

# Chapitre 2

# *Généralités sur le réseau GSM*

## **2.1 Introduction**

La famille GSM (GSM, GPRS, EDGE) est devenue l'innovation technique la plus engouée dans l'histoire. En juin 2008, plus 2.9 milliards d'abonnés utilisaient GSM, correspondant à plus de 81% du marché des communications, et son évolution continue encore, malgré l'introduction et le développement de nouvelles générations telles que l'IMT-2000 ou l'UMTS et même au-delà de la 3G.

Au même moment, les réseaux LAN sans fil ont étendu largement le marché mobile mais ceux-là sont restés spécifiques aux applications ne demandant que très peu de mobilité.

La communication partout, avec n'importe qui et à tout moment, a été le rêve et l'objectif que ce sont fixés les chercheurs, les ingénieurs et les utilisateurs depuis l'avènement des premiers systèmes de communications sans fil.

Le plus populaire des systèmes de communications sans fils est le GSM (Gobal System for Mobile communication) et qui assure aussi bien la communication à l'intérieur d'un réseau que l'itinérance entre des réseaux différents. Au début, le GSM était utilisé exclusivement pour transporter la voix, mais très vite des services comme l'introduction messages courts (SMS : Short Message Service) sont devenus très populaires entre les utilisateurs du GSM : plusieurs milliards de messages SMS sont échangés chaque mois. Entre temps, des services de données additionnels ont été réalisés, dont les plus importants sont le High Speed Circuit Switched Data (HSCSD) et le General Packet Radio Service (GPRS), qui améliore

notablement le débit de données par attribution de plusieurs time slots GSM à un terminal pour un service donné.

Une autre étape a été franchie par l'introduction des réseaux de communications mobiles de troisième génération (3G). Les réseaux 3G, connus par Universal Mobile Telecommunication System (UMTS) en Europe et comme International Mobile Telecommunication System 2000 (IMT-2000) ailleurs dans le monde, ne sont pas aussi étendus que le GSM et restent l'apanage de certaines cités. En fait, GSM est encore la majeure technologie pour assurer une couverture complète. Mais grâce aux terminaux multi modes, capables de traiter l'un et l'autre des standards (GSM et UMTS), les utilisateurs ne réalisent même pas laquelle des technologies ils utilisent [15] [22].

## **2.2 Classification des systèmes de communications mobiles**

Le GSM n'est que l'une des nombreuses facettes de la communication mobile moderne.

Pour les systèmes de communication bidirectionnels, la variante la plus simple est le téléphone sans fil avec une mobilité très limitée (Digital Enhanced Cordless Telecommunications (DECT) standard en Europe). Cette technologie est employée pour l'extension des PBXs numériques (Private Branch Exchanges) avec des capacités mobiles.

Les réseaux locaux (LANs) ont également été munis par des fonctions de mobilité ; les réseaux locaux sans fil (WLANs) ont été standardisés et commercialisés par de nombreuses compagnies. Les WLAN offre des protocoles basés IP assurant des communications de données avec de très haut débits néanmoins de faible mobilité. WLANs ont été installés, par exemple, dans les bureaux, les aéroports, comme un supplément ou une alternative aux LANs câblés. Une autre classe de réseaux sans fils en plein essor pour les communications de très courte distance est le Bluetooth, par exemple, pour remplacer les câbles et assurer une l'échange d'information par communication sans fil directe entre les équipements électroniques (entre les téléphones cellulaires, Personal Digital Assistants (PDAs), les ordinateurs et les périphériques). Ces réseaux sont communément appelés Body Area Networks ou Personal Area Networks et ont la particularité de ne dépendre d'aucune infrastructure de réseau fixe (station de base) et se mettent en œuvre d'une manière spontanée et rapide, ce qui leur a valu le nom de réseaux ad hoc [8].

Le GSM et l'UMTS appartiennent à la classe des réseaux cellulaires utilisés principalement en communication publique de masse. Ils ont d'abord eu un succès avec les systèmes

analogiques Advanced Mobile Phone System (AMPS) en Amérique, le Nordic Mobile Telephone (NMT) en Scandinavie ou le *C-Netz* en Allemagne. Le GSM a été fondu sur le système digital (avec ses variantes pour 900,1800 et 1900 MHz) et a permis la génération de millions d'abonnés à travers le monde et est considéré comme une importante force économique. Une autre technologie en compétition est la communication satellitaire basé sur les satellites Low Earth Orbiting (LEO) et les satellites Medium Earth Orbiting (MEO) et qui assure des offres globaux de services de communications [8].

En plus des systèmes de communications bidirectionnels, il existe une variété de systèmes unidirectionnels, où les abonnés ne peuvent que recevoir des données sans possibilité d'émission. On peut citer les anciens systèmes de paging qui assuraient au gens la possibilité d'être joints à un coût raisonnable et ceci sur de grandes zones de couvertures.

## **2.3 Techniques d'accès mobiles**

### **2.3.1 Séparation de directions et transmission duplex**

La forme de communication la plus fréquente est la communication bidirectionnelle qui permet la transmission et la réception simultanément. Les systèmes qui en sont capables sont dits duplex. On peut également atteindre le duplex, même si l'émission et la réception ne se font pas simultanément, en basculant entre les deux phases assez rapidement pour que les utilisateurs ne le remarquent pas.

Les systèmes radio mobiles numériques modernes sont toujours duplexes, et utilisent essentiellement deux procédures basiques : la Frequency Division Duplex (FDD) par l'emploi d'une bande différente dans chaque direction et le Time Division Duplex (TDD) qui basculent périodiquement la direction de la transmission [13] [3].

### **2.3.2 Division de Fréquence Duplex**

La division de fréquence duplex (FDD) est utilisée aussi bien pour les systèmes mobiles analogiques que les systèmes numériques. Pour une communication entre un mobile et une station de base, la bande de fréquence disponible est scindée en deux bandes partielles afin de permettre l'émission et la réception simultanées. Une bande est assignée pour les transmissions montantes (du mobile vers la BTS) et l'autre est assignée pour les transmissions descendantes (de la BTS vers le mobile)

- Bande montante: la bande de transmission du mobile et la bande de réception de la station de base.
- Bande descendante: la bande de réception du mobile et la bande de transmission de la station de base.

Pour assurer une bonne séparation des deux directions, les bandes partielles doivent être tenues à une bonne distance l'une de l'autre. Et en général, la même antenne est utilisée aussi bien pour la réception que l'émission par l'emploi d'une unité de duplexing qui assure la séparation directionnelle, et consiste essentiellement en deux filtres à bandes étroites. Le problème est que ces filtres ne peuvent pas être intégrés, aussi ce duplexing pure n'est pas approprié pour les systèmes avec des petits équipements compacts [28].

