République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Jijel

Faculté des Sciences et de la Technologie

Département d'Electronique

Mémoire de Fin d'Etude pour l'Obtention du Diplôme de

Master II en Electronique

Option : Electronique et Systèmes de Communication

Thème

Etude et conception d'un système de brouillage GSM

Présenté par :

- M^elle^ SOUIED Hasna
- M^elle^ BOUREZAK Rima

Encadré par :

Dr. BOUKERROUM Fayçal

Promotion : Juin 2015

Remerciements

Tout d'abord et avant tout Nous remercions « Allah » de nous avoir donné le pouvoir de réaliser ce modeste travail et de nous avoir guider pour arriver à ce que nous sommes maintenant.

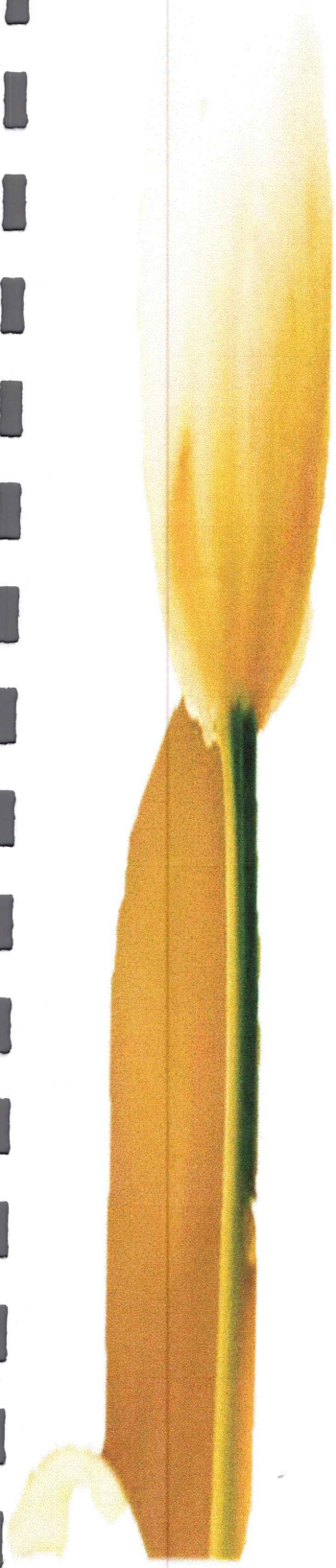
Au nom de la science, de la technologie, de l'esprit scientifique, de la vertu du travail, de l'esprit d'élévation de la connaissance, nous tenons à remercier notre encadreur Monsieur Boukerroum Fayçal Maître de conférences à la faculté de Science et de technologie, à la université de Jijel, pour l'intérêt constant qu'il a apporté à ce travail, pour les conseils qu'il n'a cessé de nous prodiguer et surtout pour la confiance qu'il nous a accordée pour la réalisation de ce projet.

Nous tenons aussi, à remercier tous les membres du jury pour avoir bien voulu examiner notre travail et statuer sur notre candidature.

Nous n'oublierons jamais nos chers profs sans exception dont nous avons le plaisir d'être leurs étudiants pendant des années.

Enfin, nous exprimons nos remerciements à toute personne ayant intervenue de près ou de loin à l'élaboration de ce travail.

Merci



Dédicace

Je tiens vivement à dédié ce travail en signe de respect et de reconnaissance :

À mes très chers parents,

À mes sœurs,

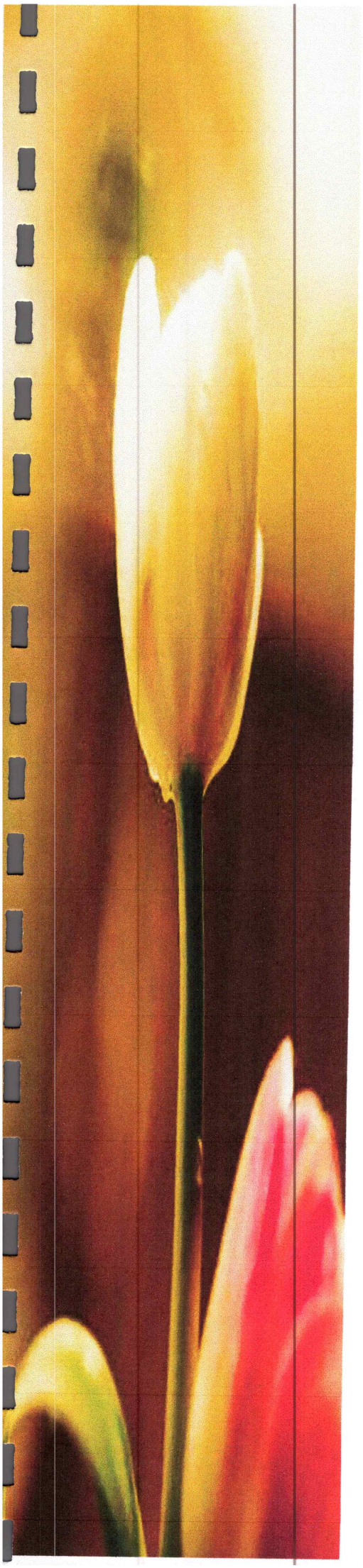
À toute ma famille.

À tous ceux que j'aime et ceux qui m'aiment.

*A mon binôme : **Rima***

À tous mes amies d'études pour les bons moments qui nous avons passé ensemble.

Hasna



Dédicace

Je tiens vivement à dédié ce travail en signe de respect et de reconnaissance :

À mes très **chers parents (Mahmoud & Najia)** qui m'ont toujours poussé et motivé dans mes études. Ce mémoire représente donc l'aboutissement du soutien, des encouragements et de confiance qu'ils m'ont prodigués tout au long de ma scolarité. Qu'ils en soient remerciés par cette modeste dédicace.

À mes frère **Oussama**, **Amine** et **Mohamad**,

À mes oncles et mes tantes,

À tous membre de ma grande famille,

À mon binôme : **Hasna**

À tous ceux que j'aime.

À tous mes amies d'études pour les bons moments que nous avons passé ensemble.

Rima

Sommaire

Chapitre 2: Notions et techniques du brouillage GSM

Chapitre 3: Etude et conception du brouilleur GSM

Liste des Abréviations et Acronymes

3G	3iéme Génération
ACCH	Associated Control Channel
AuC	Authentication Center
BCCH	Broadcasting Control Channel
BF	Basses Fréquences
BSS	Base Station Subsystem
BSS	Base Station System
BTS	Base Transceiver Station
CAN	Convertiseur Analogique Numérique
CCH	Commun Control Channel
CDMA	Code Division Multiple Access
CNA	Convertiseur Numérique Analogique
DCCH	Dedicated Control Channel
DSP	Digital Signal Processor
ECCM	Electronic Counter Counter Measures
ECCM	Electronic Counter Counter Measures
ECM	Electronic Counter Measures
EIR	Equipement Indentity Register
EMI	Electro-Magnetic Interference
ESM	Electronic Support Measures
ESM	Electronic Support Measures
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access

FI	Fréquence Intérimaire
FR	Fréquence Radio
FSL	Free Space path Loss
GMSC	Gateway MSC
GMSK	Gaussian Minimum Shift Keying
GSM	Global System for Mobile
HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Indentity
LA	Location Area
LNA	Les amplificateurs à faible bruit
MS	Mobile Station
NPN	Transistor
NSS	Network Sub-System
OSS	Operation Sub-System
PGC	Amplificateur
PLMN	Public Land Mobile Network
RACH	Random Access Channel
RTC	Réseau Téléphonique Commuté
SIM	Subscriber Indentity Module
SNR	Signal Noise Rate
SNR_{min}	Rapport Signal sur Bruit minimal
TCH	Traffic Channel
TDMA	Time Division Multiple Access

UMTS	Universal Mobile Telecommunications System
VCO	Voltage Controlled Oscillator
VLR	Visitor Location Register

Liste des figures

Liste des tableaux

Chapitre 1
Etude du réseau de téléphonie mobile GSM et du récepteur mobile GSM

Chapitre I

Etude du réseau de téléphonie mobile et du récepteur mobile GSM

1. Introduction

Le **GSM** (**G**lobal **S**ystem for **M**obile communications), est un système cellulaire et numérique de téléphonie mobile. Il a été rapidement accepté et a vite gagné des parts de marché. L'utilisation du numérique pour transmettre les données permet des services et des possibilités élaborées par rapport à tout ce qui a existé. On peut citer, par exemple, la possibilité de téléphoner depuis n'importe quel réseau GSM dans le monde. Les services avancés et l'architecture du GSM, ont fait de lui un modèle pour la troisième génération (**3G**) des systèmes cellulaires, le réseau **UMTS** (**U**niversal **M**obile **T**elecommunications **S**ystem) [1].

Dans la première partie de ce chapitre, on présentera les caractéristiques principales du système GSM. La structure du récepteur mobile GSM, sera exposée dans une deuxième partie du chapitre.

2. Structure du réseau GSM

2.1. Système cellulaire [2]

Dans un système cellulaire, la région couverte est divisée en cellule, comme illustré à la figure 1.1. Une cellule est de forme circulaire mais dépend en réalité de la topographie de la région qui est servie par l'antenne de la cellule. Ce système peut être illustré par des hexagones au centre d'une cellule on retrouve un ensemble d'émetteurs-récepteurs correspondant à une bande de fréquences.

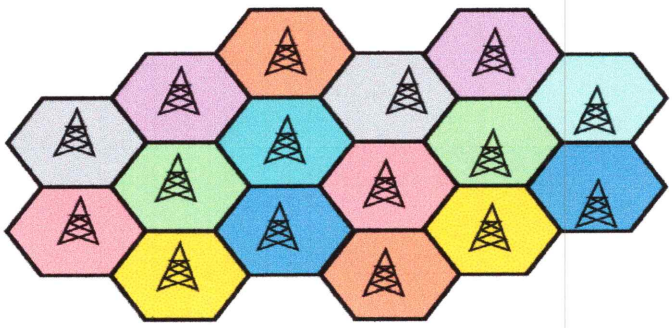


Figure 1.1 : Système cellulaire GSM.

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. Par contre, en utilisant des cellules plus petites, (émetteur-récepteur moins puissant) alors la même bande de fréquence pourra être réutilisée plus loin, ce qui augmente le nombre de communications possibles.

Dans la conception d'un réseau cellulaire, il faut considérer les aspects suivants :

- La topographie (bâtiments, collines, montagnes,...).
- La densité de la population (ou de communications) pour établir la dimension de cellule.
- Deux cellules adjacentes ne peuvent utiliser la même bande de fréquence afin d'éviter les interférences. La distance entre deux cellules ayant la même bande doit être de 2 à 3 fois le diamètre d'une cellule.

La taille des cellules peut varier entre 0.5 et 35 km et dépend de la densité d'utilisateur et de la topographie. Les cellules sont regroupées en bloc (appelé motif ou cluster). Le nombre de cellules dans un bloc doit être déterminé de manière à ce que le bloc puisse être reproduit continuellement sur le territoire à couvrir typiquement, le nombre de cellules par bloc est de 4 7,12 ou 21. La forme et la dimension des blocs et le nombre de cellules est fonction du nombre de fréquences (canaux) disponibles.

2.2. Architecteur d'un réseau GSM

Le réseau GSM a pour premier rôle de permettre des communications entre abonnés mobiles (GSM) et abonnés du réseau téléphonique fixe **RTC (R**éseau **T**éléphonique **C**ommuté). Il s'interface avec le réseau fixe et comprend des commutateurs, et se distingue par un accès spécifique : la liaison radio. L'architecture d'un réseau GSM peut être divisée en 4 parties principales :

a) La station mobile : **MS - M**obile **S**tation ;

b) Le sous-système radio : **BSS - B**ase **S**tation **S**ubsystem;

c) Le sous-système réseau : **NSS** – **N**etwork **S**ub-System;

d) Le sous-système opération : **OSS** – **O**peration **S**ub-System.

Les éléments de l'architecture d'un réseau GSM sont repris sur le schéma de la figure 1.2.

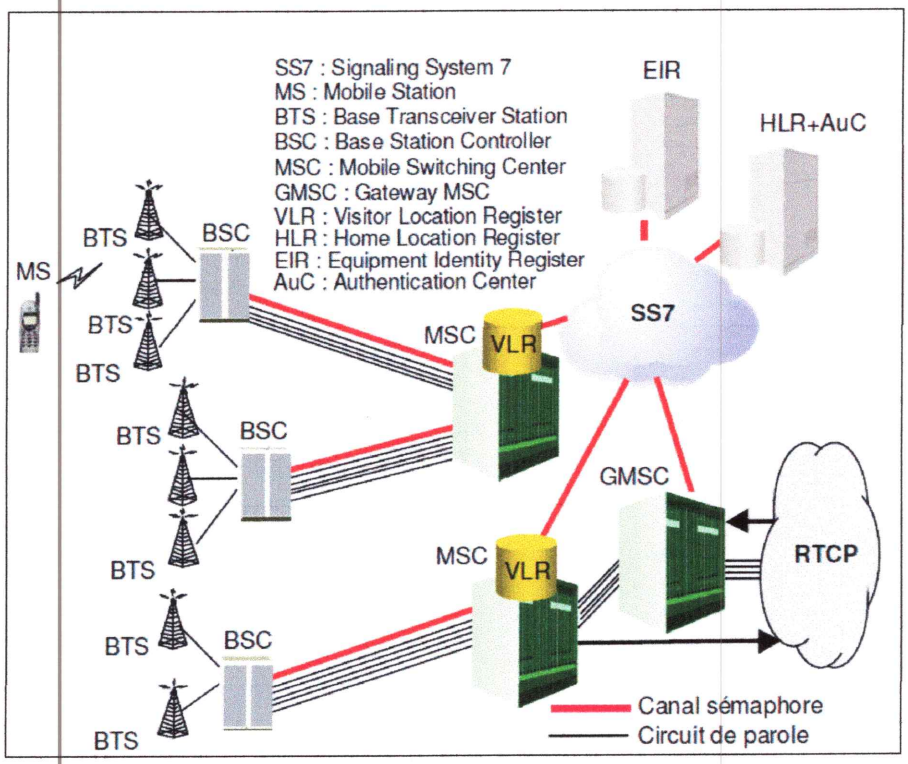


Figure 1.2 : Architecture du réseau GSM.

a. Station mobile (MS)

La station mobile est composée d'une part du **terminal mobile**, et d'autre part du module d'identité d'abonné **SIM** (**S**ubscriber **I**ndentity **M**odule).

Le terminal mobile est l'appareil utilisé par l'abonné. Différents types de terminal sont prescrits par la norme en fonction de leur application (fixé dans une voiture, portatif) et de leur puissance (de 0.8W à 20W). Chaque terminal mobile est identifié par un code unique **IMEI** (**I**nternational **M**obile **E**quipment **I**dentity). Ce code est vérifié à chaque utilisation et permet la détection et l'interdiction des terminaux volés.

La SIM est une carte à puces qui contient dans sa mémoire le code **IMSI** (**I**nternational **M**obile **S**ubscriber **I**ndentity) qui identifie l'abonné de même que les renseignements relatifs à l'abonnement (services auxquels l'abonné a droit). Cette carte peut être utilisée sur plusieurs appareils. Il est à noter que l'usager ne connaît pas son IMSI mais il peut protéger sa carte à puce à l'aide d'un numéro d'identification personnel à 4 chiffres [2].

b. Le sous-système radio (BSS – Base Station System)

Le sous-système radio gère la transmission radio, il est constitué de deux parties :

b.1. Station de base (BTS – Base Transceiver Station)

La BTS représente la partie radio du réseau GSM, elle relie les stations mobiles à l'infrastructure fixe du réseau. La BTS est composé d'un ensemble d'émetteur-récepteurs, elle assure :

- La gestion du multiplexage temporel (une porteuse est divisée en 8 slots dont 7 sont alloués aux utilisateurs), et la gestion des sauts de fréquences.
- Les opérations de chiffrements.
- Les mesures radio permettant de vérifier la qualité de service, ces mesures sont transmises directement au BSC.
- La gestion de la liaison de données (données de trafic et de signalisation) entre les mobiles et la BTS.
- La gestion de la liaison de trafic et de signalisation avec le BSC [3].

b.2. Le contrôleur de station de base (BSC – Base Station Controler)

Dont le rôle est de gérer les ressources radio (configuration des canaux, transfert intercellulaire) d'une ou plusieurs stations de base (BTS), en plus d'établir le lien physique (via l'interface **A**) entre les BTS et le commutateur de service mobile (**MSC** - **M**obile **S**witching **C**enter) [2].

c. Le sous-système réseau (NSS)

Le rôle principal de ce sous-système est de gérer les communications entre les abonnés et les autres usagers qui peuvent être d'autres abonnés, ou des usagers de réseaux téléphoniques fixes [2]. Ce système contient :

c.1. Commutateur de service mobile (MSC – Mobile Switching Center)

Cet élément peut être considéré comme le cœur d'un système cellulaire puisqu'il assure la gestion des appels et de tout ce qui est lié à l'identité des abonnés, à leur enregistrement et à leur localisation. Le MSC agit en somme comme un nœud d'un réseau commuté [3].

c.2. Commutateur d'entrée de service mobile (GMSC – Gateway MSC)

Ce commutateur est l'interface entre le réseau cellulaire et le réseau téléphonique publique. Le **GMSC** est chargé d'acheminer les appels du réseau fixe à un usage GSM [2].

c.3. Registre des abonnés locaux (HLR – Home Location Register)

Il s'agit d'une base de données contenant les informations sur les abonnés appartenant à la région desservie par le commutateur de services mobiles (MSC).Cette base de données contient également la position courante de ses abonnés [3].

c.4. Registre des abonnés visiteurs (VLR – Visitor Location Register)

Cette base de données contient temporairement des informations sur les abonnés qui visitent une région desservie par un MSC autre que celui auquel ils sont abonnés. Ces informations proviennent du HLR auquel l'abonné est enregistré et indiquent les services auxquels l'abonné a droit. Ce transfert d'informations ne se fait qu'une seule fois et n'est effacé que lorsque l'abonné ferme son appareil ou quitte la région du MSC courant.

En procédant ainsi, le VLR n'a pas à interroger le HLR chaque fois qu'une communication est demandée par ou pour l'abonné visiteur. Il est à noter que le VLR est toujours associé à un MSC [2].

c.5. Centre d'authenticité (AuC – Authentication Center)

L'AuC est une base de données protégée qui contient une copie de la clé secrète inscrite sur la SIM de chaque abonné. Cette clé est utilisée pour vérifier l'authenticité de l'abonné et pour l'encryptage des données envoyées [3].

c.6. Registre d'identification d'équipement (EIR – Equipement Indentity Register)

Comme nous l'avons vu précédemment, chaque terminal mobile est identifié par un code IMEI. Le registre EIR contient la liste de tous les terminaux valides. Une consultation de ce registre permet de refuser l'accès au réseau à un terminal qui a été déclaré perdu ou volé.

d. Sous-système opération (OSS)

Ce sous-système est branché aux différents éléments du sous-système réseau de même qu'au contrôleur de station de base (BSC). Par une vue d'ensemble du réseau le OSS contrôle et gère le trafic au niveau du BSS [3].

2.3. Régions géographiques d'un réseau GSM

La figure 1.3 ci-dessous illustre les différentes zones géographiques auxquelles on peut relier d'un réseau GSM.

