

# **Architecture des Réseaux Mobiles**

**[sofiane.elmahroug@gmail.com](mailto:sofiane.elmahroug@gmail.com)**



## **Éléments de contenu**

- 1. Introduction**
- 2. Réseaux cellulaires**
- 3. Réseaux satellitaires**
- 4. Réseaux Wifi**
- 5. Conclusion**



## Equipements ?

- Smart phone
- Personnel Digital Assistant (PDA)
- Ordinateur Portable
- Tablette
- ...





## Appareils sans fil

### **Puissance limitée**

- Batterie, mémoire, stockage non volatil
- Portée d'une transmission
- Type du réseau d'accès

### **Interface Homme Machine simplifiée**

- Taille des écrans
- Complexité d'accès aux fonctionnalités



## Motivations

### Réseaux Radios

- Diversité des services offerts (entreprise / grand public)
- Facilité d'usage pour les utilisateurs nomades
- Accès à des capacités de calcul via des terminaux peu coûteux

### Exemple de services

- Accès Internet Haut Débit
- Accès aux services streaming, et travail collaboratif
- Services de télétravail



## Enjeux économiques

### Vente des terminaux mobiles

- **1,56** milliards de smartphones vendus en 2019 contre 720 millions en 2012
- **130** millions de smartphones vendus chaque mois.
- Arrivée en force des tablettes

### Vente d'applications mobiles

- **76%** des 11-14 ans se connectent chaque jours (2h)
- **178** Milliards d'applications mobiles téléchargées en 2017, contre **205** en 2018, et **258** prévus pour 2022.
- **188,9** Milliards de \$ en 2020.

### Opportunités d'emploi

- Définition et mise en œuvre de stratégies Web/Mobile
- Développeurs Mobiles (Niveau Bac+5)



## Domaines d'utilisation

- **Travail collaboratif** : dans le cadre de réunions, de conférence, ...
- **Réseaux de capteurs** : pour des applications IoT, e-health, e-industry, ...
- **Réseaux domestiques** (Home network) : partage d'applications et communications des équipements mobiles.
- **Applications commerciales** : pour un paiement électronique distant (en taxi) ou pour l'accès mobile à l'Internet ou service de guide en fonction de la position de l'utilisateur,
- **Réseaux en mouvement** : informatique embarquée et véhicules communicants pour avoir des informations sur le trafic disponible en temps réel (Vehicular Ad hoc Network, VANET).



## Définitions

### Réseaux Mobiles

- Fournir un **accès sans fil**, tout en conservant une **même identité** en se déplaçant à travers le réseau.
- Un système est dit **sans fil** s'il propose un service de communication totalement **indépendant des prises murales**.







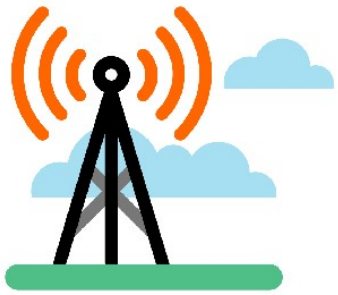
## Supports sans fil

### Infrarouge

- Onde électromagnétique de longueur d'onde  **$0,78\mu\text{m} \sim 1000\mu\text{m}$** .
- Télécommandes,
- Communication à courte distance entre PC et périphériques

### Ondes hertziennes

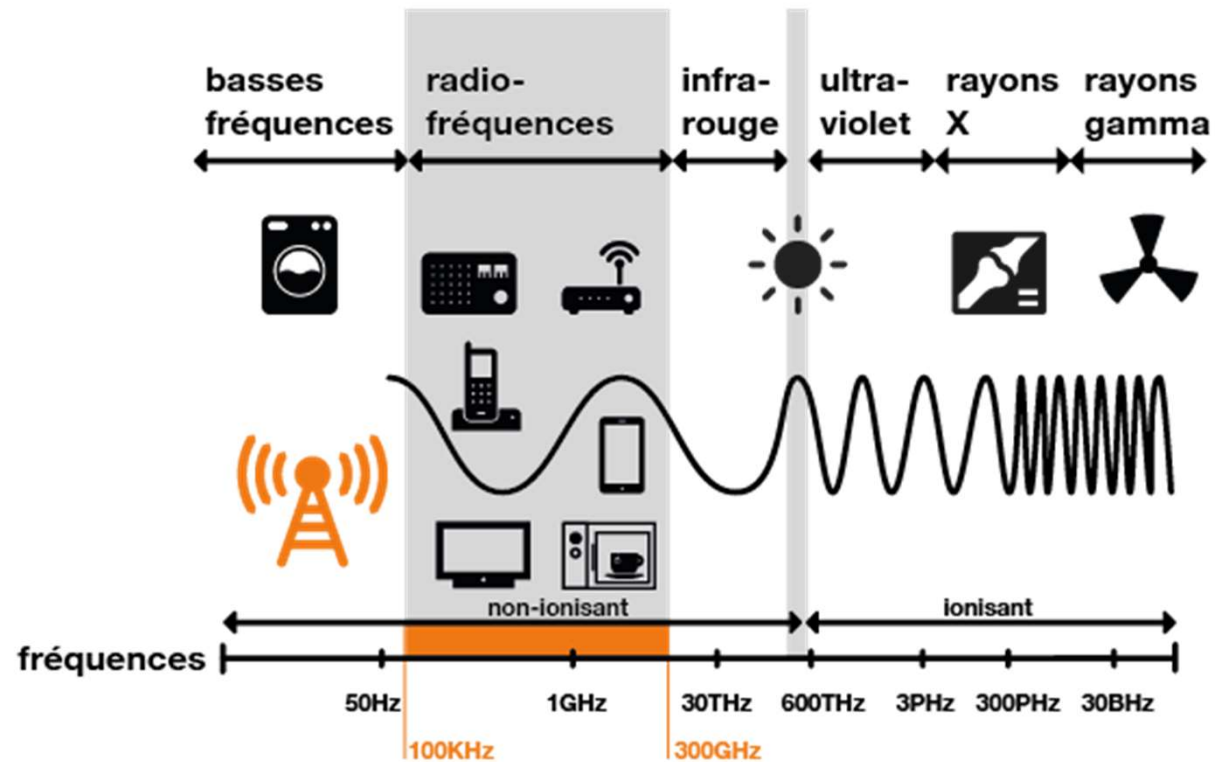
- Onde électromagnétique dont la fréquence est inférieure à  **$3000\text{Ghz}$**



## Spectre de fréquences

### Ondes Radio

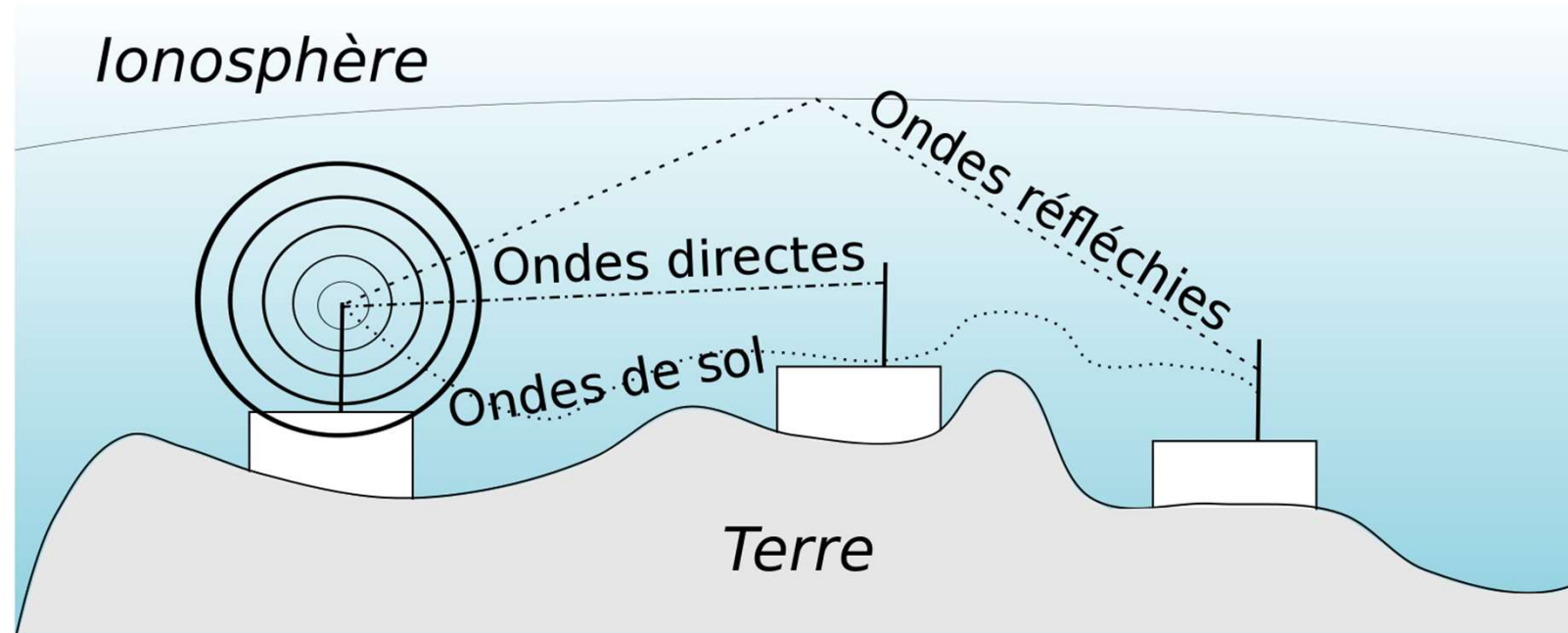
- Fréquences entre **100Khz** et **300Ghz**