### **2.3.3 Division Temporelle Duplex**

Le duplex temporel s'avère une bonne alternative, spécialement pour les systèmes numériques avec division temporelle et accès multiple. Dans ce cas, l'émetteur et le récepteur opèrent d'une manière quasi-simultanée à des instants différents, autrement dit, la séparation directionnelle est réalisée effectivement en basculant dans le temps entre la transmission et la réception, et ainsi aucune unité de duplexing n'est requise [28].

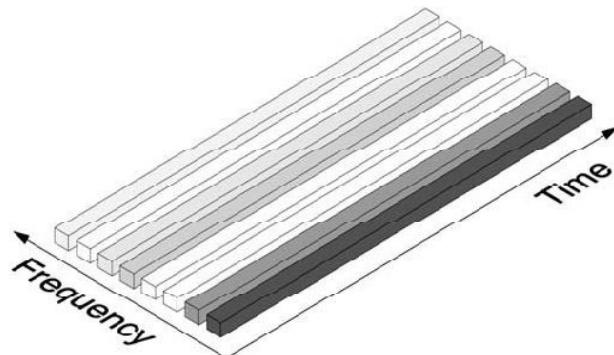
### **2.3.4 Multiple accès**

Le canal radio est un média de communication partagé par plusieurs abonnés dans une cellule. Les stations mobiles rivalisent pour la ressource fréquence pour émettre leurs flux de données. Sans aucune mesure pour contrôler l'accès à plusieurs utilisateurs, des collisions auront lieu (problème du multiple accès). Or les collisions sont très indésirables pour des communications orientées connections comme la téléphonie mobile, c'est pour cela que les stations doivent être assignées des canaux dédiés à la demande. Plusieurs procédures multiples accès sont utilisées pour diviser les bandes de fréquences disponibles en canaux de données [20].

#### **2.3.4.1 Frequency Division Multiple Access (FDMA)**

Dans le FDMA, la bande de fréquence est divisée en canaux d'une certaine bande passante de telle manière que chaque conversation est effectuée sur une fréquence différente. Au

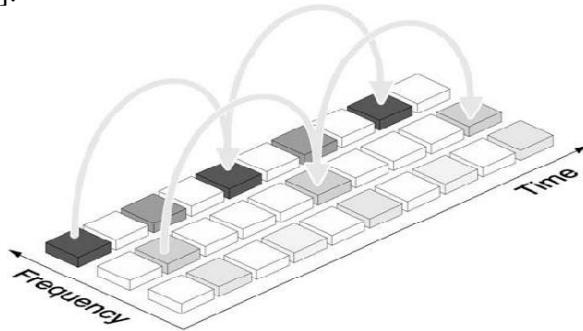
niveau de la station de base les efforts sont énormes et nécessitent une unité d'émission-réception (transceiving) pour chaque canal [13].



**Figure 2.1- Les canaux sur un système FDMA**

### 2.3.4.2 Time Division Multiple Access

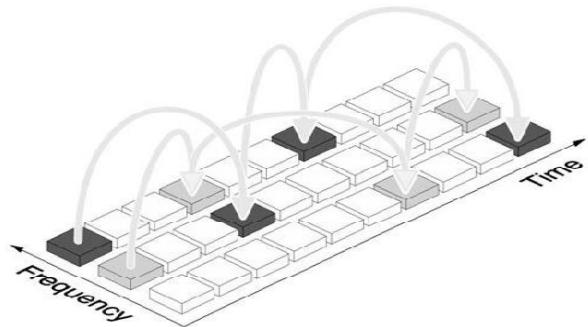
Le TDMA est utilisé dans les systèmes radios mobiles numériques. Aux stations mobiles individuelles, on assigne cycliquement une fréquence à utiliser exclusivement pour la durée d'un slot, ceci demande une synchronisation de frames entre l'émetteur et le récepteur. La bande de fréquence disponible est partagée en canaux de 200 kHz et chacun peut contenir huit conversations TDMA. La séquence de slots assignée à une station mobile représente les canaux physiques du système TDMA. Durant chaque slot, le mobile transmet une donnée sous forme de burst [13].



**Figure 2.2 Les canaux TDMA pour un système avec fréquences multiples.**

Les systèmes à bandes passantes étroites sont vulnérables à l'affaiblissement de fréquences sélectives (frequency-selective fading). Les fréquences co-canal pourraient, elles aussi, contribuer à la détérioration de la qualité de la transmission. Le TDMA offre une bonne

opportunité de réduire sensiblement ces affaiblissements par l'introduction de la technique de saut de fréquence. Avec cette technique, chaque burst d'un canal TDMA est transmis sur une fréquence différente en s'assurant bien que la séquence de sauts est orthogonale, c'est-à-dire que deux stations ne transmettent pas en même temps en utilisant la même fréquence.



**Figure 2.3- TDMA avec la technique de saut de fréquences.**

#### **2.3.4.3 Code Division Multiple Access**

Les systèmes avec CDMA sont à bandes larges, où chaque utilisateur dispose de toute la bande passante pour la durée complète de la connexion. Cependant, cet usage n'est pas exclusif, tous les abonnés dans une cellule utilisent la même bande fréquence simultanément. Pour séparer des signaux, les uns des autres, on assigne aux abonnés des codes orthogonaux.

A la base du CDMA, on trouve la technique d'étalement de spectre qui consiste à étaler le signal d'un abonné sur un spectre (avec un facteur entre 10 et 1000) pour générer un signal large bande à partir du signal original à bande étroite. On obtient, ainsi, un signal qui est moins sensible aux interférences et aux bruits, et de ce fait on assure une communication même en dessous du seuil de bruit [19].

#### **2.3.4.4 Space Division Multiple Access**

Une propriété essentielle du canal radio mobile est la propagation multi-chemins (multipath) qui génère les phénomènes d'interférences et est surtout sujette au problème d'évanouissement spatial.

En utilisant des antennes sous forme de tables, on peut séparer les signaux reçus simultanément des abonnés situés à des emplacements distincts. De tels systèmes à antennes permettent de diriger la table des antennes d'une manière intelligente et d'assurer

que le signal reçu ou transmis est exactement dirigé spatialement dans le segment où la station mobile se trouve. Une conséquence directe, est la réduction de l'interférence co-canal dans les autres cellules ou la sensibilité aux interférences dans la cellule courante. Cette technique d'accès est nommée SDMA (Space Division Multiple Access), et les systèmes utilisant cette technique sont le sujet d'actives recherches. La technique SDMA peut être combinée avec les autres techniques d'accès (FDMA, TDMA, CDMA), ce qui peut être attractif pour les réseaux existants par la mise à jour uniquement des stations de bases avec des antennes sous formes de tables et des protocoles de contrôles appropriés [13].