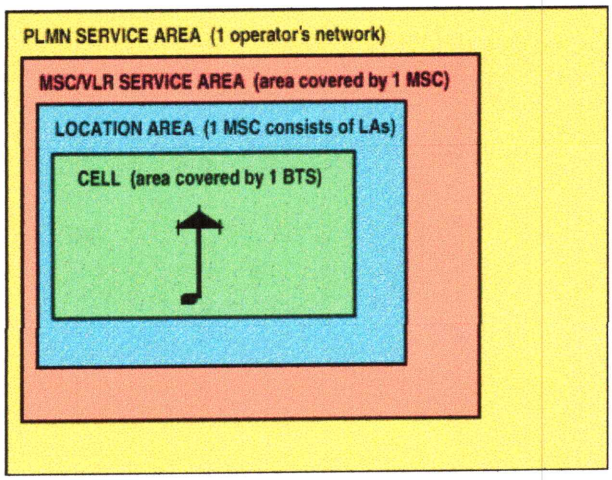


Figure 1.3 : Régions géographiques d'un réseau GSM.

- **CELL** : C'est une cellule correspond à la région couverte par une station de base (BTS).
- **LA** : Une région de repérage (**LA** – **L**ocation **A**rea) est un groupe de cellules. C'est la région par laquelle on localise un abonné. Chaque LA est servi par un ou plusieurs contrôleurs de station de base (BSC), mais par un seul MSC.
- **MSC** : C'est un ensemble de régions de services MSC/VLR qui représente la région desservie par un opérateur de réseau [2]

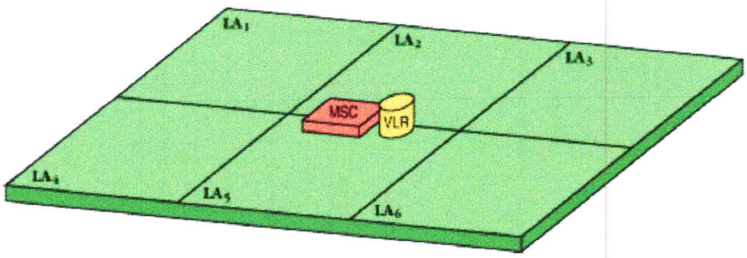


Figure 1.4 : Région de service MSC.

- Le **PLMN** (**P**ublic **L**and **M**obile **N**etwork) : réseau mobile d'une région public est défini comme un réseau installé et gère par un opérateur pour fournir un service de communication mobile au public.

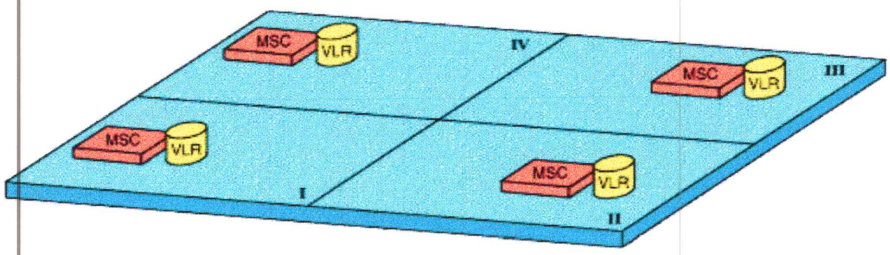


Figure 1.5 : Région de service PLMN.

2.4 Fréquences de travail GSM

Dans le système GSM, deux bandes de fréquences sont utilisées, l'une autour des 900 MHz et l'autre autour de 1,8 GHz. Chaque bande est divisée en deux sous-bandes servant l'une pour le transfert d'informations entre le mobile et la station de base (voie montante) et l'autre pour la liaison entre la station de base et le mobile (voie descendante).il s'agit d'un duplexage fréquentiel **FDD** (**F**requency **D**ivision **D**uplex): sens montant (**Uplink**) et sens descendant (**Downlink**) sur des fréquences différentes [4]. On distingue les bandes suivantes :

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

Tableau 1.1 : Fréquences de travail en GSM 900 -1800 MHz.

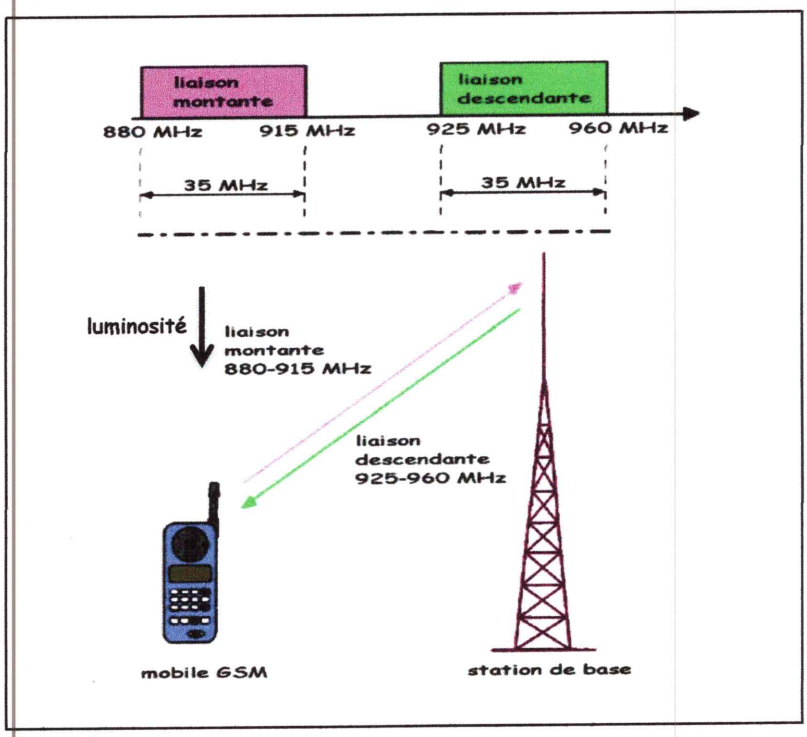


Figure 1.6 : Liaison entre stations MS et BTS.

2.5. Présentation des interfaces entre équipements du réseau GSM [3]

Les interfaces normalisées sont utilisées entre les équipements du réseau GSM pour la transmission du trafic (paroles ou données) et pour les informations de signalisation. La normalisation des interfaces garantit la communication entre des équipements hétérogènes produit par des constructeurs différents.

Toutes les liaisons entre les équipements GSM sauf avec la station de base sont des liaisons numériques. La liaison entre BTS et MS est une liaison radio numérique.

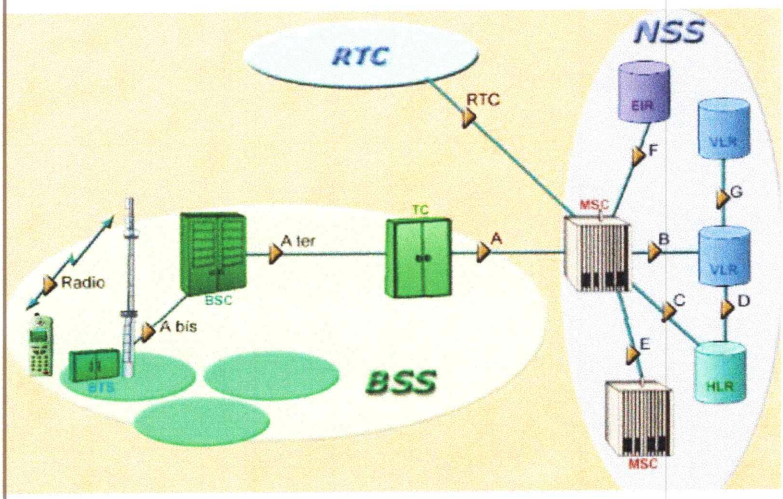


Figure 1.7 : Interfaces du réseau GSM.

- **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.
- **Interface B** entre MSC et VLR.
- **Interface C** entre MSC et HLR.
- **Interface E** entre MSC et MSC.
- **Interface F** entre MSC et EIR.
- **Interface G** entre VLR et VLR.
- **Interface D** entre VLR et HLR/AuC.
- **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.

2.6. Le multiplexage dans le GSM

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**).

a. Partage en fréquence (FDMA)

Dans cette technique de partage, chacune des bandes dédiées au système **GSM** est divisée en canaux fréquentiels d'une largeur de **200 KHz**. (figure 1.8)

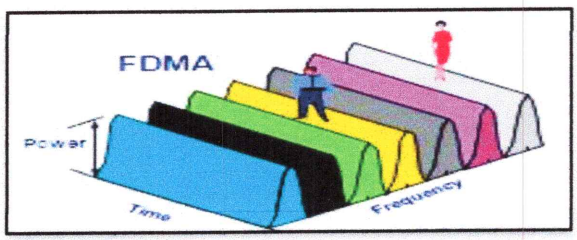


Figure 1.8 : Partage en fréquence.

Les signaux modulés autour d'une fréquence sont alloués d'une manière fixe aux différentes BTS et sont souvent désignés par le terme porteuse qui siège au centre de la bande. De plus, il faut veiller à ce que deux cellules voisines n'utilisent pas deux porteuses identiques ou proches à cause des interférences.

b. Partage en temps (TDMA)

La technique de partage retenue pour le système GSM est le partage en temps TDMA. Cette solution permet de diviser en fait chacune des porteuses utilisées en intervalle de temps appelés « Time Slot ou $\mathbf{T_{slot}}$ ».

La durée élémentaire d'un slot a été fixée pour la norme GSM sur une horloge à 13 MHz et vaut : $\mathbf{T_{slot}} = (75/130) \times 10^{-3}$s, soit environ 0,577us. Chaque slot permet de transmettre un certain nombre de bits que l'on appelle Burst [2].

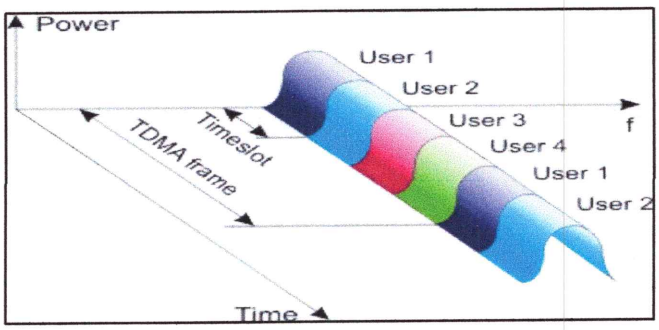


Figure 1.9 : Partage en temps.

L'accès TDMA permet aux différents utilisateurs de partager une bande de fréquence donnée. Sur une même porteuse, les slots sont regroupés par paquets de 8. La durée d'une trame TDMA ($\mathbf{T_{TDMA}}$) est donc (figure 1.10) :

$\mathbf{T_{TDMA}} = 8 \times \mathbf{T_{slot}} = 4{,}615$ ms (1.1)

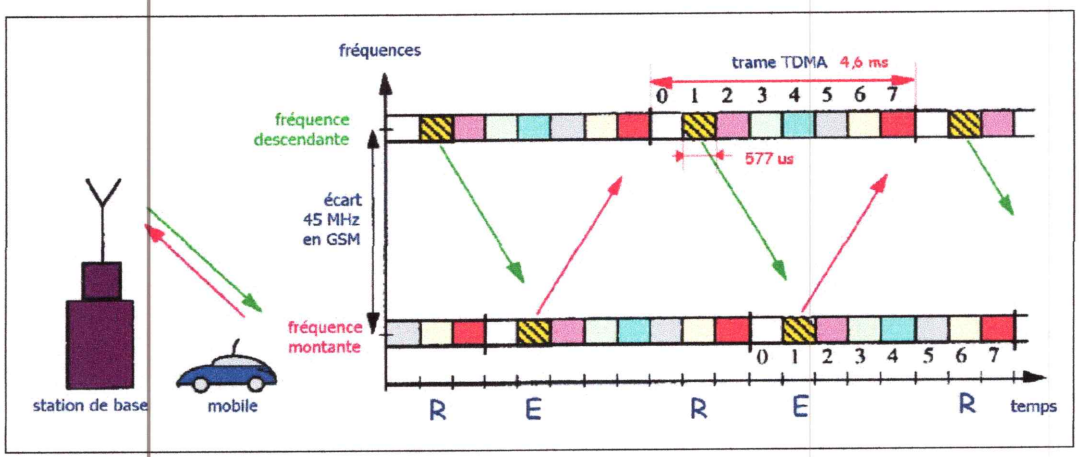


Figure 1.10 : Liaison entre BTS et MS et trame TDMA.

Chaque usager utilise un slot par trame TDMA. Le slot sont numérotés par indice T_n qui va de 0 à 7. Un « canal physique » est constitué par la répétition périodique d'un slot par trame TDMA sur une fréquence particulière [4].

2.7. Les canaux logiques

Dans la norme GSM, on utilise aussi la notion des canaux logique qui sont des séquences particulières de transmission (multi-trames) qui classent les informations suivant leur type. Deux familles de canaux logiques sont définies :

a. Les canaux de trafic (TCH : Traffic CHannel)

Transportent soit de la parole, soit des données et se divisent en deux catégories canaux plein débit et les canaux demi débit.

b. Les canaux de contrôle (Signalisation)

Les différentes classes des canaux de contrôle sont montrer par le tableau 1.2:

Classe	Classe Sous-classe	Fonction
Trafic	TCH Traffic (pour voix codée et pour données) Débit utilisateur 13kbit/s	FR: 22,8kbit/s HR: 11,4kbit/s
Diffusion	BCCH Broadcast Control FCCH Frequency Correction SCH Synchronisation	Information sur la cellule Corrige la fréquence porteuse Donne l'identité de la BTS (BSIC) et synchronise la TDMA
Commun	PCH Paging AGCH Access Grant CBCH Cell Broadcast RACH Random Access	Alerte le mobile Allocation de ressource SMS Permet l'accès au réseau
Dédié	SDCCH Stand Alone Dedicated SACCH Slow (associé à TCH ou SDCCH) FACCH Fast (associé à TCH ou SDCCH)	Signalisation (1/8 TCH) Contrôle la qualité reçue et la puissance Exécution du HO

Tableau 1.2 : Tableau des canaux logiques.

Pour les données de services entre les équipements, on distingue :

- Les canaux de diffusion : **B**roadcasting **C**ontrol **C**hannel (**BCCH**) ;
- Les canaux de contrôle commun : **C**ommun **C**ontrol **C**hannel (**CCH**) ;
- Les canaux associés : **A**ssociated **C**ontrol **C**hannel (**ACCH**) ;
- Les canaux dédiés : **D**edicated **C**ontrol **C**hannel (**DCCH**) ;

2.8. La voie balise et la voie de trafic

Toute BTS émet en permanence des informations sur son canal **BCCH** (**B**roadcast **CH**annel) appelé aussi « **voie balise** ». Ce signal constitue le lien permanent reliant mobile et station de base à partir de la mise en route du mobile jusqu'à sa mise hors service, qu'il soit en communication ou non [4].

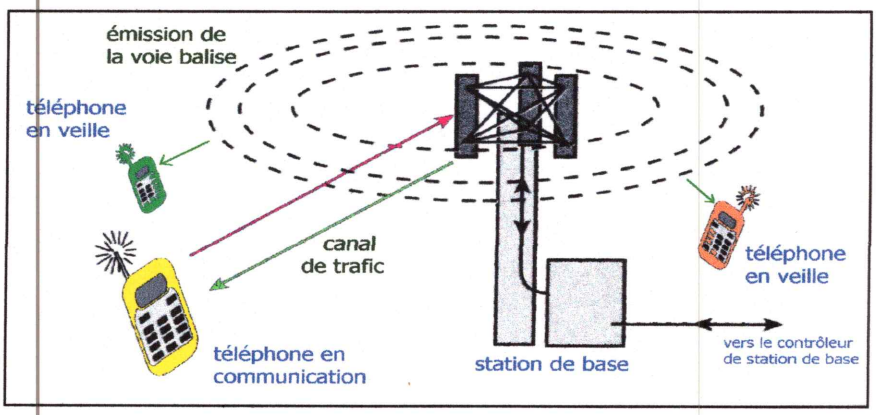


Figure 1.11 : La base diffuse ses informations vers tous les mobiles de la cellule.

Le fonctionnement du mobile se décompose en deux phases **:**

a. Mobile en veille

Le mobile échange avec sa base des signaux de contrôle sur la voie balise (émission en slot 0 à f_1, réception en slot 0 à f_1 + 45 MHz).

Le niveau de la voie balise (BCCH) est connu et sert pour un certain nombre de fonctions de contrôle **:**

- À la mise en route du mobile, son récepteur scrute la bande GSM pour chercher le signal BCCH de niveau le plus élevé. C'est avec la station de base correspondante que le mobile se mettra en communication.
- Ce signal contient des informations concernant les opérateurs de téléphonie mobile et les fréquences balise des cellules voisines.
- Ce signal véhicule les messages qui seront affichés sur l'écran du mobile.

- Il mesure la puissance toutes les 15 secondes si le signal reçu est fort, et toutes les 5 secondes s'il est faible le récepteur écoute les balises des cellules voisines pour détecter un changement de cellule.
- L'émission balise n'occupe le canal de transmission que dans le sens base - mobile.

La liaison montante pourra donc être utilisée par le mobile pour signaler son désir de se connecter au réseau pour une communication **RACH** (**R**andom **A**ccess **Ch**annel) [4].

b. Le Mobile en communication

Le mobile échange avec la base des signaux de parole et de contrôle sur la voie de trafic donc :

- L'émission en slot i à f_2.
- La réception en slot i à f_2 + 45 MHz.

Il émet et reçoit maintenant sur une nouvelle paire de fréquences allouées par la base pour la durée de la communication ; c'est le **TCH** (**T**raffic **CH**annel).

Parallèlement à cette activité principale, il écoute périodiquement les voies balises de la cellule et des cellules voisines pour détecter une variation de niveau lui indiquant un changement de cellule [4].

3. Mobile GSM

Le schéma global d'un mobile GSM est montré par la figure 1.12. Ce schéma bloc peut être décomposé en 4 parties principales :

- Le codage/décodage de la voix appelé aussi traitement en bande de base.
- Les circuits de modulation et d'émission.
- Les circuits de réception et de démodulation.
- Les circuits de contrôle (émission/ réception, porteuse, puissance, alimentations).

