الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
جامعة عين تموشنت
Université de Belhadj Bouchaib d'Ain-Temouchent
Faculté des Sciences et Technologie
Département d'électronique et télécommunications

Projet de fin d'études

Pour l'obtention du diplôme de Master en :

Domaine : SCIENCE ET TECHNOLOGIE

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Thème

Détection du Burst FCCH dans un système de communication GSM avec RTL SDR

Présenté Par :

Mlle. Ghazli Fatima Zahra

Mlle. Cherifi Achwak

Devant le jury composé de :

Dr Benosmane		**UBBAT**	**Président**
Dr Benganna		**UBBAT**	**Examinateur**
Mr. Yagoub Reda	**MCB**	**UBBAT**	**Encadrant**

Année universitaire 2022/2023

Remerciements

Nous remercions vivement tout d'abord le bon « DIEU » qui nous a aidé et nous a donné le pouvoir, le courage et la patience pour l'élaboration de ce travail.

Nous tenons à remercier profondément et spécialement :

- *Mr R.Yagoub notre encadrant : Pour son aide, ses orientations et précieux conseils*
- *MR ZIADI le Directeur de l'université Belhadj Bouchaib pour votre leadership inspirant, votre soutien précieux et votre dévouement envers l'excellence académique pour la confiance qu'il nous a accordée tout au long du projet*
- *Les enseignants 'Réseaux Télécommunications' Nous tenons à exprimer notre profonde reconnaissance envers nos professeurs pour leur engagement inébranlable et leur soutien indéfectible tout au long de notre parcours académique. Leur passion pour l'enseignement, leur expertise dans leurs domaines respectifs et leur dévouement envers notre réussite ont été des facteurs clés dans notre développement intellectuel et personnel. Leur influence positive a laissé une empreinte durable sur notre cheminement éducatif, et nous leur serons éternellement reconnaissants pour leur précieuse contribution à notre formation*
- *Nos profonds remerciements et notre gratitude vont aussi aux membres du jury, pour leur accord d'apprécier notre travail.*
- *Enfin, nous tenons à remercier tous nos amis (es) qui nous ont aidés, encouragés et soutenus pendant toute la durée de l'élaboration de ce mémoire.*

Dédicace

Je tiens à remercier Dieu, qui m'a accordé la force et le courage nécessaires pour poursuivre mes études et atteindre ce niveau.

Je voudrais également exprimer ma profonde reconnaissance envers ma mère, qui a été une source constante d'encouragement et de soutien inébranlable tout au long de mon cheminement.

Je souhaite dédier cette réalisation à la mémoire de mon père, en priant qu'Allah lui accorde le repos éternel. Son amour, son soutien et ses précieux conseils m'ont toujours inspiré et je continuerai à honorer sa mémoire dans mes accomplissements futurs.

À mes frères « Anis »et « Rabie», ainsi qu'à mes sœurs « Amara » et « Ines », je tiens à leur exprimer ma reconnaissance pour leur soutien inconditionnel. Leur présence et leur encouragement ont été des piliers essentiels dans mon cheminement académique et personnel.

Je souhaite également remercier mes belles-sœurs « Asma» et « Hadjer», dont la présence chaleureuse et le soutien constant ont été une source d'inspiration et de réconfort pour moi.

Je ne peux oublier de mentionner « Rymene», qui a été une véritable source de motivation et de soutien tout au long de ce parcours. Sa présence .

Un remerciement particulier va à ma chère sœur et binôme « Fatima ». Sa collaboration, son dévouement et son travail acharné ont été d'une importance capitale dans la réalisation de ce travail. Je lui suis reconnaissant pour sa contribution inestimable.

Enfin, j'adresse mes sincères remerciements à mon encadrant R.Yagoub qui a joué un rôle crucial en me guidant, m'aidant et me soutenant tout au long de mon travail. Sa précieuse expertise et ses conseils avisés ont grandement contribué à ma réussite.

Je souhaite également exprimer ma gratitude envers les membres du jury qui ont accepté d'examiner ce travail avec bienveillance.

Achwak

Dédicace

Je tiens à remercier Dieu, qui m'a accordé la force et le courage nécessaires pour poursuivre mes études et atteindre ce niveau.

Je voudrais également exprimer ma profonde reconnaissance envers ma mère et mon père et ma petite famille qui ont été une source constante d'encouragement et de soutien inébranlable tout au long de mon cheminement.

À mes chères sœurs et copines « Rofaida »et « Houda» et ma petite « Hawraa », je tiens à leur exprimer ma reconnaissance pour leur soutien inconditionnel. Leur présence et leur encouragement ont été des piliers essentiels dans mon cheminement académique et personnel.

Je souhaite également remercier mes enseignants

Je ne peux oublier de mentionner mes enseignants qui ont été une véritable source de motivation et de soutien tout au long de ce parcours.

Un remerciement particulier va à ma chère sœur et binôme « Achwak ». Sa collaboration, son dévouement et son travail acharné ont été d'une importance capitale dans la réalisation de ce travail. Je lui suis reconnaissant pour sa contribution inestimable.

Enfin, j'adresse mes sincères remerciements à mon encadrant R.Yagoub qui a joué un rôle crucial en me guidant, m'aidant et me soutenant tout au long de mon travail. Sa précieuse expertise et ses conseils avisés ont grandement contribué à ma réussite.

Je souhaite également exprimer ma gratitude envers les membres du jury qui ont accepté d'examiner ce travail avec bienveillance.

Fatima

Résumé

Le système GSM est largement utilisé pour les communications cellulaires, et la détection du burst FCCH est cruciale pour assurer une synchronisation correcte du récepteur GSM. Ce projet de fin d'étude propose un algorithme de détection du burst FCCH sur Matlab, nous avons utilisé le récepteur RTL-SDR pour enregistrer le signal radio GSM du canal de diffusion, afin d'appliquer les différents étapes de traitement de signal pour extraire la position exacte du burst FCCH.

Mots clefs : GSM, RTL-SDR, FCCH, detection, burst.

Abstract

The GSM system is widely used for cellular communications, and detection of the FCCH burst is crucial to ensure correct synchronization of the GSM receiver. This end-of-study project proposes an algorithm for detecting FCCH burst on Matlab, we used the RTL-SDR receiver to record the GSM radio signal of the broadcast channel, to apply the different signal processing steps to extract the exact position of the FCCH burst.

Keywords: GSM, RTL-SDR, FCCH, detection, Burst.

ملخص

يستخدم نظام GSM على نطاق واسع للاتصالات الخلوية، واكتشاف Burst FCCH أمر بالغ الأهمية لضمان التزامن الصحيح لمستقبل .GSM يقترح مشروع نهاية الدراسة هذا خوارزمية للكشف عن Burst FCCH على برنامج MATLAB، استخدمنا جهاز استقبال RTL-SDR لتسجيل إشارة راديوGSM ، لتطبيق خطوات معالجة الإشارة المختلفة لاستخراج الموقع الدقيق .Burst FCCH.

الكلمات المفتاحية : GSM ، RTL-SDR، FCCH، الكشف، Burst

.

Sommaire

Dédicace ….....

Dédicace……..

Résumé ……...

Abstract ……..

ملخص……..

Introduction générale …….....

Chapitre 1 : GSM…….....

1. Introduction 13

2. Système cellulaire 14

2.1 Architecture générique d'un réseau cellulaire..... 15

3. Architecture d'un réseau GSM..... 15

3.1 Station mobile 16

3.2 Sous-système radio (BSS)..... 16

3.3 Sous-système réseau (NSS)..... 17

3.4 Le sous-système d'exploitation et de maintenance 18

4. Les interfaces du réseau GSM..... 18

5. La Transmission radio 19

5.1 Allocation des fréquences 19

6. Conclusion..... 20

Chapitre 2 : les canaux physiques et logiques …….....

1. Introduction 23

2. Les canaux physiques..... 23

3. Les canaux logiques 25

3.1 Les canaux dédiés..... 25

3.2 Les canaux non dédiés..... 26

4. L'organisation d'un Burst 28

4.1 Le Burst FCCH (Frequency Correction Channel)..... 29

5. Conclusion..... 30

1.Introduction ..... **Erreur ! Signet non défini.**

Chapitre 3 : Algorithme de détection du burst FCCH ……...

2. Acquisition du signal 33

2.1 RTL-SDR 33

2.2 Enregistrement du signal GSM 34

3. Algorithme de détection..... 37

4. Résultats expérimentaux 38

5. Décalage de la fréquence de l'oscillateur local 41

6. Conclusion 42

Conclusion général……..

Bibliographie..... 44

Liste des Figures

Figure 1: Premier téléphone GSM français en 1992 14
Figure 2: Système cellulaire 14
Figure 3: Architecture générique d'un réseau cellulaire 15
Figure 4: Structure simplifiée des réseaux GSM (sans GPRS) 16
Figure 5: Interfaces GSM 19
Figure 6: Le principe de FDMA 24
Figure 7: Principe TDMA 25
Figure 8: burst 29
Figure 9: Types de rafales en GSM 30
Figure 10: Simplified RTL-SDR receiver architecture 34
Figure 11: RTL-SDR 34
Figure 12: Signal BCH. 35
Figure 13: Les options et les paramètres par défaut de l'outil rtl-sdr 36
Figure 14: les paramètres pour capturer de données du signal GSM 36
Figure 15: Signal GSM avec burst FCCH 37
Figure 16: Busrt FCCH 38
Figure 17:Le signal suréchantillonné 39
Figure 18: Différence de phase 39
Figure 19 : Différence de phase (zoom x fois) 41

Liste Des Tableaux

Tableau 1 :Caractéristiques technique. 20
Tableau 2: Les canaux logiques GSM 28

Introduction générale

La détection du Burst FCCH (Frequency Correction Channel) dans un système de communication GSM (Global System for Mobile Communications) avec RTL-SDR est un sujet d'intérêt dans le domaine de la radio logicielle et de la communication sans fil. Le RTL-SDR est un récepteur USB basé sur le chipset RTL2832U, qui peut être utilisé comme un outil abordable pour recevoir et traiter les signaux radio à large bande.

