Approfondimenti sul sistema GSM

A.1 Tipi di canali logici

Per comprendere appieno la necessità della definizione dei canali logici è utile delineare i passi con i quali una Mobile Station (MS) inizialmente spenta può agganciarsi alla rete per ricevere o effettuare una chiamata e quali informazioni di controllo sono necessarie.

A.1.1 Accensione della MS e suo aggancio ad una BTS.

Subito dopo l'accensione una MS effettua le seguenti operazioni (fig. A.1):

- La MS ricerca la BTS alla quale agganciarsi. Per effettuare questa operazione essa misura i livelli di potenza delle portanti utilizzate dalle BTS adiacenti per trasmettere informazioni di controllo e sceglie la BTS che viene ricevuta meglio. Per consentire un aggancio in frequenza preciso ciascuna BTS trasmette una informazione di *correzione della frequenza (frequency correction)*, data dall'emissione ad un livello superiore a tutti gli altri canali fisici di una pura sinusoide, che indica con esattezza la frequenza sulla quale la BTS trasmette le sue informazioni di controllo. Per il trasporto di tale informazione è stato definito il canale logico *FCCH (Frequency Correction CHannel)*.

- Poiché il sistema GSM è digitale risulta necessario sincronizzare la MS con la BTS. A tale scopo la BTS trasmette via radio le necessarie informazioni di sincronizzazione, costituite da una *sequenza di sincronizzazione* accompagnata dal numero di trama TDMA corrente e dall'identità della BTS (*BSIC*, Base Station Identity Code). Per il trasporto di tali informazioni è stato definito il canale logico *SCH (Synchronization CHannel)*

- A questo punto la MS è correttamente agganciata in frequenza, è sincronizzata e conosce con quale BTS è agganciata. La MS può così ricevere e utilizzare il *messaggio di informazione di sistema (system information message)* che la BTS trasmette, il quale contiene essenzialmente l'identità dell'area di localizzazione (*LAI, Location Area Identity*) a cui appartiene la BTS ed i valori dei parametri che specificano come la MS si deve presentare quando essa intende accedere alla rete (livello di potenza di trasmissione, etc.). Per il trasporto del messaggio di informazioni di sistema è stato definito il canale logico *BCCH (Broadcast Control CHannel)*.

Ogni BTS diffonde in broadcast, cioè verso tutte le MS presenti nella cella da essa servita, le informazioni sopra citate. Fino a questo momento infatti non viene instaurato alcun canale dedicato tra una MS e la BTS, ma le MS si limitano ad ascoltare ciò che viene irradiato dalla BTS a cui sono agganciate e ad utilizzare tali informazioni.

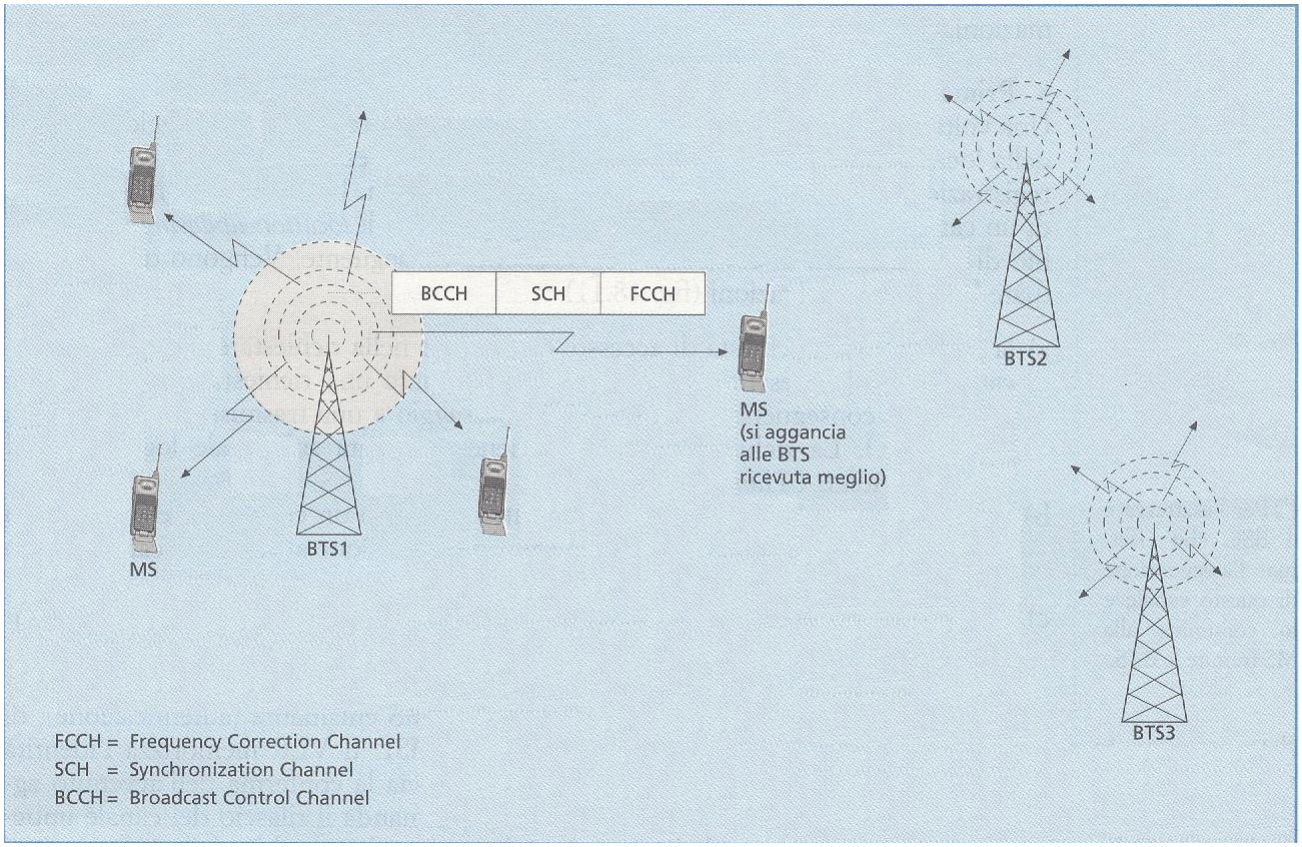

Fig. A.1 Aggancio di una MS ad una BTS e canali logici coinvolti.

A.1.2 Prima registrazione e location updating

Una volta agganciatasi ad una BTS, la MS deve richiedere alla rete un aggiornamento della localizzazione (*location updating*) affinché possa essere effettuata la sua prima registrazione (*first registration*) nel VLR di competenza. Per fare ciò la MS necessita di un canale dedicato sul quale effettuare la richiesta di location updating e lo scambio di informazioni di controllo (segnalazione) conseguente. Vengono quindi effettuate le seguenti operazioni (Fig. A.2):

- La MS invia una *richiesta di accesso*, consistente nella richiesta di un canale dedicato sul quale presentarsi alla rete per effettuare una richiesta di servizio e le operazioni conseguenti (autenticazione, passaggio ad una trasmissione in modalità cifrata, etc.). La richiesta di accesso viene effettuata sul canale logico *RACH (Random Access CHannel)*
- La rete[1] comunica alla MS che le è stato assegnato un certo canale dedicato su cui verrà scambiata la segnalazione. Tale comunicazione avviene sul canale logico *Access Grant CHannel (AGCH)*.
- La MS si sposta sul canale dedicato assegnatole ed invia alla BTS, che la inoltra all'MSC/VLR di competenza, la richiesta di aggiornamento della localizzazione (location updating); inizia così lo scambio di informazioni di controllo tra MS e rete[2] che consente di accertare l'identità della MS chiamante (autenticazione), di passare in modalità cifrata, di riallocare la TMSI. Il VLR memorizza l'identità della location area in cui si trova la MS, le invia la conferma dell'avvenuto aggiornamento della localizzazione e quindi si comanda il rilascio del canale impegnato. Il canale logico dedicato sul quale avviene lo scambio delle informazioni di controllo sopra citate è denominato *SDCCH (Stand-alone Dedicated Control CHannel)*.

La procedura descritta viene attivata anche ogni qual volta la MS, spostandosi, passa da una location area ad un'altra (riceve una nuova LAI, Location Area Identity), per consentire un aggiornamento della sua localizzazione nel VLR.

[1]Per l'esattezza è il BSC che effettua l'assegnazione di questo canale e lo comunica alla MS tramite le BTS.

[2]Da un punto di vista logico si tratta di un colloquio tra MS e MSC/VLR. In questo contesto il BSC e la BTS mettono a disposizione semplicemente il canale di terra (PCM) e (via radio) il canale fisico sui quali transitano i segnali informativi.

Una volta che la MS è stata registrata nel VLR, essa è in grado di ricevere o effettuare chiamate.

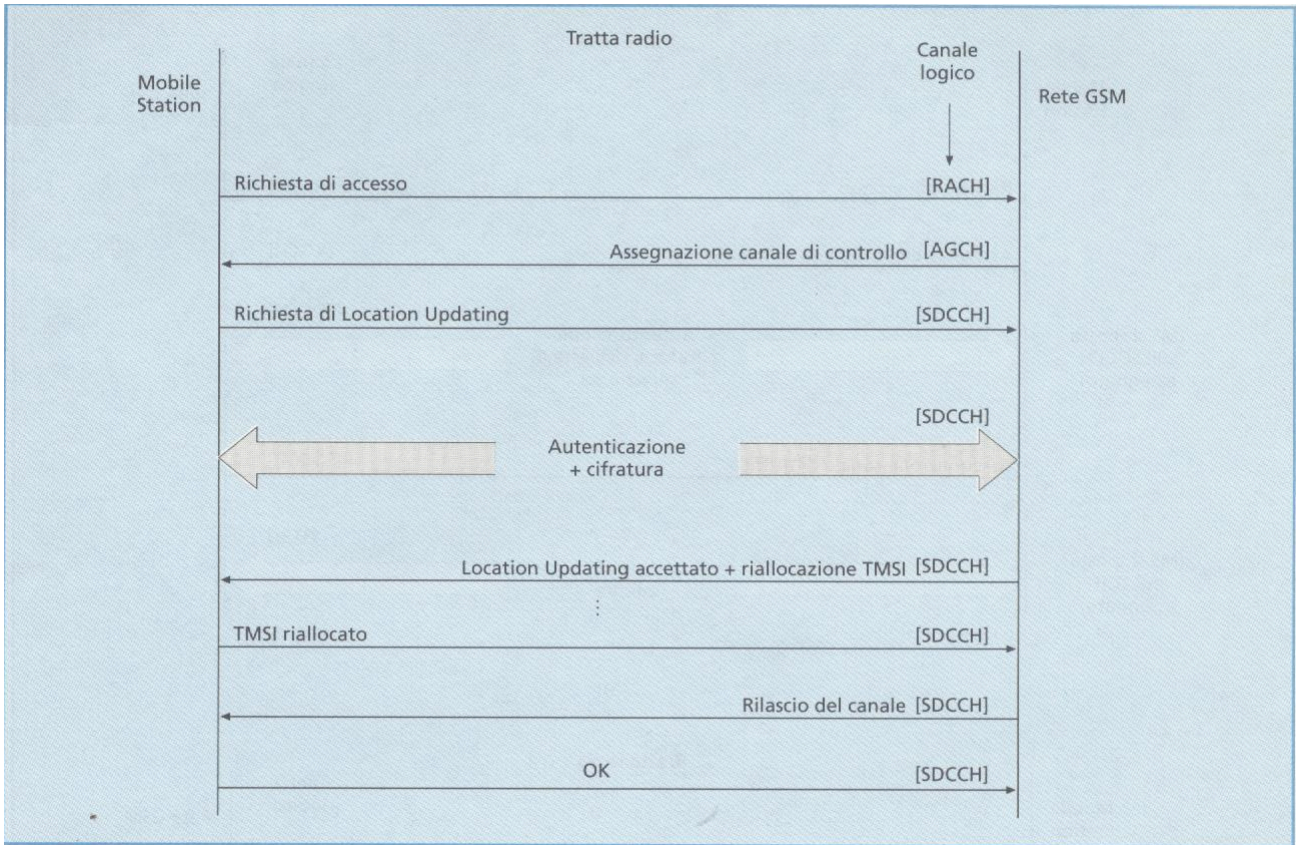

Fig. A.2 Prima registrazione e location updating.