## Propagation des ondes radio

**Vitesse de propagation**  
• 300 Km/s





## Classification des ondes radio

Nature du rayonnement	Dénomination	Fréquence	Longueur d'onde	Utilisation
ELF (Extrêmement Basses Fréquences)	ELF	de 1 Hz à 10 kHz	de 300 000 km à 100 km	Courants industriels (réseaux électriques) 50 Hz, 60Hz, 16,6 Hz.
	VLF (Très basses fréquences)	de 10 kHz à 30 kHz	de 100 km à 10 km	Radio-communications (sous-marins), Moniteurs vidéo cathodiques d'ordinateurs.
	LF (Basses fréquences)	de 30 kHz à 500 kHz	de 10 km à 600 m	Radio-diffusion, Radio-télégraphie, Radio-balises
RF (Radiofréquences)	PO (Petites ondes)	de 500 kHz à 1500 kHz	600 m à 200 m	Radio-diffusion.
	OM (Ondes moyennes)	de 1,5 MHz à 6 MHz	de 200 m à 50 m	Radio-diffusion, radio-phares (radio-balises).
	OC (Ondes courtes)	de 6 MHz à 30 MHz	de 50 m à 10 m	Radio-diffusion, radio-télégraphie à grande distance, Modèles réduits téléguidés, C.B., Appareils de diathermie pour kinésithérapie.
	VHF (Très hautes fréquence, ondes très courtes)	de 30 MHz à 300 MHz	de 10 m à 1 m	Télévision, Radio en fréquences modulée.
HF (Hyperfréquences)	UHF et SHF (micro-ondes)	de 300 MHz à 300 GHz	de 1 m à 1 mm	Radar, Téléphones mobiles, Téléphones DECT, Connexions de périphériques de P.C., Fours à micro-ondes, Faisceaux hertziens, communications par satellites.
Autres	IR (Rayonnement Infra-rouge)	de 300 GHz à 3,75.10 <sup>14</sup> Hz	de 1 mm à 800 nm	Chauffage, systèmes de surveillance et de détection.
	Lumière visible	de 3,75.10 <sup>14</sup> Hz à 7,5.10 <sup>14</sup> Hz	de 800 nm à 400 nm	Eclairage, Laser, enseignes lumineuses.



## Histoire des transmissions sans fil

### Electromagnétisme

- **1843** : **Faraday** effectue des recherches sur l'induction électromagnétique et la conduction de l'électricité dans l'air.
- **1864** : **Maxwell** reprend les travaux de **Faraday** avec la théorie dynamique des champs électromagnétiques. Il conclut à l'existence d'un rapport entre l'électricité, magnétisme, et lumière.
- **1875** : **Edison** créa des étincelles électromagnétique à partir d'un aimant vibrant.



## Histoire des transmissions sans fil (2)

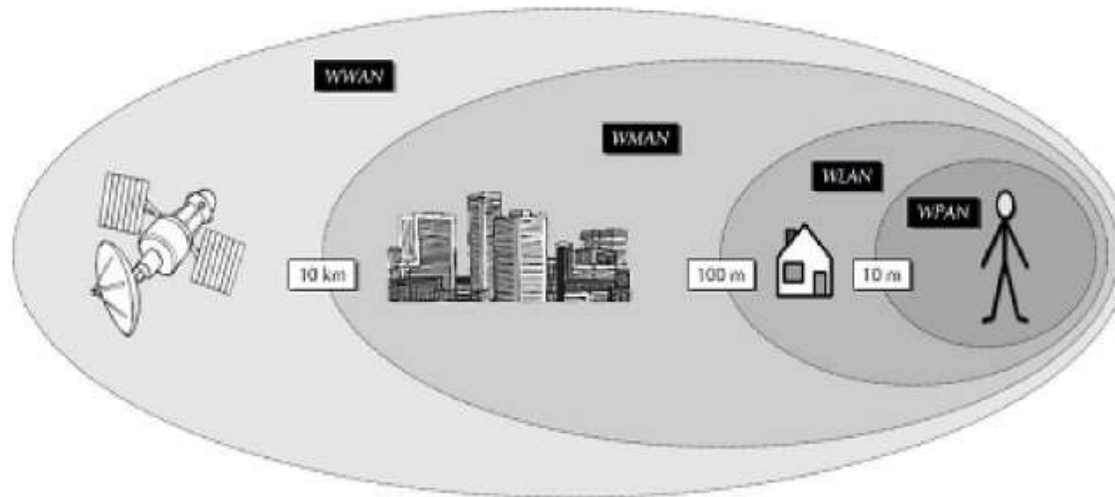
### Radioélectricité et ondes radio

- **1888** : **Heinrich Hertz** produit des ondes radio pour la 1ère fois.
- **1893** : **Tesla** décrit les principes de l'émission radio. Il fait la première expérience publique de communication radio à Saint-Louis.
- **1895~1903** : **Guglielmo Marconi**, inventeur italien, prouve la faisabilité de la communication radio en envoyant et recevant un signal radio en Italie puis, entre la France et l'Angleterre, et enfin par dessus l'océan atlantique.
- **1903** : **Tesla** accredité de la découverte des ondes radio auprès de la cour suprême au détriment de **Marconi**.



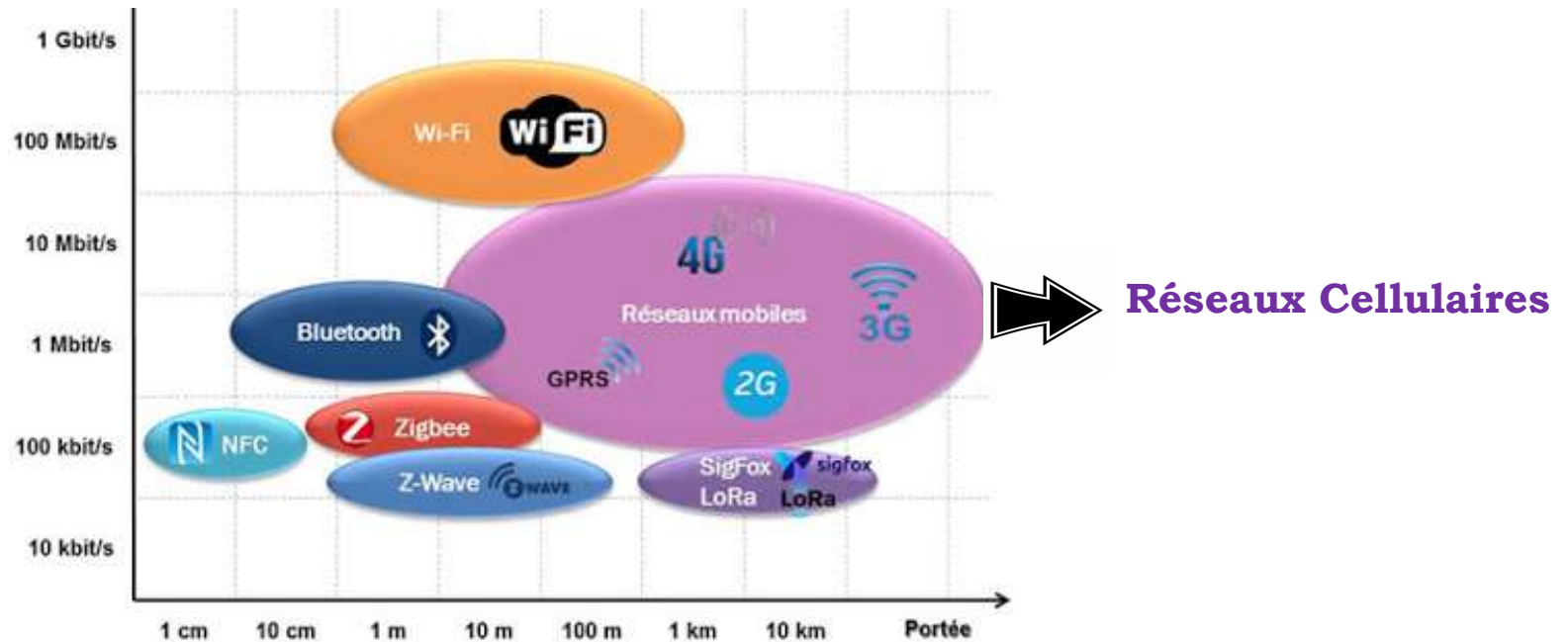
## Classification des réseaux sans fil

- **WPAN**: Wireless Personal Area Network
- **WLAN**: Wireless Local Area Network
- **WMAN**: Wireless Metropolitan Area Network
- **WWAN**: Wireless Wide Area Network