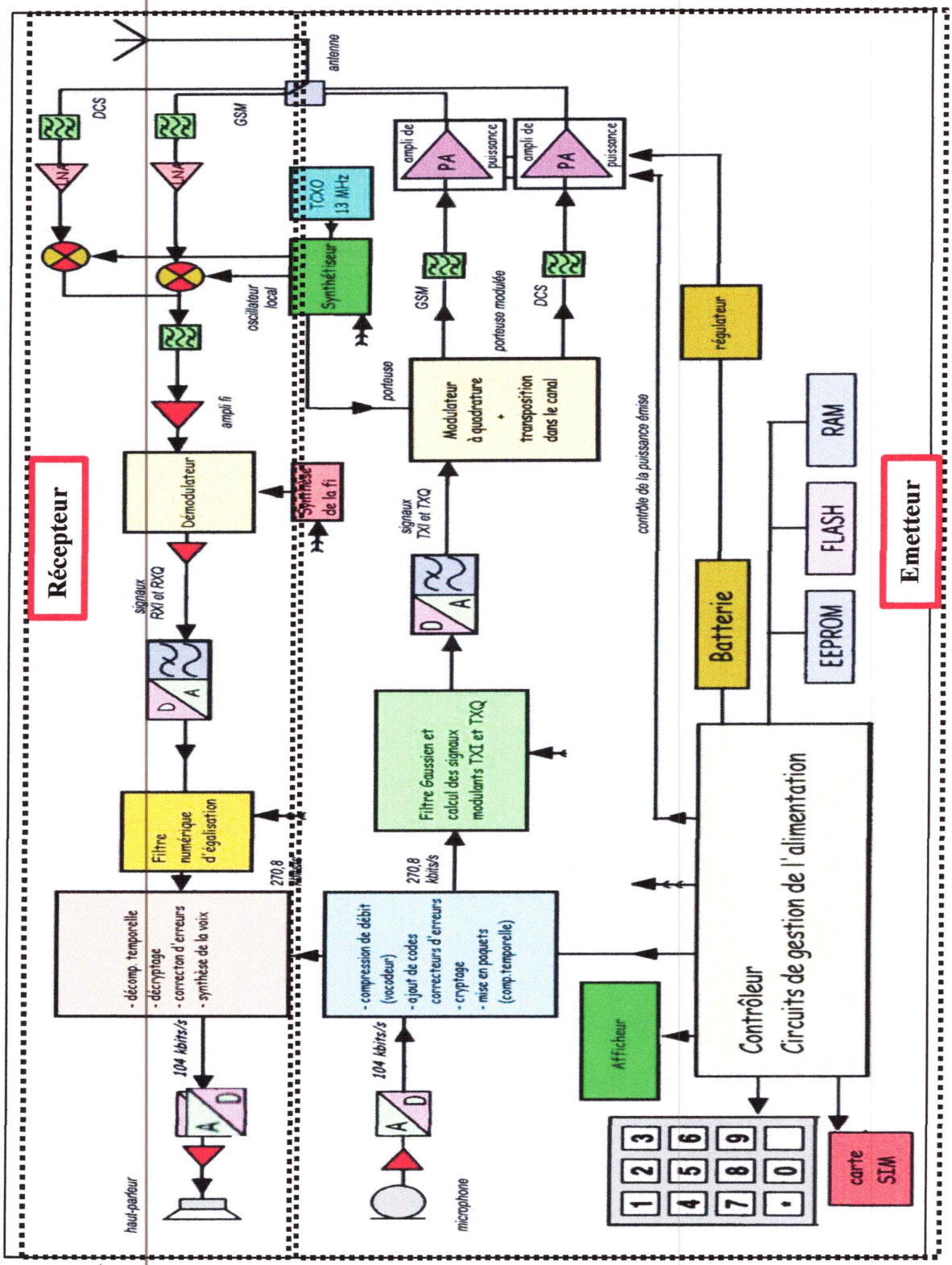


Figure 1.12 : Schéma globale d'un mobile GSM.

3.1. Schéma fonctionnel du mobile en émission [5]

Le récepteur GSM est un téléphone numérique, la voix est donc digitalisée et traitée sous forme numérique par un processeur de signal ou **DSP** (**D**igital Signal **P**rocessor) :

- Le son est capté par le microphone qui fournit un signal analogique (1).
- Il est échantillonné (2) et transformé en échantillons binaires codés sur 13 bits par un convertisseur analogique-numérique (3).
- Les mots binaires sont sérialisés (4) avec un débit brut de D=8000x13=104 Kbits/s.

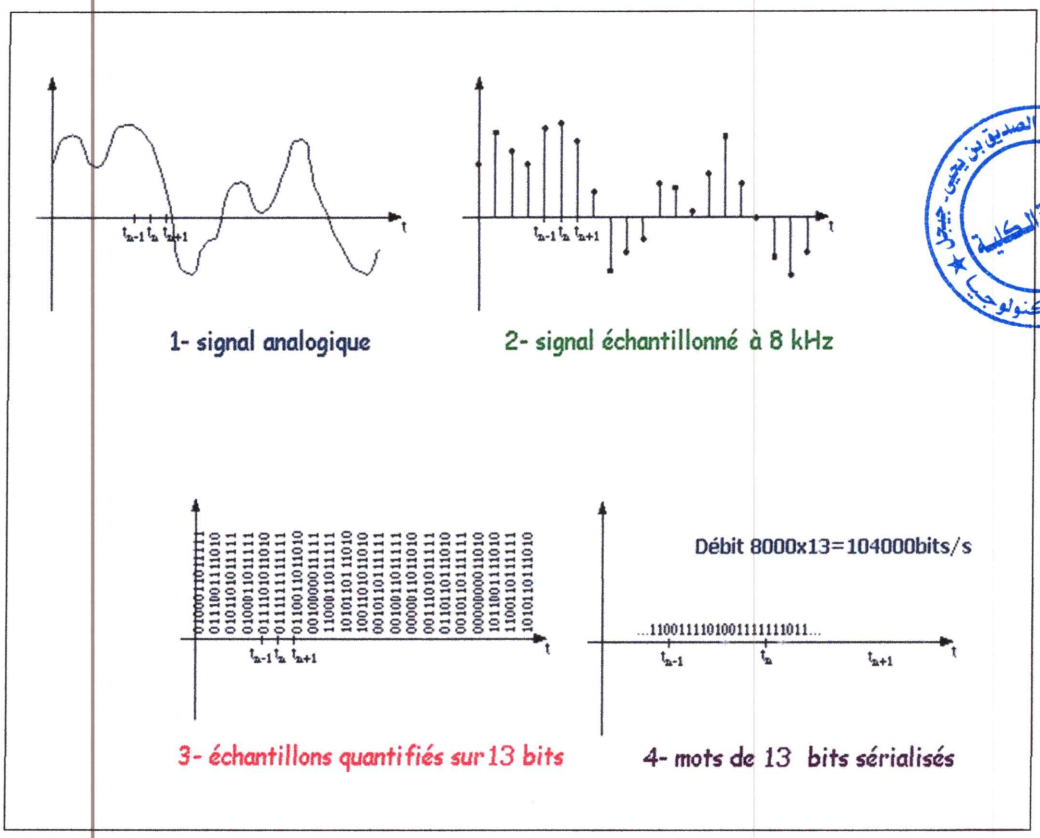


Figure 1.13 : Traitement de la voix dans un téléphone mobile.

Une fois le signal vocal numérisé, il entre dans le DSP pour y subir un certain nombre de traitements numériques :

- Le signal binaire a un débit beaucoup trop important pour être transmis tel quel. Il va donc subir une diminution de débit importante (5) grâce au vocodeur GSM qui abaisse le débit à 13 Kbits/s.
- Les données numériques ainsi obtenues sont protégées par des codes correcteurs d'erreurs permettant de réparer à l'arrivée les erreurs de transmission qui ont pu s'introduire à la suite d'aléas de propagation ou de parasites (6).
- L'application d'algorithmes de cryptage (6) assure la confidentialité des communications.
- Les données sont enfin regroupées en paquets de 156 bits et de durée 577µs (6) pour la constitution de la trame.

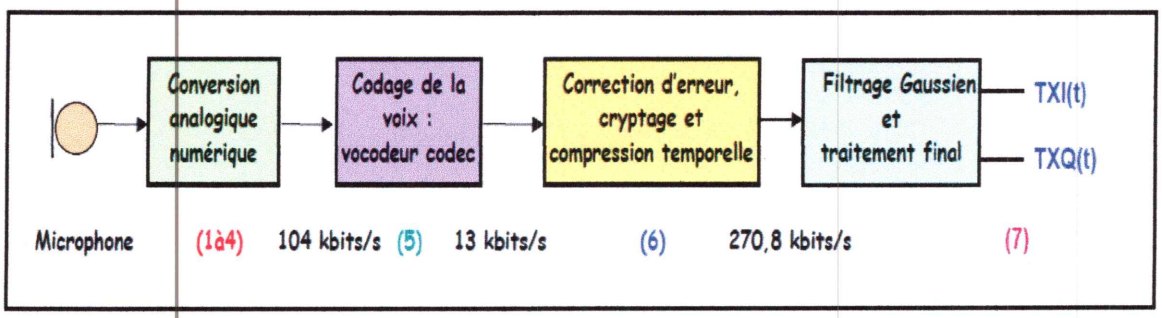


Figure 1.14 : Etapes de traitement du signal vocal.

Après tous ces traitements, les données binaires sortent en (7) regroupées en paquets de 156 bits sous la forme de deux signaux TXI et TXQ, et sont prêts à entrer dans les circuits d'émission pour moduler la porteuse [5].

- **Production de la porteuse modulée**

Le mobile GSM émet une porteuse de fréquence $\mathbf{f_o}$ modulée en phase qui s'écrit :

$$e(t) = E\cos(\omega_o t \pm \pi t/2T_{bit}) \quad (1.2)$$

+ : si on transmet un « 1 » ;

- : si on transmet un « 0 ».

Pendant la durée T_{bit} = 3,6 µs d'un bit, la phase augmente ou diminue suivant la valeur du bit.

Cette porteuse peut aussi s'écrire : $e(t) = E\cos[(\omega_o \pm \pi/2T_{bit}).t]$ (1.3)

Elle a une fréquence : $f = f_o \pm 1/T_{bit} = f_o \pm 68\ KHz$ (1.4)

e(t) : Le signal de la porteuse ; E: Amplitude du signal; w_0 : la pulsation ; f_o : Fréquence de la porteuse.

Ce qui correspond à une modulation de fréquence de type **GMSK** (**G**aussian **M**inimum **S**hift **K**eying), cette porteuse modulée est produite de la façon suivante :

- La porteuse correspondant au canal alloué est produite par un oscillateur commandé en tension du synthétiseur de fréquence piloté par le circuit de contrôle du téléphone.
- Cette porteuse est modulée par les signaux TXI et TXQ pour produire le signal modulé GMSK.
- Ce signal est débarrassé d'éventuels harmoniques par les filtres passe-bande à onde de surface.
- le signal est enfin amplifié pour être amené au niveau d'émission souhaité [5].

- **La régulation de la puissance émise**

La puissance maximale que doit fournir l'amplificateur de puissance de sortie PA est de 2W pour le GSM (33dBm) et 1W pour le DCS (30 dBm).

L'alimentation des amplificateurs de sortie ou PA est reliée directement à la batterie ce qui veut dire que celle-ci doit être capable de fournir le courant maximum nécessaire pendant un burst. Le contrôle de la puissance est indispensable pour deux raisons :

- En phase d'émission, la puissance est régulée à une valeur juste suffisante par la station de base pour une liaison sans erreurs et une consommation minimale.
- En début et fin d'émission, la forme de la montée et de la descente de la puissance est contrôlée par le circuit de gestion du mobile, pour un encombrement spectral minimal [5].

3.2. Schéma fonctionnel du mobile en réception

Dans le téléphone mobile, une structure classique à changement de fréquence permet de sélectionner le signal de la BTS qu'on souhaite recevoir :

- Les filtres d'entrée GSM et DCS fixent la bande reçue et éliminent les signaux indésirables (émissions TV, DECT, autres mobiles GSM à proximité…).
- Les amplificateurs LNA à faible bruit assurent une première amplification.
- Les filtres à ondes de surface en sortie des LNA complètent l'action des filtres d'entrée.
- Les mélangeurs du circuit RF permettent de faire la transposition en fréquence des signaux reçus vers la fréquence « $\mathbf{f_i}$ » par mélange avec le signal issu du synthétiseur.
- L'amplificateur f_i (PGC) permet de garantir des niveaux constants pour les signaux RXI et RXQ sachant que les niveaux à l'antenne sont variables (-40dBm à -110 dBm).
- Le démodulateur I/Q, récupère les signaux RXI et RXQ après mélange avec une fréquence f_i venant d'un second synthétiseur.
- Les signaux IQ sont ensuite amplifiés et filtrés par un filtre passe bas, puis entrent dans le DSP par un CAN (Convertisseur Analogique Numérique).

Ce traitement numérique va permettre de reconstituer le signal vocal :

- Le filtre d'égalisation' grâce aux mesures faites sur la séquence de formation, compense les déformations liées à la propagation dues aux échos et aux trajets multiples du signal.
- Les données binaires sont ensuite extraites des signaux RXI et RXQ par un dispositif de prise de décision logiciel.
- Elles sont décryptées et subissent la décompression temporelle.

- Le vocodeur reçoit ces données et restitue le signal binaire vocal.

Ce signal binaire est converti en analogique par le CNA (Convertisseur Numérique Analogique), amplifié et envoyé sur le haut-parleur [5].

4. Conclusion

Dans ce chapitre, nous avons en premier lieu présenté les principes de base du réseau GSM avec ses différentes techniques définies utilisées. Ces techniques offrent une meilleure qualité de communication et une signalisation en temps réel entre les entités du réseau.

Dans la deuxième partie du chapitre, nous avons présenté la structure globale d'un téléphone mobile GSM .ainsi que ses différents circuits d'émission et de réception.

✓ References bibliographies

[1] L. Deneire « Téléphonie Mobile de troisième génération Cours 3UMTS », Cours Janvier 2008.

[2] P. Brisson et P. Kropf « Global System for Mobile Communication (GSM) », Cours Université de Montréal.

[3] S. Taleb Imane et I. Boudina « développements d'un outil d'optimisation pour l'allocation des fréquences dans le réseau GSM », Mémoire fin d'Etude, Université de Tlemcen , 2013.

[4] J.P. Muller, « Le réseau GSM », Cours physique appliquée, 2007.

[5] J.P. Muller, « Le téléphone GSM », Cours physique appliqué, Septembre 2009.

Chapitre 2

Notions et techniques du brouillage GSM

Chapitre 2

Notions et techniques du brouillage GSM

1. Introduction

Le brouillage radio est une technique de transmission d'un signal radio, visant à interrompre souvent volontairement, des communications en diminuant le rapport signal sur bruit. Des brouillages non-intentionnels peuvent survenir lorsqu'un opérateur transmet des ondes sur une fréquence occupée, sans avoir vérifié préalablement l'utilisation de la fréquence. Ce concept peut être utilisé dans les réseaux sans fil pour empêcher l'information de passer.

En effet, le brouillage est une technique qui est largement utilisée dans le domaine de guerre électronique. Les dispositifs de brouillage de communication ont été développés et utilisés par les militaires. Cet intérêt vient de l'objectif fondamental de bloquer le transport des informations depuis l'expéditeur (commandants tactiques) au récepteur (les membres de l'armée), et vice-versa.

2. Brouillage et guerre électronique

La guerre électronique consiste en l'exploitation des émissions radioélectriques d'un adversaire et, inversement consiste à l'empêcher d'en faire autant. Il s'agit donc de toutes les opérations visant à acquérir la maîtrise du spectre électromagnétique, pour intercepter et/ou brouiller les ordres ou informations circulant dans les systèmes de communication de l'adversaire. La guerre électronique se subdivise en trois branches (figure I.1): l'attaque, le soutien et la protection [1].

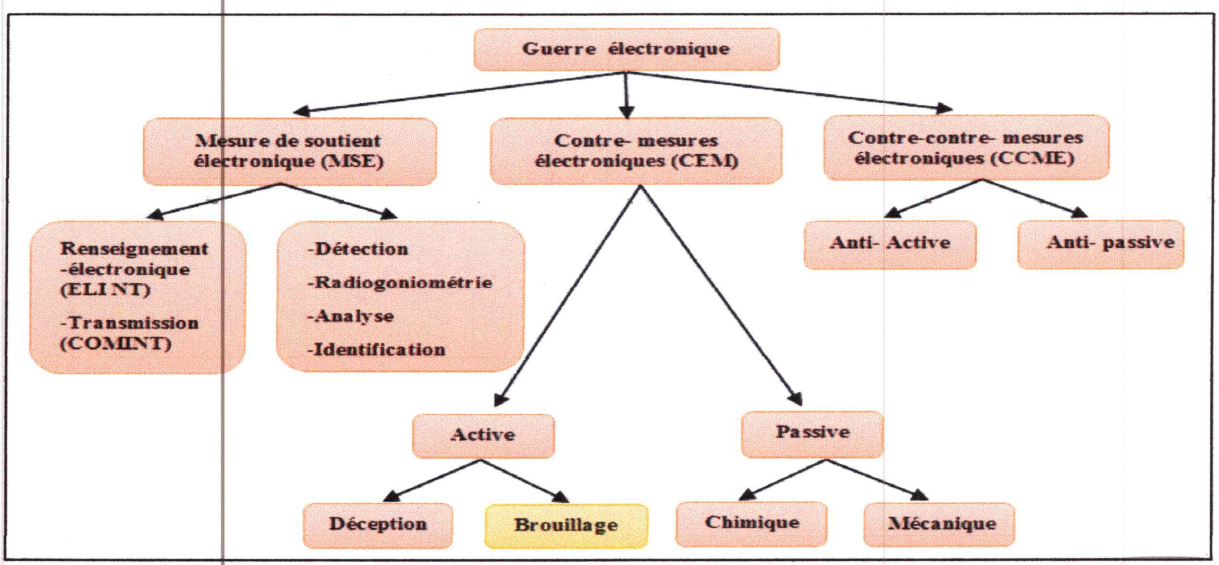


Figure 2.1: Diagramme montrant les éléments de la guerre électronique.

2.1. Le soutien électronique ou la détection électronique

Le soutien électronique ou renseignement électronique rassemble tous les moyens passifs de la guerre électronique. Son objectif est le contrôle du spectre radioélectrique. Les militaires employaient autrefois l'expression mesures de soutien électronique ou **ESM** (**E**lectronic **S**upport **M**easures). Il s'agit d'utiliser les émissions électroniques de l'adversaire pour détecter sa présence, le localiser par goniométrie, et si possible identifier ses unités obtenir des informations sur les systèmes qu'il utilise et écouter ses communications [2].

2.2. La protection électronique

La protection électronique inclut tous les dispositifs et toutes les procédures permettant de contrer les attaques électroniques et les moyens de renseignement électronique de l'adversaire.

On parlait autrefois de mesures de protection électronique et de contre contre-mesures électroniques **ECCM** (**E**lectronic **C**ounter **C**ounter **M**easures) [2].

2.3. L'attaque électronique

L'attaque électronique consiste à empêcher l'adversaire d'utiliser le spectre électromagnétique : il s'agit donc pour l'essentiel de mesures de brouillage de ses émissions et de mesures de leurrage ou d'intrusion. Le brouillage rend inexploitable les émissions de l'adversaire, le leurrage et l'intrusion lui donnent de fausses indications ou de fausses pistes. L'ensemble de ces moyens était autrefois appelé **ECM** (**E**lectronic **C**ounter **M**easures).

L'attaque électronique inclut également l'emploi d'armes à énergie, destinées à détruire les systèmes électroniques adverses. Elle implique l'utilisation de moyens actifs, donc indiscrets.

Il y a deux méthodes principales d'ECM : le brouillage et la déception qui peuvent paralyser l'adversaire. Le brouillage consiste à inonder les communications ennemies par un fort bruit électronique pour couvrir ses communications ou obscurcir les cibles sur ses radars. Bien qu'il soit efficace à perturber les systèmes ennemis, il a comme inconvénient d'empêcher de capter les signaux ennemis pour analyse [2].

3. Brouillage du téléphone mobile

Aujourd'hui, les téléphones mobiles deviennent des outils essentiels dans notre vie quotidienne. Inutile de dire que la large utilisation des téléphones mobiles pourrait créer certains problèmes comme le bruit de sonnerie gênant ou perturbateur. Cela pourrait se produire dans certains endroits comme les salles de conférence, les tribunaux, les salles de

cours et les mosquées. Une façon de mettre fin à ces problèmes est d'installer un dispositif dans les endroits qui va inhiber l'utilisation du téléphone portable, à savoir, le rendre obsolète. Un tel dispositif est connu comme "brouilleur de téléphone cellulaire", qui est essentiellement une sorte de dispositif de contre-mesure électronique [3].

Figure 2.2 : Dispositif de brouillage GSM.

