

GSM

Pierre Roulet : roulet@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
 - Localisation
 - Appel entrant
 - Appel sortant
 - Handover

Introduction

GSM, GSM 900, DCS 1800, PCS 1900

- **GSM** : **G**lobal **S**ystem for **M**obile communication
 - Norme pan-européenne de communication avec les mobiles d'ores et déjà adoptée par plus de 60 pays et constituant désormais la référence mondiale pour les réseaux mobiles. Depuis sa phase 2 en 1995 cette norme unifie les systèmes GSM 900,400,850, DCS 1800 et PCS 1900. Depuis 1998 elle des extensions que sont le GPRS et l'EDGE
- **GSM 900** :
 - Système radiomobile basé sur la norme GSM à vocation urbaine et rurale (macro_cellules) et utilisant 2 bandes de fréquences de 25 MHz autour des 900 MHz. Ce fut le premier système numérique implémenté en France et a des cellules de tailles jusqu'à 35 Km
- **DCS 1800** : **D**igital **C**ellular **S**ystem
 - Système radiomobile dérivé du GSM 900 à vocation urbaine (micro cellule) et utilisant actuellement 2 bandes de fréquences de 75 MHz autour des 1800 MHz. Ce sont les anglais qui ont demandé l'évolution de la norme GSM la bande 900 étant déjà partiellement occupée chez eux.
- **PCS 1900** :
 - Variante du DCS 1800 elle est présente pour l'instant uniquement en Amérique du Nord et du Sud, elle utilise 2 bandes de fréquences autour de 1900 MHz
- **UMTS** : **U**niversal **M**obile **T**elecommunication **S**ystem
 - Norme pan-européenne de communication 3 G adopté par l'Europe mais aussi le Japon et la chine avec quelques modifications. Basé sur une technologie d'accès le CDMA large bande elle permet dans sa première version des débits de 348 Kbits pour monter à plus de 2Mbits

L'historique des réseaux cellulaires

- La préhistoire des réseaux mobiles
 - 1946 : St Louis Missouri : première tentative de réseau unicellulaire avec connexion manuelle (très coûteux)
- 1ère génération : Réseaux cellulaires analogiques
 - 1979 : AMPS aux états unis , première tentative de réutilisation des fréquences
 - 1981 : NMT en Scandinavie , utilise les bandes des 450 et 900 MHz
 - 1985 : TACS au royaume unis, suivi du mobile hors communication, changement de cellule pendant la communication toutefois manque de confidentialité
- 2ème génération : Les réseaux numériques
 - 1991/1992 : GSM et DCS en Europe
 - 1995 : IS95 États Unis, à base de CDMA
- 3ème génération :
 - 2001 : UMTS au Japon et en Europe à base de WCDMA
 - 20?? : CDMA 2000 en Asie et aux États Unis
 -

Dates Clés 2G 3G

- 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 Itinériss (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 en France
 - 3 Mars 2003 Ouverture commerciale de l'UMTS en Europe

Les licences GSM /UMTS accordées en France

- 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 autorisé 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
- Cahier des charges pour l'UMTS
 - 20 % de la population à date de License +2 ans (144 Kbits dans les 2 sens)
 - 60 % de la population à H + 5 ans (144 Kbits montant 384 Kbits descendant)
 - 75 % de la population à H + 8 ans (144 Kbits montant 384 Kbits descendant)

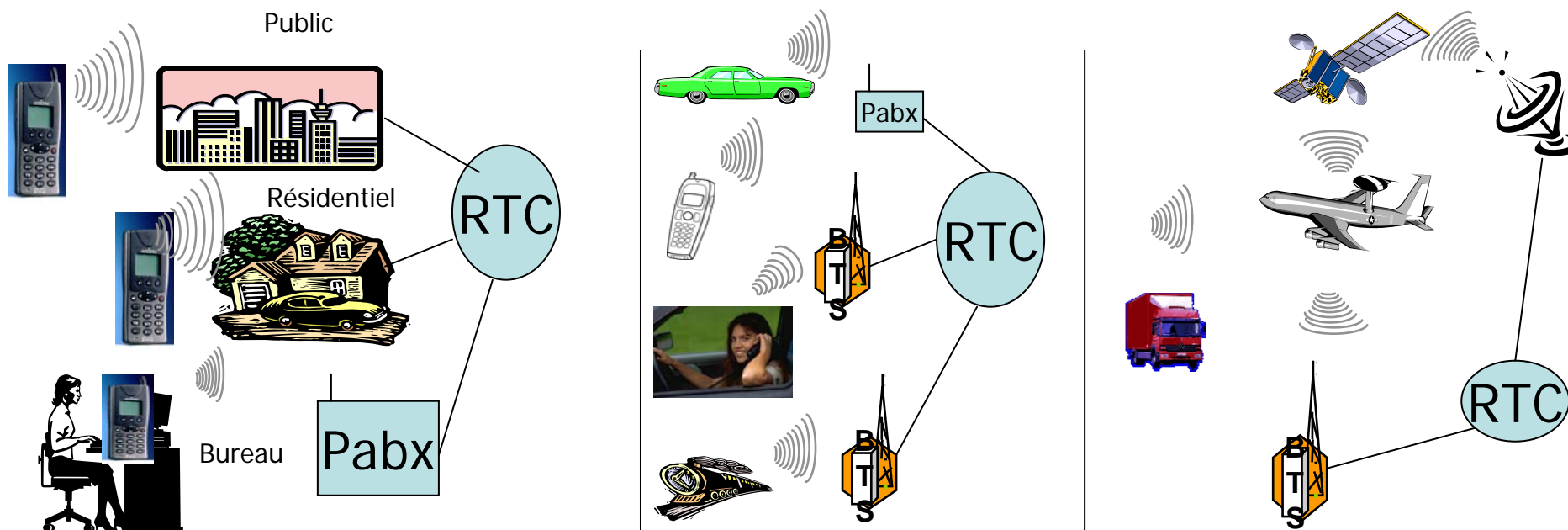
Panorama des normes actuelles

	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	Macro cellule 20 Km
Noms commerciaux	Ex BiBop	Orange, SFR, Bouygues	Bouygues, Orange, SFR	Téléphone domestique	Globalstar	Orange, SFR

Les couvertures mondiales en bandes GSM (2006)



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

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'europpéen 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

Organisation des recommandations 3GPP

Sujet de la recommandation	3G/GSM Release 99 ou plus	GSM release 4 et plus	GSM avant la release 4
Description générale			00
Requirement	21	41	01
Services aspect	22	42	02
Réalisation technique	23	43	03
Protocole de signalisation(L3) Ms vers Réseau	24	44	04
Radio aspect	25	45	05
Codecs	26	46	06
Data	27	(pas de série 47)	07
Protocole de signalisation(L3) Rss vers CN	28	48	08
Protocole de signalisation(L3) intra réseau	29	49	09
Programme Management	30	50	10
SIM/Usim requirements et test	31	51	11
OAM&P and chargin	32	52	12
Access requirement		Série 13 spécifique à l'ETSI	Série 13 spécifique à l'ETSI
Aspect sécurité	33	Inclus dans d autres normes	Inclus dans d autres normes
Test de la SIM/USIM	34	Inclus dans d autres normes	11
Algorithmes de sécurité	35	55	Non publié
Évolution de l'UTRA	36		

Organisation des recommandations GSM

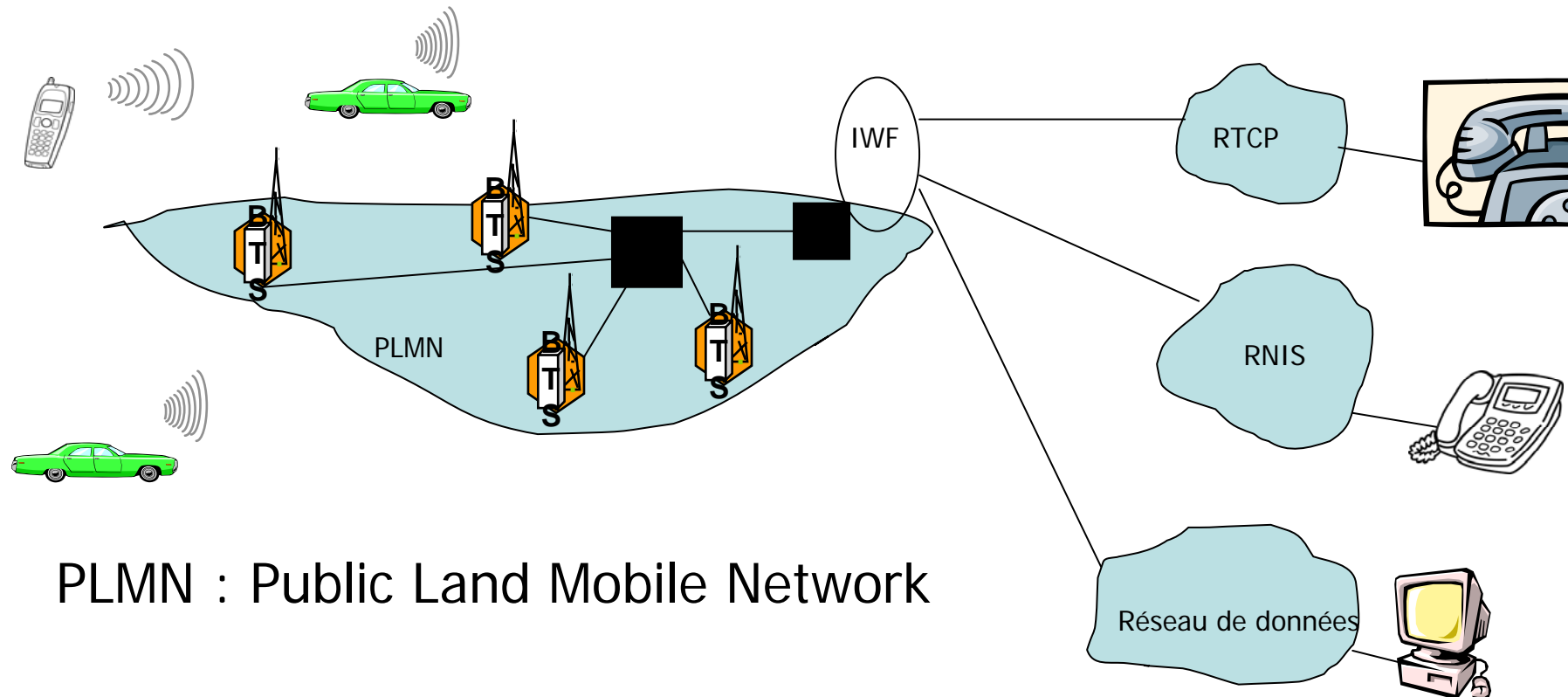
Série	Nbr Rec	Thème	Principaux contenus
01.XX	3	Aspects généraux	Description générale Vocabulaire
02.XX	35	Définition des services	Principes des services-Types de mobiles-sécurités-Licences-abonnements-circulation des mobiles-Identité d'Équipement- Carte SIM-Tonalité locale-Principe de facturation
03.XX	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 GRR GMM LLC SNDCP)
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-MS	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

Première Partie

Les caractéristiques et services
généraux de la téléphonie mobile

Concepts Généraux : PLMN et mobiles

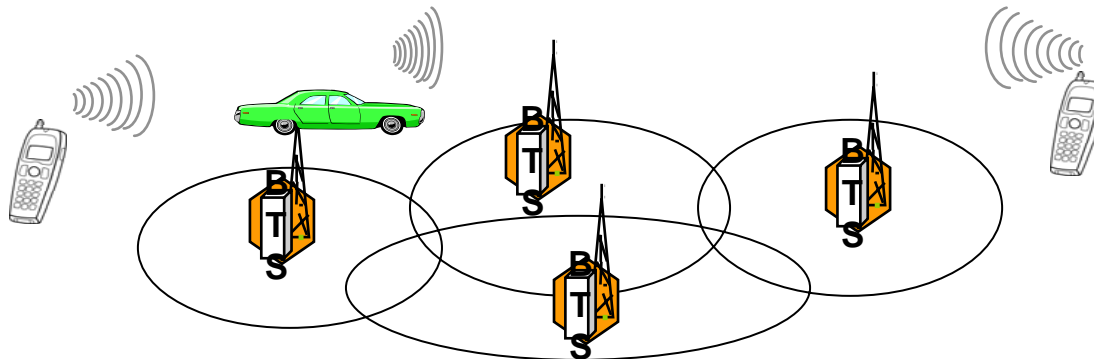
- Le PLMN est un réseau d'accès
- Les abonnés sont mobiles → Gestion des ressources radio (RR) gestion de la mobilité (MM)