A.1.3 Effettuazione di una chiamata da parte di una MS.

Nel caso in cui una MS intenda effettuare una chiamata, figura A.3a), si opera nel seguente modo:

- La MS invia la propria richiesta di accesso sul canale logico *RACH*.
- La rete assegna alla MS, tramite il canale logico *AGCH*, un canale dedicato *SDCCH*.
- La MS si sposta sul canale *SDCCH* assegnatole ed invia alla BTS, che la inoltra all'MSC/VLR di competenza, una richiesta di servizio; inizia così lo scambio di informazioni tra MS e rete che consente di accertare l'identità della MS chiamante (autenticazione), di passare in modalità cifrata, di inviare il numero di telefono del chiamato, di comandare al termine di questa fase lo spostamento della MS sul canale di traffico che la rete le ha assegnato.
- La MS si sposta sul canale di traffico assegnatole e può quindi avere inizio lo scambio di informazioni tra utenti (traffico). Il canale logico che trasporta le informazioni scambiate tra gli utenti è il *TCH (Traffic Channel)*.

A.1.4 La MS riceve una chiamata.

Nel caso in cui una MS venga chiamata, figura A.3b), si effettuano le seguenti operazioni:

- Viene irradiato nella location area in cui si trova la MS il *messaggio di paging*, contenente l'identità della MS chiamata. Tale messaggio è trasportato sul canale logico *PCH (Paging Channel)* ed è irradiato da tutte le BTS che appartengono alla location area interessata al paging.
- La MS risponde al messaggio di paging inviando, sul canale *RACH*, una richiesta di accesso.
- Si prosegue come delineato nella procedura di chiamata.

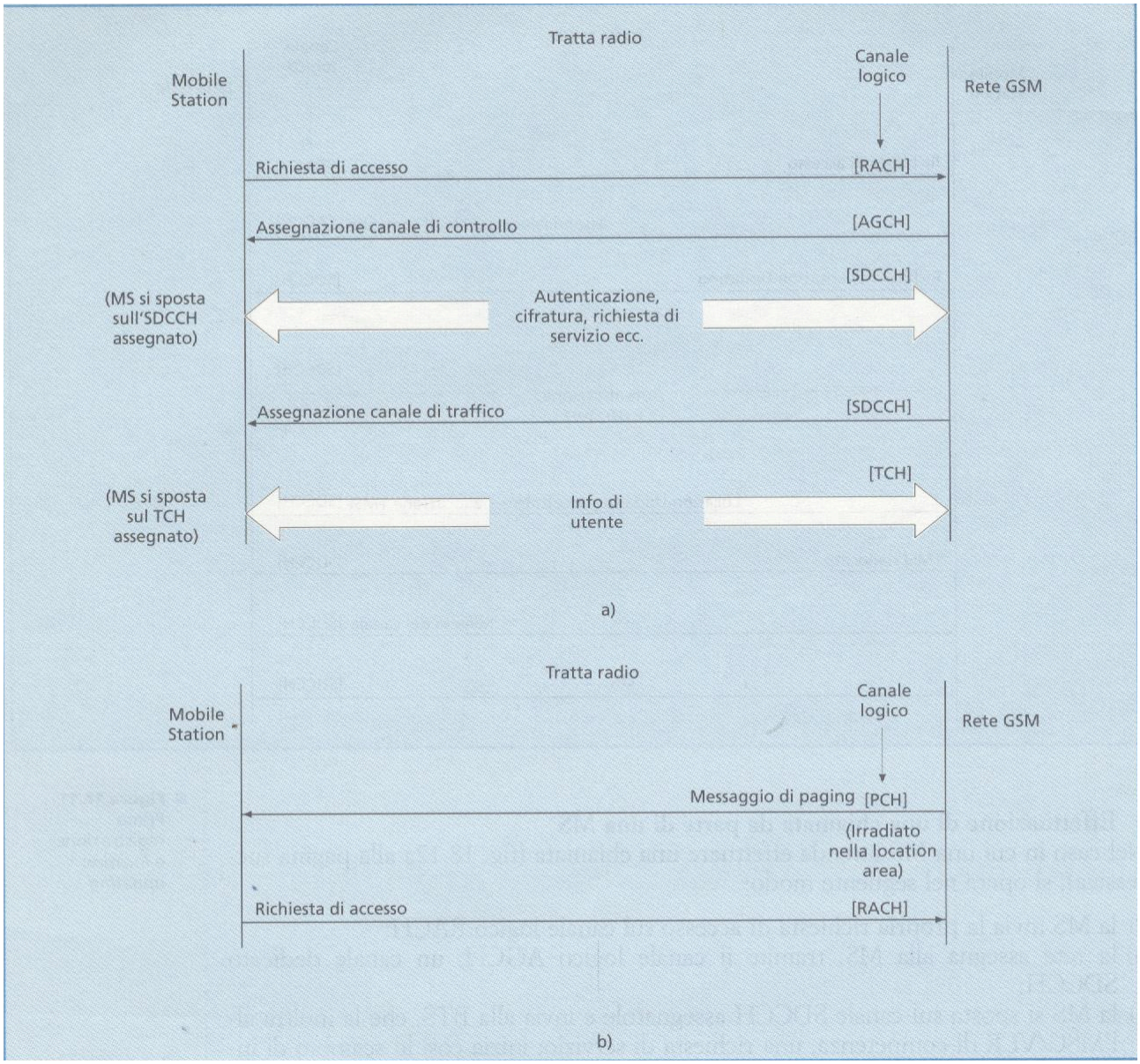

Fig. A.3 a) MS effettua una chiamata; b) MS riceve una chiamata.

Si riassumono ora tutti i canali logici definiti nel sistema GSM.

- Nella direzione **uplink** (MS⇒BTS) si definisce solamente il seguente canale di controllo:

- *Random Access CHannel (RACH)*, viene utilizzato da una MS per richiedere un accesso alla rete (richiesta di un canale) sia nel caso in cui essa intenda effettuare una chiamata oppure che risponda ad una chiamata.

- Nella direzione **downlink** (BTS⇒MS) sono stati definiti i seguenti canali logici:

- *Frequency Correction CHannel (FCCH)*, trasporta le informazioni per la correzione della frequenza (aggancio) delle MS, è diffuso in broadcast (da BTS a tutte le MS della cella).
- *Synchronization CHannel (SCH)*, trasporta le informazioni per la sincronizzazione delle MS con le BTS, oltre al numero di trama TDMA corrente ed all'identità (BSIC, Base Station Identity Code) della BTS; è diffuso in broadcast.
- *Broadcast Control CHannel (BCCH)*, trasporta il messaggio di informazione di sistema inviato dalla rete alle MS, è diffuso in broadcast.
- *Paging Channel (PCH)*, trasporta i messaggi di paging inviati per chiamare le MS.
- *Access Grant CHannel (AGCH)*, è il canale sul quale la rete comunica alla MS qual è il canale dedicato (SDCCH) che essa deve utilizzare per effettuare lo scambio preliminare di informazioni di servizio

(autenticazione, etc.) tramite il quale la rete accerta dell'identità dell'utente, comanda il passaggio in modalità cifrata ed eventualmente assegna un canale di traffico alla MS.

- Sono canali **sia uplink che downlink** (bidirezionali) i seguenti canali logici:

- *Stand-alone Dedicated Control CHannel (SDCCH)*, trasporta le informazioni di controllo preliminari scambiate tra MS e rete (autenticazione, etc.), è un canale dedicato (temporaneamente) al colloquio MS-rete.
- *Traffic Channel (TCH)*, trasporta le informazioni scambiate tra utenti che costituiscono il "traffico".

- Oltre ai canali sopra citati sono stati definiti altri due canali logici che trasportano informazioni di controllo mentre una MS è impegnata in una connessione di traffico (sta usando un canale TCH) oppure di segnalazione (sta usando un canale SDCCH):

- *SACCH (Slow Associated Control Channel)*, trasporta informazioni di controllo che devono essere periodicamente scambiate tra una MS e la rete anche nel corso di una connessione (TCH o SDCCH), quali regolazione di potenza, anticipo temporale (timing advance), risultato delle misure effettuate dalla MS, etc.
- *FACCH (Fast Associated Control Channel),* è il canale tramite il quale la rete invia ad una MS il comando di handover, cioè ordina alla MS di cambiare canale di traffico mentre è instaurata una connessione poiché, tipicamente, essa è passata da una cella ad un'altra cella (cambio di BTS).

I canali logici possono essere mappati (inseriti) sui canali fisici in vario modo. Possono essere utilizzati uno o più timeslot (canali fisici) di una frequenza portante per realizzare i canali logici di controllo, i rimanenti timeslot realizzano i canali di traffico (TCH). Se vi sono più frequenze portanti, tutti i timeslot delle altre frequenze portanti realizzano canali di traffico. Un esempio di mappatura dei canali logici sui canali fisici è riportato in Fig. A.4.

