Sommario

1) Richiami sulle reti wireless
2) Principi generali delle reti cellulari
3) Il Sistema GSM
    a) Architettura
    b) Procedure

Richiami sulle reti wireless

Reti wireless

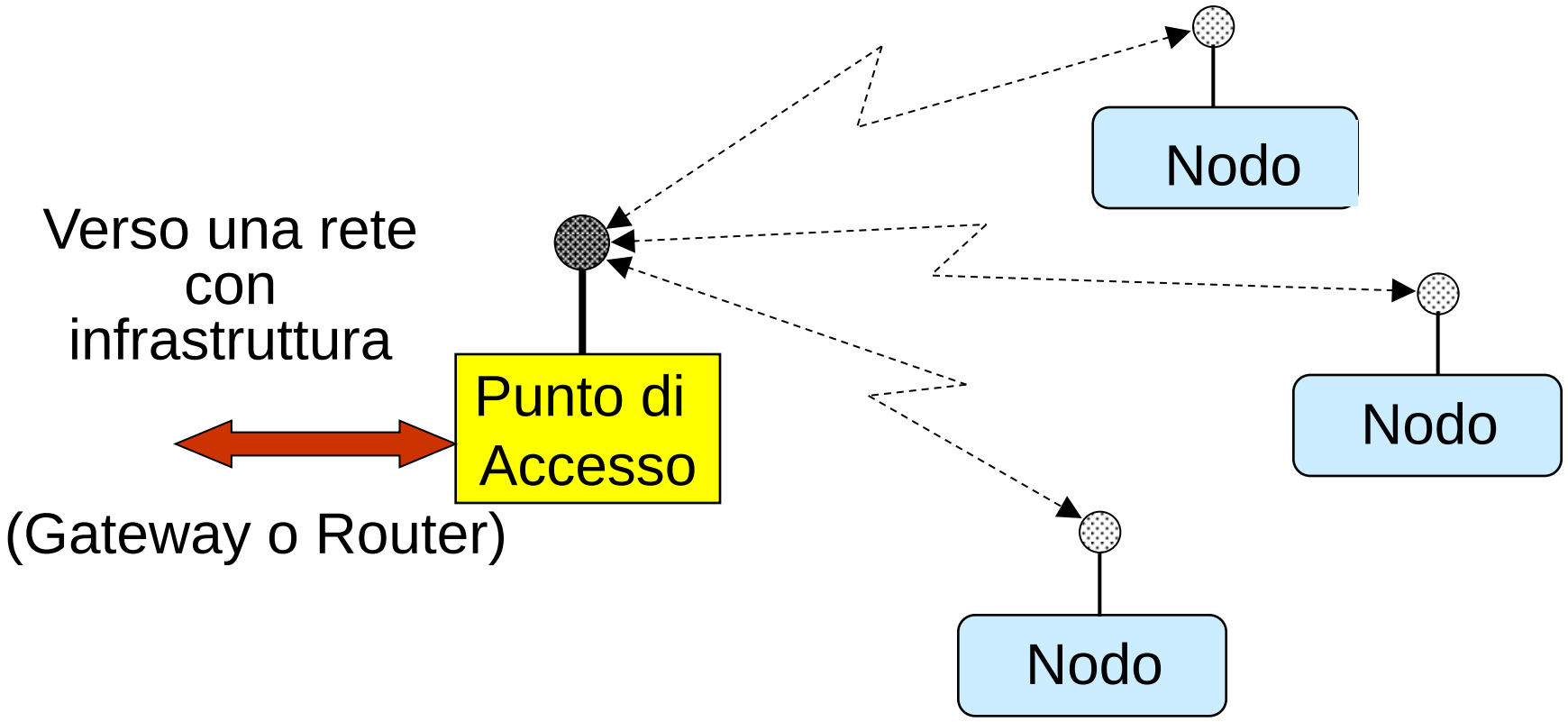
- In una rete wireless i nodi comunicano tramite un canale “senza filo” (es. canale radio, a infrarossi, ecc.)
- Caratteristiche principali
  - Mobilità dei nodi di comunicazione
  - Nodi di comunicazione con limitate risorse energetiche
  - Errori correlati e Bit Error Rate (BER) molto maggiore rispetto alla trasmissione via cavo
  - Natura broadcast del mezzo radio

Reti wireless: architettura

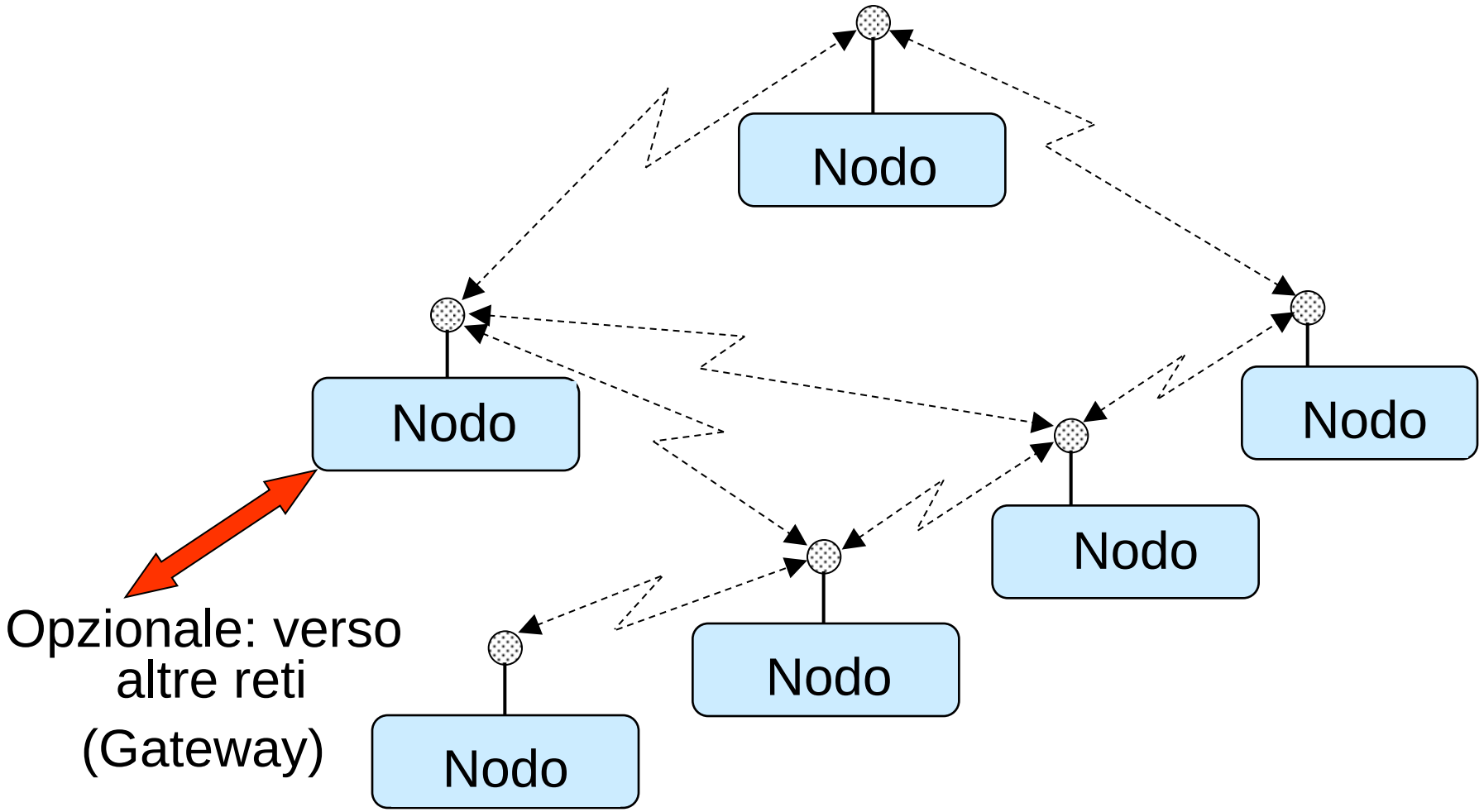
- **Con infrastruttura fissa**: tutti i nodi **comunicano direttamente con punti di accesso alla rete fissa**. Es. reti cellulari e alcune reti locali

- **Senza infrastruttura fissa (reti ad hoc):** i nodi possono **comunicare direttamente tra loro** (e.g., alcune reti locali, reti radio a corto raggio, reti di sensori)

Reti wireless con punto di accesso fisso



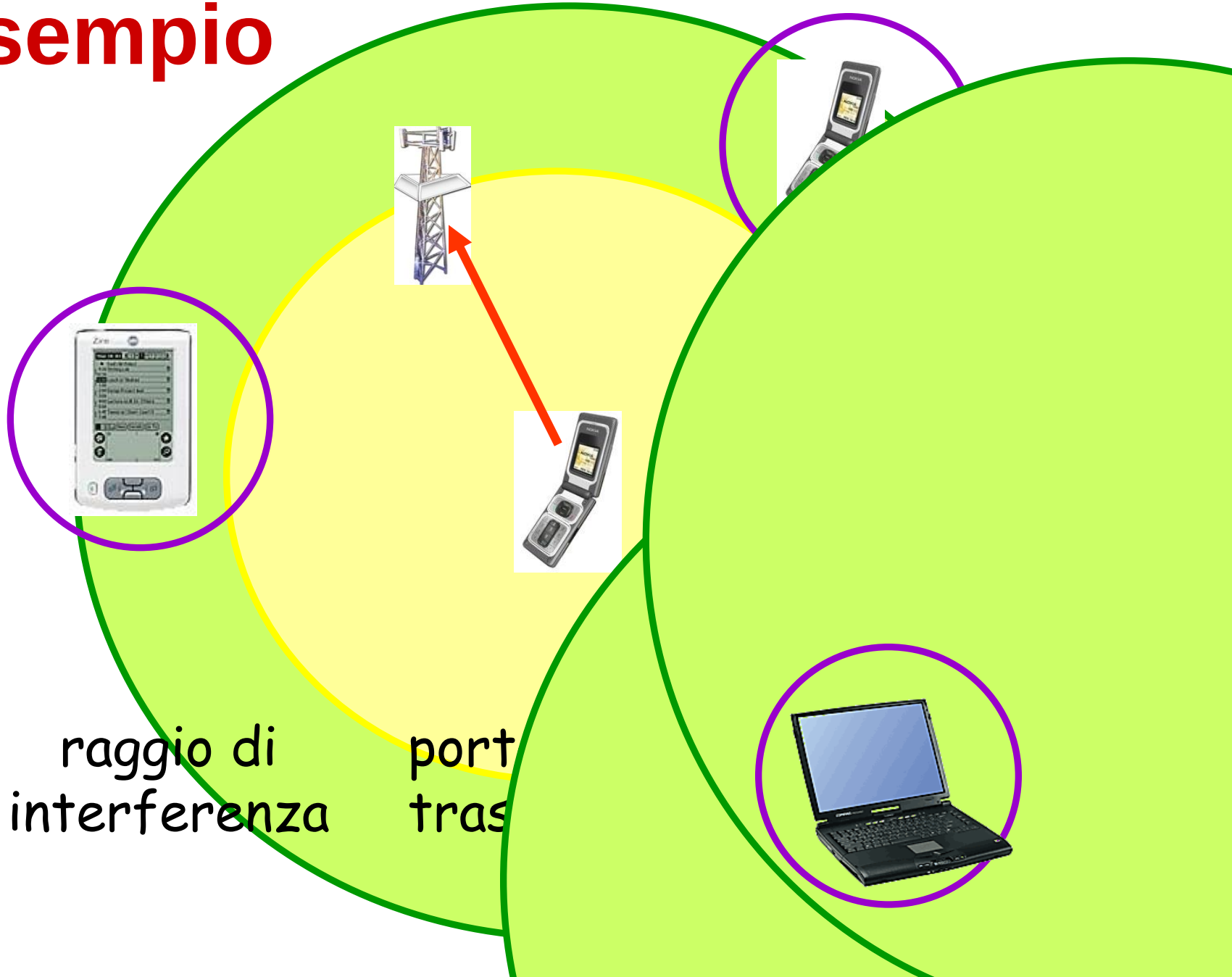
Rete ad hoc


Nodo
Nodo
Nodo
Nodo
Nodo
Nodo
Opzionale: verso altre reti
(Gateway)

Portata trasmissiva / interferenza

- Portata trasmissiva ("*transmission range*") di un nodo wireless: max distanza a cui si riceve correttamente l'informazione trasmessa
  - L'informazione è ricevuta correttamente se il segnale è sufficientemente più forte del rumore+interferenza
  - Portata trasmissiva dipende dal livello di potenza trasmessa, dal tipo di antenna, dalle condizioni di propagazione, dalla codifica di canale e dal bit rate utilizzati
- Raggio di interferenza: massima distanza entro cui l'interferenza causata dal nostro segnale non è considerata trascurabile

Esempio



Collegamento wireless

Le differenze rispetto a un collegamento cablato …

- attenuazione del segnale: le radiazioni elettromagnetiche si attenuano quando attraversano determinati ostacoli; nello spazio libero l'intensità del segnale si attenua al crescere della distanza percorsa (path loss), secondo il quadrato della distanza
- interferenze da parte di altre sorgenti: frequenze wireless standard (es. 2,4 GHz) condivise da altri dispositivi (es. telefonini); anche rumori ambientali (es. motori) causano interferenza
- propagazione su più cammini: una parte delle onde elettromagnetiche si riflette su oggetti e sul terreno, compiendo cammini di diversa distanza tra trasmittente e ricevente

… rendono la comunicazione attraverso un collegamento wireless molto più "complessa"

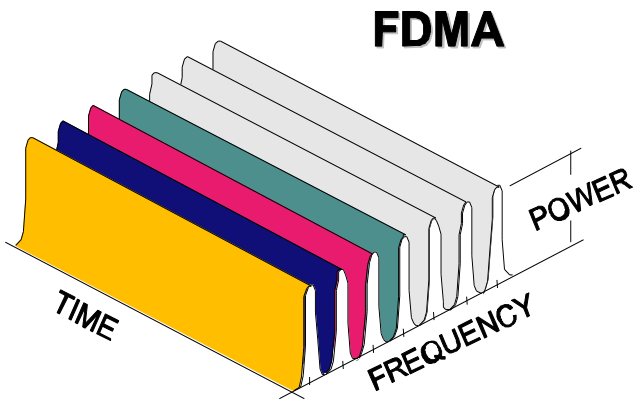
Tecniche di accesso multiplo

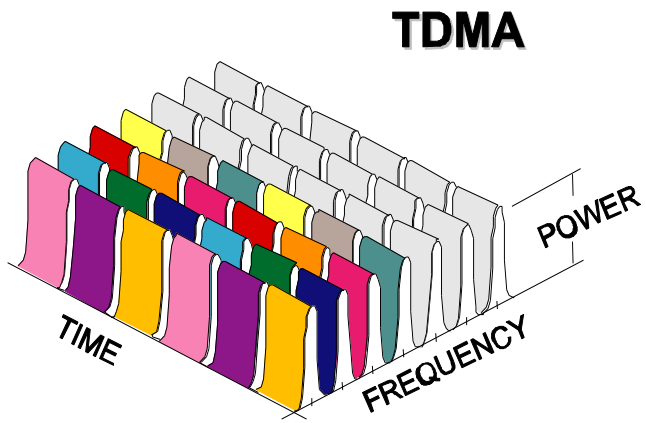
- Accesso multiplo: Il canale wireless è una risorsa condivisa da molti utenti
- Tecniche di accesso multiplo
  - FDMA (Frequency Division Multiple Access)
  - TDMA (Time Division Multiple Access)
  - CDMA (Code Division Multiple Access)
  - SDMA (Space Division Multiple Access)

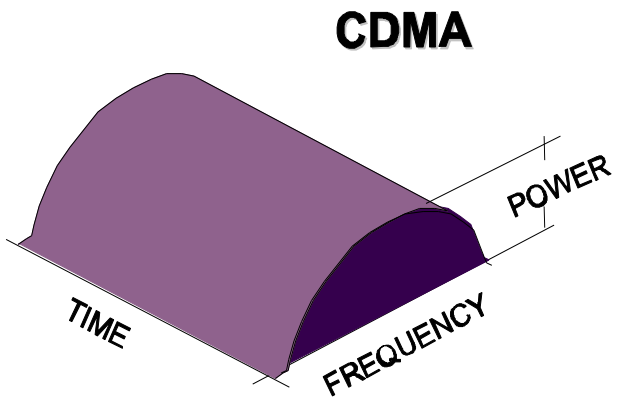
Code Division Multiple Access (CDMA)

- La tecnica di accesso al canale a divisione di codice (CDMA) è basata sullo “spreading” dei segnali
- Lo spreading è ottenuto con particolari codici (Orthogonal Variable Spreading Code - OVSC), che vengono moltiplicati per la sequenza di bit da trasmettere
- Le trasmissioni di utenti diversi usano la stessa banda di frequenza nello stesso tempo, ma si possono distinguere tra loro grazie alla proprietà di ortogonalità dei codici

Accesso Multiplo: sguardo d'insieme







SDMA

- La Space Division Multiple Access (SDMA) è alla base delle reti cellulari
- Grazie alla rapida attenuazione del segnale radio con la distanza è possibile, all'interno della stessa rete,

Usare le stesse frequenze in punti geografici diversi

RETI CELLULARI

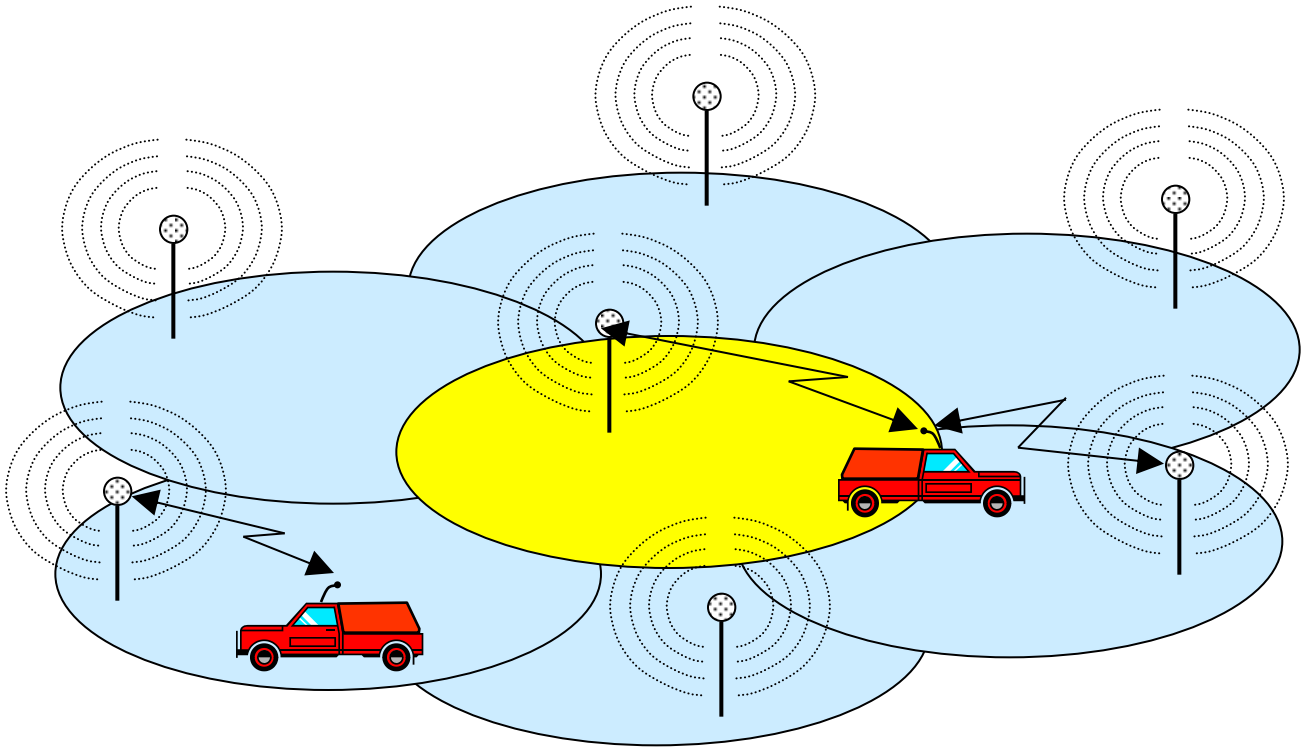
Principi generali

Definizioni

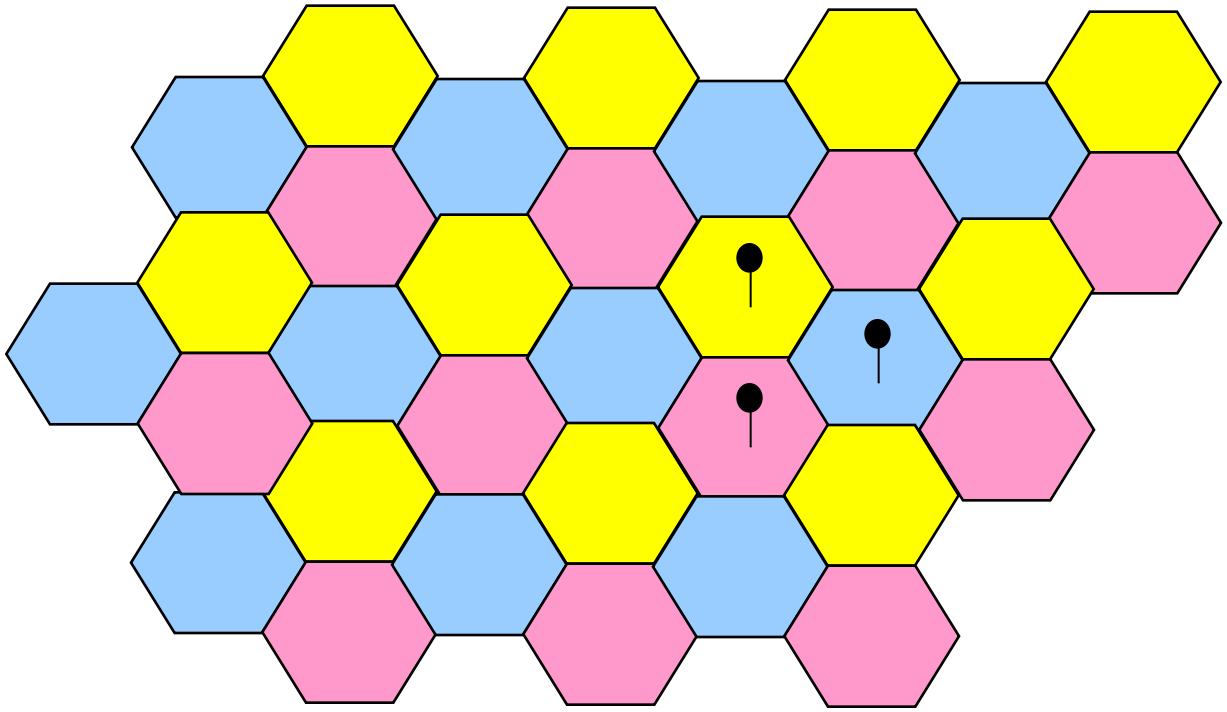
- **Rete cellulare**
  - Rete la cui copertura geografica è ottenuta con una tassellatura di aree adiacenti e/o sovrapposte dette **celle**
  - L'utente (terminale mobile) si può muovere attraverso la rete passando da una cella all'altra senza interrompere la comunicazione (**handover o handoff**)