PLMN : Public Land Mobile Network

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



Concepts généraux : Modèles de propagation et Rapport C/I

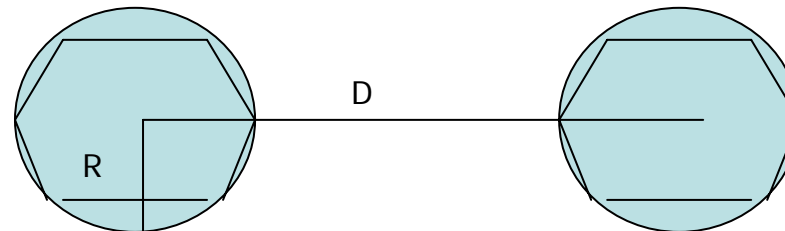
$$C = P_e \times \frac{K \lambda^2}{r^\gamma} \times A_f$$

Modèle d'atténuation réel

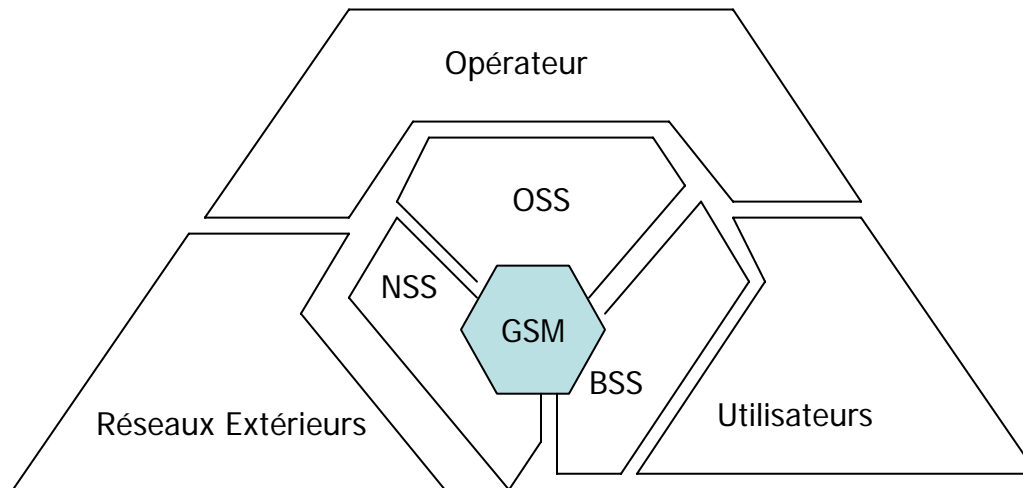
C : Niveau du signal Reçu
 Pe : puissance émission
 Ge, Gr : Gain de l'antenne en émission et réception
 λ Longueur d'onde
 γ atténuation due à la distance
 r distance mobile antenne
 As atténuation due aux obstacle
 Af évanouissement sélectif

Rapport signal à bruit systèmes limités par les interférence

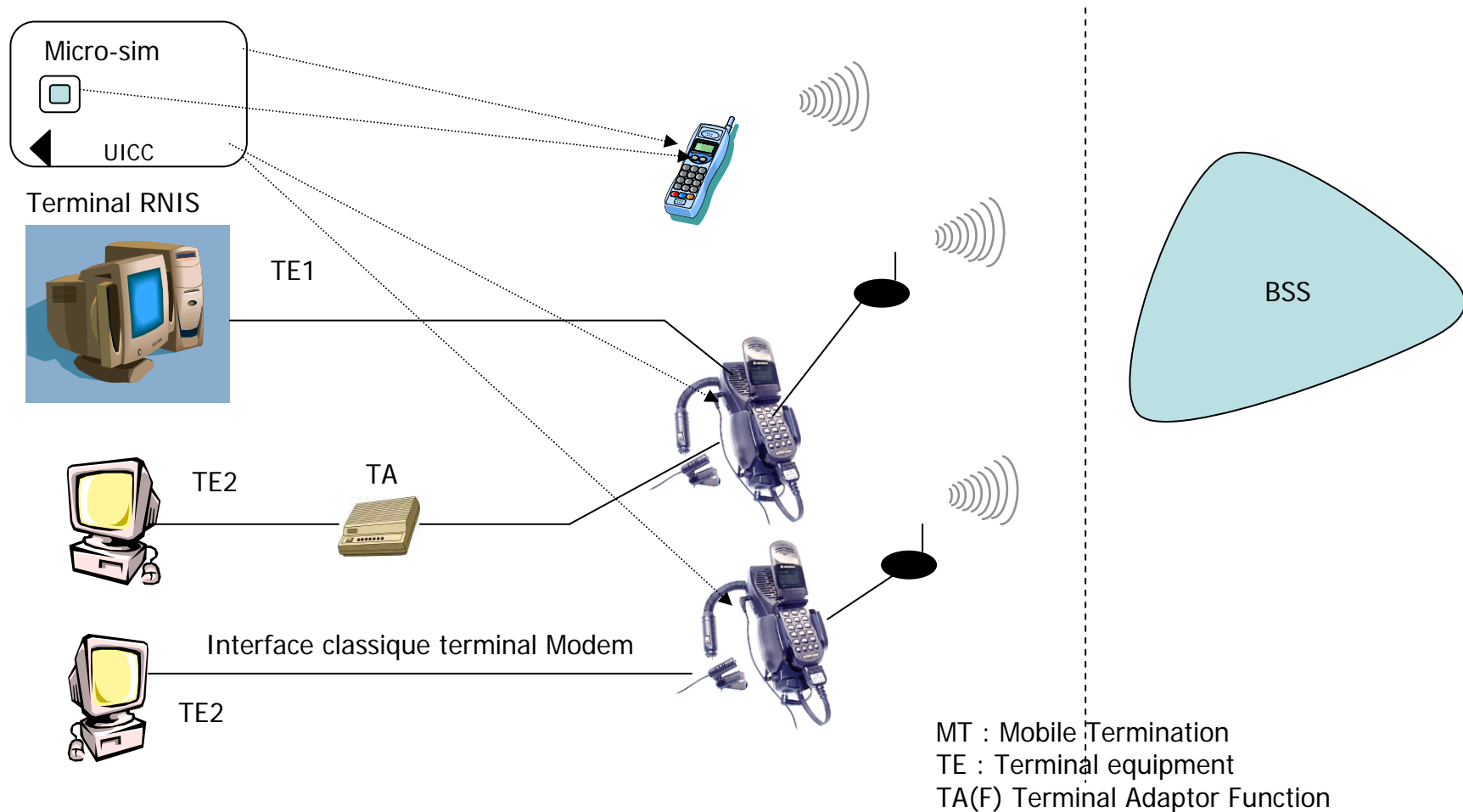
$$\frac{C}{I} = 6 \left(\frac{D}{R} \right)^\gamma$$



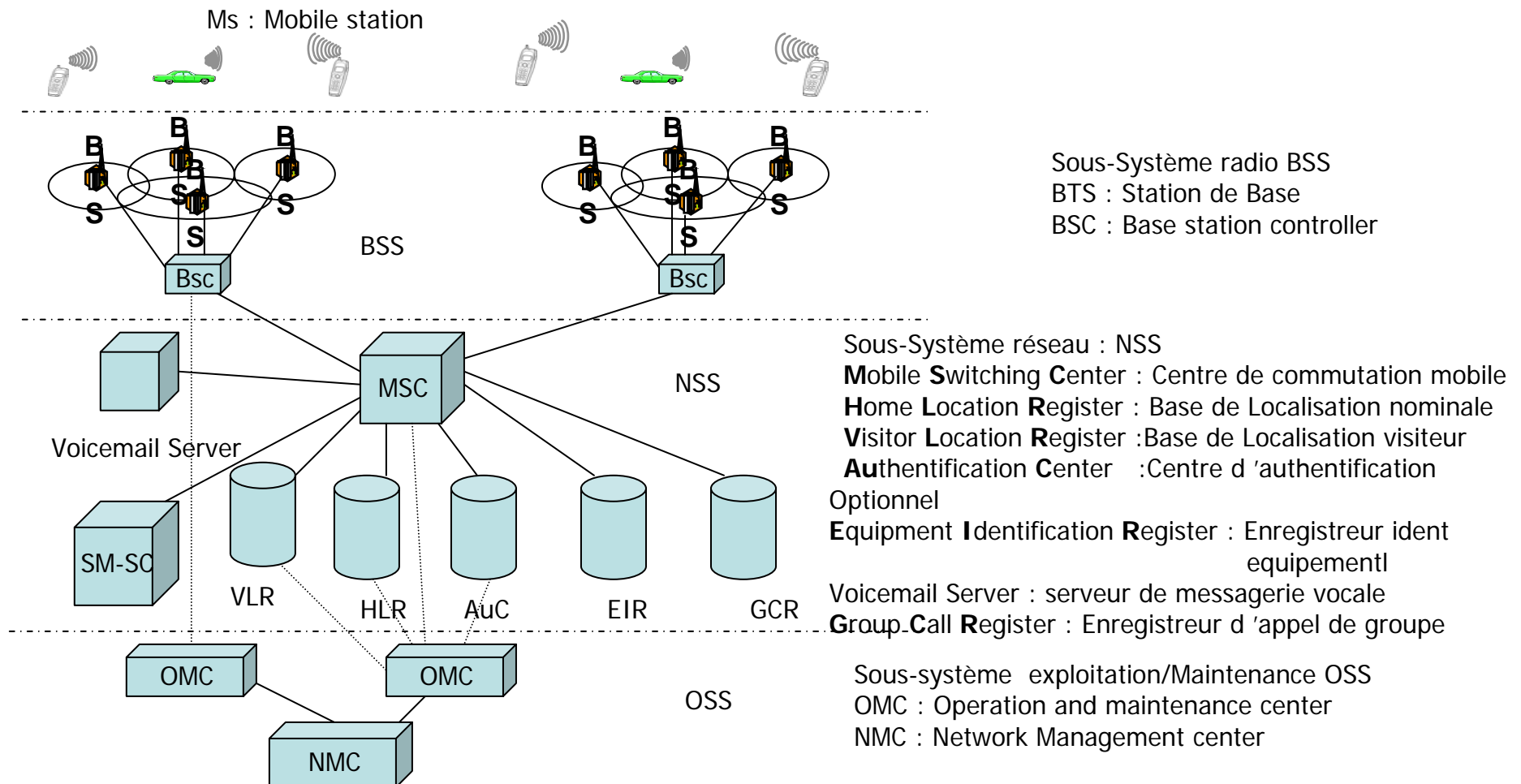
Vue générale de l'architecture GSM



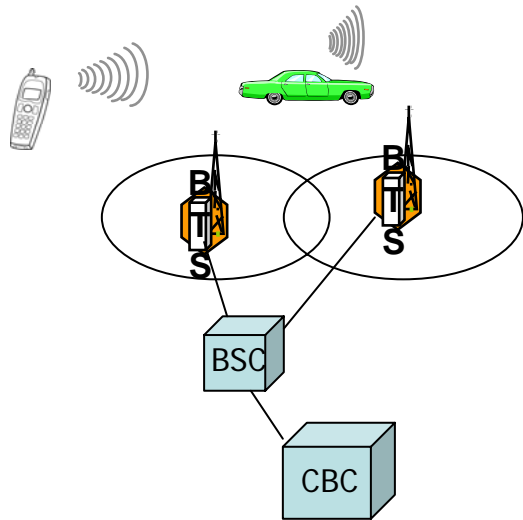
Architecture GSM : type de stations mobiles



Architecture GSM : Éléments du PLMN



Architecture GSM : sous système radio



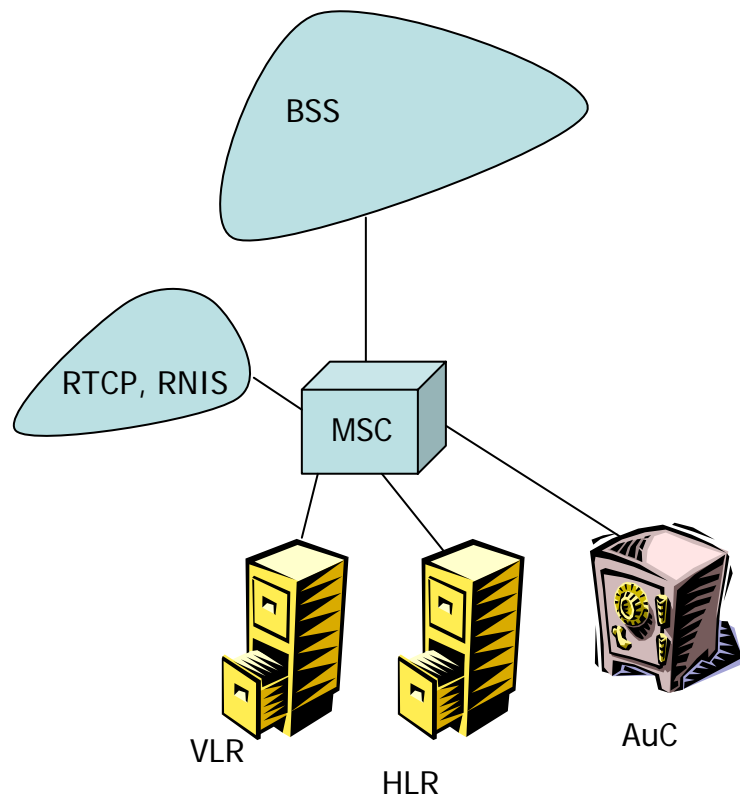
Principales fonctions :

