CHAPITRE 3: La téléphonie numérique cellulaire GSM

Plan du chapitre 3

- Introduction
- GSM
  - Généralités
  - Concept cellulaire
  - Architecture du réseau
  - Le handover
  - Identités dans le GSM
  - La sécurité

Introduction

- Marconi démontre la première transmission sans fils ...
- 1946 Premier Téléphone mobile aux U.S. (1 cellule, St Louis, ´Missouri)
- 1973 New-York, Premier téléphone cellulaire (Martin Cooper, ´Motorola, vers Joel Engel, Bell Labs)
- 1977 Bell Labs construit un proto de système cellulaire, Chicago, 2000 client
- 1981 Premier système Européen, NTM-450, Suède
- **Le réseau cellulaire analogique en Amérique du Nord :**
  - AMPS (Advanced Mobile Phone Service)
  - Déployé en 1983
  - Le premier standard au monde en téléphonie cellulaire
  - Bande de fréquences : 800-900 MHz – (en comparaison, la radio FM prend la bande 88 à 108 MHz)
  - 30 kHz de bande pour chaque usager
  - Même type de modulation que la radio FM
- **Limites de AMPS**
  - Faible capacité (nombre d'appelants simultanés)
  - Spectre de fréquences limité
  - Transmission de données peu efficace
  - Possibilité d'écoute (pas de vie privée)
  - Pas de sécurité (aucun encryptage)

1ère génération
Les réseaux cellulaires analogiques

GSM (Global System of Mobile communication)

❑ Généralités

- Développé à partir de 1990;
- **2000 :** 400 millions d'abonnés dans le monde
- Représente la première technologie de téléphonie numérique sans fil ;
- Son débit moyen est similaire à celui du FAX, c'est--à--dire 9,6 kbits/sec.
- Système radio mobile basé sur une structure cellulaire
- Le mobile transmet par radio la communication vers la station de base de sa cellule
- Chaque cellule est équipée d'une station de base ou BTS (Base Transmitter Station) munie de ses antennes installées sur un point haut (château d'eau, immeuble ...), la puissance d'émission allant de 2,5 W à 320 W .
- Le système GSM doit satisfaire les critères suivantes:
  - Bonne qualité de la voix
  - Baisse des couts des équipements et des services
  - Passage d'un pays à un autre sans interruption du service
  - Habilité pour supporter de nouveaux services
  - Utiliser efficacement le spectre de fréquences
  - Compatibilité avec les autres systèmes (RNIS, …)
- Communications montantes uplink (Mobile → station de base) : BF: 880-915 MHz
- Communications descendante downlink (station de base →Mobile) : BF: 925-960 MHz
- Téléphones mobiles pouvant opérer à la fois en Europe et en Amérique du Nord sont donc appelés « tri-bandes »

GSM (Global System of Mobile communication)

❑ Généralités

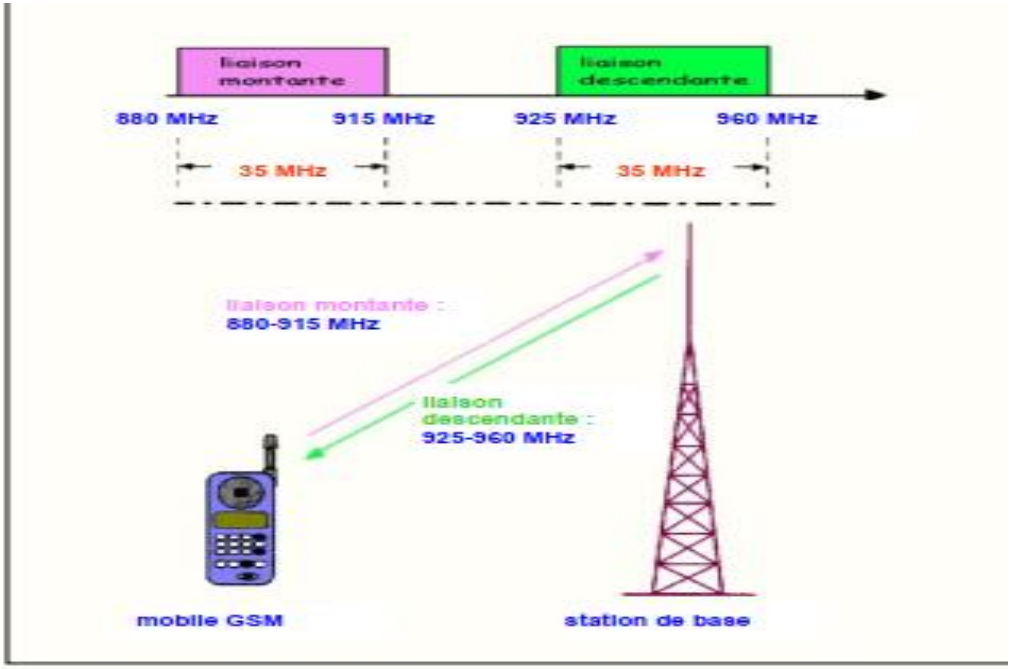
4 systemes

1. G.S.M : Global System for Mobile :

Europe + Moyen orient +Afrique

2. D-AMPS (Digital Advanced Mobile Phone System) → US
3. Code Division Multiple Access (IS-95) → US-Qualcomm
4. P.D.C. Personal Digital Cellular → Japon

- **GSM Dominant** Europe, Monde sauf USA
- **Bandes** 900 MHz, 1800 MHz (DCS-1800) ,
  1900 MHz (PCS-1900 , USA) ,
  400 MHz (rural) ,
  800 MHz (Amerique du Nord)
- 1991: première communication expérimentale par GSM, Specification de DECT (Digital European Cordeless Telephone), portée de 100 a 500 m, 120 canaux, 1,2 Mbit/s en données, voix encryptée, authentification ...



