GSM™
The wireless evolution

Global System for mobile communications

Sicurezza e Autenticazione

Sicurezza Riservatezza Autenticazione

- L'aspetto più vulnerabile di un sistema di comunicazione radiomobile è rappresentato dal canale radio al quale chiunque può accedere.
- ...bisogna garantire sicurezza e riservatezza
- L'autenticazione elemento fondamentale. Inammissibile la copia dei dati di un utente
- I sistemi analogici contro quelli digitali
  - Sistema analogico
    - Semplice l'intercettazione con radio scanner anche per dilettanti
  - Sistema digitale GSM
    - Il meccanismo di sicurezza ed autenticazione inglobato nel sistema GSM rende lo standard di comunicazione radiomobile il più sicuro attualmente disponibile, specie se confrontato ai sistemi analogici.
- Il sistema GSM è un sistema digitale che fra l'altro utilizza:
  - Un algoritmo di codifica vocale, modulazione digitale GMSK (*Gaussian minimun Shift Keying*), FrequencyHopping e architettura a slot con accesso al canale tramite TDMA.

Crittografia

- Algoritmi Simmetrici
  - Block Ciphers (cifratori a blocco)
  - Stream Ciphers (cifratori a flusso)
- Algoritmi a chiave pubblica
- One way hash functions

Dimensione della chiave

- Nel valutare l'affidabilità di un algoritmo si deve considerare la "durata" delle informazioni che devono essere protette.

Dimensione chiave in bit	32	40	56	64	128
Tempo richiesto per verificare tutte le possibili chiavi	1,19h	12,7giorni	2291anni	584542anni	$10,8*10^{24}$anni

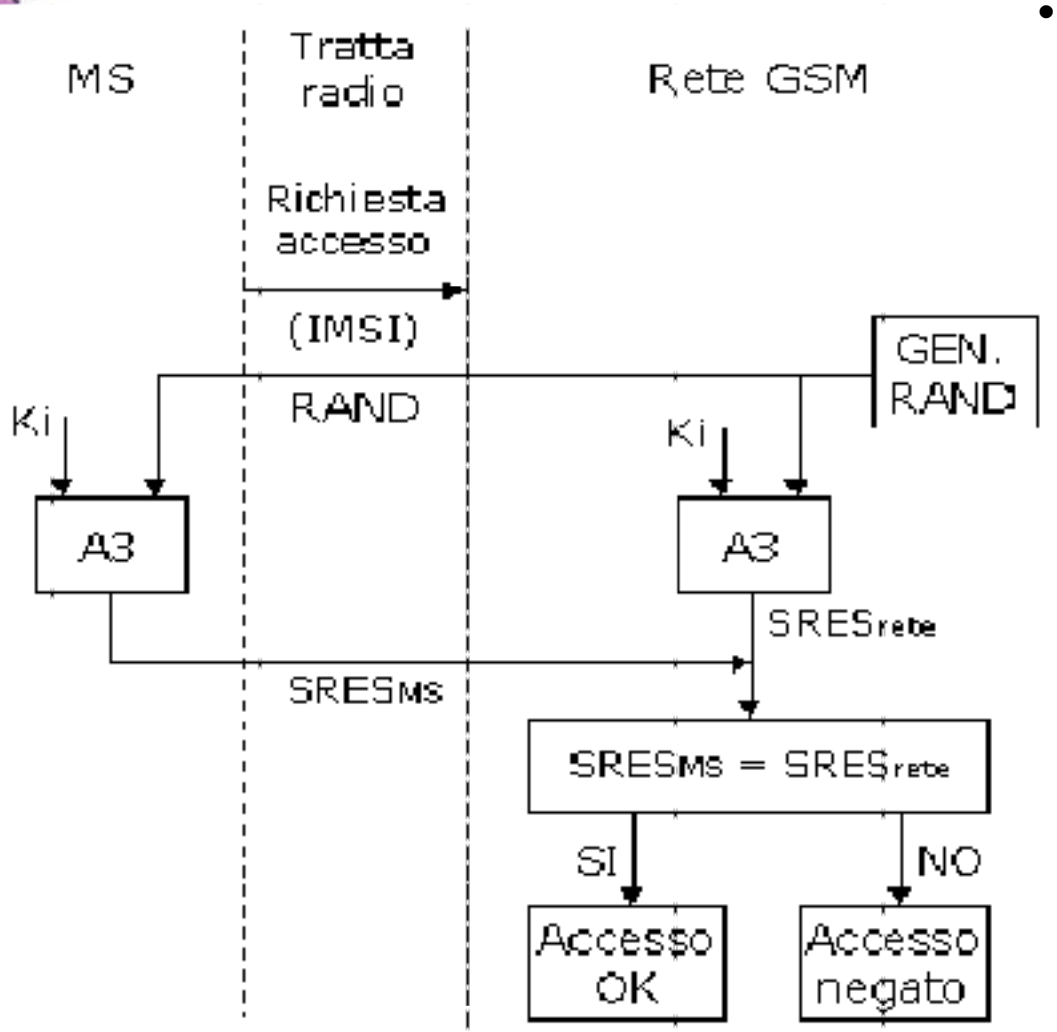
Autenticazione

- Le procedure di autenticazione e crittografia prevedono che le informazioni cruciali non vengano mai trasmesse sul canale radio. Per l'autenticazione è utilizzato un meccanismo di tipo *challenge-response*; mentre per la crittografia dei dati trasmessi viene usata una chiave temporanea **Kc** ed anch'essa non viene mai trasmessa sul canale radio.
- la distribuzione fornisce una ulteriore misura di sicurezza; gli elementi in gioco sono: la SIM, il MT e la rete GSM
  - La SIM contiene il codice **IMSI**, la chiave personale di autenticazione **Ki**, l'algoritmo **A8** che genera la chiave temporanea di crittografia **Kc**, l'algoritmo **A3** di autenticazione e il *Personal Identification Number* (**PIN**) assieme a molti altri dati
  - Il terminale mobile **MT** contiene l'algoritmo **A5** di crittografia.
  - Nella rete GSM le informazioni sono ulteriormente distribuite. Nella Base Transceiver Station (BTS) sono contenuti l'algoritmo A5 e in fase di crittografia la chiave Kc. Alla base dei processi di crittografia e autenticazione è l'unità funzionale Authentication Centerche ha a disposizione i codici **TMSI / IMSI**, il codice LAI, la chiave Ki e gli algoritmi A3 e A8 oltre ad un algoritmo per la generazione di numeri pseudocasuali. L'AuC memorizza nei database VLR e HLR i parametri di sicurezza.

Autenticazione (2)

- La procedura di autenticazione viene avviata ogniqualvolta la Mobile Station (MS) si collega alla rete
- Le unità funzionali in gioco nel processo di autenticazione sono: la SIM nel terminale e l'AuC (*Authentication Center*) nella home network
- L'autenticazione avviene adottando un meccanismo di tipo challenge-response. Nel momento in cui l'AuC riceve una richiesta di autenticazione, riconosce (vedremo in seguito come) la probabile identità dell'utente, genera e trasmette al Mobile Station (MS) un numero casuale di 128 bit (**RAND**) come sfida (*challenge*). La MS riceve e trasmette alla SIM la sfida. La SIM calcola la risposta (*response*) **SRES** di 32 bit alla sfida dando in input all'algoritmo di autenticazione **A3** (*key-dependent one-way hash function*) il numero casuale (RAND) e la chiave di autenticazione dell'utente Ki, che ha una lunghezza di 128 bit ed è memorizzata nella stessa SIM. La risposta "firmata" SRES viene trasmessa alla visited network dove viene confrontata con il valore che la home network ha calcolato applicando lo stesso algoritmo A3 al numero casuale RAND e alla chiave Ki corrispondente alla identità dichiarata dall'utente (di cui conserva copia).