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

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)

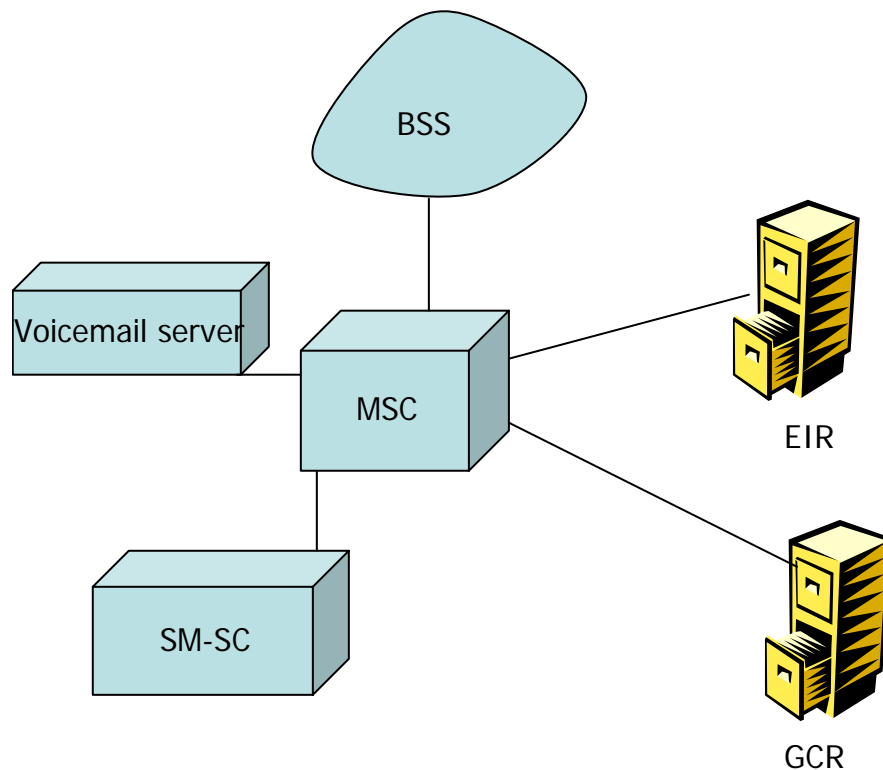
Stocke : Identité , Num annuaire,

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 authentication

Architecture GSM : équipements optionnels(NSS)



Principales Fonctions

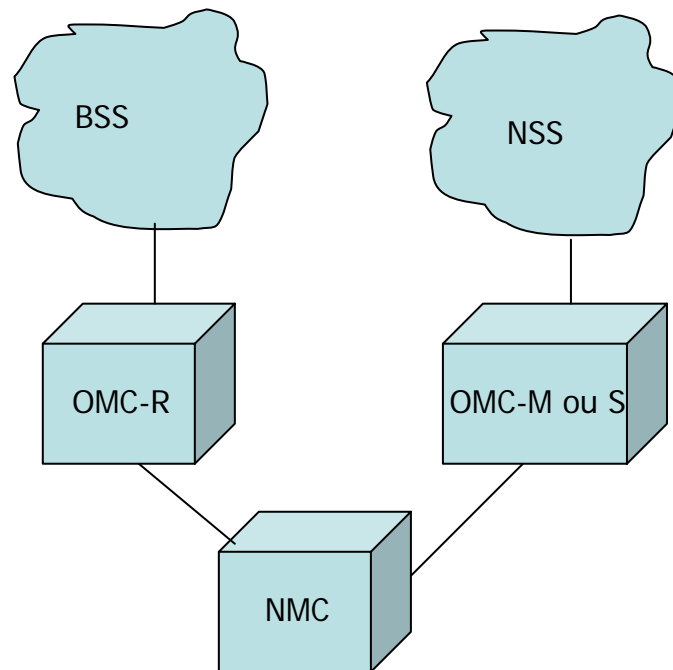
EIR : Base des équipements mobiles, notion des Mobiles blanc gris ou noir

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

Architecture GSM : exploitation et maintenance



OMC

OMC-R → radio gestion de la BSS

OMC-S → Switching gestion MSC

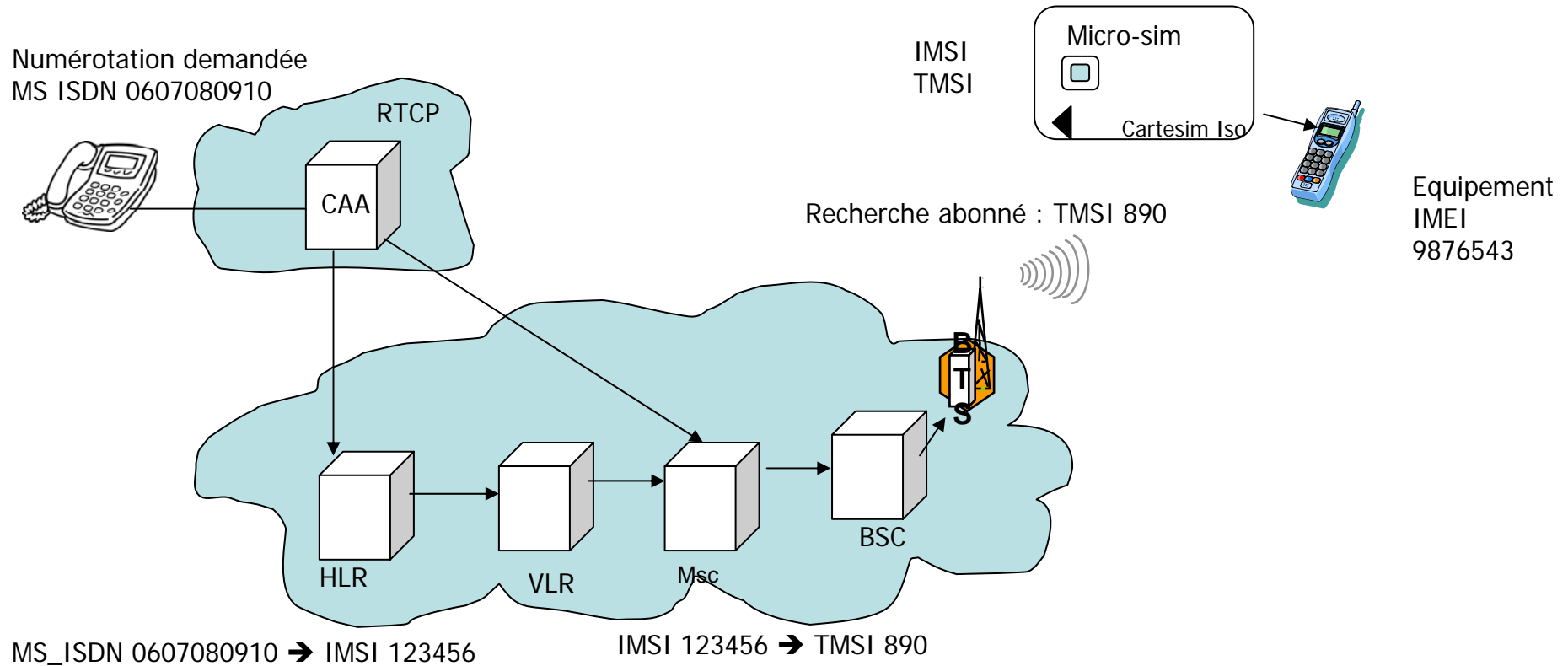
OMC-M → Mobile gestion NSS

- Gestion de la configuration
- Gestion des fautes
- Gestion des performances
- Gestion de la sécurité
- Gestion des coûts

NMC

Gestion de réseau de niveau supérieur

Architecture GSM : Numéros et identités



Les services offerts par le GSM

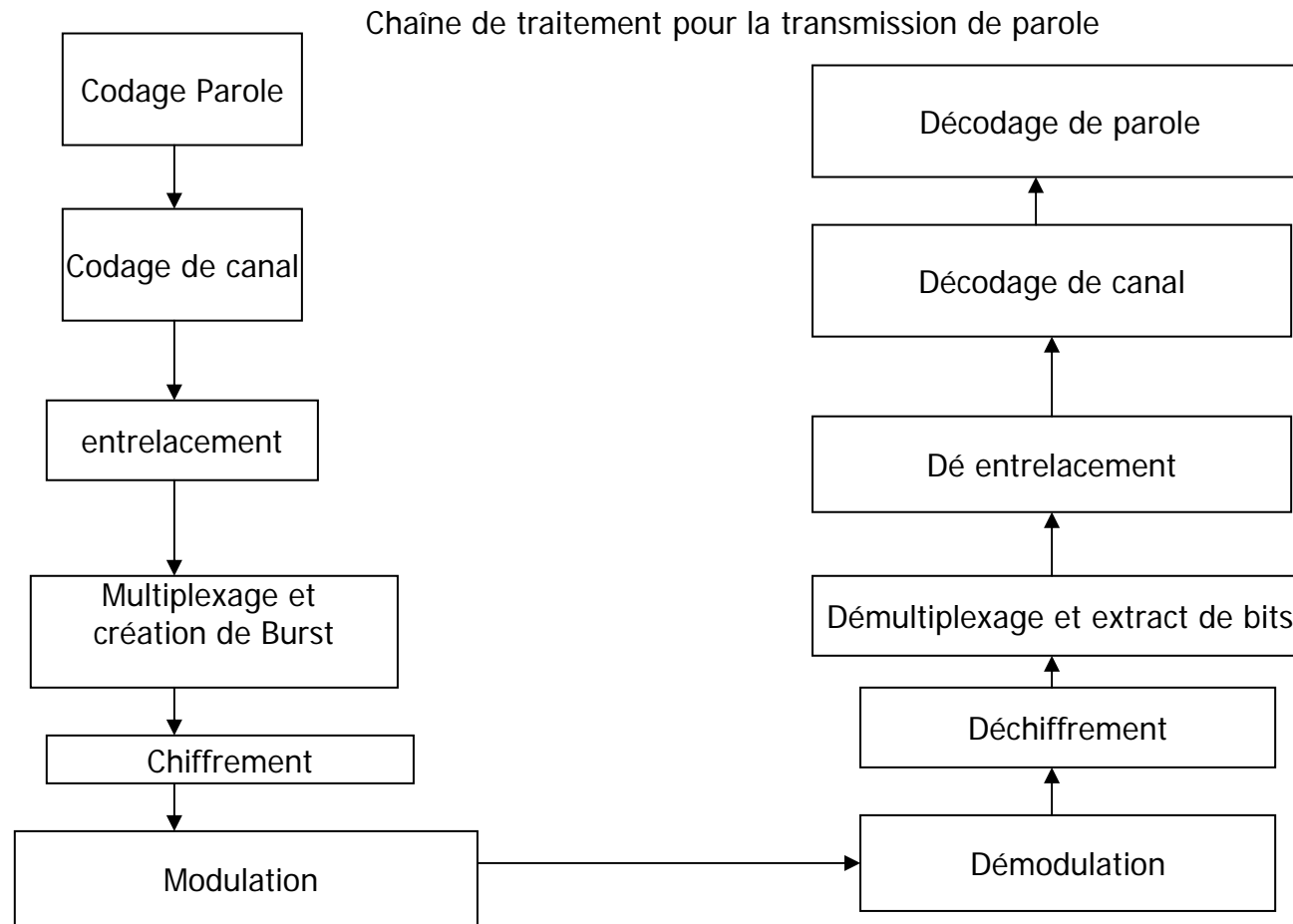
Catégorie de services Proposables en phase 2 et 2+

1. Les services vocaux:
 - Téléphonie : de loin le plus important pour l'instant avec différents débits de paroles possibles
 - Appels d'urgence : Procédure standardisée en Europe avec le 112
 - Groupe d'appel vocal : groupe de mobile se partageant des ressources radios limitées
 - Messagerie vocale: Non identifié au début par le GSM

