Codificatori vocali

Introduzione

Il segnale vocale è un'onda di pressione in aria trasformato da un microfono in un segnale elettrico analogico. Il microfono a grani di carbone, nato nel 1878 è ancora in uso. I granuli di carbone, rinchiusi in una cavità metallica e in contatto con un diaframma forniscono molti percorsi elettrici possibili. Il diaframma muovendosi per effetto della pressione dell'aria, fa muovere i granuli che vibrando fanno variare la corrente.
Il segnale vocale è un processo continuo in ampiezza e nel tempo, tramite la codifica si trasforma da segnale analogico in numerico.

Valutazione della qualità dei codificatori

Per valutare la qualità di un sistema di codifica della voce si utilizzando tecniche:

1. oggettive: es. **SNR** dove N è dato dalla differenza tra i campioni del segnale originale e il segnale codificato.
2. soggettive: es. **MOS (Mean Opinion Score)**: valutazione ottenuta in modo statistico da un campione di persone (uomini e donne) che ascoltano brevi pezzi di parlato. Esiste una scala a 5 livelli. Il GSM è considerato di qualità 'discreta', la telefonia fissa 'buona'.

Codificatori vocali

Le tecniche di codifica si dividono in:

1. **codificatori della forma d'onda**: utilizzano la sola conoscenza del segnale elettrico istantaneo (es. PCM, DPCM, ADPCM, Mod. Delta)
2. **codificatori di sorgente (vocoder)**: sfruttano soppratutto le caratteristiche dell'apparato di fonazione e uditivo (es. LPC)

In entrambe le tecniche, il primo stadio del codificatore comprende:

- filtro anti-aliasing
- campionatore
- quantizzatore

Campionamento e quantizzazione

Il campionamento e la quantizzazione sono i primi passi da effettuare per codificare qualsiasi segnale.
Il campionamento è la rappresentazione di un segnale continuo in un numero discreto di valori, senza alcun degrado se viene rispettato il teorema di Nyquist. La quantizzazione assegna ad un insieme discreto di valori dei punti campionati, si ha degrado del segnale in modo irreversibile.
Il teorema di Nyquist definisce il passo di campionamento affinchè non si abbia alcun degrado nella ricostruzione del segnale: 1/Tc >= 2B dove B è il massimo contenuto in frequenza (banda) del segnale da campionare.
La quantizzazione introduce sempre un degrado noto come *rumore di quantizzazione*. Il degrado è noto e controllabile e diminuisce con intervalli di quantizzazione più piccoli. Il degrado può essere ridotto a piacere diminuendo la dimensione dell'intervallo di quantizzazione.

PCM uniforme e non

Il PCM (Pulse Code Modulation) è un processo di campionamento e quantizzazione, la quantizzazione può essere:

- uniforme: tutti gli intervalli sono uguali. Qualità eccellente, CD, 44 kHz
- Non uniforme: intervalli diversi a seconda dell'ampiezza. Compressione prima del quantizzatore uniforme, compensata in ricezione da una espansione (compander). Qualità buona, telefonia 8 kHz.

PCM differenziale (DPCM)

Sfrutta la correlazione temporale del segnale vocale, codifica la differenza tra un campione e la stima del successivo (predizione). Se c'è correlazione tra i campioni la dinamica della differenza è minore di quella dei campioni.

Modulazione Delta
Il segnale è campionato a frequenza elevata per ottenere alta correlazione tra i campioni. La differenza è campionata su un solo bit, che indica se il segnale cresce o decresce.

PCM adattativo
Anche questa tecnica sfrutta la correlazione temporale presente nel segnale vocale. Modifica nel tempo l'ampiezza degli intervalli di quantizzazione in funzione della dinamica del segnale (adattamento). Se la variazione nel tempo del segnale è lenta (correlazione) si ottimizza l'ampiezza dell'intervallo in funzione del segnale.

PCM adattativo e differenziale (ADPCM)
Lo standard ITU G.721 usato nei telefoni cordless moderni di tipo DECT di questo tipo, ha una buona qualità e una velocità di trasmissione pari a 32 kbit/s.

Codificatori di sorgente
Il PCM e i suoi derivati codificano il segnale campione per campione. Le reti di telefonia tradizione trasmettono campione per campione. Non è possibile (o molto difficile) introdurre tecniche di correzione degli eventuali errori di trasmissione, problema significativo sui segnali radio. Le tecniche di correzione degli errori lavorano bene su blocchi di bit. Inoltre, in reti a commutazione di pacchetto bisogna accumulare campioni fino a riempire un pacchetto prima di iniziare la trasmissione. Considerando un segmento vocale è possibile usare algoritmi di codifica e compressione molto efficienti. Si parte da una codifica PCM uniforme eccellente, si raggruppano da 80 a 320 campioni e si lavora sull'insieme detto blocco.
I codificatori di sorgente si dividono in molte categorie a seconda degli algoritmi usati. Tutti i codificatori a blocco sono basati su filtri numerici a risposta finita (FIR) di cui il codificatore calcola i parametri. I parametri vengono trasmessi per la ricostruzione del segnale al ricevitore.

Modellizzazione fisica
Il filtro utilizzato rappresenta i modi vibrazionali delle corde vocali e le cavità risonanti dell'apparato di fonazione umano.

Soppressione dei silenzi
Con i codificatori a blocco è possibile effettuare la sovrapposizione dei silenzi (VAD – Voice Activity Detection). Se non vi è attività vocale non vengono generati “pacchetti” di descrizione vocale. Sul canale vengono trasmessi pacchetti di descrizione del silenzio risparmiando così banda e riducendo l'interferenza.
I silenzi vanno soppressi senza dare la sensazione di “linea caduta”. Il soppressore deve essere efficiente nell'intervenire, ma soprattutto nel riprendere la codifica, per evitare di “tagliare” l'inizio di nuove lettere/parole.
I soppressori possono essere:
- lenti: intervengono solo durante lunghe pause di parlato
- veloci: cercano di intervenire anche nei brevissimi silenzi tra prole della stessa frase

Codifica LPC-LTP
La codifica Linear Prediction Coding – Long Term Prediction si basa sulla modellizzazione fisica del tratto vocale mediante due filtri, uno a memoria breve (filtro LPC) e uno a memoria lunga (LTP)

Codifica LPC-LTP con RPE
Il segnale viene rigenerato eccitando il filtro a memoria breve con rumore gaussiano bianco e il filtro a memoria lunga con un treno di impulsi regolari (RPE – Regular Pulse Excitetion). La codifica è divisa in:
- Predizione di breve periodo (LPC): serve a codificare “bene” i fonemi con consonanti
- Predizione di lungo periodo (LTP): serve a codificare “bene” i suoni vocalizzati
- Calcolo del miglior segnale di eccitazione (RPE)

Codifica CELP (Code Excited Linear Prediction)
E' un codificatore LPC in cui l'eccitazione per ricostruire il segnale non è rumore bianco ma una sequenza di un "codebook" (catalogo) che minimizza l'errore rispetto al segnale originale.
Il codificatore è molto complesso perchè deve scegliere tra i possibili codici in modo esaustivo.

Codificatori GSM
GMS tradizionale:
- Codificatore LPC-LTP con RPE a 13 kbit/s

GSM Enhanced Full Rate (EFR):
- Telefonini dual-band e/o posteriori al 1997 con CELP a 12.2 kbit/s

Codificatori UMTS
- Codec adattativo a rate variabile (AMR – Adaptive Multi Rate), può essre usato anche con GSM

Codificatore GSM base
- Codificatore LPC-LTP con RPE
- Blocchi da 20 ms che producono 260 bit raggruppati in 3 livelli di importanza:
  - 50 ricevono massima protezione
  - 132 ricevono una protezione media
  - 78 non sono protetti
- Totale 13 kbit/s

Reti Cellulari – Principi generali
Definizioni
Rete Wireless: (sotto)rete in cui l'accesso da un terminale avviene attraverso un canale radio, "senza filo"
Rete Cellulare: rete in cui la copertura geografica è ottenuta con una tassellatura di aree adiacenti dette celle. L'utente si può muovere attraverso la rete passando da una cella all'altra senza interrompere la comunicazione

Copertura cellulare teorica
- Stazione base a centro cella con antenna isotropica
- Celle: aree esagonali regolari
- 3 antenne direzionali a 120° ad un'estremità delle celle
- 3 antenne nello stesso sito

Copertura cellulare reale
- Le celle non sono regolari e delle stesse dimensioni
- La forma e le dimensioni delle celle sono determinate da:
  - potenza delle antenne
  - guadagno di antenna
  - morfologia del territorio
  - condizioni di propagazione

Per i modelli di propagazione occorre distinguere tra macrocelle e microcelle. Per una copertura macrocellulare le caratteristiche del territorio sono normalmente rilevate da satellite: estensione aree urbane, porzioni seminative, aree di bosco fitto, aree montane.

Tecniche di accesso multiplo
Nell'accesso multiplo i canali radio sono risorse comuni a molti utenti, le tecniche principali sono:

- FDMA (Frequency Division Multiple Access)
- TDMA (Time Division Multiple Access)
- CDMA (Code Division Multiple Access)
- SDMA (Space Division Multiple Access)

FDMA: riutilizzo delle frequenze

Con un limitato numero di risorse radio si vuole assicurare la massima copertura del territorio e servire un elevato numero di utenti, questo impone di utilizzare le stesse frequenze in punti geografici diversi.
La procedura pratica per ottenere il riutilizzo delle frequenze è:

- definire la larghezza di banda di un canale (25 kHz per TACS e 200 kHz per GSM)
- dividere lo spettro a disposizione S in N canali di quella larghezza di banda e definire le frequenze associate (dette portanti)
- partizionare 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
- il fattore di riuso è 1/G

Dimensione del cluster

La dimensione del cluster è $G = i^2 + j^2 + ij$ con i e j interi

Capacità della rete cellulare

M: numero di volte necessario a ripetere il cluster per coprire l'intera area
Capacità = M G k (S/N) = M S

Considerazioni

A pari G:

- Minore R, maggiore M, maggiore capacità
- Minore R, maggiore numero di antenne per avere la stessa copertura

Parametri D e R

R = raggio cella, D = distanza tra celle che utilizzano lo stesso canale
Per celle con stessa dimensione e stazioni base con la stessa potenza, l'interferenza co-canale diventa funzione solo di R e D.

Riutilizzo delle frequenze

SIR = Interferenza co-canale valutato con C/I, si ha che:

- Maggiore è la distanza D tra i trasmettitori e minore è l'interferenza
- Maggiore è il raggio R di una cella, maggiore è la potenza usata e quindi l'interferenza
- è fondamentale Q = D/R
- considerando che celle co-canale si trovano in linea retta e poi ad angolo di 60° vale la relazione $Q = \sqrt{3G}$
- più grande è G, maggiore è Q, maggiore C/I, migliore la qualità del servizio fornito all'utente

Dimensioni dei cluster

A pari R:

- minore G, maggiore numero di canali per cella k e maggiore M -> maggiore capacità
- maggiore G, maggiore D, minore interferenza, migliore qualità

Riutilizzo delle frequenze e criteri di progetto

- maggiore D/R, maggiore C/I, migliore la qualità del servizio fornito all'utente
- minore D/R, minore G, meno celle nel cluster. A pari numero di canali N, più canali nella cella e maggiore M -> maggiore la capacità del sistema
- Alcune tecniche permettono di aumentare la capacità di traffico e diminuire l'interferenza:
  - Splitting
  - Sectoring
  - Tilting

Splitting
Consente di suddividere celle di dimensioni grandi in celle più piccole. Coesistono:
- microcelle: celle di dimensioni piccole in zone ad alta densità di traffico
- macrocelle: celle di dimensioni grandi in zone a bassa densità di traffico
- ciascuna cella grande può essere sostituita con un certo numero di celle piccole

Sectoring
- la cella è divisa in settori che utilizzano frequenze diverse con antenne direttive (60° o 120°)
- le antenne direttive riducono l'interferenza
- creazione di nuove celle senza aumentare i costi dei siti radio
- configurazione tipica è la tri-cellulare con 3 settori per cella e antenne direttive separate di 120°

Tilting
- le antenne direttive causano interferenza sostanzialmente solo lungo la direzione privilegiata
- l'interferenza in questa direzione può essere elevata
- le antenne vengono inclinate verso il basso di qualche grado (tilt)

Dimensione tipica dei cluster
Per i sistemi analogici, per es. TACS, si hanno cluster da 19 o 21 celle. Per sistemi numerici con accesso tipo TDMA o FDMA/TDMA come il GSM si hanno cluster da 7 o 9 celle. Per i sistemi numerici ad accesso CDMA si hanno cluster di una cella.

Tecniche di copertura cellulare
Per la copertura cellulare è possibile utilizzare antenne direzionali per avere celle di forma e dimensione particolare, celle stratificate (a ombrello). Sono allo studio tecniche per ottenere celle puntiformi che inseguono il terminale mobile. Queste tecniche sono utili per adattare la dimensione delle celle in base all'intensità di traffico presente nelle diverse aree.

Controllo di potenza
E' necessario per ridurre l'interferenza ed il consumo energetico, effettuato con un controllo ad anello aperto / chiuso.

Pianificazione della copertura
Si posso utilizzare tecniche di allocazione statica (Fixed Channel Allocation FCA) e dinamica (Dynamic Channel Allocation DCA) dei canali.
FCA:
- basata sul concetto di cluster
- le frequenze sono associate in modo statico
- il piano frequenziale è cambiato solo di tanto in tanto per migliorare le prestazioni di rete o per seguire le variazioni lente del numero di utenti

DCA:
- risorse assegnate alle celle da un controllore centrale, quando servono
- il controllore tiene in conto i livelli di interferenza nel gruppo di celle controllato
- l'allocazione cambia nel tempo in base al numero di connessioni attive e al livello di interferenza
- il piano frequenziale evolve nel tempo adattandosi allo stato del sistema

Si possono anche avere degli schemi ibridi (Hybrid Channel Allocation HCA) dove una porzione dei canali è allocata in modo statico e l'altra in modo dinamico.

Gestione della mobilità
Il supporto dell'elevata mobilità è di fatto l'elemento distintivo tra le reti cellulari ed ogni altro tipo di rete di telecomunicazione. Per questo servizio sono necessarie le procedure di *Roaming*, *Location Updating*, *Paging* e *Handover*.

Roaming
E' la possibilità data all'utente di essere rintracciabile anche se si sposta all'interno della rete. Il sistema deve memorizzare in una base 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. Ogni LA ha un identificativo detto LAI (Location Area Identifier)

Location Updating
E' 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 dati).

Paging
E' 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
E' 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. E' 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. Gli handover possono essere classificati in tre categorie:
- 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 (Base Station) di origine (backward) oppure tramite la BS di destinazione (forward)
- 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)

E' necessario stabilire chi e come effettua le misure necessarie per stabilire il momento opportuno per effettuare un handover.

La registrazione
E' la funzione di collegamento del terminale alla rete e di identificazione, autenticazione. Questa è la procedura da eseguire all'accensione del terminale, tutte le volte che si desidera accedere ad un nuovo servizio, associare il terminale alla rete.

