Università di Genova
Facoltà di Ingegneria

Architetture e Protocolli per Reti Wireless

3. Reti Radio-mobili Cellulari

3.2 GSM

Prof. Raffaele Bolla

Storia del GSM

- **1982**: La **CEPT** (*Conférence Européenne des Administrations des Postes et des Télécommunications*) crea un gruppo speciale di studio per la definizione di una rete cellulare pan-europea: ***Group Spécial Mobile*** (**GSM**).
- **1985**: Prima definizione della lista degli standard (alla fine saranno 12 volumi per un totale di 1500 pagine solo per lo standard base)
- **1987**: Firma del primo ***Memorandum of Understanding tra Telecom*** in rappresentanza di 12 stati europei. L'accordo permette di
  - Coordinare lo sviluppo delle reti GSM
  - Pianificare l'introduzione dei servizi
  - Coordinare l'instradamento e la tariffazione

Storia del GSM

- **1988**: Nasce l'**ETSI** (***European Telecommunication Standards Institute***) dove il GSM si sposta (gli standard GSM diventano ETSI).
- **1990**: Si decide di applicare lo standard GSM al sistema **DCS1800** (***Digital Cellular System on 1800 MHz***)
- **1992**: Viene rilasciato lo standard GSM il cui acronimo assume il significato di
  Global System for Mobile communications
  Nello stesso anno vengono introdotti i sistemi commerciali

Storia del GSM

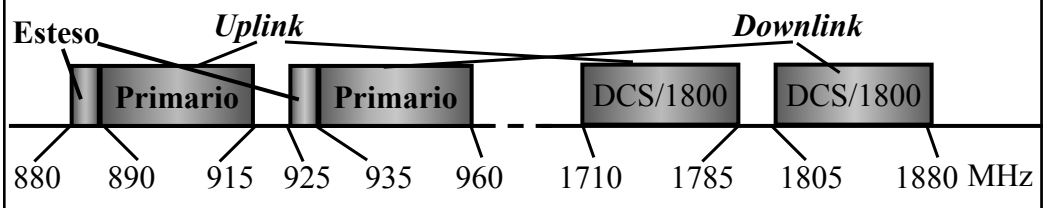
- **1994**: Introduzione degli SMS
- **1995-97**: attivazione del servizio a 1800 MHz
- **1999**: Standard **GPRS** (*General Packet Radio System*) per la trasmissione a pacchetto e primi terminali **WAP** (*Wireless Access Protocol*)
- **2000/01**: Introduzione del **GPRS**
- **2003**: La rete GSM è la rete cellulare di gran lunga più diffusa al modo con 100 Milioni di utenti in Europa e 200 nel mondo. E' anche diffusa negli USA.

Caratteristiche Principali

- Sistema digitale
- Tecnica di accesso multiplo TDMA/FDMA con
  - 8 *time-slot* per portante
  - distanza fra portanti 200 KHz
- Codifica della voce a 13 Kbps (*full rate*) o 6,5 Kbps (*half-rate*)
- Modulazione GMSK
- *Frequency Hopping* (opzionale)
- Controllo di potenza

Frequenze allocate

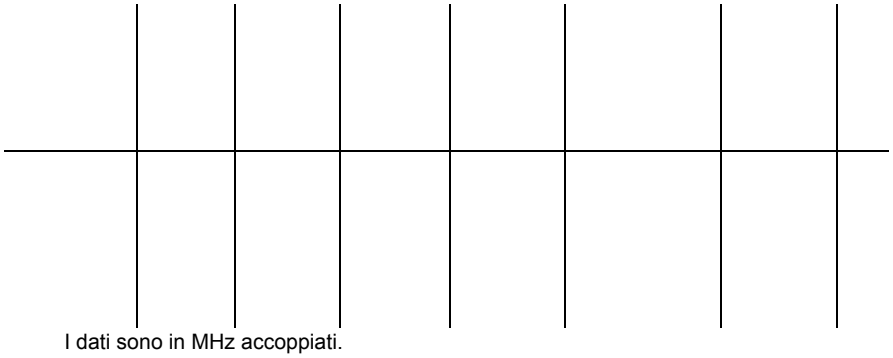
- Le frequenze allocate in paesi non europei possono differenziarsi
- In particolare in USA e UK vengono usate le bande intorno ai 1900 MHz
- I terminali possono gestire una, due o tre bande.



Frequenze allocate

- La tecnica per ottenere il full-duplex è un FDD, ed i canali *uplink* e *downlink* distano:
  - 45 MHz a 900
  - 95 MHz a 1800
- Nella banda dei 900 MHz sono disponibili in totale 124 (primari) + 50 (Estesi) = 174 canali in frequenza full-duplex, pari a 992 canali utente.
- Nella banda dei 1800 MHz sono disponibili 374 canali in frequenza pari a 2992 canali utente.
- Lo spettro è assegnato ai diversi gestori ed anche il residuale servizio ETACS.