Le GSM est un système de communication cellulaire largement utilisé pour les réseaux mobiles. Il utilise différentes canaux pour transporter les données, y compris le FCCH qui est responsable de la correction de fréquence. La détection précise du Burst FCCH est essentielle pour la synchronisation correcte du récepteur GSM.

La détection du Burst FCCH dans un système de communication GSM avec RTL-SDR implique plusieurs étapes. Tout d'abord, le récepteur RTL-SDR est utilisé pour capturer le signal GSM brut. Ensuite, un algorithme de traitement du signal est appliqué pour extraire les bursts FCCH du signal capturé.

Le premier chapitre présente le système GSM (Global System for Mobile Communication). Il décrit également l'architecture générale d'un réseau cellulaire, les différentes composantes du réseau GSM (MS, BTS, BSC, NSS and OMC), les interfaces du réseau GSM et l'allocation des fréquences pour la transmission radio.

Le deuxième chapitre se concentre sur les canaux physiques et logiques du réseau GSM. Le chapitre aborde également l'organisation des bursts, et présentation du Burst FCCH.

Le troisième chapitre présente l'algorithme de détection du Burst FCCH dans les systèmes de communication mobile GSM. L'algorithme utilise le dongle RTL-SDR pour capturer les signaux GSM et effectue plusieurs étapes de traitement de signal pour extraire la position du burst FCCH.

CHAPITRE 1

GSM

1. Introduction

GSM (Global System for Mobile Communication) a commencé en 1982 en Europe. Le premier nom du réseau était Groupe spécial mobile. Il a été créé par la Conférence européenne des administrations des postes et télécommunications. Son but initial était pour une utilisation en Europe. Le premier réseau a été lancé en 1991 en Finlande. En 1993, le réseau s'est élargi au-delà de l'Europe à 70 transporteurs répartis dans 48 pays.

Le réseau GSM est utilisé partout dans le monde comme un réseau pour des centaines de fournisseurs de services cellulaires. Le réseau a été conçu pour gérer communications voix et données sur un téléphone cellulaire. La technologie avancée sur les dispositifs de données portatifs utiliser plusieurs des fonctionnalités GSM de votre téléphone cellulaire standard. Le réseau prend en charge les appels vocaux et le transfert de données des vitesses allant jusqu'à 9,6 kbit/s . (1)

Le GSM dans le mode a plus de 747 millions d'utilisateurs dans plus de 180 pays :

***Amérique du nord :** Canada, États-Unis, Mexique

***Amérique du sud :** Argentine, Bolivie, Brésil, Chili, Paraguay, Pérou…

*** Afrique :** Afrique du Sud, Cameroun, Éthiopie, Maroc, Sénégal, Zaïre…

*** Asie :** Arabie Saoudite, Chine, Corée, Hong-Kong, Inde, Indonésie, Koweït, Malaisie, Pakistan, Russie, Thaïlande…

*** Océanie :** Australie, Nouvelle-Zélande…

Figure 1: Premier téléphone GSM français en 1992 *(2)*

2. Système cellulaire

Dans un système cellulaire, la région couverte est divisée cellule, comme illustré à la figure 2. Pour plus de clarté, on peut les illustrer par des hexagones. Au centre d'une cellule on trouve un ou plusieurs émetteurs et récepteurs.

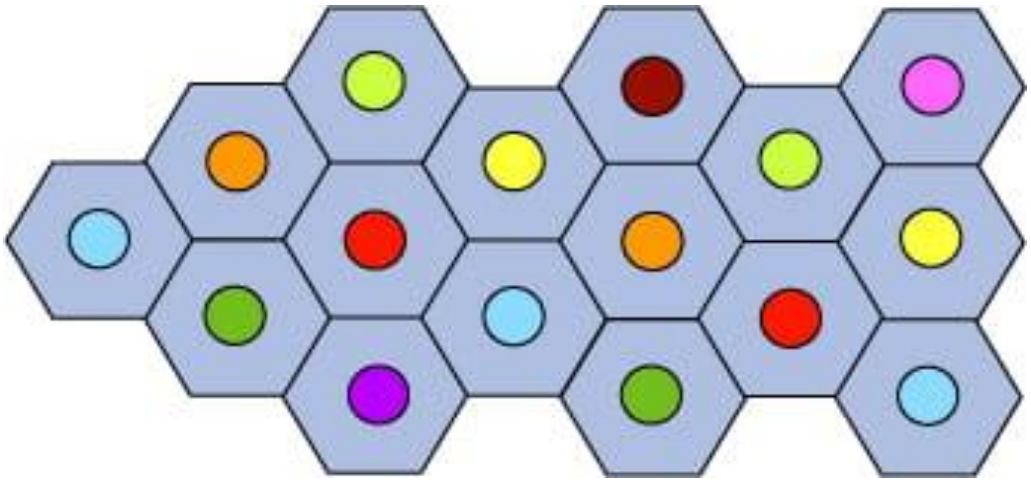

Figure 2: Système cellulaire (3)

La dimension d'une cellule est fonction de la puissance de son émetteur-récepteur. Si un émetteur-récepteur est très puissant, alors son champ d'action sera très vaste, mais sa bande de fréquence peut être rapidement saturée par des communications. D'autre part, en utilisant des cellules plus petites, la même bande de fréquence peut être réutilisée davantage, ce qui augmente la quantité de communication possible.

La taille des cellules peut varier entre (0.5 et 35 km) et dépend la densité d'utilisateur/ la topographie. Les cellules sont regroupées en bloc (appelé motif ou cluster). La forme et la dimension des blocs et le nombre de cellules est fonction du nombre de fréquences (canaux) disponibles. (4) (5)

2.1 Architecture générique d'un réseau cellulaire

Un réseau cellulaire est constitué d'un :

- Radio Access Network (RAN) : Point d'accès au réseau Gestion de l'interface air
- Core Network (CN) : Réseau fixe assurant l'interconnexion avec les autres

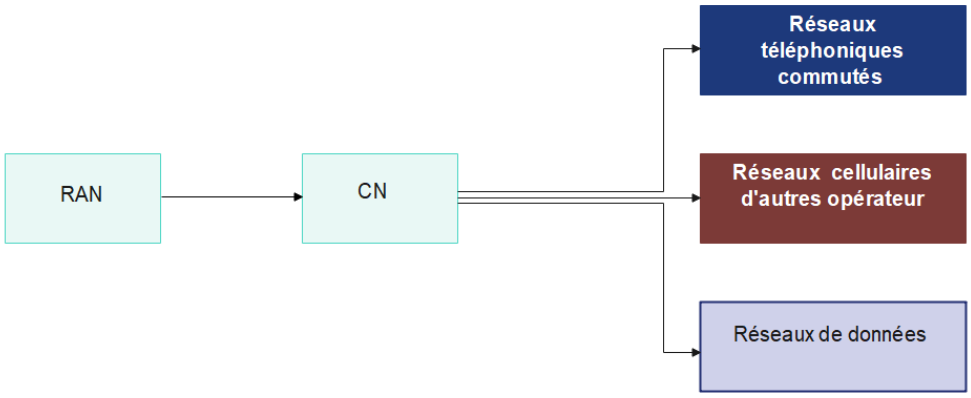

Figure 3: Architecture générique d'un réseau cellulaire

3. Architecture d'un réseau GSM

Un réseau GSM se compose de trois sous-réseaux :

Sous-système radio : BSS - Base Station Subsystem

Sous-système réseau : NSS - Network Subsystem

Sous-système d'exploitation : OSS – Operation Subsystem

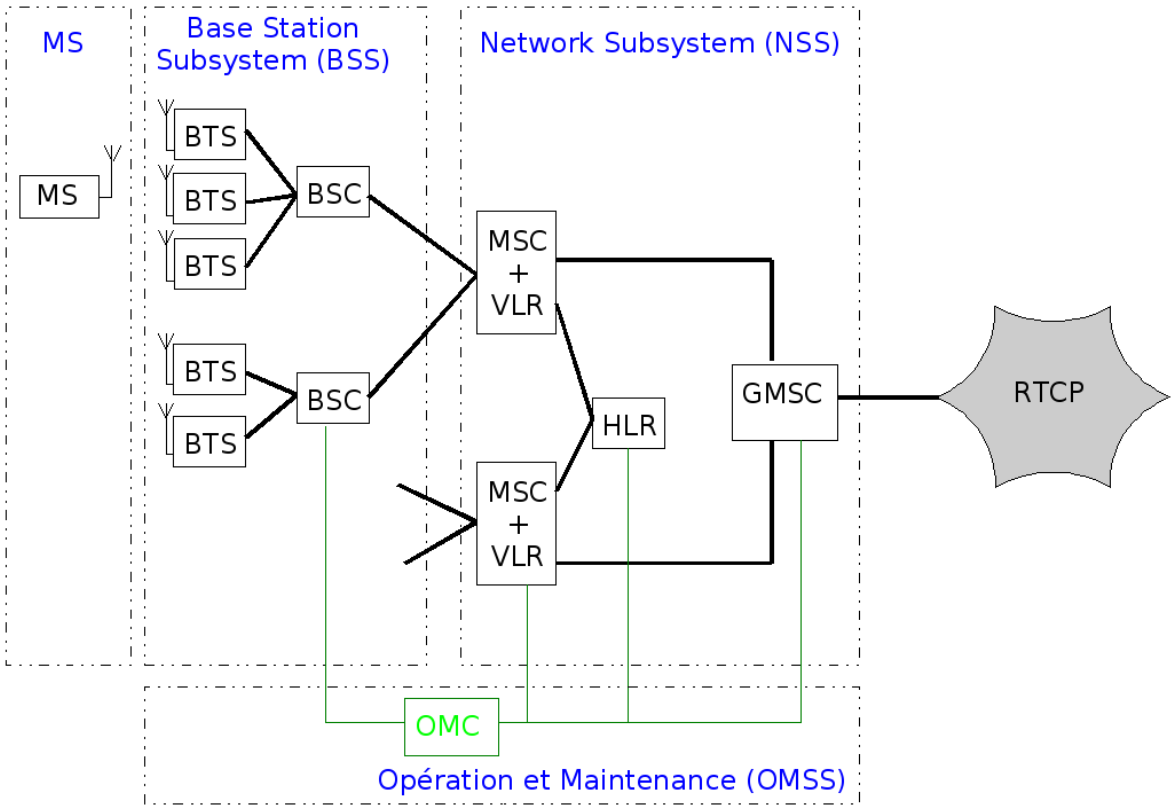

Figure 4: Structure simplifiée des réseaux GSM (sans GPRS) *(6)*

3.1 Station mobile

Station mobile est un terme qui désigne un composant fondamental du système cellulaire des téléphones mobiles GSM et de l'extension UMTS ou du réseau professionnel TeTRA.

