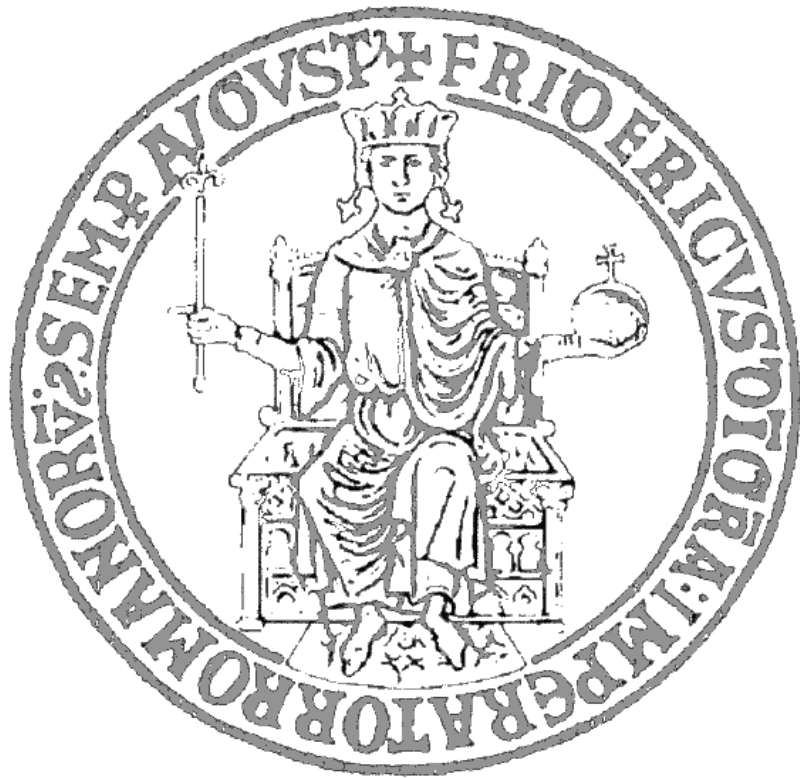


Università degli Studi di Napoli Federico II
CdLS in Ingegneria Informatica
Appunti di Reti Wireless



Reti Wireless

Autore: *MAf@*

Indice

Definizioni introduttive	1
Capitolo 1: Il canale wireless e i suoi modelli	2
1.1 Meccanismi di propagazione	2
1.2 Modelli di propagazione	3
1.2.1 Propagazione in spazio libero	3
1.2.2 Modello con due raggi	4
1.2.3 Relazione distanza-potenza	4
1.2.4 Shadow fading	5
1.2.5 Modelli di attenuazione di percorso	6
1.3 Short-Range Fading	7
1.3.1 Modelli di canale LTI ed LTV	8
1.3.2 Caratterizzazione statistica del fading a banda stretta	11
1.3.3 Caratterizzazione statistica del fading a banda larga	12
1.3.4 Contromisure per il fading	18
Capitolo 2: Tecniche di trasmissione per le W-LAN	20
2.1 Generalità	20
2.2 Tecniche di modulazione	21
2.3 Trasmissione in banda base	22
2.3.1 Tecniche di modulazione ad impulso (Infrared- IR)	22
2.3.2 Tecniche di modulazione UWB (Ultra Wide Band)	23
2.4 Tecniche Spread-Spectrum	23
2.4.1 Frequency-Hopping Spread-Spectrum (FHSS)	23
2.4.2 Direct-Sequence Spread-Spectrum (DSSS)	27
2.5 Trasmissione in banda traslata a banda larga	32
2.5.1 Modulazione CCK	32
2.5.2 Tecniche di modulazione multiportante – OFDM	36

Capitolo 3: Tecniche di accesso per WLAN	45
3.1 Protocollo ALOHA	46
3.1.1 Protocollo ALOHA slotted	47
3.1.2 Protocollo ALOHA con prenotazione	47
3.2 Carrier Sensing (CS)	48
3.2.1 CSMA/CA	49
3.3 Prestazioni delle tecniche di accesso random	49
3.3.1 Prestazioni in presenza di terminali nascosti e di effetto cattura	51
Capitolo 4: Lo standard IEEE 802.11	53
4.1 Architettura protocollare dello standard 802.11x	54
4.2 Lo strato fisico	55
4.2.1 Lo strato fisico di 802.11 base	55
4.2.2 Lo strato fisico degli standard IEEE 802.11a/b/g	59
4.2.2.1 IEEE 802.11b	59
4.2.2.2 IEEE 802.11a	61
4.2.2.3 IEEE 802.11g	63
4.2.3 Carrier Sensing	67
4.3 Lo strato DL in IEEE 802.11x	68
4.3.1 Il sottolivello 802.11 MAC sublayer	68
4.3.1.1 DCF	69
4.3.1.2 PCF	70
4.3.1.3 Formato della frame MAC	71
4.3.2 Il sottolivello 802.11 MAC management	72
Capitolo 5: Hiperlan 1 e 2	75
5.1 HIPERLAN 1	75
5.1.1 Architettura protocollare	75
5.1.1.1 Livello fisico	76
5.1.1.2 Livello Data Link	76
5.2 Hiperlan 2	78
5.2.1 Architettura protocollare	78

5.2.1.1 Livello fisico	79
5.2.1.2 Livello DLC	80
Capitolo 6: Reti Personali Wireless	82
6.1 La tecnologia Bluetooth 802.15	82
6.2 Lo stack protocollare di BT	82
6.2.1 Il livello fisico di BT	84
6.2.2 Il livello MAC di BT	84
6.2.3 Formato delle frame	85
6.3 Gestione della connessione	86
6.3.1 Paging ed Inquiry in Bluetooth	88
Capitolo 7: Reti Wireless Ad Hoc (MANET)	90
7.1 Architettura protocollare e progetto degli strati	91
7.2 Limiti della capacità e limitazioni sull'energia	94
Capitolo 8: Reti MESH	95

Note

Il corso di Reti Wireless si articola sostanzialmente nelle seguenti due parti:

1. **Concetti di base** (Cfr. Cap. 1,2,3):

- Problematiche del canale radiomobile e modelli di canale
- Tecniche di modulazione
- Tecniche di accesso

2. **Standard Wireless** (Cfr. Cap. 4,5,6,7,8):

- W-LAN (802.11, Hiperlan)
- W-PAN (Bluetooth)
- Reti ad hoc
- Reti MESH

Questa dispensa è stata realizzata basandosi sulle slides del corso di Reti Wireless del Prof. Luigi Paura (A.A. 2007/2008), sugli appunti presi a lezione, su diversi libri e su materiale vario scaricato da Internet.

Autore: 

Definizioni introduttive

Servizio di TLC: Un servizio di telecomunicazioni e un insieme di procedure per il trasporto e l'utilizzazione a distanza dell'informazione. I servizi di TLC si possono classificare:

1. In base al tipo di informazione: in Monomediali o Multimediali (+ tipi di info);
2. In base al n° di utenti coinvolti: in Punto-punto e Multipunto (>2 utenti);
3. In base all'interattività: in Interattivi (c'è interazione tra utente e fornitore) e Diffusivi (nessuna interazione);

I servizi di TLC sono caratterizzati da alcuni requisiti che possono essere più o meno stringenti a seconda del servizio. I principali requisiti sono:

- *probabilità di blocco*: probabilità che il servizio possa non essere erogato;
- *tempo di ritardo end to end*: tempo necessario affinché un pacchetto vada da un nodo ad un altro;
- *velocità media*: frequenza di cifra media (bit rate) con cui la rete trasporta l'informazione;
- *probabilità di errore/perdita*: aliquota di bit consegnati dalla rete errati o persi;

Reti di TLC: Una rete di telecomunicazioni può essere definita come un'aggregazione di apparecchiature (hardware) e di istruzioni (software) per la fornitura di servizi di telecomunicazione. Una rete di telecomunicazioni può essere divisa in 2 parti:

1. Rete di accesso: Si interfaccia con l'utenza per fornire i servizi di TLC;
2. Rete di Trasporto: Trasferisce grandi quantità di informazioni ad elevate velocità;

Le reti di TLC si possono distinguere:

1. In base alla tecnologia realizzativa: in reti fisse e reti mobili;
2. In base alle dimensioni: in WAN (geografiche), MAN (metropolitane), LAN (locali).

Convergenza: Per convergenza di reti si intende la possibilità di far interoperare diverse reti nate per scopi differenti. Le reti devono essere trasparenti rispetto ai servizi e viceversa.

W-LAN: Le wireless LAN consentono un accesso capillare alle risorse e sono l'unico modo per erogare un servizio in mobilità di apparato. Si possono classificare in:

1. Reti infrastrutturate: basate su un Access Point per collegare i terminali;
2. Reti autoconfiguranti: non c'è l'AP, gli attori interagiscono mediante protocolli peer to peer; si distinguono in reti ad hoc (Manet) e reti di sensori (meno complesse ma anche meno prestazionali).

Capitolo 1

Il canale wireless e i suoi modelli

Nel canale radiomobile il percorso seguito dalle onde elettromagnetiche dal trasmettitore al ricevitore può essere: *diretto*, se Tx e Rx sono in linea di vista (LoS), oppure *con ostacoli*, se le onde impattano contro ostacoli (come edifici, montagne, nebbia, etc...). Inoltre tale percorso varia con la posizione del terminale mobile. Tutto ciò, come vedremo, porta a rappresentare il canale radio in maniera aleatoria.

1.1 Meccanismi di propagazione

Quando tra il Tx e il Rx vi sono ostacoli, le onde radio possono raggiungere il Rx grazie ai 3 seguenti meccanismi di propagazione:

1. *Riflessione*: si ha quando le dimensioni degli ostacoli su cui incide l'onda elettromagnetica sono molto maggiori della lunghezza d'onda.
2. *Diffrazione*: si ha quando l'onda incide sui bordi di un ostacolo creando sorgenti secondarie; cioè, quando l'onda raggiunge il bordo dell'ostacolo subisce una deviazione della sua traiettoria che gli consente di raggiungere punti nascosti dall'ostacolo (ovvero punti nella sua zona d'ombra).
3. *Scattering* (Diffusione): si ha quando l'onda elettromagnetica incide su superfici irregolari di dimensioni dell'ordine della lunghezza d'onda o inferiore, le quali diffondono l'onda in tutte le direzioni.

In generale, a causa di questi fenomeni al Rx giungerà un segnale fortemente attenuato le cui componenti hanno seguito percorsi differenti (multipath fading).

1.2 Modelli di propagazione

Un modello di propagazione analizza la potenza media ricevuta ad una certa distanza dall'antenna trasmittente e la sua variabilità in prossimità dell'antenna ricevente.

Il deperimento del segnale si può classificare in due ceppi:

1. Modello su larga scala (*Path Loss*): usato per studiare le variazioni del segnale su distanze lunghe;
2. Modello su piccola scala (*Fading*): usato quando il terminale mobile si muove su percorsi brevi (un certo numero di lunghezze d'onda) intorno al punto di ricezione; ciò causa rapide fluttuazioni del segnale, dovute al fatto che i vari contributi del segnale giungono al Rx con ampiezze e fasi differenti (che occorre modellare come variabili aleatorie).

Descriviamo di seguito i diversi modelli che si possono utilizzare nelle varie situazioni di interesse.

1.2.1 Propagazione in spazio libero

Questo modello si utilizza per predire la potenza media del segnale ricevuto ad una certa distanza d dal Tx quando questo e il Rx sono in LoS. Ovvero, considero un solo raggio (segnale) trasmesso direttamente dal Tx al Rx.

In spazio libero la potenza media del segnale ricevuto è data dalla seguente equazione di Friis:

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d} \right)^2$$

cioè decresce col quadrato della distanza. L'esponente è detto gradiente di perdita (o esponente path-loss) e indica la velocità di decadimento della potenza del segnale. Passando ai decibel possiamo dire che nello spazio libero la potenza decade ad una velocità di 20 dB per decade ($d^2 \rightarrow 10\log d^2 = 20\log d \rightarrow 20\text{dB/decade}$).

Nota: 1 decade = 10 m; ogni decade devi aggiungere uno 0 (es. 2 decadi=100m).

1.2.2 Modello con due raggi

Questo modello si utilizza quando al Rx giunge un'onda diretta (LoS) ed una riflessa (NLoS) predominante. Esso si può generalizzare al caso di N raggi.

In questo modello la potenza media ricevuta è data dall'equazione di Friis:

$$P_r = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4} \Rightarrow 40 \text{ dB per decade}$$

dove h_t ed h_r rappresentano, rispettivamente, le altezze delle antenne trasmittente e ricevente. In questo caso, dunque, la potenza media decade con la quarta potenza della distanza e quindi ho un'attenuazione di 40dB per decade.

1.2.3 Relazione distanza - potenza

In realtà le equazioni di Friis richiedono ipotesi di campo lontano, cioè sono valide per distanze maggiori della distanza di Fraunhofer, che è data da $d_f = 2D^2/\lambda$, dove D è la max dimensione lineare dell'antenna Tx. Per cui i modelli di propagazione su larga scala usano una potenza calcolata ad una distanza di riferimento ($\geq d_f$), dando luogo al cosiddetto modello distanza-potenza:

$$P_r = P_0 d^{-\alpha}$$

dove α (detto gradiente distanza-potenza) dipende dall'ambiente, ed è pari a 2 in assenza di ostacoli (spazio libero) e maggiore di 2 in presenza di ostacoli ($2 \leq \alpha \leq 6$). Da questa relazione possiamo determinare la formula della perdita di percorso (ovvero la perdita di potenza nel trasferimento del segnale dal Tx al Rx); infatti, passando ai dB e detta L_p la perdita di percorso, possiamo scrivere:

$$\begin{aligned} L_p = P_t(\text{dB}) - P_r(\text{dB}) &= 10 \log P_t - 10 \log P_r = 10 \log P_t - (10 \log P_0 - 10 \alpha \log d) = \\ &= L_0 + 10 \alpha \log d \end{aligned}$$

avendo posto $L_0 = 10 \log P_t - 10 \log P_0$.

Conoscendo la potenza trasmessa (P_t) e la sensibilità del ricevitore (P_r) possiamo determinare l'attenuazione complessiva (L_p), e quindi, tramite la formula appena data, la distanza d (ovvero l'area di copertura).

1.2.4 Shadow fading

Il modello distanza-potenza stima il valor medio della potenza ricevuta, cioè il valore calcolato è mediato su una scala delle distanze sufficientemente lunga da poter trascurare le variazioni della potenza con la distanza (fading). Su scale di distanza più brevi (circa 100m), a parità di distanza, ci saranno delle variazioni rispetto al valore medio calcolato a causa degli oggetti circostanti; ovvero non tutti i punti a distanza d dal Tx riscontreranno la stessa Path Loss, perchè non tutti sono soggetti allo stesso riverbero ambientale, ma si avrà un effetto ombreggiatura (Shadowing). Misurazioni hanno dimostrato che tale effetto può essere descritto da una distribuzione LogNormale intorno al valor medio.

Nota: Si parla di shadow fading perchè il segnale è "bloccato" da ostacoli riflettenti (es. edici), o di fading lento perchè le variazioni con la distanza sono molto più contenute rispetto a quelle dovute ad altri fenomeni (multipath, doppler) che si verificano quando le medie vengono fatte su scale di distanza molto più ridotte (circa mezza λ).

Per tener conto dello Shadow fading (o fading lognormale) occorre passare ad un modello probabilistico, ovvero dobbiamo riscrivere la formula della perdita di percorso (path-loss) come:

$$\widehat{L}_p = L_0 + 10\alpha \log d + X$$

dove $X = \text{v.a. normale } N(\mu, \sigma)$, cioè la variazione $Y = e^X$ è una v.a. Lognormale (ovvero una v.a. il cui esponente è gaussiano). Questo termine additivo aleatorio rende la nostra L_p uno stimatore gaussiano a media $L_0 + 10 \alpha \log d$ poichè in genere si prende la X a media nulla. La deviazione standard σ rappresenta un indice della dispersione intorno al valore medio: più grande sarà σ tanto più consistente sarà lo shadow fading. A causa dello shadow fading l'ampiezza del segnale ricevuto può non essere sufficiente a garantire una rivelazione affidabile; ovvero, a differenza dei modelli deterministici la copertura può non essere più garantita. Per garantire che una certa percentuale di terminali sia in copertura per un certo tempo, bisogna aggiungere un'aliquota di potenza in trasmissione in più di quella strettamente necessaria per tenere conto del fading:

$$L_p = L_0 + 10\alpha \log d + F_\sigma \quad \text{con } F_\sigma \text{ margine di fading}$$

il termine aggiuntivo (detto margine di fading) è un termine deterministico che dipenderà dall'entità del fading (da quanto è grande σ) che si oppone e dalla percentuale di terminali che voglio coprire.

1.2.5 Modelli di attenuazione di percorso

Una cella di copertura radio è caratterizzata da una certa dimensione e, a seconda della dimensione e dell'ambiente circostante, il modello per descrivere il canale è differente.

Megacelle: Le megacelle sono celle di dimensioni dell'ordine delle centinaia di Km (reti satellitari Low Earth Orbit - LEO). La perdita di percorso è usualmente come quella dello spazio libero e non si considera shadow fading:

$$L_p = L_0 + 10\alpha \log d \quad \text{con } \alpha = 2$$

dove con L_p indichiamo l'attenuazione di percorso (il pedice p sta per path) ed L_0 è l'attenuazione ad una distanza di riferimento in genere un metro.

Macrocelle: Le macrocelle sono dell'ordine delle decine di Km: celle per la telefonia cellulare (900 MHz, 1800 MHz). Il modello generalmente utilizzato per descriverne la propagazione è il modello di Okumura-Hata che è un modello empirico (calcolato sulla base di misure e sperimentazioni).

Microcelle: Le microcelle sono celle dell'ordine delle centinaia di metri o al più di un Km. Le forme delle celle non sono più circolari ma rettangolari o a croce. Il modello è simile a quello di O-H ma si introduce un nuovo parametro: la differenza tra l'altezza media degli edifici e l'antenna ricevente.

Picocelle: Le picocelle sono celle che coprono un edificio o parte di esso (30m-100m). Il modello si utilizza per W-LAN, W-PBX e PCS che operano in ambiente indoor. È stata proposta una relazione distanza-potenza ed esistono modelli empirici per l'attenuazione di percorso. Si possono considerare diverse tipologie di scenari:

- **Scenario multipiano:** In questo caso la relazione sull'attenuazione di percorso è:

$$L_p = L_0 + nF + 10 \log d$$

dove n è il numero dei piani tra Tx e Rx, F è l'attenuazione per piano e dipende dalla frequenza (10 dB per misure a 900 MHz, 16 dB per misure a 1.6 GHz), d è la distanza tra trasmettitore e ricevitore. L'attenuazione aumenta linearmente.

Un modello più accurato è il JTC, che tiene conto anche dello shadow fading ed è quindi un modello probabilistico. La relazione diventa:

$$\widehat{L}_p = A + L_f(n) + B \log d + X$$

dove $L_f(n)$ è una funzione non lineare di n ovvero dei numeri dei piani, X è una variabile aleatoria che rappresenta lo shadow fading, A è un'attenuazione costante che dipende dall'ambiente, B è l'attenuazione per decade. Questo modello lavora a 1.8 GHz per cui va forzato per poter lavorare in WiFi (2.4 GHz).

- Modello con perdite dipendenti dal tipo di separazione: Modello ancora più accurato del precedente perchè tiene conto anche delle separazioni di tipo diverso tra piano e piano o tra camera e camera. La relazione in questo caso è:

$$L_p = L_0 + 20 \log d + \sum m_{type} w_{type}$$

dove m_{type} e w_{type} rappresentano rispettivamente il numero di separazioni dello stesso tipo e l'attenuazione in dB ad ogni tipo di separazione.

Femtocelle: dimensioni inferiori alle decine di metri. Sostanzialmente standard Bluetooth o HomeRF. Per queste applicazioni può essere utilizzato il modello JTC per zone residenziali con frequenze a 1.8 GHz. Per applicazioni in ISM a 2.4 5 GHz si può ricorrere al modello free space:

$$L_p = L_0 + 10 * \alpha \log d$$

1.3 Short-Range Fading

Lo short range fading è un fenomeno riscontrabile se le medie sono fatte su distanze molto brevi, dell'ordine della metà della lunghezza d'onda del segnale che utilizziamo (ovvero < 10m perchè le frequenze in gioco vanno dai GHz in su), e consiste in rapide fluttuazioni del segnale. Tale fenomeno è dovuto all'interferenza tra 2 o più versioni del segnale trasmesso che giungono al Rx con ritardi differenti, dove si combinano dando luogo ad un segnale fortemente variabile nell'ampiezza e nella fase.

Più precisamente, il fading a breve termine è dovuto al verificarsi di 2 fenomeni:

1. **Multipath**: presenza di più percorsi (a causa degli effetti di riflessione, diffrazione, e scattering). A causa di questo fenomeno il segnale ricevuto è una somma di repliche del segnale trasmesso giunte da percorsi differenti e quindi caratterizzate da attenuazioni, ritardi e fasi differenti. Ciò comporta una dispersione temporale (cioè il segnale ricevuto ha durata maggiore di quello trasmesso), a cui corrisponde una selettività in frequenza, cioè il segnale viene distorto dal canale.
2. **Effetto doppler**: dovuto al moto relativo tra Tx e Rx, che da luogo ad uno scostamento della frequenza (dispersione frequenziale), a cui corrisponde una selettività (distorsione) nel tempo, per cui il canale non si può assumere più come stazionario ma deve essere assunto tempo-variante (nel tempo il segnale è fortemente distorto, e in frequenza ho una banda di frequenze anziché una singola riga spettrale).

1.3.1 Modelli di canale LTI ed LTV

Per studiare il fading a breve termine occorre analizzare la risposta impulsiva del canale radio utilizzato. Consideriamo un modello di canale LTI o LTV a seconda se il ricevitore è fermo o in movimento; quando il terminale mobile è in movimento il canale deve essere assunto TV perchè il terminale spostandosi sperimenterà, in posizioni spaziali differenti, condizioni di propagazione differenti, ovvero canali differenti.