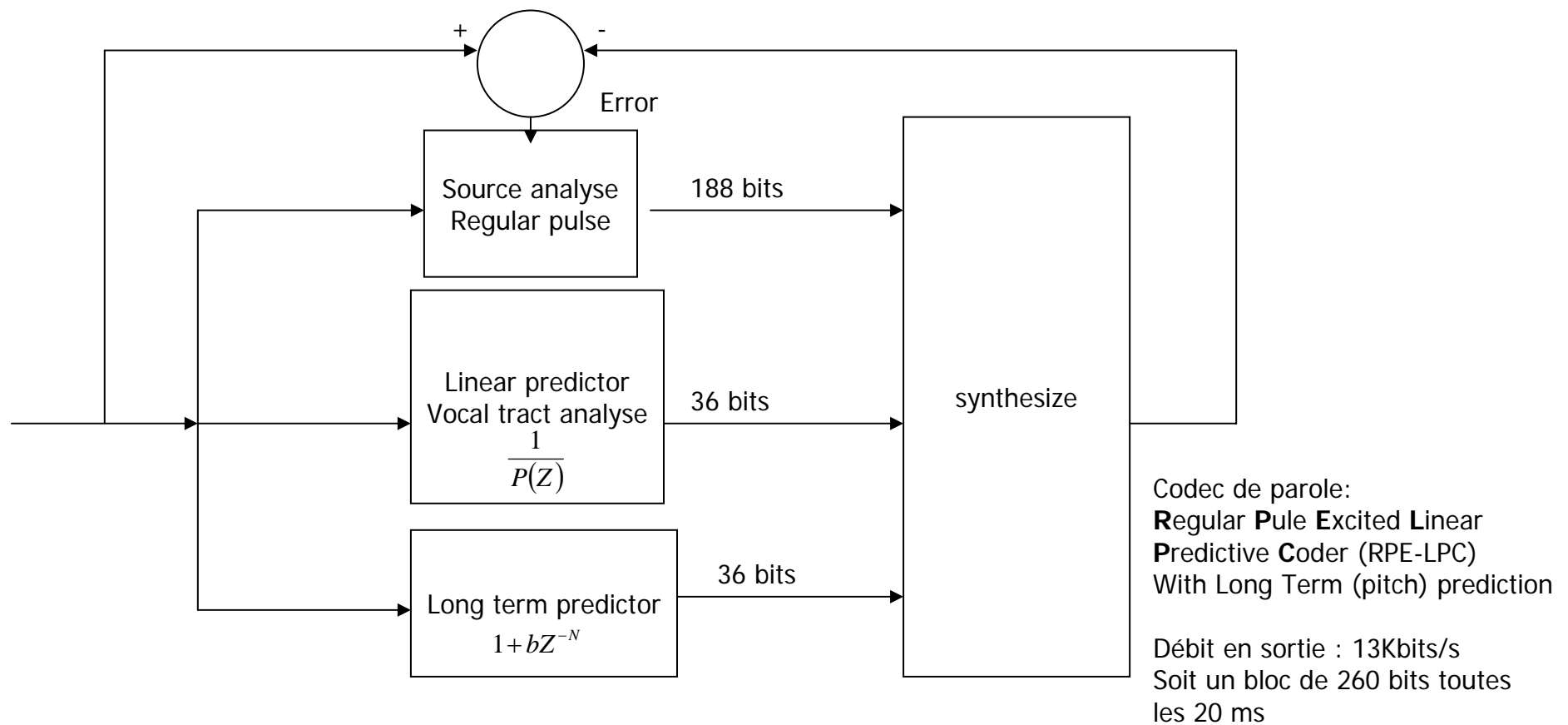
2. Les services messages courts (SMS = Short Message service)
 - Point à Point, Réseau vers mobile ou inversement
 - En diffusion Réseau vers mobile (SMS-CB)
 - Les messages multi_médias

3. Autres services Non Vocaux
 - Services supplémentaires: ces services sont essentiellement des services de maintenance
 - Les services de transmission de donnée en CSD ou HCSD

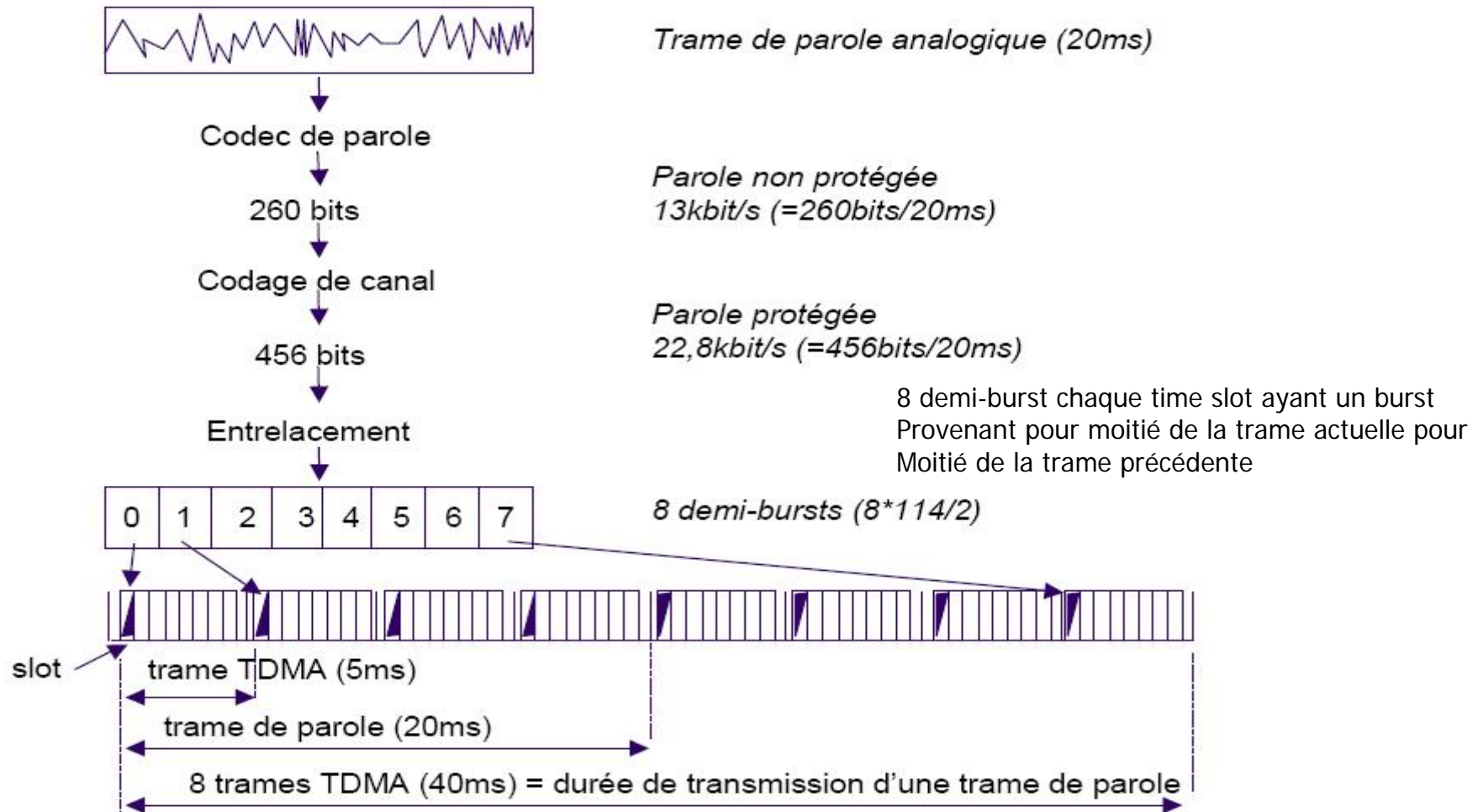
Les services du GSM : La téléphonie



Les services du GSM : le codage de parole



Les services du GSM : la protection de la parole



Les services du GSM : Le codage de canal

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

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 la et lb

La classe II sont 78 bits non protégés

La classe I 182 bits codés avec un code convolutionnel de taux $\frac{1}{2}$

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

Classe lb : 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

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

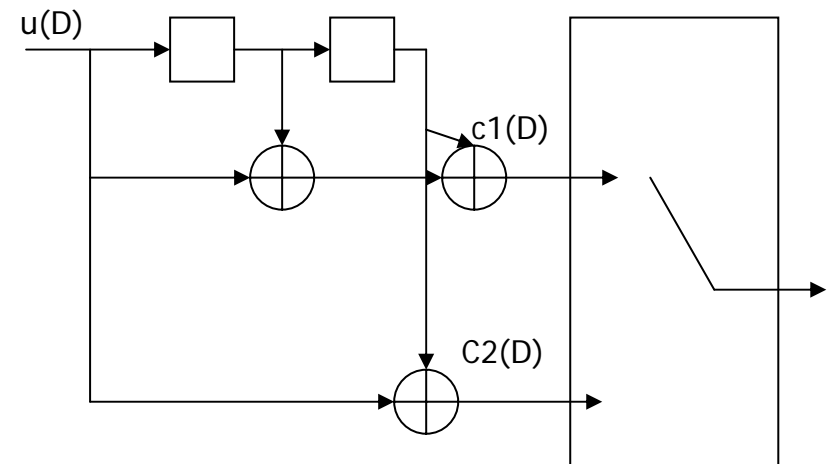
- Si la séquence d'information vaut
 1 0 0 1 1
 11 10 11 11 01 est égale à la séquence de sortie
 On rajoute à la fin 2 taillings bits pour purger les registres à décalage, cela permet aussi de connaître à l'avance les états du codeur donc finalement on se retrouve avec

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

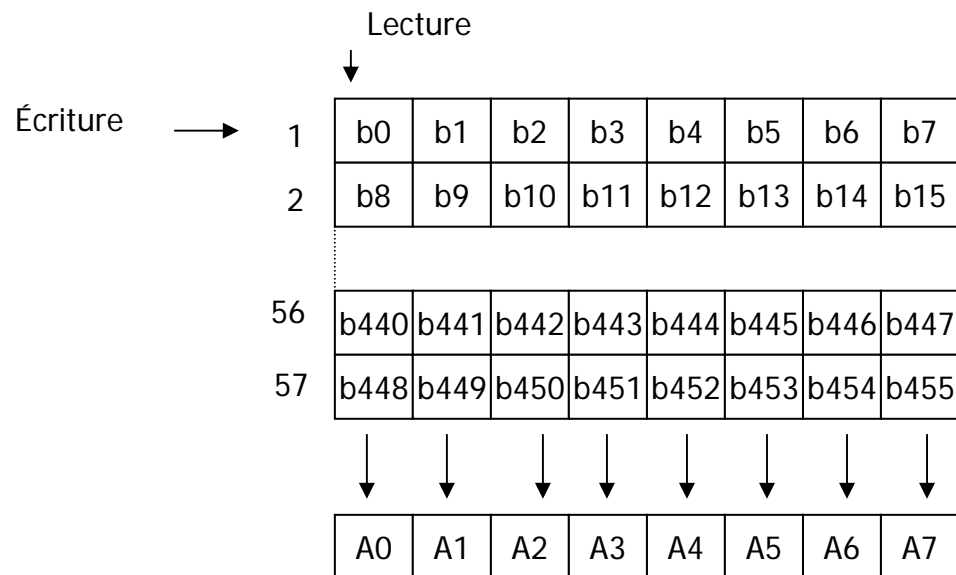
Exemple de
Codeur de taux 1/2 de longueur de contrainte 3

Les services du GSM : L'entrelacement 1/3

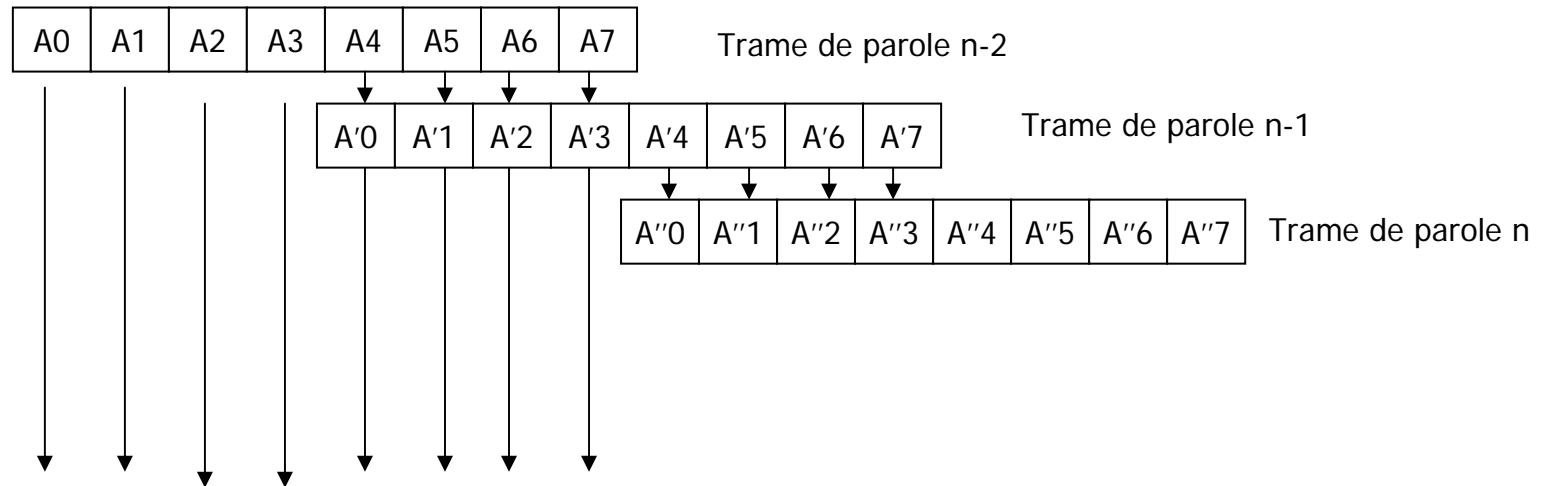
- But : étaler les erreurs dans le temps pour améliorer la correction d'erreurs ces dernières étant plus décorélées
- Il y a 2 niveaux d'entrelacement
 1. Au Niveau Bit : Permutation de bits à l'intérieur d'une trame de parole
 2. Niveau bloc : découpage de trame en blocs et transmission sur plusieurs 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



