



**Ecole Nationale des Sciences
Appliquées - Tanger**



**Université Abdelmalek
Essaadi**

Matière : Réseau GSM

Enseignée par : Dr. Mohammed Réda Britel

1. Introduction

Un système de radiotéléphonie a pour objectif premier de permettre l'accès au réseau téléphonique à partir d'un terminal portatif sur un territoire étendu (un pays, voire un continent). Ce service utilise une liaison radioélectrique entre le terminal et le réseau. Selon les systèmes, plusieurs bandes de fréquences sont utilisées : parmi les principales, on compte les bandes 450 MHz, 900 MHz et 1800 MHz.

Pour que le service soit disponible, il faut que la liaison radio entre le terminal et le réseau soit de qualité suffisante, ce qui peut nécessiter une puissance importante des émetteurs. Afin de limiter cette puissance, l'opérateur du réseau radio mobile place un ensemble de stations de base (BS, Base Station) sur le territoire à couvrir pour que le terminal soit toujours à moins de quelques kilomètres de l'une d'entre elles. Ces BS sont, pour les usagers, les points d'accès au réseau radio mobile.

La liaison entre le mobile et la BS est effectuée sur un canal radio, c'est-à-dire sur une bande de fréquences du spectre alloué à l'opérateur.

La surface sur laquelle un terminal peut établir une liaison avec une station de base déterminée est appelée une cellule. L'opérateur cherche donc à réaliser une couverture du territoire par un ensemble de cellules contiguës. Pour économiser le spectre hertzien, il réutilise les mêmes fréquences sur des cellules suffisamment éloignées les unes des autres pour que les communications qui utilisent la même fréquence ne se brouillent pas. Selon la quantité de trafic à écouler dans la cellule, l'opérateur dispose plus ou moins de canaux radios sur la station de base,

On appelle station mobile ou mobile (MS, mobile station) tout équipement terminal capable de communiquer sur le réseau. Le mobile est composé d'un émetteur / récepteur et d'une logique de commande. Il peut être :

- *Un équipement installé à demeure sur un véhicule,*
- *Un portatif, c'est-à-dire un équipement de quelques centaines de grammes et de faible puissance (de l'ordre du Watt) aisément transportable.*

2. Réseaux mobiles / Réseaux fixes

L'utilisation de l'interface radio dans les communications introduit un certain nombre de différences par rapport aux communications sur câble.

2.1. Spectre limite

Le spectre radio utilisable pour les radiocommunications, et par conséquent la capacité disponible pour l'accès radio, est généralement limitée par la réglementation. En effet, contrairement aux communications filaires où une population et une demande en capacité de plus en plus importantes peuvent être facilement desservies par le déploiement de câbles supplémentaires pour connecter les abonnés au réseau, la largeur du spectre radio ne peut être étendue arbitrairement.

La technique cellulaire résout partiellement ce problème en partageant la zone à couvrir en cellules radio, chacune équipée par une station de base et en réutilisant le spectre radio aussi souvent que possible. La réutilisation du spectre est principalement limitée par les niveaux des interférences co-canales et adjacentes.

De plus, les constructeurs ont eu recours à :

- *Une modulation spectralement efficace, c'est-à-dire transportant plus d'informations dans une bande de fréquences moins large (hausse du nombre de bits/Hz)*
- *Un codage de compression de source (parole, données) permettant d'éliminer la redondance d'informations, de manière à réduire le nombre de bits à transmettre dans le temps imparti, et donc de réduire le débit de transmission nécessaire et par là même la largeur de bande nécessaire.*

L'objectif des concepteurs et des opérateurs de réseaux mobiles consiste donc à transmettre le maximum d'informations dans des canaux de largeur de bande fixe.

2.2. Qualité fluctuante des liens radios

Alors que dans un réseau filaire les liens de transmission possèdent en fonctionnement normal une qualité élevée et constante, le lien radio est sujet à de multiples variations dues à la mobilité des usagers et aux changements des caractéristiques de l'environnement: obstacles et réflecteurs en mouvement, interférences et brouilleurs de toutes sortes,....

Ces problèmes se manifestent par un niveau de BER (Bit Error Rate, taux d'erreur binaire) sur le lien radio qui fluctue dans des marges importantes.

2.3. Point d'accès inconnu et variable dans le temps

Contrairement à une connexion filaire où les usagers communiquent via des points d'accès réseau fixes, l'accès à un réseau radio mobile permet à l'utilisateur de changer de point d'accès réseau entre deux connexions et même au cours d'une connexion. Cela suppose donc une gestion de la mobilité à deux niveaux différents :

- Du point de vue réseau pour permettre au système de retrouver un abonné ou qu'il se situe sous la couverture du réseau : gestion de la localisation (paging) ;
- Du point de vue radio pour permettre à une communication de se poursuivre sans interruption lorsque l'abonné se déplace en cours d'appel et change de point d'accès réseau (handover).

2.4. Sécurité

Un dernier aspect lié à l'utilisation du canal radio mobile est sa caractéristique de médium diffusant. Par conséquent, les communications peuvent être écoutées et le canal peut être utilisé par tout le monde (émetteurs pirates). Il est donc nécessaire de réaliser des fonctions de sécurité permettant la confidentialité des communications et l'authentification des terminaux souhaitant accéder au système.

3. La radiotéléphonie dans le monde

3.1. Les systèmes de première génération

Les systèmes de première génération sont analogiques ; le signal de parole est transmis sur la voie radio par une modulation analogique tout à fait classique. La méthode d'accès utilise un simple multiplexage en fréquence. Dans les années 80, de multiples systèmes nationaux ont été mis au point au Japon, en Italie, en Allemagne, aux États-Unis, en Norvège, en Suède et en Finlande,...

En France, l'opérateur national France Télécoms est alors en situation de monopole ; en 1986, il fait développer le système Radiocom 2000. Pour favoriser la croissance de la radiotéléphonie par un système de concurrence, une autorisation d'exploitation est accordée en décembre 1987 à un second opérateur: la Société Française de Radiotéléphone SFR. Un second réseau analogique est donc développé en France, commercialisé sous le nom de "Ligne SFR".

A leur apogée en août 1994, ces deux réseaux analogiques français totalisaient 460 000 abonnées, soit un taux de pénétration de 0,83 %. Ce taux était tout à fait modeste en comparaison des autres pays européens (8 % dans les pays nordiques).

Des le milieu de l'année 1995, le système de deuxième génération GSM, numérique, supprime les réseaux analogiques en France avec plus de 500 000 clients.

Les principales différences entre les systèmes de première génération et les systèmes de deuxième génération sont les suivantes :

- *L'utilisation d'une modulation numérique dans les systèmes de deuxième génération. Les avantages de ce type de modulation sont:*
 - *la robustesse du signal (à qualité égale, le rapport C / I nécessaire est moindre, c'est-à-dire que le signal C résiste mieux aux brouillages);*
 - *la capacité plus élevée (par compression numérique de la parole et par efficacité spectrale de la modulation, ce qui permet de faire "passer" plus d'utilisateurs simultanément)*
- *La montée dans les fréquences utilisées pour les systèmes de deuxième génération. Cette montée permet l'implantation de systèmes à haute densité grâce à la réduction de portée du signal avec la montée en fréquence : la taille réduite des cellules permet d'offrir une capacité plus élevée par unité de surface ;*
- *Un accès multiple à répartition dans le temps TDMA (GSM) ou dans les codes (IS-95 : CDMA) pour les systèmes de seconde génération ;*
- *Une normalisation européenne des systèmes de deuxième génération, qui permet aux différents réseaux nationaux de s'interconnecter.*

3.2. Normalisation par l'ETSI

La condition nécessaire pour offrir un service de téléphonie mobile sur toute l'Europe est de disposer d'une bande de fréquence commune sur l'ensemble du territoire européen.

En 1979, un accord a été conclu au sein du WARC (World Administrative Radio Conférence), dépendant de l'UIT (Union Internationale des Télécommunications), pour ouvrir la bande des 900 MHz aux services mobiles.

En 1982, la CEPT (Conférence Européenne des Postes et Télécommunications) alloue deux sous bandes précises de 25 MHz chacune :

- *Une sous bande de 890 a 915 MHz pour les transmissions des terminaux vers les réseaux (sens montant)*
- *Une sous bande de 915 a 930 MHz pour les transmissions dans le sens inverse (sens descendant)*

et crée un groupe d'étude, le Groupe Special Mobile. L'acronyme GSM sera réinterprète plus tard (1990) pour spécifier un système cellulaire européen.

En France, ce groupe d'étude est présent au CNET et lance le projet MARATHON : Mobiles ayant Accès au Réseau des Abonnes par Transmission Hertzienne Opérant en NUMERIQUE. La France s'oriente donc dès le départ pour un système numérique alors que le choix n'est toujours pas déterminé au niveau européen.

En 1987, le GSM entérine le choix de la transmission numérique avec multiplexage temporel et fréquentiel; le type de modulation, le codage de canal et le codage de la parole sont également choisis et permettent de fixer les bases nécessaires à une élaboration rapide des spécifications.

Cette même année, les exploitants des réseaux de 13 pays européens signent un protocole d'accord MoU (Memorandum of Understanding) pour l'ouverture commerciale du GSM en 1991.

En février 1988, France Télécoms et les opérateurs de 10 autres pays européens lancent un appel d'offres international auprès des industriels pour la réalisation de réseaux pilotes. En

septembre 1988, France Télécoms choisit 2 consortiums qui comprennent chacun un constructeur français (Alcatel et Matra).

Le 25 mars 1991 en France, un arrêté ministériel donne l'autorisation au deux opérateurs des réseaux analogiques, France Télécoms et SFR, de déployer un réseau GSM. Les contraintes sont les suivantes :

- *Ouverture commerciale du service en 1992*
- *70 % de la population couverte en 1995 (soit environ 45 % du territoire)*
- *85 % de la population couverte en 1997 (soit environ 60 % du territoire) et elles furent respectées par les deux opérateurs (ouverture commerciale annoncée en juillet 1992). Les premiers réseaux pilotes ouvrent à la fin de l'année 1991.*

Des 1992, des réseaux ouvrent dans toute l'Europe avec la référence au sigle GSM qui perd alors sa signification française pour l'appellation nettement plus évocatrice de "Global System for Mobile communications".

En 1991, sous l'impulsion des britanniques, les spécifications GSM sont adaptées de façon mineure pour permettre de développer des systèmes dans la bande des 1800 MHz. Ces systèmes sont désignés par le terme DCS 1800, Digital Cellular System, et sont plus ciblés pour des environnements urbains. Ils correspondent à la transposition de la norme GSM dans la bande des 1800 MHz. De manière analogue au GSM 900 MHz, deux sous bandes (de largeur 75 MHz chacune) sont réservées dans certains pays pour le DCS 1800. En septembre 1994, Bouygues Télécoms est sélectionné pour déployer un réseau DCS 1800 sur les grandes villes de France avec l'obligation de couvrir 15 % de la population française dans les 18 mois. Le réseau ouvre commercialement le 29 mai 1996.

En 1995, la phase 2 des recommandations GSM est entièrement publiée par l'ETSI (European Telecommunications Standards Institute); elle unifie les systèmes GSM à 900 MHz et DCS 1800.

En mai 1996, la phase 2+ prévoit des terminaux bimode permettant l'interfonctionnement total GSM 900 - DCS 1800. Elle envisage, entre autres, des nouveaux services supplémentaires comme l'identification d'appels malveillants et des possibilités d'appels de groupe.

3.3. La norme GSM dans le monde

La norme GSM est maintenant adoptée dans de nombreux pays. C'est l'unique norme numérique de téléphonie cellulaire acceptée en Europe. Dans la plupart des autres pays, elle est en concurrence avec d'autres normes de radiotéléphonie numérique, en général originaire des Etats-Unis ou du Japon (IS-95).