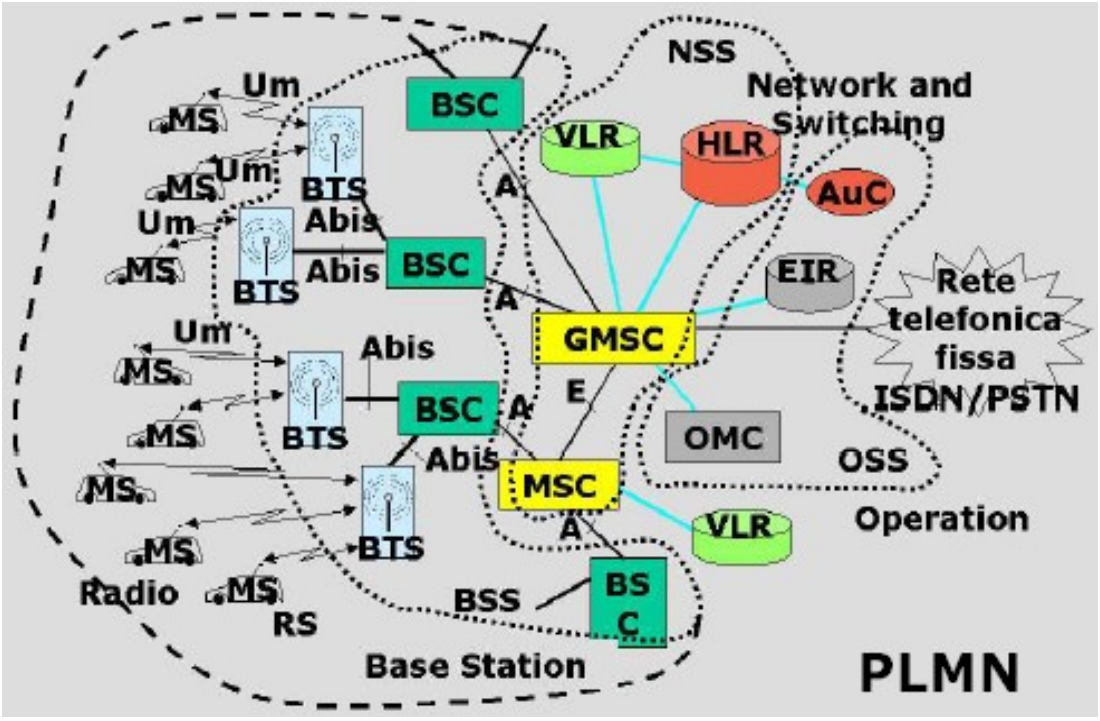
Reti Cellulari – GSM I
Breve storia
1982 – La CEPT istituisce un gruppo speciale per occuparsi della rete cellulare pan-europea
1992 – Rilasciato lo standard definitivo di GSM che diventa acronimo di Global System for Mobile-communications
1994-95 – Introduzione degli SMS
1995-97 – Servizi dual-band
1999 – Standard GPRS per la trasmissione a pacchetto, primi terminali WAP
2000-01 – Servizi GPRS

Servizi attualmente offerti dal GSM
Servizi di trasporto
- Trasmissione dati (non strutturata) sincrona e asincrona tra 300 bit/s e 9.6 kbit/s
- Accesso PAD (Packet Assembly/Disassembly) asincrono tra 300 bit/s e 9.6 kbit/s
- Trasmissione dati a pacchetto sincrona con velocità compresa fra 2.4 e 9.6 kbit/s
- Trasmissione dati con affasciamento di canali HSCSD fino a 76.8 kbit/s

Teleservizi
- Telefonia sia full rate (13 kbit/s, 12.6 Enhanced coder) sia half rate (6.5 kbit/s)
- Telefax di gruppo 3
- Messaggeria sia unicast che multicast
- Messaggi brevi SMS

Servizi supplementari
- Tutti i servizi della rete PSTN (inoltro di chiamata, richiamata su occupato, gruppi di utenti chiusi ...)

Architettura del GSM



Terminale mobile
E' il terminale di proprietà dell'utente, ne esistono di molti tipi diversi, a seconda delle applicazioni e dei luoghi di installazione. Vi sono tre categorie a seconda della potenza nominale:
- veicolari, possono emettere fino a 20W
- portatili, possono emettere fino a 8W
- personal, il classico telefonino che può emettere fino a 2W

Può essere dual band (900 Mhz, 1800 Mhz) o tri band (900 Mhz, 1800 Mhz, 1900 Mhz). Il terminale mobile è solo hardware, per poter funzionare necessita di una scheda di abilitazione che offre il servizio (SIM)

Modulo di identificazione Utente (Subscriber Identity Module – SIM)
E' una scheda che contiene processore e memoria di tipo smart card che rende operativo qualunque MS. Vi sono due formati, contiene le caratteristiche dell'utente, come il numero telefonico, i servizi accessibili, i parametri per la sicurezza. Queste informazioni sono memorizzate in modo permanente e crittografato nella SIM, che rappresenta il servizio offerto dai gestori.

Reti Cellulari – GSM II

Architettura del GSM

Stazione Radio Base (Base Station BS)
- Base Tranceiver Station BTS è l'interfaccia fisica che si occupa della rice-trasmissione
- Base Station Controller BSC svolge il controllo delle risorse sull'interfaccia radio

Base Tranceiver Station BTS

E' il punto di accesso alla rete di TLC, ovvero la controparte di MT. E' collocata in un punto opportuno della cella. Dalla potenza della BTS dipende la dimensione fisica della cella: grazie a questa caratteristica è possibile modificare in modo dinamico le dimensioni della cella. Ciascuna BTS può avere da 1 a 16 interfacce radio, corrispondenti a diversi canali in FDM. Ciascuna interfaccia radio corrisponde a 8 canali TDM.

Operazioni svolte:

- Codifica di canale e cifratura
- Modula e demodula i segnali
- Realizza il frequency hopping
- Effettua l'interleaving
- Effettua misura di qualità dei canali uplink e riceve da MT le misure relative al downlink, le invia alla BSC che decide il controllo di potenza e l'handover

Caratteristiche:

- Implementa i protocolli di livello fisico sull'interfaccia radio (Um) per il corretto scambio di informazioni tra MT e BTS
- E' un apparato di livello fisico e non ha “intelligenza”: nel GSM anche la valutazione e la decisione sugli handover da effettuare è demandata ad altre entità (MT, BSC, MSC)

Base Station Controller BSC

Un BSC controlla un numero elevato di BTS: da alcune decine ad alcune centinaia. BTS e BSC sono collegate da links a 2 Mb/s (32 canali PCM a 64 kb/s). Un canale PCM del collegamento viene utilizzato 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. La transcodifica della voce GSM a PCM e viceversa è fatta dalla BSC TRAU (Transcoder Rate Adaptation Unit).

I compiti principali della BSC sono:

- transcodifica della voce GSM <-> PCM
- analisi delle misure di qualità del segnale sulla tratta radio
- decisione se è il caso di effettuare handover
- gestione dell'hardware tra BTS controllate dallo stesso BSC o richiesta di gestione all'MSC
- controllo delle risorse radio: gestione delle frequenze, che possono essere assegnate in modo dinamico alle varie BTS
- gestione del paging
- manutenzione del BSS
- concentrazione del traffico verso MSC e lo smistamento del traffico verso le BTS

I BSC possono essere collocati nel sito di un MSC o essere autonomi, o ancora essere posizionati vicino o insieme ad alcune BTS. Normalmente vengono collocati con MSC per questioni di controllo e manutenzione.

Network and Switching Sub-system NSS

Noto anche come Switching and Management Sub-system SMSS, svolge funzioni fondamentali come la gestione della mobilità, il controllo delle chiamate ed il supporto ai servizi forniti.

E' composto da:

- Mobile Switching Center (MSC): è la centrale di commutazione che gestisce i servizi mobili
- Home Location Register (HLR): è il data base con:
  - i dati permanenti degli utenti
  - i dati dinamici per gestire la mobilità (es. identificativo del VLR)
- Visitor Locator Register (VLR): è il data base con: le informazioni relative agli MT attualmente presso l'area di competenza del MSC
- Equipment Identify Register (EIR): è il data base degli apparati rubati o difettosi
- Authentication Center (AuC): genere chiavi di cifratura

Mobile Switching Center MSC – centro di commutazione di servizi mobili
E' un commutatore PCM (commutatore a circuito) a cui sono state aggiunte le funzionalità di segnalazione per la gestione della mobilità. Le funzioni fondamentali sono:
- gestione della mobilità: location update, paging, ecc.
- controllo delle chiamate: con autenticazione
- supporto ai servizi
- alloca risorse e crea connessioni con i TM sulla rete fissa: connection management CM
- consente l'instradamento delle chiamate da un TM ad un altro

Gateway Mobile Switching Center GMSC
E' un caso particolare di MSC, che rappresenta l'interfaccia tra la rete GSM e le reti fisse (PSTN) e/o altre reti GSM (PLMN). Le sue funzioni fondamentali sono:
- internetworking con altre reti
- funzioni di gateway
- consente l'instradamento delle chiamate da un TM verso telefoni fissi e mobili in altre reti
- è il punto di partenza per la ricerca dei TM nella rete cellulare per chiamate provenienti da altre reti (fisse o mobili)

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

Home Location Register HLR – registro di localizzazione principale
E' 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 i TM. Spesso è collocato con un GSMC. Memorizza le informazioni (profilo di utente) relative a tutti i TM la cui localizzazione di default è presso l'HLR considerato. L'HLR memorizza informazioni permanenti come l'IMSI (International Mobile Subscriber Identity), il numero di telefono della SIM associata, i servizi supplementari a cui l'utente è abilitato. Le informazioni volatili memorizzate sono:
- l'indirizzo del VLR presso cui può essere reperito l'utente
- parametri temporanei per identificazione e crittografia
- eventuale numero di telefono per l'inoltro delle chiamate
- ...

Visitor Locator Register VLR – registro di localizzazione dei visitatori
E' una base dati temporanea associata a tutti gli MSC, anche GMSC (spesso MSC e VLR sono integrati). Contiene i dati essenziali per il servizio dei TM attualmente sotto la giurisdizione del (G)MSC a cui il VLR è associato. Per questione di uniformità si utilizza il VLR anche per i terminali mobili che si trovano presso il proprio MSC: l'informazione memorizzata nell'HLR viene “duplicata localmente”. Nel VLR vengono duplicati molti dei dati di un utente già presenti nell'HLR, compresi i dati usati per identificare e autenticare un utente. Il VLR crea il TMSI (Temporary Mobile Subscriber Identity) che è utilizzato al posto dell'IMSI per non trasmetterlo regolarmente via radio e lo memorizza. Il VLR invia il TMSI in modo cifrato al TM che lo memorizza nella SIM. Il TMSI viene modificato di frequente ed è legato anche alla posizione del mobile (LAI). Il VLR memorizza anche il LAI e le informazioni che servono per l'instradamento delle chiamate verso il TM (MSRN). Infine, nel VLR viene mantenuto lo stato del TM: acceso (attached) o spento (detached).

Authentication Center AuC – centro di autenticazione
E' associato a ciascun HLR ed è il “motore” per l'autenticazione delle SIM. E' in grado di effettuare correttamente le stesse operazioni di codifica che sono associate a ciascuno SIM. Inoltre gestisce alcune importanti operazioni per abilitare la cifratura della trasmissione sull'interfaccia radio.

Operation and Maintenance Center OMC – centro gestione e controllo
E' la sede in cui vendono eseguite tutte le operazioni di gstione (tecnica e non) della rete. Effettua la tariffazione, controlla il traffico in rete, gestisce i messaggi d'errore provenienti dalla rete, controlla e memorizza il carico delle singole BTS e BSC per operazioni di pianificazione (eventualmente dinamica). Consente di configurare le singole BTS tramite le BSC e di controllare il funzionamento di

tutte le apparecchiature periferiche della rete.

IMSI (International Mobile Subscriber Identity)
E' il numero di identificazione di uso interno alla rete, è composto da 3 campi:
- MMC: 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)

Il numero di telefono è assolutamente scorrelato dall'IMSI.

TMSI (Temporary Mobile Subscriber Identity)
E' il numero assegnato temporaneamente dalla rete (VLR) all'MT per questioni di privacy e protezione. E' strutturalmente uguale all'IMSI ed è legato al LAI. E' cambiato ad ogni uso, e ad ogni location update. E' trasmesso in chiaro dall'MT per autenticarsi, viene ri-assegnato dalla rete dopo aver instaurato un canale sicuro (crittografato), eventuali intercettazioni sono inutili.

MSISDN & MSRN
MSISDN (Mobile Station International ISDN Number) è il numero di telefono, MSRN (Mobile Station Roaming Number):
- è il numero usato dalla rete per l'instradamento delle chiamate
- è memorizzato presso il VLR, identifica l'MSC dove si trova il mobile, quindi anche l'eventuale operatore di roaming

IMEI e IMEISV
E' l'International Mobile Equipment Identity, ovvero è il numero di identificazione dell'apparato, identifica l'hardware, è a 60 bit. L'IMEISV identifica l'apparato ed in più può identificare eventuali versioni di software/firware, è a 64 bit. Vi sono:
- 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) in IMEISV
- 4 bit: non usati in IMEI

Reti Cellulari – GSM III
Equipment Identity Register EIR – registro di identificazione degli apparati
E' una base dati il cui uso è a discrezione dell'operatore. Contiene l'identificativo e le caratteristiche di tutti gli apparati GSM (MS – l'hardware) prodotti, insieme al produttore, al paese di fabbricazione. Può essere usato per proteggere la rete dall'uso di apparecchiature non a norma, rubate, esportate illegalmente. L'EIR contiene tre elenchi:
- white list: identifica tutti i terminali operativi
- grey list: identifica i terminali difettosi o non omologati
- black list: identifica apparati rubati o non autorizzati

Authentication Center AuC – centro di autenticazione
E' 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: protegge da tentativi di utilizzo fraudolento della rete da parte di persone non autorizzate
- cifratura: protegge da tentativi di accesso non autorizzato ai dati da parte di utenti regolari

L'autenticazione
1. La rete invia al TM un numero casuale (RAND) generato da AuC
2. MS calcola la risposta (SRES) in base a un algoritmo prefissato (algoritmo A3) usando RAND e Ki, una chiave memorizzata sia nella SIM che in AuC
3. TM spedisce SRES alla rete
4. La rete confronta SRES con il risultato del calcolo svolto da AuC (usando RAND e Ki)
5. Se i risultati coincidono è concesso l'accesso

Durante l'autenticazione viene anche generata la chiave di cifratura Kc usata poi per la trasmissione sulla tratta radio. Gli elementi in gioco durante l'autenticazione sono:
- TMSI
- IMSI
- A3: algoritmo di autenticazione
- Ki: chiave di autenticazione

La cifratura
L'obiettivo della crifratura è la riservatezza, ovvero la protezione contro le intercettazioni. L'algoritmo di cifratura (A5) è contenuto nei TM e nelle BTS e utilizza la chiave Kc. La chiave Kc è generata da un algoritmo prefissato (A8) sia da TM che da AuC in fase di autenticazione, utilizzando RAND e Ki. Gli elementi che sono utilizzati durante la cifratura sono:
- TMSI
- IMSI
- A8: algoritmo per determinazione Kc
- A5: algoritmo di cifratura
- Kc: chiave di cifratura

Operation and Maintenance Sub-system OMSS
E' la sede di tutte le operazioni di gestione della rete. Si occupa della gestione dei guasti, della gestione della manutenzione, della configurazione degli elementi di rete (configura singole BTS tramite BSC), controllo delle prestazioni degli elementi di rete. Inoltre gestisce la sicurezza del sistema, raccoglie dati per la tariffazione, gestisce la ripartizione della tariffazione tra gestori diversi per chiamate inter-gestore.

Aree del GSM
Cella
E' identificata da un Cell Global Identifier (CGI), è servita da una BTS, identificata con un Base Station Identify Code (BSIC). La BSIC è irradiata dalla BTS

Location Area
E' un insieme di celle in cui un MT si muove senza cambiare le informazioni nel VLR, è identificata da un LAI.

MSC/VLR service area
E' l'insieme di location area servite dallo stesso MSC e dal VLR associato all'MSC

Public Land Mobile Network PLMN
E' la rete GSM di un gestore

GSM service area
E' l'insieme di tutte le aree servite da PLMN

Pila protocollare

BSSMAP (BSS Mng Application Part): Layer 3 all'interfaccia A, per segnalazione tra BSC e MSC riguardante controllo di chiamate e gestione risorse.
BTSM (BTS Mng): Layer 3 all'interfaccia Abis, per segnalazione tra BSC e BTS riguardante controllo risorse radio.
CM (Connection Mng) e MM (Mobility Mng): segnalazione tra TM e MSC.
I messaggi di segnalazione del BTSM tra BTS e BSC sono trasportati col protocollo di livello 2 LAPD (Link Access Protocol – D channel).
I messaggi di segnalazione tra BTS e TM sono trasportati col protocollo di livello 2 detto LAPDm (derivato da LAPD).
SCCP (Signaling Connection Control Part) e MTP (Message Transfer Part): sono parte del canale di segnalazione SS7, servono a trasportare i messaggi di segnalazione del BSSMAP.