3.2 Sous-système radio (BSS)

Le sous-système radio gère les transmissions radio. Il se compose de plusieurs entités y compris la station mobile (MS), la station de base (BTS) et le contrôleur de station de base (BSC).

Station de base : représente la partie radio du réseau GSM, qui relie les stations mobiles aux Infrastructure de réseau fixe. BTS se compose d'un ensemble d'émetteurs/récepteurs. Elle garantit :

- Gestion du multiplexage temporel (une porteuse est divisée en 8 créneaux horaires, dont 7 créneaux horaires attribués aux utilisateurs) et la gestion des sauts de fréquence.

- Mesures radio pour vérifier la qualité de service ; ces mesures sont envoyez directement à BSC.
- Gérer les liaisons de données entre les réseaux (données de trafic et de signalisation)

La capacité maximale typique d'un (BTS) est de 12 porteuses, ou 96 communications en même temps.

Contrôleur de station de base : Ce sont des hubs BTS. Ils gèrent les ressources radio et l'exploitation d'un certain nombre de stations de base, notamment les handovers, tout en BTS applique uniquement les décisions prises par BSC. Un BSC standard peut contrôler Environ 60 BTS, ce nombre peut être réduit en milieu rural. BSC est connecté à La BTS se connecte au MSC via l'interface Abis et via l'interface A.

3.3 Sous-système réseau (NSS)

Le rôle principal de ce sous-système est de gérer la communication entre l'abonné et les autres utilisateurs qui sont d'autres abonnés, utilisateurs du réseau RNIS, utilisateurs du réseau fixe.

Commutateur (MSC) : Cet élément peut être considéré comme le cœur d'un téléphone mobile car il gère les appels et ce qui est lié à l'identité de l'abonné, à son abonnement et à sa localisation. Fondamentalement, le MSC agit comme un nœud de commutation.

Enregistreur de localisation des visiteurs (VLR) : Cette base de données contient temporairement des informations sur les inscrits qui visitent une zone desservie par le MSC plutôt que la région dans laquelle ils sont inscrits. Ces informations provenant du HLR auprès duquel l'abonné est enregistré indiquent les services auxquels l'abonné a droit

Enregistreur de localisation nominale (HLR) : Il s'agit d'une base de données contenant des informations sur les abonnés dans la zone fournie par le fournisseur de services mobile.

Centre d'authentification : L'AUC est une base de données protégée contenant une copie de la clé privée enregistrée sur la carte SIM de chaque abonné. Cette clé sert à vérifier l'authenticité de l'abonné pour chiffrer les données envoyées.

Enregistreur des identités des équipements : Chaque terminal mobile est identifié par un code IMEI. Le registre EIR contient une liste de tous les registres valides. La consultation de ce registre permet d'interdire l'accès au réseau à un terminal déclaré perdu par vol.

3.4 Le sous-système d'exploitation et de maintenance

Ce sous-système est connecté à divers éléments du sous-système ainsi qu'au contrôleur de station de base. (7) (8)

4. Les interfaces du réseau GSM

Des interfaces normalisées sont utilisées entre les entités qui transmettent le trafic et pour les informations de signalisation. Dans les réseaux GSM, les données de signalisation sont des données de trafic. Toutes les liaisons entre équipements GSM sauf avec la station mobile sont des liaisons numériques. Le lien entre BTS et MS est un lien numérique.

- **Interface Um** : appelée aussi Air ou radio, entre BTS et MS, s'appuie sur le protocole LAPDM. Il est utilisé pour le transport du trafic et des données de Signalisation.
- **Interface A bis** : entre BTS et BSC s'appuie sur le protocole LAPD. Il est utilisé pour le transport du trafic et des données de signalisation.
- **Interface A** : entre BSC et MSC, il est utilisé pour le transport du trafic et des données de signalisation.
- **Les Interfaces B** entre MSC et VLR**, C** entre MSC et HLR**, E** entre MSC et MSC, **F** entre MSC et EIR, **G** entre VLR et VLR, **D** entre VLR et HLR/AuC, s'appuient sur le protocole sémaphore N·7 du CCITT pour les couches OSI basses (MTP, Message Transfert Protocol) et sur le protocole MAP (Mobile Application Protocole) pour les couches hautes. Ces interfaces sont utilisées en particulier pour le transport des données relatives à l'application des mobiles.
- **Les Interfaces REM** : entre OMC-R et BSS ou entre OMC-S et NSS, utilisent un réseau de transmission de donnée de type X25.

- **Les Interfaces passerelles** : entre le MSC et les réseaux publics s'appuient sur le protocole sémaphore N·7 du CCITT. Elles sont utilisées pour le transport du trafic et des données de signalisation. (9)

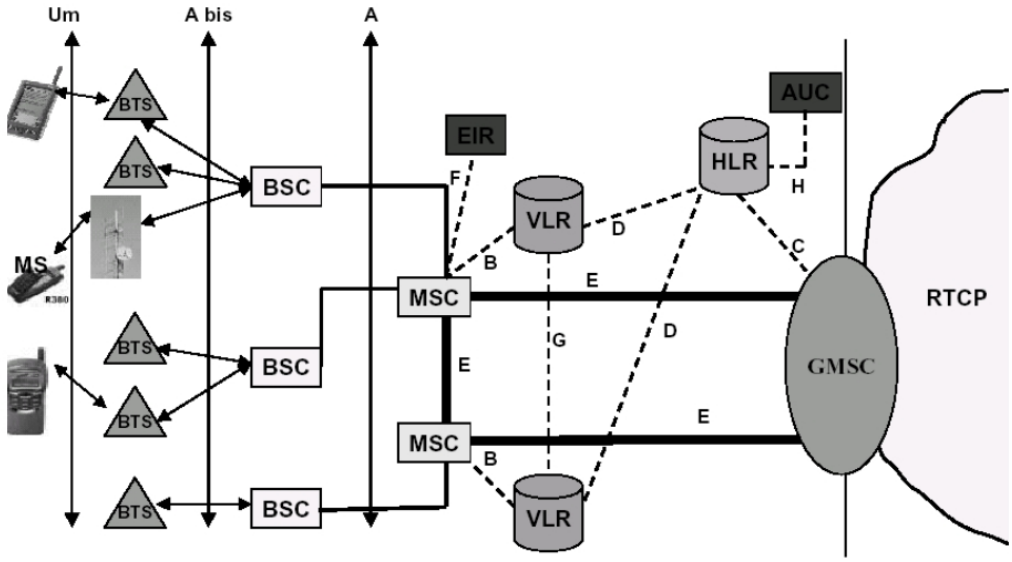

Figure 5: Interfaces GSM

.

5. La Transmission radio

5.1 Allocation des fréquences

La téléphonie mobile par GSM occupe deux bandes de fréquences aux alentours de 900 Mhz.

De 890 à 915 pour la transmission des signaux des stations mobiles vers la station de base.

De 935 à 960 pour la transmission inverse.

La bande passante de chaque direction est divisée en 124 canaux d'une largeur de 200 MHz. Ces canaux ne suffisent pas dans les grands canaux, il faut donc allouer une bande supplémentaire autour de 1800 Mhz. Ceci est un système DCS 1800 présente des caractéristiques similaires au GSM en termes de protocoles et de services. Ensuite, la communication montante se situe entre 1710 et 1785 la communication descendante se situe entre 1805 et 1880 (10).

Le tableau 1 montre les caractéristiques techniques du réseau GSM.

	GSM 900	**GSM 1800**
Banse spectrale- Canaux descendant	935 à 960 MHZ	1805 à 1880 MHZ
Bande spectrale- Canaux montant	890 0 915 MHZ	1710 à 1785 MHZ
Espacement entre les canaux (multiplexage FDMA)	45 MHZ	95 MHZ
Nombre de canaux (multiplexage FDMA)	124	374
Largeur des canaux	200 KHZ	200 KHZ
Multiplexage (TDMA)	8	8
Nombre de canaux logiques	992	2992

Tableau 1 : Caractéristiques technique.

6. Conclusion

Le réseau GSM (Global System for Mobile Communication) est un système cellulaire largement utilisé à travers le monde. Il a été conçu pour gérer à la fois les communications vocales et les transferts de données sur les téléphones cellulaires. Le réseau GSM utilise une architecture cellulaire, où les régions couvertes sont divisées en cellules, ce qui permet une meilleure gestion des ressources et une augmentation de la capacité de communication. Les trois principaux sous-systèmes du réseau GSM sont le sous-système radio (BSS), le sous-système réseau (NSS) et le sous-système d'exploitation et de maintenance (OSS). Chaque sous-système comprend divers éléments tels que les stations de base, les contrôleurs de station de base, les commutateurs et les bases de données. Des interfaces normalisées sont utilisées pour la transmission du trafic et des données de signalisation entre les différentes entités du

réseau. La transmission radio du GSM utilise des bandes de fréquences spécifiques, divisées en canaux pour le transfert des signaux des stations mobiles vers les stations de base. Le GSM a révolutionné les communications mobiles et reste un pilier essentiel des réseaux de téléphonie mobile à travers le monde.

CHAPITRE 2

Les canaux physiques et logiques

1. Introduction

Les canaux logiques et physiques sont deux types de canaux de communication qui permettent le transfert de données entre des dispositifs ou des systèmes. Les canaux logiques sont des canaux de communication virtuels qui sont créés par des protocoles de communication pour transmettre des données entre deux dispositifs, même s'ils ne sont pas connectés directement. Ils peuvent être des canaux de communication en mode connecté ou en mode déconnecté.