Dans le monde, on comptait environ 220 millions d'abonnés GSM (et DCS) en novembre 1999. Le taux de pénétration moyen en Europe de l'Ouest a dépassé la barre des 20 % en septembre 1998 avec un peu plus de 75 millions d'abonnés.

Fin 1999, la barre des 100 millions d'abonnés européens a été largement dépassée. Les données sont les suivantes :

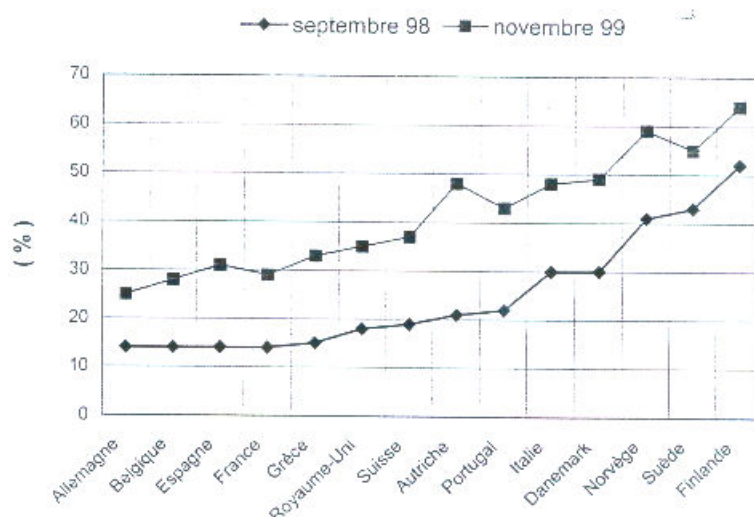


Figure 1 : Taux de pénétration du GSM en Europe

En France, les données sont les suivantes :

		PARC D'ABONNES			
		OPERATEUR	NOV.1998	FIN NOV. 1999	FIN SEP.2000
LIGNES ANALOGIQUES		SFR NMT	40 500	-	-
		Radiocom 2000	12800	fin du service	
GSM 900		SFR-Cegetel	3 664 000	6 367 700	9 169 100
		Itineris (+Ola)	4 897 000	8 656 300	12 571 500

GSM 1800 (DCS)	Bouygues Telecom	1 158 800	2 740 900	4 457 900
-----------------------	------------------	-----------	-----------	-----------

Tableau 1 : Taux de pénétration du GSM en Europe

Le taux de pénétration est de 43,6 % à la fin du mois de septembre 2000 (plus de 26 millions de téléphones portables).

4. Les principales caractéristiques du système GSM

Les différences entre le GSM à 900 MHz et le DCS (à 1800 MHz) ne portent que sur les bandes de fréquences utilisées. Du fait de l'atténuation en espace libre en f2 qui pénalise les hautes fréquences, le déploiement du système DCS est plus contraignant quant à la couverture (il demande une plus grande densité de stations de base), mais la capacité offerte est de ce fait nettement plus élevée et de plus, la largeur de bande disponible est plus confortable.

Les deux systèmes reposent sur une architecture et de interfaces identiques et ne diffèrent que sur l'aspect du déploiement cellulaire. Par la suite, l'appellation "GSM" fera donc allusion aussi bien au GSM 900 qu'au DCS 1800, sauf mention contraire.

4.1 La diversité des services

L'objectif initial était de spécifier un service de téléphonie mobile de voix et de données, compatible avec les réseaux téléphoniques fixes analogiques ou numériques (RNIS ; Réseau Numérique à Intégration de Services). Un réseau GSM permet ainsi toute la palette des services disponibles sur un réseau moderne : voix et données, fax, messagerie,.... De plus, l'utilisation de la carte à puce dans la carte SIM rend la souscription d'un abonnement indépendante de l'achat du terminal.

4.2 Une architecture de réseau spécifié

Pour un interfonctionnement complet (entre les éléments du réseau et entre les réseaux nationaux), il est nécessaire de totalement spécifier les composants, les fonctionnalités et les interfaces du réseau. La norme GSM spécifie ainsi complètement l'architecture du réseau mobile PLMN Public Land Mobile Network, avec une distinction claire entre 2 sous-systèmes:

- *Le sous-système radio*
- *Le sous-système réseau*

Elle ne se limite donc pas à l'interface radio comme la plupart des autres normes radiomobiles. Cette spécification d'ensemble rend possible l'interconnexion des différents réseaux GSM, condition indispensable à une offre de service globale sur l'Europe, voire le monde. Ainsi, un abonné à un réseau GSM donné peut accéder à des réseaux d'autres pays sous réserve d'accord entre les opérateurs de ces pays (et de souscription de l'abonnement International!), sans avoir à faire de démarche administrative et tout en recevant la facture de son opérateur d'origine. Cette possibilité est appelée roaming, ou itinérance internationale.

4.3 Une interface radio élaborée

L'interface radio, qui représente le maillon fragile de la chaîne de transmission reliant un utilisateur mobile au réseau, a été particulièrement étudiée. Tout au long de la chaîne, des traitements permettent l'établissement et le maintien d'un lien en environnement perturbé. En effet, dans un système radiomobile, le lien entre le terminal et le réseau est fluctuant du fait de l'instabilité du canal radio et du déplacement du terminal. Une architecture spécifique est définie sur l'interface radio pour permettre à chaque station mobile de surveiller très périodiquement son environnement. De plus, des procédures liées à l'état "en veille" des mobiles et au "handover" permettent d'assurer une continuité de service analogue à celle du réseau fixe.

5. Architecture du réseau GSM

Le réseau GSM est caractérisé par un accès très spécifique : la liaison radio. Il doit ensuite permettre des communications entre les abonnés mobiles et des abonnés du réseau téléphonique commuté public (RTCP : en France, France Télécoms et depuis le 01/01/1998 le "7" de Cegetel et le "9" de Bouygues Télécoms) et s'interface pour cela avec ce dernier par des commutateurs. Enfin, comme tout réseau, il doit offrir à l'opérateur des facilités d'exploitation et de maintenance. Le réseau GSM est donc séparé en 3 ensembles distincts :

- *Le sous-système radio BSS ;*

Il correspond à la fonction de distribution du réseau de radiocommunication. Il est constitué des stations de base BTS qui assurent le lien radioélectrique avec les abonnés mobiles MS. Les BTS sont gérées par un contrôleur de stations de base BSC qui assure également la fonction de concentration du trafic. En outre, le BSC est connecté à un transcodeur TCU qui permet de diminuer le nombre de liens MIC nécessaires entre le BSS et le NSS ;

➤ *Le sous-système réseau NSS ;*

Il regroupe toutes les fonctions de commutation et de routage, localisées dans le MSC. Les données de référence, propres à chaque abonné, sont enregistrées dans une base de données répartie sur des enregistreurs de localisation nominaux HLR. Le MSC, afin de minimiser les accès aux HLR, utilise un enregistreur de localisation temporaire, le VLR, contenant les données de travail relatives aux abonnés présents dans la zone gérée par le MSC.

➤ *Le sous-système d'exploitation et de maintenance OSS ;*

Il est utilisé par l'opérateur pour administrer son réseau, de manière locale par des OMC et de manière générale par le NMC. Les fonctions de sécurité et de contrôle d'accès au réseau sont assurées par le centre d'authentification AUC et l'enregistreur des identités des équipements EIR.

Le schéma suivant présente l'architecture générale d'un réseau GSM, hormis le système OSS :

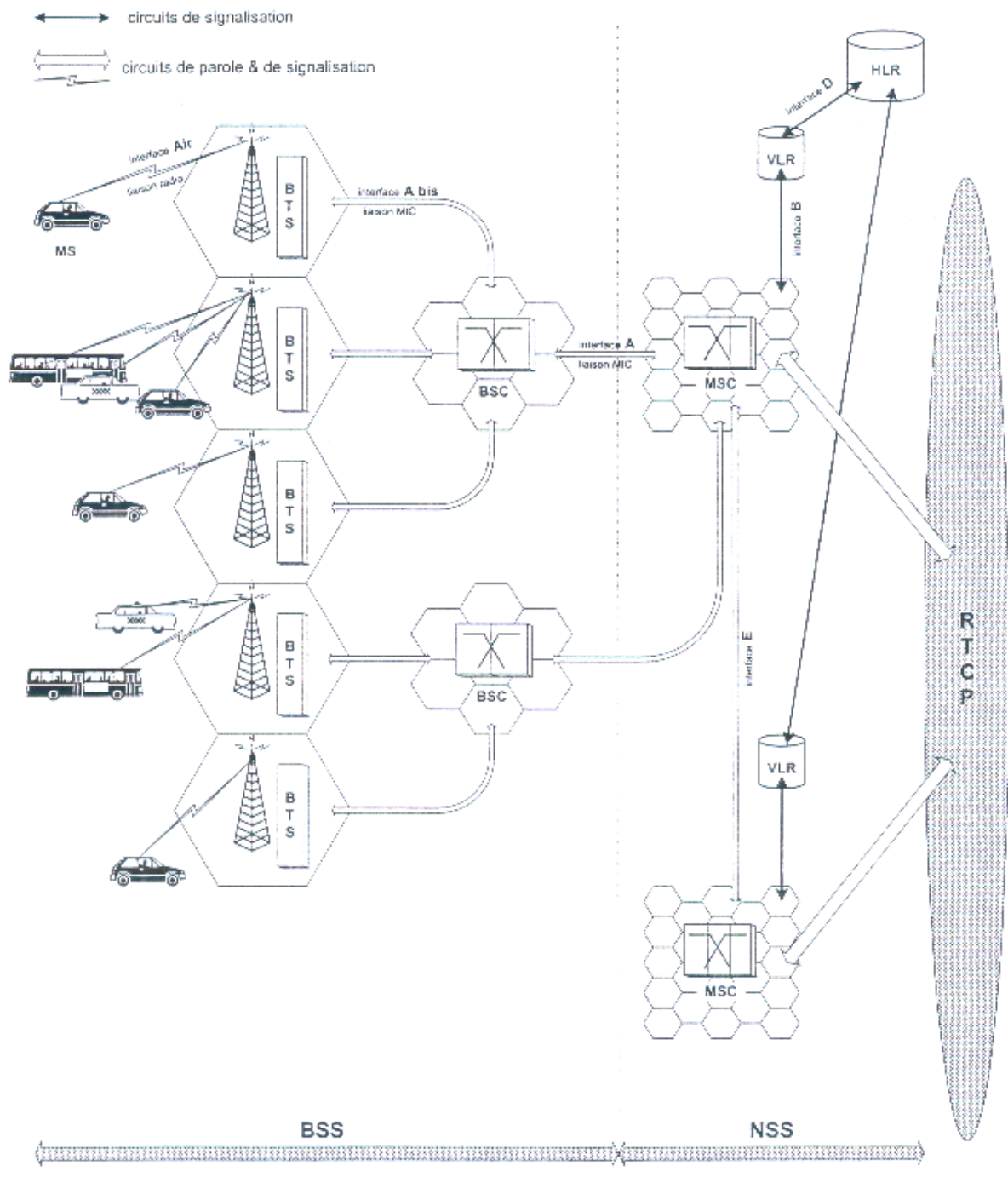


Figure 2. Architecture générale d'un réseau GSM

5.1. Le sous-système radio : BSS

5.1.1. La station de base : BTS

La BTS (Base Transceiver Station) est un ensemble d'émetteurs- récepteurs appelés TRX. Dans une première approche, un TRX peut être vu comme un couple de fréquences (f_{montante} ; $f_{\text{descendante}}$) sur lequel 8 communications bidirectionnelles simultanées peuvent être écoulées.