## 2.4 Description du GSM

### 2.4.1 Architecture du réseau GSM [8] [18]

Les composants fondamentaux d'un réseau GSM sont montrés sur la figure 2.4. Un utilisateur transporte une station mobile (MS), celle-ci peut communiquer à travers l'air avec une station de base, appelée BTS (Base Transceiver Station) en GSM. La BTS contient les équipements de transmission et de réception comme les antennes et les amplificateurs et les quelques composants pour traitement du signal et le protocole de communication. Dans l'esprit de garder les BTS les plus petites possibles, l'essentiel de l'intelligence responsable du contrôle réside dans le BSC (Base Station Controller). LE BSC contient les fonctions de protocole pour l'allocation et la configuration du canal radio ainsi que la gestion des handovers. Typiquement, plusieurs BTSs sont contrôlées par un seul BSC. Et en pratique les BTSs et le BSC sont connectés par des lignes fixes ou des liaisons radios point-à-point et forment ensemble la partie réseau accès radio (RAN).

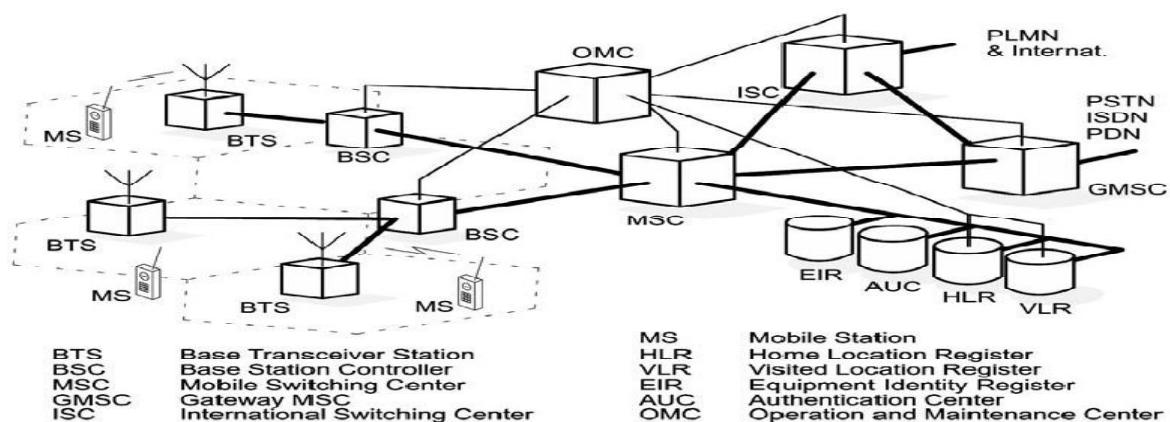
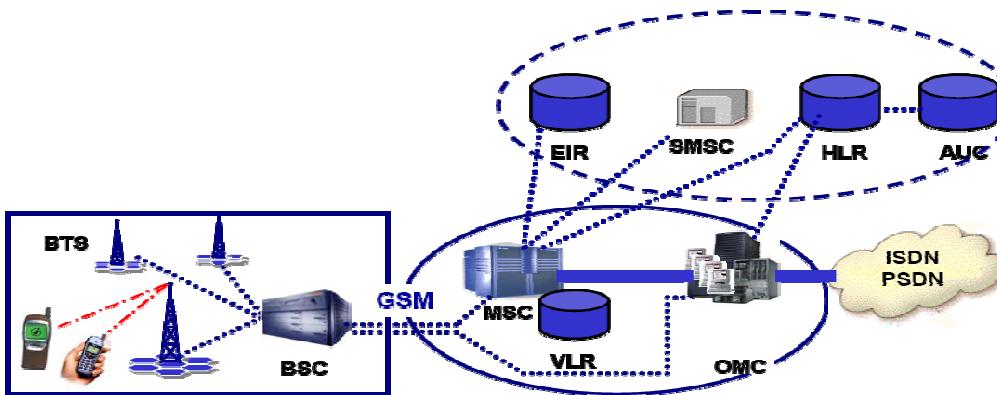


Figure 2.4- Architecture du système GSM

Tout le trafic des utilisateurs est routé à travers un commutateur, nommé le MSC (Mobile Switching Center) qui exécute toutes les fonctions de commutations qu'assure un nœud de commutation d'un réseau téléphonique type ISDN (Integrated Services Digital Network (ISDN). Ceci inclut la recherche de chemins, l'expédition de données et le traitement des services divers. La différence principale entre un ISDN et un MSC est que le MSC doit également considérer l'allocation et l'administration des ressources radios et la mobilité des utilisateurs. Le MSC doit, néanmoins, fournir des fonctions additionnelles relatives à la l'inscription des abonnées et pour le handover d'une connexion dans le cas de changement vers une autre cellule. Un réseau cellulaire peut disposer de plusieurs MSCs, chacun gérant une partie du réseau (une cité ou une zone métropolitaine).

Les appels originaires ou destinés à un réseau fixe, sont traités par un MSC dédié appelé GMSC (Gateway MSC). Et les connexions vers d'autres réseaux mobiles ou internationaux sont routées via l'ISC (International Switching Center).



**Figure 2.5- Les différentes bases de données utilisées dans le GSM.**

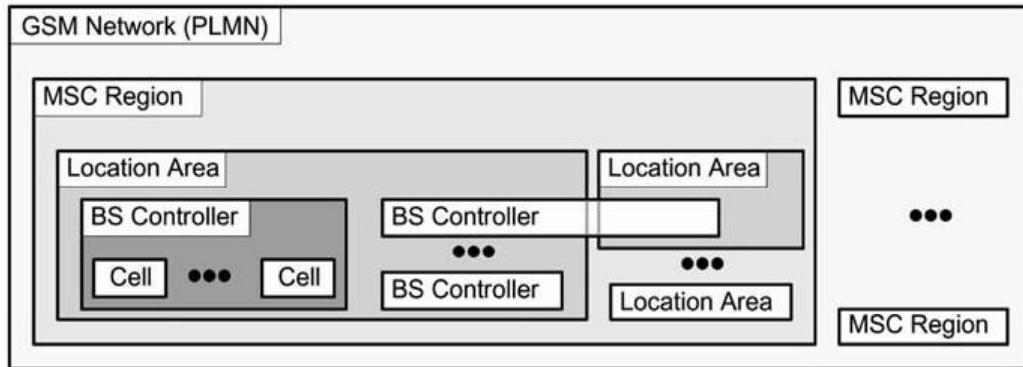
Un réseau GSM contient plusieurs types de bases de données (figure 2.5). Le HLR (Home Location Register) et le VLR (Visited Location Register) enregistrent l'emplacement courant d'un utilisateur mobile. Ceci est nécessaire car le réseau doit connaître la cellule courante d'un utilisateur pour établir un appel avec la BTS correcte. Ces registres sont également utilisés pour les opérations de paiement et facturations et d'autres questions administratives. Deux autres bases de données servent à des fins de sécurité : l'AUC (Authentication Center) qui sauvegarde les données liées à la sécurité comme les clés pour l'authentification et le cryptage ; et l'EIR (Equipment Identity Register) qui enregistre les données concernant l'équipement de l'abonné.

