Réseaux de communication Radiomobile

Esigelec : Option ITO

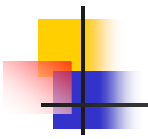
V 2.0

Pierre Roullet : roullet@aist.enst.fr

Sommaire 1/2

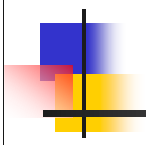
- **Introduction**
  - Les différentes normes qui se cachent derrière le mot GSM
  - Historique des réseaux cellulaires, dates clés, obligation des licences
  - Les Limites du GSM et des normes numériques
  - Les organismes de standardisation
  - L'organisation des Recommandations

- **I Les caractéristiques et les services généraux d'un réseau cellulaire**
  - Concepts généraux sur les réseaux cellulaires
  - Les caractéristiques générales d'un terminal Mobile
  - L'architecture générale du GSM
  - Les différents éléments du réseau GSM
  - Les différents services offert par le GSM



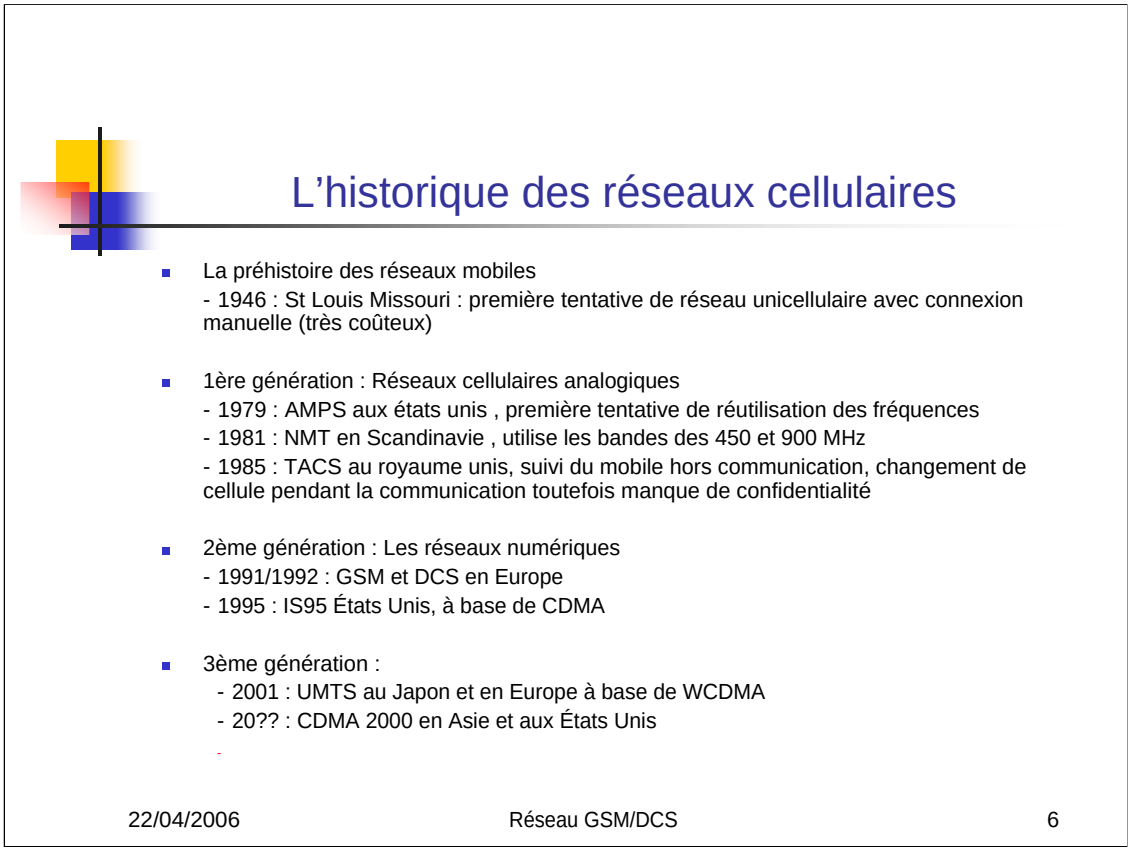
Sommaire 2/2

- **II protocoles et procédure du GSM/DCS**
  - Les différents protocoles du Mobile au MSC
  - Le multiplexage des canaux logiques
  - Les canaux dédiés
  - Les canaux diffusés
  - Les canaux de contrôle
  - Le mode veille
  - Sortie du mode veille
  - Le paging
  - Localisation
  - Handover
  - Appel entrant
  - Appel sortant



Introduction

Le GSM est maintenant devenu un mot aussi classique que frigo ou fermeture éclaire, toutefois avant de rentrer dans le vif du sujet il est important de définir la définition exacte de GSM et surtout de souligner qu'il n'y a pas un GSM mais des GSM



La volonté d’avoir de la téléphonie cellulaire ne date pas de hier car dès la fin des années 40 on peut remarquer une première tentative qui fut un échec car nous ne disposions pas à ce moment des moyens techniques requis pour assurer le succès d’un service grand public.

On peut toutefois noter que les premières tentatives réussites de réseaux analogiques furent faites aux états unis ou en Scandinavie 2 parties du globe où la densité de population est très inégale et donc où un maillage de télécommunication en réseau classique n’était pas forcément le moins cher.

Longtemps les Américains et les Nordiques gardèrent leur suprématie et leurs systèmes analogiques sont encore utilisés notamment en Amérique mais le succès du GSM n’est plus contesté.

En ce qui concerne les systèmes de troisième génération qui se voulaient universels les états unis et le reste du monde n’ont pu s’entendre il y a donc 2 systèmes concurrents, l’ UMTS soutenu par l’Europe et le Japon et le CDMA 95 soutenu par les américains, et il est bien sur trop tôt pour pouvoir dire quel système l’emportera sur l’autre, ceci est d’autant plus vrai après la crise qu’est entrain de subir le monde des télécoms en général

Dates Clés GSM et DCS

- WARC 79 : World Administrative Radio Conférence.
  Réservation de la bande 900 MHz pour la téléphonie Mobile
- CEPT 82 : (Conférence Européenne des Postes et des Télécommunications)
  Allocation des bandes suivantes
  - 890-915 MHz : Mobile vers la station de base
  - 935-960 MHz : station de base vers le mobile

  Sous l'impulsion française et allemande création du Groupe Spécial Mobile pour spécifier un système dans la bande des 900 MHz
- 1984-1986 : Les allemands et les français se concentrent sur la comparaison des techniques analogiques et numériques avec élaboration de prototypes. En France France Télécom joua un rôle important
- 1985 : La CEE annonce son intention d'imposer la norme issue du GSM
- 1987 : Le choix de la chaîne de transmission numérique est finalisée avec notamment le choix du codage canal et du codage de la parole
- Mars 90 Gel des spécifications et demande du royaume unis de l'adaptation qui donnera naissance au DCS
- 1991 premiers tests à paris entre le réseau mobile et rtc, le GSM est la star de Telecom Genève
- Juillet 92 ouverture du système GSM Itinéris (ancien nom d' Orange)
- Octobre 1994 Bouygues obtient sa licence
- Début 1996 Ouverture de la transmission data par les opérateurs Français
- 2002 Ouverture du GPRS

Dès 1979 la borne 900 MHz est réservée pour la téléphonie mobile et est occupée différemment selon les pays. En Europe on y trouvera le GSM tandis qu'aux États Unis on y trouvera plutôt la norme Etacs.

Comme on peut le voir le succès du GSM européen vient de la volonté de la CEE d'imposer sur tout son territoire une seule norme et à assurer une itinérance des abonnés.

La première version de la norme date de 1990 et est en constante évolution en fonction des demandes des opérateurs, des constructeurs mais surtout de l'attente des clients.

Les licences GSM accordées

- Mars 1991 : extension des autorisations d'exploitation des réseaux analogiques accordées à France Télécom et à SFR pour un réseau GSM
- Décembre 1994 : Bouygues Télécom est autoriser à exploiter un réseau DCS 1800, durée de la licence : 15 ans
- Cahier des charges pour le GSM 900
  - Obligation de couvrir 85% de la population à la fin 97 soit 60% du territoire
- Cahier des charges pour DCS 1800
  - exclusivité de la bande 1800 jusqu'en 2000
  - obligation de couvrir
    - 54,2% de la population fin 98 en extérieur
    - 86,6% de la population fin 2005
  - obligation de garantie de service

On peut noter que l'attribution des licences GSM furent plus sages que celle récentes de l' UMTS, en effet à cet instant la spéculation était moins importante et le succès des mobiles plus aléatoire.

Maintenant les 3 opérateurs se partagent les bandes 900 et 1800 pour assurer une couverture optimisée du territoire ce qui leur a permis de remplir toutes les obligations de leur licence.

On pourra déplorer le manque de synergie obligatoire entre opérateur notamment dans la couverture de zone ou dans le partage d'émetteur, des zones françaises se trouvent donc hors couverture ou des endroits comme Paris sont eux couvert d'antennes

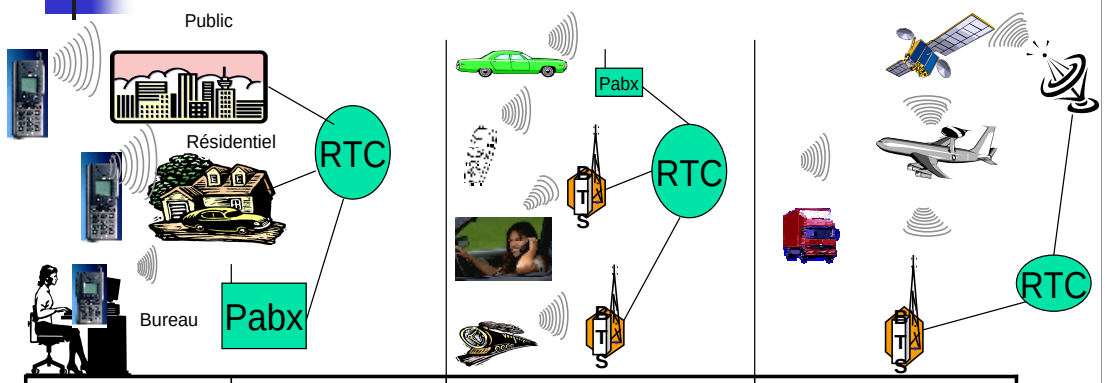
Panorama des normes actuelles

	CT2	GSM/GPRS	DCS1800	DECT	IS95	UMTS
Type de système	« sans fil extérieur »	Cellulaire	Cellulaire	« sans fil d'intérieur »	Satellite	Cellulaire
Bande de fréquence	864-868	890-915 Up 935-960 Do	1710-1785 1805-1880	1890-1900	1610-1626.5 2483.5-2500	1920 1980 2110-2170
Largeur	4 MHz	2 X 25MHz	2X75MHz	20 MHz	2X16,5 MHz	5 MHz
Espacement de porteuse	100 KHz	200 KHz	200 KHz	1728 KHz	1.25MHz	200 KHz
Multiplexage	FDMA	F/TDMA	F/TDMA	TDMA	CDMA	WCDMA
Nombre de porteuses et canaux radios	40 X 1	124 X 8	374 X 8	10 X 12	2800	TBd
Taille max des cellules	300 m	35 Km	4 Km	300 m	500 Km	TBd
Noms commerciaux	Ex BiBop	Orange, SFR	Bouygues	Téléphone domestique	Globalstar	Tbd

Le CT2 fut assez vite arrêté au profit des réseaux GSM car il avait de nombreux inconvénients comme l'impossibilité de handover et une couverture qui était trop contraignante de part la taille de ces cellules.

Le dect lui a une utilisation en entreprise assez développée car il permet à moindre coût une couverture complète d'un site et il a un confort d'écoute inégalé par le téléphone sans fil analogique.

Limites des normes actuelles



	Micro-cellule	Macro-cellule	cellule
Rayon de couverture	10 à 300 m mobilité restreinte	300 m à 35 Km mobilité développée	Plusieurs centaines de Km
Mobiles concernés	Piétons	Véhicules en tout genre, piétons	Véhicules, avions, navires
normes	CT2 DECT	GSM DCS	CDMA, Satellites

22/04/2006 Réseau GSM/DCS 10

On remarque donc que de part leur limites techniques les micro-cellules sont plutôt faite pour couvrir de petites zones et n'offrent pas forcément la mobilité surtout en communication, elles peuvent toutefois être utilisées dans des milieux urbains très denses pour augmenter la capacité des réseaux Il se pose alors les problèmes de planification cellulaire et de réutilisation des fréquences mais nous verrons cela un peu plus tard dans l'exposé.

Les macro cellules sont vraiment faites pour couvrir un environnement urbain ou rurale mais limité et offre une mobilité mais jusqu'à une certaine vitesse qui est dans le cas du GSM est 500 Km/h au delà le système ne peut plus gérer le décalage entre l'émetteur et le récepteur.

Les grosses cellules elles sont vraiment faites pour couvrir de grand territoire voir pour avoir une couverture mondiale, toutefois le marché pour de tels systèmes est assez restreint et le service est donc fort cher.

Les organismes de normalisations

- ETSI : Organisme de Normalisation pour l'Europe, il est à l'origine des différents normes de télécommunication comme le GSM et le Dect. Avant l'UMTS il était à la fois groupe de travail et institut de normalisation, maintenant l'aspect étude de la norme est faite au sein du 3GPP l'ETSI se gardant la prérogative d'établir les normes pour l'Europe.

- 3GPP : Le 3GPP n'est pas qu'européen et regroupe L'ARIB organisme de normalisation japonais, T1 organisme de normalisation américain et TTA organisme de normalisation coréen. Organisme non pas de normalisation mais groupe d'étude il a comme but de faire évoluer le GSM/GPRS vers les systèmes de troisième génération

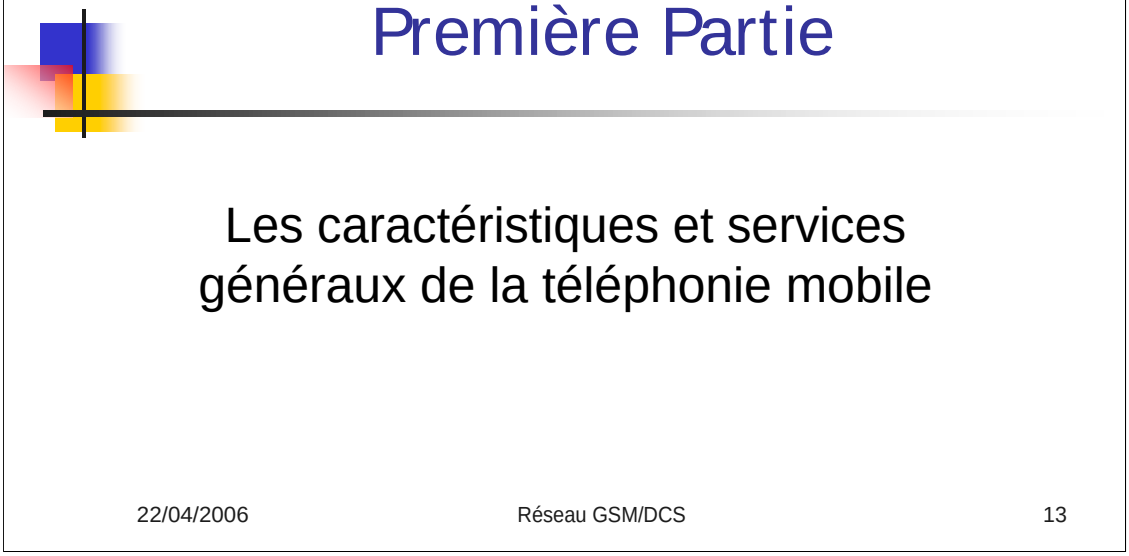
Autant le rôle de l'ETSI est indiscutable en Europe, le 3GGP a un concurrent direct le 3GGP2 qui lui est son équivalent mais pour faire évoluer les normes américaines vers le CDMA2000 candidat au système de troisième génération.