Le rôle de la BTS est d'assurer l'interface entre le réseau fixe et les stations mobiles. La communication avec les mobiles se fait par l'interface radio aussi appelée interface Um. La communication avec le réseau fixe, via le BSC, se fait par une interface filaire appelée interface A_{bis}. Le transport des canaux de signalisation, de données et de parole s'effectue sur des liaisons MIC à 2 Mbits/s (32 IT à 64 kbits/s). La BTS a la charge de la transmission radio : modulation, démodulation, égalisation, codage correcteur d'erreur. Elle gère plus généralement la couche physique : multiplexage TDMA, saut de fréquence (lent) et chiffrement. Elle réalise aussi l'ensemble des mesures nécessaires pour vérifier qu'une communication en cours se déroule correctement et transmet directement ces mesures au BSC, sans les interpréter. Elle s'occupe en outre de la couche liaison de données pour l'échange de signalisation entre les mobiles et l'infrastructure ainsi que pour assurer la fiabilité du dialogue.

Il existe deux types de BTS ; les macro BTS classiques et les micros BTS. Ces dernières sont prévues pour assurer la couverture de zones urbaines denses à l'aide de microcellules. Ce sont des équipements de faible taille, de moindre puissance, moins chers et pouvant être placés à l'extérieur des bâtiments.

Suivant le type d'environnement à couvrir (urbain dense, suburbain, rural), les BTS comportent un plus ou moins grand nombre de TRX. Plus la densité de trafic est importante (urbain dense), plus chaque BTS doit écouler un trafic important et donc plus elle nécessite des TRX.

Le minimum est bien sûr de 1 TRX, le maximum est déterminé par les constructeurs qui proposent des configurations adaptées au trafic ; il est donc en constante évolution.

Exemple 1998 :

Nokia : les BTS peuvent gérer jusqu'a 6 TRX.

NMC : les BTS peuvent gérer jusqu'a 8 TRX.

Si le mobile se trouve près d'une BTS, la norme prévoit que le mobile ou la BTS peuvent diminuer leur puissance d'émission. C'est le contrôle de puissance (power control). Les BTS sont connectées à leur contrôleur BSC :

- soit en étoile (1 MIC par BTS),
- soit en chaîne (1 MIC est partagé par plusieurs BTS),
- soit en boucle (liaison en chaîne fermée permettant la redondance : une liaison MIC coupée n'isole pas de BTS).

Cette dernière technique de connexion, dite de "drop and insert" permet de sécuriser la connexion des BTS au BSC et de réduire le nombre et la longueur des liaisons MIC nécessaires sur l'interface Abis.

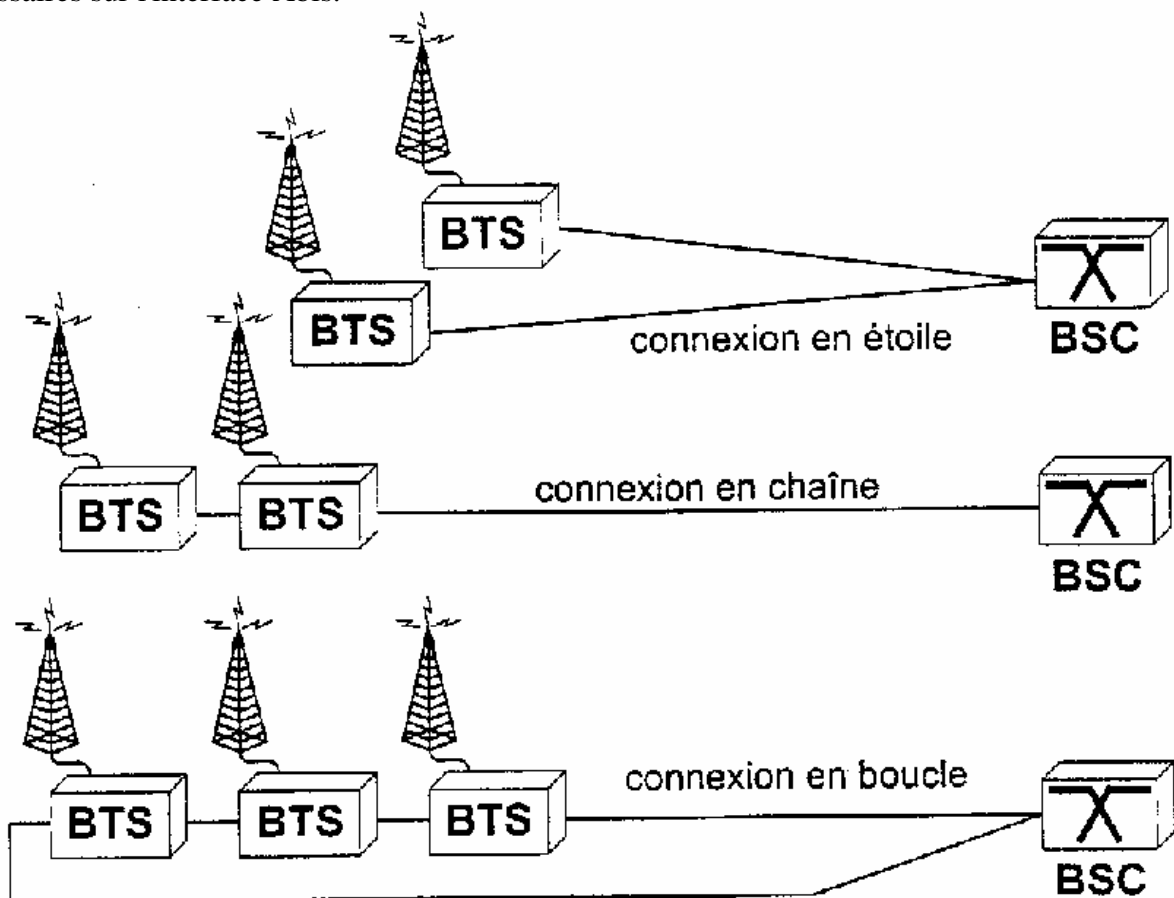


Figure 3 : Types de connexions BTS - BSC

5.1.2. Le contrôleur de station de base : BSC

Le BSC (Base Station Controller) est l'organe intelligent du BSS. Il gère les ressources radio des BTS qui lui sont attachées. Il réalise pour cela les procédures nécessaires à l'établissement ou au rétablissement des appels et à la libération des ressources à la fin de chaque appel, ainsi que les fonctions propres aux communications (contrôle de puissance, décision d'exécution et gestion du handover).

Il assure en outre une fonction de concentration des liaisons MIC vers le MSC. Initialement, les constructeurs de BSC n'ont pas eu tous la même philosophie concernant la capacité de trafic de ces éléments :

➤ *des BSC de faible capacité,*

*gérant un moins grand nombre de BTS « il faut donc davantage de BSC pour couvrir la même surface »
minimisant ainsi les distances BTS-BSC « réduction du coût d'exploitation pour l'opérateur »
particulièrement adaptés aux zones rurales faiblement peuplées*

➤ *des BSC de forte capacité*

*gérant un plus grand nombre de BTS
augmentant donc les distances BTS-BSC moyennes
particulièrement adaptés aux zones urbaines à forte densité de trafic*

Exemple 1998 :

Nokia : les BSC peuvent gérer 256 TRX chacun, soit par exemple 64 BTS à 4 TRX.

NMC : les BSC peuvent gérer 160 TRX chacun, soit par exemple 40 BTS à 4 TRX.

Fin 2000, chaque BSC pourra écouler jusqu'à 3000 Erlangs.

5.1.3. Le transcodeur : TCU

Les abonnés transmettent des informations à des débits de 13 kbits/s (parole plein débit) qui sont ensuite adaptées et transportées à partir de la BTS à 16 kbits/s. Or le réseau fixe, qui est le plus souvent numérique, gère des circuits de parole à 64 kbits/s. Il est donc nécessaire de réaliser dans le réseau un transcodage 16 kbits/s \Leftrightarrow 64 kbits/s. La norme n'impose pas d'implanter les transcodeurs en un endroit particulier du réseau mais les place forcément dans le BSS. Or, il est logique de transcoder les informations le plus tard possible, c'est-à-dire le plus près possible du MSC pour économiser les circuits de parole.

Le TCU ou TRAU {Transcoder and Rate Adaptor Unit) a donc été placé entre le BSC et le MSC dans le but de réduire le nombre des liaisons MIC nécessaires à la transmission des informations entre la BTS et le BSC. Il est généralement placé physiquement à côté du MSC mais fait fonctionnellement partie du BSC qui le commande donc à distance.

Les informations sont "physiquement" transmises sur des circuits MIC à 64 kbits/s (hormis sur l'interface radio entre le mobile et la BTS). Sur chaque circuit MIC, il est donc possible de transporter les informations de 4 circuits de parole à 16 kbits/s.

L'adaptation de débit nécessaire étant justement de 16 à 64 kbits/s (et inversement dans le sens descendant), le TCU comporte donc 1 liaison MIC vers le BSC pour 4 liaisons vers le MSC.

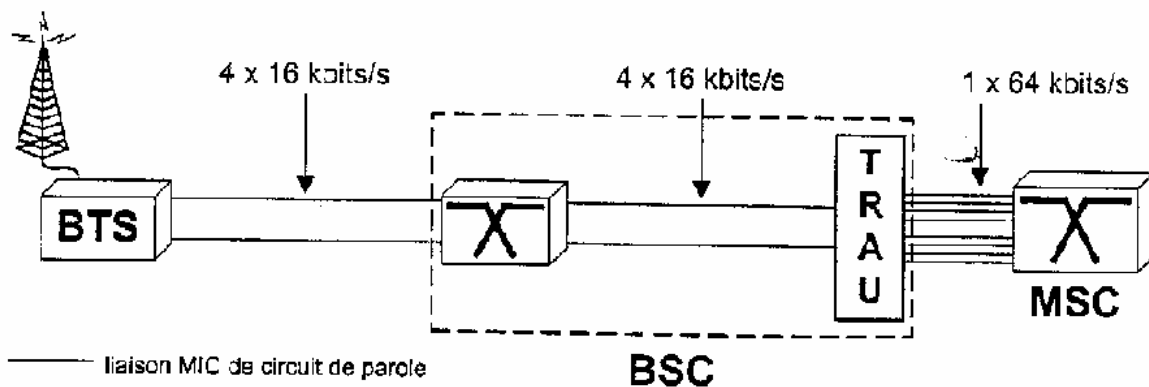


Figure 4: Transcodage de la parole

5.2. Le sous-système réseau : NSS

5.2.1. Le commutateur (G)MSC

Le commutateur du réseau mobile MSC {Mobile-services Switching Centre) assure l'interface entre le réseau mobile et les réseaux publics déjà implantés en cas d'appels entrants : il s'appelle alors GMSC (Gateway MSC). Il assure la commutation des appels et constitue le point de commande des tâches de mise à jour de la localisation des mobiles et du transfert des appels.

Il commande les appels en provenance et à destination du Réseau Téléphonique Public Commuté RTCP, du Réseau Numérique à Intégration de Services RNIS (Numeris), des réseaux publics mobiles PLMN (SFR, Itineris, Bouygues Télécoms), des réseaux publics de données PSDN (Transpac).

Le (G)MSC est essentiellement chargé de l'établissement des appels (réservation des ressources, procédures d'identification et d'authentification, acheminement vers l'abonné appelé, commutation sur les circuits dédiés à la communication,...) entre un mobile et le réseau, de la taxation des appels et de la transmission des messages courts. Il intervient aussi dans certaines procédures de handover.