En bref, il existe deux types de canaux de communication utilisés pour transférer des données entre des dispositifs ou des systèmes, à savoir les canaux logiques et physiques. Les canaux logiques sont des canaux virtuels qui sont établis grâce à des protocoles de communication, tandis que les canaux physiques sont des canaux matériels tels que des câbles ou des ondes radio. Les deux types de canaux sont essentiels dans les réseaux de communication contemporains. (11; 12)

2. Les canaux physiques

Le canal radio est utilisé pour la communication du téléphone mobile au réseau. Il existe les canaux de liaison montante et canaux de liaison descendants.

- Canaux de liaison montante : la communication va du téléphone mobile au BTS.
- Canaux de liaison descendants : la communication va de la BTS au téléphone mobile.

GSM utilise la bande comprise entre 890 - MHz pour les canaux de liaison montante et entre 935 -960 MHz pour les canaux de liaison descendante.
Pour augmenter la capacité du réseau, le GSM utilise deux techniques pour l'allocation de ses fréquences :

- L'accès multiple à répartition en fréquence ou le partage en fréquence (FDMA).
- L'accès multiple à répartition dans le temps ou le partage en temps (TDMA). (13)

La méthode d'accès FDMA ou accès multiple par répartition Fréquences repose sur un multiplexage en fréquences. Un tel procédé développe la bande de fréquences en sous bandes, chacune est placée sur une fréquence dite porteuse ou qui est la fréquence spécifique du canal.

Chaque porteuse ne peut transporter que le signal d'un utilisateur. La figure ci-dessus présente le principe de FDMA. (14) (15)

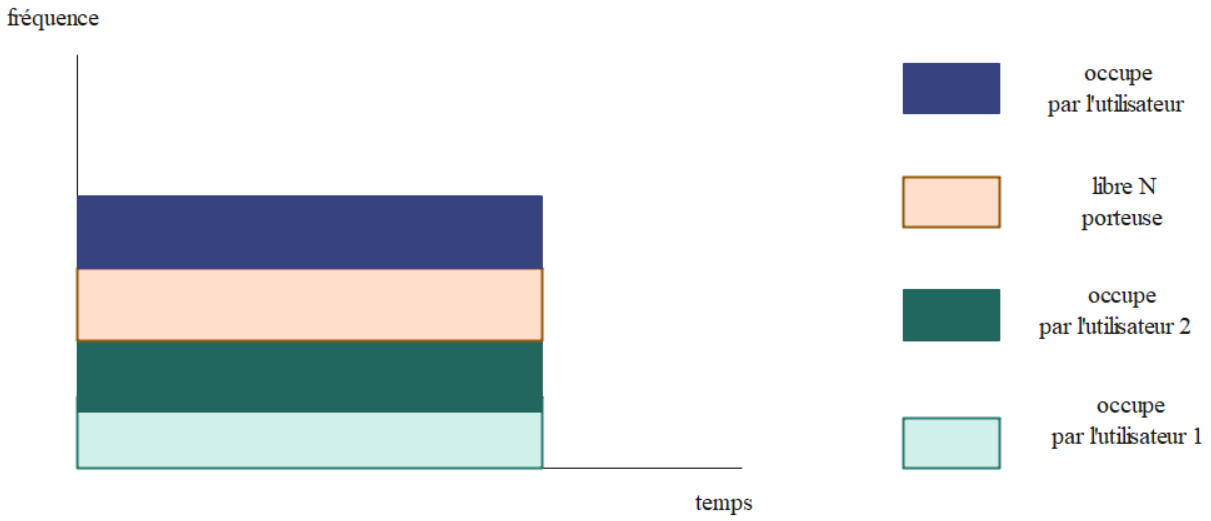

Figure 6: Le principe de FDMA

Multiplexage temporel TDMA ou techniques d'accès multiple par répartition dans le temps qui fournissent la totalité de la bande à chaque utilisateur pendant une période de temps donnée (slot). L'émetteur de la station mobile mémorise l'information avant de la transmettre sur le slot, c'est-à-dire pendant le temps qui lui est imparti. Les différents emplacements sont regroupés en ensembles, offrant ainsi au système plusieurs canaux de communication pour l'utilisateur. La succession des positions dans le cadre crée le physique de l'utilisateur.

Donc la bande spectrale est multiplexé en fréquence (FDMA) pour obtenir plusieurs canaux et chacun de ces canaux est multiplexé selon TDMA (d'ordre 8) (16)

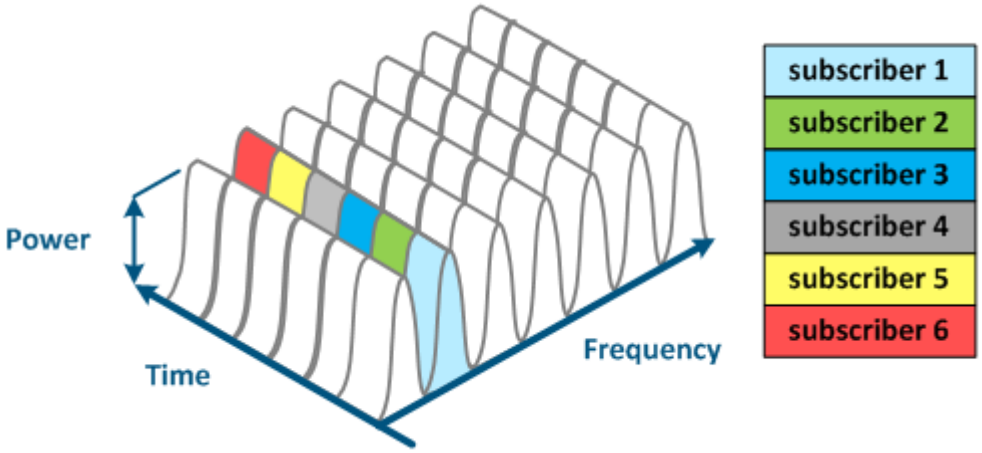

Figure 7: Principe TDMA

3. Les canaux logiques

Sur une paire de fréquences dont un slot spécifique est alloué à la communication téléphonique. Cette paire de fentes forme un canal physique duplex pour un circuit téléphonique. Ce canal physique forme alors une base avec les canaux logiques : le canal de trafic TCH véhicule la voix et le canal de contrôle SACCH les appelle et assure une QoS satisfaisante.

Les différents canaux logiques GSM sont séparés en classes (17) :

Les canaux dédiés (duplex)

Les canaux non dédiés (simplex)

3.1 Les canaux dédiés

Un canal logique dédié est réservé à un seul mobile, qui a une paire de slots allouée (un pour émission et un pour la réception) pour communiquer des informations.

Le canal de trafic (TCH) : transporte des données de voix numérisées à plein débit (13 kbps) ou à demi-débit (6,5 kbps).

Le canal de contrôle dédié autonome (SDCCH) : est utilisé pour la signalisation, pour échanger des informations de localisation IMSI lors de l'établissement d'un appel.

Le canal de contrôle lent associé (SACCH) : est utilisé pour superviser une liaison et contrôler la qualité du lien radio, la puissance d'émission du terminal, ainsi que la compensation du délai de propagation. Enfin, le canal de contrôle rapide associé FACCH a plusieurs fonctions, notamment l'exécution de handovers. (18)

3.2 Les canaux non dédiés

Les canaux partagés logiques sont utilisés pour transmettre des données de la BTS aux MS, ce qui signifie que plusieurs mobiles peuvent recevoir les mêmes données via ces canaux.

Le canal de paging (PCH) : est utilisé pour envoyer l'identité du mobile sur plusieurs cellules afin que le réseau puisse communiquer avec lui.

Le canal d'allocation de ressources (AGCH) : réserve un canal physique au mobile après son accès au réseau.

Le canal d'allocation de ressources (SCH) : fournit tous les éléments nécessaires au mobile pour une synchronisation complète des trames.

Le canal de contrôle de diffusion (BCCH) : diffuse des informations caractéristiques de la cellule, telles que le numéro de la zone de localisation et la description des cellules voisines, afin que le mobile puisse savoir s'il peut passer en mode veille.

Le canal de connexion de fréquence (FCCH) : permet au mobile de se synchroniser sur une fréquence porteuse.

Il y a également un canal de transmission dans le sens ascendant, qui est classé parmi les canaux non dédiés : le Canal d'accès aléatoire RACH. Il permet aux appareils mobiles d'accéder aléatoirement au réseau lorsqu'ils souhaitent effectuer une opération. (19) (20)

	Logical channel	Abbreviation	Uplink/Downlik	Task
Broadcast channel (BCH)	Broadcast control Channel	BBCH	DL	System information Broadcast
	Frequency correction chanel	FCCH	DL	Ceell frequency synchronization
	Synchronization Channel	SCH	DL	Cell time syncronization and identification
Common control Channel (CCCH)	Paging Channel	PCH	DL	MS paging
	Random access Channel	RACH	UL	MS random access
	Access grant Channel	RACH	DL	Ressource allocation
	Cell broadcast Channel	CBCH	DL	Short messages broadcast
Dedicated control Channel	Standalone dedicated control channel	SDCCH	UL/DL	General signaling
	Slow associated control Channel	SACCH	UL/DL	Signaling associated with the TCH
	Fast associated	FACCH	UL/DL	Handover signaling

	control Channel			
Traffic Channel	Full speech	TCH/FS	UL/DL	Full-rate voice Channel

Tableau 2: Les canaux logiques GSM

4. L'organisation d'un Burst

Un burst est l'unité de transmission d'informations dans le système GSM. Il est constitué de plusieurs parties :

- Le préambule, qui permet au récepteur de se synchroniser avec le signal envoyé.
- Le champ de données, qui contient les informations transmises, telles que des données de voix ou des données de signalisation.
- Le champ de contrôle, qui contient des informations sur la transmission, telles que la puissance du signal et le type de modulation utilisé.

