous avons utilisé un Raspberry Pi3 comme un émetteur FM, les détails sur comment construire un émetteur FM à l'aide d'un Raspberry Pi 3 sont donnés en annexe A. Les étapes de traitement du signal effectuées pour démoduler les signaux FM et récupérer le signal audio dans notre application sont illustrées dans la figure 3.9.

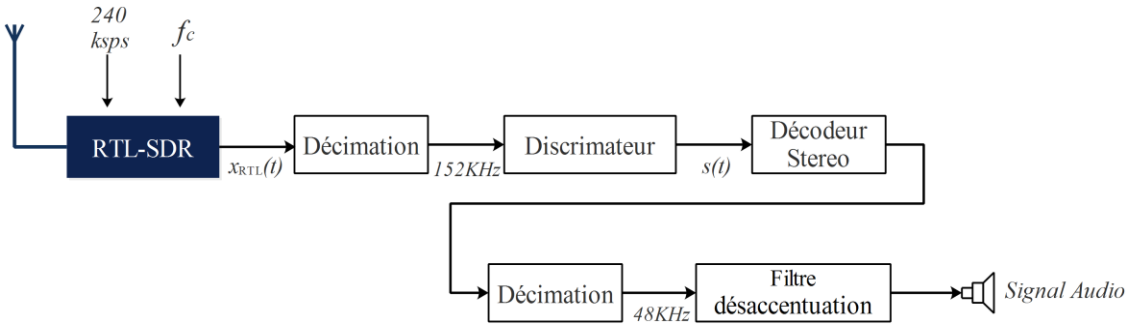



Figure 3. 9: Synoptique du récepteur FM.

La clé RTL-SDR est réglée pour recevoir le signal FM émis par Raspberry Pi3 avec une fréquence d'échantillonnage de 240Ksps qui donne une largeur de bande de la clé 240Khz. La figure 3.10 illustre le spectre du signal FM (en bande de base (0Hz)) capté par la clé

RTL-SDR, émis par le Raspberry Pi3 sur la fréquence de 107 MHz. Avant de démoduler ce signal, un processus de décimation interpolation est effectué sur le signal pour réduire le taux d'échantillonnage à 152 KHz. Pour cela, il suffit d'affecter au signal une interpolation de 19 puis une décimation de 30 :

$$fréquence\ d'échantillonage = \frac{240\ KHz}{30} \times 19 = 152KHz. \qquad (3.21)$$

Le discriminateur est utilisé pour démoduler le signal FM. Sur la figure 3.11, nous pouvons distinguer les différents composants du signal FM stéréo. Le décodeur stéréo sépare les canaux droit et gauche afin de récupérer le signal d'information, les détails sur la transmission FM stéréophonique sont donnés en annexe B.

Une deuxième décimation est appliquée sur les canaux droit et gauche pour descendre la fréquence d'échantillonnage à 48 KHz, ce taux est l'un des taux d'échantillonnage natif de la carte son de l'ordinateur hôte. Pour cela, il suffit d'affecter au signal une interpolation de 6 puis une décimation de 19 :

$$fréquence\ d'échantillonage = \frac{152\ KHz}{19} \times 6 = 48KHz. \qquad (3.21)$$

La dernière étape consiste à appliquer une désaccentuation sur le signal d'information récupéré. Cela permet une restitution conforme du signal utile et diminue fortement le bruit [67]. La figure 3.12 montre le spectre du signal utile.

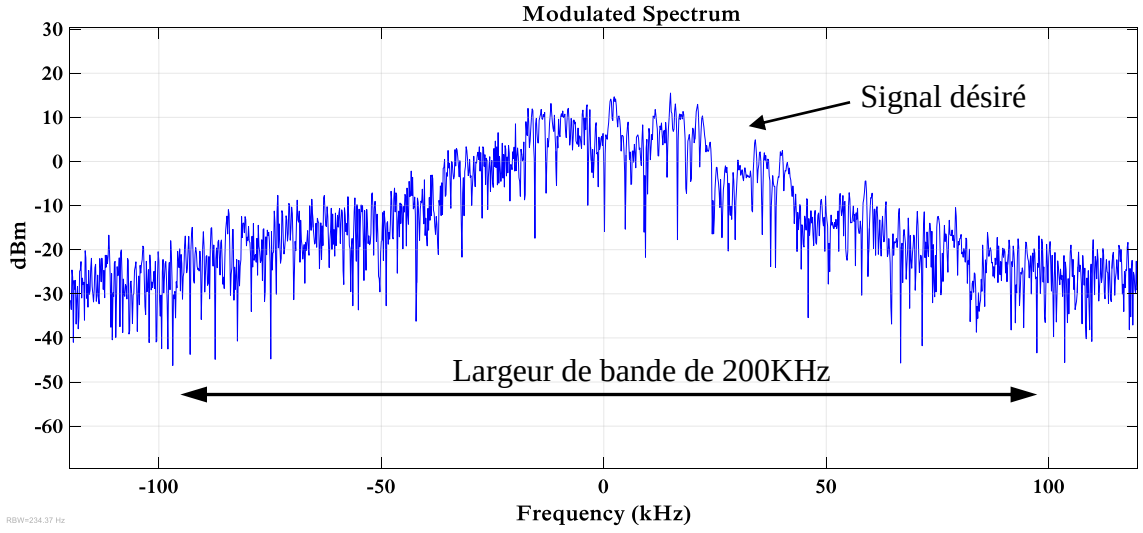



Figure 3. 10: Spectre du signal FM capté par la clé RTL-SDR, émis par le Raspberry Pi3 sur la fréquence de 107 MHz.

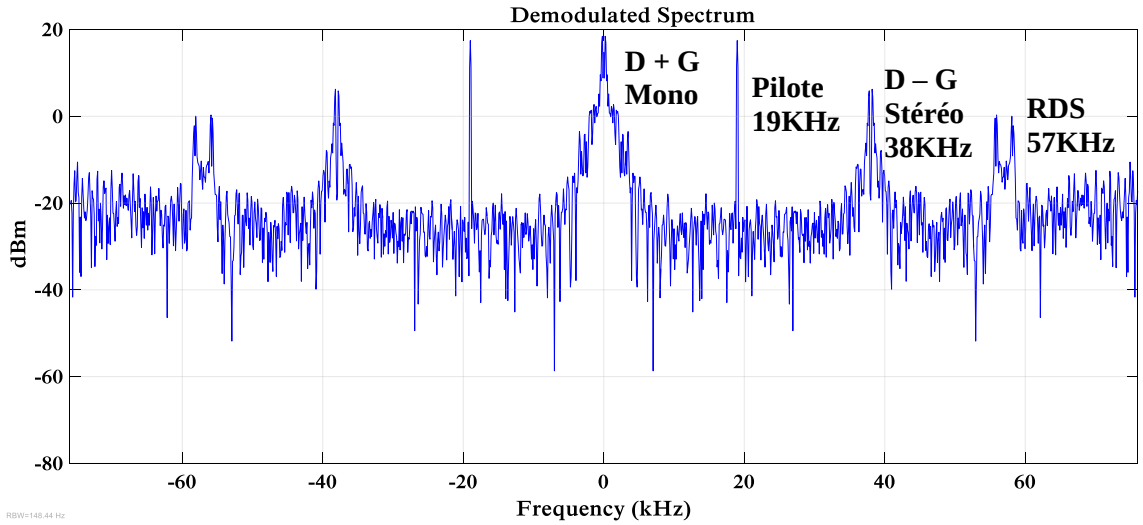



Figure 3. 11: Le spectre du signal FM Stéréo démodulé.

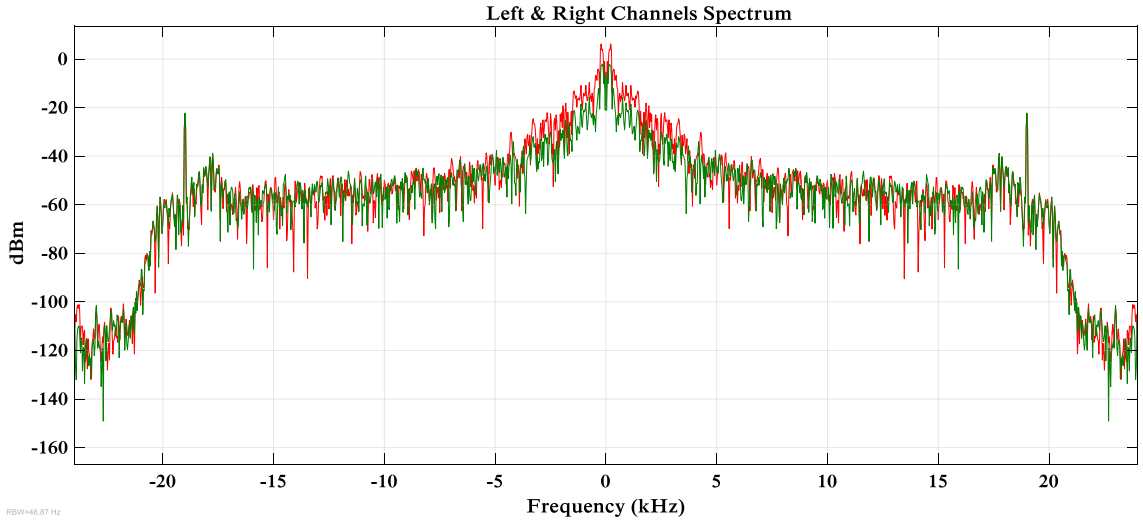



Figure 3. 12: Spectre du signal utile.

### 3.2.2 Détection des signaux en utilisant la clé RTL-SDR

#### 3.2.2.1 Présentation

Nous proposons dans cette section, une approche qui nous permet d'analyser la bande des fréquences souhaitée et de détecter les fréquences qui contiennent une activité spectrale. Cette approche est basée sur différents traitements numériques du signal appliqué aux échantillons I/Q provenant de la clé RTL-SDR sous MATLAB.

### 3.2.2.2 Conditionnement du signal

De nombreuses sources de bruit influencent les signaux captés par la clé RTL-SDR telles que les fluctuations de l'électricité, les appareils électriques, les pics causés par l'USB, l'oscillateur local et le CAN utilisé dans la clé [68]. L'utilisation des composants matériels de haute qualité peut minimiser le bruit. Cependant, il arrive souvent que, du fait des limitations matérielles, il soit nécessaire d'accepter un faible rapport signal sur bruit. Dans cette situation, il peut devenir possible d'améliorer considérablement le rapport signal sur bruit en combinant des techniques appropriées. L'une des méthodes d'amélioration du signal est appelée "moyenne d'ensemble"[69].

Cette méthode consiste à acquérir plusieurs fois le signal à la même fréquence d'échantillonnage. Toutes les copies mesurées de ce signal sont additionnées échantillon par échantillon, puis divisées sur le nombre d'acquisitions effectuées. La figure 3.13 explique cette méthode.

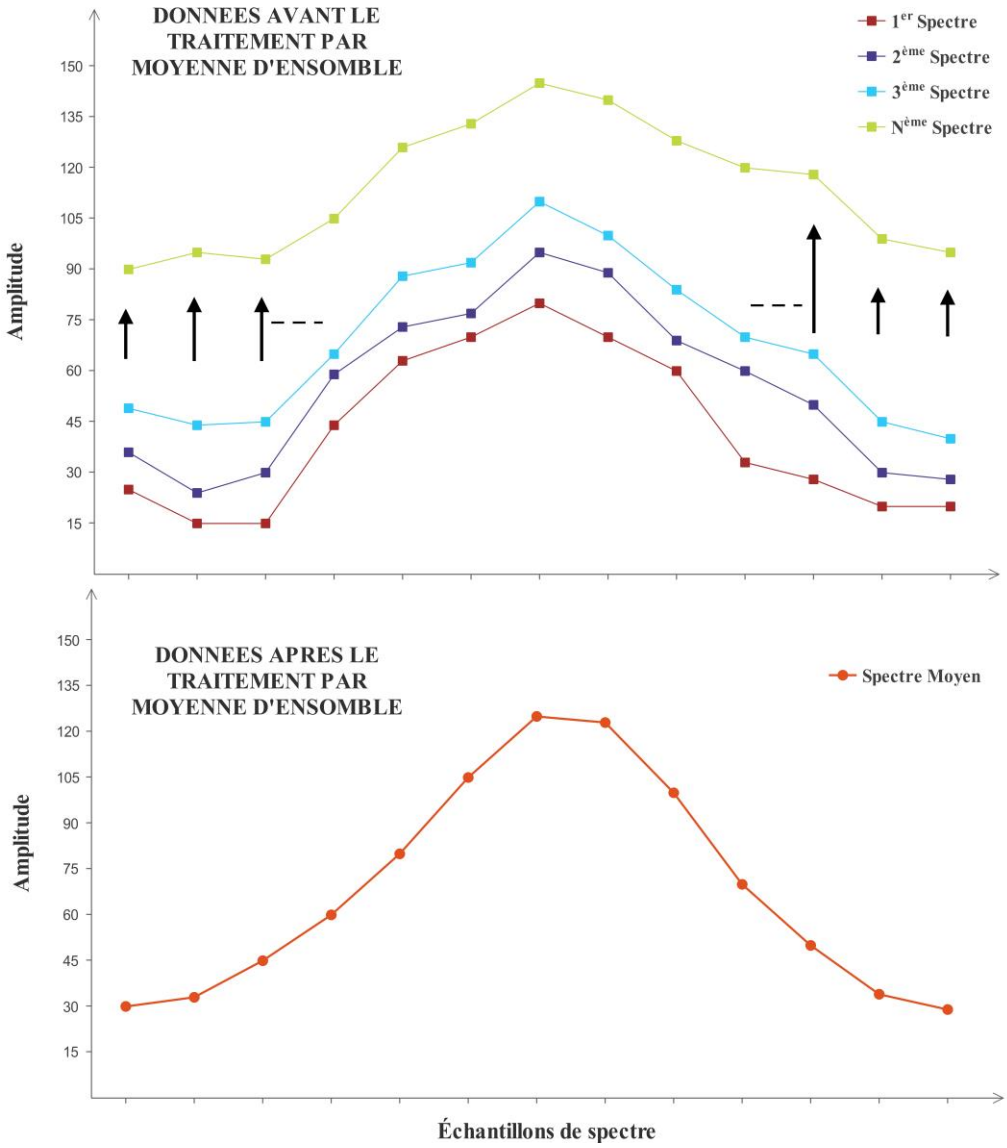



Figure 3. 13: Le principe de la méthode de moyenne d'ensemble.

Les étapes de traitements numériques du signal pour le conditionnement et avant la détection sont représentées dans la figure 3.14. Les données fournies par RTL-SDR sont exprimées dans le domaine temporel. Nous supprimons d'abord les pics DC avec la même méthode expliquée dans la section 3.2.1.3. Ensuite, nous transformons le signal dans le domaine fréquentiel à l'aide de la transformée de Fourier rapide (FFT). Ces processus sont appliqués plusieurs fois pour la même fréquence centrale de la clé RTL-SDR afin de déterminer la moyenne d'ensemble.

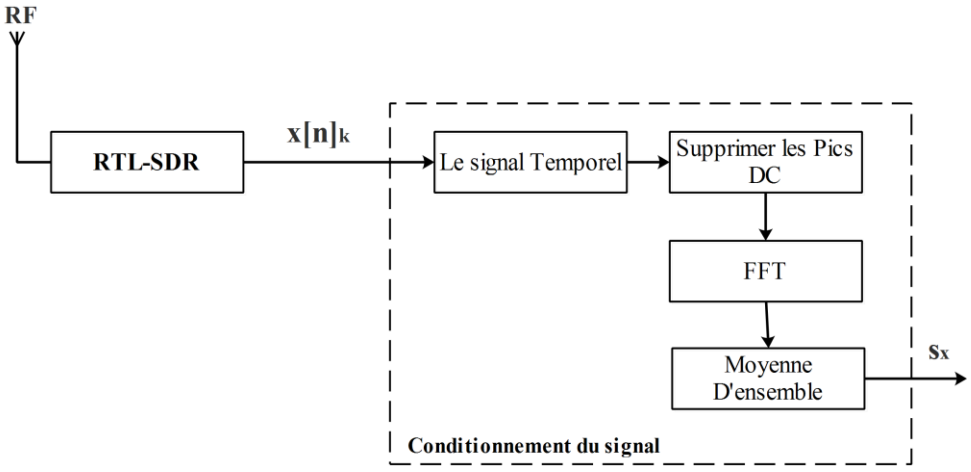



Figure 3. 14: Étapes de conditionnement appliquées au signal en bande de base capturé par la clé RTL-SDR.

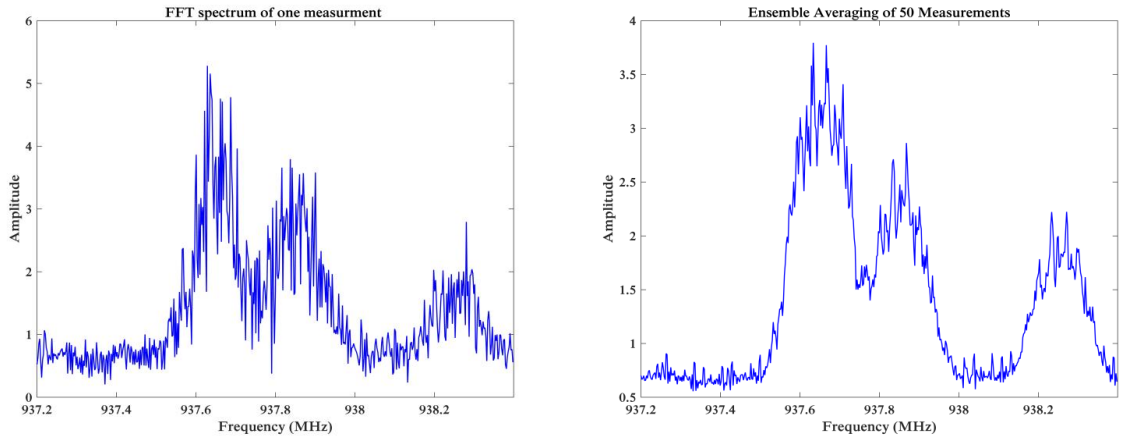
La moyenne d'ensemble est donnée par:

$$S_x = \frac{\sum_{i=1}^{m} S_i}{m} \tag{3.23}$$

Où $S_i$ représente la mesure du signal, $i$ représente le numéro de la mesure et $m$ représente le nombre de mesures effectuées.