Rete Cellulare

- La copertura radio del territorio è realizzata con tante celle
- Supporto della mobilità degli utenti

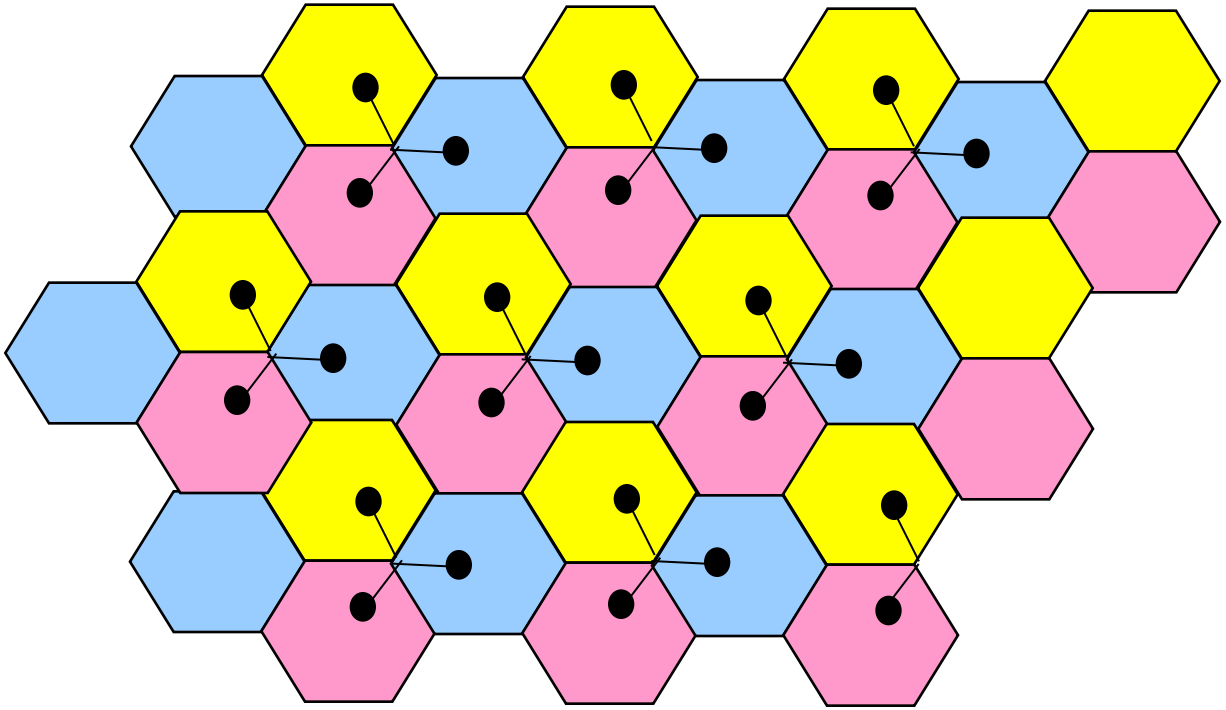


La copertura cellulare teorica



- Stazione base a centro cella con antenna isotropica
- Celle: aree esagonali regolari

La copertura cellulare teorica

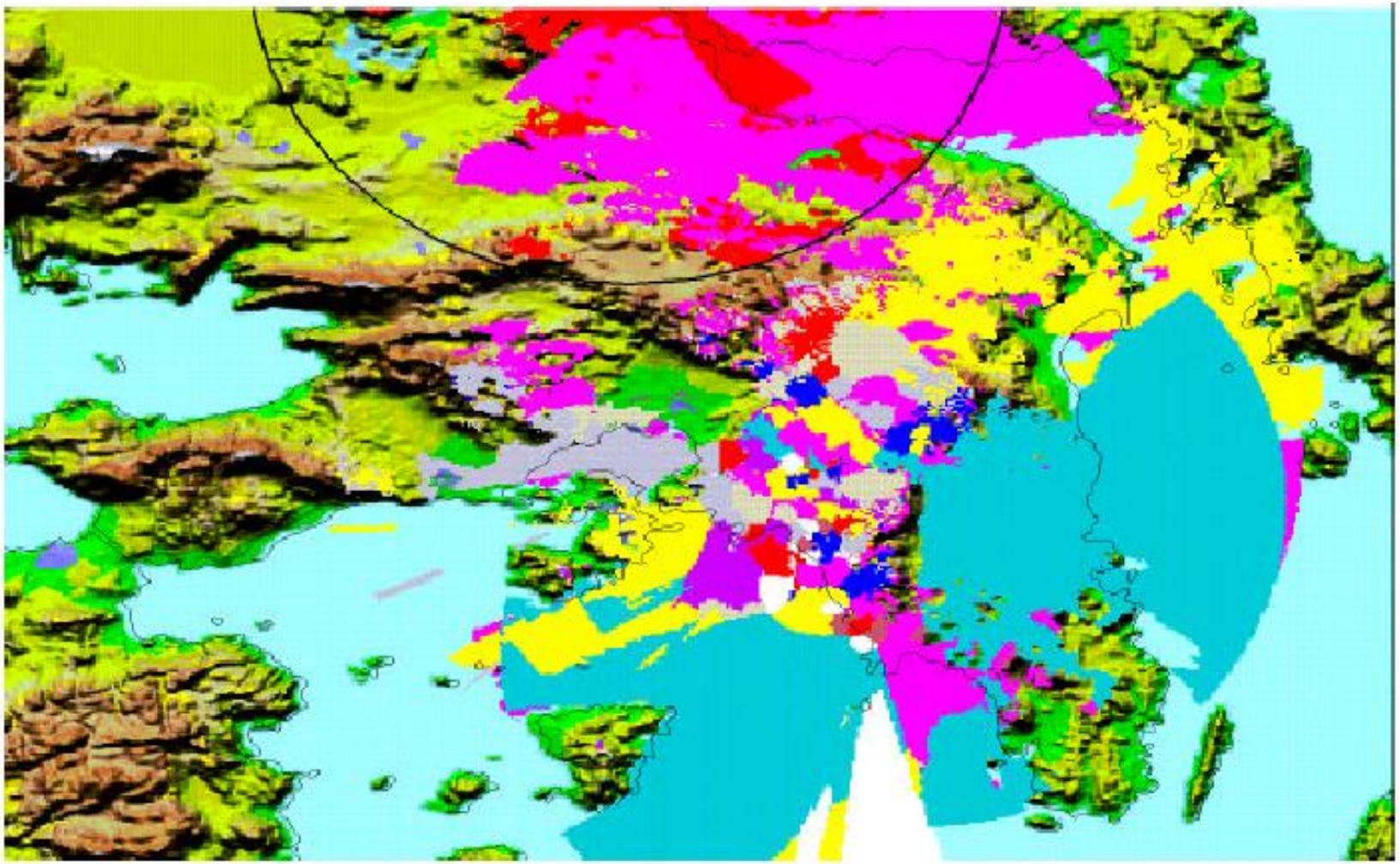


- 3 antenne direzionali a 120° ad un’estremità delle celle
- 3 antenne nello stesso sito

Le celle

- Le celle non sono regolari (esagoni) e delle stesse dimensioni
- Forma e dimensione della cella determinate da
  - Potenza delle antenne
  - Guadagno di antenna
  - Morfologia del territorio (in aree urbane dalla forma degli edifici)
  - Condizioni di propagazione

La copertura cellulare reale



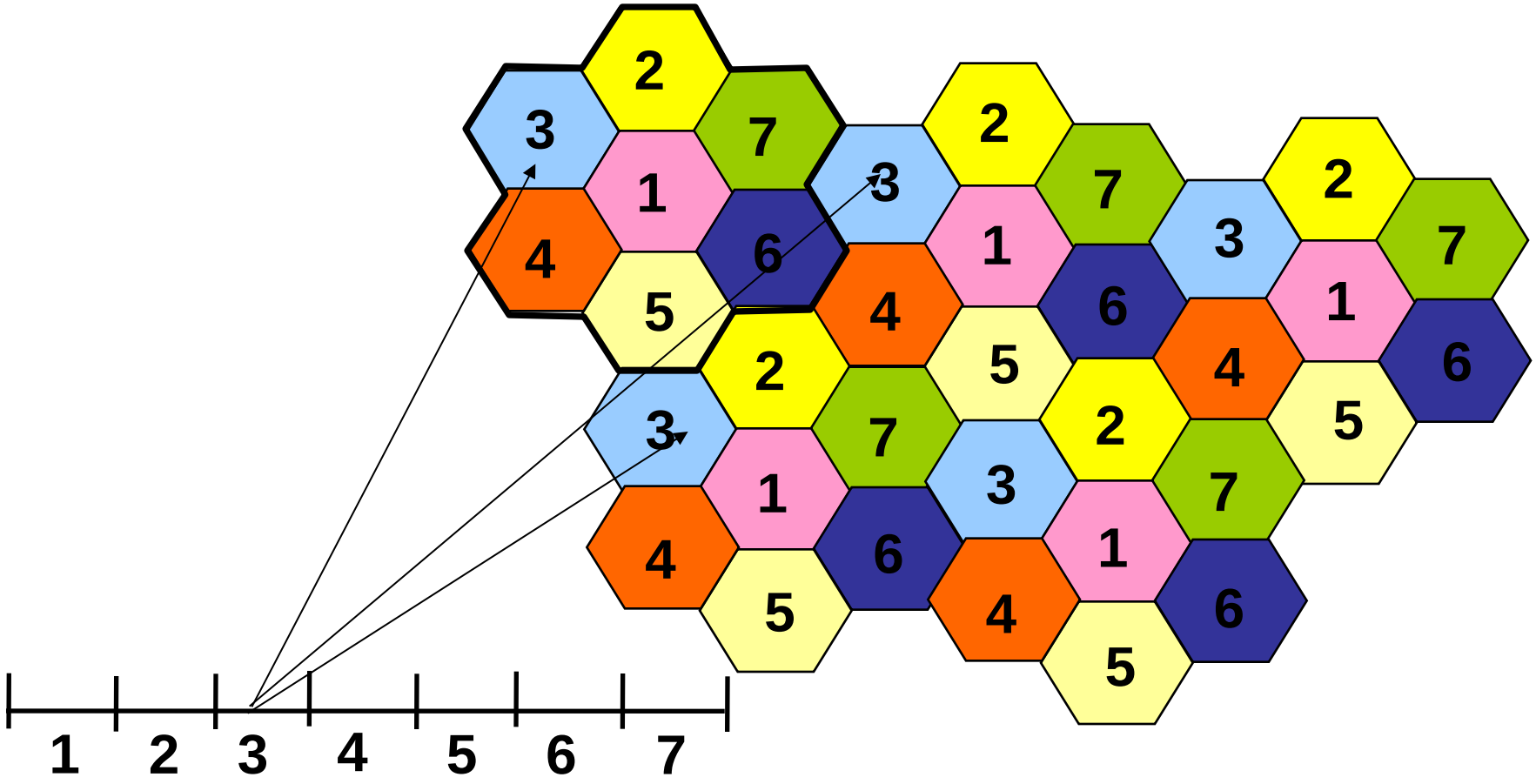
La copertura cellulare reale

- Per una copertura macrocellulare (come quella rappresentata in figura), le caratteristiche del territorio sono normalmente rilevate da satellite:
  - L'estensione delle aree urbane
  - Le porzioni seminative
  - Le aree di bosco fitto o a macchie
  - Le aree rocciose e montane…..

SDMA: riutilizzo delle frequenze

- Con un limitato numero di risorse radio si vogliono conseguire i seguenti obiettivi:
  - Assicurare la copertura del territorio
  - Servire un elevato numero di utenti
- Le frequenze usate in una cella possono essere riusate in un'altra cella, così lontana che il livello di interferenza tra le due celle è al di sotto di una data soglia.

SDMA: riutilizzo delle frequenze



SDMA: riutilizzo delle frequenze

- Si definisce la larghezza di banda B di un canale:

  Es: 200 kHz per GSM

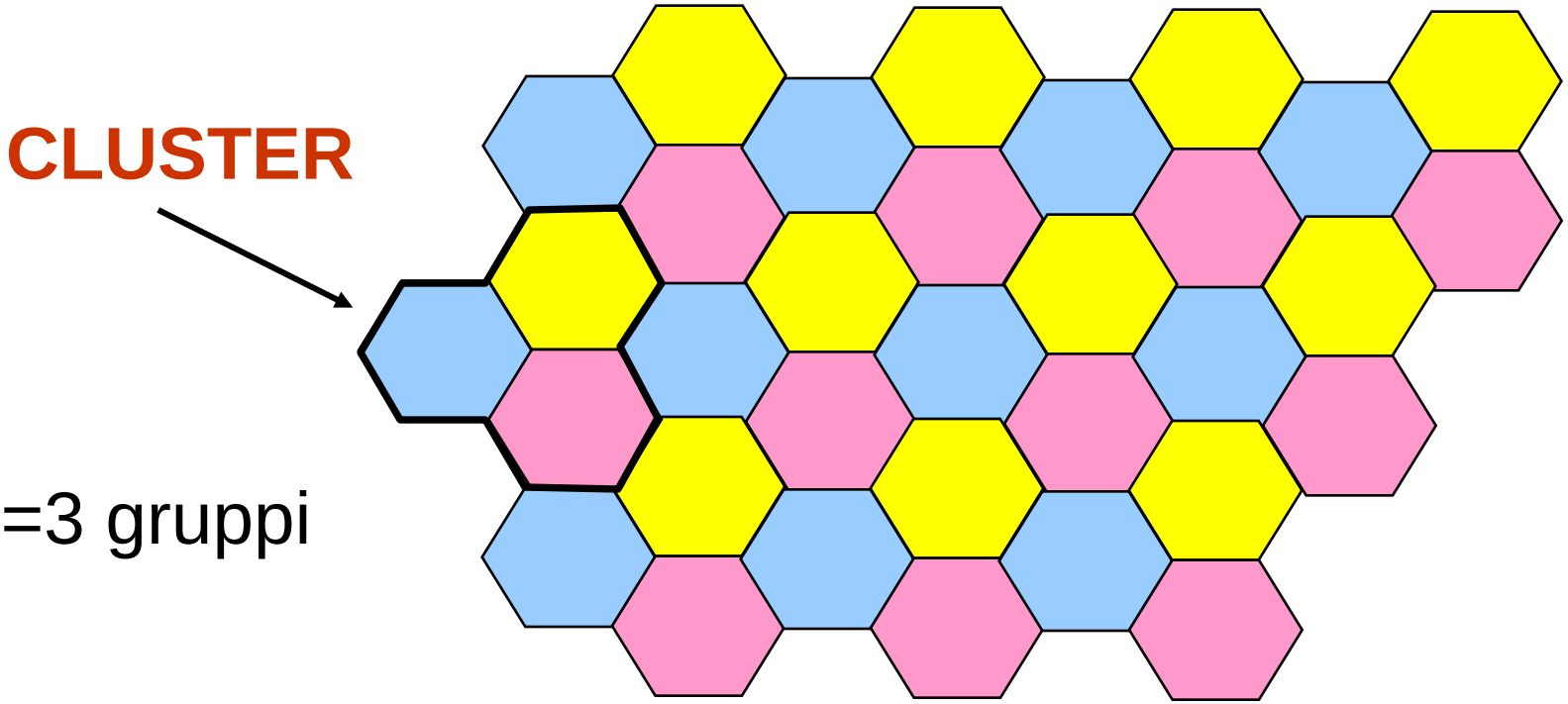
- Dato lo spettro a disposizione, largo S, si hanno a disposizione $N = S/B$ canali

- Ogni canale ha una frequenza centrale detta portante

SDMA: riutilizzo delle frequenze

- Si partizionano gli N canali in G gruppi di $k=N/G$ canali ognuno (k canali / cella)
- Si definisce cluster l'insieme delle G celle adiacenti che usano tutti gli N canali
- Si divide il territorio in cluster di celle
- Fattore di riuso: 1/ G

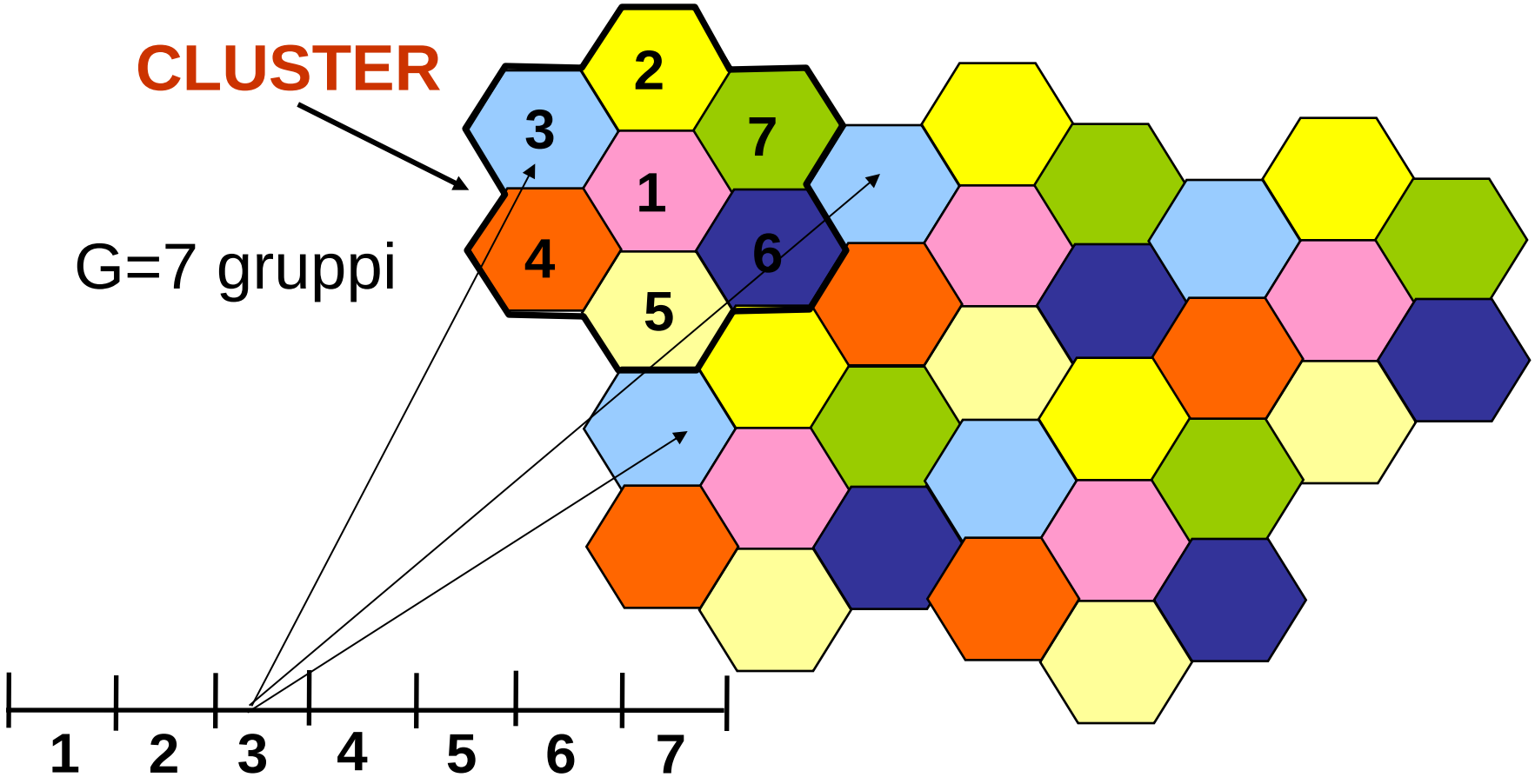
Cluster con 3 celle



G=3 gruppi

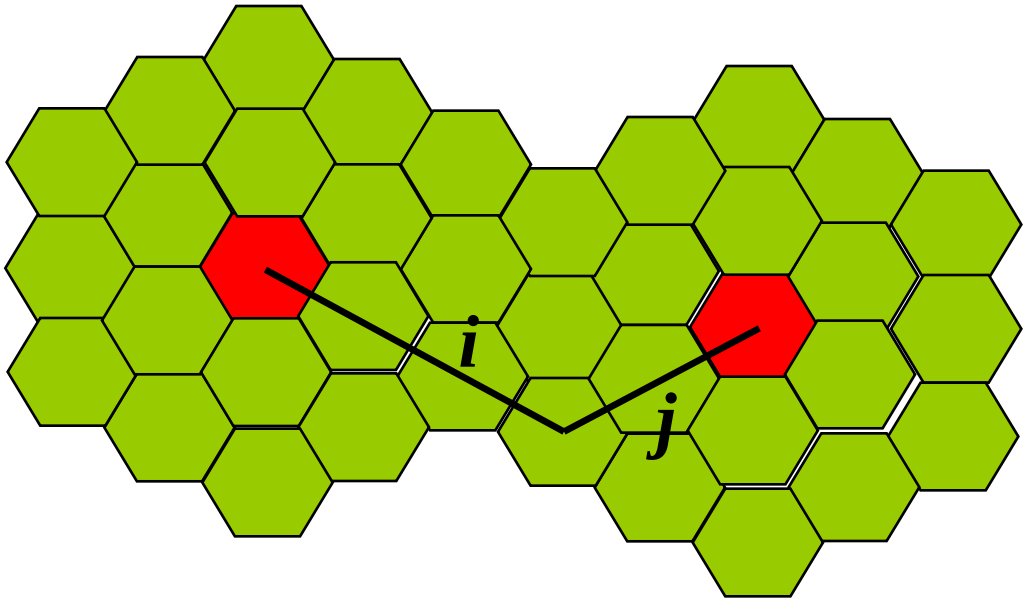
- L’insieme dei canali nel gruppo blu, giallo e rosa sono disgiunti
- Celle dello stesso colore sono dette “co-canale”