Esempio di allocazione fra operatori (Italia)

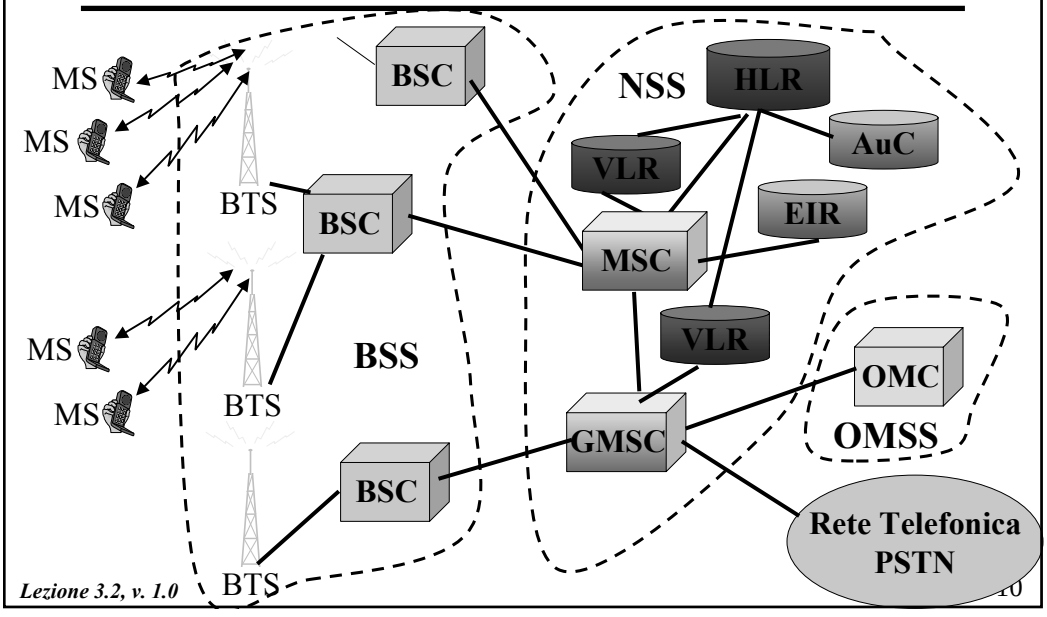


I dati sono in MHz accoppiati.
(1) 3 MHz (a 900 MHz) sono assegnati solo nelle 16 maggiori città.
(2) 2 MHz (a 900 MHz) sono assegnati solo nelle 16 maggiori città.
(3) 5 MHz (a 900 MHz) sono assegnati solo fuori dalle 16 maggiori città.
(4) Tale banda è assegnata temporaneamente fino al 31 dicembre 2002.
(5) 5 MHz (a 1800 MHz) sono assegnati solo nelle 16 maggiori città.
(6) La ponderazione della banda dentro le 16 maggiori città rispetto alla banda nazionale è ottenuta a fini esemplificativi secondo il criterio della popolazione residente (coeff. utilizzato 20%), arrotondando al canale (200 kHz) superiore.

Struttura del GSM

- Si compone di quattro sotto-sistemi che raccolgono entità con compiti funzionali analoghi:
  - **Terminali**
  - ***Base Station Subsystem*** (**BSS**): comprende le entità che svolgono funzioni legate all'utilizzo delle risorse radio
  - ***Network and Switching Subsystem*** (NSS): raccoglie le entità per il controllo delle chiamate e la mobilità degli utenti
  - ***Operation and Maintenance Subsystem*** (OMSS): esercizio e manutenzione della rete.

Struttura della rete



Mobile Station (MS)

- Il terminale mobile del GSM è caratterizzato in particolare dalla suddivisione tra l'apparato e il modulo di identificazione:
  - L'apparato vero e proprio contiene tutte le parti e gli elementi (hardware e software) che non sono legati ad un particolare utente.
  - La parte che rende un apparato "proprietà" di un utente e lo caratterizza nella rete è una smart card che viene chiamata **SIM** (***Subscriver Identity Module***).
- Il GSM è in sostanza è il primo sistema su larga scala che ha attuato questa distinzione fra apparato terminale ed utente.

Terminale

- Tre categorie di potenza:
  - 20 W all'antenna - veicolare (obsoleto)
  - 8 W all'antenna - portatile
  - 2 W (0,8 W per il 1800) all'antenna - *hand-terminal*
- Multi-banda (dual o tri - band)
- Con funzioni potenzialmente molto diverse

Subscriber Identity Module (SIM)

- E' una smart-card, ossia ha un processore e della memoria in cui viene memorizzato
  - Numero di serie (univoco per ciascuna SIM)
  - ***International Mobile Subscriver Identity*** (**IMSI) -** identificativo utente
  - ***Temporary Mobile Subscriber Identity*** (**TMSI**) -identificativo d'utente temporaneo
  - ***Mobile Station International ISDN Number*** (**MSISDN**) - numero di telefono comprensivo di prefisso internazionale
  - ***Location Area Identity*** (**LAI**)
  - ***Subscriber Athentication Key*** - chiave di autenticazione
  - Chiave di cifratura
  - Altre caratteristiche legate all'utente (num. telefonico, servizi abilitati, agenda,…)
  - SMS sia della rete che eventualmente dell'utente

Subscriber Identity Module (SIM)

- Si attiva tramite un codice a 4 cifre (**PIN** - ***Personal Identification Number***).
- Nel caso il codice venga introdotto errato per tre volte consecutive può essere "resettato" tramite l'uso di un secondo codice noto come **PUK** (***Personal Unblocking Key***)
- E' progettata per rendere molto difficoltosa (se non impossibile) la sua duplicazione.