Autenticazione (3)

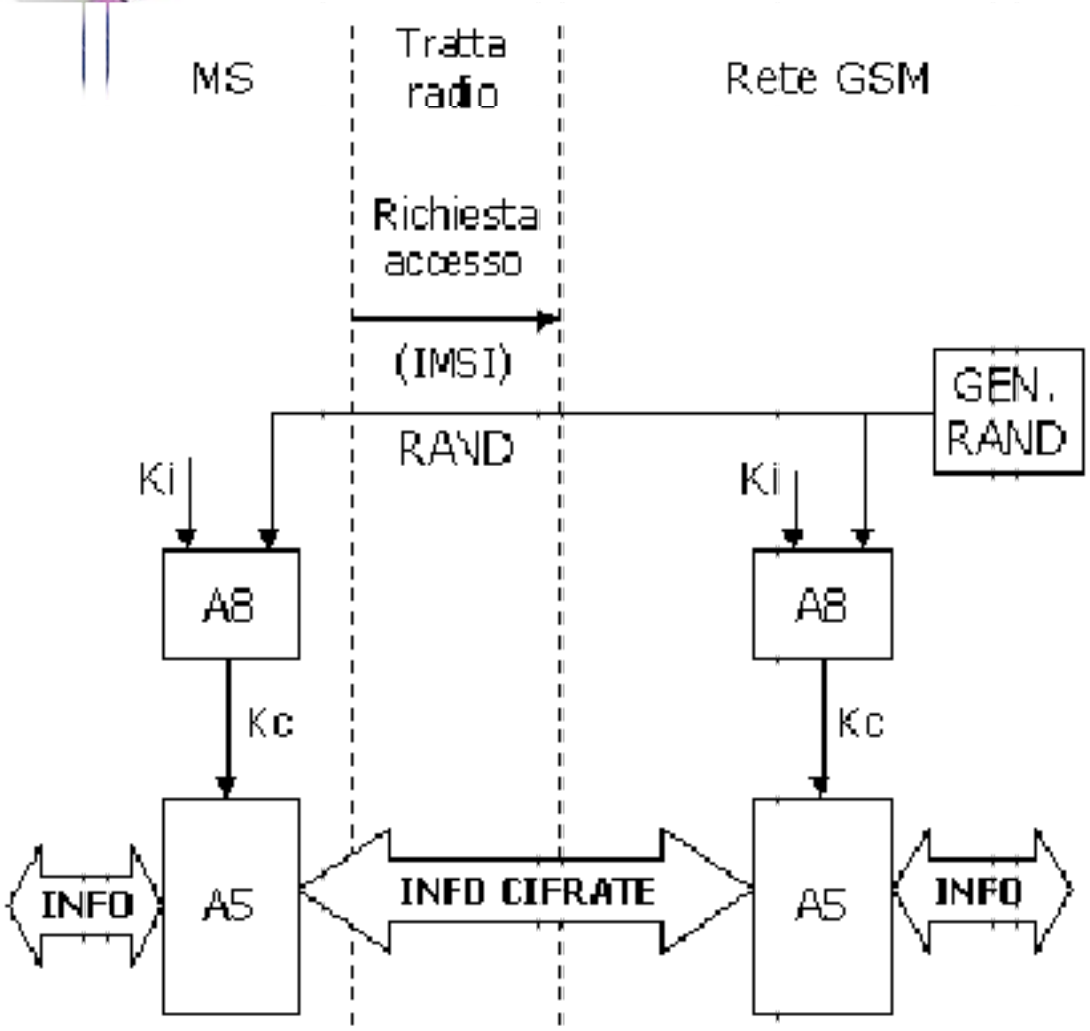


- Possiamo notare come la chiave personale di autenticazione Ki non venga mai trasmessa sul canale radio. Essa è presente nella SIM come pure nell'AuC come descritto precedentemente. Inoltre il calcolo della response viene effettuato all'interno della SIM e le informazioni riservate dell'utente, come il codice IMSI e la chiave Ki, non vengono mai rilasciate dalla SIM durante la fase di autenticazione. Questo fornisce una sicurezza ulteriore.

Riservatezza

- Uno dei nuovi servizi di sicurezza offerti dal sistema GSM è la possibilità di crittografare il collegamento tra la Mobile Station e la Base Transceiver Station (BTS).
- L'algoritmo che viene utilizzato per la crittografia è indicato con la sigla **A5**
  - A5 è un codificatore di tipo stream cipher che, utilizzando una chiave di cifratura **Kc** di 64 bit e il numero della trama TDMA di 22 bit, produce una sequenza di 114 bit (*keystream*) che viene utilizzata per crittografare i 114 bit significativi di ogni burst (cioè i due blocchi di 57 bit) attraverso un exclusive-or XOR
- La chiave di cifratura Kc utilizzata dall'algoritmo A5 viene generata all'interno della SIM e contemporaneamente nella home network dall'AuC attraverso l'algoritmo di generazione della chiave di cifratura **A8** (specifico dell'operatore), durante la fase ci autenticazione
  - A8 è una *key-dependent one-way hash function* in ingresso alla quale vengono posti: il numero casuale utilizzato nella fase di autenticazione (RAND) e la chiave di autenticazione Ki (ovvero gli stessi input utilizzati nella fase di autenticazione).

Riservatezza (2)



- Nel caso in cui si riuscisse a superare la procedura di autenticazione, ad esempio manipolando il confronto tra challenge e response, Mobile Station e Base Station utilizzerebbero chiavi di cifratura diverse risultando incomprensibili l'una all'altra.
- La chiave Kc è diversa ad ogni collegamento (viene generata una nuova Kc ogni volta che si esegue la procedura di autenticazione), dipendendo da RAND. Un ulteriore livello di sicurezza può essere raggiunto consentendo di modificare la chiave Kc ad intervalli regolari di tempo, secondo le esigenze della rete .

Riservatezza dell'abbonato

- Le procedure di sicurezza si propongono di non trasmettere mai sul canale radio le credenziali di identificazione: codice IMSI e chiave Ki. Per evitare ad esempio che possa essere monitorata la posizione dell'utente intercettandone sul canale radio l'identità etc.
- La vera identità della SIM viene trasmessa (per forza di cose) dalla MS sul canale radio, la prima volta che si usa la SIM ad esempio.
- Una volta conclusosi il processo di autenticazione la rete assegna alla SIM un **TMSI**, e lo trasmette, dopo che è stato attivato il processo di crittografia, in forma cifrata alla MS dove viene decifrato. La MS risponde confermando l'avvenuta ricezione e memorizza il TMSI nella SIM. Il codice TMSI viene da quel momento in poi utilizzato al posto del codice IMSI, dove ciò sia possibile, fino a che un nuovo TMSI non venga assegnato alla SIM.
- Ogni volta che si esegue una Location Updating cioè l'utente passa da una Location Area ad un'altra, il VLR assegna una nuova TMSI alla MS e la invia assieme al messaggio che comunica l'aggiornamento della localizzazione (Location Updating Accept). Alla ricezione di questo messaggio, la MS risponde con un messaggio di conferma (*TMSI Reallocation Complete*).

...e ancora

- Un altro livello di sicurezza è implementato nel Mobile Equipment (ME). Ogni terminale GSM è identificato univocamente dall'IMEI.
  - Come abbiamo visto è perciò previsto un particolare registro (**EIR**) che consente di memorizzare i codici IMEI e verificare quelli corrispondenti a ME cui non è consentito l'accesso alla rete (black list).
- la stessa SIM implementa un ulteriore livello di sicurezza confrontando il *Personal Identification Number* (**PIN**) digitato dall'utente con il valore di riferimento contenuto in memoria. Tale confronto è effettuato dalla CPU della SIM e permette, ancora una volta, di non rilasciare il valore all'esterno
  - Lo standard GSM ha poi previsto successivamente, oltre alla gestione dei PIN, l'introduzione di un *PIN Unblocking Key* (**PUK**) che consente di sbloccare la SIM. Quest'ultimo non può però essere modificato ed è fornito dall'operatore all'utente a specifiche condizioni di sicurezza. Dopo dieci tentativi errati di inserimento per il codice PUK la SIM risulta permanentemente bloccata.

Per concludere...