5.2.2. L'enregistreur de localisation : HLR

Le HLR {Home Location Register} est la base de données qui gère les abonnés d'un PLMN donne. Il mémorise les caractéristiques de chaque abonné :

- *L'identité internationale de l'abonné : IMSI, unique, fixe et secrète, utilisée par le réseau,*
- *Le numéro d'annuaire à 12 chiffres de l'abonné : MSISDN, commençant par 33 06 en France,*
- *Le profil de l'abonnement (services supplémentaires souscrits, autorisation d'appel à l'international,...),*
- *Un triplet (Kc, SRES, RAND) fourni au VLR, puis au MSC, lors de la procédure d'authentification de l'abonné,*
- *La localisation de l'abonné, c'est-à-dire le MSC / VLR ou il est enregistré actuellement, même si c'est sur un PLMN étranger (utile en cas de recherche de cet abonné : le réseau s'adresse directement au HLR pour savoir où se trouve l'abonné et s'il est joignable).*

Un HLR peut gérer plusieurs centaines de milliers d'abonnés et il constitue une machine spécifique. A chaque abonné est associé un HLR unique ; le réseau identifie le HLR à partir du numéro MSISDN ou de l'identité de l'abonné.

5.2.3. L'enregistreur de localisation des visiteurs : VLR

Le VLR (Visitor Location Register) est une base de données qui mémorise les informations d'abonnement des abonnés présents dans une certaine zone géographique. Plusieurs MSC peuvent être reliés au même VLR, mais un MSC ne peut être qu'à un seul VLR et en général, à un VLR correspond un seul MSC. Les données mémorisées par le VLR sont les mêmes que celles du HLR, mais concernent un sous-ensemble d'abonnés : ceux présents dans la zone considérée. De plus, le VLR contient pour chaque abonné :

- *Son identité temporaire TMSI (variable au cours du temps, parfois d'une connexion à l'autre);*
- *Sa localisation plus précise : sa zone de localisation.*

La séparation matérielle entre le VLR et le MSC n'est pas très précise. On parle souvent de l'ensemble MSC / VLR car si le MSC possède toutes ses fonctionnalités de commutation et d'établissement d'appel, c'est grâce aux informations fournies par le VLR. Un ensemble MSC / VLR peut gérer une centaine de milliers d'abonnés.

5.3. Le sous-système d'exploitation et de maintenance : OSS

L'administration de réseau comprend toutes les activités qui permettent de mémoriser et de contrôler les performances et l'utilisation des ressources de façon à offrir un certain niveau de qualité aux usagers. Les différentes fonctions d'administration comprennent:

- *L'administration commerciale (déclaration des abonnés, des terminaux, facturation,...) ;*
- *La gestion de la sécurité (intrusion);*
- *L'exploitation et la gestion des performances (observation du trafic et de la qualité, charge du réseau,...)*
- *Le contrôle de la configuration du système (mise à jour des logiciels d'évolution et des nouvelles fonctionnalités, introduction dans le réseau de nouveaux équipements);*
- *La maintenance (tests des équipements)*

5.3.1. L'administration du réseau : OMC et NMC

La diversité des équipements présents dans un réseau GSM tant par leur type (émetteurs-récepteurs, commutateurs, bases de données) que par le nombre de fournisseurs (au moins 2 pour faire jouer la concurrence) pousse à adopter une approche structurée et hiérarchique de la supervision du réseau. La norme présente 2 niveaux :

- *Les OMC Opérations & Maintenance Centre;*
- *Le NMC Network Management Centre.*

Le NMC permet l'administration générale de l'ensemble du réseau par un contrôle centralisé, alors que les OMC permettent une supervision locale des équipements. Plusieurs OMC vont,

par exemple, superviser des ensembles de BSC et de BTS sur différentes zones. D'autres OMC vont superviser les MSC-VLR. Les incidents mineurs sont transmis aux OMC qui les filtrent, tandis que les incidents majeurs remontent jusqu'au NMC.

5.3.2. L'enregistreur d'identité des équipements : EIR

L'EIR (Equipment Identity Register) est une base de données contenant les identités des terminaux IMEI. Elle peut être consultée lors des demandes de services d'un abonné pour vérifier que le terminal utilisé est autorisé à fonctionner sur le réseau.

L'accès au réseau peut être refusé parce que le terminal n'est pas homologué, qu'il perturbe le réseau ou bien parce qu'il a fait l'objet d'une déclaration de vol.

L'EIR peut contenir 3 listes :

- *Une liste blanche de l'ensemble des numéros d'homologation ;*
- *Une liste noire des équipements volés et interdits d'accès. Le réseau peut mémoriser l'identité IMSI d'un abonné utilisant un terminal inscrit sur cette liste et la transférer au système d'administration pour permettre d'identifier les accès frauduleux (cela ne sert donc à rien de voler un terminal GSM !);*
- *Une liste grise des terminaux présentant des dysfonctionnements insuffisants pour justifier une interdiction totale,*

5.3.3. Le centre d'authentification : AUC

L'AUC (AUthentication Centre) mémorise pour chaque abonné une clé secrète Ki utilisée pour authentifier les demandes de service et chiffrer les communications. De plus, il contient les algorithmes d'authentification et de Chiffrement (algorithmes A3 et AS) utilisés sur le réseau. Un AUC est généralement associé à chaque HLR. L'ensemble peut même parfois être intégré dans un même équipement: la sécurité relative au transfert des informations entre ces deux entités fonctionnelles distinctes est alors optimale.

5.4. La station mobile : MS

La station mobile Mobile Station désigne un équipement terminal muni d'une carte SIM qui permet d'accéder aux services de télécommunications d'un réseau mobile GSM.

La carte SIM d'un abonné est généralement du format d'une carte de crédit ("full sized"), parfois même juste du format de la puce ("plug-in"). Elle contient toutes les informations nécessaires au bon fonctionnement du mobile :

- *Ses identités IMSI et TMSI,*
- *Éventuellement un code PIN (bloquant la carte après 3 essais, équivalent du code de la carte bleue),*
- *Sa clé de chiffrement Kc ,*
- *Sa clé d'authentification Ki,*
- *Les algorithmes de chiffrement (A8, qui génère Kc, et A5) et d'authentification A3.*

Le terminal est muni d'une identité particulière, l'IMEI Cette identité permet, en autres, de déterminer le constructeur de l'équipement.

La norme définit plusieurs classes de terminaux suivant leur puissance maximale d'émission. Cette puissance conditionne bien sur leur portée. La majorité des terminaux vendus sont des portatifs d'une puissance de 2 W pour GSM 900, de 1 W pour DCS 1800.

5.5. Architecture en couches

5.5.1. Les principales interfaces

Une interface est le lien entre 2 entités du réseau, sur lequel transitent des informations particulières.

Par exemple, la BTS et le BSC sont connectés, il existe donc une interface entre ces deux entités, mais le HLR n'est pas directement lié à la BTS, donc il n'existe pas d'interface entre ces deux entités.

Chaque interface, désignée par une lettre, est totalement spécifiée par la norme, c'est-à-dire que les informations sont transmises dans des messages précis, sous un format et à un emplacement du message précis, à des moments précis.

Cela permet théoriquement d'utiliser les équipements de différents constructeurs sans aucune incompatibilité. L'interface à respecter de façon impérative est l'interface D car elle permet à

un MSC / VLR de dialoguer avec le HLR de tout autre réseau. Sa conformité avec la norme permet donc l'itinérance internationale. L'interface A sépare le NSS du BSS. La conformité du BSC et du MSC à la recommandation permet aux opérateurs d'avoir différents fournisseurs pour le NSS et le BSS.

NOM	LOCALISATION	UTILISATION
Um ou Air ou Radio	MS –BTS	interface radio
Abis	BTS – BSC	divers
A	BSC – MSC	divers
B	MSC – VLR	divers
E	MSC – MSC	exécution de certains handovers
D	VLR – HLR	gestion des informations d'abonnés et de localisation, services supplémentaires.

Tableau 2 : Résumé des principales interfaces, du réseau GSM, nécessaires de connaître.

5.5.2. Le sous-système radio

La recommandation GSM établit un découpage des fonctions et une répartition de celles-ci sur divers équipements. Par exemple, les handovers seront pris en charge par diverses entités selon le type de handover effectué et les différentes phases de celui-ci. La structure en couches reprend ce découpage en respectant la philosophie générale des couches OSI.

Dans le BSS, on retrouve principalement les trois couches basses de l'OSI : couche physique, couche liaison de données et couche réseau, cette dernière étant découpée en plusieurs sous-couches qui concernent plusieurs interfaces.

La couche 1 ou couche physique définit l'ensemble des moyens de transmission et de réception physique de l'information (traitement bit par bit). Sur les interfaces A et Abis, la transmission est numérique, le plus souvent sur des voies MIC à 64kbits/s. Sur l'interface radio, cette couche est plus compliquée du fait des nombreuses opérations à effectuer : codage correcteur d'erreurs, multiplexage des canaux logiques, mesures radios à effectuer.

La couche 2 ou liaison de données a pour objet de fiabiliser la transmission entre deux équipements par un protocole dit de fiabilisation (traitement trame par trame). Les protocoles

adoptés sur le BSS comportent un mécanisme d'acquittement et de retransmission des trames et sont assez similaires au protocole HDLC. Ces protocoles sont: sur la liaison Abis, le LAPD (utilise dans le RNIS) et entre la MS et la BTS, la spécificité de la couche physique requiert un protocole dérivé du LAPD : le LAPDm (m pour mobile).

La couche 3 où couche réseau a pour objet d'établir, de maintenir et de libérer des circuits commutés (parole ou données) avec un abonné du réseau fixe. Cette couche est divisée en 3 sous-couches :

- *La sous-couche Radio Ressource RR intègre l'ensemble des aspects purement radios : établissement, maintenance et libération des différents canaux logiques. Dans la MS, elle a pour rôle de sélectionner les cellules et de surveiller leur voie balise. La plupart des messages RR transitent par la BTS sans interprétation et sont directement traités par le BSC ou la MS : chiffrement, basculement du mobile vers un canal dédié à sa communication, exécution du handover,.... Cependant, certains messages, comme par exemple l'ordre d'activation d'un TRX, concernent directement la BTS et sont échangés d'abord entre le BSC et la BTS, puis entre la BTS et la MS. Pour cela, la BTS comporte donc une première entité appelée BTS Management pour traiter les commandes en provenance du BSC (entité que l'on retrouvera donc dans le BSC) et une seconde entité appelée RR' pour dialoguer avec le mobile. Cette entité RR est comprise dans la sous-couche RR du mobile.*
- *La sous-couche Mobility Management MM gère l'itinérance de la MS. Elle prend donc en charge la mise à jour de localisation du mobile, l'authentification et l'identification de l'abonné, l'allocation du TMSI et la demande de service (en cas d'appel sortant).*
- *La sous-couche Connections Management CM est elle-même découpée en 3 parties :*

*L'entité Call Control CC traite la gestion des connexions de circuits avec le destinataire final: établissement et fin d'appel, modifications en cours d'appel,
L'entité Short Message Service SMS assure la transmission et la réception des messages courts,
L'entité Supplementary Services SS gère les services supplémentaires.*

Les sous-couches CM et MM ne sont pas gérées au sein du BSS, L'ensemble des messages CM et MM transitent par la BTS et par le BSC sans être analysés.

