# Appunti di Reti di Telecomunicazioni

# Seminario sulla rete GSM

# INTRODUZIONE ALLA COMUNICAZIONE MOBILE

Da diversi anni si sta assistendo alla grande diffusione della cosiddetta **mobile communication**, ovvero di tutti quei servizi che rendono possibile il mantenimento di una connessione, tra due utenti in una rete di telecomunicazione, anche in una situazione in cui uno o entrambi gli utenti sono in movimento. In ambito militare e nei servizi pubblici, la comunicazione tra mezzi in movimento è sempre stata una esigenza fondamentale: basti pensare che nel 1921 vennero condotti degli esperimenti dal Dipartimento di Polizia di Detroit (USA), con sistemi che consentivano la comunicazione unidirezionale della centrale con i singoli autoveicoli.

Una importante svolta (forse la più importante) per le comunicazioni mobili avvenne con l'invenzione delle tecniche di **modulazione di frequenza**[1] (**FM** - *Frequency Modulation*), avvenuta nel 1935 da parte *E.H. Armstrong*. Durante la 2° guerra mondiale, si ebbe un notevole sviluppo dei sistemi FM, ma fu subito evidente una cosa: dato che ciascun servizio richiede una propria banda, ci si rese conto che non vi sarebbe stata, in futuro, la disponibilità di un numero tale di canali radio da poter soddisfare la richiesta dei vari settori (militare, polizia, vigili del fuoco, servizi di trasporto pubblici e privati, etc).

Alla fine degli anni '40 vennero introdotti i primi sistemi di **telefonia mobile**, ovviamente analogici: questi sistemi usavano un singolo trasmettitore FM, il quale perciò garantiva la copertura solo di una certa area circostante (tipicamente una città), consentendo ad una ristretto numero di utenti di effettuare chiamate telefoniche da una automobile durante spostamenti all'interno dell'area stessa. Nella stazione radio, la commutazione delle chiamate avveniva manualmente, tramite operatori. A ciascuna conversazione veniva riservato un **canale radio** FM di ampiezza 120 kHz ([2]).

Un'altra caratteristica fondamentale dei primi sistemi radiomobili era quella per cui ogni terminale di utente operava a una propria frequenza prefissata; c'erano allora un certo numero di trasmettitori indipendenti, ognuno avente in carico un certo numero di utenti (cioè di canali radio). In un secondo tempo, si introdussero sistemi di tipo **trunked**: tutti i canali erano a disposizione di tutti gli utenti e, all'occorrenza, veniva selezionato un canale libero per l'utente che ne faceva richiesta. Inizialmente la selezione del canale avveniva manualmente, poi fu automatizzata.

# I SISTEMI CELLULARI

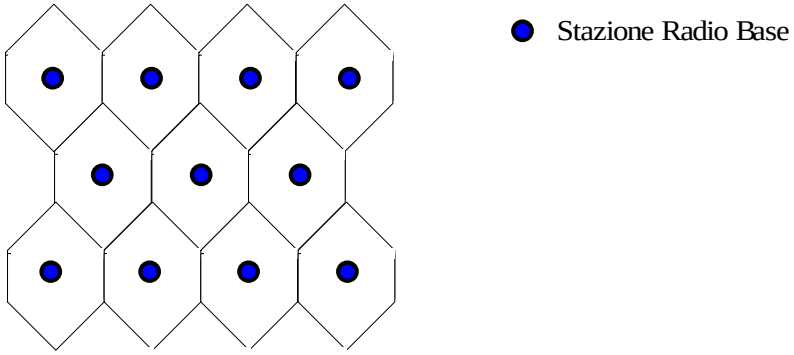
La svolta nelle comunicazioni mobili si ebbe con l'introduzione dei cosiddetti **sistemi cellulari**. L'idea base fu concepita negli anni '40, sperimentata negli anni '60, introdotta in sistemi commerciali negli anni '80.

[1] Trasmettere un segnale con modulazione FM significa far variare, proporzionalmente al segnale da trasmettere (*segnale modulante*), la frequenza di un segnale sinusoidale (*portante*), producendo il *segnale modulato* effettivamente trasmesso sul mezzo trasmissivo.

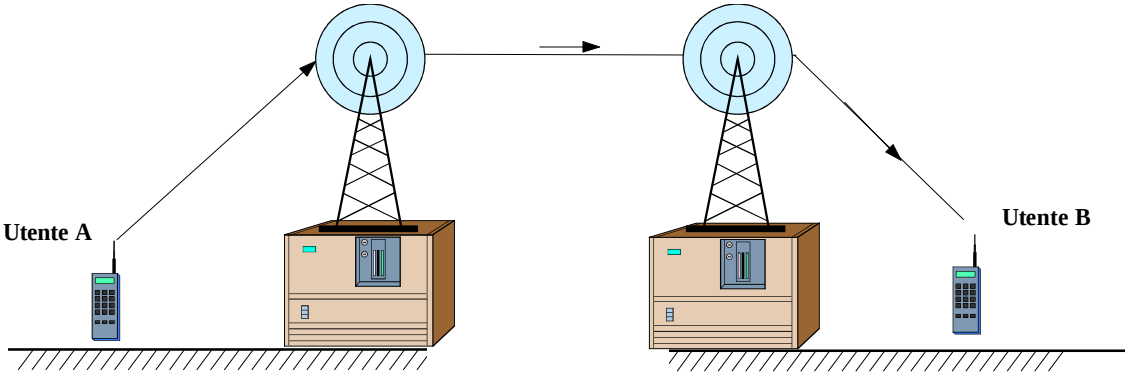
[2] Si trattava evidentemente di un enorme spreco di banda, se si considera che il singolo segnale telefonico analogico ha notoriamente una banda (lorda) di 4 kHz. Si cercò allora di ridurre la larghezza di banda del singolo canale: negli anni '60 la banda del canale si ridusse a 60 kHz e negli anni '70 si arrivò a 25 kHz.

Si è detto nel precedente paragrafo che i sistemi non cellulari effettuano sostanzialmente delle trasmissioni di tipo **broadcast** (come radio e TV): utilizzano cioè trasmettitori di potenza elevata per coprire una vasta area; all'interno di questa area, gli utenti presenti usufruiscono ciascuno di un proprio canale, allocato di volta in volta. Se il numero degli utenti è elevato, diventa difficile se non impossibile fornire il servizio contemporaneamente a tutti.

I sistemi cellulari che realizzano le **reti radiomobili**, applicano invece la tecnica del **riutilizzo delle frequenze**: una frequenza[3] viene utilizzata più volte, in luoghi diversi sufficientemente lontani tra loro. Questo è consentito da un principio di fondo, che consiste nel suddividere il territorio (l'area di servizio) in sottoaree, di dimensioni limitate, denominate **celle**:




Ogni cella è servita da una **stazione radio base**. Questa ha a disposizione un certo numero di frequenze (cioè di canali) con i quali instaurare una comunicazione con gli utenti presenti nella cella. Infatti, come si vedrà, quando un utente A vuol comunicare con un utente B, non comunica direttamente con esso, ma con la stazione base della cella in cui si trova:




La stazione radio base, con cui A si mette in contatto, si occupa, coadiuvata da una serie di altri *componenti di rete*, di instaurare una comunicazione con la stazione radio base della cella in cui si trova l'utente B.

Il concetto del **riuso delle frequenze** si può allora sintetizzare in due punti essenziali:

- intanto, i canali a disposizione della generica stazione base sono sempre diversi da quelli utilizzati nelle celle adiacenti, in modo da evitare *interferenze*;
- in secondo luogo, dato che ciascuna stazione radio base opera con potenza ridotta, i segnali da

[3] Si intende ovviamente una frequenza centrale, rappresentativa cioè del canale radio (di banda opportuna) centrato su di essa

essa trasmessi diventano trascurabili a sufficiente distanza; questo significa che è possibile *riutilizzare* le stesse frequenze in celle non adiacenti.

Questo meccanismo consente un uso estremamente efficiente dello spettro di frequenze a disposizione. Bisogna infatti considerare che lo spettro di frequenze è suddiviso in tanti intervalli, di ampiezza variabile, ognuno assegnato ad un determinato *servizio*. Tra questi *servizi* rientra anche la **rete GSM**, la quale quindi ha a disposizione una propria banda (che vedremo essere centrata attorno ai **900 MHz** per la prima versione della rete). Si tratta perciò di sfruttare al meglio questa banda di ampiezza inevitabilmente finita, al fine essenzialmente di poter connettere alla rete quanti più utenti possibile in contemporanea.

Tornando alle celle, generalmente vengono utilizzate forme regolari di celle per coprire un'area di servizio. Teoricamente, si possono immaginare celle di forma esagonale (come nell'ultima figura), anche se, in realtà, la loro forma risulta sempre inevitabilmente irregolare a causa della *non omogenea propagazione del segnale radio*, dovuta principalmente alla presenza di ostacoli (si pensi per esempio alle mura degli edifici all'interno di una città).

Un altro aspetto fondamentale, in una rete radiomobile, riguarda appunto la **mobilità** degli utenti: se, durante gli spostamenti, l'utente passa da una cella ad un'altra, è necessario che il terminale mobile si sintonizzi su una nuova frequenza (tipicamente quella ricevuta meglio tra le frequenze disponibili della nuova cella) in modo che la conversazione possa continuare e senza che l'utente si accorga del cambio di frequenza. La procedura con la quale si effettua il cambio di frequenza nel passare da una cella all'altra viene detta **handover**.

Nei sistemi cellulari, aumentando il numero delle celle che coprono una certa area (e perciò riducendo la loro dimensione), aumenta la **capacità** del sistema, cioè il numero di utenti gestibili contemporaneamente, ma diminuisce la *distanza di riuso delle frequenze* (cioè la distanza tra due celle che usano lo stesso canale), per cui aumenta l'interferenza tra canali che utilizzano la stessa frequenza (*interferenza cocanale*) ed aumenta il numero di *handover* che il sistema deve effettuare durante una conversazione. D'altra parte, diminuendo la dimensione di una cella, si può anche pensare di ridurre la potenza trasmessa, visto che il segnale deve percorrere distanze minori, in modo da ridurre l'interferenza e conservare intatta la distanza di riuso delle frequenze. Questa possibilità, però, trova un ostacolo nel fatto che bisogna sempre garantire una minima qualità prestabilita alla comunicazioni (la cosiddetta **QOS**, *Quality of Service*): ciò significa che la riduzione della potenza da trasmettere in ciascuna cella non può comunque andare oltre un minimo limite tollerabile. Come in quasi tutte le applicazioni, quindi, si tratta di trovare un compromesso tra le varie esigenze: qualità del servizio, dimensione delle celle, distanza di riuso delle frequenze e così via. A questo si aggiunga anche la difficoltà di reperire i siti in cui fisicamente installare le stazioni rice-trasmittenti.

## I SISTEMI CELLULARI ANALOGICI

I primi **sistemi cellulari**, basati sulle considerazioni di cui al precedente paragrafo, furono introdotti intorno ai primi anni '80 ed erano tutti di tipo **analogico**. Essi utilizzavano tecniche di modulazione di frequenza e presentavano sostanzialmente le seguenti limitazioni:

- ad ogni utente che effettuava una richiesta di connessione veniva assegnata una frequenza, che rimaneva impegnata per tutta la durata della conversazione, non potendo così essere utilizzata da altri terminali (**SCPC**, *Single Channel Per Carrier*)([4]);

[4] Si trattava, sostanzialmente, di uno schema del tipo **a commutazione di circuito** per la rete telefonica fissa tradizionale: alla generica conversazione vengono a priori assegnate tutte le risorse necessarie e queste rimangono assegnate per tutta la durata della conversazione.

- la capacità (cioè il numero di utenti connessi contemporaneamente) era limitata sia dal numero delle frequenze disponibili sia dal limite imposto alle dimensioni delle celle dalla interferenza cocanale;
- non si potevano applicare direttamente *algoritmi di crittografia* se non utilizzando apparati ad hoc (i cosiddetti **scrambler**, che però erano molto costosi);
- la sicurezza dell'accesso alla rete era minima, in quanto si basava solo sul riconoscimento di un numero di serie che identificava il *terminale mobile* (il telefonino), per cui non era impossibile clonare il terminale;
- non erano assolutamente adatti alla trasmissione di dati.

Il primo sistema introdotto, detto **AMPS** (*Advanced Mobile Phone Standard)*, fu sviluppato negli USA e introdotto nel mercato nel 1979 a Chicago.

La soluzione nord-europea fu il sistema **NMT** (*Nordic Mobile Telephone)*, avviato per la prima volta in Svezia nel 1981 e subito dopo in Norvegia, Danimarca e Finlandia.

Successivamente è stato sviluppato, nel Regno Unito, lo standard **TACS** (*Total Access Communications System)*, che era una versione modificata del sistema AMPS. La prima rete TACS ha iniziato la sua attività commerciale nel 1985 nel Regno Unito.

Le specifiche iniziali del sistema TACS assegnavano al sistema una banda complessiva di ampiezza **70 MHz**, (compresa precisamente tra 890 e 960 MHz), nella quale allocare 1000 canali. Successivamente, le specifiche sono state evolute nello standard **ETACS** (*Extended TACS)*, che assegna 1320 canali nella banda 872-950 MHz (quindi di ampiezza **78 MHz**).

## IL SISTEMA GSM

Quando i sistemi telefonici cellulari analogici, durante i primi anni '80, hanno avuto un rapido sviluppo in Europa, ogni nazione sviluppò un proprio sistema, che però era incompatibile con quelli degli altri paesi: il terminale mobile era perciò limitato ad operare entro i confini nazionali. Questa situazione non era gradita, per due motivi essenziali: in primo luogo, perché i sistemi mobili dovevano limitare la loro operatività all'interno dei confini nazionali; in secondo luogo, perché essa creava un mercato molto limitato per i vari tipi di apparecchiature necessarie all'implementazione ed allo sviluppo delle reti: non era infatti possibile realizzare economie di larga scala, con i conseguenti risparmi sia a favore degli utenti che degli operatori di rete.

Al contrario, la definizione di uno standard paneuropeo (per il quale fossero standardizzate funzioni ed interfacce) avrebbe consentito di operare in regime di concorrenza, che consentisse quindi ai *gestori* di utilizzare impianti forniti da diversi *costruttori*. Si sarebbe potuto aprire un vasto mercato, in grado di permettere significative economie di scala nella produzione di terminali e apparati, con conseguente diminuzione dei loro costi, e creare un servizio internazionale privo di confini.

Nel 1982, un gestore pubblico di servizi di telefonia mobile dei paesi nordici (*Nordic PTT*) inviò una proposta al **CEPT** (*Conference Européenne de Postal et Tèlécommunications*) per l'implementazione di un servizio comune di telefonia mobile europeo sulla frequenza dei **900 MHz**. Fu così creato un gruppo di studio *Groupe Speciál Mobile* (GSM) con lo scopo di studiare e sviluppare un sistema radiomobile cellulare paneuropeo comune a tutti i paesi dell'Europa occidentale. Il sistema proposto dal gruppo di studio doveva garantire dei precisi requisiti:

- assicurare una buona qualità audio della conversazione;
- bassi costi per i terminali e per la gestione del servizio;
- supporto per il *roaming* internazionale;

- supporto per terminali palmari;
- supporto per un ampio ventaglio di nuovi servizi;
- compatibilità con il sistema digitale **ISDN**;
- garantire un eccellente grado di sicurezza e riservatezza nelle comunicazioni.

Tre anni, dal 1982 al 1985, furono dedicati alla scelta tra la tecnica analogica e quella digitale. Nel 1985, dopo numerose discussioni, il gruppo ha deciso di implementare un sistema basato su *tecnologia digitale*. Si scelse però una tecnologia digitale non ancora testata, in netta antitesi con la tecnologia dei già sperimentati sistemi cellulari analogici come AMPS e TACS.

A favore della tecnologia digitale c'erano la rapida evoluzione tecnologica dei settori dell'elaborazione numerica dei segnali e l'integrazione dei componenti elettronici per effetto della disponibilità dei circuiti integrati VLSI.

Un sistema cellulare basato su sistema numerico offre numerosi vantaggi:

- consente di utilizzare un'unica frequenza per servire più utenti, tramite l'utilizzo di tecniche **TDM** (*Time Division Multiplexing*);
- ha una capacità maggiore sia per quanto sopra detto, sia perché i sistemi digitali sono meno sensibili a rumore ed interferenze e quindi consentono di ridurre le dimensioni delle celle, aumentando il numero di utenti che possono essere serviti contemporaneamente;
- consente alto grado di riservatezza, in quanto le informazioni trasmesse via radio possono essere cifrate direttamente dall'apparato utente;
- consente elevato grado di sicurezza: l'identità dell'apparato che chiede l'accesso alla rete può essere controllata tramite l'applicazione di un opportuno algoritmo e di una *chiave di autenticazione* segreta;
- consente di effettuare trasmissioni dati (il segnale vocale stesso viene digitalizzato e poi trasmesso).

Vi era poi la prospettiva di garantire la compatibilità fra la rete ISDN e la rete di supporto al sistema radiomobile (cioè la rete per lo scambio delle informazioni di controllo tra i vari componenti del sistema).

Un accordo tra i paesi aderenti portò alla decisione di riservare per questo sistema due bande di frequenza: **890-915 MHz** e **935-960 MHz**. Entrambe queste bande sono ampie **25 MHz** e, come si vedrà, servono l'una (*uplink*) alla comunicazione dai terminali mobili alle stazioni base e l'altra (*downlink*) per la comunicazione in senso contrario

Nel 1987, superati i problemi tecnici e politici affrontati per uniformare i diversi punti di vista dei paesi coinvolti e dei numerosi studiosi che portavano avanti progetti e sperimentazioni, le prime 13 nazioni (nel Regno Unito c'erano già due operatori) firmarono il **MoU** (*Memorandum of Understanding*) per l'introduzione coordinata del **sistema GSM**: esse si impegnarono a rispettare le specifiche, promettendo di avere il primo sistema basato sullo standard GSM operativo entro il 1° luglio 1991.