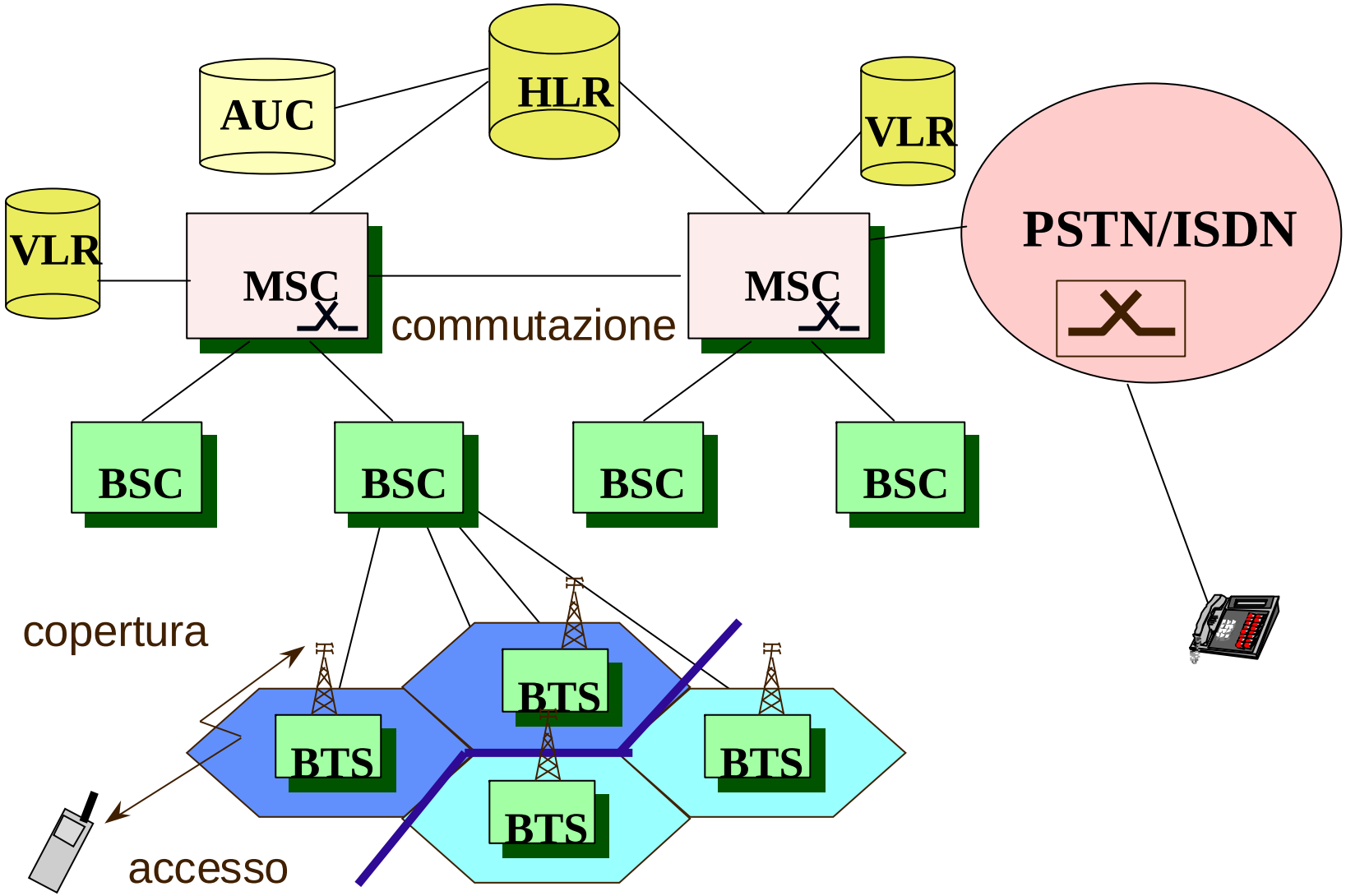
- Vari scienziati nel mondo sembrano essere unanimi sul fatto che l'intercettazione e la decodifica real-time di una chiamata via-etere sia ancora impossibile nonostante lo spazio delle chiavi sia ridotto. Ci sono, tuttavia, altri tipi di attacchi al sistema che sono attuabili e sembrano essere minacce molto reali. Sono stati, infatti, implementati alcuni attacchi che non sfruttano nessuno dei difetti trovati dalle agenzie governative degli algoritmi di sicurezza.
- Non solo, dopo la BTS, i segnali vengono trasmessi in chiaro nelle operazioni di rete. La rete di segnalazione SS7 utilizzata dagli operatori della rete GSM è completamente insicura se l'attaccante ne guadagna l'accesso diretto
- Non è inoltre esclusa la possibilità di accedere al cavo di uscita della BTS
- La sicurezza dell'intero modello GSM è basata sulla chiave segreta K_i. Se la chiave venisse scoperta l'intero accesso alla rete sarebbe compromesso. Una volta recuperata la chiave K_i, l'attaccante non solo può ascoltare le chiamate dei sottoscrittori, ma anche addebitare le proprie chiamate sul conto dell'abbonato di cui si è recuperata *la chiave segreta*

GSM™
The wireless evolution

Global System for mobile communications

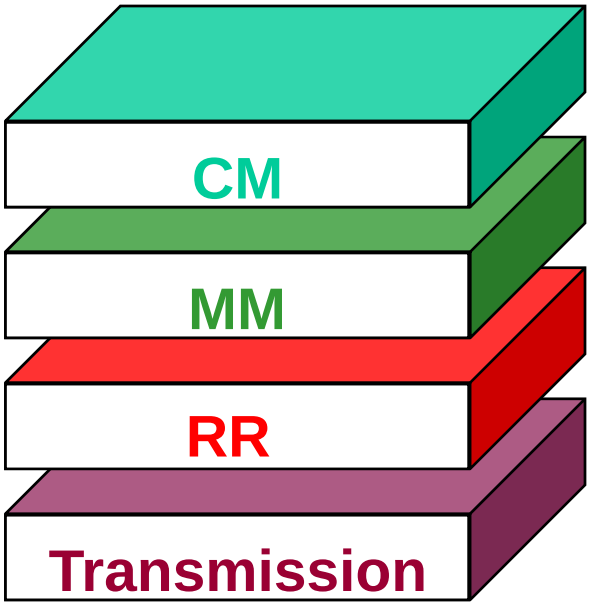
GSM – Switching & Mobility

Rete GSM


AUC
HLR
VLR
VLR
MSC
MSC
commutazione
PSTN/ISDN
BSC
BSC
BSC
BSC
copertura
BTS
BTS
BTS
BTS
accesso

Architettura GSM

- E' composta da quattro piani funzionali
  - Transmission
    - gestisce il mezzo trasmissivo
  - Radio Resource Management (RR)
    - fornisce un link stabile tra la MS e l'MSC
  - Mobility Management (MM)
    - gestisce i data base per la localizzazione della MS
  - Communication Management (CM)
    - fornisce i mezzi per le comunicazioni d'utente