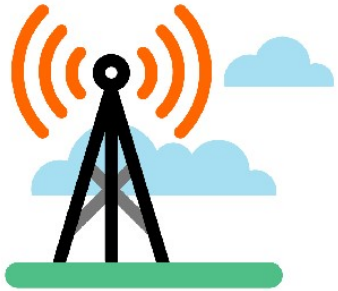




## Classification des réseaux sans fil (2)







## Réseaux cellulaires

### Développement des réseaux sans fil

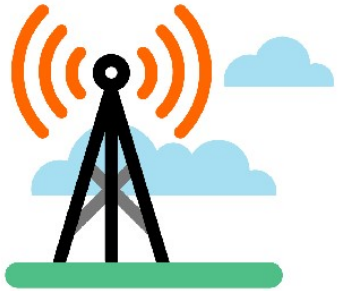
- **1986** : la première génération de réseau téléphonique voit le jour. Il est propulsé en France par Radiocom 2000 (distribué par France Télécom). Le réseau fonctionnait avec la bande de fréquence 400 Mhz..
- **1912** : Attribution des fréquences radio et des licences aux opérateurs téléphoniques.
- **1940** : L'**armée Américaine** utilise pour la première fois des signaux radio pour la transmission de données.
- **1971** : un groupe de chercheurs crée le premier réseau de communication radio basé sur la commutation de paquets appelé **ALLOHAnet**, le premier réseau sans fil constitué de **07** ordinateurs



## Réseaux cellulaires (2)

### 1G (Années 80: Fonctionnement analogique)

- **1976** : **AMPS** (Advanced Mobile Phone System), apparu aux USA.
- **TACS** : (Total Access Communication System), Version Européenne du modèle **AMPS** (900Mhz).
- **1983** : **ETACS** (Extended Total Access System), version améliorée du TACS et donc du AMPS utilisant un nombre plus important de canaux.



## Réseaux cellulaires (3)

### 2G (Années 90 : Technologie Voix numérique)

- **GSM** (Global System Mobile), utilisant les bandes de fréquences 900Mhz et 1800Mhz.
- **CDMA** (Code Division Multiple Access), utilisant une technique d'étalement de spectre permettant de diffuser un signal radio sur une grande gamme de fréquences.
- **SMS & MMS**, cette norme permet d'envoyer des messages texte et multimédia, avec un débit maximal de 9,6 Kbits/s.
- **GPRS** (General Packet Radio System) baptisé **2,5G** permettant d'atteindre des débits théorique de **40Kbits/s** et **2,75G** permettant des débits théoriques de **384kbits/s**.



## Réseaux cellulaires (4)

### 3G (Années 2000 : Technologie numérique voix & données)

- **Objectif** : Haut débit de transmission de données.
- Une compatibilité mondiale pour l'accès au réseau Internet.
- **UMTS** (Universal Mobile Telecommunication System) cette norme permet d'envoyer des messages texte et multimédia, avec un débit maximal de 9,6 Kbits/s.
- **GPRS** (General Packet Radio System) baptisé **2,5G** permettant d'atteindre des débits théorique de **40Kbits/s** et **2,75G** permettant des débits théoriques de **384kbits/s**.



## Réseaux cellulaires (5)

### 4G (Années 2010 : Haut débit)

- **LTE** (Long Term Evolution)
- Débit allant à 150Mbits/s
- **4G+** débits allant à **1Gbits/s** à l'arrêt et **500Mbits/s** en mouvement.

### 5G (Années 2020 : Ultra Haut débit)

- Débit maximal de **1Gbits/s** en download et **500Mbits/s** en upload.
- Utilisation d'ondes millimétriques à une très haute fréquence (**6GHz et 300GHz**).



## Génération des réseaux cellulaires





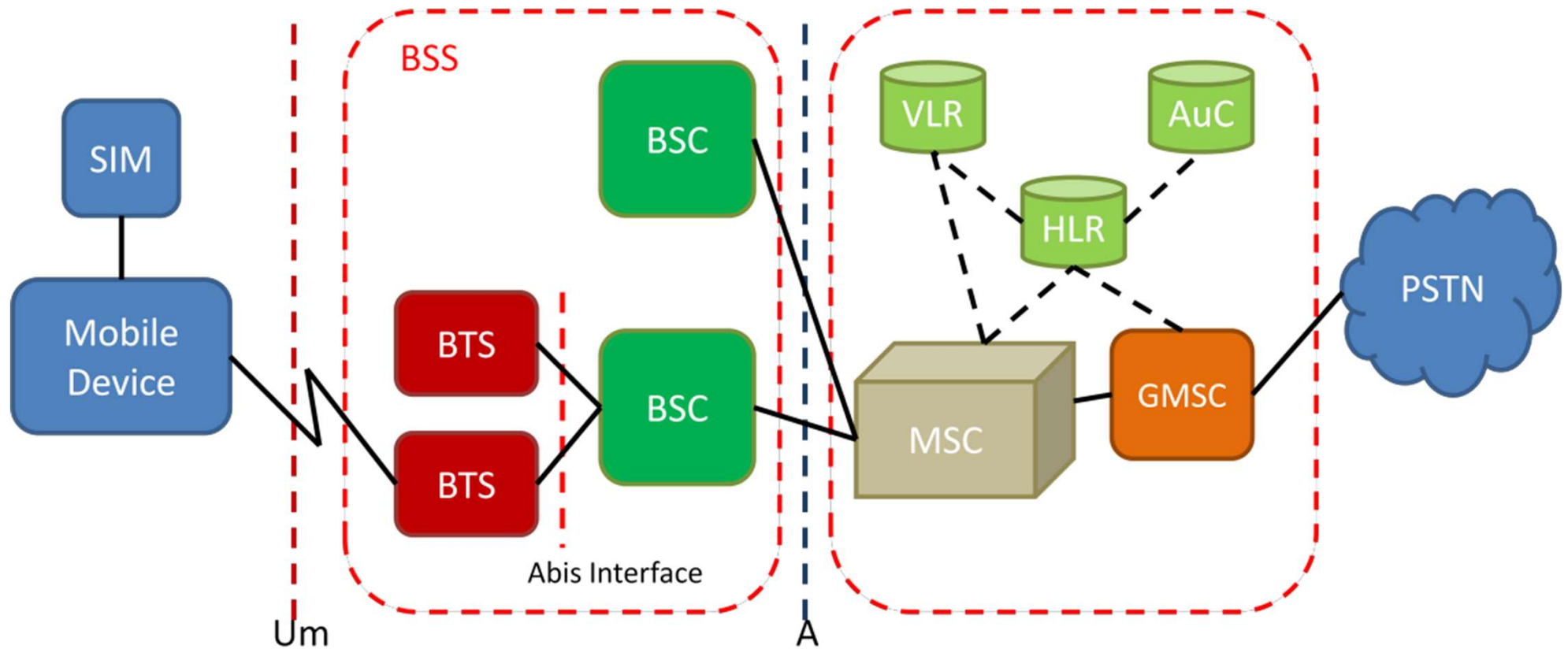
## Licences pour les opérateurs

### Partage de spectre

- Le spectre de fréquence est une ressource rare.
- 3 opérateurs (Tunisie Télécom, Orange Tunisie, Ooredoo Tunisie).
- Taux de pénétration de **126%** (Mars 2018)
- Abonnements actifs : **14 554 657**
- Parts de marché :
  - TT ~ 30%
  - Ooredoo ~ 40%
  - Orange ~ 37%



## Principes de base des réseaux cellulaires

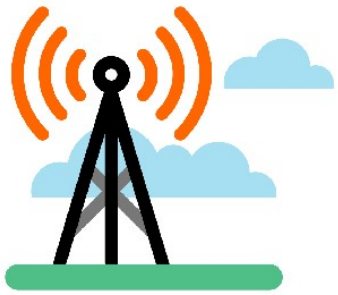






## Principes de base des réseaux cellulaires (2)

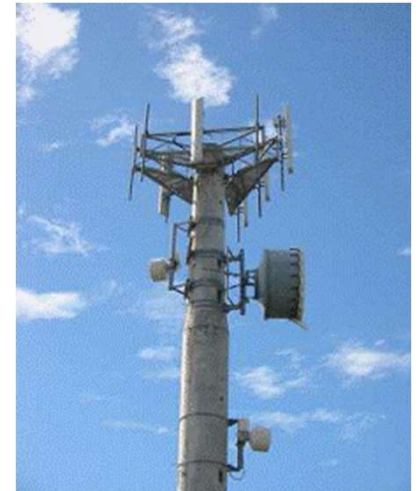
- **SIM**: Subscriber Identity Module
- **BTS**: Base Transceiver Station
- **BSC**: Base Station Controller
- **BSS**: Base Station Subsystem
- **MSC**: Mobile Switching Centre
- **HLR**: Home Location Register
- **VLR**: Visitors Location Register
- **AuC**: Authentication Centre
- **GMSC**: Gateway MSC
- **PSTN**: Public Switched Telephone Network



