

Plan

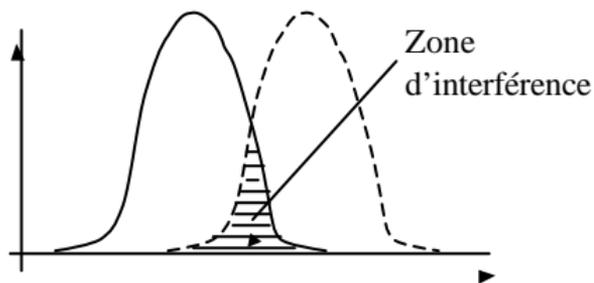
- Introduction
- Le concept cellulaire
- GSM
- GPRS et UMTS
- Conclusion

Réseaux mobiles et sans fil

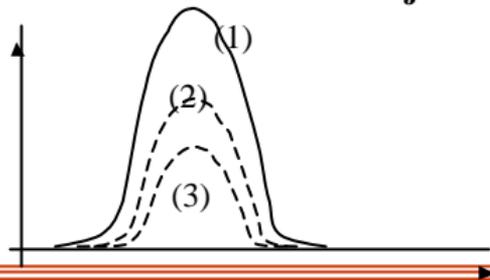
- Réseaux de mobiles et réseaux sans fil
 - Réseaux de mobiles :
 - Donner la capacité à un utilisateur mobile de communiquer à l'extérieur de son réseau d'origine en conservant son adresse (GSM, IP-mobile)
 - Problèmes de compatibilité de signalisation
 - Réseaux sans fil : lié au support de transmission
 - Support hertzien (pas de prise murale)
 - Exp : téléphone sans cordon de résidentiel

Le concept cellulaire

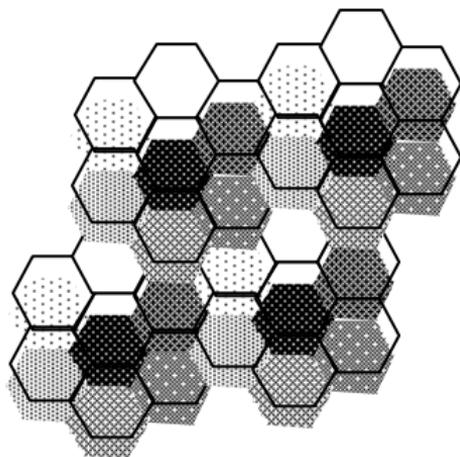
- Interférence et motif cellulaire



Interférences canaux adjacents



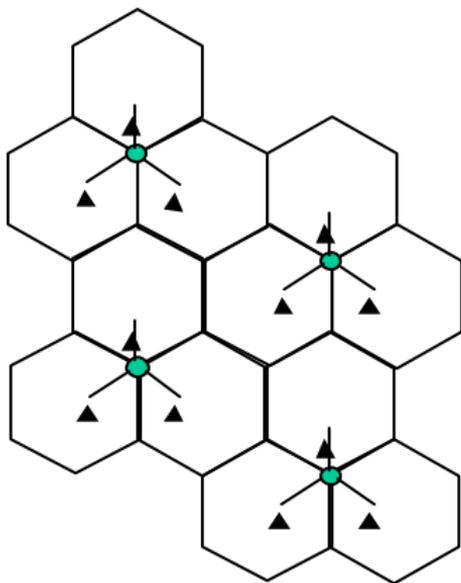
Interférences co-canales



Planification

Le concept cellulaire

- Exp :
 - Motif 4/12 (GSM) : dans un bloc contiguë de 4 sites (incluant 3 cellules par site) chaque fréquence est utilisée une seule fois
 - Antennes sectorielles



Motif 4/12

Panorama et générations

- 1G : 1ère génération : années 80, systèmes sans cordon, (DECT, CT1 et CT2)
- 2G : 2ème génération : années 90, GSM, IS-95
- 2G+ : GPRS
- 3G : 3ème génération : UMTS
- 4G et au delà.