Nous avons réglé la clé RTL-SDR à une fréquence d'échantillonnage de 2.4MHz. Pour scanner une large bande fréquentielle, afin de détecter s'il existe une activité spectrale, nous avons utilisé la même méthode expliquée dans la section 3.2.1.3.

La figure 3.15(a) illustre le spectre d'une seule mesure de données et la figure 3.15 (b) illustre la moyenne d'ensemble de 50 mesures de données pris successivement pour la même fréquence centrale. Nous pouvons clairement voir que les canaux sont améliorés et le bruit est réduit.




(a) (b)

Figure 3. 15: (a) Spectre d'une trame de largeur large de 1,2 MHz et (b) Moyenne de l'ensemble de 50 mesures de la même trame.

### 3.2.2.3 Détection des Signaux

Après le conditionnement du signal, un ensemble des traitements de signal sont appliquées afin de détecter les fréquences qui contiennent une activité spectrale [70]. Ces traitements sont présentés dans la figure 3.16. Notre solution calcule la densité spectrale de puissance pour chaque trame (dans la figure 3.15(b)), puis un processus de lissage est appliqué à l'aide de filtre de Savitzky-Golay [71]. L'équation du lissage à base de filtre de Savitzky-Golay est définie comme suit:

$$Y_k = \frac{\sum_{i=-n}^{n} A_i Y_{k+1}}{\sum_{i=-n}^{n} A_i} \qquad (3.24)$$

Avec:

$Y_{k+1}$ : Echantillons à lisser (moving window averaging).
$n$ : Nombre d'échantillons.
$A_i$ : Coéfficients du filtre.

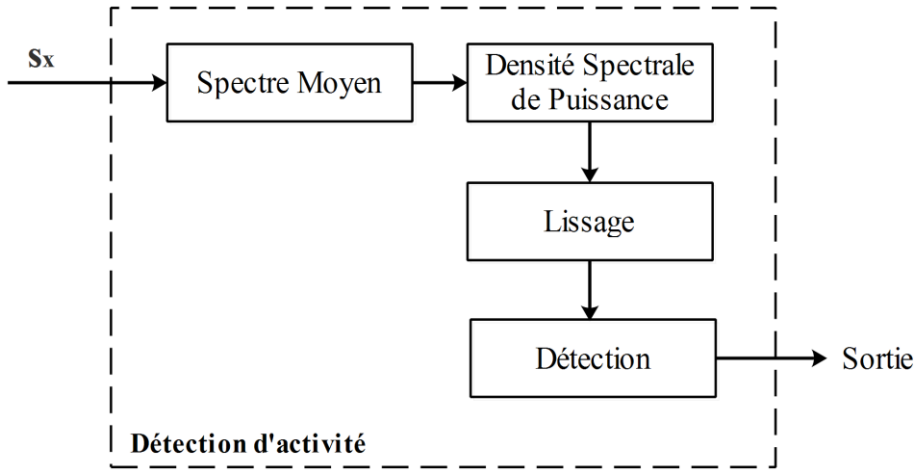
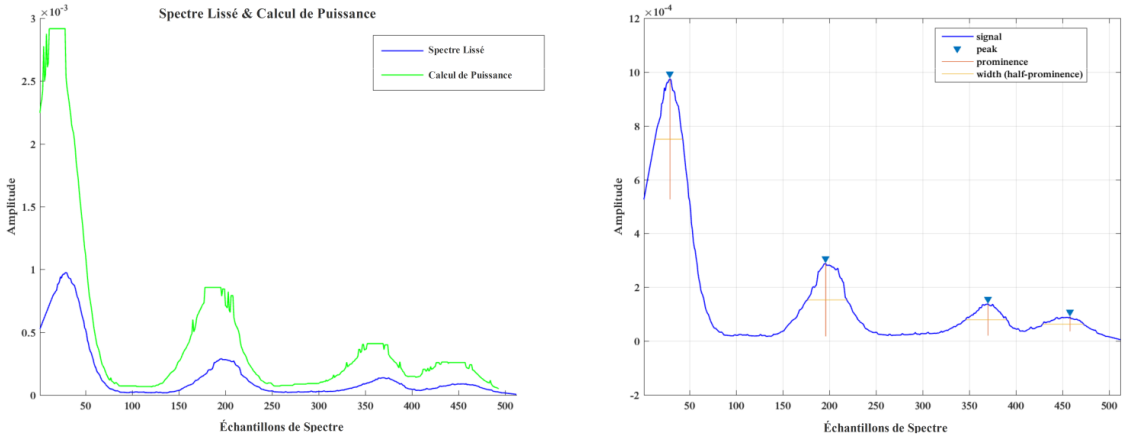



Figure 3. 16: Étapes de détection des signaux appliquées au spectre de la plage scanné.

Pour détecter les canaux qui contiennent une activité, il nous faut définir un seuil qui sépare les canaux actifs et le bruit. Notre algorithme calcule le seuil de façon automatique pour chaque trame de largeur de 1.2MHz de la bande scannée, cela revient à définir un seuil pour chaque trame. Pour déterminer un seuil nous devons tout d'abord déterminer la valeur de la puissance maximale entre chaque 20 échantillon le long de la trame, ensuite nous prenons la somme de cette puissance maximale avec la valeur précédente et la valeur suivante. La figure 3.17 (a) illustre le spectre lissé d'une seule trame (courbe en bleu) et les valeurs calculées de la puissance pour chaque 20 échantillons de la trame (la courbe verte). Cette méthode prend les sommets du spectre; le bruit ayant la valeur minimum est considéré comme le seuil. Tous les pics présentant une proéminence supérieure à cette valeur de seuil sont considérés comme une activité spectrale. Ce processus est répété pour toutes les trames de la plage scannée. La figure 3.17(b) montre les canaux détectés pour une seule trame.




(a) (b)

Figure 3. 17: (a) Spectre lissé et calcul de puissance pour une trame (largeur de 1,2 MHz). (b) Canaux détectés dans une trame de spectre.

### 3.2.2.4 Visualisation Heatmap

Le Heatmap est une représentation graphique des données en utilisant des couleurs pour indiquer le niveau d'activité, généralement les couleurs vont du bleu foncé pour indiquer une activité faible au rouge foncé pour indiquer une activité très élevée. Nous avons proposé une solution sous MATLAB pour montrer l'activité spectrale basée sur le principe de Heatmap. Cela nous aidera à découvrir dans la plage scannée les fréquences qui contiennent une activité très élevée et celles qui contiennent une activité très faible en fonction de leurs puissances. Les données provenant de la clé RTL-SDR pour toutes les fréquences balayées sont réorganisées dans une seule matrice pour créer un Heatmap.

Nous avons comparé notre solution avec l'outil *rtl-power* fourni avec le package officiel de la clé RTL-SDR qui permet aussi de présenter les niveaux de puissance des signaux captés dans une plage sélectionnée.

Pour cela, nous devons d'abord enregistrer les mesures dans un fichier CSV, puis l'utiliser via un script Python qu'il s'appelle *heatmap.py* qui crée l'image Heatmap finale. Pour une bande balayée égale à 3 MHz, l'outil *rtl-power* prend 40 minutes pour obtenir le résultat de l'activité spectrale. La figure 3.18, illustre le Heatmap obtenue pour cette bande par l'outil *rtl-power*.

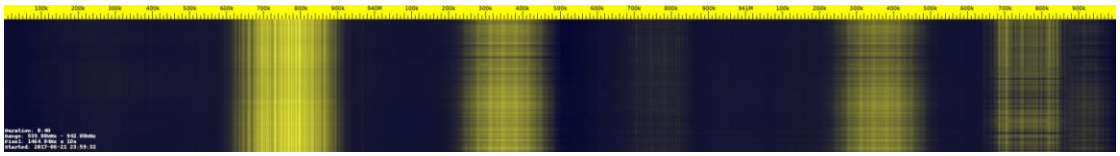


Figure 3. 18: Heatmap obtenu à l'aide de l'outil rtl-power fournit avec le package officiel de la clé RTLSDR.

La figure 3.19 montre le Heatmap obtenu avec notre solution MATLAB qui consiste à collecté les données récupérés de la clé RTL-SDR, puis un calcul de puissance de chaque signal (fréquence) est effectué. Ces puissances sont utilisées finalement pour construire une matrice de $m$ lignes et $q$ colonnes :

$$H = (P_{ij}) \tag{3.25}$$

Avec $1 \leq i \leq n$ et $1 \leq j \leq q$.

Cette matrice est utilisée pour générer le Heatmap de la bande scanné. Pour une même largeur de bande (3 MHz) notre programme réduit considérablement le temps de calcul à seulement 6 secondes.

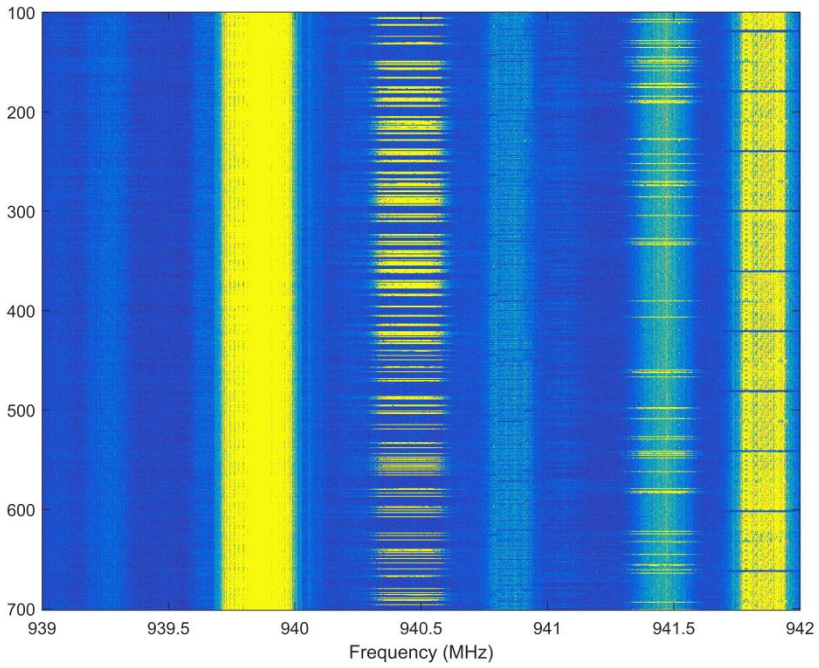



Figure 3. 19: Visualisation Heatmap obtenue avec notre solution MATLAB pour la bande de liaison descendante GSM**.**

### 3.2.2.5 Test sur la bande GSM

La figure 3.20 et la et la figure 3.21 illustrent respectivement le spectre FFT de tous les canaux GSM scannés (des trois opérateurs algériens: Mobilis, Djezzy et Ooredoo) dans la plage de fréquence allant de 945 à 950 MHz soit une bande de 5 MHz et la moyenne d'ensemble de cette plage scanné.

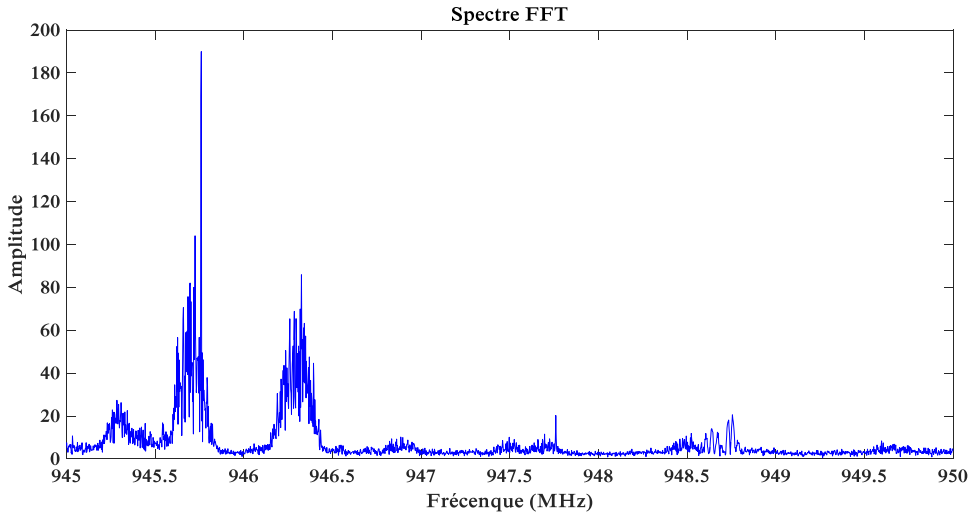



Figure 3. 20: FFT de la bande balayée de largeur égale à 5 MHz.

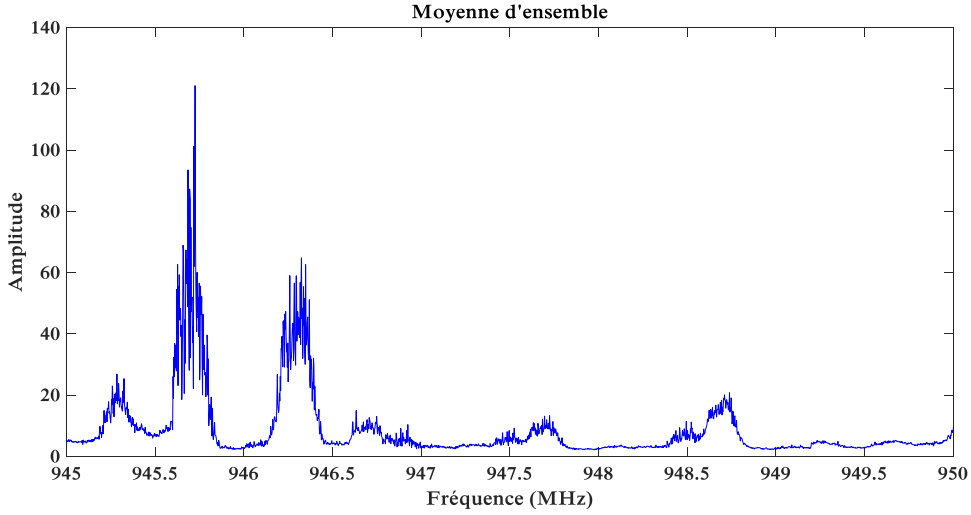



Figure 3. 21: Moyenne d'ensemble de 50 mesures pour la bande balayée.

La figure 3.22 illustre les canaux détectés automatiquement par notre algorithme. La figure 3.23 montre le Heatmap des canaux détectés en fonction de leurs puissances mesurées en ~9 secondes.

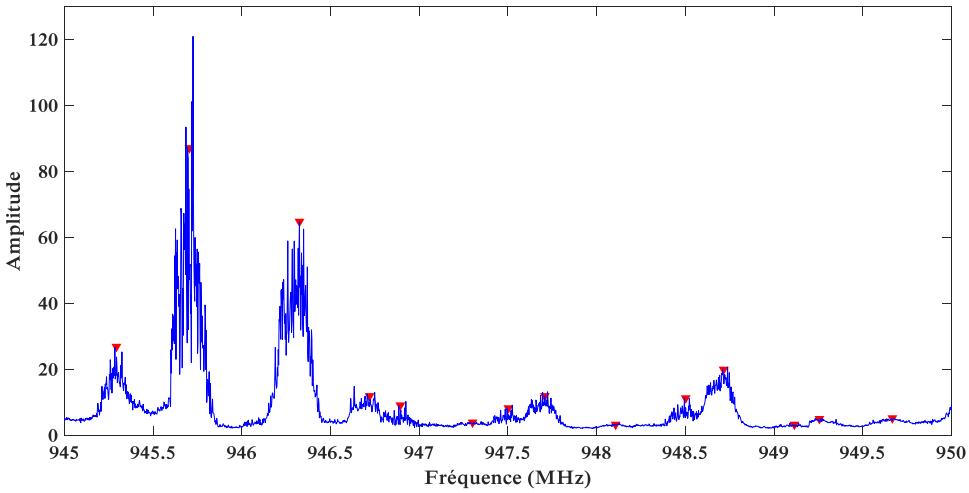



Figure 3. 22: Canaux détectés dans la bande balayée.

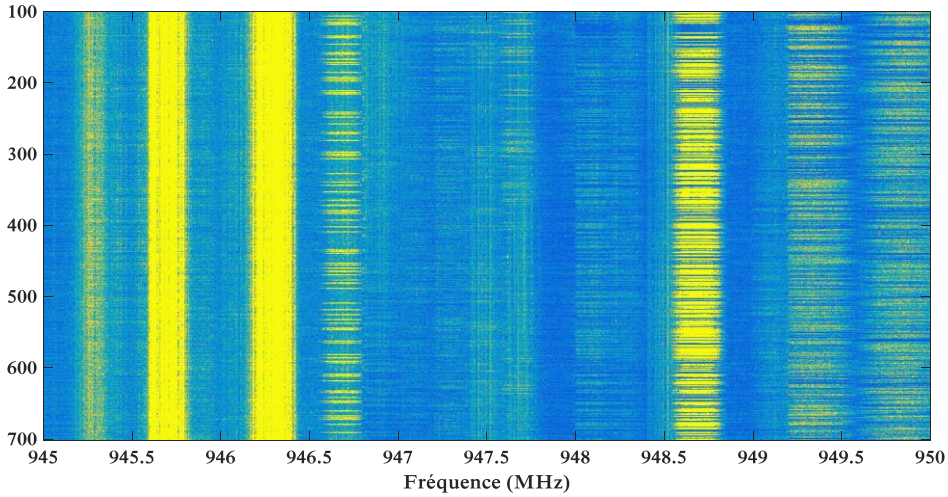



Figure 3. 23: Visualisation Heatmap de la bande balayée.