Les services du GSM : L'entrelacement 3/3



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

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'expéditeur
- 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)
 - Possibilité de concaténer 4
- 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

- Les services d'identification de numéro
- Renvoi d'appel
- Double appel
- Conférence
- Facturation
- Restriction d'appel

Deuxième partie

Protocoles et procédure du GSM/DCS

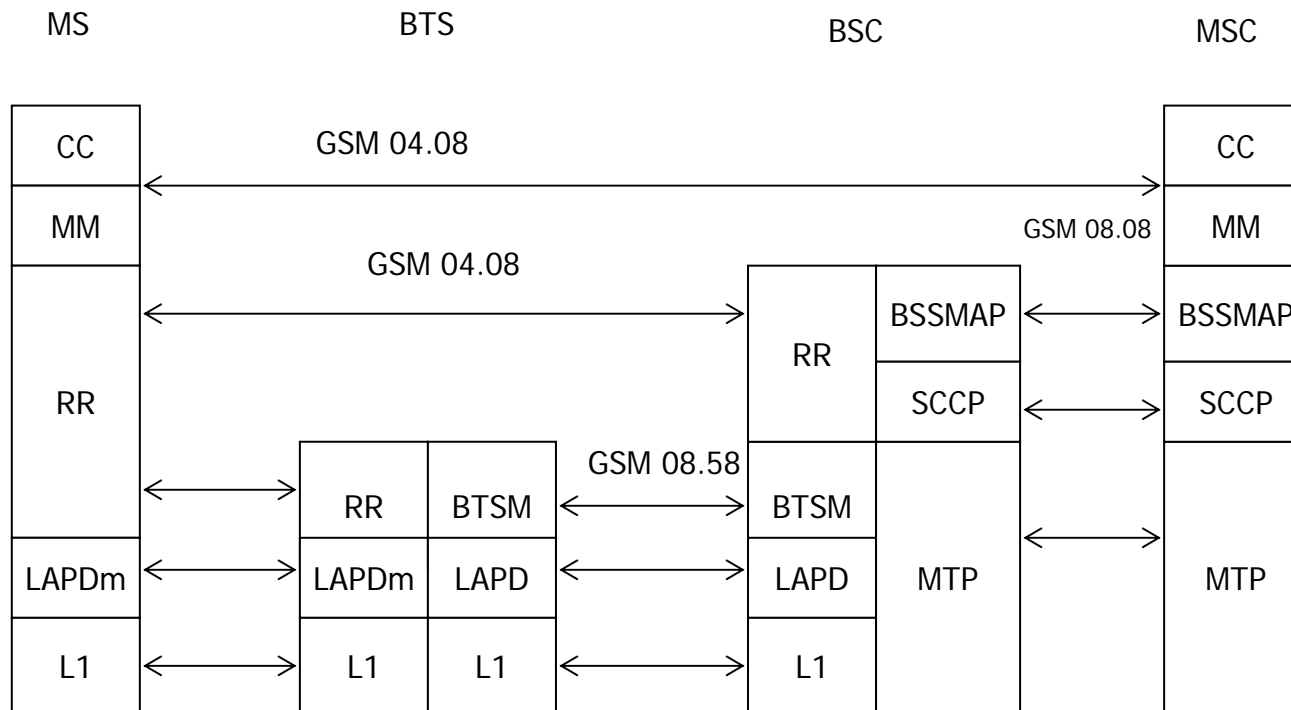
Protocoles du mobile au MSC 1/3

- **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 a un rapport avec la communication GSM de son établissement à sa terminaison
 - MM ou mobility management : cette couche gère tout ce qui a un rapport au déplacement du mobile et à sa localisation dans le réseau avant, pendant ou après la communication.
 - RR ou radio resource : 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 supplementary 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

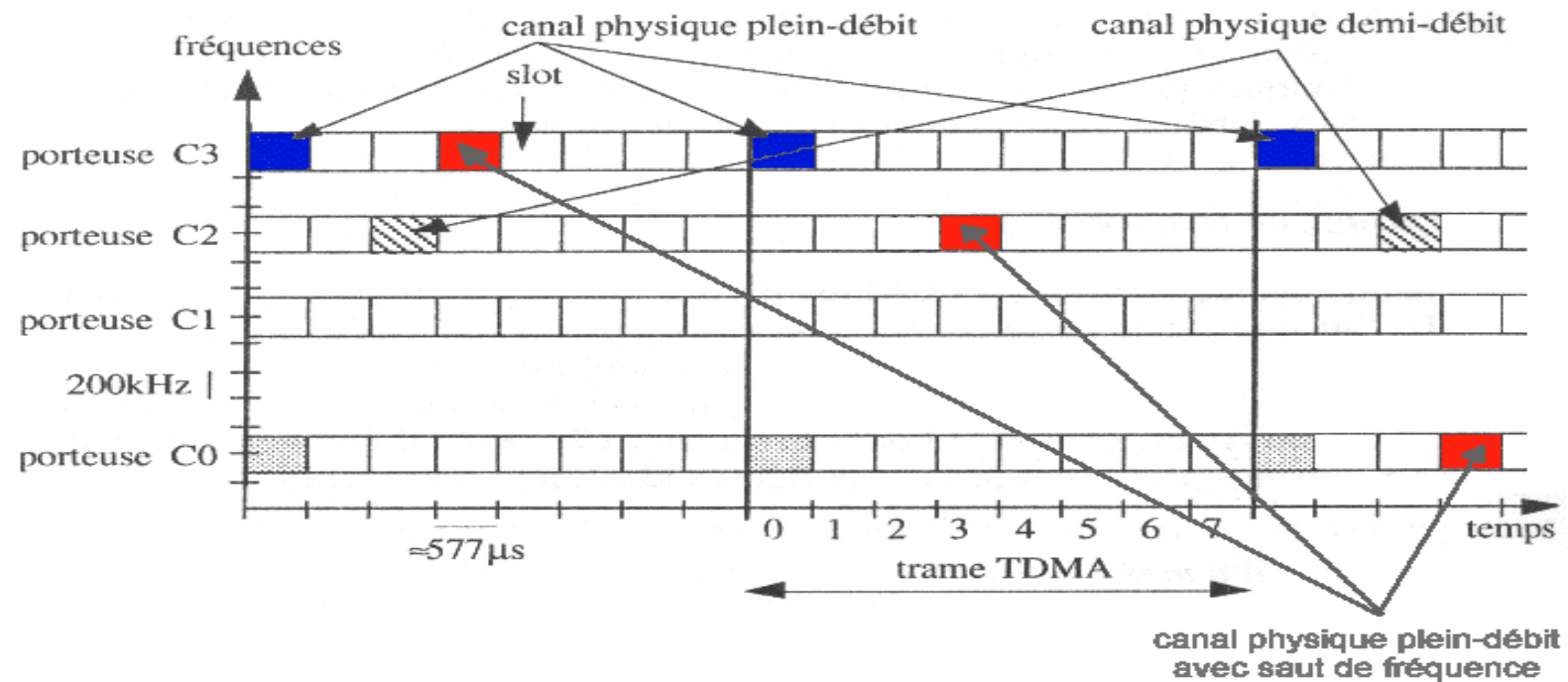
Protocoles du mobile au MSC 3/3



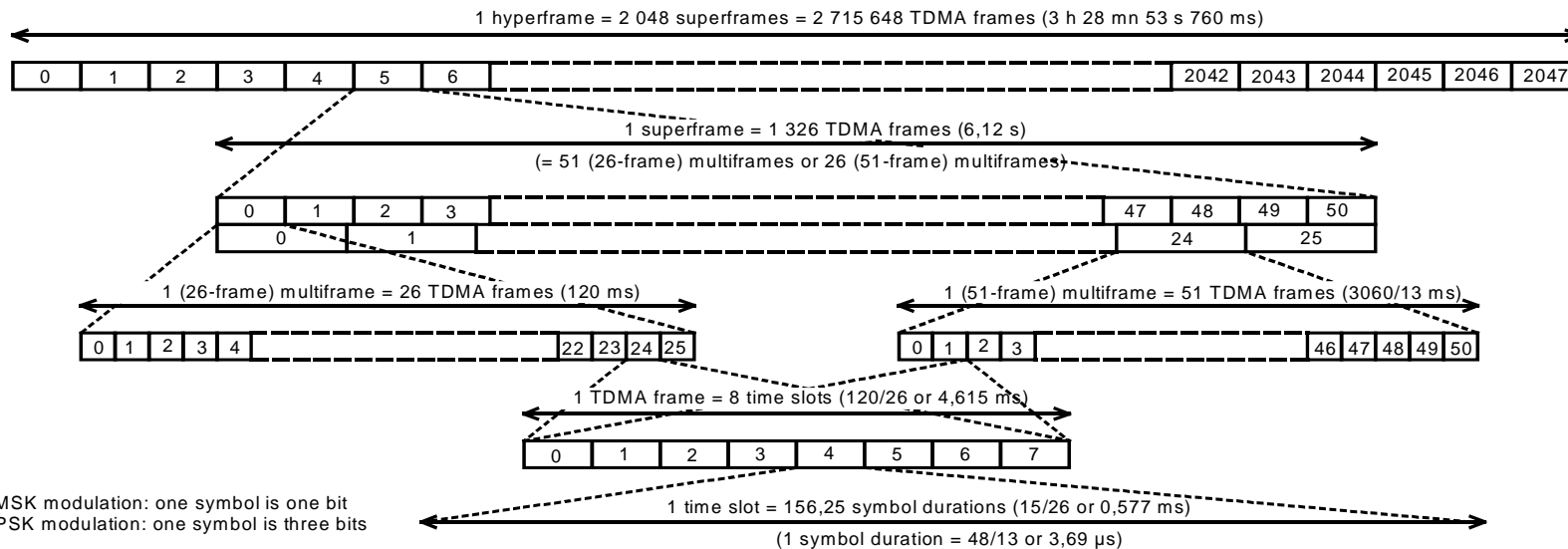
Les canaux GSM : Le multiplexage temporel 1/4

- 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 défini 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 utilisés pour la signalisation : SACCH,SDCCH, CCH, BCCH

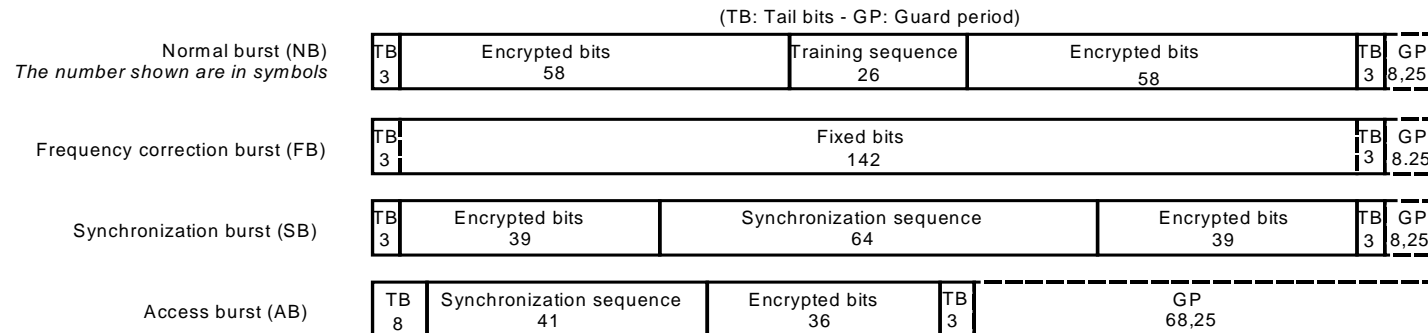
Les canaux GSM : Le multiplexage temporel 2/4