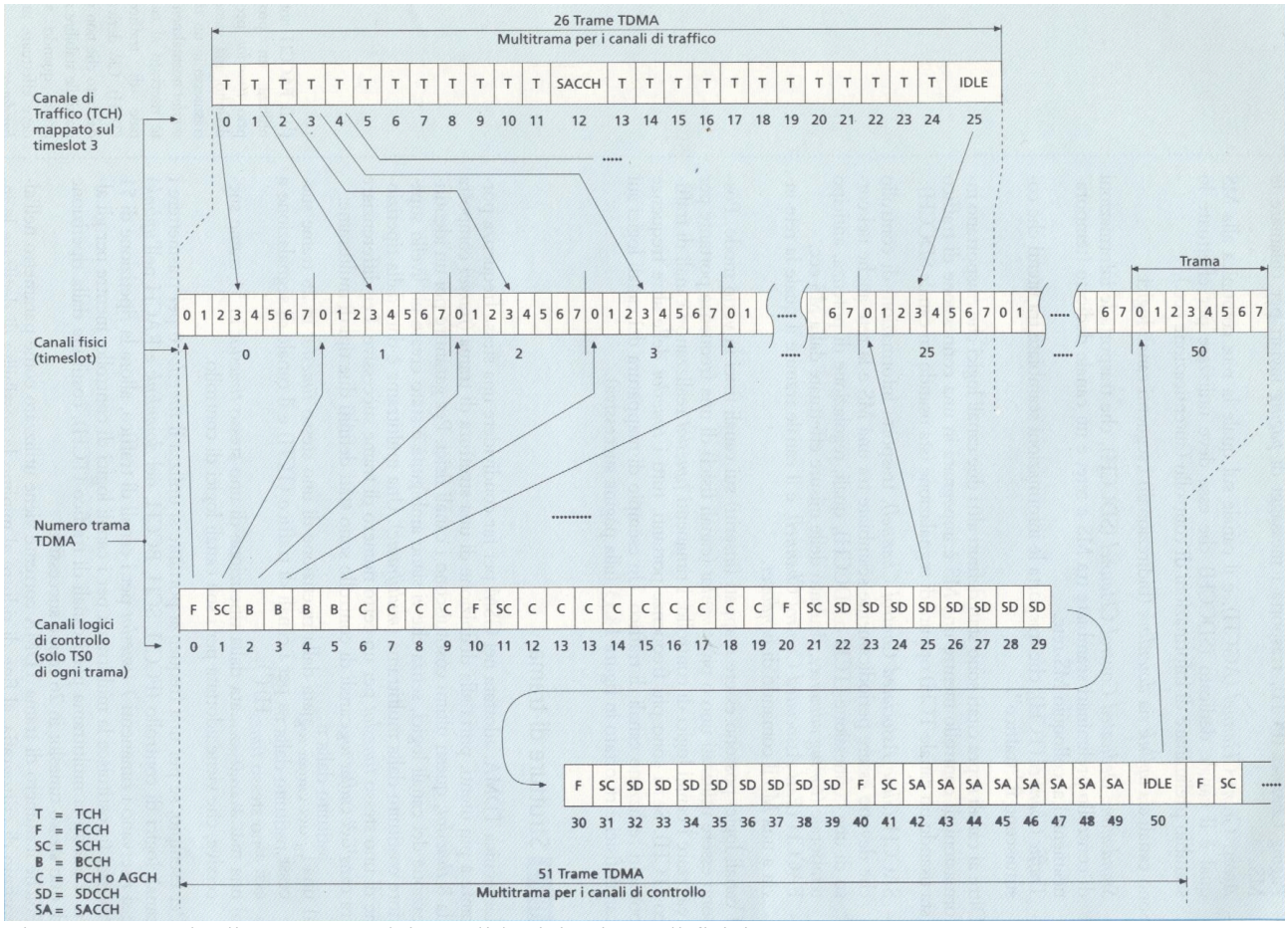

Fig. A.4 Esempio di mappatura dei canali logici sui canali fisici.

A.2 Strutture di trama

La tecnica TDMA adottata nel GSM per far condividere una stessa frequenza portante a più utenti porta alla definizione di una struttura di *trama* (frame) composta da 8 timeslot; questi ultimi costituiscono i canali fisici. Per garantire poi una identificazione dei canali logici senza che vi siano ambiguità è stato creato un livello superiore costituito dalla *multitrama* (multiframe).

> Una multitrama è data dalla ripetizione di uno stesso timeslot per un certo numero di trame successive.

Per differenziare tra canali di traffico e canali di controllo sono stati definiti due tipi di multitrame:

- Una multitrama formata dalla ripetizione di uno stesso timeslot in 26 trame successive; essa viene adottata per i canali di traffico (TCH) ed il canale di segnalazione ad essi associato (SACCH[3]).
- Una multitrama formata dalla ripetizione di uno stesso timeslot in 51 trame successive; essa viene adottata per i soli canali logici di controllo.

Per esempio se per una frequenza portante si utilizza il timeslot 0 per trasmettere i canali logici di controllo (FCCH, SCH, BCCH, etc. nel downlink e RACH nell'uplink) e si riservano i rimanenti 7 timeslot per i canali di traffico, allora la ripetizione di 51 timeslot 0 costituisce la multitrama per i canali logici di controllo, mentre per gli altri timeslot si adotta la multitrama per i canali di traffico (TCH) costituita dalla ripetizione di uno stesso timeslot in 26 trame successive.

Poiché il numero di trama TDMA corrente viene utilizzato come parametro nell'algoritmo di crittografia, al fine di ridurre al minimo le possibilità di decifrare le informazioni trasmesse via radio è necessario avere una numerazione delle trame TDMA molto grande. A tale scopo, Fig. A.5, sono state introdotte:

- La *supertrama* (superframe), è una struttura temporale che unifica le multitrame da 26 e da 51 in quanto è costituita da 1326 trame TDMA (26·51=1326, pari a 26 multitrame da 51 o 51 multitrame da 26).
- La *ipertrama* (hyperframe), è costituita da 2048 supertrame. Essa è in grado di fornire una numerazione ciclica che arriva a 2048·1326=2715648 trame TDMA. Si ottiene così un numero elevatissimo di possibili combinazioni che rende più sicura la crittografia.

In figura A.5 è riassunta la complessa strutturazione di trama del GSM.

[3] Il FACCH non utilizza un proprio timeslot predefinito, ma viene trasmesso in un timeslot normalmente riservato al canale di traffico (TCH). Ciò deriva dal fatto che non è possibile stabilire a priori quando si deve effettuare un handover.

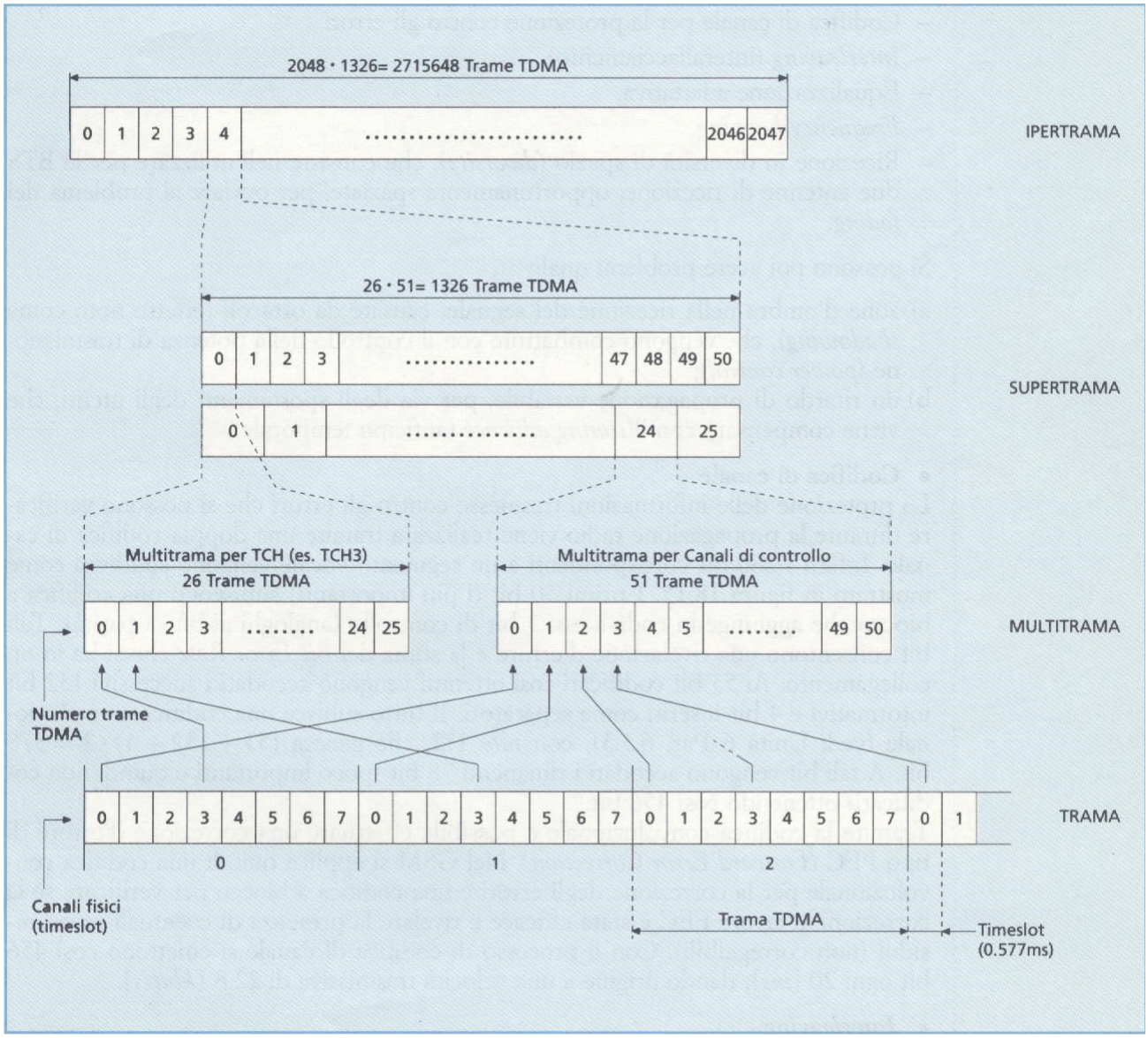

Fig. A.5 Strutture di trama definite nel GSM.

A.3 Codifica della voce e struttura del burst

La codifica della voce viene effettuata nelle Mobile Station GSM per mezzo di un *codificatore ibrido* (si veda il CAPITOLO 11 PARAGRAFO 2.1).

Il codificatore *full rate* converte un segmento fonico avente la durata di 20 ms in 260 bit, dando così origine a una velocità di emissione di 13 kbit/s.

Il segnale codificato non viene trasmesso direttamente, ma subisce una elaborazione digitale (*digital signal processing*) che gli consente di sopportare meglio gli inconvenienti che si possono avere nella propagazione radio.

Tali inconvenienti si possono così riassumere: disturbi e rumore, fading, interferenza intersimbolica.

Le tecniche utilizzate per ovviare a tali inconvenienti sono le seguenti:

- codifica di canale per la protezione contro gli errori;
- *interleaving* (interallacciamento);
- equalizzazione adattativi;
- frequency hopping;
- ricezione in diversità di spazio (*diversity*), che consiste nell'utilizzare per le BTS due antenne di ricezione per ovviare al problema del fading.

Si possono poi avere problemi quali:

a) zone d'ombra nella ricezione del segnale causate da ostacoli (effetto noto come *shadowing*), che vengono combattute con il controllo della potenza di trasmissione (*power control*).
b) un ritardo di propagazione variabile per via degli spostamenti degli utenti, che viene compensato con il *timing advance* (anticipo temporale).