Architecture générale

- PLMN (Public Land Mobile Network) relié au réseau PSTN
- PLMN se décompose en 3 sous-systèmes:
 - Sous-système radio (BSS Base Station Subsystem)
 - Sous-système réseau (NSS Network SubSystem)
 - Sous-système de gestion et de maintenance (OSS Operation Support Subsystem)

Le sous-système radio

- MS (Mobile Station) : terminal mobile
 - De plus en plus performants et légers
 - Abonnement séparé du terminal
 - Carte à puce SIM (Subscriber Identity Module)
 - Caractéristiques de l'abonnement, identités IMSI¹ et le TMSI², et les algorithmes de chiffrement
 - Identité propre au terminal : IMEI³
 - Puissance maximale d'émission de 0.8 à 8 W

¹ International Mobile Subscriber Identity

² Temporary Mobile Subscriber Identity

³ International Mobile Equipment Identity

Echanges lors d'un appel



MSISDN →

1. Le MSISDN est numéroté. Routé par le réseau fixe vers le MSC le plus proche

—— **MSISDN** →

2. GMSC interroge le HLR pour connaître le MSC

—— **IMSI** →

3. HLR traduit MSISDN en IMSI et interroge le VLR

—— **MSRN** →

4. VLR attribue un MSRN au mobile et le transmet au HLR

—— **MSRN** →

5. HLR le retransmet au GMSC

—— **MSRN** →

6. GMSC établit l'appel vers le MSC courant comme un appel tel normal (num est MSRN)

—— **TMSI / IMSI** →

7. MSC va enfin appeler le mobile en utilisant l'id temporaire TMSI

Le sous-système réseau

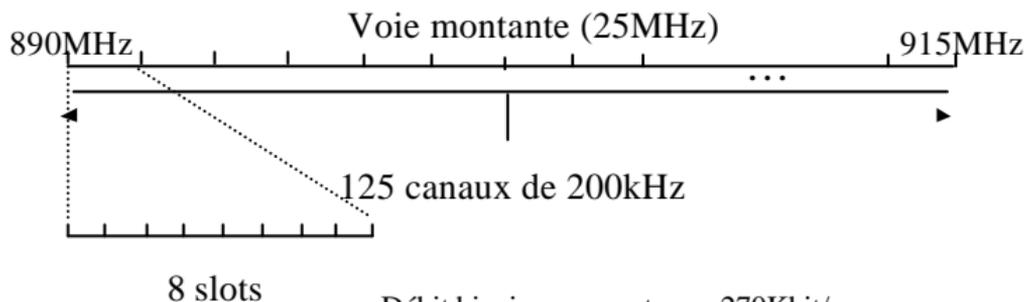
- NSS : interconnexion avec les réseaux fixes
- Gère l'établissement des appels / mobilité
- Trois éléments :
 - MSC (Mobile-services Switching center)
 - HLR (Home Location Register)
 - VLR (Visitor Location Register)
- Il utilise deux bases de données : EIR¹ et AUC²

¹ EIR : Equipment Identity Register

² AUC : AUthentication Center

L'interface radio : le canal physique

- Couche physique
 - gère l'émission et la réception des signaux
- Technique d'accès : MF-TDMA
- Écart duplex (45MHz)



Débit binaire sur une trame 270Kbit/s

Modulation GMSK (Gaussian Minimum Shift Keying)

Les fonctions du réseau cellulaire

- Gestion des ressources Radio RR (Radio resource management)
 - Sélection de cellule (choix de la porteuse), ouverture d'une connexion, contrôle en cours de communication, handover, terminaison
- Gestion de la mobilité MM (Mobility Management)
 - Gestion de l'itinérance, procédure de mise à jour de zone de localisation
 - Gestion de la sécurité
 - Protéger l'utilisateur et le réseau
 - usurpations d'identité, écoutes frauduleuses, utilisations abusives
 - Authentification
 - Cryptage
- Gestion des connexions CM (Connexion Management)
 - Établissement et relâchement des appels

Contrôle en cours de communication (RR)