Reti Cellulari – GSM IV

Livello fisico dell'interfaccia radio

In USA si usando bande intorno a 1900 Mhz anziché intorno a 1800 Mhz, per ovviare esistono anche terminali tri-band. In Italia, le frequenze in uso per il TACS erano nella banda del GSM a livello internazionale, creando quindi situazioni di conflitto.

Frequenze assegnate al GSM i Europa
A 900 Mhz dispone di 124 (125-1) canali FDM nella parte primaria dello spettro più 50 canali nella parte estesa. A 1800 Mhz dispone di 374 (375-1) canali FDM. Il canale all'estremo inferiore non è mai usato. Se possibile sia a 900 che a 1800 Mhz i canali estremi superiori sono utilizzati come “guardia”. Esiste un sistema di numerazione assoluto dei canali detto ARFCN (Absolute Radio Frequency Channel Number), che consente di identificare in modo univoco il canale da usare (o in uso) indipendentemente dal fatto ce sia GSM/900 o DCS/1800. I canali GSM-900 hanno ARFCN da 0 a 124 per la parte primaria e da 974 a 1023 per la parte estesa. I canali uplink e downlink sono sempre accoppiati in modo fisso e distano di 45 Mhz a 900 e di 95 Mhz a 1800.

Dati generali
E' importante definire degli elementi generali per l'interoperabilità dei terminali:
- definizione di interfacce standard tra elementi della rete
- distanza tra portanti di 200 kHz
- codifica a 13 kb/s in full rate e 6.5 kb/s in half rate
- modulazione GMSK (Gaussian Minimum Shift Keying)
- uso di controllo di potenza
- uso dell'interleaving

Tecniche di accesso e struttura dei canali
Il GSM utilizza una tecnica di accesso mista a divisone di tempo e frequenza FDMA/TDMA. La porzione di spettro disponibile è suddivisa in canali FDM di 200 kHz l'uno. Ciascun canale FDM è ulteriormente diviso in 8 canali TDM (slot, durata 4.615 ms, 1 slot 156.25 bit). La trasmissione è organizzata in “burst”: ogni TM trasmette un blocco di dati in un intervallo temporale (1 canale TDM) e “tace” durante gli altri 7 intervalli dedicati agli altri canali. La velocità di cifra al trasmettitore è di crica 271 kbit/s. Più precisamente si ha:
- frequenza + time slot = canale fisico
- ciascun time slot porta un burst di trasmissione

Struttura della trama GSM
La trasmissione bidirezionale in GSM è ottenuta mediante separazione sia in frequenza che in tempo, in questo modo serve una sola interfaccia radio. Le trame sui canali uplink e downlink sono sincronizzate (su base slot) e sfasate di 3 slot, in modo da consentire la separazione tra trasmissione e

ricezione.

Avanzamento temporale (timing advance)
I terminali a distanza diversa dalla BTS subiscono ritardi di propagazione diversi, il non perfetto sincronismo tra TM produce interferenza tra time-slot vicini. La BTS ordina al terminale di anticipare la trasmissione di una quantità di tempo che compensa il ritardo di propagazione, in questo modo si riduce l'interferenza.

Tecnica di Accesso e Struttura dei Canali
Per risparmiare le batterie e ridurre l'interferenza il trasmettitore RF viene spento quando non trasmette e anche quando non vi è informazione da trasmettere (soppressione dei silenzi). Questa tecnica di spegnimento ed accensione del trasmettitore RF pongono notevoli problemi di "ramping", cioè di transitorio per portare l'amplificatore a regime prima di cominciare la modulazione dei dati.

Ramp-up e inviluppo
Gli amplificatori hanno dei tempi non nulli di accesione e spegnimento (ramp-up/down). La trasmissione deve avvenire a inviluppo costante e senza interferenza con lo slot precedente o successivo, quindi è opportuno che nei time-slot si debbano prevedere tempi di "guardia". Più in particolare, servono dei periodi di guardia prima e dopo la trasmissione dell'informazione utile, e bisogna considerare che in questi periodi i segnali possono sovrapporsi.

Frequency hopping
In GSM è previsto di poter trasmettere messaggi consecutivi della stessa comunicazione su frequenze diverse. Il FH serve a ridurre gli effetti del fading da percorsi multipli: si guadagnano circa 2 dB. Il FH usato in GSM è lento perchè il cambio di frequenza avviene con cadenza di trama (8 slot=4.615 ms) e non di pochi bit come in altri sistemi. Il TM deve essere in grado di re-sintonizzare Tx e Rx in circa 1ms.

Modalità di utilizzo del Frequncy Hopping
L'utilizzo o meno del FM è una scelta dell'operatore, tuttavia è implementato in tutti i TM, in quando se la rete indica di entrare in questa modalità, il TM deve eseguire la procedura. Le sequenze di hopping sono calcolate da BTS e TM in base ad algoritmi di generazione di sequenze pseudo-casuali, in alternativa si può eseguire un più semplice hopping ciclico. Le modalità ed i parametri per il calcolo della sequenza di hopping sono decise da BTS e trasmesse al TM.

Parametri dell'algoritmo di Frequency Hopping
MA (Mobile Allocation): vettore delle frequenze disponibili
MAIO (MA Index Offset): valore di sfasamento del salto di frequenza
HSN (Hopping Sequence generator Number): seme della sequenza pseudocasuale che pilota l'algoritmo
FN (Frame Number): numero assoluto della trama GSM
RNTABLE: vettore di 128 (0-127) numeri disposti in modo pseudocasuale

Burst

Esistono 5 tipi di burst:
- Normali: per la trasmissione di messaggi sia sui canali di traffico che su quelli di controllo
- Accesso: usati nelle fasi di setup quando TM non è ancora sincronizzato con BTS (solo uplink)
- Sincronizzazione: inviati da BTS per la sincronizzazione dei TM (solo downlink)
- Correzione della frequenza: inviati periodicamente da BTS per consentire la correzione degli oscillatori dei TM (solo downlink)
- Dummy: inviati sugli slot vuoti se è necessario tenere alta la potenza della portante (usati solo dalla BTS)

Struttura dei burst normali
- Coded Data: bit di utente (voce, dati ecc.), 114 bit dopo la codifica di canale, che corrispondono a 13 kbit/s netti per la voce, a 9.6 kbit/s o meno per i dati (codifica di canale più ridondante)
- Training Sequence: bit di controllo usati per la sincronizzazione e per l'equalizzazione
- T-bits: posti sempre a 0, usati come tempi di guardia e per l'inizializzazione del demodulatore
- S-bits: indicano se il burst contiene dai utente o di segnalazione (bit di stealing)
- GP: Periodo di guardia per consentire l'accensione e lo spegnimento dei trasmettitori

Struttura dei burst di accesso
- T-bits: posti sempre a 0, usati come tempi di guardia e per l'inizializzazione del demodulatore, notare la sequenza estesa a 8 bit all'inizio del burst
- Synch-bits: sequenza nota, consente l'aggancio del ricevitore alla BTS
- Coded Data: bit di utente (dati)
- Extended GP: periodo di guardia allungato per garantire che il burst, trasmesso come se ci si trovasse alla massima distanza da BTS, non “sbordi” sullo slot successivo

La dimensione massima delle celle deve essere tale per cui il burst di accesso giunge alla BTS senza pericolo di sovrapposizione con lo slot successivo. In mancanza di altre informazioni TM si comporta come se il ritardo di propagazione tra TM e BTS fosse il massimo ammesso trasmettendo per un periodo ridotto. Con un po' di approssimazione: Rmax = (C GP)/2 = 37.5 Km. In realtà per convenienza si utilizza 35 Km.

Struttura dei burst di sincronizzazione
- T-bits: posti sempre a 0, usati come tempi di guardia e per l'inizializzazione del demodulatore
- Extended training sequence-bits: sequenza nota, consente l'aggancio del ricevitore alla BTS
- Coded Data: bit di segnalazione per la trasmissione dei dati relativi alla sincronizzazione globale. Contengono anche informazioni per identificare la rete (operatore) cui appartiene la cella e la cella stessa (codice di cella)
- GP: periodo di guardia
- T-bits: posti sempre a 0, usati come tempi di guardia e per l'inizializzazione del demodulatore

Struttura dei burst di correzione di frequenza
- T-bits: posti sempre a 0, usati come tempi di guardia e per l'inizializzazione del demodulatore
- GP: periodo di guardia
- Sequenza di tutti 0, data la modulazione GMSK equivale a trasmettere una sinusoide pura per tutta la durata del burst

Struttura dei burst dummy
Sono burst normali in cui al posto dei dati vengono trasmessi tutti zero. I bit di stealing sono eliminati. Vengono usati solo dalle BTS per l'individuazione (potenza elevata) del canale C0 che è il canale principale della cella

Assegnazione delle risorse alle celle
Ciascuna cella GSM può avere da 1 a 16 tranceiver. Lo slot '0' di una portante è sempre usato per un canale di broadcast su cui vengono trasmessi i burst di correzione della frequenza e di sincronizzazione. Questa frequenza è chiamata C0 ed è la “portante principale” della cella. Più precisamente:
- Su C0 la BTS trasmette in modo continuo, usando burst dummy se non ha dati da trasmettere
- Se ci sono più di tre portanti in una cella è possibile abilitare la funzione di Frequency Hopping per ridurre gli effetti del fading veloce

Canali fisici GSM
Un canale fisico è dato da un time-slot ogni trama. La velocità di trasmissione lorda è 148bit/4.615ms = 32 kbit/s. Nei burst normali i bit utili (a valle della codifica) sono 114 quindi 24.7 kbit/s. I dati utente sono protetti da codici, la velocità di trasmissione utile per l'utente dipende dallo schema di codifica.

I canali fisici sono mappati su canali logici. Lo schema di codifica utilizzato dipende dal canale logico. La mappatura dei canali logici sui canali fisici fa riferimento ad uno schema di temporizzazione assoluto che definisce trame, supertrame (di traffico e controllo) e ipertrame.

Tramatura GSM
- Trama: 8 slot in TDMA (4.615 ms)
- Multitrama di traffico: 26 trame (120 ms)
- Multitrama di segnalazione: 51 trame (235.4 ms)
- Supertrama: 26 multitrame di controllo, ovvero 51 multitrame di traffico (6.12 s)
- Ipertrama: 2048 supertrame (3h 28m 53s 760ms)

Temporizzazione GSM
Il modulo di FN è: 26 x 51 x 2048 = 2,715,647. Viene trasmesso da BTS nei burst di sincronizzazione. Il "quanto" di tempo in GSM è un quarto del tempo di bit. Il tempo è misurato in:
- Quarter-bit Number: QN 0-624
- Bit Number: BN 0-156
- Time slot Number: TN 0-7
- Frame Number: FN 0-2,715,647

QN, BN e TN sono calcolati localmente dal TM, inizializzandoli sugli slot in cui viene trasmesso FN

Utilità della tramatura GSM
La tramatura GSM serve per:
- sincronizzazione tra MT e BTS
- cifratura:
  - usa FN
  - l'FN è ripetuto circa ogni 3 ore, in questo modo è più difficile intercettare una chiamata
- mappatura dei canali logici su quelli fisici
- accesso iniziale a una BTS o durante un handover:
  - MT manda una richiesta alla BTS su un certo frame con FN=Y
  - BTS risponde assegnando un canale
  - MT trova la risposta tra le altre perchè l'assegnazione del canale fa riferimento a Y

Reti Cellulari – GSM V
Canali del GSM
I canali fisici sono la combinazione di un timeslot e una frequenza portante. Vi sono 8 canali fisici per portante, quindi timeslot 0-7.
I canali logici portano le informazioni utili e sono mappati sui canali fisici secondo opportuni criteri. I canali logici si suddividono in:
- canali di controllo: portano le informazioni di segnalazione (di rete e di utente)
- canali di traffico: portano le informazioni utili degli utenti

Canali di controllo
Segnalazione di rete:
- parametri della cella
- sincronizzazione
- sintonizzazione del ricevitore

Segnalazione di utente:
- controllo delle chiamate
- controllo della qualità del segnale (distribuzione delle misure)

I canali utilizzati sono:
- Common Control Channels, CCCH o canali di controllo comuni: per la fase preliminare in cui non è ancora stato assegnato un canale di segnalazione alla connessione (uso occasionale)

– Dedicated Control Channels, DCCH o canali di controllo dedicati: per la segnalazione di una specifica connessione (uso periodico)

Segnalazione di rete: Broadcast Channels, BCH, o canali di distribuzione: canali per informazioni di interesse generale
– Frequency Correction Channel, FCCH
– Synchronization Channel, SCH
– Broadcast Control Channel, BCCH

Frequency Correction CHannel FCCH
– permette la correzione di frequenza al TM
– è una sequenza di 148 bit che specifica la frequenza dalla portante
– è un canale unidirezionale downlink

Synchronization CHannel SCH
Trasporta in 25 bit le seguenti informazioni:
– Base Station Identify Code (BSIC): 6 bit che identificano la stazione base, l'operatore e il color code
– Reduced TDMA Frame Number (RFN): 19 bit che identificano il numero di trama
– è un canale monodirezionale downlink

Broadcast Control CHannel (BCCH)
Trasporta in 184 bit informazioni generali sulla cella e sulla rete:
– numero di canali di controllo comuni
– numero di blocchi riservati al canale AGCH nei canali di controllo comuni
– distanza dei messaggi di paging verso lo stesso terminale (in multipli di 51 trame)
– Location Area Identity (LAI)

Parametri dell'algoritmo di Frequency Hopping:
– CA: Cell Allocation
– MA: Mobile Allocation
– MAIO: MA Index Offset
– HSN: Hopping Sequence generator Number

E' un canale monodirezionale in downlink

Utilizzo dei canali di controllo di tipo broadcast

1. il TM si accende
2. il TM scandisce l'intera banda GSM cercando un segnale (in alternativa, cerca tra alcune frequenze memorizzate nella SIM)
3. quando trova il segnale più forte (C0), cerca il Broadcast Control CHannel (BCCH): il BCCH porta l'informazione di controllo ed è diverso in ogni cella
4. Per essere in grado di leggere l'informazione del BCCH il TM deve:
    1. sintonizzarsi sulla frequenza della cella, tramite il canale FCCH
    2. sincronizzarsi con i dati trasmessi nella cella, trasmite il SCH

Aggiornamento delle informazioni di controllo
Le stazioni base in generale non sono sincronizzate tra loro. Ogni volta che il TMP cambia cella deve nuovamente ricevere le informazioni su FCCH, SCH, BCCH, relative a quella cella.