Il existe aussi le 3GPPIP mais ce groupe d'étude étudie plutôt les moyens d'intégration des mobiles dans un réseau IP

Organisation des recommandations GSM

Série	Nbr Rec	Thème	Principaux contenus
01.XX	3	Aspects généraux	Description générale Vocabulaire
02.XX	35	Définition des services	Principes des services-Types de mobiles-sécurités-Licences-abonnements-circulation des mobiles-Identité d'Équipement- Carte SIM-Tonalité locale-Principe de facturation
03.XX	43	Aspect Réseau	Fonction-Architecture-Numérotage-Identification-Handover-Mise à jour de loc DTMF-Authentification
04.XX	25	Interface MS-BS et protocole	Principes- Modélisation-Référence-Type de canaux Specs niveaux 1 2(LAPDM)3(RR MM CM RLP)
05.XX	8	Interface Radio niveau physique	Multiplexage des canaux-codage canal-Modulation contrôle de puissance synchronisation
06.XX	23	Codage,décodage parole	Codage-Trames perdues-Transmission discontinue(DTx)
07.XX	6	Adaptateur de terminaux	Adaptation aux services supports synchrones/asynchrones
08.XX	14	Interfaces BS-MSC	Interface A- Interface Abis- Contrôle distant des TRAU
09.XX	14	Interfonctionnement	Protocole MAP, interfonctionnement avec RTCP, RNIS
11.XX	16	Équipements	Conformités des mobiles du BSS Interface SIM-ME
12.XX	15	Exploitation& Maintenance	Config, Maintenance, fonction de gestion Interface et protocole

Dans ce tableau ne sont représentées que les normes du standards GSM avec leur numéro ETSI, en effet depuis que la maintenance des normes est passé sous la coupe du 3GPP il y a eu une nouvelle découpe des normes et donc de nouveaux numéros mais ce n'est pas le but de cet exposé. Toutes ces Recs sont en téléchargement libre sur http://www.3GPP.org

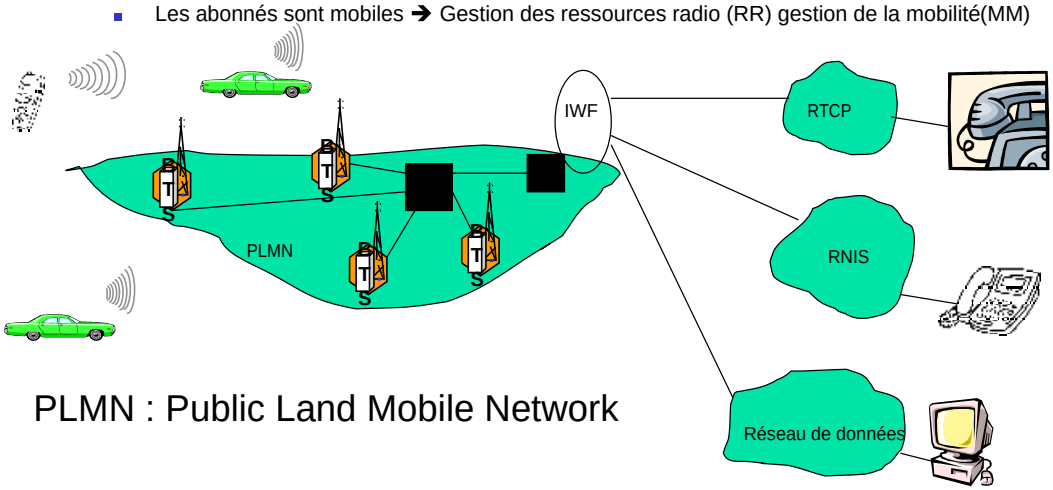


Première Partie

Les caractéristiques et services généraux de la téléphonie mobile

Concepts Généraux : PLMN et mobiles

- Le PLMN est un réseau d'accès
- Les abonnés sont mobiles ➔ Gestion des ressources radio (RR) gestion de la mobilité(MM)



PLMN : Public Land Mobile Network

22/04/2006 Réseau GSM/DCS 14

Avant de rentrer plus en détail dans la description des terminaux mobiles il est intéressant de poser les différentes problématiques que rencontre un fournisseur de service GSM.

Il doit tout d'abord faire face à des abonnés qui sont mobiles dans une zone donnée, il doit donc la couvrir avec son réseau ou PLMN, ensuite offrant plusieurs services il devra aussi gérer l'interconnexion entre son réseau et les différents autres types de réseau grâce à des passerelles ou IWF. Tous ces aspects seront évoqués un peu plus loin et plus en détail

Concepts Généraux : couverture cellulaire

- La propagation limite les performances
- Les ressources radio sont limitées ➔multiplication des cellules : toutefois des limites
- Pour accroître l'efficacité spectrale , introduction d' astuces techniques :

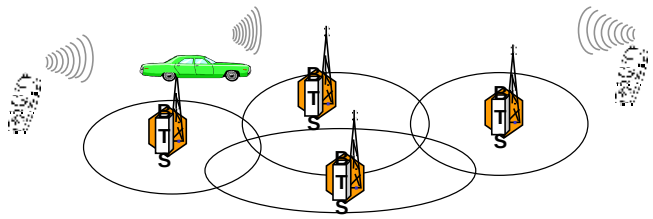
➔Contrôle de puissance

➔Transmission discontinue

➔Saut de fréquence (Limite les évanouissements)

➔Handover assisté par le mobile : mesure systématique pour garantir une qualité de service

➔Timing of Advance



22/04/2006 Réseau GSM/DCS 15

Devant couvrir une zone plus ou moins étendue avec plus ou moins d'obstacles l'opérateur est confronté à plusieurs problèmes liés au mode de transmission radio. Il y a tout d'abord les problèmes de propagation, en effet le milieu urbain ne simplifie pas la propagation d'onde surtout que l'antenne et le mobile sont rarement en ligne direct. Il faut aussi gérer les problèmes de pénuries de bande passante et sa réutilisation en zone urbaine. Enfin il y aura les problèmes de puissance , un mobile ne devra pas masquer un autre et inversement.

Pour pallier à ces problèmes des astuces ont été mise en place: à savoir le contrôle de puissance, le saut de fréquence et l'handover inter ou intra cellules.

Concepts généraux : Modèles de propagation et Rapport C/I

Modèles d'atténuation réel

$$C = Pe \times Ge \times Gr \times \frac{K\lambda^2}{r^{\gamma}} \times As \times Af$$

C : Niveau du signal Reçu
Pe : puissance émission
Ge, Gr : Gain de l'antenne en émission et réception
λ Longueur d'onde
γ atténuation due à la distance
r distance mobile antenne
As atténuation due aux obstacle
Af évanouissement sélectif

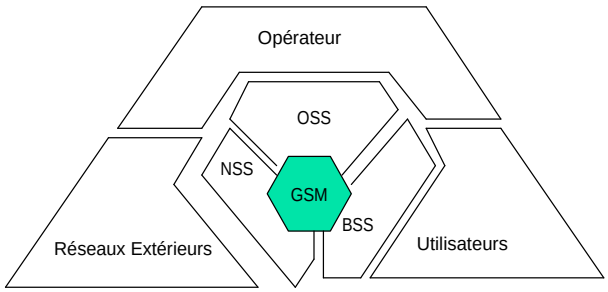
Rapport signal à bruit systèmes limités par les interférence

$$\frac{C}{I} = 6\left(\frac{D}{R}\right)^{\gamma}$$

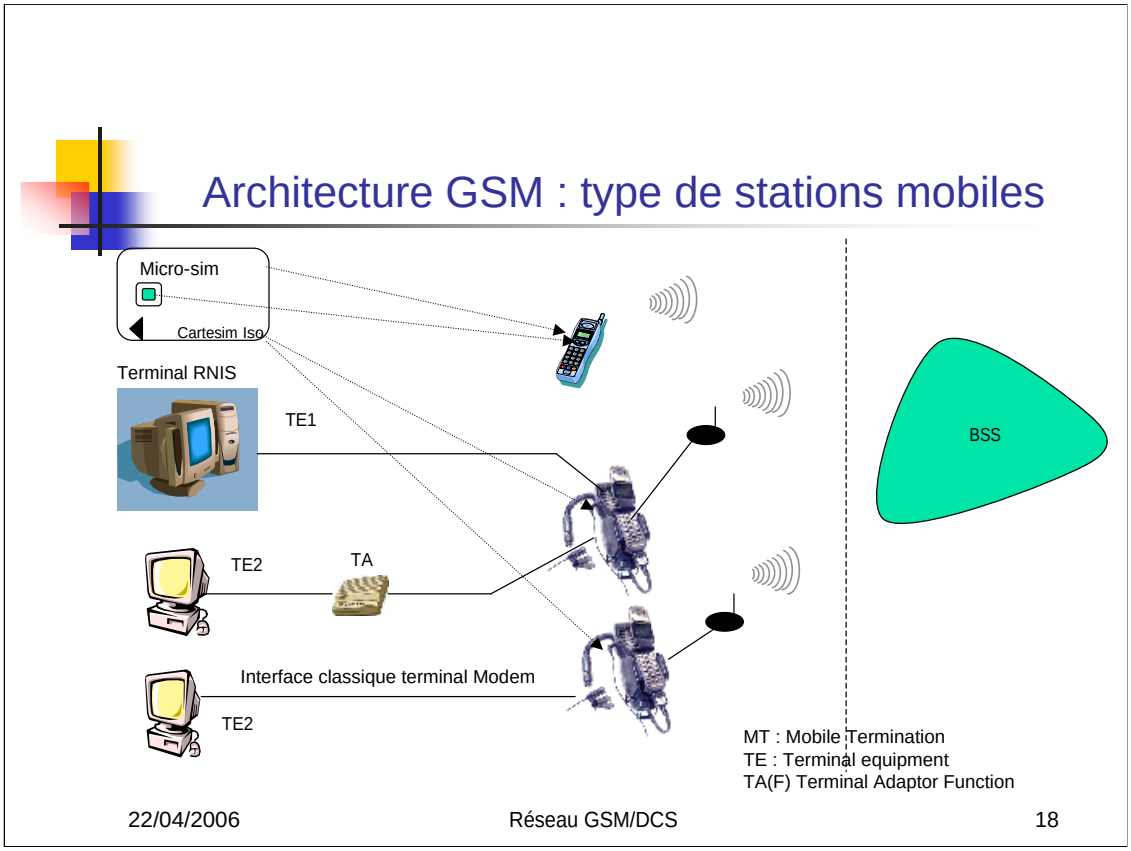
Les systèmes analogiques supportent un C/I de 20db alors qu'un système GSM avec correction d'erreurs peut descendre à un C/I de 10db, donc en prenant un As de l'ordre de 8db et un gamma de 4 on peut exprimer C/I en fonction de la taille des motifs c'est à savoir le maillage que va faire l'opérateur et la distance minimum entre 2 cellules ayant la même fréquence. On s'aperçoit alors que le nombre K nombre de motif utilisé peut s'exprimer en fonction de D/R et qu'il faut généralement un maillage de 12 pour tenir compte de l'irrégularité des cellules. On définit ainsi la notion de Motif.

Attention toutefois pour distinguer sans problème les cellules car 2 cellules de 2 motifs adjacents pouvant avoir la même fréquence balise on ajoutera à la fréquence de la cellule un code dit code de couleur de la station qui jouera un rôle important pour distinguer les cellules mais aussi jouera un rôle dans l'égalisation, en effet à chaque couleur correspond une séquence d'apprentissage particulier.

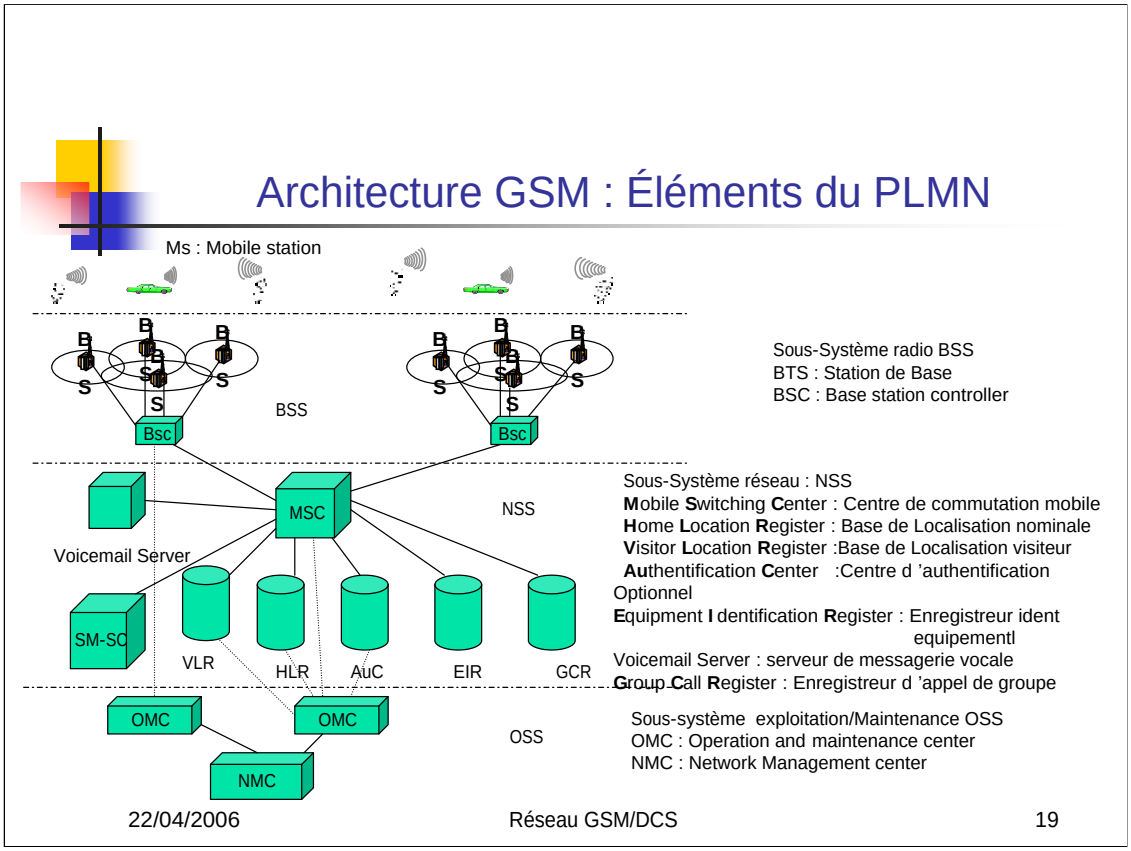
Vue générale de l’architecture GSM



Ce transparent nous donne une vison globale de l’architecture GSM et de son interaction avec les acteurs de ce système. Il y a tout d’abord l’utilisateur du service, il s’interconnecte au monde GSM par l’intermédiaire de l’interface Radio à savoir le BSS (Base Station System). Il y a ensuite l’opérateur qui offre le service, il a surtout un rôle de supervision du GSM grâce à l’OSS (sous système d’exploitation). Enfin le réseau GSM peut s’interconnecter avec d’autres réseaux pour cela il utilise le NSS (Network sub system)

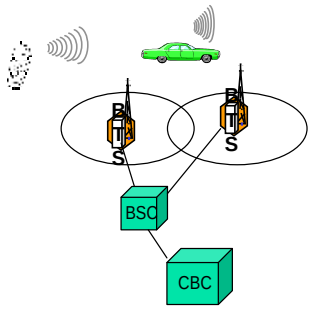


Il y a différent types de Terminaux GSM toutefois tous possède une interface pouvant lire une carte SIM qui contient les renseignements sur l'abonnement et l'abonné. Les terminaux mobiles peuvent servir juste à transmettre de la parole ou d 'autre avoir le rôle de modem avec les interfaces de connexions plus ou moins incorporées au terminal. De nos jours la notion de terminal GSM peut même s 'étendre à des systèmes d 'alarmes par exemple où on utilise surtout l'aspect facilité d 'implémentation et surtout le coût modique de l'installation.



Ce transparent nous donne un bon aperçu du réseau GSM, chaque élément sera bien sur plus développé dans les transparents qui vont suivre. On trouve tout d 'abord bien sur l'élément principal l 'utilisateur du réseau à savoir vous moi tout le monde à pied en train ou en voiture, la vitesse limite théorique du réseau GSM étant de l'ordre de 500 km/h. Ensuite on trouve directement l'interface entre le terminal et le réseau à savoir le sous système réseau qui se compose des stations de base (BTS) que nous voyons fleurir un peu partout même en haut des montagne et des BSC qui sont des concentrateurs de stations de Bases dont nous verrons le rôle plus tard. Ce sous système radio est relié directement à la partie qui gère le protocole du réseau à savoir le sous système réseau. Ce sous système réseau va gérer à la fois l 'aspect mobilité et localisation du terminal que l'établissement et la terminaison des appels. Enfin le dernier élément que nous voyons et le sous système d'exploitation qui permet à l 'opérateur de maintenir son réseau et surtout de le gérer. Cette dernière partie ne sera pas vu dans cet exposé car étant trop réseau dépendant.

Architecture GSM : sous système radio



Principales fonctions :

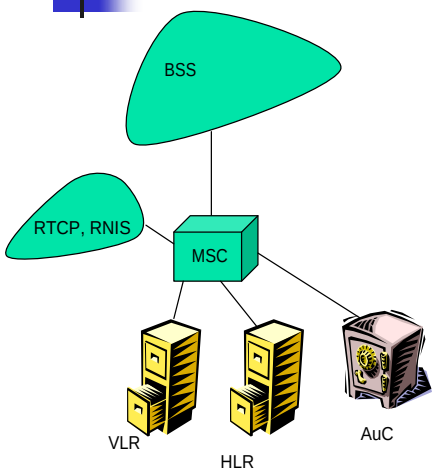
BTS :
gestion des canaux physiques (16 porteuses Max)

BSC :
Gestion des interfaces avec NSS & OSS
Gestion des canaux logiques radios
contrôle des BTS

CBC :
(optionnel) cell broadcast centre
Stockage tampon et génération des messages courts diffusés

Comme nous avons vu dans le transparent précédent le premier élément que nous voyons est le sous système radio, c'est l 'interface direct entre le mobile et le réseau. Il est composé tout d'abord de la station de base qui couvre une certaine cellule où le service sera rendu. La dimension de la cellule varie de 35 Km en zone rurale à quelques centaines de mètres en zone urbaine. Ces BTS gèrent jusqu'à 16 fréquences et sont chargées de la gestion des canaux physiques que nous verrons plus tard dans l'exposé. Les BTS sont toutes liées à un BSC qui gère un regroupement de stations de Base. Dans cette zone de couverture il va gérer les canaux logiques et les différentes interfaces avec les autres sous systèmes. Enfin on peut trouver le centre de diffusion de message court, ce service pas utilisé en France permet de diffuser un message court à tous les abonnés d'une zone, ce service est optionnel d 'un point de vue recommandation.