Nel 1989, la responsabilità del progetto GSM venne trasferita all' *European Telecommunication Standards Institute* (**ETSI**), ossia l'ente avente il mandato CEE per l'unificazione normativa in Europa nel settore delle telecomunicazioni. In quella sede venne ridefinito l'acronimo **GSM** come **Global System for Mobile Communications**. Il Comitato Tecnico dell'ETSI ha elaborato normative, standard e specifiche tecniche descritte in 12 serie di raccomandazioni. La prima parte delle specifiche del sistema GSM venne pubblicata nel 1990 (*GSM PHASE 1*).

Il corpo dello standard era costituito inizialmente da poco più di cento raccomandazioni alla cui stesura hanno collaborato PTT, centri di ricerca ed aziende manifatturiere di tutta Europa e rappresenta uno dei progetti più ambiziosi degli ultimi dieci anni dell'ETSI.

I primi servizi commerciali furono lanciati a metà del 1991, e nel 1993 erano già operativi 36 network GSM in 22 paesi.

Dopo la fase iniziale (**PHASE 1**) terminata nel 1991, in cui si è provveduto alla definizione delle specifiche relative ai servizi base essenziali e ad alcuni servizi supplementari, si è passati ad una seconda fase (**PHASE 2**) conclusasi nel 1993, durante la quale si sono integrati servizi base e supplementari e si sono corretti gran parte degli errori della *PHASE 1*.

Le quasi 6000 pagine delle raccomandazioni ETSI lasciano spazio a flessibilità e innovazioni competitive da parte dei produttori, ma forniscono una sufficiente standardizzazione per garantire l'effettivo internetworking tra le componenti del sistema.

Le specifiche sono state estese in seguito, assegnando una nuova banda, intorno a 1800-1900 MHz (**DCS1800** - **PCS1900**). In particolare, negli USA è stata concessa la banda dei 1900 MHz ed in Europa e negli altri paesi extraeuropei quella dei **1800 MHz**.

Il servizio venne commercializzato per la prima volta verso la metà del 1991, e nel 1993 esistevano già 36 reti GSM in 22 paesi.

*Nonostante sia stato standardizzato in Europa, il sistema GSM non è uno standard solo europeo:* infatti reti GSM sono operative o pianificate nel 1996 in oltre 100 paesi di tutto il mondo. La crescita degli abbonati è stata vertiginosa : 1,3 milioni all'inizio del 1994, 5 milioni all'inizio del 1995, per raggiungere i 10 milioni alla fine del 1995 solo in Europa.

## *Pregi fondamentali*

In generale, possiamo dunque dire che lo standard GSM definisce una serie di miglioramenti e innovazioni rispetto alle reti radio cellulari preesistenti, mirando ad un uso efficiente dello spettro delle radio frequenze, alla sicurezza della trasmissione, al miglioramento della qualità delle conversazioni, alla riduzione dei costi dei terminali, delle infrastrutture e della gestione, alla capacità di supportare nuovi servizi e alla piena compatibilità con la rete **ISDN** (*Integrated Services Digital Network*) e con altre reti di trasmissione dati.

Inoltre, *la rete radiomobile GSM costituisce il primo sistema standardizzato ad usare una tecnica di trasmissione numerica su canale radio:* questo punto rappresenta una caratteristica peculiare della rete, in quanto tutti i sistemi radio cellulari antecedenti utilizzavano tecniche di trasmissione analogiche.

Altra caratteristica di base del sistema é il **roaming** (*mobilità*), ossia la possibilità offerta all'utente mobile di accedere ai servizi GSM anche quando si trova fisicamente al di fuori dell'area di copertura della propria rete di sottoscrizione, registrandosi come *utente visitatore*. Il roaming è completamente automatico all'interno di tutte le nazioni coperte dal sistema GSM ed è regolato da precisi (ma non sempre chiari) accordi commerciali tra i vari operatori.

Oltre alla possibilità di effettuare il Roaming, il GSM fornisce nuovi servizi per l'utente, quali ad esempio la trasmissione dati, il servizio fax ed il servizio trasmissione brevi messaggi di testo (**SMS**).

Riassumendo, le principali caratteristiche richieste da questo nuovo progetto riguardavano il raggiungimento dei seguenti **obbiettivi**:

- possibilità di usare lo stesso terminale radio in tutti i Paesi dell'area CEE, ed in quei Paesi non appartenenti alla Comunità ma che utilizzano lo stesso standard (*Roaming internazionale*).
- miglioramento dell'efficienza spettrale rispetto alle attuali reti radiomobili cellulari di tipo analogico.
- sicurezza della trasmissione radio (per impedire l'intercettazione delle conversazioni e dei dati identificativi dell'utente)

- impiego della tecnica numerica, per consentire il miglioramento della qualità fonica, della trasmissione dati e della compatibilità con gli standard internazionali a livello **OSI** (*Open System Interconnection*) e **ISDN** (*Integrated Services Digital Network*).

## L'EVOLUZIONE SUCCESSIVA: STANDARD DCS1800 E PCS1900

La naturale evoluzione del sistema GSM è il cosiddetto protocollo *Personal Communications Network* (**PCN**). Ad esso, l'ETSI ha assegnato una banda di **75 MHz** nell'intorno dei 1800 MHz. Un nuovo standard, chiamato **DCS1800** (*Digital Cellular System*), è stato sviluppato appositamente per queste frequenze. Virtualmente il DCS1800 utilizza le stesse specifiche del GSM, il che significa che i componenti di una rete GSM possono essere usati in reti DCS1800. Solo i trasmettitori radio e i telefoni palmari necessitano di apposite specifiche, date le diverse frequenze di funzionamento.

Le proprietà che differenziano il DCS1800 dal GSM sono:

- frequenze di lavoro più alte, che comportano caratteristiche di propagazione diverse: generalmente hanno un raggio d'azione più corto e penetrano meglio all'interno degli edifici (il che lo rende un sistema ideale per le zone ad alta densità abitativa come le città).
- l'ampiezza di banda di **75 MHz**, triplicata rispetto ai **25 MHz** del GSM iniziale, che permette sostanzialmente di raddoppiare gli 800 utenti (teorici) massimi per cella.
- una minore potenza di trasmissione, che garantisce meno interferenze e un migliore sfruttamento delle batterie del telefono palmare.

E' stata ormai completata la standardizzazione delle procedure che permetteranno una integrazione (*inter-working*) tra le reti GSM e DCS1800 così che una **SIM card GSM** potrà essere usata su un telefono DCS1800 e viceversa.

La prima rete DCS1800 (la rete *Mercury One-2-One*) è entrata in servizio nel 1993 nel Regno Unito.

Negli Stati Uniti, dove non esiste una rete GSM, sono stati riservati 140 MHz nella banda 1900 MHz (1850-1990 MHz) per il *sistema PCN*. Questa ulteriore variante del GSM, chiamata **PCS1900** (*Personal Communications Service*), continua ad essere GSM compatibile se non per la frequenza di lavoro e la potenza di trasmissione.

## TELEFONI MOBILI MULTI-STANDARD

A causa della crescente domanda di capacità dei sistemi radiomobili attuali, che spesso crea saturazioni dei singoli network, specialmente nelle zone densamente popolate, si è resa necessaria l'implementazione di **terminali multi-standard**, capaci cioè di commutare tra sistemi con frequenze e tecnologie digitali diverse, permettendo all'abbonato di muoversi più liberamente all'interno di aree coperte da più networks.

Un terminale che può funzionare su due network differenti, può essere classificato come:

* **dual band**, quando utilizza la stessa tecnologia, ma frequenze differenti; ad esempio, un terminale capace di funzionare sulla rete GSM 900 e sulla rete DCS 1800 (chiamata anche GSM1800 o PCN) è di tipo *dual mode*, perché in questo caso entrambe le reti utilizzano lo stesso standard di trasmissione e l'unica differenza tra i due sistemi è solo la banda utilizzata;
* **dual mode**, quando è capace di connettersi con reti tecnologicamente diverse (standard di trasmissione e/o banda di frequenza utilizzata); un esempio in questo caso sono i telefoni che funzionano sia sulle reti terrestri che su quelle satellitari.

Interessante è il terminale che combina le tecnologie GSM e **DECT**, consentendo all'abbonato di usare il roaming e l'estesa copertura del servizio GSM quando si allontana dall'ambito cittadino e di sfruttare invece il servizio DECT e tutti i suoi vantaggi (stesso numero di casa o ufficio, caratteristiche PABX, ottima qualità del segnale anche all'interno di edifici, tariffe inferiori a quelle delle reti radiomobili).

La commercializzazione dei primi telefoni GSM *dual-band* è iniziata dopo il Cebit '97, con alcuni telefoni in grado di operare sia nei networks GSM 900, che in quelli DCS 1800/PCS1900. Il PCS1900 è lo standard adottato dagli USA che sfrutta la stessa tecnologia del GSM, ma sulla banda dei 1900 MHz.

Chi è in possesso del GSM dual-band GSM-PCS1900 può effettuare roaming anche negli Stati Uniti, mantenendo la propria SIM card ed il proprio numero.

Interessante la caratteristica del **dual band handover**, che, ad esempio, consente all'abbonato, che si trova in un area coperta sia dal sistema GSM 900 che da quello DCS 1800, di poter commutare automaticamente tra un sistema e l'altro anche quando si trova in conversazione. Naturalmente in questo caso sia il telefono che la rete devono supportare tale modalità di funzionamento.

Nel 1998, con l'apertura delle **reti telefoniche satellitari**, sono stati commercializzati i telefoni mobili *dual mode*, cioè quelli che combinano le tecnologie GSM-satellitare, DCS1800-satellitare, PCS1900-satellitare, AMPS-satellitare, ecc. Questi terminali sono capaci di commutare automaticamente sulla rete satellitare, quando non è più presente copertura radio sulla rete cellulare terrestre. Infatti anche se i sistemi cellulari terrestri continueranno a crescere velocemente, saranno in grado di coprire solo una piccola parte della superficie terrestre; così le nuove potenti reti radiomobili satellitari saranno un utile complemento ad essi, facilitando le comunicazioni in aree remote in qualunque punto del pianeta.

# Caratteristiche tecniche del sistema GSM

## SUDDIVISIONE DEL TERRITORIO IN CELLE

A differenza di quanto avviene nella rete telefonica fissa, in cui il terminale di ogni utente è collegato alla rete attraverso un punto di accesso dedicato e univoco, in una **rete radiomobile**, l'abbonato è libero di spostarsi in qualsiasi punto della rete[5].

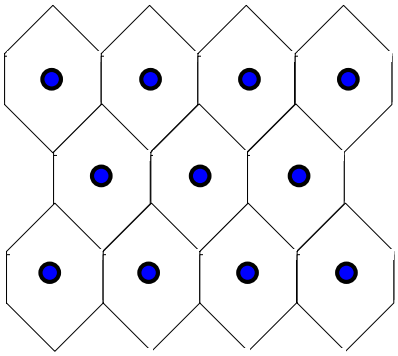
La caratteristica di base di un sistema radiomobile può essere riassunta in termini di *networking* (interazione) tra le apparecchiature radio, i nodi radiomobili, i database e la rete telefonica pubblica (**PSTN** per la rete analogica e **ISDN** per quella digitale), al fine di identificare i terminali mobili, di stabilire, controllare e terminare le connessioni e di aggiornare i dati di gestione.

In tutti i sistemi di radiocomunicazione, il fattore che ha una primaria importanza é lo *spettro di frequenza disponibile* ( o **larghezza di banda**): infatti, il numero di frequenze radio assegnato a questi servizi è limitato. Ad esempio, nel caso del GSM, le specifiche iniziali assegnarono le seguenti bande:

*Up-Link* (da terminale mobile a stazione base): **890-915 MHz**
*Down-Link* (da stazione base a termine mobile): **935-960 MHz**

[5] Come si vedrà, questo impone che i dati relativi all'abbonato vengano memorizzati in un *database* che sia consultabile e aggiornabile da qualsiasi punto della rete ed in qualunque momento.

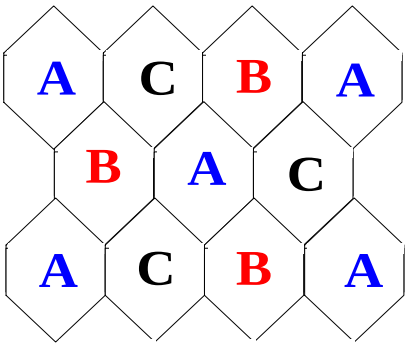
Entrambe queste bande sono ampie **25 MHz**, per cui si pone il problema di sfruttare al massimo questa larghezza di banda disponibile, al fine di connettere quanti più utenti possibile contemporaneamente in uno stesso settore. Per ottenere questo risultato, il sistema è realizzato suddividendo *l'area di servizio* (*Service Area*) in zone confinanti denominate **celle.**



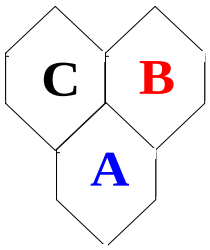
Stazione Radio Base

Come già detto, ogni cella fa riferimento ad una *Stazione Radio Base* (**BTS**) che opera su un set di canali radio, diversi da quelli utilizzati nelle celle adiacenti (per evitare interferenze). Questo tipo di suddivisione permette il riutilizzo delle stesse frequenze in celle non adiacenti.

Per fare un esempio concreto, supponiamo che la banda disponibile[6] venga suddivisa in 3 sottobande, che indichiamo rispettivamente con A, B e C. Se una data cella usa i canali del gruppo A, nessuna delle celle adiacenti potrà usare gli stessi canali. Stesso discorso, ovviamente, per le altre due sottobande. Di conseguenza, la ripartizione delle sottobande, ad esempio nel caso dell'ultima figura, non potrà che essere il seguente:




Suddivisione del territorio in ***celle***




***Cluster***: insieme di celle tra cui ripartire tutte le frequenze disponibili

*La figura mostra la divisione del territorio in celle, nonché il fatto che lo spettro radio sia stato suddiviso (per esempio) in 3 gruppi di frequenze (indicati rispettivamente con A,B e C). Ogni cella ha a disposizione un solo gruppo di frequenze. L'insieme di 3 celle adiacenti, che quindi utilizzano tutti e 3 i gruppi di frequenze, prende il nome di* ***cluster****.*

Si nota immediatamente che è possibile individuare un insieme di celle adiacenti che usino, nel complesso, tutte le frequenze disponibili: a tale insieme di celle si dà il nome di **cluster**. Possiamo perciò affermare che l'area totale coperta dal servizio può essere suddivisa in celle oppure, ad un livello superiore, in cluster. Vedremo che è anche possibile considerare una suddivisione a livello ancora superiore, che quindi metta insieme più cluster.

[6] Si tenga presente che quando parliamo di banda disponibile non ci riferiamo a tutti i 25 MHz messi a disposizione delle specifiche. Infatti, questi 25 MHz vengono ripartiti, in ciascuna nazione e a cura del Governo, tra i vari operatori presenti (in Italia, parliamo di Tim, Omnitel, Wind e del prossimo gestore Blutel). Quindi, ciascuna operatore ha solo una frazione della banda messa complessivamente a disposizione della rete GSM. Di questo aspetto, comunque, ci occuperemo anche più avanti.

Generalmente, vengono utilizzate forme regolari di *celle* e quindi di *cluster* per coprire un'area di servizio.

Possiamo fare un banale conto per renderci conto del fatto che il riuso delle frequenze consente di aumentare il numero di canali disponibili, a parità di area coperta. Supponiamo di voler utilizzare la banda a nostra disposizione usando N canali di ampiezza costante. Questo numero N è pari evidentemente al rapporto tra la banda complessiva a disposizione e l'ampiezza di banda che vogliamo riservare a ciascun canale: ad esempio, se la banda complessiva è di 25 MHz e ogni canale deve essere ampio 200 kHz, il numero di canali ottenibili è

$$N = \frac{25(\text{MHz})}{200(\text{kHz})} = 125$$

Quindi, se consideriamo l'area complessiva coperta dal servizio e non volessimo utilizzare il riuso delle frequenze, potremmo connettere non più di 125 utenti contemporaneamente.

Adesso consideriamo la suddivisione dell'area in celle, ad esempio nelle 11 celle dell'ultima figura. Usiamo inoltre la tecnica del riuso delle frequenze, dividendo lo spettro a disposizione nelle tre sottobande A,B e C di cui si diceva prima. E' ovvio che ciascuna sottobanda corrisponde ad un numero di canali inferiore rispetto ad N: precisamente, disponiamo, per ciascuna sottobanda, di $\frac{N}{3} = 41$ canali (dove abbiamo ovviamente arrotondato il risultato della divisione all'intero più piccolo). Visto, però, che usiamo 11 celle, in ciascuna delle quali disponiamo di 41 canali, il numero totale di canali disponibili nell'area considerata è $\frac{N}{3} \cdot 11 = 451$.

Quindi, rispetto ai 125 canali ottenibili, senza il riuso delle frequenze, sull'intera area di copertura del servizio, ci basta considerare un'area di 11 celle per ottenere un numero di canali più che triplicato.

E' ovvio che questo è un conto di massima, perché comunque non tutti i canali disponibili vengono usati per trasmettere le conversazioni.