Canali di controllo comuni

Servono per la fase di inoltro di una richiesta di connessione, sono unidirezionali:
– Paging CHannel (PCH)
– Random Access CHannel (RACH)
– Access Grant CHannel (AGCH)

Paging CHannel PCH
E' un canale unidirezione in downlink:

- utilizzato per notificare ad un terminale una chiamata entrante
- è utilizzato per l'invio di SMS
- è trasmesso in tutte le celle della stessa Location Area

Random Access CHannel RACH
E' un canale unidirezionale in uplink:
- è utilizzato per chiedere l'accesso alla rete:
  - inizio chiamata
  - richiesta di location update
- è soggetto a collisioni

Utilizzo del RACH
1. Chiamata entrante:
   1. TM riceve sul PCH un messaggio di paging
   2. risponde chiedendo un canale dedicato tramite il RACH
2. Chiamata uscente:
   1. TM chiede un canale tramite il RACH
3. TM rileva un cambiamento di LA:
   1. TM chiede un location update tramite RACH

Access Grant CHannel AGCH
E' unidirezionale in downlink:
- è utilizzato per rispondere ad una richiesta del TM, ricevuta su RACH
- alloca un canale di segnalazione detto Stand-alone Dedicated Control CHannel (SDCH)

Canali di controllo dedicati

Dedicated Control Channels (DCCH)
Servono per il controllo di chiamata, sono bidirezionali (uplink e downlink):
- Stand Alone Dedicated Control CHannel SDCCH
- Slow Associated Control CHannel SACCH
- Fast Associated Control CHannel FACCH

Stand Alone Dedicated Control CHannel SDCCH
Uplink e downlink
- assegnato dalla BS tramite il canale AGCH
- usato per lo scambio di informazioni di autenticazione, identificazione, call setup
- usato prima dell'assegnazione di un canale di traffico alla chiamata

Slow Associated Control CHannel SACCH
In downlink traspota le informazioni di:
- timing advance
- controllo di potenza
- informazioni del BCCH che sarebbero perse dal TM cui è stato assegnato un canale di traffico

In uplink (180 bit ogni 480 ms):
- misurazioni del TM: RXLEV e RXQUAL (cella propria e celle vicine)

Fast Associated Control CHannel FACCH
Per segnalazione immediata di parametri che non possono attendere i tempi del SACCH: tipicamente per handover immediato. L'informazione è inviata, in stealing mode, al posto dell'informazione vocale (20 ms di parlato)

Riepilogo sull'uso dei canali di controllo

All'accensione il TM:
1. cerca il segnale più forte
2. Frequency Correction CHannel FCCH

3. Synchronization CHannel SCH
4. Broadcast Control CHannel BCCH
5. se la rete non è ammessa (es. altro operatore), ripete la procedura per il successivo canale più forte

Quando la rete deve contattare il TM:
1. usa il Paging CHannel, PCH
2. TM risponde tramite il Random Access CHannel RACH
3. la rete assegna un canale di segnalazione dedicato (SDCCH) tramite il canale Access Grant CHannel, AGCH

Quando il TM deve contattare la rete:
1. TM usa il Random Access CHannel RACH
2. la rete assegna un canale di segnalazione dedicato (SDCCH) tramite il canale Access Grant CHannel AGCH

Reti Cellulari – GSM VI

Canali di traffico

Trasportano voce o dati utente e sono di tipo:
- Canali a velocità piena (Full rate Traffic CHannel: TCH/F) a 22.8 kbit/s (velocità lorda)
- Canali a velocità dimezzata (Half rate Traffic CHannel: TCH/H) pari a 11.4 kbit/s

Due canali TCH/H condividono lo stesso canale fisico in trame alterne. Un canale di traffico viene assegnato ad una connessione per tutta la durata della chiamata. La trasmissione di voce e dati avviene a commutazione di circuito. La trasmissione utilizza un solo canale di traffico.

Canali di traffico voce
Vi sono due possibili velocità:
- Full rate: 13 kbit/s
- Half rate: 6.5 kbit/s

Canali di traffico dati
La velocità di trasmissione dipende dalla codifica FEC impiegata:
- Full rate: 4.8 o 9.6 o 14.4 kbit/s
- Full reate e utenti veloci: 2.4 kbit/s
- Hald rate: 2.4 o 4.8 kbit/s

SMS

Gli SMS hanno le seguenti caratteristiche:
- lunghezza: 160 caratteri
- scambiati tra un Centro Servizi ed il TM
- se il TM è spento, la rete GSM informa il centro servizi che inoltrerà il messaggio all'accensione del TM
- se il TM è acceso ma in stato IDLE si utilizza SDCCH
- se il TM è attivo si usa il SACCH
- il TM notifica la ricezione dell'SMS
- al TM il messaggio è memorizzato nella SIM

Cell Broadcast CHannel CBCH
E' un tipo di SMS inviato a ogni TM nella cella (per es. informazioni sul traffico), ed a bassa velocità sul canale SDCCH in downlink.

Canali logici e tipi di burst

Il burst di tipo normale è usato per:
- TCH: traffico utente

– BCCH, PCH, SACCH, FACCH, SDCCH: segnalazione

Il burst di tipo correzione di frequenza: FCCH
Il burst di tipo sincronizzazione: SCH
Il burst di tipo accesso: RACH

Mapping dei canali logici sui canali fisici

TCH e SACCH
– Relativi ad una chiamata in corso
– ogni normal burst porta 24.7 kbit/s
– la voce codificata usa 22.8 kb/s
– la banda rimanente corrisponde a 2 trame per ogni multitrama (26 trame)
  – una trama ogni 26 usata per SACCH
  – l'altra è inutilizzata e permette al TM di effettuare misure sul canale

BCCH, FCCH
Informazioni fisse. Informazioni per tutti gli utenti.

SCH
Informazioni che variano periodicamente. Informazioni per tutti gli utenti.

SDCCH
Informazioni per periodi di tempo limitati. Informazioni per tutti gli utenti

PCH, RACH, AGCH
Informazioni asincrone. Informazioni per tutti gli utenti

Altre caratteristiche
– FCCH, SCH usano sempre il timeslot 0 (TS0) della frequenza C0 in downlink
– BCCH, PCH, RACH, AGCH usano sempre C0 (in uplink/downlink); sono consentiti tutti gli slot pari
– SDCCH usa TS0 oppure TS1 della frequenza C0
– Tipicamente, se sono richiesti al più 4 SDCCH, usa TS0 altrimenti usa TS1 di C0 e lascia TS0 disponibile per trasmettere gli altri canali
– In downlink C0 è a potenza maggiore per consentire ai TM di riconoscerla dalle altre
– BCCH, FCCH e SCH (in C0 downlink) devono essere sempre trasmessi
– PCH, AGCH, SDCCH, e a volte SACCH, (in C0 downlink) sono multiplati nel tempo:
  – PCH è privilegiato perchè ha impatto sulle prestazioni del sistema
  – AGCH e SDCCH sono allocati a seguito di una richiesta
– Sono possibili diversi tipi di mapping a seconda della cella e dell'operatore
– Il mapping può cambiare in celle diverse
– Il mapping impiegato è comunicato sul BCCH
– la multitrama di segnalazione dura 51 trame
– Configurazione tipica della portante fondamentale C0 in downlink:
  – trame organizzate in 5 blocchi di 10 corrispondono a TS0 di trame successive
  – primo blocco: FCCH, SCH, 4-BCCH, 4-CCCH (PCH, AGCH)
  – blocchi successivi: FCCH, SCH, 8-CCCh (PCH, AGCH) / 8-SDCCH / 8-SACCH
  – in celle con alto traffico si possono usare configurazioni diverse
– La tipica configurazione per l'uplink:
  – il timeslot TS0 della portante fondamentale C0 è dedicato al RACH
  – si fa eccezione per alcuni timeslot assegnati per il SDCCH

Reti Cellulari – GSM VII

Procedure Parte I

- Registrazione all'accensione
- Roaming e location updating
- Procedura di detach
- Chiamata originata da mobile

Accesione
Quando il TM è spento, l'IMSI del TM è marcato come detached nell'ultimo VLR visitato. All'accensione, il TM scandisce le portanti radio alla ricerca di C0 che sente meglio (C0 non è soggetta a frequency hopping). Il TM si sintonizza tramite il FCCH, acquisisce il sincronismo sul SCH. Tramite il BCCH, acquisisce informazioni sulla rete, tra cui il LAI.
Se il LAI è uguale a quello memorizzao nel TM si esegue la procedura di ISMI attach ed il VLR registra l'IMSI come attached.

Se il LAI è diverso (o se nessun LAI è memorizzato nel TM) si esegue la procedura first registration. Il TM richiede location updating inviando l'IMSI. Il VLR conetatta HLR per aggiornare il puntatore e ottenere dati sul TM, marca l'IMSI come attached. Il VLR risponde assegnando un nuovo TMSI

Roaming entro una LA
Mentre si sposta, il TM misura la potenza ricevuta su C0 della BTS cui è agganciato e sui C0 delle BTS che riesce a sentire. Il TM si aggancia alla BTS che riesce a sentire meglio. Il cambiamento di BTS (cella) è una decisione autonoma del TM. Per questa operazione non è necessario avvertire (interloquire con) la rete, finchè la LA non cambia.

Roaming entro una VLR service area
1. Il TM sul nuovo BCCH riceve un LAI diverso dal precedente
2. Invia una richiesta di accesso sul RACH
3. La BTS assegna un SDCCH al TM tramite AGCH
4. Il TM invia una richiesta di location update contenente il TMSI e il vecchio LAI
5. Procedura di autenticazione
6. Procedura di cifratura
7. L'MSC accetta la nuova localizzazione, aggiorna il VLR e riassegna il TMSI al TM
8. Il TM conferma la ricezione del nuovo TMSI
9. Il BSC rilascia il SDCCH

L'HLR non è informato del cambiamento perchè il VLR non è cambiato.

Roaming tra MSC service area diverse
La prima parte della procedura è identica:
1. Il TM sul nuovo BCCH riceve un LAI diverso del precedente
2. Il TM invia una richiesta di accesso sul RACH
3. La BTS assegna un canale al TM tramite AGCH
4. Il TM invia una richiesta di location updating sul SDCCH contenente il TMSI e il vecchio LAI

Nella seconda parte si cambia MSC:
5. L'MSC contatta il vecchio VLR per ottenere i dati del TM (IMSI)
6. L'MSC contatta l'HLR affinchè aggiorni il puntatore al VLR
7. Procedura di autenticazione
8. Procedura di cifratura
9. L'HLR ordina al vecchio VLR di cancellare i dati del TM
10. L'MSC accetta la nuova localizzazione e riassegna il TMSI al TM
11. Il TM conferma la ricezione del nuovo TMSI
12. Il BSC rilascia il SDCCH

Location Update
Nel GSM esiste anche un location update periodico. Anche se un TM non cambia LA, periodicamente

deve effettuare la procedura di Location Update

Chiamata originata dal TM
1. l'utente compone il numero
2. il TM invia una richiesta di accesso sul RACH
3. la BTS assegna un canale al TM tramite AGCH
4. il TM invia una richiesta di servizio sul SDCCH
5. procedura di autenticazione
6. procedura di cifratura
7. l'MSC rialloca il TMSI
8. il TM inizia la procedura di setup con un messaggio sul SDCCH
9. l'MSC e la BTS assegnano un TCH
10. l'MSC completa la chiamata verso il chiamato
11. l'MSC avvisa il TM che il chiamato sta ricevendo la segnalazione (squillo)
12. l'MSC avvisa il TM che il chiamato ha risposto
13. il TM connette la chiamata sul TCH e conferma (SDCCH è rilasciato)

Reti Cellulari – GSM VIII

Procedure Parte II

- chiamata diretta ad un mobile
- handover
- procedura di detach

Chiamata diretta ad un mobile
1. l'utente compone il MSISDN del TM
2. le centrali della rete fissa tramite il MSISDN instradano la chiamata verso un GSMC
3. il GSMC determina l'HLR del TM
4. il GSMC invia all'HLR un messaggio con il MSISDN
5. l'HLR determina l'IMSI del TM e il VLR presso cui il TM è temporaneamente registrato
6. l'HLR invia al VLR una richiesta di informazioni di roaming
7. il VLR invia all'HLR il MSRN
8. l'HLR invia al GMSC il MSRN
9. il GMSC instrada la chiamata verso il MSC relativo al VLR del TM
10. il MSC, tramite l'IMSI del TM, individua la location area dove si trova il TM
11. il MSC invia un messaggio di PAGE ordinando ai BSC di mandare il paging su tutte le BTS della location area del TM
12. ogni BSC fa eseguire dalle BTS il paging sul PCH con TMSI del TM
13. il TM risponde con un access burst sul RACH
14. la BTS assegna al TM un SDCCH con AGCH
15. procedura di autenticazione
16. procedura di cifratura
17. l'MSC rialloca TMSI
18. l'MSC e la BTS assegnano un TCH
19. il TM avvisa l'MSC che il chiamato sta squillando
20. il TM avvisa l'MSC che il chiamato ha risposto
21. l'MSC connette la chiamata sul TCH e conferma

Handover
Gli handover sono decisi dalla BSC sulla base di misure effettuate da TM e BTS. Ogni TM comunica le misure con la procedura di locating.

Handover – procedura di LOCATING

1. la BSC comunica al TM (sul SACCH, se il TM è in conversazione) gli identificativi delle 6 BTS su cui fare le misure relative al C0
2. il TM misura:
    1. intensità del segnale ricevuto su C0, RXLEVNCEL
    2. intensità del segnale su TCH, RXLEV
    3. qualità del segnale su TCH, RXQUAL
3. la BTS misura RXLEV, RXQUAL sull'uplink, valuta la distanza del TM
    1. ad intervalli regolari (es. 480 ms) il TM comunica alla BTS le misure sul SACCH
    2. la BTS invia le misure alla BSC
    3. la BSC crea una lista ordinata di preferenza
    4. 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

Motivi per cui effettuare l'handover

- RXLEV o RXQUAL sotto una soglia prestabilita
- distanza del TM dalla BTS superiore a un valore massimo consentito
- eccesso di traffico nella cella
- altre esigenze, per es. manutenzione

Tipi di handover

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

- la BSC comanda al TM di cambiare canale di traffico ma non BTS
- si verifica solitamente quando:
    - la qualità del segnale è bassa (RXQUAL)
    - il livello del segnale non è adeguato (RXLEV)
    - nessuna BTS può servire meglio il TM

Handover tra BTS dello stesso BSC

- la BSC raccoglie misure effettuate da TM e BTS:
    - decide se cambiare BTS
    - sceglie la BTS migliore per il TM
    - sceglie un TCH per il TM
- la BSC apre un circuito con la BTS e prenota il TCH
- la BSC ordina al TM di sincronizzarsi sul nuovo TCH (utilizzando il FACCH)
- il TM si sintonizza sul nuovo TCH
- la BSC rilascia il vecchio circuito
- la BSC avvisa il MSC dell'avvenuto handover

Handover tra BSC diversi, ma stesso MSC

- La BSC raccoglie le misure effettuare da TM e BTS
    - decide se cambiare BTS
    - sceglie la BTS migliore per il TM
- La BSC contatta il MSC che apre un circuito verso la nuova BSC che, a sua volta, prenota un TCH presso la BTS prescelta
- il MSC, tramite la BSC, ordina al TM di sintonizzarsi sul nuovo TCH (tramite FACCH)
- il TM cambia TCH, nel contempo il MSC commuta la chiamata sulla nuova BSC
- l'MSC rilascia il vecchio circuito

Handover tra BSC diversi, con diverso MSC
- La BSC raccoglie le misure effettuate da TM e BTS:
  - decide se cambiare BTS
  - sceglie la BTS migliore per il TM
- la BSC contatta il MSC vecchio, che contatta il nuovo 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
- quando il nuovo TCH è allocato, il vecchio MSC è avvertito e la vecchia BSC ordina al TM di sintonizzarsi sul nuovo TCH (tramite il FACCH)
- il TM cambia TCH e il vecchio MSC commuta la chiamata
- il vecchio MSC rilascia il vecchio circuito

Procedura di detach
E' la procedura eseguita allo spegnimento del TM:
- il TM invia un messio di IMSI detach (richiesta di detach)
- il VLR marca il TM come detached (inattivo)
- quando è detached, un TM non riceve messaggi di paging

La procedura di detach non prevede alcuna conferma, né la comunicazione all'HLR.

Reti Cellulari – GSM IX

GSM – Phase 2+
- HSCSD
- EDGE
- GPRS

HSCSD High Speed Circuit Switched Data Service
- i canali di dati portati sulla stessa frequenza vengono raggruppati
- fino a 4 full rate channels possono essere raggruppati per raggiungere 57.6 kbit/s (14.4 kbit/s per time slot)
- Per utilizzare più di 4 time slot è necessario duplicare l'apparato RF

Caratteristiche del servizio
- Data transmission
- Symmetric service

Impatto sulla rete GSM
- Utilizzo del multislot MS
- Alle BTS, BSC ed MSC sono richieste modifiche limitate:
  - Internetworking Unit
  - (De-)Multiplexing alla BSC

Blocco delle connessioni
Utilizzando diversi canali TCH sulla stessa portante si possono avere dei blocchi, specialmente nel trattare gli handover. E' necessario utilizzare delle tecniche di allocazione delle risorse più complesse:
- Intra-cella handover: spesso necessaria per liberare qualche portante
- Dynamic assignment: assegnazione dinamica del numero di canali TCH alle connessioni HSCSD comprese tra un valore minimo RNC e massimo DNC
  - RNC: Required Number of Channels
  - DNC: Desired Number of Channels

Non implementato in Italia.