Toute la gestion du réseau est centralisée en un seul lieu, l'OMC (Operation and Maintenance Center). Les missions de l'OMC incluent l'administration des abonnés, terminaux, la facturation, la configuration du réseau, le monitoring de performance et la maintenance de réseau.

Le réseau GSM peut être divisé en trois sous-réseaux : le réseau accès radio (radio access network), le noyau du réseau et le réseau de gestion. Ces sous-réseaux sont appelés sous-systèmes dans la norme GSM. Ces trois sous-systèmes sont :

- le BSS (Base Station Subsystem),
- le NSS (Network switching Subsystem) et
- l'OMSS (Operation and Maintenance Subsystem).

La figure 2.6 résume la relation d'hiérarchie entre les composants du réseau (MSC, BSC et BTS). Le réseau en entier, le PLMN (Public Land Mobile Network), est divisé en régions MSC, chacune contient au moins un LA (Location Area) formé d'une ou plusieurs groupes de cellules.



**Figure 2.6- L'hiérarchie dans le système GSM**

### **2.4.2 Le concept SIM**

Chaque utilisateur possède une carte à puce personnelle, la SIM (Subscriber Identity Module) Comme illustré dans la figure 2.7, elle peut être intégrée dans un équipement mobile [13].



**Figure 2.7- La personnalisation de l'équipement mobile avec la carte SIM**

En fait, c'est la SIM qui rend un équipement mobile une complète station avec des priviléges d'utilisation du réseau, et lui permet de faire ou recevoir des appels. La carte SIM peut enregistrer des petits messages et possède la fonctionnalité d'un annuaire téléphonique. Et l'utilisation de la SIM et donc du MS entier peut être protégée avec un PIN (Personal Identification Number) contre des accès non autorisés.

### **2.4.3 Adressage [13] [8]**

Les entités d'un réseau GSM doivent avoir une certaine adresse ou identité pour l'identification, l'authentification ou la localisation dans le réseau. Le numéro de téléphone est parmi les plus connus des identificateurs, mais plusieurs d'autres ont été définis pour gérer la mobilité et pour servir de base à l'adressage des autres éléments du réseau.

#### **2.4.3.1 L'identité internationale de l'équipement station mobile**

L'IMEI (International Mobile Station Equipment Identity) identifie d'une manière unique le MS à l'échelle internationale et donne des indications sur le constructeur et la date de sortie d'usine. L'IMEI est fourni par le constructeur et enregistré par l'opérateur du réseau dans

la base EIR. A l'aide de l'IMEI on peut déceler les équipements dérobés et procéder à un déni de service si nécessaire.

L'IMEI est requis par le réseau à l'enregistrement, mais peut être exigé périodiquement. C'est une adresse hiérarchique contenant les parties suivantes :

- TAC (Type Approval Code), six chiffres assignés par une autorité centrale.
- FAC (Final Assembly Code), six chiffres assignés par le constructeur.
- SN (Serial Number), six chiffres assignés par le constructeur.
- Un chiffre disponible.

#### **2.4.3.2 L'identité internationale de l'abonné mobile**

Quand un utilisateur souscrit un abonnement chez un opérateur mobile, il reçoit un identificateur unique, l'IMSI (International Mobile Subscriber Identity). L'IMSI est enregistré dans la carte SIM.

Le MS ne peut fonctionner que si une carte SIM avec un IMSI valide est insérée dans un équipement avec un IMEI valide. Car c'est l'unique moyen de facturer correctement l'abonné.

L'IMSI utilise un maximum de 15 chiffres et contient trois parties :

- Le MCC (Mobile Country Code), trois chiffres internationalement standardisés.
- Le MNC (Mobile Network Code), deux chiffres, pour l'identification unique des réseaux mobiles à l'intérieur d'un pays.
- Le MSIN (Mobile Subscriber Identification Number), au maximum 10 chiffres, pour l'identification de l'abonné dans son réseau d'origine.

L'IMSI est différent du plan de numérotation ISDN. Trois chiffres MCC sont assignés pour chaque pays et deux chiffres MNCs assignés à l'intérieur de ces pays (par exemple, 262 comme MCC pour l'Allemagne, et MNC 01, 02 et 07 pour les réseaux T-Mobile, Vodafone et O2, respectivement)

#### **2.4.3.3 Le numéro ISDN de l'abonné mobile**

Le numéro de téléphone réel d'un abonné est appelé le numéro MSISDN (Mobile Subscriber ISDN).

Il est assigné à l'abonné (leur SIM), de telle manière qu'il peut avoir plusieurs MSISDNs, une pour chaque service souscrit.

Le MSISDN suit le plan international de numérotation ISDN, et a la structure suivante :

- Le CC (Country Code), jusqu'à trois chiffres.
- Le NDC (National Destination Code), typiquement deux ou trois chiffres.
- Le SN (Subscriber Number), un maximum de 10 chiffres.

Les CCs sont internationalement standardisés, selon les recommandations E.164 de l'ITU-T (1 pour l'USA, 358 pour la Finlande, 213 pour l'Algérie etc.). L'administration de régulation locale assigne le NDC et le SN.

Le MSISDN est enregistrée centralement dans le HLR.

#### **2.4.3.4 Le numéro d'itinérance de la station mobile**

Le MSRN (The Mobile Station Roaming Number) est un numéro ISDN temporaire, assigné par le VLR à chaque MS dans sa zone. Les appels sont routés à la station mobile en utilisant le MSRN.

Le MSRN a une structure similaire au MSISDN :

- Le CC du réseau visité.
- Le NDC du réseau visité
- Le SN dans le réseau mobile courant.

Les composants CC et NDC sont déterminés par le réseau visité et dépendent de l'emplacement courant. Le SN est assigné par le VLR courant et est unique à l'intérieur du réseau mobile. Le plus important est que l'assignation du MSRN est faite de telle manière que le nœud de commutation MSC dans le réseau visité peut être déterminé à partir du numéro de l'abonné, ce qui rend possible la prise de décisions de routage.