## 3.3 Conclusion

La technologie de la SDR présente des avantages économiques significatifs. Elle permet de réaliser rapidement et à moindre coût les développements nécessaires pour prendre en charge de nombreux protocoles existants ainsi que ceux en cours de spécification. La clé RTL-SDR à faible coût peut être utilisée comme récepteur SDR pour balayer, analyser et démoduler certains signaux dans la plage de fonctionnement de son tuner. La clé RTL-SDR et MATLAB ouvrent de nombreuses possibilités pour la découverte et la mise en œuvre des fonctions des traitements de signal.

Dans ce chapitre, nous avons proposé deux applications dans un contexte de la radio logicielle, en se basant sur les signaux captés par la clé RTL-SDR et l'environnement de développement MATLAB. La première application est une interface graphique capable de communiquer facilement avec toutes les clés RTL-SDR. Cette interface peut être utilisée pour balayer une large bande de fréquence, comme analyseur de spectre en temps réel ou comme démodulateur de signaux FM ou AM. Dans la deuxième application, nous avons décrit l'implémentation DSP que nous avons réalisée pour la détection d'activités fréquentielles sans amélioration matérielle. Notre solution propose la méthode de la moyenne d'ensemble et le lissage pour réduire le bruit à des faibles niveaux. Nous proposons également une nouvelle approche pour calculer automatiquement le seuil de détection. Cela permet de détecter facilement les canaux de fréquence actifs dans la bande autorisée complète de la clé RTL-SDR. Nous avons également proposé une solution simple basée sur la représentation du Heatmap pour montrer les activités des canaux actifs dans une bande balayée.

# Chapitre 4

# Système embarqué pour la localisation à l'aide du réseau GSM à base de la clé RTL-SDR et Raspberry Pi.

## 4.1 Introduction

Au cours des dernières années, la recherche dans le domaine des systèmes de positionnement est devenue un sujet intéressant et d'actualité. Le GPS (Global Positioning System) est l'une des technologies les plus connues. Il est basé sur les signaux du système cellulaire pour trouver la localisation d'un téléphone mobile.

Les systèmes cellulaires n'ayant pas été conçus à l'origine pour le positionnement, la mise en œuvre de différentes méthodes de localisation peut nécessiter des nouveaux équipements pour effectuer les mesures nécessaires à la détermination de l'emplacement et une nouvelle signalisation pour transférer les résultats de mesure à l'unité de détermination de l'emplacement.

Basé sur les fonctions du téléphone mobile et du réseau, on peut diviser les méthodes de localisation en trois catégories [72] :

- Méthode basée sur le réseau (Network-based) : Une ou plusieurs stations de base effectuent les mesures nécessaires et envoient les résultats de mesure à un centre de localisation où la position est calculée. Cette méthode ne nécessite aucune modification matérielle
- Méthode basée sur le Mobile (Mobile-Based) : Le téléphone mobile prend des mesures et détermine la position. Cela permet de se positionner en mode veille en mesurant les canaux de contrôle diffusés par les stations de base.
- Méthode assisté par mobile (Mobile-Assisted) : Elle inclut des solutions dans lesquelles le téléphone mobile effectue des mesures et envoie les résultats à un centre de localisation du réseau pour un traitement ultérieur. Ainsi, la charge de calcul est transférée vers un centre de localisation où des puissants processeurs sont disponibles.

Dans ce chapitre, nous présentons un système embarqué de localisation à base de la clé RTL-SDR et Raspberry Pi3. En utilisant le réseau GSM (Annexe C), l'estimation de la localisation de l'utilisateur s'effectue par le calcul du centre géographique de plusieurs stations de base proches à l'utilisateur. La réception des signaux GSM (canaux de contrôle en diffusion qui contient les informations des stations de base) s'effectue par le récepteur RTL-SDR et la démodulation et l'extraction des données des cellules s'effectuent sur la carte Raspberry Pi3. Ces informations sont utilisées pour trouver les latitudes et longitudes des stations de base proches à l'utilisateur. Le centre géographique de ces stations de base est considéré comme étant la position estimée de l'utilisateur.

La nouveauté et l'avantage de ce système résident dans les points suivants :

- L'utilisation d'un téléphone mobile ou d'une carte SIM (Subscriber Identity Module) n'est pas du tout nécessaire.
- L'extraction des données des réseaux s'effectue sur la carte Raspberry Pi3.
- Il est possible d'utiliser les stations de bases (BTS) des différents opérateurs de réseaux GSM (Ooreedo, Mobilis, Djeezy pour l'Algérie) activant dans une zone géographique pour estimer la localisation.
- Les latitudes et longitudes des stations de base sont obtenues à l'aide de la base de données de Google.
- De plus, il est possible de se localiser d'une manière totalement invisible (sans être détecté ou localisé).

## 4.2 Méthodes de positionnement basé sur le réseau GSM

Il existe deux approches de base pour localiser un téléphone mobile. Le téléphone peut être localisé à l'aide des signaux du système cellulaire ou peut être intégré à un récepteur GPS. Il existe aujourd'hui plusieurs méthodes pour obtenir des informations sur la localisation du téléphone mobile à l'aide des signaux du réseau GSM, tels que : Le temps d'arrivée (ToA, Time of Arrival), La différence de temps d'arrivée (TDOA, Time Difference of Arrival), L'angle D'arrivée (AOA , Angle of Arrival), etc [73]. L'implémentation de ces méthodes de localisation nécessite certaines modifications, logicielles ou matérielles, ou les deux, sur le téléphone mobile et/ou le réseau pour effectuer les mesures nécessaires à la détermination de l'emplacement. La précision de ces méthodes de localisation varie également, comme le montre le tableau 4.1.

| ***La Méthode*** | ***La Précision*** |
|---|---|
| Cell-ID | 10m - 35km |
| L'avance en Temps | 100m - 550m |
| L'angle D'arrivée | 50m - 150m |
| Le Temps D'arrivée | 50m - 150m |
| Assisted-GPS | 3m - 10m |

Tableau 4. 1: Comparaison entre les différentes techniques de localisation en termes de la précision [74].

Nous présentons dans ce qui suit, une brève description des différentes méthodes de localisation (non exhaustive) basée sur les signaux du réseau GSM.

### 4.2.1 Cell Identification

La méthode la plus simple utilisée pour le positionnement en utilisant le réseau GSM est basée sur l'identité de la cellule (Cell Identification), aussi appelée Cell ID. Dans le réseau de l'opérateur, chaque cellule est identifiée de manière unique par un code, qui est l'identité de la cellule (Cell Idendity - CI). En plus du CI, il existe une identité de zone de localisation (Location Area Identity - LAI) composée de l'indicatif du pays du mobile (Mobile Country Code - MCC), de l'indicatif du réseau mobile (Mobile Network Code - MNC) et de l'indicatif de zone géographique (Location Area Code - LAC). CI et LAI combinés sont appelés identité globale de cellule (Global Cell Identity - GCI) et est utilisée pour identifier chaque cellule dans le monde. Avec cette méthode, l'emplacement du mobile est déterminé en identifiant la cellule attachée comme le montre la figure 4.1. La taille d'une cellule peut varier de quelques mètres à quelques kilomètres (voir tableau 4.2). L'estimation de la position ne peut pas être définie en termes de location (x, y) mais en termes de la zone dans laquelle le téléphone mobile peut être trouvé. L'inconvénient de cette méthode est que la précision dépend directement de la taille de la cellule, qui peut être très grande dans les zones rurales. Dans les zones urbaines à forte densité de population, la précision est nettement meilleure en raison de la petite taille des cellules utilisées [75].

| ***Type de Cellule*** | ***Taille de Cellule (km)*** |
|---|---|
| Grande macro-cellule | 3-30 |
| petite macro-cellule | 1-3 |
| Micro-cellule | 0.1-1 |
| Pico-cellule | 0.01-0.1 |
| Nano-cellule | 0.01-0.001 |

Tableau 4. 2 : Différentes Tailles des cellules utilisées dans le réseau GSM [75].

Cette technique de localisation ne nécessite aucune modification dans le réseau ou dans le téléphone mobile. Elle est donc économique.

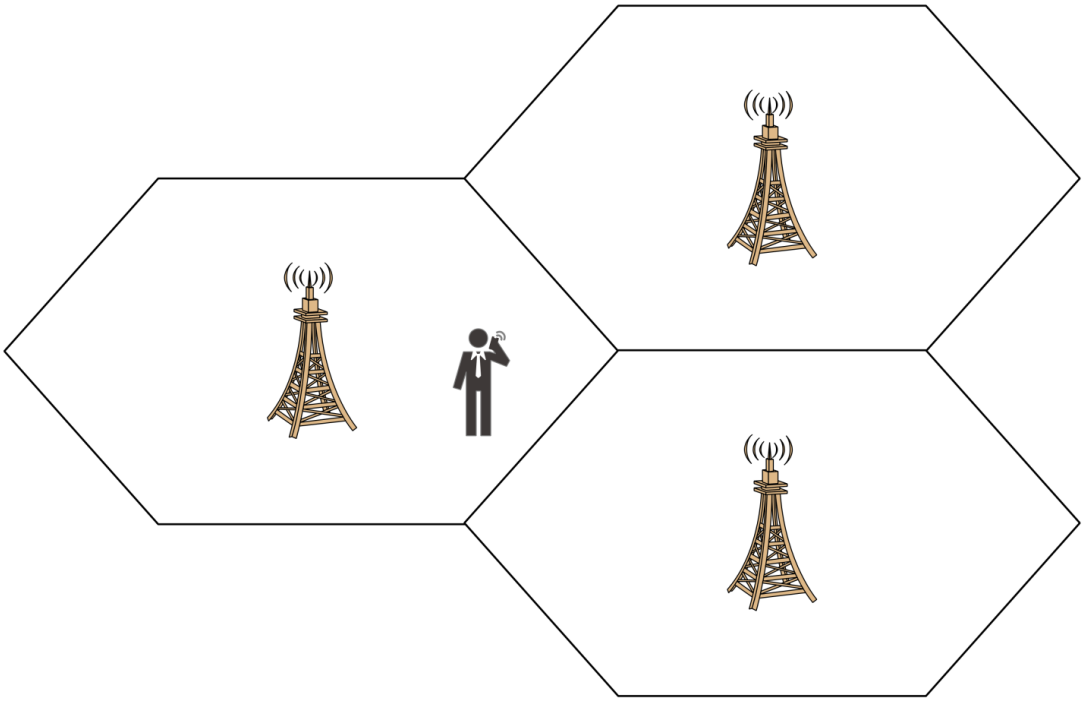


Figure 4. 1: La technique Cell ID.

### 4.2.2 Le temps d'arrivée

Les techniques de positionnement basées sur le temps reposent sur la mesure des temps de parcours des signaux entre les nœuds. Si deux nœuds ont une horloge commune, le nœud recevant le signal peut déterminer le temps d'arrivée (ToA) du signal entrant horodatée (time stamp) par le nœud de référence. Avec cette technique le téléphone mobile mesure le temps d'arrivée des transmissions en provenance d'au moins trois BTSs. Avec ces trois valeurs, le téléphone mobile peut calculer la position par trilatération ou multilatération en sachant la position exacte des BTSs [76] (Voir la figure 4.2).

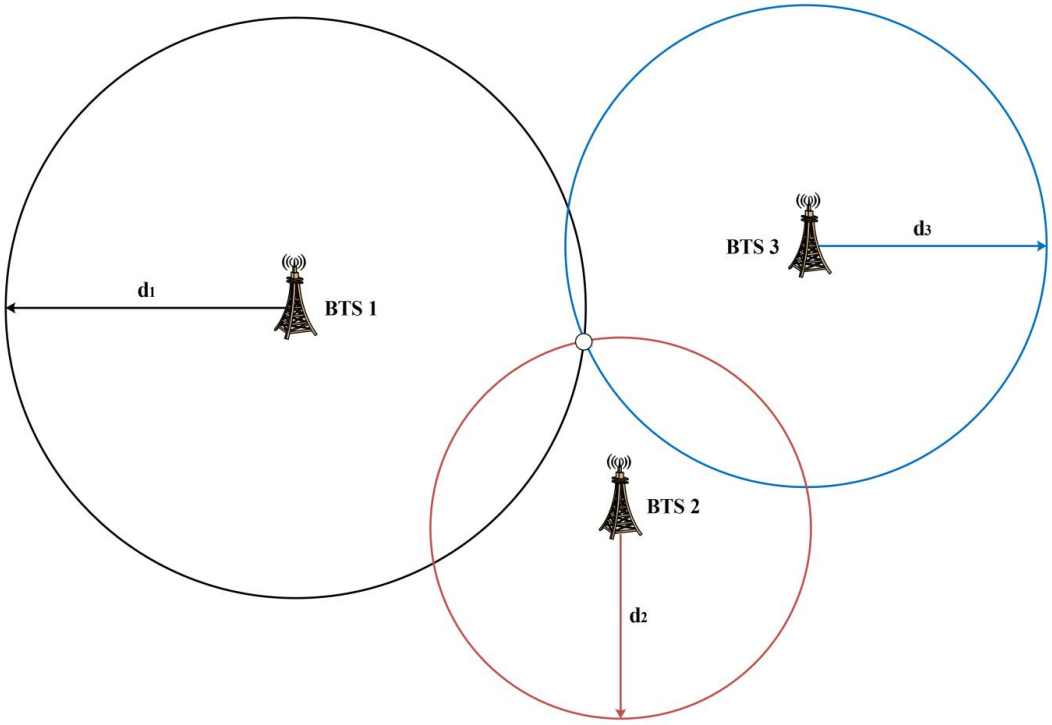



Figure 4. 2: Technique ToA.

Le temps d'arrivée $t_a$ équivaut à la somme du temps de transmission $t_d$ (horodatage de l'horloge de l'émetteur lorsque le signal est transmis) et du temps de propagation (temps nécessaire au signal depuis l'émetteur jusqu'au récepteur). Trois calculs ou plus provenant de différentes BTSs déterminent la position par la triangulation.

$$t_a = t_d + \frac{d}{c} \qquad (4.1)$$

Où $c$ est la vélocité dans le milieu de propagation, généralement la vitesse de la lumière, et $d$ la longueur physique de la liaison de communication.

L'avantage de cette technique est qu'aucune unité de mesure de localisation (Location Measurment Units - LMU) n'est nécessaire dans le réseau et l'algorithme de positionnement est simple. L'inconvénient est que le téléphone mobile doit disposer d'une base de données volumineuse avec les positions géographiques des BTSs ou d'une unité de mesure exacte permettant de mesurer la propagation des signaux. Le coût de cette technique est relativement élevé par rapport à la performance qu'elle offre en matière de précision.

### 4.2.3 La différence de temps d'arrivée

La méthode de différence de temps d'arrivée (TDOA) utilise la différence de temps d'arrivée entre deux signaux provenant de deux nœuds. Cette technique a été proposée comme une solution permettant d'éliminer l'exigence de la synchronisation d'horloge entre l'émetteur et le récepteur.

Dans cet algorithme, le téléphone mobile mesure le ToA à partir de tous les BTSs, puis la différence de temps d'arrivée pour tous les couples de mesures possibles est évaluée. Les différences de distance qui en résultent donnent des courbes hyperboliques entre les BTSs, comme illustré à la figure 4.3. La position d'un téléphone mobile se situe à l'intersection de ces hyperboles. En supposant que les positions des BTSs soient connues, la multilatération peut être effectuée avec un minimum de trois stations de base synchronisées dans le temps [77].

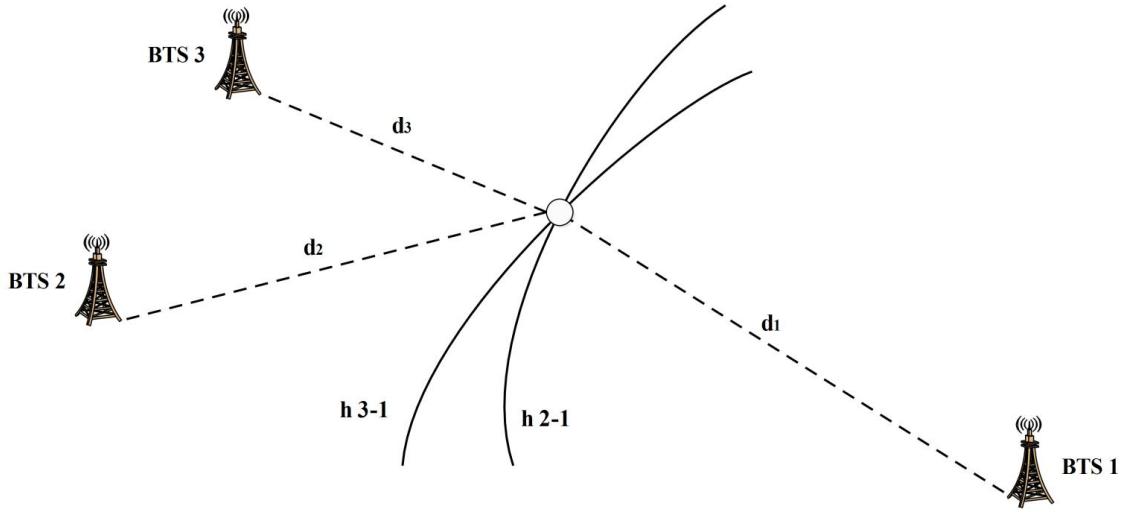



Figure 4. 3: Technique TDOA.