La technologie du brouillage du téléphone cellulaire est très simple. Le dispositif de brouillage diffuse un signal **FR** (**F**réquence **R**adio) dans la gamme de fréquences réservée pour les téléphones cellulaires qui interfère avec le signal de téléphone cellulaire, ce qui entraîne une "absence de réseau" affichée sur l'écran du téléphone cellulaire. Tous les téléphones dans le rayon efficace du brouilleur sont réduits au silence. En 1997, Raoul Girod a déposé le premier brevet d'invention de brouilleurs de téléphone portable [4].

3.1. Utilité du brouillage de téléphonie mobile

Quelques années avant la sortie du brouilleur GSM sur le marché, ces équipements furent seulement utilisés dans le secteur de la défense. De nos jours, les dispositifs de brouillage deviennent des produits civils et nécessaires à l'usage dans certains milieux [5] tels que :

- **Les places religieuses**

L'utilisation de ce type d'appareil n'est intervenu qu'après avoir constaté que plusieurs fidèles s'entêtent à laisser leur mobile en marche au lieu de le mettre en mode silencieux ou de l'éteindre, malgré les campagnes de sensibilisation.

- **Les prisons**

Les établissements pénitentiaires sont également fortement concernés par le brouillage des ondes. En effet, certains détenus se procurent des téléphones mobiles pourtant interdits. Ils peuvent ainsi communiquer à l'intérieur de l'enceinte de la prison, facilitant ainsi les

mutineries ou trafics en tout genre. Ils communiquent également depuis leur cellule vers l'extérieur dirigeant ainsi leurs trafics en toute impunité, ou correspondant avec d'autres personnes avant leur procès.

- **Les milieux sécurisés**

Les hautes personnalités ayant des responsabilités sur le plan national ou international (présidents, ministres, hommes d'affaires...) sont potentiellement les cibles d'actes terroristes. En effet, une bombe déposée sur le trajet d'un convoi de personnalité peut être activée à distance par un simple téléphone mobile.

Le brouilleur transportable situé dans le convoi est destiné à neutraliser toute communication au passage de celui-ci, et ainsi empêcher la détonation de la bombe.

- **Salles de conférences**

Les réunions, conférences, conventions, briefings et autres meetings sont régulièrement la cible d'actes d'espionnage ou d'écoutes à distance par le biais de micros et caméras espions mais également via les ondes de téléphonie mobile.

Le brouillage de ces ondes permet donc de s'assurer qu'aucune information confidentielle ne filtre hors des murs et des oreilles autorisées à les entendre.

Enfin, les théâtres, les cinémas, les salles de spectacle, les musées, les galeries d'art, les bibliothèques... Et de façon générale, partout où l'on assiste à la représentation d'une œuvre de l'esprit. En effet, une sonnerie intempestive ou la réception d'un SMS peut déranger les spectateurs, les comédiens, les visiteurs etc.

3.2. Principe de fonctionnement d'un brouilleur GSM

Lorsque vous démarrez le brouilleur de téléphone cellulaire légal, vous bloquez littéralement tout signal de téléphone mobile dans une zone d'un périmètre donné. Nous savons que nos téléphones mobiles utilisent des antennes d'un réseau particulier afin d'établir une communication. La fonction d'un brouilleur de téléphone mobile est simplement de transmettre un signal perturbateur (bruit) sur les mêmes fréquences radio que celles des signaux des téléphones mobiles. De cette façon, le brouilleur rompt la connexion entre le téléphone et l'antenne la plus proche [6]. En général, les dispositifs de brouillage ont une émission assez puissante qui permet à la même fréquence radio et à une puissance assez haute d'établir la collision avec le signal GSM afin de l'éliminer.

Mais le système des téléphones mobiles peut ajouter de la puissance électrique dès qu'il rencontre une diminution de sa puissance dûe à l'interférence avec d'autres dispositifs. Le brouilleur doit reconnaître cette augmentation en puissance et doit réagir pour compenser.

Les téléphones mobiles sont des dispositifs full-duplex utilisant deux fréquences séparées l'une pour la parole et l'autre pour entendre simultanément. Certains brouilleurs bloquent l'une des deux fréquences, ce qui a pour effet de bloquer les deux. Le téléphone mobile va afficher un message d'absence de service, car à ce temps-là il ne reçoit pas l'une des deux fréquences.

La puissance du brouilleur dépend de quelques facteurs à savoir, la proximité des obstacles, intérieur et extérieur aux bâtiments, humidité et température ... Il ne faut pas que le brouilleur soit proche des pacemakers et doit avoir une puissance inférieur à 1 Watt pour éviter le mal fonctionnement d'autres dispositifs fonctionnant à des fréquences et puissances proches surtout à l'intérieur des hôpitaux [7].

3.3. Paramètre de conception d'un brouilleur GSM

La conception d'un brouilleur nécessite la définition de certains paramètres à vérifier afin que le dispositif de brouillage puisse accomplir sa tâche correctement. Les plus importants de ces paramètres sont :

a. Porté du brouilleur

C'est la distance maximale de brouillage *d* que le signal de brouillage peut atteindre en ayant une puissance suffisante pour accomplir la tâche de brouillage. Ce paramètre est très important dans la conception, puisque la quantité de la puissance de sortie du brouilleur dépend de la surface qu'il faut recouvrir. Plus tard, nous verrons la relation entre la puissance de sortie et la distance de brouillage *d* [3].

b. Bande de fréquence d'opération

La bande de fréquences d'opération du dispositif de brouillage est un facteur important dans sa conception. En effet, le système de téléphonie mobile est un system de communication full-duplex. Cela signifie qu'une partie de la bande de fréquences est attribuée aux signaux de liaison montante (de téléphone mobile à la station de base), l'autre partie est attribuée aux signaux de liaison descendante (de la station de base vers le téléphone mobile) [7].

Le brouillage sur la voie descendante (Downlink) est plus simple que celui exercé sur la voie montante (uplink), puisque l'antenne de la station de base est ordinairement placée loin du mobile. Mais le signal Random Access Channel (RACH) contrôle les canaux de toutes les

BTS dans la région et il est nécessaire de le brouiller pour arrêter la transmission. Donc, pour couper une connexion existante, le brouillage doit durer jusqu'à ce que le " call re-establishment timer " soit finit et la connexion soit lâchée, ce qui signifie qu'un appel existant peut être coupé après quelques secondes de brouillage effectif.

Le principe de fonctionnement du RACH du système GSM est très simple: Quand un appel (request) ne reçoit pas de réponse, la MS va répéter cet appel après un intervalle aléatoire. Le nombre maximal des répétitions et la durée entre elles, sont diffusés régulièrement. Après qu'une MS ait essayé de faire un request service sur RACH et était rejetée, elle va essayer de faire un request service d'une autre cellule. Donc, la cellule dans la région doit être brouillée. Dans beaucoup de cas, l'efficacité de brouillage est très difficile à déterminer, puisqu'elle dépend de plusieurs facteurs, ce qui met le brouilleur en confusion [6].

Les deux bandes de fréquences du système GSM à brouiller sont présentées dans le tableau suivant:

	La voie montante (Uplink)	**La voie descendante (Downlink)**
GSM 900	890-915 MHz	935-960 MHz
GSM 1800 (DCS)	1710-1785 MHz	1805-1880 MHz

Tableau 2.1 : Bandes de fréquences du système GSM.

c. Pertes par propagation en espace libre (*FSL*)

Comme notre signal de brouillage se propage en espace libre, il va subir une atténuation. Il existe quelques paramètres qui influent sur l'amplitude du facteur de pertes en espace libre ***FSL*** (***F**ree **S**pace path **L**oss*). Ces paramètres peuvent être vus dans la formule de calcul du *FSL* [7].

$$FSL = \left(\frac{(4\times\pi\times d)}{\lambda}\right)^2 = \left(\frac{(4\times\pi\times d\times f)}{c}\right)^2 \qquad (2.1)$$

L'expression (2.1), peut être écrite sous forme logarithmique comme suite :

$$FSL\ (dB) = 32.45 + 20\times\log_{10}(f\times d) \qquad (2.2)$$

Où λ : longueur d'onde ; c: vitesse de la lumière dans le vide, d la distance de l'émetteur.

d. Rapport signal sur bruit

Le brouillage est efficace lorsque le signal de brouillage réussi à rompre la transmission de la communication. Dans le cas des communications numériques, la transmission est considérée inefficace lorsque le taux de transmission d'erreur ne peut être compensé par la correction d'erreur. Dans le cas des communications analogiques, le brouillage réussi si au niveau du récepteur (téléphone mobile) la puissance du signal de brouillage est égale à la puissance du signal utile [3].

L'expression générale du rapport signal brouillage/ signal utile est donné par:

$$\frac{S_B}{S} = \frac{P_B . G_{BR} . G_{RB} . R_{ER}^2 . L_R . B_R}{P_E . G_{ER} . G_{RE} . R_{BR}^2 . L_B . B_B} \quad (2.3)$$

P_B : Puissance du brouilleur ;

P_E : Puissance de l'émetteur (BTS);

G_{BR} : Gain de l'antenne du brouilleur au récepteur (MS);

G_{RB} : Gain de l'antenne du récepteur au brouilleur;

G_{ER} : Gain de l'antenne de l'émetteur au récepteur;

G_{RE} : Gain de l'antenne du récepteur à l'émetteur;

B_R : Bande de fréquences de communication au récepteur;

B_B : Bande de fréquences du brouilleur;

R_{ER} : Distance entre émetteur et récepteur;

R_{BR} : Distance entre brouilleur et récepteur;

L_B : Pertes dans le signal du brouilleur;

L_R : Pertes dans le signal de communication.

Pour le système GSM le SNR spécifié est de 9dB.Cette valeur sera utilisé comme le cas le plus déformable pour le brouilleur.

4. Stratégie et techniques de brouillage

Il existe plusieurs manières pour brouiller un dispositif FR. Parmi les stratégies sur lesquels les techniques de brouillage sont basées on peut citer :

- Le brouillage avec gestion des appels d'urgence;
- Le brouillage après détection d'appel;
- Saturation du récepteur MS et dégradation de son rapport signal sur bruit SNR;
- Brouillage par blindage électromagnétique.

La figure 2.3, montre des exemples de stratégies du brouillage.

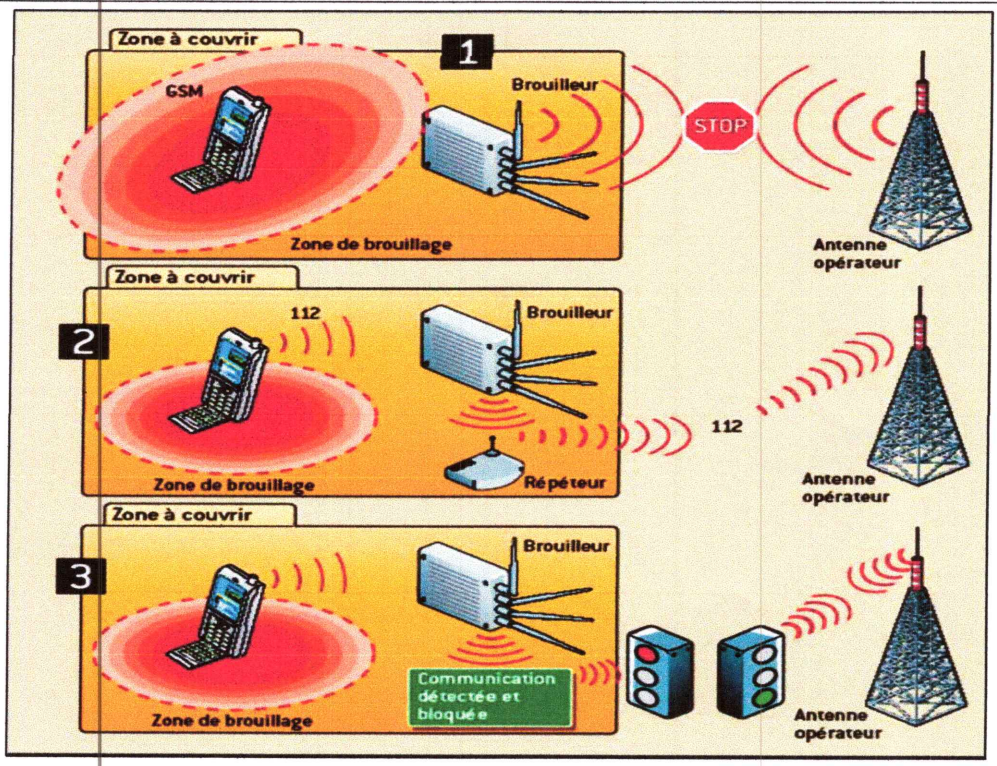


Figure 2.3 : Fonction du brouilleur.

4.1. Brouilleur Type A: Pollueur

Ce type de brouilleur sature le téléphone cellulaire avec un signal plus fort que le signal GSM. Le dispositif équipé de plusieurs oscillateurs indépendant pour la transmission de signaux de brouillage est capable de bloquer les fréquences utilisées par les canaux de contrôle de téléphonie mobile.

Quand il est actif dans une zone désignée, un tel dispositif va empêcher (au moyen d'interférences radiofréquences) tous les téléphones mobiles situés dans cette zone de recevoir et de transmettre des appels.

Ce type de dispositif ne transmet qu'un seul signal de brouillage et a une très faible sélectivité de fréquence, ce qui conduit à une interférence avec une large bande de spectre de communication qui a été à l'origine destiné à cibler

4.2 Type B: Inhibiteurs cellulaires intelligents

Le dispositif inhibiteur cellulaire intelligent (Intelligent Cellular Disabler) ne transmet pas des signaux d'interférences sur les canaux de commande. Il fonctionne essentiellement comme un détecteur, capable de communiquer avec la station cellulaire de base BTS. Lorsque l'appareil détecte la présence d'un téléphone mobile dans la région «silencieuse» (1), il signale aux BTS que l'utilisateur cible est dans une région silencieuse (2). Par conséquent, un filtrage est effectué par le logiciel d'autorisation d'établissement d'appel au sein de la station. Les

messages peuvent être acheminés vers la boîte vocale de messagerie de l'utilisateur, si ce dernier est abonné à un service de messagerie vocale (3).

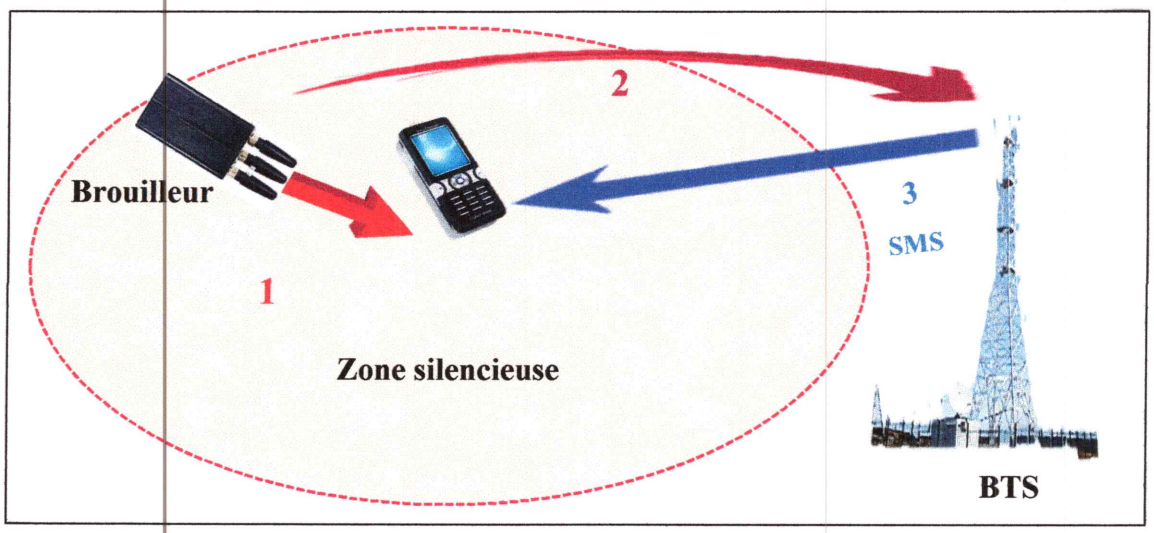


Figure 2.4 : Inhibiteurs cellulaires intelligents.

Ce processus de détection et l'interruption de l'établissement d'appel est fait pendant l'intervalle normalement réservée à la signalisation et de prise de contact. Pour les communications d'urgence, le dispositif de détection intelligente prévoit des dispositions pour les utilisateurs qui ont le statut d'urgence. Ces utilisateurs doivent être préinscrits chez les fournisseurs de services. Quand un appel urgent arrive, le détecteur reconnaît le numéro et l'appel est établi pour une durée maximale spécifiée.

4.3. Type C : Inhibiteur balise Intelligent

Contrairement au brouilleurs, le dispositif de type "C" ne transmet pas un signal d'interférence sur les canaux de contrôles. Lorsque le dispositif est situé dans une zone désignée silencieuse, il fonctionne comme une balise et tout terminal compatible est chargé de désactiver son propre fonctionnement. Cette technologie ne provoque aucune interférence et ne nécessite aucune modification des systèmes cellulaires existants.

Cette technologie nécessite des téléphones intelligents dotés de récepteurs séparés pour le système de balise Type C. Donc, l'inhibiteur balise ne saura pas empêcher le fonctionnement normal des terminaux incompatibles au sein d'une zone silencieuse. Ainsi l'implémentation efficace de cette méthode de brouillage sera problématique pour de nombreuses années encore [8].

4.4 Type "D" : Brouilleur Récepteur/Emetteur

Ce type de brouilleur se comporte comme une petite station de base mobile. Indépendante qui interagit et communique directement avec le téléphone mobile local. Le

brouilleur est initialement en mode de réception (1) et va intelligemment choisir d'interagir et de bloquer le téléphone mobile qui se trouve à sa proximité (2). Cette technique pourrait être appliquée sans la coopération des fournisseurs de services cellulaires.

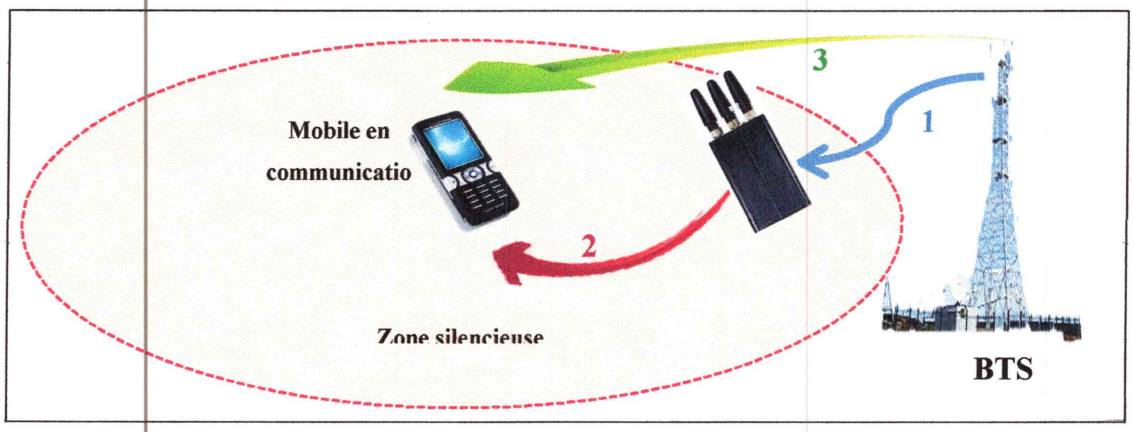


Figure 2.5 : Brouilleur Récepteur/Emetteur.

Cette technique de brouillage sélectif utilise un récepteur discriminant pour cibler l'émission de signal de brouillage. L'avantage d'une telle sélectivité de ciblage est de diminuer la pollution électromagnétique. Le signal de brouillage ne serait actif que durant la période de communication entre le mobile et la station de base (3). Comme pour le type B, ce type de dispositif pourrait discriminer et permettre les communications vers les numéros d'urgence [8].