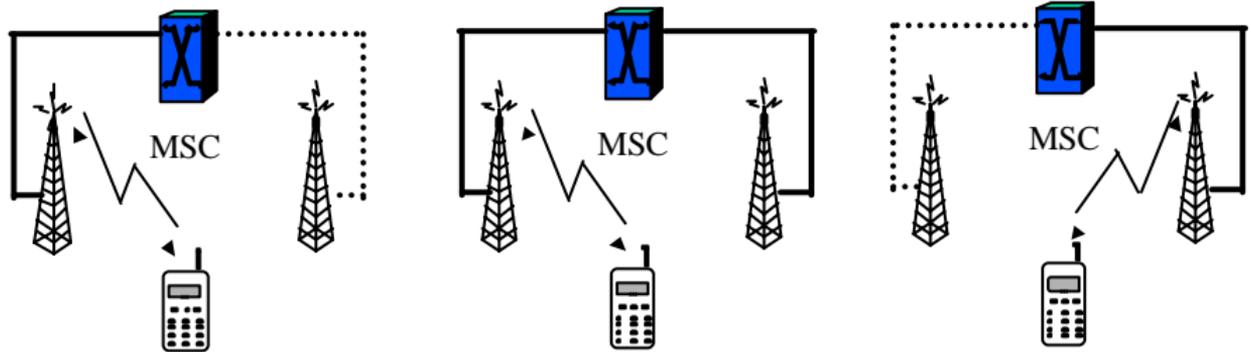
- Garantir une bonne qualité de la liaison
- Contrôle de puissance (via SACCH)
- Le BSS détermine les niveaux de puissance adéquats (grâce aux mesures)
- Utilisation du SACCH pour la compensation temporelle (ou *timing advance*)

Le handover : phase de mesures

- Ms et BTS effectuent des mesures
- Paramètres recueillis :
 - La puissance du signal reçu (qualité du lien)
 - MS (canal descendant), BTS (canal montant)
 - Le taux d'erreur binaire (BER) (calcul du C/I)
 - Distance entre le mobile et la station de base (grâce à la valeur de l'avance en temps)
- Paramètres diffusés par une station :
 - Identité de la station
 - Les fréquences des canaux balise des stations voisines
- Les intervalles de mesures doivent être petits
 - GSM : remontées de mesures au BSC toutes les 480ms
 - Au maximum : mesure de 6 stations

Le handover : phase d'exécution

- Si déclenchement
 - Etablissement du nouveau canal
 - Transfert de la connexion vers le nouveau lien
 - Libération de l'ancien



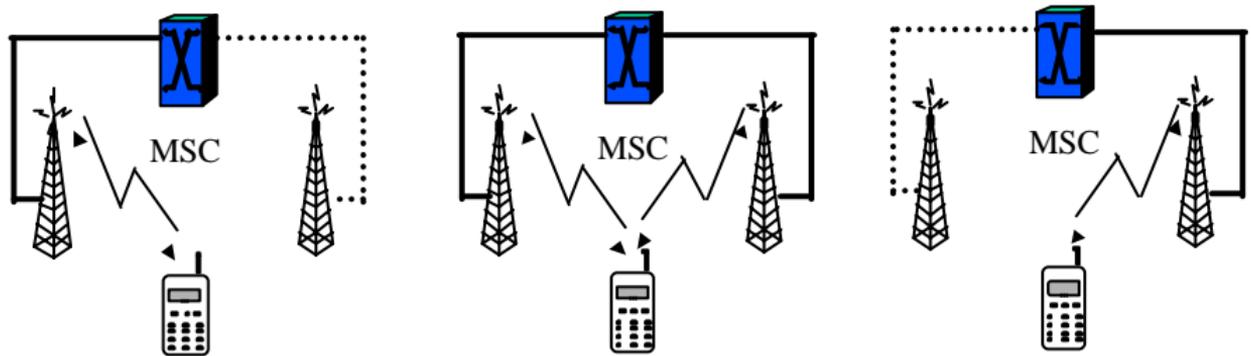
Le MS ne gère qu'un seul canal

Hard Handover

(GSM)