#### **2.4.3.5 L'identité de zone de localisation**

Chaque LA (Location Area) d'un réseau cellulaire possède sa propre identité LAI (Location Area Identifier). Le LAI est structuré hiérarchiquement et est internationalement unique :

- Le CC, trois chiffres.
- Le MNC, deux chiffres

- Le LAC (Location Area Code), un maximum de cinq chiffres.

Le LAI est régulièrement diffusé par la station de base sur le canal BCCH (Broadcast Control Channel), permettant à chaque MS de déterminer sa location courante via le LAI.

#### **2.4.3.6 L'identité temporaire de l'abonné mobile**

Le VLR, responsable de la localisation courante, peut assigner un TMSI (Temporary Mobile Subscriber Identity) à l'abonné. Cet identifiant n'a de signification que dans la zone gérée par le VLR, et est utilisé à la place de l'IMSI pour l'identification et l'adressage du MS. Le TMSI est assigné uniquement durant la présence du MS dans la zone d'un seul VLR et n'est pas passé au HLR, de cette façon, personne ne peut usurper l'identité de l'abonné par écoute du canal radio. Le MS enregistre le TMSI sur la carte SIM et il est assigné librement par l'opérateur et consiste en 4x8 bits. Le TMSI et le LAI ensemble permettent d'identifier d'une manière univoque l'abonné (i.e. l'IMSI peut être remplacé par le couple (TMSI, LAI)).

#### **2.4.4 Registres et données de l'abonné [13] [8]**

##### **2.4.4.1 Registres de localisation (HLR et VLR)**

Le standard GSM définit deux types de bases de données pour la gestion des données utilisateurs et la localisation : le HLR et VLR (figure 2.8). Ces bases sont interrogées par le réseau pour l'enregistrement et la localisation de l'abonné. Le HLR possède un enregistrement pour chaque abonné avec l'opérateur. Il sauvegarde, par exemple, les numéros de téléphone de chaque utilisateur, les services souscrits, les permissions et les authentifications.

A ces données administratives permanentes, s'ajoute les données temporaires telles que la localisation courante d'un abonné. Le VLR est responsable d'un groupe de zones et enregistre les données des utilisateurs présents dans cette zone. Les données incluent une partie des données utilisateurs permanentes copiée du HLR pour accélérer l'accès. Le VLR, peut aussi assigner et enregistrer des données locales telles que les identificateurs temporaires.

Typiquement, il y a un seul HLR central par réseau et un VLR pour chaque MSC. Cette organisation dépend du nombre d'abonnés et la capacité de traitement et de stockage des commutateurs.

#### 2.4.4.2 Les registres de sécurité (AUC et EIR)

La sécurité GSM est basée principalement sur l'authentification de l'équipement et l'identité de l'abonné. Deux bases de données additionnelles sont responsables des différents aspects de la sécurité du système.

Les données confidentielles et les clés sont sauvegardées ou générées dans l'AUC (Authentication Center). L'EIR (Equipment Identity Register) enregistre le numéro de série fournit par le constructeur du terminal (IMEI).

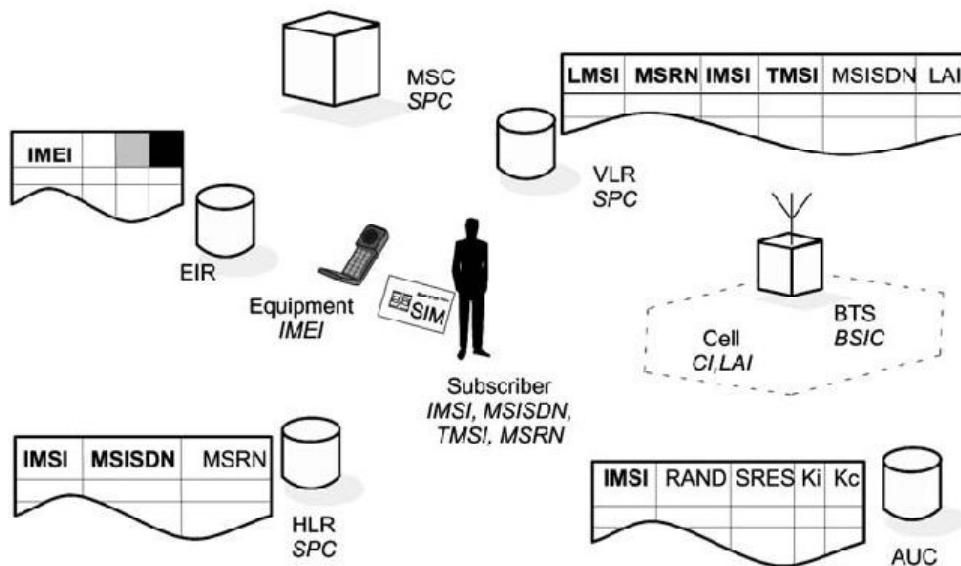


Figure 2.8- Les bases de données et les adresses du GSM

#### 2.4.5 Interfaces réseaux

Les relations de communication entre les composants du réseau GSM sont formalisées par un certain nombre d'interfaces standards (figure 2.9).

L'interface A entre le BSS et le MSC est utilisée pour le transfert de données de gestion du BSS, le contrôle de connexion et la gestion de la mobilité. Cette interface est basée sur l'utilisation d'une ou plusieurs liaisons numériques à 2Mbit/s qui supportent le trafic ainsi que la signalisation nécessaire.