Adaptative Multirate AMR
Nuovo codec impiegato in GSM e UMTS, consente il bit rate adattativo per: il tipo di canale di traffico (hald o full rate), le condizioni di propagazione delle onde radio, le condizioni di congestione della rete.

EDGE Enhanced Data-Rates for GSM Evolution

Modifiche sulla modulazione e codifica per aumentare la velocità dell'interfaccia radio mantenendo la compatibilità con il GSM.

GMSK
Correntemente utilizzato dal GSM e DCS1800, occupazione di banda 200 kHz, trasporta un 1 bit per simbolo.

L'EDGE è una tecnologia che sfrutta meglio le risorse assegnate al GSM, per aumentare i servizi dati. Aumento del data rate attraverso l'utilizzo di multi-signal constellations e adaptative coding. Es di bit rate: 384 kbit/s per MT a 100km/h di velocità, 144 kbit/s per MT a 250 km/h di velocità.

SIR e Requisiti di traffico
- qualità del canale
  - il canale mobile è tempo variante, e le modifiche del canale cambiano su un range di SIR elevato
  - il massimo del valore di SIR, il minimo del guadagno di codifica
- streaming: servizi che richiedono una qualità stabile e costante del canale
- elastic data: applicazioni che possono resistere ai cambiamenti della qualità del canale e di velocità.

Proposta dell'EDGE
- utilizzo di codici a bassa protezione per aumentare il SIR
- utilizzo dello schema di modulazione 8-PSK quando il SIR è elevato

Provvedere ad algoritmi e protocolli per cambiare automaticamente la modulazione e/o lo schema di codifica quando cambia il SIR

EDGE: modulazione
- utilizza 3/8 shifted 8-PSK
- modulazione derivata da 8-PSK:
  - 8 simboli, ognuno corrisponde a 3 bit
- incrementa il bit rate a 3 relativamente alla modulazione GMSK, mentre mantiene l'occupazione di bande costante.

L'attraversamento in zero implica portante nulla che genera frequenze spurie, ottenendo occupazione di banda elevata, inaccettabile. La soluzione è:
- la definizione di un doppio insieme:
  - ogni simbolo modulato è addizionato allo spostamento di fase di 3/8 pi
  - passaggi tra due differenti stati devono essere tra un insieme e un altro
  - in questo modo il passaggio per zero è evitato

EDGE e GSM
Completamente retro compatibile, può essere utilizzato autonomamente su ogni canale fisico GSM (frequenza + time slot). Utilizza la stessa forma d'onda gaussiana sulla stessa maschera di frequenza. Fornisce sia la commutazione di circuito (E-CSD) che la commutazione di pacchetto (E-GPRS)

Impatto sulla infrastruttura di rete GSM
La porzione di rete interessata per l'EDGE è costituita da BSS ed MT, per introdurre EDGE è necessario:
- inserire un modulatore/demodulatore 8-PSK
- la BSC deve essere in grado di assegnare canali fisici a E-CSD/E-GPRS dinamicamente
- l'interfaccia Abis (tra BTS e BSC) deve essere adattata (GSM 16 kb/s, EDGE 64 kb/s)

Riepilogo
L'EDGE è adatto per tutte le applicazioni con data-link layer non trasparente, è particolarmente efficace

per il GPRS (EGPRS), ha poco impatto sull'infrastruttura di rete. Può essere adottato per fornire servizi di 3G.

GPRS General Packet Radio Service

Motivazioni

Crescita della domanda di servizi orientati ai dati, collegati ad Internet e alla intranet aziendali. Queste reti e sottoreti, utilizzano architetture a commutazione di pacchetto e la suite TCP/IP come protocolli. Le aree PSTN/ISDN tendono a diventare isole collegate con backbone IP. La soluzione nel GSM è il GPRS, associando la rete tradizionale GSM con architettura a commutazione di circuito con quella a commutazione di pacchetto su rete IP. Il GPRS sfrutta la stessa occupazione di banda, la stessa interfaccia radio, aumenta le funzionalità ed i protocolli per abilitare l'accesso a pacchetto sul collegamento radio.

Introduzione

Caratteristiche di base

Utilizza da 1 a 8 time slot sulla stessa portante (max bit rate 171.2 kb/s = 8 * 21.4 kb/s), si basa sull'effettiva quantità di dati trasmessi, così da poter permettere connessioni always on, interagisce con IP e X.25, supporta diversi livelli di QoS.

Possibili applicazioni

Tra le possibili applicazioni ricordiamo: transazioni finanziarie ed economiche, always on connection per telelavoro, sopporto WAP, gestione logistica, gestione sorveglianza, servizi di email. Il GPRS è stato studiato per rispondere ad esigenze di trasmissioni discontinue di pacchetti di piccole dimensioni (< 500 Byte), più volte al minuto e raro trasferimento di pochi kilobytes. Quindi non è adeguato al trasferimento massiccio di dati.

Architettura

Il GPRS coesiste con il GSM e utilizza le stesse celle radio, utilizza anche la stessa infrastruttura di rete ma introduce una nuova infrastruttura logica di rete che è aggiunta a quella del sistema GSM. In particolare:

- due nodi di rete:
  - SGSN (Serving GPRS Support Node)
  - GGSN (Gateway GPRS Support Node)
- una nuova unità di rete:
  - PCU (Packet Control Unit)
- un nuovo data base:
  - GLR (GPRS Location Register)

Il SGSN ha lo stesso ruolo dell'MSC ma viene utilizzato per la rete a pacchetti, il GGSN inerconnette la rete GPRS con le altre reti a pacchetto (PDN – Public Data Network) o a commutazione di circuito (simile a GMSC). La PCU è parte della BSS e permette il trasferimento di traffico a pacchetti sulla interfaccia radio. GLR è implementato sia per SGN che per GGSN, gestisce le informazioni relative agli utenti GPRS.

L'HLR deve essere potenziato, perchè deve contenere le informazioni degli utenti GPRS (localization and subscription), deve essere in grado di comunicare con gli MCS come con gli GSN. Anche MSC/VLR, EIR e SMS Service Center devono comunicare con MSC e GSN.

Confronto tra GMS e GPRS

GSM	***GPRS***
1. commutazione di circuito per voce e servizi dati	1. commutazione di pacchetto per dati

GSM	***GPRS***
2. i nodi di rete sono MSC	2. i nodi di rete sono router IP
3. gateway MSC	3. GGSN
4. per traffico voce si utilizza solo il PHY layer, tra MSC e BSS (PCM PDH, SDH), per dati si usa anche L2 LAPD	4. sia per dati che per segnalazione L1: SDH, L2: ATM, Frame Relay, L3: IP
5. BSS	5. BSS con PCU
6. Canali fisici: FDMA/TDMA	6. Canali fisici: FDMA/TDMA
7. Canali logici: TCH e BCCH, un MT può occupare solo 1 TCH, eccezione fatta per HSCSD	7. Canali logici: PD TCH e PBCCH, un MT può occupare fino a 8 slots. un PDTCH è assegnato ad un MT solo per il tempo della trasmissione del pacchetto. Fino a 8 MT possono essere multiplati sullo stesso time slot
8. location update quando MT cambia LA	8. localizzazione più fine (LA è divisa in Routing Area composte da diverse celle)
9. l'utente è identificato dall'MSISDN (num. tel.)	9. utente identificato dall'IP
10. Uno stato operazionale	10. Tre stati operazionali

Servizi GPRS
Il GPRS coesiste con il GSM, utilizza le stesse celle radio e il traffico voce ha la priorità. Vi sono connessioni Point to Point, Multicast e “Group Call”. I datagrammi, es. IP, sono come gli altri servizi connection-oriented, es. X.25. Gli MS sono classificati:
- Class A: accesso simultaneo a servizi GSM e GPRS
- Class B: accesso GSM e GPRS ma non simultaneo
- Class C: accesso solo GPRS

Stati operazioni dell'MT
- Idle: l'MT non è raggiungibile
- Standby: segnalazione tx/rx e paging possibili ma data unicast no
- Ready: MT può tx/rx data, nessuna esigenza di paging

Gestione della mobilità: localizzazione
Una LA è divisa in Routing Area (RA), ognuna delle quali è composta da diverse celle. Ogni LA è identificata da un LAI, ogni RA è identificata da un RAI, trasmessi sul BCCH.
Se SGSN conosce la cella dell'MT non è necessario il paging, ma la location updating è effettuata quando l'MT cambia cella: conveniente solo durante il trasferimento dati per minimizzare il ritardo. Se SGSN conosce la routing area dell'MT, il paging è effettuato sulla RA: un location updating è necessario quando cambia la RA dell'MT (conveniente quando l'MT è in standby).
Quando l'MT è idle non è raggiungibile, quando è in standby, la sua posizione è conosciuta all'interno della RA. Quando l'MT è nello stato ready, la sua posizione è conosciuta dentro la cella ed identificata dal CGI, Cell Global Identify, CGI = CI+RAC+LAC.

Gestione della mobilità:
Stato di standby: quando un MT cambia RA e SGSN (mentre sta cambiando RA), HLR e GSGN sono informati, e HLR spedisce il profilo di utente dell'MT al nuovo SGSN. Se il cambiamento di una RA corrisponde con il cambiamento anche di una LA, il nuovo SGSN spedisce un LA update all'associato (GSM)VLR.
Anche se l'MT non cambia RA, è necessario periodicamente effettuare un Periodic RA Update.

Riepilogo
- GPRS Location Update:

  - Ready MT aggiorna la sua locazione ad ogni cambio di cella
  - Standby MT aggiorna la sua locazione quando cambia RA
- Per le classi A e B, alcune procedure GSM e GPRS possono essere unite:
  - GPRS attach/detach e GSM attach/detach
  - cambiamento RA (con SGSN) e cambiamento LA (con VLR)
  - Dato che la localizzazione GPRS è più precisa, il GSM paging può essere effettuato dal SGSN che serve l'MT

PDP Context
Il Packet Data Protocol Context è generato per ogni MT in stato ready o standby, che desiderano scambiare traffico con le reti esterne, contiene:
- prodotollo impiegato (es. IPv4)
- IP address dell'MT
- QoS richiesto
- l'indirizzo del GGSN da utilizzare come gateway per le reti esterne

L'MT deve richiedere l'attivazione del PDP context al suo SGSN, che richiederà al GGSN per la generazione del PDP context. Il PDP context è memorizzato dal GGSN, dall'SGSN e dall'MT

Classi QoS
Le classi di QoS sono definite attraverso:
- Precedence Class (classe di precedenza): 3 livelli che indicano l'importanza di garanzia richiesta del QoS in caso di condizioni anormali della rete (es. congestione)
- Delay Class: 4 livelli, nessuno adatto per servizi real-time interattivi. Include:
  - ritardo d'accesso al canale radio in uplink, o il ritardo di radio scheduling in downlink
  - ritardo di propagazione
  - ritardo di transito della rete GPRS
- Reliability (affidabilità): 3 livelli, ottenuti attraverso il controllo ed i meccanismi di ack ai diversi livelli dei protocolli
- Mean Throughput
- Peak Throughput

QoS Provisioning
La rete GPRS-PLMN supporta un insieme di classi di QoS, l'MT può negoziare un livello di QoS alla generazione o modifica del PDP context. Basandosi sulle risorse disponibili, la rete provvede al QoS desiderato. L'RLC/MAC sopportano 4 livelli di priorità radio, più uno per la segnalazione. Questa priorità è determinata dal SGSN basata sul QoS negoziato con l'MT e passato alla BSS e all'MT attraverso il PDP context. La BSS utilizza queste informazioni per determinare la priorità d'accesso, e la precedenza del servizio in condizioni di congestione della rete.

Accesso GPRS, un esempio
Un utente, che desidera trasmettere e ricevere dati:
1. effettua la procedura di attach
   1. MT spedisce il suo ID (TLLI se disponibile o IMSI), la sua classe e le informazioni per la cifratura
   2. se l'SGSN di riferimento è diverso da quello precedente, autenticazione, cifratura, inizializzazione, location update sono necessarie
   3. MT entra nello stato ready: scambio SMS e ricezione multicast message
2. attivazione del proprio PDP context
   1. MT richiede l'attivazione del PDP al suo SGSN, che richiederà al suo GGSN di riferimento, la generazione del PDP context
3. a questo punto, MT è pronto a ricevere e trasmettere dati

Entità, funzionalità e stack di protocolli

SGSN - Serving GPRS Support Node
Implementa tutte le funzionalità di un router standard, (sicurezza, routing, QoS), è incaricato

dell'autenticazione dell'utente (come nel GSM), gestisce le risorse radio insieme alle funzioni RRM alla BSS, per provvedere al QoS richiesto. Inoltre memorizza informazioni utili alla fatturazione. Gestisce i pacchetti da e per gli MT sotto il suo controllo, gestisce la cifratura (come nel GSM), gestisce la mobilità: il GLR contiene la localizzazione e le informazioni di sottoscrizione dell'utente. Gestisce le connessioni LLC con l'MT e le connessioni di dati con le BSS. I pacchetti sono trasferiti attraverso il backbone GPRS (encapsulation e tunneling).

GGSN - Gateway GPRS Support Node
Implementa tutte le funzionalità di un router standard per le reti esterne, instrada pacchetti da e per le reti esterne (se necessario mappa gli indirizzi IP usati dalla rete GPRS su quelli utilizzati sulla rete esterna). Encapsula e decapsula i pacchetti, filtra i pacchetti che provengono dall'esterno, collezione informazioni per la fatturazione. Registra nel suo GLR il SGSN di riferimento che utilizza l'utente, i profili utente e il PDP context. Crea su richiesta un IP dinamico ed il PDP context.

PCU - Packet Control Unit
Permette ad MT e SGSN di scambiarsi pacchetti di dati, provvedere all'allocazione dinamica RR per GSM CS e GPRS, può essere collocato ovunque tra SGSN e la BTS (spesso è nella BTS), comunica direttamente con CCU Channel Coding Unit della BTS (CCU è incaricata del FEC, interleaving, RSS, misure timing advance). Le funzionalità principali sono:
1. segmentation/reassembly per i frame LLC da e per blocchi RLC/MAC
2. physical channel scheduling
3. ARQ
4. le funzionalità di controllo:
    1. Medium Access Control (gestione richieste e allocazione permessi)
    2. informazioni di controllo broadcast
    3. controllo di potenza

SubNetwork Dependent Convergence Protocol (SNDCP)
E' l'interfaccia tra LLC e livello 3 che provvede al trasferimento trasparente dei pacchetti di livello 3. Al livello di SNDCP, l'MT seleziona i protocolli di L3 da utilizzare (IP o X.25). Multipla e demultipla le connessioni di livello 3, segmenta e riassembla i pacchetti, comprime e decomprime le informazioni ridondanti di alcuni protocolli come gli header TCP e i dati dell'utente

Logical Link Control (LLC)
Provvede alle connessioni di livello 2 tra MT e SGSN: cifratura dei dai scambiati, segnalazione ed SMS. Supporta due modalità di trasmissione:
– Acknowledged: SACK Bitmap
– Unacknowledged: Protected (error detection) e Unprotected mode (segnalazione e SMS)
LLC identifica attraverso TLLI (Temporary LL ID, relativo alla RA dell'MT):
– l'MT univocamente e fornisce riservatezza all'utente
– passato al livello inferiore e inserito nell'header RLC

Radio Link Control (RLC)
Segmenta e riassembla i frame LLC in e da i blocchi RLC. Esistono due modalità operative:
– Acknowledged: ritrasmissioni selettive dei blocchi RLC, finestra di dimensione 64
– Unacknowledged

Medium Access Control (MAC)
Permette a molti MT di condividere il mezzo comune:
– allocando risorse: l'accesso uplink utilizza lo slotted aloha reservation protocol (request e ack), il traffico in downlink è schedulato dalla BSS
– multiplazione dei dati e della segnalazione
– priority handling (trattamento delle priorità)

Physical Layer
Stabilisce un canale fisico (PHY) tra MT e BSS, chiamato nel GPRS PDCH. Provvede al FEC, timing advance, misure di ricezione del segnale, controllo di potenza

Data Flow

Radio Block
Radio Block = RLC/MAC Header + Data RLC + BCS. Il livello fisico segmenta 1 Radio Block in 4 normal burst che sono trasmessi sullo stesso time slot in 4 frame consecutivi.