Le champ de données est divisé en plusieurs sous-parties, chacune représentant un intervalle de temps appelé « time slot ». Chaque créneau horaire peut transporter une quantité spécifique de données, selon qu'il s'agit d'un time slot plein débit ou demi-débit. La taille du burst peut également varier en fonction de la méthode de codage utilisée. (21) (22)

Burst normal.

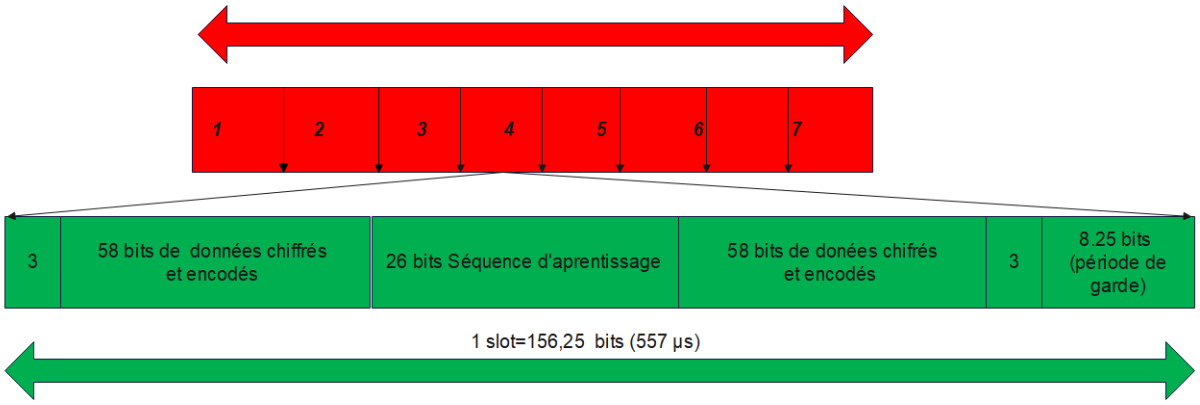

Figure 8: burst

- 3bits début et fin : augmenter et diminuer la puissance de l'émetteur.
- séquence d'apprentissage : synchronisation (minimise l'apparition d'erreurs)
- délais de garde : protège le slot suivant des inexactitudes d'alignement temporel
- 2*5 bits de données utilisateurs Ou de signalisation (1er bit indique la présence éventuelle de signalisation)

4.1 Le Burst FCCH (Frequency Correction Channel)

Le Burst FCCH est un type de burst utilisé dans les réseaux de téléphonie mobile GSM pour la synchronisation en fréquence. Il est émis périodiquement par la station de base (BTS) sur le canal de diffusion BCCH. Le Burst FCCH contient une séquence de bits connue et fixe, qui permet au téléphone mobile de se synchroniser sur la fréquence porteuse de la BTS.

Le Burst FCCH est constitué de 148 bits et dure environ 577 µs. Il est composé d'un préambule, d'un champ d'identification de fréquence (Frequency Burst Identification - FBI), d'un champ de synchronisation de fréquence (Frequency Synchronization Burst - FSB), et d'un champ de remplissage (Idle).

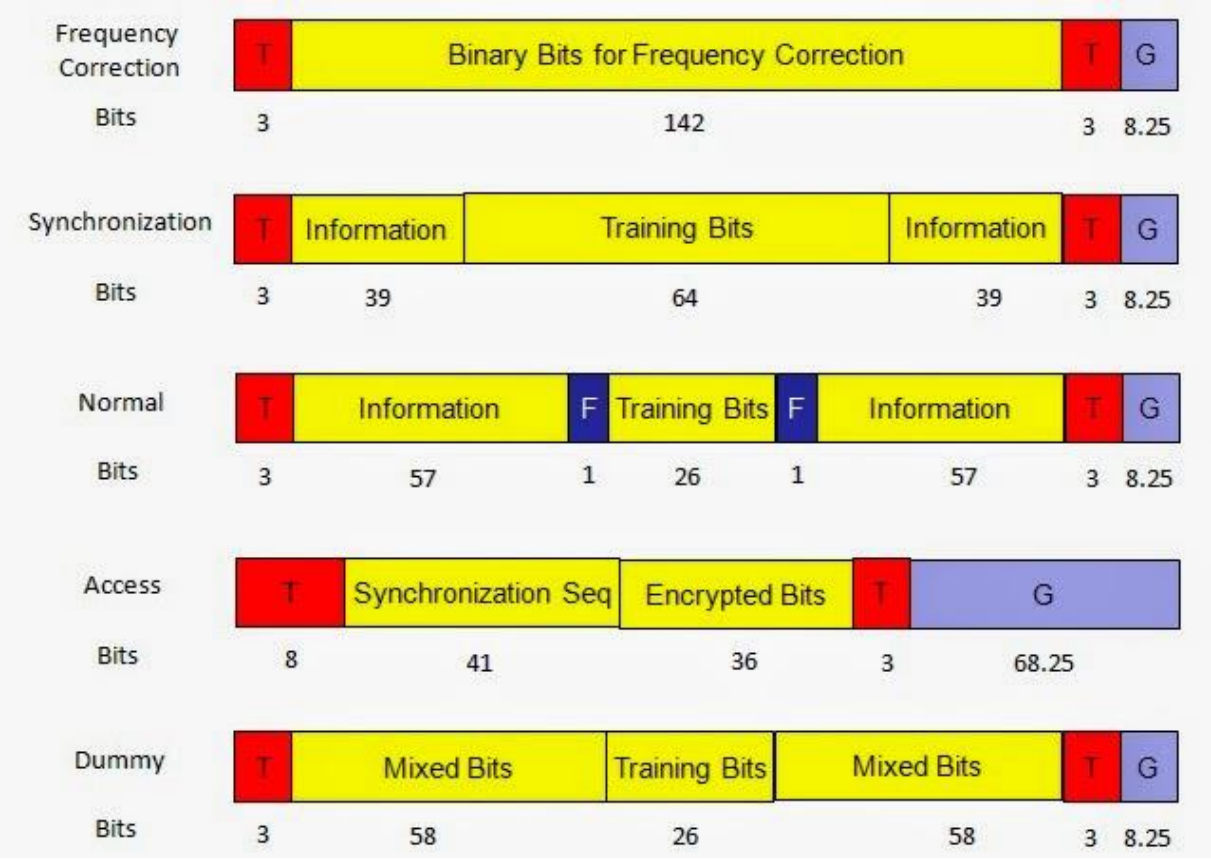

Figure 9: Types de rafales en GSM (23)

Le préambule est une séquence de 64 bits qui permet au téléphone mobile de détecter le début du Burst FCCH. Le champ FBI contient l'identifiant de la BTS, qui permet au téléphone mobile de savoir sur quelle BTS il est en train de se synchroniser. Le champ FSB contient une séquence de 36 bits qui permet au téléphone mobile de se synchroniser sur la fréquence porteuse de la BTS.

Le champ de remplissage (Idle) est utilisé pour remplir le reste du Burst FCCH avec des bits nuls. Le Burst FCCH est émis avec une puissance constante et une modulation de phase de type BPSK (Binary Phase Shift Keying).

Une fois que le téléphone mobile est synchronisé sur la fréquence porteuse de la BTS à l'aide du Burst FCCH, il peut commencer à écouter les autres canaux de la BTS pour trouver un canal de trafic sur lequel établir une communication. (24) (25)

5. Conclusion

En conclusion, les canaux logiques et physiques sont deux types de canaux de communication importants dans les réseaux de communication modernes. Les canaux logiques permettent une transmission de données plus flexible et plus efficace, tandis que les canaux physiques assurent une transmission de données plus rapide et plus fiable.

En somme, les canaux logiques et physiques ont chacun leurs avantages et leurs inconvénients, et leur utilisation dépend du contexte et des besoins spécifiques d'un réseau de communication donné. Les deux types de canaux sont complémentaires et leur combinaison permet d'assurer une transmission de données efficace, fiable et adaptée aux besoins des utilisateurs.

CHAPITRE 3

Algorithme de détection du Burst FCCH

1. Introduction

Le FCCH (Frequency Correction Channel) est un canal de signalisation utilisé dans les systèmes de communication mobile GSM (Global System for Mobile Communications) pour transmettre des informations de synchronisation et de correction de fréquence. Le FCCH est transmis en rafales (bursts) de longueur fixe à une fréquence d'environ 100 Hz et peut être détecté à l'aide d'un algorithme de détection de burst FCCH. L'algorithme de détection de burst FCCH est un processus qui consiste à rechercher des Burst FCCH dans un signal reçu.

Dans ce chapitre nous présentons l'algorithme de détection du burst FCCH sous Matlab.

2. Acquisition du signal

2.1 RTL-SDR

RTL-SDR est un acronyme pour "Software-Defined Radio" (radio logicielle) basé sur le tuner TV RTL2832U. Ce tuner USB économique, qui était initialement conçu pour la réception de la télévision numérique terrestre, a été découvert par des passionnés de radio pour être utilisé comme récepteur radio à large bande. Il est devenu populaire en raison de sa polyvalence et de son faible coût.

Le RTL-SDR permet de transformer un ordinateur personnel en récepteur radio à large bande grâce à un logiciel spécifique. Le RTL-SDR peut être utilisé pour détecter et analyser les signaux radio.