GSM (Global System of Mobile communication)

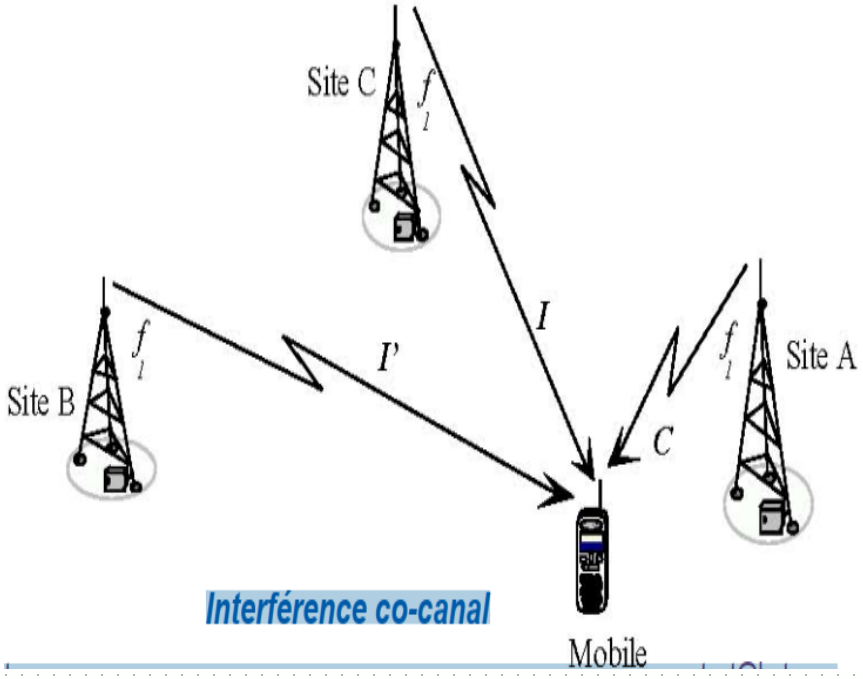
❑ Concept cellulaire

➢ **Problème de base** = Comment desservir une région de taille importante (pays, continent)

- Avec une bande de fréquences limitée,
- Avec une densité de trafic importante, qui varie dans le temps et dans l'espace et pouvant augmenter,
- Offrir des services téléphoniques à des usagers fixes et mobiles ?

➢ **Réutilisation des fréquences**

- Repose sur l'utilisation des mêmes fréquences porteuses pour couvrir des zones différentes séparées par des distances suffisantes pour que l'interférence co--canal ne soit pas importante.



➢ **Spécificité des systèmes cellulaires**

- Gestion de la **mobilité des abonnés.**
- Gestion de l'**interface radio**.

GSM (Global System of Mobile communication)

❑ Concept cellulaire

➢ Cellule

Région couverte par le réseau est divisée en cellules dont les tailles sont fixées par :

- Puissance transmise et la sensibilité des émetteurs - récepteurs,
- Rapport C/I fixé par le système, C=signal utile , I: signal d'interférences
- Capacité à gérer le maximum de communication possibles sur la surface allouée avec la QoS (Quality of service) demandée,

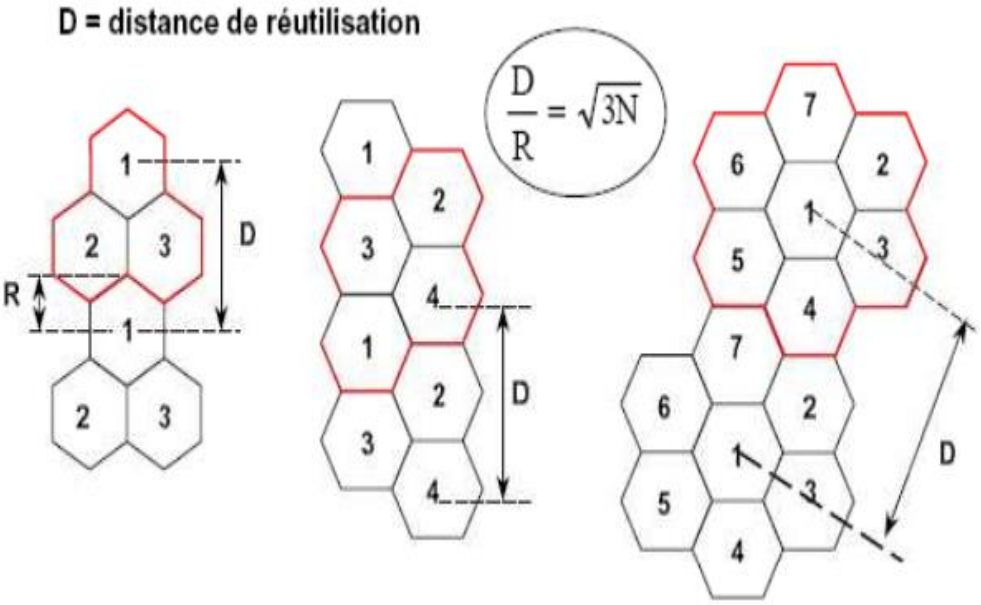
Taille: milieu rural (3-30Km) , milieu urbain (300m -3Km)