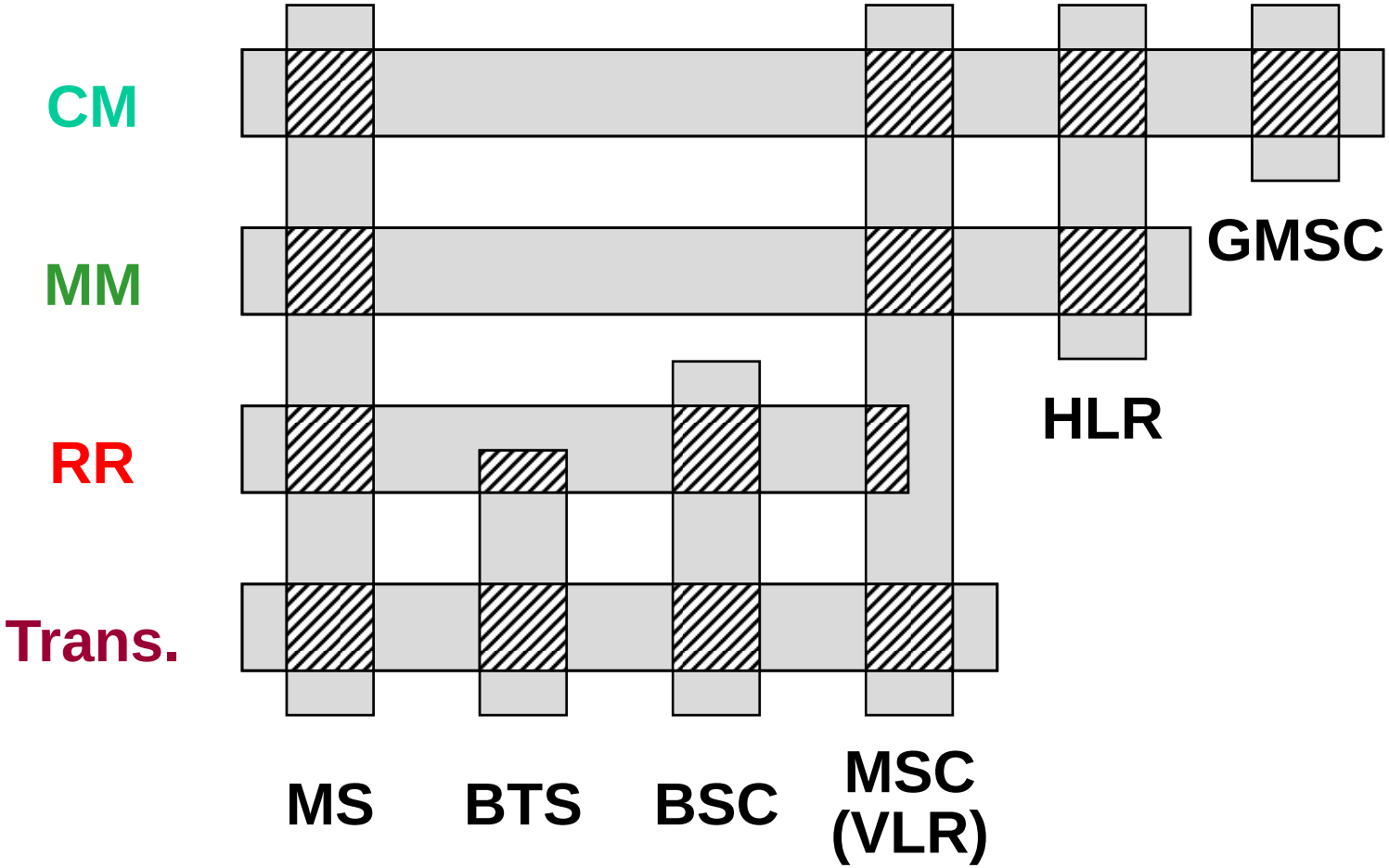
Architettura GSM

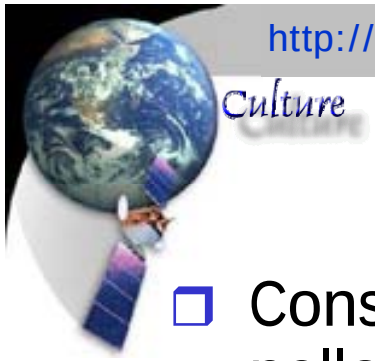
- Trasmissione
  - Fornisce i mezzi per trasferire informazione di utente (voce e dati) su tutti i segmenti tra macchine remote nel percorso della comunicazione (MS-BTS-BSC-MSC(s)-GMSC-reti esterne)
  - Fornisce i mezzi per trasferire segnalazione tra entità GSM
  - Include funzioni dello strato fisico (modulazione, codifica, accesso multiplo TDM e FDM) e degli strati di collegamento e di rete (queste ultime solo per la segnalazione)
- Radio Resource
  - Coinvolge soprattutto la MS e la BSC, ma anche BTS e MSC (inter-MSC handover)
  - Le funzioni essenziali sono accesso iniziale, paging e handover

Architettura GSM

- Mobility Management
  - Coinvolge la SIM nella MS e le basi di dati HLR e VLR.
- Communication Management
  - Call Control
    - Coinvolge gli MSC/VLR, i GMSC, l'HLR
    - Le funzioni essenziali instaurazione, mantenimento e abbattimento delle chiamate e instradamento delle stesse
  - Supplementary Services Management
    - Coinvolge solo la MS e l'HLR
  - Short Message Service
    - Per i messaggi punto-punto agisce un cosiddetto Short Message Service Centre (SM-SC)

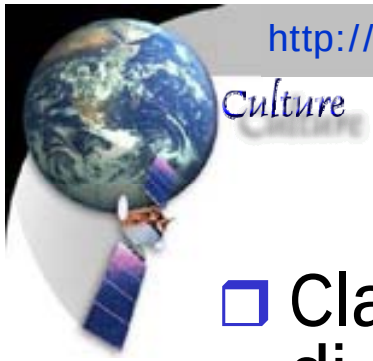
Architettura GSM





Funzione di handover

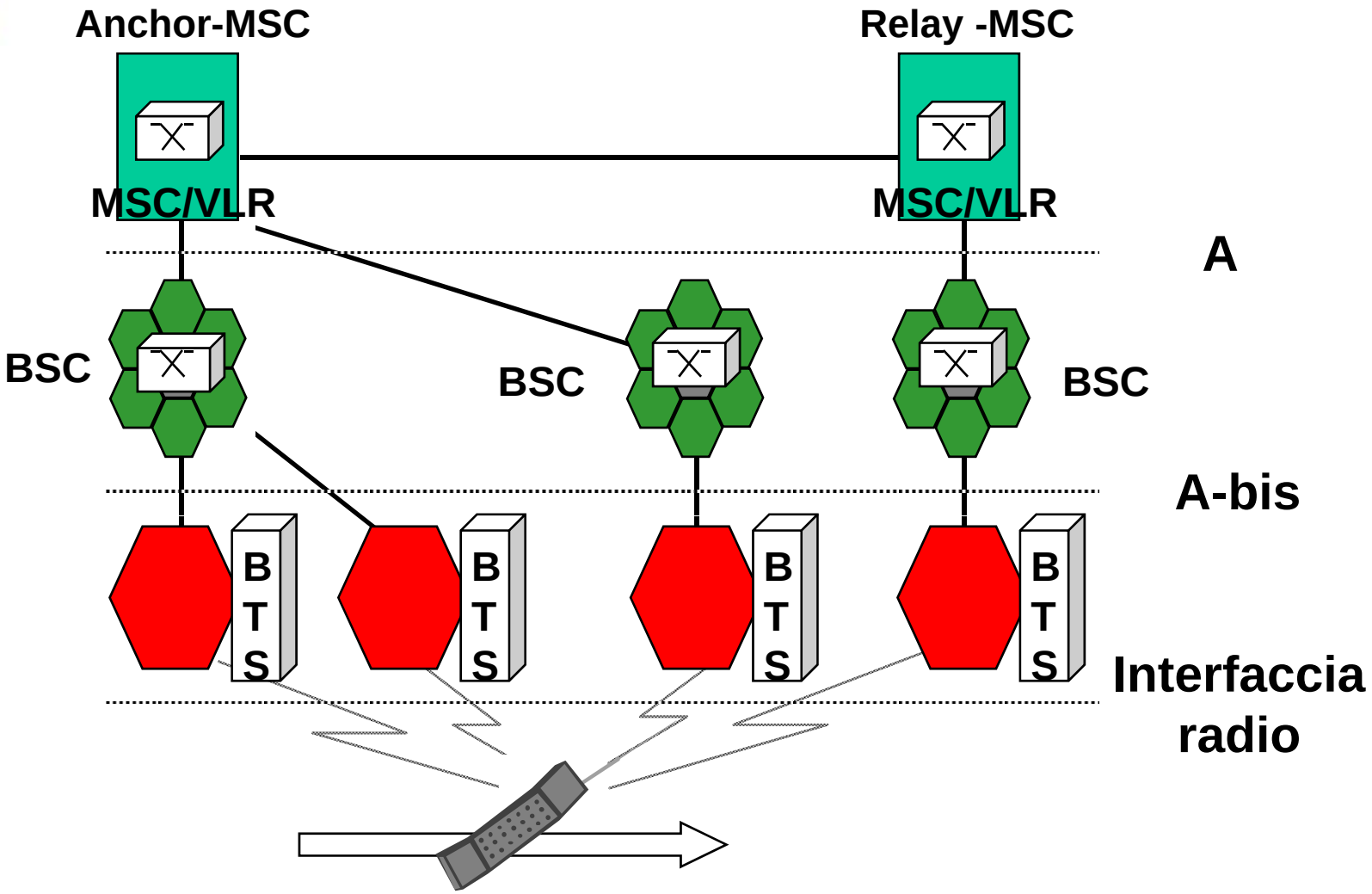
- Consente il cambio di canale radio mentre la MS è nello stato “dedicato”, senza interruzione della comunicazione
- Classificazione dell’handover in relazione alla causa
  - Rescue Handover
    - è provocato da condizioni di degradazione della qualità del canale radio (rischio di interruzione della comunicazione, cut-off)
  - Confinement Handover
    - si pone l’obiettivo di minimizzare l’interferenza globale nell’interfaccia radio; a tale scopo, confina le MS in un'area geografica ottimale in relazione all'interferenza complessiva
  - Traffic Handover
    - si applica in caso di sovraccarico di una cella passando, se possibile, utenti a celle adiacenti più scariche