Essendo limitato il numero di canali in ogni cella, è anche limitato il numero di utenti che possiamo servire contemporaneamente. Come già anticipato in precedenza, possiamo pensare di ridurre la dimensione delle celle, al fine di aumentare il riuso delle frequenze e quindi, a parità di area coperta, di aumentare il numero complessivo di canali. Il problema, però, è nell'interferenza: riducendo la dimensione di una cella, ma mantenendo invariata la potenza trasmessa, il segnale potrebbe non diventare più trascurabile in una cella non adiacente che però usa la stessa frequenza; si avrebbe perciò la sovrapposizione delle comunicazioni, che prende appunto il nome di **interferenza cocanale**. Quanto più diminuisce la dimensione della cella, tanto più il problema dell'interferenza diventa pesante. Si può chiaramente ridurre la potenza[7], ma anche questa soluzione, come già detto, ha una controindicazione nel fatto che comunque bisogna garantire una qualità minima del servizio.

Si capisce dunque quanto importante sia il problema dell'interferenza ed è per questo che il sistema GSM utilizza delle opportune tecniche tendenti a minimizzarla.

[7] La riduzione della potenza va anche a vantaggio della soluzione dei problemi di inquinamento elettromagnetico.

## *Cenni alla tecnica di accesso*

Anche se questo aspetto sarà discusso in seguito, possiamo anticipare che lo standard GSM utilizza la tecnologia di accesso a divisione di frequenza (**FDMA**) combinata con quella ad accesso a divisione di tempo (**TDMA**): questo significa che, dopo aver diviso la banda disponibile in un certo numero di canali radio (FDM), ogni canale viene utilizzato da 8 (*Full Rate*) oppure 16 (*Half Rate*) utenti secondo una tecnica a divisione di tempo (TDM). In altre parole, dato il singolo canale radio (da **200 kHz**), esso è utilizzato da 8 o 16 utenti contemporaneamente, a ciascuno dei quali è assegnato uno slot temporale di durata prefissata. Gli slot temporali sono talmente brevi e ravvicinati, che l'utente non si accorge minimamente della temporizzazione, avendo cioè la "sensazione" di essere l'unico ad usare quel dato canale.

## RIEPILOGO GENERALE DEI PARAMETRI TECNICI DEL SISTEMA GSM

Sono adesso riassunti i principali parametri tecnici del network GSM, alcuni dei quali sono stati già descritti, mentre gli altri saranno descritti in seguito:

- **Banda operativa:**
  - GSM: *Up-Link* (Mobile→Base) **890-915** MHz e *Down-Link* (Base→Mobile) **935-960** MHz .
  - Extended GSM: *Up-Link* **880-915** MHz e *Down-Link* **925-960** MHz. Recentemente la banda operativa è stata estesa (**Extended GSM**) per aumentare la capacità del sistema.
  - DCS: *Up-Link* (Mobile-Base) **1710-1785** MHz e *Down-Link* (Base-Mobile) **1805-1880** MHz

    GSM Italia: *Up-Link* **905-914** MHz e *Down-Link* **950-959** MHz. In Italia la banda operativa è meno estesa a causa dell'utilizzo di parte della stessa da parte della rete analogica ETACS.
- **Portanti radio per singola banda**
  - GSM: **124** portanti
  - Extended GSM: **174** portanti
- Spaziatura di canale: **200** kHz
- Modulazione **GMSK** (*Gaussian Minimum Shift Keying*) digitale, a inviluppo costante con prefiltraggio gaussiano B.T.= 0,3
- Algoritmo di *Frequency Hopping* (Frequenza di Hopping = 217 hops/s)
- Accesso alla rete di tipo **TDMA** (*Time Division Multiple Access*) combinato con **FDMA** (*Frequency Division Multiple Access*) con 8 intervalli per portante radio (*Time Slot*)
- **Numero totale canali vocali con 124 portanti radio:**
  - **992** con campionamento di ogni portante a 16 kbit/s (*Full Rate*)
  - **1984** con campionamento di ogni portante a 8 kbit/s (*Half Rate*)
- Codifica voce con algoritmo **RPE - LTP - LPC** (*Regular Pulse Exitation - Long Term Prediction - Linear Predictive Coding*) con campionamento a 13 kbit/s

- Procedura di compensazione del ritardo di propagazione della tratta radio fino a 233 microsecondi (che consente un raggio massimo della cella di 35 Km)
- Recupero di dispersione (equalizzazione del canale radio) tipicamente fino a 20 microsecondi
- Controllo dinamico di potenza dell'apparato mobile (**MS**) e opzionalmente della *Stazione Radio Base* (**BTS**) durante il collegamento radio
- Trasmissione e ricezione di tipo discontinuo (**DTX**). I burst vengono trasmessi solo durante l'effettiva attività fonica.

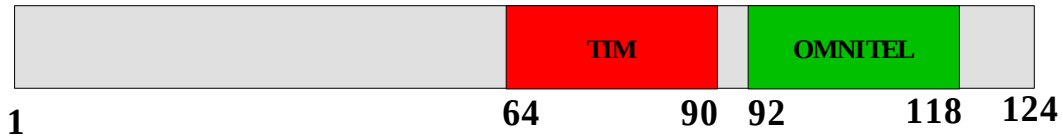
## ASSEGNAZIONE DELLE FREQUENZE IN ITALIA

Come detto in precedenza, solo una porzione dello **spettro radio** è stata assegnata alla *rete cellulare GSM*. Ogni nazione ha il completo arbitrio di ripartire tale porzione tra i vari operatori che ne fanno richiesta. Vediamo allora alcune tappe dell'assegnazione delle frequenze in Italia.

Inizialmente, l'unico operatore di telefonia mobile GSM presente in Italia era **TIM** (Telecom Italia Mobile). Nel **dicembre 1994** è subentrato il nuovo operatore **Omnitel**. Al momento della concessione al nuovo operatore, il piano delle frequenze fu il seguente:

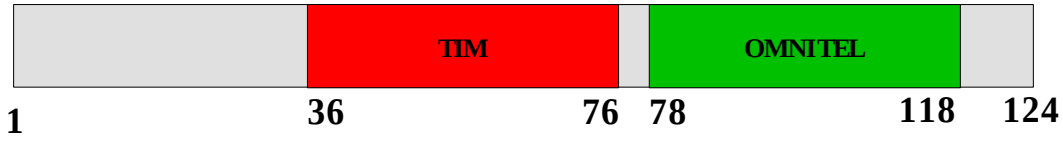
| | | | |
|---|---|---|---|
| **GSM TIM** | *uplink* | 902.7 - 908.1 MHz | 5.4 MHz canali da 64 a 90 |
| | *downlink* | 947.7 - 953.1 MHz | |
| **GSM OMNITEL** | *uplink* | 908.3 - 913.7 MHz | 5.4 MHz canali da 92 a 118 |
| | *downlink* | 953.3 - 958.7 MHz | |

Come si vede, entrambi gli operatori hanno avuto a disposizione una banda di **5.4 MHz** (per un totale di **27 canali**[8]) sia per l'uplink sia per il downlink:




Il **16 settembre 1997**, quando ancora gli unici operatori presenti erano Tim e Omnitel, la banda assegnata a ciascuno di essi fu ampliata ad **8.2 MHz** (per cui il numero di canali passò a **41 canali**):

| | | | |
|---|---|---|---|
| **GSM TIM** | *uplink* | 897.1 - 905.3 MHz | 8.2 MHz canali da 36 a 76 |
| | *downlink* | 942.1 - 950.3 MHz | |
| **GSM OMNITEL** | *uplink* | 905.5 - 913.7 MHz | 8.2 MHz canali da 78 a 118 |
| | *downlink* | 950.5 - 958.7 MHz | |

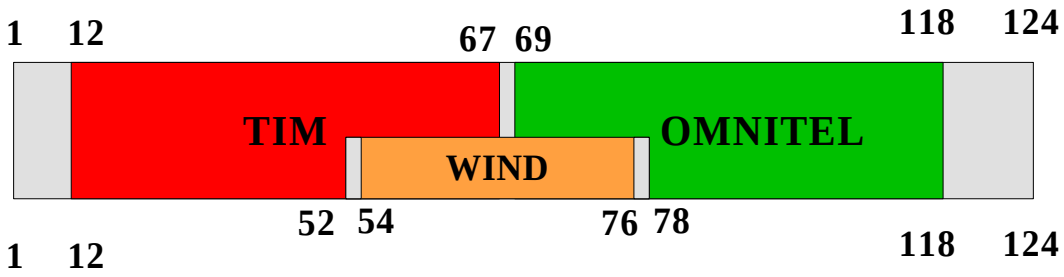



[8] Basta dividere l'ampiezza totale (5.4 MHz) per l'ampiezza del singolo canale (200 kHz).

A partire dal **1 Novembre 1998** è subentrato il nuovo operatore **WIND** e venne fatta una assegnazione delle frequenze un po' "particolare", nel senso che WIND ottenne frequenze solo al di fuori delle 16 più grandi città, mentre OMNITEL e TIM conservarono lo stesso numero di canali, però spostati in frequenza rispetto al piano precedente. La tabella completa è la seguente:

| | | | |
|---|---|---|---|
| **GSM TIM** | *uplink* | 892.3-900.5 (903.5*) MHz | 8.2 (11.2*) MHz<br>Canali da 12 a 50 (67*) |
| | *downlink* | 937.1-945.5 (948.5*) MHz | |
| **GSM WIND** | *uplink* | 900.7-905.3 MHz | 4.6 MHz<br>Canali da 54 a 76 |
| | *downlink* | 945.7-950.3 MHz | |
| **GSM OMNITEL** | *uplink* | 905.5 (903.7*)-913.7 MHz | 8.2 (10) MHz<br>Canali da 78 (69*) a 118 |
| | *downlink* | 950.5 (948.7*)-958.7 MHz | |

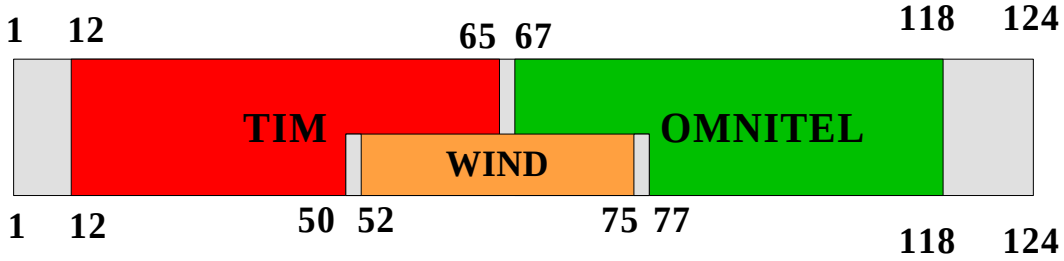
Gli *asterischi* che compaiono in questa e nelle prossime tabelle indicano la sovrapposizione di alcune frequenze tra i vari operatori, come indicato nel seguente prospetto:




Il **1° Luglio 1999** è stato varato un nuovo piano di assegnazione delle frequenze, che incrementò di 200 kHz (cioè 1 canale radio) la banda di tutti e tre gli operatori:

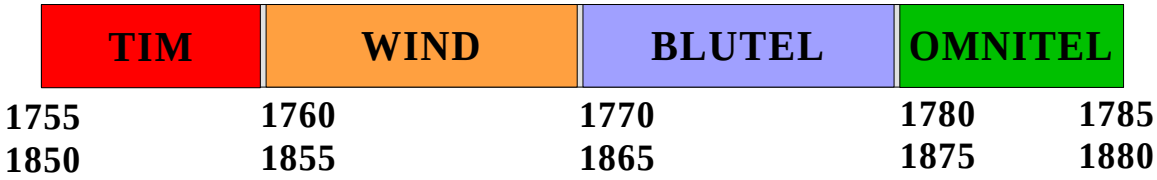
| | | | |
|---|---|---|---|
| **GSM TIM** | *uplink* | 891.7 - 900.1 (903.1*) MHz | 8.4 (11.4*) MHz<br>Canali da 9 a 50 (65*) |
| | *downlink* | 933.7 - 945.1 (948.1*) MHz | |
| **GSM WIND** | *uplink* | 900.3 - 905.1 MHz | 4.8 MHz<br>Canali da 52 a 75 |
| | *downlink* | 945.3 - 950.1 MHz | |
| **GSM OMNITEL** | *uplink* | 905.3 (903.3*)-913.7 MHz | 8.4 (10.4) MHz<br>Canali da 77 (67*) a 118 |
| | *downlink* | 950.3 (948.3*)-958.7 MHz | |

Secondo questa tabella, TIM e OMNITEL disponevano di 42 canali ciascuno al di fuori delle 16 più grandi città e di 57 canali all'interno di tali città), mentre invece WIND aveva 24 canali, tutti al di fuori delle 16 più grandi città:



Tuttavia, sempre nella data del 1° Luglio 1999 è stato anche varato il piano di assegnazione delle frequenze del nuovo **sistema DCS** (nelle bande 1710-1785 MHz, 1805-1880 MHz). Tale piano ha assegnato **4.8 MHz** (**24 canali**) ciascuno ai gestori Tim e Omnitel, mentre ha assegnato **10 MHz** (**50 canali**) ciascuno agli operatori Wind e **Blutel** (ultimo nato), secondo la seguente tabella::

| | | | |
|---|---|---|---|
| **TIM** | *uplink* | 1755 - 1759.8 MHz | 4.8 MHz |
| | *downlink* | 1850 - 1854.8 MHz | |
| **WIND** | *uplink* | 1760 - 1770 MHz | 10 MHz |
| | *downlink* | 1855 - 1865 MHz | |
| **BLUTEL** | *uplink* | 1770 - 1780 MHz | 10 MHz |
| | *downlink* | 1865 - 1875 MHz | |
| **OMNITEL** | *uplink* | 1780.2 - 1785 MHz | 4.8 MHz |
| | *downlink* | 1875.2 - 1880 MHz | |

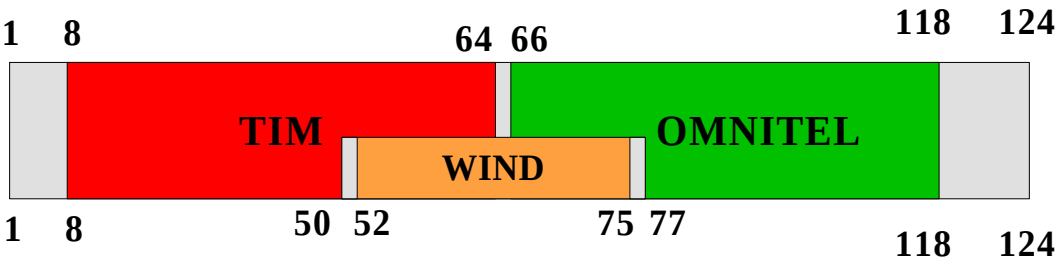



Infine, il **15 Settembre 1999** è stato varato il piano delle frequenze del nuovo sistema **Extended GSM** (880-915 MHz, 925-960 MHz), con il quale la banda intorno ai 900 MHz è stata ampliata dai 25 MHz iniziali a **35 MHz**:

- al gestore **Tim** sono assegnati **11,4 MHz** (57 portanti) con l'obbligo di utilizzare le portanti da 51 a 64 solo per il territorio all'interno dell'area urbana delle grandi città;
- al gestore **Omnitel** sono assegnati **10.6 MHz** (53 portanti), in virtù del suo minore carico d'utenza, con l'obbligo di utilizzare le portanti da 66 a 76 solo per il territorio all'interno dell'area urbana delle grandi città;
- al gestore **Wind** sono assegnati **4.8 MHz** (24 canali) solo per il territorio all'esterno dell'area urbana delle grandi città;

| | | | |
|---|---|---|---|
| **GSM TIM** | *uplink* | 891.7-900.1 (903.1*) MHz | 8.6(11.4*) MHz<br>Canali da 8 a 50 (64*) |
| | *downlink* | 933.7-945.1 (948.1*) MHz | |
| **GSM WIND** | *uplink* | 900.3 - 905.1 MHz | 4.8 MHz<br>Canali da 52 a 75 |
| | *downlink* | 945.3 - 950.1 MHz | |
| **GSM OMNITEL** | *uplink* | 905.3 (903.3*)-913.7 MHz | 8.4(10.6) MHz<br>Canali da 77 (66*) a 118 |
| | *downlink* | 950.3 (948.3*)-958.7 MHz | |

Rispetto al precedente piano di assegnazione, Tim e Omnitel hanno avuto 3 canali in più all'interno delle 16 più grandi città:




Come si evince da questi prospetti, i gestori WIND e BLUTEL non hanno avuto alcun canale all'interno delle grandi città. Questo, ovviamente, non preclude la copertura su tali città, in quanto viene utilizzato il già citato **roaming**: un utente WIND o BLUTEL che si trovi in un'area non coperta dal proprio gestore, può comunque effettuare le proprie comunicazioni appoggiandosi ai ripetitori degli altri operatori (OMNITEL e TIM) presenti in quella stessa area. Laddove ci fosse una zona non coperta da alcun operatore, l'utente non potrebbe effettuare alcuna comunicazione.