4.5. Type E : Brouillage passif par blindage électromagnétique

Cette méthode utilise les techniques de suppression **EMI** (**E**lectro-**M**agnetic **I**nterference) par blindage électromagnétique en créant une zone de type cage de Faraday, de façon que n'importe quel dispositif à l'intérieur de cette cage ne peut transmettre ou recevoir des signaux RF provenant de l'extérieur de la cage.

Figure 2.6 : Cage de faraday.

Avec les progrès actuels dans les techniques de blindage EMI, il serait concevable d'implémenter la technique de brouillage passif par blindage électromagnétique dans

l'architecture des bâtiments conçus pour créer des zones silencieuse. Les appels d'urgence seront bloquées à moins qu'il y ait un moyen de les recevoir, les faire passer par coaxial, puis les réémettre dans la zone silencieuse [8].

Le tableau ci-dessous donne une comparaison entre ces techniques de brouillage :

Type	Appel d'urgence	Efficacité	Approbation de régularité	Implémentation
"A"	Bloqué	Faible	Interdis	Très simple
"B"	Permis	Moyenne	Requis	Complexe (requis la troisième partie cellulaire)
"C"	Permis	Élevé	Requis	Complexe (nécessaire le Handset intelligente)
"D"	Permis	Moyenne	Requis	Simple
"E"	Bloqué	Élevé (aucun signal transmis)	Permis	Simple

Tableau 2.2 : Comparaisons entre les différentes techniques de brouillage.

5. Conclusion

Dans ce chapitre nous avons d'abord exposé un résumé sur le brouillage de téléphonie mobile son utilité, et son principe de fonctionnement.

Nous avons, par suite, effectuer une étude détaillée des différentes techniques de brouillage de téléphonie mobile GSM.

✓ Références bibliographiques

[1] « Guerre électronique », http://fr.wikipedia.org/wiki/Guerre_%C3%A9lectronique (consulté le 19 mai 2015).

[2] P. Vaillant, « Les principes du radar », http://www.radartutorial.eu/16.eccm/ja05.fr.html.

[3] A. Jisrawi, « GSM 900 Mobile Jammer », Projet fin d'Etude, Université de Jordan 2006.

[4] M. King, « Conception et simulation d'un brouilleur GSM », Ecole Nationale Supérieure Polytechnique, 2010.

[5] «Brouilleur GSM portable», https://brouilleurgsm.wordpress.com/2012/08/15/brouilleur-gsm/ , (consulté le 3 mai 2015).

[6] T.M. Saad, « Détecteur et brouilleur de téléphones mobiles », Mémoire fin d'Etude Institut des Sciences Appliquées et Economique, Liban, 2011.

[7] H.T. Eyyuboglu, « Mobile phone jammer design », Mémoire fin d'Etude, Université de Çankaya, 2013.

[8] Mobile & Personal Communications Committee of the Radio Advisory Board of Canada, « Use of jammer and disabler Devices for blocking PCS, Cellular & Related Services »: http://www.rabc.ottawa.on.ca/e/Files/01pub3.pdf.

Chapitre 3

Etude et conception du brouilleur GSM

Chapitre 3

Etude et conception du brouilleur GSM

1. Introduction

Ce chapitre est consacré à l'étude de la structure ainsi que le principe de fonctionnement des différentes parties d'un système de brouillage typique pour téléphonie mobile. Notre étude et conception du brouilleur GSM est divisée en deux parties.

Dans la première partie on étudiera les étages basses fréquences (FI : Fréquences Intermédiaires) du brouilleur, utilisant le simulateur des circuits électroniques ISIS Proteus de la firme Labcenter Electronics. La deuxième partie, sera réservée à l'étude détaillée de la partie FR (Fréquences Radio) du brouilleur utilisant le simulateur ADS (Advanced Design System) de la firme Agilent, qui est destiné pour la simulation et la conception des systèmes FR et micro-ondes. Les résultats obtenus sous forme de courbes, simulations et réalisations sont présentés et discutés.

2. Schéma bloc d'un brouilleur mobile GSM

Le brouilleur du type "A", qu'on se propose d'étudier dans ce mémoire est constitué de quatre parties principales, comme il est illustré par la figure 3.1:

- Le circuit d'alimentation ;
- La partie **FI** qui assure la production du signal de commande;
- La partie **FR** qui génère le signal de brouillage;
- Une antenne qui permet la diffusion du signal du brouilleur.

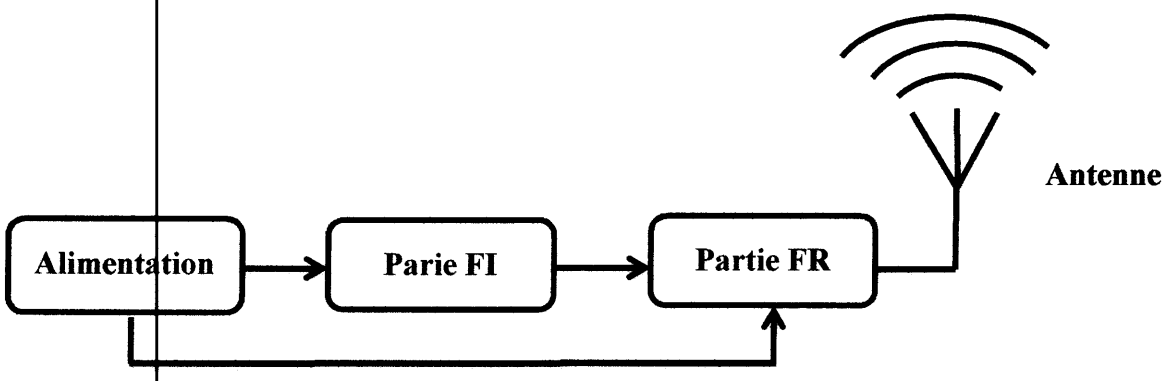


Figure 3.1 : Schéma synoptique typique d'un brouilleur de téléphones mobiles.

3. Etage d'alimentation

Cette partie sert à délivrer les tensions continues nécessaires pour alimenter les autres sections du brouilleur.

4. Partie de commande FI (Fréquences Intermédiaire)

Aussi nommée la partie BF (Basse Fréquence), elle permet de produire un signal de commande (tuning) de l'oscillateur commandé en tension VCO de la partie FR. Ce signal est en effet, obtenu par le mélange d'un signal triangulaire et un signal de bruit. Cette partie comporte trois étages principaux (figure 3.2) :

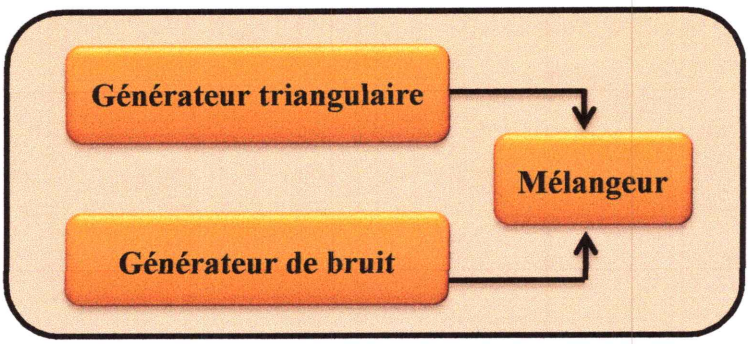


Figure 3.2 : Schéma synoptique de la partie FI.

4.1. Générateur du signal triangulaire

L'utilisation principale du signal triangulaire est la commande du VCO pour permettre le balayage de la bande de fréquence de signal GSM à brouiller. Le circuit de génération du signal de balayage est basé sur le circuit intégré NE555 fonctionnant dans le mode astable (figure 3.3).

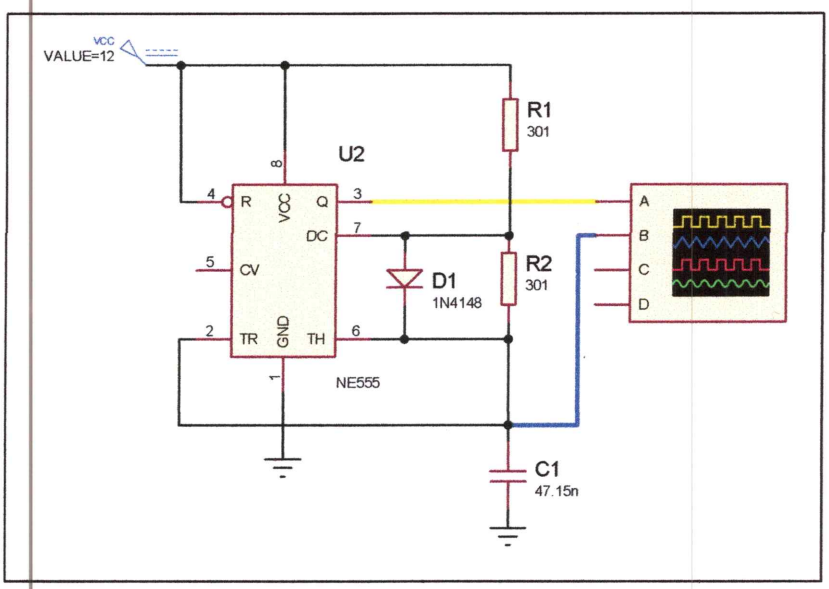


Figure 3.3 : Circuit astable pour générer le signal triangulaire dans le simulateur ISIS.

La configuration astable permet d'utiliser le NE555 comme oscillateur. Deux résistances R_1 et R_2 et un condensateur C_1 permettent de modifier la fréquence d'oscillations ainsi que le rapport cyclique. L'arrangement des composants est tel que présenté par le circuit de la figure 3.3. Une oscillation complète est effectuée lorsque le condensateur C_1 se charge jusqu'à 2/3 de Vcc et se décharge à 1/3 de Vcc (figure 3.4). Lors de la charge, les résistances R_1 et R_2 sont en série avec le condesateur, mais la décharge s'effectue à travers R_2 seulement.

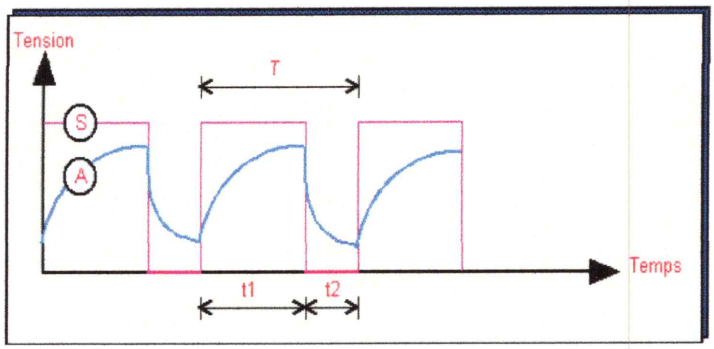


Figure 3.4 : Temps de charge et de décharge du condensateur.

Le temps de charge du condensateur peut être calculé par l'expression suivante :

$$T_C = 693 \times (R_1 + R_2) \times C_1 \quad (3.1)$$

Le temps de décharge, est donné par :

$$T_D = 693 \times R_2 \times C_1 \quad (3.2)$$

La fréquence de sortie, est calculée utilisant l'expression 3.3 :

$$f_{osc} = \frac{1.44}{(R_1+R_2)\times C_1} \quad (3.3)$$

On prend $R_1 = R_2$ et une diode à travers R_2 pour obtenir un cycle de service de 50 %, ce qui signifie que le temps nécessaire pour la charge est égal au temps de décharge.

Sur la figure 3.5, on montre les résultats de la simulation du circuit de la figure 3.3. La sortie 3 du NE555 donne le un signal rectangulaire de l'astable ; tandis que la sortie 2 (6) fournie le signal triangulaire de charge-décharge du condensateur. Pour notre circuit, nous avons utilisé un condensateur C_1=46.15 µF et deux résistance R_1=R_2=301Ω, pour obtenir des temps de charge et de décharge égaux. La fréquence du signal de sortie vaut :

$$f_{osc} = \frac{1.44}{(301+301)\times 46.15\times 10^{-9}} = 51.83 \text{ KHz} \quad (3.4)$$

$$\text{soit } T_{osc} = \frac{1}{F_{osc}} = \frac{1}{51.83\times 10^3} = 0.19\ us. \quad (3.5)$$

Nous avons choisi cette valeur de fréquence d'oscillation relativement au temps de

garde T_G du GSM qui est de l'ordre de 30.5µs (correspondant à 8.25 bits soit $T_{osc} < T_G$).

Pour une source d'alimentation de tension 12V (cc), l'amplitude du signal de sortie varie entre 4V pour (Vcc/3) et 8V pour (2Vcc/3).

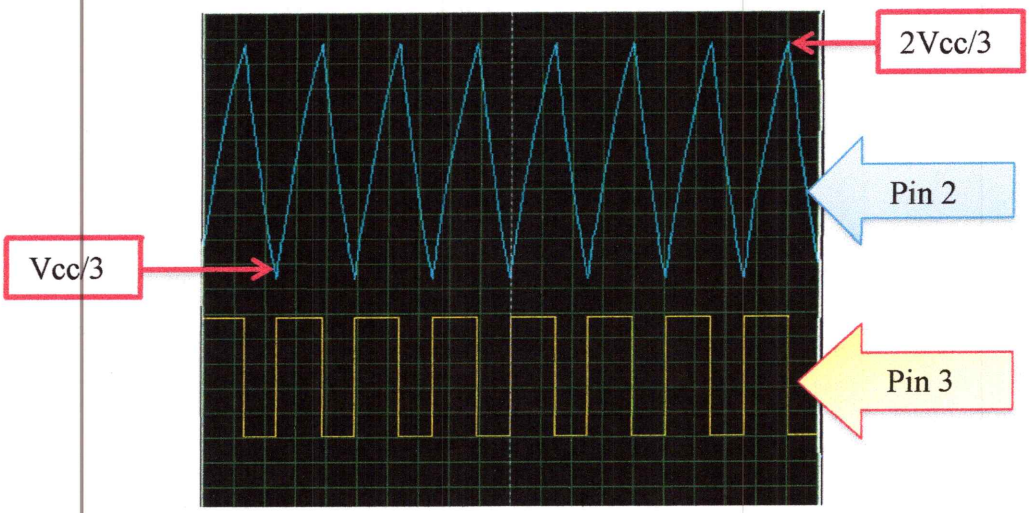


Figure 3.5 : Signaux du générateur d'onde triangulaire sous ISIS.

La Photographie de la figure 3.6 montre le circuit astable que nous avons réalisé. Les signaux de sorties visualisés sur oscilloscope numérique sont présentés par figure 3.7.

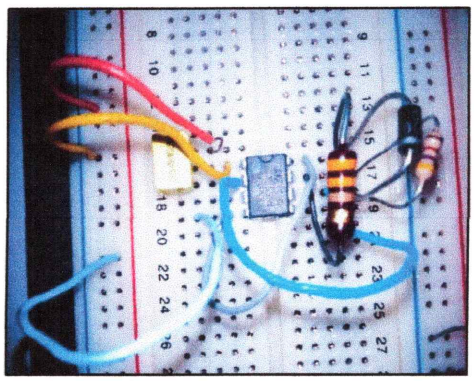


Figure 3.6 : Circuit générateur du signal triangulaire.

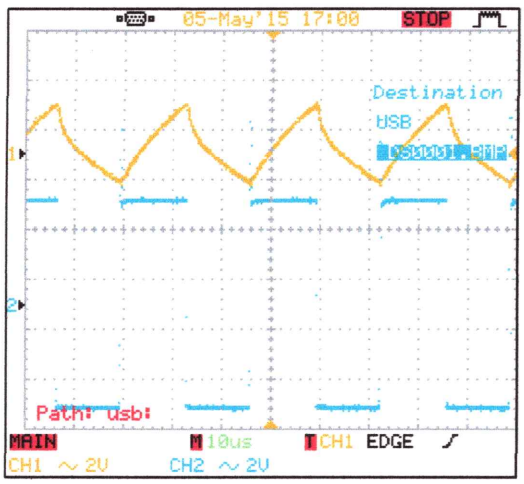


Figure 3.7 : Signaux de sorties de l'astable visualisés sur oscilloscope.

4.2. Générateur de signal bruit

C'est un générateur qui permet de produire un signal bruit qui sera mélangé au signal triangulaire à la sortie de la partie FI. Sans ce bruit, le signal de brouillage n'est qu'une oscillation qui ne peut pas interférer la communication de téléphonie mobile.

Le circuit présenté par la figure 3.8 représente un générateur de bruit typique.

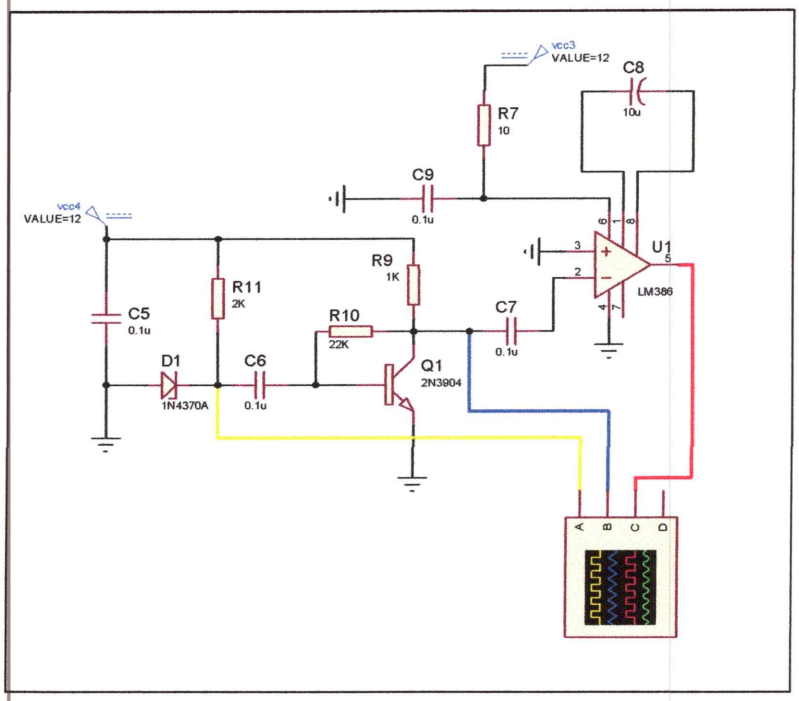


Figure 3.8 : Circuit de génération de bruit sous ISIS.

Le générateur de bruit est constitué de deux parties :

- Le circuit de génération de bruit à base d'un transistor NPN monté en émetteur commun et d'une diode Zener polarisée en inverse afin de provoquer ce qu'on appelle "l'effet d'avalanche" qui permet d'obtenir un bruit large bande. Ce bruit a pour origine les phénomènes d'avalanche dans la jonction PN polarisée en inverse où les porteurs peuvent acquérir une énergie suffisante pour créer aléatoirement des paires électron-trou par collisions. Ce bruit, caractéristique de l'effet Zener, est toujours associé à un courant de polarisation. Il est difficilement prévisible [3].
- Le circuit d'amplification du bruit, à base de l'amplificateur audio le LM386. Ce circuit intégré conçu pour réaliser avec très peu de composants extérieurs un amplificateur de petite puissance (0.5 W), peut être alimenté par une simple pile de 12V. C'est donc le composant de base idéal pour construire un mini-amplificateur. Le brochage du circuit LM386 est représenté dans la figure 3.9.