Poiché siamo interessati a segnali di tipo passa-banda, consideriamo la rappresentazione analitica (o di Rice) dei segnali.

Detto $s(t)$ il segnale trasmesso e $u(t)$ il suo equivalente passabasso (ovvero la replica nell'origine), $s(t)$ si può rappresentare come:

$$s(t) = \Re \left\{ u(t) e^{j2\pi f_c t} \right\}$$

Il segnale ricevuto a meno del rumore additivo sarà una somma di repliche di quello Tx:

$$r(t) = \Re \left\{ \sum_{n=0}^{L(t)} \alpha_n(t) u(t - \tau_n(t)) e^{j(2\pi f_c(t - \tau_n(t)) + \phi_{Dn})} \right\}$$

dove $\alpha_n(t)$ e $\tau_n(t)$ sono l'ampiezza e il ritardo associato all'n-esima replica (ovvero all'n-simo percorso), $\phi_{Dn}(t)$ è lo shift di fase dovuto al doppler sull'n-simo percorso, $n = 0$ indica la replica principale dovuta al percorso diretto (LOS) mentre $n \neq 0$ porta in conto le repliche NLOS, e $L(t)$ è il numero dei percorsi risolvibili all'istante t .

Due percorsi si dicono risolvibili se le repliche non si sovrappongono fra di loro (ovvero quando hanno ritardi prossimi tra loro), ovvero se le repliche sono distanziate di un intervallo ampio rispetto alla loro durata e quindi sono riconoscibili. L'n-simo percorso risolvibile può essere generato da un singolo scatterer o da un cluster di scatterer non risolvibili.

Se i ritardi τ_i e τ_j di due componenti (repliche) sono molto diversi si ha che:

$$|\tau_i - \tau_j| \gg \frac{1}{B_u} = T \quad (B_u \equiv \text{banda di } u(t)) \Rightarrow$$

i percorsi i e j sono risolvibili (le repliche non si sovrappongono) e si parla di **fading a banda larga**.

Se invece i ritardi τ_i e τ_j di due componenti sono molto simili:

$$\tau_1 \simeq \tau_2 \Rightarrow u(t - \tau_1) \simeq u(t - \tau_2)$$

allora i percorsi non sono risolvibili (le repliche si sovrappongono) e si parla di **fading a banda stretta**. In questo caso i percorsi combinano in un unico percorso (cluster di scatterers non risolvibili).

Osservazione: Un canale è a banda larga o a banda stretta a seconda di come lo usiamo: se la durata del segnale trasmesso è sufficientemente piccola affinché le repliche non si sovrappongano allora sono in condizioni di fading a banda larga, altrimenti sono in condizioni di banda stretta.

Modello lineare tempo-variante (LTV)

Riprendendo in considerazione il nostro segnale ricevuto, esplicitando l'esponenziale, definiamo il contributo di fase globale (dovuto sia al doppler che al ritardo):

$$\phi_n(t) = 2\pi f_c \tau_n(t) - \phi_{D_n}$$

In tal modo possiamo visualizzare la presenza dell'equivalente passabasso di $r(t)$, che indichiamo con $\tilde{r}(t)$:

$$r(t) = \Re \left\{ \underbrace{\sum_{n=0}^{L(t)} \alpha_n(t) e^{-j\phi_n(t)} u(t - \tau_n(t)) e^{j2\pi f_c t}}_{\tilde{r}(t)} \right\} \Rightarrow$$

$$u(t) \rightarrow \tilde{r}(t) = \sum_{n=0}^{L(t)} \alpha_n(t) e^{-j\phi_n(t)} u(t - \tau_n(t))$$

che è il legame ingresso-uscita di un sistema lineare tempo variante, la cui risposta impulsiva è:

$$\delta(t - (t - \tau)) \rightarrow h(t, \tau) = \sum_{n=0}^{L(t)} \alpha_n(t) e^{-j\phi_n(t)} \delta(\tau - \tau_n(t))$$

dove t è l'istante di osservazione, e rappresenta le variazioni temporali dovute al moto, mentre $\tau = t - t_0$ (con t_0 istante di applicazione dell'impulso), e rappresenta il ritardo dovuto ai cammini multipli introdotti dal canale per un fissato t . Tale modello tiene conto del fatto che se il terminale (Rx) è in movimento, le ampiezze, i ritardi e le fasi delle repliche che riceve variano al variare della sua posizione e quindi dell'istante di tempo t considerato.

Modello lineare tempo-invariante (LTI)

Questo modello si usa quando il terminale ricevente è fermo, nel qual caso i percorsi che vede sono sempre gli stessi. In altri termini, se i parametri $\alpha_n(t)$ e $\tau_n(t)$ non dipendono dal tempo, ossia sono stazionari, il modello diventa lineare tempo invariante (LTI). Tale modello si utilizza quando si sfrutta il canale per un tempo breve per cui i parametri possono essere considerati costanti. La risposta impulsiva diventa:

$$h(t, \tau) = \sum_{n=0}^L \alpha_n e^{-j\phi_n} \delta(\tau - \tau_n) = h(\tau)$$

in cui non prendiamo più in considerazione l'effetto doppler (che è legato alla tempo varianza): $\phi_n = 2\pi f_c \tau_n$ perchè $\phi_{D_n} = 0$ se il canale è LTI (visto che sto trascurando il doppler).

La risposta impulsiva del canale deve essere modellata come un processo aleatorio, in quanto le condizioni in cui può trovarsi il canale dipendono dai fattori ambientali (se piove, se il terminale si muove o sta fermo, se c'è nebbia, etc...), i quali non si riescono facilmente a portare in conto.

Delay Spread e canali a banda larga e a banda stretta

In ogni caso (sia LTI che LTV), il canale introduce una dispersione temporale (cioè un ritardo) la cui entità, se i τ_n sono deterministici, può essere misurata come il massimo ritardo rispetto al contributo LOS (τ_0) (perchè il demodulatore è sincronizzato su τ_0) oppure rispetto al ritardo medio se i τ_n non sono tutti deterministici:

$$T_M = \begin{cases} \max_n |\tau_n - \tau_0| \\ \max_n |\tau_n - \bar{\tau}| \end{cases}$$

T_M è detto **tempo di multipath o di dispersione o delay spread** e rappresenta il massimo tra tutti i possibili ritardi (cioè il ritardo tra la prima e l'ultima replica che ricevo). Più T_M è grande più il canale sarà caratterizzato da dispersione temporale. Questa definizione però non porta in conto il fatto che la dispersione va calcolata anche rispetto all'entità delle repliche. Quando le repliche hanno attenuazioni molto differenti la formula da adottare è:

$$\tau_{rms} = \sqrt{\frac{\sum_{k=1}^L \tau_k^2 \sigma_k^2}{\sum_{k=1}^L \sigma_k^2} - \left(\frac{\sum_{k=1}^L \tau_k \sigma_k^2}{\sum_{k=1}^L \sigma_k^2}\right)^2} \quad \text{RMS delay spread}$$

Con tale parametro possiamo essere più precisi nella definizione del fading a banda stretta o larga; si parlerà di fading a banda stretta quando:

$$T_M \ll \frac{1}{B_u} \approx T \Rightarrow \text{percorsi non risolvibili}$$

cioè quando la dispersione temporale (T_M) è trascurabile rispetto alla durata del segnale (T); mentre si parlerà di fading a banda larga quando:

$$T_M \gg 1/B_u \approx T \rightarrow \text{percorsi risolvibili}$$

1.3.2 Caratterizzazione statistica del fading a banda stretta

Nel caso di fading a banda stretta la dispersione temporale è trascurabile rispetto alla durata del segnale:

$$T_M \ll \frac{1}{B_u} \approx T \Rightarrow \tau_n \leq T_M \Rightarrow u(t - \tau_n) \approx u(t)$$

cioè le repliche sono sovrapposte e non si è più in grado di risolvere le singole repliche. Poiché le varie repliche si sovrappongono, nella relazione di $r(t)$ nel caso di banda stretta posso scrivere $u(t)$ al posto di $u(t - \tau_n)$ e portarlo fuori dalla sommatoria:

$$r(t) = \Re \left\{ \sum_{n=0}^L \alpha_n u(t - \tau_n) e^{j2\pi f_c(t - \tau_n)} \right\} = \Re \left\{ u(t) e^{j2\pi f_c t} \underbrace{\sum_{n=0}^L \alpha_n e^{-j2\pi f_c \tau_n}}_{Z \equiv \text{v.a. complessa}} \right\} \Rightarrow h(\tau) = Z \delta(\tau)$$

In pratica trasmetto $u(t)$ e ricevo $Zu(t)$, cioè il canale si è limitato solo a modificare ampiezza e fase del segnale trasmesso ma non introduce distorsione. Per caratterizzare il canale occorre caratterizzare la variabile aleatoria Z . Nell'ipotesi di numerosi scatterer indipendenti la variabile Z (e quindi il canale) è una v.a complessa gaussiana, le cui componenti (parte Re e parte Im) sono indipendenti, a media nulla (se non c'è LoS) e con uguale varianza, e quindi il modulo è distribuito secondo Rayleigh la fase è distribuita uniformemente in $(0, 2\pi)$.

La pdf di una variabile aleatoria Rayleigh si scrive come:

$$f_{ray}(r) = \frac{r}{\sigma} \exp\left(-\frac{r^2}{2\sigma^2}\right) u(r)$$

Se vi è un contributo predominante (LOS) dovuto a raggio diretto, avrò una componente deterministica ed una aleatoria; Z sarà ancora una v.a. gaussiana, in cui però le medie non sono più nulle a causa della componente deterministica. In questo caso la distribuzione della ampiezza è di tipo Rice:

$$f_{rice}(r) = \frac{r}{\sigma} \exp\left(-\frac{r^2 + K^2}{2\sigma^2}\right) I_0\left(\frac{K r}{\sigma^2}\right) u(r)$$

con $u(r)$ gradino unitario, e K che misura la strength (ampiezza) della componente LOS; se $K = 0$ (NLOS) la Rice si riduce alla Rayleigh perchè la I_0 , che è la funzione di Bessel di prima specie e di primo ordine, nello zero vale 1. Tanto più K è grande tanto più mi devo aspettare degradazioni inferiori come prestazioni.

Se il canale è LTV (cioè se si tiene in conto anche l'effetto doppler) si può generalizzare il discorso sostituendo la variabile aleatoria Z con un processo aleatorio $z(t)$, che nelle stesse ipotesi precedenti si può assumere gaussiano:

$$r(t) = \Re \left\{ u(t) e^{j2\pi f_c t} \underbrace{\sum_{n=0}^{L(t)} \alpha_n(t) e^{-j2\pi f_c \tau_n(t)}}_{z(t) \equiv \text{s.a. complessa}} \right\} = \Re \left\{ z(t) u(t) e^{-j2\pi f_c t} \right\}$$

quindi trasmetto $u(t)$ e ricevo $z(t)u(t)$, cioè il canale è selettivo (distorcente) nel tempo (introduce un rumore moltiplicativo $z(t)$).

Sia nel caso LTI che LTV riceviamo comunque il nostro segnale in banda base $u(t)$, e ciò significa che i ritardi introdotti dal canale incidono solo sulle fasi e non sulle ampiezze delle repliche.

1.3.3 Caratterizzazione statistica del fading a banda larga

Ricordiamo che si parla di fading a banda larga quando la durata T dell'impulso che trasmetto è sufficientemente stretta rispetto al ritardo del canale T_M in maniera tale che le repliche non si sovrappongono. T rappresenta la slot temporale in cui trasmetto un certo numero di bit, ovvero un certo segnale; se la durata del segnale ricevuto non è più T ma $T+T_M$ avrò il fenomeno dell'ISI (Interferenza intersimbolica), cioè il segnale trasmesso in una certa slot temporale va ad interessare segnali associati a slot temporali differenti.

Se il fading è a banda larga i ritardi introdotti dai vari percorsi incidono anche sui segnali in banda base (ovvero sulle ampiezze di $u(t)$) e non solo sulle fasi. In tal caso per caratterizzare statisticamente il fading si ricorre alle statistiche della risposta impulsiva del canale $h(t, \tau)$, che è una famiglia di processi aleatori complessi. In particolare, la funzione di autocorrelazione statistica (o meglio di mutua correlazione), che è per definizione una media statistica, se il canale è stazionario in senso lato dipende solo dalla differenza tra $t+\Delta t$ e t , e se gli scatterer sono incorrelati è nulla per valori di τ differenti:

$$r_h(t, t + \Delta t, \tau_1, \tau_2) = E[h^*(t, \tau_1)h(t + \Delta t, \tau_2)] = r_h(\Delta t, \tau_1, \tau_2) = \Gamma_h(\Delta t, \tau) \delta(\tau)$$

dove $\tau = \tau_1 - \tau_2$. Δt è la separazione temporale tra gli istanti in cui si va a misurare il canale (ovvero la separazione temporale dei campioni in uscita dal canale), ed è legato alla tempo-varianza del canale, e τ è il ritardo associato agli scatterer ed è legato al multipath.

Nota: Si ricordi che la funzione di autocorrelazione di un segnale (integrale del segnale per la sua versione ritardata) rappresenta il grado di similitudine tra due versioni del segnale; se è nulla le due versioni del segnale sono uguali, e quindi non c'è dispersione temporale, --> non c'è ISI. E che due processi sono incorrelati se hanno covarianza nulla, nel qual caso la media statistica si fattorizza nel prodotto delle medie.

La trasformata di Fourier della funzione di autocorrelazione rispetto alla variabile Δt , ovvero lo spettro di densità:

$$S_h(\tau, \rho) = F\{r_h(\tau, \Delta t)\}_{\Delta t}$$

è detta **funzione di scattering** e descrive la potenza media in uscita dal canale in funzione del multipath τ e della frequenza doppler ρ (che è il duale di Δt , cioè della tempo-varianza), che è la variazione di frequenza corrispondente allo spostamento del Rx (maggiore è la velocità del Rx maggiore sarà ρ), ovvero ρ è lo shift di frequenza dovuto al doppler, a causa del quale trasmettiamo un tono a frequenza f_c e ritorna un tono a frequenza $f_c + \rho$.

Da queste due funzioni ($S_h(\tau, \rho)$ e $r_h(\tau, \Delta t)$) possiamo ricavare 4 parametri sintetici che consentono di valutare l'entità del multipath e del doppler sia nel tempo che in frequenza, e quindi di classificare i canali con fading. In particolare la $S_h(\tau, \rho)$ o la $r_h(\tau, \Delta t)$ consentono di valutare il *tempo di multipath*, la *banda di coerenza*, la *banda doppler* e il *tempo di coerenza*, i primi due consentono di valutare il multipath e gli ultimi due il doppler.

Nelle seguenti relazioni si tenga presente che quando poniamo $\Delta t=0$ ci concentriamo sul multipath (trascurando il doppler), quando poniamo $\Delta f=0$ ci concentriamo invece sul doppler.

Multipath

Per ricavare i parametri di valutazione del multipath, ovvero T_M e B_c , ragiono sulla risposta impulsiva. Ponendo $\Delta t=0$ nell'espressione ricavata della funzione di autocorrelazione si ha, nel tempo, :

$$r_h(\tau, \Delta t)|_{\Delta t=0} = r_h(\tau) \text{ PDP} \Rightarrow T_M = \min T : r_h(\tau) \approx 0 \text{ se } \tau \geq T$$

che ci consente di descrivere il tempo di multipath come il minimo valore del periodo di simbolo per cui il Power Delay Profile è nullo (ovvero, per $T_M < T$ non c'è dispersione, dunque T_M è il min T per avere dispersione temporale (multipath)).

Nel dominio della frequenza si ha:

$$F[r_h(\tau)] = r_H(\Delta f, \Delta t)|_{\Delta t=0} = r_H(\Delta f) \Rightarrow B_c = \frac{1}{T_M} = \min \Delta f : r_H(\Delta f) = 0$$

$$\forall \Delta f : |\Delta f| \geq \frac{B_c}{2}$$

che definisce la banda di coerenza come la minima separazione tra le componenti spettrali affinché il canale si comporti selettivamente in frequenza (ovvero sia distorsivo); ovvero le componenti spettrali separate di $\Delta f \geq B_c$ sono incorrelate, cioè saranno trattate diversamente dal canale (che quindi introduce distorsione).

Dunque confrontando i parametri del segnale che trasmettiamo con quelli appena ricavati possiamo dire che:

- $T=1/B < T_M=1/B_c$ --> fading selettivo in frequenza (cioè c'è multipath, c'è ISI)
- $T=1/B > T_M=1/B_c$ --> fading piatto in frequenza (no dispersione, no ISI)

I due parametri introdotti consentono quindi di valutare il multipath sia nel tempo che in frequenza: il tempo di multipath è il massimo ritardo introdotto dal canale e consente di stabilire se esso è dispersivo nel tempo, la banda di coerenza è l'intervallo di frequenze in cui il canale è non distorto (non selettivo) in frequenza. Alla dispersione nel tempo corrisponde selettività in frequenza.

Nota: Si ricordi che a causa del multipath al Rx giungono più versioni (repliche) del segnale Tx, ognuna delle quali subisce un certo ritardo di propagazione dipendente dal cammino seguito; il maggiore di questi ritardi è detto tempo di multipath, o di dispersione. Qui lo abbiamo definito usando il Power Delay Profile $r_H(\tau)$, che rappresenta il contributo alla potenza media degli scatterer che introducono un ritardo τ , indipendentemente dalla frequenza spettrale, ovvero posto $\Delta t=0$; ponendo $\Delta t=0$ stiamo di fatto calcolando l'autocorrelazione nell'origine ovvero la potenza media. La banda di coerenza consente di valutare lo stesso fenomeno nel dominio della frequenza, in cui rappresenta la minima separazione frequenziale affinché due sinusoidi che si propagano attraverso il canale sperimentino attenuazioni differenti (indipendenti), ovvero siano trattate dal canale in modo differente; se $\Delta f < B_c$ le due sinusoidi saranno trattate allo stesso modo dal canale, cioè saranno attenuate e sfasate allo stesso modo, altrimenti saranno trattate indipendentemente (cioè fuori dalla B_c il canale si comporta selettivamente).

Doppler

Per ricavare i parametri di valutazione del doppler, ovvero T_c e B_D , ragiono sulla risposta in frequenza (trasformata di F. rispetto a τ (che porta in conto il multipath) della $h(\tau, t)$):

$$F\{h(\tau, t)\}_{\tau} = H(f, t)$$

poiché $h(\tau, t)$ è un p.a. gaussiano, per la linearità della F, anche $H(f, t)$ è un p.a. gaussiano (o meglio una famiglia di processi aleatori al variare di f) che posso caratterizzare con la funzione di autocorrelazione (o meglio di mutua correlazione), la quale se il processo è SSL e gli scatterer sono incorrelati si può scrivere come:

$$r_H(t, t + \Delta t, f_1, f_2) = E[H^*(t, f_1)H(t + \Delta t, f_2)] = r_H(\Delta t, f_1, f_2) = r_H(\Delta t, \Delta f)$$

dove $\Delta f = f_2 - f_1$, e porta in conto il multipath, mentre Δt porta in conto la tempo varianza.

Ponendo $\Delta f=0$ si ha, nel dominio del tempo, :

$$r_H(\Delta f, \Delta t) \Big|_{\Delta f=0} = r_H(\Delta t) \Rightarrow T_c = \min \Delta t : r_H(\Delta t) \approx 0$$

che definisce il tempo di coerenza come la minima separazione temporale affinché il canale si comporti selettivamente nel tempo (cioè sia tempo variante); ovvero i campioni separati di $\Delta t \geq T_c$ sono incorrelati, cioè saranno trattati diversamente dal canale (che quindi introduce distorsione temporale).

Nel dominio della frequenza si ha:

$$F\{r_H(\Delta f, \Delta t)\}_{\Delta t} = S_H(\Delta f, \rho) \Big|_{\Delta f=0} S_H(\rho) \Rightarrow B_D = \frac{1}{T_c} = \min \rho : S_H(\rho) \approx 0$$

$$\forall |\rho| \geq \frac{B_D}{2}$$

che definisce la banda doppler come la minima frequenza doppler affinché lo spettro doppler sia nullo (cioè, per $\rho < B_D$ non c'è dispersione spettrale, dunque B_D è la minima ρ affinché il canale sia dispersivo in frequenza (doppler)).

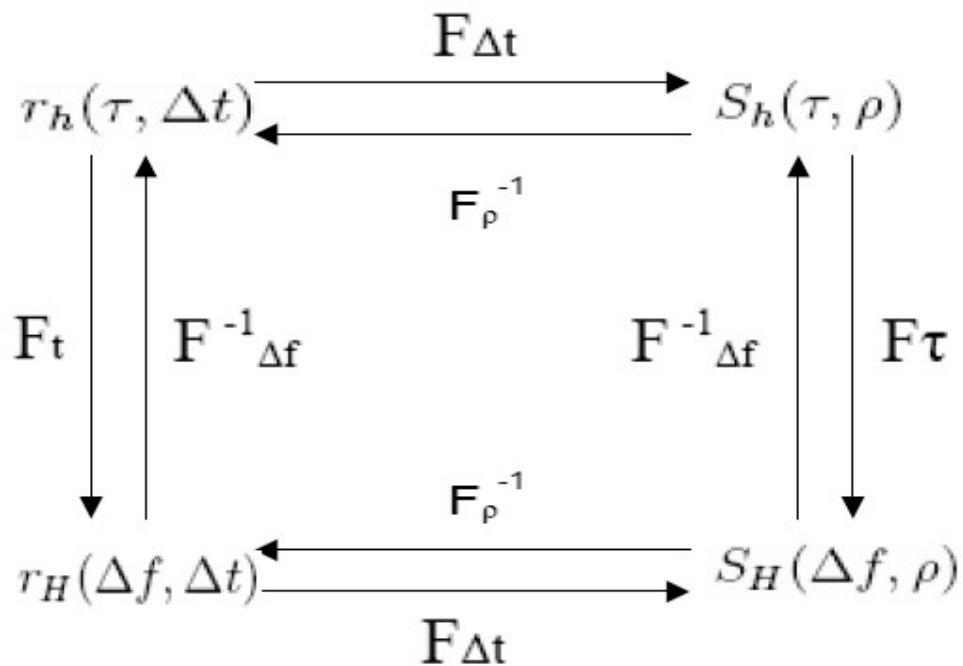
Dunque confrontando i parametri del segnale che trasmettiamo con quelli appena ricavati possiamo dire che:

- $T=1/B < T_c=1/B_D$ --> canale stazionario (fading piatto nel tempo)
- $T=1/B > T_M=1/B_c$ --> canale non stazionario (fading selettivo nel tempo)

I due parametri introdotti consentono quindi di valutare il doppler sia nel tempo che in frequenza: il tempo di coerenza è l'intervallo temporale in cui il canale si può ritenere tempo invariante (non selettivo, non distorcente), la banda doppler è l'intervallo di frequenze in cui il canale è non dispersivo in frequenza. Alla dispersione in frequenza corrisponde selettività nel tempo.