# Architettura del sistema GSM

## INTRODUZIONE: PRINCIPALI *SOTTOSISTEMI*

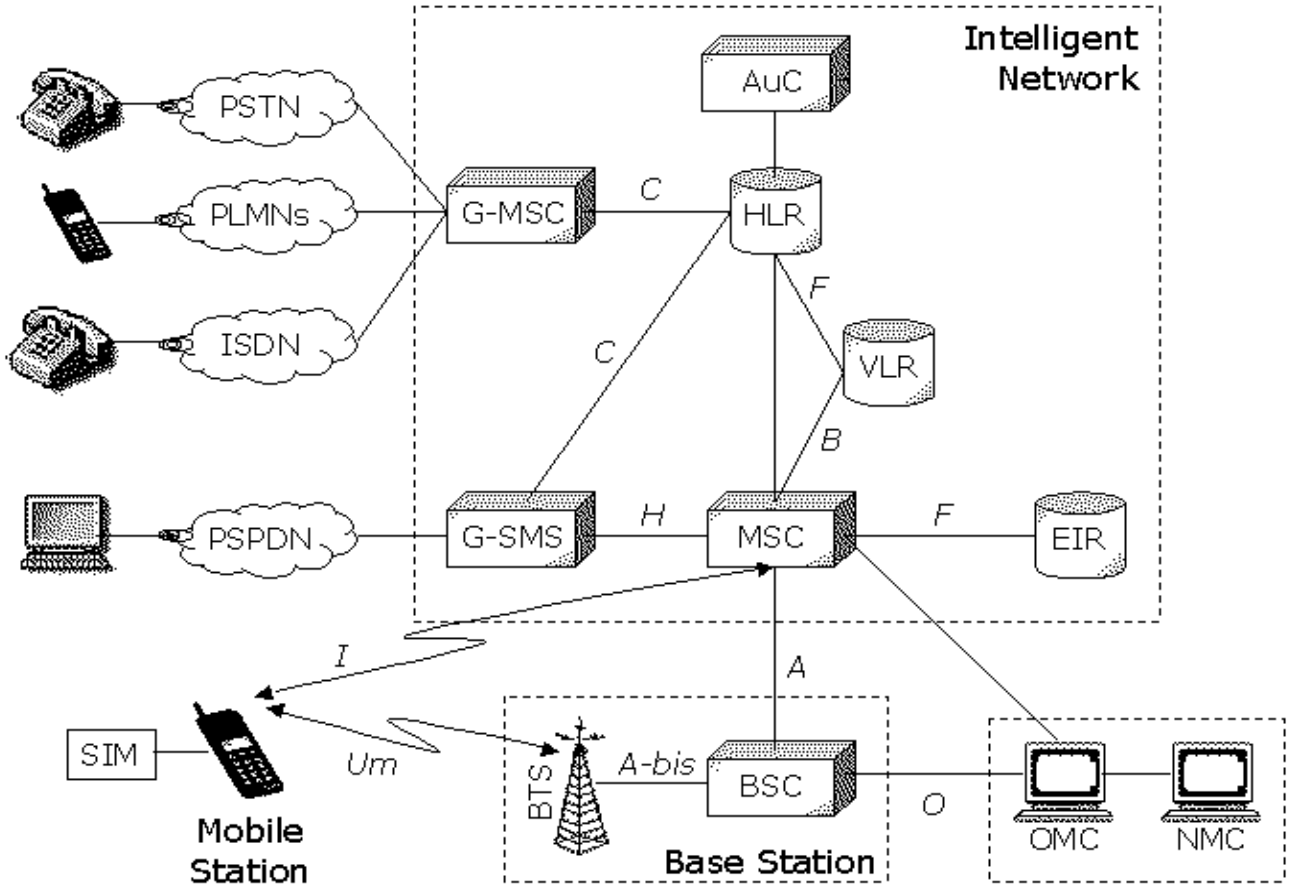
Una rete GSM é composta di numerose entità funzionali che possono essere raggruppate in quattro **sottosistemi**:

- la **Stazione Mobile** (*Mobile Station*) é il terminale mobile usato dall'abbonato;
- la **Stazione Base** (*Base Station Subsystem*) controlla la trasmissione radio con il terminale;
- il **Sottosistema di rete** (*Network Subsystem*), la cui parte principale é il **Centro di Commutazione** (*Mobile services Switching Center*), realizza la connessione tra l'utente della rete mobile e gli utenti delle altre reti, fisse o mobili che siano;
- il **Sottosistema di esercizio e manutenzione** (*Operation and Support Subsystem*) sovrintende al corretto funzionamento e settaggio della rete.

La comunicazione tra le diverse entità del sistema GSM è assicurata da specifiche **interfacce**.

La possibilità di effettuare il **roaming**, cioè di potersi spostare liberamente sia sul territorio servito dal proprio gestore sia anche su quello servito dagli altri gestori delle nazioni che aderiscono al GSM, richiede di memorizzare in un database la posizione degli utenti ed aggiornarla man mano che questi si spostano. A tal scopo l'area geografica di servizio del sistema GSM è suddivisa gerarchicamente in diverse aree. Un operatore GSM è quindi sempre in grado di individuare la posizione di ciascun suo abbonato.

Nella figura seguente è riportata una visione generale delle principali unità funzionali che costituiscono la rete GSM:




I prossimi paragrafi sono destinati alla descrizione delle singole unità qui rappresentate.

## MOBILE STATION

La **mobile station** (**MS**) rappresenta la stazione mobile con la quale un utente può usufruire dei servizi offerti dal GSM. Essa consiste di due componenti:

- il **terminale mobile** (*Mobile Equipment*, **ME**), ossia l'apparecchio telefonico (il "telefonino");
- una **smart-card intelligente**, detta **SIM card** (*Subscriber Identity Module*), che permette ad un utente di caratterizzare come proprio un qualsiasi terminale mobile GSM.

E' importante sottolineare la netta distinzione tra l'apparecchio mobile vero e proprio e la SIM che contiene tutti i dati dell'abbonato. Quest'ultima è distinta rispetto al terminale ed è da esso rimovibile.

### *Sim card*

La SIM card contiene una **memoria seriale**, nella quale vengono memorizzate diverse informazioni, e un **processore** in grado di eseguire alcuni algoritmi di cifratura (*Encryption algorithms*).

Le possibilità offerte da queste smart-card possono variare notevolmente da operatore a operatore, in dipendenza delle specifiche implementazioni.

La SIM card contiene le seguenti informazioni:

- *International Mobile Subscriber Identity* (**IMSI**): codice per identificare l'utente;
- *Temporary Mobile Subscriber Identity* (**TMSI**);
- *Individual subscribers authentication key* (**Ki**) : chiave segreta di autenticazione

Il codice **IMSI** e la chiave di autenticazione **Ki** costituiscono le credenziali di identificazione dell'abbonato, equivalenti al numero seriale **ESN** (*Equipment Serial Number*) dei sistemi analogici[9]. *L'IMSI è quindi associato all'utente che ha sottoscritto l'abbonamento al GSM, mentre è svincolato dall'apparato mobile (ME) utilizzato.*

- *Ciphering key generating algorithm* (**A8**) : algoritmo di cifratura;
- *Authentication algorithm* (**A3**) algoritmo di autenticazione;

- *Personal Identity Number* (**PIN** e **PIN2**)
- *PIN Unblocking Key* (**PUK** e **PUK2**)

La SIM card è ciò che fornisce l'abilitazione al servizio e, all'atto dell'accensione del terminale, viene attivata (per evitarne un uso non autorizzato) tramite un numero di identificazione personale di 4 o 8 cifre, denominato **PIN** (*Personal Identity Number*). Per garantire una sicurezza ancora maggiore, se il codice PIN viene digitato erroneamente per 3 volte consecutive, la carta si blocca ed è necessario utilizzare il codice **PUK** di 8 cifre (*PIN Unblocking Key*) per sbloccarla. Se anche quest'ultimo venisse digitato erroneamente per 10 volte consecutive la carta andrebbe in blocco totale e sarebbe necessario sostituirla.

L'introduzione di alcuni nuovi servizi nella **Phase 2** di sviluppo del sistema GSM ha richiesto l'introduzione di un secondo PIN (**PIN2**) per proteggere il contenuto di alcuni nuovi campi e differenziare così l'accesso (ad esempio un abbonato può prestare la propria SIM card ad un amico fornendogli il solo PIN; sarà così sicuro che questo, pur potendo telefonare, non potrà usufruire di tutti i servizi che richiedono invece il PIN2). Chiaramente, esiste anche un **PUK2** con le stesse funzionalità del PUK.

- *Rubrica telefonica* dell'abbonato
- *Messaggi SMS* dell'abbonato
- Lista degli *operatori GSM preferenziali* scelti

La SIM card può memorizzare 100 numeri telefonici (per ognuno sono disponibili 12 caratteri alfanumerici descrittivi), 10 messaggi **SMS** (queste quantità possono comunque variare secondo le specifiche implementazioni delle case produttrici) e una lista degli operatori GSM preferenziali dell'abbonato. Ogniqualvolta non é più presente il segnale della rete su cui si é registrati, il sistema GSM provvede in modo automatico a chiedere l'accesso alla prima delle reti indicate in questa lista; se la registrazione ha esito negativo, provvede a rieseguire la stessa operazione con la successiva, e così via. La procedura continua ciclicamente fino alla avvenuta registrazione su una rete.

[9] Il **codice ESN** é un numero di 11 cifre: le prime tre identificano il costruttore, quindi due cifre sono di uso riservato (spesso sono poste a zero), le restanti sei cifre sono un numero seriale che identifica il terminale

- Campi informativi previsti dalle specifiche **GSM Phase 2**

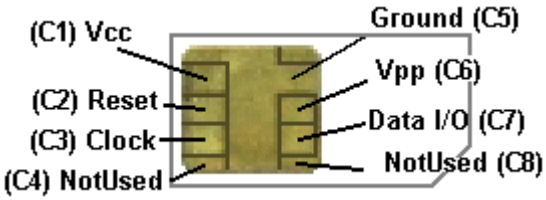
Il processore contenuto nella SIM card tipicamente è una **CPU a 8 bit** e di alcuni Kbytes di memoria (di tipo RAM, ROM ed EEPROM), in tecnologia CMOS:

- la *Read Only Memory* (ROM) contiene il sistema operativo, il sistema amministrativo (che gestisce i servizi GSM Phase II) e gli algoritmi di sicurezza A3 e A8;
- la *Random Access Memory* (RAM) é usata per l'esecuzione degli algoritmi e come buffer per la trasmissione dei dati;
- la *Electrically Erasable Programmable Read Only Memory* (EEPROM) contiene tutti i dati dell'abbonato (già elencati in precedenza);

Un grosso problema per le tutte le SmartCard è rappresentato dal degrado subito dalle EEPROM nelle fasi di lettura/scrittura, il che ne consente un utilizzo limitato nel tempo (solitamente viene garantito il funzionamento corretto di una SIM card GSM per circa due anni). Le celle di memoria contenute nelle normali EEPROM attualmente in commercio possono infatti sopportare al massimo 10.000 cicli di lettura/scrittura. Per particolari applicazioni sono state sviluppate delle SmartCard che riescono ad elevare questa soglia a 100.000 cicli.

## Interfacciamento elettrico e contatti

La *SIM card* ed il *terminale mobile* (ME) in cui è inserita si interfacciano mediante otto contatti elettrici, denominati da C1 a C8. La loro posizione sulla SIM e le loro dimensioni sono rigidamente fissate e sono quelle indicate nella figura seguente:




*Contatti elettrici sulla SIM card*

I contatti C4 e C8 non sono utilizzati dallo standard GSM, ma, essendo la SIM una carta multi-applicazione, potrebbero però essere utilizzati da altre applicazioni in futuro.

La tensione di alimentazione di una SIM Card di phase I è **5 volt**. Per ridurre i consumi, le SIM card di **Phase 2** necessitano invece di una alimentazione di soli 3 volt.

Le funzioni dei singoli contatti sono qui di seguito riassunte:

- **C1: Tensione di alimentazione (+Vcc)**
- **C2: Reset (RST)**
- **C3: Clock (CLK)**
  La SIM ammette segnali di clock da 1 a 5 MHz, però non dispone di un "clock interno", per cui il segnale è fornito dal ME.

- **C6: Tensione di programmazione (+Vpp)**
  La SIM card non necessita di una tensione di programmazione. Il contatto C6 può non essere presente nel ME, nel caso in cui lo sia la sua tensione è sempre posta a Vcc, mai a massa (**C5** - Ground).
- **C7: Data Input/Output**

## MOBILE EQUIPMENT (ME)

Il codice **IMEI** (*International Mobile Equipment Identity*) identifica in modo univoco un *Mobile Equipment* (ME). E' quindi cablato nel ME, in modo sicuro, direttamente dal costruttore.

I codici IMEI e IMSI sono completamente indipendenti l'uno dall'altro.

L'IMEI, che ha una lunghezza massima di 15 cifre, serve ad identificare il modello del telefono (campo **TAC** - 6 cifre), il luogo di costruzione e assemblaggio finale (campo **AC** - 2 cifre), il numero seriale (campo **NR** - 6 cifre):

**IMEI = TAC / FAC / SNR / sp**

### *Trasmissione discontinua (DTX)*

Nel corso di una normale conversazione, si è stimato che la comunicazione in una direzione occupa meno del 50% del tempo totale. Per il resto, il trasmettitore continuerebbe a codificare e trasmettere solo il rumore di fondo. La **trasmissione discontinua** (**DTX** - *Discontinuous Transmission*) sfrutta questo risultato disattivando la trasmissione durante i periodi di silenzio. Si ottiene così di risparmiare potenza ed anche di minimizzare le interferenze di co-canale. Questa funzione è implementata obbligatoriamente nelle MS.

E' stato verificato, però, che la soppressione di qualsiasi segnale risulta sgradevole all'utente che ascolta: esso ha infatti la sensazione che la conversazione sia terminata, quando invece non è così. Di conseguenza, durante i periodi di non trasmissione, la MS dell'utente ricevente introduce del rumore (detto **comfort noise**) che sia simile a quello dell'ambiente del trasmettitore, in modo che l'ascoltatore non abbia la sgradevole sensazione di interruzione della comunicazione.

Da quanto detto scaturisce che una fondamentale funzione di un ME sia la **Rilevazione di Attività Vocale** (*Voice Activity Detection*): il sistema deve essere in grado di distinguere tra la voce e il rumore di fondo, compito tutt'altro che semplice.

### *Controllo dinamico della potenza (Dynamic Power Control, DPC)*

I terminali GSM sono suddivisi in **cinque classi** in base alla massima potenza con cui possono trasmettere sul canale radio (**MSMaxTxPwr,** *Mobile Station Maximum Transmission Power*). Il valore massimo di potenza trasmissibile non è specificato, mentre esiste un valore minimo di 0.8 Watt.

La seguente tabella riassume queste cinque classi.

| CLASSE | MSMaxTxPwr | TIPO |
|---|---|---|
| 1 | ..... | Veicolare |
| 2 | 8 Watt (39 dBm) | Portatile |
| 3 | 5 Watt (37 dBm) | Palmare |
| 4 | 2 Watt (33 dBm) | Palmare |
| 5 | 0.8 Watt (29 dBm) | Palmare |

Per minimizzare le interferenze tra canali attigui e risparmiare potenza, sia il *terminale mobile* sia la *stazione base* operano al valore minimo di potenza che assicura ancora un accettabile livello del segnale ricevuto (**RxLev**). La potenza di emissione sul canale radio può variare in modo dinamico su **32 livelli**, dal valore massimo (per la classe di appartenenza) ad un minimo di 5 dBm, a passo di 2 dB.

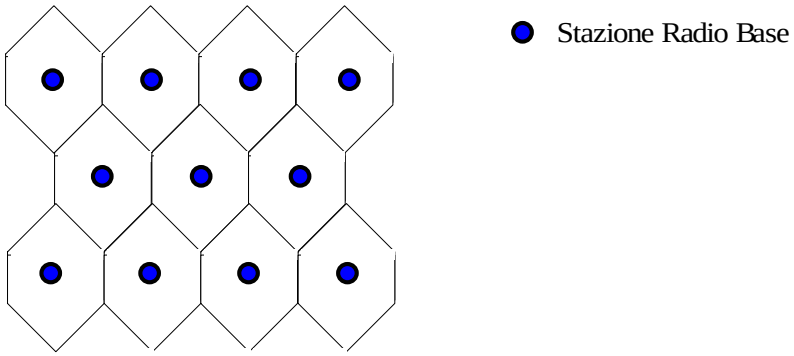
La MS misura l'intensità e la qualità del segnale e trasferisce queste informazioni alla stazione radio base (come vedremo in seguito, questo avviene attraverso un apposito canale denominato **SACCH**), che decide se e quando cambiare il livello di potenza. In particolare, la BTS informa la MS della massima potenza che può utilizzare nella comunicazione (anche se quest'ultima potrebbe trasmettere a potenza maggiore). Ad esempio, nelle zone urbane dove le celle sono piccole e ravvicinate, la massima potenza è solitamente 33 dBm (2 Watt) così da evitare che gli apparati con potenza superiore ai 2 Watt (ad es. i veicolari) trasmettano a pieno regime creando forti interferenze di cocanale.

# Network Subsystem (NS)

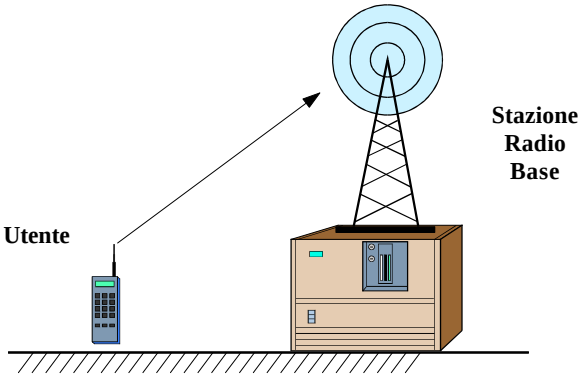
## INTRODUZIONE

Il **sottosistema di rete** (*Network Subsystem*), identificato a volte come *Intelligent Network*, fornisce diversi servizi. Vediamoli nel dettaglio.