Architecture GSM : sous-système Réseau



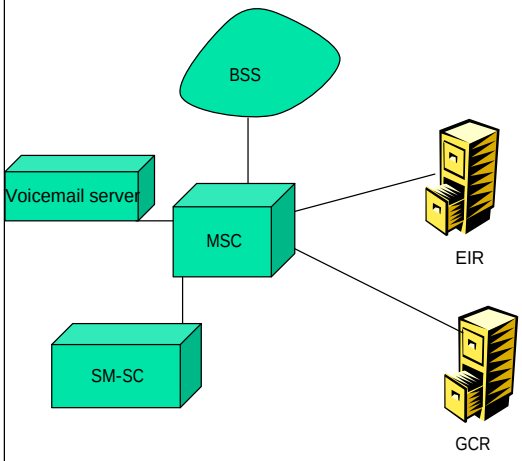
Principales Fonctions
MSC :
Traitement d 'appels
Gestion des ressources radio
- Mise a jour des bases VLR/HLR
- Recherche radio d 'un abonné
- Gestion du « Handover »
Fonction passerelle « Gateway »pour les appels arrivés

HLR : Base de données de référence (pour une région)
Stocke : Identité , Num annuaire,
services souscrit +localisation grossière (VLR)
VLR : Base de donnée locale(associée à 1 ou plusieurs MSC)
AuC : Base de donnée de sécurité, génération des clefs et authentification

22/04/2006 Réseau GSM/DCS 21

Un des élément principal du sous système radio est le MSC, il gère en effet le traitement de l'appel des son établissement jusqu'à sa terminaison et notamment la recherche de l'abonné au sein de la zone surveillée. Il gère aussi la mobilité du terminal en s'occupant des processus de Handover qui sera décrit plus en détail dans la deuxième partie. Il mettra aussi à jour les différentes bases de données qui gèrent les informations relatives au client et à son type d'abonnement. Enfin une des missions importantes du MSC est de jouer la passerelle entre les différents réseaux téléphoniques (paquets ou numériques) ou par paquets et le réseau GSM. Ces fonctions passerelles ne sont pas développées ici mais joue un rôle important notamment dans l'aspect signalisation 7 le MSC étant en effet le point d'ancrage ou d'entrée du réseau GSM quelque soit la progression du terminal au sein du réseau.

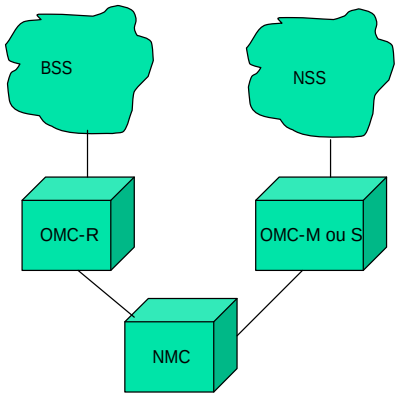
Architecture GSM :équipements optionnels(NSS)



Principales Fonctions
EIR : Base des équipements mobiles, notion des Mobiles blanc gris ou noir
Voicemail server : Serveur de messagerie vocale
Ce service n'est pas standardisé
SM-SC : Stockage des messages courts pendant L'indisponibilité des mobiles
GCR (Group Call register) serveur des groupes d'appel vocaux

Enfin nous allons voir le système optionnel du réseau GSM. L'équipement peux être le plus connu est le serveur de boîte vocale qui n'est pas du tout standardisé, en effet son appel diffère d'un opérateur à l'autre et les services attachés à cet équipement aussi. On trouve aussi comme équipement optionnel l'EIR qui est une base de donnée qui référence les mobiles qui sont interdits sur le réseau ou avec des services restreints, ainsi l'interdiction des mobiles volés se fait par la mise en place d'un EIR plus ou moins commun ou en tout cas synchronisé entre les opérateurs. Le rôle du SM-SC est lui d'assurer la bonne arrivée d'un message court en le stockant ce message lors des phases d'indisponibilité des mobiles. Ce stockage a biens sur un temps limité défini lors de l'envoie du message. Enfin on trouve le serveur des groupes vocaux qui s'occupe de la mise en commun des besoins radios entre des groupes d'utilisateurs.

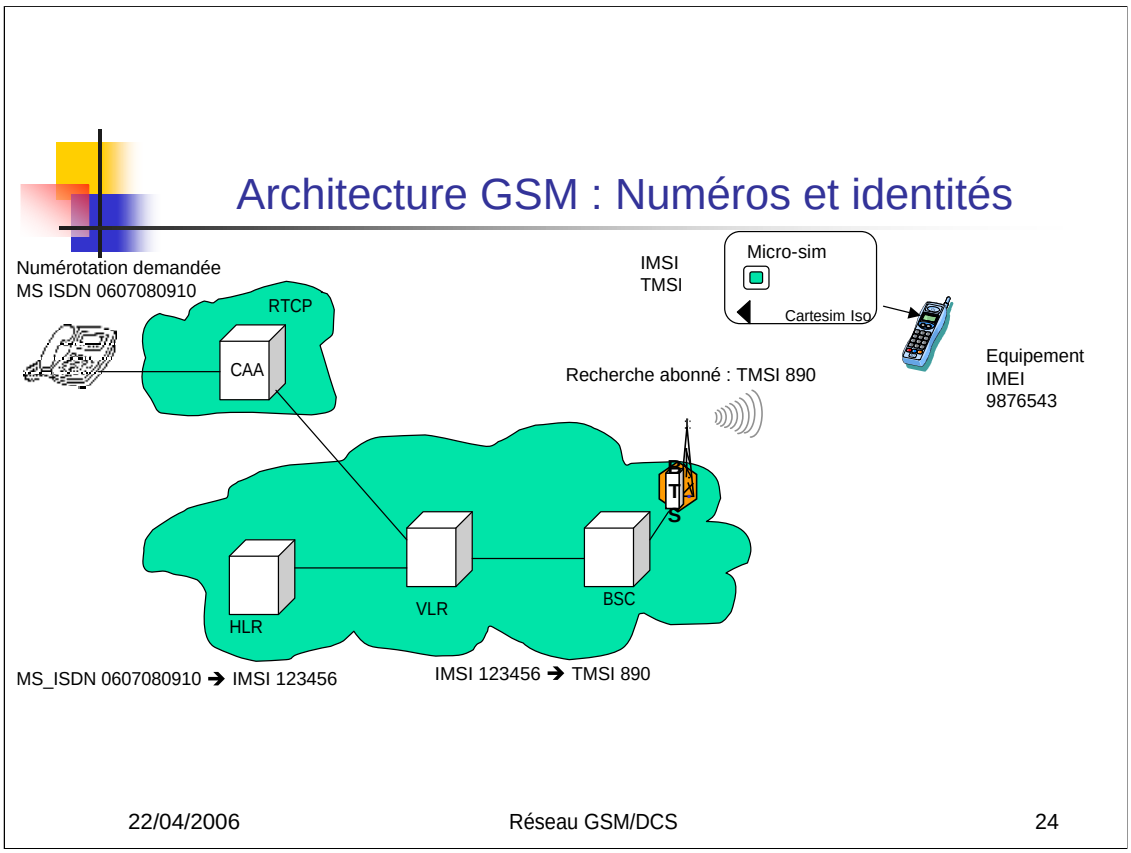
Architecture GSM : exploitation et maintenance



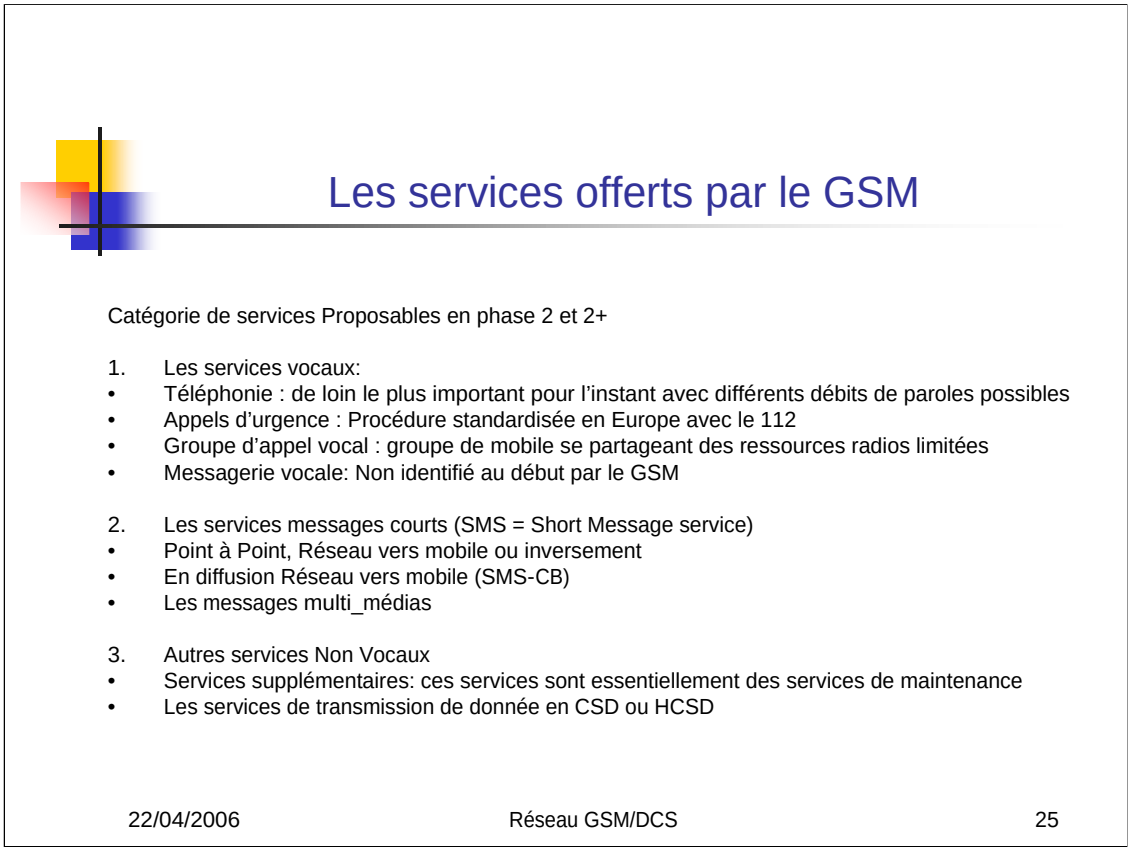
OMC
OMC-R➔radio gestion de la BSS
OMC-S➔Switching gestion MSC
OMC-M➔Mobile gestion NSS
-Gestion de la configuration
-Gestion des fautes
- Gestion des performances
-Gestion de la sécurité
-Gestion des coûts

NMC
Gestion de réseau de niveau supérieur

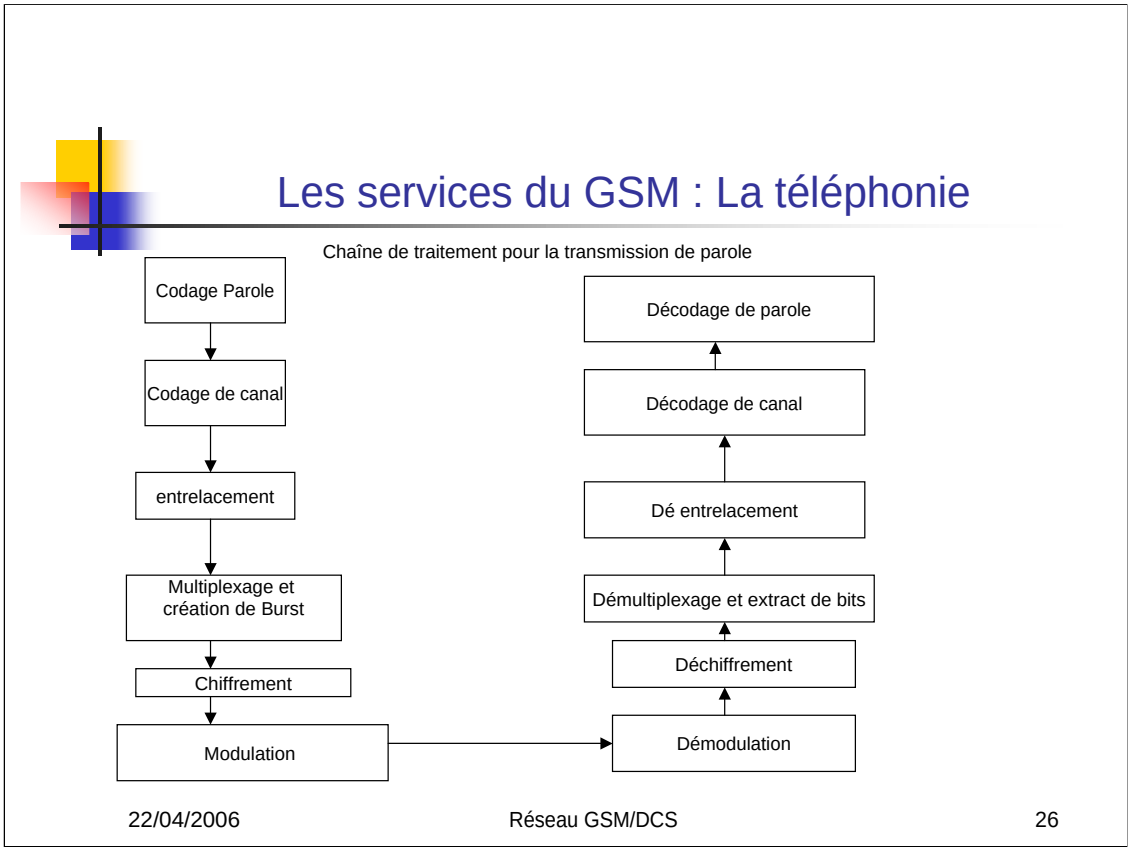
Ce transparent là montre les différents éléments qui constituent la partie supervision du réseau avec comme superviseur final le NMC. Il a sous sa coupe deux sous éléments le OMC R qui gérer plutôt l'aspect radio du réseau et notamment de la BSS et enfin les OMC M ou S pour tout ce qui est plutôt protocolaire



Avant de rentrer plus en détail dans les services du réseau GSM et pour compléter la description de l'architecture GSM il convient de définir les différents Numéros et identités qui rentrent en jeux lors d'un appel à destination d'un portable. Lorsqu'un abonné d'un réseau externe au GSM veut joindre un abonné du réseau il ne possède que son numéro ISDN qu'il va composer. Cet appel sera routé vers le Msc le plus proche qui va interroger le HLR correspondant. De l'interrogation du HLR on va en tirer 2 informations, tout d'abord le VLR sous lequel se trouve le Mobile et enfin son IMSI. L'IMSI est l'identifiant du client sur le réseau GSM et grâce à ce numéro en interrogeant le VLR on pourra connaître le TMSI associé à l'IMSI et grâce à cela le mobile pourra être joint par un processus dit de recherche. Le mobile sera que c'est lui qui est recherché car dans la carte SIM est stocké l'IMSI et le TMSI

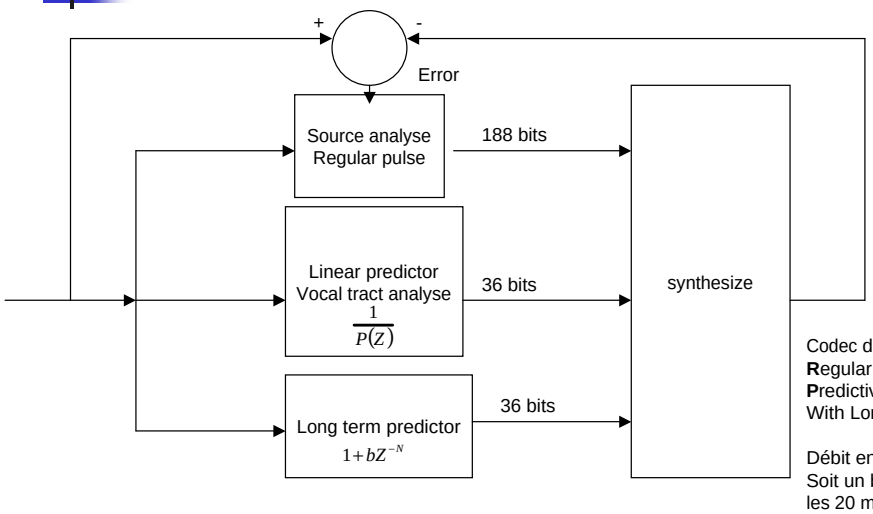


On regroupe les services offerts par le réseau GSM en 3 groupes. Le groupe le plus important et de loin est les services vocaux avec la téléphonie avec différent débits de parole possible et même des débits variables. Dans le groupe des services vocaux il y a aussi les appels d'urgence , procédure standardisée en Europe avec le 112 contrairement à la messagerie vocale qui ne fut identifié comme besoin que plus tard dans le réseau GSM. Le deuxième groupe peu utilisé à ses débuts et qui explose maintenant est le groupe des services de messages courts. Il y a bien sur les services de messages courts point à point c 'est à dire la transmission de message de 160 caractères de ou vers un mobile ainsi que la diffusion de messages courts vers des mobiles entrant dans une zone particulière de couverture. Ce dernier service est utilisé notamment pour des raisons publicitaires. Enfin plus récemment est apparu le message dit multi média qui ajoute à la transmission de messages courts un caractère multimédia comme des sonneries ou des images voir de la vidéo. Enfin le dernier groupe est celui des services supplémentaires et surtout des services de transmission de donnée dans notre cas en GSM uniquement en mode connecté, le mode paquet n 'apparaissant en effet que dans le GPRS.