Nota: Si ricordi che a causa dell'effetto doppler le repliche che giungono al Rx presentano shift doppler differenti; il più grande di questi spostamenti è detto banda doppler. Il suo reciproco, il tempo di coerenza, rappresenta l'intervallo temporale in cui il canale è non selettivo (cioè stazionario), ovvero la minima separazione temporale affinché 2 segnali che si propagano attraverso il canale sperimentino attenuazioni differenti (indipendenti), cioè osservano 2 canali differenti; se $\Delta t < T_c$ allora le 2 repliche subiscono la stessa attenuazione.

Quadro sinottico: legame tra le 4 funzioni considerate



Ognuna delle 4 funzioni considerate (i 4 vertici del quadro della figura seguente) contiene in sé i parametri sintetici per analizzare l'entità del fading, ovvero T_M oppure $B_c=1/T_M$ per caratterizzare il multipath, e B_D oppure $T_c=1/B_D$ per caratterizzare l'effetto doppler. Infatti:

$$r_H(\Delta f, \Delta t) \Big|_{\Delta t=0} = r_H(\Delta f) = F[r_h(\tau)]$$

↪ $B_c=1/T_M$ ↪

e analogamente:

$$S_H(\Delta f, \rho) \Big|_{\Delta f=0} = S_H(\rho) = F\{r_H(\Delta t)\}$$

↪ $B_D=1/T_c$ ↪

I valori tipici dei parametri caratteristici del multipath fading sono:

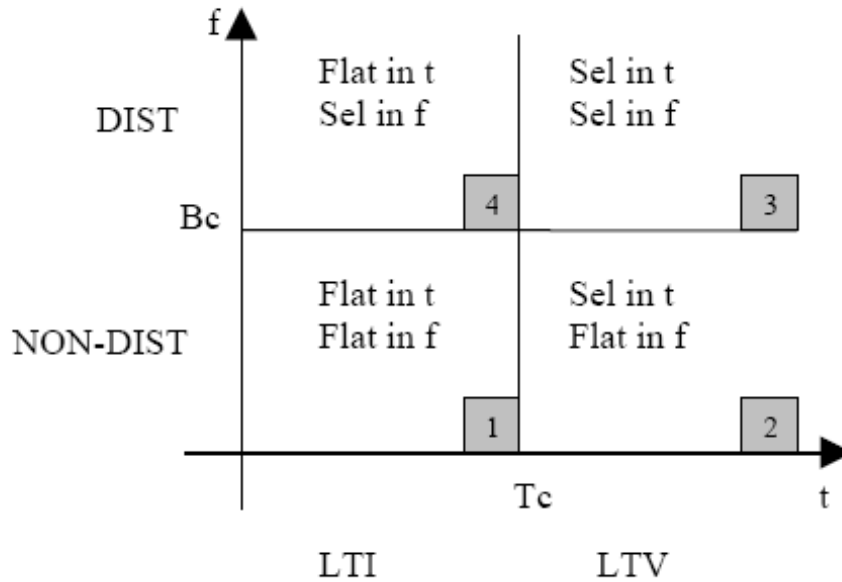
$T_M=1-30$ microsecondi in outdoor (urban), $10-1000$ nanosecondi in indoor;

$B_c=1/T_M= 1- 30$ Mhz in outdoor, $1-100$ Mhz in indoor;

Dunque il problema del multipath è più significativo in ambienti outdoor; ad es. è più significativo nella telefonia cellulare che nel bluetooth.

Classificazione dei canali con fading

A seconda delle relazioni tra i parametri del segnale trasmesso (T, B) e quelli del canale (T_M, B_c, T_c, B_D), il segnale sperimenterà diversi tipi di canali (ovvero di fading). La seguente figura mostra i 4 tipi di canali che si possono avere:



in tale figura usiamo T_c per valutare la tempo-varianza (dovuta al doppler) e B_c per valutare la distorsione in frequenza, ma si possono usare equivalentemente anche gli altri due parametri (T_M e B_D); come si può osservare, se il segnale trasmesso ha durata $T < T_c$ sarà soggetto a fading piatto nel tempo, ovvero tutte le componenti del segnale saranno trattate allo stesso modo dal canale (sono assenti gli effetti della tempo-varianza), altrimenti sarà soggetto a fading selettivo nel tempo, cioè le diverse repliche del segnale T_x saranno trattate dal canale in modo indipendente; e se il segnale T_x ha $B < B_c$ sarà soggetto a fading piatto in frequenza, cioè non verrà distorto dal canale, altrimenti verrà distorto.

Il modello 1 (canale flat-flat) non descrive una situazione realistica e viene usato solo per analisi di prestazioni, i modelli 2 e 3, che tengono conto della tempo-varianza, sono usati per descrivere canali radiomobili terrestri (il 3 si usa per le comunicazioni avioniche, in cui le velocità in gioco sono molto più elevate), il modello 4 descrive canali a banda limitata (che sono stazionari) caratterizzati da ISI.

1.4 contromisure per il fading

In presenza di fading l'SNR deve essere grande per abbassare il BER (percentuale di bit errati in ricezione), e ciò richiede di aumentare molto la potenza, il che è improponibile; in assenza di fading invece basta un piccolo incremento dell'SNR per avere sensibili miglioramenti; infatti la $P(e)$ è proporzionale a e^{-SNR} in assenza di fading, e a $1/SNR$ in presenza di fading.

Nel caso del fading a lungo termine (Shadow fading) come contromisura abbiamo considerato essenzialmente il margine di fading, ovvero si aumenta di una certa aliquota la potenza trasmessa per coprire una certa percentuale di ricevitori. Col fading a breve termine questa contromisura è improponibile perchè bisognerebbe aumentare enormemente la potenza in trasmissione.

Le soluzioni realistiche che si possono adottare sono invece le seguenti:

- **Interleaving**: poichè la maggior parte delle tecniche di codifica di canale introdotte permette di rilevare e correggere pochi errori isolati ma non burst di errori come nel caso del fading, si usa l'interleaving ovvero il flusso informativo da trasmettere viene interallacciato ad altri flussi informativi in modo che le ostilità del fading siano distribuite tra più flussi informativi ritornando al caso di pochi errori isolati per ogni flusso anzichè burst di errori sul singolo flusso.
- **Tecniche di diversità**: trasmetto più volte il segnale. In pratica si trasmette la stessa informazione su più canali (ridondanza).
- **Tecniche di controllo di errore (codifica)**.
- **Antenne direzionali**: con le antenne direzionali si hanno benefici sui guadagni e quindi sull'aliquota di potenza aggiuntiva.
- **Sistemi MIMO**: si riferiscono sostanzialmente alla diversità spaziale cioè a più antenne in trasmissione e/o più antenne in ricezione (Multiple Input Multiple Output).

La seguente tabella mostra i problemi che comportano i vari tipi di fading e i provvedimenti per mitigarli:

Table 2.6 Radio Channel Effects on Performance and Techniques to Improve Performance

Issue	Performance Affected	Mitigation Technique
Shadow fading	Received signal strength	Fade margin—Increase transmit power or decrease cell size
Fast fading	Bit error rate Packet error rate	Error control coding Interleaving Frequency hopping Diversity
Multipath delay spread	ISI and irreducible error rates	Equalization DS-spread spectrum OFDM Directional antennas

Focalizziamo l'attenzione sul multipath delay spread: in questo caso siamo in condizioni di fading a banda larga ($T_M \gg T_u$) cioè c'è dispersione temporale e dunque ISI. Per combattere l'ISI posso fare un'egualizzazione del canale, ma l'egualizzazione prevede la conoscenza del canale ed è dunque necessaria dapprima un'operazione di identificazione del canale (che è molto difficile se il canale è fortemente tempo variante). Si preferisce quindi reagire con tecniche di modulazione multiportante (OFDM) o con tecniche DSSS che allargano la banda e fanno in modo che la durata temporale sia minore o infine con antenne direzionali.

Capitolo 2

Tecniche di trasmissione per le W-LAN

Fino ad ora abbiamo visto i modelli di canale wireless e l'ostilità di tale canale. Ora ci occuperemo delle tecniche di modulazione in grado di controbattere gli effetti degradanti del canale. Si ricordi che la modulazione è l'operazione che traspone l'info da trasmettere in una delle possibili forme d'onda (fisiche), per poterla trasferire sul canale radio.

2.1 Generalità

Un sistema di modulazione è qualitativamente soddisfacente se consente di ottenere basse $P(e)$ usando bassi livelli di potenza in Tx, occupa poca banda, è robusto rispetto al fading e all'interferenza a banda stretta (dovuta ad altri sistemi che operano nella stessa banda), ed è poco complesso e quindi facilmente realizzabile. La scelta del sistema da utilizzare nella situazione di interesse si basa principalmente su due parametri, l'efficienza in banda e l'efficienza in potenza.

Efficienza in banda (o in frequenza):

L'efficienza in frequenza è il rapporto tra la velocità di trasmissione e la banda impegnata (dal segnale trasmesso):

$$\text{efficienza in frequenza} = \frac{\text{bit/sec (trasmessi)}}{\text{Hertz}}$$

e indica la capacità di un sistema di modulazione di allocare dati in una porzione limitata di banda.

Efficienza in potenza:

L'efficienza in potenza indica la potenza spesa per una fissata prestazione (BER bit error rate) e per una fissata banda impegnata, e indica la capacità dello schema di modulazione di conservare la fedeltà del segnale Tx con bassi livelli di potenza. E' definito come il rapporto tra l'energia associata ad un bit e la densità spettrale di potenza del rumore, E_b/N_0 . E' un parametro particolarmente importante nelle reti wireless, in quanto le apparecchiature sono tipicamente alimentate a batteria, la cui durata dipende proprio da questo parametro.

Tecniche di modulazione a modulo costante:

La tecnica di modulazione adottata influenza anche la tolleranza alla presenza di multipath, che è una realtà sempre presente nella trasmissione wireless. Le tecniche di modulazione a modulo costante sono modulazioni in cui l'informazione è associata alla fase e dunque l'ampiezza è costante. Ne sono esempi le tecniche QPSK, BPSK, FSK, mentre le tecniche PAM, QAM, in cui l'informazione è associata proprio all'ampiezza, non sono una tecniche a modulo costante.

Queste tecniche di modulazione sono da preferirsi innanzitutto perchè la maggior parte delle apparecchiature mobili utilizzano nella sezione radio amplificatori fortemente non lineari e dunque se utilizziamo una modulazione lineare come la PAM, in cui associo l'informazione all'ampiezza del segnale, quando passiamo attraverso dispositivi non lineari perdiamo l'informazione. Dunque è necessario che il segnale da amplificare abbia inviluppo costante. Un altro motivo per cui le tecniche a modulo costante sono attraenti è che se usiamo una tale tecnica e in ricezione riceviamo un segnale a modulo non costante vuol dire che il canale ha introdotto distorsione. Per recuperare il modulo costante, si possono utilizzare degli appositi algoritmi.

2.2 Tecniche di modulazione

Nelle W-LAN le tecniche di modulazione utilizzate sono:

1. Tecniche di modulazione ad impulso (Infrared- IR);
2. A spettro diffuso (Spread Spectrum Technology). Opera nella banda radio ed è una soluzione piu vecchia;
3. Tecniche multicarrier (OFDM). Utilizzate nell 802.11 a,g, consentono di raggiungere velocità di 100 Mbps e combattono meglio il multipath;

Descriveremo prima le tecniche di trasmissione in banda base (IR e UWB), poi ci occuperemo delle tecniche a spettro diffuso (FH e DS) e delle tecniche di trasmissione in banda traslata (OFDM).

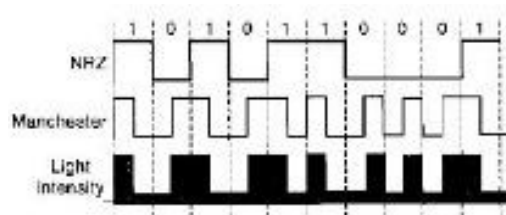
2.3 Trasmissione in banda base

2.3.1 Tecniche di modulazione ad impulso (Infrared- IR)

Per capire queste tecniche facciamo riferimento alla Codifica di linea Manchester, che è utilizzata nelle WLAN che utilizzano la tecnologia Infrared.

Poichè la sincronizzazione tra Tx e Rx è basata sulla commutazione da 0 ad 1 e da 1 a 0, se trasmettiamo troppi bit 0 o troppi bit 1 consecutivi non ci saranno commutazioni e avrò problemi sulla sincronizzazione; la Codifica di Manchester cerca di evitare questi problemi.

Tale codifica opera nel seguente modo:



la stringa binaria NRZ (NON RETURN ZERO), che rappresenta il segnale in banda-base cioè quello ancora non codificato in cui si susseguono più 1 o 0 consecutivi, è codificata in accordo al codice di Manchester: ci sarà una transizione per ogni simbolo binario (cioè in ogni intervallo di bit vi è una transizione), ovvero se devo trasmettere un 1 si ha una commutazione 1->0 all'inizio dell'intervallo di simbolo, mentre se devo trasmettere uno 0 si ha una commutazione 0->1 alla fine dell'intervallo di simbolo; in tal modo anche se abbiamo molti bit consecutivi dello stesso segno la sincronizzazione è garantita.

Il TX genera una intensità luminosa in accordo al segnale codificato e in RX un fotodiode (sensibile all'intensità luminosa trasmessa) rivela il segnale.

Le tecniche in banda base ad impulso si classificano in:

- **Pulse Amplitude Modulation (PAM):** info associata all'ampiezza dell'impulso.
- **Pulse Position Modulation (PPM):** si usano più impulsi per simbolo (per risparmiare potenza) posizionati all'inizio dell'intervallo di segnalazione se si deve Tx un bit 1 e al centro se si deve Tx un bit 0; il ricevitore conosce la corrispondenza tra posizione degli impulsi e bit trasmessi perchè c'è sempre una fase preliminare di learning in cui Tx ed Rx si accordano sul sincronismo. La codifica cambia anche a seconda della velocità che si vuole ottenere: ad 1 Mbps si considerano simboli a 4 bit per cui servono 16 segnali (impulsi), mentre a 2 Mbps si considerano simboli a 2 bit e servono 4 segnali. IEEE 802.11 IR specifica uno strato fisico per alte velocità che usa il canale IR ricorrendo alla PPM.

2.3.2 Tecniche di modulazione UWB (Ultra Wide Band)

Sono tecniche di modulazione ad impulso in cui si trasmettono impulsi di durata molto piccola con potenze molto ridotte. Lo spettro è molto ampio (alcuni GHz) ma il livello spettrale molto basso (cioè la potenza è distribuita su un ampio range di frequenze), e quindi lo spettro è assimilabile allo spettro del rumore rendendone possibile la convivenza con altre reti nella stessa banda (Overlay Systems). Le tecniche Ultra Wide-Band sono recentemente considerate nelle applicazioni indoor per i loro vantaggi:

- *Basse potenze in gioco*: va bene soprattutto nell'ottica delle apparecchiature mobili. (Lo svantaggio, però, è che si hanno raggi di copertura piccoli).
- *Trasmettitori e Ricevitori semplici*: operano in banda base (lo spettro degli impulsi è lo spettro in banda base).
- *Elevate velocità di trasmissione*.
- *Compatibilità con sistemi radio esistenti*: lo spettro del segnale UWB è visto dagli altri sistemi come lo spettro di un rumore e quindi è garantita la convivenza con le altre tecniche di modulazione (paradigma overlay) .

2.4 Tecniche Spread-Spectrum

Le tecniche SS cercano di usare più banda possibile per contrastare il fading; sono state introdotte nelle W-LAN per garantire tolleranza nei confronti dell'interferenza a banda stretta (eventualmente intenzionale: Jamming) dovuta ad altri sistemi che operano nello stesso spettro, e al multipath cioè alla selettività in frequenza (la quale porta a ridurre il bit-rate), in modo da consentire la coesistenza nella stessa banda di più sistemi (overlay systems). A tale scopo le con tecniche SS si distribuisce la potenza del segnale su una banda 2W molto più ampia di quella originaria 2B in modo da avere livelli di PSD molto più bassi (la potenza è l'area sottesa dalla densità spettrale di potenza che si abbassa se spaliamo la potenza su una banda più ampia), ottenendo così uno spettro noise-like. Il segnale che otteniamo a valle dell'operazione di spread è un segnale noise-like (simile al rumore) e chi non possiede la sequenza di spreading usata in Tx lo vede rumore e non ha possibilità di recuperare il segnale originario.

A differenza dell'UWB, nello SS la banda è più contenuta per cui più segnali SS condividono lo spettro. Un vantaggio dell'UWB è che le apparecchiature in Tx ed Rx sono particolarmente semplici; ma le potenze in gioco sono più basse e quindi UWB ha raggi di copertura inferiori alle tecniche SS.

Esistono due possibili tecniche SS:

1. **Frequency Hopping (FHSS)**
2. **Direct Sequence (DSSS)**

2.4.1 Frequency-Hopping Spread-Spectrum (FHSS)

Tale tecnica consiste nel fatto che la frequenza portante salta (hop), ad intervalli di tempo prefissati, da una frequenza ad un'altra in accordo ad un pattern (pseudo-random) noto solo al ricevitore. L'espansione dello spettro si ottiene quindi modulando il segnale in banda base su un certo numero di frequenze portanti.

I parametri caratteristici del FH sono:

- La durata della slot temporale, ovvero per quanto tempo usiamo una frequenza del pattern, detta dwell time e si indica con T_c ;
- Il numero delle slot temporali, ovvero il numero di frequenze del pattern che possiamo utilizzare, che è dato dal rapporto tra la banda disponibile $2W$ e la banda del segnale modulato convenzionalmente $2B$:

$$\#slot = N = \frac{2W}{2B}$$

La FHSS può essere classificata in due modi in base alla relazione tra T_c e il periodo di simbolo T :

- **Slow FHSS** : $T_c = KT$ dove T è la durata di un bit (in un hop (cioè con la stessa portante) si trasmettono KT simboli); ovvero trasmetto k bit con la stessa frequenza;
- **Fast FHSS** : $T_c = T/K$ (in un intervallo di bit k hops); cioè lo stesso bit è spalmato su diverse (k) frequenze; è usata in apparecchiature militari.

In altri termini, se la velocità di cambiamento della frequenza portante (canale) è molto maggiore della velocità di simbolo si parla di FH veloce, altrimenti di FH lento.

Con la tecnica Fast FHSS l'intervallo di segnalazione è suddiviso in k slot temporali in ognuna delle quali è scelta (in maniera pseudo-random in un insieme di N valori) la frequenza della portante che si manterrà costante in tutta la slot, auspicando che quando si salta da una frequenza all'altra il canale abbia cambiato stato in maniera da risolvere i problemi di fading e di interferenza introdotti.

Nota: Nel FH la banda è narrow (stretta, limitata) nel singolo slot temporale e wide (larga) nell'intero canale.

Vantaggi del FH (rispetto alle tecniche tradizionali):

Innanzitutto la tecnica FHSS non ha alcuna influenza sulle prestazioni del RX in presenza del solo rumore additivo (rumore termico) perchè il livello di densità spettrale del rumore è lo stesso (costante) in ogni slot di frequenza.

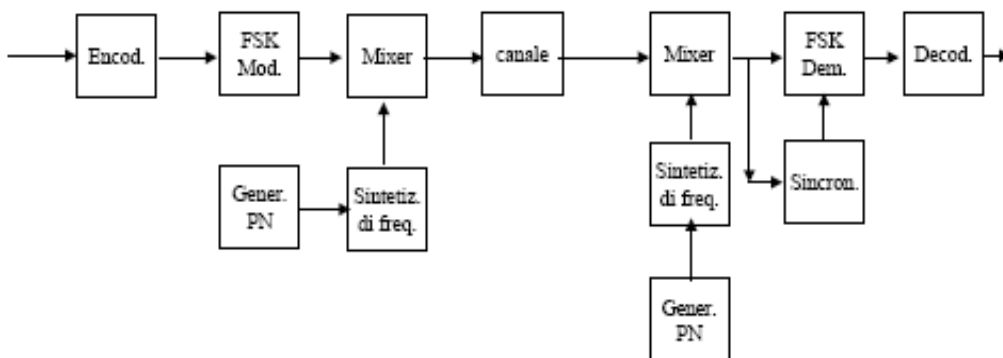
Il FHSS consente inoltre di limitare i fade (attenuazioni) e l'interferenza a banda stretta. Per quanto riguarda i fade, poiché tipicamente ci sono range di frequenze in cui il canale si comporta meglio e altri in cui si comporta peggio (il segnale è più attenuato), ovvero in certe bande di frequenze il segnale sarà molto più attenuato che in altre, un sistema tradizionale che opera con una banda "cattiva", cioè in cui l'attenuazione è molto forte, darà prestazioni insoddisfacenti (perchè lavorerà sempre in quella banda); un sistema che invece utilizza la tecnica FHSS presenterà un miglioramento perchè userà quella banda solo per una percentuale di tempo ridotta, quando la sequenza pseudo-random prevede di utilizzarla; quindi un sistema che utilizza la tecnica FHSS presenterà un miglioramento perchè il fade interesserà solo un certo numero di slot frequenziali. Per le stesse ragioni il sistema FHSS è più tollerante all'interferenza a banda stretta, infatti se in una certa banda c'è un sistema di TLC che impegna in maniera fissa quella frequenza, utilizzando la tecnica FH l'interferenza a banda stretta non interesserà tutta la trasmissione ma solo la parte che avviene con quella particolare frequenza del pattern a disposizione.