Abbiamo detto che l'area di copertura della rete GSM è divisa in un numero elevato di **celle**, ciascuna servita da una **stazione radio base** (BTS, Base Transceiver Station):




Quando un utente vuole effettuare una conversazione, il suo "telefonino" si mette in comunicazione con la BTS che *serve* la cella in cui l'utente stesso si trova:



La comunicazione avviene via radio ed è importante sottolineare che si tratta dell'unico caso di collegamento via radio. In altre parole, ***nella rete GSM l'unico collegamento radio è quello che avviene tra i terminali mobili e le stazioni radio base, mentre ogni altro collegamento avviene via cavo.***

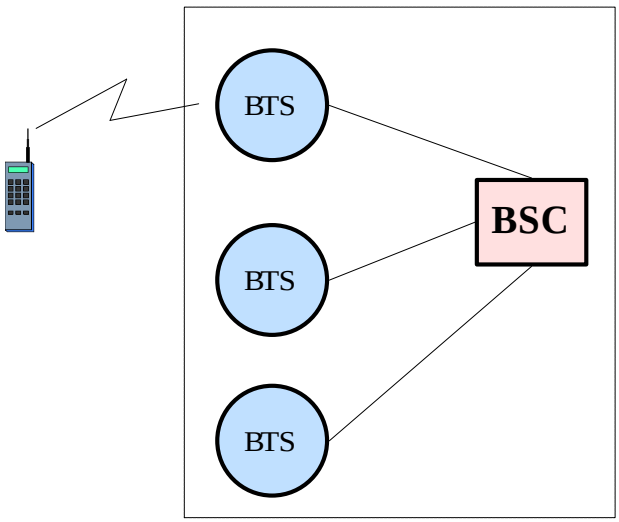
Il motivo di questo fatto è duplice:

- in primo luogo, tranne la comunicazione terminale-BTS tutte le altre comunicazioni avvengono tra unità funzionali della rete che non devono quindi avere il requisito della mobilità, il che permette di effettuare il collegamento tra queste unità in modo cablato;
- in secondo luogo, la banda trasmissiva offerta dai collegamenti via cavo può essere scelta a proprio piacimento (basta scegliere il tipo di cavo) e quindi risulterà senz'altro maggiore della banda radio che viene messa a disposizione per il sistema GSM.

In aggiunta a queste osservazioni, si deve considerare che la maggior parte delle reti di telecomunicazioni, inclusa la rete GSM, hanno bisogno di scambiare, tra le proprie unità funzionali, non solo i dati veri e propri (nel caso del GSM, le conversazioni telefoniche), ma anche le cosiddette **informazioni di segnalazione**, necessarie per la cooperazione tra le varie unità. Per lo scambio di queste informazioni, la soluzione più efficiente è quella di usare dei canali appositi (**canali di segnalazione**): ad esempio, se un dato canale fisico di comunicazione (via radio o cablata) è gestito con la tecnica FDM (multiplazione a divisione di frequenza), uno o più canali logici saranno destinati alla segnalazione e gli altri canali logici ai dati veri e propri. In particolare, la rete GSM (insieme ad altre reti) usa una *rete dedicata* per la segnalazione, che cioè trasmetta solo le informazioni di segnalazione. Tale rete è nota con la sigla **SS7**.

Ogni BTS comunica con la propria *Base Station Controller* (**BSC**), secondo lo schema della prossima figura. L'interfaccia di comunicazione tra le due entità, detta **A-bis**, è standardizzata.

Il sistema è composto da un certo numero di BSC, ciascuna delle quali controlla a sua volta un certo numero di BTS:

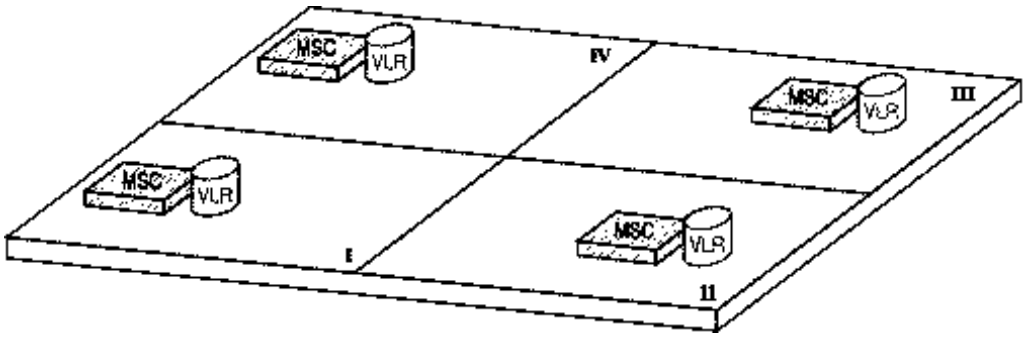



L'insieme di una BTS e della BSC da cui è controllata prende il nome di **stazione base** (BS, *Base Station*).

Ogni BSC è a sua volta collegata ad una delle unità principali della rete, il cosiddetto **Mobile Services Switching Center** (**MSC**). Ogni operatore mobile dispone di un certo numero di MSC sparsi sul territorio: ad esempio, la TIM dispone, in Italia, di circa 40 MSC.

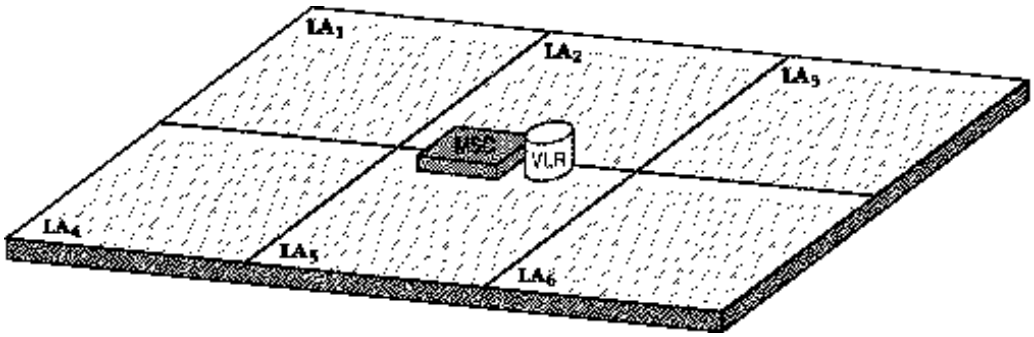
L'MSC ha diverse funzioni. Prime tra tutte, quella di individuare la posizione di un utente che sia destinatario di una chiamata e quella di instradare le chiamate provenienti dagli utenti[10].

Come detto poco fa, un MSC ha in carico una certa area del territorio, detta **MSC/VLR service area**:




*Suddivisione del territorio in **MSC/VLR service area***

Ogni *MSC/VLR service area* è a sua volta suddivisa in un certo numero di **location area**:




*Suddivisione di una MSC/VLR service area in diverse **location area***

A sua volta, ogni location area è divisa in un certo numero di celle.

Il compito dell'MSC è quello di sovrintendere al funzionamento di tutte le BSC della sua *MSC/VLR service area*, ossia quindi di servire tutte le MS che transitano in quell'area.

Immaginiamo allora che un utente voglia effettuare una comunicazione. La sua richiesta arriva (via radio) alla BTS della cella in cui l'utente stesso si trova; la BTS trasmette la richiesta alla propria BSC e questa, a sua volta, la trasmette al proprio MSC. L'MSC ha adesso il compito di individuare la posizione dell'utente chiamato.

Per fare questo, cioè in generale per gestire la **mobilità** degli utenti, l'MSC deve scambiare delle informazioni con dei **database** che gli consentano di individuare la posizione dell'utente chiamato.

La prima comunicazione avviene tra l'MSC e uno dei database centrali posseduti da ciascun operatore e denominati **Home Location Register** (**HLR**). Ognuno di questi database ha in carico un certo numero (abbastanza elevato) di utenti e per ciascuno di questi utenti memorizza, in modo permanente, le seguenti informazioni:

[10] In generale, essendo il sistema radiomobile GSM una rete pubblica di telecomunicazioni, che quindi deve comprendere delle centrali di commutazione che si occupino dell'*instradamento* delle chiamate, è proprio l'MSC a comportarsi da centro di commutazione.

- i dati di abbonamento (noti come *statici*);
- i dati (detti *dinamici*) che possono variare a seguito di azioni degli utenti stessi (attivazione servizi supplementari, ecc.);
- l'identità del **VLR** (**Visitor Location Register**) presso cui la MS dell'utente è registrata come "visitor".

Andiamo con ordine.

In primo luogo, l'MSC è in grado di individuare l'HLR di appartenenza dell'utente che chiede di effettuare la chiamata: l'associazione tra l'utente ed il corrispondente HLR avviene semplicemente in base alle prime cifre del numero telefonico dell'utente stesso (per prime cifre intendiamo quelle successive alla combinazione iniziale **03** che è comune a tutti gli utenti: **03**38-..., **03**47-...., **03**29-...).

Una volta individuato l'HLR dell'utente che vuol chiamare, l'MSC verifica che l'utente stesso sia autorizzato a richiedere il servizio[11]. In caso affermativo, l'MSC passa alla fase di individuazione dell'utente che si vuol chiamare.

Anche in questo caso, in base al numero telefonico di tale utente, l'MSC risale all'HLR di appartenenza dell'utente chiamato ed entra in comunicazione con esso. Tra le varie informazioni che l'MSC chiede all' HLR c'è l'identità del **VLR** in cui l'utente risulta temporaneamente registrato.

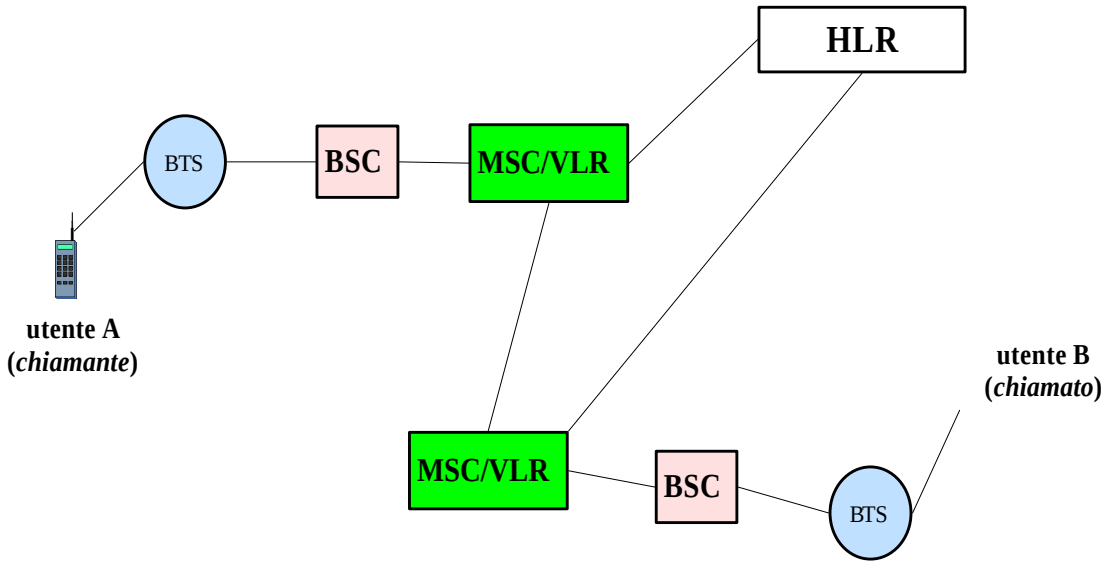
Il problema da considerare è il seguente: quando un utente acquista una SIM card, esso viene registrato come appartenente ad una data regione geografica, servita da un preciso HLR; l'utente, però, può spostarsi in qualunque regione, che può non essere quella coperta dal suo HLR. Di conseguenza, è necessario predisporre un certo numero di *database secondari* (rispetto agli HLR), ciascuno dei quali controlla una determinata area e conserva tutte le informazioni degli utenti che, in ogni istante, si trovano in tale area. La suddivisione che si considera è quella rispetto alle già citate **MSC/VLR service area**: in pratica, ognuna di queste aree è servita da un MSC e da un VLR.

In generale, è possibile che un VLR controlli più *MSC/VLR service area*, ma una serie di motivi tecnologici spingono ad integrare fisicamente, nello stesso sito, l'MSC ed il corrispondente VLR, il che significa che c'è un VLR per ciascuna *MSC/VLR service area*, da cui appunto questa denominazione.

Quando un utente entra in una *MSC/VLR service area*, il VLR di quell'area individua l'HLR di appartenenza dell'utente e preleva da esso le informazioni (IMEI, numero telefonico, parametri di autenticazione, ecc.) dell'utente stesso, registrando quest'ultimo come *visitatore*. Contemporaneamente, l'HLR di appartenenza dell'utente registra su quale VLR sono state inviate le informazioni, il che evidentemente consente l'individuazione dell'utente stesso.

Possiamo quindi tornare al problema di partenza: avevamo un utente A che aveva chiesto di comunicare con un altro utente B ed avevamo un MSC (quello cui fa riferimento A) che aveva interpellato l'HLR di B per conoscere la posizione di B:

[11] L'HLR è semplicemente un database e quindi memorizza i parametri di sicurezza, ma non provvede alla loro generazione. Il compito di calcolare, tramite degli appositi algoritmi, questi parametri è demandato ad una unità funzionale denominata **Authentication Center** (**AuC**).




L'MSC legge, nell'HLR di B, su quale VLR l'utente B risulta attualmente registrato. Entra quindi in comunicazione con tale VLR e con il corrispondente MSC. Quest'ultimo ha adesso il compito di individuare l'utente B all'interno della propria *MSC/VLR service area*. Ci sono allora due possibilità:

- la prima è quella in cui l'utente B sta "parlando" in quel momento: in questo caso, l'MSC sta inevitabilmente già comunicando con esso, per cui ne conosce la posizione esatta, ossia sostanzialmente la BTS che lo sta servendo;
- la seconda è quella invece in cui l'utente B non è comunicazione: in questo caso, l'MSC trasmette, in broadcast, le informazioni a tutte le BTS da esso controllate, fin quando non riceve risposta da parte della BTS che individua l'utente B all'interno della propria cella. Quando questa individuazione avviene, la comunicazione può partire.

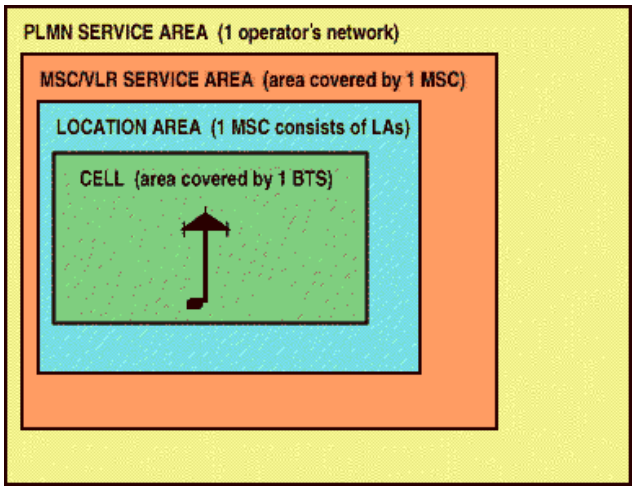
## MOBILE SERVICES SWITCHING CENTER (MSC)

Abbiamo dunque capito che il componente centrale del sottosistema di rete é il centro di commutazione **MSC** (*Mobile services Switching Center*). Esso svolge le funzionalità di un normale *nodo di commutazione* di una rete, vale a dire essenzialmente instaurare, instradare, controllare e tassare le chiamate da/verso le MS presenti nell'area geografica da esso servita. In più, esegue tutti quei compiti essenziali per gestire la mobilità degli utenti. Come si è visto, queste funzioni sono eseguite in collaborazione con le altre entità del network subsystem.

L'MSC fornisce anche la connessione con le reti fisse, che possono essere così classificate:

- *Public State Telephone Network* (**PSTN**): rete pubblica (generalmente analogica) per la telefonia fissa;
- *Integrated Services Digital Network* (**ISDN**): rete digitale di servizi vari (inclusa la telefonia);
- rete dati a commutazione di pacchetto (**PSPDN**, *Packet Switched Public Data Network*) o di circuito (**CSPDN**, *Circuit Switched Public Data Network*).

L'insieme degli MSC costituisce essenzialmente la **rete pubblica mobile terrestre** (**PLMN**, *Public Land Mobile Network*):




## GATEWAY MOBILE SWITCHING CENTER (GMSC)

Abbiamo detto poco fa che l'MSC fornisce la connessione tra la rete GSM e le altre reti telefoniche/telematiche, sia fisse sia mobili. Vediamo allora con maggiore dettaglio cosa significa questo.

Per semplicità, consideriamo il caso di un utente della rete fissa che voglia effettuare una chiamata ad un utente della rete GSM. Questa chiamata viene per prima cosa inoltrata dalla rete telefonica fissa ad un particolare MSC, chiamato **Gateway MSC** (**GMSC**): questa unità costituisce il vero punto di accesso alla **PLMN GSM** (*Public Land Mobile Network*) a cui appartiene l'utente mobile chiamato. Il GSMC segue un criterio in qualche modo già visto in precedenza: esso, infatti, va ad interrogare il registro HLR dell'abbonato, che a sua volta interroga il corrispondente registro VLR; in questo modo, viene individuata la posizione (a livello di *MSC/VLR service area*) dell'utente e quindi il GMSC può instradare la chiamata verso il centro MSC che controlla la zona nella quale si trova l'abbonato chiamato.

Questo meccanismo non vale solo per una chiamata da rete fissa a rete mobile, ma anche quando entrambi gli utenti appartengono ad una rete mobile, purché ovviamente di operatori diversi: ad esempio, una chiamata tra un utente TIM ed un utente OMNITEL o viceversa.