Le handover : phase d'exécution

- Si déclenchement
 - Etablissement du nouveau canal
 - Transfert de la connexion vers le nouveau lien
 - Libération de l'ancien



Soft Handover

(CDMA)

Le handover

- Pour résumer :
 - Pendant la communication
 - Le lien radio est mesuré
 - Si la qualité passe sous un seuil : déclenchement
 - Décision d'effectuer le HO
 - L'ancienne station transmet à la nouvelle les paramètres du mobile impliqué (clé de chiffrement, débit,...)
 - Le réseau transmet au mobile un message (référence sur le nouveau canal de transmission)
 - L'ancien canal est libéré
 - Si pas de ressources disponible : *échec de handover (call dropped)*

Gestion de la mobilité (MM)

- Gestion de l'itinérance et de la sécurité
- États d'un mobile

- Éteint

- mémorisation de la dernière localisation connue
- Commutation sur la messagerie

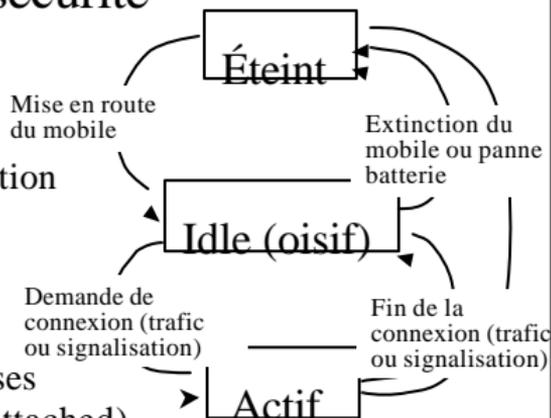
- Idle

- Informe régulièrement le réseau de ses changements de localisation (IMSI-attached)

- actif

- Procédure d'attachement

- pour indiquer le retour du mobile dans le réseau



Mise à jour de la localisation (MM)

- Procédure de mise à jour de localisation :
 - Le mobile sait qu'il change de zone de localisation grâce au canal BCCH
 - Il prévient le nouveau VLR (donne son TMSI)
 - Le nouveau VLR (qui peut être l'ancien) récupère auprès de l'ancien le profil du mobile
 - Le VLR informe le HLR de la nouvelle zone de localisation du mobile
 - Le HLR demande à l'ancien VLR d'effacer les infos relatives au mobile (si VLR différent)
- Procédure qui met à jour les informations de localisation du mobile dans le VLR et le HLR

Sécurité (MM)

- Cryptage
 - Protection contre les écoutes inopportunes
 - De $K_i + \text{Rand} + A_8$ est calculée la clé K_c
 - K_c : 64 bits
 - Séquence générée par $A_5(K_c, \text{numéro de trame})$
 - Combinaison avec la séquence à émettre
- IMEI (terminal physique)
 - Vol,...
 - EIR (Equipment Identity Register)

Gestion des connexions (CM)

- Établissement et relâchement des connexions
- Basé sur la signalisation SS7
- Appel issu du mobile
 - Allumé
 - Parcours des fréquences
 - État Idle
 - Signalisation périodique pour la localisation
 - Composition d'un numéro
 - Envoi d'une demande de connexion (via RACH)
 - Allocation d'un canal dédié de signalisation SDCCH (via AGCH)
 - Procédures d'authentification et d'autorisation d'appel
 - Le réseau route la demande vers le PSTN (SS7)

Etablissement d'appel

Mobile station	Base station	Category	Logical Channel
→	←		FCCH
←	→	RRM	SCH
←	→	RRM	BCCH
←	→	RRM	PCH
←	→	RRM	RACH
←	→	RRM	AGCH
←	→	RRM	SDCCH
←	→	MM	SDCCH
←	→	MM	SDCCH
←	→	RRM	SDCCH
←	→	RRM	SDCCH
←	→	CM	SDCCH
←	→	CM	SDCCH
←	→	CM	SDCCH
←	→	RRM	SDCCH
←	→	RRM	SDCCH
←	→	CM	FACCH
←	→		TCH
←	→		TCH
←	→	CM	FACCH
←	→	CM	FACCH
←	→	CM	FACCH
←	→	RRM	FACCH

2G, pourquoi un tel succès?