Les canaux GSM : Les structures de trames



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



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 différents 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 Access 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 Access 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:

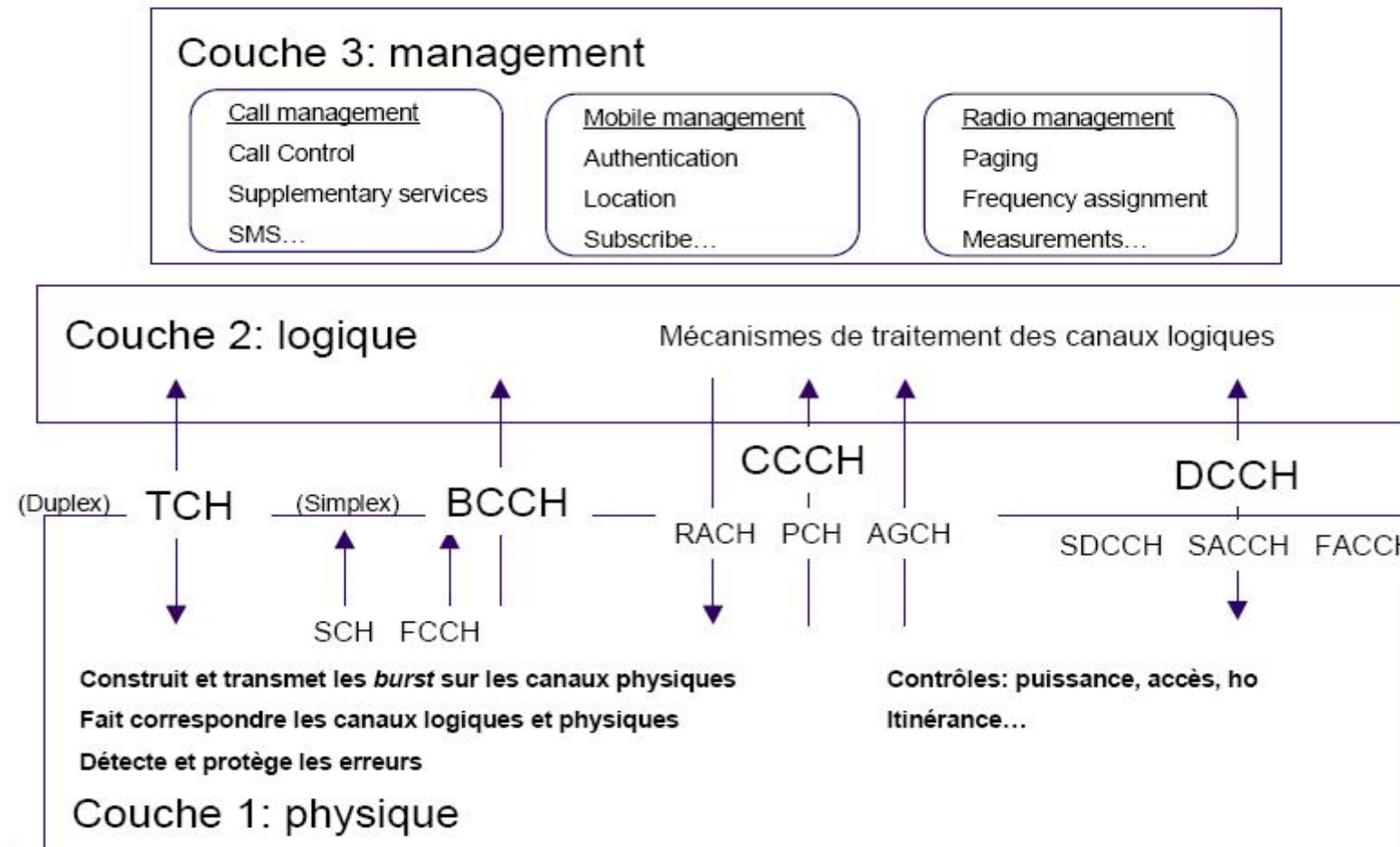
- **TCH** : Trafic Channel

- Il y a 2 types de TCH, le TCH/F pour Traffic Channel Full Rate et le TCH/H pour Traffic 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

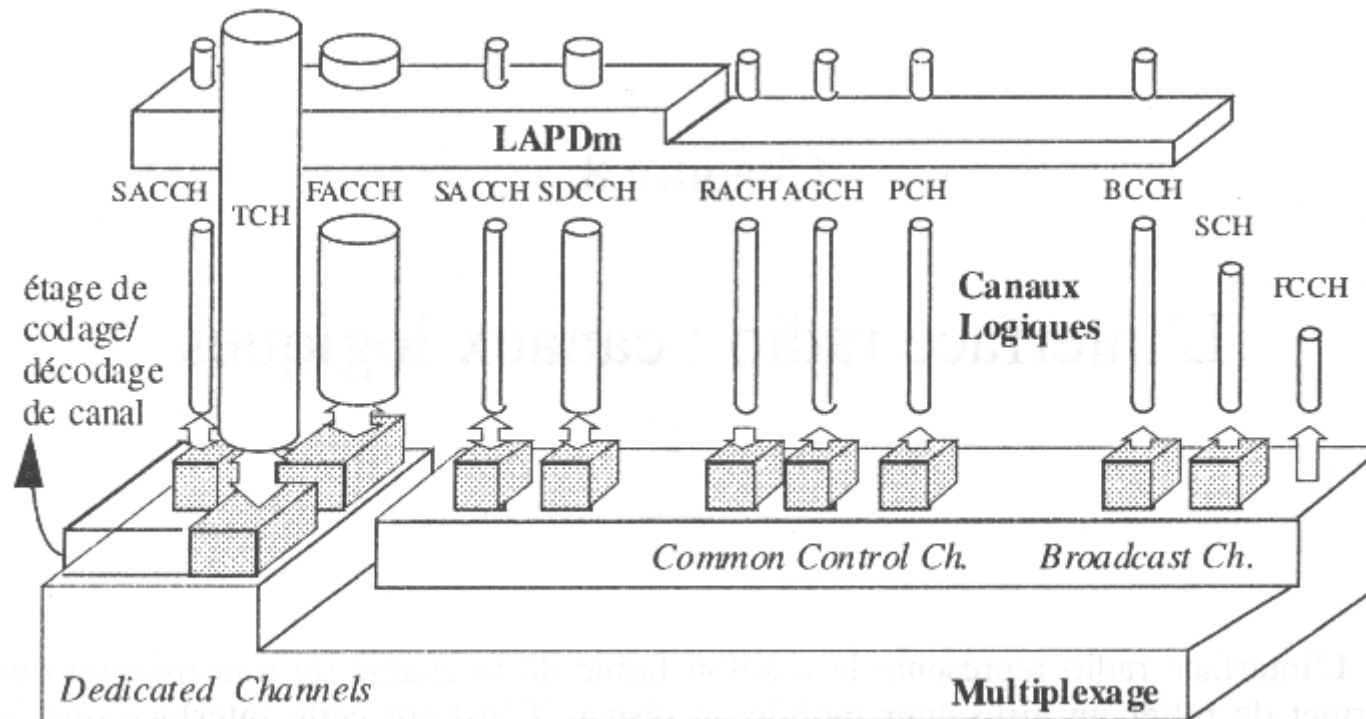
- Les canaux de trafic diffusés:

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

Les canaux GSM



Les canaux GSM



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 sélection initiale
- 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 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 548 fréquences du GSM ou DCS OU EGSM 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 (GSM 900,450 et 800)40 en DCS/PCS) 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 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 réseaux 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

- BCCH :
La sélection de cellule utilise
 - soit les BCCH 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 enregistréDans 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
- C1 se calcule en fonction d'un niveau minimum de réception et la puissance maximum d'émission.
- C2 est égale à C1 avec un offset et potentiellement un offset de pénalisation

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

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 au 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'Immediate 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 alloué
 - une avance en temps

 - Immediat assignment extended
Il permet d'adresser plusieurs mobiles en même temps

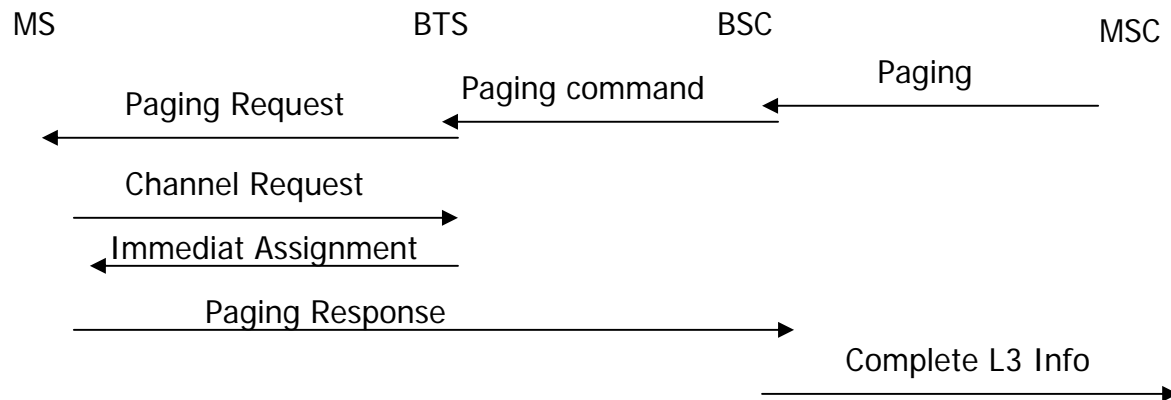
 - Immediat assignment reject
Il sert à rejeter les accès aléatoires et est utilisé lorsqu'il n'y a plus de ressources disponibles dans la cellule. On notifie alors au mobile d'attendre avant de recommencer sa tentative d'accès. Il contient donc les infos suivantes : la référence aléatoire, le numéro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

Allocation initiale : Message initial

- Lorsque le mobile a pris en compte une allocation immédiate 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 chiffrement
- Les messages initiaux sont les suivants :
 - Location Updating request
 - Paging Response
 - CM service request
 - CM reestablishment request

Procédure de Paging 1/2

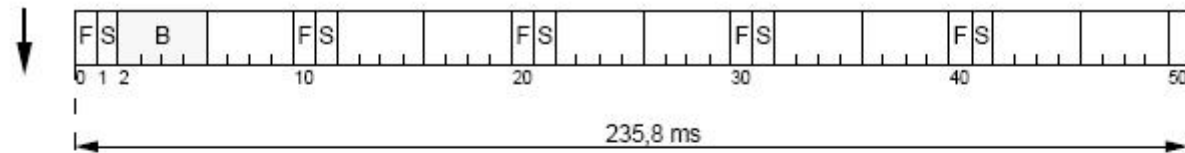
- C'est la fonction de « recherche » qui permet les appels entrants
- Le mobile écoute le PCH en fonction du paging mode et prend en compte tous les messages correspondants
- Les différents modes de paging sont les suivants
 - Normal : Le mobile écoute son sous canal seulement
 - Etendu : Le mobile écoute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

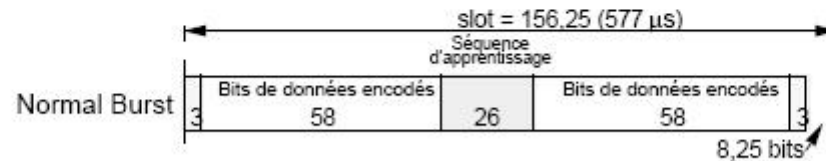
- On peut pager avec IMSI ou le TMSI mais pas avec l'IMEI
- Il y a différents types de *Paging Request*
 - Le type 1 qui permet de chercher jusqu'à 2 mobiles
 - Le type 2 qui permet de chercher jusqu'à 3 mobiles, les 2 premiers étant pagés avec le TMSI
 - Le type 3 qui permet de chercher jusqu'à 4 mobiles 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