GPRS Tunneling Protocol (GTP)
GTP permette il trasferimento dei pacchetti utente attraverso il GPRS IP backbone, effettuando:
- incapsulazione: tutti i pacchetti da e per gli altri GSN sono incapsulati nelle PDU del GTP
- tunneling: trasferimento di pacchetti incapsulati attraverso i backbone GPRS intra- e inter-PLMN.

Nello user plane, GTP utilizza tunnel per portare i dati utenti, scegliendo il protocollo di trasmissione TCP o UDP in base a dove sarà inviato il pacchetto. Nel control (signal) plane, il GTP è utilizzato per creare, modificare e cancellare i tunnel.

Incapsulazione
Il GGSN incapsula i pacchetti provenienti dalle altre reti e il SSGN serve l'MT destinatario decapsulando i pacchetti. Il GGSN decapsula i pacchetti provenienti provenienti dall'MT per spedirli su altre reti. I pacchetti destinati ad un altro MT appartenente alla stessa PLMN sono instradati da SGSN senza passare attraverso GGSN. Tutti i pacchetti da e verso l'MT sono encapsulati o decapsulati, da e in PDU del SNDCP Protocol all'SGSN.

Tunneling
Le PDU appartenenti alla stessa connessione sono marcate dello stesso identificatore, chiamato Tunneling Identifier TID. Questo identificatore è derivato dall'IMSI ed è unico per ogni utente.

BSS GPRS Protocol (BSSGP)
Funzionalità primarie:
- Indownlink (dal SGSN alla BSS): provvedere alle informazioni del QoS relative alla interfaccia radio da utilizzare da RLC/MAC e BSS, meccanismi di controllo di flusso
- In uplink (da BSS a SGSN): provvedere alle informazioni e misure derivate dall'RLC/MAC, nessun meccanismo di controllo di flusso

Network Service
Basato sul Frame Relay, circuiti virtuali stabiliti tra SGSN e BSS. Le PDU provenienti dal BSSGP sono multiplate sui circuiti virtuali del Frame Relay. I circuiti virtuali possono essere multi-hop e attraversare una rete costituita da diversi nodi di commutazione FR.

GPRS Mobility Management (CMM) & Session Management (SM)
Il GMM si occupa dell'autenticazione, dell'attach/detach, di gestire la Routing Area e del local update. L'SM si occupa di assegnare il TLLI, si occupa della generazione e modifica del PDP context (assegnazione dell'indirizzo IP all'MT, negoziazione del QoS, connessioni verso reti esterne a cui l'MT si vuole connettere, informazioni circa la fatturazione)

Accesso GPRS: un esempio
Quando un utente GPRS vuole trasmettere e/o ricevere dati:
1. effettua una procedura di attach
2. attiva il suo PDP context
3. è disponibile a ricevere e trasmettere dati

Quando l'MT sta trasmettendo:
1. All'MT, il datagramma IP è compresso e incapsulato nella SNDC PDU, spedita attraverso LLC, RLC/MAC e RF all'SGSN

2. quando l'SGSN riceve un dato libero da errore, crea un tunnel in cui inserisce il pacchetto al GGSN di riferimento attraverso il backbone GPRS
3. GGSN rimuove il tunnel e inoltra il pacchetto IP alla rete Internet, che recapiterà i dati alla destinazione finale

Quando l'MT sta ricevendo:

1. l'host corrispondente spedisce il pacchetto IP al GPRS MT, utilizzando l'indirizzo IP dell'MT
2. i protocolli di routing di Internet sono utilizzati per instradare i dati alla sottorete dell'MT
3. GGSN estrae l'indirizzo IP dell'MT lo mappa sulla posizione corrente assunta dall'MT
4. GGSN crea un tunnel inserendo il pacchetto attraverso il backbone GPRS verso l'SGSN che serve l'MT
5. SGSN rimuove il tunnel, encapsula il pacchetto IP dentro la SNDC PDU e lo inoltra alla BSS
6. il pacchetto è spedito all'MT attraverso LLC, RLC/MAC e RF

Interfaccia radio

Packet Data Logical Channels

- Packet Broadcast Control Channel (PBCCH)-DL
- Packet Common Control Channels (PCCCHs):
  - Packet Random Access Channel (PRACH) – UL
  - Packet Paging Channel (PPCH) – DL
  - Packet Access Grant Channel (PAGCH) - DL
- Packet Dedicated Control Channels (PDCCHs) – UL/DL:
  - Packet Associated Control Channel (PACCH) – UL/DL
  - Packet Timing advance Control Channel (PTCCH) – UL/DL
- Packet Data Traffic Channels (PDTCHs) – UL/DL

Osservare che:

- Packet Data Traffic Channel (PDTCHs) sono unidirezionali (uno in uplink ed uno in downlink) e sono separati tra loro
- nelle celle con basso traffico GPRS, il common control channel (PP/PRA/PAG-CH) e il PBCCH possono essere condivisi con il GSM

Radio Interface

E' divisa in GSM multiframes di 52 (26x2), 48 frames sono utilizzati per trasmettere, 12 sono radio blocks. 2 frames sono dedicati alla segnalazione (es. timing advance parameter transmission), 2 frame sono persi in idle. Il radio block è la minima unità di dato

Radio Block Header

Include:

- RLC header + MAC header
- Uplink Status Flag (USF): 3 bit usati in DL per assegnare il corrispondente canale di uplink
  - per allocare dinamicamente il PRACH: (USF=111)
  - USF può identificare fino a 7(8) utenti multiplati sullo stesso time slot
- Block Type Indicator (T): indica quale canale logico è mappato su quello fisico (PHY CH (PDCH))
- Power Reduction R (in DL): per il controllo di potenza

MAC: Accesso al canale

1. MT trasmette a burst sul PRACH (può essere la riposta ad un paging di rete)
2. la rete assegna all'MT PDTCH(s) attraverso il Packet Assigment Message
   1. la BSS assegna il minimo numero di risorse (fino a 8 radio blocks)
3. Per ogni PDTCH assegnato (Radio block in multiframe), la rete assegna l'UFS all'MT
4. Per allocare realmente il PDTCH (per es. radio block (B(n)(n=0,...,11)) in un UL multiframe) all'MT, USF associato è trasmesso sullo stesso PDTCH nel precedente DL Radio Block (B(n-1))
5. le fasi di accesso 1 e 2 dipendono dalla quantità di dati da trasmettere
   1. la 2° fase permette la negoziazione delle risorse

MAC: Radio Resource Allocation
Vi sono due tecniche di allocazione RR supportate:
- Dynamic Allocation: es. 0-2-3 PDTCHs individualmente allocati attraverso USF
- Extended Dynamic Allocation: es. un USF alloca il PDTCH associato e quelli più elevati

Medium Access: alcune definizioni
- Temporary Flow Block (TFB): insieme delle risorse (PDCHs, buffer, ..) allocati per un trasferimento dati
- Temporary Flow Identity (TFI): identifica un Temporary Flow Bock
  - TFI è inserito nell'header di ogni RLC/MAC block
  - in DL identifica il ricevitore tra i GPRS MTs che stanno aspettado i dati

Reti Wireless

Introduzione

In una rete wireless i nodi comunicano tramite un canale "senza filo" (es. canale radio, infrarossi, ecc.). Le caratteristiche principali sono: mobilità dei nodi di comunicazione, natura broadcast del mezzo radio, nodi di comunicazione a basso costo e con limitate risorse energetiche, errori correlati e BER molto maggiore rispetto alla trasmissione via cavo.

Portata trasmissiva
La portata trasmissiva (transmission range) di un nodo wireless è la massima distanza a cui si riceve correttamente l'informazione trasmessa. L'informazione è ricevuta correttamente se il SINR è al di sopra di una certa soglia. La 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.

Nodi di comunicazione
Due nodi wireless comunicano tramite un canale unidirezionale se solo uno dei due è all'interno della portata trasmissiva dell'altro, o con un canale bidirezionale se i nodi sono all'interno della portata trasmissiva l'uno dell'altro.

Classificazione delle reti wireless
Le reti wireless sono caratterizzate dalla copertura, della mobilità dei nodi e dall'architettura.

Architettura
Possono essere di due tipi: con infrastruttura fissa e senza infrastruttura fissa. Nelle reti con infrastruttura fissa, tutti i nodi comunicano direttamente con un punto di accesso alla rete fissa (es. reti cellulari e alcune reti locali). Nelle reti senza infrastruttura fissa (ad hoc) i nodi possono comunicare direttamente tra loro (es. alcune reti locali, reti radio a corto raggio, reti di sensori).

Reti wireless con punto di accesso fisso

Reti wireless "ad hoc"
La rete può essere creata in modo estemporaneo, da nodi che si trovano ad operare nella stessa area. E' un sistema distribuito, e si ha la comunicazione diretta tra i nodi. Le comunicazioni sono multihop. La topologia della rete può cambiare rapidamente e inaspettatamente. La rete può essere autonoma o connessa ad una infrastruttura.
Vantaggi e svantaggi delle reti ad hoc:
I vantaggi sono:
- rete facile e veloce da creare
- costo ridotto
- svariate applicazioni

- comunicazioni personali: telefoni, laptop
- ambienti di lavoro cooperativi: rete di taxi, sale riunioni
- operazioni di emergenza
- ambienti militari

Gli svantaggi sono:
- copertura limitata
- sistema distribuito
- difficoltà di gestione della rete
- difficile mantenere la comunicazione in caso di elevata mobilità dei nodi

Panoramica delle reti wireless

Reti via satellite
Radiodiffusione via satellite:
- bande Ka, Ku: da 12 a 40 Ghz
- propagazione in visibilità, attenuazione dovuta all'atmosfera (forte attenuazione del vapor acqueo)

Televisione, GPS:
- UHF: 0.3-3 Ghz
- propagazione in visibilità, rumore cosmico

Reti satellitari GEO:
- tempo di vita di circa 10 anni
- pesano 4000 kg
- 40 transponder da 80 Mhz di banda
- sensibili agli ostacoli e alla pioggia
- 270 ms di latenza one-way
- tipicamente per servizi diffusivi (TV)

Reti satellitari MEO: 5000-15000 Km
- impiegano 6 ore per un'orbita completa
- ce ne vogliono 10 per copertura completa della superficie terrestre
- 35-85 ms di latenza one-way
- per applicazioni militari e GPS

Reti satellitari LEO: < 5000 Km
- ce ne voglio decine (50) per la copertura completa della superficie terrestre
- 1-7 ms di latenza one-way
- iridium, globalstar

Iridium:
E' un progetto di Motorola, 66 satelliti a 780 Km, 48 celle per satellite, collegamenti anche fra satelliti, meccanismo di handover tra celle, tecnica TDMA (downlink) e FDMA (uplink)
Globalstar:
Progetto Qualcomm, 48 satelliti in orbita a 1400 Km, non c'è handover tra le celle, CDMA

Reti wireless locali
Reti locali (Wireless Local Area Networks – WLAN), lo standard dominate è IEEE 802.11, sfrutta un canale radio, la tipologia della rete può essere con infrastruttura o ad hoc. Attualmente non forniscono qualità del servizio, solo servizio dati. Le wireless ethernet hanno elevate velocità di trasmissione.

Reti wireless personali
Reti personali (Wireless Personal Area Networks – WPAN), lo standard dominante è Bluetooth, IEEE 802.15.1, sfrutta un canale radio, la tipologia è ad hoc, sevizio voce e dati, velocità di trasmissione inferiore rispetto alle reti locali wirelss.

Reti di sensori
Il mezzo trasmissivo può essere radio, infrarosso o ottico, non c'è uno standard dominante, la tipologia è ad hoc. Molti nodi inviano informazioni a un nodo gateway tramite multihop. Sono dispositivi molto

semplici, con basse velocità di trasmissione (1-100 kb/s).

Gli standard
E' necessario standardizzare per facilitare la comprensione, diminuire i costi per effetto delle economie di scala, fondere idee provenienti da fonti diverse, assicurare che i dispositivi di diverse compagnie siano compatibili per avere interoperabilità. Si ottiene maggiore affidabilità, si possono prevedere le evoluzioni e far avanzare la tecnologia integrando i risultati della ricerca. Negli standard si decidono: l'interfaccia radio, il funzionamento della rete, la sicurezza e le procedure di autenticazione, le prestazioni minime del sistema, i servizi (es. SMS, MMS).
Alcuni organi di standardizzazione sono:
- IEEE
- IETF: internet
- OMA: applicazioni cellulari
- ETSI: GSM e GPRS

Wireless Local Area Network WLAN
Esistono due tecnologie: IEEE 802.11 e Hiperlan

IEEE 802.11
Lo standard delle Wireless LAN specifica un'interfaccia wireless tra i client e la base station (access point) e tra client e client. Definisce i livelli PHY e MAC (LLC è definito in 802.2). Il media fisico è radio o infrarossi. Prima release nel 1997.

Architettura
Costituita da:
- BSS (Basic Service Set): insieme di nodi che utilizzano la stessa funzione di coordinamento per accedere al canale
- BSA (Basic Service Area): area spaziale coperta da una BSS (cella WLAN)

La configurazione della BSS può essere: ad hoc, oppure infrastruttura: la BSS è connessa ad un'infrastruttura fissa attraverso un controller centralizzato, chiamato Access Point (AP)

WLAN con infrastruttura
La BSS contiene i wireless host e gli access point (base station). Le BSS sono interconnesse da un distribuition system (DS).

WLAN ad hoc
Le reti “ad hoc” possono essere costituite dinamicamente dalle stazioni IEEE 802.11 senza necessità di access point. Le stazioni possono colloquiare direttamente tra loro. Tra le applicazioni delle reti ad hoc vi sono i laptop meeting, interconnessioni di dispositivi in auto, interconnessioni di dispositivi personali e in campo militare. Il gruppo di lavoro che si occupa di questa architettura di rete è l'IETF MANET.

Extended Service Set (ESS)
Diverse BSS sono interconnesse tra loro attraverso il livello MAC, il backbone che si occupa dell'interconnessione degli access point è un distribution system che può essere: classica LAN, wired MAN o IEEE 802.11 WLAN. Una ESS può dare accesso alla rete Internet attraverso un nodo di gateway. Se il backbone è costituito da una rete IEEE 802.X, il gateway funziona come bridge così da effettuare la conversione della trama.

Scenari possibili

Diventare membro di una BSS
Per diventare membro di una BSS con access point, è necessario eseguire lo scanning, autenticarsi ed associarsi. Nel caso di una Idipendent BSS (IBSS) queste procedure non sono necessarie.
L'operazione di scanning, serve a ricercare l'access point a cui accedere. Esistono due tipologie di

scanning:
- passivo: la stazione esegue lo scan dei canali per ricercare i Beacon frame (che contengono informazioni di sincronizzazione) che sono periodicamente spediti dagli access point.
- attivo: la stazione spedische pacchetti di ProbeRequest, tutti gli access point raggiunti inviano un ProbeResponse

L'operazione di autenticazione è eseguita dopo che l'access point è stato identificato, vi sono due modalità:
- open system authentication: le stazioni spediscono un authentication frame con la loro identità e l'access point risponde con un frame di ack o nack
- shared key authentication: le stazioni ricevono una shared secret key attraverso un canale sicuro, indipendente da 802.11, successivamente si autenticano attraverso l'utilizzo della secret key (richiede cifratura WEP)

L'operazione di associazione avviene successivamente alle altre due e si occupa di concordare le impostazioni di trasferimento dati e roaming, come per esempio la velocità. In particolare viene seguita questa procedura:
- STA -> AP: AssociateRequest frame
- AP -> STA: AssociationResponse frame
- il nuovo AP informa gli altri via DS

Solo dopo che la procedura di associazione è completata, la stazione può trasmettere e ricevere dati.