- Spécifications rigoureuses
 - Interfonctionnement complet
- Standardisation européenne
- Un système bien conçu :
 - Interface radio, réseau cœur
 - Gestion de la mobilité, de l'itinérance des utilisateurs
- Complexité limitée : coûts réduits

Motivations

- GSM
 - Téléphonie : circuit, faible débit
 - Services données ?
- Evolutions
 - HSCSD (High Speed Circuit Switched Data)
 - Transfert de données en utilisant les circuits de voix
 - GPRS (General Packet Radio Service)
 - Architecture réseau en mode paquet
 - EDGE (Enhanced Data for GSM Evolution)
 - Débits supérieurs (modulation)

Le HSCSD

- High Speed Circuit Switched Data
 - Débit plus élevé
 - Allouer jusqu'à 4 slots par user par trame TDMA
 - Débit max : $4 \times 14,4 = 57,6$ Kbit/s
 - Manque de souplesse dans l'allocation des ressources radio
 - Pas d'investissement dans le HSCSD

GPRS

- Deux nœuds
 - SGSN : Serving GPRS Support Node
 - Connexion avec la station de base (relais de trames), semblable au MSC
 - GGSN : Gateway GPRS Support Node
 - Connexion avec les réseaux de type paquet (Internet)
- Encapsulation des paquets avec le protocole GPRS (tunneling)
- Greffé sur le réseau GSM (même bande de fréquences)

EDGE

- Enhanced Data for GSM Evolution
- HSCSD et GPRS augmentation de débit / GSM
- Mais :
 - Même débit brut sur un time slot (GSM)
- Solution EDGE
 - Introduction d'une nouvelle modulation
- EDGE + HSCSD  ECSD
- EDGE + GPRS  E-GPRS

Conclusion 2,5G

- Limitation de débit du GSM
- HSCSD
 - Autorise l'allocation de plusieurs slots
 - Mais architecture réseau pas adaptée au transfert de données
- GPRS
 - Autorise l'allocation de plusieurs slots
 - Allocation dynamique des ressources radio
 - Réseau fixe adapté au transfert de paquet
- EDGE
 - Encore plus de débit : schémas de modulation et de codage plus efficaces

Motivations

- Succès de la 2G
- Saturation des réseaux existants
- Marché en pleine expansion
- Services multimédias
- Couverture universelle
- IMT-2000 (Universal Mobile Telecommunications for the year 2000)
 - Niveau mondial (UIT)
 - FPLMTS
- UMTS
 - En Europe (ETSI)

Les fréquences

- Bande de 230MHz (autour des 2GHz)
 - Bandes appairées ($2 \times 60\text{MHz}$) : 1920-1980 et 2110-2170 FDD/W-CDMA
 - Bandes non appairées (50MHz) : TDD/TD-CDMA
 - Satellites (MSS) : 60 MHz
- IP et mode paquet :
 - 384 Kbps pour une mobilité complète et 2 Mbps pour une mobilité limitée

UMTS

- La migration du GSM vers l'UMTS
 - Progressive
 - Radio
 - Réutilisation de la bande existante
 - Déploiement par îlots
 - Terminaux bi-modes
 - Réseau
 - Rajout de nouveaux équipements
 - Intégration du mode paquet et de IP
 - 2 phases :
 - Services offerts semblables à ceux du GSM
 - Évolution vers des services haut débit multimédias de bout en bout

Architecture

UTRAN : UMTS Terrestrial Radio Access

GSM et UTRAN

- | | | |
|---------------------------------|---|---|
| • MS (Mobile Station) | ↔ | • UE (User Equipment) |
| • BTS | ↔ | • NodeB |
| – Contrôle des ressources radio | | – Contrôle partiel des ressources radio |
| – Contrôle du lien radio | | |
| • BSC | ↔ | • RNC (Radio Network Controller) |
| – Allocation des ressources | | – Allocation des ressources |
| – Contrôle du lien radio | | – Contrôle du lien radio |
| • MSC | ↔ | • UMSC (UMTS MSC) |
| • BSS | ↔ | • RNC (Radio Network Subsystem) |
| • Abis(BTS/BSC) | ↔ | • Iubis (NodeB/RNC) |
| • A (BSC/MSC) | ↔ | • Iu (RNC/CN) |
| • Inexistante | ↔ | • Iur (RNC/RNC) |