Funzione di handover

- Classificazione degli handover secondo il punto di scambio
  - Intra BTS
    - si ha cambio di canale nell'interfaccia radio con la stessa BTS (stessa cella)
  - Inter BTS (Intra BSC)
    - il nuovo canale appartiene ad una diversa BTS, ma sempre sotto il controllo della stessa BSC
  - Inter BSC (Intra MSC)
    - il nuovo canale è gestito da una nuova BCS, ma sempre sotto il controllo dello stesso MSC
  - Inter MSC
    - si ha transizione tra due aree gestite da due MSC diversi (R-MSC)

Funzione di handover



Funzione di handover

- La decisione di effettuare l'handover è sempre del BSC
- Il BSC decide di attivare la procedura sulla base di misure di qualità di trasmissione effettuate dalla MS e dalla BTS, indicando al R-MSC una lista di celle candidate
- L'R-MSC sceglie la cella destinazione migliore, mediando tra considerazioni radio (elaborate dal BSC) e considerazioni di traffico
- In caso di cella di destinazione gestita da un altro MSC, la gestione della procedura passa all'A-MSC

Funzione di handover

- Un handover di qualunque tipo richiede
  - La fase di preparazione
    - Si raccolgono misure sul canale radio utilizzato e sulle BTS vicine
  - La fase di decisione
    - Le misure raccolte sono elaborate (principalmente dal BSC) in un algoritmo che può innescare un handover, indicando una o più BTS candidate
  - La fase di esecuzione
    - Sotto il coordinamento del punto di “scambio”, si instaura un percorso trasmissivo completo attraverso una delle BTS candidate e si rilascia il vecchio percorso, commutando la comunicazione sul nuovo

Misure per handover

- I parametri presi in esame nei criteri di handover sono
  - Dati statici
    - Max potenza della MS, della BTS che la serve e di quelle limitrofe
    - Configurazione delle celle confinanti
  - Misure in tempo reale eseguite dalla MS
    - La qualità trasmissiva del downlink (BER)
    - Il livello di ricezione sul downlink del canale radio in uso
    - Il livello di ricezione dalle BTS limitrofe
  - Misure in tempo reale eseguite dalla BTS
    - La qualità trasmissiva dell'uplink (raw BER)
    - Il livello di ricezione sull'uplink del canale radio in uso
    - il valore di TA (Tempo di Anticipo)

Handover preparation

➔ Measurements performed at BTS

- ⇨ Up-link signal level received from MS lower than threshold
  - →RXLEV_UL < L_RXLEV_UL_H
- ⇨ Up-link signal quality (BER) received from MS
  - →RXQUAL_UL < L_RXQUAL_UL_H
- ⇨ Distance between MS and BTS
  - →adaptive timing advance parameter > MAX_MS_RANGE
- ⇨ Interference level in unallocated time slots.

➔ Measurements performed at MS.

- ⇨ Down-link signal level received from serving cell
  - →RXLEV_DL < L_RXLEV_DL_H
- ⇨ Down-link signal quality (BER) received from serving cell
  - →RXQUAL_DL < L_RXQUAL_DL_H
- ⇨ Down-link signal level received from *n*-th neighbor cell
  - →RXLEV_NCELL(n) > RXLEV_MIN(n)

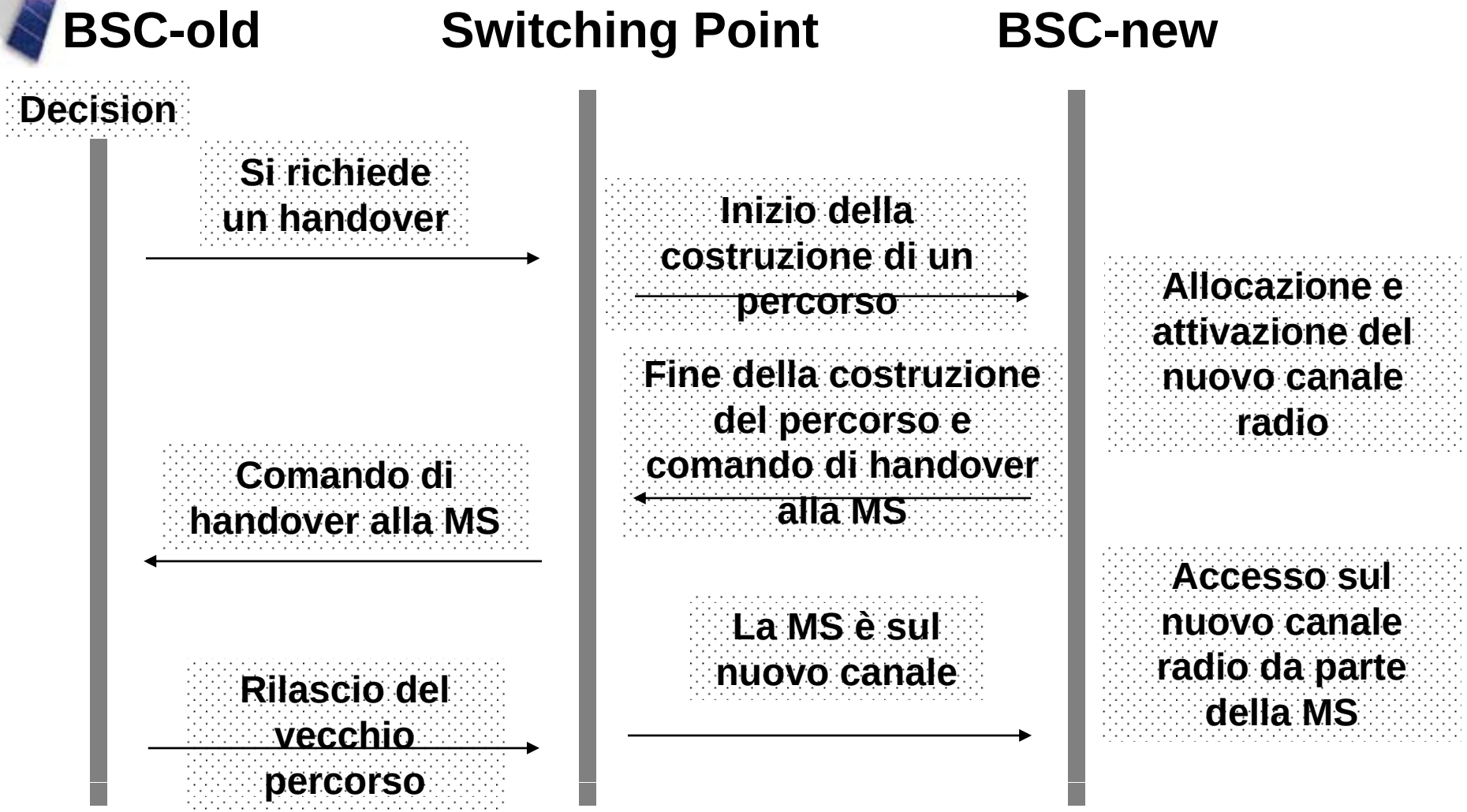
RX signal level	From (dBm)	To (dBm)
RXLEV_0	-	-110
RXLEV_1	-110	-109
RXLEV_2	-109	-108
RXLEV_3	-108	-107
…	…	…
…	…	…
RXLEV_62	-49	-48
RXLEV_63	-48	-