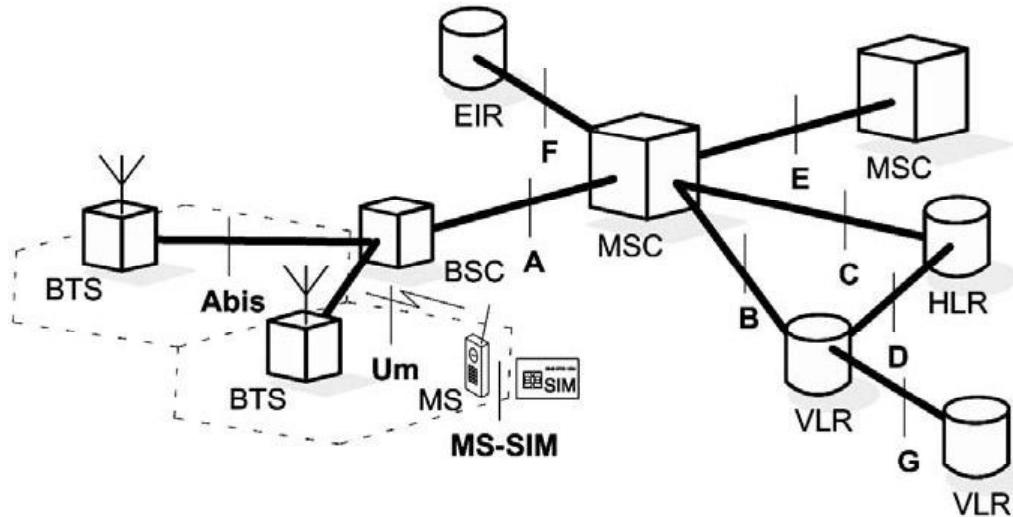


Figure 2.9- Les interfaces du réseau GSM

L'interface **A** est définie à la sortie du MSC et le débit du canal de parole y est égal à 64 kbit/s. Or, le débit correspondant sur l'interface radio est égal au plus à 16 kbit/s. Une fonction de transcodage (TRAU, Transcoder / Rate Adaptor Unit) pour la parole ou de conversion de débit pour les canaux de données est donc nécessaire. L'interface **A** permet que ces fonctions soient géographiquement situées près du MSC ou du BSC ; cependant, fonctionnellement, le transcodeur est considéré comme faisant partie du BSS. Le protocole de signalisation sur l'interface A est BSSAP (Base Station Subsystem Application Part) qui s'appuie sur un transport SS7. Cette interface est parfaitement spécifiée et permet un réel interfonctionnement entre des MSC et des BSC provenant de différents fournisseurs.

A l'intérieur du BSS, deux interfaces, l'interface **Abis** entre la BTS et le BSC et l'interface air **Um** ont été définies. Un MSC qui requiert des données sur un MS situé dans sa zone administrative, les réclame au VLR responsable à travers l'interface **B**. Et inversement, le MSC transmet à ce VLR toutes les mises à jour sur la position du MS ou la reconfiguration pour l'activation de services supplémentaires afin que le VLR mette à jour le HLR. Par l'interface **D**, le VLR informe le HLR sur la position courante de l'abonné et reporte le MSRN courant et le HLR transfère au VLR toutes les données de l'abonné pour lui donner accès à ses services personnalisés. Sur cette interface également, le HLR est responsable d'émettre l'annulation des données de l'abonné à l'ancien VLR, une fois l'acquittement de

la nouvelle position arrive du nouveau VLR. Maintenant s'il arrive, en cours de mise à jour, que le nouveau VLR a besoin des données de l'ancien VLR il le demande sur l'interface **G**. la demande ou la vérification de l'identité d'un équipement se fait sur l'interface **F** entre le MSC et le EIR.

Le MSC possède deux autres interfaces, en l'occurrence **C** et **E**. L'interface **C** est utilisée par le MSC, en cours d'établissement d'un appel, pour avoir des informations de routages du HLR et lui envoie les informations de taxation par cette interface.

Si l'abonné mobile passe d'un MSC à un autre pendant une conversation, une procédure de handover inter-MSC doit être entreprise via l'interface **E**.

## **2.5 Spécification GSM**

### **2.5.1 Les fréquences de travail du GSM**

Dans le système GSM/DCS, 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**) [25] :

- Bande GSM (bande de largeur totale 25 MHz)
  - de 890 à 915 MHz du mobile vers la base
  - de 935 à 960 MHz de la base vers le mobile
  - écart entre les deux fréquences 45 MHz
  - 124 canaux espacés de 200 kHz
- bande EGSM étendue (bande de largeur totale 35 MHz)
  - de 880 à 915 MHz du mobile vers la base
  - de 925 à 960 MHz de la base vers le mobile
  - écart entre les deux fréquences 45 MHz
  - 174 canaux espacés de 200 kHz
- bande DCS (bande de largeur totale 75 MHz)
  - de 1710 à 1785 MHz du mobile vers la base
  - de 1805 à 1880 MHz de la base vers le mobile
  - écart entre les deux fréquences 95 MHz
  - 374 canaux espacés de 200 kHz

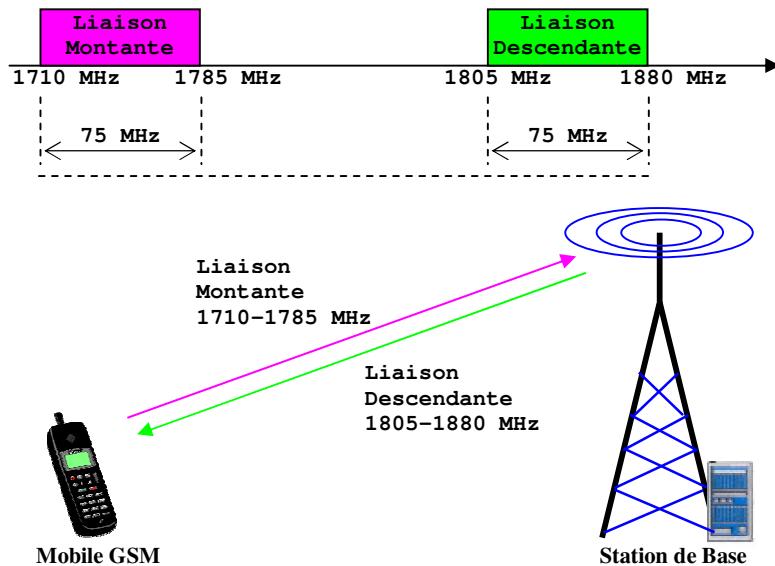


Figure 2.10- Liaison Montante et Liaison Descendante dans le GSM

Chaque porteuse GSM ou DCS est identifiée de manière unique par un numéro n, désigné par le sigle ARFCN et codé sur 10 bits conformément au plan suivant :

$$\text{Pour } 1 \leq n \leq 124$$

$$fd = 935 + (0,2 \times n) \quad (\text{GSM})$$

$$\text{Pour } 975 \leq n \leq 1024$$

$$fd = 935 + (0,2 \times (n-1024)) \quad (\text{GSM étendu EGSM})$$

$$\text{Pour } 512 \leq n \leq 885$$

$$fd = 1805,2 + (0,2 \times (n-512)) \quad (\text{DCS 1800})$$

**Remarque :** ce numéro de canal peut changer durant une communication lorsque la qualité devient insuffisante (saut de fréquence ou frequency hopping).

## 2.5.2 Le multiplexage temporel

A l'intérieur d'une cellule, on dispose d'un certain nombre de fréquences ou canaux qu'il faut répartir entre les différents utilisateurs. Chaque porteuse est divisée en 8 intervalles de temps appelés **time-slots**. La durée d'un slot a été fixée pour le GSM à 7500 périodes du signal de référence fourni par un quartz à 13 MHz qui rythme tous les mobiles GSM [25]:

$$\text{Tslot} = 7500 / 13 \text{ MHz} = 0,5769 \text{ ms soit environ } 577 \mu\text{s}$$

Sur une même porteuse, les slots sont regroupés par paquets de 8 qui constituent une trame TDMA.