Ce transparent représente la chaîne de traitement complet de la parole. Chaque élément va être étudié plus en détail dans ce qui va suivre. On a tout d'abord un codage de la parole qui revient à compresser la parole pour rendre sa transmission compatible avec les débits du GSM, on a ensuite un codage de canal qui en mettant de la redondance dans le signal va rentre la transmission plus robuste. Cette robustesse va être augmentée par les processus d'entrelacement dans le temps et le multiplexage de Burst qui va permettre de rentre le signal moins sensible aux erreurs radios. Il peut y avoir un aspect chiffrement dans la transmission de la parole et enfin une modulation pour permettre un transferts sur l'air. A la réception il y aura bien sur un processus inverse qu'à l'émission.

Les services du GSM : le codage de parole

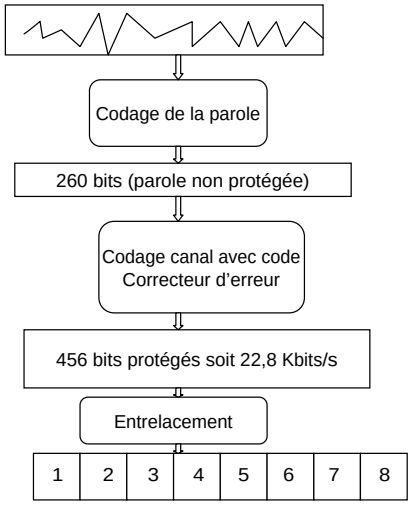


Codec de parole:
Regular **P**ule **E**xcited **L**inear **P**redictive **C**oder (RPE-LPC)
With Long Term (pitch) prediction

Débit en sortie : 13Kbits/s
Soit un bloc de 260 bits toutes les 20 ms

Le premier codeur normalisé fut le codeur RPE-LTP (**R**egular **P**ulse **E**xcitation **L**ong **T**erm **P**rediction) maintenant on trouve en plus de ce codeur le codeur AMR qui est un codeur qui adapte le flux de codage en fonction des données. Ce codeur est avant tout un compresseur de parole qui au lieu d'avoir un débit de 64 Kbits code 260 Bits tout les 20 ms soit un débit de 13 Kbits/s. Ce codeur est composé de 3 éléments, tout d'abord un filtre qui s'occupe de la corrélation à long terme qui reproduit essentiellement les fréquences fondamentales de la voix, puis un corrélateur à court terme qui s'occupe plutôt à reproduire la forme de la trachée et enfin un signal d'excitation. Les paramètres de chaque élément ne sont bien sur pas protégés de la même manière d'un point de vue codage. Les coefficients des filtres sont bien sur plus protégés que les coefficients du signal d'excitation qui peut donc être assimilé à du bruit seule la puissance du signal est important.

Les services du GSM : la protection de la parole



8 demi-burst chaque time slot ayant un burst
Provenant pour moitié de la trame actuelle pour
Moitié de la trame précédente

22/04/2006 Réseau GSM/DCS 28

La protection de la parole utilise plusieurs mécanismes de traitement du signal qui vont être développés plus en détail dans les transparents suivants. Il y a tout d'abord le code correcteur d'erreur qui en rajoutant de la redondance va permettre de passer outre certaines erreurs enfin on va ajouter un entrelacage entre trame et on va étaler cet entrelacement sur plusieurs slots pour rendre le signal plus robuste au bruit.

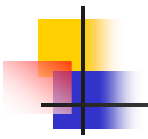
Les services du GSM : Le codage de canal 1/3

Amélioration apportées par la numérisation et le codage de canal

Systèmes	Seuil de fonctionnement C/I (porteuses sur interférences)
Analogique(FDMA)	20 dB
Numérique (TDMA avec codage et entrelacement)	9 dB
Numérique (CDMA)	-15 dB

Le codage et l'entrelacement avec le saut de fréquence
effectuent un moyennage des caractéristiques du canal dans le temps et en fréquence

Ce transparent nous montre bien l'intérêt du codage et de l'entrelacement par rapport au système analogique sans protection de traitement du signal, le rapport signal à bruit est beaucoup plus important en système analogique qu'en numérique. Le cas du CDMA ici est plus informatif, le CDMA est la technique d'accès sélectionnée par l'UMTS on voit donc que le rapport signal à bruit minimal est encore plus faible que pour le GSM.



Les services du GSM : Le codage de canal 2/3

Il y a 2 catégories de code correcteur d'erreur qui sont utilisés dans le GSM

- Les codeurs en Bloc (détection des erreurs grâce à un CRC)

  - code dit de Fire pour corriger un paquet simple (de longueur <= 11)

- Les codes convolutionnel (correction d'erreur, possibilité de décodage pondéré en un décodeur de viterbi)

Les données sont protégées avec un code convolutionnel tandis qu'on ajoute un CRC dans le cas de la signalisation

- La parole est protégée judicieusement de manière inégale

On distingue 3 classes de bits II Ia et Ib

La classe II sont 78 bits non protégés

La classe I 182 bits codés avec un code convolutionnel de taux ½

Classe Ia : 50 bits protégés par un CRC de 3 bits

Classe Ib : 132 bits sans protection supplémentaire

Total classe I+II (50+3 +132+4)*2+78 =456 bits tout les 20 ms

Les services du GSM : le codage de canal 3/3

- Les équations de sortie sont

$c^1(D) = u(D)(1 + D + D^2)$ $\quad$ $c^2(D) = u(D)(1 + D^2)$

- Si la séquence d'information vaut

  1 0 0 1 1

  11 10 11 11 01 est égale à la séquence de sortie

  On rajoute à la fin 2 taillings bits pour purger les registres à décalage, cela permet aussi de connaître à l'avance les états du codeur donc finalement on se retrouve avec

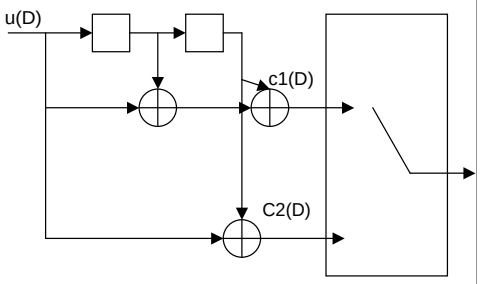
  1 0 0 1 1 0 0 en entrée

  11 10 11 11 01 01 11 en sortie

- Dans le GSM on utilise le code suivant

$g^1(D) = (D^4 + D^3 + D + 1)$

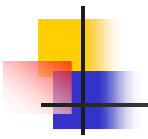
$g^0(D) = (D^4 + D^3 + 1)$



Multiplexeur

Exemple de
Codeur de taux ½ de longueur de contrainte 3

Ce transparent explique bien la notion de code correcteur d'erreur. Le but de ce code est de substitué la transmission d'un signal U(D) par la transmission de X signaux Ci(D), 1/X étant le taux du code. Les Ci(D) sont en fait des combinaisons de U(D) à différent moment temporel. Le but étant de faire du signal.



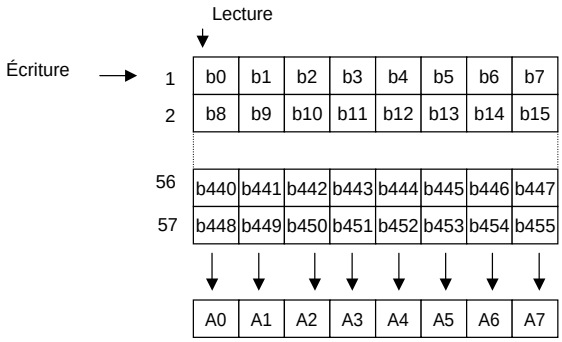
Les services du GSM : L'entrelacement 1/3

- But : étaler les erreurs dans le temps pour améliorer la correction d'erreurs ces dernières étant plus décorelées
- Il y a 2 niveaux d'entrelacement

1. Au Niveau Bit : Permutation de bits à l'intérieur d'une trame de parole
2. Niveau bloc : découpage de trame en blocs et transmission sur plusieurs bursts et surtout sur plusieurs trames voir sur plusieurs fréquences

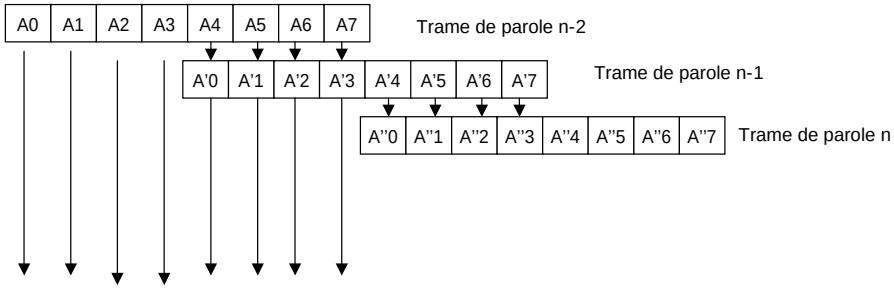
Les services du GSM : L'entrelacement 2/3

Les 456 bits de la trame de parole encodés sont transformés en 8 blocs de 57 bits : A0 à A7 grâce à la matrice d 'entrelacement



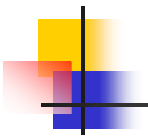
Ce transparent met bien en évidence la notion de matrice d'entrelacement qui est utilisée pour l'entrelacement au niveau Bits. On écrits 57 blocs de 8 bits en ordonnées qui sont lus en abscisse, on est ainsi passé de 57 blocs de 8 bits à 8 blocs de 57 bits. Ce sont ces 8 blocs qui vont être émis

Les services du GSM : L'entrelacement 3/3



Les trames de paroles générées toutes les 20 ms sont étalées sur 8 trames TDMA

Suite à l'entrelacement de bits on va faire un entrelacement au niveau trame, moitié par moitié on va mélanger les différentes trames et c'est ce mélange qui va être transmis sur l' interface air



Les services du GSM : Les messages courts

- Ce service est la transmission d'un message court entre un serveur et un mobile ou inversement
- Le SC ou service center est l'élément réseau qui rentre en jeu
  - Possibilité de stockage des messages en cas d'indisponibilité du mobile demandé
  - Horodatage des messages
  - Gestion d'accusé de réception sur demande de l'envoyeur
- Il y a différents types de messages courts
  - Les suites d'entiers
  - les suites de demi-octets ou d'octets (140 Max)
  - une chaîne de caractères ASCII codés sur 7 bits (160 caractères Max)
- Les applications possibles
  - Messagerie bi-directionnel
  - MMS ou EMS : Messages Multi-medias
  - Programmation ou lecture de la carte SIM à distance
  - Services supplémentaires non structurés

Les services du GSM:Les services sup 1/6

- Les services d'identification de numéro

CLIP :Calling Line Identification Presentation	Permet à l'appelé de recevoir l'identité de l'appelant
CLIR: Calling Line Identification Restriction	Permet à l'appelant d'interdire la présentation de son numéro à l'appelé
ColP Connected Line Identification Presentation	Permet d'indiquer le n°du correspondant quand l'appel est établi
CoLR Connected Line Identification Restriction	Permet à l'appelé d'interdire la présentation de son numéro à l'appelant (appel arrivé)
MCI : Malicious Call Identification	Permet l'enregistrement des paramètres de la communication

Au fur et à mesure du développement du réseau GSM se sont greffés des services autres que la transmission de la parole. Les transparents suivants vont décrire ceux définis pour la phase 2+ du GSM. Tous ces services sont appelables directement par un menu du téléphone ou en utilisant certains codes prédéfinis comme *#06# qui donne l'imei du téléphone. Ces codes prédéfinis sont standardisés et permettent ainsi aux mobiles non pourvu de l'accès direct à la fonctionnalité de faire appel à ces services

Les services du GSM:Les services sup 2/6

- Les services de renvois d'appels

CFU : Call Forwarding Unconditional	▪ Ces 4 services permettent le renvoi vers le PLMN Local ou un autre ▪ Max 5 renvois en cascade ▪ Notification possible au demandeur ou au demandé ▪ possibilité de désactivation globale
CFB : Call Forwarding on mobile subscriber busy	
CFNRy Call Forwarding On no reply	
CFNRC : Call forwarding on mobile not reachable	
CD : Call Defection	Permet à l'abonné de filtrer ses appels et de renvoyer les appels qu'il désire appel par appel

Les services du GSM:Les services sup 3/6

- Les services d'aboutissement d'Appel

CW : Call Waiting	▪ Réponse dans un délai de 30 s à 3 minutes ▪ Indication dans le canal si les 2 appels sont de type voix ou donnée ▪ Sur acceptation appel, possibilité de mise en garde de la première comm
HOLD	Mise en garde de la comm avec reprise possible
CCBS Call completion to busy subscriber CCNRy Call completion on No Reply	Indication lorsque le demandé se libère avec rappel possible. Ce service tendrait à disparaître en phase 2+

Les services du GSM:Les services sup 4/6

- Services Multi-abonnés

MPTY : Multi Party Service	Service de mise en garde de comm ou de mise en conférence
CUG : Closed user Group	Possibilité de restreindre les appels sortant ou rentrant d'un groupe d'utilisateurs
ECT : Explicit Call Transfer	Permet de mettre en relation 2 abonnés avec qui nous étions en comm phonie

Les services du GSM:Les services sup 5/6

- Les services de facturations

AoCI : Advice of charge Information	Indication du coût de communications à la fin ou en temps réel, s'applique à tous les services sauf les SMS et les communications paquets
AoCC : Advice of charge charging	Interdiction des appels dans un PLMN ne supportant pas l'advice of charge

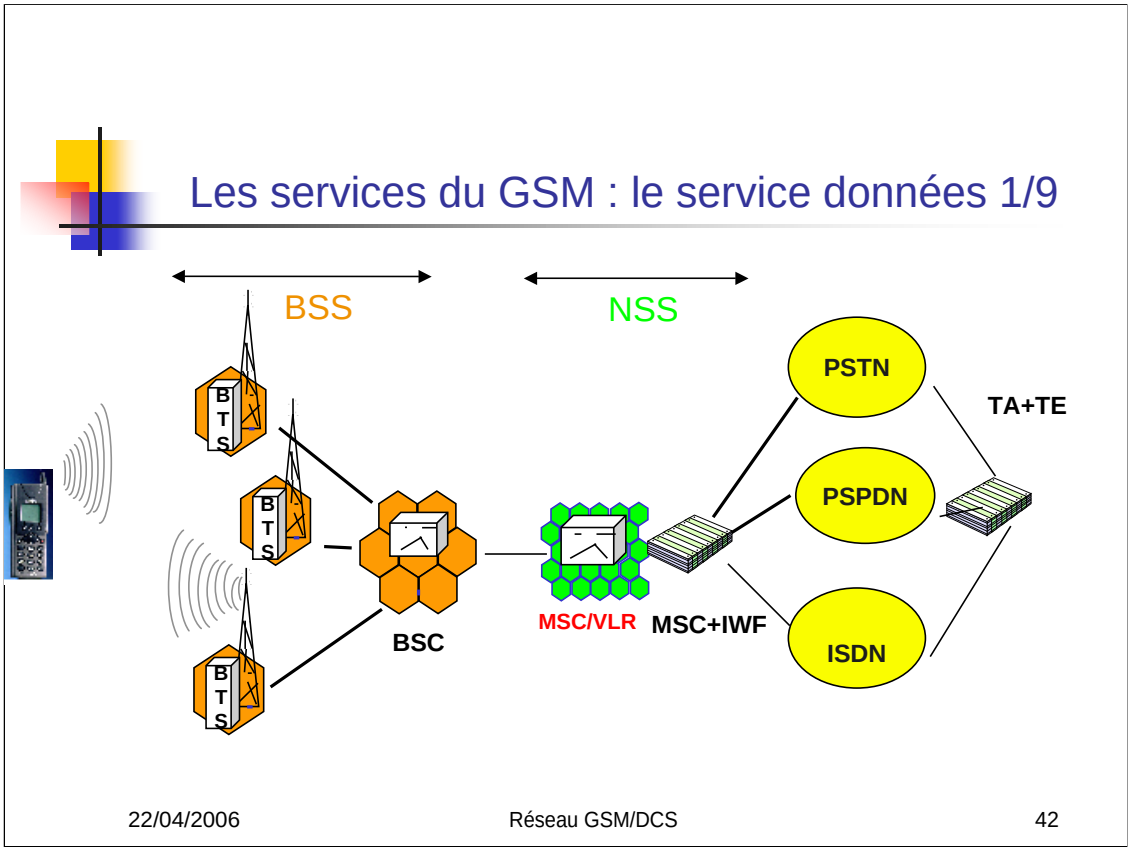
- Les services de restriction d'appels

BAOC: Barring All Outgoing Call	▪ Abonnement possible à toute combinaison ▪ Activation protégé par mot de passe généralement
BOIC : Barring All outgoing International Call	
BOIC ex HC : Barring All outgoing International Calls except those to the Home PLMN	
BAIC : Barring All Incoming Calll	
BAIC-Roam : Barring All Incoming Call when roaming	