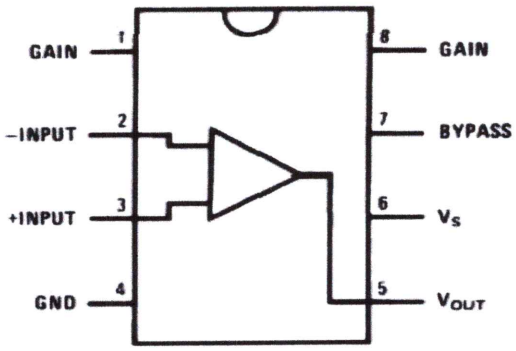


Figure 3.9 : Brochage de l'amplificateur audio LM386.

Pour obtenir un gain de l'amplification de 20 (26 dB), On ne raccord rien aux broches 1 et 8 (en air). Tandis que, pour obtenir un gain de 20 à 200 (26 dB à 46 dB), un condensateur et une résistance doivent être raccordé entre broches 1 et 8. Par contre pour obtenir un gain de 200 (46dB), le condensateur est raccordé seul entre les broches 1 et 8 [4].

Afin d'illustrer le fonctionnement de notre générateur de bruit, nous avons simulé le circuit de la figure 3.9 en remplaçant la diode Zener (source de bruit) par une source sinusoïdale. Nous avons procédé ainsi, parce que nous avons constaté que le simulateur ISIS ne prend pas en considération le phénomène d'avalanche dans la diode, donc, il ne peut pas générer le signal bruit désiré. Les résultats de cette simulation sont montrés sur la figure 3.10.

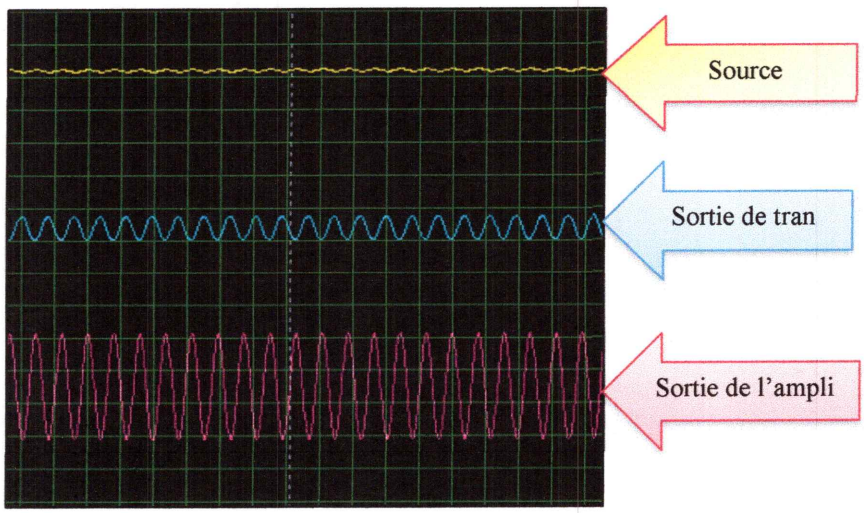


Figure 3.10 : Simulation du signal bruit sous ISIS.

- La source a une amplitude de 0.25 mV.
- L'amplitude du signal à la sortie de transistor est de 25 mV. Soit un gain d'amplification du premier étage égal à: 100
- La sortie de l'amplificateur a une amplitude de 4V. Soit un gain d'amplification du second étage égal à: 160.

La photographie du circuit générateur de bruit est donnée par la figure 3.11.

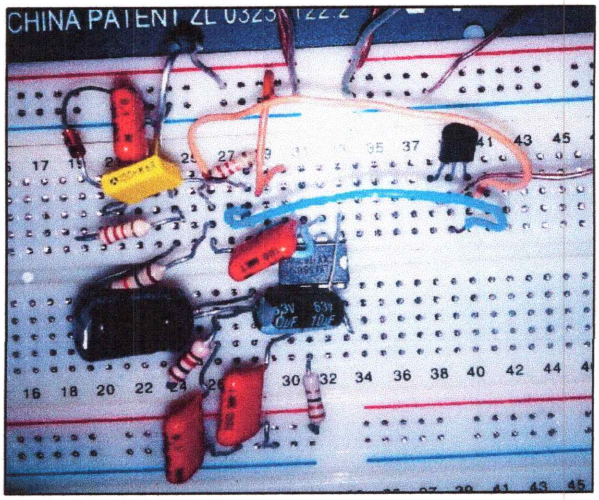


Figure 3.11 : Circuit de génération du bruit.

4.3. Mélangeur

C'est un dispositif non linéaire qui permet d'effectuer le mélange du signal triangulaire avec le signal bruit afin d'obtenir le signal tuning. Un circuit de mélange typique et simple peut être obtenu utilisant un amplificateur opérationnel monté en additionneur, comme il est illustré par la figure 3.12.

La tension de sortie s'exprime en fonction des tension d'entrées par :

$$V_{out} = \left(-\frac{R}{R_1}\right)V_1 + \left(-\frac{R}{R_2}\right)V_2 \qquad (3.6)$$

Soit : $V_{out} = -(V_1 + 2V_2)$ (3.7)

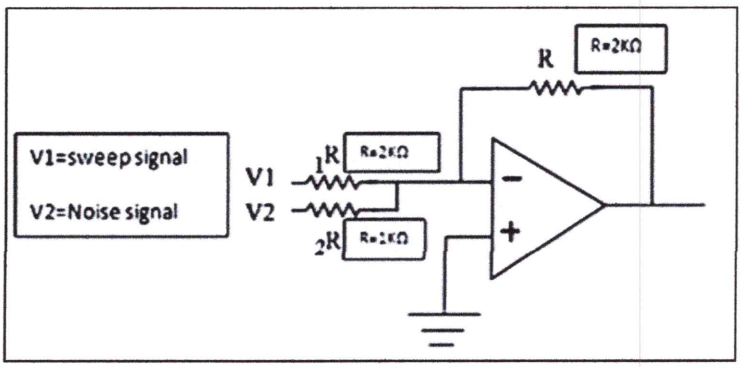


Figure 3.12 : Circuit mélangeur.

Dans notre projet on utilise l'amplificateur opérationnel **LM741**. Le brochage de ce circuit intégré est donné par la figure 3.13.

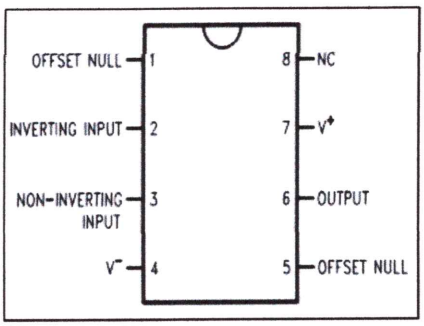


Figure 3.13 : Brochage de l'amplificateur opérationnel LM741.

Les figures 3.14 et 3.15 montrent un exemple de simulation du mélangeur sous ISIS avec deux sources sinusoïdales. La première source V_1 a une amplitude de 100mV et une fréquence de 1KHz. La seconde source V_2 a une amplitude de 1mV, et une fréquence de 100KHz.

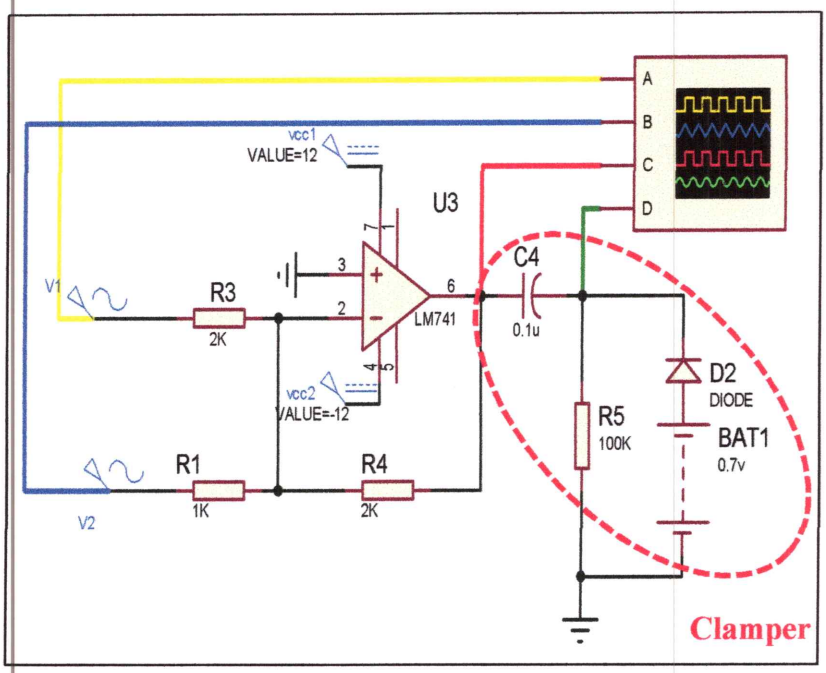


Figure 3.14 : Circuit du mélangeur sous ISIS.

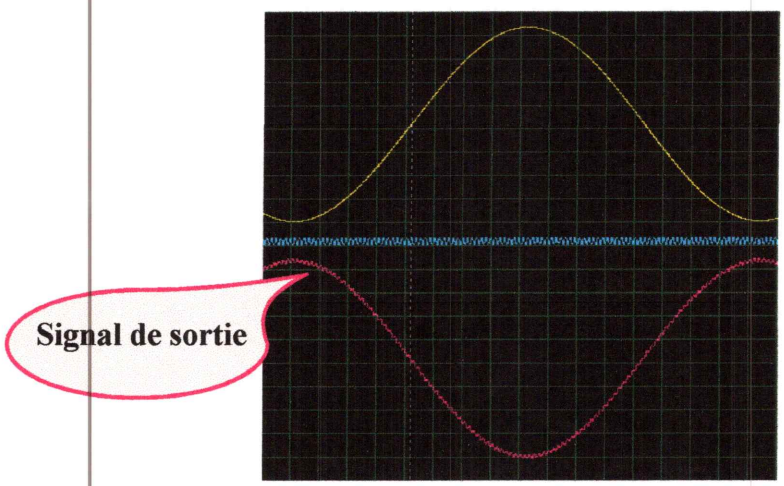


Figure 3.15 : Signaux d'entrées et de sortie du mélangeur sous ISIS.

4.4. Clamper : circuit de décalage

L'entrée du VCO doit être délimitée de 0 à 3,5 V pour obtenir la gamme de fréquences nécessaire. Et puisque notre signal est centré à l'origine, nous devons ajouter un élément de décalage pour atteindre notre objectif. Le dispositif de décalage se compose d'un condensateur connecté en série avec une résistance et une diode, comme le montre la figure 3.16.

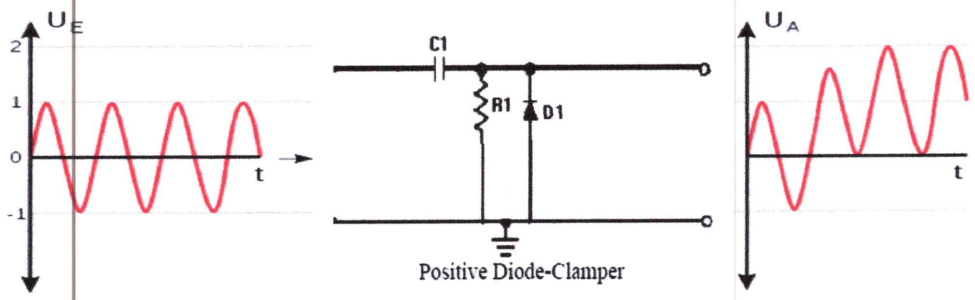


Figure 3.16 : Circuit du clamper.

Le signal de sortie du clamper est représenté dans la figure 3.17.

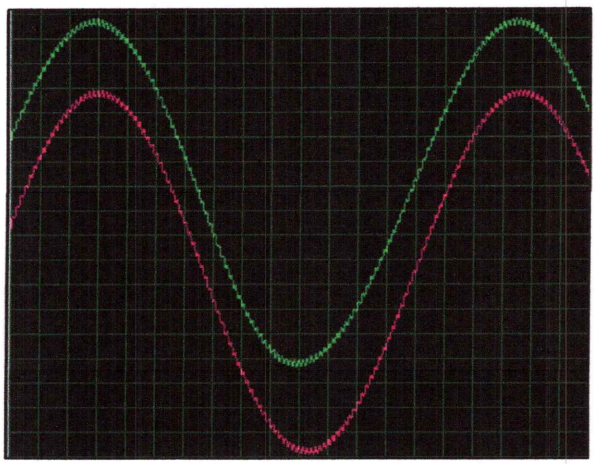


Figure 3.17 : Signal à la sortie du clamper sous ISIS.

- **Schéma global de la partie FI**

Après simulation et garantie le bon fonctionnement de chaque bloc du circuit séparément, nous avons simulé l'ensemble de la partie FI pour avoir le signal de commande (signal tuning) de l'oscillateur VCO (figures 3.18 et 3.19).

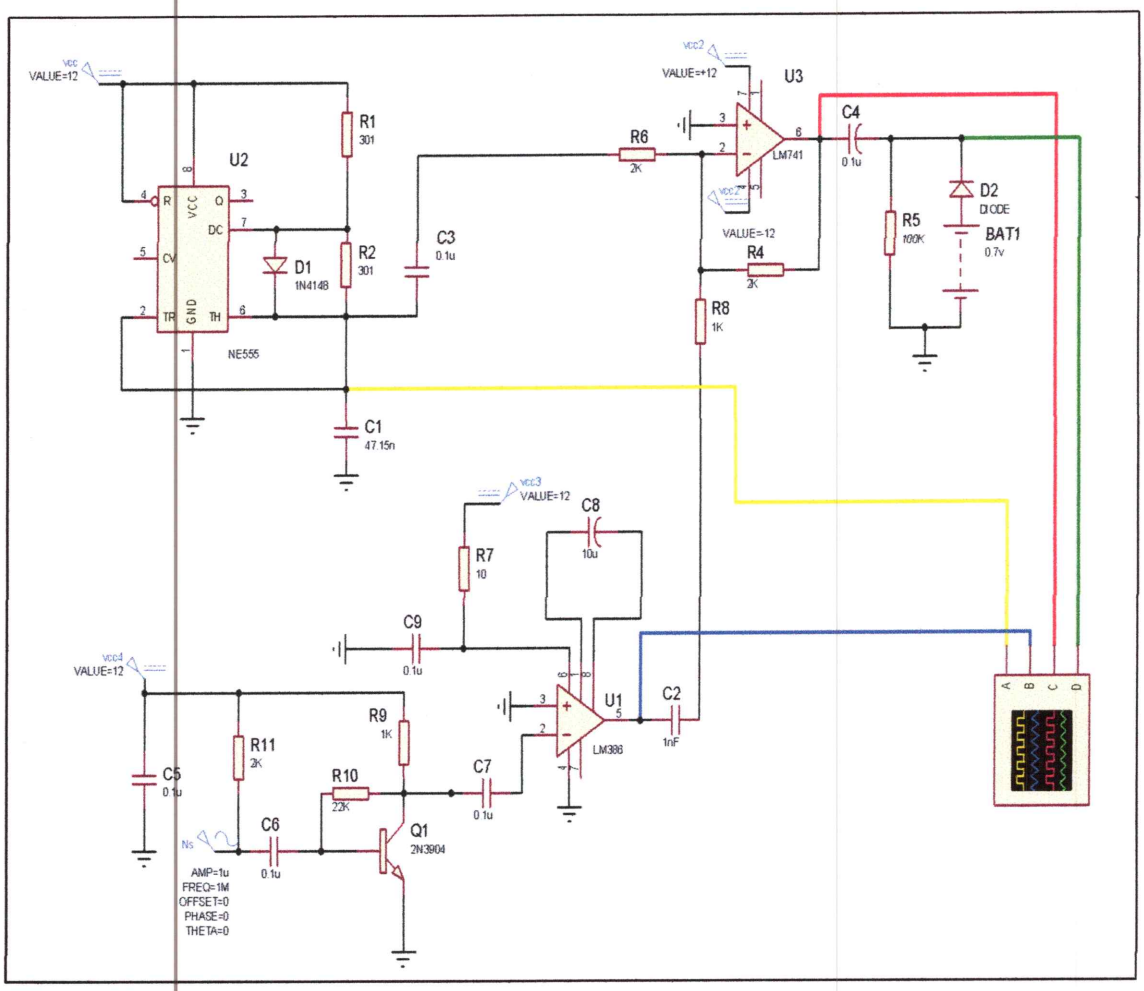
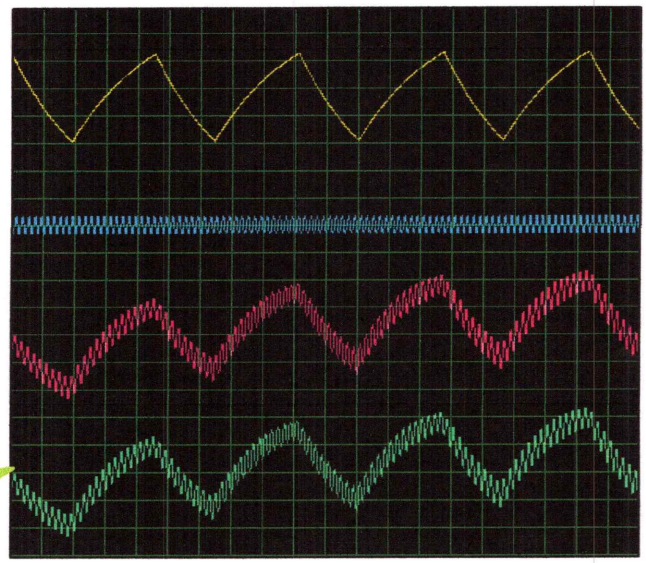


Figure 3.18 : Simulation du circuit de la partie FI sous ISIS.



Signal de sortie

Figure 3.19 : Signaux générer par la partie FI.

5. Etude de la partie des Fréquences Radio (FR)

C'est la partie la plus importante dans notre système. Il permet de générer le signal de brouillage qui va interférer avec le signal GSM au niveau du mobile. Cette partie comprend trois étages (figure 3.20) :

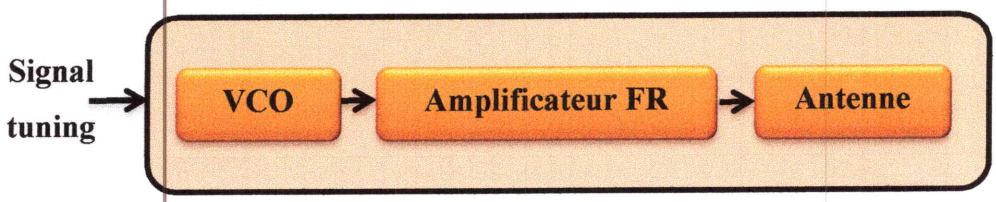


Figure 3.20 : Schéma synoptique de la partie FR.

- **Oscillateur commandé en tension VCO**

Le VCO est un oscillateur dont la fréquence de résonnance varie en fonction d'une tension d'entrée de commande

- **Amplificateur de puissance**

L'amplificateur de puissance est l'élément actif clé d'un système de communication (station de base, téléphones mobiles, satellites...), car c'est le principal consommateur d'énergie. Son rôle est d'amplifier le signal micro-onde issu du VCO.

- **L'antenne**

Une antenne appropriée est nécessaire pour transmettre le signal de brouillage. Afin d'avoir un transfert de puissance optimal, le système d'antenne doit être adapté au système de transmission.