International Mobile Subscriver Identity (IMSI)

- Identifica l'utente
- E' composto da tre campi
  - **MCC**: Mobile Country Code (3 cifre)
    - » 222 è l'Italia
  - **MNC**: Mobile Network Code (2 cifre)
    - » 222-01 TIM Telecom Italia Mobile
    - » 222-10 voda IT Vodafone Omnitel SpA
    - » 222-88 WIND Wind Telecomunicazioni SpA
    - » 222-99 3ITA H3G
  - **MSIC**: Mobile Subscriver Identification Number (identifica la SIM, 10 cifre)
- Il valore dell'IMSI non è in alcun modo correlato al numero di telefono

BSS

- È la parte che controlla e gestisce la parte *wireless* della rete cellulare
- Si compone di due elementi
  - ***Base Transceiver Station*** (**BTS**) che raccoglie tutte le parti di ricetrasmissione
  - ***Base Station Controller*** (**BSC**) che realizza le funzioni di controllo delle risorse radio

BSS - Base Transceiver Station

- Rappresenta il vero punto di accesso alla rete, l'elemento con cui colloquia direttamente la MS.
- E' composta, in sostanza, da tutte le parti che realizzano la trasmissione su canale radio, comprese quelle che realizzano la modulazione/demodulazione, il *frequency hopping* (se presente), la codifica di canale e la cifratura.
- Possiede un numero variabile di interfacce, in genere limitato ad un massimo di 16
- Può avere potenze trasmissive diverse (2,4 a 640 W a 900 MHz, da 2,4 a 40 W per i 1800 MHz)
- Effettua le misure di qualità dei canali (per *handover*) e le invia alla BSC.

BSS - BSC

- Controlla un certo numero di BST, da una ad diverse decine.
- Gestisce i canali radio (li assegna alle chiamate)
- Gestisce l'*handover* fra le proprie BTS e collabora nella gestione di *handover* da una BSC diversa (coordinato dalla MSC)
  - Quindi elabora le misure di qualità delle BTS
- Gestisce il *paging*
- Realizza la codifica GSM-PCM

BSS - BSC

- Si osservi che la rete cellulare GSM al proprio interno ha una struttura molto simile a quella delle reti telefoniche tradizionali.
- In particolare, a partire dalla BSC, il traffico telefonico viaggia nella rete in flussi PCM da 64 Kbps.
- Sulle linee di trasporto tale traffico viene multiplato con metodi tradizionali (PDH, SDH), ma le centrali di commutazione "vedono" flussi sincroni a 64 Kbps.

BSS - BSC

- Anche i collegamenti fra BTS e BSC sono realizzati con flussi sincroni 64 Kbps su canali TDM tradizionali a 2 Mbps
- Ma grazie al fatto che la codifica audio è realizzata sulla BSC, in ogni canale si riescono a trasportare 4 flussi voce.
- Il risparmio di risorse è ingente perché le BTS sono in genere molte (il rapporto medio fra BSC e BTS è di 1 a 10)
- Un ordine di grandezza relativo al numero di apparati su una rete nazionale potrebbe essere 200-400 BSC e 2000-4000 BTS.

NSS

- Viene anche indicato come ***Switching and Management Sub-System*** (**SMSS**)
- Realizza le funzioni di
  - Commutazione dei flussi
  - Gestione delle chiamate
  - Gestione della mobilità
- E' composto da cinque elementi
  - ***Mobile Switching Center*** (**MSC**)
  - ***Home Location Register*** (**HLR**)
  - ***Visitor Location Register*** (**VLR**)
  - ***Equipment Identity Register*** (**EIR**)
  - ***Authentication Center*** (**AuC**)

Mobile Switching Center (MSC)

- E' in sostanza una centrale di commutazione telefonica a cui sono state aggiunte le funzionalità necessarie alla gestione della mobilità.
- Realizza principalmente le funzioni di
  - Gestione della chiamata (controllo, commutazione, autenticazione)
  - Gestione della mobilità
  - Tariffazione
  - *Internetworking*
- La funzione di interconnessione verso altre reti o altri operatori è svolta dalle ***Gateway*** **MSC** (**GMSC**)
- Spesso si distingue fra due tipi di MSC: quelle di transito (che non hanno da gestire BSC direttamente connesse) e quelle di accesso.

Home Location Register (HLR)

- E' una base dati in cui risiedono le informazioni relative a tutti gli utenti (SIM).
- In una rete ce ne può essere più di uno, ma ogni HLR memorizza dati di utenti diversi.
- Possono accedere al HLR solo le MSC e i VLR, anche se appartengono ad altre reti (*roaming* nazionale ed internazionale)

Home Location Register (HLR)

- HLR memorizza per ogni utente:
  - Informazioni statiche, quali:
    - » *International Mobile Subscriber Identity* (IMSI)
    - » MSISDN , ossia il numero di telefono della SIM
    - » La chiave di autenticazione
    - » I servizi supplementari abilitati
  - In modo dinamico
    - » L'indirizzo del VRL presso cui può venir reperito l'utente
    - » *Temporary Mobile Subscriber Identity* (TMSI)
    - » *Mobile Subscriber Roaming Number* (MSRN)

Visitor Location Register (VLR)

- E' un data base anch'esso
- Ce ne è uno ogni MSC
- Contiene le informazioni duplicate dal HRL relative a tutti gli utenti che si trovano all'interno dell'area controllata dalla MSC a cui è associato.
- Quindi le informazioni in esso contenute sono temporanee.
- Il movimento dell'utente da una MSC ad una altra provoca
  - la cancellazione dei dati di tale utente dal VRL origine,
  - la copia dall'HRL degli stessi dati nel VRL di destinazione
  - e infine l'aggiornamento nel HLR del VRL attuale.