IEEE 802.11 / 802.11b

Livello fisico (Physical Layer)
Vi sono tre differenti tecniche d'accesso: InfraRed (IF), Frequency Hopping Spread Spectrum (FHSS) e Direct Sequence Spread Spectrum (DSSS).

InfraRed
Utilizza il classico range dei LED, viene utilizzato solo all'interno di edifici, impiegato nelle trasmissioni diffusive, i nodi possono ricevere sia in ordine sparso che a vista. Si raggiungono velocità di 2 Mbps, attraverso l'utilizzo di una modulazione 4-pulse position. La potenza massima in uscita è di 2W, in realtà non è molto utilizzato, in quanto l'IrDA è più comune e più economica.

Spread Spectrum
L'idea è quella di diffondere il segnale su un'ampia banda di frequenze che può essere realizzato attraverso:
- Frequency Hopping: trasmettere su una sequenza casuale di frequenze
- Direct Sequence: trasmettere su una frequenza casuale conosciuta sia dal trasmettitore che dal ricevitore chiamata chipping code.

Frequency Hopping Spread Spectrum (FHSS)
Non è molto utilizzata, la frequenza è intorno ai 2.4 Ghz, sono stati specificati 79 canali ISM, ognuno con ampiezza pari a 1 Mhz. Tre canali corrispondono ad 1 Mbps con modulazione GFSK. Vengono utilizzati tre insiemi di sequenze di hopping per ridurre le interferenze tra le BSS adiacenti. Ogni insieme include 26 sequenze.

Direct Sequence Spread Spectrum (DSSS)
La potenza irradiata è limita, tipicamente 85 mW, la frequenza di base è intono ai 2.4 Ghz, la banda è divisa in 3 canali, ognuno ampio 11MHz e spaziati di 25 Mhz. La diffusione del segnale è effettuata utilizzando la sequenza di Barker con lunghezza 11 chips (11 chips/symbol)/11MHz = 1Mbps usando DBPSK. La sequenza è fissata per tutte le stazioni dentro alla BSS. Le BSS adiacenti coesistono senza interferire se la separazione tra la loro f0 è almeno uguale a 25 Mhz, non più di tre BSS adiacenti sono permesse. Gli schemi di modulazione sono DBPSK @ 1Mbps, DQPSK @ 2Mbps e CCK @ 5.5 e 11 Mbps. Il range è di un centinaio di metri a 1Mbps per interni e cinquecento metri all'esterno.

Rate Adaptation (adattamento di velocità)
Le stazioni effettuano costantemente operazioni per accertare e automaticamente impostare il migliore data rate. Le informazioni di controllo sono sempre inviate in basic rate. Lo standard, non specifica come adattare la velocità di trasmissione. L'Automatic Rate Adaptation è basato sulla misura del SIR, ovvero sul rapporto segnale/rumore.

IEEE 802.11 MAC Protocol
Il protocollo di livello MAC effettua le funzionalità: allocazione di risorse, segmentazione e riassemblamento di dati, indirizzo MAC Protocol Data Unit (MPDU), formato MPDU frame, controllo d'errore. I frame del livello MAC sono di tre tipi:
- Control: positive ACK, handshaking per l'accesso al canale
- Data Transfer: informazioni che sono trasmesse sul canale
- Management: stabilisce/rilascia connessioni, sincronizzazione, autenticazione. Sono scambiati come i data frame ma non sono riportati ad alto livello.

Data Transfer
Può essere di due tipi, asincrono e sincrono. Quello di tipo asincrono è tollerante ai ritardi di traffico, come il file transfer, è il DCF (Distributed Coordination Function). Quello sincrono, è utilizzato per il traffico real-time, come l'audio ed il video, è il PCF (Point Coordination Function). E' basato sul polling delle stazioni e controllato dall'AP. La sua implementazione è opzionale.

Time slot
Il tempo è diviso in intervalli, chiamati slot. La slot è un'unità di tempo del sistema, e la sua durata dipende dall'implementazione del livello fisico, 802.11b: 20 µs. Le stazioni sono sincronizzate con l'access point nella modalità infrastruttura e tra di esse nella modalità ad hoc -> si dice che il sinstema è sincrono. La sincronizzazione è mantenuta dai Beacon frames.

InterFrame Space (IFS)
E' l'intervallo di tempo che intercorre tra la trasmissione di due frame, utilizzato per stabilire la priorità nell'accesso al canale. Esistono 4 tipi di IFS:
- Short IFS (SIFS)
- Point coordination IFS (PIFS)
- Distributed IFS (DIFS)
- Extended IFS (EIFS)

La durata dipende dall'implementazione del livello fisico.

Short IFS (SIFS)
E' utilizzato a separare le trasmissioni appartenenti allo stesso dialogo, associato all'alta priorità, la sua durata dipende dal tempo di propagazione sul canale, dal tempo di trasporto delle informazioni dal livello PHY al livello MAC e dal tempo di commutazione dalla modalità TX a RX, in 802.11b è di 10 µs.

Point coordination IFS (PIFS)
Utilizzato per dare la priorità d'accesso al Point coordinator, solo il PC può accedere al canale tra SIFS e DIFS, PIFS = SIFS + 1 time slot

Distributed IFS (DIFS)
Utilizzato dalle stazioni che aspettano che il canale conteso sia libero. Impostato a PIFS + 1 time slot.

Extended IFS (EIFS)
Utilizzato da una stazione quando il livello PHY notifica al livello MAC che la trasmissione non è stata correttamente ricevuta.

Schema di accesso DCF: generalità

Caratteristiche base

L'implementazione è obbligatoria, il DCF è basato sullo schema Carier Sence Multiple Access/Collision Avoidance (CSMA/CA):

- le stazioni che devono trasmettere dati, si contendono l'accesso al canale
- la stazione deve ripetere la procedura di contesa ogni volta che ha nuovi dati da trasmettere

Riepilogo dello schema di accesso DCF

Basic:

- lo schema più semplice
- utilizzato quando i data frame da trasmettere hanno una breve durata

Con handshaking

- utilizza frame di controllo aggiuntivi per l'accesso al canale
- progettato per risolvere il problema dei terminali nascosti dietro ostacoli o con basso segnale
- fornisce affidabilità nella trasmissione dei dati

Schema di accesso DCF: modalità Basic

Carrier Sensing

E' utilizzato per determinare quando il canale è occupato o idle, eseguito a livello fisico (physical carrier sensing) e a livello MAC (virtual carrier sensing). A livello fisico (physical carrier sensing) determina le sorgenti di energia vicine. A livello MAC (virtual carrier sensing) l'header del frame indica la durata della MAC PDU (MPDU) inclusa.

Network Allocation Vector (NAV)

Utilizzato dalle stazioni vicino al trasmettitore per memorizzare la durata del frame che sta occupando il canale. Il canale diventa idle quando scade il NAV. Anche dopo lo scadere del NAV, le stazioni che hanno dati da trasmettere ascoltano ancora il canale.

Utilizzo di DIFS e SIFS

Trasmettitore: ascolta il canale, se è idle, aspetta un tempo pari a DIFS, se il canale rimane idle per il tempo DIFS, trasmette la sua MPDU.
Ricevitore: computa il checksum per verificare se la trasmissione è corretta. Se è corretta, spedisce un ACK dopo aver aspettato un tempo SIFS. Trasmette l'ACK sempre con un rate minore o uguale alla velocità con cui il trasmettitore ha trasmesso.
Stazioni vicine: impostano i loro NAV con il valore indicato nella MPDU, il NAV è impostato come MPDU tx time + 1 SIFS + ACK

Trasmissione delle MPDU

Ritrasmissione dei frame

La trasmissione di un frame, può fallire a causa di collisioni o errori sul canale radio. Una trasmissione fallita, è ritentata fino a un numero massimo di volte, si utilizza lo schema ARQ (Stop&Wait)

Collision Avoidance (CA)

Si utilizza la procedura di Backoff:

- se la stazione sente il canale occupato, attende che il canale diventi idle
- non appena il canale è idle per il DIFS, la stazione:
  - computa il backoff time interval
  - imposta il backoff counter a questo valore
- la stazione può trasmettere quando il backoff counter raggiunge 0

Valore di Backoff

Valore intero che corrisponde al numero di time slot. Il numero di slot è una variabile reale uniformemente distribuita tra [0, CW]. CW è la Contention Window che a ogni tentativo di trasmissione

è aggiornata utilizzando un algoritmo.
Quando il canale è occupato, il contatore di Backoff è bloccato, quando il canale diventa idle, la stazione fa decrescere il contatore fino a che il canale diventa nuovamente occupato, oppure il contatore raggiunge il valore 0.
Se i contatori di più di una stazione raggiungono il valore 0 allo stesso istante, si ha collisione. Le stazioni che collidono devono rigenerare un nuovo valore di Backoff.

Post-Backoff
Dopo aver completato la trasmissione, una stazione aspetta l'ACK ed effettua la procedura di backoff. Solo in due casi la stazione spedisce un frame dopo aver ascoltato il canale come idle per il tempo DIFS:
- la stazione è appena entrata a far parte della BSS
- la sua coda è libera ed il post backoff è passato

Data Fragmentation
Una MSDU è frammentata in una o più MPDU quando la sua dimensione è maggiore di una certa soglia, in caso di fallimento della trasmissione la banda sprecata è poca. Tutte le MPDU hanno la stessa dimensione, eccetto che l'ultima, perchè può essere più piccola. L'header PHY è inserito in ogni frammento, conveniente se la soglia di frammentazione non è troppo piccola.
Le MPDU originate dallo stesso MSDU sono trasmesse alla distanza di SIFS + ACK + SIFS. Il trasmettitore rilascia il canale quando la trasmissione di tutte le MPDU appartenenti ad una MSDU è completata, l'ACK associato alla MPDU è stato perso.
Il contatore di Backoff è aumentato per ogni frammento ritrasmesso durante lo stesso frame. Il ricevitore, riassembla le MPDU nell'MSDU originale che sarà passato ai livelli più elevati. I dati di tipo broadcast e multicast non sono mai frammentati.

Ricontesa del canale
Una stazione ricontende il canale quando:
- ha completato la trasmissione di una MSDU ma ha ancora dati da trasmettere
- la trasmissione di una MPDU fallisce e l'MPDU deve essere ritrasmessa

Prima di ricontendere il canale, la stazione deve eseguire la procedura di Backoff.

EIFS
E' utilizzato da una stazione quando il livello PHY notifica al livello MAC che c'è stato un errore durante la trasmissione. Inizia dall'istante in cui il livello PHY determina un canale in stato idle, dopo il frame erroneo, senza considerare il meccanismo del carrier-sense. La ricezione di un frame libero da errori durante l'EIFS risincronizza la stazione sullo stato del canale (busy/idle): in questo caso, l'EIFS termina e viene riutilizzato la modalità di accesso normale (DIFS + backoff se necessario). L'EIFS deve essere abbastanza lungo perchè le altre stazioni devono capire che c'è stato un errore.

Schema di accesso DCF: access with handshaking

Utilizzato per riservare il canale, per risolvere i problemi inerenti:
- alle stazioni nascoste
- le stazioni che collidono devono ritrasmettere le loro MPDU, spreco di banda
- necessità di evitare le collisioni, specialmente quando il frame ha dimensioni elevate
- particolarmente utile quando si ha un elevato numero di stazioni

RTS/CTS
La procedura di handshaking utilizza la Request To Send (RTS) e Clear To Send (CTS). Entrambe trasmesse alla velocità di 1 Mbps, l'accesso con handshaking è utilizzato per frame più grandi di una certa dimensione, soglia dell'RTS.

DCS con handshaking
Il trasmettitore spedisce un RTS (20 bytes) alla destinazione, le stazioni vicine leggono la durata del campo dell'RTS e impostano il NAV. Il ricevitore informa il trasmettitore di aver ricevuto la richiesta, dopo il SIFS spedendo un CTS (14 bytes). Le stazioni durante l'invio del CTS aggiornano il loro NAV, il trasmettitore, ricevuto il CTS inizia la trasmissione.

Il problema dei terminali nascosti
E' necessario osservare che:
- se una stazione sente solo il messaggio RTS, imposta il NAV
- se la stazione che origina l'RTS non riceve il CTS, entro un certo il timeout, pensa che la destinazione sia irraggiungibile, inizia la procedura di backoff per riacquistare il canale di trasmissione
- una stazione che riceve solo il CTS può impostare il NAV, anche se non riceve l'RTS: in questo modo il problema dei terminali nascosti è risolto
- tuttavia, se la stazione non sente il CTS per colpa di collisioni, potrà ritentare di utilizzare il canale e collidere insieme al trasmettitore

MACA (Multiple Access with Collision Avoidance)
Algoritmo che origina il meccanismo RTS/CTS usato in 802.11, il MACA evita che si verifichi il problema dei terminali nascosti (hidden terminal) e quello dei terminali esposti (exposed terminal).
Il MACA risolve il problema degli exposed terminals in questo modo:
- se una stazione rileva un messaggio RTS, imposta il NAV
- tuttavia, se non riceve il corrispondente CTS entro un certo timeout, pensa di poter provare ad accedere al canale e resetta il suo NAV

MACAW (MACA Wireless)
Utilizza la sequenza di messaggi: RTS-CTS-DS (Data Sending)-DATA-ACK. Il DS è introdotto perchè:
- se B non percepisce il CTS da D, B può accedere al canale
- se B spedisce un RTS ad A mentre C ha iniziato a trasmettere verso D, B può non essere in grado di ricevere il CTS da A (la trasmissione di C e di A collideranno in B)

Per risolvere il problema, C spedisce un messaggio DS per informare i suoi vicini che la trasmissione dati sta per iniziare, nessun'altra trasmissione con RTS/CTS da parte dei vicini di C potrà essere iniziata durante questo periodo di tempo.
Sono utilizzati dei contatori di ritrasmissione.

Schema di accesso DCF: riepilogo
A lungo termine, fornisce ad ogni nodo la stessa possibilità di accedere al canale. E' l'unica funzione di coordinamento possibile in reti ad hoc: quando esiste un'infrastruttura, è implementato il PCF insieme al DCF.

Schema di accesso PCF (Centralized access scheme)
Caratteristiche base
Utilizzato per servizi con requisiti di QoS, provvede alla contesa per accedere al canale. E' necessario disporre di un punto di coordinamento (Point of Coordination PC) che interroghi le stazioni, può essere implementato in reti con access point. Le stazioni abilitate ad operare con la modalità PCF sono dette CF-aware (CF = Contention Free)

PCF
Le stazioni dichiarano di voler partecipare alla fase CF con un'Association Request. PC costruisce una polling list (statica) in base alle stazioni che ne hanno fatto richiesta, l'implementazione della lista è lasciata al system operator.

PCF Duration

E' progettata per coesistere con il DCF. Il Collision Free Period (CFP) Repetiton Interval (o Superframe) determina la frequenza di ripetizione del PCF in rispetto del Collision Period (CP), durante cui il DCF è effettuato. Il CFP inizia con un beacon signal, periodicamente inviato dall'access point come broadcast, utilizzato per sincronizzare le stazioni. Il CFP termina con un frame di CF_end. La durata è determinata dal parametro CFP_Max_Duration (incluso del beacon), dipende dal traffico, quando inizia il CFP, le stazioni impostano il loro NAV con il CFP_MAX_Duration.