5.1. Bilan de puissance de la liaison du brouillage [1]

Le paramètre à considérer pour le calcul du bilan de puissance du brouillage dans une région particulière est le rapport signal sur bruit SNR $= \frac{S}{N}$. Pour assurer le brouillage d'un récepteur mobile, on a besoin de réduire son SNR, de façon à ce que le signal GSM ne soit plus intelligible. Pour cela, on considère le cas le plus problématique du point de vue brouillage :

On sait que la station BTS transmit une puissance maximale de -47 dBm, et avec la valeur minimale de la " handling capability " d'un dispositif mobile est de 23dBm. Donc, la puissance du brouilleur au niveau du mobile doit être :

$$S_{max} = -47\text{dBm} + 23\text{dBm} = -24dBm \qquad (3.8)$$

Donc pour que le brouillage soit efficace, le signal de brouilleur doit avoir une puissance maximale au niveau du mobile égale à S_{max}.

D'autre part le signal rayonné de notre brouilleur doit subir une atténuation depuis sa transmission de l'antenne jusqu'à son arrivée à l'antenne du mobile. Les pertes de puissance le long de ce trajet peuvent être calculées utilisant l'expression (2.1) du *FSL*. Par exemple pour la bande Downlink du GSM 900 la fréquence centrale est $f = 947.5$MHz, et pour une surface de recouvrement d'un rayon de 20m, on obtient des pertes en puissance d'une valeur égale à 58 dB.

Donc, en tenant compte de la puissance perdue durant le trajet, on a besoin de transmettre un signal de puissance telle que: $S_0 = -24 + 58 = 34$ dBm. Où S_0 désigne la puissance transmise par le brouilleur.

Si par exemple, la puissance de sortie du VCO est de 10 dBm (S_{VCO}), donc elle doit être amplifiée de : $S_0 - S_{VCO} = 34 - 10 = 24$ dBm, pour réaliser le brouillage. Donc, l'étage d'amplification de puissance utilisé doit être capable d'élever la puissance à la sortie du VCO au-delà de 28 dBm (au-delà -24 dBm au niveau du mobile). La figure 3.21 illustre les puissances mise en jeu dans cette liaison.

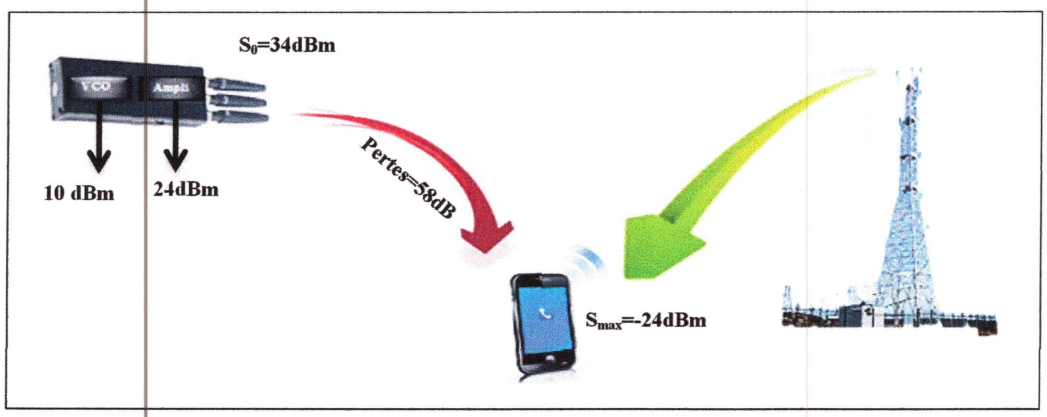


Figure 3.21 : Bilan de puissance d'une liaison de brouillage.

5.2. L'oscillateur commandé en tension (VCO)

L'oscillateur commandé en tension (VCO) est le cœur de la partie FR. Il est le dispositif qui génère le signal FR qui va interférer avec le signal de téléphonie mobile. La caractéristique principale d'un oscillateur commandé en tension est que la fréquence du signal de sortie est linéairement proportionnelle à la tension d'entrée, par conséquent, on peut contrôler la fréquence de sortie en changeant la tension d'entrée. Lorsque la tension d'entrée est continue, la sortie est à une fréquence spécifique, tandis que si l'entrée est d'une forme d'onde triangulaire la sortie couvre une gamme de fréquences spécifique.

Nous allons exposer, dans ce qui va suivre, l'étude d'un circuit VCO typique destiné pour les applications de téléphonie mobile. Cette étude est basée sur l'utilisation du simulateur ADS de la firme "**Agilent Technologies**". Ce logiciel dédié à la simulation et à la conception des circuits et des systèmes électroniques FR, offre tout un ensemble d'environnements de simulation de types circuit et électromagnétique, dans les domaines temporel et fréquentiel.

La conception de l'oscillateur commandé en tension s'effectue en 3 étapes :

a. Etude de la chaîne de contre réaction : Le circuit résonateur.
b. Etude de la chaîne de réaction directe : L'amplificateur à résistance de base.
c. Analyse de l'oscillateur en boucle ouverte et en boucle fermée.

a. Etude de la chaîne de contre réaction : Le circuit résonateur [5]

Le circuit résonateur est un filtre sélectif passif (gain 1), dont le rôle est de fixer la fréquence de résonnance de l'oscillateur. Le composant principal de ce circuit est une diode Varicap qui permet le changement de la fréquence du VCO.

Le circuit résonateur tracé dans ADS est illustré par la figure 3.22.

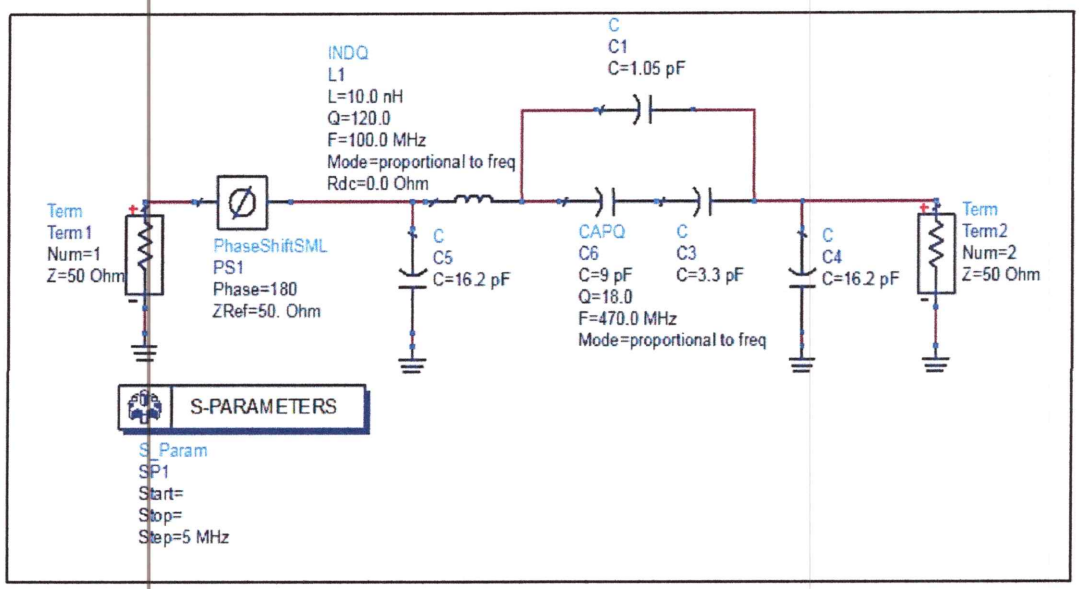


Figure 3.22 : Simulation sous ADS de de la chaîne de contre réaction.

Le coefficient de transmission S_{21} du circuit en module et en phase est représenté sur la figure 3.23.

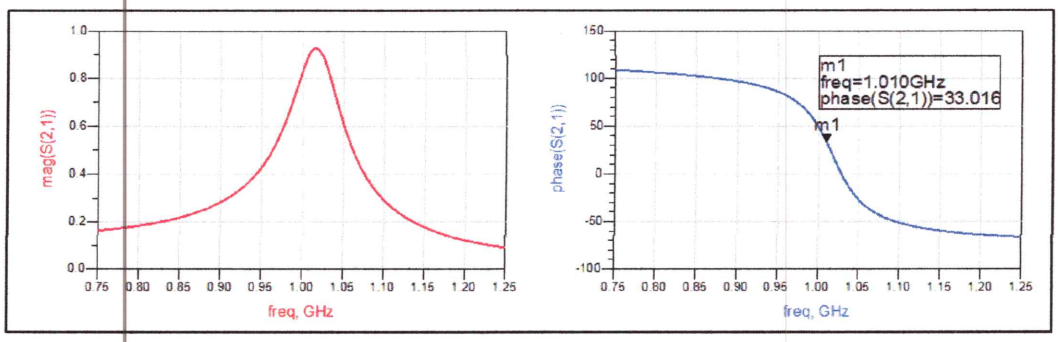


Figure 3.23 : Amplitude et phase du coefficient de transmission S_{21}.

b. Etude de la chaine de réaction directe : l'amplificateur

La chaine de réaction est constituée d'un amplificateur à base d'un transistor bipolaire polarisé par une résistance base-collecteur. Cette configuration est la plus utilisée pour la réalisation des oscillateurs dans le domaine des micro-ondes (figure 3.24).

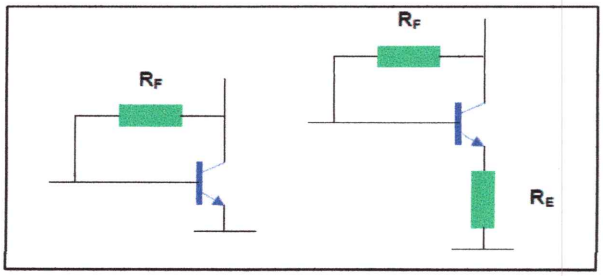


Figure 3.24 : Amplificateur à résistance de base.

Nous avons utilisé pour l'étude de notre amplificateur un transistor bipolaire destiné pour les applications micro-ondes, le AT41486 de la firme Avago Technologies. Les paramètres du transistor sont donnés par le constructeur sous forme d'un fichier S2P dans les conditions de polarisation : V_{ce} =8V et I_c =10mA. Le circuit de la figure 3.24 tracé dans ADS permet d'afficher les paramètres S du transistor (figures 3.25 et 3.26).

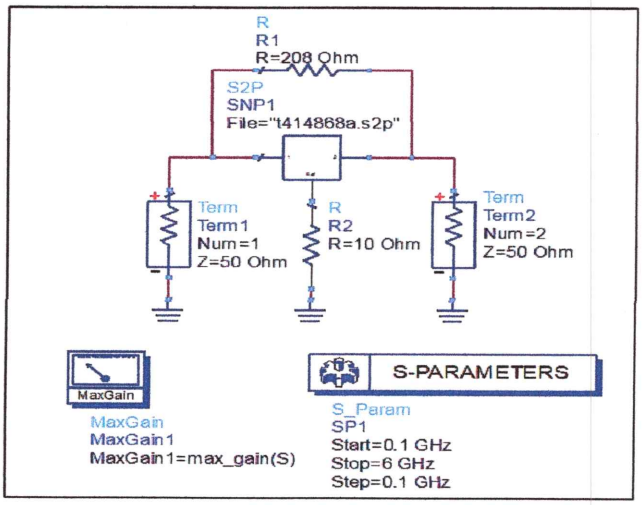


Figure 3.25 : Circuit ADS du transistor AT41486 monté en émetteur commun.

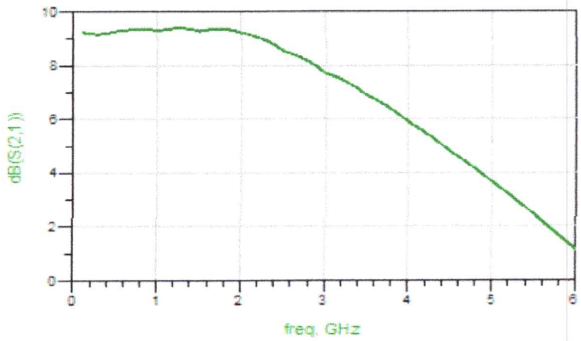


Figure 3.26 : Coefficient de transmission S_{21} du transistor AT41486 en montage émetteur commun et avec résistance de base.

L'amplificateur de réaction a ensuite été simulé en utilisant un modèle du transistor AT41486 et en ajoutant le circuit de polarisation comme le montre la figure 3.27. Les résultats de la simulation sont donnés par la figure 3.28:

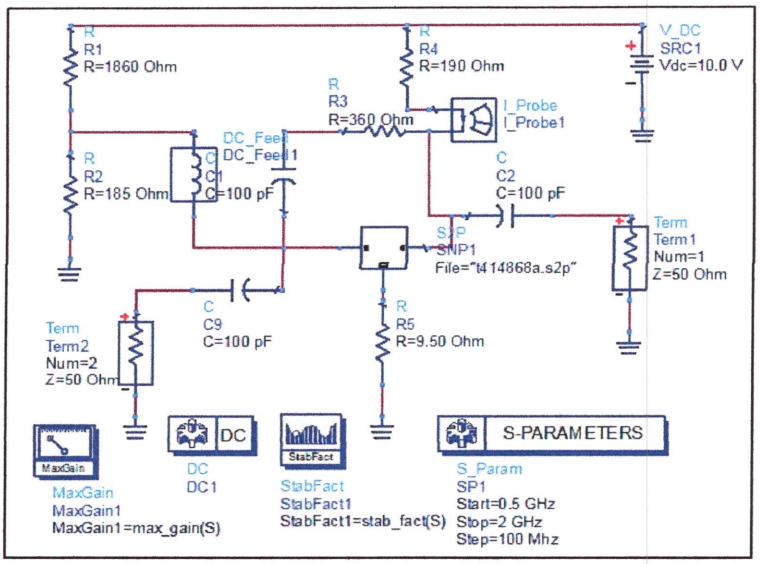


Figure 3.27 : Circuit ADS pour simuler l'amplificateur de la chaîne de réaction.

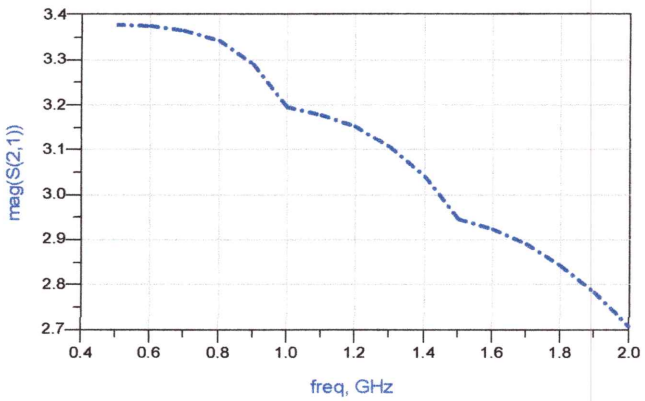


Figure 3.28 : Coefficient de transmission S_{21} de la chaîne de réaction.

c. Analyse de l'oscillateur contrôlé en tension [6]

L'ensemble du circuit amplificateur et le résonateur sont simulé d'abord en boucle ouverte afin de vérifier la fréquence centrale d'oscillation ainsi que la phase totale de la boucle (figure 3.29).

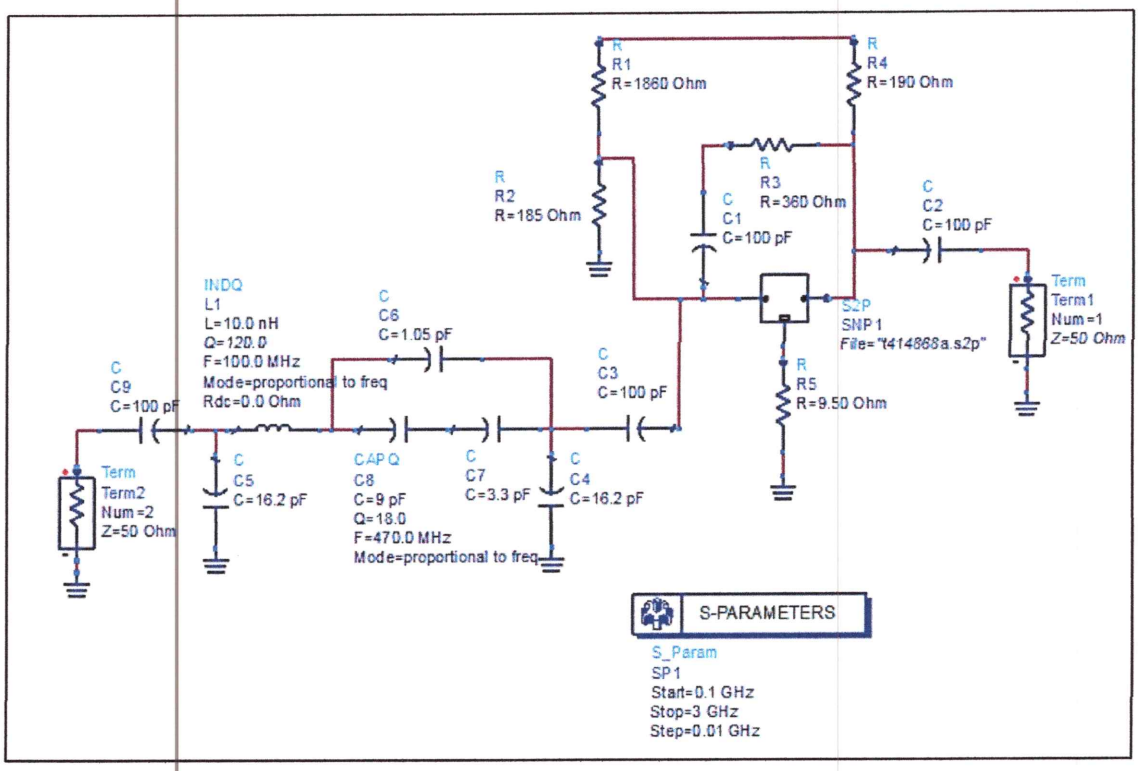


Figure 3.29 : Circuit du VCO en boucle ouverte.

Les résultats de la simulation sont montrés par la figure 3.30. La phase d'insertion est égale à zéro degré avec un gain de 10 dB. Par conséquent, le circuit devrait osciller à 1GHz.

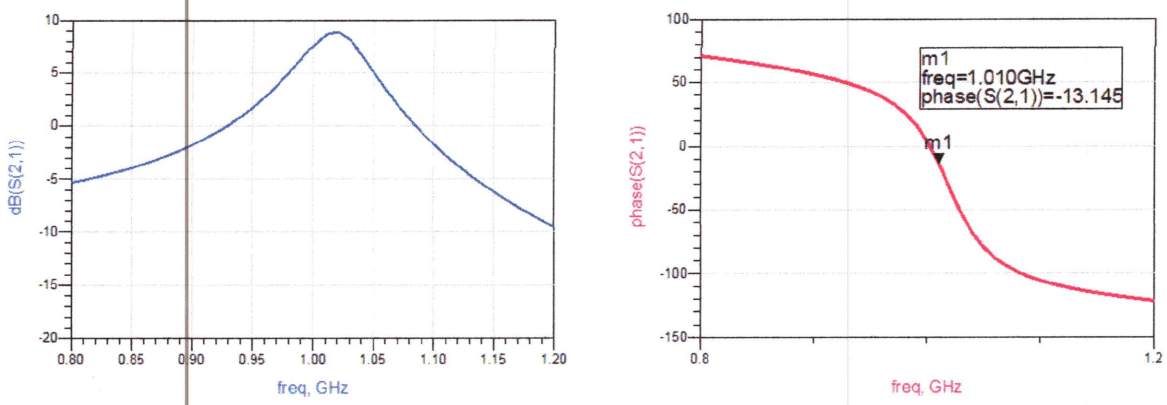


Figure 3.30 : Amplitude et phase du paramètre S_{21} du VCO en boucle ouverte.