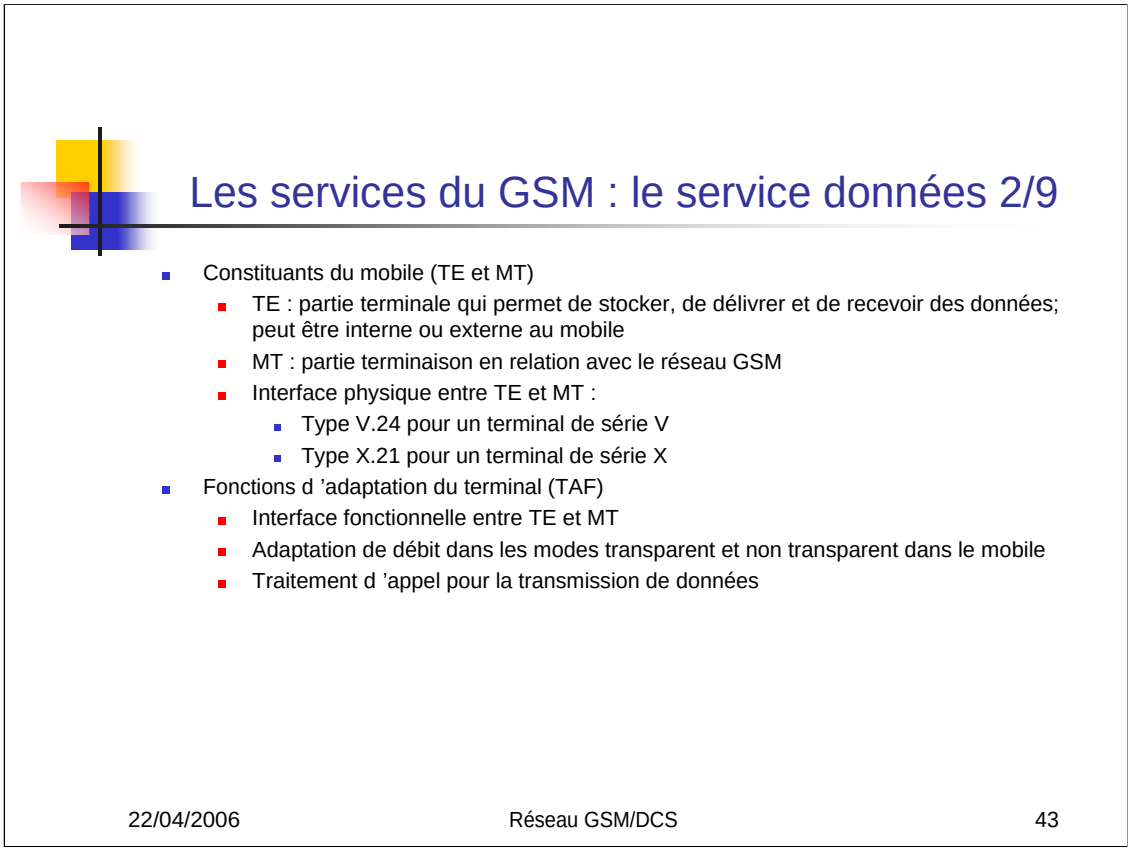
Les services du GSM:Les services sup 6/6

- Les Nouveaux services Phase 2+

UUS : user to user signaling	Permet d'émettre ou recevoir des SMS d'usagers à usagers pendant une communication ou en cours d'établissement
eMLPP : enhanced Multi_level precedence & preemption	Permet d'affecter un niveau de priorité au mobile leur permettant d'accéder plus facilement ou plus difficilement au réseau
SNPN : Support de plan de numérotation privé	Accès au sein d'un réseau privé virtuel, les traductions de numéros privés étant assurées par un manager externe



Après avoir vu les services basés sur la parole attachons nous à décrire les services de transmission de données. En effet très vite les clients ont senti le besoin de transmettre des données, au début du fax mais après des données quelconque. On voit sur ce transparent les différents acteurs du mode des données, bien sur le mobile et sa liaison au réseau GSM et ensuite les passerelles qui permettent d interconnecter un réseau GSM avec des réseaux soit numériques soit analogique avec différentes passerelles.



Ce transparent décrit plus en détail les acteurs de la transmission de donnée décrite dans le transparent précédent, on peut toutefois noté que même si les interfaces avec les réseaux de la série X sont standardisées maintenant on passe de plus en plus à des réseaux pur Ip. On voit donc que même si le réseau GSM est un réseau dit à connexion dédiée on peut s 'interfacer à des réseaux paquets

Les services du GSM : le service données 3/9

- IWF (InterWorking Functions)
  - Interface fonctionnelle entre le réseau GSM et les réseaux fixes; localisé dans le MSC
  - Adaptation de débit dans les modes transparent et non transparent
  - Traitement d 'appel (mapping des protocoles de signalisation pour la transmission de données)
- Interconnexion avec différents réseaux
  - Réseau téléphonique commuté PSTN (ou RTC)
  - Réseau à commutation de circuit ISDN (ou RNIS)
  - Réseau à commutation de paquet PSPDN (ex : TRANSPAC)

Un des aspects les plus importants du réseau est bien sur l 'aspect adaptation entre réseau, il permet notamment de gérer les différence de taille de segmentation mais aussi si nécessaire les différents protocoles . Ces fonctions là sont souvent situées dans le MSC.

Les services du GSM : le service données 4/9

- Interconnexion avec le réseau PSTN
  - Utilisation d 'un modem
    - Modem V21 : 300 bit/s asynchrone
    - Modem V22 : 1200 bit/s asynchrone - synchrone
    - Modem V22bis : 2400 bit/s asynchrone - synchrone
    - Modem V23 : 1200/75 bit/s asynchrone
    - Modem V26ter : 2400 bit/s asynchrone - synchrone
    - Modem V32 : 4800, 9600 bit/s asynchrone - synchrone
    - Modem V34 : 1200, 2400, 4800, 9600,14400 bit/s asynchrone - synchrone
  - Terminaux de série V normalisés par ITU_T qui peuvent avoir un accès au réseau PSTN

Ce transparent dresse la liste des différents modems supportés dans le cadre du GSM, on va du V21 au V34 sachant qu'aujourd'hui c'est essentiellement le V34 qui est utilisé en tout cas en europe. La qualité de débit est suffisante pour du Wap et ne trouve ces limites que lorsque l'on se sert du terminal comme Modem. Des propositions d'extensions ont été faites et augmente le débit en proposant des allocations de plusieurs slots à un même utilisateur.Ce HCSD n'est pour l 'instant pas proposé en France.

Les services du GSM : le service données 5/9

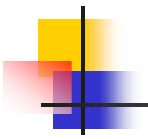
- Gestion d'appel : utilisation des commandes AT pour établissement et libération d'appel
- Interface avec le GSM
  - DTE localisé dans le TE du mobile GSM
  - Accès du modem (DCE) situé au niveau de l 'IWF
  - Comportement du réseau GSM comme un modem
  - État des signaux physiques V24 entre TE et MT transportés entre MT et IWF dans des trames de données
- Transmission du fax
  - Incorporation des modems V21, V27ter, V29
  - Débits supportés 2400,4800,7200,9600,12000,14400 b/s
  - Utilisation du protocole T30 pour les différentes phases d 'une communication entre fax

L'utilisation du mobile est vu comme un modem classique avec la gestion des commandes AT intégrée ou non dans le terminal. Il y a aussi un service de fax intégré dans la transmission de donnée même si ce service tombe un peu en désuétude avec l'arrivée du courrier électronique.

Les services du GSM : le service données 6/9

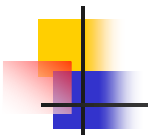
- Interconnexion avec le réseau ISDN
  - Liaison numérique de bout en bout
  - Interface physique S : 2 canaux B (données) à 64 kbit/s chacun et 1 canal D (signalisation) à 16 kbit/s
  - Interface avec le GSM
    - Conversion de protocole évidente entre l 'interface S et l 'interface radio puisque la couche de signalisation CC (Call Control) découle directement de l 'interface usager-réseau ISDN (I440/I450 sur canal D)
    - Modification des trames V110 pour faire passer d 'un débit de 64kbit/s (débit canal B) à un débit sur l 'interface radio de 14400, 9600, 4800, 2 400 kbit/s

Les 3 transparents suivants précisent les principes d' interconnexion entre les différents réseaux et notamment les fonctions d' adaptation.



Les services du GSM : le service données 7/9

- Interconnexion avec le réseau PSPDN
  - Accès au réseau PSPDN
    - Via un gestionnaire de paquet PH (Packet Handler)
    - Indirectement par le réseau PSTN
    - Indirectement par le réseau ISDN
  - Terminaux de série X normalisés par ITU_T qui peuvent avoir un accès direct ou indirect au réseau PSPDN
  - Protocoles d 'accès
    - X25 : accès direct à un réseau PSPDN à partir d 'un DTE
    - X32 : accès indirect à un réseau PSPDN via le réseau PSTN ou RTC avec une interconnexion faite par un gestionnaire de paquet



Les services du GSM : le service données 8/9

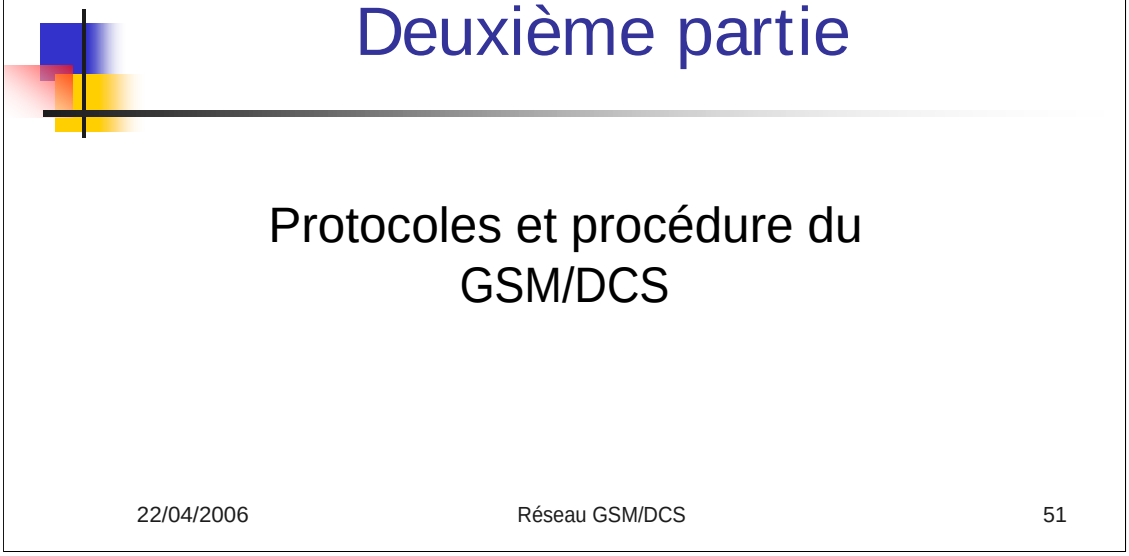
- X28 : accès indirect à un réseau PSPDN via le réseau PSTN ou RTC avec une interconnexion PAD (Packet Assembler / Disassembler)

- Interface avec le GSM
  - Accès au PSPDN par un PAD
    - accès de base PAD via PSTN : pas connaissance du réseau GSM qu 'il va accéder au réseau PSPDN
    - accès dédié PAD : connaissance du réseau GSM qu 'il va accéder au réseau PSPDN via un PAD ou un gestionnaire de paquet PH.

Les services du GSM : le service données 9/9

- 2 modes de transmission des données :
  - Mode transparent (V110)
    - Assure un flot continu d'information
    - Aucun contrôle d'erreur
    - Pas de retransmission des données
    - Contrôle de flux
  - Mode non-transparent (RLP)
    - Assure un transfert de données sans erreur
    - Débit non constant
    - Contrôle de flux

Comme dans toute transmission de données il y a 2 modes un mode dit protégé où l'on contrôle la bonne réception des données émises (RLP) et un mode transparent où il y a pas de contrôle d'erreur. Le choix entre ces 2 modes se faisant en fonction des contraintes de l'application en terme de rapidité et de sûreté. En effet pour une application nécessitant des temps de réponse rapide on privilégiera plutôt le mode transparent en reportant la gestion des erreurs sur les couches supérieures, inversement pour des transferts comme le FTP ou on a besoin des données garanties on prendra alors le mode RLP. En GPRS on retrouve la même analogie avec les modes de LLC mais ceci est un autre cours.



Deuxième partie

Protocoles et procédure du GSM/DCS

Protocoles du mobile au MSC 1/3

- **Interface MS-Réseau** :

  - niveau 1 : Protocole Radio

  - niveau 2 : LAPDm pour information il est dérivé du LAPD CCITT Q921, c'est protocole d'acquittement ou non par fenêtre glissante de taille 1. Il assure et garantie le bon acheminement des messages de couches supérieures. Il a aussi un rôle de segmentation et assemblage en fonction des profils utilisateurs.

  - niveau 3 :

    Interface avec le BSS, spécifique GSM : RR

    Interface avec le MSC : dérivé de CCITT Q931

- **Interface BTS-BSC** :

  - niveau 1 : G703, G705 CCITT

  - niveau 2 : LAPD

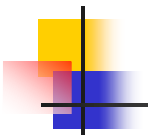
  - niveau 3 : BTSM aux BTS et BSC, RR au BSC

- **Interface BSC- MSC**

  - niveau 1 : G703 G705 CCITT, MTP SCCP

  - niveau 2 : au BSC et au MSC BSSAP

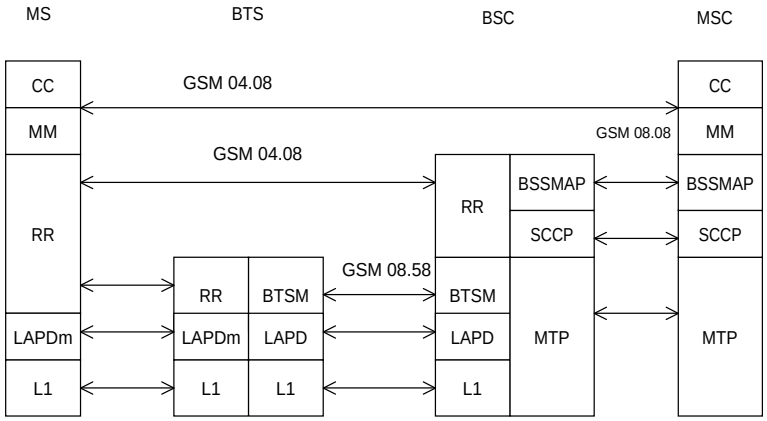
  - niveau 3 : MM, CM



Protocoles du mobile au MSC 2/3

- Les protocoles sur l'interface radio sont les suivants
  - CC ou Call Control : cette couche gère tout ce qui à un rapport avec la communication GSM de son établissement à sa terminaison
  - MM ou mobility management : cette couche gère tout ce qui à un rapport au déplacement du mobile et à sa localisation dans le réseau avant, pendant ou après la communication.
  - RR ou radio ressource : cette couche gère la liaison radio entre le téléphone et la BTS la plus proche et surtout aide à conserver la qualité du lien.
  - SS ou suplementary services : cette couche gère tout ce qui a trait aux services supplémentaires
  - SMS ou short message services : cette couche gère tout ce qui traite des messages courts
- Physiquement les informations circulent entre le mobile et la BTS
- Logiquement le Mobile communique avec les entités du BSS et le MSC

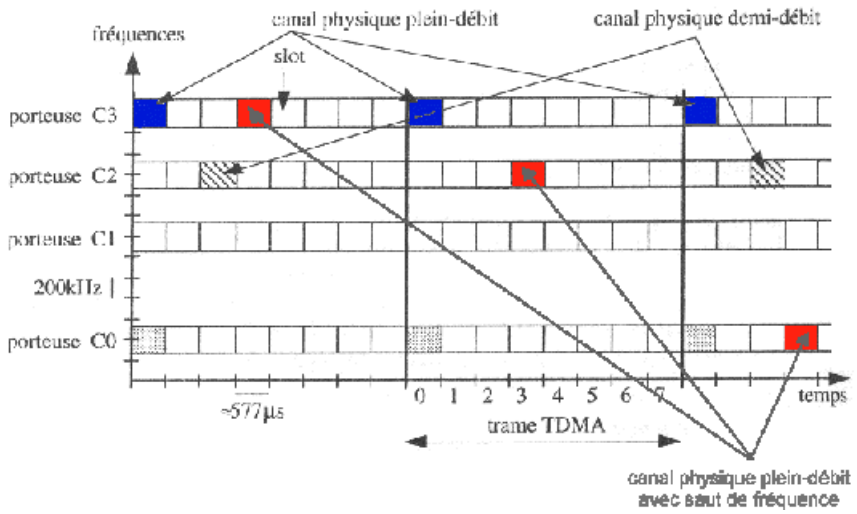
Protocoles du mobile au MSC 3/3



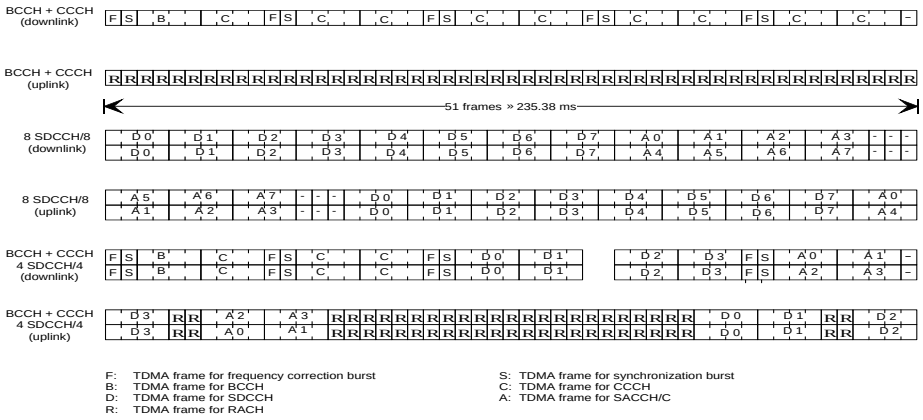
Les canaux GSM : Le multiplexage temporel 1/4