Inoltre lo spread spectrum consente di usare una tecnica CDM anziché FDM per la suddivisione del canale e ciò evita la pianificazione delle frequenze per evitare l'interferenza.

La tecnica FHSS consente anche di risolvere il problema dei pacchetti ricevuti errati o persi; infatti, se i pacchetti sono ritrasmessi sulla stessa slot frequenziale (trasmissione tradizionale a banda stretta) essi saranno di nuovo corrotti, mentre se utilizziamo la tecnica FHSS verosimilmente la ritrasmissione utilizzerà una slot differente e quindi potrà dare esito positivo.

Schema a blocchi completo del FHSS:

Prima di commentare il seguente schema, osserviamo che si preferisce la modulazione FSK piuttosto che la PSK perchè essa evita problemi dovuti alla sincronizzazione, infatti la FSK garantisce una ricezione non coerente (cioè non è necessario recuperare il sincronismo di fase tra Tx ed Rx), che è più semplice, e nelle W-LAN l'enfasi è proprio sulla semplicità. Diffondere l'energia associata ad un simbolo su più salti comporta una penalizzazione del SNR perchè i contributi sono combinati in maniera non coerente. FH evita dunque i requisiti stringenti di sincronizzazione, imposti invece dal DS, ma se andiamo oltre i 2 Mbit/sec va in crisi perchè la tolleranza al rumore e al multipath non è più adeguata.



In trasmissione, l'encoder effettua l'eventuale codifica di sorgente; i simboli binari (indipendenti) vanno a pilotare il modulatore FSK, che produrrà un impulso sinusoidale ad una certa frequenza per il simbolo 0 e ad una altra frequenza (diversa) per il simbolo 1; sul segnale così modulato viene effettuato lo spreading (blocchi Gen.PN, Sintetizzatore, e Mixer): il blocco Generatore PN genera una sequenza PN (ovvero un pattern di simboli binari) in accordo alla quale il sintetizzatore di frequenza detta il pattern dei salti di frequenza; le frequenze random così generate vengono moltiplicate dal mixer per il segnale in uscita dal modulatore FSK in modo da cambiarne la frequenza (Dal punto di vista funzionale il mixer è un moltiplicatore --> cambio la frequenza del segnale). Il segnale in banda traslata in uscita dal mixer va in ingresso al canale, il quale non ha più la banda stretta del segnale ma ha la banda espansa (è un canale SS).

In tal modo occupo più banda ma abbasso il livello spettrale (a parità di potenza) e quindi la banda può essere condivisa da più sistemi a banda stretta; inoltre maschero il mio segnale FSK, in quanto chi non conosce la sequenza PN vede il segnale come rumore.

In ricezione si effettuano le operazioni inverse: de-spreading seguita da una demodulazione FSK e poi dalla decodifica; inoltre c'è una sincronizzazione di simbolo per sapere dove inizia e dove finisce un simbolo.

Specifica FHSS in IEEE 802.11

Nella versione base di 802.11 FHSS specifica 78 hops (frequenze), separati da 1 MHz, divisi in tre gruppi di 26 hops, ciascuno corrispondente ai numeri di canale (0, 3, 6, . . .), (1, 4, 7, . . .) e (2, 5, 8, . . .). Queste scelte sono disponibili per tre differenti sistemi che possono coesistere nella stessa area geografica senza alcuna collisione tra gli hops (la stazione TX e quella RX si accordano su una sequenza di salti).

I dati si trasmettono utilizzando una modulazione 2-GFSK o 4-GFSK per ottenere una velocità di 1 o 2 Mbps. La tecnica GFSK è un FSK ottenuta filtrando il segnale dati con un filtro gaussiano in modo da eliminare le discontinuità (che fa aumentare la banda) e, quindi, limitare la banda impegnata (il filtro gaussiano fa in modo di non allargare troppo la banda, che nel FH è limitata nei singoli slot). Si assicurano spettri confinati in una banda di 1 MHz sia per la velocità di 1 Mbps che per quella di 2Mbps. La massima velocità con FHSS è 2 Mbps: a velocità superiori la tecnica GFSK diventa sensibile al rumore e ad altri disturbi (multipath); le tecniche DSSS hanno proprio il compito di ridurre questi effetti.

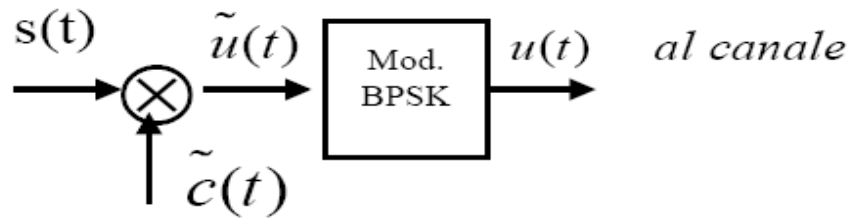
Riepilogando, le specifiche FHSS per 802.11 sono:

1. 3 set frequenze (hopping), 26 sequenze/set;
2. 78 canali (USA ed EU), 23 canali (Giappone) da 1MHz;
3. Modulazione: 2-GFSK (1 Mb/s), 4-GFSK (2 Mb/s); nelle due modulazioni l'intervallo di simbolo, e quindi la banda impegnata, è lo stesso solo che nel primo caso un segnale trasporta 1 bit mentre nel secondo caso 2 bit;
4. Hopping rate: 2.5 hop/s (slow hopping) durata della hop 400msec;
5. Bit scrambling $s(z) = z^7 + z^4 + 1$ (DC blocking/whitening);
6. Frequenza di campionamento: 1Msps.

2.4.2 Direct-Sequence Spread-Spectrum (DSSS)

La tecnica DS consuma più potenza ed è più complessa rispetto al FH; in particolare la frequenza di campionamento è molto più elevata (44000 campioni al secondo contro i 2000 campioni al secondo di FH) perchè il ricevitore DS richiede più banda (22Mhz rispetto ai 2 Mhz di FH-->è 11 volte maggiore), inoltre la sincronizzazione richiede più tempo in quanto occorre sincronizzarsi anche con la portante (e non solo sui simboli come nel FH), cioè si usa una modulazione coerente.

Nel DS, come mostra la seguente figura, il segnale da Tx (considero gli equivalenti passabasso dei segnali) viene moltiplicato per una opportuna sequenza di spreading che ne riduce il periodo (e quindi ne aumenta la banda) prima di essere trasmesso sul canale.



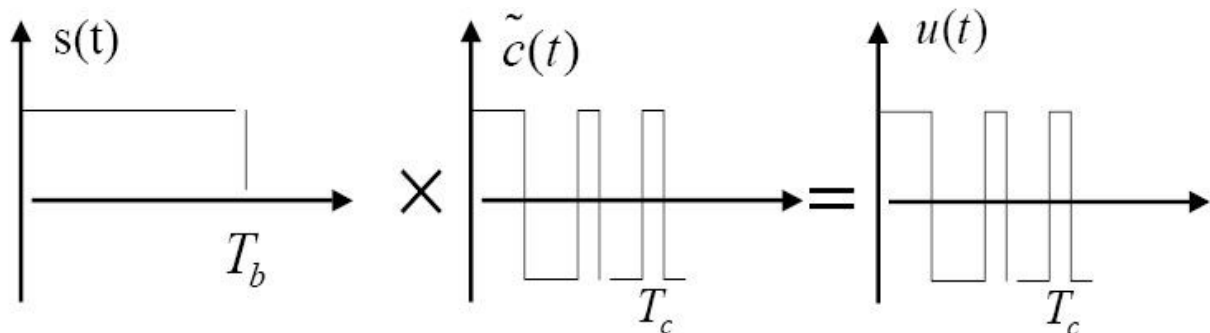
In particolare $s(t)$, sequenza di bit che voglio trasmettere, può essere rappresentato come una somma di impulsi (rect di durata T_b , dove T_b è la durata di un bit) di ampiezza a_k :

$$s(t) = \sum_{k=-\infty}^{\infty} a_k \text{rect}\left(\frac{t - kT - T_b/2}{T_b}\right) \quad a_k \in \{-1, +1\}$$

tale segnale viene moltiplicato per il segnale $\tilde{c}(t)$ periodico di periodo $T_c = NT_b$ (ovvero per un segnale molto più veloce):

$$\tilde{c}(t) = \text{rept}_{T_b} \left[\sum_{m=1}^N b_m c(t - mT_c - T_c/2) \right]$$

in modo da trasmettere un segnale $\tilde{u}(t)$ con un periodo molto più breve (e quindi di banda maggiore).



In tal modo modifichiamo la fase del segnale (stiamo usando una BPSK) ogni $T_c = T_b/N$ secondi anziché ogni T_b secondi (nel tempo T_b trasmettiamo T_c impulsi); poiché T_c è N volte minore della durata di bit T_b , la banda impegnata dal segnale che ha subito lo spreading sarà N volte maggiore (si ricordi che ad una compressione nel tempo corrisponde un allargamento in frequenza), ovvero $\mathbf{W} = \mathbf{N} \times \mathbf{B}$; dove N è detto fattore di allargamento.

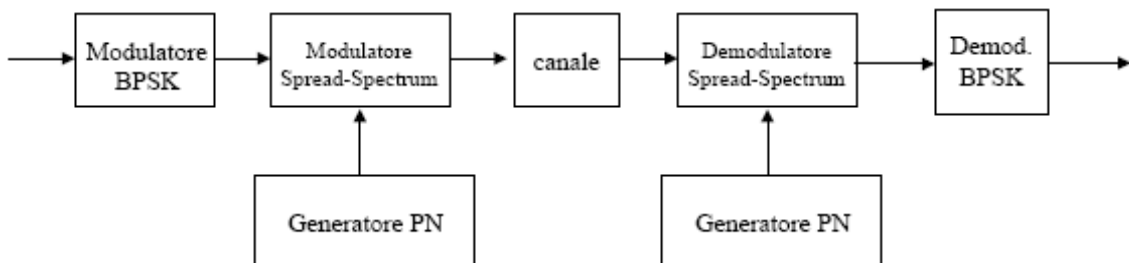
Poiché il ricevitore usa l'autocorrelazione per sincronizzarsi, occorre allargare la banda con un treno di impulsi con autocorrelazione quanto più possibile impulsiva, in quanto il picco dell'autocorrelazione indica l'inizio della sequenza trasmessa; se l'autocorrelazione è larga il ricevitore può sincronizzarsi su una posizione diversa dal primo simbolo della sequenza (ad es. potrebbe considerare il terzo simbolo come inizio della sequenza). Inoltre si tenga presente che più T_c è piccolo più ho tolleranza al multipath.

Specifiche DSSS di 802.11: IEEE 802.11 usa, come sequenza di spreading per la tecnica DSSS, il codice di Baker (sono codici con ottime proprietà di autocorrelazione) di lunghezza $N=11$ e $\underline{b} = (1, 1, 1, -1, -1, -1, 1, -1, -1, 1, -1)$. Ovvero ogni bit di ingresso è associato ad $N=11$ chips a valori binari 1 e -1:

- $1 \rightarrow 1, 1, 1, -1, -1, -1, 1, -1, -1, 1, -1$
- $0 \rightarrow -1, -1, -1, 1, 1, 1, -1, 1, 1, -1, 1$

quindi si usano 2 parole codice complementari a sue valori.

Schema di Tx e Rx del DSSS:



Il segnale $s(t) \times \tilde{c}(t)$ modula in ampiezza la sinusoide prodotta dall'oscillatore locale del modulatore BPSK $A_c \cos(2\pi f_c t)$ ottenendo, così, il segnale BPSK:

$$u(t) = s(t)\tilde{c}(t)A_c \cos 2\pi f_c t = A_c \cos[2\pi f_c t + \theta(t)]$$

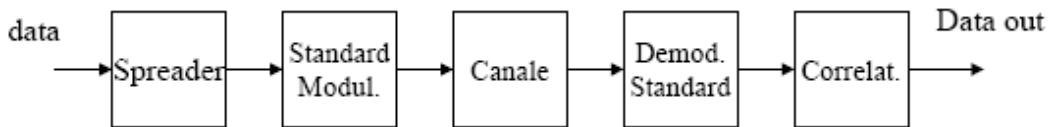
che è modulato dalla sequenza di spreading e non più dai bit di info; $s(t)$ e $\tilde{c}(t)$ possono assumere solo valore ± 1 e $\theta(t)$ rappresenta il segno positivo o negativo del coseno, cioè:

$$\theta(t) = \begin{cases} 0 & \text{se } s(t)\tilde{c}(t) = 1 \\ \pi & \text{se } s(t)\tilde{c}(t) = -1 \end{cases}$$

ovvero il mod BPSK, che fa una modulazione di fase binaria, associa al bit 0 una portante con fase nulla (e ampiezza 1) e al bit 1 la stessa portante sfasata di π (e ampiezza -1).

Lo spreading viene effettuato da un generatore PN, che genera la sequenza pseudo-rumorosa (per esempio la sequenza di Baker: in tal caso nell'intervallo T_b devo generare 11 impulsi; cioè nello stesso intervallo in cui prima Tx un simbolo binario ora ne trasmetto 11), e dal modulatore SS, che a livello funzionale è un moltiplicatore (che è un sistema lineare). Dopo lo spreading la banda è dell'ordine di $1/T_c$, cioè si è allargata di N volte ($N = T_b/T_c$). In ricezione faccio l'operazione di de-spreading, cioè moltiplico il segnale ricevuto per $\tilde{c}(t)$ ($\tilde{c}(t) \times \tilde{c}(t) = 1$), in modo da eliminare l'effetto dello spreading, e vado al demodulatore B-PSK.

Alternativamente fare lo spreading direttamente in digitale:



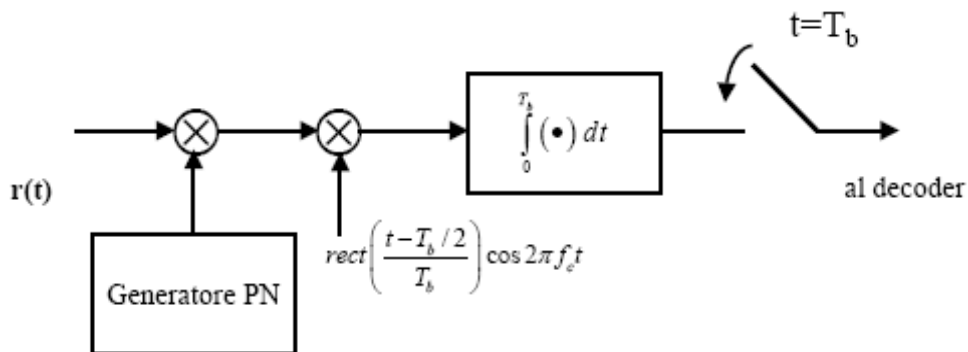
cioè ad esempio ogni bit di ingresso è associato ad N chips (con Baker N=11):

- 1 → 1, 1, 1, -1, -1, -1, 1, -1, -1, 1, -1
- 0 → -1, -1, -1, 1, 1, 1, -1, 1, 1, -1, 1

questa sequenza va a pilotare un modulatore tradizionale, al quale, quindi, i simboli binari arrivano con un rate N/T_b e non $1/T_b$. In ricezione faccio l'operazione duale: ho prima il demodulatore standard, che opera con una banda N/T_b , dopodichè effettuo la correlazione (con la sequenza di spreading che ho utilizzato in Tx).

Capacità di soppressione NBI:

Il DS consente di limitare l'interferenza a banda stretta, infatti in ricezione si ha:



$r(t)=u(t)+i(t)$ è il segnale che ricevo a meno del rumore termico (che non viene attenuato dalla tecnica DS perchè ha un livello spettrale costante), che viene sottoposto al de-spreading (ovvero moltiplicato per $c(t)$) per sincronizzarsi con i simboli, e poi decorrelato con una demodulazione coerente (moltiplico per un coseno) per sincronizzarsi con la portante. Se in ricezione ho anche una interferenza a banda stretta $i(t)$, all'ingresso del correlatore (ovvero a valle dello spreading) avrò il segnale:

$$r(t)c(t) = (u(t) + i(t))c(t) = c^2(t)s(t)A_c \cos 2\pi f_c t + i(t)c(t) = s(t)A_c \cos 2\pi f_c t + i(t)c(t)$$

se assumiamo che:

$$i(t) = A_I \cos 2\pi f_I t$$

la potenza media associata ad $i(t)$ prima dello spreading è:

$$P_I = A_I^2/2$$

dopo lo spreading (in Tx) la PSD di $i(t)$ è $P_I/2W$, cioè la potenza iniziale è spalmata su una banda $2W$; poiché il demodulato usa un filtro (passabasso (l'integrale in figura)) con banda pari a quella del segnale utile, ovvero $2B = 2W/N$, la potenza media dell'interferenza all'uscita del demodulatore è:

$$\frac{P_I}{2W} 2B = \frac{P_I}{N}$$

cioè si è ridotta di N volte rispetto a quella di ingresso. Per cui conviene fare N più grande possibile. All'uscita del ricevitore a correlazione (o il filtro adattato) avrò il segnale trasmesso $s(t)$ che viene campionato ogni T_b secondi.

Dunque con la tecnica DS risolviamo il problema dell'interferenza a banda stretta tanto meglio quanto più N (processing gain) è elevato. Questo è importante perchè stiamo considerando sistemi overlay e ricordiamo che le tecniche W-LAN usano bande non regolamentate dove c'è, quindi, notevole congestione. Per risolvere il problema occorre diffondere lo spettro del segnale di informazione usando uno speciale codice: in ricezione solo chi conosce l'effettiva sequenza di spreading, cioè il codice riuscirà a riconvertire il segnale.

Ricevitore RAKE

In un sistema DSSS un ricevitore che, sfruttando la diversità temporale insita nel fenomeno del multipath, combina in maniera ottima (cioè min la $P(e)$ o, in presenza di AWGN, max l'SNR) le repliche ricevute per migliorare l'affidabilità della decisione è detto RAKE. A differenza dei normali ricevitori, che reiettano le repliche NLoS, il ricevitore RAKE usa anche le altre repliche per migliorare le prestazioni. A tale scopo il ricevitore RAKE deve identificare il canale, cioè i ritardi di multipath introdotti dal canale, per combinare in maniera costruttiva le repliche.

Tale ricevitore correla le repliche ricevute e poi le combina; il segnale così ottenuto viene poi con una soglia per decidere qual'è il simbolo trasmesso.

2.5 Trasmissione in banda traslata a banda larga

Si usano sostanzialmente 3 tecniche:

1. *Modulazione CCK* (tecnica a singola portante): utilizzata da IEEE 802.11 b nella banda 2.4 GHz;
2. *OFDM* (tecnica multiportante);
3. *Modulazione multisimbolo* (trasmetto k bit anziché 1).

2.5.1 Modulazione CCK

Per aumentare la velocità di trasmissione dei segnali lasciando inalterata la banda impegnata occorre arricchire l'alfabeto delle parole codice; ovvero, anziché associare una parola codice ad un bit, come si fa nel DSSS, si associa una parola codice ad un blocco di un certo numero di bit. A tale scopo si usano i codici polifase complementari (CCK) per fare lo spreading (allargamento della banda). In 802.11b i codici CCK utilizzano chip con valori complessi quaternari ($\pm 1, \pm j$), piuttosto che chip a valori binari reali (± 1), aumentando così il numero di parole codice disponibili (xkè aumenta l'alfabeto dei simboli) e dunque, a parità di banda (ovvero di durata associata al simbolo), aumenta la velocità di TX, perchè nello stesso tempo trasmetto più informazione.

Schema di principio di TX/RX per sistemi CCK:

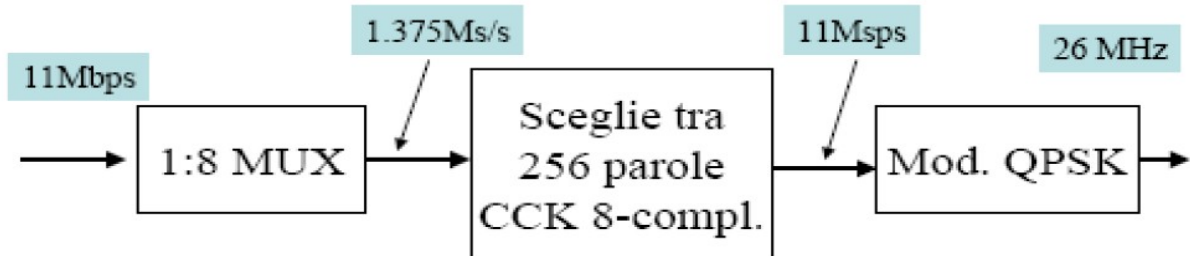
I bit di informazione sono raggruppati con un convertitore serie/parallelo in blocchi da N bit, passando così da una velocità di R_b bit/s a R_b/N bpcchi/s; ad ognuno di questi blocchi il codificatore associa una parola codice di k chips (simboli) appartenenti ad un alfabeto L-ario. Ogni chip della parola codice viene poi trasmesso sequenzialmente, con una velocità di R_b chips/s, sul canale con una modulazione L-aria senza memoria (ad es. con una L-PSK).