Bit error Ratio	From (%)	To (%)
RXQUAL_0	-	0.2
RXQUAL_1	0.2	0.4
RXQUAL_2	0.4	0.8
RXQUAL_3	0.8	1.6
RXQUAL_4	1.6	3.2
RXQUAL_5	3.2	6.4
RXQUAL_6	6.4	12.8
RXQUAL_7	12.8	-

Procedura di handover

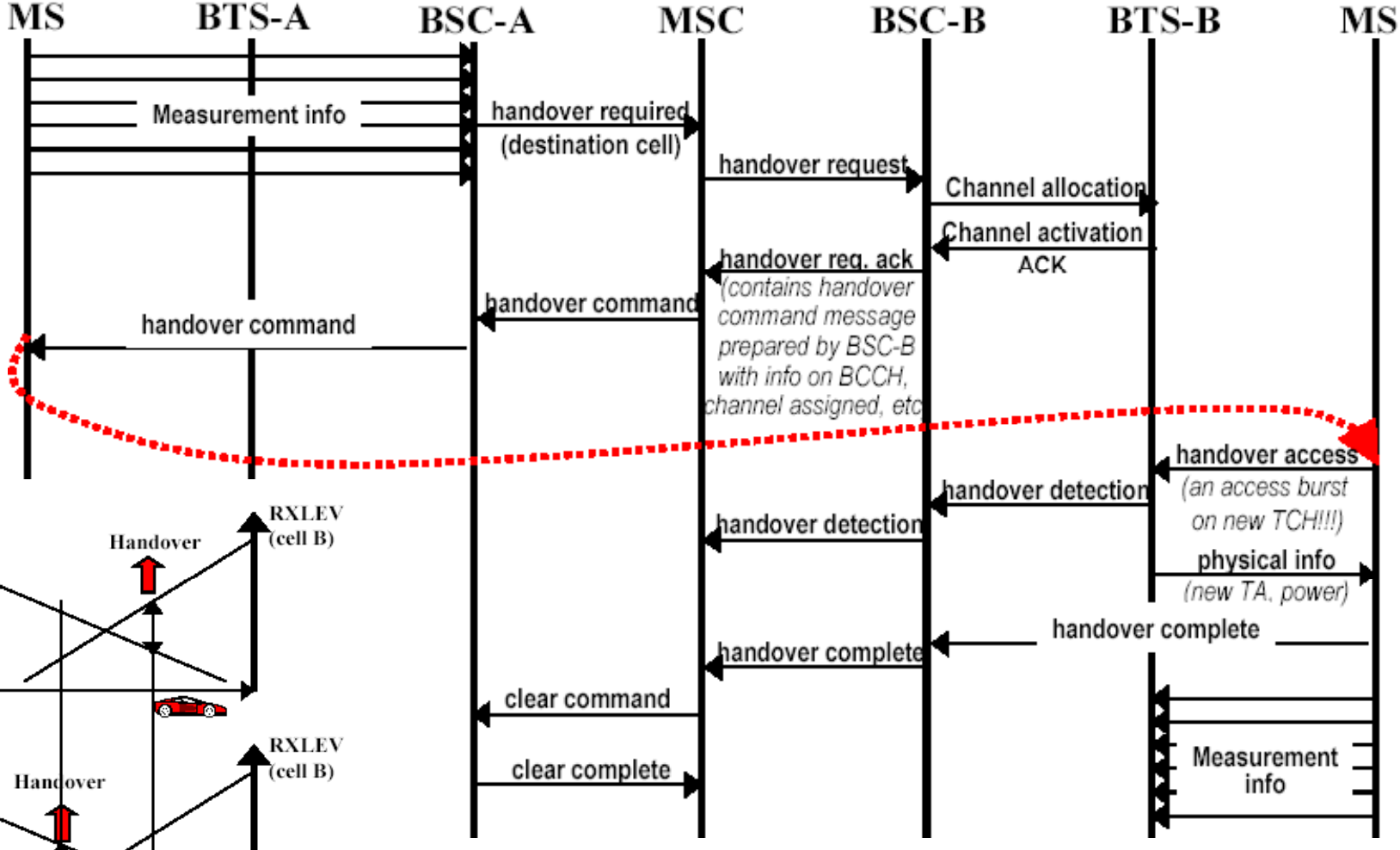
- In tutti i casi di handover si distinguono tre fasi
- Fase 1
  - presentazione della richiesta di un handover
  - tentativo di instaurazione di un nuovo path di trasmissione
- Fase 2
  - indicazione dell'instaurazione di un nuovo path
  - invio del comando di handover alla MS
- Fase 3
  - accesso della MS al nuovo canale
  - attivazione del nuovo path
  - rilascio del vecchio path

Procedura di handover



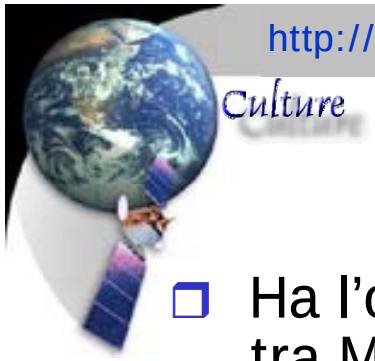
Signaling for intra-MSC handover

(simplified)



Controllo della potenza

- Deve essere inizializzato ogni volta che cambia il canale radio; le caratteristiche sono
  - Si applica indipendentemente ad ogni MS e su uplink e downlink
  - Il vantaggio principale è la riduzione dell'interferenza globale; inoltre si ottiene un risparmio delle batterie
  - E' gestito dal BSC e si basa sulle misure di livello e qualità di BTS (uplink) e MS (downlink)
  - Per l'accesso sul RACH e a seguito dell'assegnazione iniziale si usa il valore di default emesso sul BCCH (ovvero la max potenza della MS, se questa è inferiore); in caso di handover o assegnazione successiva, è il BSC che comunica il nuovo valore iniziale di potenza che MS e BTS devono usare
  - Il campo di variazione della potenza va da 20 a 30 dB
  - Il passo di cambiamento è 2 dB



Controllo dell'anticipo temporale 1/2

- Ha l'obiettivo di eliminare l'effetto dei ritardi di propagazione tra MS e BTS: una MS deve anticipare di TA l'istante di emissione dei burst rispetto all'istante nominale Si inizializza ogni volta che cambia il canale radio
- E' necessario per mantenere elevata efficienza spettrale (piccoli guard times) ed evitare la sovrapposizione di burst in slots contigui
  - Il guard time del burst normale è circa 300 µs
- Si applica quando una MS è nel modo dedicato: il valore di TA che la MS deve usare è controllato dalla BTS, che lo aggiorna tramite il SACCH ogni 480 ms
- Il limite massimo sul valore di TA a sua volta implica un limite sulla massima distanza tra MS e BTS (raggio della cella); con i valori dati, il limite è 35 km

Controllo dell'anticipo temporale 2/2

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:

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

Gestione delle Comunicazioni

- La gestione delle comunicazioni consiste nelle procedure di controllo delle chiamate
- Procedura di instaurazione delle chiamate
- Procedura di abbattimento delle chiamate
- Gestione dei servizi supplementari
- Gestione del servizio “Short Messages”