- L'accès au canal GSM est dit FTDMA c'est à dire que c'est une combinaison de 2 techniques le FDMA et le TDMA
- Pour chaque fréquence on a définit une trame que nous avons subdivisée en 8 intervalles de temps (IT)
- Un canal est donc une occurrence ou plutôt un intervalle de temps occupé régulièrement dans une trame pour une fréquence donnée ou un saut de fréquences données.
- Sur ces canaux physiques sont portés les canaux logiques du GSM qui sont multiplexés dans le temps. Leurs définitions exactes et leurs rôles seront définis plus tard dans cet exposé
- Il y a 2 types de canaux
  - Les canaux de trafic : TCH/F ou TCH/H
  - Les canaux de contrôle utilisé pour la signalisation : SDCCH, CCH, BCCH

Les canaux GSM : Le multiplexage temporel 2/4



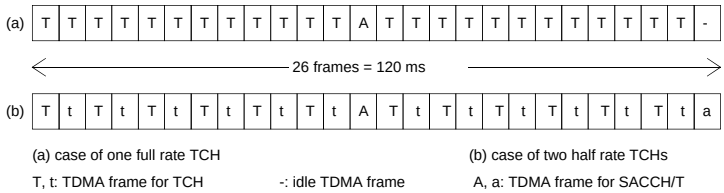
Les canaux GSM : Le multiplexage temporel 3/4



F: TDMA frame for frequency correction burst
B: TDMA frame for BCCH
D: TDMA frame for SDCCH
R: TDMA frame for RACH
S: TDMA frame for synchronization burst
C: TDMA frame for CCCH
A: TDMA frame for SACCH/C

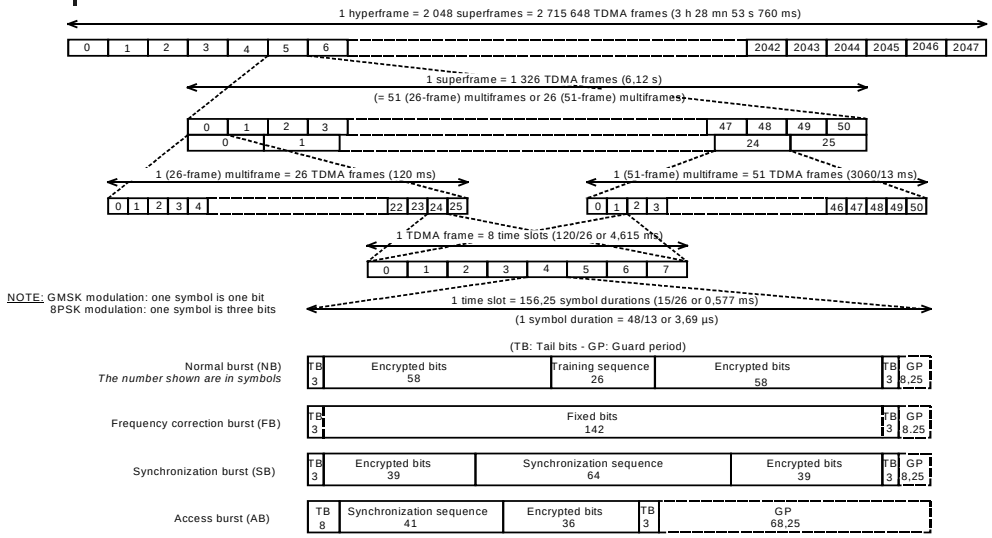
Multiplexage temporel pour les canaux de contrôle ou partagés

Les canaux GSM : Le multiplexage temporel 4/4



Multiplexage temporel dans le cas des canaux de traffic

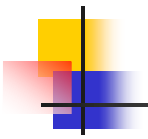
Les canaux GSM : Les structures de trames



NOTE: GMSK modulation: one symbol is one bit
8PSK modulation: one symbol is three bits

(TB: Tail bits - GP: Guard period)

Normal burst (NB) *The number shown are in symbols*	TB 3	Encrypted bits 58	Training sequence 26	Encrypted bits 58	TB 3	GP 8,25
Frequency correction burst (FB)	TB 3	Fixed bits 142			TB 3	GP 8,25
Synchronization burst (SB)	TB 3	Encrypted bits 39	Synchronization sequence 64	Encrypted bits 39	TB 3	GP 8,25
Access burst (AB)	TB 8	Synchronization sequence 41	Encrypted bits 36	TB 3	GP 68,25	



Les canaux GSM : Les canaux de contrôle 1/2

- Les canaux de contrôle diffusés

  Ce sont les canaux **BCCH** et **CCCH**, ils sont généralement sur le « time slot » 0 d'une fréquence de la cellule

  - **BCCH** : Broadcast Control Channel, il est utilisé pour la diffusion d'informations système appelés SYSTEM INFORMATION. Il y a différent types de SYSTEM INFORMATION qui correspondent aux différentes informations que le système a besoin de diffuser pour une bonne marche de celui ci

  - **CCCH** : Common Control Channel, ces canaux permettent l'accès à la cellule

    - **RACH** : Random Acces Channel, il correspond au CCCH montant où s'effectuent les accès aléatoires du mobile à travers le message Channel Request

    - **PCH** et **AGCH** Paging channel et Acces Grant Channel, ils composent le CCCH descendant.Toutefois il y a une certaine flexibilité du partage du CCH descendant, le PCH et l'AGCH ne sont pas forcément disjoints et même dans le cas combiné une partie de la ressource du CCH est utilisée pour des SDCCH.

      Sur le PCH sont envoyés les messages de type PAGING REQUEST type 1,2,3 leur rôles seront développés plus tard dans cet exposé

      Sur l'AGCH le réseau envoie l'allocation immédiate suite à un accès aléatoire du mobile, le message est donc IMMEDIATE ASSIGNMENT

Les canaux GSM : Les canaux de contrôle 2/2

- Les canaux de contrôle dédiés ou **DCCH**

  Il y a 3 types de canaux de contrôle dédiés SACCH, FACCH et le SDCCH

  - **SACCH** : Slow Associated Control Channel, ce canal est toujours associé à un TCH ou SDCCH. Il permet pendant une communication dédiée de recevoir les informations systèmes à savoir dans le sens montant les SYSTEM INFORMATION de type 5 et 6 qui donnent les cellules voisines à surveiller d'un point de vue mesures mais aussi les messages courts entrants. Dans le sens montant il remonte les mesures du mobile à travers les messages MEASUREMENT REPORT mais aussi les messages courts sortants.

  - **SDCCH** : Stand Alone Dedicated Channel, ce canal n'est pas associé à un autre canal. Il sert seulement aux échanges de signalisation et est souvent utilisé lors de la première phase d'établissement du canal dédié. Il est de même utilisé pour des transactions ne nécessitant pas de canal de trafic comme les messages courts, les services supplémentaires

  Plusieurs SDCCH peuvent utiliser un seul Time Slot ou IT et permettent d'économiser des ressources radio se substituant à un TCH

  - **FACCH** : Fast Associated Control Channel, il est obtenu par vol de trames sur un TCH dans certaines situations où un besoin de signalisation rapide est indispensable comme dans le cas d'un HandOver

Les canaux GSM : Les canaux de trafic

- Les canaux de trafic dédiés:

  - **TCH** : Trafic Channel

  Il y a 2 types de TCH, le TCH/F pour Trafic Channel Full Rate et le TCH/H pour Trafic Channel Half Rate. Ils sont utilisés en fonction du débit de l'application que nous avons à transmettre, à l'origine c'était uniquement de la parole codée à plein débit ou à demi_débit en fonction du codeur utilisé. Sur un IT peuvent passer un TCH/F ou 2 TCH/H

- Les canaux de trafic diffusés:

  - **CBCH** : Cell Broadcast Channel, utilisé par les messages courts diffusés il a la même structure qu'un SDCCH

Les informations système dans le GSM

- Ces informations ont un rôle indispensable aussi bien avant l'attachement GSM qu'avant la communication ou pendant celle ci.
- Sur l' IT 0 on doit trouver les informations dont dispose le MS en veille à savoir les SYSTEM INFORMATION 1,2,3,4 voir 5 bis 7 et 8. On doit aussi trouver les informations dont dispose le réseau à l'établissement de la communication à travers AGCH et le PCH.
- En veille les SYSTEM INFORMATION de type 1,2,3 ou 4 permettent de transmettre
  - L'identifiant de la cellule
  - Les cellules voisines à surveiller
  - La zone de localisation
  - les informations indispensables à l'accès de la cellule exemple : la cellule est interdite ou non, les classes d'accès……
- En communication les SYSTEM INFORMATION de type 5 ou 6 permettent
  - de connaître les cellules voisines
  - les codes de couleurs autorisés par le réseau (NCC)
  - les options de la cellule (radio link timeout, DTX...)

Les fonctions et les procédures du système

- La localisation :
  - suivre les déplacements des abonnés en terme de LA (Zone de localisation) au moyen des HLR et des VLR
- Établissement d'appel :
  - établir des communications entre abonné mobile et abonné d'un autre réseau
  - appel sortant normalement effectué par un abonné enregistré dans un VLR, le système doit donc fournir les données nécessaires au VMSC
- Transfert de communication :
  - assurer la continuité d'un appel quand l'abonné mobile quitte la cellule de service (Handover)
- Fonction de sécurité :
  - confidentialité de l'IMSI par utilisation du TMSI
  - authentification
  - chiffrement

Le mode veille en GSM : présentation générale

- La tâche du mobile en mode veille peut se décomposer en 3 sous processus
  - La sélection du PLMN
  - La sélection et la resélection de cellule
  - La mise à jour de localisation

  Les 2 premières sont invisibles d'un point de vue réseau n'impliquant aucune demande sur un canal partagé ou dédié

Le processus global de sélection initial et resélection

- La sélection initiale

  Elle a lieu à la mise sous tension ou suite à un trou de couverture. Le mobile doit rechercher un BCCH parmi les 124 fréquences du GSM ou DCS et sélectionner un réseau

  Les étapes sont les suivantes :

  - Mesures de niveau sur toutes les porteuses du système ou sur les dernières stockées en SIM
  - Recherche de BCCH parmi les 30 canaux les plus forts (40 en DCS) et lecture des informations dans l'ordre décroissant des puissances
  - Sélection de la cellule acceptable(PLMN correct, accès autorisé, C1 >0) dont le niveau reçu est le plus fort
  - Mise à jour de la localisation

- La resélection

  En permanence le MS déroule le processus suivant

  - Resélection de cellule avec ou sans mise à jour de la localisation
  - Resélection éventuel de PLMN en fonction de la liste de priorités et surtout la recherche périodique du HPLMN en roaming

Sélection de PLMN 1/2

- Sélection de PLMN en mode automatique

  Ce mode est celui par défaut de nombreux mobiles ses principes sont les suivants:

  - Le mobile sélectionne et tente une mise à jour de localisation sur les autres PLMNs présents et autorisés dans l'ordre suivant

    1 : HPLMN si ce n'était pas le PLMN sélectionné

    2 : les PLMNS du champ SIM « PLMN selector » par ordre de priorité

    3 : les autres PLMN pour lesquels le signal reçu est supérieur à -85 dBM dans un ordre aléatoire

    4 : tous les autres PLMN dans l'ordre décroissant des puissances

  En mode automatique le Mobile en itinérance nationale doit périodiquement tenter de sélectionner le réseau nominal (HPLMN)

  Si la sélection a échoué par absence de PLMN le mobile sera dans l'état « No service », si elle a échoué suite à des échecs de mise à jour le mobile sera en « service limité » sur le premier réseau disponible, il ne pourra alors passer que des appels d'urgence.

  Si l'utilisateur force la resélection de PLMN, le PLMN de départ n'est pas éligible à la liste des PLMN candidats sauf si c'est le seul

Sélection de PLMN 2/2

- Sélection de PLMN en mode manuel

  Le mobile indique tous les réseau disponibles y compris ceux interdits. Ils sont présentés dans l'ordre décroissant de puissance.

  Sur sélection d'un PLMN le mobile tentera une mise à jour de localisation sur ce réseau, sinon il restera sur le précédent.

  En cas d'échecs pour les mêmes causes que celles du mode automatique le mobile rentrera dans les mêmes états finaux à savoir « service limité » ou « pas de service »

Sélection/resélection de cellule

- BBCH :

  La sélection de cellule utilise

  - soit les BBCH identifiés parmi les canaux RF présents les plus forts
  - soit la liste de BCCH mémorisés lors de la dernière remontée de mesures
  - soit la liste de BCCH voisins diffusés par le PLMN sur lequel le mobile est enregistré

  Dans les cas normaux de sélection le mobile utilise la liste diffusé de BCCH, cela permet d'éviter au mobile de scanner toutes les fréquences du systèmes.

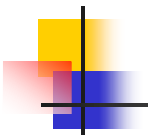
  De plus une bonne planification et une diffusion correct de cette liste, permet d'éviter de capter et de rester prisonnier d'une résurgence de cellules lointaines.

  En permanence le mobile effectue des mesures sur son BCCH et ceux voisins ce qui permet d'affiner la liste diffusée.

- Les conditions et critères de sélection/resélection

  Une cellule est sélectionnée si elle n'est pas barrée,si son critère C1 de puissance est positif et si sa priorité donnée par le critère C2 est la meilleure.

  Le mobile part en resélection si C1 devient négatif, si le critère c2 d'une cellule voisine est meilleur que la cellule courante, si ces RACH sont infructueux ou enfin s'il y a une coupure de communication



Activité du mobile en veille

- En veille le mobile écoute et décode le BCCH de service où sont diffusés les SYSTEM INFO 1 à 4, il a ainsi la description du CCCH, la zone de localisation, la liste des cellules voisines à surveiller…..
- Il écoute le canal de recherche PCH dans l'attente d'un éventuel appel entrant, en fait le mobile n'écoute que son canal propre qu'il détermine en fonction de son IMSI et d'un paramètre réseau le BS-PA-MFRMS. Cette écoute discontinue lui permet d'économiser sa batterie
- Il exécute en permanence l'algorithme de sélection/resélection décrit précédemment

Sortie du mode veille

- Le mobile quittera le mode veille pour recevoir des appels, émettre des appels, effectuer une localisation ou pour faire toutes autres transactions liées aux services supplémentaires. Dans ce cas il passera en mode dédié.
- On parlera de mode dédié lorsque un canal est alloué au mobile pour ses échanges avec le réseau, la transition du mode veille au mode dédié se fera par la procédure IMMEDIAT ASSIGN
- Pour mener à bien la procédure d'IMMEDIAT ASSIGN le mobile devra passer par 3 étapes indispensables
  - L'accès aléatoire
  - L'allocation initial
  - Les messages initiaux

L’accès aléatoire 1/2

- Rappel : le CCCH montant est le RACH, le CCCH est commun à tous les mobiles de la cellule
  Pour accéder le mobile émet un Burst sur le RACH correspondant à son CCH group et ceci d’une manière aléatoire. Ensuite il se mettra en attente de la réponse du réseau sur l’AGCH. En cas de non réponse le mobile retente son accès jusqu’à MAX RETRANS+1 fois, ensuite s ’il n’a toujours pas de réponse il partira en resélection.
- Les CCCH se trouvent sur les IT 0,2,4,6 et les mobiles se répartissent sur ces IT en fonction de leur CCCH-Groups qui dépendent de l’IMSI. Il y a autant de groupes que de IT de CCH
- Chaque abonné possède en plus une classe de priorité d’accès au réseau
  - Classes 0 à 9 : normales
  - Classes 10 à 15 : prioritaires par exemple les pompiers ou la police
- Dans les informations du BCCH 1 bit par classe, indique si cette classe est autorisée ou non sur la cellule donc si le mobile à droit d’accès sur la cellule , les appels d’urgences sont classés classe 10

L’accès aléatoire 2/2

- Le message envoyé pour l’accès aléatoire sur le RACH est CHANNEL REQUEST
  Ce message est très court et contient un octet et un seul pour laisser des bits de gardes en nombre important. L’identité du mobile n’est pas contenu dans le message et le réseau ne distingue pas les différentes tentatives d’accès du mobile

- Le CHANNEL REQUEST contient :
  - Une référence aléatoire : elle permet de distinguer les mobiles et éviter les collisions (résolution de contention)
  - Une cause d’établissement sur 5 bits en phase II du GSM, réponse au paging, reprise d’appel, appel sortant, service supplémentaire, mise à jour de localisation, appel entrant….