In IEEE 802.11b, per trasmettere a 11Mbps a parità di banda di 802.11 base (cioè a 22Mhz, o 26Mhz se si considera la banda lorda), si sceglie $N=8$, $k=8$ e $L=4$; ovvero, si raggruppano i bit in blocchi da 8 a ciascuno dei quali viene associata una parola codice di 8 chip a valori complessi quaternari. Si hanno quindi $L^k = 4^8 = 65.536$ possibili parole codice, tra le quali si scelgono le $2^N=2^8=256$ necessarie a codificare blocchi di 8 bit, possibilmente ortogonali (cioè non interferenti). In tal modo la banda occupata è sempre di 22Mhz; infatti, tenendo presente che 1 Mcps corrisponde ad una banda di 2MHz, si ha:

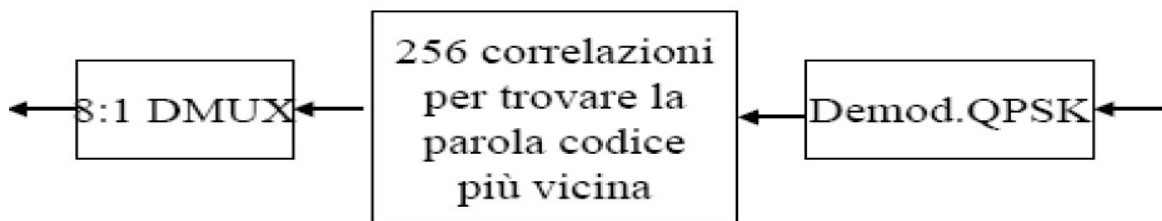
11 Mbps ---> 11/8 = 1375 Mblocchi/s ---> 1375x10⁶x8=11 Mcps ---> 22 Mhz.

Le seguenti figure mostrano gli schemi di modulatore e demodulatore per IEEE 802.11b;

Modulatore



Demodulatore



Vediamo ora, sempre con riferimento a 802.11b, come opera il codificatore.

Codificatore:

Ho 8 bit in ingresso che si possono vedere come quattro coppie da 2 bit, ciascuna delle quali specifica una delle possibili fasi (4 coppie --> 4 fasi), che possono essere:

$$\phi_1, \phi_2, \phi_3, \phi_4 \in \left\{ 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2} \right\} \quad \text{oppure} \quad e^{j\Phi_i} \in \{ \pm 1, \pm j \}$$

Tali fasi mi consentono di costruire le 256 parole codice necessarie a codificare i blocchi di 8 bit in ingresso. La generica parola codice sarà:

$$c \equiv \left(e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_4)}, e^{j(\phi_1+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_3)}, e^{j(\phi_1+\phi_3)}, e^{j(\phi_1+\phi_2)}, e^{j\phi_1} \right)$$

Ogni chip nella parola codice è funzione di un certo numero di fasi.

Osserviamo che, in questa parola codice, Φ_1 è presente in tutti gli otto chip, quindi posso semplificare il codificatore usando una regola di mapping (metto in evidenza Φ_1) che definisce solo 64 parole codice, anziché 256, che poi subiranno una rotazione di fase su tutti i chip (4 possibili rotazioni).

La seguente tabella mostra la regola di codifica dello standard CCK:

Dibit	Parametro di fase
(d_1, d_0)	φ_1
(d_3, d_2)	φ_2
(d_5, d_4)	φ_3
(d_7, d_6)	φ_4

Dibit (d_{i+1}, d_i)	Parametro di fase
00	0
01	π
10	$\pi/2$
11	$-\pi/2$

Esempio: $d_7, \dots, d_0 = 10110101 \Rightarrow \varphi_1, \varphi_2, \varphi_3, \varphi_4 = \pi, \pi, -\frac{\pi}{2}, \frac{\pi}{2} \Rightarrow$
 $c \equiv (1, -1, j, j, -j, j, -1, -1)$

l'esempio in figura mostra come viene costruita, in maniera algoritmica, una parola codice; \underline{d} è la sequenza da codificare (va letta da dx verso sx) e c è la parola codice costruita applicando la regola in tabella. Tale regola consente di realizzare una soluzione compatibile con 802.11 base.

La tabella seguente, invece, mostra che delle 256 parole codice (costruite con la regola precedente) solo 148 sono ortogonali. Quindi se voglio utilizzare CCK a 11Mbps, e quindi mi servono 256 parole codice, dovrò attingere alle parole codice non ortogonali. Se si dimezza la velocità di trasmissione, ovvero se penso di utilizzare CCK con 5.5 Mbps servono solo $2^4 = 16$ parole codice (perchè sto dimezzando da 8 a 4 il blocco di ingresso), e quindi posso sceglierle tutte ortogonali.

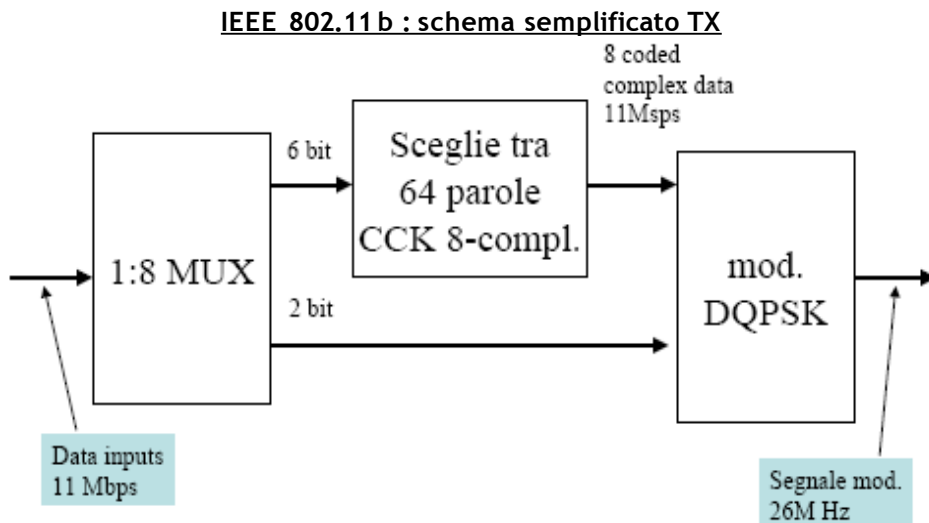
Cross-correlazione tra le parole codice

Magnitude	number
256	4
128	24
64	48
32	32
0	148

Soluzione compatibile con IEEE 802.11:

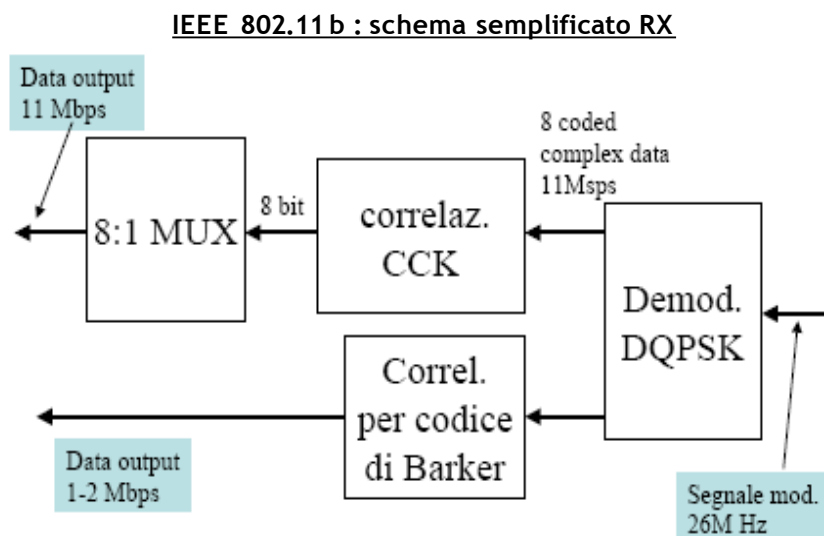
Per poter fornire differenti velocità di trasmissione: 1, 2, 5.5 e 11 Mbps, in 802.11b sono previste due tipi di intestazione (contenente l'info sulla velocità) per la frame dello strato fisico. Tale informazione è necessaria per facilitare il lavoro del ricevitore e rendere 802.11b compatibile con 802.11 base (che opera a velocità 1 e 2 Mbps).

Per questa soluzione gli schemi (semplificati) di Tx e Rx sono i seguenti:



I simboli binari da trasmettere sono raggruppati in blocchi da 6+2 (xkè Φ_1 è comune a tutti i blocchi) --> ad ognuno dei blocchi da 6 (definiscono le fasi Φ_2, Φ_3, Φ_4) è associata una delle $2^6 = 64$ parole codice di dispersione ad 8 chip, ognuna delle quali subisce una rotazione in base al valore di Φ_1 (codificato dai rimanenti 2 bit).

Si usa una modulazione differenziale (DQPSK) per avere una demodulazione non coerente.



Il ricevitore è costituito di due parti (una per 802.11 base e l'altra per 802.11b); dal campo data rate della frame PLCP si riconosce quale ramo utilizzare:

- ricevitore per DSSS con il codice di Baker (802.11)
- ricevitore per CCK (802.11b)

Per trasmettere a 5.5 Mbps si raggruppano blocchi di 4 bits (anziché 8): due bit sono ancora usati per scegliere tra 4 parole codice ortogonali a 8 chips quaternari e due bit sono usati per ruotare tali parole.

2.5.2 Tecniche di modulazione multiportante - OFDM

Per aumentare ulteriormente la velocità di trasmissione ($> 11\text{Mbps}$), fermo restando la banda, occorre passare a modulazioni multiportanti, che dividono il flusso informativo in più parti trasmesse, in parallelo, su portanti differenti. Se ad esempio voglio trasmettere a 10 Mbps , che richiederebbe una banda $> B_c$ --> trasmetto, in parallelo, dieci flussi da 1 Mbps su dieci portanti diverse; ognuno di questi flussi, avendo ridotto di dieci volte la banda, darà meno problemi per la selettività in frequenza, cioè avrà $B < B_c$.

Si tenga presente che l'OFDM non è una tecnica a divisione di frequenza, in quanto gli spettri si possono anche sovrapporre e dunque si risparmia in banda rispetto a FDM (OFDM si realizza con tecniche digitali mentre FDM con tecniche analogiche), e la discriminazione delle portanti viene fatta in base alle loro proprietà di ortogonalità. La tecnica OFDM (orthogonal frequency division multiplexing) è diventata popolare da pochi anni grazie alla possibilità di una realizzazione in digitale semplice via IFFT/FFT.

Vantaggi:

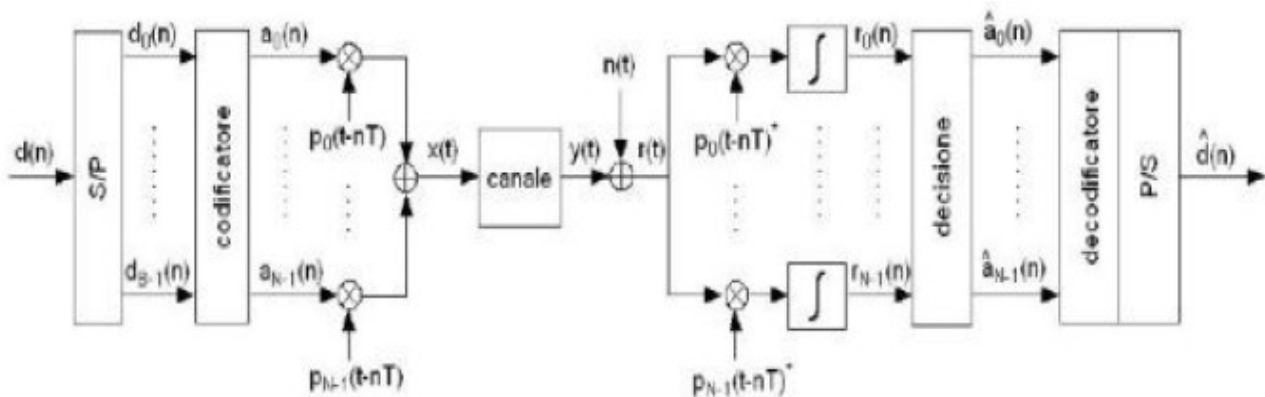
In OFDM il flusso dati ad elevata velocità (elevata banda) si suddivide in flussi a bassa velocità, ognuno trasportato, in parallelo, da una sottoportante diversa; in tal modo invece di modulare una singola portante a R_s bps si usano N portanti modulate a R_s/N bps. Se N è sufficientemente grande, la durata di simbolo è sufficientemente grande da poter, eventualmente, trascurare il multipath spread e quindi semplificare l'egualizzazione (xkè devo egualizzare una banda N volte minore). Oltre ad essere multiportante, OFDM è anche *Multirate*, cioè il Tx adatta il rate di trasmissione alla qualità del canale (aumentando il numero di sottoportanti utilizzate), e *Multisimbolo*, cioè si usano alfabeti multisimbolo per aumentare il bit-rate a parità di banda.

Svantaggi di una tecnica multiportante:

- **Elevato fattore di cresta (Potenza di picco/Potenza media):** Il segnale multiportante è la somma di molti contributi indipendenti nessuno dei quali sovrasta gli altri, dando luogo ad una distribuzione delle ampiezze gaussiana. In Tx l'auspicio è di usare tecniche che richiedono una potenza media costante (ovvero tecniche a involuppo costante), quindi quanto più $P_p \simeq P_m$ tanto meglio è, ma questo non accade nel caso delle tecniche multiportante.
- **Sensibilità agli errori di sincronizzazione:** oltre all'ISI, dovuta alla banda finita del canale, si ha anche interferenza tra le portanti (ICI), dovuta agli offset di frequenza.

Schema di principio di OFDM:

Lo schema di massima del sistema OFDM prevede l'unione di due blocchi, un moltiplicatore e un integratore, che effettua un prodotto scalare<-->correlazione. La decisione può essere presa usando il criterio MAP oppure ML (min P(e)). Ipotizzando che i simboli binari $d(n)$ da trasmettere siano indipendenti ed equiprobabili, ovvero di prendere le decisioni sui simboli l'uno indipendentemente dall'altro, lo schema di massima del sistema OFDM può essere schematizzato nel seguente modo:



Il flusso informativo $d(n)$, trasmesso nella n -sima slot temporale, viene suddiviso in blocchi (sottoflussi) di B bit, a ciascuno dei quali il codificatore associa un simbolo di una parola codice $a(n)$ di lunghezza $N \leq B$, e ognuno di questi simboli viene impresso su una portante differente, $p_k(t-nT)$, tramite un banco di moltiplicatori; a valle di questo banco di moltiplicatori ho il segnale trasmesso nella n -sima slot temporale (dato dalla somma dei segnali $f_n(t)$ in uscita dai moltiplicatori); la somma di questi segnali trasmessi su tutto l'arco temporale, $x(t)$, viene trasmessa sul canale. Ad es., se $d(n)$ è composto da 12 bit, viene suddiviso in 3 blocchi da 4 bit ciascuno dei quali viene codificato con un dei simboli di una parola codice $a(n)$ composta da 3 simboli (ovviamente ogni simbolo sarà composto da un certo numero di bit), ciascuno dei quali sarà trasportato da una portante differente.

In ricezione, il segnale ricevuto viene decorrelato con le N portanti; se le portanti sono ortogonali (cioè se non c'è ICI) l'uscita di ogni integratore sarà influenzata soltanto dal simbolo associato a quella portante; il decisore stabilisce poi, a minima distanza, quale parola codice è stata trasmessa; tale parola viene infine decodificata per recuperare i sottoflussi che vengono riconvertiti, tramite il convertitore P/S, nel flusso trasmesso.

Condizione di ortogonalità:

Per essere ortogonali le portanti devono avere la forma di impulsi rettangolari di durata T modulati da un fasore a frequenza multipla di 1/T. Ovvero, in frequenza, devono essere spaziate tra loro di 1/T. Infatti:

Il segnale che trasmetto nella slot temporale n-esima sarà la somma dei singoli segnali a valle dei modulatori:

$$f_n(t) = \underbrace{\sum_{i=0}^{N-1} a_i(n)p_i(t - nT)}_{\text{Frame multicanale}} \quad nT \leq t \leq (n+1)T$$

Il segnale complessivo trasmesso (dopo la moltiplicazione) per tutto l'arco temporale è:

$$x(t) = \sum_{n=-\infty}^{\infty} f_n(t) = \sum_{n=-\infty}^{\infty} \left[\sum_{i=0}^{N-1} a_i(n)p_i(t - nT) \right]$$

In ricezione tale segnale deve essere correlato (prodotto scalare) con le N portanti; l'uscita dell'i-esimo correlatore è:

$$\begin{aligned} r_i(n) &= \int_{-\infty}^{\infty} x(t)p_i^*(t - nT)dt = \int_{-\infty}^{\infty} \sum_{m=-\infty}^{\infty} \left[\sum_{k=0}^{N-1} a_k(m)p_k(t - mT) \right] p_i^*(t - nT)dt = \\ &= \sum_{m=-\infty}^{\infty} \sum_{k=0}^{N-1} a_k(m) \int_{-\infty}^{\infty} p_k(t - mT)p_i^*(t - nT)dt \end{aligned}$$

dove, l'integrale finale rappresenta una funzione di mutua correlazione tra due portanti (k-esima e i-esima) osservate in due intervalli diversi (m ed n). Il mio auspicio è che, poichè sto correlando in riferimento all'intervallo [nT, (n+1)T], l'effetto della doppia sommatoria dovrebbe essere solo il simbolo a_i(n). Affinchè ciò avvenga l'integrale deve valere zero per ogni k ≠ i (ovvero per portanti differenti) e per ogni m ≠ n (ovvero slot differenti). In tal caso si ha infatti:

$$\int_{-\infty}^{\infty} p_k(t - mT)p_i^*(t - nT)dt = \langle p_k(t - mT), p_i(t - nT) \rangle = \delta_{k-i}\delta_{m-n} \Rightarrow r_i(n) = a_i(n)$$

Se scelgo come portanti impulsi rettangolari p_i di durata T (devo modulare il generico simbolo in T), moltiplicati per un fasore a frequenza f_i (nel dominio della frequenza traslo di f_i), i loro spettri saranno delle sinc centrate in f_i; per cui devo scegliere le f_i in modo tale che le portanti siano tra loro ortogonali; e ciò avviene quando la separazione tra le portanti f_k - f_i è un multiplo di 1/T. Infatti, eseguendo i calcoli si ha che:

$$\begin{aligned}
 p_i(t) &= \frac{1}{\sqrt{T}} \text{rect}\left(\frac{t - T/2}{T}\right) e^{j2\pi f_i t} \Rightarrow \langle p_k(t - mT), p_i(t - nT) \rangle = \\
 &= \frac{1}{T} \int_{-\infty}^{\infty} \text{rect}\left(\frac{t - T/2 - mT}{T}\right) e^{j2\pi f_k(t - mT)} \text{rect}\left(\frac{t - T/2 - nT}{T}\right) e^{-j2\pi f_i(t - nT)} dt \\
 &= \frac{1}{T} \delta_{n-m} e^{-j2\pi(f_k - f_i)nT} \underbrace{\int_{nT}^{(n+1)T} e^{-j2\pi(f_k - f_i)t} dt}_{=0 \text{ per } f_i \neq f_k} = \delta_{k-i} \delta_{m-n}
 \end{aligned}$$

essendo il fasore un segnale periodico basta che $f_k - f_i$ sia un multiplo di $1/T$ affinché l'integrale vada a 0; ovvero:

$$\begin{aligned}
 \text{Se } f_i &= l/T : \langle p_k(t - mT), p_i(t - nT) \rangle = \delta_{k-l} \delta_{m-n} \\
 l = 1 &\Rightarrow \text{minima spaziatura in frequenza tra le portanti} \Rightarrow \text{parlo di OFDM.}
 \end{aligned}$$

Spettro di densità di potenza per OFDM:

Il segnale trasmesso $x(t)$ è un segnale aleatorio per cui per calcolarne la PSD devo fare la trasformata di Fourier della sua funzione di autocorrelazione media. Se ipotizzo che la sorgente è senza memoria, cioè i simboli sono indipendenti ed identicamente distribuiti, si ha che:

$$E[a_i(n)a_k^*(m)] = \sigma_{a_i}^2 \delta_{k-i} \delta_{m-n}$$

dove $\sigma_{a_i}^2$ se $k = i$ ed $m = n$ rappresenta il valore quadratico medio. Quindi la funzione di autocorrelazione statistica di $x(t)$ è:

$$r_x(t, \tau) = E[x(t)x^*(t - \tau)] = \sum_{i=0}^{N-1} \sigma_{a_i}^2 \text{rep}\left[p_i(t)p_i^*(t - \tau)\right]$$

ed è periodica di periodo T , per cui $x(t)$ è ciclostazionario, e quindi l'autocorrelazione media (che è la media temporale di quella statistica) è periodica e posso calcolarla evitando l'operazione di limite.

Nota: un segnale aleatorio $x(t)$ che ha una $R_x(t, \tau)$ periodica in t si dice ciclostazionario; se la funzione di autocorrelazione statistica è funzione del solo ritardo il segnale si dice stazionario in senso lato.