➢ Notion de motif (bloc, cluster)

- ➢ Cellules regroupées en bloc
- ➢ 4,7,12 ou 21 cellules / bloc

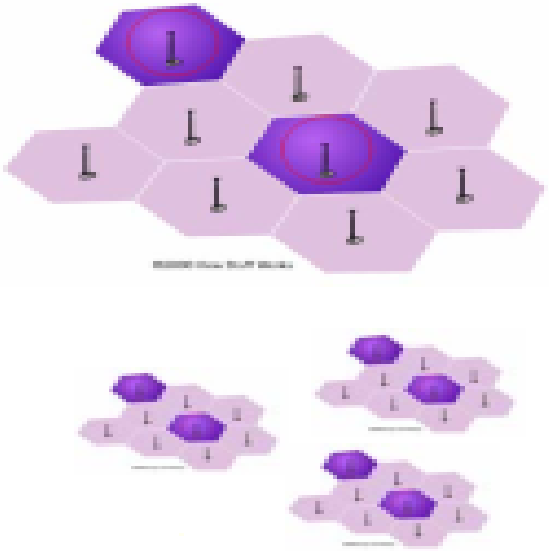
en fonction du nombre de fréquences (canaux) disponibles.

- ➢ But : Réutiliser les mêmes fréquences à une distance suffisante pour éviter les interférences.
  D: Distance inter motif.



GSM (Global System of Mobile communication)

❑ Concept cellulaire



➢ **Compromis sur la taille des cellules:**

- Emetteur-récepteur très puissant: champ vaste mais BP se sature par les communications
- Emetteur-récepteur moins puissant: cellule petite mais communication en nombre plus important

Par exemple :

– Rayon de 10 km : capacité de A canaux
– Rayon de 1 km : capacité de 100 A canaux (autrement dit, un rayon 10 fois plus petit permet d'augmenter la capacité d'un facteur 100)
– Rayon plus petit : encore plus d'usagers possibles

➢ **La conception du réseau cellulaire dépend de:**

- Topographie (bâtiments, collines, montagnes, …)
- Densité de la population pour définir la dimension de la cellule
- Deux cellules voisines ne peuvent pas utiliser la même Bande fréquentielle
- La distance entre deux cellules qui ont la même BF doit être 2 fois le diamètre de la cellule,
- La capacité du réseau peut être augmentée en découpant une cellule en sous cellules (diminuer la puissance d'emission et augmenter le nombre d'utilisateurs)

GSM (Global System of Mobile communication)

❑ Architecture du réseau

➢ Mobile Station (MS)

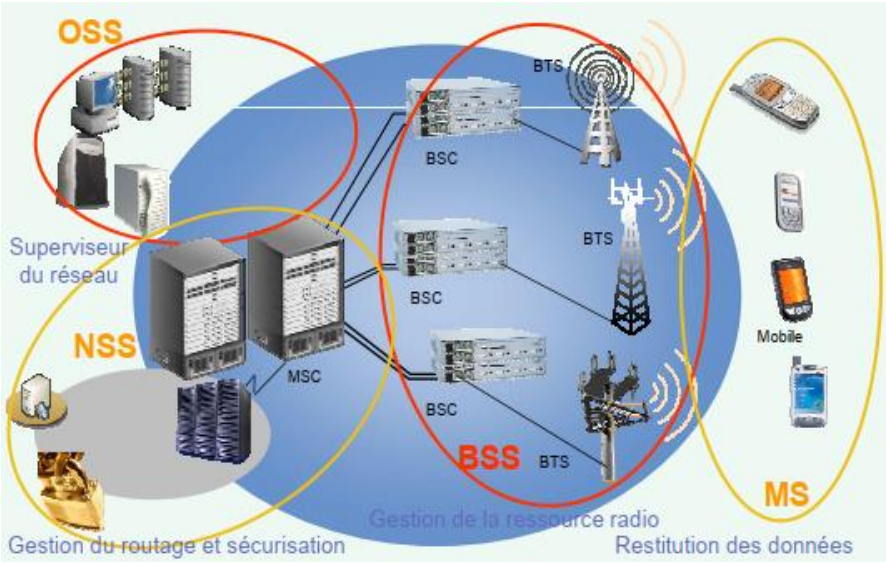
1. IMEI (International Mobile Equipement Identity)
2. La carte SIM (Subscriber Identity Module):