- Le CHANNEL REQUEST est transmis par la BTS au core network et notamment auu BSC dans le message Channel Required en y joignant le délais d’accès ainsi que le numéro de trame, le réseau pourra ainsi calculer le timing of advance du mobile ou en français, le décalage temporel entre la station et le mobile.

Allocation Initiale : description générale 1/2

- Channel request reçu à la BTS sur l'interface radio est transporté dans Channel Required sur l'interface Abis
- Recevant Channel Required, le BSC active un canal à la BTS : elle envoie le message Channel Activation au TRX à activer et y indique le canal qui doit être activé. Channel Activation Ack est envoyé par la BTS comme acquittement.
- Le BSC ordonne à la BTS d'allouer ce canal : il envoie sur l'Abis le message Immediate Assignment Command :
- La BTS traduit ce message en un message Immediate Assignment sur l'Interface Radio
- L 'Immediat Assign est envoyé sur l'interface radio sur le CCH descendant à savoir l' AGCH sur le même IT que le channel request a été reçu, et permet d'allouer le canal. Il contient en plus la description physique du canal

Allocation Initiale : description générale 2/2

- En fait 3 messages permettent de répondre à un accès aléatoire :
  - Immediate Assignment :

    Il contient
    - Le numéro de trame
    - la référence aléatoire
    - la description d'un canal aloué
    - une avance en temps

  - Immediat assignment extended

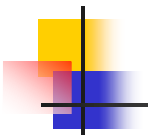
    Il permet d'adresser plusieurs mobiles en même temps

  - Immediat assignment reject

    Il sert à rejeter les accès aléatoires et est utilisé lorsqu'il n'y a plus de ressources disponibles dans la cellule. On notifie alors au mobile d'attendre avant de recommencer sa tentative d'accès. Il contient donc les infos suivantes : la référence aléatoire, le numéro de trame et l'indication d'attente(T 3122)

Allocation initiale : Message initial

- Lorsque le mobile a pris en compte une allocation immediate correspondant à l'un de ses 3 derniers Channel Request, il stoppe les retransmissions et établit le niveau 2.
- Du point de vue réseau l'établissement du niveau 2 sur ce canal termine la procédure d'allocation immédiate : la connexion RR existe et le Niveau MM en est informé
- Le mobile a encapsulé dans le premier message de niveau 2 un message de niveau 3 de demande de service, ce message est appelé message initial.
- Les messages initiaux jouent aussi un rôle important lors de la résolution de contention, car suite à ces messages il y aura au niveau 2 un échange de SABM/UA et seul le mobile le plus fort se verra accorder le canal
- Les messages initiaux sont des Messages MM, ils contiennent tous l'identité du mobile son classmark et sa clef de chiffremenent
- Les messages initiaux sont les suivants :
  - Location Updating request
  - Paging Response
  - CM service request
  - CM reestablishment request



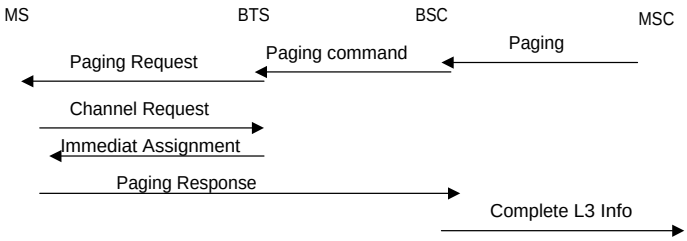
Allocation initiale : Avance en temps

- L'avance en temps est destiner à compenser le délai de transmission fonction de la distance entre le mobile et la BTS.
- Le mobile accède avec une avance en temps nulle; La BTS calcule le retard d'accès du mobile et cette information est transmise au BSC dans le channel required.
- Dans l' Immediat Assignment, l'avance en temps que devra utiliser le mobile pour accéder sur le canal dédié est indiqué.
- Par la suite un asservissement de cette avance est faite entre le mobile et la BTS, le mobile indique dans le SACCH l'avance qu'il utilise, le réseau en réponse lui dit celle qu'il doit utiliser.
- Lors du Handover l'avance en temps n'est plus la même il faut donc l'acquérir par une procédure assez proche

  Channel Request ⇔Handover Acces, Channel Required ⇔Handover Detection, Immediate Assignment ⇔Physical Information

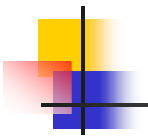
Procédure de Paging 1/2

- C'est la fonction de « recherche » qui permet les appels entrants
- Le mobile écoute le PCH en fonction du paging mode et prend en compte tous les messages correspondants
- Les différents modes de paging sont les suivants
  - Normal : Le mobile écoute son sous canal seulement
  - Etendu : Le mobile écoute son sous canal et 2 blocs plus loin
  - Réorganisation : Le mobile écoute tous les pagings
  - Pas de changement : Le mobile garde son mode précédent



Procédure de Paging 2/2

- On peut pager avec IMSI ou le TMSI mais pas avec l'IMEI
- Il y a différent types de Paging Request
  - Le type 1 qui permet de chercher jusqu'à 2 mobiles
  - Le type 2 qui permet de chercher jusqu'à 3 mobiles, les 2 premiers étant pagés avec le TMSI
  - Le type 3 qui permet de chercher jusqu'à 4 mobiles mais dans ce cas là tous avec le TMSI
- Le Paging Reponse est un message initial et doit contenir l'IMSI si jamais le paging a été fait avec celui ci
- Sur l'interface A le Paging contient l'IMSI, éventuellement le TMSI et la liste des cellules
- Sur l'interface Abis le Paging Command contient la description du CCCH, le paging group et l'identité du mobile TMSI ou IMSI



Procédure de sécurité : description générale

- La sécurité a été une préoccupation importante lors de la définition de la norme GSM et ceci pour se distinguer des normes analogiques pas assez sures.

- Les fonctions de sécurité sont définis dans la norme GSM 02.09 et reposent sur 3 notions
  - L'authentification de l' IMSI (lors de l'accès à un service ou lors de l'accès initial au réseau)
  - Confidentialité de l 'IMSI qui n'est utilisé que dans les cas obligatoires, dans les autres cas le mobile ou le réseau utilise le TMSI, seul le VLR connaît la correspondance entre l' IMSI et le TMSI
  - Confidentialité des données abonné grâce au chiffrement des transmissions après une phase d'authentification et d'échange de paramètres de chiffrement.

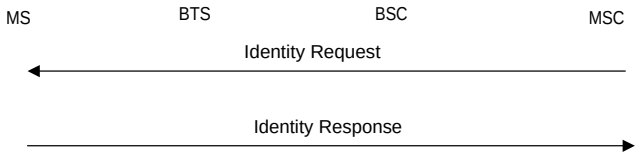
Procédure de sécurité : Identification 1/2

- Il y a 3 types d'identité dans le mobile comme nous avons vu dans la première partie

1. IMSI : International Mobile Subscriber Identity , c'est une identification unique valable dans tous le réseau GSM. Elle est allouée une fois pour toute par l'opérateur à l'abonnement et reste normalement inconnu de l'abonné. Elle est stockée à la fois dans la SIM et dans un des HLR du HPLMN. Elle offre en partie une fonction d'adressage (le VLR en dérive l'adresse du HLR)
2. TMSI : Temporary Mobile Subscriber Identity, elle est allouée par le VLR à ses visiteurs. Sa signification est locale et est valable dans une zone de localisation donnée. Elle est stockée dans la zone de localisation de la SIM et dans le VLR. Elle est optionnel pour l'opérateur mais elle permet de protéger l' IMSI mais surtout étant de longueur plus courte que l' IMSI, elle est lors des procédures de paging plus efficace permettant d'adresser plus de mobiles.
3. IMEI : International Mobile Equipment Identity, cette identification unique par mobile est allouée par l'autorité réglementaire qui délivre l'agrément du mobile. Le réseau peut accéder à cette IMEI pour pouvoir le contrôler et interdire ou pas l'accès de tel ou tel mobile.

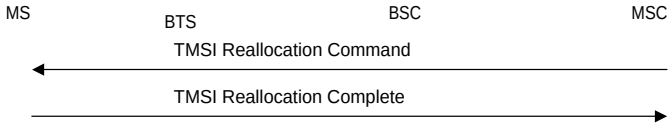
Procédure de sécurité : Identification 2/2

- Cette une procédure MM

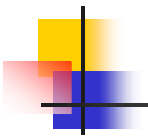


Procédure de sécurité : Allocation de TMSI

- Pour protéger l'identité de l'abonné on utilise le plus souvent possible le TMSI
- Rappel : Le mobile transmet son identité dans le message initial. Le type d'identité obéit à la règle suivante : Le TMSI si possible, sinon l' IMSI, l' IMEI n'étant utilisé si on tente un appel d'urgence sans SIM
- Il y a 2 façons d'allouer un TMSI, une procédure MM de réallocation de TMSI ou une procédure de mise à jour de localisation



Le TMSI et la zone de localisation sont stockés dans la carte SIM. Le réseau peut effacer le TMSI en envoyant l' IMSI dans le TMSI Reallocation Command

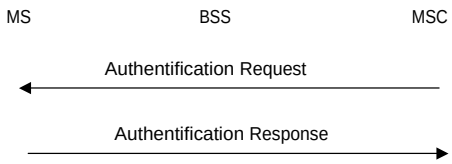


Procédure de sécurité : Authentification 1/2

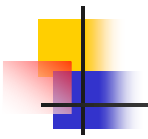
- L'authentification a 2 buts :
  - Vérifier que l'identité fournie par le mobile est correct
  - Fournir les paramètres permettant de calculer la clé de chiffrement
- Chaque abonné possède une clé **KI** allouée avec l' **IMSI** lors de l'abonnement. La carte SIM calcule alors la signature **SRES** associée au nombre aléatoire **RAND** en utilisant **l'algorithme A3** et la clé KI. Le réseau compare ce résultat à celui qu'il calcule de son coté si les 2 sont égaux le mobile est identifié.
- Les seules données à être transmises sont RAND et SRES et jamais KI.
- Seul le HPLMN a connaissance de la clef KI donc en roamming l' Authentification center du HPLMN transmet des triplets associés à l'IMSI au VLR. En phase I la clef KI pouvait être transmise au VLR mais la sécurité n'était pas optimum

Procédure de sécurité : Authentification 2/2

- Procédure MM



Le message **Authentification Request** contient : CKSN, RAND
Le message **Authentification Response** contient : SRES
Dans le cas où le SRES est incorrect le réseau envoie le message **Authentification Reject**, le mobile ne peut plus que faire des appels d'urgence.
Toutefois si le TMSI a été utilisé on réessaye avec l' IMSI avant d'envoyer l' Authentification Reject.



Procédure de sécurité : Chiffrement 1/3

- Le chiffrement a 2 buts : protéger les identités des usagers mais aussi protéger les donnés des usagers.
- La première étape est la détermination de la clef de chiffrement. Lors de l' authentification le mobile calcule également la clef **Kc** de chiffrement associé à **RAND** à partir de **l'algorithme A8** et de la clef **KI**. On parle alors de triplets d'authentification (RAND, SRES, Kc)
- Le chiffrement s'effectue dans la couche de niveau en fonction des versions disponibles de **l'algorithme de chiffrement A5** disponible avec la clef Kc.
- A Kc est associé le numéro de clef **CKSN** qui est contenu dans le message initial, ceci permet de ne pas réauthentifier dans tous les cas, tout en s'assurant que le mobile et le réseau utilise la même clef lors du chiffrement

Procédure de sécurité : Chiffrement 2/3

- Le chiffrement est ordonné par le MSC grâce au **Cipher Mode Command**, ordre transmis sur l'Abis par **Encryption Command**.
- Sur l'interface Radio les messages sont les suivants :

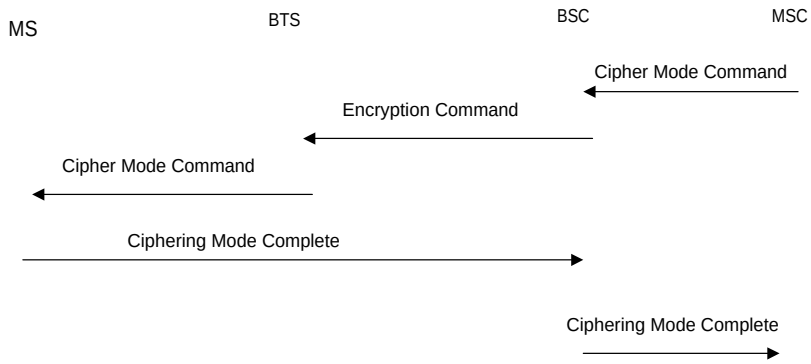
  - **Ciphering Mode Command** : Il contient le type d'algorithme à utiliser et le mode de chiffrement (marche ou arrêt). La BTS commence le chiffrement dès qu'elle a envoyé ce message, le mobile lui commence le chiffrement dés sa réception.

  - **Ciphering Mode Complete** : La BTS commence le déchiffrement à partir de la réception d'un premier message L2 correctement chiffré

  - **Ciphering Mode Reject** : si le démarrage ou l' arrêt du chiffrement c'est mal passé

- L' IMEI peut être demandé lors des phases de chiffrement et lors de Handover il peut être nécessaire de stopper provisoirement ou définitivement le chiffrement en fonction de la disponibilité de cette fonctionnalité sur la cellule cible.

Procédure de sécurité : Chiffrement 3/3



Mise à jour de Localisation vue du mobile : 1 / 6

- Afin de recevoir des appels entrants le mobile doit être localisé en permanance dans le réseau. La localisation n'est pas au niveau cellule mais plutôt groupement de cellule.
- Cette mise à jour est à l'initiative du mobile qui pour cela doit quitter le mode veille et demander une mise à jour de localisation.
- Il effectue un accès aléatoire (channel request)et se voit allouer un canal dédié (immediat assignment) qui est généralement un SDCCH et effectue alors sa demande par le message initial **Localisation Updating Request**.
- Le réseau notifie la prise en compte de la localisation par le message **Localisation Updating Accept**.
- Il existe 3 types de mise à jour de localisation :
  - La Normale : lorsque le mobile détecte un changement de LA suite à la mobilité
  - La périodique : à échéance d'une temporisation
  - IMSI attach : dans certain cas au démarrage du mobile

Mise à jour de Localisation vue du mobile : 2 /6

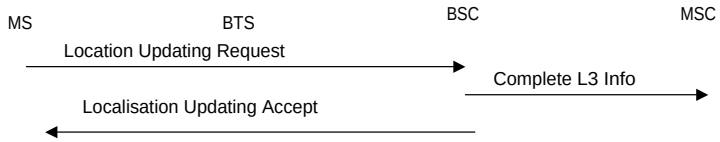
- Mise à jour de localisation Normale : Le mobile compare la LA (Localisation Area) diffusée à la LA mémorisée sur sa SIM, il effectue une mise à jour de localisation lorsqu'il détecte un changement suite par exemple à une resélection ou tout simplement à l'allumage

- Mise à jour périodique : Le mobile effectue une mise à jour de localisation périodique à l'échéance d'une temporisation qui court en mode veille, quels que soient les événements de sélection ou resélection. Cette mise à jour permet de borner le temps pendant lequel le mobile peut être perdu suite à un problème de perte de données dans le réseau. La valeur limite de cette temporisation T3212 est diffusée dans les SYS INFO 3 et 4 et peut être infinie. Dans ce cas là aucune mise à jour périodique aura lieu. Cette temporisation est aussi remise à zéro à chaque accès réussi au réseau.