Dunque lo spettro di densità di potenza è:

$$S_x(f) = \mathbf{F}\left\{\frac{1}{T} \int_0^T r_x(t, \tau) dt\right\} = \frac{1}{T} \sum_{i=0}^{N-1} \sigma_{a_i}^2 |P_i(f)|^2$$

dove la $P_i(f)$ è la trasformata di $p_i(t)$, cioè di una rect , e quindi è una sinc ; per cui lo spettro del segnale OFDM si può esprimere come somma di sinc^2 traslate tra loro di $1/T$:

$$P_i(f) = \mathbf{F} \left\{ \frac{1}{\sqrt{T}} \text{rect} \left(\frac{t - T/2}{T} \right) e^{j2\pi \frac{i}{T} t} \right\} = \sqrt{T} \text{sinc}(fT - i) e^{-j\pi(fT - i)} \Rightarrow$$

$$S_x(f) = \sum_{i=0}^{N-1} \sigma_{a_i}^2 \text{sinc}^2(fT - i)$$

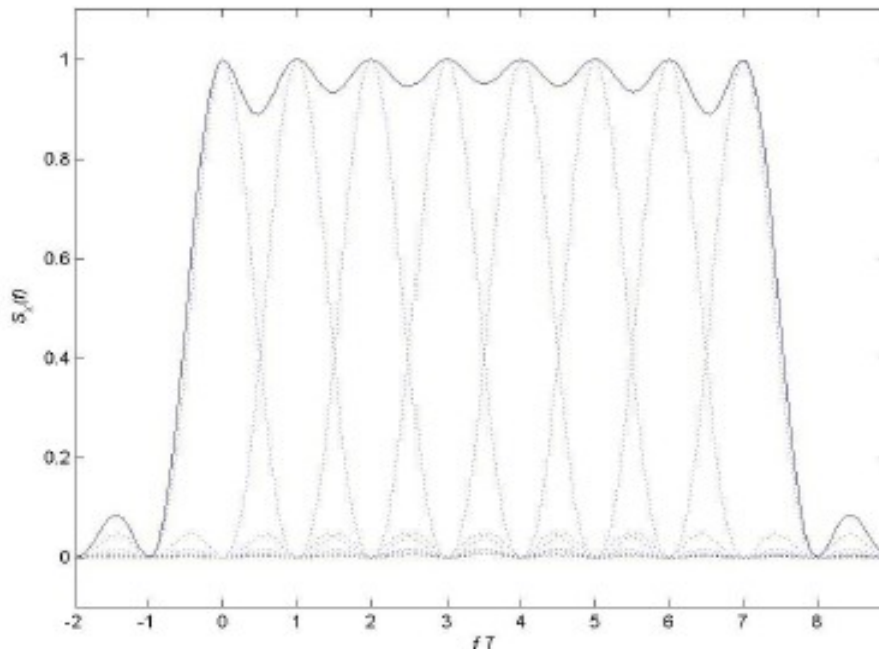
Dunque la banda impegnata (consideriamo la banda null to null, cioè il lobo principale di tutte queste sinc) è:

$$B_T = \frac{N-1}{T} + \frac{2}{T} = \frac{N+1}{T} \approx \frac{N}{T}$$

dove $(N-1)/T$ sono tutte le spaziature tra le portanti interne e $2/T$ è il contributo delle due portanti più esterne. Questo vuol dire che la banda cresce linearmente con N.

Nell'immagine seguente si vede come lo spettro si ottiene componendo le N sinc distanziate di $1/N$. Le sinc si sovrappongono (ho maggiore efficienza spettrale) e ciò sottolinea che si tratta di OFDM e non FDM.

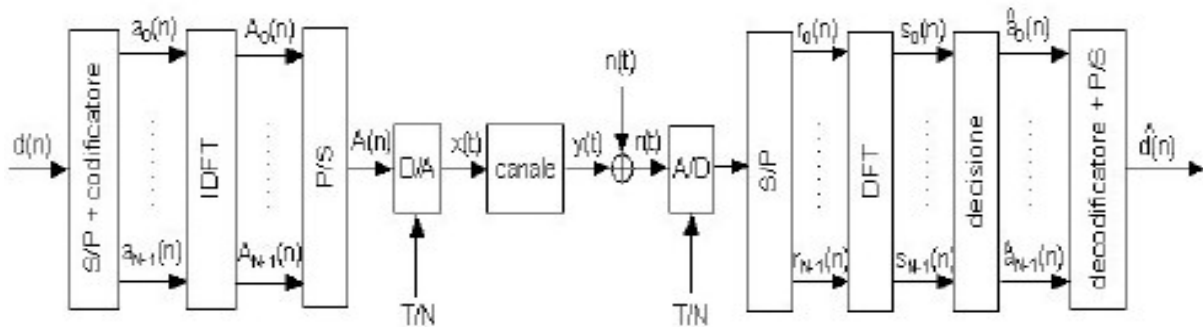
Spettro OFDM



Schema di OFDM digitale:

L'immagine seguente mostra lo schema di OFDM realizzato con tecnica digitale:

Realizzazione TX/RX con IFFT/FFT



L'unica parte analogica dello schema sono i convertitori A/D e D/A. La IDFT viene fatta con l'algoritmo IFFT, che è veloce ed efficiente. La DFT è un mapping che associa ad un blocco di N simboli un altro blocco di N simboli. T/N è la frequenza di campionamento.

Osservazioni conclusive:

OFDM è un'efficace contromisura nei confronti di canali multipath (es. canali radiomobili) selettivi in frequenza. Per aumentare il data rate complessivo, avendo fissato la banda di ogni sottoportante, basta aumentare il numero di portanti (sottocanali), in modo che il data rate sul singolo sottocanale resti costante (così il livello di fading rimane lo stesso). Per evitare la sovrapposizione tra "simboli consecutivi" (ISI) è prevista l'introduzione di un tempo di guardia (ovvero un intervallo di tempo tra un blocco ed un altro), e questo fa abbassare un pò il bit-rate (perchè diminuisce l'efficienza del sistema) visto che nel tempo di guardia non trasmetto. Per poter utilizzare una implementazione con IFFT/FFT al posto del tempo di guardia si introduce un prefisso ciclico, ossia piuttosto che porre dei campioni pari a 0 si utilizzano dei campioni come prefisso (cioè si ritrasmette un certo numero degli ultimi simboli per garantire di poter effettuare la DFT in ricezione).

Trasmissione multisimbolo:

Per aumentare il bit rate a parità di banda si utilizzano modulazioni con un maggior numero di simboli; se cresce il numero di simboli cresce l'efficienza spettrale poichè, a parità di banda (o di durata del simbolo), trasmetto più informazione. Se, fissato il periodo di simbolo e quindi la banda disponibile, uso 4 segnali (es. 4-PSK) piuttosto che 2, raddoppio il bit-rate perchè nello stesso intervallo di tempo trasmetto 2 bit anzichè 1. Segnalazioni efficienti in banda sono quelle con più simboli, per esempio le QAM.

Trasmissione multirate:

Se il terminale mobile è vicino alla stazione radio base (oppure all'access point), posso utilizzare una tecnica di modulazione multisinbolo per aumentare il bit-rate; ma se il terminale si allontana il SNR ricevuto diminuisce e, se si vuole mantenere l'affidabilità (P(e)) ad un certo livello (ovvero per gestire il problema del rumore) bisogna ridurre la velocità di trasmissione (il bit-rate), e quindi l'efficienza spettrale; cioè devo diminuire il numero di segnali della tecnica di modulazione (per modificare il rate di trasmissione si agisce sulla cardinalità dell'alfabeto). Quindi sulla base della stima dell'SNR il trasmettitore deve adattare la velocità di trasmissione a seconda delle condizioni del canale.

OFDM in 802.11a (e in HIPERLAN2):

Per IEEE 802.11a sono previste 64 portanti, di cui 48 per il trasporto dei dati, 4 pilota per la sincronizzazione e 12 virtuali utilizzate per altri scopi.

La durata dei simboli OFDM è di $4\mu s \gg 20nsec$ (delay-spread nelle applicazioni indoor) --> l'effetto multipath è molto ridotto --> egualizzazione di canale molto semplice (filtro FIR del secondo ordine, cioè con una linea di ritardo). Più portanti ci sono più si riduce il bit rate sul singolo flusso, ed aumenta la durata del simbolo fino a diventare sufficientemente grande rispetto alla dispersione del canale. L'intervallo di guardia è 800 nsec (lo usiamo per fare in modo che non ci sia ISI). La banda impegnata è 20MHz. La banda del sottocanal è $20MHz/64 = 312,5 KHz$. Il symbol-rate è di 250 Ksps. La velocità effettiva di trasmissione dipende da quanti bit di ridondanza sono introdotti (per introdurre ridondanza si usa un codice convoluzionale con tasso x/y: ogni x bit di informazione trasmetto y simboli binari), cioè dalla codifica di canale. In 802.11a si usa un codice convoluzionale con tasso $R = 3/4$, ovvero ogni 3 bit di informazione trasmetto 4 simboli binari --> la massima velocità di trasmissione è $78 \times 3/4 = 54Mbps$:

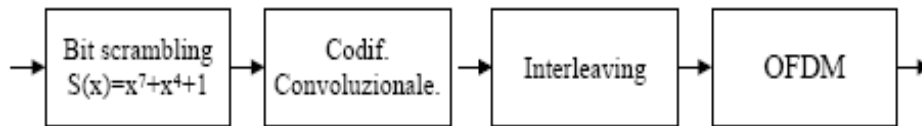
$$R_b/48 = 750 Kbps \text{ per } 16QAM \rightarrow R_b = 36 Mbps$$

$$R_b/48 = 1.125 Mbps \text{ per } 64QAM \rightarrow R_b = 54 Mbps$$

Velocità di TX	6,9,12,16,24,36,48,54Mbps
Modulazione	BPSK, QPSK, 16 QAM, 64QAM
Numero di sottoportanti	64 (48 per dati ,4 pilota,12 virt.)
Spaziatura sottoportanti	312.5 KHz
Durata del simbolo OFDM	4 μsec
Intervallo di guardia	800 nsec
Spaziatura dei canali	20 MHz

MODEM IEEE 802.11a e HIPERLAN 2:

802.11a è uno standard americano ed è data-oriented, HIPERLAN 2 è uno standard europeo ed è voice-oriented, ha quindi una certa attenzione sulla qualità del servizio; a livello fisico non c'è differenza tra i due standard ma ai livelli superiori si.

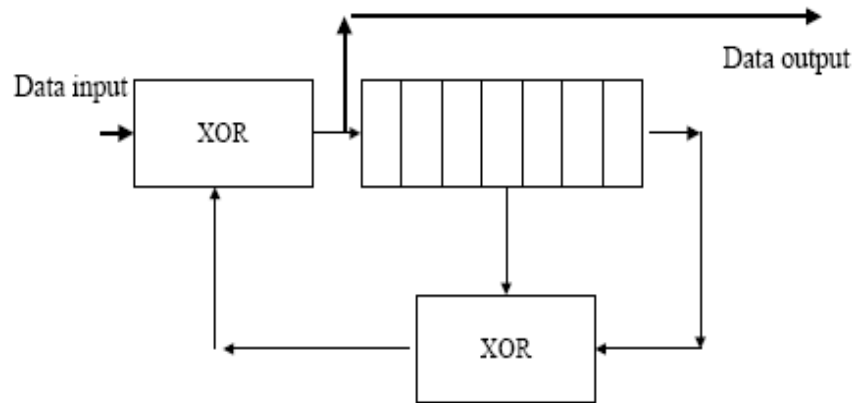


- *bit scrambling* (sbiancamento dei dati): cerca di rendere lo spettro del segnale in ingresso quanto più piatto possibile in modo che i simboli in uscita siano incorrelati.
- *Codificatore convoluzionale*: mappa blocchi di bit in ingresso in simboli di uscita. Se il tasso di codifica è $R = 3/4$, ogni 3 bit che entrano il codificatore restituisce in uscita 4 simboli binari. In tal modo si introduce ridondanza, quindi dipendenza statistica tra i simboli in uscita. Ciò consente in ricezione, di rilevare e correggere errori isolati usando una tecnica FEC. Lo svantaggio della codifica è che, se per 3 simboli binari di info ne trasmetto 4 nello stesso tempo in cui trasmetto 3 simboli, la durata del generico simbolo si accorcia ovvero la banda aumenta; se non voglio pagare in banda devo pagare in bit.rate.
- *Interleaving*: è una contromisura contro burst di errori in ricezione (fading temporale). Se c'è un burst di errori il decodificatore non è più in grado di riconoscere gli errori e correggerli.
- *OFDM*: contromisura per fading selettivo in frequenza (dispersione temporale).

Nota: L'inverso del tasso di codifica rappresenta l'espansione in banda: più introduco ridondanza più riduco la $P(e)$ ma più aumento la banda. Il simbol-rate deve essere sempre 250Ksps xkè così è richiesto dal Tx (fissare il symbol-rate significa fissare la frequenza di campionamento). I tassi di codifica per i codici convoluzionali vanno da 1/2, che è la situazione di max ridondanza e quindi si utilizza quando l'SNR è molto basso <--> sto molto lontano dall'AP --> se la banda è fissata devo ridurre il bit-rate. Con $R = 1/2$, a parità di bit rate, raddoppio la banda, oppure, a parità di banda dimezzo il bit-rate. La situazione più favorevole è $R = 3/4$.

Il bit scrambling si può realizzare con uno schema di questo tipo:

Schema bit scrambling



Il circuito è, in pratica, un divisore (il suo reciproco, usato in ricezione, è un filtro FIR, che è un moltiplicatore): il data input è diviso per il polinomio $S(x)=x^7+x^4+1$ (le potenze indicano le posizioni del registro a scorrimento che sono collegate con le porte xor), e il quoziente è trasmesso come data output.

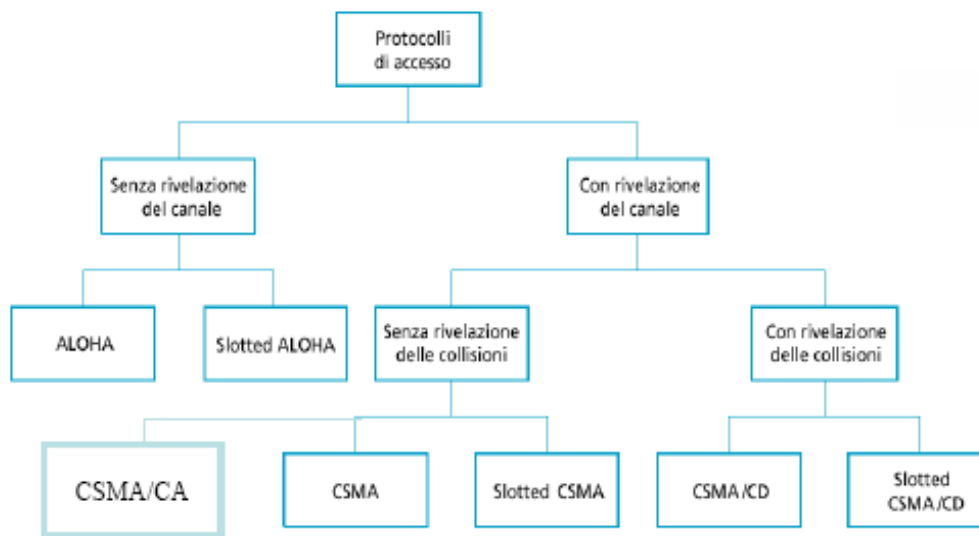
Capitolo 3

Tecniche di accesso per WLAN

Il canale radio è un canale condiviso da una molteplicità di utenti e quindi bisogna regolarne l'accesso per evitare conflitti. Le tecniche di accesso deterministiche come FDMA, TDMA, CDMA assegnano la connessione in maniera statica e ciò dà luogo ad uno spreco di risorse di canale in scenari con traffico intermittente tipici delle WLAN, nelle quali è più conveniente usare tecniche di accesso random, che si distinguono in tecniche ALOHA e tecniche Carrier Sense: con ALOHA non ci si preoccupa di verificare se il canale è occupato o meno prima di trasmettere mentre nel CS prima di trasmettere occorre verificare se il canale è libero.

La figura seguente mostra le diverse caratteristiche su cui si basano le varie tecniche. Nel caso *slotted* sono imposti degli istanti predeterminati in cui cominciare la trasmissione.

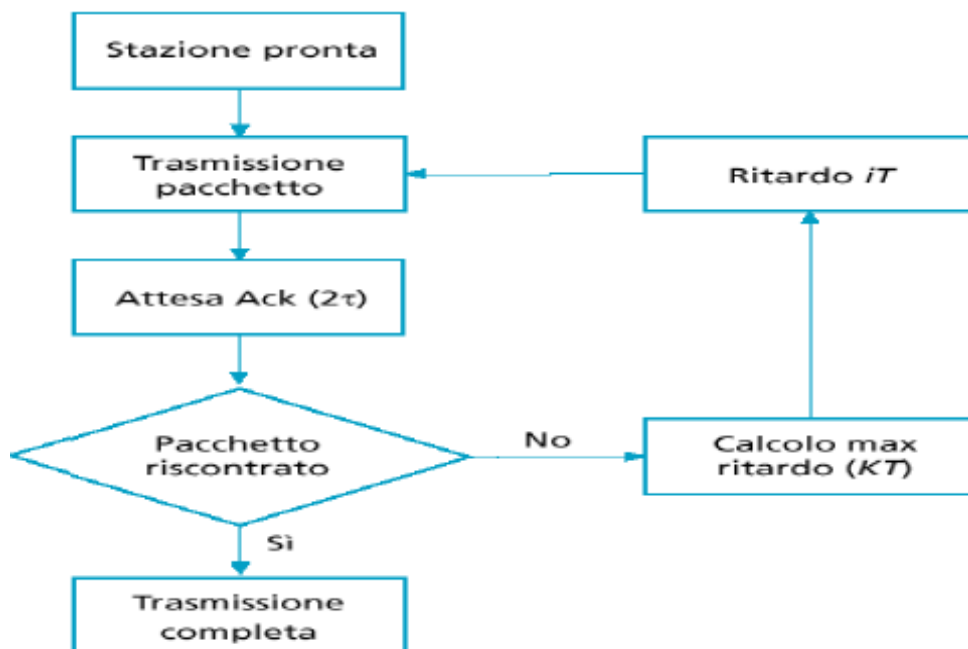
Tassonomia delle tecniche di accesso casuale



Nel wireless siamo interessati a protocolli di accesso con rivelazione del canale ma senza rivelazione delle collisioni, in quanto la rivelazione delle collisioni non è affidabile in un canale wireless, perchè la dinamica dei segnali coinvolti è talmente ampia che non si può rivelare con certezza un'eventuale collisione.

3.1 Protocollo ALOHA

E' un protocollo molto semplice: quando la stazione riceve un pacchetto dagli strati superiori della pila protocollare, lo trasmette immediatamente, e attende il riscontro (ACK) dell'avvenuta ricezione per un tempo pari al round trip time (2τ , dove τ è il tempo di propagazione); se l'ACK arriva entro questo tempo la trasmissione è completata, altrimenti la stazione ritrasmette il pacchetto in una slot scelta a caso in una finestra temporale di dimensione variabile col numero di ritrasmissioni (ovvero di dimensione kT , con $k=n^\circ$ di slot e T =tempo di trasmissione). Se ci sono varie stazioni che devono trasmettere, è improbabile che scelgano tutte la stessa slot i, e quindi è improbabile che si verifichino collisioni.



Il protocollo ALOHA è molto semplice perchè non richiede alcuna sincronizzazione, ovvero alcun coordinamento. In condizioni di traffico intenso, con pacchetti della stessa lunghezza, arrivi random (distribuiti secondo Poisson) e generati da molti terminali, il Troughput (cioè la percentuale di utilizzo del canale) è $\leq 18\%$, cioè per l'82% del tempo il canale è sprecato (--> sto usando male il canale!).

3.1.1 Protocollo ALOHA slotted

Nello scenario ALOHA, se vogliamo aumentare il throughput dobbiamo introdurre un minimo di coordinamento tra le stazioni terminali, cioè fare in modo che le stazioni non trasmettano quando vogliono ma solo in particolari istanti: in questo caso si parla di slotted ALOHA. Per introdurre questa sincronizzazione dobbiamo introdurre una base dei tempi comune, ovvero un *orologio comune* (ad esempio potrei usare il GPS per acquisire l'informazione temporale e garantire il coordinamento tra le stazioni, poichè ogni stazione deve sapere quali sono gli istanti in cui può trasmettere).

La BS invia in broadcasting un segnale di beacon per consentire alle MS (terminali) di sincronizzarsi (cioè c'è una forma di gerarchia). Si dimostra che nelle stesse condizioni considerate per ALOHA puro il throughput massimo si raddoppia (cioè è del 36%).

Nota: Si trasmette solo all'inizio di un dato intervallo. Le slot sono dimensionate in base alla dimensione del pacchetto. Il vantaggio dello slotted è che l'unica collisione può avvenire nell'arco temporale della slot.

3.1.2 Protocollo ALOHA con prenotazione

Esiste un altro tipo di ALOHA, detto ALOHA con prenotazione (*R-ALOHA*), in cui l'ALOHA è combinato con la tecnica TDMA: Il tempo è diviso in intervalli di contesa ed intervalli senza contesa; negli intervalli di contesa le MS gareggiano per accreditarsi gli intervalli privi di contesa (molto più lunghi) in cui inviare i pacchetti da trasmettere.

Esistono varie forme di R-ALOHA; ad esempio l'ALOHA slotted dinamico, che si differenzia per il fatto che le slot di contesa aumentano o diminuiscono a seconda delle condizioni della rete (cioè in base al numero di collisioni).

3.2 Carrier Sensing (CS)

Il carrier sensing prevede che venga ascoltato il canale prima di trasmettere. Affinchè possa operare efficacemente il tempo di propagazione deve essere \ll del tempo di trasmissione, perchè altrimenti possiamo pensare che il canale è libero, anche se è occupato. Se il canale è occupato si ritrasmette con un ritardo random.

Il CS riduce notevolmente le collisioni aumentando così il Troughput. Esso è alla base della tecnica **CSMA** (*Carrier Sense Multiple Access*), detta anche **LBT** (*Listen Bifore Talk*), che è una tecnica decentralizzata (cioè non c'è bisogno di un'infrastruttura di rete), quindi va bene in modo particolare nelle reti ad hoc (cioè reti in cui non prevediamo la presenza di un access point, ovvero in cui non c'è una gerarchia statica).