Le processus global de sélection initial

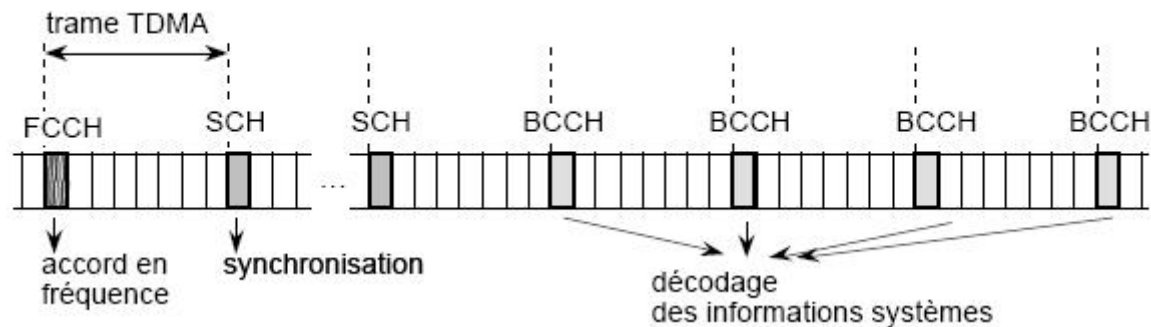


B : BCCH

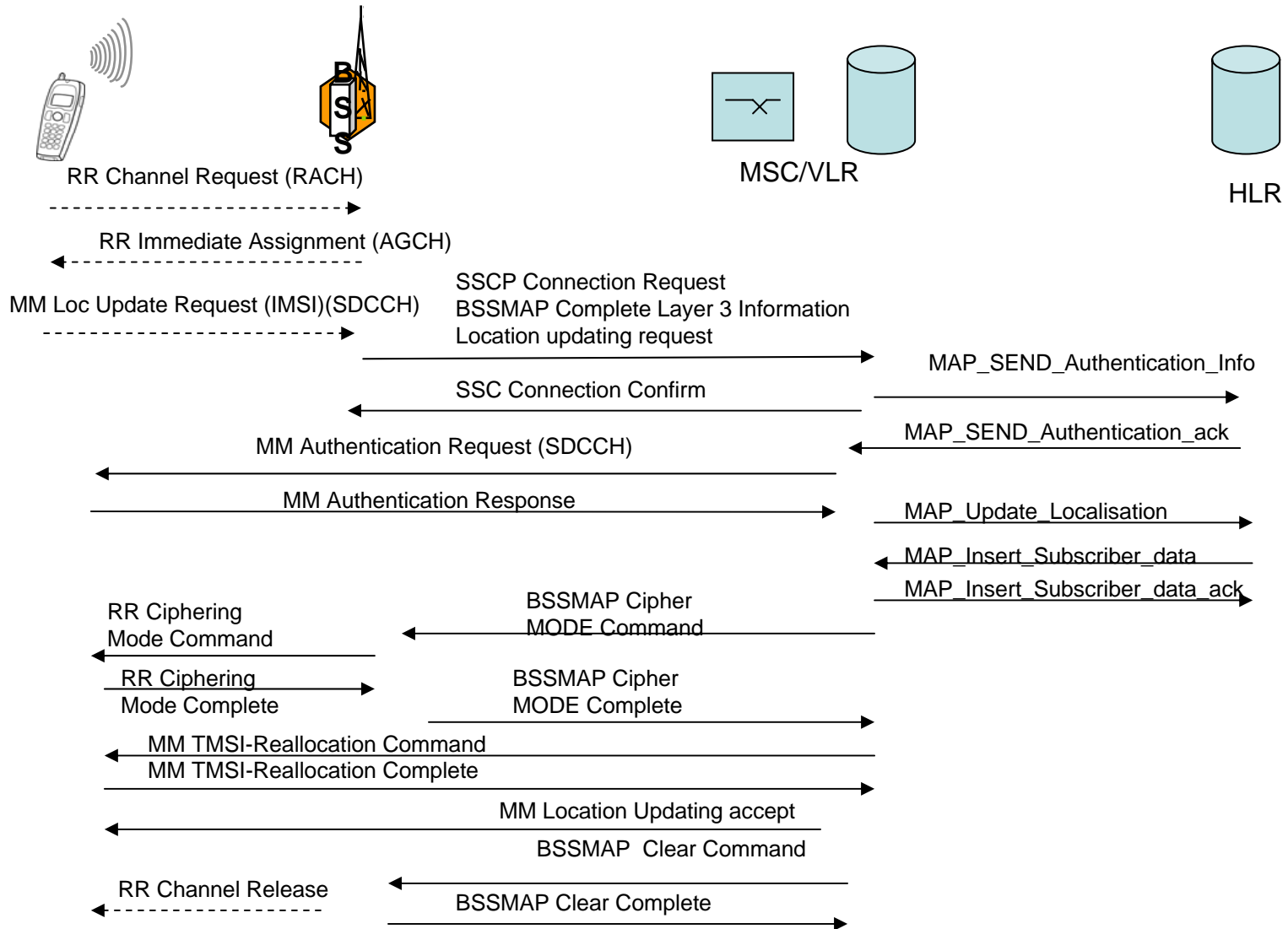
Situation du canal BCCH dans la multi-trame à 51 trames