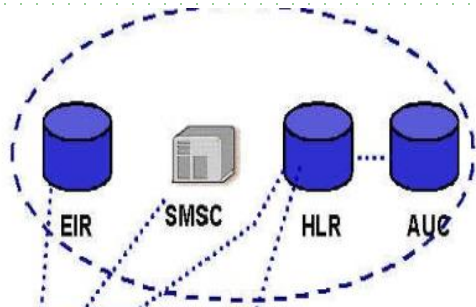
circuit intégré, elle contient:

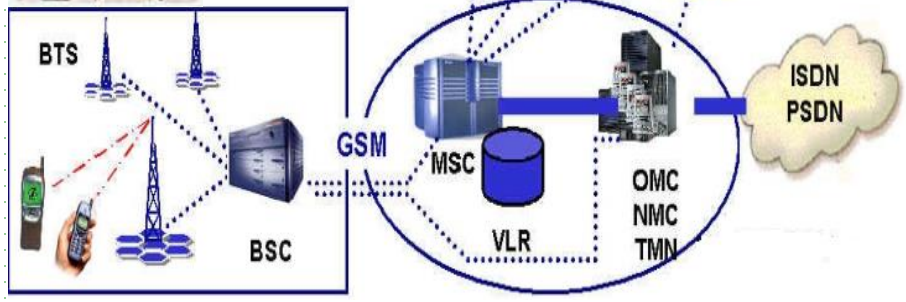
- Identités de l'abonné :

IMSI : (International Mobile Subscriber Identity).
MSISDN: (Mobile Station International ISDN).
TMSI: (Temporary Mobile Subscriber Identity).

- PIN (Personal Identification Number);
- La clé d' authentification Ki,
  et les algorithmes A3, A5 et A8.







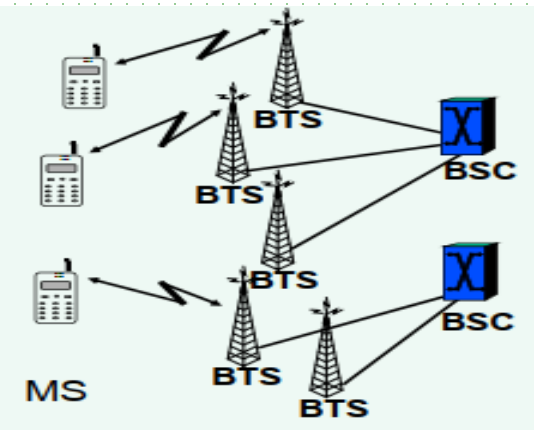
Fonctions de la SIM:

- Transmission de la voix et la donnée.
- Synchronisation fréquentielle et temporelle.
- Mesure de l'énergie et de la qualité de signal.
- Mise à jour de localisation.
- Affichage des SMS.

GSM (Global System of Mobile communication)

❑ Architecture du réseau

➢ Sous système Radio (BSS: Base Station Sub-system)



- **BTS (Base Transceiver Station):** Emetteurs-récepteur

1. Chargée de la transmission radio :
   modulation, démodulation, égalisation, codage
   correcteur d'erreur
2. Gère toute la couche physique : multiplexage
   TDMA, chiffrement, saut de fréquence…
3. Réalise l'ensemble des mesures radio nécessaires pour vérifier qu'une communication se déroule normalement
4. Gère la couche liaison de données pour l'échange
   de signalisation entre les mobiles et l'infrastructure
5. Capacité maximale : 16 porteuses (~100
   communications simultanées.

Les BTS rayonnantes : couvrent des zones à faible densité d'abonnés (jusqu'à 20 kms).

Les BTS ciblés : Elles couvrent des zones de plus forte densité d'abonnés et permettent d'émettre suivant un angle très précis.

Les micro BTS : Elles couvrent les microcellules où la densité d'abonnés est importante installées dans les centres villes

GSM (Global System of Mobile communication)

❑ Architecture du réseau

➢ Sous système Radio (BSS: Base Station Sub-system)

- **BCS (Base Station Controler):** Controleur de BTS, il gére:
  - ✓ L'allocation des fréquences
  - ✓ Le contrôle de puissance,
  - ✓ Les handover : décision et exécution
  - ✓ Contrôle d'admission des appels.
  - ✓ Les mesures reçues par les BTS
- Un BSC standard gère jusqu'à 60 BTS

➢ Sous système Réseau (NSS : Network Sub-System)

- S'occupe de l'interconnexion avec le RTC et autres opérateurs, et l'établissement de la communication avec les mobiles.
- **MSC (Mobile-services Switching Center):** commutateur de services (cœur du système cellulaire), il assure:
  - ✓ L'interconnexion avec le réseau fixe et les autres opérateurs ;
  - ✓ Le routage après consultation du **VLR** associé.
  - ✓ La gestion de la mobilité pendant une communication.
  - ✓ Comporte des fonctions de taxations
- **GMSC** : Gateway MSC (quand on quitte son operateur), Ce commutateur est l'interface entre le réseau cellulaire et le réseau téléphonique publique