In IEEE 802.3 (Ethernet (wired)) il sensing del canale è molto semplice: il Rx confronta il livello del segnale presente sul canale con una soglia, se il livello del segnale è inferiore alla soglia il canale viene reputato libero e si può trasmettere. Nelle reti wireless il meccanismo di sensing è più complicato perchè la dinamica del segnale è molto ampia (a causa del Fading) e l'interferenza può mascherare il segnale utile, inoltre l'algoritmo di sensing può essere messo in crisi dal **problema del terminale nascosto**: due MS sono nel raggio di copertura di una terza MS ma tra di loro non c'è link, in tal caso il CSMA non può evitare le collisioni dei pacchetti inviati dai terminali nascosti.

In IEEE 802.11 il problema del terminale nascosto è alleviato con una procedura *4-handshaking*, in cui il terminale, dopo aver fatto il sensing ed abilitato a trasmettere, prima di trasmettere i suoi pacchetti trasmette un pacchetto RTS (contenente il suo identificativo, l'indirizzo del destinatario e la lunghezza del pacchetto dati da Tx) al terminale destinatario, che risponderà con un pacchetto CTS (contenente il suo indirizzo) che, verosimilmente, sarà sentito anche dal terminale nascosto evitando così collisioni.

Esistono numerose variazioni rispetto all'algoritmo base, in particolare si distinguono le tecniche persistenti e non persistenti:

- *Non persistente*: una volta che mi sono reso conto che il canale è libero non trasmetto subito ma aspetto un tempo scelto a caso in una finestra temporale (tempo di back-off).
- *Persistente*: quando sento il canale libero trasmetto subito (1-persistente) o con probabilità p (p -persistente).

Algoritmo di back-off esponenziale:

L'algoritmo di back-off binario esponenziale (BBE) individua il ritardo nella trasmissione allorchè il canale è rilevato busy.

Si fissa una finestra di contesa w la cui dimensione viene raddoppiata (fino ad un valore massimo) ogni volta che viene rilevata una trasmissione fallita. Quando la stazione sente il canale occupato fa partire la sua procedura di back-off, ovvero sceglie a caso in w una slot temporale in cui ritrasmettere (tempo di back-off), cioè quante slot aspettare prima di ritrasmettere, con cui inizializza il suo contatore di back-off, e continua il sensing del canale; ogni volta che sente il canale libero decrementa il suo contatore, ogni volta che lo sente occupato sospende il conteggio e lo riprende quando lo sente di nuovo libero. Quando il contatore si azzerava, se il canale è libero la stazione trasmette il suo pacchetto altrimenti ripete la procedura.

3.2.1 CSMA/CA

E' una tecnica che cerca di evitare che avvengano collisioni. A tale scopo, ogni terminale sceglie a caso, tramite la procedura di back-off, una slot temporale nella finestra di contesa. Quando un terminale può trasmettere però non lo fa subito, ma solo dopo un certo tempo detto Interframe space (IFS). Tramite gli IFS si possono introdurre delle priorità, assegnando IFS di durate differenti.

Un metodo diverso per introdurre le priorità di trasmissione è il metodo Combining, che divide il tempo in intervalli "comb" durante i quali le stazioni alternano ascolto e trasmissione in accordo ad un codice loro assegnato (composto da un certo numero di bit: i bit 1 indicano la Tx e i bit 0 l'ascolto); se durante un periodo di ascolto una stazione sente altre stazioni rinvia la contesa al successivo intervallo comb, se invece non sente altre stazioni termina il suo ciclo (codice) e trasmette il pacchetto.

3.3 Prestazioni delle tecniche di accesso random

Le prestazioni dei metodi ad accesso random sono misurate in termini di:

- **Troughput di canale S:**

$$S = \frac{\text{\#medio di pacchetti TX con successo/sec}}{\text{\#medio di pacchetti che il canale è in grado di TX/sec}} \Rightarrow S \leq 1$$

che indica la percentuale di utilizzo del canale.

- **Ritardo medio D:** tempo medio di attesa prima della Tx con successo normalizzato a T (durata della slot di Tx); è misurato in numero medio di slot di Tx che bisogna aspettare prima della Tx. D è fondamentale nei casi in cui non è accettabile la latenza, come ad esempio nelle Tx multimediali.
- **Traffico G:**

$$G = \frac{\text{\#medio di pacchetti in arrivo/sec}}{\text{\#medio di pacchetti TX/sec}} = \frac{\text{\#medio di pacchetti in arrivo/sec}}{1/\text{tempo medio per la Tx di un pacchetto}}$$

Il traffico si misura in *Erlang*: 1 Erlang = numero medio di pacchetti generati al secondo eguaglia il numero di pacchetti trasmessi al secondo.

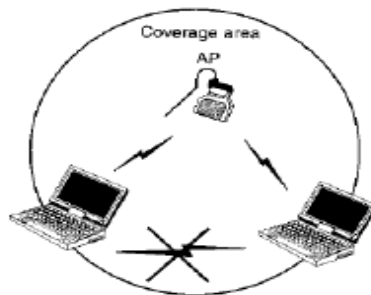
Le relazioni tra S, G e D dipendono dai modelli di protocollo considerati, dalle ipotesi sul comportamento statistico del traffico, dal numero di terminali, e dalla durata relativa dei pacchetti. In ALHOA S dipende solo da G, mentre nei protocolli CS dipende anche dal parametro $a = \tau/T$, detto ritardo normalizzato (τ è il max ritardo di propagazione, e T è il tempo di trasmissione del pacchetto), perchè nel CS deve essere $\tau \ll T$ altrimenti potrei rilevare il canale libero anche quando è occupato.

Se si assume un elevato numero di terminali che generano pacchetti con una distribuzione di Poisson e di lunghezza fissata, si riscontra in tutti i protocolli, che per valori bassi del traffico il throughput aumenta (**regione stabile**) perchè la tecnica di accesso è in grado di sostenere quel traffico fino a raggiungere un valore massimo S_{max} , dopodichè S diminuisce (**regione instabile**). La regione instabile può essere ridimensionata adottando nella ritrasmissione algoritmi di back-off, perchè con essi si riducono in maniera significativa le collisioni. Le tecniche che offrono prestazioni migliori sono quelle CSMA che però non possono essere utilizzate per valori troppo bassi di a, in particolare le versioni non persistenti funzionano meglio di quelle persistenti all'aumentare del traffico. All'aumentare di S aumenta anche D, e anche rispetto a D le tecniche migliori sono le CSMA non persistenti.

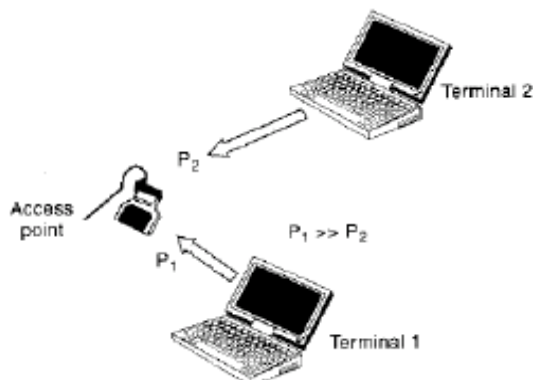
3.3.1 Prestazioni in presenza di terminali nascosti e di effetto cattura

L'analisi del S di un protocollo wireless dovrebbe portare in conto anche altri effetti:

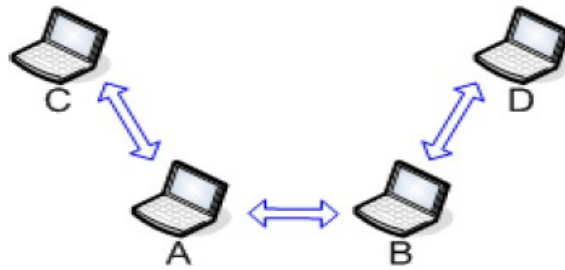
1. **Terminale nascosto:** due terminali sono in copertura (cioè in connessione diretta) con l'Access Point (o un altro terminale) ma non lo sono tra di loro --> Nei metodi che utilizzano il CS si ha una degradazione delle prestazioni perchè i due terminali non sentono le loro "carrier". Nei metodi ALOHA non si alcuna degradazione dovuta al terminale nascosto poichè non usiamo il CS. In presenza di terminali nascosti il S delle MS in copertura tra loro è quello del CSMA (assenza di terminali nascosti), mentre quello rispetto ai terminali che si trovano nell'area nascosta è quello di ALOHA (18%-36%). Il S complessivo si ottiene mediando su entrambe le aree (ovviamente peserà di più quello associato all'area maggiore).



2. **Effetto cattura:** può accadere che, nonostante la collisione tra due pacchetti, la MS sia in grado di recuperare uno dei due pacchetti perchè è stato trasmesso da una MS molto più vicina oppure perchè uno dei due pacchetti è soggetto a fading meno ostile. L'effetto cattura da luogo ad un incremento delle prestazioni perchè una aliquota di collisioni ha un buon fine. L'effetto cattura dipende dallo schema di modulazione utilizzato, dalla lunghezza del pacchetto e dal SNR. In generale S aumenta sia per AHLOA che per CSMA. Tale effetto migliora le prestazioni anche in presenza di terminali nascosti, rispetto al caso in cui ci sono solo terminali nascosti (senza effetto cattura).



3. **Terminale sovraesposto:** due terminali sono in copertura l'uno con l'altro ma non devono trasmettere a terminali raggiungibili da entrambi --> uno non trasmette poichè il CS rileva una portante mentre invece potrebbero trasmettere entrambi.



In figura, A è in copertura con B e C, mentre B è in copertura con A e D; se uso il CSMA A e B non possono Tx simultaneamente a C e a D rispettivamente, perchè essendo in copertura tra loro si accorgono quando l'altro trasmette.

Capitolo 4

Lo standard IEEE 802.11

Cominciamo ora ad occuparci degli standard per reti wireless. Tipicamente tali standard definiscono soltanto i due strati inferiori dello stack protocollare, ovvero lo strato fisico e lo strato data link, in quanto le WLAN sono reti di accesso collegate ad una rete di trasporto (gerarchicamente superiore) che si occupa delle funzionalità dei livelli superiori, come il networking, il trasporto etc. Una eccezione in tal senso è costituita dalle reti ad hoc, dove non c'è un AP, e quindi i vari nodi che compongono la rete devono necessariamente collaborare alla distribuzione dei pacchetti.

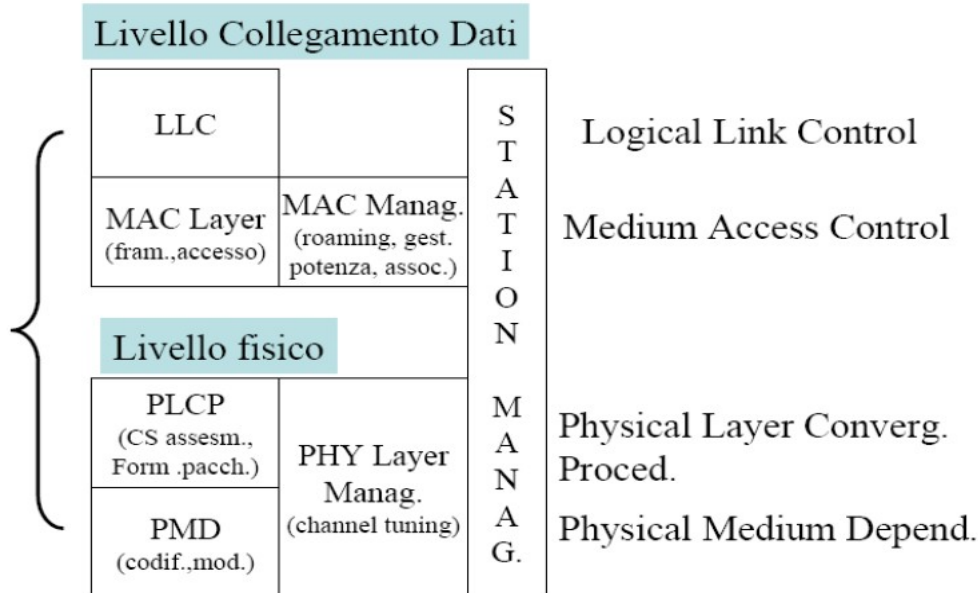
Si tenga presente che rispetto ad una LAN wired, le WLAN sono più complesse e costose, lavorano con bande più limitate (perchè il canale wireless è più ostile), hanno coperture più ridotte (max 100m), maggiori problemi di interferenza (perchè usano tipicamente bande non regolamentate(ISM)), ed hanno limitazioni in potenza (per poter gestire l'interferenza).

In questo capitolo analizzeremo lo standard IEEE 802.11 e le sue evoluzioni, nei capitoli successivi introdurremo lo standard HIPERLAN, lo standard IEEE 802.15 (Bluetooth), usato nelle WPAN, le problematiche relative alle reti mobili ad hoc (MANET) ed infine accenneremo alle reti MESH, che rappresentano il campo di ricerca più avanzato per la realizzazione delle reti di prossima generazione (NGN) che dovrebbero consentire l'interoperabilità tra reti eterogenee.

4.1 Architettura protocollare dello standard IEEE 802.11x

Come già accennato lo stack protocollare di 802.11x specifica soltanto il livello fisico ed il livello data link.

L'architettura stratificata di IEEE 802.11



Lo **Station management** fa interagire tra loro strato data link e strato fisico, i quali sono suddivisi in 3 sottostrati. Il data Link prevede il sottostrato **LLC**, che si interfaccia con i livelli superiori e si occupa dell'attivazione, la gestione e il rilascio della connessione; il sottostrato **MAC Layer**, che gestisce l'accesso al mezzo e la frammentazione e il riassetto dei pacchetti; e il sottostrato **MAC Management**, che gestisce il roaming (cioè il trasporto dei pacchetti tra BSA diverse), la potenza, la sicurezza e la mobilità (associazione, dissociazione e riassociazione). Lo strato fisico prevede il sottostrato di convergenza **PLCP**, che si occupa dell'assistenza al carrier sense e del framing dei pacchetti; il sottostrato **PMD**, che definisce le funzionalità di codifica e modulazione a seconda del mezzo trasmissivo; e il **PHY Management**, che si occupa del tuning del canale (ovvero della scelta del canale più opportuno: con meno interferenza).

Tutte le versioni di 802.11 condividono lo stesso strato data link e si differenziano per lo strato fisico (in particolare per il PMD). Di seguito analizziamo lo strato fisico delle versioni principali dello standard e poi vedremo lo strato data link.

4.2 Lo strato fisico

4.2.1 Lo strato fisico di 802.11 base

La versione iniziale di 802.11 lavora nella banda a 2.4 Ghz, raggiunge velocità di 1-2 Mbps, e specifica tre diverse opzioni per il livello fisico:

1. **FHSS** (*Frequency Hopping Spread Spectrum*)
2. **DSSS** (*Direct sequence Spread Spectrum*)
3. **DFIR** (*Diffused Infrared*)

La tecnica Spread Spectrum

Nata per l'esigenza di garantire tolleranza nei confronti dell'interferenza (eventualmente intenzionale) e del multipath, e la coesistenza nella stessa banda di più sistemi (overlay systems). Per soddisfare tali esigenze, con la tecnica SS si distribuisce la potenza del segnale su una banda 2W molto più ampia di quella originaria 2B in modo da avere livelli di PSD molto più bassi.

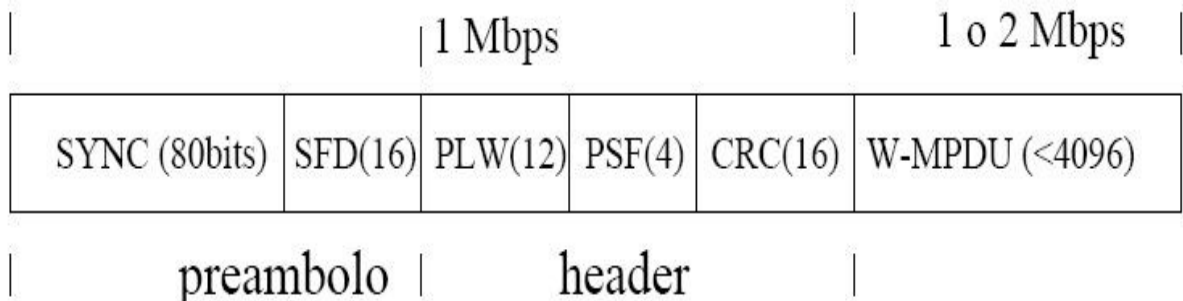
Frequency-hopping Spread-Spectrum (FHSS):

In IEEE 802.11 FHSS specifica 78 hops separati da 1 MHz. Queste "frequenze" sono divise in tre gruppi di 26 hops, ciascuno corrispondente ai numeri di canale (0, 3, 6, . . .), (1, 4, 7, . . .) e (2, 5, 8, . . .). Queste scelte sono disponibili per tre differenti sistemi che possono coesistere nella stessa area geografica senza alcuna collisione tra gli hops.

La frame FHSS :

Quando la MPDU (MAC Protocol Data Unit) arriva allo strato PLCP, viene incapsulata nella frame PLCP, ovvero gli vengono aggiunti un preambolo e un header.

Frame PLCP IEEE 802.11 FHSS



L'overhead (preambolo+header) è trasmesso a 1Mbps usando una modulazione 2-GFSK, mentre il payload è trasferito a 1-2 Mbps usando rispettivamente una 2-GFSK o una 4-GFSK.

- **Preambolo.** E' lungo 12 byte e contiene due campi:
 - **SINC** : sequenza di 80 simboli 0 e 1 alternati (10 byte), che servono solo per acquisire la sincronizzazione.
 - **SFD (Start Frame Delimiter)**: sequenza di 2 byte (0000110010111101), che definisce l'inizio della frame.
- **Header.** E' lungo 4 byte e contiene tre campi:
 - **PLW (Packet Length Width)**: 12 bit che danno informazioni sulla lunghezza della frame (che ha lunghezza variabile).
 - **PSF (Packet Signaling Field)**: 4 bit che indicano il data rate in passi da 500 kbps, cioè specificano la velocità di trasmissione (4bit<-->max 8.5Mbps).
 - **CRC (Cyclic Redundancy Check)**: codice per la rilevazione di errori; l'overhead, fino al campo PSF, viene esteso con 16 bit 0 e diviso per il polinomio generatore (in questo caso $G(x) = x^{16} + x^{12} + x^5 + 1$); il resto della divisione, costituito da 16 bit, viene poi inserito al posto dei 16 bit aggiunti inizialmente. In ricezione l'overhead viene diviso per il polinomio generatore, e se il resto è nullo probabilmente non ci sono stati errori. Tale codice può rilevare errori su 15 bit (perchè i bit sono a distanza di Hamming 16-1=15).
- **MPDU (MAC Protocol Data Unit)**: è il campo dati, ovvero la PDU del livello MAC che viene incapsulata nelle frame dello strato fisico; può viaggiare a 1 o 2 Mbps e può avere una lunghezza non superiore a 4096 bit.

Le specifiche di FHSS sono mostrate nella seguente tabella:

FHSS

- | |
|---|
| <ul style="list-style-type: none"> - 3 set frequenze hopping, 26 sequenze/set - 79 canali (USA ed EU), 23 canali (Giappone) da 1MHz - modulazione: 2-GFSK (1 Mb/s), 4-GFSK (2 Mb/s) - hopping rate: 2.5 hop/s (slow hopping) - bit scrambling $s(z) = z^7 + z^4 + 1$ (DC blocking/whitening) - Frequenza di campionamento: 1Msps |
|---|

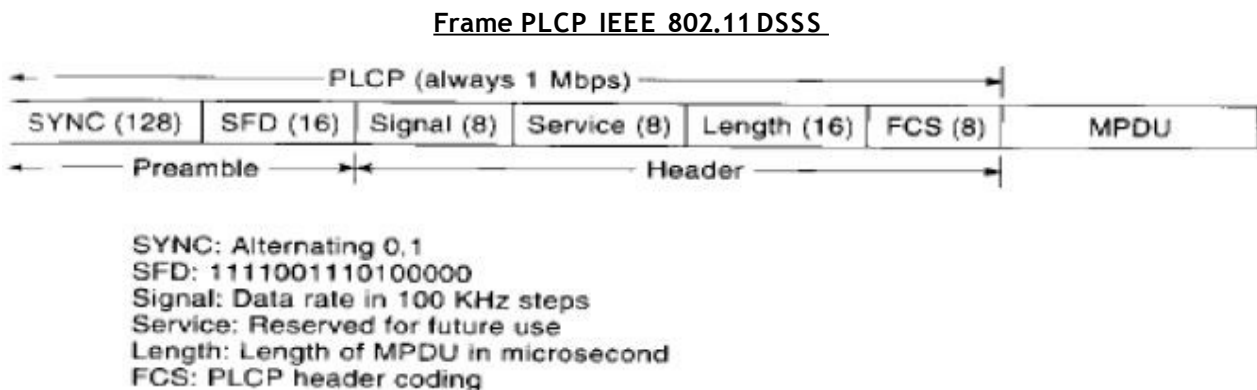
Direct-Sequence Spread-Spectrum (DSSS):

La tecnica DSSS richiede maggiore complessità e consumo di potenza rispetto al FHSS, in quanto usa una frequenza di campionamento più elevata (44000 campioni al secondo contro i 2000 del FHSS), perchè il ricevitore richiede una banda di più grande (circa 22 MHz contro 1MHz del FHSS, quindi la banda è 11 volte maggiore); inoltre non c'è bisogno di fare lo scrambling, in quanto ogni bit è trasmesso con una sequenza di chip e quindi è già sbiancato (si usa un codice di Baker di lunghezza 11), e la sincronizzazione è più complessa perchè occorre sincronizzarsi anche con la portante e non solo con i simboli (cioè si usa una modulazione coerente).

Nota: si ricordi che il fatto che gli spettri associati a più reti si sovrappongono non deve preoccupare perchè la discriminazione è fatta sulle proprietà di ortogonalità dei codici che vado ad utilizzare (CDMA).