L'analyse petit signal en boucle ouverte est utile pour vérifier que le fonctionnement de l'oscillateur est ajusté à la bonne fréquence. Toutefois, en boucle fermée l'amplificateur sera forcé en compression et en conséquence les paramètres micro-ondes du VCO seront altérés.

La réalisation d'une simulation "Harmonique Balance" en boucle fermée, sous ADS, va permettre l'optimisation et l'ajustement de ces différents paramètres. La figure 3.31 montre le circuit de simulation sous ADS de l'oscillateur VCO en boucle fermée.

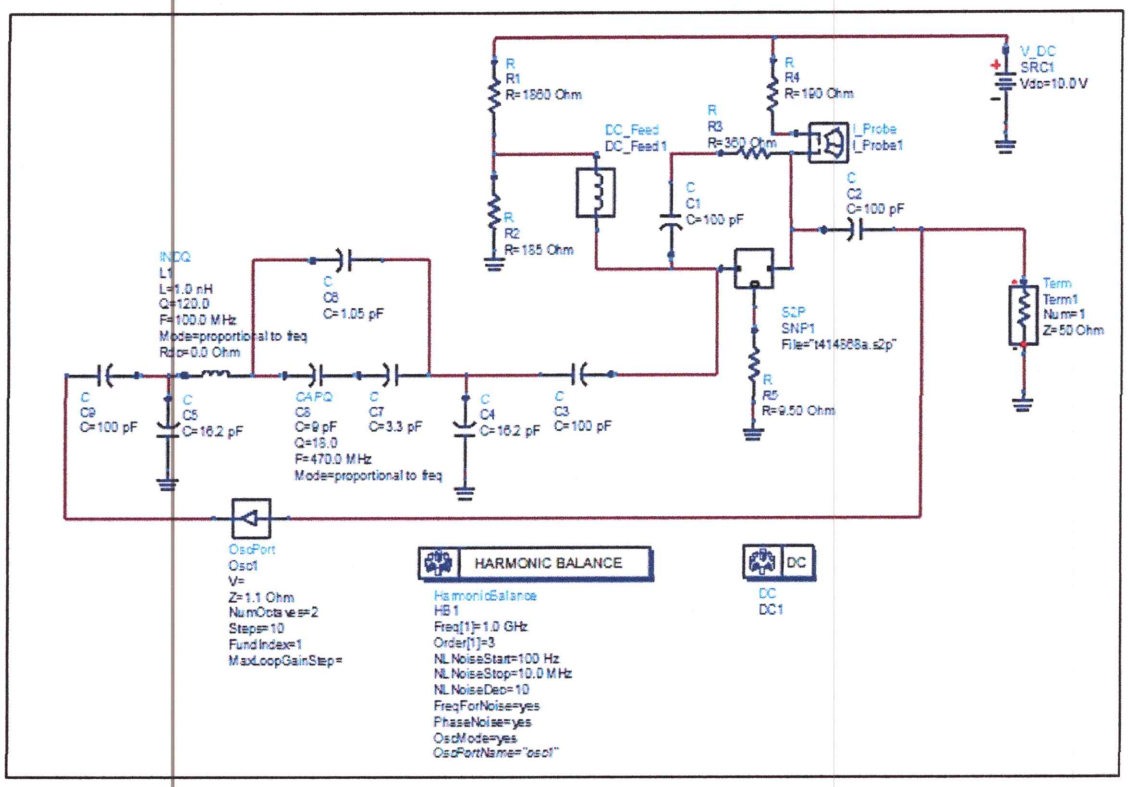


Figure 3.31 : Simulation sous ADS de l'oscillateur VCO en boucle fermée.

Afin de réduire la largeur de bande, le condensateur de couplage en série avec la diode varicap doit être réduit, (il sera nécessaire d'ajuster globalement le condensateur parallèle à la fréquence centrale). Le tableau ci-dessous résume les valeurs de la fréquence du VCO, en fonction de la tension de commande de la varicap :

Tension de commande (V)	Capacité de la Varicap (pf)	Fréquence (MHz)
1	11	985
4	9	1002
10	3	1055

Tableau 3.1 : Fréquence du VCO en fonction de la tension de commande de la varicap.

Le dernier ajustement des éléments du VCO, consiste à réduire les valeurs des condensateurs connecté à la charge de 10pf à 100pf, afin d'optimiser l'adaptation d'impédance et augmenter la puissance de sortie du VCO à une valeur d'environ 10dBm.

Les résultats de simulation du circuit aprés optimisation et ajustement sont montrés sur la figure 3.32.

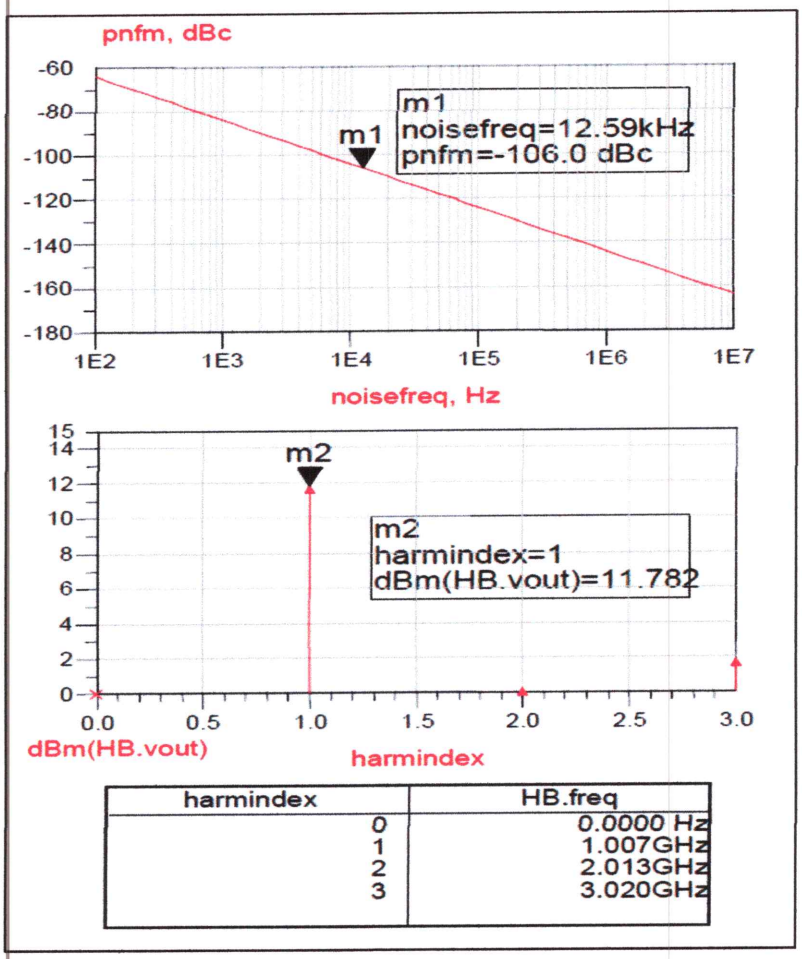


Figure 3.32 : Résultats de la simulation du circuit VCO en boucle fermée. Les condensateurs de couplage sont réduits de 10 pF à 100 pF. Aussi varicap parallèle a été augmenté de 1.7 pF à 1.95 pF.

Le tableau 3.2 résume les paramètres obtenus de la conception de notre oscillateur commandé en tension :

Paramètre	Résultat	Unité
Fréquence centrale	1000	MHz
Largeur de bande passante	62	MHz
Sensibilité	6.8	MHz/V
Puissance	152	mV
Bruit de phase @10 KHz	-106	dBc/Hz
Puissance de sortie	11.78	dBm

Tableau 3.2 : Résumé des paramètres de l'oscillateur VCO.

5.3. Conception et simulation de l'antenne du brouilleur [7]

Dans cette section on va effectuer l'étude et la modélisation électrique de l'antenne du brouilleur GSM sous ADS. C'est une antenne imprimée type patch, opérante dans la bande de fréquence 935-960MHz.

La structure rayonnante montrée par la figure 3.33 est composée de l'antenne patch et d'une ligne de transmission qui assure l'adaptation entre la source et l'antenne.

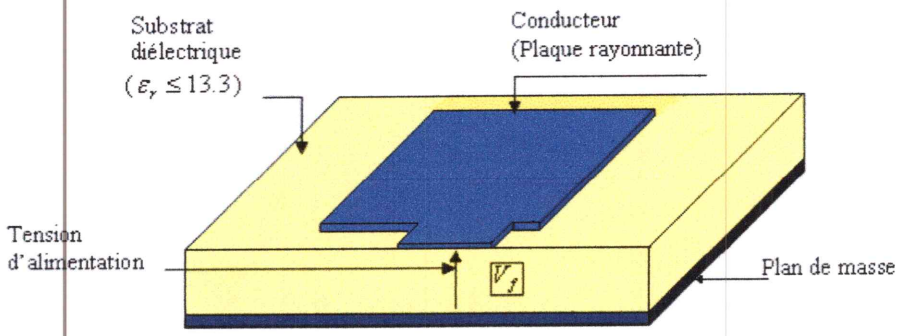


Figure 3.33. Structure de l'antenne patch.

Les matériaux constituants le patch de dimensions (W et L) et le plan de masse sont supposés parfaitement conducteurs et d'épaisseur négligeable.

Le tableau ci-dessous donne les différents paramètres géométriques de la structure d'antenne :

Paramètre	Patch	Ligne quart d'onde
Longueur L (mm)	76	38.71
Largeur W (mm)	97.05	0.155
Epaisseur du substrat H (mm)	1.52	1.52

Tableau 3.3 : Dimension de 'Patch'

Le substrat est constitué d'un diélectrique de type Epoxy très répandu sur le marché pour la réalisation des circuits imprimés micro-ondes. Il est caractérisé par une permittivité relative $\varepsilon_r = 4.32$, une épaisseur H = 1.52 mm et un angle de pertes $\tan\delta = 0.018$.

Le schématique du circuit de l'antenne et donné par la figure 3.34, le coefficient de réflexion à l'entrée de l'antenne permet d'ajuster sa fréquence de résonance et son gain. Nous l'avons représenté sur la figure 3.35.

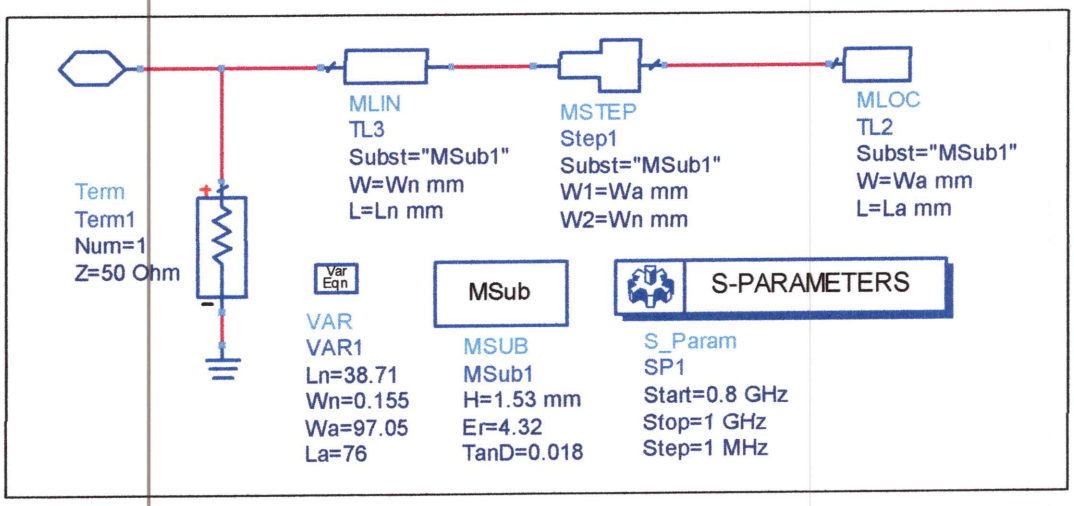


Figure 3.34. Schématique de l'antenne patch.

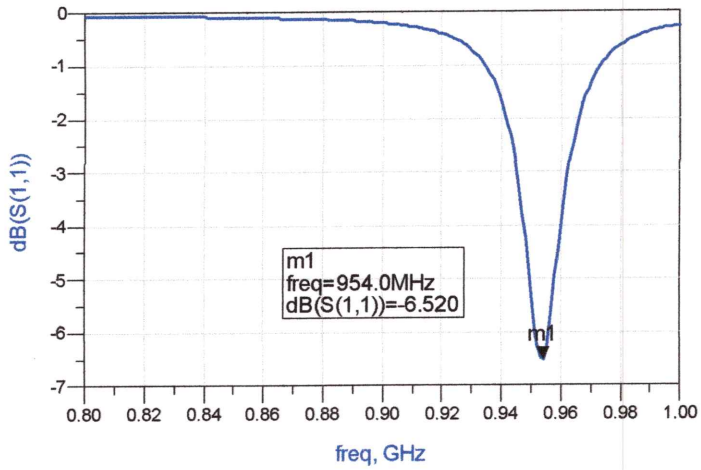


Figure 3.35 : Variation en fonction de la fréquence coefficient de réflexion S_{11} du Patch.

La figure 3.35 montre que l'antenne résonne à une fréquence de 954 MHz avec une valeur minimale de S_{11} égale à -6.52 dB. Ce résultat est inacceptable, puisque la fréquence centrale de notre bande de conception (GSM 935-960MHz) est à 947.5MHz. En outre les pertes par réflexions de l'antenne sont importantes (S_{11} = -6.52dB).

La commande TUNING nous a permis d'ajuster les dimensions de notre patch afin d'atteindre les objectifs de la conception de notre antenne. La procédure d'optimisation de l'antenne est illustrée par la figure 3.36.

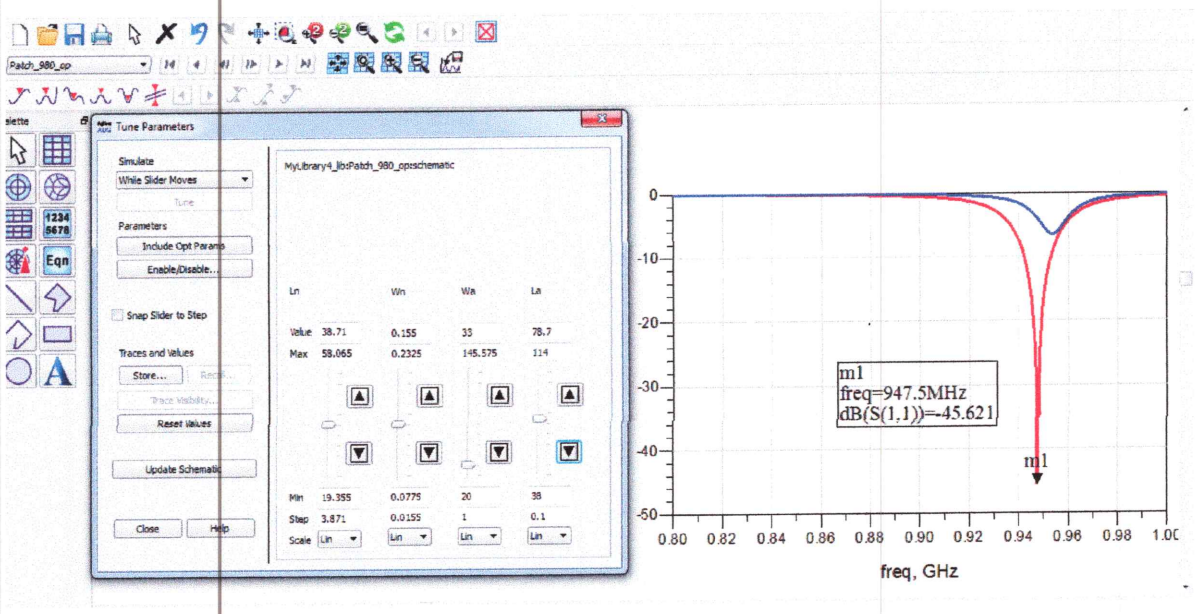


Figure 3.36 : Optimisation des dimensions de l'antenne patch.
(En en bleu avant optimisation – en rouge après optimisation)

Après ajustement des dimensions du patch (W= 33mm et L= 78.8mm), notre antenne résonne maintenant à une fréquence désirée de 947.5 MHz avec une valeur minimale des pertes par réflexions minimale S_{11} = –45.62dB.

6. Conclusion

Dans ce chapitre nous avons effectué une étude détaillée d'un système de brouillage typique pour téléphonie mobile. Ce système est constitué de deux parties principale : La partie basses fréquences (FI : Fréquences Intermédiaires) et la partie FR (Fréquences Radio). Les circuits électriques des différents étages du brouilleur ont été présentés leurs fonctionnements ont été expliqués, et simulés utilisant le simulateur de circuits électroniques ISIS Proteus (partie FI) et le simulateur ADS (partie FR).

Références bibliografiques

[1] T. M. Saad, « Détecteur et brouilleur de téléphones mobiles », Mémoire fin d'Etude Institut des Sciences Appliquées et Economique, Liban, 2011.

[2] A.S. H. Abd -El-Rahman et A.N. Raja Mohammad, « Dual Band Mobile Jammer for GSM 900 & GSM 1800 », Faculty of Engineering, Department of Electrical Engineering-Jordan 2008.

[3] F. Boukerroum, « Etude et caractérisation des circuits micro-ondes linéaires bruyants » Thèse de Doctorat en Sciences, Université Ferhat Abbas, Sétif.

[4] Fiche technique du LM386, www.alldatasheet.com/Lm386-1, (consulté le 8 Mai 2015).

[5] R.W.Rhea « Oscillator Design & Computer Simulation», Noble Publishing 1995 ISBN 1-884932-30-4, p36, p191 – p211.

[6] J.Everard« Fundamentals of RF Circuit Design (with Low Noise Oscillators)»Wiley Interscience, 2001, ISBN 0-471-49793-2, p156.

[7] Y. Hmeydi et M. Bouthlija« Réalisation et mise au point d'un système de brouillage GSM 900-1800 »,Projet de Fin d'Etudes, Institut Supérieur des Etudes Technologiques en Communications de Tunis.

Conclusion générale

Le travail réalisé dans ce mémoire s'inscrit dans le cadre de l'étude d'un domaine un peu particulier : "Le brouillage des récepteurs de téléphonie mobile GSM" qui s'impose comme un moyen fiable et légale pour interdire les communications téléphoniques (ou du moins restreindre) dans les zones où les téléphones mobiles GSM ne sont pas les bienvenus.

L'objectif de notre travail était l'étude, la conception et l'implémentation d'un système de brouillage de téléphonie mobile.

Dans un premier temp, nous avons effectué une étude théorique détaillée du système de téléphonie GSM, du récepteur mobile GSM et de leurs différentes caractéristiques. Nous avons présenté, par suite, les différentes techniques de brouillage de téléphonie mobile connues et adoptées par différentes technologies.

Dans la suite du travail, nous avons effectué une étude détaillée d'un système de brouillage typique pour téléphonie mobile. Ce système est constitué de deux parties principale : La partie basses fréquences (FI : Fréquences Intermédiaires) et la partie RF (Fréquences Radio). Les circuits électriques des différents étages du brouilleur ont été présentés leurs fonctionnements ont été expliqués. Plusieurs simulations des différentes parties du brouilleur ont été réalisées, utilisant le simulateur de circuits électroniques ISIS Proteus (partie IF) et le simulateur ADS (partie IF). En outre, le générateur du signale triangulaire et du bruit ont été réalisés et testés expérimentalement.

En perspective, ce travail peut être complété et amélioré par une implémentation du brouilleur complet.