GSM (Global System of Mobile communication)

❑ Architecture du réseau

➢ Sous système Réseau (NSS : Network Sub-System)

- **VLR (Visitor Location Registe):** Base de données qui contient temporairement des informations sur les abonnés qui visitent une région desservie par un MSC autre que celui auquel ils sont abonnés. Elle contient:
  - Les informations du HLR .
  - La zone de localisation (sous ensemble de cellules).
  - L'enregistrement des terminaux de passage;
  - L'authentification des terminaux par contrôle du numéro IMEI
- **HLR (Home Location Registe):** Base de données contenant les informations sur les abonnés appartenant à la région desservie par le commutateur de services mobiles (MSC). Contient également la position courante de ses abonnés. Elle permet :
  - Fourniture des informations d'un abonné à un **VLR**;
  - Acquisition d'informations issues d'un **VLR**;
  - Acquisition des informations de **chiffrement** d'abonné
- **Centre d'authenticité (AuC – Authentication Center)**

  Base de données protégée qui contient une copie de la clé secrète inscrite sur la SIM de chaque abonné. Cette clé est utilisée pour vérifier l'authenticité de l'abonné et pour l'encryptage des données envoyées.

GSM (Global System of Mobile communication)

❑ Architecture du réseau

➢ Sous système maintenance(OSS: Operation and Maintenance Subsystem)

- **L'OMC ET LE NMC**

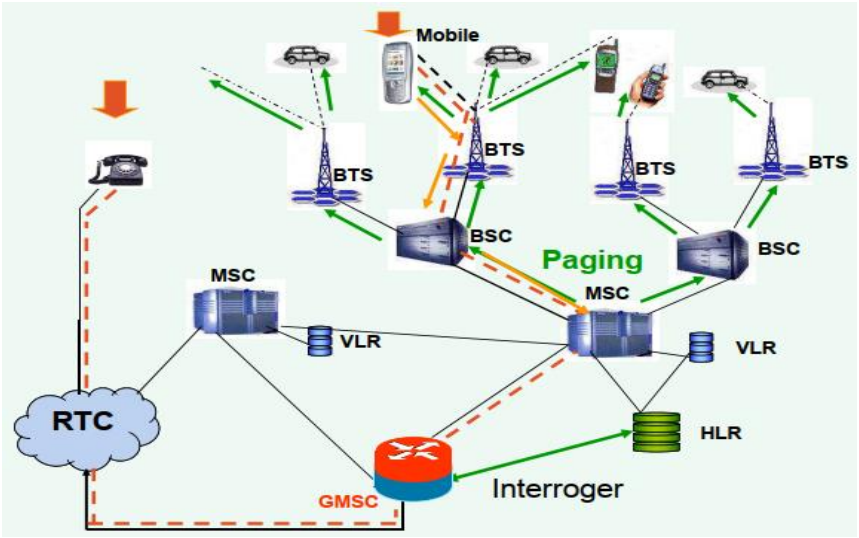
  Contrôler les performances et l'utilisation du système et d'ouvrir une interface homme-machine à l'opérateur responsable de l'exploitation du réseau.
  Le NMC (Network Management Center) opère de manière centralisée. L'OMC (Operation and Maintenance Center) effectue une supervision locale des équipements.
  Parmi les principales fonctions d'administration, citons :
  - la déclaration des abonnés et des terminaux,
  - la facturation,
  - l'observation de trafic et détection des surcharges,
  - la configuration des équipements et des logiciels du réseau,
  - la remontée des alarmes,

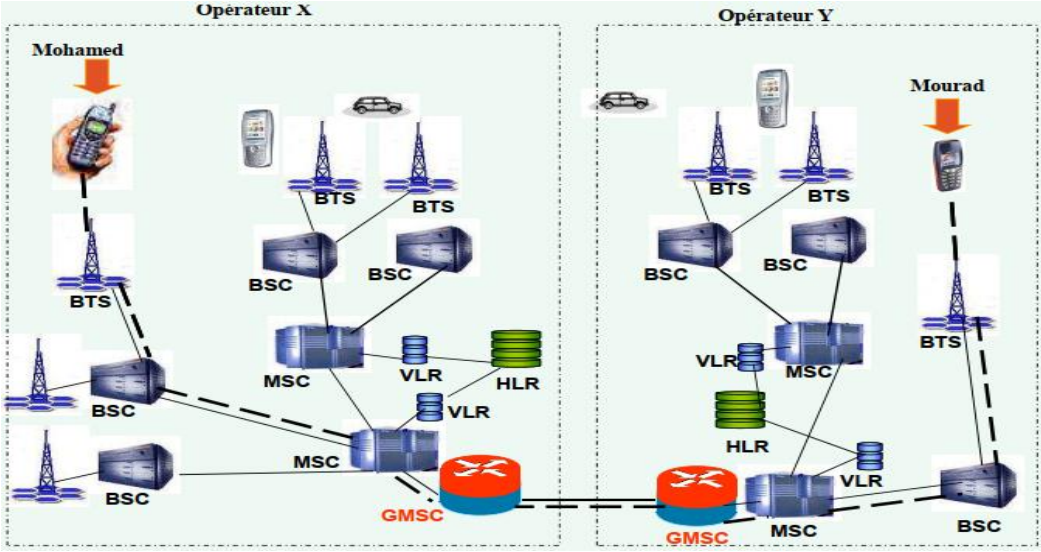
- **L'EIR** (Equipment Identity Register)

  La base de données des abonnés. Elle est consultée pour s'assurer de la légitimité d'un mobile. C'est en particulier dans l'EIR que sont identifiés les mobiles volés et interdits d'accès au réseau.