La durée de la trame est donc :

$$\text{TTDMA} = 8 \text{ Tslot} = \mathbf{4,6152 \text{ ms}}$$

Un mobile GSM en communication n'utilisera qu'un time-slot, ce qui permet de faire travailler jusqu'à 8 mobiles différents sur la même fréquence de porteuse. Le signal radio émis dans un time-slot est appelé **burst**.

Les slots sont numérotés par un indice TN qui varie de 0 à 7. Un « canal physique » est donc constitué par la répétition périodique d'un slot dans la trame TDMA sur une fréquence particulière.

Durant une communication téléphonique, le mobile GSM reçoit des informations de la station de base et émet des informations vers celle-ci :

- ces échanges se font sur deux fréquences différentes et n'ont pas lieu au même moment
- au niveau du mobile, l'émission et la réception sont décalés dans le temps de 3 time-slots

Le mobile reçoit donc le signal émis par la base sur la fréquence descendante f durant un time slot soit 577 µs, puis 3 time-slots soit 1,7 ms plus tard, émet son signal vers la station de base sur la fréquence montante plus basse (f-95 MHz pour le GSM 1800).

### **2.5.3 Canaux logiques [13]**

Sur la couche 1 du modèle de référence OSI, le GSM définit une série de canaux logiques. Ces canaux sont soit disponibles selon un mode d'accès aléatoire, soit assignés selon un mode dédié à un utilisateur spécifique. Et ils sont divisés en deux catégories: les canaux de trafic et les canaux de signalisation (contrôle) (table 2.1).

Groupe		Canal	Fonction	Direction
Traffic channel	TCH	TCH/F, Bm	Full-rate TCH	MS ↔ BSS
		TCH/H, Lm	Half-rate TCH	MS ↔ BSS
Signalling	BCH	BCCH	Broadcast Control	MS ← BSS
Channels (Dm)		FCCH	Frequency Correction	MS ← BSS
		SCH	Synchronisation	MS ← BSS
	CCCH	RACH	Random Access	MS → BSS
		AGCH	Access Grant	MS ← BSS
		PCH	Paging	MS ← BSS
		NCH	Notification	MS ← BSS
	DCCH	SDCCH	Stand-alone Dedicated Control	MS ↔ BSS
		SACCH	Slow Associated Control	MS ↔ BSS
		FACCH	Fast Associated Control	MS ↔ BSS

**Table 2.1- Classification des canaux logiques en GSM.**

### **2.5.3.1 Canaux de trafic**

Les canaux de trafic (TCHs) sont utilisés pour la transmission des données utilisateur (parole, données). La communication sur le TCH peut être à commutation de circuits ou à commutation de paquets. Dans le premier cas, le TCH fournit une connexion transparente, i.e. une connexion traitée spécialement selon le service transporté (exemple la téléphonie). Pour la commutation de paquets, le TCH transporte des données utilisateur de couches 2 et 3 selon les recommandations du protocole standard X.25 ou un protocole de paquets similaire.

Un TCH peut être utilisé plein débit (full-rate, appelé aussi Bm) ou scindé en deux semi-débit canaux (half-rate, appelé Lm), qui peuvent être attribués à des utilisateurs différents.

Le canal Bm transmet une suite de bits de 13 Kbits/s de la parole codée numériquement ou une suite de données à un débit de 14.5, 12, 6 ou 2.6 bits/s. Le Lm transporte les signaux de la parole à un débit de moitié (6.5 kbits/s) et les données au début 6 ou 2.6 kbits/s.

### **2.5.3.2 Canaux de signalisation**

Le contrôle et la gestion du réseau cellulaire exige un effort de signalisation considérable.

Même en l'absence d'une communication active, des informations de signalisations (par exemple, la mise à jour de la position) sont transmises en permanence sur l'interface air. Les canaux de signalisations GSM (canaux Dm) offre un service orienté paquets au MSs et sont classés en trois catégories : les canaux de diffusion (BCH), les canaux de contrôles communs (CCCH) et enfin les canaux de contrôles dédiés (DCCH).

Le canal unidirectionnel BCH est utilisé par le BSS pour diffuser la même information à toutes les stations mobiles. Il consiste en trois canaux :

- **BCCH (Broadcast Control Channel):** une série d'informations caractérisant le canal radio sont diffusées aux MSs sur ce canal, ceci inclut les configurations du canal radio, les paramètres de synchronisations (fréquences et les numéros des frames), les identificateurs d'enregistrement (LAI, CI, BSIC) et en particulier, le format du canal CCCH de la BTS locale. Le BCCH est émis sur la première fréquence assignée à la cellule.
- **FCCH (Frequency Correction Channel):** sur ce canal, des informations sur la correction des fréquences de transmissions sont diffusées aux MSs.
- **SCH (Synchronization Channel):** le SCH diffuse une information pour identifier la BTS (identificateur BSIC, Base Transceiver Station Identity Code) et d'autres données de synchronisation au niveau des frames.

Le CCCH est un canal de signalisation point-à-multipoints qui s'occupe des fonctions de la gestion d'accès. Ceci inclut l'assignation des canaux dédiés. Il comprend :

- **RACH (Random Access Channel):** le RACH constitue la portion montante du canal CCCH. Il est accédé par la station mobile, dans une cellule sans réservation et d'une manière compétitive, pour demander un canal de signalisation dédié.
- **AGCH (Access Grant Channel) :** il est émis par la BTS pour assigner un SDCCH ou un TCH à un MS.

- **PCH (Paging Channel)** : il est émis par la BTS pour rechercher un MS spécifique.
- **NCH (Notification Channel)**: le NCH est utilisé pour informer les MSs sur l'arrivée d'appels de groupe et de diffusion.

Le dernier type de canaux de signalisation, le DCCH, est un canal bidirectionnel point-à-point et comprend les canaux dédiés suivants :

- **SDCCH (Stand-alone Dedicated Control Channel)** : il est utilisé pour la signalisation entre un MS et la BTS pendant qu'aucune connexion n'est active. Le SDCCH est demandé via le RACH et assigné par le canal AGCH. Après la terminaison de la transaction de signalisation, il est libéré et peut être assigné à un autre MS. Comme exemple d'utilisation du SDCCH on peut citer la mise à jour de la position du MS.
- **SACCH (Slow Associated Control Channel)** : il est toujours assigné et utilisé en conjonction avec un TCH ou un SDCCH. Le SACCH transporte les informations permettant d'assurer une opération radio optimale comme les commandes de contrôle de la puissance et reporte les mesures effectuées sur le niveau du signal radio.
- **FACCH (Fast Associated Control Channel)** : il est utilisé uniquement en connexion avec un TCH pour transmettre des informations courtes et nécessitant un traitement rapide (exemple handover). La transmission du FACCH va aux dépens de celle du TCH (emprunt de slots).