Visitor Location Register (VLR)

- VRL gestisce alcuni dati aggiuntivi rispetto al HLR (alcuni dei quali vengono poi inseriti anche nell'HLR):
  - Stato del mobile (libero/occupato …)
  - *Local Area Identity* (LA)
    Ogni VRL (MSC) gestisce più *location area*, quando il mobile passa da una all'altra questa informazione viene aggiornata
  - *Temporary Mobile Subscriber Identity* (TMSI)
  - *Mobile Subscriber Roaming Number* (MSRN)
    usato per instradare una chiamata proveniente da un GSMC.

Temporary Mobile Subscriber Identity (TMSI)

- Usato al posto dell'IMSI per ragioni di sicurezza.
- Al momento della prima registrazione l'utente deve inviare in chiaro alla rete il proprio IMSI per realizzare la procedura di autenticazione.
- Da quel momento in avanti, il VRL assegna un TMSI alla MS che viene cambiato spesso
  - al cambiare di L
  - al cambiare di VLR
  - all'attivazione di una chiamata
- Questo rende difficile un uso improprio dell'identificativo, come ad esempio il rintracciare una chiamata

International Mobile Equipment Identity (IMEI)

- E' un numero identificativo del terminale mobile.
- Lo si può leggere usando il comando ***#06***
- Fino al 1° aprile 2004 a un formato del tipo
  aabbbb-cc-dddddd-e
  - **aa bbbb** è il ***Type Approval Code*** (TAC).
    - » Le prime 2 cifre (aa) rappresentano il codice del paese.
    - » il secondo gruppo di cifre (**cc**) è il ***Final Assembly Code*** (FAC). Identifica il produttore:
      - 01,02 = AEG; 60 = Alcatel; 07,40 = Motorola; 61 = Ericsson; 10,20 = Nokia 65 = AEG; 30 = Ericsson; 70 = Sagem; 40,41,44 = Siemens; 75 = Dancall; 50 = Bosch; 80 = Philips; 51 = Sony, Siemens, Ericsson; 85 = Panasonic
  - **dddddd** rappresenta il ***Device Serial Number*** (SNR)
  - L'ultima cifra (**e**) è una cifra di controllo (solitamente è 0).

International Mobile Equipment Identity (IMEI)

- Dal 1° gennaio 2004 ha un nuovo formato
  xxxxxxxx-dddddd-e
- Il valore di **FAC** è scomparso e il *Type Approval Code* è stato sostituito dal ***Type Allocation Code*** (**TAC xxxxxxxx**)
- **dddddd** ed **e** hanno lo stesso significato che avevano nel vecchio formato
- In alcuni casi sono presenti anche due ulteriori cifre che indicano la versione del software installato.

Equipment Identity Register (EIR)

- E' il database che contiene i dati che servono a validare IMEI e quindi a verificare che la MS usata dall'utente sia conforme allo standard e non rubata.
- Gestisce tre liste di IMEI:
  - **Black**: IMEI di MS rubate o malfunzionanti
  - **Grey**: IMEI di MS con malfunzionamenti non gravi
  - **White**: IMEI di MS corrette
- Viene interrogato dalla MSC, possono essercene più di uno ed ognuno controlla un gruppo di IMEI

Authentication Center (AuC)

- E' il centro preposto alla realizzazione della procedura di autenticazione dell'utente.
- E' normalmente associato ad un HLR.
- Entra in gioco almeno ogni volta che un utente tenta di accedere alla rete (accende il terminale e tenta di fare una chiamata).

Canali logici

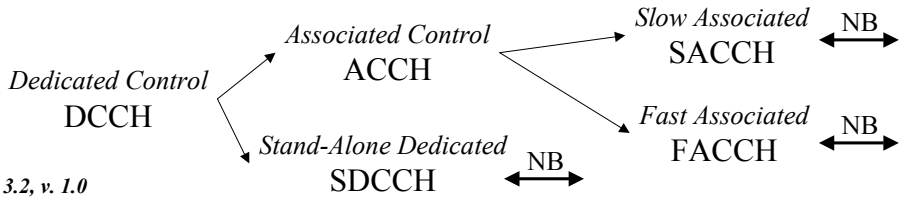
- Il GSM mette a disposizione sulla tratta radio due insiemi di canali logici :
- Canali di Traffico
- Canali di Controllo
- Tali canali sono realizzati utilizzando struttura TDM del canale fisico
- In sostanza le slot vengono opportunamente associate sia in *uplink* che in *downlink* ai diverse canali nel tempo.