TDMA

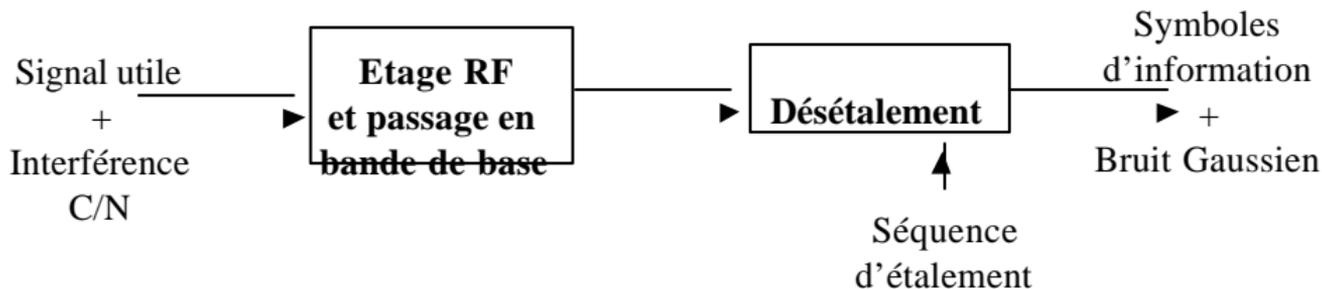
CDMA

L'interface radio UTRA

- Mode W-CDMA (Wideband CDMA) en FDD (Frequency Domain Duplex)
- Mode TD-CDMA en TDD (Time Domain Duplex)

Le mode FDD W-CDMA

- Le récepteur CDMA



- L'accès multiple

- Plusieurs séquences orthogonales

- Pbm : trajets multiples

émission asynchrone des mobiles

} ➡ perte partielle de l'orthogonalité

- ✍ pour détecter le signal utile :

- ✍ l'ensemble des signaux (signal utile + brouilleurs) reçus à la station radio avec les mêmes niveaux de puissance

- ✍ besoin de contrôle de puissance

Le mode FDD W-CDMA

Accès multiple	DS-CDMA
Duplex	FDD
Débit chip	3.84 Mchip/s
Durée trame	10ms
Débit variable	Facteur d'étalement variable et multicode (384 kbit/s par code)
Bande de fréquence	Entre 4.4 et 5 MHz

Le mode TDD TD-CDMA

- Duplex temporel TDD
 - Multiplexage temporel des deux sens de transmission sur une même porteuse
- Avantages
 - Allocation de spectre : pas de contraintes d'espacement (FDD)
 - Bonne gestion du trafic assymétrique (exp : www, rapatriement de fichiers,...)
 - Partage dynamique adapté aux conditions variables de trafic (temps + espace)

UTRA

Déploiement et couverture	grandes cellules	petites cellules (contraintes de sync. et temps de garde)
Services supportés	services symétriques	mode paquet, asymétrique
Transfert intercellulaire	soft handoff	handoff normal
Synchronisation entre stations de base	pas de synchronisation	synchronisation
Planification	couverture cellulaire en fonction du trafic - pas de plan de fréquence	plan de fréquence - ne varie pas en fonction du trafic

Evolution 2G-3G dans le monde

	Etats Unis		Japon	Europe	
	TDMA	CDMA		TDMA	CDMA
2 ^e Génération	IS136	IS95/CDMA One	PDC	GSM	
3 ^e Génération	Edge GPRS	CDMA2000	W-CDMA	TD-CDMA	W-CDMA
Normalisation	TIA		ARIB	ETSI	
Système	UWC-136	CDMA2000	W-CDMA	UMTS	