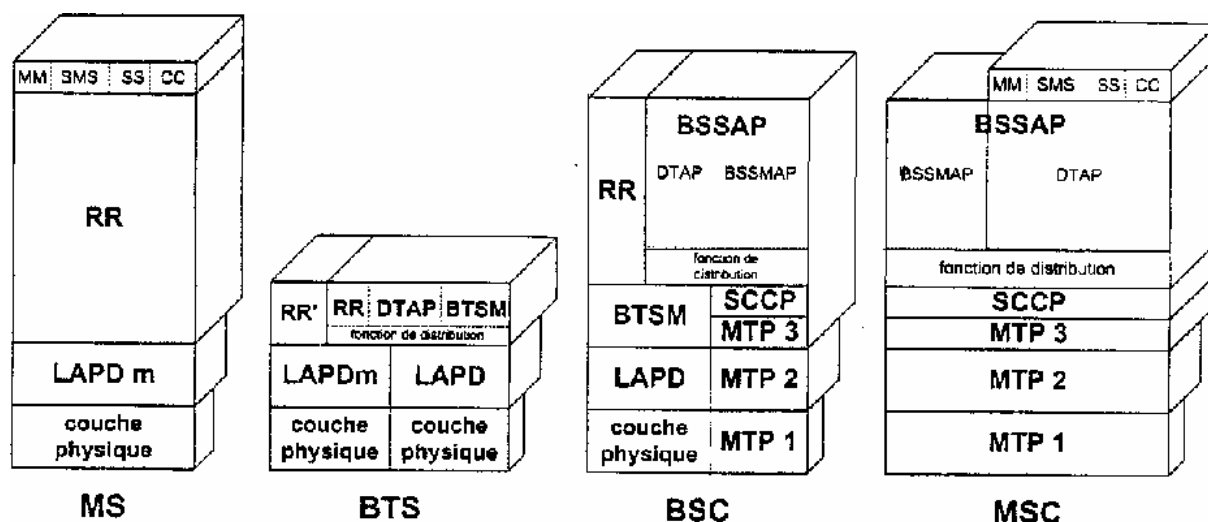


Figure 5. : Empilement des protocoles dans le BSS

5.5.3 Le sous-système réseau

L'échange de signalisation au sein du NSS se fait en utilisant la Signalisation Sémaphore n°7 SS7. Cette signalisation n'est pas détaillée dans ce polycopie car elle ne concerne pas le système GSM en particulier : elle définit un standard au niveau mondial, optimisé pour les réseaux numériques, d'un haut niveau de fiabilité et évolutif pour convenir à l'élaboration de services futurs. Par opposition à la signalisation voie par voie, la signalisation par canal sémaphore peut se définir comme une méthode dans laquelle une seule voie, le "canal sémaphore", achemine, grâce à des messages étiquetés, l'information de signalisation se rapportant à une multiplicité de circuits de parole.

Les avantages de la SS7 sont les suivants :

- *la possibilité de transférer de la signalisation pure indépendamment de l'établissement d'un circuit,*
- *la possibilité de transférer la signalisation à fort débit pendant une communication sans que l'utilisateur ne soit gêné,*
- *la possibilité de réserver les circuits pour un appel seulement lorsque le correspondant demandé est réellement joignable.*

La gestion de l'itinérance nécessite le développement du protocole Mobile Application Particular au GSM et gérant les dialogues entre les équipements du NSS.

Le protocole Message Transfer Part MTP en est une application aux 3 premières couches du modèle OSI. Il est implanté dans les MSC, VLR et HLR et offre un service de transfert fiable des messages de signalisation repartit sur 3 niveaux :

- *Le niveau 1 définit les caractéristiques physiques, électriques et fonctionnelles de la liaison et les moyens d'y accéder. Les supports utilisés sont en général les conduits numériques MIC à 64 kbits/s,*
- *Le niveau 2 définit les fonctions et les procédures de transfert des messages de signalisation de façon à fournir un transfert fiable entre deux points. Il contient un mécanisme de contrôle de flux, de détection d'erreur et de correction par retransmission ;*
- *Le niveau 3 définit une fonction de routage au sein du réseau SS7 national et une fonction de gestion du réseau. La gestion du réseau est effectuée par des procédures de rétablissement et de maintien des conditions normales de fonctionnement. Elles peuvent avoir pour effet de détourner le trafic de signalisation sur un ou plusieurs canaux de secours. Pour détecter les défaillances, elles utilisent les informations de surveillance répercutées par le niveau 2.*

De même, les protocoles *Signalling Connection Part SCCP* et *Transaction Capabilities Application Part TCAP* sont implantés à partir du BSC et sont utilisés pour offrir l'itinérance internationale et l'échange de signalisation non liée à l'établissement d'un circuit.

Le protocole de gestion d'appel, le SSUTR2 en France ou VISUP dans d'autres pays, est utilisé pour l'établissement des appels entre les différents MSC / VLR du réseau GSM et avec les centraux du réseau fixe.

Enfin, entre le BSC et le MSC, une des applications du MAP, le *BSS Application Part BSSAP* permet, grâce à deux nouveaux protocoles :

- *l'échange des messages de gestion du lien BSC - MSC par le BSSMAP ;*
- *l'encapsulation des messages des couches MM et CM par le protocole Direct Transfer Application Part DTAP, rendant ainsi le BSC transparent aux messages échangés entre la MS et le MSC.*

6. Canaux radios

6.1 Structure des canaux

Un système radio mobile a besoin d'une partie du spectre radio pour fonctionner. Avant de le spécifier en détail, les concepteurs du système doivent demander une bande de fréquence auprès de l'instance officielle chargée de la gestion du spectre. Les bandes dédiées par l'UIT, d'où une reconnaissance au niveau mondial, au système GSM sont spécifiées dans le tableau suivant:

	GSM 900	DCS 1800
bandes de fréquences MHz	890 - 915 (Up) 935 - 960 (Down)	1710-1785 (Up) 1805-1880 (Down)
largeur de bande	2 x 25 MHz	2 x 75 MHz
écart duplex	45MHz	95MHz
nb intervalles de temps par trame TDMA	8	
rapidité de modulation	~ 271 kbits/s	
Débit de la parole	13/12,2 et 5,6 kbits/s	
accès multiple	multiplexage temporel et fréquentiel	
puissance des terminaux	2 et 8W	0,25 et 1 W

Tableau 3-1 : Caractéristiques fréquentielles

6. 2 Rappels:

6. 2. 1 Écart duplex et canal duplex

L'écart duplex du système GSM est le décalage en fréquence entre la voie montante (du mobile vers la BTS) et la voie descendante (de la BTS vers le mobile). Cette séparation entre les voies montantes et descendantes facilite le filtrage et la séparation des voies.

Un canal est donc dit duplex s'il comporte une voie montante et une voie descendante. Dans le système GSM, tous les canaux de trafic alloués aux abonnés sont duplex (il faut pouvoir parler sur la voie montante et écouter sur la voie descendante).

6. 2. 2 Partage en fréquence :

Chaque bande de fréquences est partagée en canaux (ou porteuses) duplex de largeur 200 kHz. La bande GSM 900 dispose donc de 125 canaux montants et autant de canaux descendants, la bande DCS 1800 de 375 canaux montants et autant de canaux descendants. En réalité, 124 et 374 porteuses sont disponibles dans les systèmes GSM 900 et DCS 1800.

Numérotation des porteuses :

GSM 900 : pour $1 \leq n \leq 124$ $f = 935 + (0,2 \times n)$ MHz

DCS 1800 : pour $512 \leq n \leq 885$ $f = 1805,2 + [0,2 \times (n - 512)]$ MHz

Itineris dispose des 62 premiers canaux duplex de la bande GSM 900 et SFR des 62 derniers, tandis que Bouygues Telecom dispose des 75 derniers canaux de la bande DCS 1800. Dans la suite, le terme "fréquence" désignera le plus souvent le numéro de la porteuse (entre 811 et 885 pour Bouygues Telecom) et non la valeur exacte de la fréquence en MHz.

6. 2. 3 Partage en temps :

Chaque porteuse est divisée en 8 intervalles de temps (IT, slots ou timeslots). La durée de chaque timeslot est fixée à 577 us (environ). Sur une même porteuse, les timeslots sont regroupés par 8 en une trame TDMA. La durée de cette dernière est donc 4,615 ms. Les timeslots sont numérotés de 0 à 7.

Chaque utilisateur plein débit utilise un slot par trame TDMA (toutes les 2 trames TDMA pour un utilisateur demi- débit). Un "canal physique" est donc constitué de la répétition périodique d'un slot de la trame TDMA sur une fréquence particulière. Dans ce slot, qui a une notion temporelle, l'élément d'information est appelé burst. On dit que le GSM est orienté circuit: il réserve à chaque utilisateur une portion des ressources (1 timeslot parmi 8 sur une paire de fréquences), qui n'est partagée avec personne d'autre, jusqu'à la de connexion de l'utilisateur.

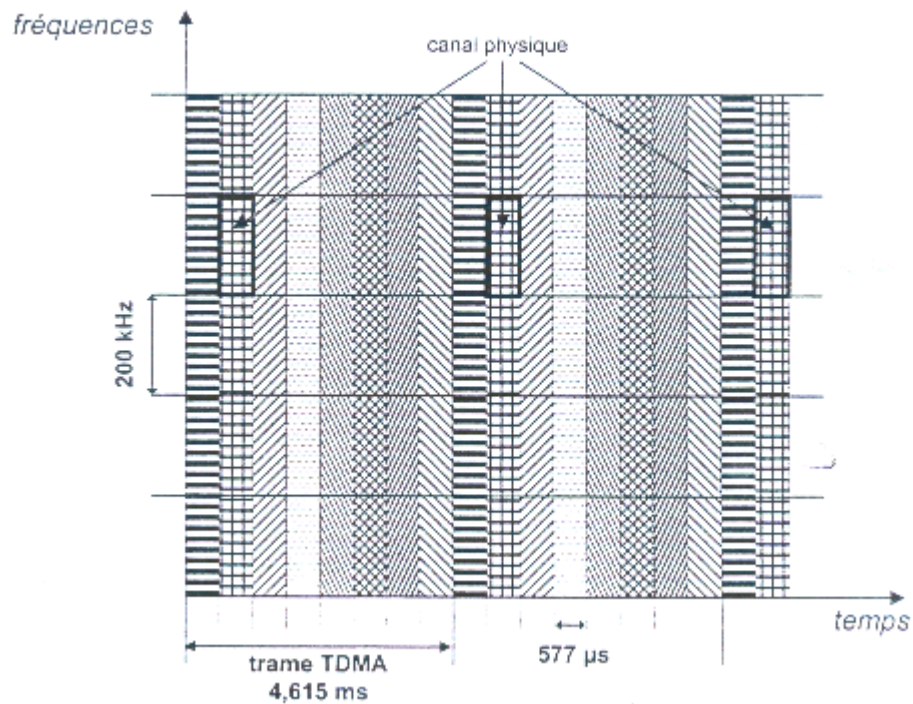
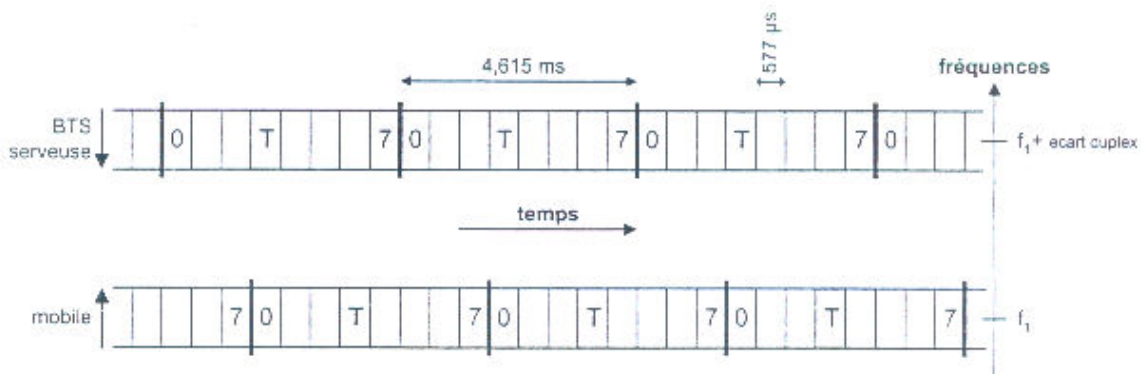


Figure 5-1 : Partage en temps et en fréquence d'une bande de fréquences GSM

On peut donc dire que le GSM est un système F/TDMA puisque les ressources sont partagées en fréquence et en temps.