Per riassumere le operazioni sopra citate, in figura A.6 si riporta lo schema a blocchi, di riferimento, di una Mobile Station e di una BTS. Le operazioni svolte nella BTS non comprendono ovviamente la conversione A/D del segnale vocale, la segmentazione, la codifica vocale GSM e le operazioni inverse.

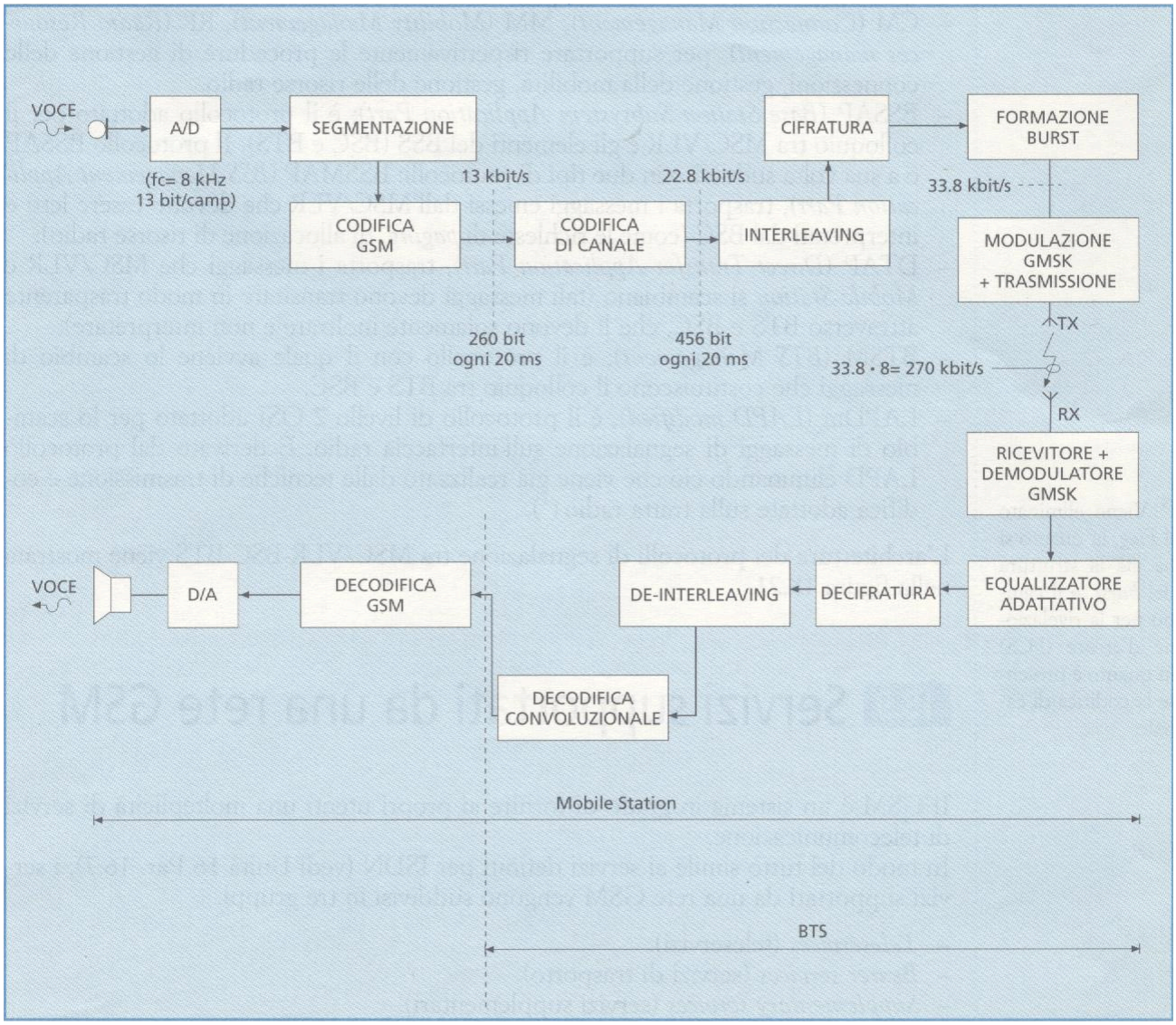

Fig. A.6 Schema a blocchi di riferimento di una Mobile Station e di una BTS.

A.3.1 Codifica di canale

La protezione delle informazioni trasmesse contro gli errori che si possono verificare durante la propagazione radio viene realizzata tramite una doppia codifica di canale.

Infatti i 260 bit corrispondenti ad un segmento vocale vengono suddivisi come mostrato in figura A.7. I primi 50 bit (i più importanti) subiscono una codifica a blocco che aggiunge in coda a essi 3 bit di controllo (analoghi ai bit di parità).

Tali bit consentono una rivelazione d'errore e la stima del *Bit Error Rate* che si ha in un collegamento.

Ai 53 bit codificati così ottenuti vengono accodati i successivi 132 bit informativi e 4 bit inseriti come separatori.

Il tutto subisce una codifica convoluzionale (si veda il CAPITOLO 9 PARAGRAFO 9.4), con *code rate* 1:2, che genera (53+132+4)·2=378 bit.

A tali bit vengono accodati i rimanenti 78 bit (poco importanti e quindi non codificati) ottenendo così 456 bit.

Tramite la codifica convoluzionale è possibile effettuare una correzione d'errore di tipo FEC (*Forward Error Correction*).

Nel GSM si applica quindi una *codifica convoluzionale*, per la correzione degli errori, e una *codifica a blocco*, per verificare se la correzione d'errore FEC è stata efficace e rivelare la presenza di eventuali errori residui (non correggibili).

Con il processo di codifica di canale si emettono così 456 bit ogni 20 ms, dando origine a una velocità trasmissiva di 22.8 kbit/s.

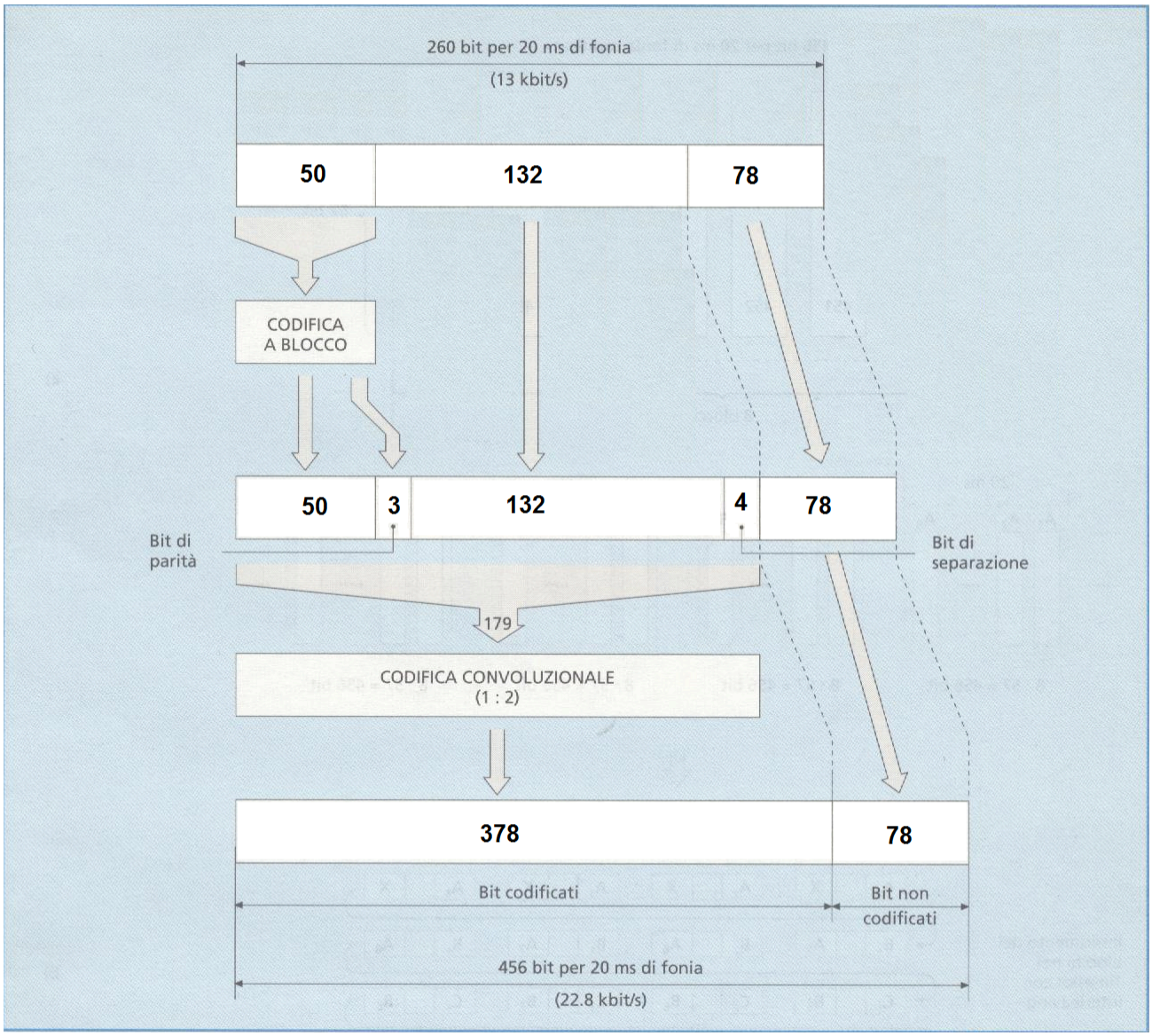

Fig. A.7 Codifica vocale e di canale di un segmento vocale di 20 ms.

A.3.2 Interleaving

L'*interleaving* (interallacciamento) è una tecnica che migliora le prestazioni della codifica di canale. Essa consiste nel trasmettere in un *timeslot* blocchi di bit originati dalla codifica di due segmenti fonici (di 20 ms) diversi.

Così facendo eventuali errori derivanti da problemi trasmissivi (rumore, fading, ecc.) che intervengono nel timeslot ma sono dispersi su due segmenti fonici, limitando il numero degli errori relativi a un singolo segmento fonico.

Ciò rende più efficace la correzione degli errori (FEC) in fase di decodifica. L'*interleaving* viene realizzato nel seguente modo:

a) i 456 bit derivanti da un segmento fonico di 20 ms vengono suddivisi in 8 blocchi da 57 bit (fig. A.8a);
b) in un timeslot si trasmettono due blocchi di due segmenti fonici diversi, fig. A.8b).