Canali di Traffico (TCH, Traffic Channels)

- Ci sono due velocità di riferimento
  - Full Rate: 22.8 Kbps
  - Half rate: 11,4 Kbps
- L'effettivo tasso trasmissivo disponibile dipende poi dal grado di protezione imposto
- A livello base le comunicazioni avvengono tutte nella forma a commutazione di circuito
- Si hanno
  - Canali voce
    - » Full a 13 Kpbs
    - » Helf a 6,5 Kbps
  - Canali dati
    - » Full 2,4; 4,8; 9,6 o 14 Kbps
    - » Half: 2,4 4,8 Kbps

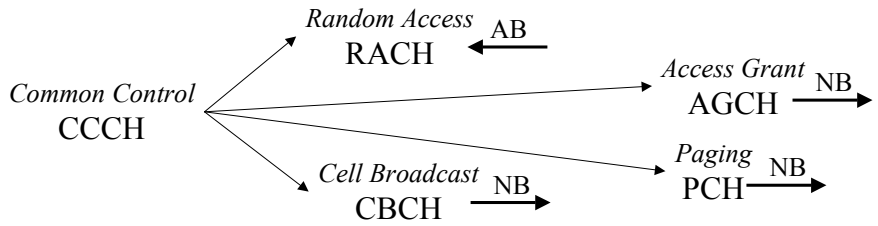
Canali di segnalazione
Dedicated Control Channels

- In generale sono utilizzati ed assegnati ad una singola connessione per il *call-set-up* o per le misure relative all'*handover*
- **SDCCH**: Per il *set-up* e l'aggiornamento della posizione, è attivo prima che il canale di traffico venga allocato.
- **SACCH**: associato ad un TCH (o SDCCH), trasporta le misure per il controllo della qualità del canale, della potenza trasmissiva ed altro.
- **FACCH**: associato ad un TCH (o SDCCH), ruba banda al TCH ed è usato nell'autenticazione e nell'*handover*.



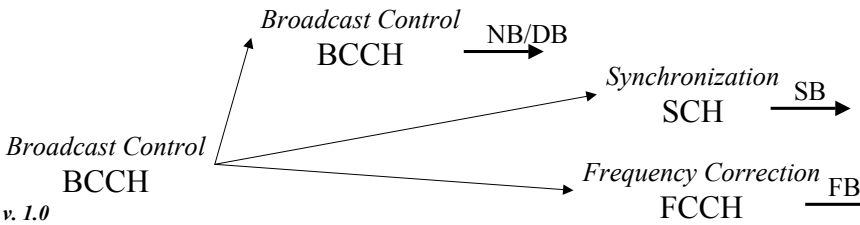
Canali di segnalazione
Common Control Channels

- **PCH**: usato dalla stazione base per il *paging* di chiamata
- **AGCH**: Serve per le comunicazioni stazione base mobile
- **RACH**: Serve per permettere comunicazioni mobile stazione base (è gestito tramite accesso casuale)
- **CBCH**: serve a diffondere comunicazioni broadcast per i mobili in una cella



Canali di segnalazione
Broadcast Control Channels

- **BCCH**: trasmesso nella slot 0 del canale a frequenza più bassa, trasporta informazioni relative alla celle fra cui: *Location Area Identity*, lista celle adiacenti monitorabili, elenco delle freq. usate nella cella, *Cell Identity*.
- **SCH**: permette la sincronizzazione del mobile.
- **FCCH**: permette di correggere la frequenza dell'oscillatore locale.



Trama e slot

time slot (Burst) = 156.25 bits = 577 µs
Di cui 114 bit utilizzabili per rate di 24,7 Kbps
tasso = 270.833 kbit/s

Normal Burst (NB)

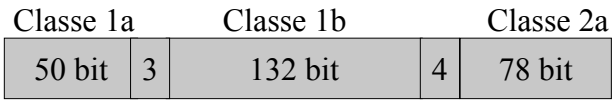
trama = 8 slots = 4.62 ms

multitrama = 26 trame = 120 ms

*: Canali DCCH tranne SDCCH

Le trame sono sfasate di tre slot fra *uplink* e *downlink*

Voce e canali di segnalazione



456 bit per 20 ms di voce

- Questa codifica da origine a 456 bit/blocco * 50 blocchi/s= 22,8 Kbps contro i 24,7 Kbps disponibili
- Considerando l'informazione divisa in slot da 114 bit si può verificare che resta libero una slot ogni 13.
- Infatti 13 slot durano circa 60 ms, periodo durante il quale vengono generati 456 * 3 = 1368 bit, ma 13 slot trasportano in totale 13*114 = 1482 bit; da cui 1482-1368 = 114 bit.

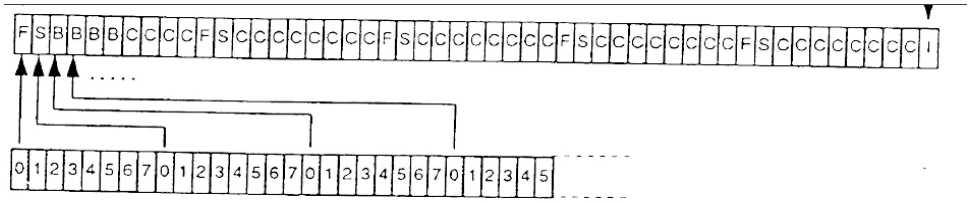
Posizionamento dei canali di controllo

Canali BCCH e CCCH (*downlink*)
Per l'*uplink* il disegno è lo sterro ma tutte le Slot disponibili sono usate per il RACH