## Principes de base des réseaux cellulaires (2)

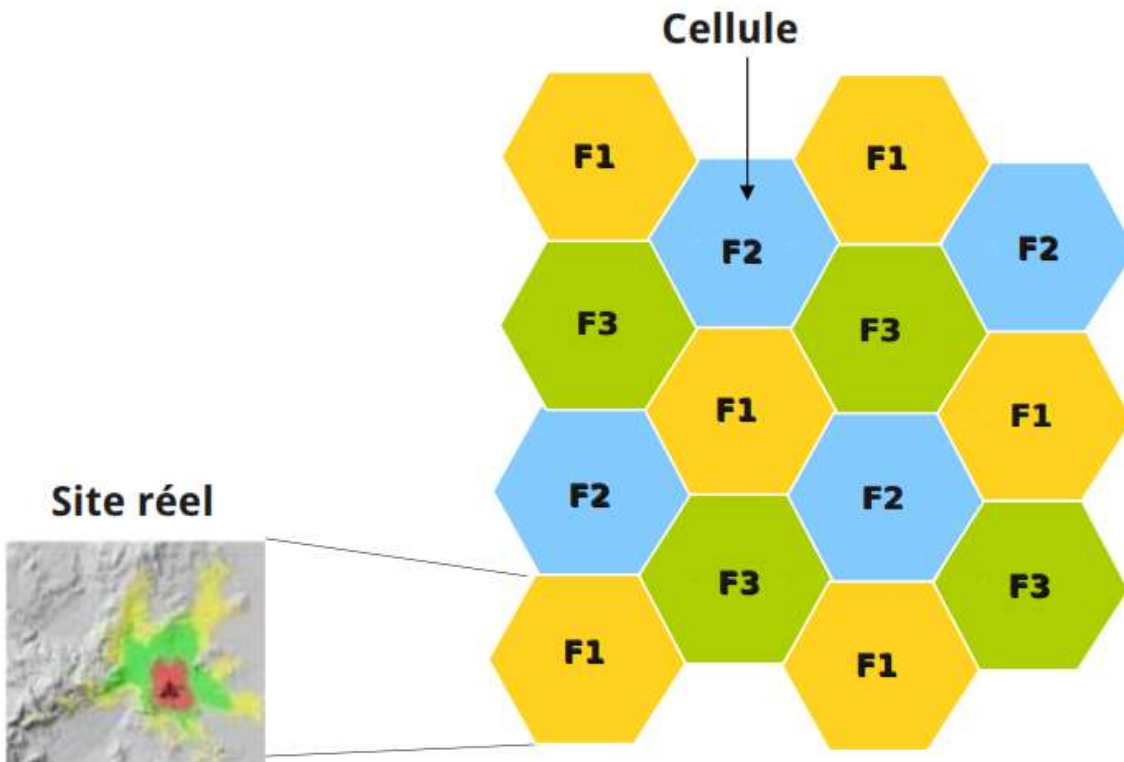
### BTS : Base Transceiver Station

- Un système de radiotéléphonie qui utilise une **liaison radioélectrique** entre le terminal mobile et le réseau mobile.
- Chaque **BTS** réalise la couverture radio d'un certain territoire appelé **cellule** dont le rayon varie entre quelques centaines de mètres et quelques kilomètres.
- La **BTS** est un ensemble d'émetteurs-récepteurs appelés **TRX**, elle a la charge de la **transmission radio**.
- Elle gère plus généralement toute la **couche physique**.
- Elle réalise aussi l'ensemble des **mesures radio** nécessaire pour vérifier qu'une communication en cours se déroule correctement.





## Principes de base des réseaux cellulaires (3)

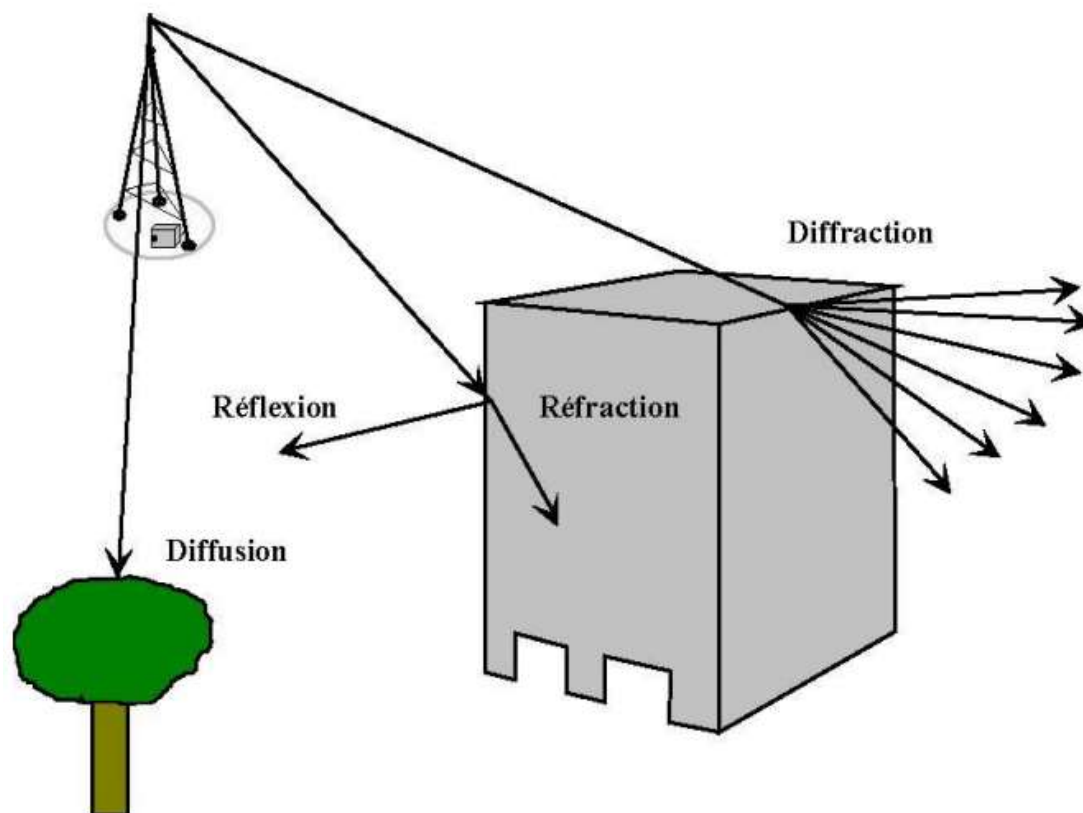


### Cellule

- Chaque cellule a sa fréquence de communication
- Possède **6 voisins**
- pour éviter de gaspiller les fréquences et d'interférer entre les cellules : technique **SDMA**
- les cellules adjacentes ne doivent pas avoir la même fréquence de communication



## Environnement Radio Mobile





## Environnement Radio Mobile (2)

### Dégradation de l'onde

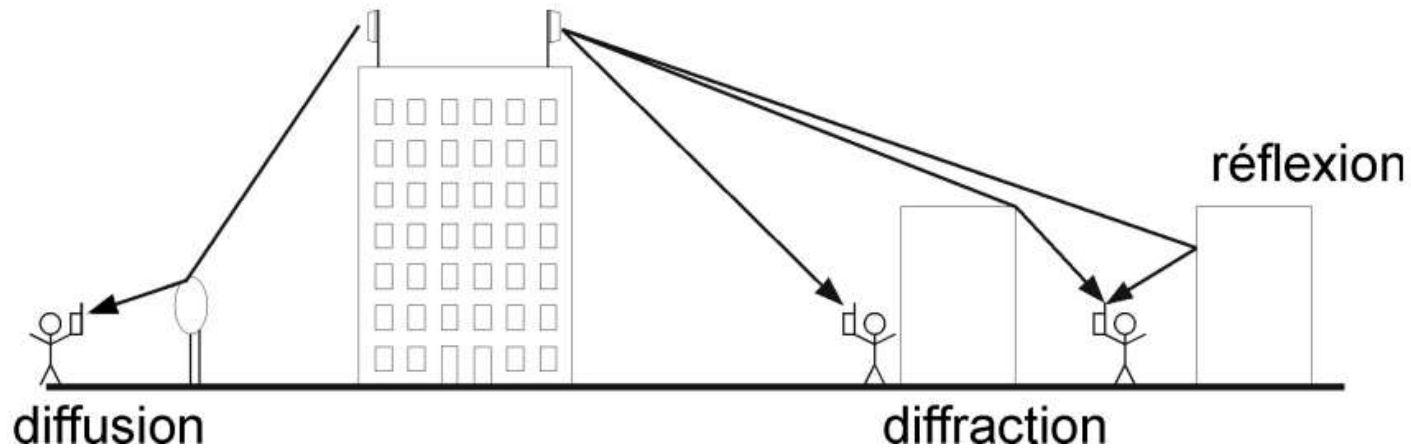
- Atténuation due à la distance parcourue (**pathloss**)
- Effets de masques (**shadowing effects**)
- Evanouissements (**fadings**) par propagation multitrajet.
- Brouillages causés par d'autres émissions :
  - Interférences (co-canal ou canal adjacent)
  - Bruit ambiant.