### 4.2.4 L'angle d'arrivée

L'angle d'arrivée (AoA) est une technique de positionnement basée sur la mesure des angles du nœud cible vu par les nœuds de référence. Cette technique est réalisée en utilisant un réseau d'antennes. Pour déterminer l'emplacement d'un nœud dans un espace à deux dimensions (2D), il suffit de mesurer les angles des lignes droites qui relient le nœud et deux nœuds de référence [78].

Dans le réseau GSM et avec cette méthode, deux BTSs séparées par une distance connue mesurent l'angle d'arrivée du signal émis par le téléphone mobile. Ceci est illustré dans la figure 4.4, où l'emplacement de téléphone mobile (utilisateur) est déterminé comme le point d'intersection de deux lignes tirées des BTSs. On voit que la technique AoA nécessite un trajet en visibilité directe (line of sight) entre le téléphone mobile et les BTSs pour des résultats précis. En outre, l'incertitude dans la mesure de l'AoA provoque une incertitude de position qui augmente avec la distance entre le téléphone mobile et le BTS. La précision obtenue dépend du nombre de mesures disponibles. Cette méthode nécessite des BTSs équipées de réseaux d'antennes ou d'antennes directionnelles afin de mesurer les angles des signaux, ce qui augmentent le coût du système.

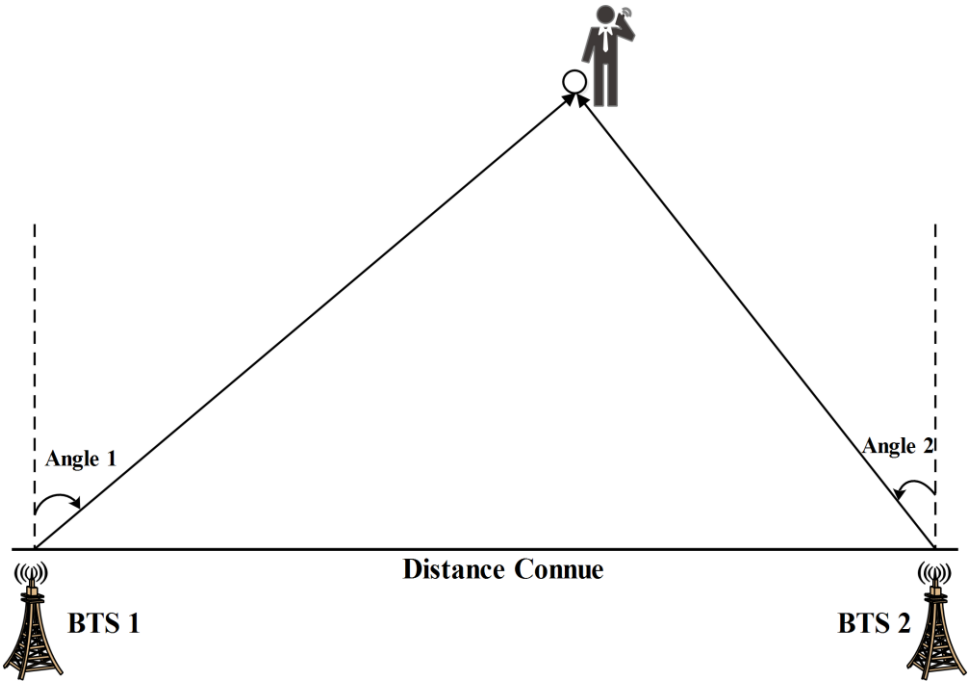



Figure 4. 4: La technique AoA.

## 4.3 Proposition d'un Système de localisation

### 4.3.1 Introduction

La localisation de l'utilisateur à base d'un téléphone mobile ou d'une carte SIM (Subscriber Identity Module) a fait le sujet de plusieurs publications. Trevisani, *et al*, [75], proposent une étude expérimentale de la technique de positionnement Cell ID effectuée aux États-Unis et en Italie. Les résultats obtenus montrent que la distance moyenne entre la position

calculée par le GPS et la position estimée avec le Cell ID est d'environ 500 mètres en Italie et d'environ 800 mètres aux États-Unis. Le système de localisation appelé Place Lab est proposé par LaMarca, *et al*,[79] est basé sur l'utilisation des différents signaux GSM/WiFi/Bluetooth. Les expériences expérimentaux de ce système en utilisant uniquement des signaux GSM et qui utilise la technique Cell ID donnent une précision de 107,2 mètres à Seattle, de 161,4 mètres à Ravenne et de 216,2 mètres à Kirkland. Borenovic, *et al*, [80], propose une technique de localisation améliorée (E-CIDTA) basé sur le Cell ID et le paramètre TA (Time Advance). L'étude montre que la précision de positionnement augmente avec le nombre de BTSs dont le téléphone mobile reçoit, comme indiqué dans le tableau 4.3.

| ***Nombre de BTSs*** | ***Précision (m)*** |
|---|---|
| 2 - 3 | 595 |
| 4 - 5 | 425 |
| 6 - 7 | 200 |
| 8 - 9 | 105 |

Tableau 4. 3: Précision de la technique de localisation E-CIDTA.

Dans ce qui suit, nous proposons une nouvelle technique de localisation basée sur la clé RTL-SDR et la carte Raspberry Pi3 capable d'estimer la position de l'utilisateur en captant les informations des cellules diffusées par les BTSs des différents opérateurs téléphoniques algériens (Ooreedo, Mobilis et Djeezy), sans avoir besoin ni d'un téléphone mobile et ni d'un abonnement téléphonique (carte SIM).

### 4.3.2 Conception du système

Le schéma bloc de notre système est illustré à la figure 4.5. Il comprend deux unités :

- Une clé RTL-SDR de type RTL2832U/R820T2 connectée à une antenne GSM pour la capture et l'acquisition des signaux GSM transmis par les différentes BTSs dans la région.
- Une carte Raspberry Pi3 modèle B avec un processeur à architecture ARM de 1200 MHz, de 1 Go de RAM, de quatre ports USB et d'un un port Ethernet 10/100 [81], pour le traitement numérique des données et l'estimation de la position de l'utilisateur.

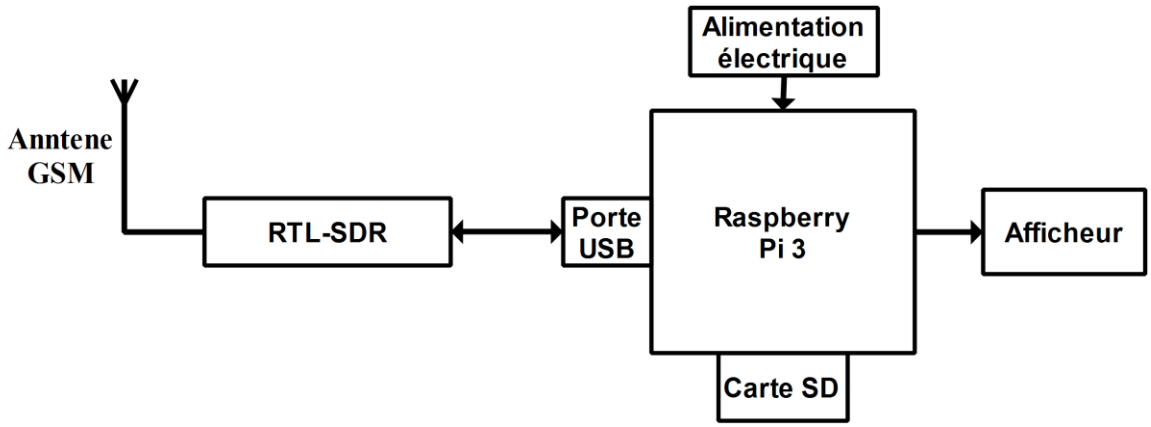



Figure 4. 5: Schéma bloc du système de localisation proposé.

La figure 4.6 illustre une photo du système proposé.


Figure 4. 6: Système proposé à base de la clé RTL-SDR et la carte Raspberry Pi 3.

### 4.3.3 Algorithme de localisation

Le système proposé est passif. Contrairement aux autres méthodes de localisation, notre nouveau système ne nécessite aucune souscription à un opérateur de réseau. Notre système commence par acquérir tous les signaux GSM transmis par les BTSs détectées. Ces signaux sont démodulés pour extraire les données des cellules détectées (Cell Id, LAC, MCC, MNC) utilisées pour le calcul des positions géographiques (latitude et longitude) des BTSs.

L'extraction des données cellulaires est effectuée à l'aide du projet gr-gsm [82]. Après avoir obtenu les informations des cellules, les emplacements des BTSs seront déterminés à l'aide d'une base de données (section 4.3.4). Le système calcule le centroïde (figure 4.7), qui représente la position estimée de l'utilisateur, en utilisant les latitudes et les longitudes de toutes les BTSs détectées.

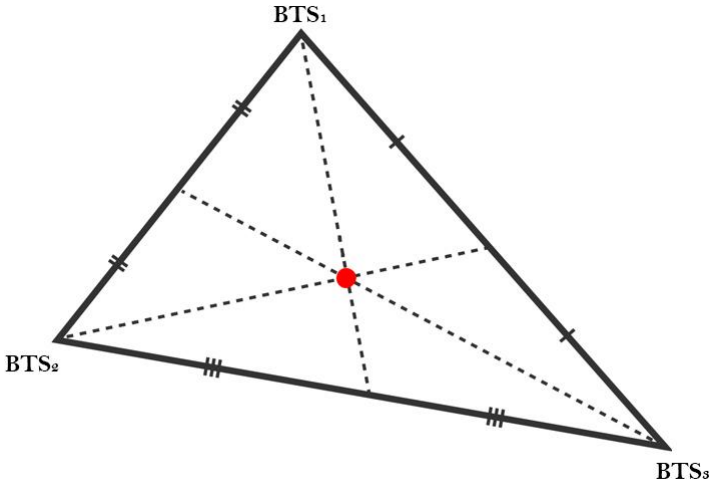



Figure 4. 7: Centroïde de trois BTSs.

L'algorithme de l'estimation de la position de l'utilisateur est donné comme suit :

1- Les latitudes et les longitudes de toutes les BTSs détectées sont converties en coordonnées cartésiennes par les relations suivantes :

$$X_i = \cos(lat_i) \times \cos(lng_i) \quad (4.2)$$
$$Y_i = \cos(lat_i) \times \sin(lng_i) \quad (4.3)$$
$$Z_i = \sin(lat_i) \quad (4.4)$$

Où$(lat_i,\ lng_i)$ sont les emplacements des BTSs en radians.

2- Le centroïde est donné par :

$$X_w = \frac{[(X_1)+(X_2)+\cdots+(X_i)]}{i} \quad (4.5)$$
$$Y_w = \frac{[(Y_1)+(Y_2)+\cdots+(Y_i)]}{i} \quad (4.6)$$
$$Z_w = \frac{[(Z_1)+(Z_2)+\cdots+(Z_i)]}{i} \quad (4.7)$$

Où$(X_w\ , Y_w\ , Z_w)$est la position estimée.

3- Convertir le centroïde $(X_w\ , Y_w\ , Z_w)$ en valeurs de latitude et de longitude :

$$Longitude = \text{atan2}(Y_w, X_w) \quad (4.8)$$

$$Latitude = \text{atan2}(Z_w, H) \quad (4.9)$$

Où $H = \sqrt{X_w^2 + Y_w^2}$

4- Les valeurs de latitude et de longitude données sont en radians et nous devons les convertir en degrés pour obtenir la position estimée finale.

L'organigramme de l'ensemble du système est présenté à la figure 4.8.

### 4.3.4 Base de données des BTSs

Pour appliquer l'algorithme de centroïde géographique à notre système, nous avons besoin d'une base de données contenant l'ensemble des positions géographiques des BTSs. Cette base de données n'est pas accessible au public pour des raisons de confidentialité. Pour surmonter ce problème, nous avons utilisé une base de données basée sur le crowdsourcing [83]. Il existe plusieurs bases de données fournissant des informations sur les emplacements des BTSs, telles que Google Geolocation [84], OpenCellId [85], Mylnikov [86]. Ces bases de données sont accessibles via une API (Application Programming Interface) pour récupérer des données sur les BTSs.

Cependant, ces bases données créent des erreurs par rapport aux positions réelles des BTSs. Nous présentons sur la figure 4.9 l'erreur moyenne introduite par les différentes bases de données : Google Geolocation, OpencellId et Mylnikov en fonction du nombre de BTS utilisées. Nous remarquons que l'erreur moyenne entre la position réelle et la position estimée est plutôt élevée pour les bases de données OpenCellId et Mylnikov. Ceci est principalement dû à l'imprécision des positions géographiques des BTSs. Pour la base de données Google, nous constatons une augmentation nette de la précision.

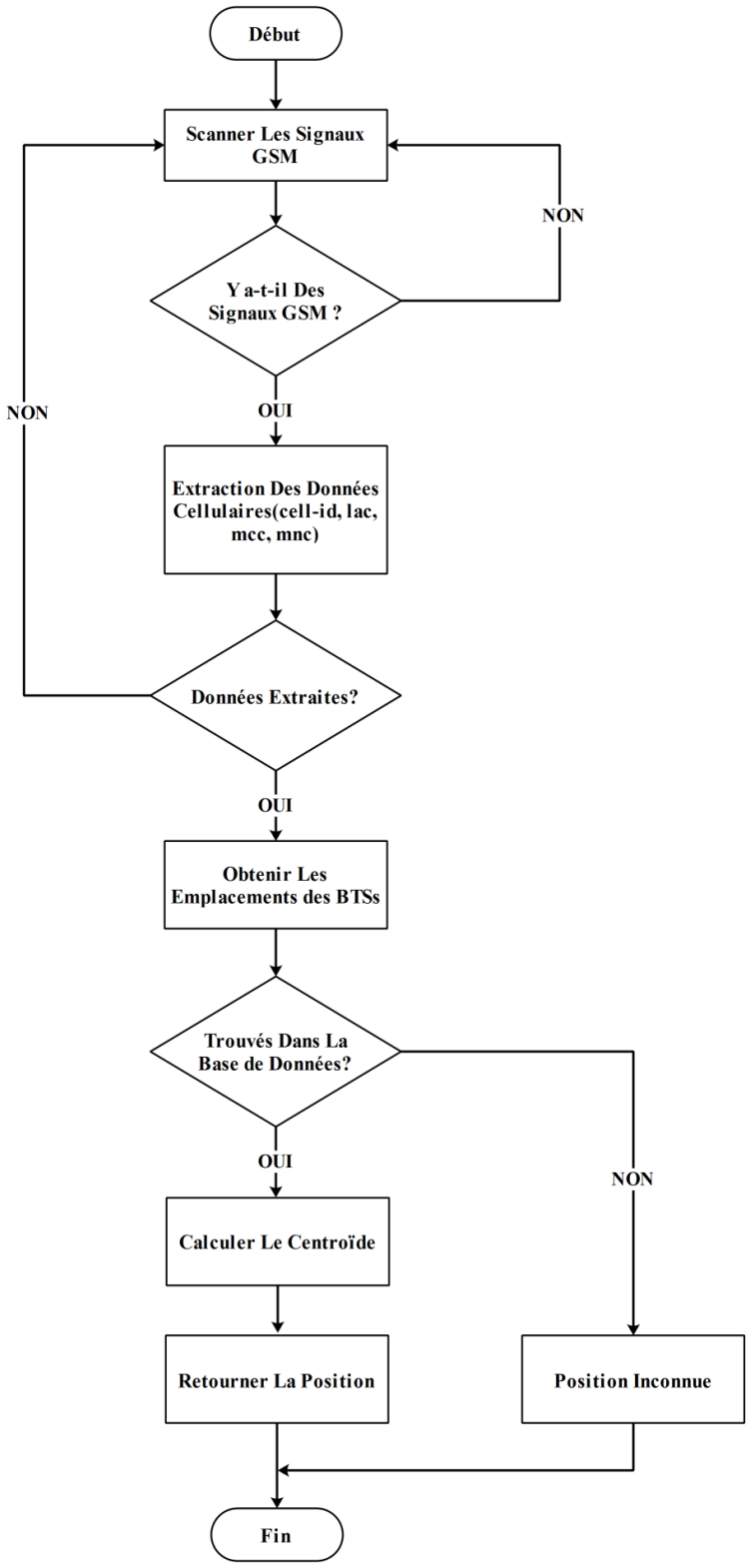



Figure 4. 8: Organigramme du système proposé.

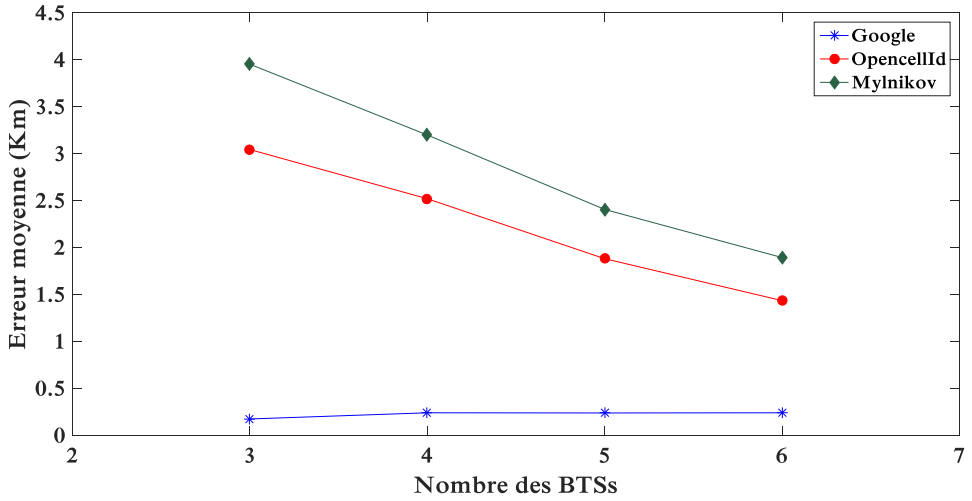



Figure 4. 9: Précision des bases de données Google, OpenCellId, etMylnikov.