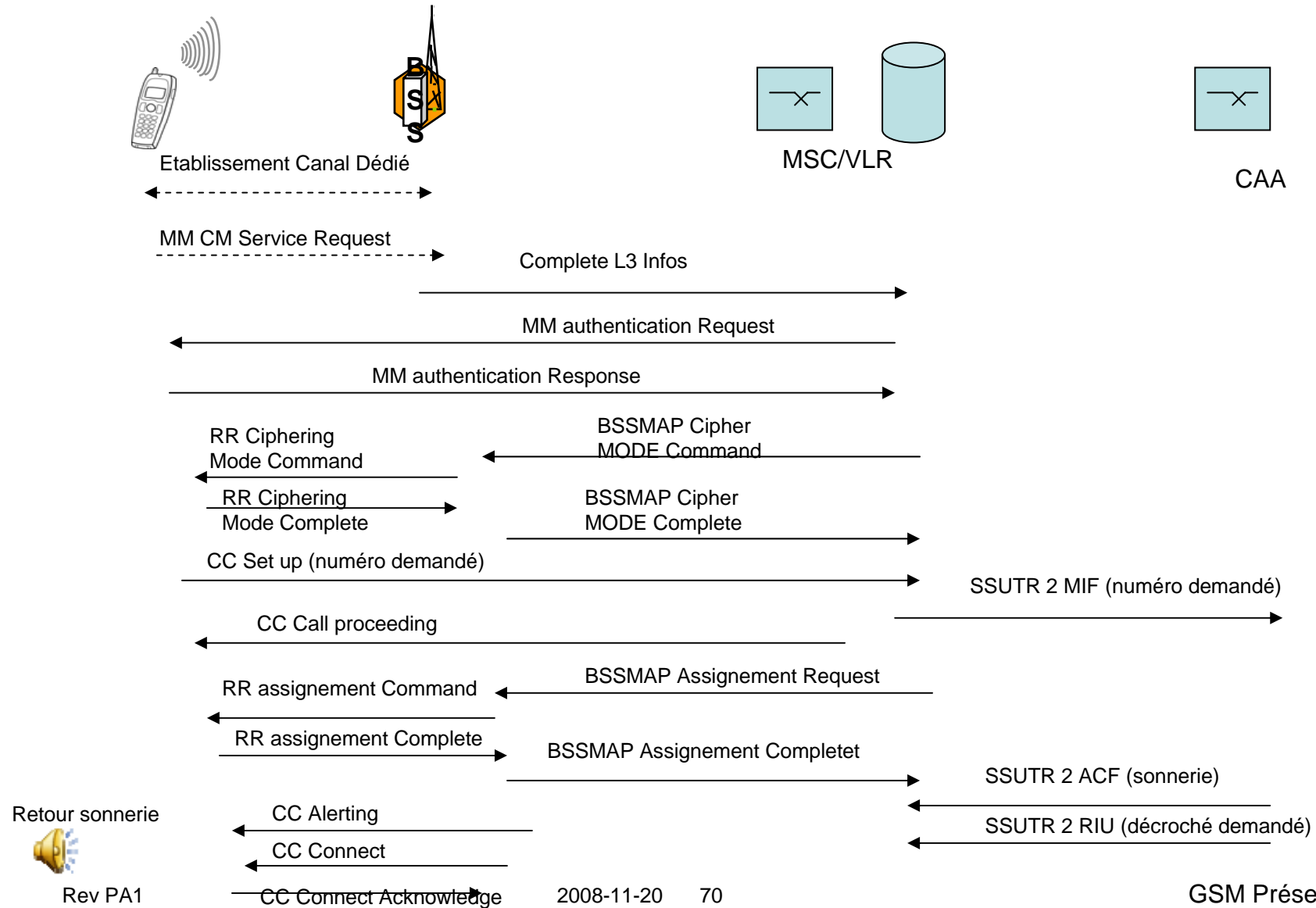
Structure du burst normal



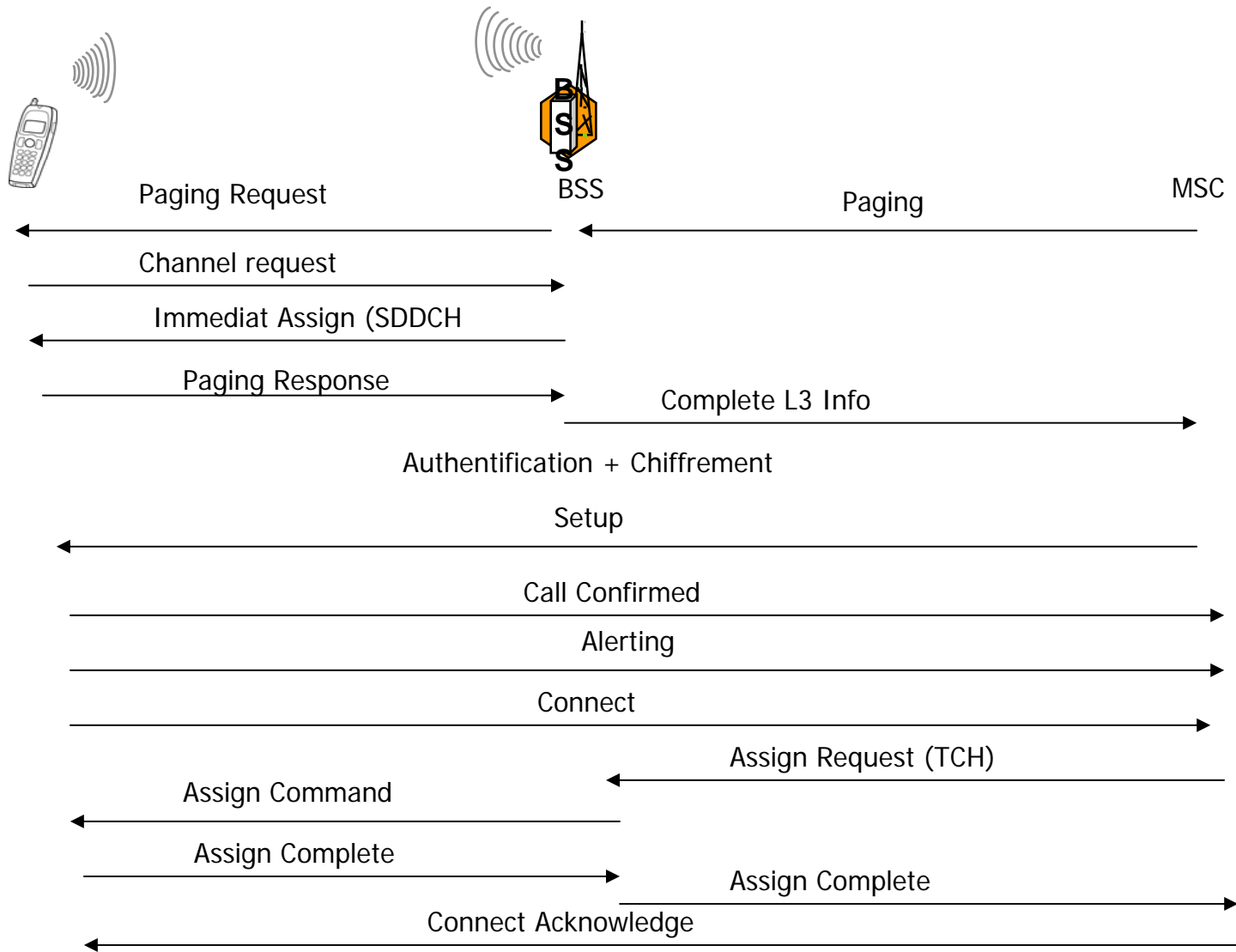
La localisation



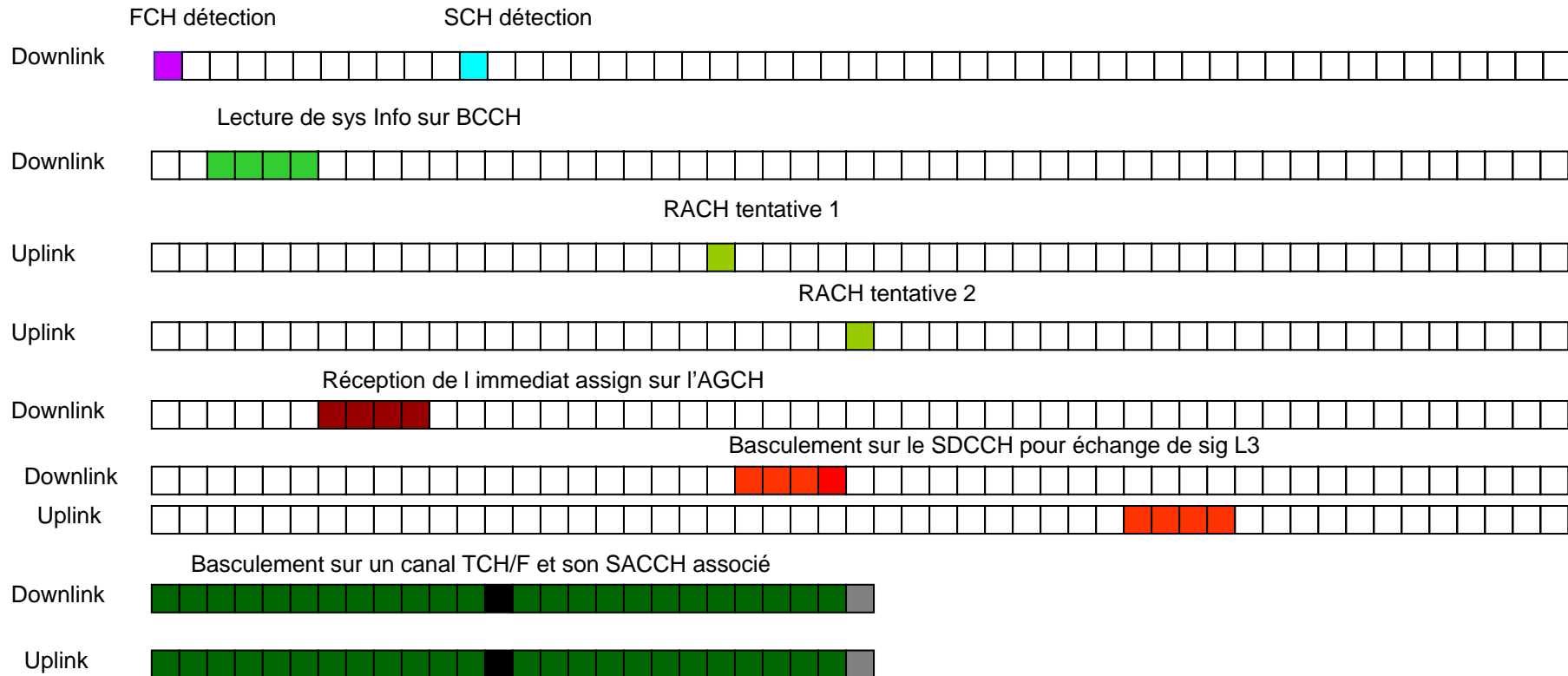
Etablissement Communication Sortante



Etablissement Communication entrante



Etablissement Communication Sortante



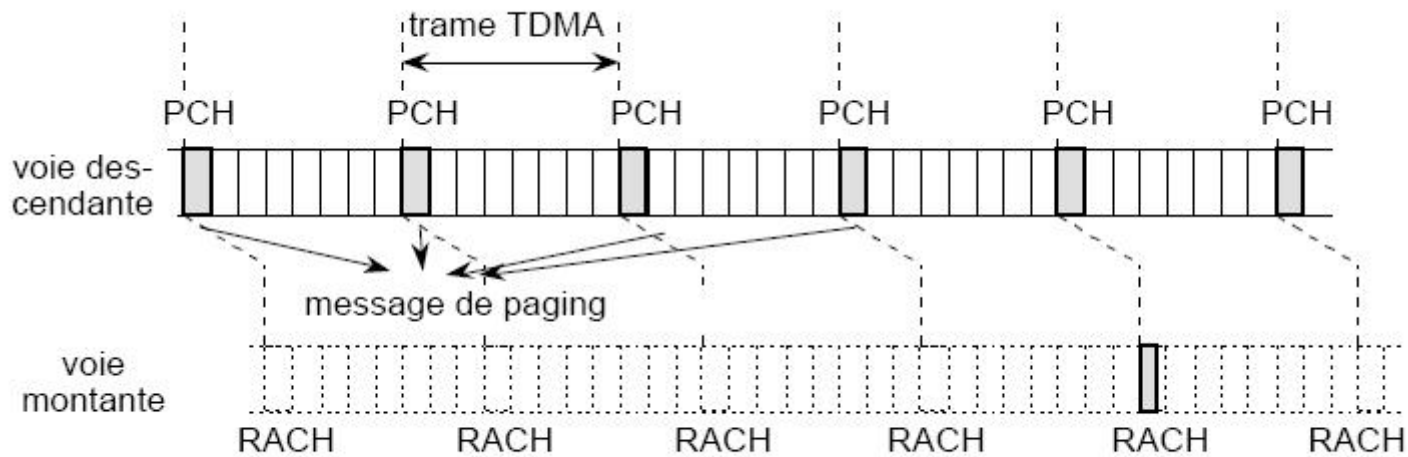
F: TDMA frame for frequency correction burst
 B: TDMA frame for BCCH
 D: TDMA frame for SDCCH
 R: TDMA frame for RACH

S: TDMA frame for synchronisation burst
 C: TDMA frame for CCCH
 A: TDMA frame for SACCH/C
 T TDMA frame for TCH/F

Etablissement Communication entrante

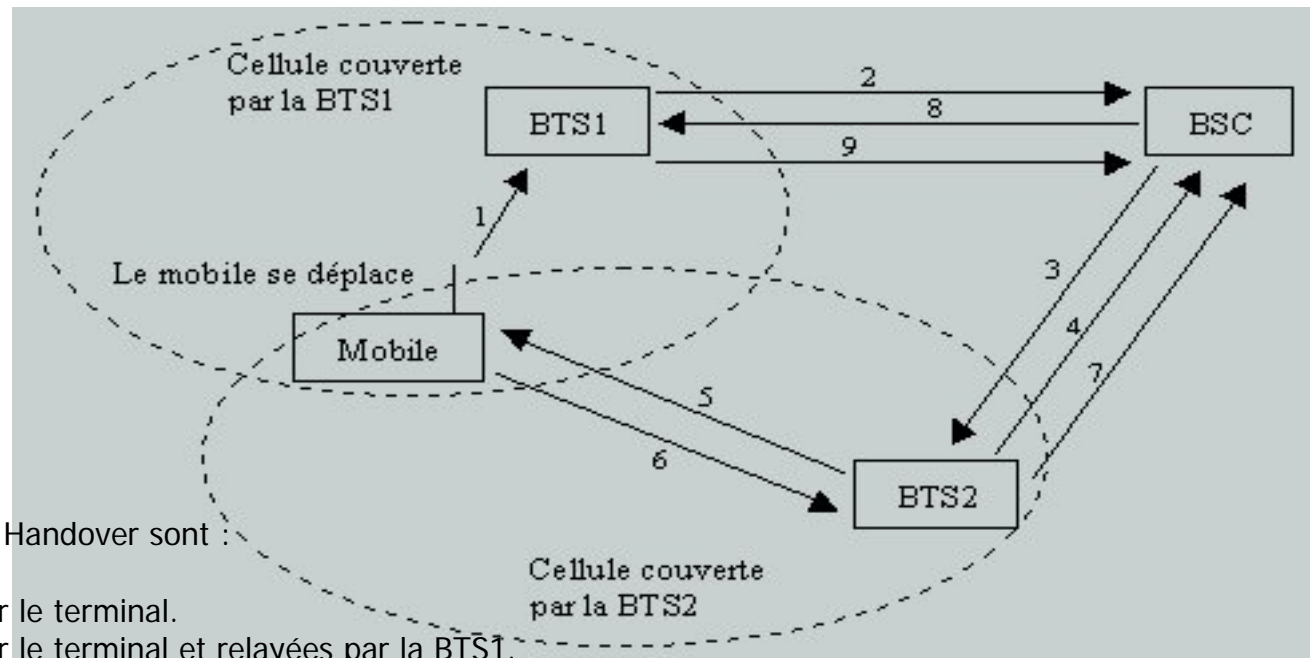
Mobile déjà localisé

Procédure de recherche du Mobile grâce au paging



Procédure ensuite identique à la communication sortante

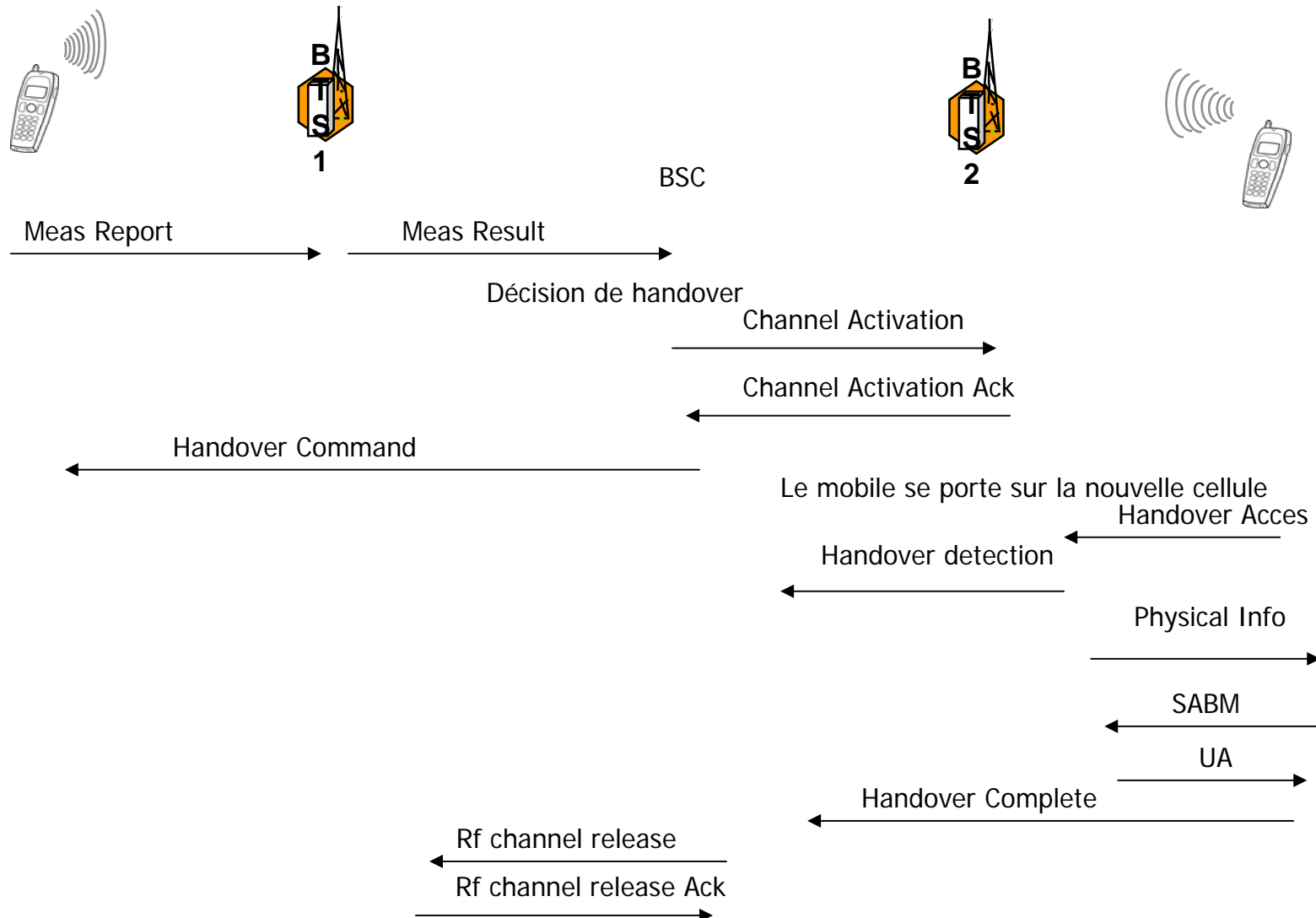
La procédure de Handover



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. Acquiescement de la BTS2.
5. Envoi de la commande de handover au terminal via la BTS2.
6. Acquiescement du terminal.
7. Acquiescement du terminal relayé par la BTS2.
8. Commande de libération du canal.
9. Acquiescement de la BTS1.

La procédure de Handover



La procédure de Handover

- 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 un handover et un changement de MSC, le deuxième MSC ne sera qu'un relais du premier

Conclusion

- Le GSM a démocratisé l'usage du téléphone Mobile en Europe en s'appuyant sur
 - Des technologies « tout numérique » (FTDMA, codage de parole...)
 - La sécurité (authentification, chiffrement)
 - L'itinérance entre pays et même entre opérateurs
 - La collaboration entre pays
- Le GSM a toutefois quelques lacunes
 - La transmission de données et l'utilisation de la ressource radio n'est pas optimum
 - Convergence vers l'internet pas aisé

Mon site sur les télécommunications

- <http://www.roullet.eu>