### Caractéristiques de la propagation

- Morphologie du terrain
- Densité de végétation
- Hauteur, combinaison, nature et densité des bâtiments
- Conditions météo,...



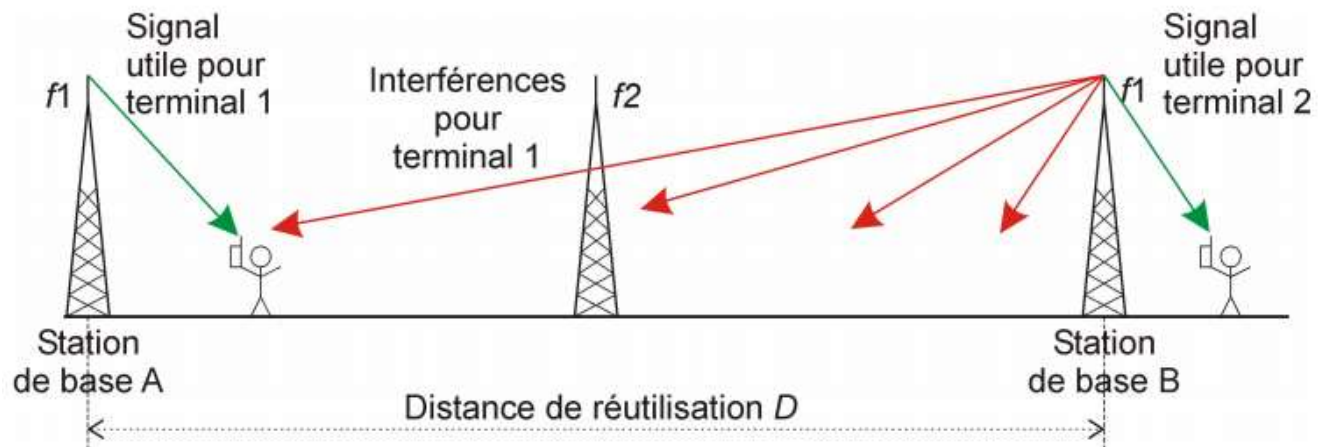
## Multi-trajets



- Il y a rarement visibilité directe entre l'émetteur et le récepteur
- un terminal reçoit en général plusieurs échos du même signal transmis



## Interférences Co-canal

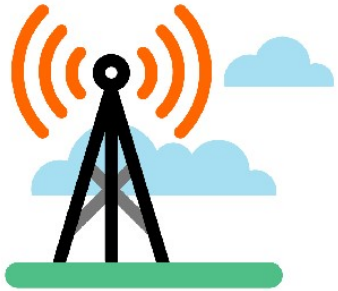




## Problématique de la mobilité

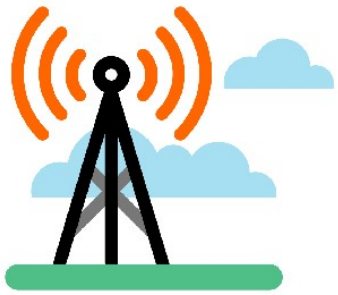
- **Localisation des utilisateurs** : pour établir une communication il faut savoir dans quelle cellule l'abonné se trouve.
- **Transfert inter-cellulaire (Handover)** : Il doit y avoir continuité de communication lorsque l'abonné passe d'une cellule à l'autre.
- **Roaming** : Si la mobilité s'étend à plusieurs pays, des accords de roaming entre opérateurs permettent le traitement et l'aboutissement des communications.
- **Sécurité** : Authentification, cryptage, identité temporaire, permettent d'éviter des écoutes frauduleuses.



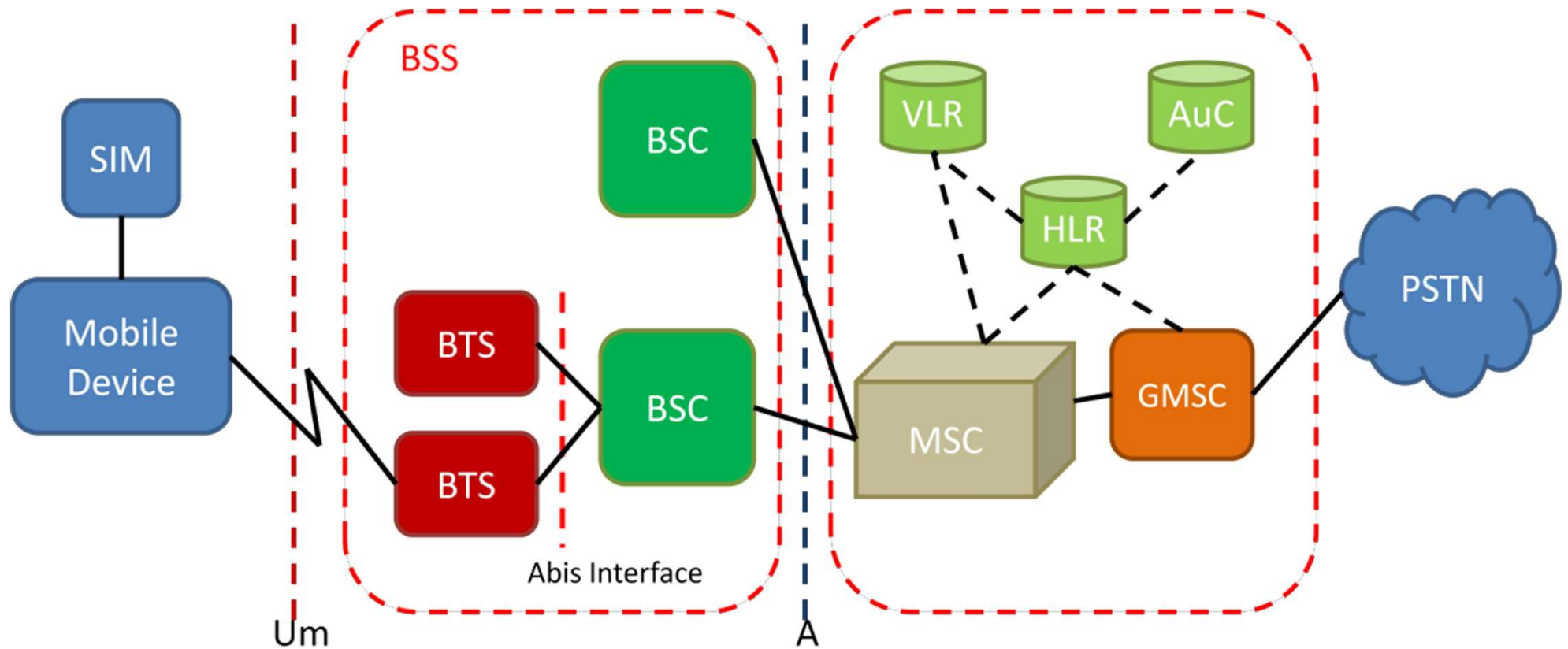


## Services GSM

- **La voix**
- **Les données**
- **le WAP** (Wireless Application Protocol), le Fax ou bien les fonctions d'un modem filaire classique
- **Les messages**
  - Les messages écrits courts (SMS)
  - Le MMS (Multimedia Messaging Service)
- **Le Cell Broadcast** (diffusion dans les cellules)
  - Permet d'envoyer le même SMS à tous les abonnés à l'intérieur d'une zone géographique
- **Les services supplémentaires**
  - renvois d'appels, présentation du numéro, etc.
- **Les services à valeur ajoutée**
  - Les services de localisation (Location Based Services), d'information à la demande (météo, horoscope), de banque (consultation de compte, recharges de compte prépayées)