Gestione delle Comunicazioni

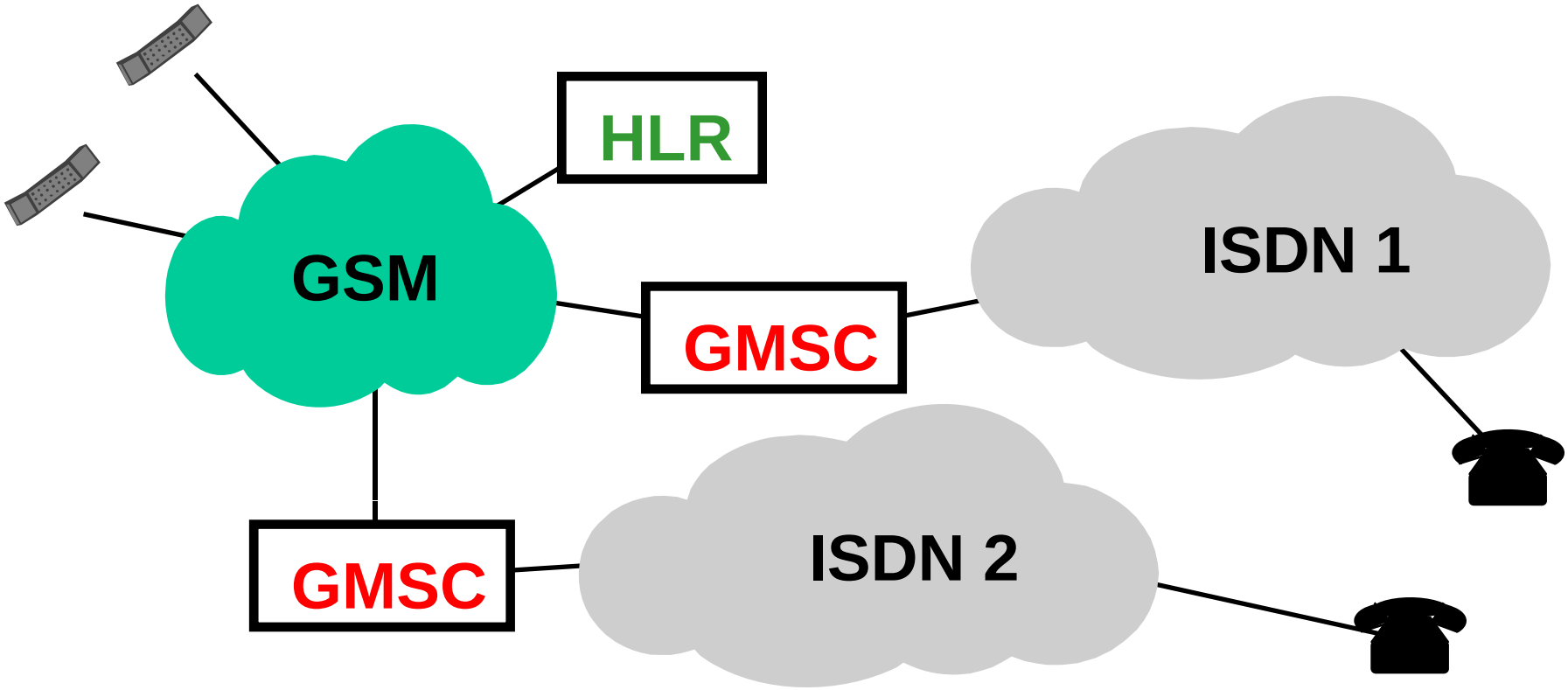
- La rete GSM può essere considerata come una rete di accesso alla rete terrestre (PSTN, ISDN)
- Le procedure di segnalazione sono un estensione di quelle ISDN
- Occorre tener conto degli aspetti legati alla gestione della mobilità del terminale
- Dal punto di vista della gestione delle chiamate il collegamento tra Mobile Station (MS) e Mobile Switching Centre (MSC) è considerato fisso

Tipologie di chiamate

- La chiamata GSM coinvolge due “Parties”
- Calling Party: corrisponde all’utente chiamante
- Called Party: corrisponde all’utente chiamato
  - se è attivo il servizio “Call Forwarding” la Called Party può cambiare nel corso della chiamata
- Mobile Originating Call (MOC): è una chiamata originata da un utente GSM
- Mobile Terminating Call (MTC): è una chiamata diretta ad un utente GSM

Scenario di rete

GMSC: Gateway Mobile Switching Centre, è l'MSC che esegue le funzioni di gateway con la/le reti terrestri



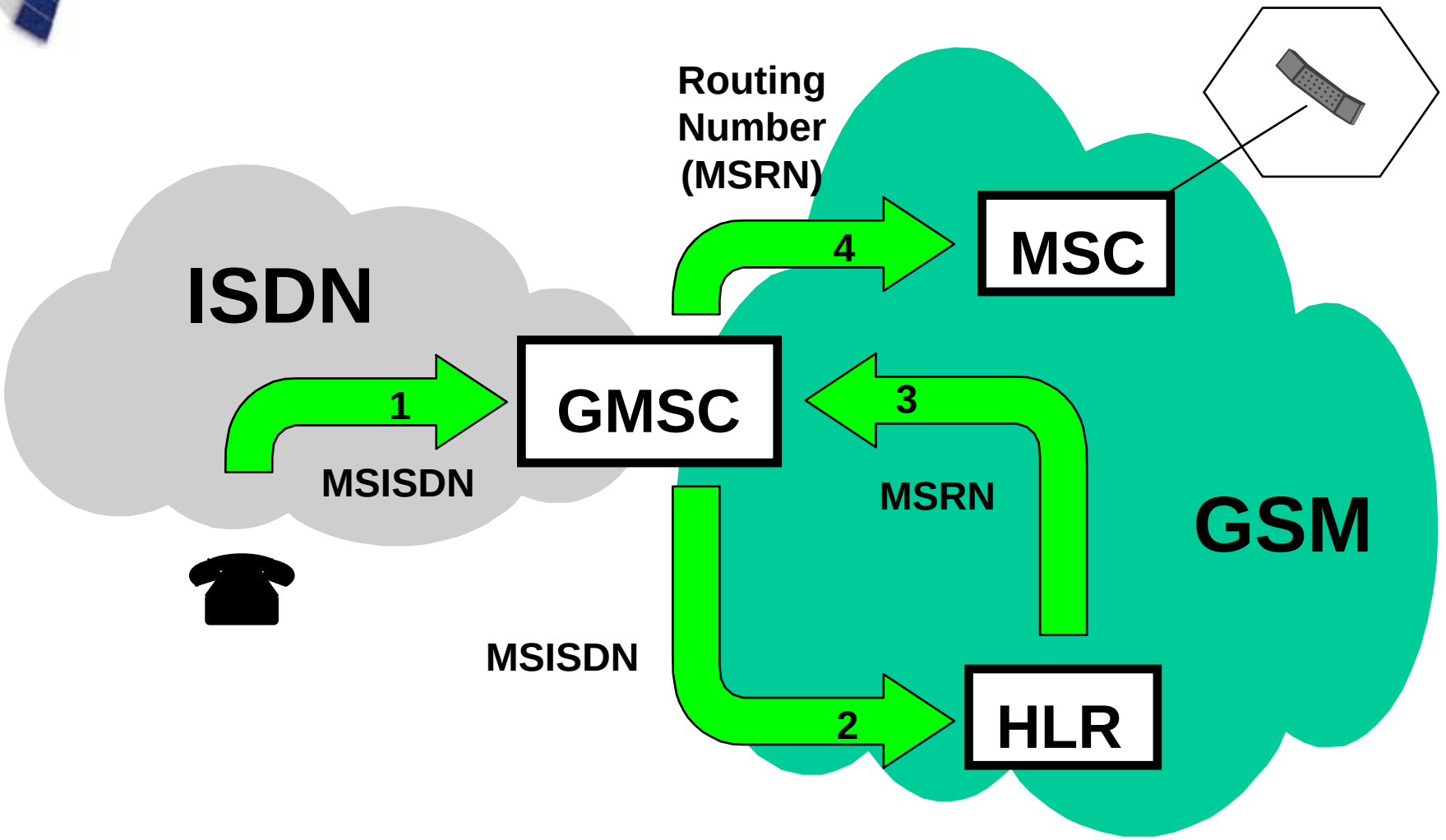
Instradamento di una MTC

- L'instradamento di una chiamata diretta ad un utente mobile si basa sul numero MSISDN (Mobile Station ISDN Number)
- La posizione fisica del terminale è contenuta nell'HLR
- L'HLR restituice al GMSC l'informazione di instradamento che identifica l'MSC di destinazione
- MSRN : Mobile Station Roaming Number