## EQUIPMENT IDENTITY REGISTER (EIR)

Per cercare di risolvere il problema del possibile utilizzo di apparati mobili ME rubati, difettosi o non omologati, esiste una unità funzionale, detta **Equipment Identity Register** (**EIR**), che memorizza al suo interno tutti i codici IMEI segnalati come difettosi o rubati. La rete può così effettuare un controllo sull'IMEI richiedendolo alla MS e vietarne l'accesso nel caso questo non sia in regola.

## HOME LOCATION REGISTER (HLR)

Come già detto in precedenza, *l'**HLR** costituisce il database su cui un gestore di rete GSM memorizza, in modo permanente, i dati relativi agli utenti che hanno sottoscritto un abbonamento presso di lui.* Ogni azione di tipo amministrativo che il gestore di rete effettua sui dati di utente viene svolta attraverso l'HLR.

Ad ogni HLR viene associato un identificativo (**HLR number**): questo serve affinché tutti i VLR, ricevendo in carico una nuova MS (cioè una MS che sia entrata nella MSC/VLR Service Area di

competenza), possano sempre sapere quale sia l'HLR di appartenenza di tale utente. A sua volta, ogni VLR è identificato da un **VLR number**, in modo tale che l'HLR sappia presso quale VLR è registrata correntemente ogni sua MS.

Poiché una rete GSM è interconnessa con altre reti (PSTN, ISDN, altri PLMN), essa deve prevedere un piano di numerazione con esse compatibile. Ad ogni MS è assegnato un **numero di telefono** (**MSISDN**), che identifica univocamente un abbonato nel piano di numerazione della *rete telefonica commutata pubblica internazionale*, in conformità con le **specifiche E.164** sulla numerazione per reti **ISDN** (naturali sostitute delle tradizionali PSTN).

L'MSISDN ha una lunghezza massima di 15 cifre con la seguente struttura:

**MSISDN = CC / NDC / SN**

dove

- **CC** (*Country Code*) è il prefisso internazionale secondo le specifiche E.163 (per Italia: 39);
- **NDC** (*Nation Destination Code*) è l'identificativo di una PLMN GSM in ambito nazionale; in Italia, abbiamo ad esempio TIM (alla quale sono attribuiti gli NDC 335, 338, 399) oppure OMNITEL (347,348,349) e così via per gli altri operatori (cioè attualmente Wind e Blutel);
- **SN** (Subscriber Number) è il numero che identifica l'abbonato nella PLMN del proprio operatore.

I codici CC e NDC permettono di identificare l'operatore GSM cui appartiene l'utente, mentre le prime cifre di SN permettono di risalire all'HLR presso cui è registrata la MS.

I principali dati d'utente memorizzati nell'HLR sono i seguenti:

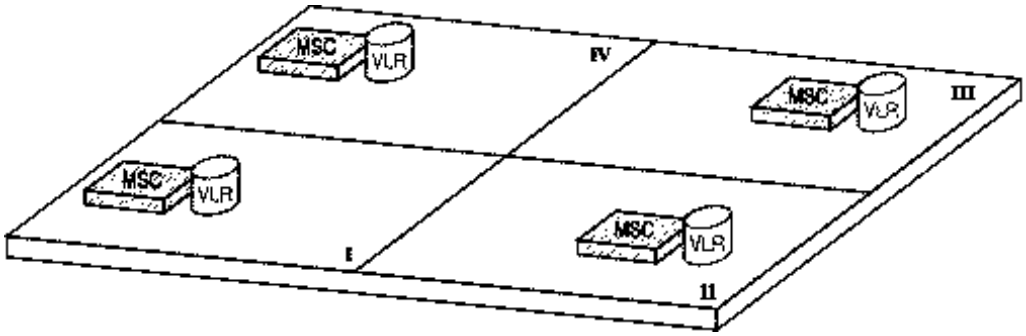
- *International Mobile Subscriber Identity* (IMSI), che identifica univocamente l'abbonato all'interno di una qualunque rete GSM e che é contenuto anche all'interno della SIM card;
- *Mobile Station ISDN Number* (MSISDN), che identifica univocamente un abbonato nel piano di numerazione della rete telefonica commutata pubblica internazionale. Possono essere più d'uno in funzione dei servizi sottoscritti (ad esempio si possono avere numeri distinti per voce, dati e fax);
- tipo e stato dei servizi supplementari e dei servizi sottoscritti dall'abbonato a cui gli é consentito accedere (voce, servizio dati, SMS);
- VLR number, per conoscere il VLR in cui è correntemente registrata la MS.

I principali compiti di un HLR possono essere riassunti come segue:

- sicurezza: dialogo con l'AuC (Authentication Center) e il VLR;
- gestione della localizzazione: dialogo con il VLR;
- informazioni sull'instradamento (MSRN): dialogo con il GSMC;
- gestione dei dati di utente e dei costi delle chiamate;
- gestione dei servizi supplementari (attivazione, disattivazione).

## VISITOR LOCATION REGISTER (VLR)

Il registro VLR contiene e mantiene aggiornate le informazioni relative alle MS che sono presenti, temporaneamente, nell'area da esso servita, secondo uno schema già considerato in precedenza e riproposto nella figura seguente




*Suddivisione del territorio in* ***MSC/VLR service area***

Si tratta di informazioni selezionate dal registro HLR e necessarie per il controllo delle chiamate e la gestione dei servizi supplementari.

I principali dati d'utente memorizzati nel VLR sono i seguenti:

- MSISDN, MSRN e parametri di sicurezza;
- *HLR number*, per poter identificare l' HLR di appartenenza dell'utente;
- *Temporary Mobile Subscriber Identity* (TMSI), usato per garantire la sicurezza del IMSI, viene assegnato ogni volta che si cambia Location Area (LA);
- Stato della MS (spenta, non raggiungibile, ecc.), categoria (operatore, utente ordinario, chiamata di test) ed eventuale priorità;
- Stato dei servizi supplementari (*Call Waiting, Call Divert, Call Barring*, etc.);
- Tipi e stato dei servizi sottoscritti dall'abbonato a cui gli é consentito accedere (voce, servizio dati, fax, SMS, ecc.), detti *bearer e teleservices services*;
- **Location Area Identity** (*LAI*) in cui si trova la MS all'interno di quelle sotto il controllo del MSC/VLR. Ricordiamo, infatti, che ogni VLR controlla una *MSC/VLR Service Area*, la quale è a sua volta divisa in *location areas*, ciascuna individuata da un proprio *LAI*.

## AUTHENTICATION CENTER (AUC)

L'**AuC** è l'unità funzionale del sistema GSM incaricata di generare i parametri necessari per l'autenticazione degli utenti. Si occupa di verificare se il servizio è stato richiesto da un abbonato legittimo, fornendo sia i codici per l'autenticazione sia quelli per la cifratura, per garantire tanto l'abbonato quanto l'operatore di rete da violazioni indesiderate del sistema da parte di terzi.

Il meccanismo di autenticazione verifica la legittimità della SIM (senza trasmettere sul canale radio le informazioni personali dell'abbonato, quali IMSI e chiave di cifratura), al fine di verificare che l'abbonato che sta tentando l'accesso sia quello vero e non un **clone**; la cifratura invece genera

alcuni codici segreti che verranno usati per criptare tutta la comunicazione scambiata sul canale radio[12].

L'AuC contiene il codice IMSI, la chiave di autenticazione (Ki), il codice TMSI corrente e il codice LAI corrente, usati per autenticare e codificare i canali radio, oltre ad un generatore di numeri casuali (RAND) ed agli algoritmi A3 e A8.

L'autenticazione viene sempre effettuata ogni volta che la MS si collega al network: quando riceve o effettua una chiamata, alla scadenza dei location update periodici, alla richiesta di attivazione, disattivazione o interrogazione dei servizi supplementari.

Poiché i dati trattati dall'AuC sono di fondamentale importanza per la rete e per l'utente, vengono normalmente prese particolari misure di sicurezza e protezione per il loro mantenimento.

## EQUIPMENT IDENTITY REGISTER (EIR)

*Nel GSM ogni apparato mobile (ME) è identificato univocamente dal codice IMEI.* L'IMEI è distinto rispetto all'identità della persona che ha sottoscritto l'abbonamento (IMSI). L'EIR é un database che memorizza gli IMEI. Un IMEI può essere invalido quando l'unità mobile risulta rubata oppure quando é di tipo non approvato.

Per consentire all'EIR di operare correttamente, sono state definite diverse "liste", tra le quali citiamo le seguenti:

| | |
|---|---|
| **White list** | contiene gli IMEI di tutti i ME di tipo omologato ed in condizioni operative, presenti nei paesi aderenti al GSM. Sono quindi autorizzati a connettersi alla rete. |
| **Black list** | contiene tutti gli IMEI che sono considerati bloccati (per esempio quelli rubati oppure di tipo non autorizzato) che non sono quindi autorizzati a connettersi con la rete. |
| **Grey list** | contiene tutti gli IMEI marcati come *faulty* oppure quelli relativi ad apparecchi non omologati (a discrezione del gestore). I terminali inseriti in questa lista vengono segnalati agli operatori di sistema mediante un allarme quando richiedono l'accesso, consentendo l'identificazione dell'abbonato che utilizza il terminale e l'area di chiamata in cui si trova. |

Ad ogni tentativo di collegamento di un terminale con la rete, l'MSC mediante l'EIR verifica che il ME non sia contenuto nella *Black list* o *Grey list*, nel qual caso gli viene sbarrato all'accesso alla rete.

L'EIR può essere unico per tutto il sistema oppure può essere implementato in una configurazione distribuita. In genere si preferisce mantenerlo fisicamente separato dalle altre entità (HLR, AuC, etc.) per ragioni di sicurezza. Esso é accessibile anche in modo remoto, da ogni punto della rete, per consentire l'aggiornamento della varie liste in esso contenute. In futuro é prevista l'interconnessione di tutti gli EIR dei vari operatori GSM, per evitare l'utilizzo di apparati rubati, in nazioni diverse da quelle in cui é avvenuto il furto.

[12] Ricordiamo ancora una volta che il tratto in cui il segnale è vulnerabile (ossia intercettabile) è solo quello radio tra apparato mobile e stazione radio base, per cui solo su tale tratto è fondamentale la crittografia delle informazioni.

## OPERATION AND MAINTENANCE CENTER (OMC)

L'**OMC** é l'entità funzionale che permette all'operatore GSM di monitorare e controllare il corretto funzionamento di una parte della rete GSM costituita da uno o più MSC, con i BSC e BTS ad essi associati. L'OMC ha le seguenti funzioni fondamentali:

- gestione delle configurazioni e delle prestazioni di tutti gli elementi che compongono il network GSM (BSC, BTS, MSC, VLR, HLR, EIR ed AUC);
- gestione dei guasti, degli allarmi e dello stato del sistema con possibilità di effettuare vari tipi di test per analizzare le prestazioni e per verificare il corretto funzionamento dello stesso;
- gestione della sicurezza;
- raccolta di tutti i dati relativi al traffico degli abbonati necessari per la fatturazione.

## NETWORK MANAGEMENT CENTER (NMC)

*Il NMC fornisce la visibilità globale di tutte le attività di controllo.* Coordina e gestisce tutti gli OMC presenti nel network. Esso è generalmente installato nella sede centrali di ciascun operatore mobile.

## LE INTERFACCE GSM

Nei precedenti paragrafi abbiamo descritto le principali unità funzionali sulle quali si basa il funzionamento della rete GSM. E' importante stabilire il modo con cui tali unità devono interagire tra loro, ossia sostanzialmente devono scambiarsi informazioni. Le raccomandazioni GSM hanno definito diverse **interfacce** per permettere la comunicazione tra le varie entità del sistema. Ad esse corrispondono protocolli diversi o porzioni specifiche di protocolli generali. Di seguito sono brevemente spiegate le loro principali caratteristiche:

- **Um**: questa interfaccia è quella utilizzata per trasportare la comunicazione tra MS e BTS; si tratta perciò dell'unica *interfaccia radio* del sistema;
- **A-bis**: è l'interfaccia che consente la comunicazione tra BTS e BSC. L'interfaccia A-bis permette il controllo e l'allocazione delle frequenze radio nelle BST.
- **A**: è l'interfaccia posta tra BSS e MSC; gestisce l'allocazione delle risorse radio alle MS e la loro mobilità.
- **B**: questa interfaccia é posta tra MSC e VLR. Generalmente, l'MSC contiene al suo interno il VLR, per cui l'interfaccia diventa interna.
- **C**: l'interfaccia C é posta tra HLR e G-MSC o G-SMS. Ogni chiamata originata al di fuori della rete GSM e diretta ad un MS (ad esempio una chiamata dalla rete fissa PSTN) deve necessariamente passare dal *Gateway* per ottenere le informazioni sull'intradamento e completare la chiamata. Inoltre, l'MSC può opzionalmente trasferire delle informazioni all'HLR sui costi delle chiamate effettuate;
- **D**: l'interfaccia D é posta tra VLR e HLR e serve a scambiare informazioni riguardanti la posizione o la gestione di un MS;
- **E**: questa interfaccia interconnette due MSC; in particolare, essa permette di scambiare i dati riguardanti gli handover, connettendo l'MSC di partenza (detto *anchor MSC*) e quello di arrivo (*relay MSC*);

- **F**: questa interfaccia interconnette un MSC con l'EIR, al fine di verificare lo stato dell'IMEI di un MS;
- **G**: l'interfaccia G interconnette due VLR di due MSC differenti per trasferire le informazioni di un MS, ad esempio durante una procedura di *location update*;
- **H**: l'interfaccia H é posta tra un MSC e il G-SMS e serve a trasferire i *brevi messaggi di testo* (**SMS**);
- **I**: l'interfaccia I interconnette un MSC direttamente con un MS;
- **O**: questa interfaccia interconnette una BSC/BTS con l'OMC.

# Comunicazione ed interfaccia radio

## TECNICHE DI ACCESSO NEL GSM: COMBINAZIONE FDMA/TDMA

Per gestire l'accesso degli utenti alle risorse radio a disposizione, il sistema GSM utilizza una combinazione delle tecniche di multiplazione a divisione di frequenza (FDMA) e di tempo (TDMA).

## MULTIPLAZIONE FDMA E RIUTILIZZO DELLE FREQUENZE

In primo luogo, il GSM utilizza la tecnica **FDMA** per dividere l'ampiezza di banda concessa in **canali**, ciascuno di ampiezza **200 kHz** centrato su una **frequenza portante**. Ad ognuna di queste portanti è associato un numero, detto **ARFCN** (*Absolute Radio Frequency Channel Number*), per identificarle in modo univoco.

Abbiamo visto che, inizialmente, il sistema **GSM standard** (P-GSM) ebbe a disposizione una banda complessiva di **25 MHz**, sia per l'uplink (890-915 MHz) sia per il downlink (935-960 MHz). Ciascuna di queste bande è stata divisa in **124 portanti**, numerate da 1 a 124. Esiste una semplice formula per individuare la generica portante di numero n (ARFCN n):

- $F_{uplink}(n) = 890 + n \cdot 0.2 \quad MHz \qquad 1 \le n \le 124$
- $F_{downlink}(n) = 45 + 890 + n \cdot 0.2 \quad MHz \qquad 1 \le n \le 124$

Il concetto di queste formule è semplice: si parte dalla frequenza più bassa (890 MHz per l'uplink e 935 MHz per il downlink) e si aggiungono 200 kHz per ciascun canale, progressivamente.

Per il successivo sistema **Extended GSM** (E-GSM), sappiamo che le due bande sono state estese a **35 MHz**. Ciascuna è stata allora divisa in **174 portanti**, organizzate nel modo seguente:

- i primi 125 canali (da ARFCN 0 ad ARFCN 124) sono esattamente gli stessi visti prima:
  - $F_{uplink}(n) = 890 + n \cdot 0.2 \quad MHz \qquad 1 \le n \le 124$
  - $F_{downlink}(n) = 45 + 890 + n \cdot 0.2 \quad MHz \qquad 1 \le n \le 124$

- i successivi canali, numerati da 975 a 1023, si ottengono invece nel modo seguente:

  - $F_{uplink}(n) = 890 + (n - 1024) \cdot 0.2 \quad MHz \qquad 975 \le n \le 1023$
  - $F_{downlink}(n) = 45 + 890 + (n - 1024) \cdot 0.2 \quad MHz \qquad 975 \le n \le 1023$

Come sappiamo, all'interno di una stessa nazione, le frequenze portanti sono suddivise tra i vari operatori, sia GSM sia di eventuali sistemi analogici già esistenti (in Italia, ad esempio, la situazione è complicata per la compresenza del sistema analogico **ETACS**).

Gli N canali (frequenze portanti) assegnati ad un operatore sono divisi in M gruppi in modo che ognuno disponga di N/M canali. Ad ogni cella è assegnato un gruppo di canali in modo da diversificare le frequenze utilizzate da celle geograficamente adiacenti. Si definisce **cluster** l'insieme delle M celle adiacenti in cui si utilizzano tutti gli N canali disponibili.

## INTERFERENZA DI COCANALE

Se la distanza tra due trasmettitori che operano sulle stesse frequenze non è sufficientemente grande, può accadere che ad una MS arrivino, sullo stesso canale, i segnali di due o più celle, dando così origine ad un fenomeno di interferenza noto appunto come **interferenza di cocanale**.