F=FCCH
S=SCH
B=BCCH
C=CCCH (PCH/AGCH)
I = IDLE

1 51

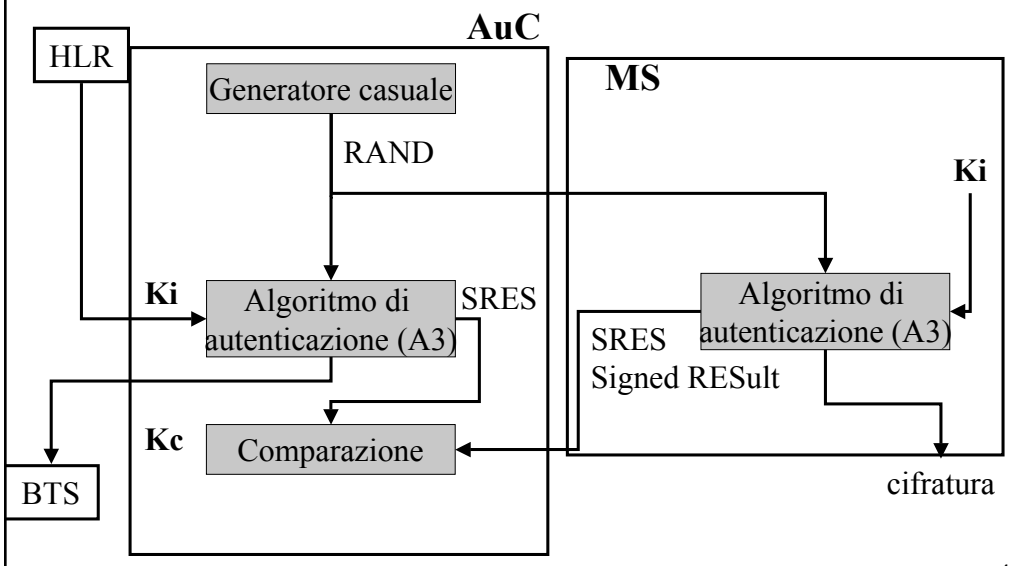
Trame



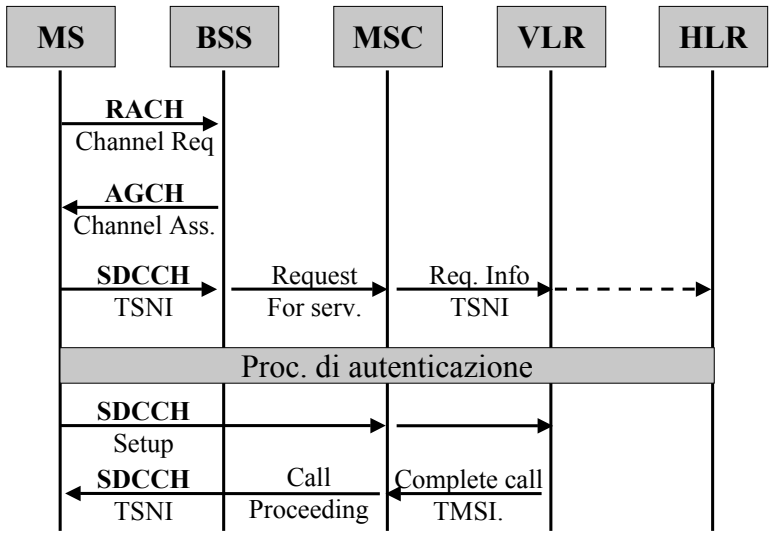
Procedura di Accensione

- Quando la MS dell'utente è spenta il corrispondente IMSI è marcato come *detached* nell'ultimo VRL visitato.
- All'accensione la MS controlla tutte le portanti radio alla ricerca dei canali BCCH migliori (non sono soggetti a *frequency hopping*)
- Individuato il canale usa FCCH e il SCH per sincronizzarsi
- Quindi dal canale BCCH acquisisce le informazioni sulla rete (LAI, …) ed esegue la seguente procedura
  - La MS richiede *Location Updating* inviando l'IMSI
  - Il VRL aggiorna HLR con la nuova locazione e marca IMSI *attached* ed assegna un TMSI.