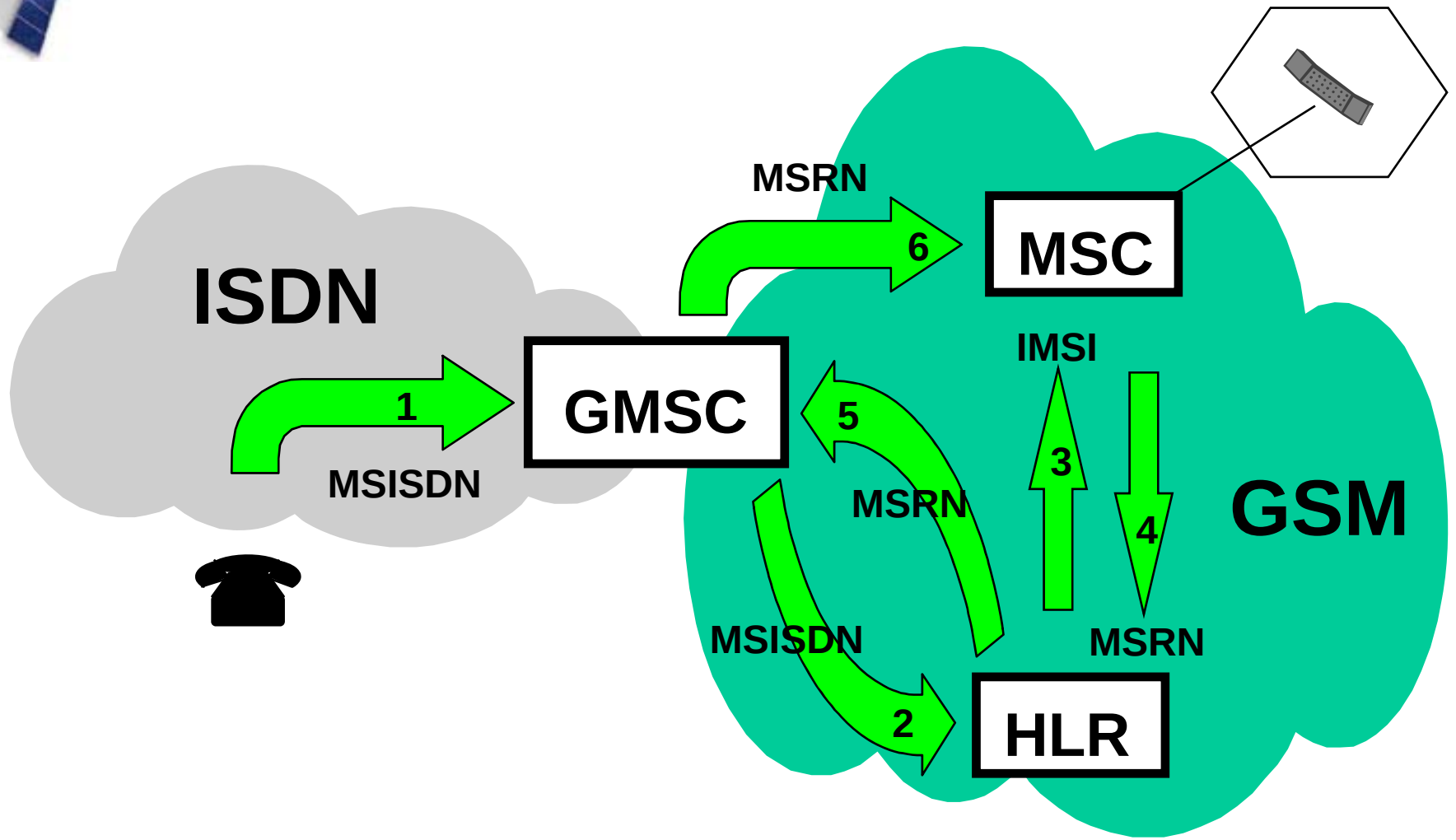
Instradamento di una MTC

- Il primo tratto di instradamento si effettua in base al destination code che individua il GMSC di accesso alla rete GSM di destinazione
- Il GSMC interroga l'HLR inviando il subscriber number
- L'HLR contiene le informazioni relative all'area in cui si trova l'utente chiamato Mobile Station Roming Number (MSRN)
- L'instradamento finale avviene mediante il MSRN

Instradamento di una MTC Soluzione diretta



Instradamento di una MTC soluzione indiretta



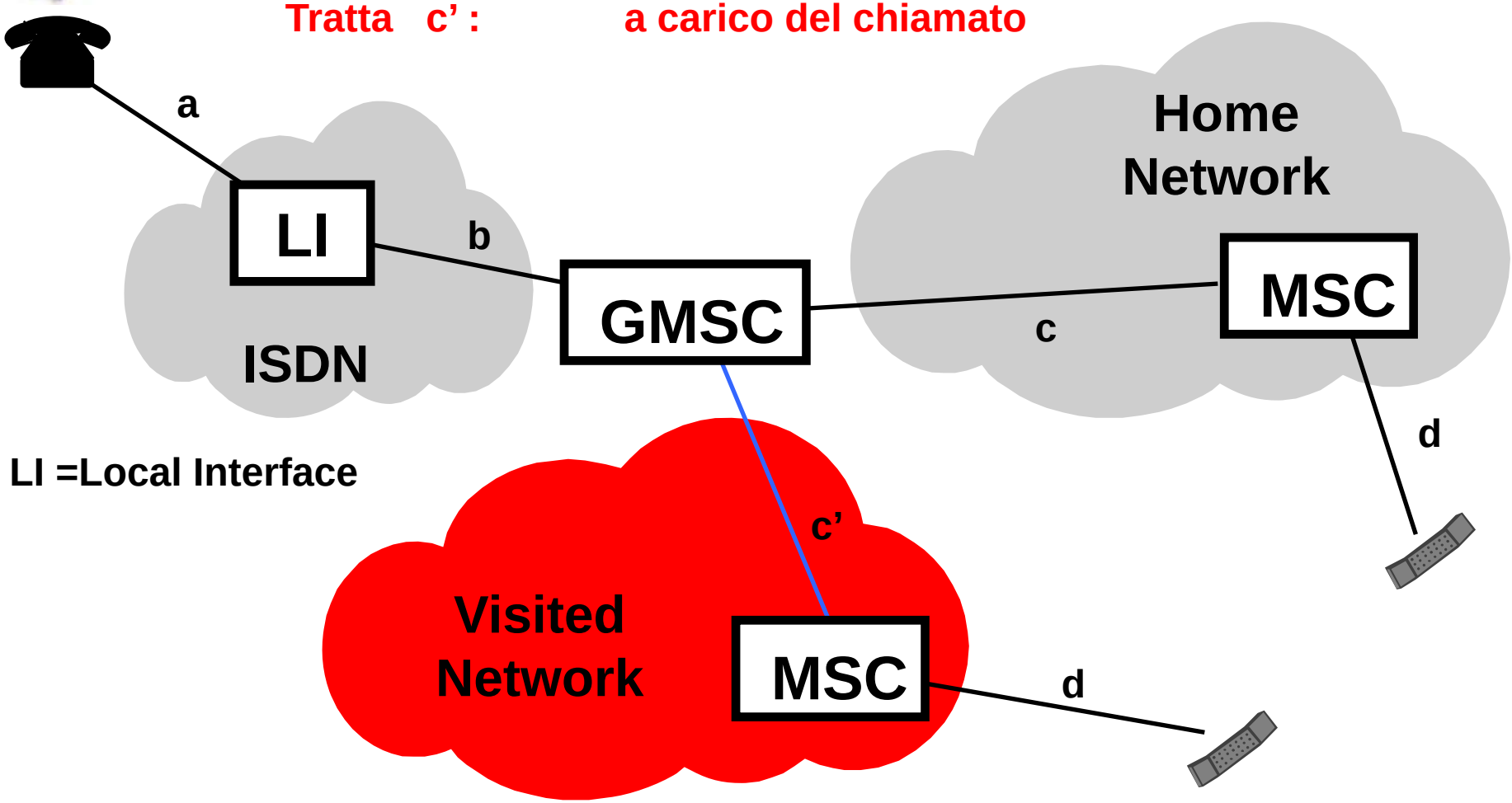
Principi di tariffazione

- *Ipotesi*:
- La posizione dell'utente chiamato non è nota al chiamante
- L'utente chiamato ha diritto alla riservatezza sulla sua posizione attuale
- *Soluzione*:
- La tariffazione è basata sul principio della suddivisione

Principi di tariffazione

Tratte a, b, c, d : a carico del chiamante

Tratta c' : a carico del chiamato



Principi di tariffazione

- La tariffazione è sempre gestita dal GMSC
- La tariffazione della chiamata dipende dalla posizione del GSMC
- L'instradamento non è sempre ottimale
- Le modalità di tariffazione e di instradamento sono state scelte per la loro semplicità