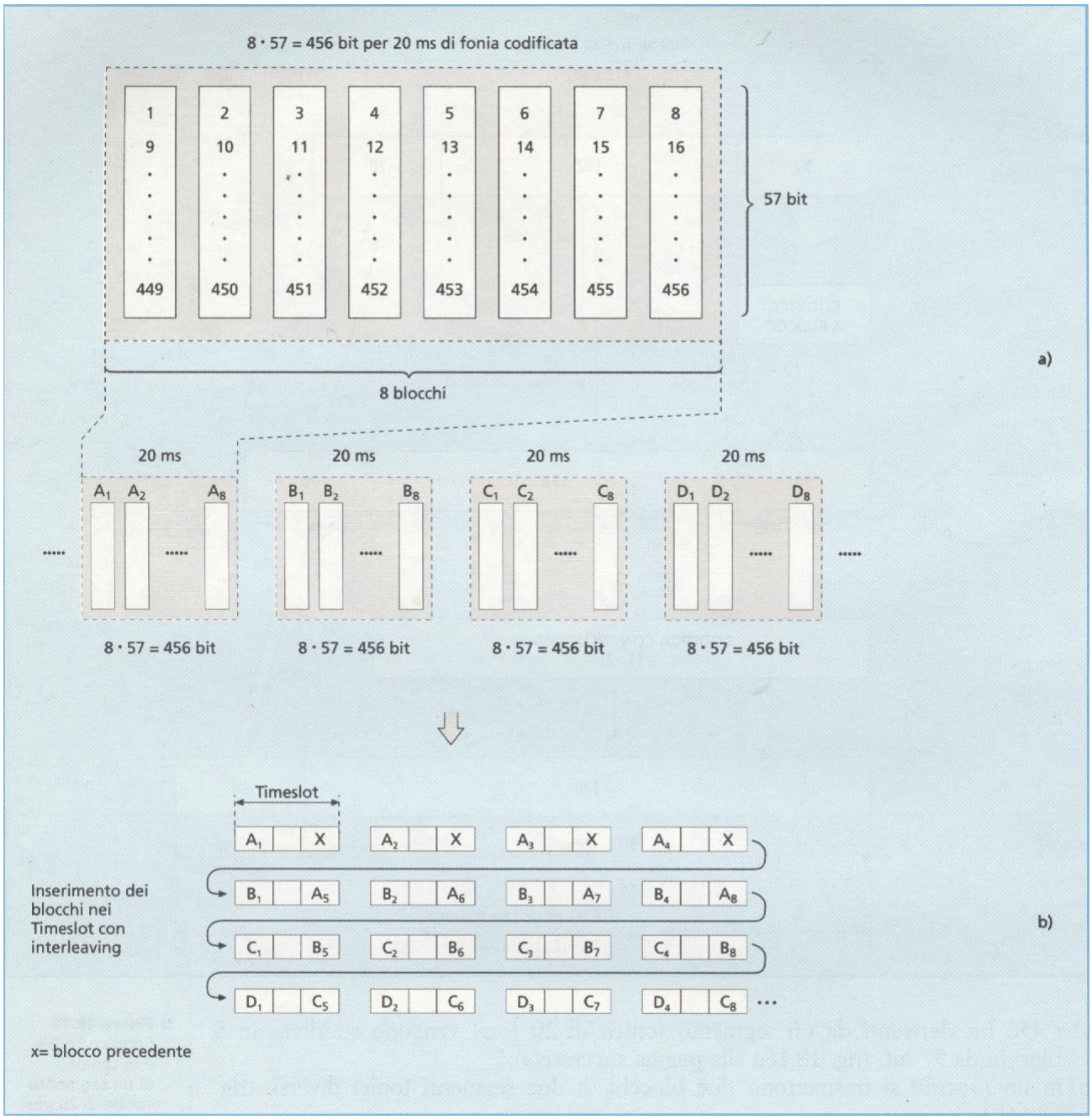

Fig. A.8 a) Formazione dei blocchi; b) Interleaving.

A.3.3 Equalizzazione adattativa

I problemi relativi all'interferenza intersimbolica (ISI) vengono affrontati impiegando in ricezione l'equalizzazione adattativa.

Con l'equalizzazione adattativa il ricevitore costruisce un modello del canale di comunicazione per effettuare l'equalizzazione e la successiva correzione d'errore di tipo FEC[4].

Per consentire ciò viene inserita al centro di ogni *timeslot* una sequenza di training (*training sequence*), la cui analisi consente all'equalizzatore di creare un modello che rappresenti le condizioni del canale al momento della trasmissione di ciascun *timeslot*.

A.3.4 Frequency hopping

Il *frequency hopping* (salti di frequenza) è una tecnica adottata nel GSM per ridurre gli effetti del fading e diminuire nel contempo i livelli di interferenza.

Infatti mentre la ricezione con diversità di spazio (due antenne riceventi) è implementabile nelle BTS (*Base Transceiver Station*), essa non lo è nelle MS (*Mobile Station*), per ovvi motivi di spazio.

Per ridurre i fading può però essere implementata una forma di diversity in frequenza (si vedi IL CAPITOLO 4 PARAGRAFO 5.1 del VOLUME 2) nota come *frequency hopping*.

Tale tecnica consiste nel cambiare la frequenza di trasmissione a ogni *timeslot*, in modo ciclico o pseudocasuale, nel corso di una connessione tra BTS e MS (fig. A.9).

Così facendo se il segnale trasmesso in un *timeslot* è soggetto a *fading*, nel *timeslot* successivo tale fenomeno non si verifica più in quanto viene cambiata la frequenza di trasmissione, migliorando la qualità del segnale ricevuto.

Inoltre con questa tecnica si riducono i livelli di interferenza in quanto capita meno di frequente che due MS (o BTS) operino sulle stesse frequenze nello stesso istante.

Le modalità di effettuazione del *frequency hopping* vengono comunicate dalla BTS alla MS in modo tale che i salti di frequenza avvengano in modo sincronizzato (i salti di frequenza devono essere gli stessi per entrambe).

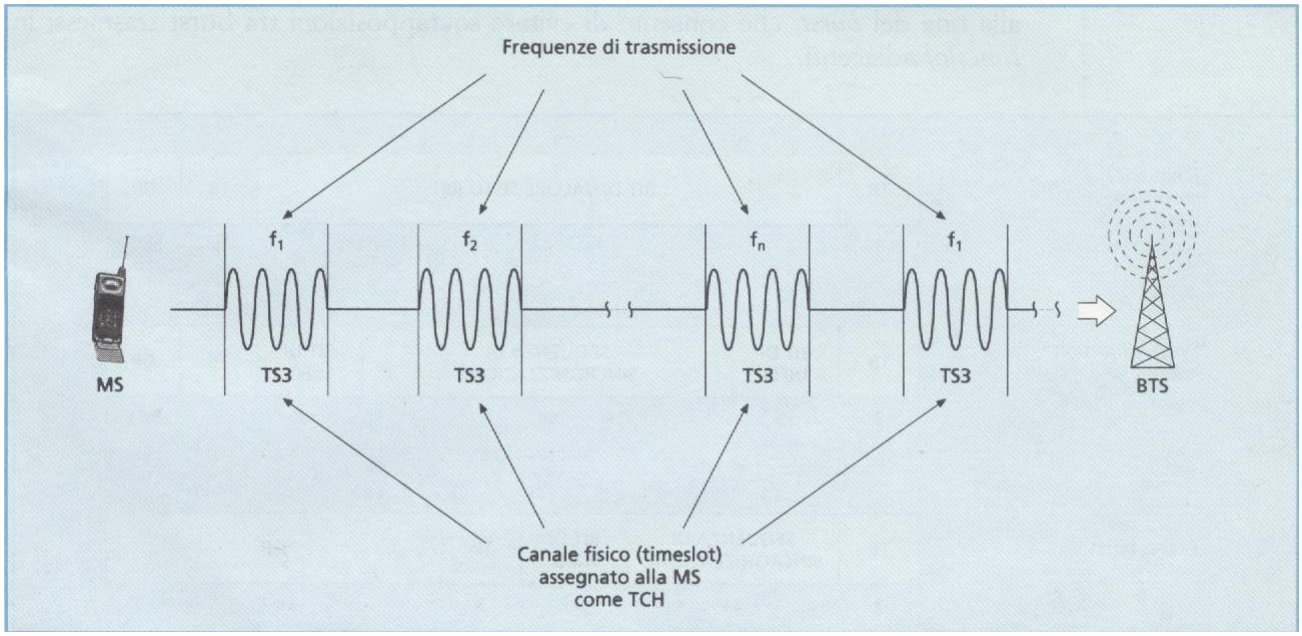

Fig. A.9 Schema di principio del frequency hopping.

[4]Il ricevitore utilizza l'algoritmo di Viterbi per fare ciò.

A.3.5 Tipi di burst e loro struttura

Con il termine *burst* (letteralmente "raffica" di bit) si indica l'insieme dei bit trasmessi in un timeslot.
In relazione al canale logico in cui vengono trasmessi, sono stati definiti i seguenti 5 tipi di burst (fig. A.10).

1. *Frequency correction burst*, è trasmesso nei *timeslot* riservati al canale logico *FCCH*. E' caratterizzato da una sequenza di 142 bit di valore 0, i quali producono in trasmissione una pura sinusoide che consente alle MS di agganciarsi in frequenza.
2. *Synchronization Burst*, è trasmesso nei timeslot riservati al canale logico *SCH*. Contiene: una lunga sequenza di sincronizzazione (64 bit), che permette alle MS di sincronizzarsi con la BTS della cella in cui esse si trovano; il numero di trama TDMA corrente e il codice che identifica la BTS (*Base Station Identity Code*, BSIC).
3. *Access burst*, è trasmesso nei timeslot riservati al canale logico RACH. Contiene una sequenza di sincronizzazione e la richiesta di accesso di una MS.
4. *Normal Burst*, è trasmesso nei *timeslot* riservati ai rimanenti canali logici (BCCH, SDCCH, SACCH, FACCH, TCH). Nel caso dei canali di traffico (TCH) contiene: due blocchi da 57 bit generati dalla codifica di due segmenti vocali adiacenti, crittografati; la sequenza di training che l'equalizzatore in ricezione utilizza per creare il modello del canale di comunicazione che consente l'equalizzazione adattativa (è usato anche in fase di decodifica per la correzione d'errore di tipo FEC). Sono poi presenti due bit che consentono di distinguere tra i canali logici che condividono lo stesso timeslot (TCH, SACCH e FACCH).
5. *Dummy burst*, è trasmesso nei timeslot riservati ai canali logici PCH ed AGCH quando essi non sono impegnati per effettuare chiamate. Non contiene informazioni vere e proprie, ma solo una sequenza pseudocasuale di riempimento[5]. Ha lo stesso formato del normal burst.

Oltre agli elementi informativi che caratterizzano ciascun burst, vi sono dei bit comuni a tutti i tipi di burst:

- *Tail bit* (bit di coda); sono bit di valore 0 che indicano l'inizio e la fine del burst.
- *Guard period* (periodo di guardia); è un periodo di assenza di trasmissione posto alla fine del burst che consente di evitare (entro certi limiti) sovrapposizioni tra burst trasmessi in timeslot adiacenti. Se il *guard period* non è più sufficiente a evitare ciò interviene il *timing advance*, che riallinea i *timeslot* in ricezione. *L'access burst* è caratterizzato da un periodo di guardia più lungo, in quanto esso viene emesso da una MS che può trovarsi in un punto qualsiasi della cella e per la quale non è stato ancora attivato il *timing advance*, dato che essa invia in quel momento una richiesta di accesso alla rete.