Cluster con 7 celle



Dimensione del cluster

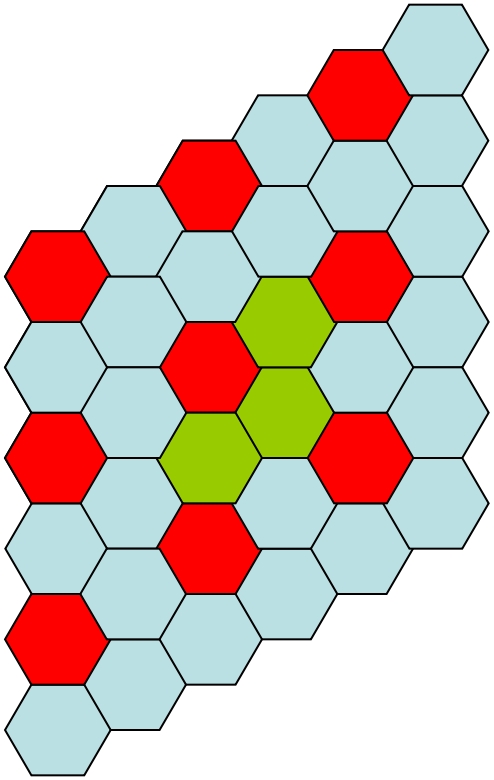
- No. celle/cluster: $G = i^2 + j^2 + ij$



***i* e *j* interi**

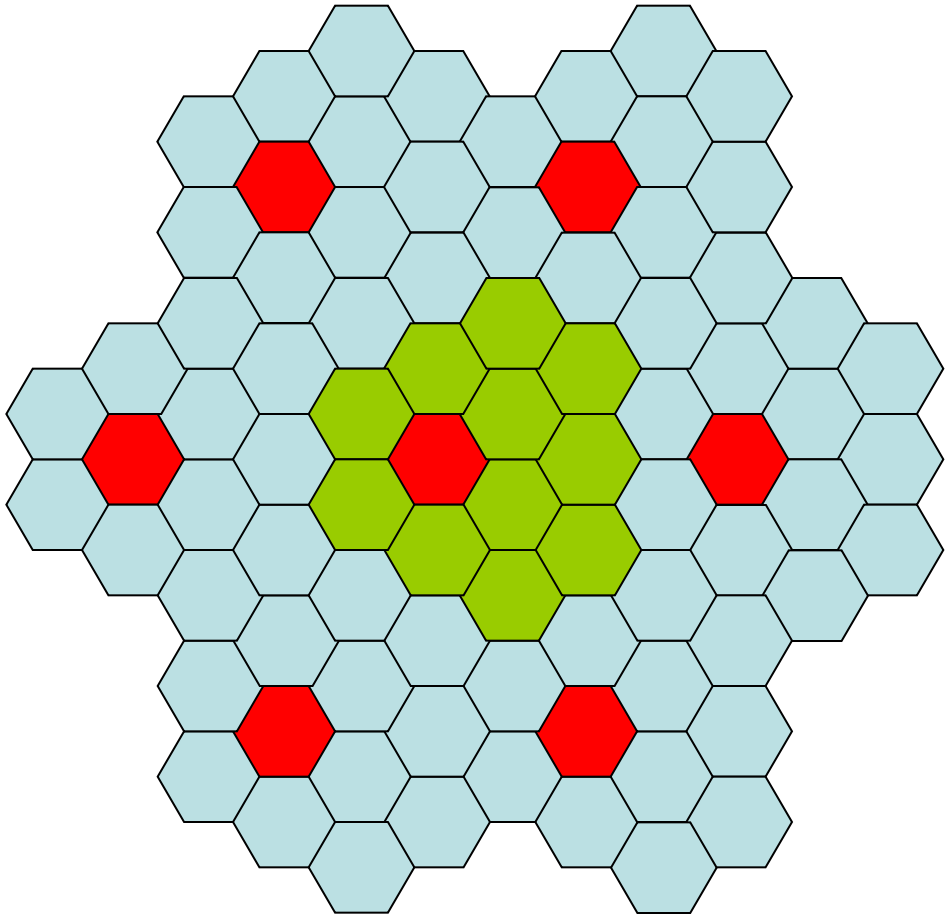
- Possibili valori di G: 1, 3, 4, 7, 9, 12, 13, 16, 19, 21, …

i = 2, j = 0 → G = 4



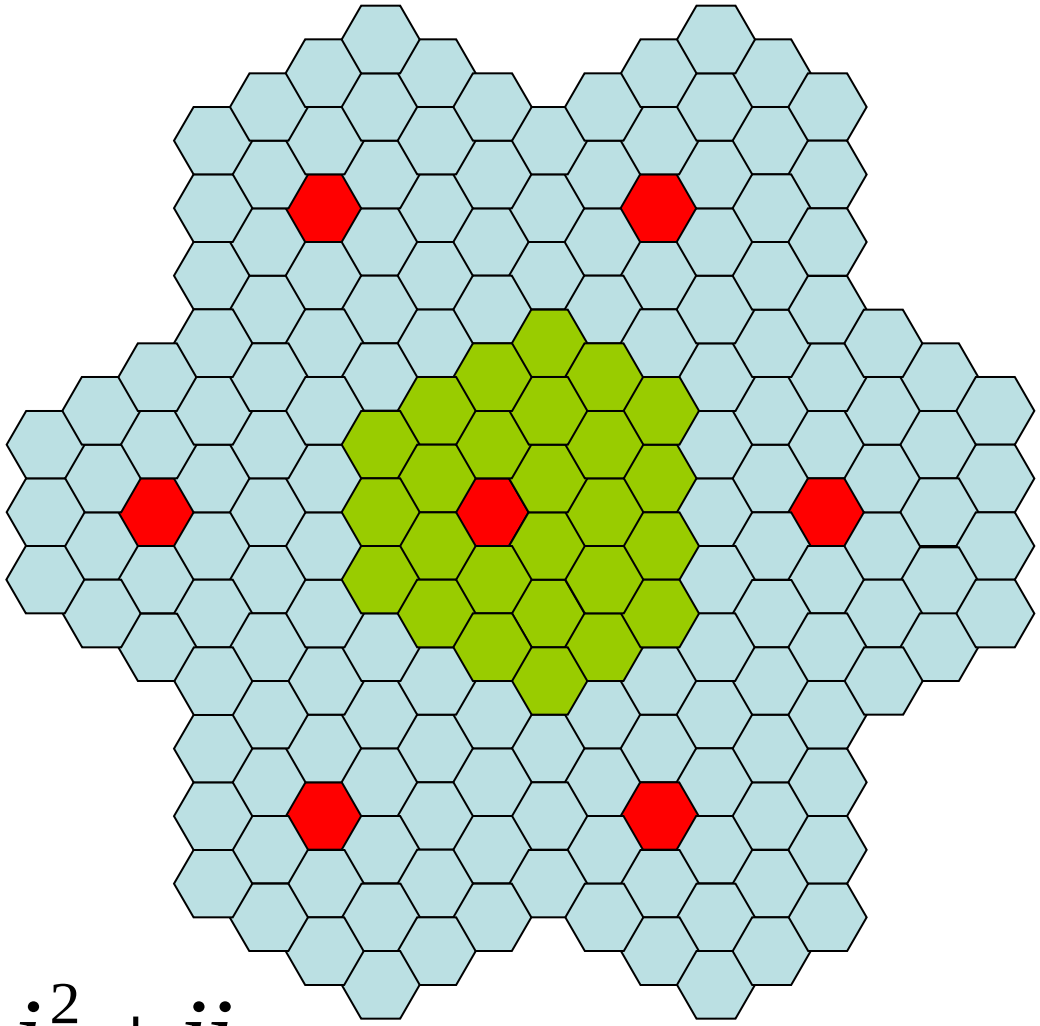
$$G = i^2 + j^2 + ij$$

i = 2, j = 2 → G = 12



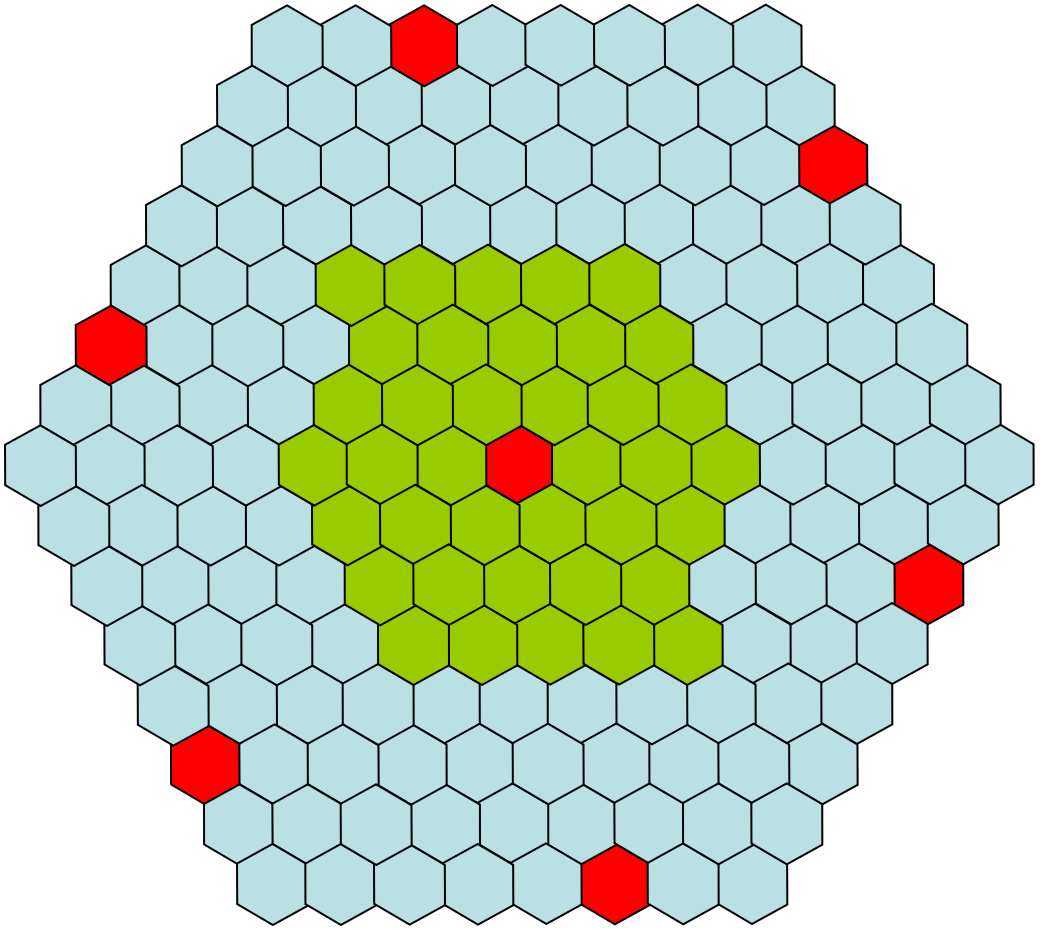
$$G = i^2 + j^2 + ij$$

i = 3, j = 3 → G = 27

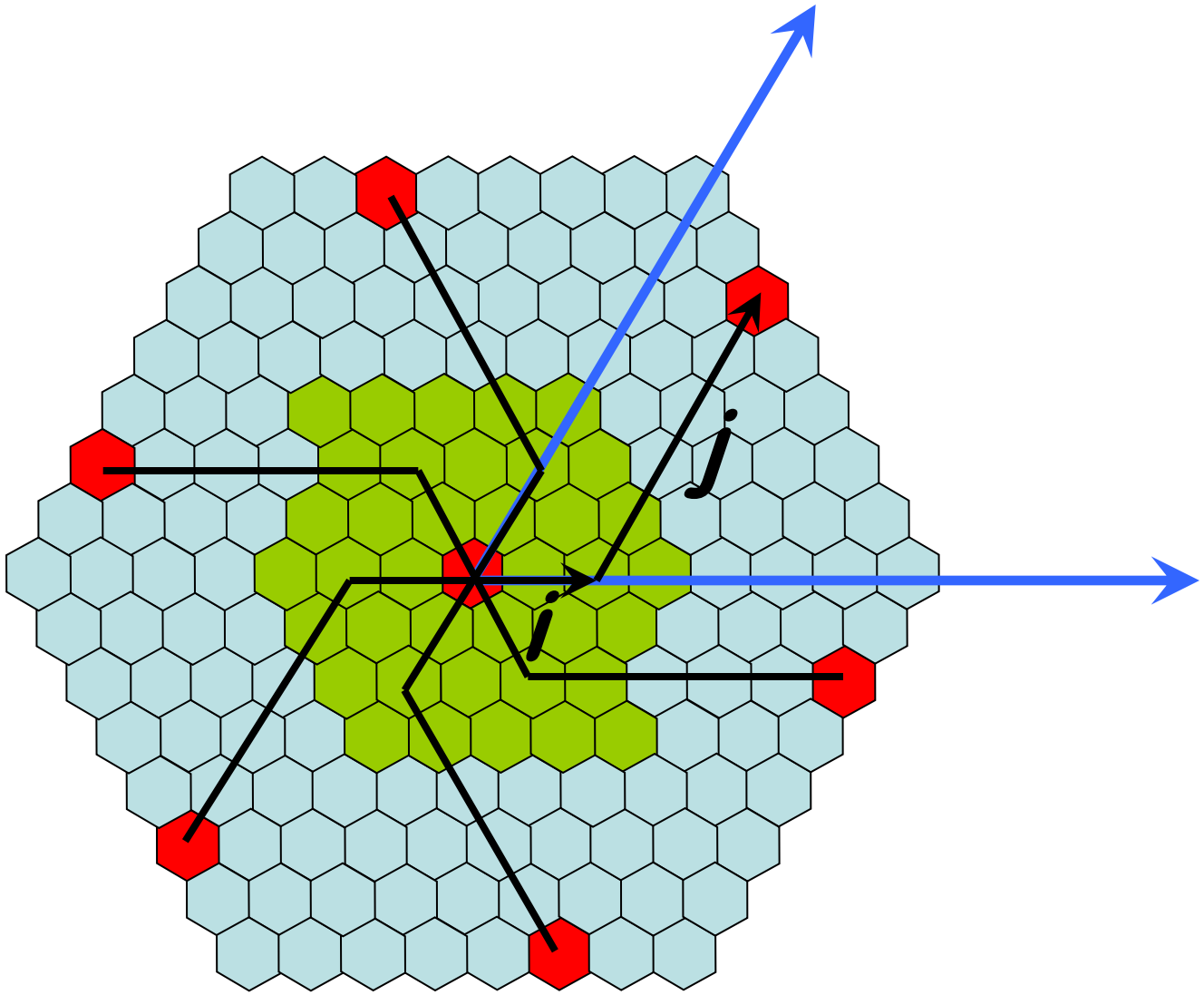


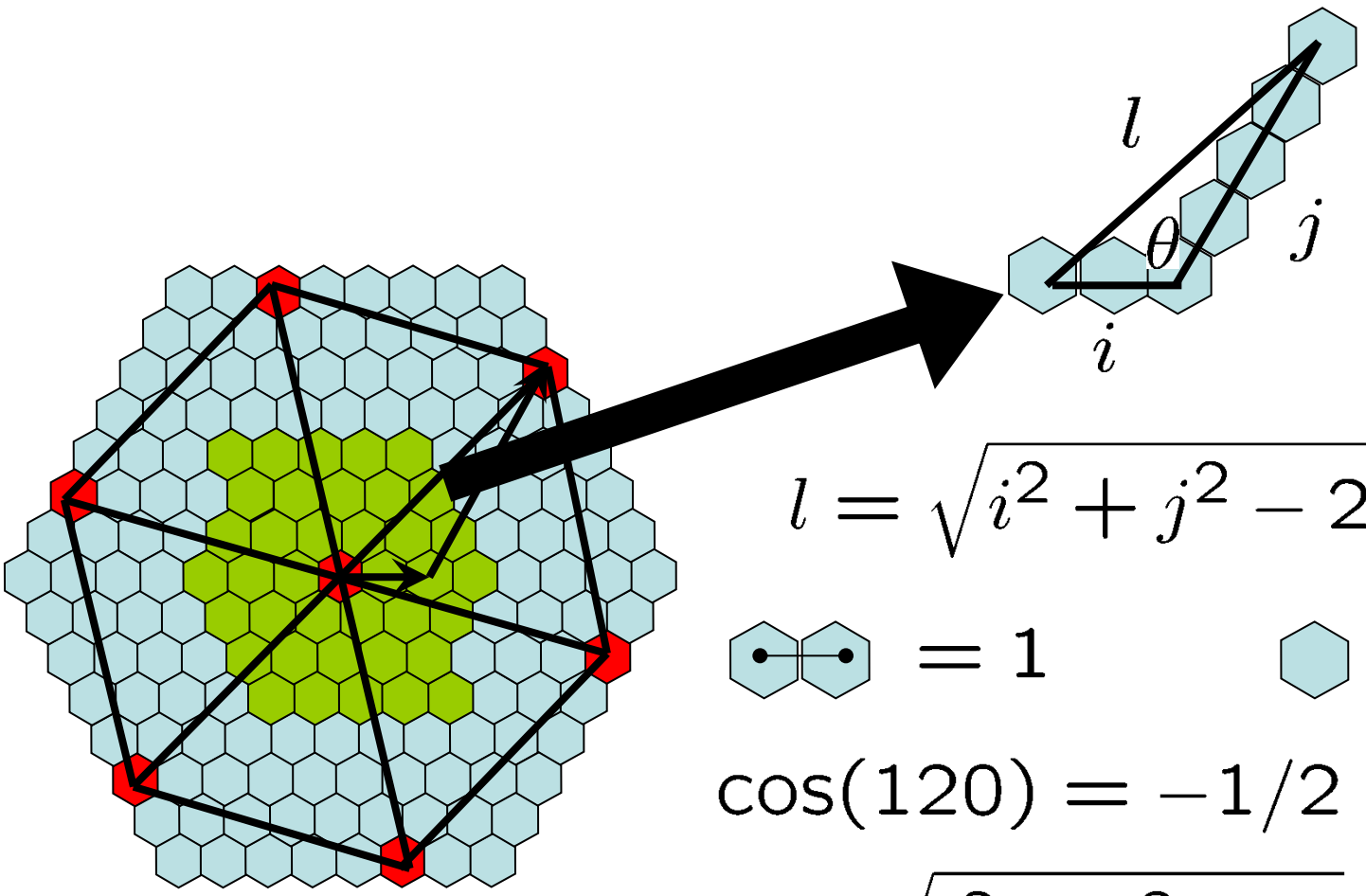
$$G = i^2 + j^2 + ij$$

i = 2, j = 5 → G = 39



$$G = i^2 + j^2 + ij$$


j
i



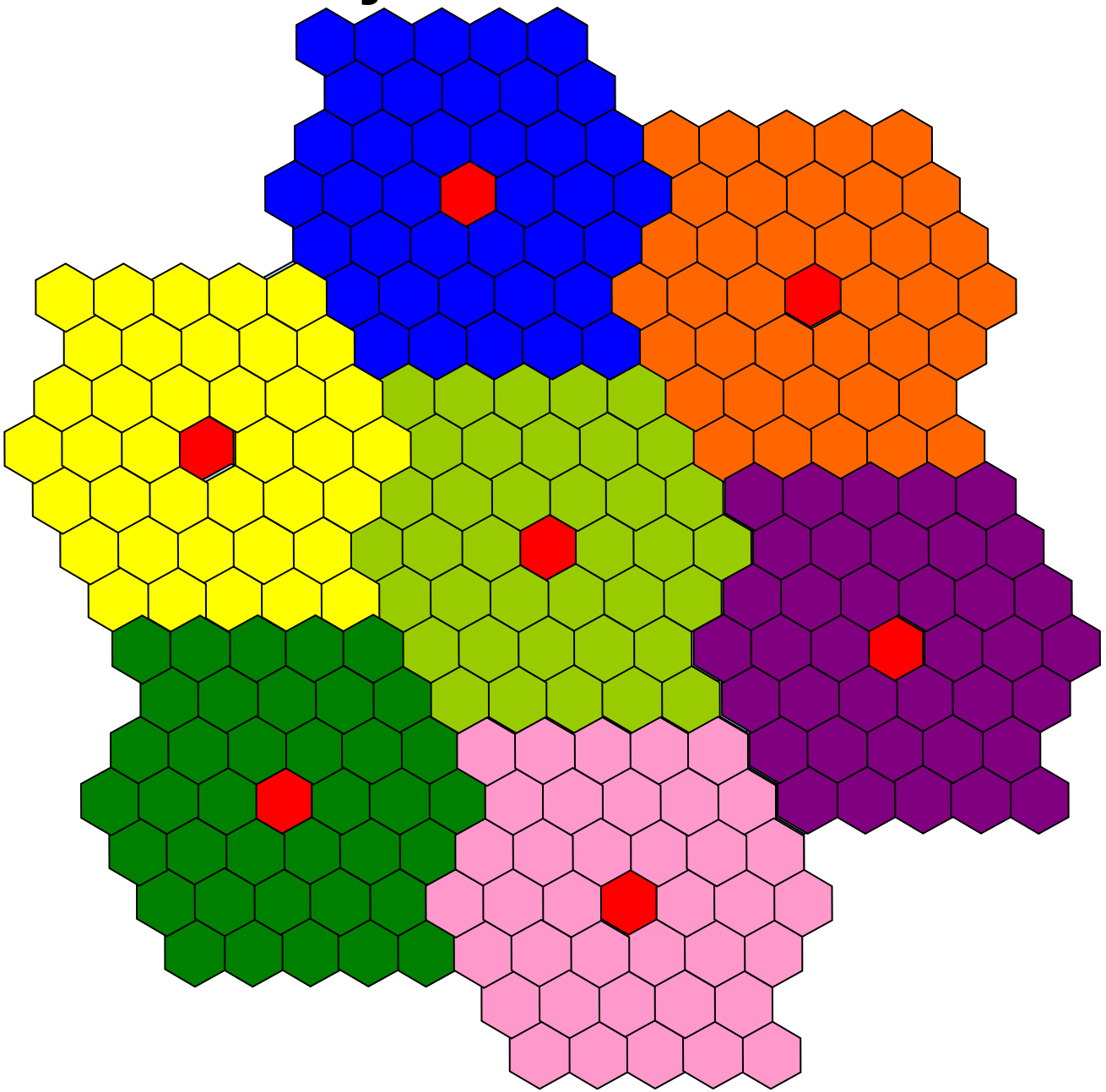
$$l = \sqrt{i^2 + j^2 - 2\cos(\theta)ij}$$