## FADING

La propagazione delle onde elettromagnetiche, non avvenendo in uno spazio libero ideale, è influenzata da diversi fenomeni: *riflessione* (contro ostacoli di dimensioni maggiori della lunghezza d'onda del segnale), *rifrazione* (nel passaggio da un mezzo trasmissivo ad un altro, ad es. aria-cemento) e *diffrazione*. Di particolare interesse il fenomeno della riflessione, che può provocare degli improvvisi e momentanei affievolimenti del segnale ricevuto, che vengono indicati come **fading** (evanescenza). Esistono vari tipi di fading:

- il **fading lento** è dovuto alla presenza di grossi ostacoli (colline o grossi edifici) che creano delle zone d'ombra;
- il **fading veloce** è dovuto alla presenza di numerose superfici riflettenti, che fanno giungere all'antenna ricevente numerosi segnali, tutti con fasi diverse. Quando questi sono in opposizione di fase determinano, un **fading profondo**;
- il **fading di Rice** si ha infine quando all'antenna giunge un segnale diretto (l'antenna trasmittente è in visibilità ottica) insieme a diversi segnali riflessi.

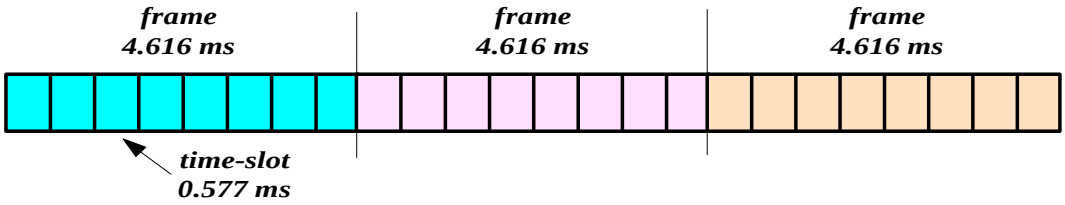
Per ridurre gli effetti del fading vi sono due metodi:

- metodo della **diversità nello spazio** (*antenna diversity*): si utilizzano due antenne riceventi, poste a qualche lunghezza d'onda di distanza. Dato che i segnali ricevuti dalle due antenne compiono percorsi diversi, è meno probabile che entrambe siano affette contemporaneamente da fading;
- metodo della **diversità di frequenza** (frequency diversity): si trasmette lo stesso segnale a frequenze diverse, in modo che, se una frequenza è soggetta a fading, ad un'altra frequenza esso sicuramente non si verifica (dato che cambiano le fasi). Questa tecnica è anche nota come **frequency hopping**.

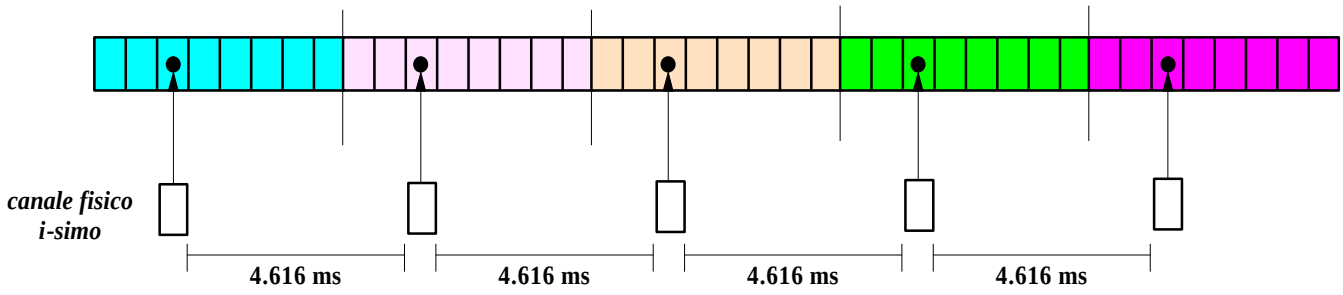
## MULTIPLAZIONE TDMA

Abbiamo detto prima che il GSM usa una combinazione delle tecniche FDMA/TDMA. Con la tecnica FDMA, si divide lo spettro radio a disposizione in un certo numero di canali radio (124 per il GSM standard e 174 per la versione Extended). Consideriamo allora il singolo **canale radio**, di ampiezza 200 kHz.

Ogni canale radio viene diviso nel tempo, secondo la tecnica **TDMA** (*Time Division Multiple Access*), in **frame** (in italiano *trame*), ciascuna della durata di **4.616 ms**; a sua volta, ciascuna trama è divisa in 8 intervalli temporali (detti **time slot**) della durata di **0,577 ms**. Si ha perciò una suddivisione temporale del tipo seguente:

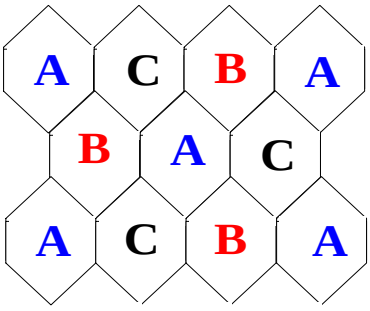


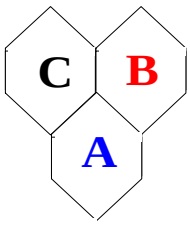

Per il generico canale radio i-esimo, il time slot k-esimo di ogni trama costituisce un **canale fisico.** In altre parole, un canale fisico è costituito dalla successione, a distanza di 4.616 ms uno dall'altro, dello stesso time-slot in ciascuna trama:




Possiamo fare un banale calcolo di quanti canali fisici abbiamo in tutto: dato che abbiamo 124 canali radio, abbiamo 8*124=**992** canali fisici in totale. Tali canali vanno poi distribuiti all'interno del **cluster** di celle, ossia l'insieme di celle adiacenti tra le quali vengono ripartite tutte le frequenze. Si ricordi, in proposito, la figura seguente:

Suddivisione del territorio in ***celle***




***Cluster***: insieme di celle tra cui ripartire tutte le frequenze disponibili

Il conto appena fatto consente di dedurre quante persone, approssimativamente, possono parlare contemporaneamente: se tutti e 992 i canali fossero adibiti a conversazioni, sarebbe possibile mantenere 992 conversazioni contemporanee all'interno di un cluster; se il cluster è composto da M celle, in ogni cella sarebbero permesse 992/M conversazioni contemporanee. In realtà, non tutti i canali sono adibiti al cosiddetto *traffico* (cioè appunto alle conversazioni), ma ci sono anche i *canali di segnalazione*, per cui il numero di utenti contemporanei scende al di sotto di 992/M.

Questa semplice valutazione vale ovviamente solo per la versione del GSM standard. Se invece consideriamo la versione Extended GSM e vi aggiungiamo le frequenze sui 1800 MHz (sistema

DCS), allora i canali fisici disponibili totali sono più di 992. Una stima di massima (ottenuta tenendo conto, oltre che delle considerazioni di cui sopra, anche della presenza dei vari operatori e del fatto che non tutta la banda a disposizione è riservata al GSM, ma viene condivisa con i vecchi sistemi analogici), ci dice che, *all'interno della singola cella, possono parlare circa **250-300** persone contemporaneamente.*

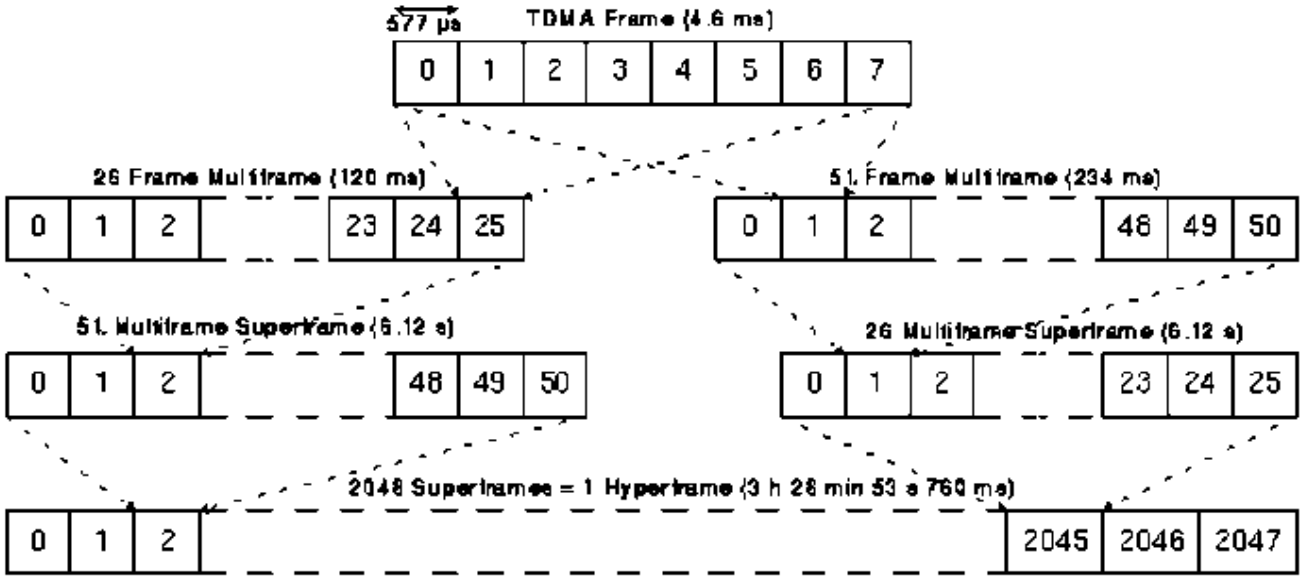
Tornando adesso all'accesso TDM, abbiamo visto una prima suddivisione basata sul TDM. Una ulteriore suddivisione, una specie di *TDMA di secondo livello*, comporta che la sequenza delle trame venga anche divisa periodicamente tra più canali, assegnando una o più trame ad un singolo canale. In base a questa seconda suddivisione, si opera nel modo seguente: i **canali di traffico** (cioè quelli dedicati alle conversazioni vere e proprie) sono organizzati in base a gruppi di **26 trame** (numerate da 0 a 25) mentre i **canali di controllo** (usati per l'instaurazione delle conversazioni) sono organizzati in base a gruppi di **51 trame** (numerate da 0 a 50).

Sia l'insieme delle 26 trame di traffico sia quello delle 51 trame di controllo prendono il nome di **multitrama** (*multiframe*). La multitrama di traffico ha una durata di 120 ms, mentre quella di controllo dura 235,4 ms.

Mettendo insieme 51 multitrame di traffico e 26 multitrame di controllo (per un totale di 1326 trame), si ottiene la cosiddetta **supertrama** (*superframe*), che dura **6.12 s**. Essa consente evidentemente di unificare la struttura dei due canali (traffico e controllo): infatti, la supertrama è costituita da 1326 trame di traffico e 1326 trame di controllo.

A loro volta, 2048 supertrame formano una **ipertrama** (*hyperframe*) composta di $2^{22}$=2715648 trame. Queste trame, come si è detto, vengono numerate progressivamente (**frame number**, FN), ma non all'infinito, bensì in modo ciclico: si usa infatti una periodicità di 3 ore, 28 min, 53 s e 773 ms, trascorsa la quale la numerazione riprende da zero[13].

Lo schema seguente aiuta a comprendere le suddivisioni di cui abbiamo appena parlato:



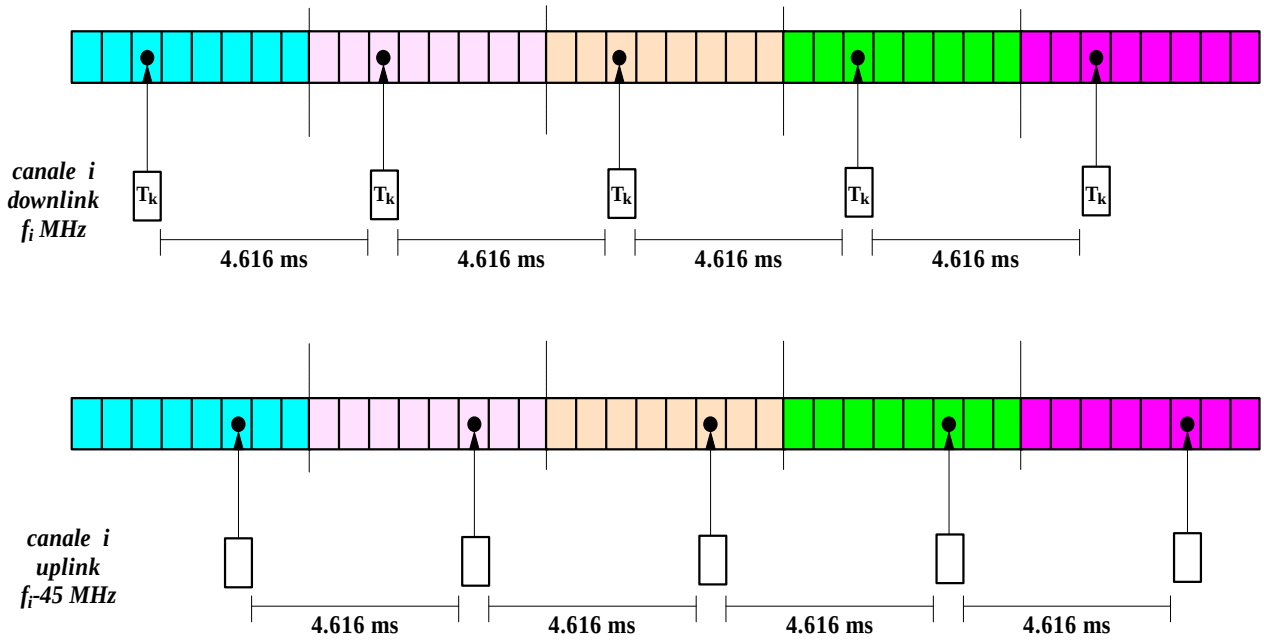

*Struttura TDMA del sistema GSM: una **trama** è composta da 8 **time-slot**; una **multitrama** può essere di traffico (26 trame) o di controllo (51 trame); una **supertrama** è costituita da 51 multitrame di traffico e 26 multitrame di controllo, per un totale di 1326 trame di controllo e altrettante di traffico; una **ipertrama** è costituita da 2048 supertrame ( per un totale di $2^{22}$ trame, ossia $2^{25}$ time-slot). La numerazione (**Frame Number**) avviene solo sulle trame di una ipertrama*

[13] Il motivo per cui si adotta una periodicità di circa 3 ore è che si presume che una qualsiasi conversazione non duri più di 3 ore, per cui è possibile riprendere la numerazione senza creare confusione tra le trame.

In definitiva, si comprende come un canale fisico sia identificato sostanzialmente da 3 parametri:

- numero di time slot (TS);
- numero di trama (FN);
- numero di frequenza portante (cioè numero del canale radio).

Ulteriori considerazioni vanno fatte circa il funzionamento degli apparecchi telefonici (le MS, Mobile Station): per semplificare l'elettronica necessaria in una MS, in modo da non avere simultaneamente trasmissione e ricezione, i canali di uplink (MS→BTS) e downlink (MS←BTS) sono separati nel tempo da 3 time slot. Questo significa quanto segue: una MS che riceva nel time slot $T_k$ della portante $f_i$ MHz, ritrasmetterà nel time slot $T_{(k+3)}$ sulla frequenza $f_i$ - 45 MHz:




Con questo meccanismo, la MS ha a disposizione un tempo pari a 6 time slot per ogni trama, durante il quale può *ascoltare* gli altri canali che riesce a ricevere, in modo da pilotare efficacemente le procedure di **handover**, di cui parleremo più avanti.

Come vedremo meglio in seguito, ai **canali di segnalazione** (che chiameremo BCCH, SCH, FCCH, AGCH, PCH, RACH, SDCCH) è di norma riservato il time slot 0 (per tutte le trame) di una sola delle frequenze assegnate ad una cella in entrambe le direzioni: tale frequenza prende il nome di **portante fondamentale** (o *portante BCCH*) per quella cella.

## FREQUENCY HOPPING

Un'altra caratteristica della gestione dell'interfaccia radio è il cosiddetto *salto di frequenza* (**frequency hopping**, FH): come già accennato in precedenza, si tratta di trasmettere messaggi successivi, di una stessa comunicazione, su frequenze portanti diverse, mantenendo però sempre lo stesso time slot assegnato inizialmente. In questo modo si riescono a combattere efficacemente quei problemi legati direttamente alla propagazione radio, ad esempio *fenomeni di fading* o *battimenti* che si possono verificare, temporaneamente, solo su una certa frequenza.

## MASSIMA DISTANZA TRA BTS E MS

Affinché ci possa essere una comunicazione, la distanza tra stazione trasmittente (BTS) e terminale mobile (MS) non può superare i **35 km** anche quando le condizioni morfologiche del terreno lo permetterebbero (ad esempio in una vasta zona pianeggiante). Vediamo di capire perché.

Quando la stazione base invia un messaggio ad un terminale, può aspettare da questo una risposta solo per un breve periodo di tempo, dopo il quale dovrà passare ad analizzare le altre MS sullo stesso canale, in base alla tecnica TDMA. Se il terminale si trova a più di 35 Km dalla stazione base, la sua risposta arriva troppo tardi e l'utente risulta quindi non raggiungibile.

Per ottenere questo valore di 35 km, basta ragionare nel modo seguente: il sistema GSM riesce a compensare fino ad un ritardo massimo di **233 microsecondi** tra l'invio di un messaggio e la ricezione della risposta; questi 233 μsec corrispondono ad un viaggio BTS → MS → BTS di circa 70 km, in quanto, considerando che la velocità della luce è di 300000 km/sec, si ha

$$233(\mu\text{sec})\cdot 300000\left(\frac{\text{km}}{\text{sec}}\right)=233\cdot 10^{-6}(\text{sec})\cdot 300000\left(\frac{\text{km}}{\text{sec}}\right)\cong 70(\text{km})$$

Quindi, la distanza massima tra BTS e MS dovrà essere la metà di 70 km, ossia appunto 35 km.