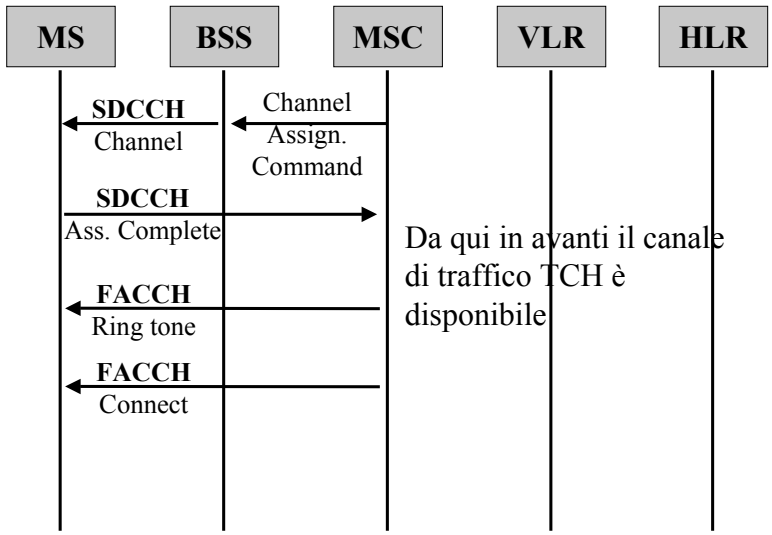
Procedura di Autenticazione



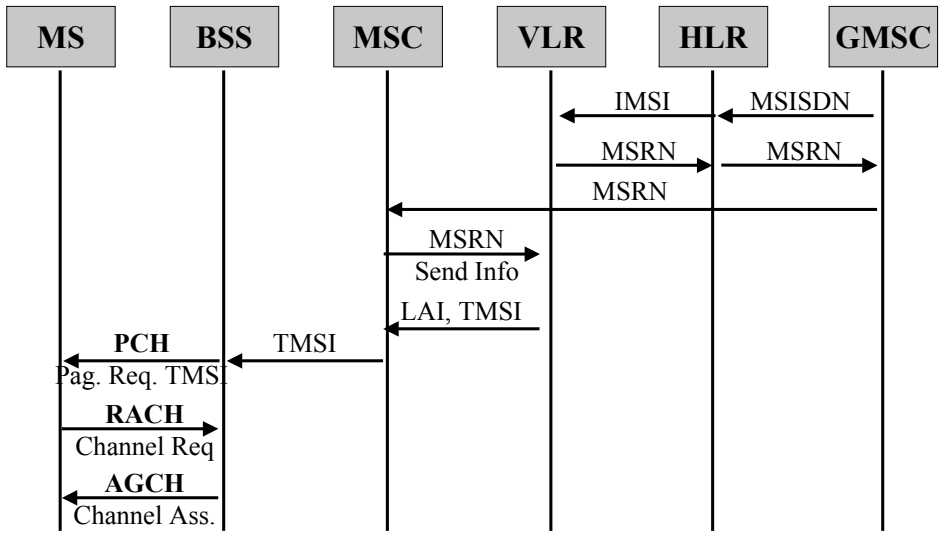
Chiamata da mobile a rete fissa



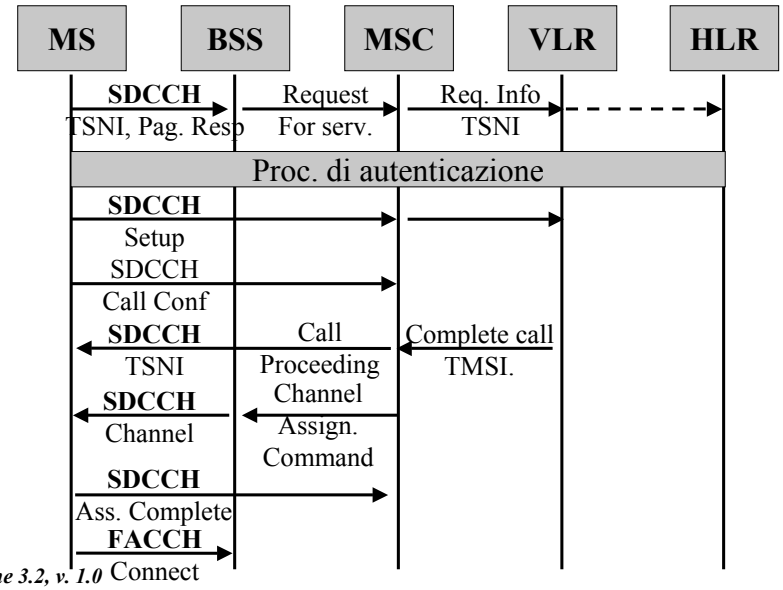
Chiamata da mobile a rete fissa



Chiamata da rete fissa a mobile



Chiamata da mobile a rete fissa



Handover

- La procedura di *handover* serve a realizzare un cambio di canale ed eventualmente di punto di accesso (BTS) durante lo svolgersi di una chiamata in corrispondenza di un abbassamento al di sotto di una certa soglia della qualità del canale utilizzato fino a quel momento
- In generale tale procedura si attiva in corrispondenza dello spostamento da una cella ad un'altra di una MS con una "conversazione" in corso.
- Questa operazione viene gestita dalla BSC sulla base di misure fatte sia dalla MS che dalla BTS.
- Deve essere portata a termine in tempi brevi (100 ms)

Handover - Misure

- Nel corso di una chiamata vengono effettuate le seguenti misure:
- Dalla MS
  - L'intensità del segnale sui sei canali BCCH delle sei celle vicine (l'identificativo delle corrispondenti 6 BTS viene inviato dalla BTS attuale alla MS sul canale SACCH).
  - L'intensità e il tasso di errore (qualità) del canale TCH in uso (*downlink*)
  - Le misure sono inviate alla BSC attraverso il canale SACCH)
- Dalla BTS
  - L'intensità e il tasso d'errore sul canale TCH in uso (*uplink*)
  - L'intensità di un canale non usato (per verificare interferenza)

Handover: Misure

- Le misure sono inviate periodicamente alla BSC che aggiorna una lista preferenziale
- Se succede che:
  - La qualità scende sotto una soglia prestabilita
  - Distanza dalla BTS supera il valore massimo consentito
  - Troppo traffico nella cella
  - Altro (manutenzione, guasti,..)

Handover

- Tipologie
  - Intra-cella (cambio di canale ma non di BTS);
  - Fra BST connesse alla stessa BSC;
  - Fra BTS connesse a BSC diverse ma legate alla stessa MSC/VLR;
  - Fra BTS connesse a BSC diverse e legate a MSC/VLR differenti.