[5]Il riempimento è necessario per fare in modo che la frequenza utilizzata per mappare i canali logici di controllo venga sempre trasmessa, anche se non vi sono messaggi o informazioni di controllo vere e proprie da trasmettere. Il livello di ricezione di tale frequenza viene misurato dalle MS ed inviato alla rete, assieme ad altre misure, per determinare in modo sicuro quando è necessario effettuare un handover e qual è la BTS in grado di servire al meglio la MS che necessita dell'handover stesso.

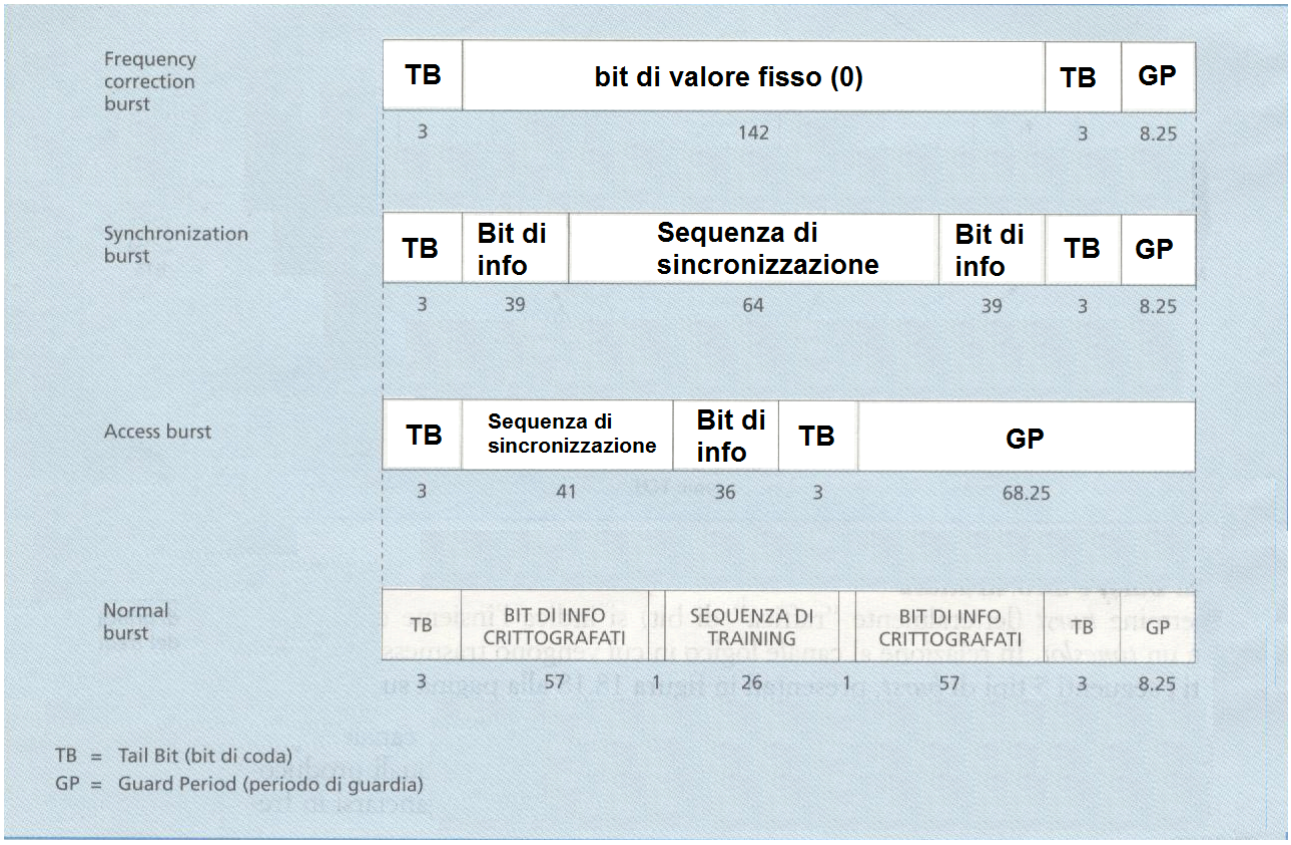

Fig. A.10 Struttura dei burst.

A.3.6 Modulazione

La modulazione adottata nel GSM è una modulazione digitale denominata *GMSK (Gaussian Minimum Shift Keying)*, descritta nel CAPITOLO 8 PARAGRAFO 5.5, a cui si rimanda.

Essa è in sostanza una modulazione derivata dalla MSK (Minimum Shift Keying) anteponendo al modulatore un filtro[6] avente una risposta di tipo gaussiano (da cui il nome Gaussian).

A.4 Architettura dei protocolli di segnalazione

Per il colloquio tra le unità funzionali del GSM vengono utilizzati degli opportuni protocolli.

Per il trasporto delle informazioni di segnalazione sono utilizzati sia dei protocolli già definiti per altre reti sia dei protocolli definiti ad hoc per il colloquio tra le unità funzionale del GSM.

I protocolli già esistenti sono i seguenti:

- I protocolli definiti nell'architettura del canale comune di segnalazione (*CCSS7*), ed in particolare *MTP* (Message Transfer Part), *SCCP* (Signalling Connection Control Part), *TCAP* (Transaction Capabilities Application Part) nei collegamenti di segnalazione tra BSC, MSC/VLR, HLR, centrali PSTN/ISDN.
- Il protocollo *LAPD* (Link Access Protocol - D channel) nei collegamenti di segnalazione tra BSC e BTS.

I protocolli definiti appositamente per il GSM sono i seguenti:

- *MAP (Mobile Application Part)* per il colloquio tra MSC/VLR ed HLR
- *CM (Connection Management)*, *MM (Mobility Management)*, *RR (Radio Resources management)*, per supportare rispettivamente le procedure di gestione delle connessioni, gestione della mobilità, gestione delle risorse radio.
- *BSSAP (Base Station Subsystem Application Part)*; è il protocollo adottato per il colloquio tra MSC/VLR e gli elementi del BSS (BSC e BTS).

[6] Un parametro caratteristico del filtro è il prodotto *BT*, con BT=0.3, dove B è la banda a 3 dB del filtro e $T=1/f_{bit}$, è il tempo di bit (in sostanza si normalizza la banda rispetto alla frequenza di bit). Il bit rate sulla tratta radio è $33{,}8 \cdot 8 \approx 270$ [kbit/s][6] (8 segnali multiplati in TDM, per un singolo segnale si hanno 33,8 kbit/s dei quali 22,8 kbit/s sono dovuti alla codifica completa della voce e il resto alle informazioni di controllo), per cui la banda del filtro risulta pari a $B=0.3 \cdot 270 \cdot 10^3=81$ kHz.

Il protocollo BSSAP è a sua volta suddiviso in due tipi di protocolli:

- *BSSMAP (BSS Management Application Part)*; trasporta i messaggi emessi dall'MSC/VLR che devono essere letti ed interpretati dal BSC (come le richieste di paging, di allocazione di risorse radio, etc.).
- *DTAP (Direct Transfer Application Part)*; trasporta i messaggi che MSC/VLR e Mobile Station si scambiano; tali messaggi devono transitare in modo trasparente attraverso BTS e BSC, che li devono solamente inoltrare e non interpretare.

- *BTSM (BTS Management)*; è il protocollo con il quale avviene lo scambio di messaggi che costituiscono il colloquio tra BTS e BSC.
- *LAPDm (LAPD modified)*, è il protocollo di livello 2 OSI adottato per lo scambio di messaggi di segnalazione sull'interfaccia radio. Esso è derivato dal protocollo LAPD eliminando ciò che viene già realizzato dalle tecniche di trasmissione e codifica adottate sulla tratta radio[7].

L'architettura dei protocolli di segnalazione viene mostrata nella figura A.11.

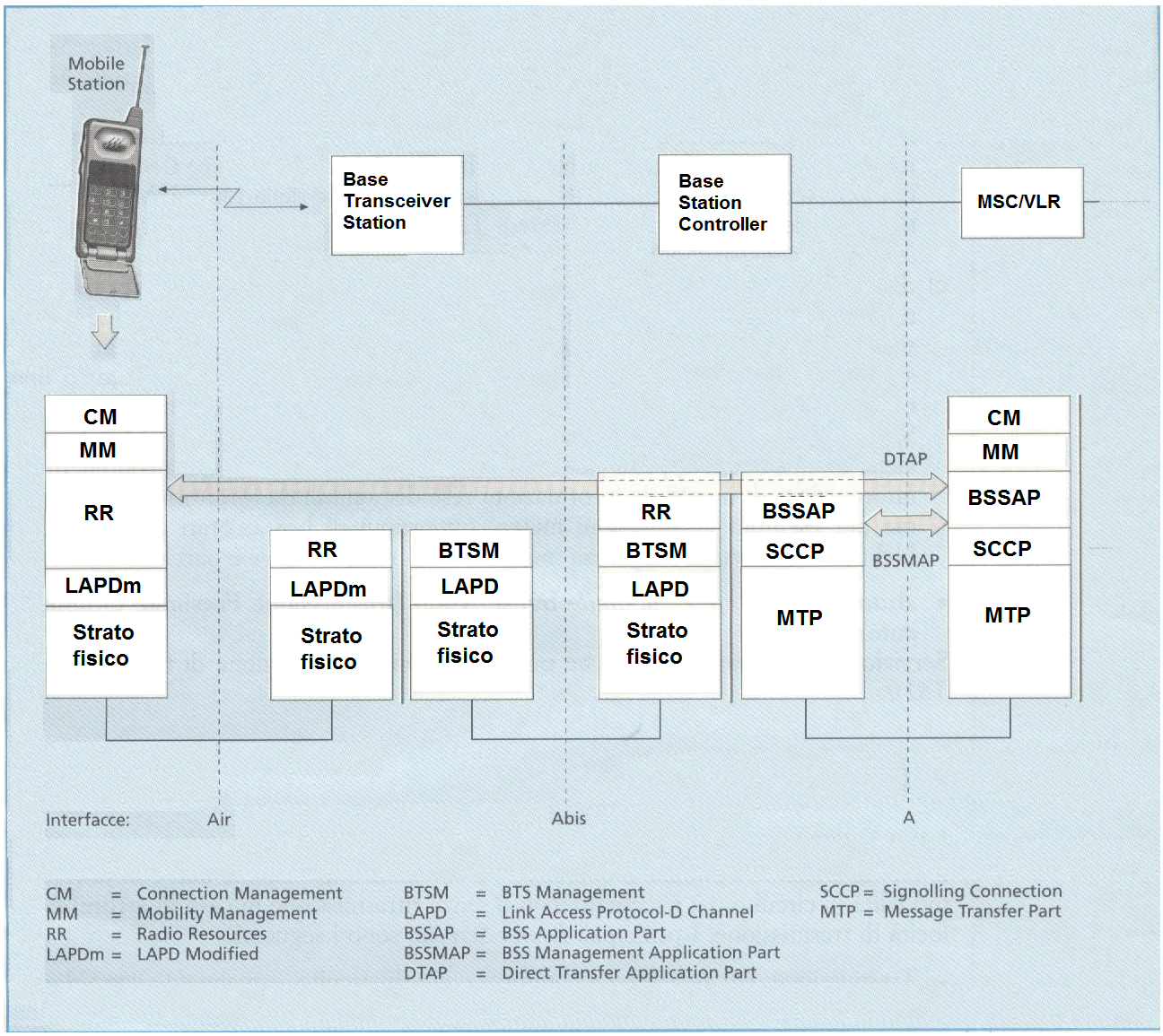

Fig. A.11 Architettura dei protocolli di segnalazione per il colloquio tra MSC/VLR - BSC - BTS - MS.