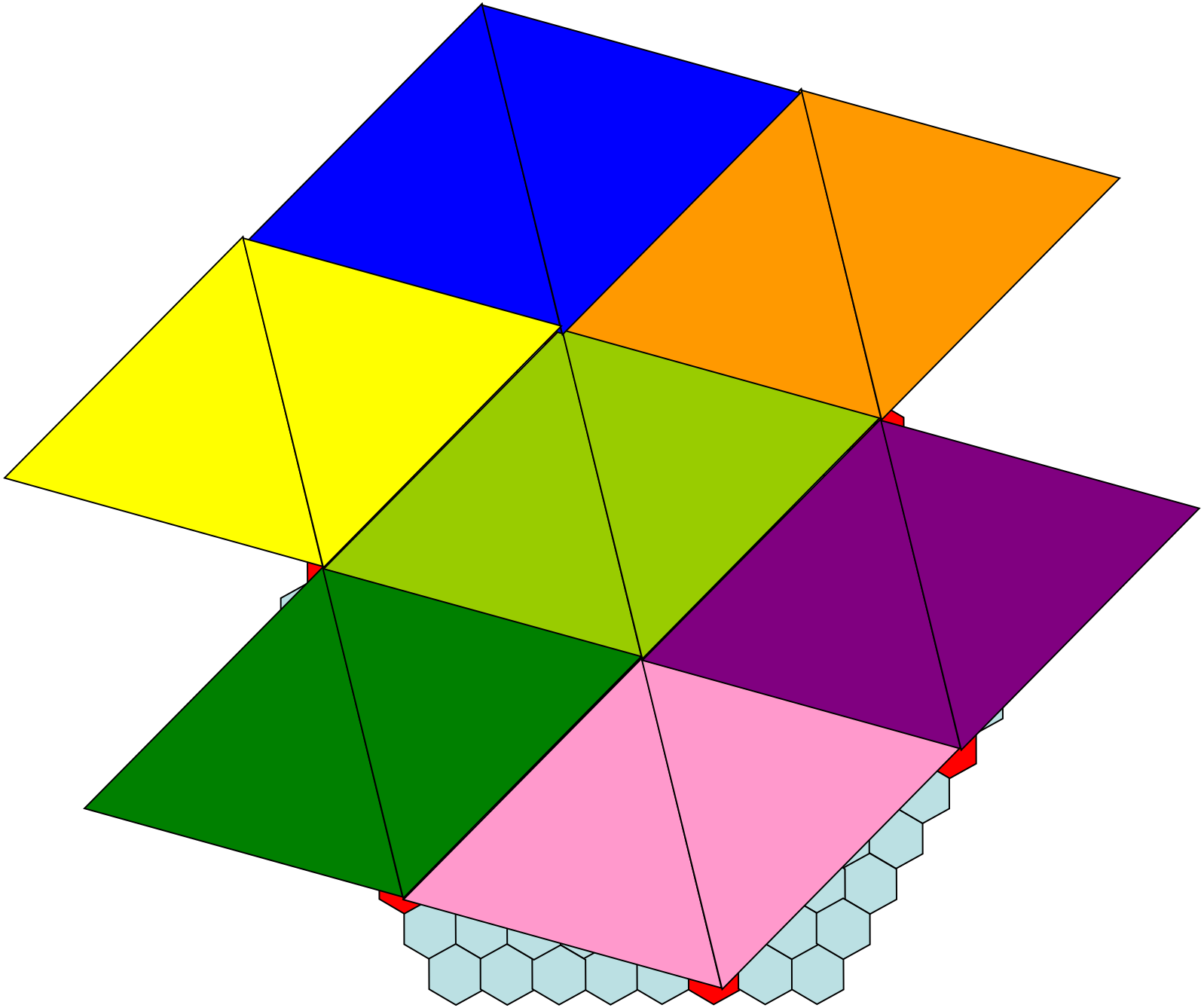
 $= 1$ $= \sqrt{3}/2$

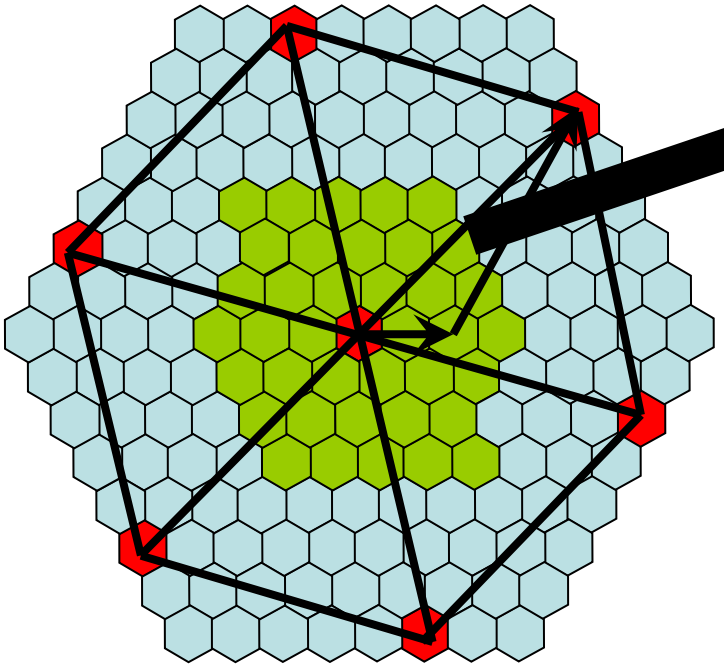
$$\cos(120) = -1/2$$

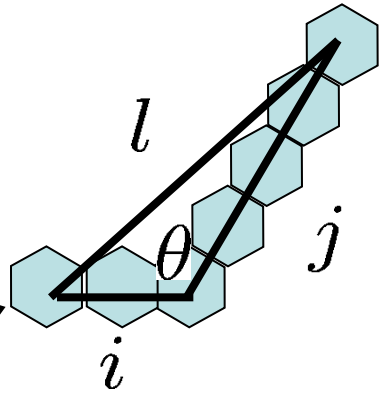
$$l = \sqrt{i^2 + j^2 + ij}$$

i = 2, j = 5 → G = 39

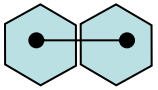






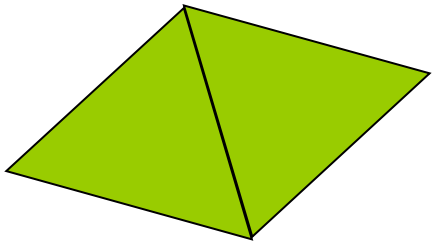


$$l = \sqrt{i^2 + j^2 - 2\cos(\theta)ij}$$

 $= 1$  $= \sqrt{3}/2$

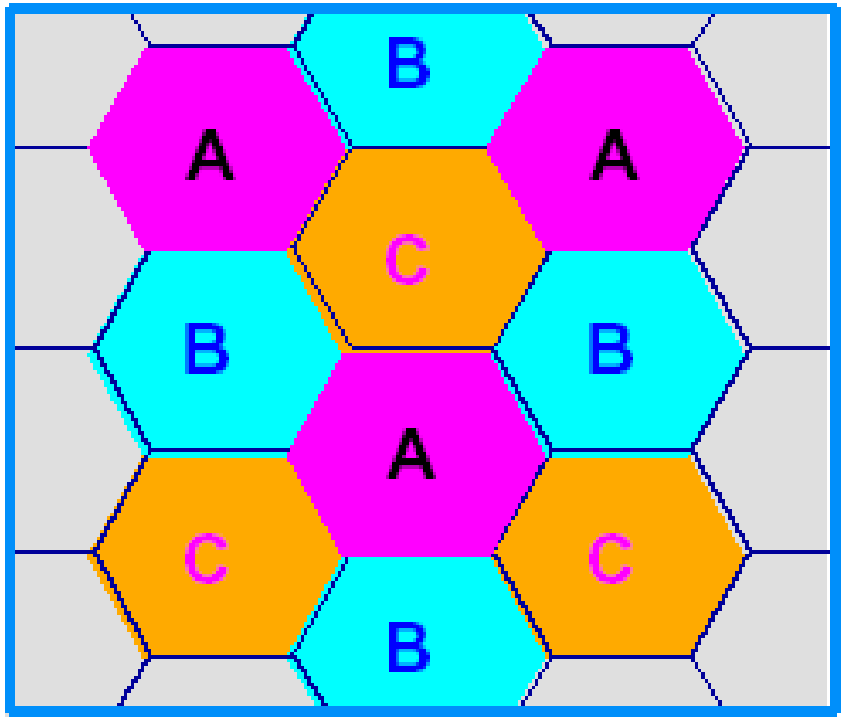
$$\cos(120) = -1/2$$

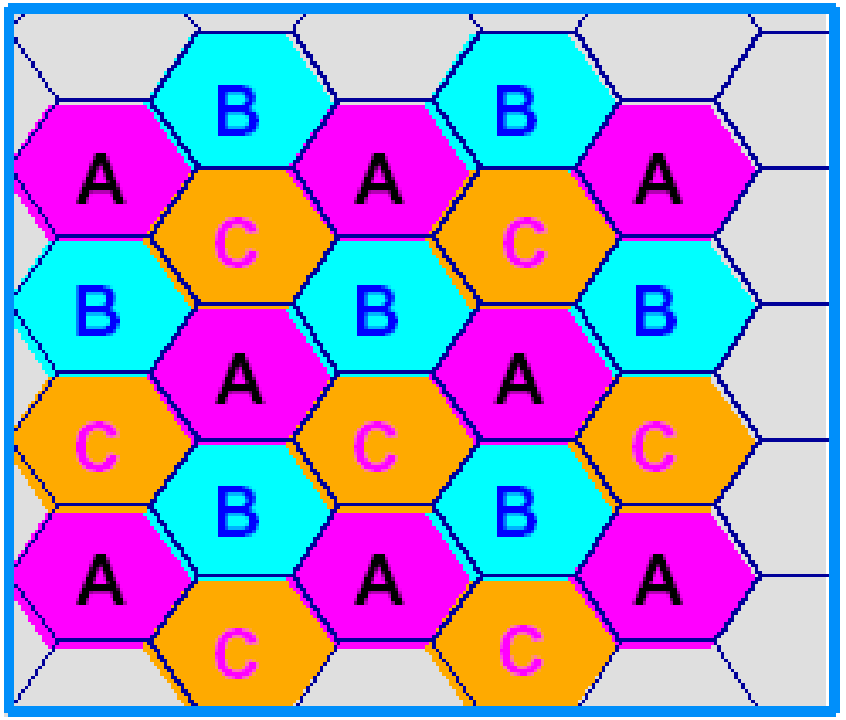
$$l = \sqrt{i^2 + j^2 + ij}$$

 $= l^2\sqrt{3}/2$

$$G = l^2 = i^2 + j^2 + ij$$

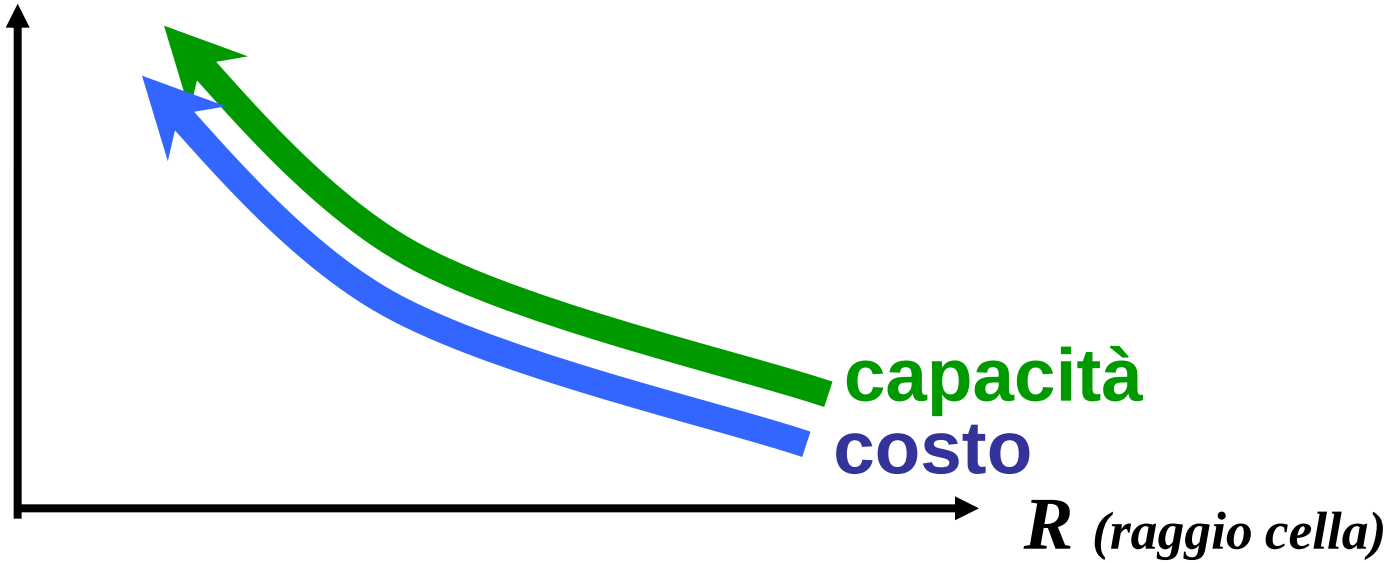
La dimensione della cella





Al diminuire della dimensione delle celle, aumenta la capacità del sistema (densità di canali per unità di superficie), ma anche il costo della rete

La dimensione della cella

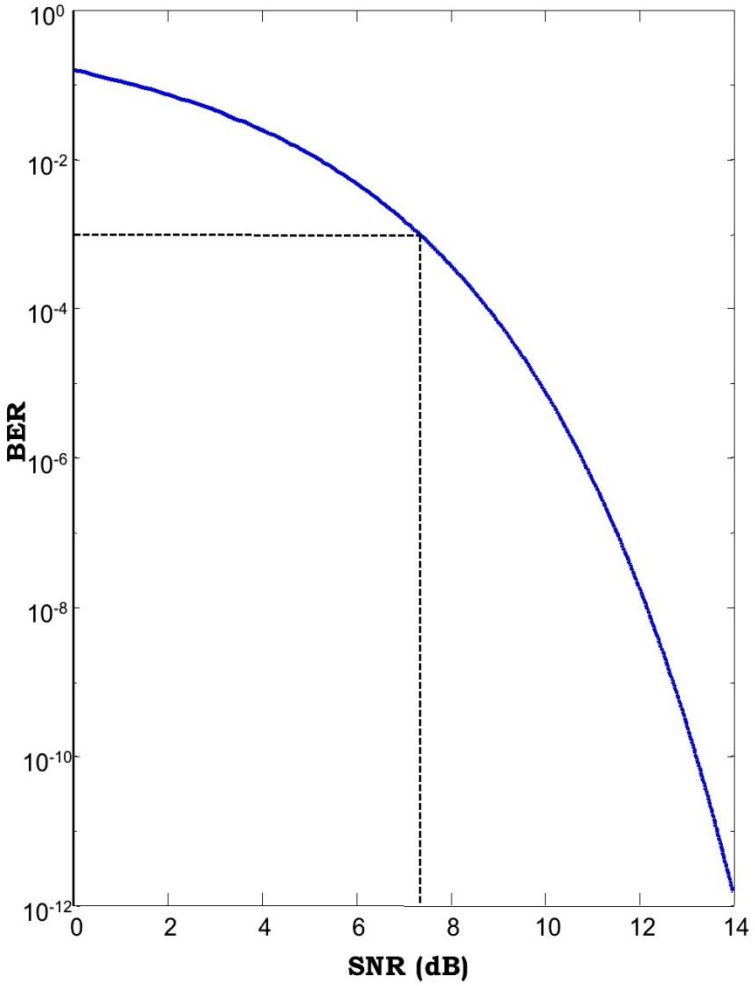


A pari G:

- Minore R, maggior numero di canali per unità di superficie
- Minore R, maggiore numero di antenne per avere la stessa coperura

Qualità

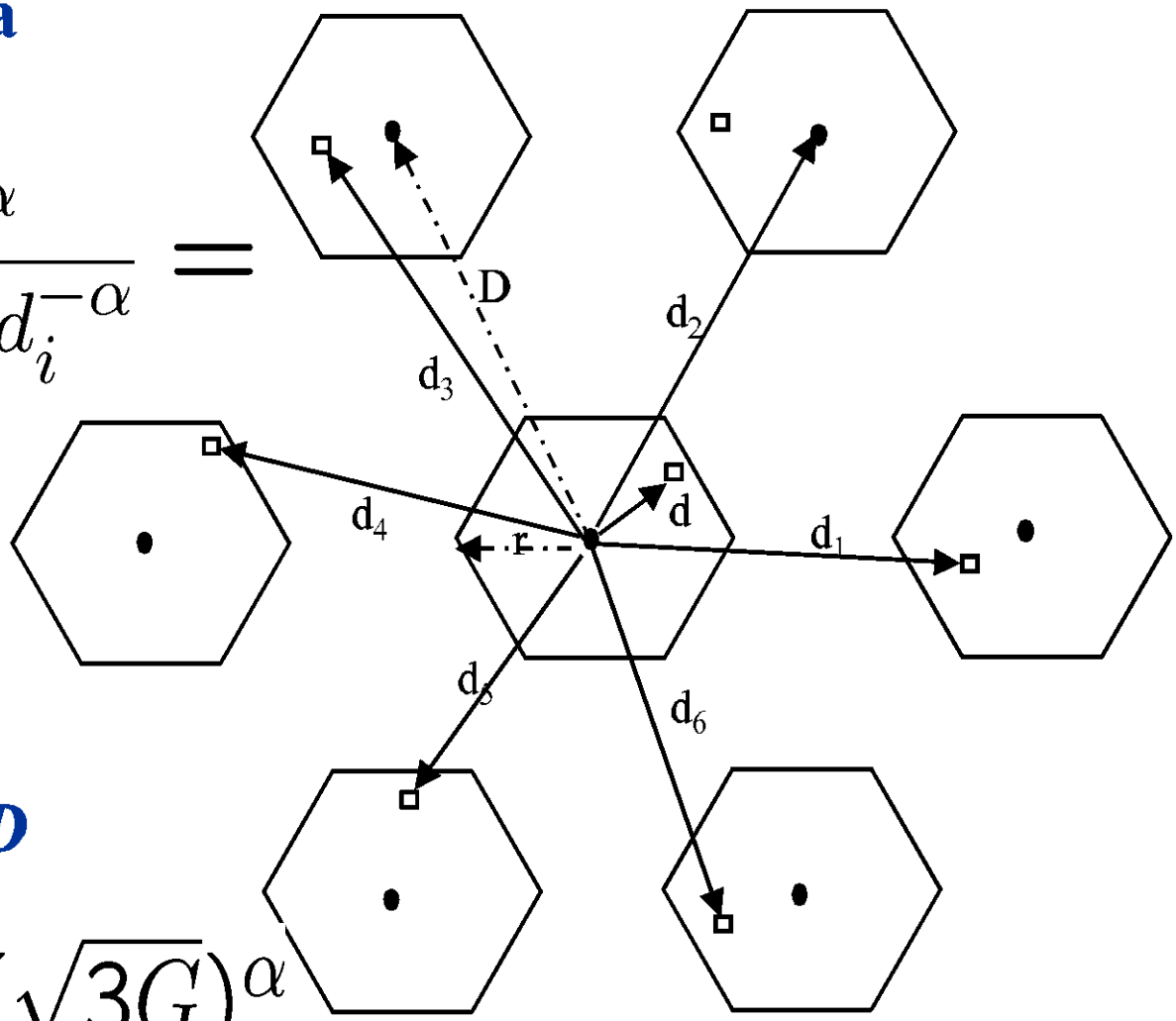
- Nei normali sistemi di comunicazione la qualità (in termini di BER – Bit Error rate) di collegamento dipende dal rapporto segnale-rumore (*SNR* – Signal-to-Noise Ratio)
- Nei sistemi radiomobili si considera il rapporto tra potenza del segnale e potenza dell'interferenza *SIR* (Signal-to-Interference Ratio)



Dimensionamento del Cluster

- **stesse antenne e stessa potenza** P

$$SIR = \frac{Pd^{-\alpha}}{\sum_{i=1}^{6} Pd_i^{-\alpha}} = \frac{d^{-\alpha}}{\sum_{i=1}^{6} d_i^{-\alpha}}$$