Accesso CFP
Quando inizia il CFP, il PC sente il canale, se è ancora idle per PIFS, PC invia il beacon frame. In CFP, le stazioni possono trasmettere solo come riposta di un polling del PC, oppure dopo SIFS acknowledge di una MPDU. Dopo il SIFS dal beacon, il PC trasmette:
– frame CF-Poll oppure
– un data frame oppure
– un data frame + un frame CF-Poll
Il PC può finire il CFP inviando un frame CFP_end dopo la prima trasmissione. Nel caso in cui CFP avanzi, le stazioni interrogate possono rispondere dopo l'intervallo di SIFS inviando:
– un data frame
– un data frame + CF-ACK (se riceve dati)
– un frame NULL se non c'è nessun dato
Il PC riceve un data frame+ACK in questo modo:
– aspetta SIFS
– poi trasmette un data frame+CF-ACK+CF-Poll a un'altra stazione
Se il PC non riceve il CF-ACK che sta aspettando, aspetta un tempo PIFS e poi trasmette alla stazione successiva della lista.

Problema del QoS nelle WLAN
Il PCF è stato progettato per provvedere al QoS del traffico real-time, tuttavia, ciò che rende difficoltoso il QoS in 802.11 è:
– un ritardo non predicibile dei beacon
– il fatto che non si conosca la durata della trasmissione
– lista di polling statica, polling globale

Dettagli di 802.11

Power Saving
Consumo elevato: Ptx = 1.6 W, Prx = 1.45 W, Pidle = 1.15 W, Pdoze = 0.085 W. Le stazioni possono andare in Pwer Saving Mode. L'AP mantiene un record delle stazioni in PSM ed un buffer per i pacchetti finchè le stazioni non si svegliano. L'AP periodicamente trasmette i beacon per la sincronizzazione, questi includono anche quali stazioni in PSM stanno aspettando dati. Le stazioni in PSM, ogni tanto si svegliano e interrogano l'AP. I messaggi multicast sono tramessi ad un tempo conosciuto a priori: tutte le stazioni che vogliono ricevere queste informazioni si devono svegliare.

Struttura del Frame
Il **Preamble** è dipendente dal livello PHY, è trasmesso a 1 Mbps, ha una sequenza di sincronizzazione (80 bit) e uno star frame delimiter SFD (16 bit). Il PLCP Header, trasmesso al basic rate, contiene la lunghezza del pacchetto, ed altro.
Il **Frame Control Filed** contiene alcuni campi importanti:
– Protocol version: per differenziare 802.11a, 802.11b, 802.11g
– Type e Subtype: management, control, data, 30 tipi diversi
– WEP: indica se il body è crittografato oppure no
– Order: se il frame è in uno stream ordinato
Il **MAC Header Fields** contiene:
– Duration: utilizzato per il calcolo del NAV
– ID: l'id della stazione per il polling PSM
– Sequence Control: numerazione del frame e numerazione del frammento

– Standard 48 bit long IEEE address, indirizzo a cui è destinato il pacchetto e indirizzo da cui proviene il pacchetto

Frame RTS
Il Frame Request To Send, che contiene:
– Duration: durata, tempo di trasmissione del pacchetto data
– RA: indirizzo a cui trasmettere il pacchetto
– TA: indirizzo della stazione che trasmette il pacchetto

Frame CTS
Il Frame Clear To Send, contiene:
– Duration: durata del precedente frame RTS
– RA: il campo TA del frame RTS

Frame ACK
Contiene:
– Duration
– RA: copiato dal frame precedente

Standard 802.11a

Livello fisico
Standard approvato anni fa, difficile introduzione per via dell'usatissima frequenza di 5 Ghz, negli USA:
– 4 canali solo per uso interno
– 4 canali uso interno ed esterno
– 4 canali per bridging esterno: punto-punto, punto-multipunto
In Europa è stato approvato con difficoltà per via di Hiperlan 2
Utilizza la modulazione OFDM (Orthogonal Frequency Division Modulation), usata anche per l'ADSL, modulazione BPSK, QPSK, data rate fino a 54 Mbps, raggio ridotto.

OFDM (Orthogonal Frequency Division Modulation)
Le narrow band sono più facili da compensare localmente.

Confronto tra 802.11b e 802.11a
Il consumo di potenza è simile, l'aspetto importante è che 802.11a ha 8 canali indipendenti mentre 802.11b ne ha solo 3, questo è importante per il cluster di celle riguardo alle interferenze. In 802.11a non ci sono altri apparecchi che possono interferire, mentre l'802.11b è alla stessa frequenza di Bluetooth.

Standard 802.11g

Standard approvato nel Giugno 2003, opera nella banda ISM 2.4 Ghz, è compatibile con 802.11b, usa OFDM come tecnologia di trasmssione, stessa modulazione di 802.11a, stesso data rate, consumo di potenza pari a 802.11b. Sicurezza migliorata, WPA.

Sicurezza in 802.11

Problematiche circa la sicurezza
La trasmissione di dati su un mezzo condiviso utilizza tecniche di cifratura per assicurare la segretezza e l'integrità del messaggio. E' necessario utilizzare l'autenticazione e l'identificazione tramite certificati. Le soluzioni di security possono apparire a più livelli di rete.

Chiavi
La legge di crittografia prevede che l'algoritmo sia pubblico e diffuso mentre la chiave sia segreta. Esistono due tecniche di crittografia:

- a chiave simmetrica: chi invia e chi riceve utilizzano la stessa chiave
- a chiave pubblica: chi invia e chi riceve utilizzano due chiavi distinte: una pubblica, conosciuta da tutti e una privata che è segreta.

Crittografia a chiave simmetrica
Ci sono tre tecniche:
- monoalfabetica: facilmente individuabile, con l'analisi della frequenza
- polialfabetica: non è possibile utilizzare l'analisi di frequenza, non è individuabile se la chiave è utilizzata una volta sola: generare e diffondere la chiave è problematico
- permutazione: non ci sono tecniche di criptoanalisi conosciute, è necessario un attacco brute-force alla chiave. (DES standard)

Crittografia a chiave pubblica

Problematiche
La logistica della tecnica a chiave pubblica ha dei vantaggi ma i suoi algoritmi sono computazionalmente pesanti. Le chiavi simmetriche invece utilizzano algoritmi computazionalmente leggeri ma logisticamente scomodi. La soluzione migliore:

Sicurezza in 802.11
Lo standard incorpora tre meccanismi per provvedere alla sicurezza dell'accesso:
- Service Set IDentifier (SSID)
- filtro indirizzo Media Access Control (MAC)
- Wired Equivalent Privacy (WEP)

Service Set IDentifier (SSID)
Serve ad identificare le apparecchiature appartenenti ad un Basic Service Set (BSS). E' utilizzato per identificare il Service Set a con cui si vuole comunicare, non ha un livello di autenticazione, anche quando si usa il WEP, il SSID rimane visibile.

MAC address filtering
E' possibile restringere l'accesso specificando quali indirizzi MAC possono accedere al servizio, specificando una ACL (Access Control List) nell'AP. Tutti gli indirizzi MAC specificati all'interno di schede sono uniche, tuttavia è possibile cambiarlo via software, spoofing.

Wired Equivalent Privacy (WEP)
Originarinariamente progettato per provvedere alla cifratura e all'autenticazione come parte dello standard 802.11. Utilizza un algoritmo polialfabetico con chiave simmetrica. Le stazioni e l'AP devono essere configurate manualmente e con la stessa chiave (symmetric key). Utilizza l'algoritmo RC4 con 40 o 104 bit di lunghezza di chiave.

Difetti del WEP
Vi sono due difetti principali:
- non esistono metodi per aggiornare e distribuire la chiave, si utilizzano chiavi configurate durante l'installazione degli AP e delle schede WLAN e raramente si cambia configurazione, comunque da fare manualmente
- RC4 è stato progettato per la cifratura one-time e non per essere riutilizzato in diversi messaggi. Così, è possibile monitorare il traffico, acquisire i pacchetti e dopo diversi tentativi scoprire la chiave utilizzata.

Standard per migliorare la sicurezza in 802.11

Esistono tre standard migliorativi:
- 802.1x Authentication
- WPA (Wi-Fi Protected Access)
- 802.11i IEEE Security Enhancements

802.1x Authentication Framework
E' un framework (infrastruttura) per il controllo delle porte d'accesso tra le stazioni, l'AP e i server di autenticazione. Le porte sono il punto d'ingresso della LAN. L'802.1x descrive l'architettura e i requisiti per un'autenticazione per protocolli di alto livello. Incorporato ultimamente in 802.11, utilizza EAP come protocollo di autenticazione.

Extensible Authentication Protocol (EAP)
Standardizzato dall'IETF, permette di utilizzare chiavi dinamiche invece delle chiavi statiche del WEP. Richiede un protocollo comune di autenticazione, le trasmissioni dell'utente devono attraversare l'AP e raggiungere il server di autenticazione: sono permessi diversi metodi di autenticazione, standard di fatto, RADIUS.
L'EAP è un'estensione del PPP utilizzato per supportare gli altri metodi di autenticazione:
- TLS (Transport Layer Security): autenticazione comune, scambio delle chiavi
- richiede certificati client e server

WPA
Migliora il WEP, soluzione tra WEP e 802.11i, provvede a migliorare i vecchi sistemi 802.11 perchè tipicamente richiede solo l'aggiornamento del firmware e non nuovo hardware. Sponsorizzato dalla Wi-Fi Alliance.
Sia client che AP devono supportare il WPA e deve essere abilitato in entrambi, è necessaria una pass phrase (master key) sia per i client che per gli AP, se la frase è corretta, l'AP consente l'accesso alla rete. La pass phrase rimane costante per ogni sessione, ma la chiave di crifratura è generata periodicamente.

E' basato sul protocollo e algoritmo TKIP:
- cambiato il modo con cui sono cambiate le chiavi
- le chiavi vengono rigenerate più spesso
- aggiunta dei messaggi d'integrità

Gli aspetti positivi riguardano il miglioramento della cifratura, la protezione dell'investimento.

Temporal Key Integrity Protocol (TKIP)
- Risoluzione delle problematiche circa il riuso della chiave del WEP
- combina le pre-shared key con il client MAC address per assicurare che i client utilizzino differenti keystream
- utilizza WEP RC4, ma genera una nuova chiave temporanea ogni 10K pacchetti
- utilizza Message Integrity Control per prevenire la falsificazione dei pacchetti

Il beneficio maggiore riguarda la possibilità di utilizzare i dispositivi già disponibili per computare le operazioni di crittografia.

802.11i Security
Utilizzato per risolvere i problemi del WEP e dell'autenticazione condivisa:
- TKIP
- Message Integrity Control
- AES al posto di RC4
- Robust Security Network

Richiede nuovo hardware.

Robust Security Network
L'RSN utilizza la negoziazione dinamica:

- per l'autenticazione e gli algoritmi di cifratura tra l'AP e i client devices
- l'autenticazione è basata su 802.1X ed EAP
- utilizza l'algoritmo AES, basato su permutazioni

Hiperlan

Standard dell'ETSI, bande di frequenza 5 Ghz e 17 Ghz, H/1 bit rate fino a 23.5 Mbps per dati e 2 Mbps per traffico real-time . Hiperlan 2 raggiunge i 54 Mbps. Funziona con nodi statici o in movimento lento, 50m ad alto rate e 800m a basso rate. Modulazione GMSK per H/1 e OFDM per H/2, configurazione ad hoc e infrastruttura con AP.

H/2 MAC

Può utilizzare più di un canale in frequenza, accesso TDD/TDMA, time slotted, capacità di assegnazione dinamica in uplink e downlink. Ha 4 tipi di canali:

- Broadcast Channel: in dowlink trasporta informazioni circa le celle radio, es. AP ID, ID rete, ...
- Frame Channel: in dowlink trasporta informazioni sulla struttura MAC del frame
- Access feedback Channel: in dowlink trasporta ack o nack per i frame precedenti
- Random Channel: in uplink per spedire segnalazione di dati da trasmettere.

Le risorse sono trasmesse all'AP con il numero di PDU che devono essere trasmesse, utilizzando lo schema ALOHA, corrispondente al time slot allocato dall'AP. L'AP determina gli slot in base al ritardo max e medio d'accesso. In caso di collisioni, un nodo è avvisato dall'AP attraverso il canale Access feedback Channel (ACH), poi il nodo computa il backoff. Se la richiesta di trasmissione è andata a buon fine, l'AP schedula le trasmissioni in uplink e downlink. Periodicamente l'AP può interrogare i nodi a proposito del livello di occupazione dei buffer.

H/2 RLC

Contiene informazioni circa l'autenticazione e altre funzioni di sicurezza, RRC, handover management, power saving e controllo di potenza. Informazioni circa le instaurazioni e i rilasci delle connessioni.

Hiperlan vs 802.11

Le differenze fondamentali riguardano:

1. accesso TDD/TDMA in Hiperlan e CSMA/CA in 802.11
2. L'Hiperlan è stata progettata per supportare il traffico real-time, 802.11 no!

Telefonia ed evoluzioni

Evoluzione delle reti telefoniche

1876: telefono di Bell, trasmissione analogica e commutazione manuale, architettura di rete non gerarchica
1891: brevetto del selettore Strowger
1895: esperimenti di Marconi
Anni 40 e 50: autocommutatori elettromeccanici (relè), prima teleselezione, coinvolge più centrali
Anni 60: introduzione della trasmissione e della commutazione numerica PCM, elaboratori elettronici per controllo delle centrali
Anni 70: diffusione delle reti PCM, introduzione dei sistemi di segnalazione a canale comune SS7
Anni 80: completamento della IDN (Integrated Digital Network), definizione e prime installazioni di ISDN (Integrated Services Digital Network), diffusione delle reti cellulari analogiche
Anni 90: diffusione di ISDN e introduzione delle reti intelligenti, definizione della Broadband ISDN (ATM), diffusione reti cellulari numeriche
2000: trasporto della voce su reti a pacchetto (Internet telephony), reti cellulari a commutazione di pacchetto (GPRS) e a larga banda (UMTS)

Apparati

Telefono di Bell
Fino agli anni 60, il telefono è rimasto praticamente identico a quello realizzato da Bell, comprende:
- microfono (trasmettitore)
- altoparlante (ricevitore)

collegati da un circuito elettrico con una batteria in serie. Il trasmettitore è una resistenza variabile che trasforma le onde di pressione sonore in un segnale elettrico, il ricevitore opera la trasformazione inversa, vibrando al variare della corrente.
L'attivazione della selezione avviene sganciando il micro-telefono, che chiude l'interruttore di linea. Il selettore è inserito in serie al circuito del telefono.

Centrale e 'local loop'
Il sensore di sgancio è un relè a induttanza che sente il passaggio della correnti di alimentazione e abilità la porta di ingresso in centrale dedicando un convertitore A/D e una posizione di commutazione alla linea attiva.

Toni di centrale
La centrale invia diversi segnali all'utente:
- squillo
- selezione
- linea disponibile
- linea occupata

Filtri e banda fonica
Il segnale analogico tra telefono e centrale viene filtrato tra 300 e 3400 Hz, per consentire il passaggio della continua di alimentazione e limitare la banda passante del sistema.

Il sistema POTS (Plain Old Telephony Service)
La rete telefonica fornisce connessioni bidirezionali e simmetriche tra coppie di utenti. Il servizio base funziona secondo un modello di chiamata in 3 fasi:
- fase di formazione (call setup)
- fase di conversazione
- fase di abbattimento

L'organizzazione è gerarchica ed il numero di livelli, la nomenclatura delle centrali e degli apparati variano da nazione a nazione. Riflettono sia le dimensioni del paese che la “storia” della telefonia nella nazione.

La rete PSTN (Public Switched Telephone Network)
L'attuale rete telefonica è sostanzialmente una IDN (Integrated Digital Network), con commutazione a circuito, trasmissione e commutazione numerica PCM e segnalazione a canale comune.
L'architettura è divisa in piano utente, piano di controllo (segnalazione) e piano di gestione che non è visualizzato. L'informazione e il controllo “viaggiano” separati

Organizzazione
Piano utente su 3 livelli:
- rete di accesso (da casa dell'utente alla centrale locale)
- reti di giunzione (tra le centrali locali e il centro distrettuale – non necessariamente coincide con un prefisso telefonico)
- rete di lunga distanza (connette tra loro le centrali di gerarchia più elevata)