Bien que les bases de données basées sur le Crowdsourcing incluent des erreurs dans les positions des stations de base, nous avons obtenu de bons résultats avec notre système en utilisant la base de données Google, ce qui prouve que notre système proposé peut améliorer la technique de positionnement Cell ID si nous avons les positions exactes des BTSs sans la nécessité d'une connexion Internet où la base de données donnée sera incluse dans le système.

### 4.3.5 Résultats expérimentaux et discussion

Dans ce qui suit, nous présentons les résultats obtenus par notre système de localisation. Les expériences sont effectuées dans trois villes algériennes : Oran, Sidi Bel Abbes et Aïn Témouchent. Dans le tableau 4.4, $\Delta E$ représente l'erreur moyenne de la distance entre la position réelle et la position estimée, et les valeurs *Max* et *Min* sont, respectivement, l'erreur de distance maximale et minimale obtenues entre la position réelle et la position estimée. Afin de mieux évaluer la précision de notre système, nous avons comparé la position estimée par notre système à la position réelle en utilisant 3, 4, 5 et 6 BTSs et ceci pour les différents opérateurs (Ooredoo, Mobilis et Dejezzy), pour 20 positions différentes comme indiqué dans le tableau 4.5. Les valeurs en gras soulignées données sur chaque ligne du tableau 4.5, représentent les plus petites erreurs introduites par notre système en fonction du nombre de BTSs utilisées. Nous constatons clairement qu'il nous est impossible de définir le nombre de BTSs à utiliser pour obtenir une meilleure estimation de la position de l'utilisateur. Nous nous sommes contentés à ajuster notre système à utiliser jusqu'à 6 BTSs, sachant que celui-ci peut recevoir jusqu'à 20 BTSs.

| | ***3 BTSs*** | ***4 BTSs*** | ***5 BTSs*** | ***6 BTSs*** |
|---|---|---|---|---|
| $\Delta \boldsymbol{E}$ (km) | 0.271 | 0.259 | 0.268 | 0.271 |
| $\boldsymbol{Max}$ (km) | 0.5328 | 0.4671 | 0.5160 | 0.8987 |
| $\boldsymbol{Min}$ (km) | 0.09378 | 0.04088 | 0.02176 | 0.02123 |

Tableau 4. 4: Résultats expérimentaux pour Oran, Sidi Bel Abbes et Aïn Témouchent.

| | ***3 BTSs*** | ***4 BTSs*** | ***5 BTSs*** | ***6 BTSs*** |
|---|---|---|---|---|
| **Erreur de Position 1 (km)** | 0.4380 | 0.4485 | 0.3985 | **0.1607** |
| **Erreur de Position 2 (km)** | 0.4873 | 0.3410 | 0.5160 | **0.3052** |
| **Erreur de Position 3 (km)** | 0.5328 | 0.3423 | 0.2286 | **0.1895** |
| **Erreur de Position 4 (km)** | **0.3415** | 0.4430 | 0.3581 | 0.5054 |
| **Erreur de Position 5 (km)** | 0.1264 | 0.08308 | **0.04565** | 0.08520 |
| **Erreur de Position 6 (km)** | 0.0999 | **0.04181** | 0.2790 | 0.3521 |
| **Erreur de Position 7 (km)** | 0.3114 | 0.2651 | 0.3010 | **0.2464** |
| **Erreur de Position 8 (km)** | **0.1138** | 0.1468 | 0.2394 | 0.8987 |
| **Erreur de Position 9 (km)** | 0.1211 | 0.04088 | **0.02176** | 0.09113 |
| **Erreur de Position 10 (km)** | 0.3898 | 0.4540 | 0.2614 | **0.2309** |
| **Erreur de Position 11 (km)** | **0.2210** | 0.3188 | 0.3866 | 0.4054 |
| **Erreur de Position 12 (km)** | **0.1811** | 0.1304 | 0.3403 | 0.2991 |
| **Erreur de Position 13 (km)** | **0.1632** | 0.4671 | 0.2892 | 0.2738 |
| **Erreur de Position 14 (km)** | 0.2502 | **0.2325** | 0.3042 | 0.2428 |
| **Erreur de Position 15 (km)** | 0.09378 | 0.1048 | 0.08588 | **0.02123** |

| | | | | |
|---|---|---|---|---|
| **Erreur de Position 16 (km)** | 0.3653 | 0.3200 | 0.2689 | **0.1513** |
| **Erreur de Position 17 (km)** | 0.5318 | 0.3178 | 0.2715 | **0.2178** |
| **Erreur de Position 18 (km)** | **0.2120** | 0.2869 | 0.3760 | 0.3482 |
| **Erreur de Position 19 (km)** | 0.2505 | 0.2378 | 0.2262 | **0.2176** |
| **Erreur de Position 20 (km)** | 0.2059 | 0.1744 | **0.1740** | 0.1788 |

Tableau 4. 5: Erreur de localisation en utilisant un nombre différent des BTSs.

Le choix des BTSs utilisées pour l'estimation de la position est basé sur la puissance du signal reçue. Sur la figure 4.10, les BTSs sont illustrées en marqueur noir et la position estimée en bleu.


Figure 4. 10: Emplacements des BTSs détectées avec leurs puissances reçus.

La figure 4.11 illustre quelques expériences menées à Oran. Les marqueurs en bleu indiquent la position exacte et les marqueurs en noirs montrent les positions estimées. Le tableau 4.6 illustrent les différentes erreurs introduites par l'utilisation de notre système.

| *Position* | *Erreur en mètre* |
|---|---|
| ***Position 1*** | 246 |
| ***Position 2*** | 91 |
| ***Position 3*** | 898 |
| ***Position 4*** | 352 |
| ***Position 5*** | 230 |

Tableau 4. 6: Différentes erreurs introduites par notre système à Oran.

Les performances sont fortement influencées par les positions imprécises des BTSs dans la base de données Google. Il est donc très difficile d'estimer avec une précision très élevée la position de l'utilisateur. Cependant, l'erreur moyenne est d'environ 270 mètres, ce qui est très satisfaisant en la comparant aux résultats obtenus dans [75], qui est 500 mètres en Italie et de 800 mètres aux États-Unis.


Figure 4. 11: Quelques expériences à Oran.

L'avantage de notre système proposé consiste à l'utilisation des données cellulaires de tous les opérateurs dans la région. D'autre part, ce système pourrait être utile dans d'autres services de localisation, tels que *resourcediscovery services* et *voice location based*

*services*. *resourcediscovery services* consiste à chercher toutes les ressources autour de l'emplacement de l'utilisateur (banque, restaurant, etc.), avec une précision de 270 mètres, notre système pourrait être efficace. Dans la technique *voice location based services*, l'utilisateur fournit sa position vocalement, puis le système essaie de localiser l'utilisateur en fonction de l'entrée vocale [75]. Notre système peut améliorer les performances du processus de reconnaissance dans les *voice location based services* en réduisant la zone de recherche et donc la taille de la grammaire à la reconnaissance vocale automatique (Automatic Speech Recognizer).

## 4.4 Conclusion

Dans ce chapitre, nous avons présenté un système de localisation à faible coût utilisant un récepteur RTL-SDR et une carte Raspberry Pi3 basé sur la méthode de positionnement Cell ID. Ce nouveau système de localisation est indétectable, et n'a nullement besoin d'une carte SIM. Il utilise les BTSs des différents opérateurs de réseau GSM activant dans une zone géographique de l'utilisateur.

Malgré les erreurs introduites par la base de données Crowdsourcing de Google, les résultats obtenus par notre système sont très encourageants. En effet, en utilisant une base de données de positions exactes des BTSs intégrée à notre système, notre algorithme pourrait probablement améliorer la technique de positionnement Cell ID et ceci sans utiliser de connexion Internet.

# Conclusion Générale & Perspectives

La technologie de la radio logicielle a de nombreuses applications qui permettent la manipulation des signaux radio avec un ordinateur personnel. Une des plateformes SDR peu coûteuse est celle dite RTL-SDR. Ces plateformes SDR peuvent être combinés avec un logiciel libre, beaucoup plus il est intéressant et aisé de développer des algorithmes propres pour implémenter différents traitements sur les signaux acquis afin de créer des récepteurs numériques.

Ce travail de thèse a porté sur l'étude et la réalisation des applications liées à la radio logicielle en se focalisant sur la plateforme RTL-SDR, la plateforme qui a été mise à notre disposition. Pour cela, nous avons introduit les concepts de la radio logicielle idéale et restreinte. Ensuite nous avons détaillé le fonctionnement de la plateforme RTL-SDR, son architecture et ses limites. Nous avons réussi à développer un algorithme dédié à la correction de la fréquence de l'oscillateur local au sein des clés RTL-SDR. L'algorithme proposé peut facilement être utilisé avec d'autres dispositifs SDR. L'algorithme en question est basé sur le burst de correction de fréquence transmit par les stations de base GSM dans le canal de signalisation.

Nous avons développé une application SDR avec une interface graphique qui simplifie aux utilisateurs les manipulations des dongles RTL-SDR et automatiser les différentes tâches de configuration et d'acquisition assujettis à des commandes tordus. L'application ainsi proposée permet d'effectuer des balayages manuelles sur une bande spectrale souhaitée, la démodulation des signaux FM et les signaux AM, etc. L'objectif consiste à appliquer des fonctions de traitement de signal (DSP) sur les données I / Q captés par la clé RTL-SDR, ce qui ouvre un horizon infini de perspectives.

Nous avons proposé un algorithme de détection des fréquences qui contiennent une activité spectrale. Nous avons utilisé la méthode de la moyenne d'ensemble pour améliorer la qualité du signal et minimiser le bruit, nous avons montré que cette méthode est efficace pour la diminution des niveaux des bruits. Après le conditionnement du signal, un ensemble des traitements du signal sont appliqués afin de détecter les fréquences qui contiennent une activité spectrale. En outre, une solution a été aussi proposée pour montrer l'activité spectrale basée sur le principe de la représentation dite Heatmap. Cela nous aidera à découvrir dans la plage scannée les fréquences qui contiennent une activité très élevée et celle qui contiennent une activité très faible en fonction de leurs puissances reçues. A ce niveau la quasi-totalité des développements ont été réalisés sous l'environnement MATLAB ©.

Dans le dernier chapitre, nous avons proposé un système embarqué dédié à la localisation. Ce dernier est à base de la clé RTL-SDR et la carte Raspberry Pi3. La localisation est effectuée en utilisant les signaux de signalisations du réseau GSM. Ce système utilise les

données des cellules (MCC, MNC, LAC, CID) transmises par les BTSs de tous les opérateurs dans la région afin d'estimer où l'utilisateur se trouve. Les résultats des expériences sont effectués dans trois villes algériennes, Oran, Sidi Bel Abbes et Aïn Témouchent, nous avons trouvé des résultats intéressants sans avoir besoin d'un téléphone mobile ou d'une carte SIM, ce qui rend notre système totalement invisible (sans être détecté ou localisé). Ce système aussi pourrait être utile dans d'autres services de localisation, tels que *resource discovery services* et *voice location based services.*

L'objectif majeur reste l'application des algorithmes développés et leurs améliorations sur l'une des plateformes SDR performantes à l'image de celles cités dans les premiers chapitres.

# Annexe A

# Transmission FM avec Raspberry PI

## A.1 Description

À l'aide d'une application appelée Pi-FM-RDS [87], la carte Raspberry Pi peut être utilisé pour produire un signal FM sur le port GPIO 4 (General Purpose Input/Output pins). Ce programme génère une modulation FM, avec des données RDS (Radio Data System) générées en temps réel, inclure un son monophonique ou stéréophonique.

## A.2Installation et Utilisation

L'application Pi-FM-RDS repose sur la bibliothèque *sndfile* , alors la premier étape consiste à installer cette bibliothèque en utilisant la commande suivante :

```
sudo apt-get install libsndfile1-dev
```

Nous exécutons ensuite les commandes suivantes pour installer l'application Pi-FM-RDS :

```
git clone https://github.com/ChristopheJacquet/PiFmRds.git
cd PiFmRds/src
make clean
make
```

Maintenant l'application est installée, pour tester la transmission Fm en utilisant la commande suivante(voir figure A.1):

```
sudo ./pi_fm_rds -audio sound.wav
```

Ceci générera une transmission FM sur la fréquence 107,9 MHz, avec le nom de station par défaut (PS), le text radio (RT) et le code PI. Le signal radiofréquence est émis sur leport GPIO 4 de la carte Raspberry Pi.

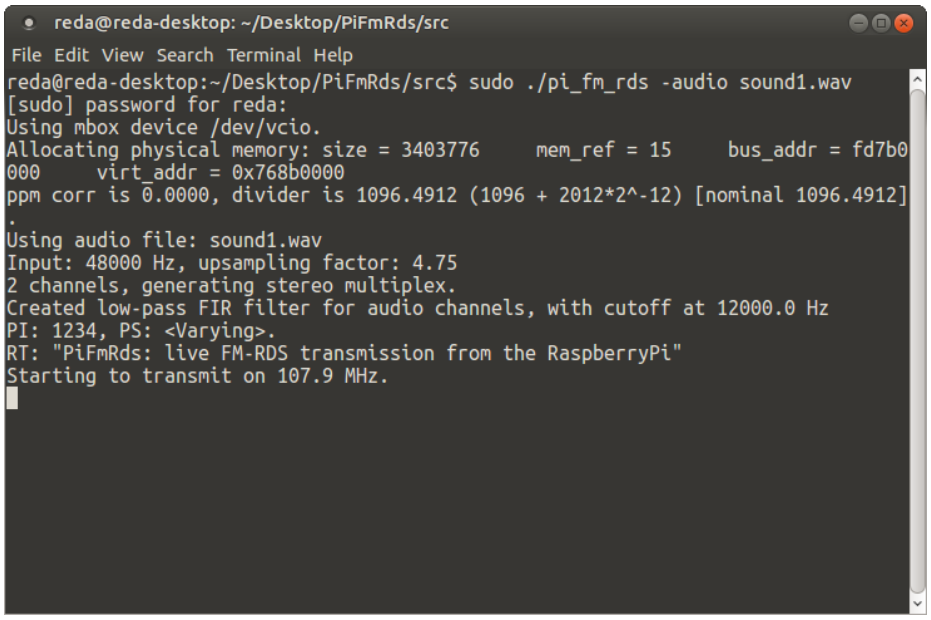



Figure A. 1: Résultat d'exécution l'application Pi-FM-RDS avec succès.

Pour changer la fréquence de transmission, le nom de station, le text radio, et les autres paramètres, en utilisant la syntaxe suivante :

*pi_fm_rds [-freq freq] [-audio file] [-ppm ppm_error] [-pi pi_code] [-ps ps_text] [-rt rt_text]*

- **-freq** spécifie la fréquence porteuse (en MHz). Exemple: -freq 107.9,
- **-audio** spécifie un fichier audio à lire en tant qu'audio,
- **-pi** spécifie le code PI de la diffusion RDS. 4 chiffres hexadécimaux,
- **-ps** spécifie le nom de la station FM,
- **-rt** spécifie le text radio (RT) à transmettre,
- **-ppm** spécifie l'erreur d'oscillateur de la carte Raspberry Pi en ppm.

Elle est préférable de connecter un fil de cuivre sur leport GPIO 4 de la carte Raspberry Pi comme une antenne pour augmenter la portée de transmission.

# Annexe B

# Transmission FM Stéréophonique

## B.1 Modulation de Fréquence

La modulation de fréquence (FM) est largement utilisée dans la radiodiffusion. La modulation de fréquence est réalisée par la variation de la fréquence du signal porteuse en fonction du signal modulant ou message. L'une des méthodes les plus simples pour générer des signaux FM consiste à utiliser un oscillateur commandé en tension (VCO) [88].

Une analyse mathématique pour la modulation de fréquence d'une sinusoïde $s_i(t)$(signal de message) donnera l'équation de signal FM $x_{FM}(t)$ suivante :

$$x_{FM}(t) = A_c\,[\cos\left(2\pi f_c t + \ 2\pi k_m \int_0^t s_i(t)d(t)\right)]$$

Nous allons définir un exemple de signal d'information sinusoïdal $s_i(t)$ ayant l'amplitude $A_i$ et la fréquence $f_i$, en substituant ce signal de message dans la formule ci-dessus, nous trouvons :

$$x_{FM}(t) = A_c\,[\cos\left(2\pi f_c t + \frac{k_m A_i}{f_i}\sin(2\pi f_i t)\right)]$$

$$x_{FM}(t) = A_c\,[\cos\left(2\pi f_c t + \frac{\Delta f}{f_i}\sin(2\pi f_i t)\right)]$$

$$x_{FM}(t) = A_c\,[\cos(2\pi f_c t + \beta\,\sin(2\pi f_i t))]$$

Où $\Delta f$c'est de déviation de fréquence et $\beta$c'est l'indice de modulation.

La figure B.1 montre le signal d'information où c'est un signal sinusoïdal et le signal modulé FM, on peut constater que la fréquence instantané du signal modulé FM varie en fonction de signal d'information.