[7]Viene eliminato il Flag, in quanto si ha già la struttura del burst, ed il campo per la rivelazione d'errore (FCS) in quanto è presente la codifica di canale.

A.5 Numeri e identità utilizzati nel GSM

Nel sistema GSM vengono utilizzati numerosi numeri e identificativi per consentire ad una Mobile Station di muoversi liberamente sia all'interno della rete del proprio operatore (*HPLMN*, Home Public Land Mobile Network) sia in reti di altri operatori (*VPLMN*, Visited PLMN), nonché per garantire un elevato livello di sicurezza contro le "clonazioni". Essi possono venire classificati come qui di seguito indicato.

A.5.1 Numeri ed identità assegnati alle Mobile Station

- *MSISDN - Mobile Station International ISDN Number*[8]

L'MSISDN è il numero di telefono che consente di chiamare un utente GSM. Esso non è tanto correlato all'apparato mobile utilizzato quanto al servizio di telecomunicazione che si utilizza. E' quindi possibile assegnare ad un singolo utente più numeri di telefono, ciascuno dei quali viene associato ad uno specifico servizio di telecomunicazioni. Ad esempio un utente può avere un numero MSISDN per le chiamate foniche ed un altro numero per le chiamate fax. L'MSISDN è memorizzato nell'HLR, lato rete, e nel SIM (Subscriber Identity Module) della Mobile Station. L'analisi dell'MSISDN consente ad una centrale di individuare l'HLR dell'operatore presso cui la Mobile Station è registrata e quindi di ottenere le informazioni necessarie per instradare una chiamata. L'MSISDN è composto da tre parti:

- *CC (Country Code)*, identifica la nazione nel caso di chiamate internazionali (è preceduto dal prefisso internazionale, +)
- *NDC (National Destination Code)*, è l'equivalente dell'indicativo distrettuale telefonico ed identifica un'area di numerazione, cioè in sostanza consente di identificare l'HLR fisico presso cui l'utente è registrato. Per chiamate in ambito nazionale non viene utilizzato il CC e si fa precedere l'NDC dalla cifra 0.
- *SN (Subscriber Number)*, identifica univocamente un utente all'interno di un'area di numerazione.

Esempio di MSISDN: +39 338 5955966
CC NDC SN

- *IMSI - International Mobile Subscriber Identity*

L'IMSI identifica in modo univoco un utente, sia in ambito nazionale che internazionale. Esso consente alla rete di riconoscere senza ambiguità una Mobile Station e di recuperare tutte le informazioni di servizio ad essa associate (localizzazione, triplette, etc.). Per questo motivo l'IMSI è segreto e deve essere adeguatamente protetto contro intercettazioni. E' memorizzato permanentemente nell'HLR e nell'AuC, nonché nel SIM contenuto nella Mobile Station, e solo temporaneamente nel VLR. Un utente può avere più MSISDN ma ha sempre un solo IMSI e l'HLR del proprio operatore è in grado di effettuarne il collegamento (in base all'MSISDN l'HLR può recuperare l'IMSI e viceversa). L'IMSI è composto da tre campi: *MCC (Mobile Country Code)*, identifica la nazione in cui l'utente ha la sua residenza, *MNC (Mobile Network Code)*, identifica la rete GSM presso cui l'utente ha sottoscritto l'abbonamento, MSIN (Mobile Subscriber Identification Number), identifica univocamente un utente mobile entro la propria rete GSM.

- *TMSI - Temporary Mobile Subscriber Identity*

E' una identità temporanea, che cambia in continuazione, la quale viene assegnata ad una MS dal VLR presso cui essa è registrata. La MS memorizza la TMSI ed ogni volta che accede alla rete per effettuare una richiesta di servizio si presenta ad essa con la TMSI invece che con la sua vera identità (IMSI). In base alla TMSI ricevuta il VLR è in grado di recuperare l'IMSI e quindi i dati di abbonamento dell'utente. In questo modo si limita il più possibile la trasmissione via radio della vera identità dell'utente (IMSI), aumentando la sicurezza contro le intercettazioni.

- *IMEI - International Mobile Equipment Identity*

L'IMEI identifica univocamente un Mobile Equipment (ME) GSM. E' una sorta di numero di serie dell'apparato vero e proprio e non è correlato ad uno specifico utente, i cui dati di abbonamento (IMSI, MSISDN, etc.) sono contenuti nel SIM.

[8] Il nome MSISDN deriva dal fatto che la numerazione utilizzata per il GSM è conforme a quella utilizzata per la rete ISDN.

A.5.2 Numeri ed identità associati ad elementi di una rete GSM

- *MSRN - Mobile Station Roaming Number*

E' il numero che viene analizzato dagli MSC (in particolare dal GMSC, Gateway MSC) coinvolti in una chiamata per realizzare l'instradamento verso l'MSC di destinazione, nella cui area di servizio si trova la Mobile Station chiamata. E' assegnato dal VLR presso cui la MS è registrata. Il primo MSC a cui giunge il numero di telefono[9] della MS (MSISDN) richiede l'MSRN all'HLR presso cui l'utente è registrato (individuato grazie all'analisi dell'MSISDN), il quale a sua volta lo richiede al VLR. Una volta ricevuto l'MSRN il primo MSC è in grado di instradare la chiamata verso l'MSC di destinazione.

- *LAI - Location Area Identity*

Identifica in modo univoco una Location Area (LA), o area di localizzazione. Una Mobile Station è considerata localizzata quando si conosce l'area di localizzazione (LA) in cui essa si trova. Una LA è infatti definita come l'area geografica all'interno della quale una Mobile Station si può muovere liberamente senza che essa debba richiedere alla rete un aggiornamento della localizzazione (*location updating*). L'area servita da un MSC/VLR è suddivisa in un certo numero di LA ed il messaggio di paging, con il quale la rete chiama una Mobile Station, viene irradiato solo all'interno della LA in cui la MS si trova. Una LAI è composta da tre campi: *MCC (Mobile Country Code)*, identifica la nazione entro cui si trova la Location Area, *MNC (Mobile Network Code)*, identifica la rete GSM a cui appartiene la Location Area, *LAC (Location Area Code)*, identifica la Location Area all'interno della rete GSM di appartenenza.

- *CGI - Cell Global Identity*.

Identifica univocamente una cella. E' composta dai campi *LAI (Location Area Identity)*, che identifica la Location Area (LA) a cui appartiene la cella, e *CI (Cell Identity)*, che identifica la cella entro la Location Area.

- *BSIC - Base Station Identity Code*.

Codice che identifica una BTS (Base Transceiver Station). Permette ad una Mobile Station di identificare le BTS su cui si sintonizza per effettuare misure di segnale. E' composto da due campi: *NCC (Network Color Code)*, che identifica la rete GSM a cui appartiene la BTS, e *BCC (Base station Color Code)*, che identifica la BTS.

- *HON - Handover Number*.

E' un numero che viene inviato da un MSC ad un altro MSC affinché tramite la sua analisi possa essere reinstradata una chiamata, nel caso in cui si debba effettuare un handover tra due celle appartenenti ad aree di servizio di MSC/VLR diversi.

[9] A seconda dei casi il numero può provenire da una centrale telefonica PSTN, da un altro utente mobile, etc.

A.6 Esempi di procedure

Si illustrano qui di seguito le principali procedure messe in atto dal sistema GSM per servire i propri utenti.

A.6.1 Chiamata originata da un utente della rete telefonica (PSTN) e terminata su una Mobile Station GSM

La procedura evolve nel seguente modo:

1. L'utente della rete telefonica compone il numero di telefono della MS, denominato MSISDN.
2. La centrale telefonica a cui fa capo il chiamante analizza il numero MSISDN ed in base al campo NDC (National Destination Code) si accorge che è il numero di una Mobile Station (di un cellulare). Attraverso la rete di segnalazione a canale comune, CCSS7, la centrale telefonica inoltra il numero MSISDN al GMSC (Gateway MSC) della rete GSM a cui appartiene la MS chiamata ed instaura una connessione (eventualmente coinvolgendo altre centrali di transito) che parte dal chiamante e giunge fino al GMSC.
3. Il GMSC analizza l'MSISDN e determina l'HLR presso cui è registrata la MS. Quindi, attraverso la rete CCSS7, invia all'HLR un messaggio del protocollo MAP[10] che richiede il numero da analizzare (l'MSRN) per instradare la chiamata verso l'MSC/VLR nella cui area di servizio si trova la MS da raggiungere.
4. L'HLR traduce l'MSISDN nell'IMSI (identità dell'utente mobile) e, sempre attraverso la rete CCSS7, con un altro messaggio del protocollo MAP richiede il numero MSRN al VLR presso cui la MS è registrata.
5. Il VLR fornisce l'MSRN all'HLR che a sua volta lo fornisce al GMSC. Il GMSC analizza l'MSRN ed instrada la chiamata verso l'MSC/VLR che serve la MS. A questo punto è stata instaurata una connessione che parte dal chiamante e giunge fino all'MSC di destinazione.
6. Il VLR utilizza l'IMSI per ricercare la location area in cui è presente la MS chiamata. Con un messaggio del protocollo BSSMAP, il VLR ordina al/ai BSC che fanno parte della location area di far irradiare dalle BTS da essi controllate, sul canale logico PCH, il messaggio di paging con il quale la MS viene chiamata. Il messaggio di paging contiene usualmente l'identità temporanea della MS chiamata (TMSI).
7. La MS chiamata risponde inviando sul canale logico RACH una richiesta di accesso. Attraverso il canale logico AGCH, il BSC assegna alla MS un canale di controllo dedicato (SDCCH). Si instaura quindi un collegamento di segnalazione che consente alla MS di colloquiare con l'MSC/VLR. La MS si sposta sul canale dedicato ed ha inizio un colloquio di segnalazione, con protocollo DTAP, tra MS e VLR. In particolare il VLR effettua l'autenticazione della MS, per accertare che essa abbia diritto ad accedere alla rete, ordina il passaggio in modalità cifrata, impegna un canale verso il BSC e richiede a quest'ultimo che venga assegnato alla MS un canale di traffico (TCH) sul quale possa avvenire la trasmissione di informazioni via radio, tra BTS e MS. In questo modo si prepara una connessione che parte dall'utente chiamante e giunge fino alla BTS della cella in cui è presente la MS chiamata; nel contempo la MS genera localmente l'avviso di chiamata per l'utente mobile (squilla il telefonino). Non appena l'utente chiamato risponde, la MS passa sul canale di traffico assegnatole e può avere inizio la conversazione tra utente chiamante e utente mobile chiamato.
8. Quando un utente riaggancia viene inviato un messaggio con il quale si richiede l'abbattimento della connessione ed il rilascio delle risorse impegnate.