L'architecture simplifiée du dongle RTL-SDR est illustrée dans la figure 10. La puce du tuner (le plus souvent Raphael R820T et Elonics E4000) traduit le signal RF capturé en une fréquence intermédiaire (FI) ou à fréquence nulle, selon le tuner utilisé, puis la puce Realtek RTL2832U convertit le signal analogique en signal numérique. Le signal en bande de base complexe I/Q (en phase et en quadrature) sur 8 bits est transmis à l'ordinateur hôte via le port USB, où le traitement numérique du signal a lieu (filtrage, démodulation, etc.). (27) (28)

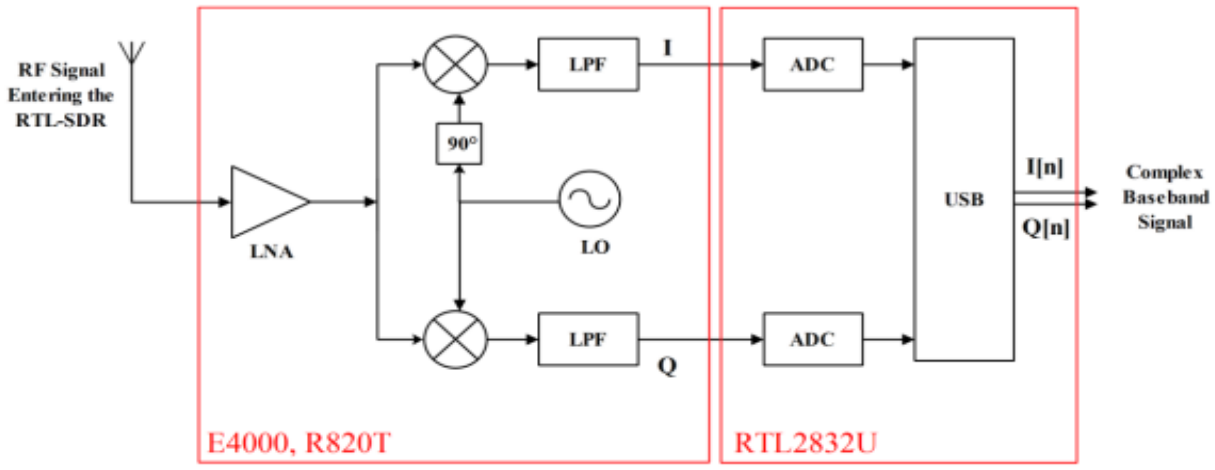

Figure 10: Simplified RTL-SDR receiver architecture (29)

Figure 11: RTL-SDR

2.2 Enregistrement du signal GSM

Dans un système radio mobile cellulaire GSM il existe un signal de référence, ce signal permet au téléphone mobile de détecter la présence du système, de choisir la meilleure station de base (BS), de connaître le paramétrage local du système et de se synchroniser dans le temps et fréquence, ce signal est appelé porteuse de canal de diffusion (BCH), qui transmet à une puissance maximale constante, comme nous avons mentionné dans le 2ème chapitre, le réseau GSM utilise une combinaison de FDMA et TDMA, par conséquent, la station mobile doit se synchroniser en temps et en fréquence. A cet effet, le burst de correction de fréquence (FCH) et le burst de synchronisation (SCH) sont utilisées. La figure 12 montre le signal de diffusion BCH.

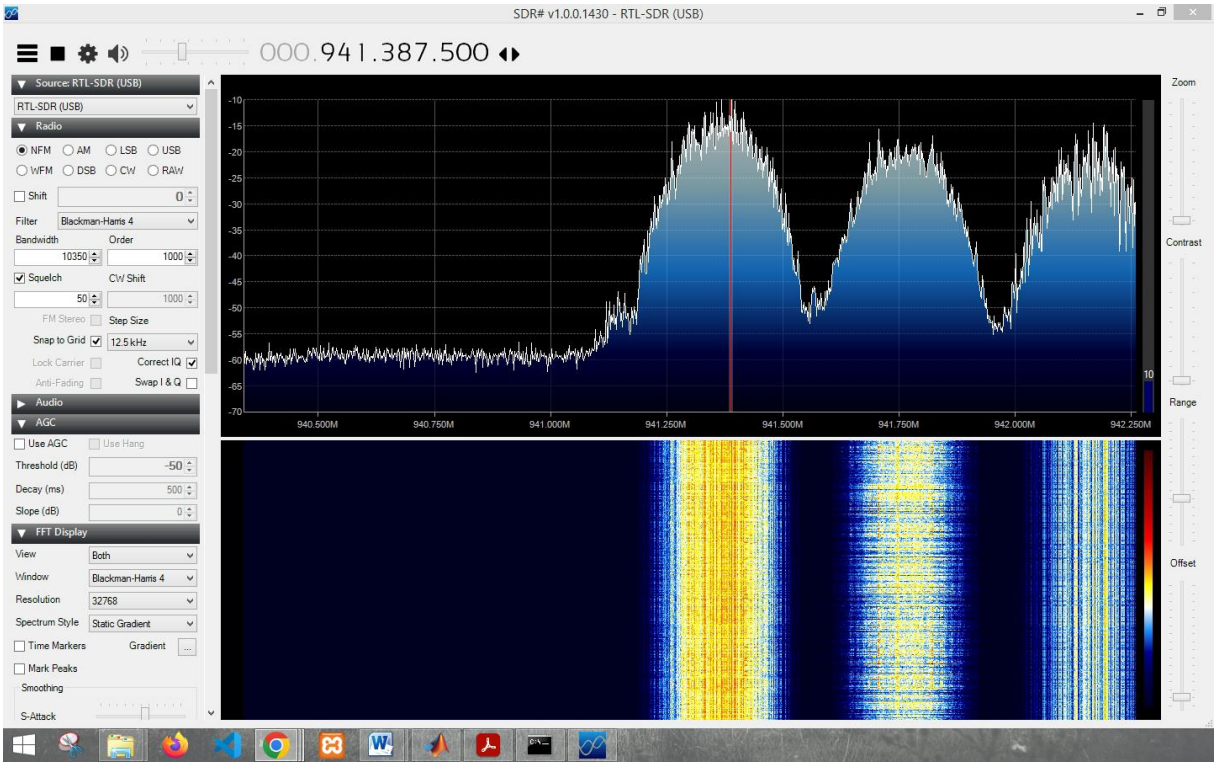

Figure 12: Signal BCH.

Comme le montre la figure le canal de diffusion BCH est située sur la fréquence 941.38 Mhz.

Pour enregistré ce signal nous avons utilisé l'outil d'enregistrement rtl-sdr IQ (30)

Pour afficher les options et les paramètres par défaut de l'outil rtl-sdr, on utilise la commande « rtl_sdr » comme le montre la figure 13.

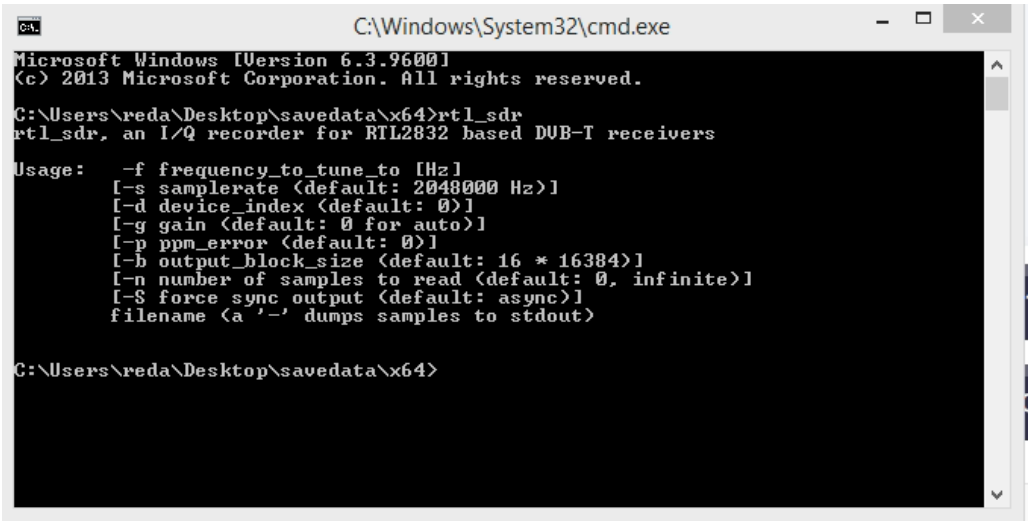

Figure 13: Les options et les paramètres par défaut de l'outil rtl-sdr

Maintenant, pour capturer 10 secondes de données du signal GSM, avec une fréquence centrale de 941.38 MHz et un gain de 25 dB. Nous réglons le taux d'échantillonnage sur 2600000 échantillons/sec (ce qui équivaut à une bande passante de 2,6 MHz), je devrai capturer 26000000 échantillons (260000000 [échantillons]/ (2600000 [échantillons/sec]) = 10 [sec]), la figure 14 montre la commande utilisé sur le terminal.

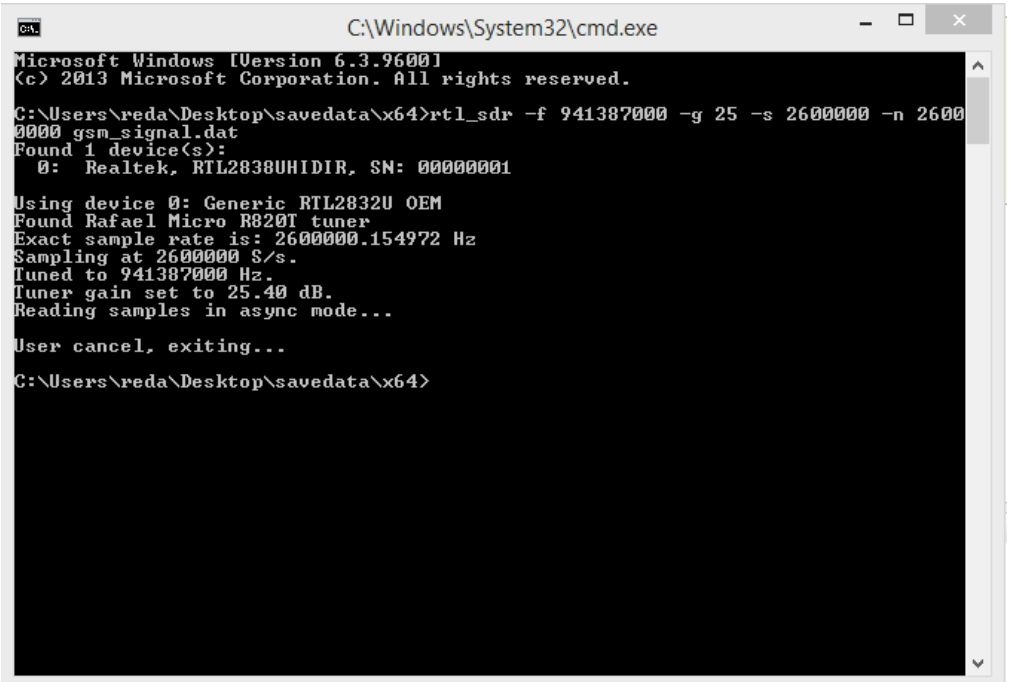

Figure 14: les paramètres pour capturer de données du signal GSM

Les données IQ brutes capturées sont enregistrées dans un fichier appelé gsm_signal.dat, qui est stocké par défaut dans le même dossier de l'outil rtl-sdr.