Enfin, dans le système GSM, un mobile émet et reçoit à des instants différents. Au niveau du canal physique alloué au mobile, l'émission et la réception d'informations sont donc décalées dans le temps de 3 timeslots :



T : Canal TCH de trafic alloué à un utilisateur

Figure 5-2 : Canal physique GSM pour une transmission duplex sans saut de fréquence

6.3 Structure des informations

6.3.1 Codage des informations

Suivant la nature de l'information à transmettre, les messages d'information n'ont pas la même longueur ni la même protection.

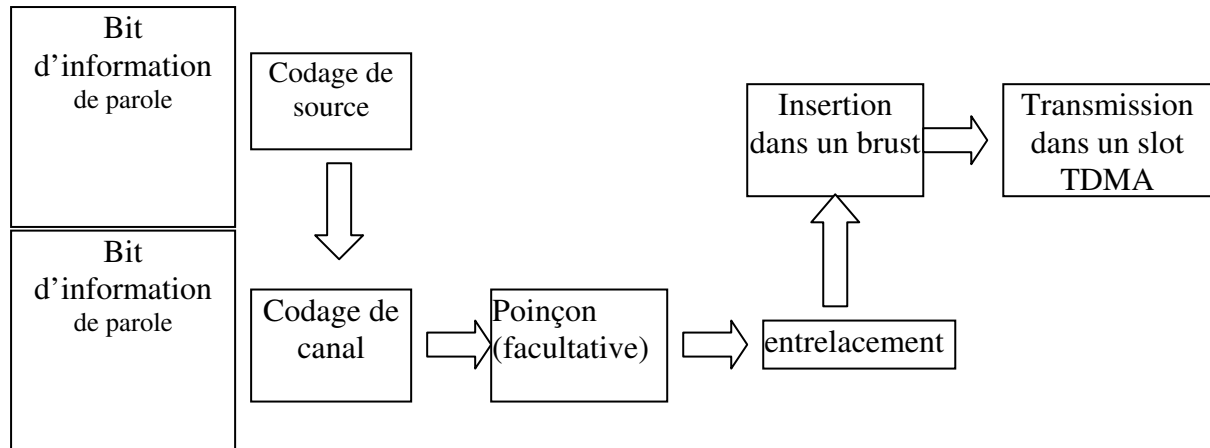


Figure 6-1 : Chaîne de transmission

La modulation utilisée dans le système GSM est la modulation GMSK (Gaussian-filtered Minimum Shift Keying). Ses principales caractéristiques sont les suivantes :

- modulation de fréquence ;
- variation linéaire de la phase sur un temps bit provoquant un déphasage de $\pm\pi/2$ à chaque transmission de symbole ;
- débit en ligne : 270, 833 kbits/s (156,25 bits transmis en 577 μ s);

Le codage de source de la parole sert à transformer le signal analogique de parole en un signal numérique. Le but de ce codage est de réduire le débit de façon à minimiser la quantité d'information à transmettre. En effet, dans le système GSM, à la sortie de ce codeur, ne sont transmis que les coefficients des filtres numériques linéaires (long terme LTP et court terme LPC) et le signal d'excitation (RPE) et non pas le signal de parole initial. L'élément qui effectue ces opérations en émission et en réception est appelé un "codec".

Pour la parole plein débit, les 260 bits en sortie du codeur de source sont repartis en 3 classes suivant leur importance, et le codage de canal n'est appliqué qu'aux classes qui doivent être les plus protégées, c'est-à-dire les deux premières.

Les bits de CRC (Cyclic Redundant Control) sont utilisés pour la détection d'erreurs ; pour la parole, si les 3 bits de CRC indiquent une erreur toute la trame est rejetée; pour les canaux de contrôle, les 40 bits de CRC ont en plus une légère capacité de correction d'erreur.

Les bits de traînée sont utilisés pour vider le registre à décalage du codeur de canal.

Le codage de canal sert à protéger contre les erreurs en introduisant de la redondance. Ceci conduit à une augmentation du débit, mais cette redondance est utilisée en réception pour corriger les erreurs.

Le codage de canal est réalisé par des codes convolutionnels qui, avec l'algorithme de Viterbi, assurent une correction efficace d'erreurs. Le codeur de canal utilisé en GSM est de taux 1/2,

Le poinçonnage est un élément facultatif de la chaîne d'émission. Il consiste à supprimer un certain nombre de bits dans le train de bits codes prêts à être entrelacés, Ceci est fait dans le but de faire "rentre" le train de bits codes dans une boîte du format voulu, 456 bits en l'occurrence pour les données GSM. Tous les bits supplémentaires devront être éliminés. Cependant, si un train de bits a une longueur de $(456 + n)$ bits, il est hors de question de lui enlever les n derniers bits codes : cela supprimerait toute la dernière partie des informations. On enlève donc les n bits régulièrement tout au long du train de bits, et on compte sur la redondance et les performances du récepteur pour corriger les effacements qui ont été ainsi "volontairement" introduits et dont le récepteur connaît l'emplacement.

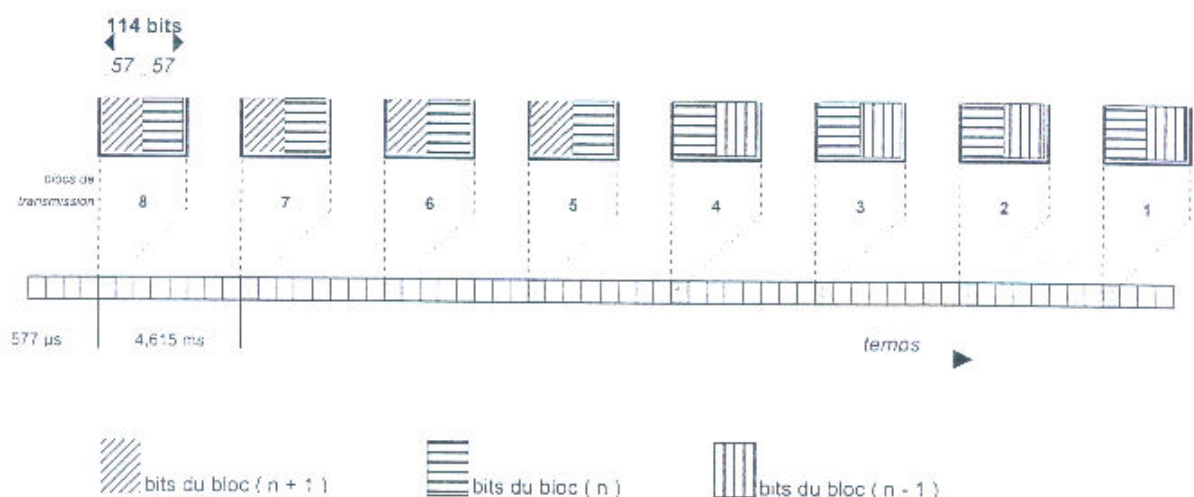


Figure 6-2 : Poinçonnage

L'entrelacement est utilisé pour rendre plus aléatoire les positions des erreurs qui arrivent généralement en salves dans le contexte radio du fait des divers obstacles auxquels sont soumis les signaux radios : immeubles, camions, feuillage...

La technique consiste à mélanger les bits codes avant leur transmission dans un burst pour augmenter les performances de correction des codes correcteurs. En fait l'entrelacement permet de fragmenter les paquets d'erreurs et de les transformer en erreurs "isolées" afin de faciliter leur correction.

6.3.2 Structure d'un burst d'information

Le burst d'information le plus couramment utilisé a la structure générale suivante: une séquence d'apprentissage, des bits de données et quelques bits supplémentaires. La séquence d'apprentissage se trouve au milieu du burst car le canal radio étant fluctuant, il faut mieux estimer le canal à cet endroit; cela donne une estimation à un demi-burst près et non à un burst près comme ce serait le cas si la séquence était placée en fin ou en début de burst. Il existe 8 séquences d'apprentissage sur le réseau, qui correspondent chacune à un code BSIC de BTS.

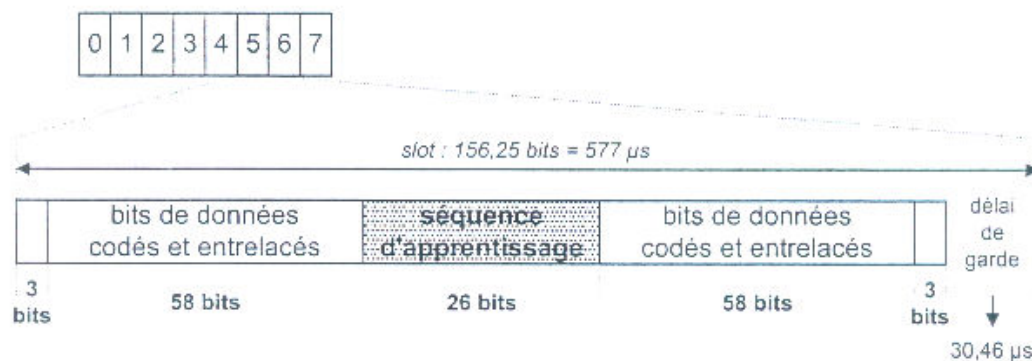


Figure 6.3: Format d'un burst normal

En réalité, il n'y a que 57 bits d'information de part et d'autre de la séquence d'apprentissage : le 58^{ème} bit est utilisé pour indiquer un transfert spécial de signalisation sur le canal logique FACCH.

Dans le cas général (cf. Tableau 6.2), l'entrelacement des 456 bits se fait sur 8 demi-bursts. Il se fait de la manière suivante :

- les 456 bits de chaque bloc sont mélangés suivant un ordre défini par la norme ;

- les 456 bits sont regroupés en 8 groupes de 57 bits ($8 \times 57 = 456$);
- chaque groupe est inséré dans une moitié de burst; l'autre moitié du burst est occupée par un autre groupe de 57 bits d'un autre bloc de 456 bits.

6.4 Canaux logiques

Pour renforcer l'interface radio, qui est le maillon faible de la chaîne de transmission, un certain nombre de fonctions de contrôle ont été mises au point pour que le mobile se rattache à une BTS favorable, pour établir une communication, surveiller son déroulement et assurer les handovers.

Ces fonctions de contrôle engendrent des transferts de données: remontées des mesures, messages de contrôle... Plusieurs canaux logiques ont été ainsi définis pour les différents types de fonction (veille, scrutation, mesures, contrôle...); ils forment une architecture complexe qu'il est nécessaire de connaître pour comprendre le fonctionnement d'un mobile pendant les différentes phases de communication ou pendant sa veille. Ils n'existent que sur l'interface radio et perdent ensuite toute leur signification sur les autres interfaces du système : Abis, Ater, A,...

Il faut sur l'interface radio :

- diffuser des informations système :

Broadcast Channels

- prévenir les mobiles des appels entrants et faciliter leur accès au système :

Common Control Channel

- contrôler les paramètres physiques avant et pendant les phases actives de transmission :

FACCH et SACCH

- • fournir des supports pour la transmission de la signalisation :

SDCCH

On n'utilise pas un canal physique plein pour chacune de ces tâches : ce serait gâcher de la ressource radio car elles ne nécessitent pas, en général, un débit comparable à celui de la voix codée (TCH).