#### **2.5.4 Configuration de la connexion d'un appel entrant**

La figure 2.10 montre l'établissement d'une connexion d'un appel entrant sur l'interface air. Le MS est contacté sur le canal PCH et demande un canal de signalisation sur le RACH. Il obtient le SDCCH à travers un message d'assignation immédiate sur l'AGCH. Ensuite débute une phase d'authentification, de cryptage et de configuration sur le SDCCH. Un message de commande d'assignation donne un canal de trafic TCH au MS, qui acquitte la réception sur le FACCH de ce TCH. Le FACCH est utilisé pour continuer la configuration de la connexion [13].

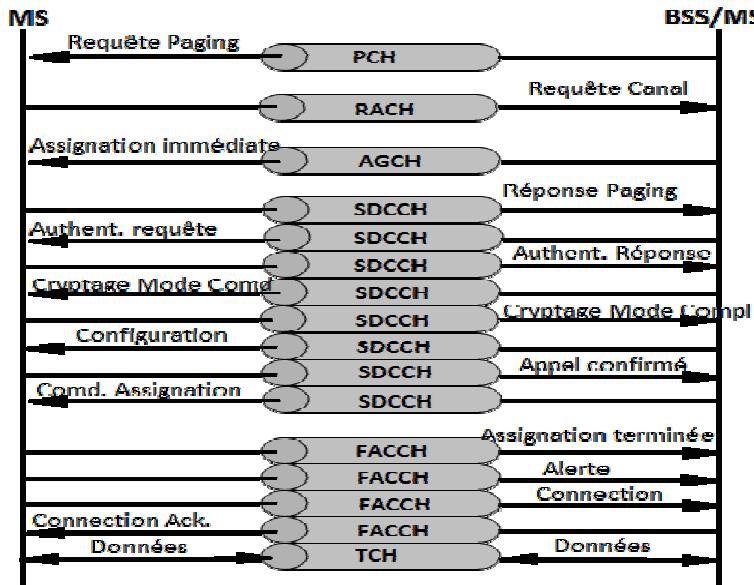


Figure 2.11- Canaux logiques et signalisation  
(Configuration d'une connexion pour un appel rentrant)

### 2.5.5 Services de l'abonné GSM

Les services offerts aux clients GSM sont de deux types : service de téléphonie et services de données. La téléphonie consiste en le transfert de la voix qui prémuni le abonnées avec la capacité et les équipements terminaux nécessaires de se communiquer sur des lieux divers. Les services de données offrent la capacité de transmettre des signaux de données entre deux points d'accès munis d'interfaces au réseau.

En plus de la téléphonie normale et les appels d'urgence, le GSM supporte les services suivants [35] :

- **Le DTMF (dual-tone multifrequency)** : le DTMF est un schéma de signalisation de tonalité utilisé souvent pour diverses raisons de contrôle via le réseau téléphonique, comme un télé-contrôle d'une machine répondeuse.
- **Le facsimile groupe III** : le GSM supporte le CCITT groupe 3 facsimile. Un abonné est en mesure d'envoyer un fax (en utilisant un convertisseur spéciale GSM)

à un autre abonné y compris à une machine fax standard connecté au téléphone analogique.

- **SMS (short message services)** : une facilité remarquable des réseaux GSM est le service des messages courts. Un message d'une certaine taille (vers 160 caractères alphanumériques) peut être envoyé et reçu par une station mobile. Ceci peut être considéré comme une forme évoluée du système de paging avec plus d'avantages. Le message n'est pas perdu si le terminal mobile est éteint ou hors de couverture. Le message est stocké et est réexpédié une fois le mobile détecté sur le réseau.
- **Diffusion de cellule** : une variante du SMS est la diffusion de cellule. Ca consiste en l'envoi d'un maximum de 93 caractères sous forme de diffusion à tous les abonnés d'une certaine région. Des applications typiques incluent les alertes de congestion ou les rapports d'accidents.
- **La messagerie vocale** : ce service est une machine répondeuse, contrôlé par l'abonné. les appels peuvent être expédiés à une boîte vocale que seul l'abonné peut consulter en manipulant un code de sécurité spéciale.
- **Renvoi d'appel** : ce service permet à l'abonné de renvoyer les appels entrants vers un autre numéro si l'unité mobile n'est pas joignable, la ligne est actuellement occupée, absence de réponse ou si le renvoi inconditionnel est activé.
- **Inhibition des appels sortants** : cette fonctionnalité permet d'empêcher l'émission de tous les appels.
- **Inhibition des appels rentrants** : cette fonctionnalité permet d'empêcher les appels rentrants. Deux variantes existent : empêcher tous les appels rentrants ou seulement dans le cas d'itinérance hors du PLMN d'origine.
- **Attente d'appel** : ce service notifie l'abonné de l'arrivée d'un nouvel appel en cours de conversation. L'abonné peut répondre, rejeter ou ignorer l'appel rentrant.
- **Service appel de groupe** : avec ce service, l'abonné mobile peut établir une conversation de groupe, i.e. une conversation simultanée entre trois et six abonnés.
- **Identification/Masquage d'appel** : ce service procure, à l'abonné mobile appelé, le numéro ISDN de l'abonné appelant. Et le masquage empêche l'appelé de connaître le numéro de l'appelant.

- **Groupes d'utilisateurs clos (CUGs)** : CUGs sont généralement comparable aux PBX. C'est des groupes d'abonnés qui ne peuvent communiquer qu'avec eux-mêmes ou certains numéros.

## **2.6 Conclusion**

Dans ce chapitre on a essayé de passer en revue des notions importantes de la norme GSM. Comme l'architecture générale d'un réseau GSM, les différents liens filaires et sans fil reliant le mobile à la BTS et la BTS au MSC mais aussi les entités qui contribuent à fournir un tas de services de téléphonie à l'abonné d'une manière efficace et sécurisée.

Seulement la diversité des liens qui relient le mobile et MSC rend très complexe l'apprehension de toute la norme GSM puisqu'il est question :

- 1- Du Type de support de transmission permettant de véhiculer le trafic,
- 2- De la Capacité disponible pour véhiculer le trafic

Ce qui fait que la majeure partie des opérations d'optimisation du réseau de transmission vise en premier lieu à trouver comment utiliser les capacités (ressources) disponibles au niveau des liens existants (déjà installés) pour acheminer des informations d'un mobile à un MSC ; et cela en évitant au maximum de faire appel à une implémentation d'un autre lien pour l'extension de la capacité.

Dans le chapitre suivant nous aborderons les méthodes qui permettraient l'optimisation du réseau GSM par une planification adéquate en région urbaine.