A.6.2 Chiamata originata da una Mobile Station GSM

Nel caso di chiamata originata da una Mobile Station l'evoluzione della procedura è la seguente:

1. La MS invia sul canale RACH una richiesta di accesso, che attraverso la BTS viene inoltrata al BSC.
2. Il BSC, attraverso il canale AGCH, assegna un canale di controllo dedicato (SDCCH) sul quale avviene il colloquio di segnalazione preliminare tra MS e VLR. Si instaura una connessione di segnalazione tra MS e MSC/VLR sulla quale avviene l'autenticazione, il passaggio in modalità cifrata sulla tratta radio, l'invio da parte della MS del numero dell'utente chiamato (messaggio di "setup").
3. Il VLR richiede che venga assegnato alla MS un canale di traffico e viene preparata una connessione di terra tra la BTS che serve la Mobile Station e l'MSC/VLR.

[10] Il messaggio in questione è il seguente "send routing information" (invia le informazioni necessarie per l'instradamento).

4. L'MSC/VLR analizza il numero del chiamato ed instaura una connessione (eventualmente attraverso altre centrali di transito) con la centrale a cui fa capo il chiamato.
5. Non appena il chiamato risponde si informa di ciò la MS, che passa sul canale di traffico assegnatole. Può così avere inizio la conversazione tra chiamante e chiamato.
6. Quando un utente riaggancia viene inviato un messaggio con il quale si richiede l'abbattimento della connessione ed il rilascio delle risorse impegnate.

A.6.3 Handover

Viene denominata *handover* la procedura con la quale si effettua un cambio di canale di comunicazione nel corso di una conversazione (o più in generale di un collegamento dedicato su TCH o SDCCH).

In questo modo si evita che venga interrotta una comunicazione in corso per qualità e/o livello di ricezione insufficienti, tipicamente dovuti al passaggio della MS da una cella ad un'altra.

L'unità funzionale che decide quando è necessario effettuare un handover è il BSC, in quanto esso riceve (ogni 480 [ms]) i risultati delle misure che MS e BTS effettuano per definire la qualità di una conversazione in corso.

Le misure effettuate dalla MS sono le seguenti:

- Livello di ricezione sul canale di traffico per la tratta downlink.
- Qualità (BER) del segnale ricevuto per la tratta downlink.
- Livello di ricezione della frequenza utilizzata da sei BTS adiacenti per trasmettere i canali logici di controllo (FCCH, SCH, etc.).

Le misure effettuate dalla BTS sono le seguenti:

- Livello di ricezione sul canale di traffico (TCH) per la tratta uplink.
- Qualità (BER) del segnale ricevuto per la tratta uplink.
- Distanza MS-BTS, valutata per mezzo del timing advance.

Le BTS inoltre determinano il livello di interferenza sui canali liberi.

Le misure effettuate vengono inoltrate al BSC, il quale le elabora ed è in grado di determinare:

- quando un canale di traffico non è più adatto a garantire una buona qualità di conversazione e quindi è necessario effettuare un handover;
- qual è la BTS che è in grado di servire al meglio la MS.
- qual è il nuovo canale di traffico sul quale far spostare la MS per proseguire la conversazione con buona qualità.

Si sottolinea che la decisione di effettuare un handover in base ai risultati delle misure è sempre una decisione autonoma del BSC che controlla la BTS a cui è inizialmente agganciata la MS.

I risultati delle misure vengono utilizzati dal BSC anche per determinare i livelli di trasmissione ottimali per MS e BTS, cioè per il controllo della potenza di MS e BTS (power control).

Un handover può anche essere ordinato (dall'MSC) per motivi di traffico (cella sovraccaricata) e per motivi legati alla manutenzione degli impianti (un transceiver viene momentaneamente escluso).

In generale la procedura di handover evolve nel seguente modo:

1. Il BSC riceve i risultati delle misure, li elabora e li confronta con delle soglie predefinite.
2. Quando un parametro (livello di ricezione, qualità, distanza, etc.) va sotto soglia il BSC decide l'effettuazione di un handover e determina qual è la BTS più adatta per servire la MS.
3. Viene preparato un collegamento verso la nuova BTS e si riserva su essa un canale di traffico libero (il migliore).
4. Non appena tutto è pronto viene inviato alla MS, sul canale logico FACCH, l'ordine di effettuazione dell'handover.
5. La MS si sposta sul nuovo canale di traffico assegnatole.
6. Vengono rilasciate le risorse non più utilizzate (vecchio canale di traffico e canali di terra precedentemente impegnati).

A seconda delle unità funzionali che vi prendono parte, si distinguono i seguenti tipi di handover:

- Handover intra-cella.

Il BSC ordina alla MS di effettuare un cambio di canale all'interno della stessa cella (non si cambia BTS), tipicamente nel caso in cui con il canale in uso si ha un livello di ricezione adeguato, ma una qualità (BER) scadente.

- Handover inter-cella tra BTS controllate dallo stesso BSC.

E' necessario ordinare un handover verso una nuova BTS, in quanto la MS è passata da una cella all'altra; entrambe le BTS sono però controllate dallo stesso BSC. L'effettuazione dell'handover è controllata dal BSC, che comunque informa l'MSC/VLR dell'avvenuto handover.

- Handover inter-cella tra BTS controllate da BSC diversi, ma facenti capo allo stesso MSC/VLR.

Il BSC che controlla la BTS a cui è inizialmente agganciata la MS decide che è necessario effettuare un handover e, visto che la nuova BTS è controllata da un altro BSC, chiede all'MSC/VLR di sovrintendere all'effettuazione dell'handover. L'MSC/VLR ordina al nuovo BSC di preparare una connessione di terra verso la nuova BTS e di riservare su essa un canale di traffico libero. Quando tutto è pronto l'MSC comanda al vecchio BSC di ordinare (tramite la BTS) alla MS l'effettuazione dell'handover, cioè di cambiare il canale di traffico. Vengono quindi rilasciate le risorse non più utilizzate.

- Handover inter-cella tra BTS controllate da BSC diversi, facenti capo a MSC/VLR diversi.

E' il caso più complesso. Oltre alle azioni citate nel punto precedente, è infatti necessario reinstradare completamente la chiamata che, partendo dal vecchio MSC/VLR, deve ora giungere al nuovo MSC/VLR. Per effettuare il reinstradamento della chiamata l'MSC/VLR di partenza chiede (attraverso il CCSS7) al nuovo MSC/VLR che gli venga fornito l'*handover number (HON)*. La procedura prosegue poi come delineato al punto precedente.

A.7 Raccomandazioni relative al GSM e al GPRS

Nelle raccomandazioni GSM, note come *GSM Technical Specifications*, vengono specificate nel dettaglio le funzioni che devono essere svolte e le interfacce tra i vari elementi del sistema GSM. Non si entra invece nel merito di come tali funzioni vengono realizzate, cioè dell'hardware che si impiega. Le specifiche tecniche GSM originarie sono racchiuse in 12 serie di raccomandazioni, riportate in Tab. A.1.

L'attività di standardizzazione è iniziata in ambito ETSI a cura di Comitati tecnici (ETSI Subtechnical Committees) denominati SMG (Special Mobile Group), come indicato in Tab. A.2. Attualmente la standardizzazione è a carico del 3GPP (3rth Generation Partnership Project).

Tab. A.1 Specifiche tecniche GSM originarie.

GSM Technical Specification	
01	Generalità (General Description of a GSM PLMN).
02	Servizi (Services aspects).
03	Aspetti di rete (Network aspects).
04	Interfaccia e protocolli tra Mobile Station e Base Station Subsystem (MS-BSS Interface & protocols).
05	Strato fisico sul percorso radio (Physical Layer on the radio path).
06	Codifica ed elaborazione del segnale vocale (Speech processing functions).
07	Adattatori di terminali per le stazioni mobili (Terminal adaptors for MS).
08	Interfaccia tra Base Station Subsystem e Mobile Services switching Centre (BSS-MSC Interface).
09	Interconnessione con altre reti (Network interworking).
[10]	[Services Interworking]. E' stata rimossa.
11	Specifiche per l'omologazione di apparati (Equipment & type approval specifications).
12	Esercizio e manutenzione (Operation and maintenance).

Tab. A.2 Comitati tecnici ETSI originari

ETSI Subtechnical Committees	
SMG1:	Services and facilities.
SMG2:	Radio aspects.
SMG3:	Network aspects.
SMG4:	Data services.
SMG5: (UMTS).	Universal Mobile Telecommunications System
SMG6:	Operation & Maintenance.
SMG7:	MS testing.
SMG8:	BSS testing.
SMG9:	SIM Aspects.

Raccomandazioni relative al GPRS

Le Raccomandazioni ETSI e 3GPP relative al GPRS sono immerse nelle serie GSM .
Segnaliamo qui di seguito alcune Raccomandazioni (scaricabili gratuitamente dal sito www.etsi.org):

- GSM 01.02 Digital cellular telecommunications system (Phase 2+); General description of a GSM Public Land Mobile Network;
- GSM 01.04 Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms;
- GSM 02.06 Digital cellular telecommunications system (Phase 2+); Types of Mobile Stations (MS);
- GSM 02.60 Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 1;
- GSM 03.02 Digital cellular telecommunications system (Phase 2+); Network architecture;
- GSM 03.03 Digital cellular telecommunications system (Phase 2+); Numbering Addressing and identification;
- GSM 03.60 Digital cellular telecommunications system (Phase 2+); Overall description of the General Packet Radio Service (GPRS); Stage 2;
- GSM 03.64 Digital cellular telecommunications system (Phase 2+); Overall description of the General Packet Radio Service (GPRS) Radio interface; Stage 2;
- GSM 04.60 Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); MS – BSS interface; Radio Link Control / Medium Access Control (RLC/MAC) protocol;
- GSM 04.64 Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Logical Link Control (LLC);
- GSM 04.65 Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Subnetwork Dependent Convergence Protocol (SNDCP);
- GSM 05.01 Digital cellular telecommunications system (Phase 2+); Physical layer on the radio path, General description;
- GSM 05.02 Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path;
- GSM 05.03 Digital cellular telecommunications system (Phase 2+); Channel coding;
- GSM 07.60 Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station Supporting GPRS;
- GSM 09.60 Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP);
- GSM 09.61 Digital cellular telecommunications system (Phase 2+); General requirements on interworking between the PLMN supporting General Packet Radio Service (GPRS) and Packet Data Networks;

Altri standard di interesse per il GPRS sono quelli promulgati dall'IETF (Internet Engineering Task Force) e relativi alla suite di protocolli TCP/IP; in particolare si citano i seguenti:

- RFC 791 Internet Protocol;
- RFC 792 Internet Control Message Protocol;
- RFC 793 Transmission Control Protocol;
- RFC 768 User Datagram Protocol;

RFC 1034 Domain Names – Concepts and Facilities.