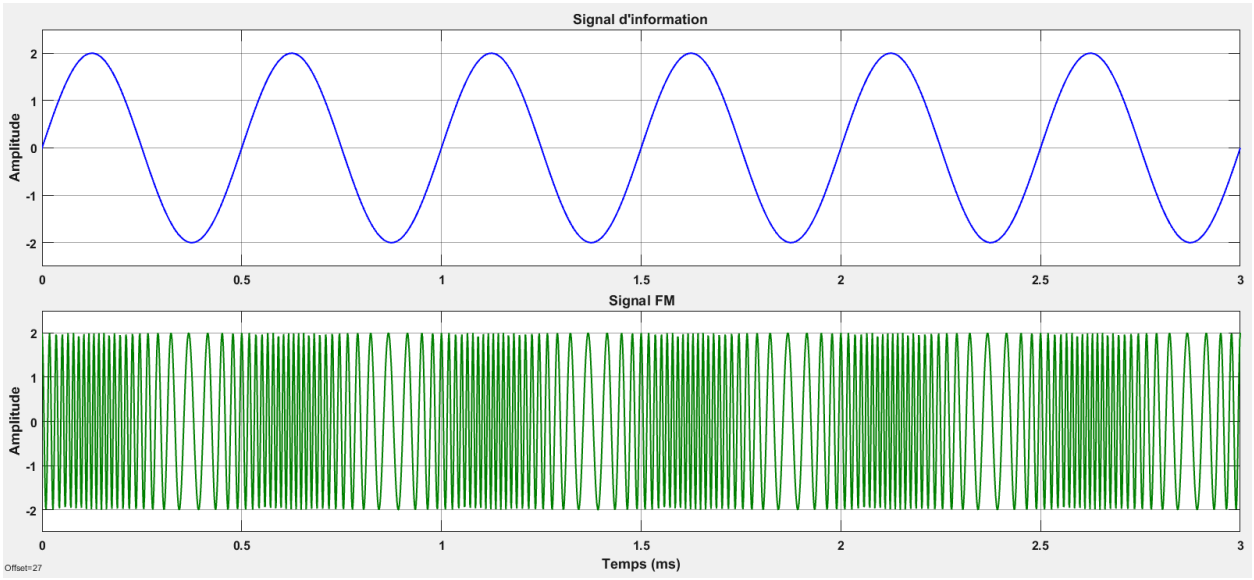



Figure B. 1 : modulation de fréquence.

## B.2 L'émission FM Stéréophonique

En 1961, la FCC (Federal Communications Commission) a approuvé la transmission du son stéréophonique, ce qui élargit l'idée du multiplexage des signaux pour générer un son stéréo [87]. L'une des principales exigences du signal multiplex stéréo était la compatibilité avec les anciens récepteurs monophoniques FM largement utilisés. Pour atteindre cet objectif, la partie du signal stéréophonique en bande de base comprise entre 0 et 15 KHz devait contenir les la somme des signaux issus des deux microphones gauche (G) et droit (D), (G + D) pour la réception monophonique. Pour le son stéréophonique, le signal différence (G-D) module en amplitude sans porteuse (bande latérale double) une sous-porteuse à 38 kHz dans la région de 23 à 53 kHz du spectre en bande de base. Une fréquence pilote de 19 kHz est ajoutée au signal composite pour permettre aux récepteurs FM stéréophonique de détecter et de décoder les canaux stéréo gauche et droit [89]. Le schéma block d'un multiplexeur stéréophonique est donné en figure B.2.

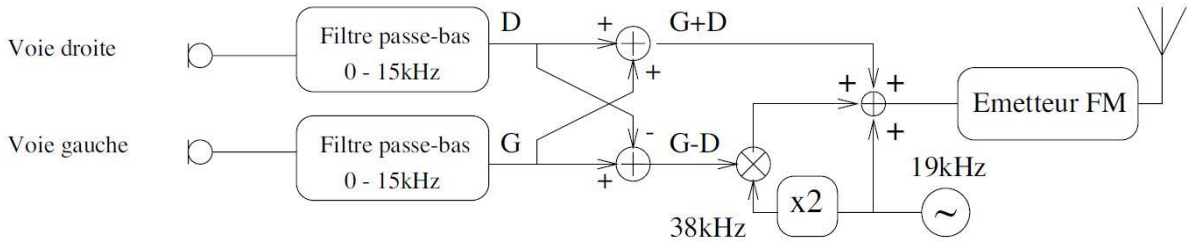



Figure B. 2: Schéma d'un multiplexeur stéréophonique.

Le signal stéréophonique actuellement comprend une sous-porteuse de 57 kHz qui achemine les signaux RDS (Radio Data System) permet de transporter des informations textuelles, telles que des informations sur la circulation, la météo et la station de radio, qui peuvent être affichées sur l'écran de l'appareil de l'utilisateur. [90]. La figure B.3 montre le spectre d'un signal stéréophonique en bande de base.

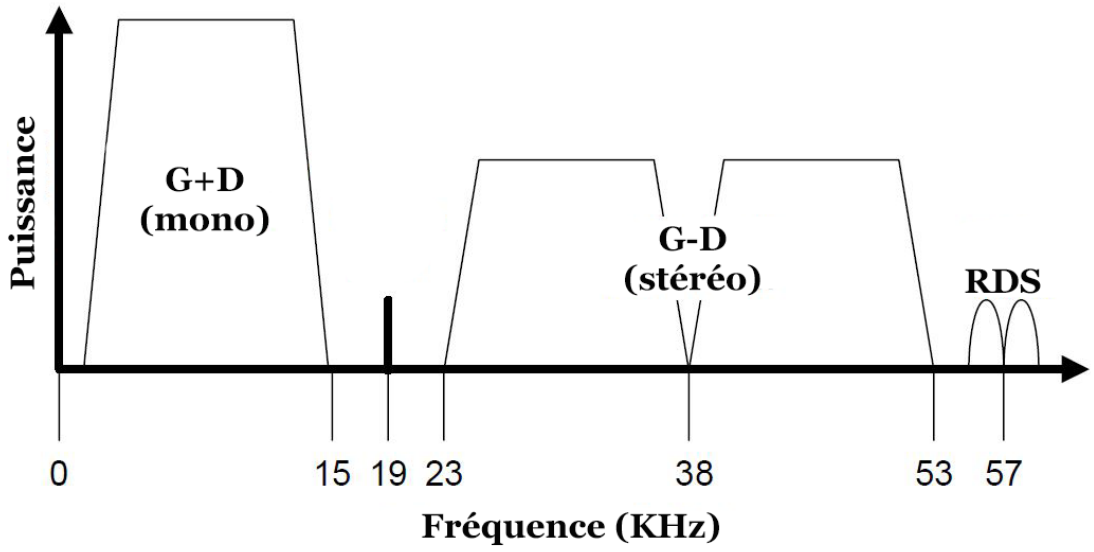



Figure B. 3: Spectre de signal stéréo en bande de base.

A la réception et à la sortie de démodulateur FM, on retrouve ce signal stéréophonique (figure B.3) composite et le décodeur va séparer les canaux G et D. Un filtre passe-bas à 15KHz récupère l'information G+D, et un filtre passe-bande ou une PLL récupère la fréquence pilote pour produire le 38 kHz afin d'effectuer une démodulation synchrone et un filtre passe-bas en sortie du multiplieur récupère l'information G-D. Par addition et soustraction des deux signaux G+D et G-D, on retrouve les deux canaux G et D.

# Annexe C

# Présentation du réseau GSM

## C.1 Introduction

GSM est un acronyme qui signifie Global System for Mobile Communications. L'acronyme français original signifie Groupe Spécial Mobile. Le GSM est une technologie cellulaire numérique utilisée pour la transmission de services de voix et de données élaborée par l'ETSI (The European Telecommunications Standards Institute) au cours des années 80 et 90. Le GSM permet aux utilisateurs de se déplacer de manière transparente d'un réseau à l'autre, tout en offrant une mobilité personnelle. De plus, les canaux de parole et de signalisation sont numérisés. Depuis son lancement en 1991, le GSM est rapidement devenu le système de téléphonie mobile le plus populaire au monde. En octobre 2018, environ 5,1 milliards d'abonnés dans plus de 219 pays utilisaient le GSM [91].

Ce système fonctionne sur plusieurs bandes de fréquences (voir tableau C.1), les plus courantes sont les 900 MHz, 1800 MHz et 1900 MHz.

| ***Système*** | ***Bande (MHz)*** | ***Liaison Montante*** | ***Liaison Descendante*** | ***Numéro du canal*** |
|---|---|---|---|---|
| GSM 850 | 850 | 824 - 849 | 869 - 894 | 128 - 251 |
| GSM 900 (P-GSM) | 900 | 890 - 915 | 935 - 960 | 1 - 124 |
| GSM 900 (E-GSM) | 900 | 880 - 915 | 925 - 960 | 975 -1023, (0, 1-124) |
| GSM-R (R-GSM)) | 900 | 876 - 880 | 921 - 925 | 955 - 973 |
| DSC 1800 | 1800 | 1710 - 1785 | 1805 - 1880 | 512 - 885 |
| PCS 1900 | 1900 | 1850 - 1910 | 1930 - 1990 | 512 - 810 |

Tableau C. 1: Bandes de fréquences allouées en GSM.

Le réseau GSM est basé sur un système cellulaire. Dans un système cellulaire, la région couverte est divisée en cellule, ces cellules sont modélisées de manière simplifiée sous forme d'hexagones comme illustré à la figure C.1 et gérés par des stations de base (BTS – Base Transceiver Station). La plupart des modèles montrent la station de base au milieu de la cellule. L'idée de base d'un réseau cellulaire est de partitionner la gamme de fréquences disponible, de n'affecter que des parties de ce spectre de fréquences à une station de base et de réduire la portée d'une station de base afin de réutiliser les fréquences dans des autres cellules. Afin d'éviter les interférences entre les différentes stations de base, deux cellules adjacentes ne doivent jamais utiliser les mêmes fréquences [58].

La taille des cellules peut varier de quelques mètres à quelques kilomètres selon qu'il s'agisse d'une zone urbaine, suburbaine ou rurale. Dans les zones urbaines à forte densité d'utilisateurs, de petites cellules sont utilisées pour prendre en charge un plus grand nombre d'utilisateurs. Contrairement aux zones rurales où la densité d'utilisateurs est faible, les grandes cellules sont préférées.

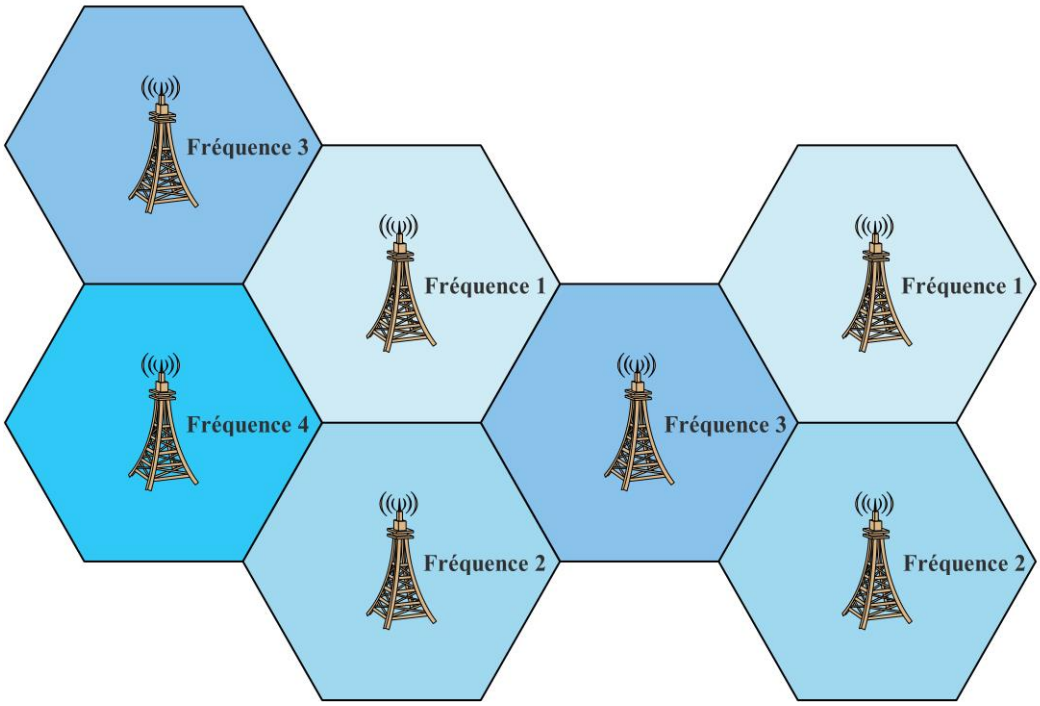



Figure C. 1: Architecture cellulaire dans un réseau GSM.

## C.2 Architecture du réseau

L'architecture simplifiée du réseau GSM est illustrée dans la figure C.2. Un réseau GSM unique établi et exploité par un fournisseur de services est appelé réseau mobile terrestre public (PLMN - Public Land Mobile Network). Un système GSM comprend deux composants principaux : l'infrastructure fixe installée et les abonnés mobiles, qui utilisent les services du réseau et communiquent via l'interface radio (air interface). Le réseau GSM fixe peut être divisé en trois sous-système: le sous-système radio (BSS - Base Station Subsystem), le sous-système réseau (NSS - Network Subsystem), et le sous-système opérationnel (OSS - Operating Sub-System). Les sous-sections suivantes décrivent brièvement les entités clés d'un réseau GSM.

### C.2.1 La station mobile

Les fonctions principales de la station mobile consistent à transmettre et à recevoir de la voix et des données via l'interface radio du système GSM. La station mobile exécute les fonctions de traitement du signal consistant à numériser, coder, protéger contre les erreurs, chiffrer et moduler les signaux transmis. Il exécute également les fonctions inverses sur les signaux reçus de la station de base. La station mobile est composée d'une part du téléphone mobile appelé équipement mobile (ME – Mobile Equipment) et d'autre part du module d'identité d'abonné (SIM – Subscriber Identity Module). Chaque téléphone mobile est identifié par un code unique appelé IMEI (International Mobile Equipment Identity). La carte SIM est uniquement identifiée par l'International Mobile Subscriber Identity (IMSI), qui sert à identifier l'abonné dans n'importe lequel des systèmes GSM. Elle assure un accès sécurisé à un réseau particulier car elle contient des algorithmes utilisés pour l'authentification et pour la génération d'une clé de cryptage et contient également des informations relatives à l'abonné [92].

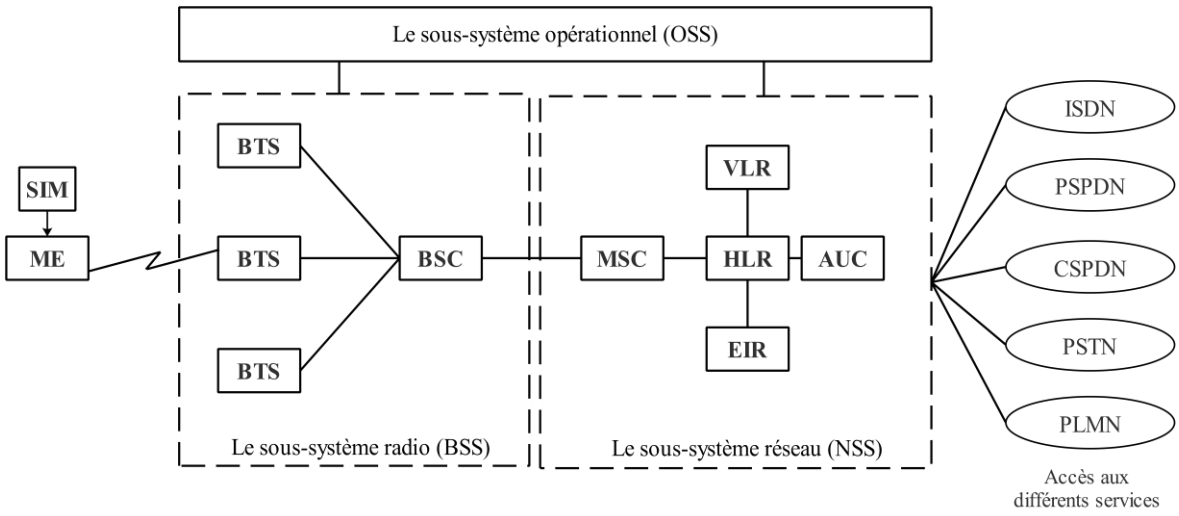



Figure C. 2: Architecture simplifiée d'un réseau GSM [93].

### C.2.2 Le sous-système radio

Le sous-système radio(BSS) comme la montre dans la figure C.2 comprend deux éléments, le premier est la station de base (BTS). Le BTS est le point d'accès de la station mobile au réseau. Il s'agit d'un émetteur-récepteur responsable sur les communications radio entre le réseau et la station mobile. Il gère le codage de la parole, le cryptage, et la modulation / démodulation des signaux radio …etc. L'interface entre la station mobile et le BTS est appelée l'interface radio ou l'interface air.

Le second est le contrôleur de station de base (BSC – Base Station Controler). Le BSC est le centre d'intelligence du sous-système radio. Un seul BSC contrôle un ou plusieurs BTS, et gère la configuration des canaux radio les transferts intercellulaires (handover intra-BSC)

et les autres fonctions de contrôle nécessaires, en plus établit le lien physique entre les BTS et le commutateur de service mobile (MSC – Mobile Switching Center). L'interface entre le BTS et le BSC s'appelle l'interface A bis. La station de base (BTS) et le contrôleur de station de base (BSC) constituent le sous-système radio (BSS).

### C.2.3 Le sous-système réseau

Le sous-système réseau (NSS) comprend les centres de commutation mobile (MSC - Mobile Switching Center) et les bases de données qui stockent les données nécessaires à la gestion supplémentaire des abonnés et de la mobilité (voir figure C.2). Le NSS contrôle plusieurs BSS et son rôle principal est d'établir les communications entre deux utilisateurs. L'interface entre les deux sous-systèmes BSS et le NSS s'appelle l'interface A [92]. Les différentes composantes du NSS sont :

*Centre de commutations mobiles (MSC - Mobile Switching Center)* :Le MSC est le composant de base du sous-système réseau. Ce composant contrôle plusieurs BSC, il gère l'acheminement des appels, l'établissement des appels, il fournit également les fonctions de gestion pour la mobilité des terminaux, telles que l'authentification, les informations de localisation et les transferts intercellulaire (inter-BSC, inter-MSC handover), il assure également l'interconnexion entre le réseau de téléphone cellulaire et le réseau fixe.