Chaque multitrame transporte, avec une périodicité bien définie, un certain type d'informations de contrôle ou de signalisation. Cet ensemble de timeslots forme un canal logique. Certaines multitrames sont définies à 26 trames, d'autres à 51 trames.

6. 4. 1 Classification des canaux logiques

On distingue deux grandes classes de canaux logiques : les canaux dédiés et les canaux non dédiés :

- Un canal logique dédié est duplex et fournit une ressource réservée à un mobile. Le réseau attribue au mobile dans une structure de multitrame un slot en émission et un slot en réception dans lesquels le mobile est seul à transmettre et à recevoir. Dans la même cellule, aucun autre mobile ne peut transmettre dans le même slot (c'est-à-dire en même temps) de la même fréquence.
- Un canal logique non dédié est simplex et partagé par un ensemble de mobiles. Dans le sens descendant: diffusion des données, plusieurs mobiles sont à l'écoute du canal
Dans le sens montant: accès multiple selon la technique d' « Aloha slotte ».

Le tableau ci-dessous liste tous les types de canaux logiques et leur fonction

Broadcast Channel non dédié diffusion ↓	Frequency Correction Channel (FCCH)	calage sur fréquence
	Synchronization Channel (SCH)	synchronisation en temps & identification de la BTS
	Broadcast Control Channel (BCCH)	information systeme
Common Control Channel non dédié diffusion ↓ et accès multiple ↑	Paging Channel (PCH) ↓	recherche du mobile en cas d'appel entrant
	Random Access Channel (RACH)↑	accès aléatoire du mobile
	Access Grant Channel (AGCH) ↓	allocation de ressources
	Cell Broadcast Channel (CBCH) ↓	diffusion de messages courts
Dedicated Control Channel dédié ↓↑	Stand-Alone Dedicated Control Channel (SDCCH)	signalisation
	Slow Associated Control Channel (SACCH)	supervision lente de la communication
	Fast Associated Control Channel (FACCH)	signalisation rapide (handover)
Traffic Channel (TCH) dédié ↓↑	Full rate. Enhanced Full Rate & Half Rate	parole
	débit utilisateur < 14.4 kbits/s	données

Tableau 6. 5 : Types de canaux logiques et leur fonction

6. 4. 2 La voie balise

Chaque BTS d'un réseau radiomobile dispose d'une voie balise. La voie balise correspond à une fréquence particulière appartenant à l'ensemble des fréquences allouées à la BTS. Sur cette fréquence sont diffusées des informations particulières permettant aux mobiles de détecter la BTS, de se caler en fréquence et en temps et de donner les caractéristiques de la cellule (identité, particularités et autorisation d'accès...).

A la mise sous tension, un mobile cherche à se caler sur la voie balise de la BTS la plus favorable autorisée. En état de veille, il surveille constamment le signal reçu sur cette voie et sur les voies balises des BTS du voisinage. Dès que cela est nécessaire, il se cale sur une nouvelle voie et change ainsi de cellule de service.

En communication, un mobile du voisinage de cette BTS mesure périodiquement sur cette voie le niveau de signal qu'il reçoit. Il détermine par cette simple mesure s'il est à portée de la station, et s'il en est proche ou éloigné. Il remonte ensuite ces mesures dans les messages MEASUREMENT REPORT en vue de l'exécution d'un handover .

La voie balise des BTS correspond à :

- une fréquence descendante: fréquence balise sur laquelle les informations sont diffusées à puissance constante pour permettre aux mobiles de faire des mesures de puissances reçues fiables; le contrôle de puissance ne peut donc pas être implanté sur cette voie ;
- et a un ensemble de canaux logiques en diffusion sur cette fréquence balise, généralement sur le slot 0 de la fréquence; FCCH, SCH et BCCH. Le saut de fréquence ne peut donc pas être implanté sur cette voie;

a. Canal FCCH

Le canal FCCH consiste en un burst très particulier émis environ toutes les 50 ms. Ce burst est composé de 148 bits à "0". Émis sur une fréquence f_0 par la modulation GMSK., il donne

une sinusoïde parfaite de fréquence $f_0 + 1625/24$ kHz qui permet au mobile de caler finement son oscillateur. Le canal FCCH est présent uniquement sur le slot 0 de la voie balise (f_0).

b. Canal SCH

Le canal SCH fournit aux mobiles tous les éléments nécessaires à une synchronisation complète en temps. La séquence d'apprentissage est plus longue que dans un burst normal (64 bits au lieu de 26) pour permettre au mobile de faire une analyse fine du canal de transmission.

Les informations diffusées sur le canal SCH sont les suivantes :

- un numéro de trame permettant au mobile de savoir quel canal SCH de la multitrame il a décodé,
- le code BSIC de la BTS dont le rôle est de discriminer plusieurs BTS peu éloignées ayant la même fréquence balise :

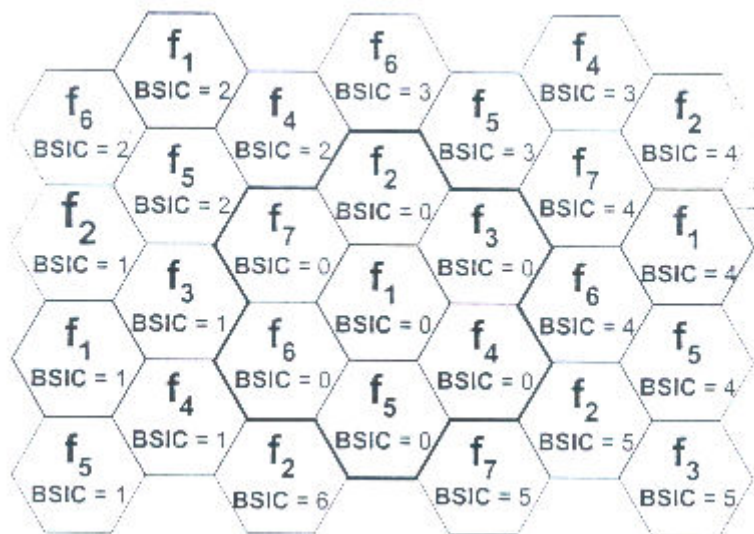


Figure 6. 7 : Utilisation des codes BSIC dans un motif a 7 cellules

Le canal SCH est présent uniquement sur le slot 0 de la voie balise; il est situé juste après le canal FCCH.

c. Canal BCCH

Le canal BCCH permet la diffusion de données caractéristiques de la cellule. Il comprend la diffusion régulière d'informations de plusieurs types dans les messages SYSTEM INFORMATION. Les informations les plus importantes sont les suivantes:

- le contrôle de l'accès aléatoire des mobiles sur le canal RACH (appels d'urgence acceptés ou refusés, nombre maximal de tentatives d'accès, classes de mobiles autorisées dans la cellule...);
- la liste des fréquences balises voisines à scanner ;
- l'identité de la cellule, sa zone de localisation ;
- la structure exacte de la voie balise courante, qui permet au mobile de savoir quand il doit écouter les éventuels appels entrants ;
- l'utilisation optionnelle du contrôle de puissance et de la transmission discontinue (sur les canaux autres que la voie balise);
- les paramètres de sélection de cellule (hysteresis, niveau minimal de puissance);

Le canal BCCH est présent au moins sur le slot 0 de la voie balise et peut parfois aussi se trouver sur les slots 2,4 ou 6 de cette même voie.

6. 4.3 Les canaux de contrôle commun

a. Canal RACH

Lorsque les mobiles veulent effectuer une opération sur le réseau, quelle qu'elle soit (mise à jour de localisation, envoi de messages courts, appel d'urgence ou normal (entrant ou sortant)...), ils doivent établir une liaison avec le réseau. Pour cela, ils envoient vers la BTS une requête très courte codée sur un seul burst. Cette requête est envoyée sur des slots particuliers en accès aléatoire de type ALOHA discrétisé (émission sans vérification préalable de l'occupation du canal, mais seulement possible à des instants précis). L'ensemble des slots réservés à cette procédure s'appelle le canal RACH.

Le burst d'information utilisé est très court et ne suit pas le format de la Figure si dessous car il faut laisser une marge de fluctuation au sein du slot RACH. En effet, le mobile ne connaît pas à cet instant le délai de propagation entre l'endroit où il se trouve et la BTS. Le délai de garde est de 252 μ s, ce qui permet d'envisager une distance maximale entre la BTS et le mobile d'environ 35 km.

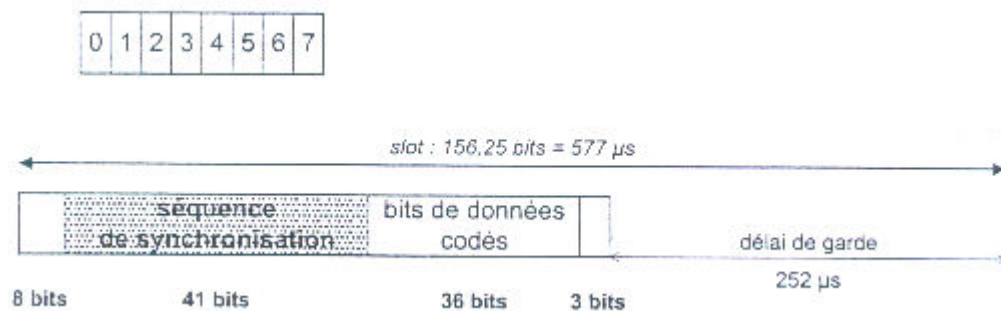


Figure 6. 8 : Format du burst RACH

Le burst transmet les informations suivantes :

- type de service demandé (appel entrant, appel sortant, appel d'urgence, mise à jour de localisation, émission de message court),
- un nombre aléatoire utilisé pour discriminer les mobiles en cas de collision qui permet au mobile de repérer si la réponse lui est véritablement destinée.

La séquence d'apprentissage est un peu plus longue que dans les bursts normaux car le mobile n'est pas complètement synchronisé avec la BTS : il ne connaît pas la distance qui les sépare.

b. Canal AGCH

Lorsque le réseau reçoit une requête de la part du mobile sur le canal RACH, il décide de lui allouer un canal de signalisation SDCCH afin d'identifier le mobile et déterminer précisément sa demande. L'allocation d'un tel canal dédié se fait sur des slots définis qui forment le canal AGCH.

Le burst d'information contient les informations suivantes:

- numéro de slot
- fréquence allouée ou description du saut de fréquence
- valeur du timing advance

Le canal AGCH est présent au moins sur le slot 0 de la voie balise et peut parfois aussi se trouver sur les slots 2,4 ou 6 de cette même voie.

c. Canal PCH

Lorsque le réseau désire communiquer avec le mobile (appel entrant ou réception de message court), la BTS diffuse l'identité du mobile sur un ensemble de cellules appelé "zone de localisation". Cette diffusion (appelée paging) a lieu sur un ensemble de slots qui forment le canal PCH. Tous les mobiles de la cellule écoutent périodiquement le canal PCH et le mobile concerné par l'appel répondra sur le canal RACH.

En utilisant comme identité d'appel le TMSI et non l'IMSI, il est possible pour le réseau d'appeler jusqu'à 4 mobiles simultanément dans le même message de paging.

Le canal PCH est présent au moins sur le slot 0 de la voie balise et peut parfois aussi se trouver sur les slots 2,4 ou 6 de cette même voie.

d. Canal CBCH

Le canal CBCH est un canal descendant qui permet de diffuser aux usagers présents dans la cellule des informations spécifiques (informations routières, météo, promotions...). Il peut utiliser certains slots 0 de la multitrame, mais son emploi est actuellement très marginal.