- Mise à jour de localisation de type IMSI attach : le réseau indique par un flag sur le BCCH s'il souhaite que le mobile effectue des mises à jour de localisation de type IMSI attach. Une telle mise à jour a alors lieu lorsque le mobile est allumé dans une zone qui est la LA qu'il a en mémoire. Si le réseau ne demande pas l'attach, ce cas ne donnerait pas lieu à une mise à jour de localisation. Si la LA est différente de la LA mémorisée dans ce cas une mise à jour normale à lieu

Mise à jour de Localisation vue du mobile : 3 /6

Procédure MM



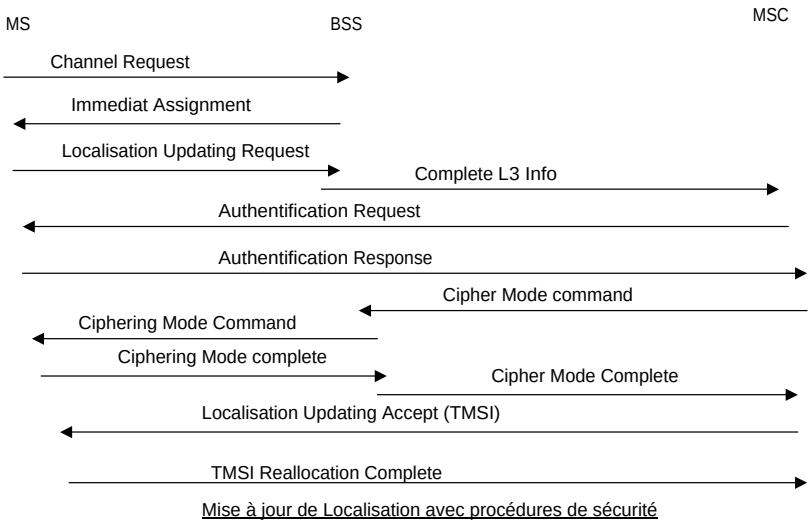
Sur l'interface Radio on trouve les messages suivants :

- **Location Updating Request** :
  L'identité du mobile
  La classe du mobile
  CKSN
  LA Mémorisé
  Type de localisation
- **Localisation Updating Accept** :
  La nouvelle LA
  L'identité du mobile (optionnel)
- **Localisation Updating Reject** :
  La cause

Mise à jour de Localisation vue du mobile : 4 /6

- La réallocation de TMSI au cours de la mise à jour de localisation peut se faire de 2 façons
- Une manière de réallocation de TMSI peut être l'envoie de la commande **TMSI Reallocation Command** ou bien implicitement en mettant un nouveau TMSI dans le message **Location Updating Accept**. La présence de l'IMSI dans ce message provoquera alors l'effacement du TMSI
- Le mobile répondra au **TMSI Reallocation Command** par un **TMSI Reallocation Complete**
- On notera que c'est le VLR qui gère les TMSI donc un changement de VLR impliquera un changement de TMSI. Un VLR couvre plusieurs LA et bien souvent le TMSI n'est valable que dans une LA donnée

Mise à jour de Localisation vue du mobile : 5 /6

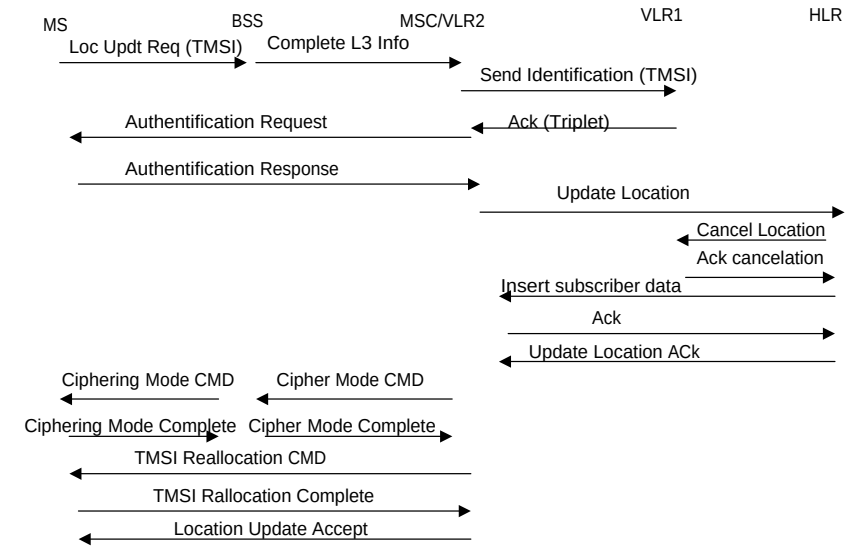


Mise à jour de Localisation avec procédures de sécurité

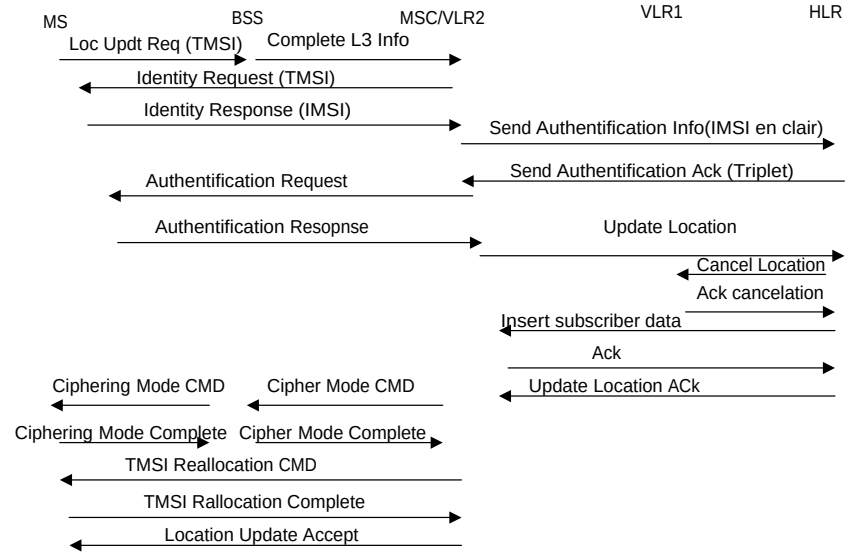
Mise à jour de Localisation vue du mobile : 6 /6

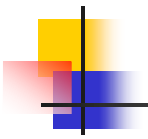
- Toutefois la localisation peut échouer, en fonction de la cause d'échec le mobile adopte un comportement différent
- Si la localisation est refusée par ce que l'IMSI est inconnue ou que le mobile n'est pas autorisé, on efface toutes les données de la SIM et la carte est considérée invalide, seuls les appels d'urgence sont autorisés
- Si la localisation est refusée avec comme cause PLMN Not allowed ou LA not allowed ou National Roaming Not Allowed on efface les données d'identification de la SIM et on active le compteur d'échec de localisation. Le mobile mettra ensuite à jour ses listes de PLMN ou LA interdits à jour. En cas de refus de roaming le Mobile devra faire une nouvelle sélection de PLMN.
- Le compteur n'est là que pour limiter le nombre d'essais de localisation infructueux

Mise à jour de Localisation vue du réseau 1/2



Mise à jour de Localisation vue du réseau 2/2



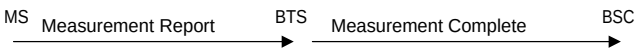


Procédure de detach vue du mobile

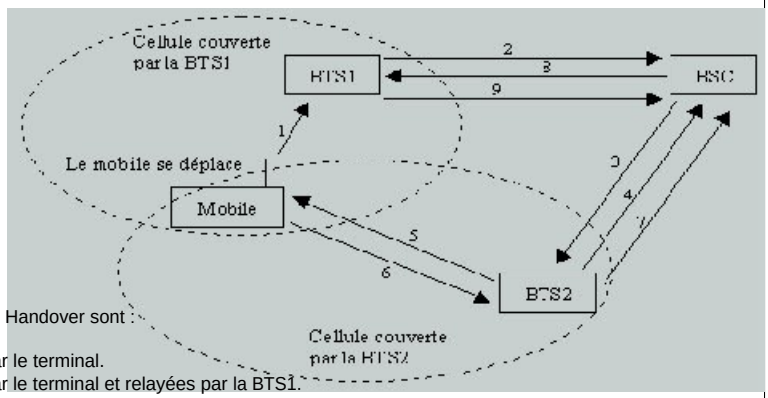
- Le Flag ATT sur le BCCH indique si les procédures d'attach/detach sont requises sur le réseau.
- La procédure d'IMSI detach est un détachement explicite du réseau (contrairement au détachement implicite qui est un effacement de la présence du mobile après un certain délais de non contact avec celui ci).
- Cette procédure est déclenchée lorsque le mobile est désactivé ou lors du retrait de la carte
- Le mobile envoie alors le message **IMSI Detach Indication** qui ne nécessite pas d'acquittement du réseau

La procédure de Handover 1/6

- C'est la procédure de « transfert » qui permet le maintien des communications au changement de la cellule. Cette procédure s'appuie sur les différentes mesures faites par le mobile.
- La procédure de mesure : Lorsqu'il est en communication, la station mobile doit en permanence effectuer des mesures sur des cellules voisines qui lui sont indiquées dans les SYS INFO 5 et 6. Il constitue des messages **Measurement Report** envoyés sur le SACCH montant, ces messages contiennent entre autre les mesures de puissances et de qualité sur son canal BCCH et sur les voisins. Cette remonté de mesures ce fait au moins tous les 1 à 2 blocs selon la présence ou non de messages courts.
- La BTS associe aux mesures du mobile ses propres mesures sur le canal dédié et transmet vers le MSC le **Measurement Result**.
- Sur la Base de ces mesures et d'autres critères de planification réseau le mobile ou le réseau décide que la cellule courante n'est pas la meilleure et initie la procédure de Handover

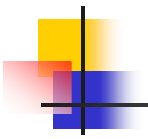


La procédure de Handover 2/6



Les phases successives permettant Le Handover sont :

1. Rapport des mesures effectuées par le terminal.
2. Rapport des mesures effectuées par le terminal et relayées par la BTS1.
3. Décision d' handover, allocation d'un canal de trafic à la BTS2.
4. Acquittement de la BTS2.
5. Envoi de la commande de handover au terminal via la BTS2.
6. Acquittement du terminal.
7. Acquittement du terminal relayé par la BTS2.
8. Commande de libération du canal.
9. Acquittement de la BTS1.



La procédure de Handover 3/6

- C'est une procédure gérée par la couche RR et les messages que l'on voit sur l'interface radio sont les suivants:
- **Handover command** : ce message contient la description du canal cible (type, porteuse, saut de fréquence éventuel et mode s'il ya changement), le handover reference, contrôle de puissance, la synchronisation indication. Le timing of advance est optionnel s'il y a eu une présynchro avant et on peut avoir aussi en option un starting time.
- **Handover Access** : c'est un burst d'accès non chiffré qui ne contient que le Handover Reference (1 octet).
- **Physical Information** : ce message est envoyé lors de Handover non synchronisé, il contient le Timing of advance et est éventuellement chiffré.
- **Handover Complete** : ce message est envoyé après établissement du niveau 2 SABM sur le nouveau canal (pas de résolution de contention)
- **Handover Failure** : ce message est envoyé lors de l'échec de l'établissement sur le nouveau canal, le mobile se replie donc sur son ancien canal. Si le mobile ne le fait pas le MSC libère au bout de l'échéance d'une temporisation le canal.

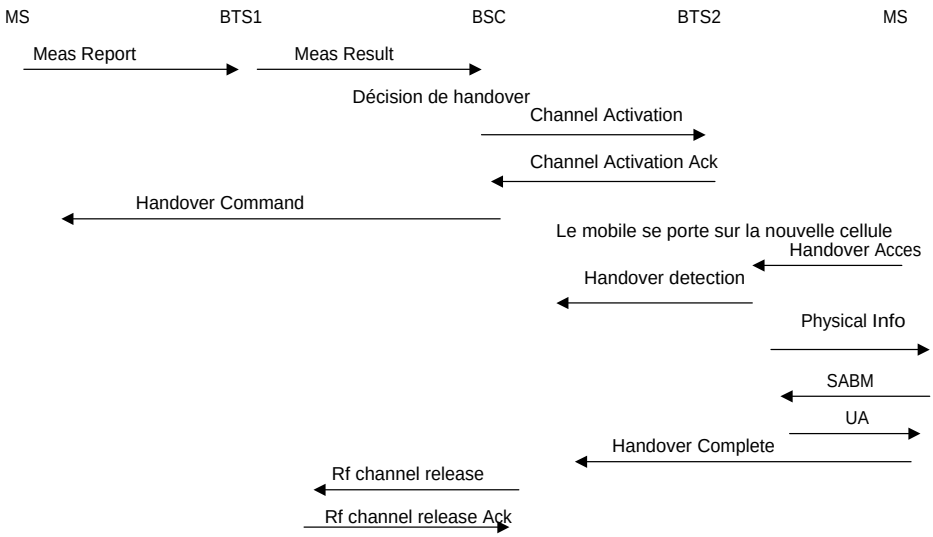
La procédure de Handover 4/6

- Le type du Handover est indiqué par le champ Synchronisation Command dans le Handover Command, il peut être non synchronisé ou synchronisé. En mode synchronisé on différenciera 3 sous modes le finement synchronisé ou le mobile connaît à l'avance tout les paramètres de la cellule cible, le présynchronisé où le mobile connaît le timing of advance et enfin le pseudo synchronisé.

- Handover synchronisé : 4 bursts sont envoyés dans 4 trames de niveaux successives sur le DCCH principal(avance en temps 0)Ces bursts sont optionnels si jamais le mobile connaît à l'avance le Timing Of Advance à appliquer. Le mobile en fonction du Timing Of advance précédent calcule le nouveau ayant en plus connaissance des BCCH voisins.

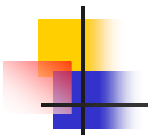
- Handover non synchronisé : Entre 2 cellules non synchronisé le réseau doit envoyer au mobile l'avance en temps qu'il doit appliquer pour se synchroniser sur la nouvelle cellule. Le mobile répète des bursts successifs à partir desquels le BSS cible est à même de déterminer l'avance en temps. Le mobile attend ensuite les Physical Infos.

La procédure de Handover 5/6



La procédure de Handover 6/6

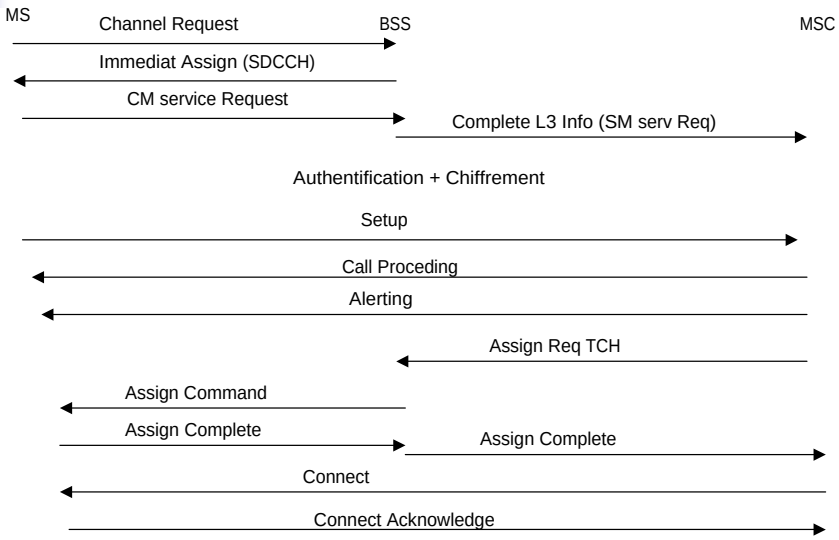
- Il y a 2 types de Handovers, les Handovers inter-cellulaires et les Handovers Intra-cellulaires
- Le Handover inter-cellulaire permet de changer de canal à l'intérieur d'une cellule. Il est déclenché pour des raisons de trafic ou de changement du paysage radio et peut être piloté par le MSC (il est dit inter BSS) ou par le BSC (intra BSS)
- Le Handover intra-cellulaire permet un changement de cellule, il est déclenché par exemple pour réduire les interférences lorsque la qualité se dégrade malgré un signal fort. Il est toujours piloté par le BSC
- On notera toutefois que le MSC initial restera le point d'ancrage entre le réseau RTC et le réseau GSM, s'il y a handover et changement de MSC, le deuxième MSC ne sera qu'un relais du premier

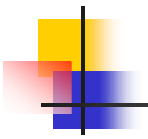


Gestion d'appel : appels sortants 1/2

- Un appel sortant commence comme tout accès à la ressource radio par un accès aléatoire par l'intermédiaire d'un RACH, cette demande est généralement suivi d'un Immediat Assignment
- Le mobile envoie ensuite son message initial pour spécifier le type de canal dont il va avoir besoin en fonction du type de service (appel sortant, appel d'urgence, message court …) et ceci par l'intermédiaire d'un CM request.
- La demande de service au CM (Call Manager) peut être chiffré ou non et donne suite à une réponse du réseau par un CM Accept.
- A ce stade là le mobile envoie un message de Setup précisant l'identité de son appelant (Called BCD Number) ainsi que son type de canal (BC : bearer capability) en fonction du service attendu (voix, donnée,message court….)
- Le MSC prévient de l'état d'appel en court par l'intermédiaire du message Call Proceding
- Un message Alerting peut être utilisé pour simuler un retour de sonnerie.
- Le message Connect lui notifie au mobile l'acceptation par le distant de l'appel et il acquittera ce message par Connect Acknowledge

Gestion d'appel : appels sortants 2/2





Gestion d'appel : appels entrants 1/2

- Le réseau demande au mobile de faire un accès aléatoire par l'intermédiaire d'un Paging Request. A l'accès aléatoire le réseau répond par un Immediat Assign (SDCCH). Sur ce canal le mobile envoie son message Initial à savoir Paging Response
- Les différentes procédures d'identifications et de sécurités peuvent être mise en place ou non
- Le MSC peut à ce niveau commencer sa transmission notamment le message Setup où il précise le numéro appelé(Called BCD Number), le type de profile de service demandé (Bearer Capabilities).
- Le mobile répond au Setup par Call Confirmed ou Release Complete selon la compatibilité du mobile avec le type de profile demandé. Le message Alerting permet un retour de sonnerie.
- A réception du message Connect le réseau entre en état actif, le mobile lui le sera à l'émission du message Connect Acknowledge
- On peut sécuriser l'établissement de communication en anticipant le besoin d'un canal TCH dès l'établissement du SDCCH mais cela n'est pas obligatoire

Gestion d'appel : appels entrants 2/2