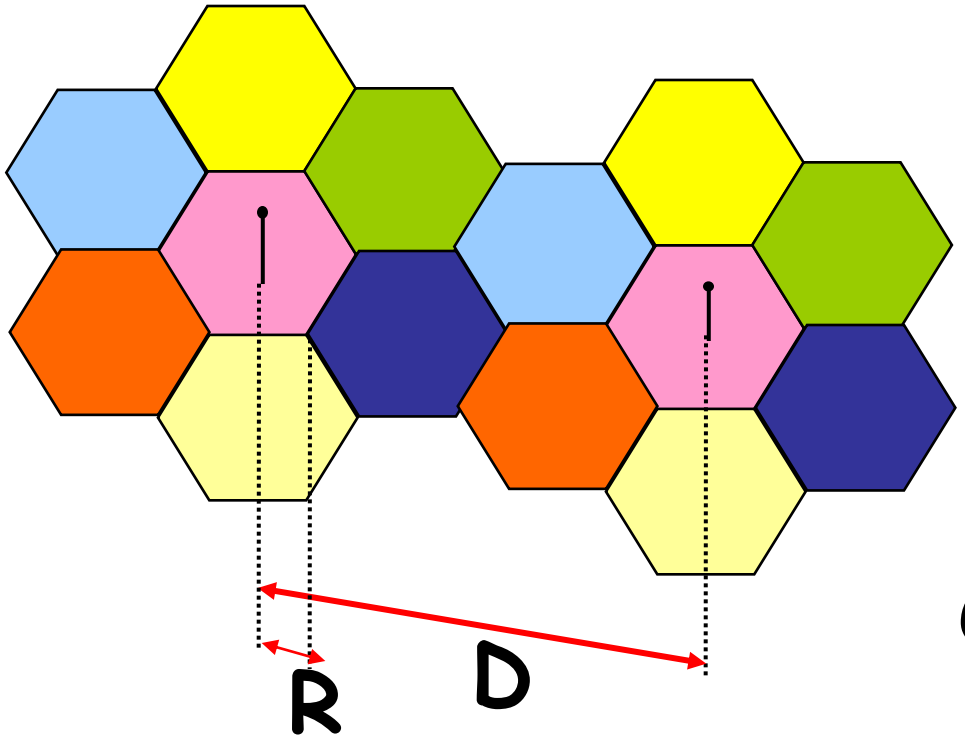


- **caso peggiore** $d = r$
- **approssimazione** $d_i = D$

$$SIR \sim \frac{r^{-\alpha}}{6D^{-\alpha}} = \frac{1}{6}(\sqrt{3G})^{\alpha}$$

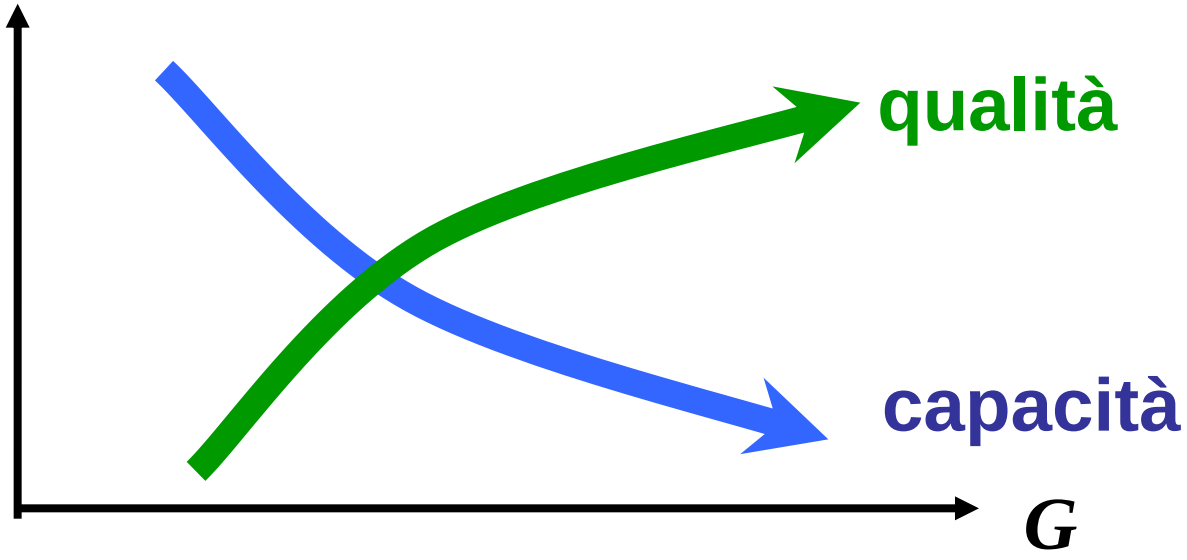
Il parametro Q

- Per celle con stessa dimensione e stazioni base con la stessa potenza, il SIR (qualità del canale) dipende (in modo approssimanto) solo da G



$$Q = D / R = \sqrt{3G}$$

La dimensione del cluster



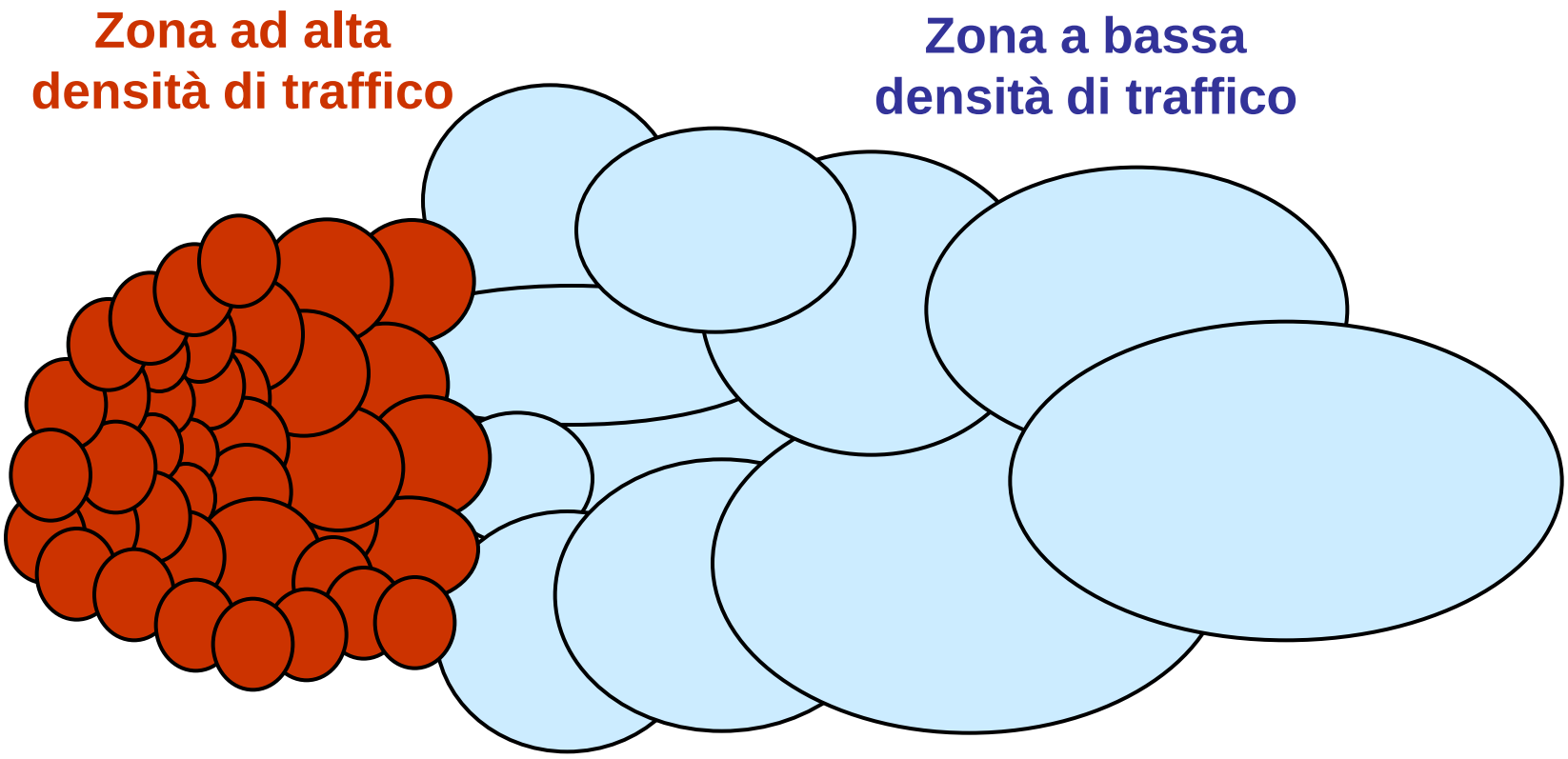
A pari R (= a parità di copertura di una cella):

- Minore *G*, maggiore numero di canali per cella (k) e maggiore la capacità
- Maggiore G, maggiore D, minore interferenza, migliore qualità

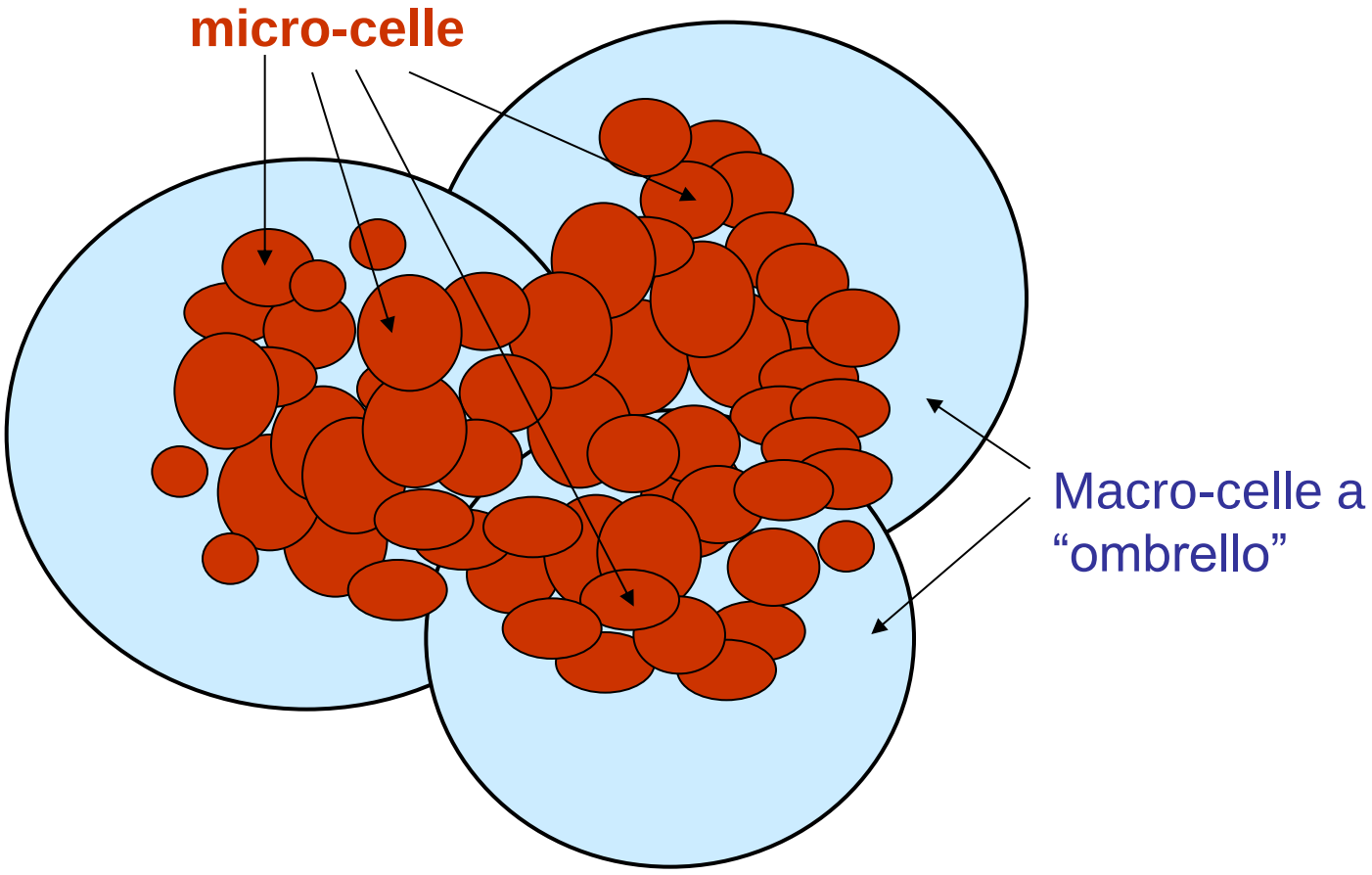
Tecniche di copertura cellulare

- È possibile usare antenne direzionali per avere celle di forma e dimensione particolare
- Celle di dimensione (e forma) diversa
- Celle “stratificate” (celle a ombrello)
- Sono allo studio tecniche per ottenere celle “puntiformi” che “inseguono” il terminale mobile

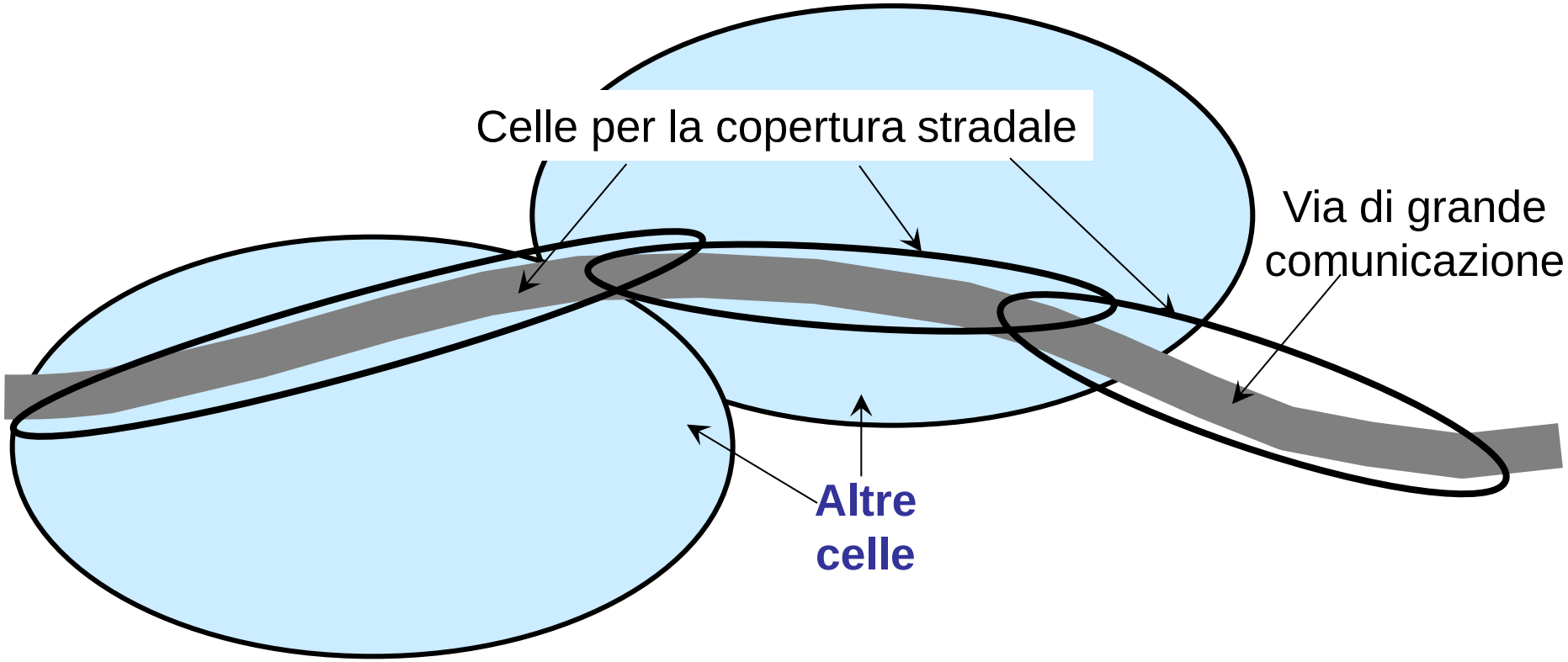
Adattare la dimensione delle celle alle aree con diversa intensità di traffico



Copertura cellulare stratificata



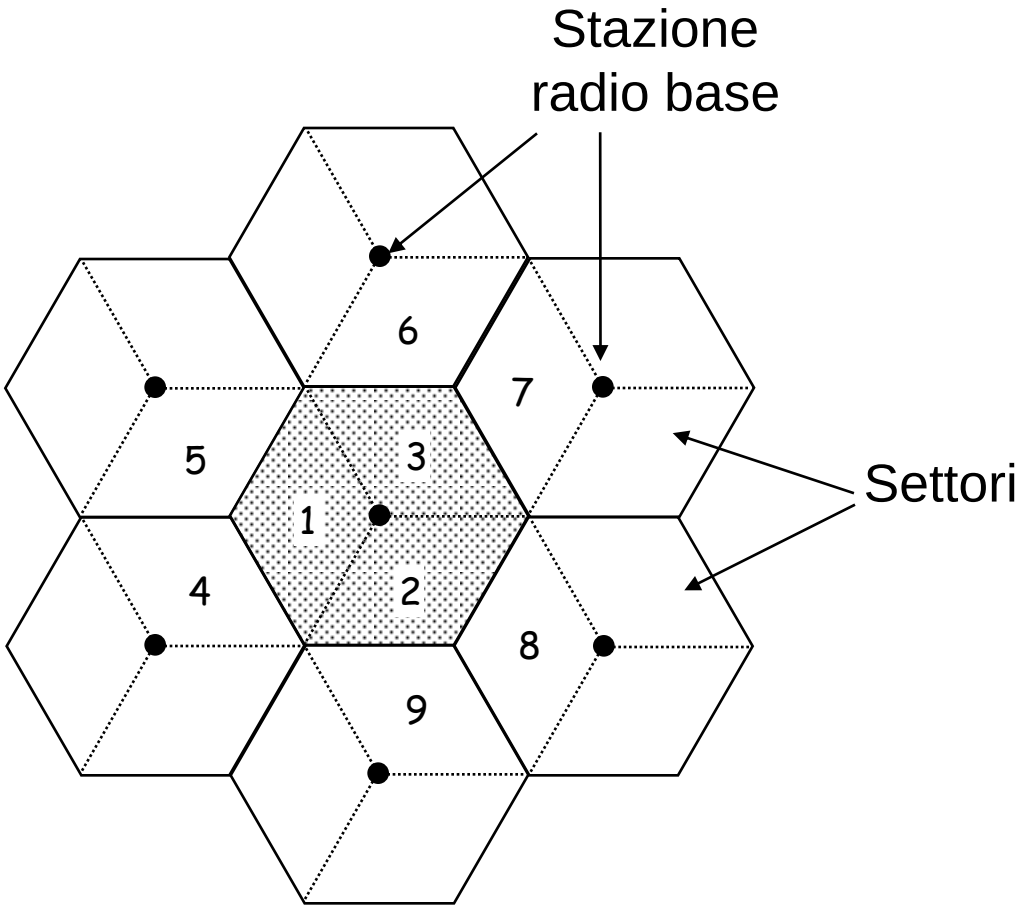
Copertura cellulare di tipo autostradale



Sectoring

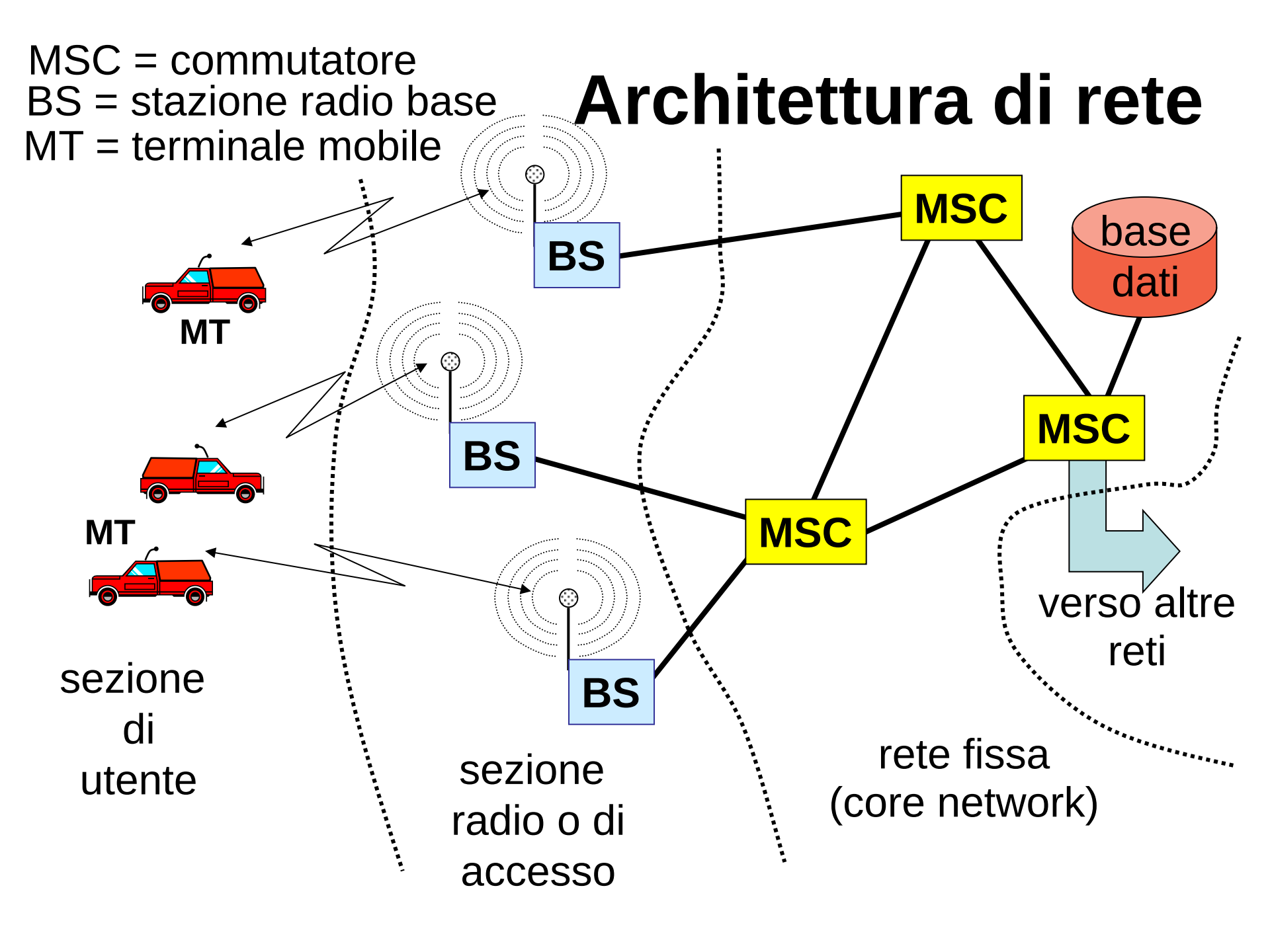
- La cella è divisa in settori che usano frequenze diverse con antenne direttive (a 60° o 120°)
- Le antenne direttive riducono l'interferenza
- Creo nuove "celle" senza aumentare i costi dei siti radio
- Configurazione tipica è la tri-cellulare con 3 settori per cella (3 celle per sito) e antenne direttive separate di 120°

Copertura cellulare con cluster di 9 celle e antenne settoriali a 120°



MSC = commutatore
BS = stazione radio base
MT = terminale mobile

Architettura di rete



Gestione della mobilità

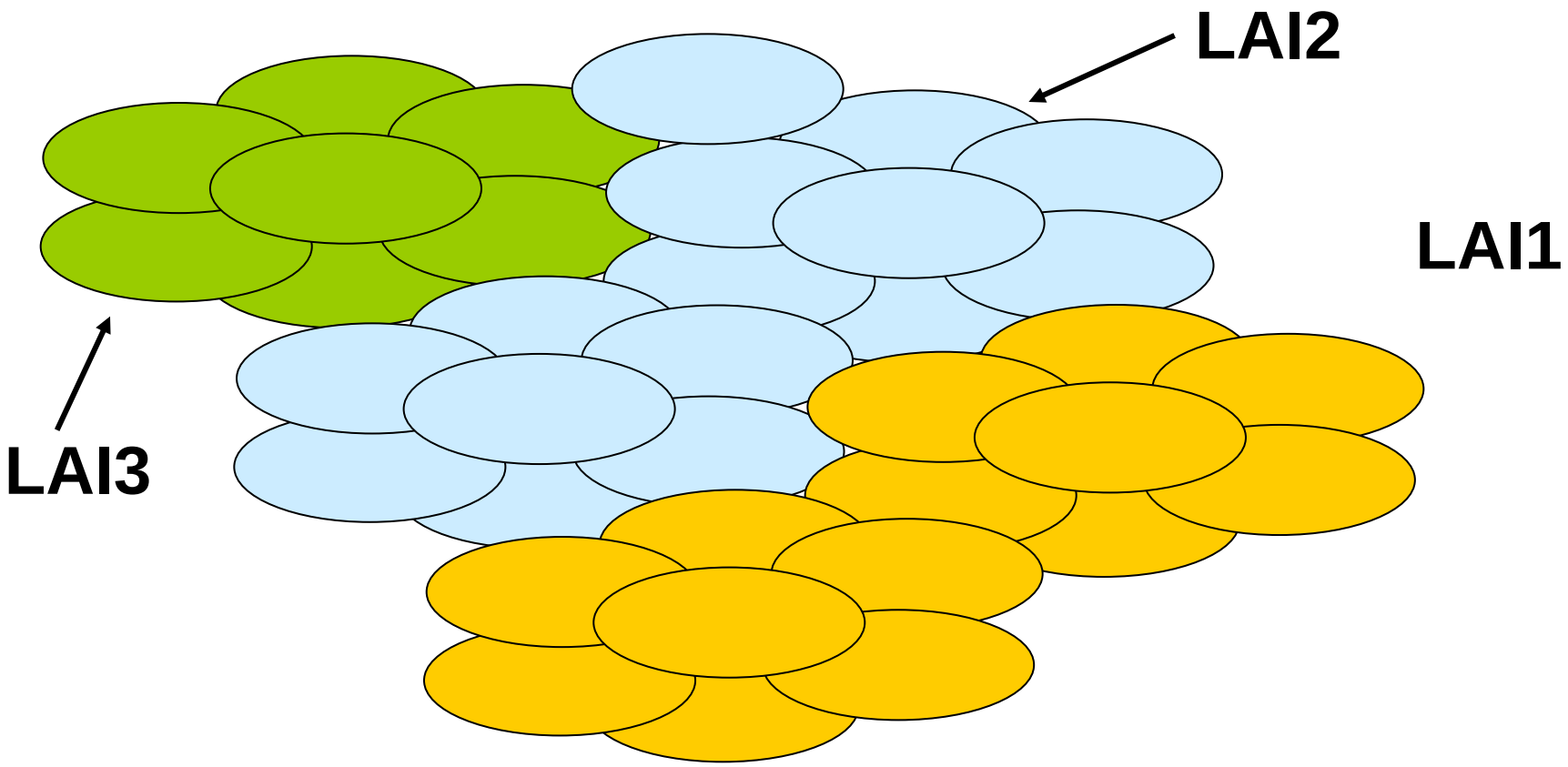
- Il supporto dell'elevata mobilità è di fatto l'elemento distintivo tra le reti cellulari ed ogni altro tipo di rete TLC
- Sono necessarie alcune procedure
  - Roaming
  - Location updating
  - Paging
  - Handover