*Registre des abonnés locaux (HLR – Home Location Register)* : Le HLR est la base de données centrale qui stocke en permanence des données sur les abonnés. Le HLR conserve des informations spécifiques à l'abonné, telles que le MSISDN (Mobile Subscriber Integrated Services Digital Network), l'IMSI (International Mobile Subscriber Identity), l'emplacement actuel de la station mobile, les fonctionnalités supplémentaires de l'abonné. Un PLMN peut contenir un ou plusieurs HLR: cela dépend du nombre d'abonnés mobiles, de la capacité de l'équipement et de l'organisation du réseau [94].

*Registre des abonnés visiteurs (VLR – Visitor Location Register)* : Le VLR est une base de données conçue pour limiter le nombre de demandes de renseignements adressées au HLR. Il contient des informations similaires à celles du HLR, mais uniquement pour les abonnés se trouvant actuellement dans sa zone de localisation, il mémorise donc de façon temporaire les données concernant tous les abonnés qui appartiennent à la surface géographique qu'il contrôle. Le VLR réduit le nombre total de requêtes adressées au HLR et réduit donc le trafic réseau. Les VLR sont souvent identifiés par l'indicatif régional (LAC - Location Area Code) de la région qu'ils desservent. Un VLR peut être responsable des zones d'un ou de plusieurs MSC.

*Centre d'authenticité (AuC – Authentication Center)* : Outre les registres HLR et VLR, deux bases de données supplémentaires sont définies dans le système GSM. Ils sont

responsable de divers aspects de la sécurité du système, il s'agit du centre d'authenticité (AuC) et registre d'identification d'équipement et registre d'identification d'équipement (EIR – Equipement Indentity Register).

Le centre d'authentification (AuC) est associé à un HLR. Il mémorise une clé d'identité secrète pour chaque abonné mobile enregistré avec le HLR associé. Cette clé est utilisée pour générer les données utilisées pour authentifier l'identité internationale d'abonné mobile (IMSI) et pour chiffrer la communication entre la station mobile et le réseau [94].

*Registre d'identification d'équipement (EIR – Equipement Indentity Register)* : L'EIR est une base de données annexe contenant les identités IMEI des terminaux mobiles. Il n'y a qu'une seule base de données EIR par réseau. Elle est composée de trois listes. La liste blanche, la liste noire et la liste grise. La liste blanche contient toutes les identités d'équipement (liste des IMEI) autorisées à communiquer. La liste noire contient toutes les identités d'équipement refusées pour une raison quelconque, incluent l'IMEI répertorié comme volé ou cloné ou le téléphone n'est pas homologué pour fonctionner sur le réseau. La liste grise est une liste d'IMEI dont l'activité suspecte doit être surveillée.

### C.2.4 Le sous-système opérationnel

Le sous-système opérationnel (OSS) contient toutes les fonctions nécessaires à l'exploitation et à la maintenance du réseau, l'OSS est relié avec le sous-système NSS et avec les contrôleurs des stations de base (BSC) [93]. Il assure :

- détection de pannes ;
- administration commerciale (déclaration des abonnés, terminaux, facturation…) ;
- gestion de la sécurité ;
- exploitation et gestion des performances (trafic) ;
- contrôle de la configuration du système ;

## C.3 Interface radio

La liaison sans fil entre la station de base (BTS) et le téléphone mobile est appelé l'interface radio ou l'interface air. Dans l'interface radio, le GSM utilise une combinaison de deux techniques de multiplexage, la technique d'accès multiple par répartition en fréquence (FDMA - Frequency Division Multiple Access) et la technique d'accès multiple par répartition dans le temps (TDMA - Time Division Multiple Access), la figure C.3 la structure FDMA/TDMA dans le réseau GSM. La technique de modulation utilisée pour

porter le signal à haute fréquence est la modulation GMSK (*Gaussian Minimum Shift Keying*).

Avec la technologie FDMA, la bande de fréquence est divisée en porteuses ou canaux, d'une largeur de 200 kHz chacun. Chaque canal est divisé en huit intervalles de temps distincts (nommé TS0 à TS7 pour Time Slot en anglais) comme le montre dans la figure C.3. Cette division de fréquence dans le domaine temporel est appelée TDMA. Ces huit intervalles de temps ensemble constituent une trame TDMA. Un abonné est autorisé à utiliser un intervalle de temps par trame. La durée d'une trame est de 4,615 ms, donc un seul intervalle de temps ne dure que 0,5769 ms et le signal radio émis dans un intervalle de temps est souvent appelé burst.

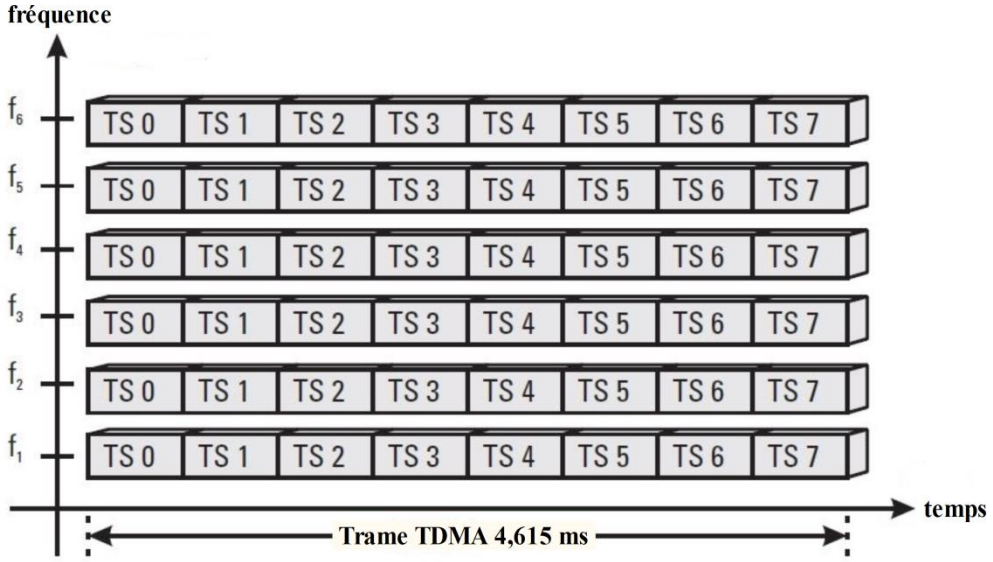



Figure C. 3: Structure FSMA/TDMA dans le réseau GSM [92].

Les trames TDMA sont regroupées pour former des multi trames. On distingue deux types de multi trame, l'une avec 26 trames TDMA élémentaires utilisé pour transporter le trafic et l'autre avec 51 trames élémentaires pour la signalisation. Une super trame est composée de 26 multi trames de type 51 ou indifféremment 51 multi trames de type 26. L'hyper trame est composé de 2048 super trames, sa période est de 3h 28mn 53s 760 ms. La figure C.4 présente la structure hiérarchique de trames, leurs périodes et d'autres détails, jusqu'au niveau d'une burst (un seul intervalle de temps) unique constituant la plus petite unité.

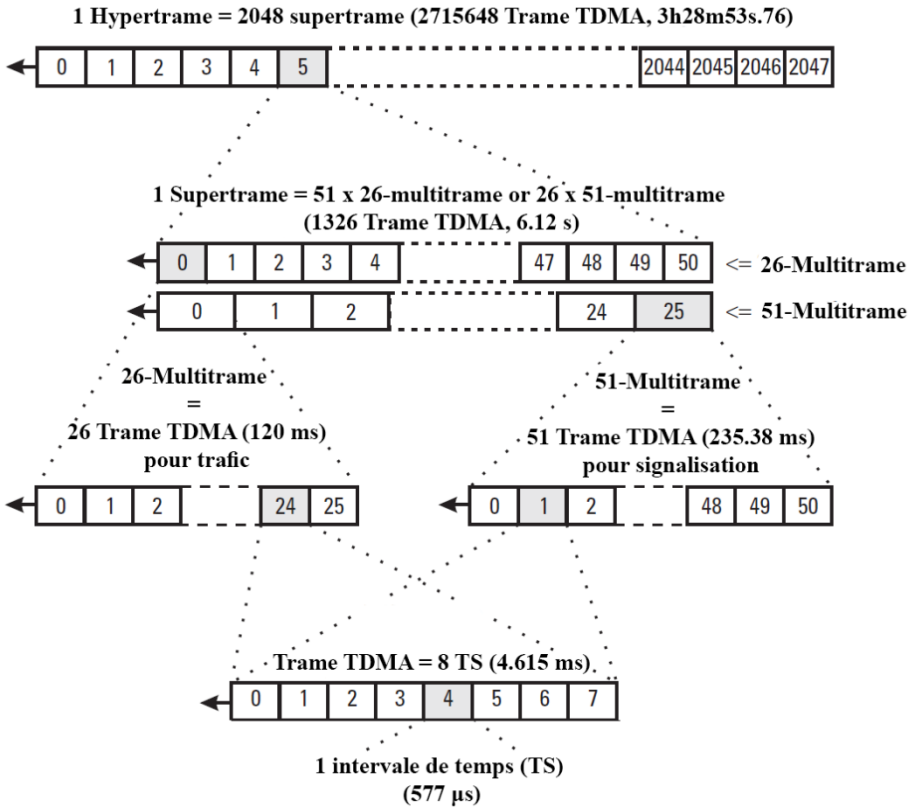



Figure C. 4: Structure hiérarchique de trames dans le GSM [92].

La répétition périodique d'un intervalle de temps dans la trame TDMA sur une fréquence particulière constitue un canal physique. Ces canaux physiques transportent des canaux logiques via l'interface radio.

Les canaux logiques remplissent une multitude de fonctions, tels que le transport de charge utile, la signalisation, la diffusion d'informations générales sur le système, la synchronisation et l'attribution de canaux, etc. À n'importe quel moment, une fréquence/intervalles de temps peut être soit un canal de trafic, soit certains canaux de contrôle. En d'autres termes, un canal logique décrit le fonctionnement et la fonction d'un canal physique à un moment donné [95].

Les canaux logiques sont divisés en deux catégories les canaux de trafic (Trafic Channel) et les canaux de signalisation (Broadcast Channel, Common Control Channel, Dedicated Control Channel). Le tableau C.2 montre ces canaux avec une brève description.

| *Type* | *Nom* | *Fonction* |
|---|---|---|
| **Voie Balise (Unidirectionnel en diffusion) Broadcast Channel (BCH)** | Frequency Correction Channel (FCCH) | Correction de la fréquence porteuse |
| | Synchronisation Channel (SCH) | Synchronisation en temps et l'identité de la BTS |
| | Broadcast Control Channel (BCCH) | Informations sur la cellule |
| **Common Control Channel (CCCH)** | Paging Channel (PCH) | Utilisé pour informer le téléphone mobile du trafic entrant. |
| | Random Access Channel (RACH) | Utilisé par le téléphone mobile pour demander un canal sur lequel il peut envoyer ou recevoir des informations de trafic ou de signalisation. |
| | Access Grant Channel (AGCH) | Allocation de ressource. |
| | Cell Broadcast Channel (CBCH) | Utilisé pour diffuser des informations spécifiques aux abonnés du réseau. comme la météo, la circulation, etc. |
| **Dedicated Control Channel** | Standalone Dedicated Channel (SDCCH) | Principalement utilisé pour la configuration de l'appel, les mises à jour de localisation et les SMS. |
| | Slow Associated Control Channel (SACCH) | Transmet des informations sur la cellule voisine, telles que la qualité du signal, et la cellule serveur, ce qui aide à prendre la décision du Handover. |
| | Fast Associated Control Channel (FACCH) | Utilisé pour la signalisation urgente (non planifiée) comme les déconnexions d'appels et l'handover. |
| **Traffic** | Traffic Channel (TCH) | Utilisé pour envoyer de la parole et des données à et de l'utilisateur. |

Tableau C. 2: Classification des canaux logiques GSM [96].

## C.4 La voie balise

La voie balise ou les canaux de contrôle en diffusion (Broadcast Channel - BCH) utilisés par le BTS pour envoyer les paramètres de système et les informations de synchronisation vers les téléphone mobile dans l'entourage. Ce signal ne véhicule pas les informations d'utilisateur, et sert au contrôle du système.

La voie balise fournit des informations générales (informations spécifiques à une cellule), y compris les informations nécessaires pour que la téléphone mobile puisse s'enregistrer dans le système et choisir le meilleur BTS. Après avoir initialement accédé au mobile, le BTS calcule le niveau de puissance requis de la téléphone mobile et envoie un ensemble de commandes de puissance sur ce canal. Les autres informations envoyées sur ce canal comprennent l'indicatif de pays du mobile (Mobile Country Code - MCC), l'indicatif de réseau mobile (Mobile Network Code - MNC) et de l'indicatif de zone géographique (Location Area Code – LAC), les canaux RF utilisés dans la cellule où se trouve le mobile, les fréquences balise des cellules voisines, etc [93].

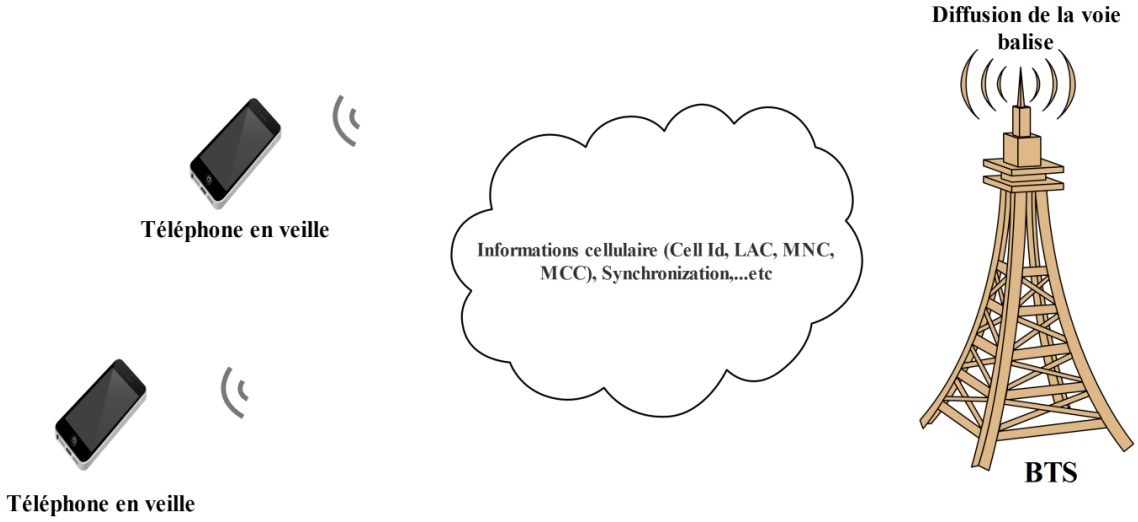



Figure C. 5: Par la voie balise le BTS diffuse les informations de contrôle vers tous les mobiles dans la cellule.

# Références Bibliographiques


**[1]** Joseph III. Mitola. Software radio architecture: object-oriented approaches to wireless systems engineering. Wiley, 2000.

**[2]** Tribble, Alan C. "The software defined radio: Fact and fiction." In 2008 IEEE Radio and Wireless Symposium, pp. 5-8. IEEE, 2008.

**[3]** Mitola, Joe. "Software radios." IEEE Communications magazine 33, no. 5 (1995): 24-25.

**[4]** Galustov, G. G., S. P. Brovchenko, and V. V. Klimenko. "Effects of Noise Parameters of a Radio Receiver on its Dynamic Blocking Range." Telecommunications and Radio Engineering 71, no. 13 (2012).

**[5]** Bondarev, I. N., A. P. Platonov, and A. M. Sukhov. "Technologies for Digital Television Broadcasting in the Internet and Cellular Networks." Telecommunications and Radio Engineering 67, no. 19 (2008).

**[6]** Microwaves101, " Why Fifty Ohms? ". Accessed April 29, 2019. https://www.microwaves101.com/encyclopedias/why-fifty-ohms.

**[7]** Semlali, Hayat. "Développement de nouvelles structures et d'algorithmes appliquant l'échantillonnage aléatoire pour des systèmes de types radio logicielle et radio cognitive." PhD diss., Université De Nanates, 2015.

**[8]** Mao, Shiwen, Yingsong Huang, Yihan Li, Prathima Agrawal, and Jitendra Tugnait. "Introducing software defined radio into undergraduate wireless engineering curriculum through a hands-on approach." In Proc. The 2013 ASEE Annual Conference, pp. 1-10. 2013.

**[9]** Johnson, P. "New research lab leads to unique radio receiver." E-Systems Team 5, no. 4 (1985): 6-7.

**[10]** Cook, Peter G., and Wayne Bonser. "Architectural overview of the SPEAKeasy system." IEEE Journal on Selected areas in Communications 17, no. 4 (1999): 650-661.

**[11]** Mitola, Joseph. "Software radios: Survey, critical evaluation and future directions." IEEE Aerospace and Electronic Systems Magazine 8, no. 4 (1993): 25-36.

**[12]** Wirelessinnovation. "About the Wireless Innovation Forum". Accessed April 29, 2019. http://www.wirelessinnovation.org/about-us.

**[13]** Hasan, M. S., M. LaMacchia, L. Muzzelo, R. Gunsaulis, LTC Richard Housewright, and J. Miller. "Designing the joint tactical radio system (JTRS) handheld, manpack, and small form fit (HMS) radios for interoperable networking and waveform applications." In MILCOM 2007-IEEE Military Communications Conference, pp. 1-6. IEEE, 2007.