GSM (Global System of Mobile communication)

❑ Architecture du réseau

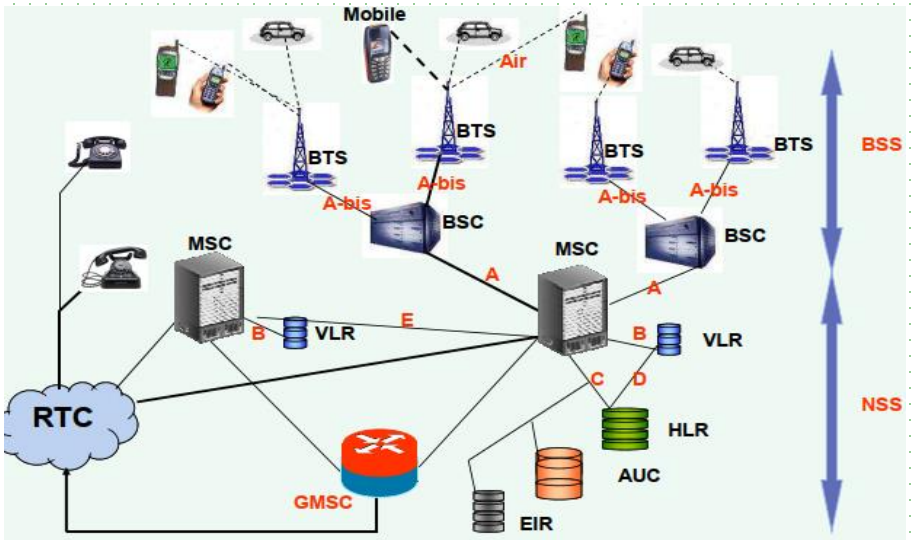




Acheminement d'appels: Appel vers le mobile

Nom	Localisation	Utilisation
Air	Terminal - BTS	Interface radio
Abis	BTS - BSC	Divers (transfert des communications...)
A	BSC - MSC	Divers (transfert de données)
B	MSC - VLR	Divers (transfert de données)
C	GMSC - HLR	Interrogation HLR pour appel entrant
D	VLR - HLR	Gestion de localisation et des abonnés
E	MSC - MSC	Exécution des "handover"
G	VLR - VLR	Gestion des informations d'abonnés
H	HLR - AUC	Echange des données d'authentification

Interfaces réseau



GSM (Global System of Mobile communication)

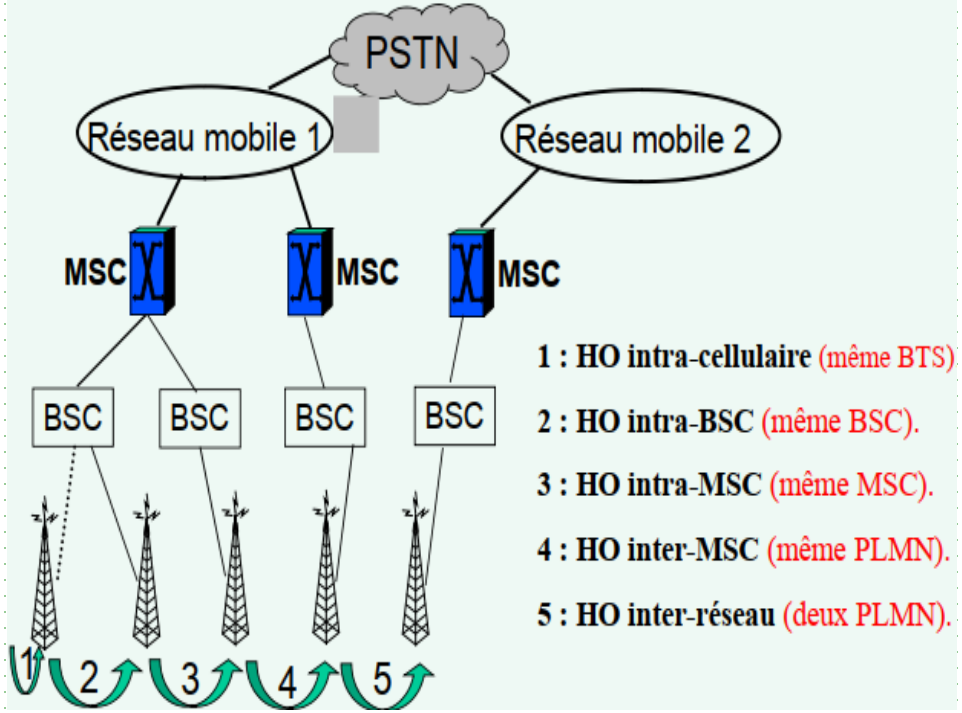
❑ Le Handover

- Procédure de transfert inter cellulaires au cours de communication.
- La décision d'effectuer un handover est à la charge de (MSC + BSC).
- Les causes du Handover sont:

  La qualité de la liaison entre MS et BTS devient mauvaise.