Roaming

- È la possibilità data all'utente di essere rintracciabile anche se si sposta all'interno della rete
- Il sistema deve memorizzare in una base di dati la posizione degli utenti per poterli rintracciare
- Per memorizzare la posizione dell'utente si divide il territorio in aree dette location area (LA) che sono insiemi di celle

Roaming

- Ogni location area ha un identificativo, il location area identifier (LAI)



Location Updating

- È la procedura con cui avviene l'aggiornamento della posizione dell'utente
- In ogni cella di una LA viene diffuso periodicamente il LAI su un canale di controllo
- Il terminale mobile che riceve un LAI diverso da quello precedentemente memorizzato richiede al sistema una procedura di location updating (aggiornamento della base di dati)

Paging

- È la procedura con cui il sistema avvisa un terminale mobile di una chiamata in arrivo
- Il sistema invia un messaggio di paging all'interno della LA in cui è localizzato l'utente

Handover

- È la procedura che consente il trasferimento di una chiamata attiva da una cella alla successiva, mentre il terminale mobile si sposta all'interno della rete
- È un'operazione complessa che pone alla rete notevoli requisiti in termini di architettura di rete, di protocolli e di segnalazione per la gestione delle procedure connesse agli handover

Classificazione handover

- **Intra <-> Inter Cell**
  - Indica se l'handover avviene tra frequenze all'interno della stessa cella o tra celle diverse
- **Soft <-> Hard**
  - indica se durante l'handover sono attivi entrambi i canali radio (soft) o solamente uno per volta (hard)
- **Forward <-> Backward**
  - indica se la segnalazione avviene tramite la BS di origine (backward) oppure la BS destinazione (forward)

Classificazione handover

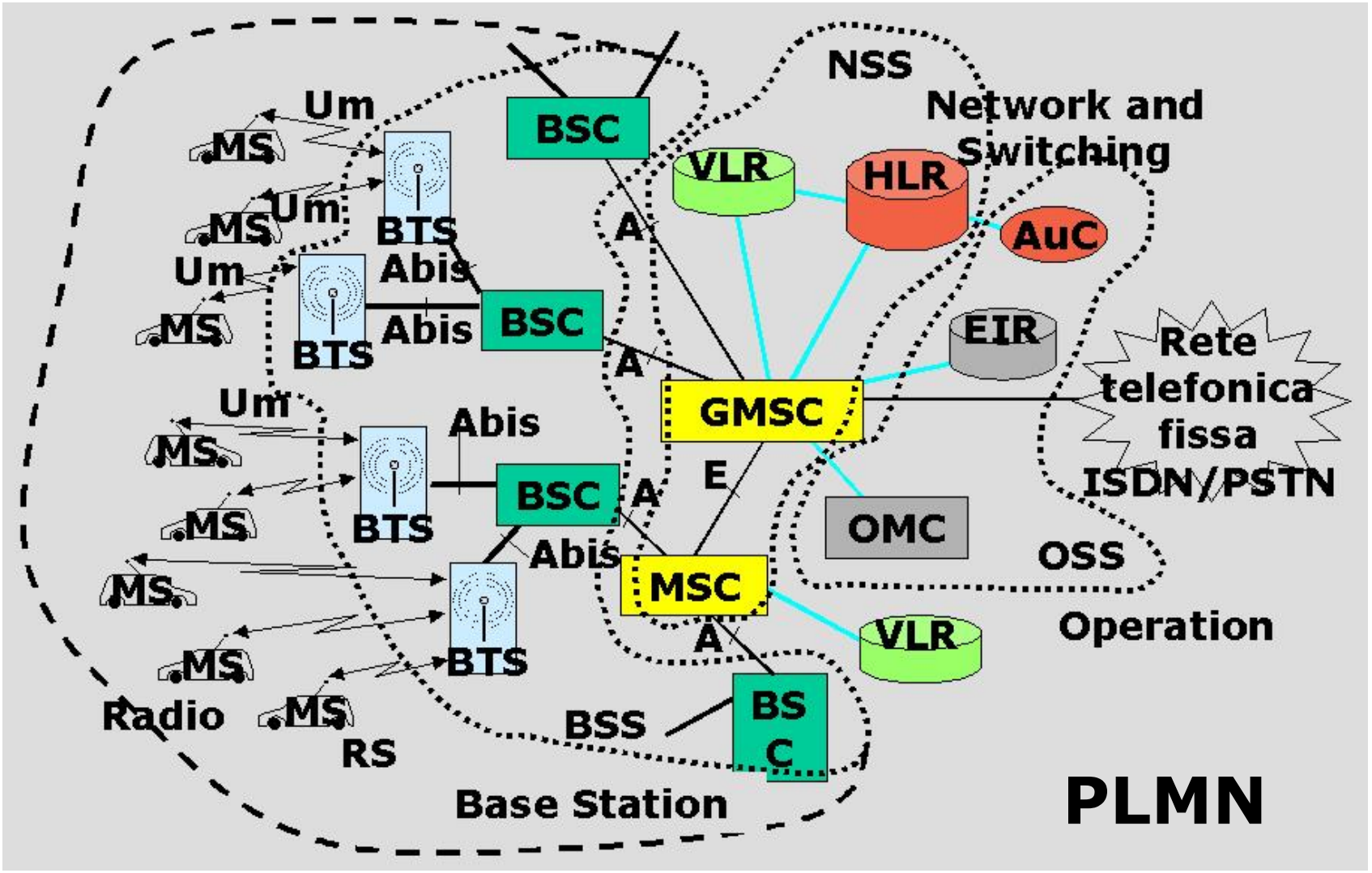
- **MT <-> BS initiated**
  - indica se il primo messaggio di segnalazione per l'inizio di handover viene inviato dal terminale utente come richiesta (MT initiated) oppure da BS come comando (BS initiated)
- inoltre bisogna anche stabilire chi e come effettua le misure necessarie per stabilire il momento opportuno per effettuare un handover

Altre funzioni: la registrazione

- E’ la funzione di
  - collegamento del terminale alla rete
  - identificazione, autenticazione
- Procedura da eseguire:
  - all’accensione del terminale
  - tutte le volte che si desidera accedere ad un nuovo servizio (es. fare una nuova chiamata)
  - serve ad associare il terminale alla rete

GSM
Architettura

Architettura del GSM



Terminale Mobile (Mobile Equipment – ME)

È il terminale di proprietà dell'utente

Ne esistono molti tipi diversi, a seconda delle applicazioni e dei luoghi di installazione

Terminale Mobile (Mobile Equipment – ME)

Tre categorie a seconda della potenza nominale:

Veicolari: possono emettere fino a 20 W all'antenna

Portatili: fino a 8 W all'antenna, sono trasportabili, ma richiedono elevata energia

Personali (hand-terminal): fino a 2 W all'antenna, è il "telefonino"

Terminale Mobile (Mobile Equipment – ME)

- "Dual-Band" se funziona sia a 900 MHz che a 1800 MHz
- "Three-Band" se funziona a 900, 1800 e 1900 MHz
- ME è solamente "hardware", per poter funzionare e collegarsi alla rete ha bisogno di una scheda di abilitazione: la **SIM**

Terminale Mobile (Mobile Equipment – ME)

- Nei paesi dove i numeri di emergenza (Ambulanza, Polizia, Pompieri, etc.) sono considerati un bene primario ME è abilitato a chiamare questi numeri anche senza la SIM

In Italia funziona il 112

Modulo di Identificazione Utente (Subscriber Identity Module – SIM)

- È una scheda intelligente (con processore e memoria) di tipo *smart card* che rende "operativo" un qualunque ME
- Deve essere inserita nell'apposito alloggiamento all'interno del ME

Modulo di Identificazione Utente (Subscriber Identity Module – SIM)

- Le caratteristiche dell'utente (# telefonico, servizi accessibili, parametri per la sicurezza, ecc.) sono memorizzate in modo permanente e crittografato nella SIM, che rappresenta quindi il vero e proprio "servizio" offerto dai gestori...

Modulo di Identificazione Utente (Subscriber Identity Module – SIM)

- …ad esempio è possibile acquistare SIM da gestori diversi e usarle nello stesso ME a seconda delle esigenze, oppure è possibile recarsi all'estero portando solo la SIM, affittare un ME localmente e connettersi (o viceversa, portare un ME e acquistare una SIM localmente)

Modulo di Identificazione Utente (Subscriber Identity Module – SIM)

- Memorizza messaggi brevi inviati dalla rete (più evolve la tecnologia maggiori capacità potranno essere associate alla SIM) tra cui gli SMS
- La SIM viene abilitata attraverso un codice di 4 cifre (**PIN** - Personal Identification Number)

Modulo di Identificazione Utente (Subscriber Identity Module – SIM)

- Se il PIN viene sbagliato 3 volte consecutive, la SIM si autoblocca e può essere sbloccata solo con un codice di sblocco a 8 cifre (PUK - Personal Unblocking Key)

Modulo di Identificazione Utente (Subscriber Identity Module – SIM)

+

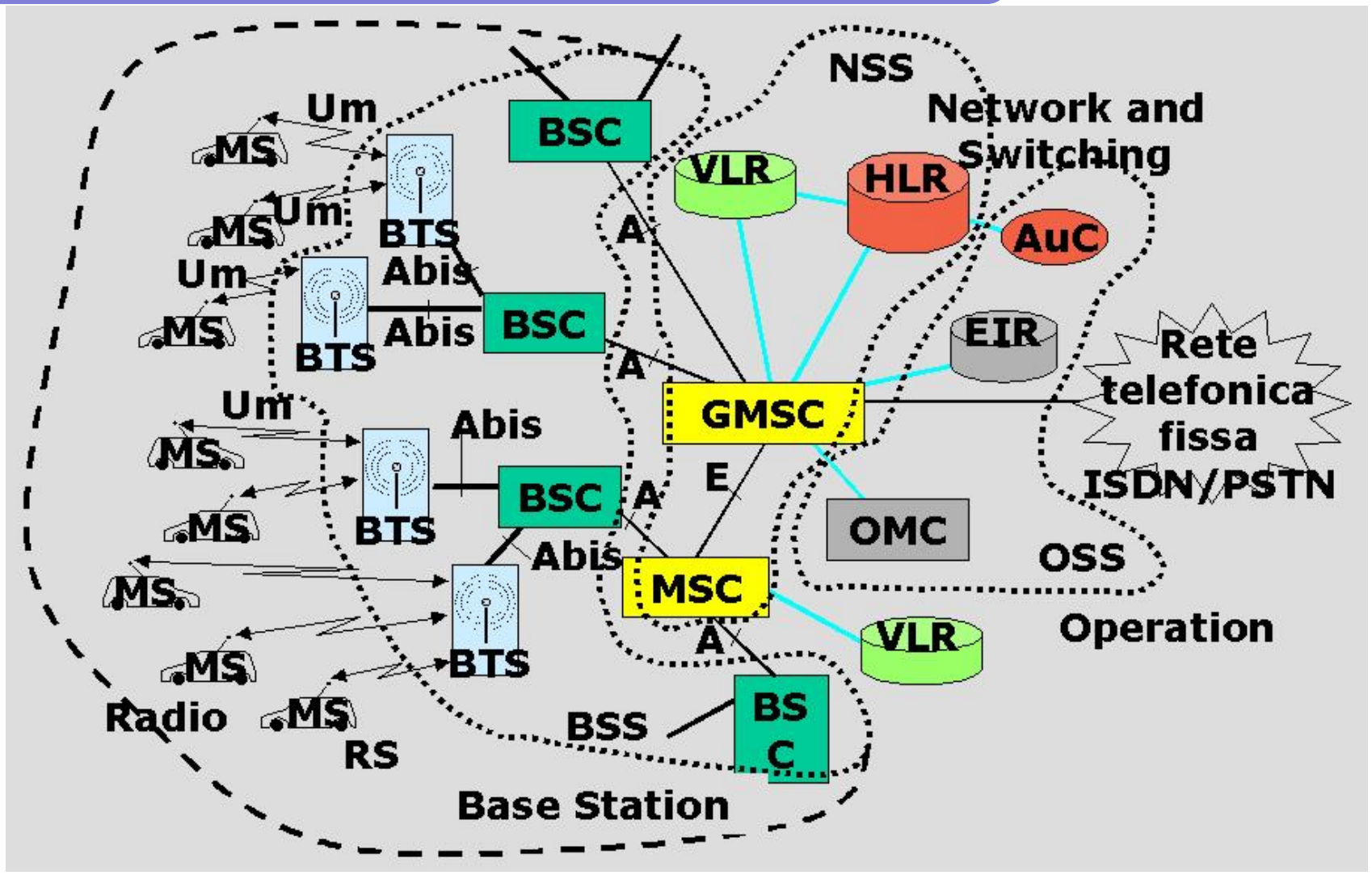
=

ME

SIM

MS
(Mobile Station)

Architettura del GSM



Stazione Radio Base

Base Station (BS)

Base Tranceiver Station (BTS)

Interfaccia fisica che si occupa della rice-trasmissione

Base Station Controller (BSC)

Controllo delle risorse sull'interfaccia radio

Stazione Radio Base

Base Tranceiver Station
BTS

Stazione Radio Base

Base Tranceiver Station - BTS

È il punto di accesso alla rete di TLC, o se si vuole, la "controparte" di MS

Stazione Radio Base

Base Tranceiver Station - BTS

È collocata in un punto opportuno della cella (es. al centro per celle circolari, nel vertice delle celle settorizzate, ad un estremo delle celle oblunghe per la copertura stradale...)

Stazione Radio Base

Base Tranceiver Station - BTS

Dalla potenza del BTS dipende la dimensione fisica della cella: grazie a questa caratteristica è possibile "aggiustare" in modo dinamico le dimensioni delle celle

Stazione Radio Base

Base Tranceiver Station - BTS

Ciascuna BTS può avere da 1 a 16 interfacce radio, corrispondenti a diversi canali in FDM

Ciascun canale FDM corrisponde a 8 canali TDM

Stazione Radio Base

Base Tranceiver Station - BTS

Effettua la codifica di canale (Channel Coding Unit –CCU) e la cifratura

Modula / demodula i segnali

Realizza il frequency hopping

Effettua l'interleaving

Stazione Radio Base

Base Tranceiver Station - BTS

Effettua misura di qualità dei canali uplink e riceve da MT le misure relative al downlink, le invia al BSC che decide il controllo di potenza e l'handover

Stazione Radio Base

Base Tranceiver Station - BTS

Implementa i protocolli di livello fisico sull'interfaccia radio (Um) per il corretto scambio di informazioni tra MS e BTS

Stazione Radio Base

Base Tranceiver Station - BTS

È un apparato di livello fisico e non ha praticamente alcuna "intelligenza": nel GSM anche la valutazione e la decisione sugli handover da effettuare è demandata ad altre entità (MT, BSC e MSC)

Stazione Radio Base

Base Station (BS)

Base Tranceiver Station (BTS)

Interfaccia fisica che si occupa della rice-trasmissione

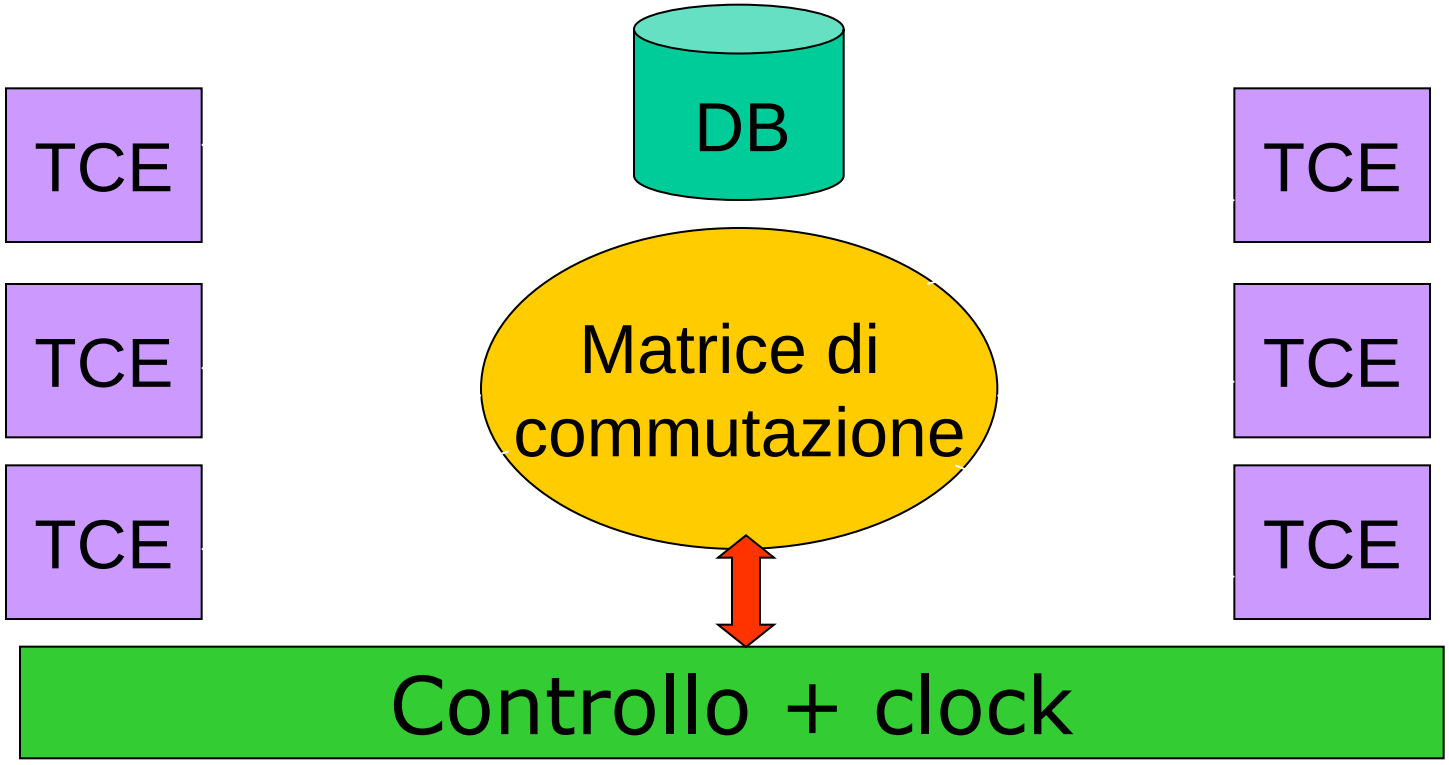
Base Station Controller (BSC)

Controllo delle risorse sull'interfaccia radio

Controllore della Stazione Radio Base (Base Station Controller-BSC)

Un BSC controlla un numero elevato di BTS:
da alcune decine
ad alcune centinaia

Controllore della Stazione Radio Base (Base Station Controller-BSC)



Controllore della Stazione Radio Base (Base Station Controller-BSC)

- **BTS e BSC sono collegate da collegamenti a 2 Mb/s (32 canali PCM a 64 kb/s)**
- **Un canale PCM del collegamento a 2 Mb/s viene usato per trasportare 4 canali di traffico GSM a 13 kb/s**
- **Per ogni portante occorrono 3 canali PCM: 1 per segnalazione, 2 per trasportare 8 canali di traffico GSM**

Controllore della Stazione Radio Base (Base Station Controller-BSC)

- La transcodifica della voce GSM (13 kb/s) ↔ PCM (64 kb/s) e viceversa è fatta dalla BSC (Transcoder Rate Adaptation Unit - TRAU)

Controllore della Stazione Radio Base (Base Station Controller-BSC)

I compiti principali del BSC sono:

Transcodifica della voce

GSM ↔ PCM

Controllore della Stazione Radio Base (Base Station Controller-BSC)

I compiti principali del BSC sono:

Analisi delle misure di qualità del segnale sulla tratta radio

→ Gestione dell'handover tra BTS controllate dallo stesso BSC o richiesta di gestione all'MSC

Controllore della Stazione Radio Base (Base Station Controller-BSC)

I compiti principali del BSC sono:

Controllo delle risorse radio: gestione delle frequenze, che possono essere assegnate in modo dinamico alle varie BTS

Controllore della Stazione Radio Base (Base Station Controller-BSC)

I compiti principali del BSC sono:

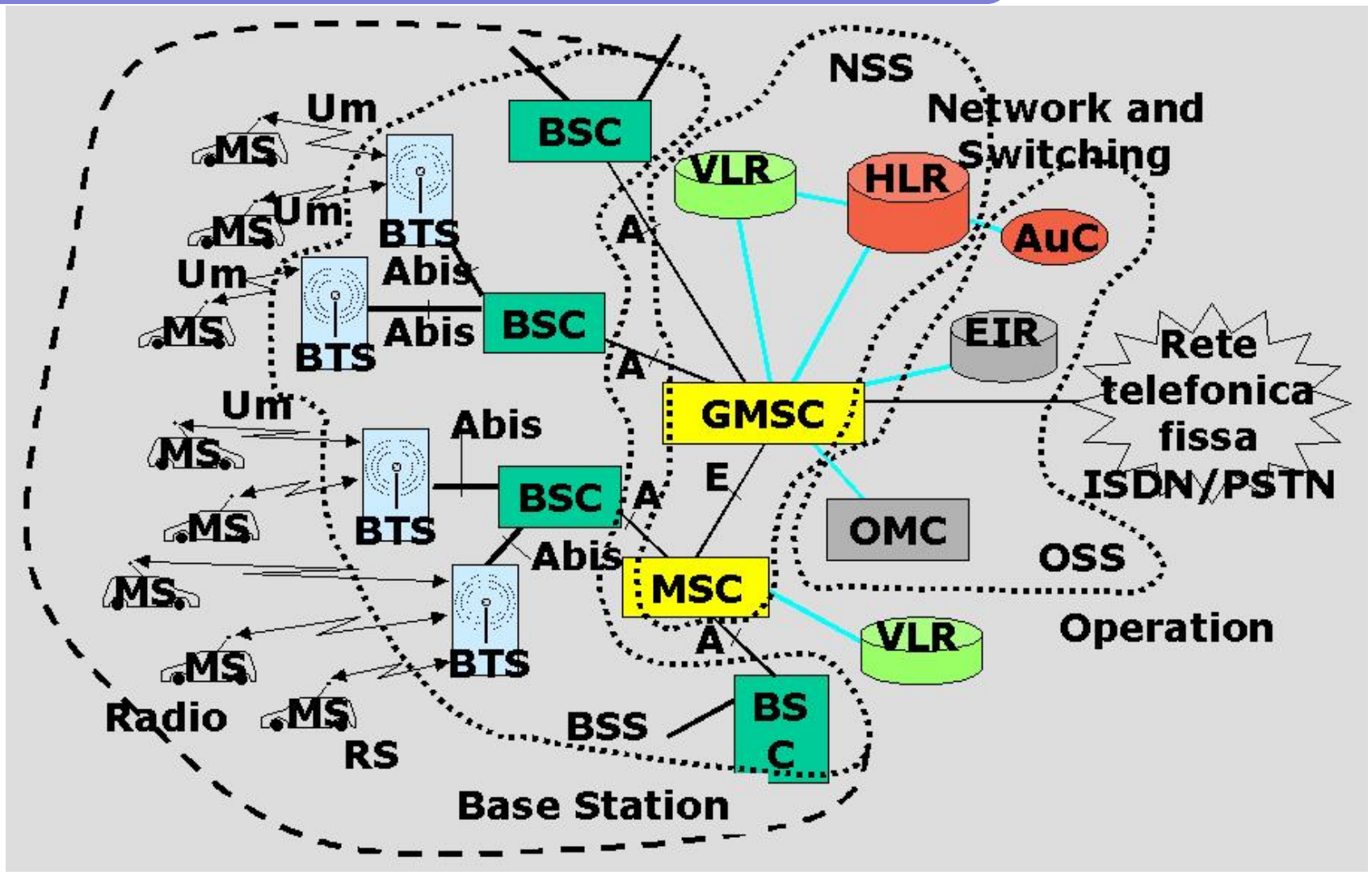
- **Gestione del paging**
- **Manutenzione del BSS**

Controllore della Stazione Radio Base (Base Station Controller-BSC)

I compiti principali del BSC sono:

La concentrazione del traffico verso un MSC e lo smistamento del traffico verso le BTS

Architettura del GSM



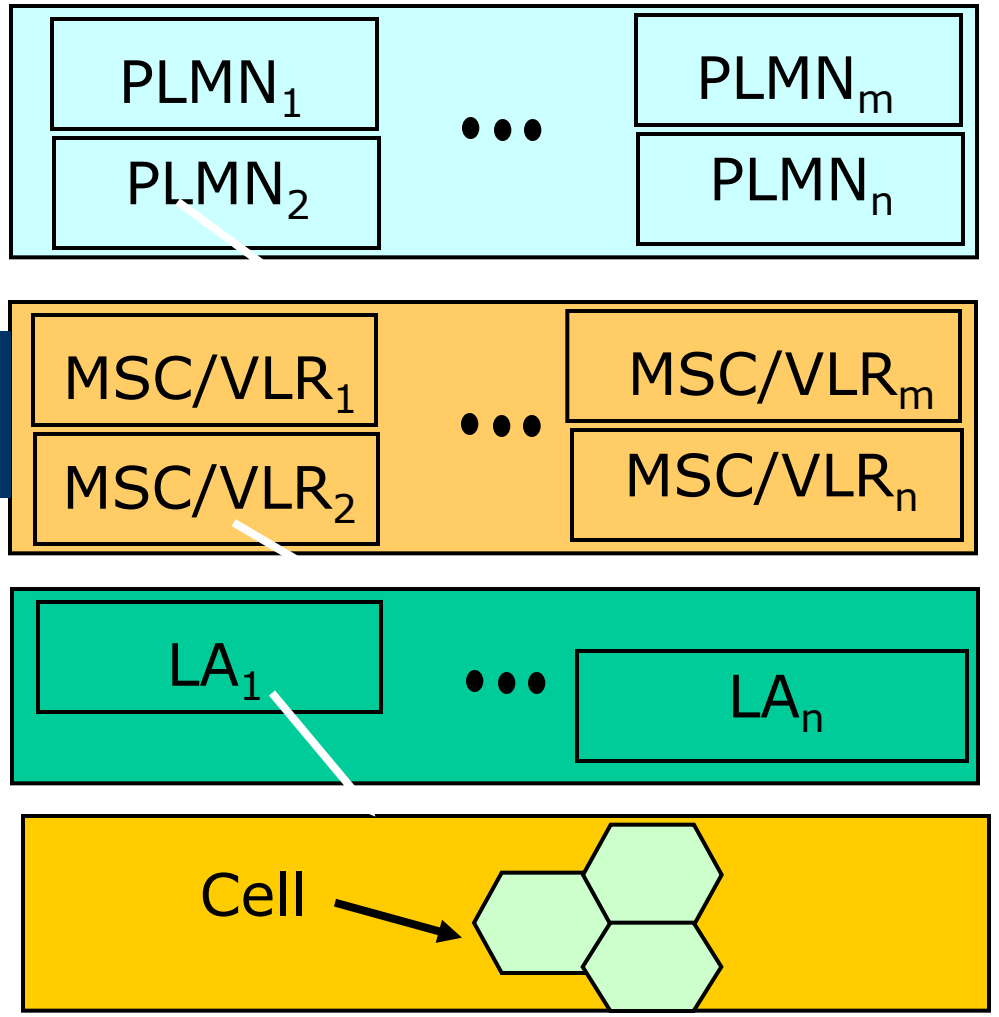
Aree del GSM

GSM Service Area

PLMN Service Area
(es. TIM, Vodafone, ...)

MSC/VLR Service Area

Location Area

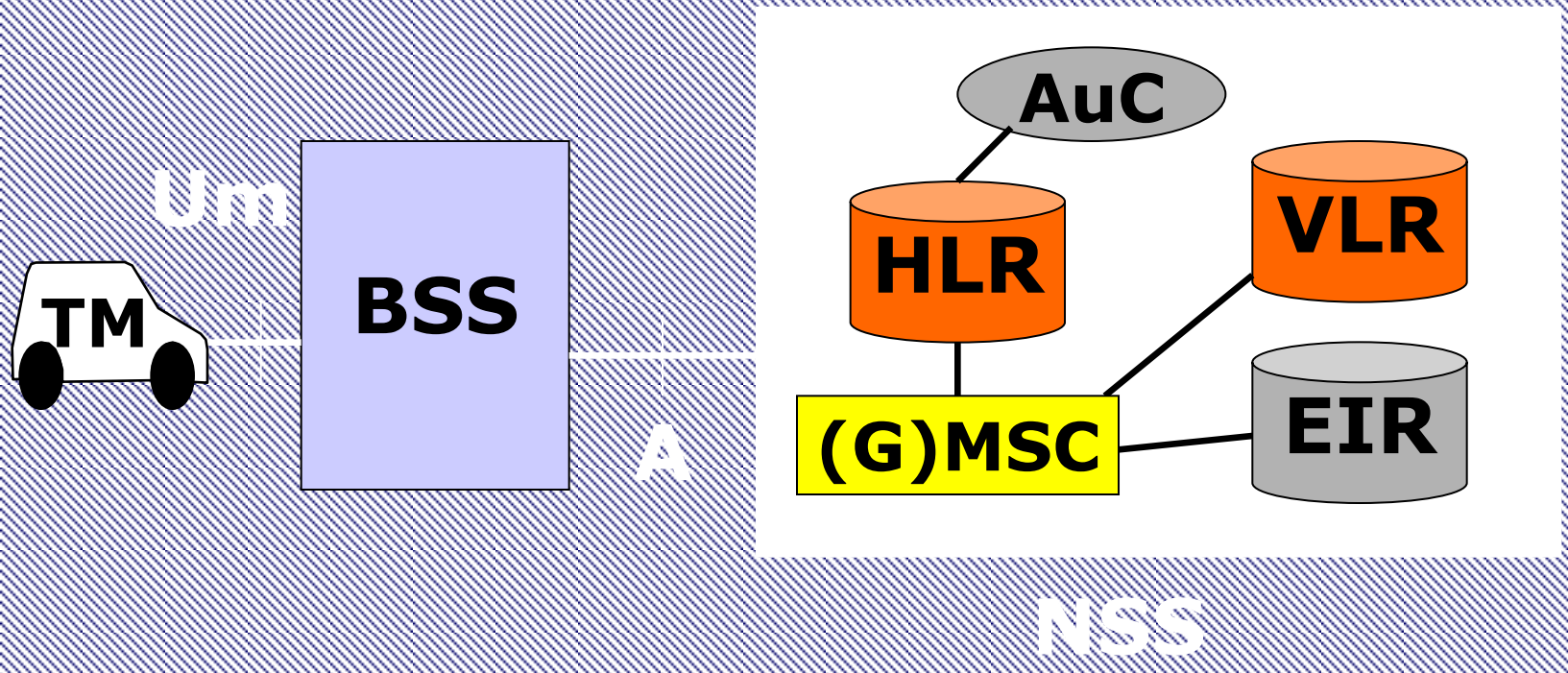


Network and Switching Sub-system (NSS)

Noto anche come Switching and Management Sub-system (SMSS), svolge funzioni fondamentali

- → **Gestione della mobilità**
- → **Controllo delle chiamate**
- → **Supporto ai servizi forniti**

Network and Switching Sub-system (NSS)



Centro di Commutazione dei Servizi Mobili (Mobile Switching Center-MSC)

- E' un "normale" commutatore PCM (commutatore a circuito) cui sono state aggiunte funzionalità di segnalazione per la gestione della mobilità

Centro di Commutazione dei Servizi Mobili (Mobile Switching Center-MSC)

- Funzioni fondamentali:
  - Alloca risorse e crea connessioni con le MS sulla parte di rete fissa (Connection Management - CM)
  - Consente l'instradamento delle chiamate da una MS ad un'altra

Centro di Commutazione dei Servizi Mobili (Gateway Mobile Switching Center-GMSC)

- Un caso particolare di MSC è il **GMSC** (*Gateway*-MSC), che è l'interfaccia tra la rete GSM e le reti fisse (PSTN) e/o altre reti GSM (PLMN)

Centro di Commutazione dei Servizi Mobili (Gateway Mobile Switching Center-GMSC)

- Funzioni fondamentali:
  - Interworking con altre reti
  - Funzioni di gateway

Centro di Commutazione dei Servizi Mobili (Gateway Mobile Switching Center-GMSC)

- Consente l'instradamento delle chiamate da una MS verso telefoni fissi e mobili in altre reti

- GMSC è anche il "punto di partenza" per la ricerca delle MS nella rete cellulare per chiamate provenienti da altre reti (fisse o mobili)

Centro di Commutazione dei Servizi Mobili (Mobile Switching Center-MSC)

- A seconda delle dimensioni della rete e del numero di utenti un operatore può avere uno o più GMSC

Registro di Localizzazione Principale (Home Location Register)

- È una base dati **permanente** associata in modo univoco ad una PLMN
- A seconda delle dimensioni della rete e del numero di utenti un operatore può avere uno o più HLR a cui sono associati in modo fisso le MS. Spesso è colocato con un GMSC

Registro di Localizzazione Principale (Home Location Register)

- Memorizza le informazioni (profilo di utente) relative a tutti le MS la cui localizzazione di *default* è presso l'HLR considerato

Registro di Localizzazione Principale (Home Location Register)

- HLR memorizza informazioni **permanenti** come l'IMSI (International Mobile Subscriber Identity), il numero di telefono della SIM associata (che **NON** sono la stessa cosa), i servizi supplementari a cui l'utente è abilitato

Registro di Localizzazione Principale (Home Location Register)

- HLR memorizza anche informazioni **volatili**:
  - L'indirizzo del VLR presso cui può essere reperito l'utente
  - Parametri temporanei per identificazione e crittografia

Registro di Localizzazione Principale (Home Location Register)

- HLR memorizza anche informazioni volatili:
  - Eventuale numero di telefono per l'inoltro delle chiamate
  - ...

Registro di Localizzazione dei Visitatori (Visitor Location Register-VLR)

- È una base dati **temporanea** associata a tutti gli MSC, **anche ai GMSC** (spesso MSC e VLR sono integrati)
- Contiene i dati essenziali per il servizio delle MS attualmente sotto la giurisdizione del (G)MSC a cui VLR è associato

Registro di Localizzazione dei Visitatori (Visitor Location Register-VLR)

Si noti che per questione di uniformità viene usato il VLR anche per i terminali mobili che si trovano presso il proprio MSC: l'informazione memorizzata nell'HLR viene "duplicata localmente"

Registro di Localizzazione dei Visitatori (Visitor Location Register-VLR)

- Nel VLR vengono duplicati molti dei dati di un utente già presenti nell'HLR
- Anche i dati usati usati per identificare e autenticare l'utente

Registro di Localizzazione dei Visitatori (Visitor Location Register-VLR)

➔ Il VLR crea il TMSI (Temporary Mobile Subscriber Identity), che è usato invece dell'IMSI per non trasmettere regolarmente l'IMSI via radio (protezione da intrusioni), e lo memorizza

➔ Il VLR invia il TMSI in modo cifrato al TM che lo memorizza nella SIM

Registro di Localizzazione dei Visitatori (Visitor Location Register-VLR)

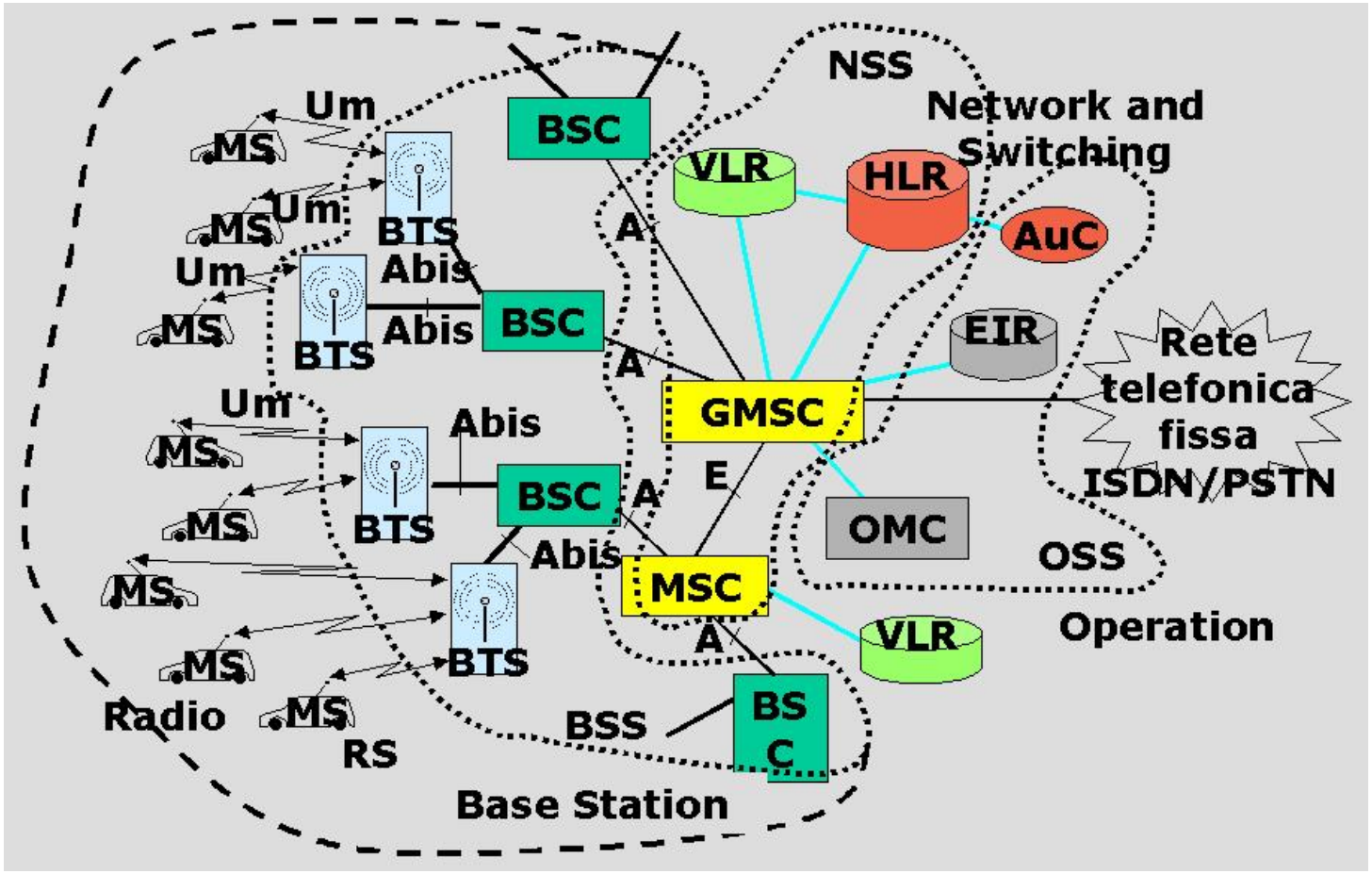
- Il TMSI viene modificato frequentemente ed è legato anche alla posizione del mobile (LAI)

- Il VLR memorizza anche il LAI e informazioni che servono per l'instradamento delle chiamate verso il TM (MSRN)

Registro di Localizzazione dei Visitatori (Visitor Location Register-VLR)

- Nel VLR viene mantenuto lo stato del TM: acceso (attached) o spento (detached)

Architettura del GSM



Registro di Identificazione degli apparati (Equipment Identity Register)

- È una base dati il cui uso è a discrezione dell'operatore
- Contiene l'identificativo e le caratteristiche di tutti gli apparati GSM (hardware) prodotti, insieme al produttore, al paese di fabbricazione...

Registro di Identificazione degli apparati (Equipment Identity Register)

- Può essere usato per proteggere la rete dall'uso di apparecchiature non a norma, rubate, esportate illegalmente...

Registro di Identificazione degli apparati (Equipment Identity Register)

L'EIR contiene 3 elenchi:

- **White list: identifica tutti i terminali operativi**
- **Grey list: identifica i terminali difettosi o non omologati**

Registro di Identificazione degli apparati (Equipment Identity Register)

L'EIR contiene 3 elenchi:

- **Black list: identifica apparati rubati o non autorizzati**

Centro di Autenticazione (Authentication Center–AuC)

Genera le chiavi di cifratura necessarie per la trasmissione sicura sull'interfaccia radio

Centro di Autenticazione (Authentication Center–AuC)

- È associato all'HLR
- È il "motore" per l'autenticazione delle SIM
- È in grado di effettuare correttamente le operazioni di codifica che sono associate a ciascuna SIM

Procedure di sicurezza

- Le procedure di sicurezza hanno 2 obiettivi:
  - **Autenticazione:** proteggere da tentativi di utilizzo fraudolento della rete da parte di persone non autorizzate
  - **Cifratura:** proteggere da tentativi di accesso non autorizzato ai dati da parte di utenti regolari

Centro Gestione e Controllo (Operation and Maintenance Center)

È la sede di tutte le operazioni di gestione (tecnica e non) della rete

Centro Gestione e Controllo (Operation and Maintenance Center)

Effettua la tariffazione,
controlla il traffico in rete,
gestisce i messaggi di errore
provenienti dalla rete,
controlla e memorizza il carico
delle singole BTS e BSC
per operazioni di pianificazione
(eventualmente dinamica)

Aree del GSM

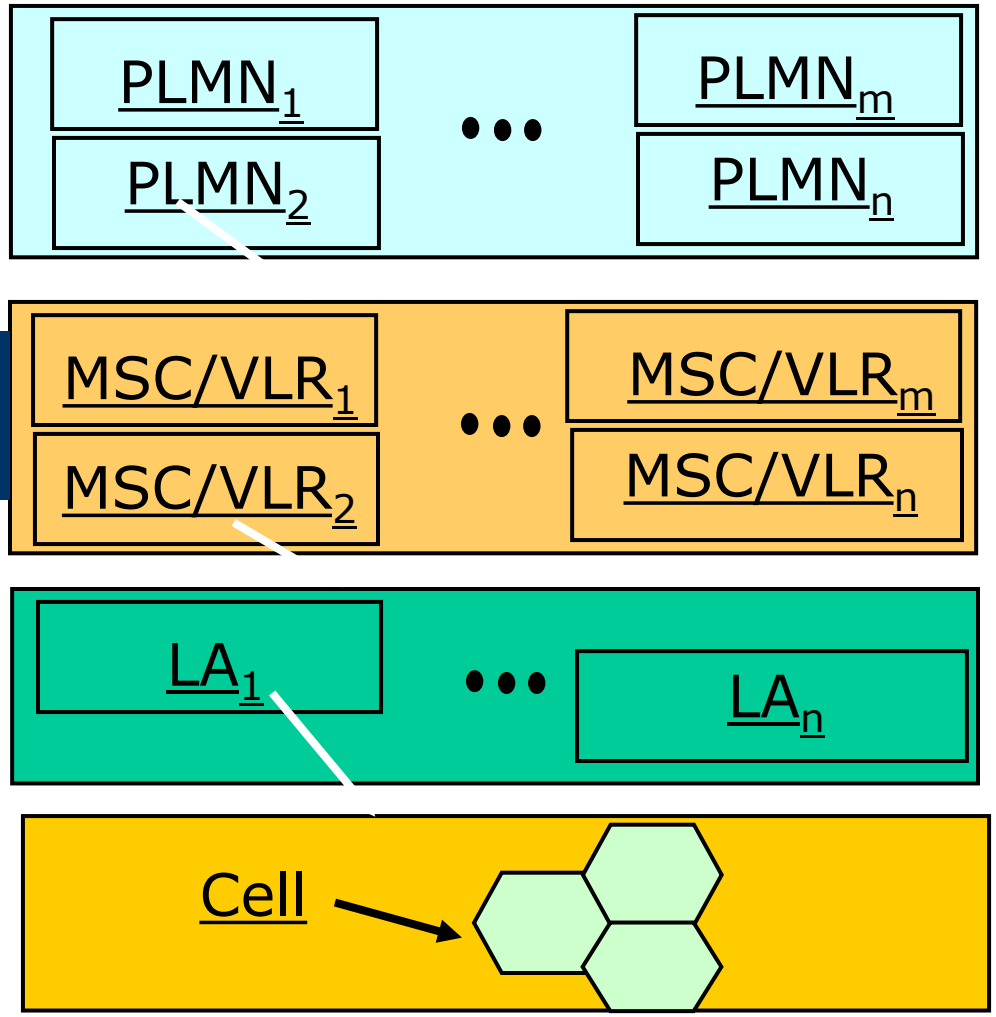
Aree del GSM

GSM Service Area

PLMN Service Area
(es. TIM, Vodafone, ...)