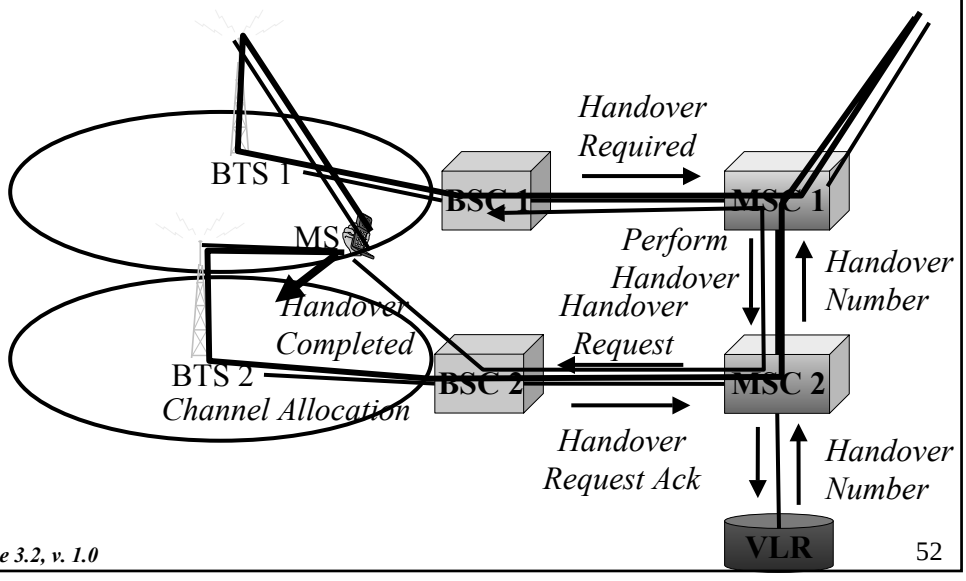
Handover - BSC e MSC diversi

- BSC1
  - identifica una condizione di *handover*
  - identifica la nuova BTS
  - contatta il proprio MSC1 (*handover required*) indicandogli il nuovo MSC2 da coinvolgere
- MSC1 contatta MSC 2 inviandogli una richiesta di *handover* (*perform handover*)
- MSC2
  - richiede al proprio VRL un numero di instradamento
  - Istruisce il propri BSC2 a preparare l'handover (handover request)

Handover - BSC e MSC diversi

- BSC2 assegna un canale di traffico (TCH) e conferma (*handover request ack*)
- MSC2 invia all'MSC1 *l'handover number* e le info sul canale di traffico assegnato
- MSC1 attiva il circuito con MSC2 e la MS viene istruita a cambiare canale
- La MS invia al BSC2 il messaggio *handover completed* che viene propagato fina al MSC1 e al BSC1 che può quindi rilasciare il canale

Handover - BSC e MSC diversi



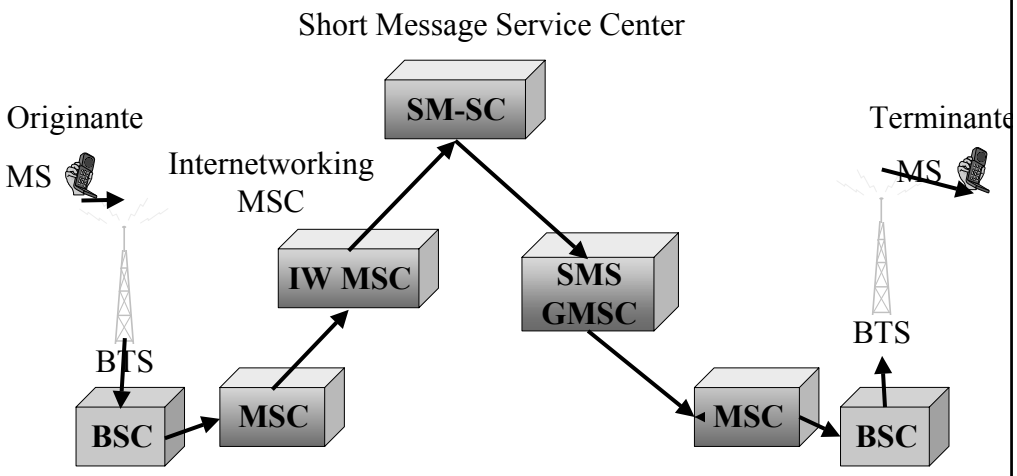
Short Message Service (SMS)

- E' un servizio proposto in origine solo per scopi di segnalazione e controllo da parte del gestore nei confronti dei terminali, che è stato poi evoluto in un servizio utente.
- Il successo di questo servizio ha poi suggerito il suo potenziamento e l'evoluzione verso gli MMS (*Multimedia Message Service*)
- Permette l'invio e la ricezione da parte di una MS di "messaggi" testo di dimensioni pari a 140 ottetti o 160 caratteri (e' previsto anche l'invio di più messaggi concatenati per testi di maggior lunghezza)

Short Message Service (SMS)

- Ci sono due tipologie di messaggi
  - Cell broadcast
  - Point-to-point
- E tre tipologie di messaggi
  - *User specific* -indirizzato direttamente all'utente e quindi in genere viasualizzato
  - *Mobile Equipment specifici* - indirizzato al terminale mobile e quindi capace di attivarne funzionalità o trasferire elementi in esso (ad es. suonerie)
  - *SIM specific* - indirizzato alla SIM e quindi in grado "interagire" con essa per funzioni particolari

Short Message Service (SMS)



Short Message Service (SMS)

- Sull'interfaccia radio è più in generale dalla MS al MSC il trasferimento di uno SM avviene aprendo una connessione.
- Il trasferimento dell'informazione su tale tratto viene confermato, ed in assenza di conferma entro un certo tempo la MS ritrasmette per un massimo di tre volte.
- Di *default* la consegna del messaggio al destinatario finale non è invece confermata.