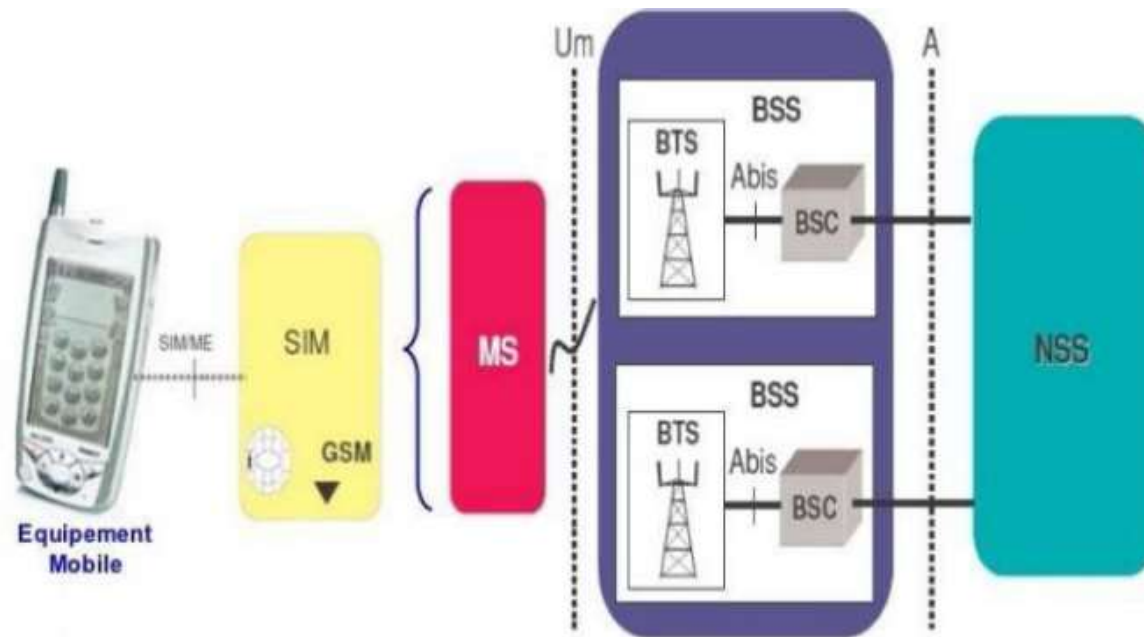


## Architecture du réseau GSM





## Architecture du réseau d'accès BSS



Le MS assure les communications sans fil entre le mobile et le réseau d'accès BSS

Le BSS assure les communications sans fil entre le mobile et le réseau de cœur NSS



## Station mobile (MS)

### La Station Mobile

- Mobile Equipment (le terminal GSM)
- Subscriber Identity Module (SIM).



### Mobile Equipment

- Le Mobile Equipment est identifié (exclusivement) à l'intérieur de n'importe quel réseau GSM par l'International Mobile Equipment Identity (**IMEI**).
- Les terminaux GSM sont divisés en cinq classes en fonction de leur puissance maximale de transmission sur le canal radio.



## Station mobile (2)



### Carte SIM

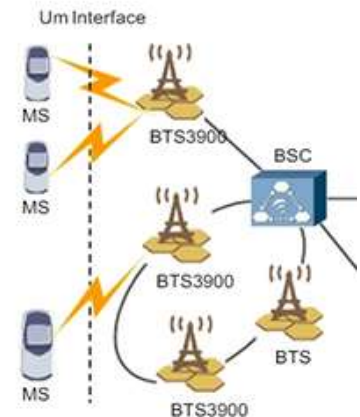
- Contient l'International Mobile Subscriber Identity (**IMSI**), qui sert à identifier l'abonné dans n'importe quel système GSM, et les procédures de cryptographie qui sauvegardent le secret de l'information de l'utilisateur ainsi que d'autres données telles que :
  - la mémoire alphanumérique du téléphone
  - la mémoire relative aux messages de texte (SMS)
  - Les informations sur le réseau.
- L'**IMSI** présente la structure suivante: MCC / MNC / MSIN où:
  - **MCC** = Mobile Country Code (2 ou 3 chiffres, pour la Tunisie 216)
  - **MNC** = Mobile Network Code (2 chiffres)
  - **MSIN** = Mobile Station Identification Number (maximum 10 chiffres)



## BSS (Base Station Subsystem)

**BSS = BTS + BSC**

- Sa fonction principale est la gestion de l'**attribution des ressources radio** indépendamment des abonnés, de leur identité ou de leur communication.
- **BTS** (Base Transmission Station)
  - L'antenne
  - Gère la liaison radio antenne – mobile
  - Gère la couche physique et liaison de donnée
- **BSC** (Base Station Controller) Organe intelligent du BSS
  - Gère plusieurs BTS
  - Allocation des canaux de communication
  - Surveillance de la puissance des MS et des BTS
  - Gestion itinérance et transfert communication
  - Interagit avec le réseau de cœur NSS

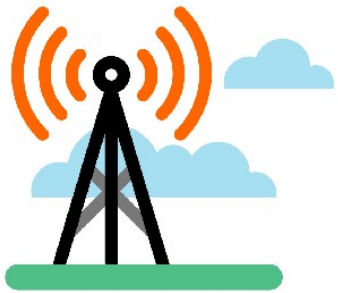




## BSS (2)

### Gestion du transfert inter-cellulaire (handover)

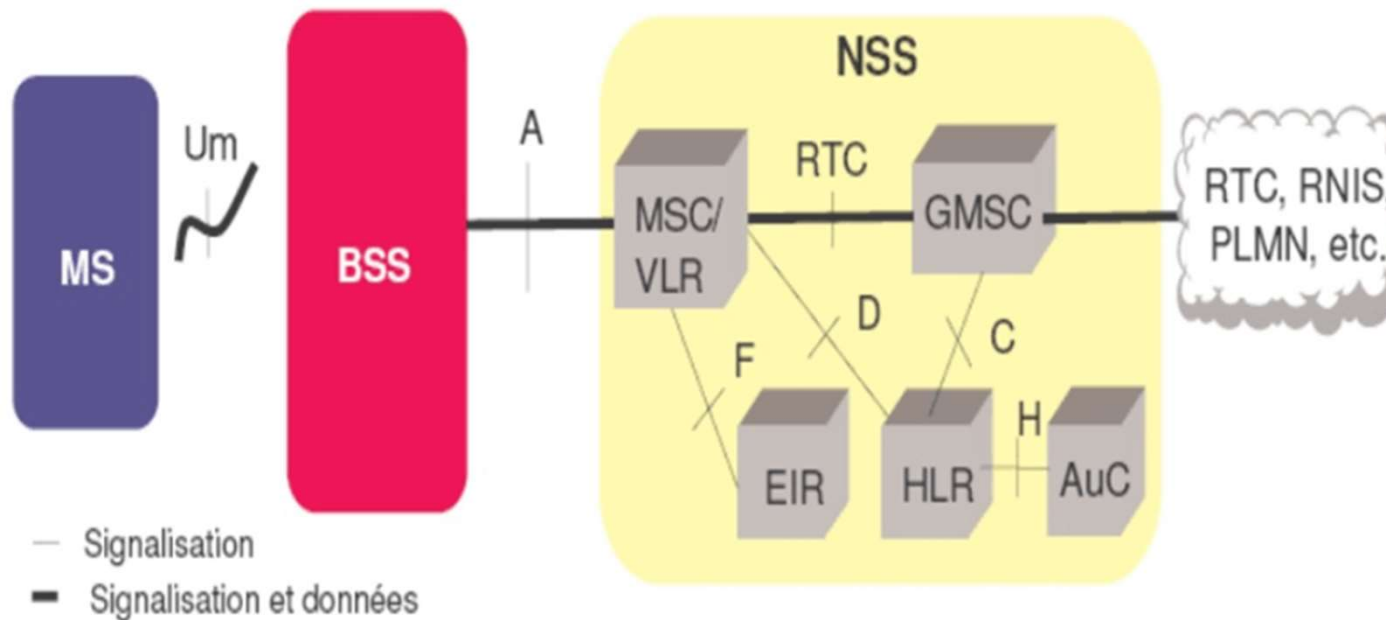
- **Définition** : ensemble d'opérations permettant à une station de **changer de cellule sans interruption de service**.
- **Principe** : lorsque le **signal** entre une **MS** et la **BTS** s'**affaiblit**, la **MS** cherche une autre **BTS** dans une autre **cellule capable d'assurer le service**.
- **Protocole** : Lorsque la MS quitte la cellule pour une autre, c'est la qualité de transmission qui détermine la nécessité du handover
  - Taux d'erreurs
  - Intensité du signal
  - Niveau d'interférences
  - Délai de propagation



## Architecture du réseau Cœur NSS

### NSS : Network Switching Subsystem

Il comprend l'ensemble des fonctions nécessaires à l'**établissement des appels** et à la **gestion de la mobilité** ( en charge de la **gestion des services à commutation** de circuits : voix, fax, sms, données, ...)