## HANDOVER

*Una delle caratteristiche peculiari dei sistemi cellulari è la possibilità di mantenere attiva una comunicazione pur continuando a spostarsi liberamente nel territorio.* Una rete cellulare che non garantisse questa possibilità non avrebbe ragione di esistere.

Questa **mobilità** degli utenti può causare la necessità di cambiare frequentemente cella di servizio oppure canale di trasmissione, per continuare a garantire all'utente una buona qualità del segnale. Questa commutazione automatica, che avviene senza interruzione nel collegamento, è chiamata **handover**.

Esistono quattro tipi differenti di handover nel sistema GSM, che coinvolgono il trasferimento di una comunicazione tra:

- canali (o TDMA time-slot) diversi di una stessa cella, cioè di una stessa BTS;
- celle diverse ma controllate da una stessa BSC;
- celle di diverse BSC, ma controllate da uno stesso MSC;
- celle controllate da diversi MSC.

I primi due tipi, chiamati **handover interni**, coinvolgono solo una stazione BSC. Sono quindi gestiti direttamente dalla BSC, senza coinvolgere l'MSC, eccetto che per notificargli il completamento dell' handover, così da non sovraccaricare inutilmente la rete.

Gli ultimi due tipi, chiamati **handover esterni**, sono invece trattati dagli MSC direttamente coinvolti (uno o due). Nel primo caso, c'è un solo MSC coinvolto; nel secondo caso, invece, gli MSC coinvolti sono due: l'MSC originale, detto **anchor MSC**, continua a rimanere responsabile della maggior parte delle funzioni relative alla chiamata in corso; contemporaneamente, gli handover interni (inter-BSC) che dovessero eventualmente verificarsi saranno gestiti dal nuovo MSC, detto **relay MSC**.

Gli handover possono venire richiesti sia da un MSC (per bilanciare il carico del traffico) sia direttamente dal terminale. Concentriamoci su questo secondo caso: durante i time-slot di inattività (che abbiamo visto essere 6 per ogni trama), la stazione mobile *sonda* i cosiddetti **canali di broadcast** (se ne parlerà più avanti) delle celle geograficamente adiacenti che riesce a ricevere (al

massimo di 16 celle) e compie delle misure sulla potenza che da essi riceve; queste informazioni sono passate, almeno una volta al secondo, alla BSC, la quale prepara una lista delle 6 migliori candidate per un eventuale handover, in base appunto alla potenza del segnale ricevuto. Può capitare, ad esempio, che la MS misuri, dalla BTS che in quel momento la sta servendo, una potenza ricevuta inferiore a quella ricevuta da una o più altre BTS vicine. Questa è una tipica situazione in cui la MS invia una segnalazione alla BSC, richiedendo l'handover.

Si tratta poi di decidere se effettuare l'handover oppure no, usando appositi algoritmi, strettamente vincolati al controllo della potenza. I problemi fondamentali vengono dal fatto che, spesso, la BSC non sa quando una bassa qualità del segnale sia imputabile alle eccessive riflessioni raccolte lungo il percorso oppure al terminale mobile che si è avvicinato ai confini di copertura della cella (questo è tanto più vero quando le celle sono molte e geograficamente vicine, ad esempio nelle zone urbane).

Esistono due algoritmi di base utilizzati per decidere quando effettuare un handover:

- l'algoritmo cosiddetto **Minimum Acceptable Performance** dà la precedenza al controllo della potenza sugli handover: quando la qualità del segnale degrada oltre un certo valore, il livello di potenza del terminale viene aumentato; se questo aumento non produce nessun beneficio, allora si prende in considerazione la possibilità di effettuare un handover. Questo metodo è il più semplice e il più comunemente adottato. Il problema è, però, che continuare ad incrementare la potenza può portare ad avere un terminale che trasmette con elevata potenza, producendo una elevata interferenza di co-canale, fuori dai naturali confini della cella a cui è agganciato (e quindi dentro ad una cella adiacente);
- un'altra possibilità è quella dell'algoritmo **Power Budget**: esso usa gli handover per mantenere o migliorare la qualità del segnale senza aumentare, o addirittura cercando di diminuire, il livello di potenza. Così facendo, non si hanno problemi di `sconfinamenti' e viene anche ridotta l'interferenza tra canali. Lo svantaggio è che si tratta di un metodo molto più complicato da implementare.

Facciamo infine osservare, come si vedrà anche in seguito, che, *quando c'è da effettuare un handover, le informazioni di segnalazione che la MS scambia con la BTS sono in quantità maggiore o minore a seconda di quante unità funzionali sono coinvolte nell'handover stesso:* in altre parole, le informazioni di segnalazione sono poche se bisogna semplicemente passare da una BTS ad un'altra, ma diventano di più quando il passaggio tra due BTS corrisponde anche a cambiare BSC o addirittura MSC; in quest'ultimo caso, le informazioni da scambiare diventano molte, ma il tempo a disposizione è sempre lo stesso (quello massimo affinché l'utente non si accorga del cambio): è necessario perciò usare un canale di segnalazione particolarmente veloce e vedremo che esso corrisponde al cosiddetto **canale FACCH** (*Fast Association Control Channel*).

# I canali logici

## INTRODUZIONE

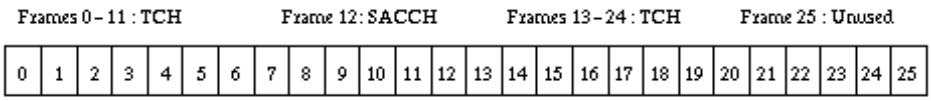
I **canali logici** sono quelli che si ottengono, al fine di trasmettere le conversazioni e le informazioni di controllo, suddividendo lo spettro radio tramite le tecniche FDMA e TDMA descritte nei precedenti paragrafi. Sono dunque tutti dei canali radio. Abbiamo due categorie di canali logici:

- i **canali di traffico** (*traffic channels*, **TCH**), riservati alle conversazioni vere e proprie;
- i **canali di controllo** (*control channels*, **CCH**), riservati alle informazioni di controllo e segnalazione.

## CANALI DI TRAFFICO

I canali di traffico sono quelli che trasportano la voce (codificata) e i dati. Come abbiamo già detto in precedenza, essi sono definiti in base a gruppi di 26 trame, della durata di 120 ms ciascuna. Di queste 26 trame, 24 sono usate per trasportare il traffico, 1 per il SACCH e 1 è ancora inutilizzata.

Possono essere di tipo *Full rate* (TCHf) a 13 Kbps o *Half rate* (TCHh) a 7 Kbps.



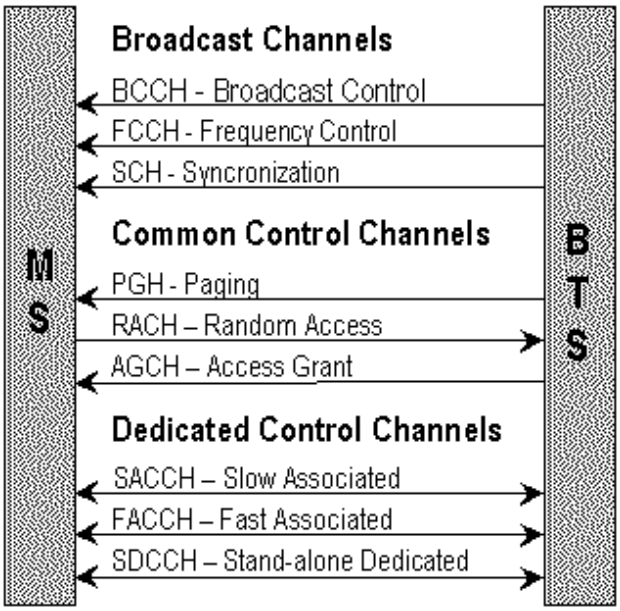

*Struttura TDMA di un canale TCH*

## CANALI DI CONTROLLO

I **canali di controllo** sono a loro volta divisi nel modo seguente:

- **canali broadcast** (*broadcast channels*, **BCH**): sono canali che trasportano informazioni di interesse generale, che tutte le MS possono e devono ascoltare. Le informazioni su tali canali vengono perciò trasmesse in modo monodirezionale downlink (da BTS a MS) punto-multipunto.
- **canali comuni** (*common control channels*, **CCCH**): sono canali che portano informazioni di controllo relative ad una data connessione in una fase preliminare (cui non corrisponde una associazione di un canale di sistema per la connessione). Si tratta ancora di canali monodirezionali, ma alcuni di essi servono per il downlink, mentre altri per l'uplink;
- **canali dedicati** (*dedicated contro channels*, **DCCH**): questi sono canali assegnati ad una connessione per lo scambio di informazioni di segnalazione relative alla specifica connessione.

Una tabella generale, nella quale sono indicati i singoli canali appartenenti alle 3 categorie appena enunciate, è la seguente:




*Classificazione dei canali di controllo (CCH)*

In questa tabella, sono evidenziate, tra l'altro, le direzionalità dei vari canali: si notano alcuni canali monodirezionali (BCH e CCH) ed altri bidirezionali (DCH).

Aggiungiamo, prima di proseguire, una importante osservazione: tutte le informazioni che transitano da una BTS ad una specifica MS viaggiano via radio (come del resto quelle in senso opposto), per cui sono teoricamente intercettabili da chiunque (purché opportunamente attrezzato); questo è il motivo per cui tali informazioni sono cifrate. Quando le informazioni arrivano alla BTS, quest'ultima provvede alla decrittazione, dopo di che le informazioni, viaggiando su cavi protetti, diventano sicure.

## BROADCAST CHANNELS (BCH)

Cominciamo l'analisi dei canali di broadcast (monodirezionali in downlink). Tutti questi canali sono trasmessi dalla BTS sulla **frequenza fondamentale** della cella da essa controllata.

### *Broadcast Control Channel (BCCH)*

Per ciascuna cella, questo canale trasporta informazioni a tutti gli utenti serviti dalla corrispondente BTS. Tali informazioni vengono trasmesse in continuazione e in modo downlink.

Il canale è costituito da 184 byte, che trasportano numerosi parametri, tra i quali: l'identità della cella (**Cell Identity**), dell'area di localizzazione (**Local Area Code**), dell'operatore di rete (MCC e MNC), oltre ai parametri richiesti dall'algoritmo di *Frequency-Hopping*.

Tra le varie informazioni trasmesse, c'è anche l'identità delle BTS più vicine (oltre quella della cella in cui la MS si trova). Questo si rende necessario in quanto, come detto in precedenza, la MS effettua continuamente delle misure della potenza ricevuta sia dalla BTS da cui è servita in quel momento sia dalle BTS vicine. Inviando poi tale misure alla BTS e, successivamente, alla BSC, questa può decidere se e quando passare la MS al controllo di un'altra BTS.

### *Frequency Correction Channel (FCCH) e Synchronization Channel (SCH)*

Entrambi questi canali sono monodirezionali e di tipo downlink.

Il **canale FCCH** trasporta alla MS informazioni per la correzione di frequenza. Consente cioè alla MS di agganciarsi alla portante che le è stata assegnata.

Una volta agganciatasi alla portante, la MS deve individuare, all'interno di quella portante, i frame ed i time slot da usare per il traffico e quelli da usare per il controllo. A tale scopo serve il **canale SCH** che quindi trasporta, in 25 bit, le informazioni per la **sincronizzazione**.

Ogni BTS irradia un solo canale FCCH (trama 0) e un solo canale SCH (trama 1) nel time slot 0 della portante fondamentale della cella.

## COMMON CONTROL CHANNELS (CCCH)

Come già detto, i canali CCCH servono allo scambio delle informazioni durante la fase preliminare di una data connessione. Essi consentono sostanzialmente, ad una MS che ne faccia richiesta, di accedere alle risorse del sistema.

Si tratta di canali monodirezionali, alcuni per il downlink ed altri per l'uplink.

### *Paging Channel (PCH)*

Con il termine **paging** si indica l'evento per cui un utente viene avvisato che qualcuno lo sta chiamando. In realtà, è la MS che viene avvisata di una richiesta di connessione da parte di una MS remota. Quindi, il canale PCH è usato dalla BTS per segnalare ad un terminale mobile l'arrivo di una chiamata.

E' dunque un canale downlink, che però presenta una fondamentale differenza con i canali downlink di tipo broadcast: infatti, mentre in quel caso le informazioni di broadcast vengono trasmesse dalla BTS a tutti i terminali mobili della cella, le informazioni del PCH vengono ancora trasmesse dalla BTS a tutte le MS presenti nella cella, ma sono destinate solo a quella particolare MS che è stata chiamata; di conseguenza, solo la MS che si riconosce nel PCH ricevuto elabora il PCH stesso, mentre tutte le altre se ne disinteressano.

### *Random Access Channel (RACH)*

Quando una MS si è riconosciuta in un PCH (ossia è stata avvisata che qualcuno la sta chiamando), usa il canale RACH per richiedere l'accesso alla rete, in modo da poter rispondere alla chiamata. Si tratta dunque di un canale di uplink, che è gestito tramite il protocollo **slotted-Aloha**.

Può capitare che la MS interessata dalla chiamata sia in quel momento spenta o non raggiungibile. In questo caso, la BTS non riceve il RACH in risposta al PCH precedentemente mandato, dal che deduce che la comunicazione non è attuabile.

### *Access Grant Channel (AGCH)*

Se una MS, ricevendo un PCH, ha risposto con un RACH, la BTS della cella deduce che la comunicazione è attuabile. Tuttavia, prima di allocare alla MS le risorse che ha richiesto (tramite il RACH), la BTS deve necessariamente accertarsi che la MS (l'utente) sia autorizzata a disporre di tali risorse. E' necessaria, cioè, una fase di **autenticazione** dell'utente. Allora, la BTS, dopo aver

ricevuto il RACH, risponde inviando alla MS delle informazioni, tramite all'AGCH, con le quali comunica alla MS che sta eseguendo l'autenticazione e richiede alla MS le proprie "generalità".

Se l'autenticazione viene superata con successo, solo allora la BTS alloca le risorse necessarie alla MS per rispondere alla chiamata.

E' ovvio che questo meccanismo non vale solo quando un utente viene chiamato, ma anche quando esso vuole chiamare. In questo caso, la MS invia direttamente la propria richiesta sul canale RACH, aspettando poi il corrispondente AGCH dalla BTS.

## DEDICATED CONTROL CHANNELS (DCCH)

Una volta attivata una connessione tra BTS e MS, alla stessa connessione vengono riservati, oltre al canale di traffico, dei canali dedicati, cioè specifici per lo scambio di informazioni di segnalazione relative a quella specifica connessione.

### *Stand-alone Dedicated Control Channel (SDCCH)*

Il canale SDCCH viene assegnato ad una MS, mediante una segnalazione sul canale AGCH, quando essa ha inviato una richiesta RACH alla BTS e tale richiesta è stata accolta. In pratica, quando la MS ha ricevuto un AGCH, tramite esso gli viene indicato quale SDCCH dovrà usare per l'autenticazione.

Tramite il canale SDCCH transitano perciò le informazioni necessarie all'autenticazione dell'utente: sostanzialmente, *l'utente dice chi è*. Queste informazioni giungono alla BTS, dalla quale vengono inoltrate, in base ad un meccanismo già descritto in precedenza, all'MSC dell'area interessata; l'MSC interpreta il proprio VLR (o, eventualmente l'HLR di appartenenza dell'utente) per verificare le autorizzazioni di cui dispone l'utente. Se tali autorizzazioni sono valide, allora è l'MSC che assegna all'utente un canale di traffico (TCH) da usare per la comunicazione.

Ci sono però altre informazioni che transitano sul canale SDCCH: superata la fase di autenticazione, esso viene infatti usato per il trasporto dei **messaggi di testo** (**SMS**) in direzione uplink (come è noto dall'esperienza comune, gli SMS possono essere inviati dal terminale verso il destinatario solo con il terminale stesso in *standby* e non nel corso di una chiamata) e per lo scambio delle segnalazioni durante la fase di *location update* (cioè di individuazione della posizione).

### *Slow Associated Control Channel (SACCH)*

Questo canale trasporta informazioni di segnalazione tra MS e rete all'interno di una comunicazione. Quindi, ad ogni comunicazione è associato un canale SACCH. Le informazioni vengono trasmesse periodicamente (ogni 12 trame).

Nella direzione *downlink*, esso trasporta anche i messaggi di testo SMS (che, come è noto, possono essere recapitati sia con il telefono in *standby* sia anche durante una chiamata, al contrario degli SMS in direzione *uplink*, come detto in precedenza) e le informazioni sulle misurazioni effettuate dalla BTS. Esso trasporta anche tutte le informazioni del BCCH, che altrimenti andrebbero perse dalla MS che si è assestata sul proprio canale di traffico.

Nella direzione uplink, invece, trasporta le misurazioni effettuate dalla MS necessarie per un corretto *link monitoring*.

## *Fast Associated Control Channel (FACCH)*

Questo canale viene utilizzato per trasmettere le cosiddette **segnalazioni time-critical**, che cioè non possono attendere di essere inserite nel canale SACCH (che è un canale lento, slow). Si tratta cioè di un canale veloce (fast) da utilizzare in tutti quei casi in cui il ritmo di informazioni di segnalazione da scambiare tra MS e BTS subisce un aumento. Una tipica situazione in cui si verifica questo è una segnalazione di handover.

Proprio per la criticità delle informazioni, il canale FACCH viene occupato in modo asincrono, sopprimendo l'informazione che avrebbe dovuto essere trasmessa.

Autore: **SANDRO PETRIZZELLI**
e-mail: sandry@iol.it
sito personale: http://users.iol.it/sandry
succursale: http://digilander.iol.it/sandry1