  Les communications d'une cellule chargée sont transférées vers des cellules moins chargées.

- Différents type de HO vus du réseau



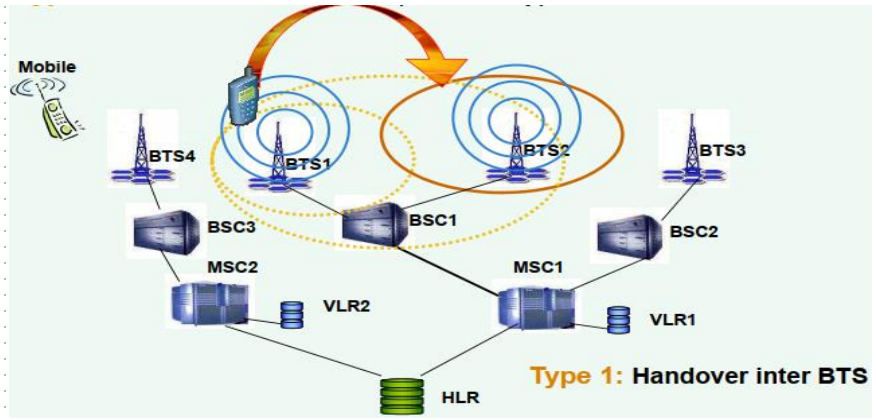
1 : HO intra-cellulaire (même BTS)

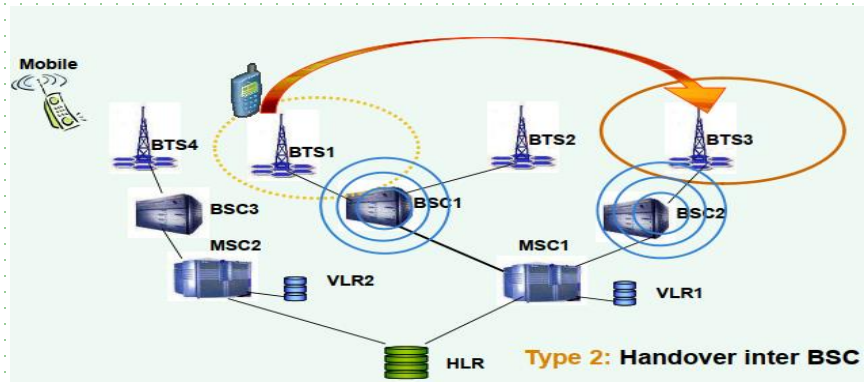
2 : HO intra-BSC (même BSC).

3 : HO intra-MSC (même MSC).

4 : HO inter-MSC (même PLMN).

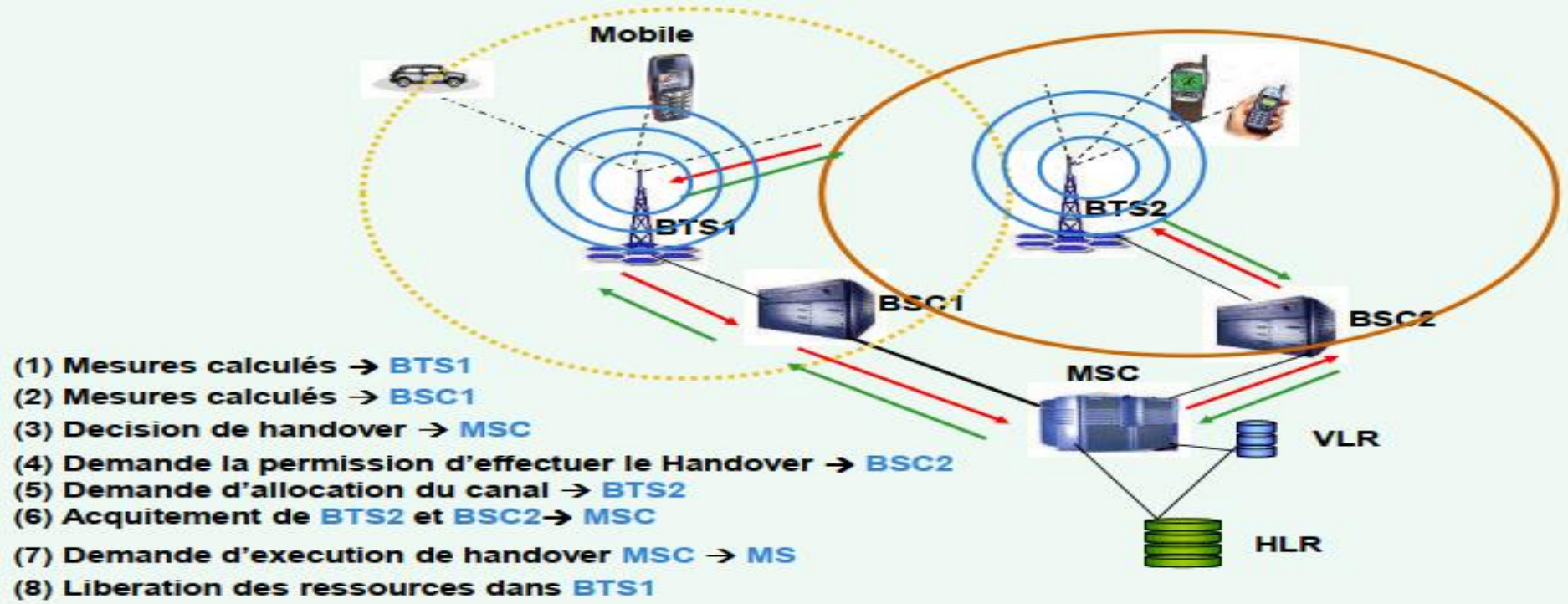
5 : HO inter-réseau (deux PLMN).