## MSC (Mobile Switching Center)

- Centre de commutation radio mobile : Commutateur en charge des services en mode circuit des stations mobiles enregistrées dans la **zone géographique** qu'il gère
- Prend en charge **plusieurs BSS**
- Fonctionnalités :
  - Gestion des appels
  - Gestion du handover
  - Interconnexion avec le réseau fixe (RTC, RNIS, Internet) via le **GMSC**
  - Gestion des terminaux visiteurs
- **GMSC** (Gateway MSC) : Effectue le routage des appels du **MSC** vers le réseau fixe et inversement



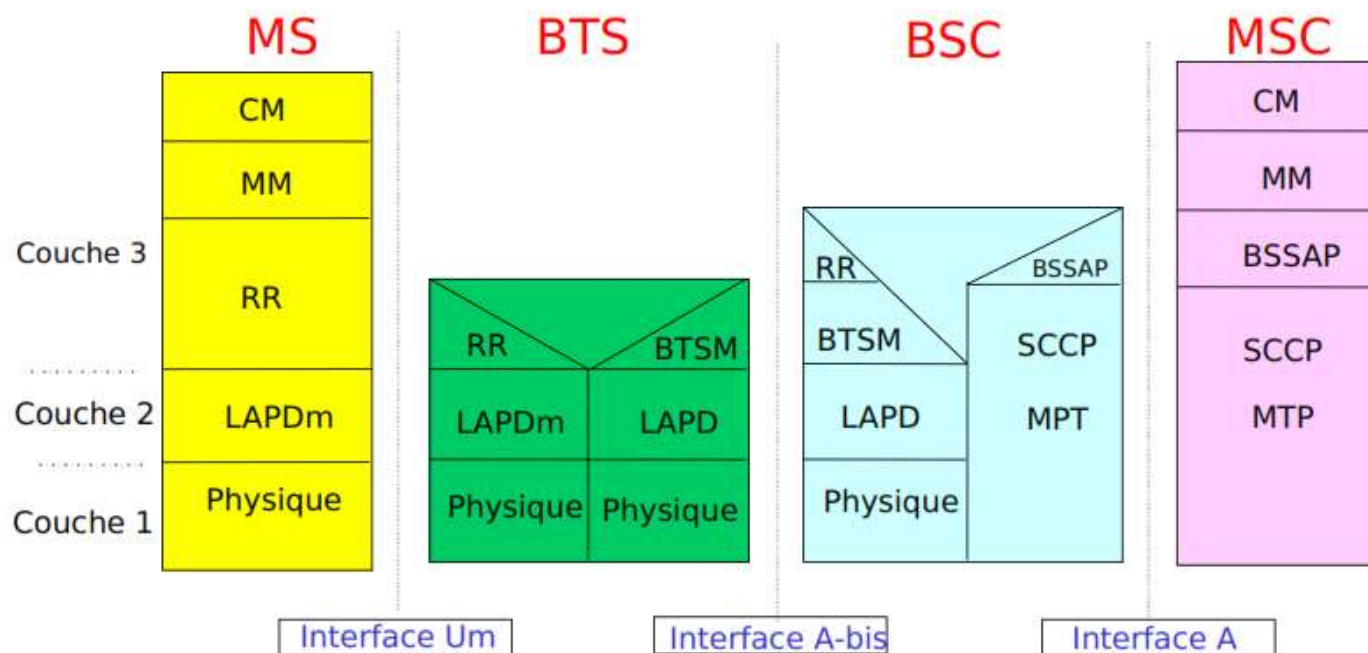


## Bases de données

- **HLR** (Home Location Register) :
  - Registre des informations des mobiles locaux (IMSI, MSISDN)
  - Adresse du VLR où le mobile est localisé
- **VLR** (Visitor Location Register)
  - Registre des terminaux visiteurs
  - Informations précises sur la position actuelle du visiteur mobile et de son déplacement dans une zone de localisation
  - Zone de localisation (location area) = ensemble de cellules gérées par un même MSC/VLR
- **EIR** (Equipment Identity Register)
  - Registre des identifiants des équipements mobiles (conditions d'abonnement)
  - Informations grossières sur la localisation de l'abonné
- **AuC** (Authentication Center)
  - Registre contenant les informations confidentielles destinées à l'authentification de l'abonné



## Architecture en couches





## Protocoles

- **CM** (Connection Managment) : Établissement et relâchement des appels
- **MM** (Mobility Managment) : 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
- **RR** (Radio Ressource Managment) : Sélection de cellule (choix de la porteuse), ouverture d'une connexion, contrôle en cours de communication, handover, terminaison,



## Protocoles (2)

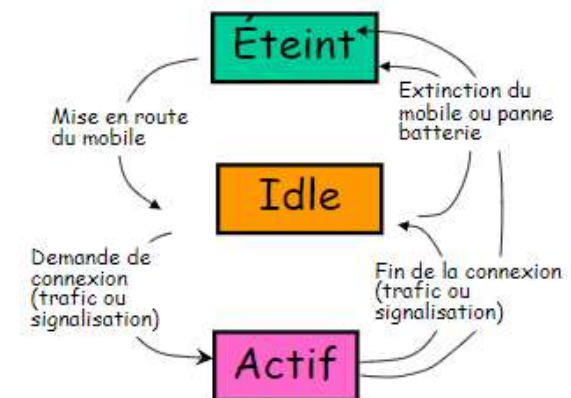
- **LAPD** : Link Access Protocol(Authentication Center)
- **MTP** : Message Transfert Part.
- **SCCP** : Signaling Connection Part
- **BSSAP** : BSS Application Part



## Fonction du réseau Cellulaire

### 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





## Fonction du réseau Cellulaire (2)

### Mise à jour de la localisation (MM)

- Gestion de l'itinérance : deux mécanismes de base
  - Localisation (**précise**) : Savoir où se trouve le mobile à tout moment (coût de localisation important mais pas de recherche rapide).
  - Recherche (**paging**) : Émettre des messages d'avis de recherche dans les cellules visitées dernièrement ,coût de recherche élevé (signalisation élevée) mais coût de localisation faible.
- Zones de localisation
  - Ensemble de cellules, critères : nombre moyen d'appels, direction privilégiée des HO, autoroutes,...
  - Plusieurs zones par VLR/MSC

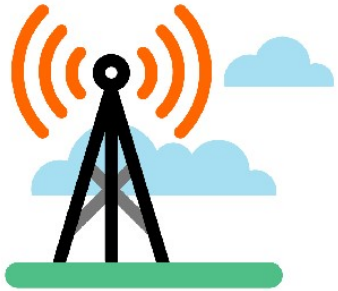


## Fonction du réseau Cellulaire (2)

### Mise à jour de la localisation (MM)

- Gestion de l'itinérance : deux mécanismes de base
  - Localisation (**précise**) : Savoir où se trouve le mobile à tout moment (coût de localisation important mais pas de recherche rapide).
  - Recherche (**paging**) : Émettre des messages d'avis de recherche dans les cellules visitées dernièrement ,coût de recherche élevé (signalisation élevée) mais coût de localisation faible.
- Zones de localisation
  - Ensemble de cellules, critères : nombre moyen d'appels, direction privilégiée des HO, autoroutes,...
  - Plusieurs zones par VLR/MSC





## Fonction du réseau Cellulaire (3)

### Mise à jour de la localisation (MM)

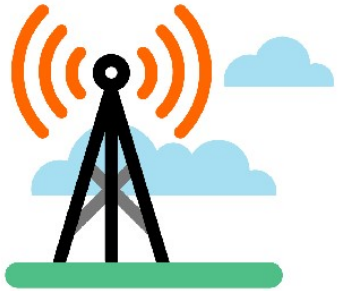
- Procédure de mise à jour de localisation (Procédure qui met à jour les informations de localisation du mobile dans le **VLR** et le **HLR**):
  1. Le mobile sait qu'il change de zone de localisation grâce au canal BCCH (Broadcast Common Channel)
  2. Il prévient le nouveau VLR (donne son **TMSI**)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



## Fonction du réseau Cellulaire (4)

### Gestion des connexions (CM)

- Établissement et relâchement des connexions
- Basé sur la signalisation SS7
- Appel issu du mobile
  - Allumé
  - Parcourt 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)



## Fonction du réseau Cellulaire (5)

### Gestion des connexions (CM)

- Appel vers un mobile
- Appel en utilisant le MSISDN
- Appel acheminé jusqu'au GMSC le + proche
- Le HLR du mobile est interrogé pour
  - trouver le VLR courant
  - vérifier les caractéristiques de l'abonnement
  - traduction du MSISDN en IMSI
- Le VLR diffuse le message de paging (PCH) dans la zone de localisation
- Réponse du mobile (demande d'ouverture de canal (via RACH, réponse paging)
- Établissement comme précédemment (entre GMSC et le mobile via VLR-MSC)



## Connexion au réseau

- Les **BTS** ont pour fonction de détecter la présence d'un téléphone portable ; ils émettent périodiquement des signaux qui sont reçus par le **MS**.
- **MS** sélectionne le **BTS** qui est le plus adéquat sur des critères énergétiques (niveau de réception) ou de disponibilité (la **BTS** la moins chargée).
- **MS** envoie au **BTS** choisi une requête de connexion composée de l'identifiant de l'abonné (qui est dans la carte **SIM**)
- **BTS** envoie sa réponse:
  - Si elle peut accepter la connexion, elle envoie un acquittement ACK.
  - Si elle ne peut accepter la connexion (par exemple si elle n'a pas de canaux disponibles) elle envoie un message ALERT (le **MS** doit alors choisir une autre **BTS**).



## Connexion au réseau (2)

### Identification de MS

- Une BTS peut recevoir simultanément des requêtes de connexion provenant de deux MS différents ; dans ce cas ces requêtes se superposent et donnent lieu à un signal incompréhensible → collision
- La collision ne peut être détectée par le MS (qui ne l'entend pas) → le protocole Aloha
- Si au bout d'un certain délai (timeout), le message ACK n'est pas reçu par le MS, on considère que la requête n'est pas arrivée et on émet une nouvelle requête après un délai aléatoire compris entre 0 et  $t_{\max}$ .
- Le choix de timeout et de  $t_{\max}$  influe sur le débit effectif du réseau.