3. Algorithme de détection

Ce code est une implémentation MATLAB de l'algorithme de détection du Burst FCCH. Il commence par définir les paramètres du système tels que la fréquence d'échantillonnage, la largeur de bande de filtrage, le débit binaire, l'interpolation, et le nombre de trames TDMA.

Ensuite, il applique un filtre FIR pour filtrer le signal d'entrée. Ensuite, une transformation de Fourier est effectuée sur le signal filtré pour visualiser son spectre de fréquence.

Il existe plusieurs méthodes pour détecter le burst FCH (31). Le moyen le plus simple consiste à trouver la différence de phase entre une paire d'échantillons de signal, et puisque le burst FCCH est une onde sinusoïdale continue, la différence de phase doit être constante (32). La figure 15 montre le signal GSM capté avec le burst FCCH.

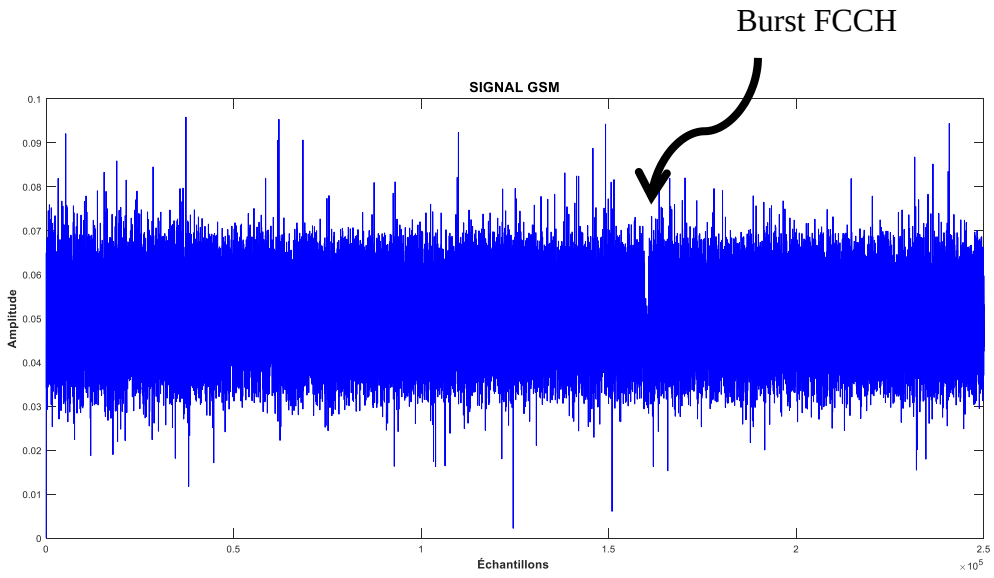

Figure 15: Signal GSM avec burst FCCH

Mathématiquement, on considère n_1 et n_2 deux échantillons complexes consécutifs :

$$n_1 = A_1 e^{j\emptyset_1} \qquad (1)$$

$$n_2 = A_2 e^{j\emptyset_2} \qquad (2)$$

Pour calculer le déphasage entre n_1 et n_2 , on multiplie n_1 par le conjugué de n_2 :

$$n_1 * n_2 = A_1 A_2 e^{j(\emptyset_1 - \emptyset_2)} \qquad (3)$$

4. Résultats expérimentaux

La figure (16) représente le signal GSM capturé par le dongle RTL-SDR dans le domaine temporelle. Cette représentation montre l'évolution du signal au fil du temps.

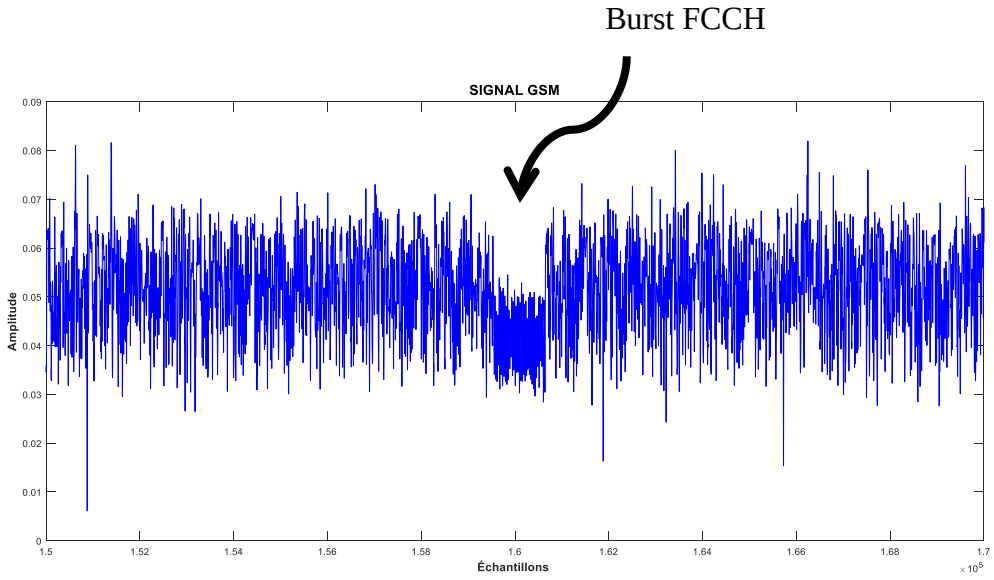

Figure 16: Busrt FCCH

.

La deuxieme étape consiste à sur-échantillonner, la méthode du sur-échantillonnage consiste à échantillonner le signal à une fréquence beaucoup plus grande que la largeur de bande utile, de manière à échantillonner correctement les hautes fréquences présentes dans le signal. On fait subir au signal numérique un filtrage passe-bas avant de réduire sa fréquence d'échantillonnage pour le stockage ou la transmission. Le signal GSM sur-échantillonner est montré dans la figure 17.

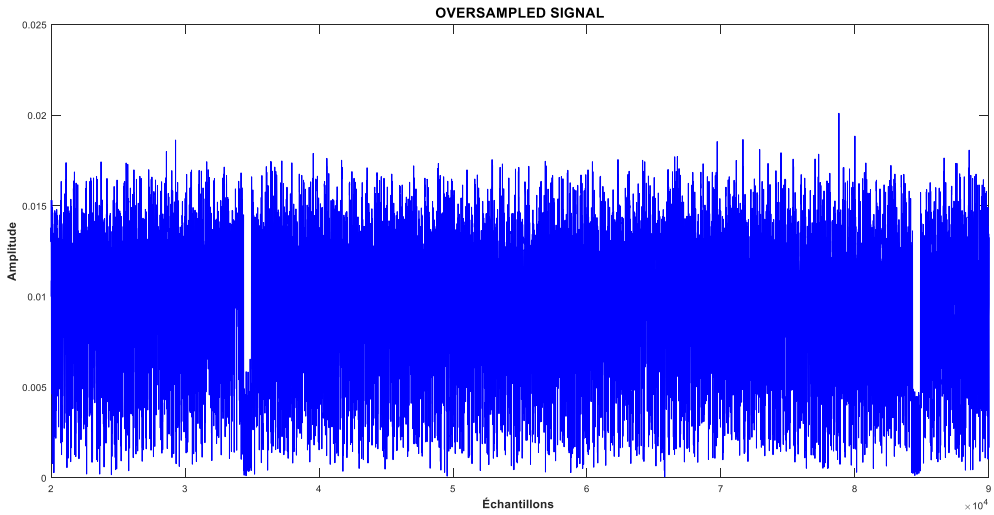

Figure 17: Le signal Suréchantillonné.

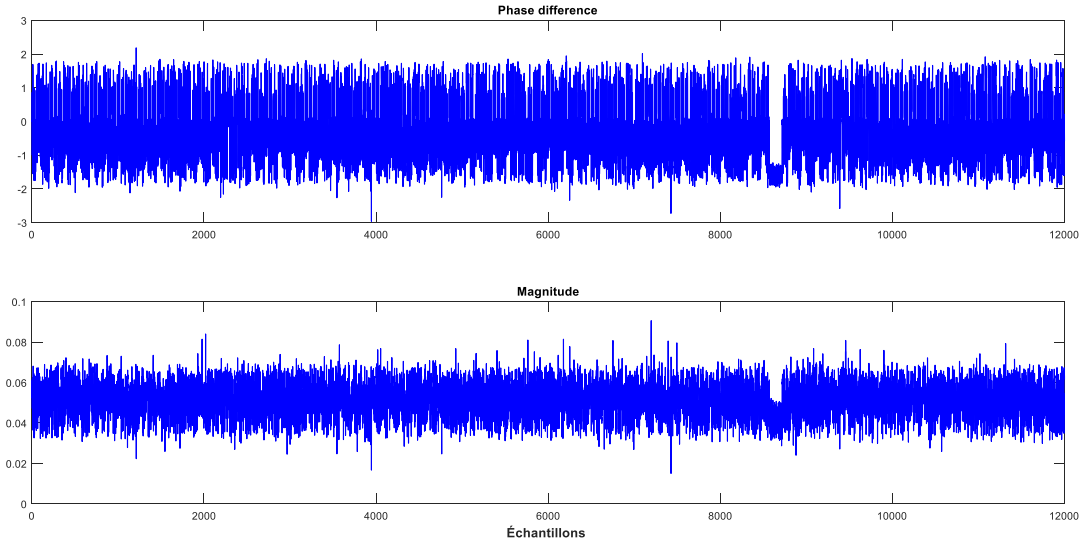

Figure 18: Différence de phase

Dans la figure 18, nous pouvons observer la différence de phase du signal capturé sur 941,3 MHz. L'algorithme de détection du burst FCCH utilise cette différence de phase pour localiser précisément le début du burst FCCH.