MSC/VLR Service Area

Location Area



Aree del GSM

Cella

- Identificata da un Cell Global Identifier (CGI)
- Servita da una BTS, identificata con un Base Station Identity Code (BSIC). BSIC è irradiata dalla BTS

Aree del GSM

Location Area:

- Insieme di celle in cui un MT si muove senza cambiare le informazioni nel VLR
- Identificata da un LAI

Aree del GSM

MSC/VLR service area:

- Insieme di location area servite dallo stesso MSC e dal VLR associato al MSC

Public Land Mobile Network (PLMN):

- Una rete GSM di un gestore

GSM service area:

- Insieme di tutte le aree servite da PLMN

GSM

Numeri associati a una MS

IMSI

- Numero di identificazione di uso interno alla rete
- Composto da 3 campi

IMSI

Composto da 3 campi:

- MCC: Mobile Country Code (3 cifre)
- MNC: Mobile Network Code, che identifica l'operatore che fornisce il servizio (2 cifre)
- MSIN: Mobile Subscriber Identification Number, che identifica la SIM (fino a 10 cifre)

IMSI

- Es: 222 01 4572228769, identifica una SIM italiana (222) del gestore TIM (01)
- Il numero di telefono dell'apparato in questione è completamente scorrelato dall'IMSI

TMSI

- Numero assegnato temporaneamente dalla rete (VLR) a MS per questioni di privacy e protezione
- Strutturalmente uguale a IMSI
- È legato al LAI (alla Location Area)

TMSI

- Cambiato ad ogni uso, e ad ogni location update
- Trasmesso in chiaro dalla MS per autenticarsi, viene ri-assegnato dalla rete dopo aver instaurato un canale sicuro (crittografato) ⇒ una eventuale intercettazione è inutile

MSISDN & MSRN

- MSISDN: Mobile Station International ISDN Number…il numero di telefono che conosciamo

- MSRN: Mobile Station Roaming Number

MSISDN & MSRN

MSRN:
Mobile Station Roaming Number

- Numero usato dalla rete per l'instradamento delle chiamate
- Memorizzato presso VLR, identifica l'MSC dove si trova il mobile, quindi anche l'eventuale operatore di roaming

IMEI e IMEISV

- International Mobile Equipment Identity
- Numeri di identificazione dell'apparato
- IMEI (60 bit) identifica l'hardware

IMEI e IMEISV

IMEISV (64 bit) identifica anche eventuali diverse versioni di software/firmware

- 24 bit: TAC (Type Approval Code)
- 8 bit: FAC (Final Assembly Code) - il produttore
- 24 bit: SN (Serial Number)
- 8 bit: SVN (Software Version Number)

GSM Procedure

Esempi di procedure

Registrazione all'accensione

Roaming e location updating

- Nella stessa location area
- Nella stessa MSC/VLR service area
- Tra MSC/VLR service area diverse

Procedura di detach

Esempi di procedure

Chiamata originata da mobile

Chiamata diretta a un mobile

Esempi di procedure

Handover

- Intra-cella
- Tra BTS dello stesso BSC
- Tra BSC diverse ma stesso MSC/VLR
- Tra BSC diverse e diverso MSC/VLR

Accensione

Accensione di un terminale

Quando la MS è spenta, l'IMSI della MS è marcato come detached nell'ultimo VLR visitato

All'accensione, la MS scandisce le portanti radio alla ricerca di C0 che sente meglio (C0 non è soggetta a frequency hopping)

Accensione di un terminale

La MS si sintonizza tramite il FCCH

La MS acquisisce il sincronismo sul SCH

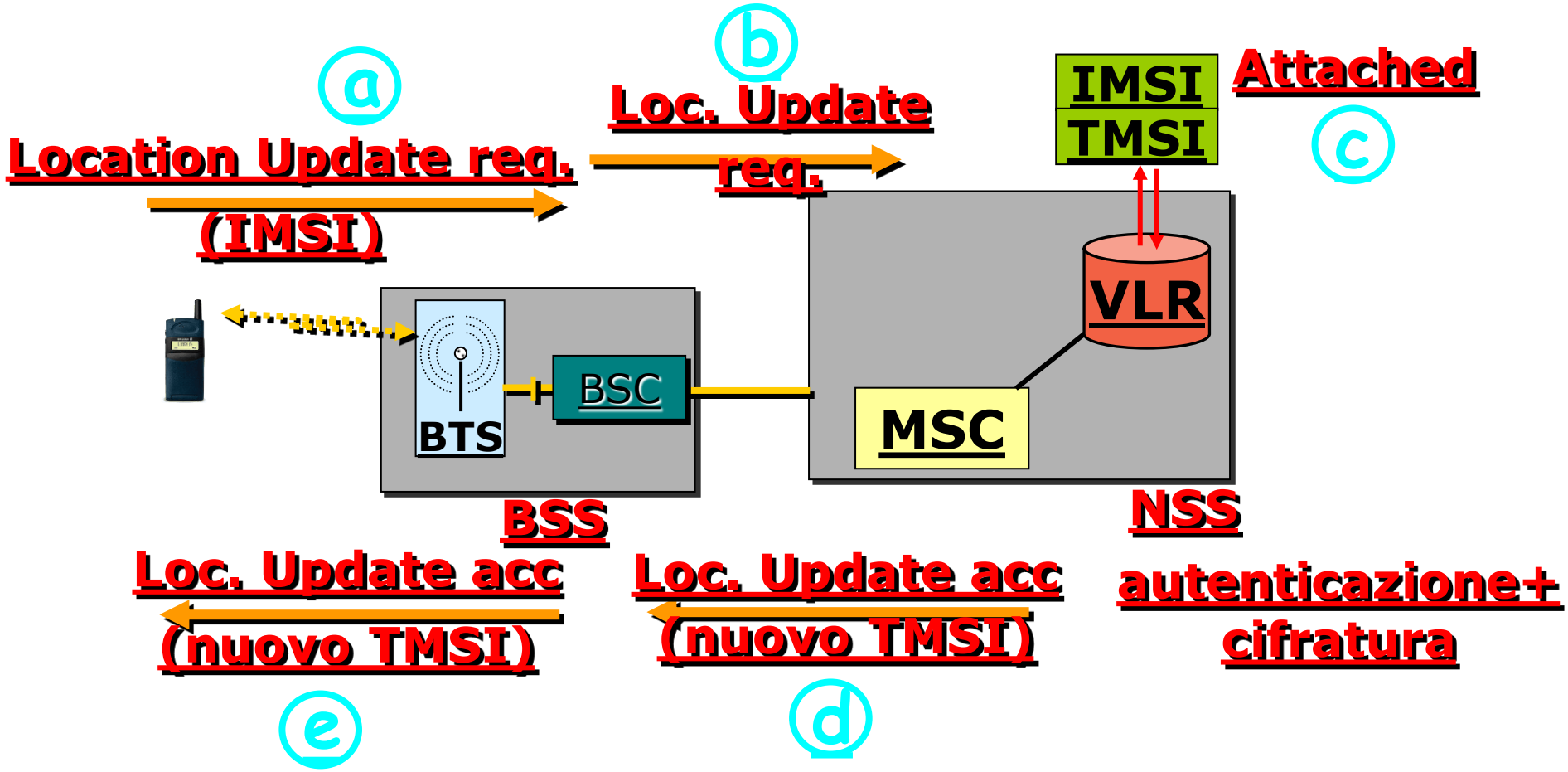
Tramite il BCCH,
la MS acquisisce informazioni sulla rete, tra cui il LAI

Accensione di un terminale

Se il LAI è diverso da quello registrato nella SIM (o se nessun LAI è memorizzato nella MS) si esegue la procedura first registration

- → **MS richiede Location Updating inviando l'IMSI**
- → **VLR contatta HLR per aggiornare il puntatore e ottenere dati sulla MS, marca l'IMSI come attached**
- → **Il VLR risponde assegnando un TMSI**

Accensione di un terminale



Accensione di un terminale

Se il LAI è uguale a quello memorizzato nella MS si esegue la procedura *IMSI attach*

- **MS richiede Location Updating inviando il TMSI**
- **Il VLR registra l'IMSI della MS come attached**
- **Il VLR risponde assegnando un nuovo TMSI**

Chiamata diretta ad una MS

Chiamata destinata a MS

- Ipotesi: Chiamata originata da rete fissa
- L'utente compone il MSISDN della MS
- Le centrali della rete fissa tramite il MSISDN instradano la chiamata verso un GMSC
- Il GMSC determina l'HLR del TM

Chiamata destinata a MS

- Il GMSC invia all'HLR un messaggio con il MSISDN
- L'HLR determina l'IMSI della MS e il VLR presso cui la MS è temporaneamente registrata
- L'HLR invia al VLR una richiesta di informazioni di roaming

Chiamata destinata a MS

- Il VLR invia all'HLR il MSRN
- L'HLR invia al GMSC il MSRN
- Il GMSC instrada la chiamata verso il MSC relativo al VLR della MS

Chiamata destinata a MS

- Il MSC, tramite l'IMSI della MS, individua la location area dove si trova la MS
- Il MSC invia un messaggio di PAGE ordinando ai BSC di mandare il paging su tutte le BTS della location area della MS

Chiamata destinata a MS

- Ogni BSC fa eseguire dalle BTS il paging sul PCH con TMSI del TM
- La MS risponde con un access burst sul RACH
- La BTS assegna alla MS un SDCCH con AGCH

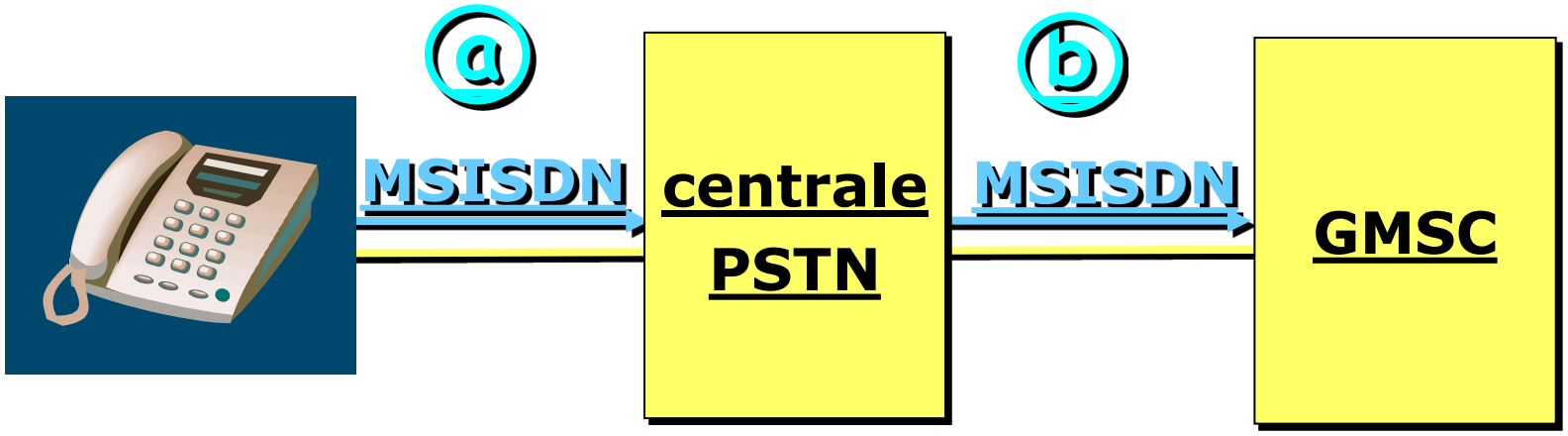
Chiamata destinata a MS

- Procedura di autenticazione
- Procedura di cifratura
- L'MSC rialloca TMSI
- L'MSC e la BTS assegnano un TCH

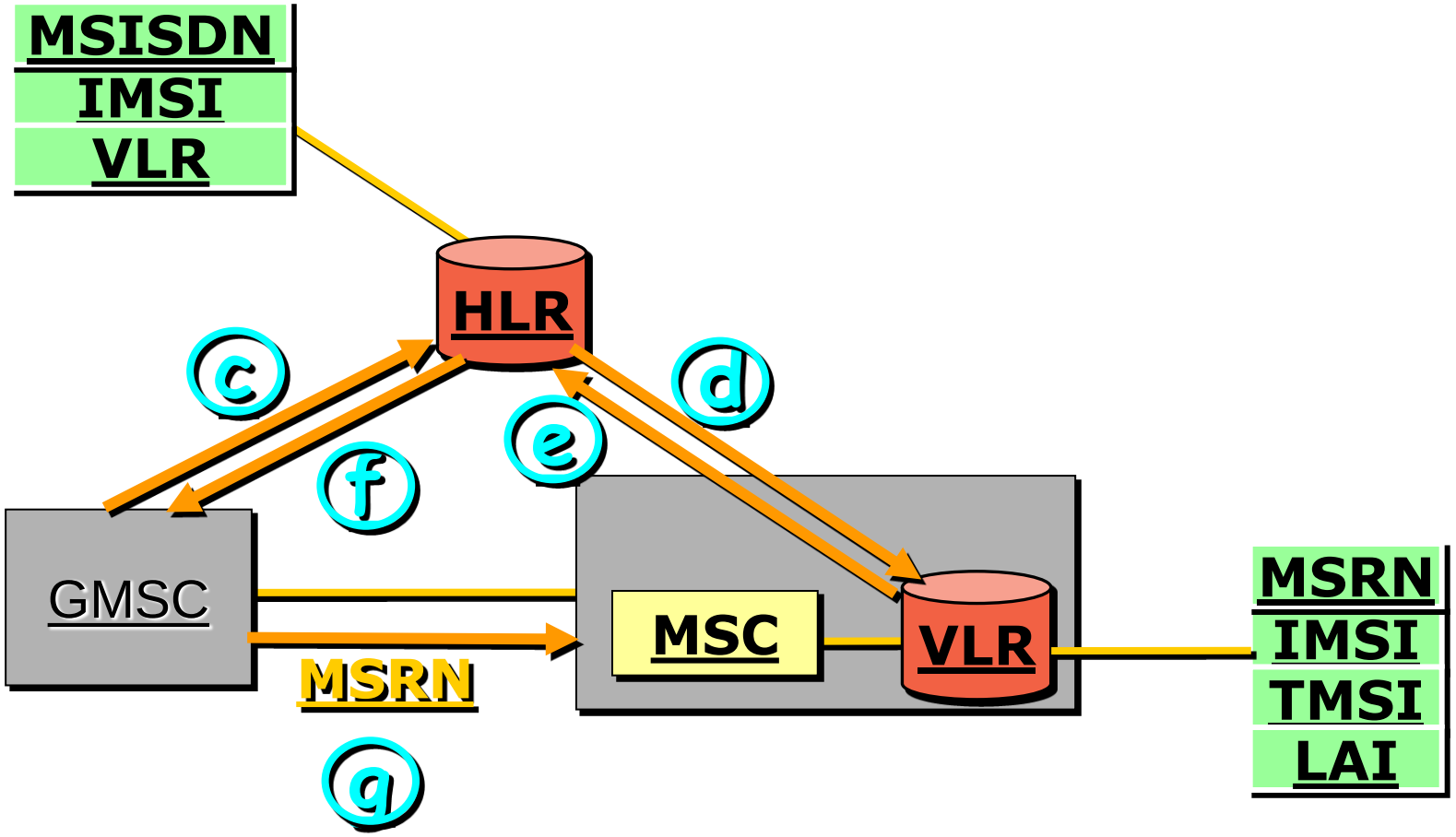
Chiamata destinata a MS

- La MS avvisa l'MSC che il chiamato sta squillando
- La MS avvisa l'MSC che il chiamato ha risposto
- L'MSC connette la chiamata sul TCH e conferma

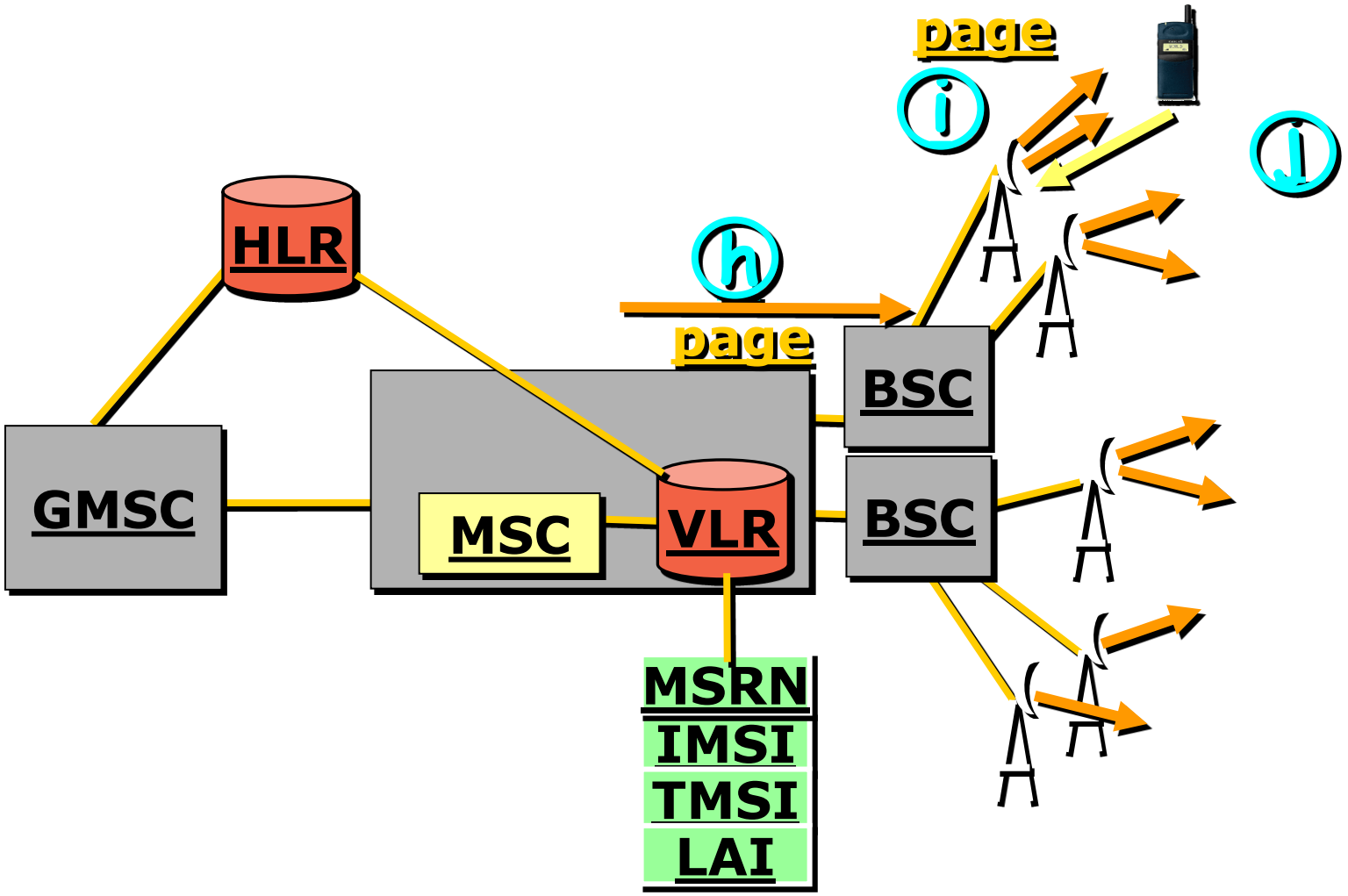
Chiamata destinata a MS



Chiamata destinata a MS



Chiamata destinata a MS



Handover

Gli handover sono decisi dalla BSC sulla base di misure effettuate da MS e BTS

Ogni MS comunica le misure con la procedura di locating

Handover - procedura di LOCATING

1

La BSC comunica alla MS (sul SACCH, se MS è in conversazione) gli identificativi delle 6 BTS su cui fare le misure relative alla C0

Handover - procedura di LOCATING

2 MS misura:

- Intensità del segnale ricevuto su C0, RXLEVNCEL
- Intensità del segnale su TCH, RXLEV
- Qualità del segnale su TCH, RXQUAL

Handover - procedura di LOCATING

La BTS misura RXLEV, RXQUAL sull'uplink, e valuta la distanza della MS

- **A intervalli regolari (p. es., 480ms) la MS comunica alla BTS le misure sul SACCH**
- **La BTS invia le misure alla BSC**

Handover - procedura di LOCATING

La BTS misura RXLEV, RXQUAL sull'uplink, e valuta la distanza della MS

➔ La BSC crea una lista ordinata di preferenza

Handover - procedura di LOCATING

La BTS misura RXLEV, RXQUAL sull'uplink, e valuta la distanza della MS

- **Quando la BSC decide l'handover, la BTS destinazione è scelta sulla base della lista. Alla BTS di provenienza è associata una penalità per evitare l'effetto ping-pong**

Handover

Motivi per effettuare un handover:

- RXLEV o RXQUAL sotto una soglia prestabilita
- Distanza della MS dalla BTS superiore a un valore massimo consentito

Handover

Tipi di handover:

- Intra-cella
- Tra BTS facenti capo allo stesso BSC
- Tra BTS appartenenti a BSC diversi facenti capo allo stesso MSC/VLR

Handover

Tipi di handover:

- Tra BTS appartenenti a BSC diversi facenti capo a MSC/VLR diversi

I tempi di un handover
devono essere molto brevi
(meno di 100 ms)

Handover tra BSC diversi, con diverso MSC

- La BSC raccoglie le misure effettuate da MS e BTS
  - Decide se cambiare BTS
  - Sceglie la BTS migliore per la MS
- La BSC contatta il MSC vecchio, che contatta il nuovo MSC

Handover tra BSC diversi, con diverso MSC

- Il nuovo MSC alloca un handover number e lo comunica al vecchio MSC che lo usa per instradare la chiamata
- Il nuovo MSC apre un circuito verso la nuova BSC e questa verso la nuova BTS e prenota un TCH

Handover tra BSC diversi, con diverso MSC

- Quando il nuovo TCH è allocato, il vecchio MSC è avvertito e la vecchia BSC ordina alla MS di sintonizzarsi sul nuovo TCH (tramite il FACCH)
- La MS cambia TCH e il vecchio MSC commuta la chiamata
- Il vecchio MSC rilascia il vecchio circuito

Handover tra BSC diversi, con diverso MSC