## Connexion au réseau (3)

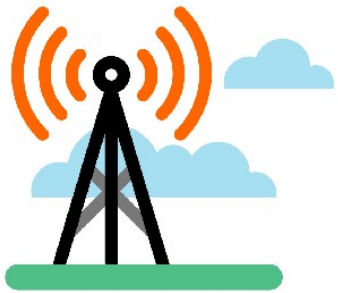
- Si connexion acceptée, la **BTS** transmet la requête au **BSC** qui elle même la transmet au **MSC** avec le numéro de la **BTS** ce qui permet de mettre à jour la **VLR** (enregistrement de la localisation).
- **VLR** transmet également les informations de localisation au **HLR** pour mise à jour. Tout ce processus correspond à l'identification de l'abonné.



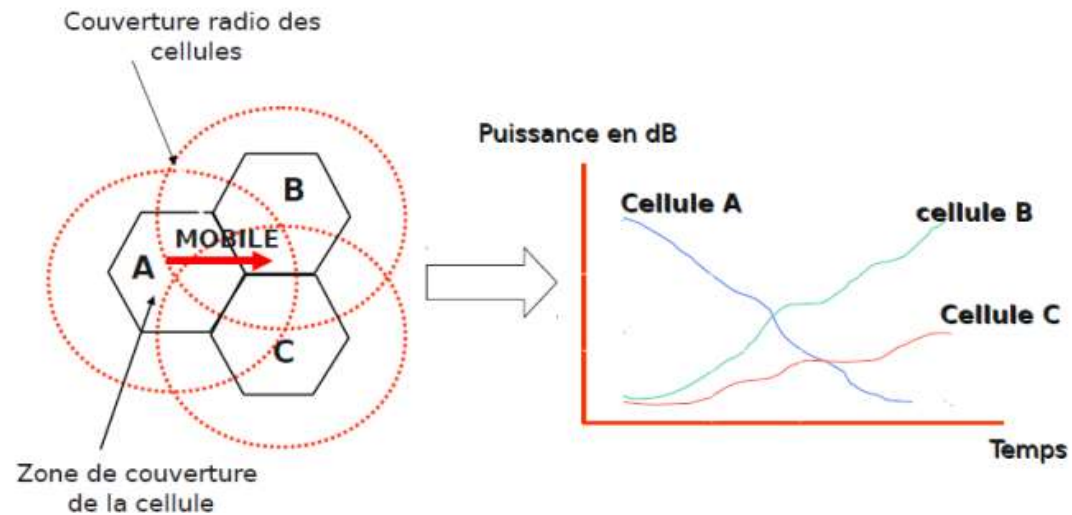
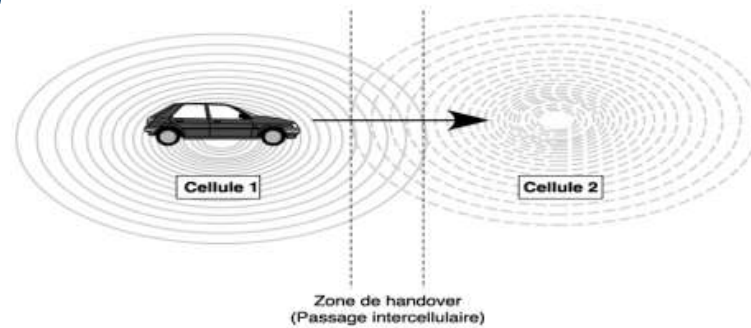
## Connexion au réseau (4)

### Authentification de MS

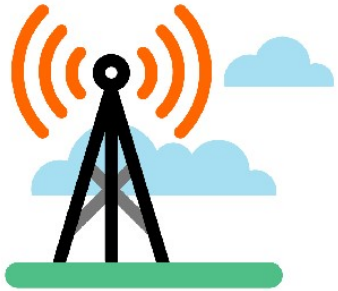
- La carte **SIM** comporte l'identifiant ID de l'abonné et une clé secrète composée en fait de deux clés C1 et C2.
- **AUC** comporte les mêmes informations : connaissant ID, il trouve les clés C1 et C2 dans ses tables.
- **AUC** construit un message à partir d'un nombre N généré aléatoirement et qu'il encode avec la clé C1 ; il envoie ce message (via la chaîne AUC-HLR-MSCBSC-BTS-MS) au **MS**.
- **MS**, à l'aide de la clé C1, décode le message et récupère donc le nombre N qu'il encode avec la clé C2 ; ce nouveau message est envoyé à **AUC** (via la chaîne MS-BTS-BSC-MSC-HLR-AUC) ;
- **AUC** peut le décoder avec la clé C2 et récupère donc N ; il peut vérifier que c'est bien le nombre initial.
- Si c'est le cas, l'authentification a réussi. Il faut alors avertir le **MS** qu'il a été authentifié.



## Gestion du transfert intercellulaire (Handover)







## Gestion du transfert intercellulaire (2)

### Phase de mesures

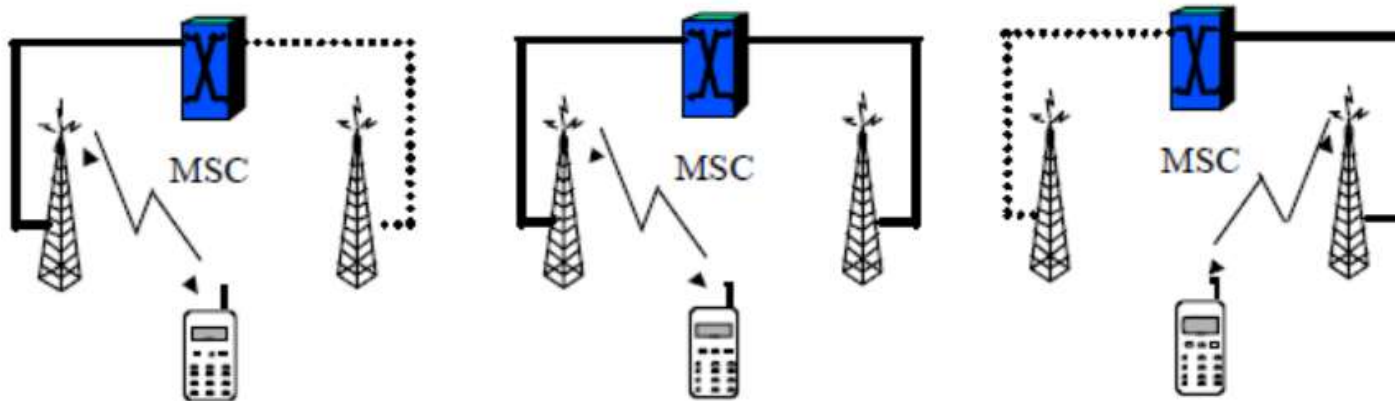
- MS et BTS effectuent des mesures
- Paramètres recueillis :
  - La puissance du signal reçu (qualité du lien)
    - MS (canal descendant), BTS (canal montant)
  - Le taux d'erreur binaire (BER)
  - Distance entre le mobile et la station de base (grâce à la valeur de l'avance en temps)
- Paramètres diffusés 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



## Gestion du transfert intercellulaire (3)

### Phase d'exécution

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

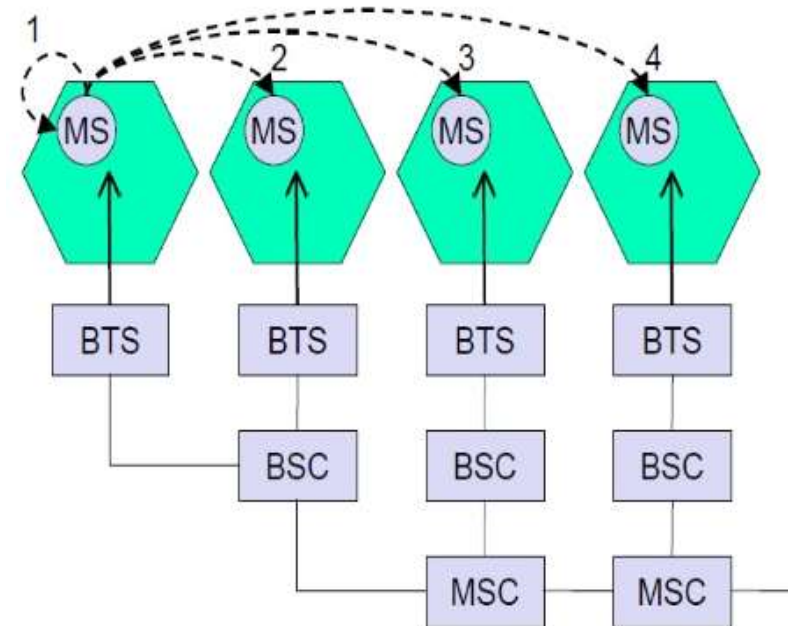




## Gestion du transfert intercellulaire (4)

### Types du handover

1. Intra-cellule
2. Inter-cellule, intra-BSC
3. Inter-BSC, intra-MSC
4. Inter-MSC





## Gestion du transfert intercellulaire (5)

- 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)