**[14]** Naoues, Malek. "Management d'opérateurs communs dans les architectures de terminaux multistandards." PhD diss., Supélec, 2013.

**[15]** Badarou, Aminath. "Etude et développement d'une architecture radio numérique innovante dans le contexte des communications aéronautiques." PhD diss., université de Nantes, 2013.

**[16]** Palicot, Jacques, Christophe Moy, Merouane Debbah, Romain Couillet, Hamidou Tembine, Renaud Séguier, Daniel Le Guennec et al. "De la radio logicielle à la radio intelligente." (2010): 432-p.

**[17]** Taj, Muhammad Imran. "Network on chip based multiprocessor system on chip for wireless software defined cognitive radio." PhD diss., Université Paris-Est, 2011.

**[18]** Grayver, Eugene. Implementing software defined radio. Springer Science & Business Media, 2012.

**[19]** Reed, Jeffrey Hugh. Software radio: a modern approach to radio engineering. Prentice Hall Professional, 2002.

**[20]** Alaus, Laurent. "Architecture reconfigurable pour un équipement radio multistandard." PhD diss., Université Rennes 1, 2010.

**[21]** Tuttlebee, Walter HW, ed. Software defined radio: enabling technologies. John Wiley & Sons, 2003.

**[22]** Barrandon, Ludovic. "Synthèse architecturale analogique/numérique appliquée aux systèmes sur puce dans un contexte radio logicielle." PhD diss., Université Rennes 1, 2005.

**[23]** Giannini, Vito, Jan Craninckx, and Andrea Baschirotto. Baseband analog circuits for software defined radio. Springer Science & Business Media, 2008.

**[24]** Tucker, D. G. "The history of the homodyne and synchrodyne." Journal of the British Institution of Radio Engineers 14, no. 4 (1954): 143-154.

**[25]** Colin, Elizabeth. "Architecture reconfigurable pour la numérisation du signal radio de récepteurs mobiles multi-standards." PhD diss., Télécom ParisTech, 2003.

**[26]** Razavi, Behzad. "Design considerations for direct-conversion receivers." IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing 44, no. 6 (1997): 428-435.

**[27]** Mirabbasi, Shahriar, and Ken Martin. "Classical and modern receiver architectures." IEEE Communications Magazine 38, no. 11 (2000): 132-139.

**[28]** Burciu, Ioan. "Architecture de récepteurs radiofréquences dédiés au traitement bibande simultané." PhD diss., INSA de Lyon, 2010.

**[29]** Traverso, Sylvain. "Transposition de fréquence et compensation du déséquilibre IQ pour des systèmes multiporteuses sur canal sélectif en fréquence." PhD diss., Université de Cergy Pontoise, 2007.

**[30]** Yamada, Shuhei, Olga Boric-Lubecke, and Victor M. Lubecke. "Cancellation techniques for LO leakage and DC offset in direct conversion systems." In 2008 IEEE MTT-S International Microwave Symposium Digest, pp. 1191-1194. IEEE, 2008.

**[31]** Mikkelsen, Jan Hvolgaard, Troels Emil Kolding, Torben Larsen, Thomas Klingenbrunn, Klaus Ingemann Pedersen, and P. Mogensen. "Feasibility study of DC offset filtering for UTRA-FDD/WCDMA direct-conversion receiver." In Proceedings 17th NORCHIP Conference, vol. 1999, pp. 34-39. 1999.

**[32]** Sampei, Seiichi, and Kamilo Feher. "Adaptive DC-offset compensation algorithm for burst mode operated direct conversion receivers." In [1992 Proceedings] Vehicular Technology Society 42nd VTS Conference-Frontiers of Technology, pp. 93-96. IEEE, 1992.

**[33]** Grave, Baptiste. "Techniques de sous-échantillonnage appliquées aux récepteurs radio à 60 GHz en technologie 28 nm CMOS." PhD diss., Lille 1, 2013.

**[34]** Sun, Yi-Ran, and Svante Signell. "Effects of noise and jitter in bandpass sampling." Analog Integrated Circuits and Signal Processing 42, no. 1 (2005): 85-97.

**[35]** Sun, Yi-Ran. "Generalized bandpass sampling receivers for software defined radio." PhD diss., KTH, 2006.

**[36]** Wang, Xiangyang, and Shuyang Yu. "A feasible rf bandpass sampling architecture of single-channel software-defined radio receiver." In 2009 WRI International Conference on Communications and Mobile Computing, vol. 1, pp. 74-77. IEEE, 2009.

**[37]** Rtl-sdr. "ROUNDUP OF SOFTWARE DEFINED RADIOS". Accessed April 29, 2019, https://www.rtl-sdr.com/roundup-software-defined-radios/.

**[38]** Ettus. "USRP". Accessed April 29, 2019. https://www.ettus.com/product/quick-order.

**[39]** Dickens, Michael L., Brian P. Dunn, and J. Nicholas Laneman. "Design and implementation of a portable software radio." IEEE Communications Magazine 46, no. 8 (2008): 58-66.

**[40]** Akeela, Rami, and Behnam Dezfouli. "Software-defined Radios: Architecture, state-of-the-art, and challenges." Computer Communications 128 (2018): 106-125.

**[41]** Haldren III, Harold A. "Studies in Software-Defined Radio System Implementation." (2014).

**[42]** Minden, Gary J., Joseph B. Evans, Leon Searl, Daniel DePardo, Victor R. Petty, Rakesh Rajbanshi, T. Newman et al. "Kuar: A flexible software-defined radio development platform." In 2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 428-439. IEEE, 2007.

**[43]** Cao, Siyang, Yuan F. Zheng, and Robert L. Ewing. "S-band radar based on Lyrtech Software Defined Radio." In NAECON 2014-IEEE National Aerospace and Electronics Conference, pp. 415-419. IEEE, 2014.

**[44]** Nagel, Stefan. "Portable Waveform Development for Software Defined Radios." PhD diss., KIT-Bibliothek, 2011.

**[45]** Digikey. "LMS6002D Field-Programmable RF (FP-RF) Transceiver IC". Accessed April 29, 2019. https://www.digikey.com/en/product-highlight/l/lime-microsystems/lms6002d-fieldprogrammable-rf-fprf-transceiver-ic

**[46]** Nuand. "bladeRF USB 3.0 Software Defined Radio". Accessed April 29, 2019. www.nuand.com/bladeRF-brief.pdf

**[47]** Nuand. Accessed April 29, 2019. https://www.nuand.com/

**[48]** Stewart, Robert W., Louise Crockett, Dale Atkinson, Kenneth Barlee, David Crawford, Iain Chalmers, Mike McLernon, and Ethem Sozer. "A low-cost desktop software defined radio design environment using MATLAB, simulink, and the RTL-SDR." IEEE Communications Magazine 53, no. 9 (2015): 64-71.

**[49]** Laufer, Carl, and Edward J. Hoffman. The Hobbyist's Guide to the RTL-SDR: Really Cheap Software Defined Radio: A Guide to the RTL-SDR and Cheap Software Defined Radio by the Authors of the RTL-SDR. com Blog. Carl Laufer, 2016.

**[50]** Radioforeveryone. "RTL-SDR Generations". Accessed April 29, 2019. http://www.radioforeveryone.com/p/rtl-sdr-generations-this-is-absolutely.html.

**[51]** Rtl-sdr. "What is RTL-SDR? ". Accessed April 29, 2019. https://www.rtl-sdr.com/about-rtl-sdr/.

**[52]** Datasheet. " R820T". Accssed 29 April, 2019. https://rtl-sdr.com/wp-content/uploads/2013/04/R820T_datasheet-Non_R-20111130_unlocked.pdf

**[53]** Wickert, Mark A., and McKenna R. Lovejoy. "Hands-on software defined radio experiments with the low-cost rtl-sdr dongle." In 2015 IEEE Signal Processing and Signal Processing Education Workshop (SP/SPE), pp. 65-70. IEEE, 2015.

**[54]** Markgraf, S. "kalibrate-rtl." Accessed April 29, 2019. https://github.com/steve-m/kalibrate-rtl.

**[55]** Rtl-sdr. "Turns your Realtek RTL2832 based DVB dongle into a SDR receiver." Accessed April29, 2019. https://github.com/steve-m/librtlsdr.

**[56]** Evrytania. "LTE Cell Scanner. "Accessed April 29, 2019. http://www.evrytania.com/lte-tools/78-default-category/77-lte-cell-scanner.

**[57]** Calvo-Palomino, Roberto, Fabio Ricciato, Domenico Giustiniano, and Vincent Lenders. "Ltess-track: A precise and fast frequency offset estimation for low-cost sdr platforms." In Proceedings of the 11th Workshop on Wireless Network Testbeds, Experimental evaluation & CHaracterization, pp. 51-58. ACM, 2017.

**[58]** Heine, Gunnar, and Matt Horrer. GSM networks: protocols, terminology, and implementation. Artech House, Inc., 1999.

**[59]** Varma, G. Narendra, Usha Sahu, and G. Prabhu Charan. "Robust frequency burst detection algorithm for GSM/GPRS." In IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004, vol. 6, pp. 3843-3846. IEEE, 2004.

**[60]** Gabriel C, Pablo FM , Beatriz GS , Carlos HV . " Alessandro M, Pol T . GSM sniffer for "passive" radio infrastructure mapping – and channel characterization." Aalborg university, 2011.

**[61]** Rtl-sdr. "THE BIG LIST OF RTL-SDR SUPPORTED SOFTWARE." Accessed April 29, 2019. https://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/.

**[62]** Yagoub R., B. Benadda , M. Benaissa, A. Taleb-Ahmed, A. Lahouel, F. Zane. "Low Cost SDR receiver implementation using RTL-SDR dongle." Telecommunications and Radio Engineering 78, no. 8 (2019).

**[63]** Mathworks. "Display frequency spectrum of time-domain signals." Accessed April 29, 2019. https://www.mathworks.com/help/dsp/ref/dsp.spectrumanalyzer-system-object.html.

**[64]** Stewart, Robert W., Kenneth W. Barlee, Dale SW Atkinson, and Louise H. Crockett. Software defined radio using MATLAB & Simulink and the RTL-SDR. Strathclyde Academic Media, 2015.

**[65]** Smith, Steven W. "The scientist and engineer's guide to digital signal processing." (1997).

**[66]** Wickert, Mark A., and McKenna R. Lovejoy. "Hands-on software defined radio experiments with the low-cost rtl-sdr dongle." In 2015 IEEE Signal Processing and Signal Processing Education Workshop (SP/SPE), pp. 65-70. IEEE, 2015.

**[67]** Sonelec."Préaccentuation/Désaccentuation." Accessed April 29, 2019. https://www.sonelec-musique.com/electronique_bases_diffusion_fm_preac_desac.html

**[68]** Laufer, Carl, and Edward J. Hoffman. The Hobbyist's Guide to the RTL-SDR: Really Cheap Software Defined Radio: A Guide to the RTL-SDR and Cheap Software Defined Radio by the Authors of the RTL-SDR.com Blog. Carl Laufer, 2016.

**[69]** Wilkins, Charles L., Sam P. Perone, Charles E. Klopfenstein, Robert C. Williams, and Donald E. Jones. "Ensemble Averaging of Repeatable Noisy Signals." In Digital Electronics and Laboratory Computer Experiments, pp. 121-128. Springer, Boston, MA, 1975.

**[70]** Yagoub R., M. Benaissa, and B. Benadda. "Nearby Carrier Detection Based on Low Cost RTL-SDR Front End." Wireless Personal Communications: 1-18.

**[71]** Press, William H., Saul A. Teukolsky, William T. Vetterling, and Brian P. Flannery. Numerical recipes 3rd edition: The art of scientific computing. Cambridge university press, 2007.

**[72]** Laitinen, Heikki, Suvi Ahonen, Sofoklis Kyriazakos, Jaakko Lähteenmäki, Raffaele Menolascino, and Seppo Parkkila. "Cellular location technology." Public deliverable of IST/CELLO project (2001).

**[73]** Gustafsson, Fredrik, and Fredrik Gunnarsson. "Mobile positioning using wireless networks: possibilities and fundamental limitations based on available wireless network measurements." IEEE Signal processing magazine 22, no. 4 (2005): 41-53.

**[74]** Willaredt, Jonas. "WiFi and Cell-ID based positioning-protocols, standards and solutions." SNET Project WT (2011).

**[75]** Trevisani, Emiliano, and Andrea Vitaletti. "Cell-ID location technique, limits and benefits: an experimental study." In Sixth IEEE workshop on mobile computing systems and applications, pp. 51-60. IEEE, 2004.

**[76]** Sayed, Ali H., and Nabil R. Yousef. "Wireless location." Wiley Encyclopedia of Telecommunications (2003).

**[77]** Zimmermann, Lars, Alexander Goetz, Georg Fischer, and Robert Weigel. "GSM mobile phone localization using time difference of arrival and angle of arrival estimation." In International Multi-Conference on Systems, Sygnals & Devices, pp. 1-7. IEEE, 2012.

**[78]** Gezici, Sinan, Zhi Tian, Georgios B. Giannakis, Hisashi Kobayashi, Andreas F. Molisch, H. Vincent Poor, and Zafer Sahinoglu. "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks." IEEE signal processing magazine 22, no. 4 (2005): 70-84.

**[79]** LaMarca, Anthony, Yatin Chawathe, Sunny Consolvo, Jeffrey Hightower, Ian Smith, James Scott, Timothy Sohn et al. "Place lab: Device positioning using radio beacons in the wild." In International Conference on Pervasive Computing, pp. 116-133. Springer, Berlin, Heidelberg, 2005.

**[80]** Borenovic, Milos N., Mirjana I. Simic, Aleksandar M. Neskovic, and Milos M. Petrovic. "Enhanced cell-ID+ TA GSM positioning technique." In EUROCON 2005-The International Conference on" Computer as a Tool", vol. 2, pp. 1176-1179. IEEE, 2005.

**[81]** Raspberry."What is a Raspberry Pi? ." Accessed April 29, 2019. https://www.raspberrypi.org/help/faqs/#generalDifference.

**[82]** Krysik P. "The gr-gsm project." Accessed April 29, 2019. https://github.com/ptrkrysik/gr-gsm.

**[83]** Alexander J. "Localizing Cell Towers from Crowdsourced Measurements." Bergensis university, 2015.

**[84]** Google. "Developer Guide. "Accessed April 29, 2019. https://developers.google.com/maps/documentation/geolocation/intro.

**[85]** Opencell. "The world's largest Open Database of Cell Towers." Accessed April 29, 2019. www.opencellid.org.

**[86]** Mylnikov A. "Public mobile cells position database. Geo-Location API." Accessed April 29, 2019. https://www.mylnikov.org/.

**[87]** Jacquet C. "FM-RDS transmitter using the Raspberry Pi." Accessed April 29, 2019. https://github.com/ChristopheJacquet/PiFmRds.

**[88]** Lawrence D. "Frequency Modulation (FM) Tutorial". Silicon Laboratories Inc.

**[89]** Muller JP. "La modulation de fréquence". Université internationale de Monaco.

**[90]** Wright SA. "Radio Broadcast Data System (RBDS). " National Association of Broadcasters Engineering Handbook. 9th Edition. pgs. 633 – 642. 1999.

**[91]** Gsma. "GSM Association." Accessed April 29, 2019. https://www.gsma.com/.

**[92]** Eberspaecher, Joerg, Christian Bettstetter, and Hans-Jhorg Vhogel. GSM: Switching, Services and Protocols. John Wiley & Sons, Inc., 2001.

**[93]** Mehrotra, Asha. GSM system engineering. Artech House, Inc., 1997.

**[94]** GSM Technical Specification. "Digital cellular telecommunications system (Phase 2+); Network architecture." Accessed April 29, 2019. https://www.etsi.org/deliver/etsi_gts/03/0302/05.00.00_60/gsmts_0302v050000p.pdf.

**[95]** GSM Technical Specification. "Digital cellular telecommunications system (Phase 2+); Mobile Station - Base Station System (MS - BSS) interface; Channel structures and access capabilities. "Accessed April 29, 2019. https://www.etsi.org/deliver/etsi_gts/04/0403/05.01.00_60/gsmts_0403v050100p.pdf.

**[96]** Nicolas, Michaël. "Radio logicielle: analyse d'architectures matérielles et outils informatiques." École d'ingenieurs CNAM. 2011.

**Publications Scientifiques Parues**

- Reda YAGOUB, Mohamed BENAISSA, and Belkacem BENADDA. "Nearby Carrier Detection Based on Low Cost RTL-SDR Front End." Wireless Personal Communications: 1-18, (2019).

- Reda YAGOUB, Belkacem Benadda , Mohamed Benaissa, Abdelmalik TALEB-AHMED, Ahmed LAHOUEL, Fatima ZANE. "Low Cost SDR receiver implementation using RTL-SDR dongle." Telecommunications and Radio Engineering 78, no. 8 (2019).

**Communications Internationales**

- Reda YAGOUB, Mohamed BENAISSA, Belkacem BENNADA, Fatima Zohra OUNADJELA, and Nafissa BOUHAFNA. "Low cost RTL-SDR based receiver to monitor neighboring 3MHz-2GHz frequency activities." In 2018 International Conference on Signal, Image, Vision and their Applications (SIVA), pp. 1-2. IEEE, 2018.

**Communications Nationales**

- Reda YAGOUB, Mohamed BENAISSA, et Belkacem BENADDA. "Développement d'un procédé SDR hybride pour différentes générations de Télécommunications mobiles." 5ème semaine de la technologie, la technologie au service du développement durable, CUBBAT, 23-24 Avril 2018.

- Reda YAGOUB, Mohamed BENAISSA, et Belkacem BENADDA. "Présentation et mise en œuvre du SDR." Journée d'étude sur Les Télécommunications, CUBBAT, 04 Mars 2019.