À chaque itération de la boucle, un segment de largeur w se déplace d'une position dans le vecteur de différence de phase avec :

$$W = \frac{142\ bits * fs}{Débit\ GSM} \qquad (4)$$

$Où\ \ fs\ =\ 2.6\ Mhz\ et\ DébitGSM\ =\ 270.833kbps$

Lorsque le segment est positionné, nous calculons la différence entre les valeurs maximales et minimales de ce segment. Si la valeur minimale de cette nouvelle fenêtre est inférieure à un seuil prédéfini, cela indique la présence du burst FCCH à cet emplacement. En détectant le minimum de la différence de phase, nous pouvons déterminer le moment précis où le burst FCCH commence.

Une fois que nous avons localisé le burst FCCH, nous souhaitons connaître la fréquence à laquelle il se trouve. Pour cela, nous extrayons une petite portion du signal où le burst FCCH est présent. En appliquant une transformation de Fourier rapide (FFT) à cette portion de signal, nous obtenons le spectre de fréquence.

Le pic le plus élevé dans le spectre de fréquence correspond à la fréquence détectée du burst FCCH. En identifiant cette fréquence, nous pouvons estimer l'offset de fréquence, qui est la différence entre la fréquence réelle du burst FCCH et la fréquence attendue.

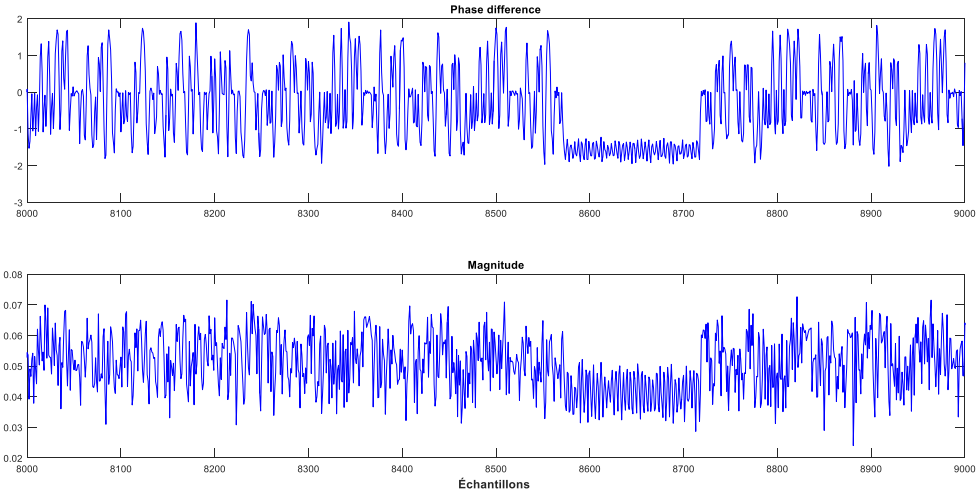

Figure 19 : Différence de phase (zoom x fois)

Dans la figure 19 , En zoomant sur la différence de phase, on peut mieux visualiser les variations de phase à une échelle plus réduite.

5. Décalage de la fréquence de l'oscillateur local

Le dongle RTL-SDR et de nombreux autres appareils SDR présentent un degré d'imprécision dans la sélection de la fréquence d'intérêt (fréquence de réception). Les oscillateurs à cristal sont souvent construits avec une tolérance mesurable, exprimée en PPM (par million de pièces), qui peut varier d'un appareil à l'autre en raison de l'imprécision de fabrication et/ou de la température. Une grande tolérance signifie que la fréquence sélectionnée peut ne pas correspondre exactement à la fréquence que vous vous attendez à recevoir. Vous pouvez constater que le canal reçu n'est pas centré sur la fréquence sélectionnée f_c et est toujours décalé de quelques kilohertz, ce sera à $f_c + \Delta_f$, où Δ_f est un décalage de fréquence.

La détection de la position de du Burst FCH dans le signal reçu permet de déterminer à quelle fréquence elle se trouve, afin de pouvoir calculer le décalage à partir de 67,7 KHz. Le pic le plus élevé dans le spectre du signal reçu correspond à la fréquence détectée de cette burst. Ce pic est ensuite utilisé pour déterminer le décalage de fréquence où :

$$\Delta_f = 67.7KHz - f_{fcch}$$

Δ_f Est le décalage de fréquence et f_{fcch} est la fréquence du burst FCCH détectée dans le signal GSM capturé.

6. Conclusion

Le chapitre présente un l'algorithme de détection du Burst FCCH, en se concentrant sur l'utilisation du dongle RTL-SDR pour capturer les signaux GSM. L'algorithme propose une approche en plusieurs étapes pour extraire la position du burst FCCH du signal GSM capturé. L'algorithme est appliqué aux données enregistrées à l'aide du RTL-SDR, et les résultats expérimentaux démontrent son efficacité dans la détection des bursts FCCH. Des améliorations et des développements futurs sont envisagés pour optimiser la performance de l'algorithme.

Conclusion générale

En conclusion, ce mémoire s'est concentré sur la détection du BURST FCCH dans un système de communication GSM en utilisant RTL-SDR. À travers une exploration approfondie du GSM, nous avons acquis une compréhension approfondie de son architecture, de ses canaux physiques et logiques, ainsi que de son fonctionnement global.

Nous avons développé un algorithme de détection du burst FCCH basé sur des techniques de traitement du signal. Nous avons décrit en détail les différentes étapes de l'algorithme. Nos expérimentations ont été réalisées en capturant des signaux GSM réels à l'aide de SDR-RTL. Les résultats obtenus ont démontré l'efficacité de notre algorithme de détection, avec des taux de réussite élevés dans la détection du burst FCCH.

Ce travail de recherche présente plusieurs contributions significatives. Tout d'abord, il fournit une méthodologie précise pour la détection du BURST FCCH dans un environnement GSM, en utilisant des outils accessibles tels que RTL-SDR. De plus, il offre une compréhension approfondie des canaux physiques et logiques du GSM, ce qui peut être utile pour d'autres recherches et développements dans ce domaine.

Bibliographie

1. **inchbald, Guy.** *Introduction to GSM: Second Edition.* [éd.] 2017 lulu.com. 2017.

2. **Chipman, Robert A.** *"Transmission Lines and Antenna Principles".*

3. **https://www.memoireonline.com/01/13/6746/Image-5-Supervision-et-exploitation--distance-des-plateformes-de-services-via-le-modele-client-serveur-et.html). [En ligne]**

4. poole, Lan. ***Cellular Communications Explained: From Basics to 3G.*** **[éd.] 2006 Newnes. illustrée,Réimprimé. 2006. p. 201.**

5. Jeffrey H. Reed, Nishith Tripathi. ***Cellular Communications: A Comprehensive and Practical Guide.*** **[éd.] 2014 John Wiley & Sons. illustrée, réimprimée. 2014. p. 1044.**

6. http://ftpmirror.your.org/pub/wikimedia/images/wikipedia/fr/0/08. [En ligne]

7. André, Pérez. ***Architecture des réseaux de mobiles: GSM/GPRS, UMTS/HSPA, EPS, NGN, IMS.*** **[éd.] 2011 Hermes Science Publications. 2011.**

8. Marie-Bernadette Pautet, Michel Mouly. ***The GSM System for Mobile Communications.*** **Telecom Pub juin 1992. 1992.**

9. Siegmund M. Redl, Matthias K. Weber, Malcolm W. Oliphant. , ***GSM and Personal Communications Handbook. ,*** **Artech House, mai 1998. 1998.**

10. Chipman, Robert A. ***"Transmission Lines and Antenna Principles".***

11. Madhow, Upamanyu. ***"Introduction to Communication Systems".***

12. Poli., Alain. ***"Channel Coding: Theory, Algorithms, and Applications", .***

13. Lagrange, Xavier. ***Réseaux GSM.*** **HERMES. 2000.**

14. Abramson, Norman. ***"Information Theory and Coding".***

15. Jr, Peyton Z. Peebles. ***"Probability, Random Variables, and Random Signal Principles",.***

16. Sklar, Bernard. ***"Digital Communications: Fundamentals and Applications".***

17. Haykin., Simon. ***"Digital Communication Systems",.***

18. Gallager, Robert G. ***"Principles of Digital Communication.***

19. Forouza, Behrouz A. ***"Data Communications and Networking",.***

20. Stremler., Ferrell G. ***ntroduction to Communication Systems", .***

21. Gibson, Jerry D. ***"Mobile Communications Handbook".***

22. Pautet., e Michel Mouly et Marie-Bernadette. ***"The GSM System for Mobile Communications",.***

23. https://telecomstudy18.blogspot.com/2014/04/ttypes-of-burst-in-gsm.html. [En ligne]

24. Pautet, Michel Mouly et Marie-Bernadette. ***"The GSM System for Mobile Communications", .***

25. Goldsmith., Andrea. ***"Wireless Communications".***

26. Stremler, e Ferrell G. ***"Introduction to Communication Systems", .***

27. Laufer, C.,. The Hobbyist's Guide to the RTL-SDR: Really Cheap Software Defined Radio, . (2015) .

28. Cass, S. A $40 software-defined radio, IEEE Spectrum, 50(7), pp. 22-23. . (2013) .

29. R. Yagoub, 1 M. Benaissa,1,2 B. Benadda,3 et A. Taleb-Ahmed4. LOCAL OSCILLATOR FREQUENCY OFFSET.

30. https://inst.eecs.berkeley.edu/~ee123/fa12/rtl_sdr.html. [En ligne]

31. Varma, G.N., Sahu, U., and Charan, G.P. Robust frequency burst detection algorithm for GSM/GPRS,IEEE 60th Vehicular Technology Conference, 6, pp. 3843-3846. 2004.

32. Gabriel, C., Pablo, F., Beatriz, G.S., Carlos, H.V. et al.,. GSM Sniffer for "Passive" Radio Infrastructure Mapping – and Channel Characterization, Aalborg university. 2011.