6. 4. 4 Les canaux dédiés

a. Canal TCH

Le canal TCH est utilisé pour transmettre les informations utilisateurs :

- la parole à 13 kbits/s ("full rate" plein débit), 12,2 kbits/s ("enhanced full rate", commercialisé sous le nom de "Digital Haute Resolution" chez Bouygues Telecom) ou 5,6 kbits/s ("half rate" demi- débit, pas encore utilisé par les opérateurs du fait de sa relativement mauvaise qualité),
- les données jusqu'à un débit utilisateur de 14,4 kbits/s.

b. Canal SDCCH

Le canal SDCCH est utilisé pour les établissements des communications, les émissions/réceptions de messages courts et les mises à jour de localisation. C'est le premier canal dédié alloué au mobile, avant son basculement éventuel sur un canal TCH. Sur ce canal se déroulent toutes les procédures d'authentification, d'identification et de chiffrement.

Le canal SDCCH sert en particulier à l'émission / réception de messages courts (Télémessages) ou à la réception de services personnalisés (abonnement aux services

"SCOOP" chez Bouygues Telecom: sport, news," astrologie, courses, loto,..) lorsque le mobile n'est pas en communication à l'instant de réception.

c.Canal SACCH

Le canal SACCH est un canal à faible débit: 1 burst d'information toutes les 26 trames. Il sert à contrôler la liaison radio et à ajuster en conséquence certains paramètres afin de conserver une qualité de service acceptable. Le canal SACCH supporte les informations suivantes :

- dans le sens montant ↑, remontée :
 - dans l'en-tête de tous les messages, des valeurs actuelles de puissance d'émission du mobile et de son timing advance
 - dans le message MEASUREMENT REPORT, des mesures effectuées par le mobile sur le canal courant et sur les BTS voisines
- dans le sens descendant ↓, transmission dans les messages SYSTEM INFORMATION :
 - dans l'en-tête de tous les messages, des valeurs commandées par la BTS serveuse au mobile de puissance d'émission et de timing advance du mobile
 - de l'identité et la zone de localisation de la cellule serveuse
 - de la liste des fréquences à scanner (correspondant aux voies balises des BTS voisines)
 - des diverses fonctionnalités implémentées sur la cellule serveuse : contrôle de puissance, transmission discontinue et valeur du Radio Link Timeout (RLT) en nombre de trames SACCH.

. 4. 5 Multiplexage TCH plein débit -SACCH

Le codeur de source de parole plein débit délivré toutes les 20 ms un ensemble de bits qui sont codés sur 8 demi-bursts. De manière temporelle, il faut donc transmettre 4 bursts de

parole toutes les 20 ms. Pendant une période de 120 ms, il y a donc 24 bursts de parole à transmettre.

D'autre part, on a vu que le mobile pouvait émettre et recevoir des données toutes les 4,615 ms (un slot déterminé sur une fréquence particulière). Pendant une période de 120 ms, il y a donc $120/4,615$ soit 26 bursts d'information à transmettre.

Il reste donc deux slots libres. Un slot est utilisé pour le canal SACCH, l'autre slot est appelé slot idle et cette structure de multiplexage est répétée toutes les 120 ms, c'est-à-dire toutes les 26 trames TDMA (d'où le nom de multitrame à 26).

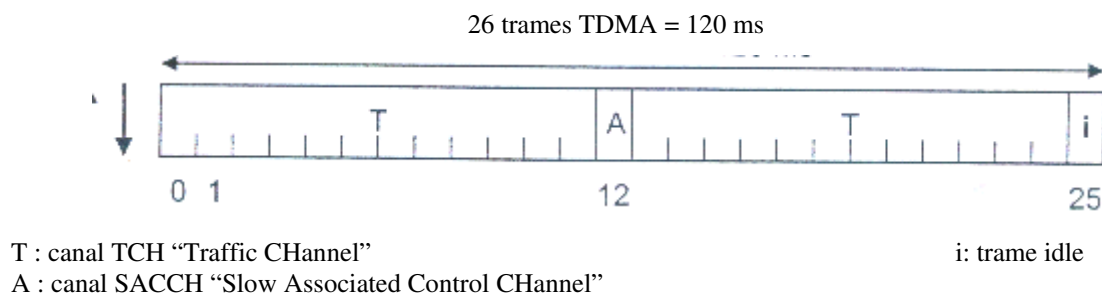


Figure 6. 9 : Multitrame à 26 pour le multiplexage TCH plein débit / SACCH

Le slot idle est utilisé par le mobile non pas pour se reposer mais pour scruter les voies balises voisines que la BTS serveuse lui a indiquées. Pendant ce laps de temps disponible, le mobile tente de décoder le code BSIC diffuse sur le canal SCH du slot 0 des voies balises, puis il renvoie ces informations dans les messages MEASUREMENT REPORT, accompagnées des mesures de puissance effectuées.

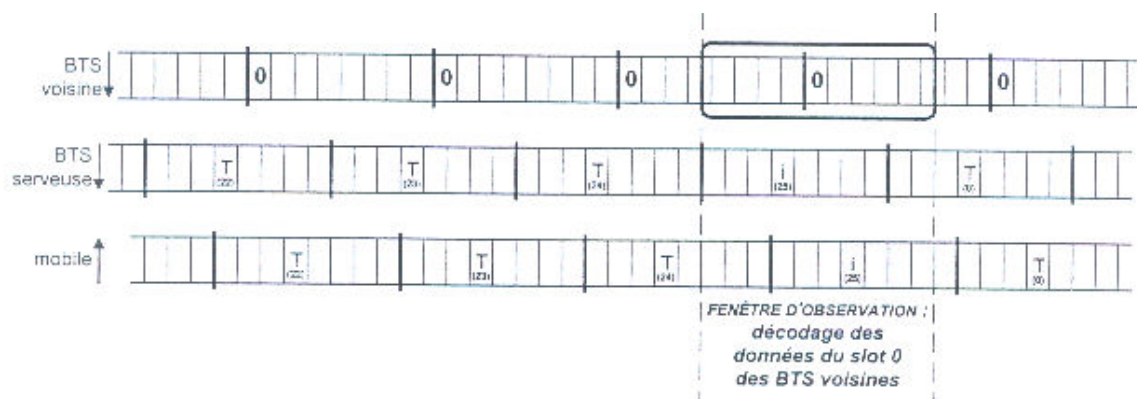


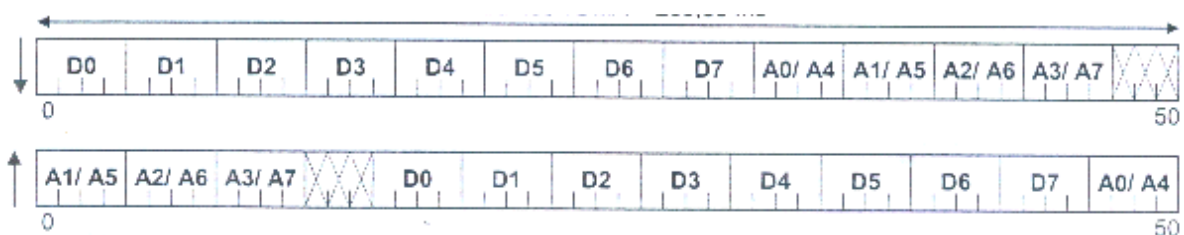
Figure 6. 10 : Utilisation du slot idle

Le canal SACCH transporte, comme nous l'avons vu, de la signalisation à faible débit. Il ne convient donc pas aux actions qui doivent être faites rapidement comme le handover. En ces cas d'urgence, on suspend la transmission des informations utilisateurs sur le canal TCH et on utilise la capacité ainsi libérée pour un autre canal, le canal FACCH, pour la transmission de la signalisation rapide. Ce canal est vu comme un vol de capacité du TCH, il n'a pas de structure

fixe dans les multitrames puisqu'il intervient ponctuellement, en cas de handover.

6. 4. 6 Multiplexage SDCCH-SACCH

De même manière que pour le canal TCH, un canal SACCH est alloué conjointement à chaque canal SDCCH, mais la structure de la multitrame est différente puisqu'il s'agit d'une multitrame à 51 trames. Sur la multitrame à 26 étaient multiplexés 1 canal TCH et son canal SACCH associé. Sur cette multitrame à 51 sont multiplexés 8 canaux SDCCH et leurs canaux SACCH associés (une multitrame sur deux), comme illustre sur la Figure 6. 11.



51 frames TDMA = 235,38 ms

D: canal SDCCH Stand Alone Dedicatées Control Channel

A: Canal SACCH Stow Associated Control Channel

Figure 6. 11 : Multiplexage SDCCH-SACCH

6. 4. 7 Multiplexage des canaux non dédiés

Suivant la capacité de la BTS, le PCH et l'AGCH ont des configurations variables. Cependant, tous les canaux logiques non dédiés sont multiplexés sur une multiframe à 51 trames. Celle-ci se trouve sur le slot 0 de la voie balise et parfois, en cas de forte capacité de la BTS, sur les slots 2, 4 et 6 de cette voie.

Dans le cas contraire d'une configuration minimale (faible capacité de la BTS), le multiplexage peut être éventuellement complété par 4 canaux de signalisation dédiés SDCCH et leurs SACCH associés. La Figure 6. 12 : illustre la configuration minimale sur te slot 0 de la voie balise :

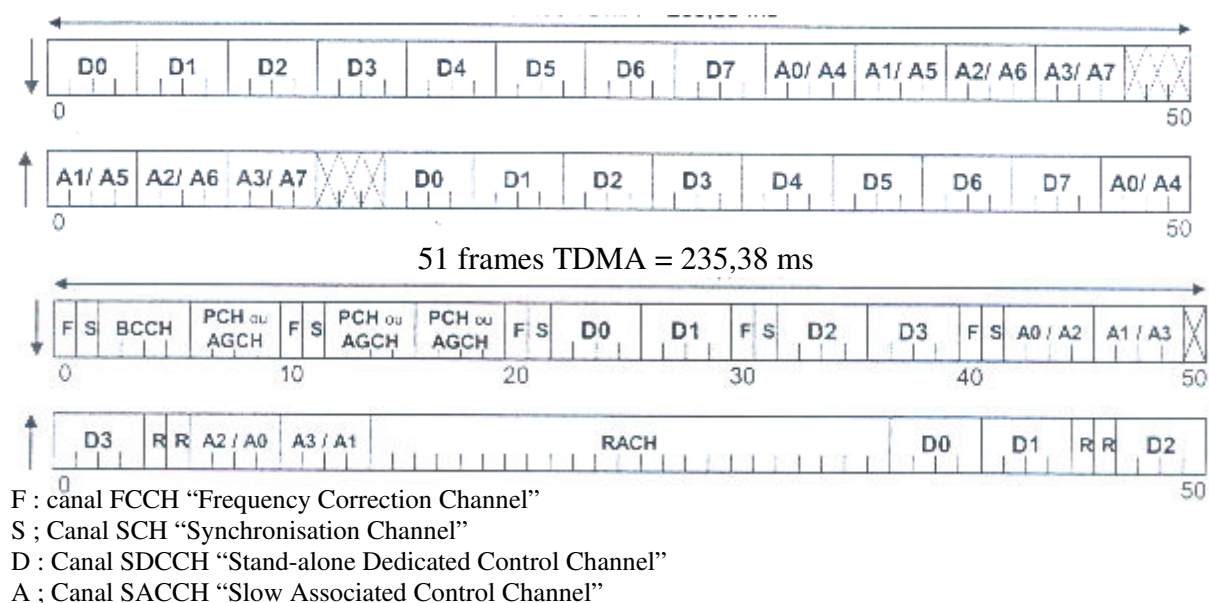


Figure 6. 12 : Configuration minimale des canaux de contrôles sur le slot 0 de la voie balise