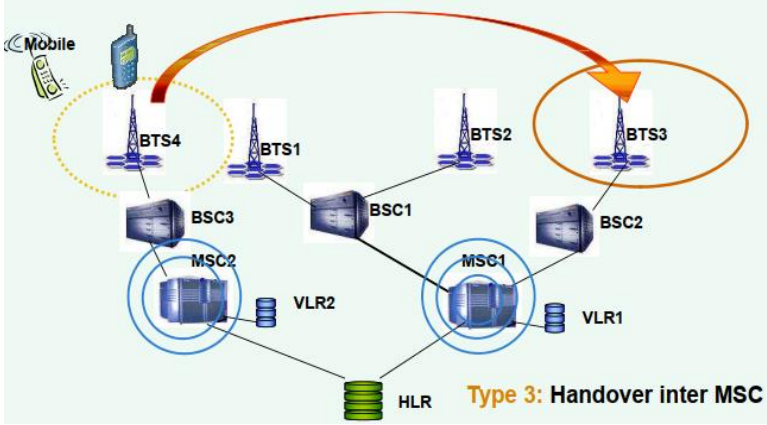


GSM (Global System of Mobile communication)

❑ Le Handover



Scenario de handover inter BTS



GSM (Global System of Mobile communication)

❑ Identités dans le GSM

IMSI (International Mobile Subscriber Identity)

❍ Identité invariante de l'abonné (15 chiffres), stocké dans la carte SIM et dans le HLR

❍ Elle doit rester secrète autant que possible → recours au TMSI

TMSI (Temporary Mobile Subscriber Identity)

❍ Identité temporaire propre à un VLR

❍ Utilisée pour identifier le mobile lors des interactions Mobile/Réseau

MSISDN (Mobile Station International ISDN Number)

❍ Numéro de l'abonné (ex 213 660 00 00 00)

❍ Seul identifiant de l'abonné connu dans le monde téléphonique

MSRN (Mobile Station Roaming Number)

❍ Numéro attribué lors d'un établissement d'un appel

❍ Permet l'acheminement des appels par les commutateurs MSC et GMSC (contient des informations de localisation : MSC courant)

❍ Compréhensible par le réseau fixe (même structure que MSISDN : pays, PLMN, numéro abonné)

IMEI (International Mobile station Equipment Identity)

❍Identificateur du terminal (15 chiffres)

GSM (Global System of Mobile communication)

❑ La sécurité

La carte SIM: personnalise le téléphone, abonnement de manière unique. .
Le code PIN : doit être initialisé lors de la première mise en service de la carte SIM. garantie que l'appareil ne peut être utilisé par une personne non autorisée.
Le verrouillage du téléphone: il est possible de verrouiller le téléphone au moyen d'un Autre code confidentiel, un numéro ou un code alphanumérique, il agit sur l'appareil lui-même en bloquant les appels, les SMS, l'accès au répertoire…
L'authentification: Ceci permet de filtrer les mobiles qui ne sont pas autorisés à accéder à ce réseau et les mobiles interdits de trafic. L'authentification est réalisée par une transaction chiffrée avec la BTS, au moyen d'une clé et un algorithme mémorisés dans le mobile sur la carte SIM et, côté réseau, gérés par l'AUC.
L'interdiction de trafic: Ceci concerne essentiellement les mobiles perdus ou volés. L'opérateur passe le mobile dans un mode « interdit de trafic » qui rend sa carte SIM Inopérante (blocage de la SIM), il est possible de bloquer le téléphone lui-même en donnant son identifiant physique IEMI à l'opérateur..
Le masquage des identifiants: un identifiant temporaire TMSI est délivré au mobile lorsqu'il s'inscrit. Cet identifiant est utilisé dans toutes les transactions entre le mobile et la BTS, afin d'interdire l'interception du véritable identifiant IMSI. L'IMSI n'est utilisé que lors de la mise sous tension du mobile. Ensuite, il ne sera plus identifié que par le TMSI courant attribué à l'inscription lors du déplacement du mobile. La correspondance est gérée par le VLR.