La frame **DSSS** :

Il formato della frame è simile a quello del FHSS ma i campi hanno lunghezze differenti.



Il preambolo, come per FHSS, viaggia sempre ad 1 Mbps usando una BPSK. La MPDU è trasmessa a 1 o 2 Mbps usando una BPSK o una QPSK. La differenza con la frame per il FHSS è che il campo SYNC è più lungo (128 bit anziché 80) perchè il DSSS, dovendosi sincronizzare anche con la portante, ha bisogno di più tempo per la sincronizzazione, e inoltre è presente un campo Service riservato per usi futuri.

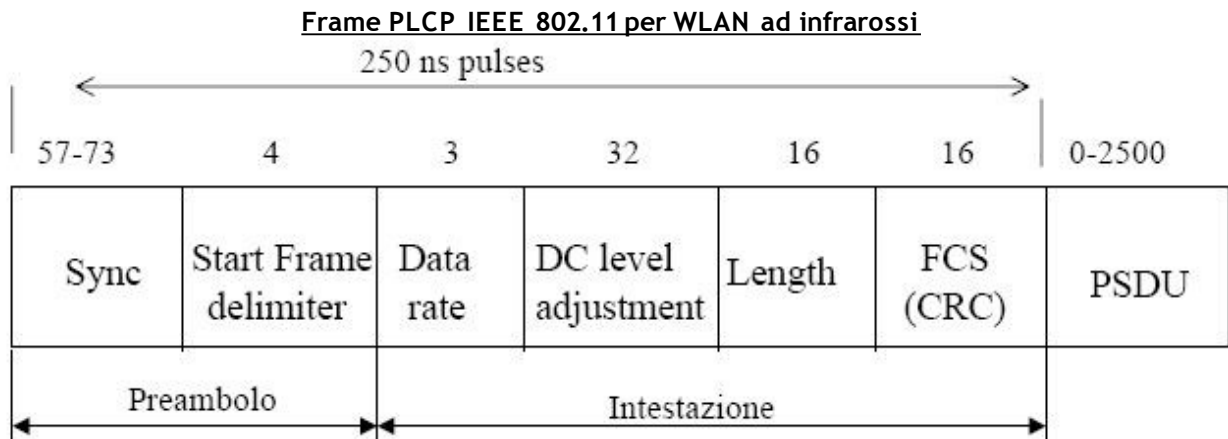
Nota: in figura c'è un errore; il campo FCS (che è il codice CRC) è di 16 bit.

La tecnica IR

Le reti WLAN IEEE 802.11 ad infrarossi sono più sicure perchè non sottoposte alle interferenze ed al rumore nelle bande radio.

La tecnica di modulazione utilizzata è la PPM (Pulse Position Modulation) a 16 o a 4 impulsi a seconda della velocità (rispettivamente di 1 o 2 Mbps).

La frame per le reti W-LAN ad infrarossi:



- **SYNC** : da 57 a 73 simboli 0 e 1 alternati;
- **SFD** (start frame delimiter): 1001;
- **Data rate** : 000 (1 Mbps) oppure 001 (2 Mbps);
- **DCLA** : per settare la soglia del ricevitore; in demodulazione devo verificare se in uno slot è presente l'informazione e quindi il ricevitore si deve settare su una soglia;
- **Length** : lunghezza della MPDU in microsecondi;
- **FCS** (cyclic redundancy check): $G(x) = x^{16} + x^{12} + x^5 + 1$.

La PSDU è trasmessa a 1-2 Mbps usando rispettivamente una 16-PPM o una 4-PPM.

4.2.2 Lo strato fisico degli standard IEEE 802.11a/b/g

Tutte le versioni di IEEE 802.11x condividono lo stesso strato DL e si distinguono per lo strato fisico. Il livello DL sarà descritto dettagliatamente nella sezione successiva, in questa sezione descriviamo, invece, il livello fisico delle versioni b,a e g.

4.2.2.1 IEEE 802.11b

La versione "b" è compatibile con IEEE 802.11 ed opera nella banda ISM a 2.4GHz con velocità di 1,2,5.5 o 11 Mbps grazie all'uso dei codici CCK che hanno ottime proprietà di immunità nei confronti del multipath (autocorrelazione stretta). Si usa una modulazione differenziale per avere una demodulazione non coerente (più semplice).

Richiamo: Ricordiamo che i codici CCK utilizzano chip con valori complessi quaternari piuttosto che chip a valori binari reali (ho più parole codice su cui agire e posso aumentare la velocità di trasmissione), ma non tutte le parole codice sono ortogonali perchè si vuole trasmettere a velocità a di 11 Mbps (con le sole parole ortogonali posso arrivare max a 5.5 Mbps). Ricordiamo inoltre che lo spreading (allargamento della banda del segnale da Tx (con abbassamento però del livello di segnale)) consente di ottenere una serie di vantaggi, come una maggiore tolleranza al multipath (perchè allargare la banda vuol dire rendere le repliche risolvibili), robustezza nei confronti dell'interferenza a banda stretta, possibilità di far convivere più reti diverse nello stesso spazio (grazie all'utilizzo di sequenze di chip differenti (esempio codice di Barker)).

La frame PLCP:

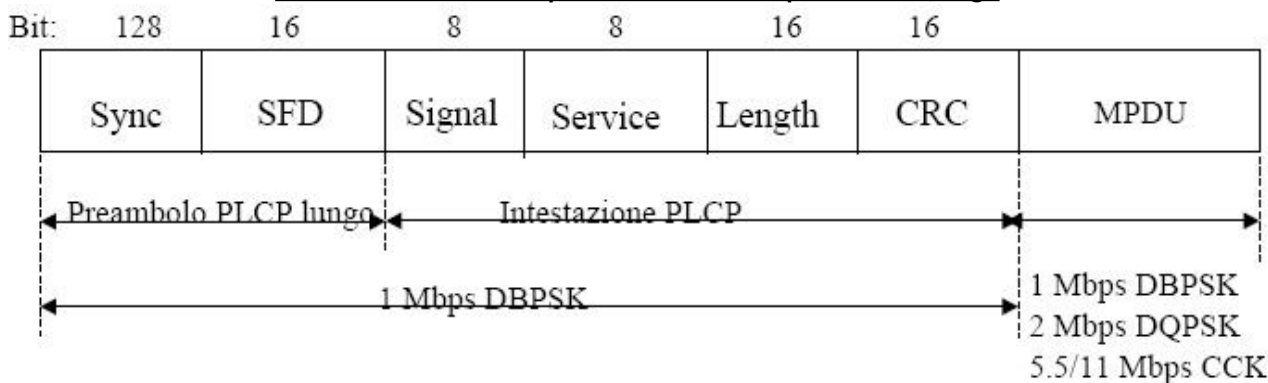
Per la frame PLCP IEEE 802.11b prevede due diverse intestazioni, per cercare di migliorare l'overhead (ovvero gestire la rete con meno byte):

1. **Preambolo lungo:** intestazione standard per velocità a 1, 2, 5.5 e 11 Mbps (preambolo a 18 byte = 16(sinc.)+ 2 (SFD))
2. **Preambolo corto:** intestazione per velocità a 2, 5.5 e 11 Mbps (preambolo a 9 byte = 7 (sinc.) + 2 (SFD)).

Nota: Il preambolo significa overhead, dunque se uso il preambolo corto ho maggiore efficienza perchè trasmetto, percentualmente, più payload rispetto alle informazioni di servizio.

Il preambolo lungo utilizza l'intestazione standard di IEEE 802.11 a 1 o 2 Mbps per essere compatibile con esso. Il preambolo corto è usato per la trasmissione di frame di controllo e per traffico sensibile al ritardo (pacchetti di fonia/video in tempo reale).

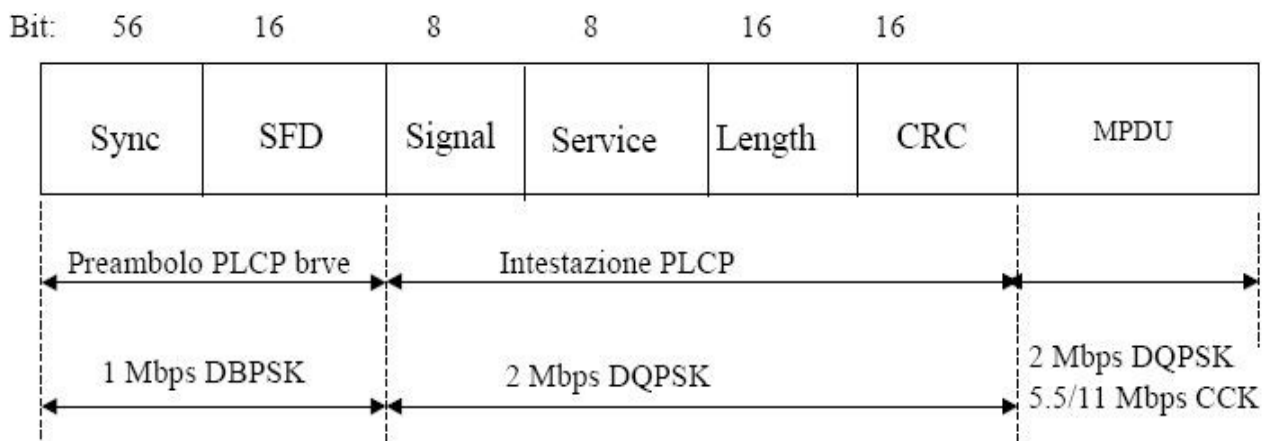
Formato frame PLCP per IEEE 802.11 b: preambolo lungo



- **SYNC** : simboli 0 e 1 alternati;
- **SFD** (start frame delimiter): 1111001110100000;
- **Signal**: data rate in passi da 100 Kbps;
- **Service**: riservato per esigenze future;
- **Length**: lunghezza della MPDU in microsecondi;
- **FCS** (come CRC di FHSS: (cyclic redundancy check)): $G(x) = x^{16} + x^{12} + x^5 + 1$.

L'intestazione + il preambolo (ovvero l'overhead(24 byte)) sono trasmessi a 1 Mbps, perchè voglio essere compatibile con le versioni precedenti, mentre l'MPDU (che contiene l'info) può essere trasmesso a velocità diversa, specificata nel campo Signal. Il campo Sync serve al demodulatore per sincronizzarsi, mentre l'SFD serve al demodulatore per capire quando sta cominciando una nuova frame. La frame è identica a quella di 802.11 base per DSSS se non per la modulazione che qui è differenziale.

Formato frame PLCP per IEEE 802.11 b: preambolo breve



Il preambolo breve per migliorare il throughput utilizza 7 byte (anziché 16) per il campo Sync e trasmette l'intestazione a 2 Mbps (quindi è come se avessi dimezzato anche questa parte perchè 6 byte Tx a 2 Mbps <--> 3 byte Tx a 1 Mbps). La MPDU può essere trasmessa a velocità di 2 , 5.5 o 11 Mbps.

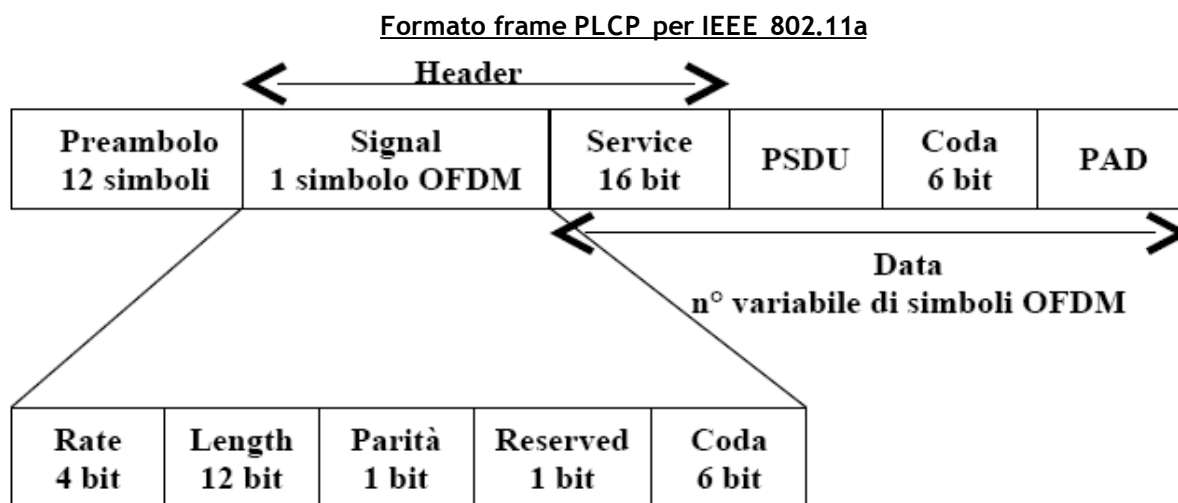
Con il preambolo breve + il raddoppio di velocità per l'intestazione si ha una diminuzione del sovraccarico del 50% passando di fatto da 24 a 12 byte --> Aumenta il throughput della rete --> Vantaggio nella trasmissione di frame per il controllo e pacchetti dati frammentati per traffico sensibile al ritardo (pacchetti di fonia, video in tempo reale).

4.2.2.2 IEEE 802.11a

La versione "a" opera nella banda 5.7 GHz (che in Europa è licenziata) con velocità fino a 54 Mbps (è previsto un aumento fino a 100 Mbps per offrire un servizio Fast Ethernet full duplex). Per offrire velocità fino a 54Mbps, al posto delle tecniche SS, a singola portante si utilizza la tecnica di modulazione multiportante OFDM.

La frame PLCP:

La frame PLCP per 802.11a (a differenza di quella di 802.11g) può essere progettata senza alcun vincolo perchè non deve essere compatibile con le versioni precedenti del protocollo (a 2.4Ghz). Questa frame è, cioè, ottimizzata per OFDM.



- **Preambolo:** serve per il training e la sincronizzazione del demodulatore, ed è costituito da 12 simboli (simboli e non bit perchè con OFDM i simboli possono essere costituiti da un numero diverso di bit a seconda della codifica);
- **Signal:** 24 bits, codificati in un simbolo OFDM e trasmessi con una BPSK e con tasso di codifica 1/2, che specificano la velocità di Tx (che varia da 6Mbps a 54Mbps, a seconda della modulazione usata e del tasso di codifica) 12 bit per la lunghezza della PSDU, 1 bit riservato per esigenze future, 1 bit di parità, e 6 bit di coda per ripulire il registro del codificatore e del decodificatore.

- **PLCP Header:** Signal + 16 bit del campo Servizio;
- **Data:** costituito da 16 bits per il campo servizio, la PSDU (Physical Sublayer Service Data Unit) che contiene i dati da incapsulare nella frame, 6 bits per la coda e bits di padding (riempimento con zeri), necessari a garantire che numero di bits nel campo DATA sia sempre un multiplo dei bit codificati in un simbolo OFDM; i bit di pad sono necessari per garantire che il numero di bit per simbolo sia sempre quello previsto dalla tecnica di modulazione usata.

Nota: Ovvero, poiché l'OFDM opera con la FFT (o con la IFFT), che è un algoritmo efficiente per calcolare la DFT, e quindi il numero di campioni è fissato, per garantire che la DFT sia sempre fatta su un numero fissato di campioni è necessario fare zero-padding; o in altri termini, devo fare zero-padding per garantire che il n° di bit per simbolo sia quello previsto dalla tecnica di modulazione usata (Le portanti per i dati sono 48; se su ogni sottoportante uso un BPSK allora ogni sottoportante porta 1 bit e dunque ho 48 bit per simbolo, se invece uso un QPSK su ogni sottoportante mando 2 bits --> 96 bit per simbolo OFDM).

La seguente tabella (che vale anche per 802.11g) riassume i parametri caratteristici di 802.11a per ciascuna velocità:

Rate-dependent parameter of 802.11a

Data rate (Mbps)	Modulation	Coding rate (R)	Coded bits per subcarrier (N _{BPSK})	Coded bits per OFDM symbol (N _{QPSK})	Data bits per OFDM symbol (N _{DATA})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16 QAM	1/2	4	192	96
36	16 QAM	3/4	4	192	144
48	64 QAM	2/3	6	288	192
54	64 QAM	3/4	6	288	216

Le colonne, da sx a dx, indicano la velocità di Tx, il tipo di modulazione da usare, il tasso di codifica (n°bit di info/n°bit Tx: esprime il n° di bit che Tx per ogni bit di info), il n° di simboli per portante, il n° di bit per simbolo, e il n° di bit utili.

La prima riga esprime che se considero un rate di 6 Mbps, adotto la modulazione BPSK con un coding rate $R = 1/2$; in questo caso su ogni sottoportante, poichè ho utilizzato il BPSK, ci sarà 1 bit e, poichè le sottoportanti per i dati sono 48, avrò 48 bit associati al simbolo OFDM; poichè però il tasso è $1/2$, i bit d'informazione sono la metà cioè 24.

Il 54 Mbps viene ottenuto utilizzando una modulazione QAM con un numero elevato di simboli (64) e con un elevato tasso di codifica ($3/4$); i bits per sottoportante sono 6 ($2^6 = 64$); ad un simbolo OFDM corrisponderanno $6 \times 48 = 288$ bits, dei quali i bits di informazione sono $3/4 \times 288 = 216$.

La seguente tabella riassume invece i parametri caratteristici di 802.11a relativi al tempo:

Timing-related parameter of 802.11a

Parameter	Value
N_{SD} : Number of data subcarriers	48
N_{SP} : Number of pilot subcarriers	4
N_{ST} : Number of subcarriers, total	52 ($N_{SD} + N_{SP}$)
ΔF : Subcarrier frequency spacing	0.3125 MHz ($=20 \text{ MHz}/64$)
T_{FFT} : IFFT/FFT period	3.2 μs ($1/\Delta F$)
$T_{PREAMBLE}$: PLCP preamble duration	16 μs ($T_{SHORT} + T_{LONG}$)
T_{SIGNAL} : Duration of the SIGNAL BPSK-OFDM symbol	4.0 μs ($T_{GI} + T_{FFT}$)
T_{GI} : GI duration	0.8 μs ($T_{FFT}/4$)
T_{GI2} : Training symbol GI duration	1.6 μs ($T_{FFT}/2$)
T_{SYM} : Symbol interval	4 μs ($T_{GI} + T_{FFT}$)
T_{SHORT} : Short training sequence duration	8 μs ($10 \times T_{FFT}/4$)
T_{LONG} : Long training sequence duration	8 μs ($T_{GI2} + 2 \times T_{FFT}$)

Sono riportati il n° di portanti, sottoportanti, la spaziatura, il periodo per la DFT, la durata del preambolo ($T_{corto}+T_{lungo}=8\mu\text{s}+8\mu\text{s}=16\mu\text{s}$) ovvero il tempo per la sincronizzazione, l'intervallo di guardia GI (per controllare la dispersione) e la sua durata ($0.8\mu\text{s}$), la durata del GI del simbolo di training ($1.6\mu\text{s}$ per garantirsi che non ci sia inversione durante il periodo di training), etc.

Osservazioni: Ricordiamo che in OFDM al posto di GI mettiamo un precodice. Con la DFT si campiona lo spettro (lo spettro in esame è di 26Mhz) con spaziatura $1/T=\Delta f$, dove Δf è il passo di campionamento in frequenza e il suo inverso T è il periodo di simbolo (ovvero la durata di un blocco OFDM). Il tempo di guardia GI è il codice CRC e va sommato al tempo per fare la DFT e a quello per trasmettere un simbolo. L'ultima tabella mostra come si ottengono i tempi necessari per trasmettere la sincronizzazione (sia lunghi che corti): occorrono $16\mu\text{s}$ per il preambolo e $4\mu\text{s}$ per l'header.

4.2.2.3 IEEE 802.11g

La versione "g" nasce perchè la versione "a" non è supportata in Europa ed opera nella banda ISM a 2.4 GHz (liberalizzata in Europa) con velocità fino a 54 Mbps come la versione "a". Si utilizza la tecnica di modulazione multiportante OFDM al posto delle tecniche SS a singola portante, con più opzioni a livello di strato fisico per garantire la compatibilità con le altre tecniche: IEEE 802.11g, a differenza di IEEE 802.11a, assicura la convergenza con IEEE 802.11 e IEEE 802.11b che operano a 2.4 Ghz.

Note: La versione "g" deve essere compatibile con quelle precedenti nel senso che deve almeno rendersi conto se il canale è impegnato da esse. Si noti inoltre che "g" supporta un maggior numero di velocità di Tx.

Le caratteristiche fondamentali di questa versione sono: la definizione di 4 differenti strati fisici (per garantire la convergenza con le versioni già esistenti), il supporto obbligatorio per un preambolo corto, l'attributo ERP, (Extended Rate Physicals) e nuovi meccanismi di protezione per esigenze di interoperabilità (introduce il meccanismo CTS-to-self).

4 differenti strati fisici:

La novità di “g” è che, mentre “a” utilizza un unico strato fisico (OFDM) e lo può fare perchè lavora a 5.7 GHz dove non ha problemi di compatibilità, prevede quattro possibili opzioni per la compatibilità con le altre reti convenzionali a 2.4 Ghz. Ovvero, definisce un'architettura estesa di strati fisici di cui i primi 2 sono obbligatori:

1. **ERP-DSS/CCK** : per compatibilità con IEEE 802.11b.
2. **ERP-OFDM** : per compatibilità con IEEE 802.11a;
3. **ERP-DSSS/PBCC** : introdotto in IEEE 802.11b dove il max era 11 Mbps, anche se ora si hanno rate di 22 e 33 Mbps (PBCC: Packet Binary Convolutional Coding);
4. **DSSS-OFDM**: combinazione di DSSS e OFDM in quanto il physical header (intestazione) è trasmesso in DSSS e il packet payload in OFDM.

L'attributo ERP:

IEEE 802.11g adatta dinamicamente la durata di slot e la minima finestra di contesa in relazione allo strato fisico utilizzato:

- 20 µsec e 31 slot per layers che adottano DSSS;
- 9 µsec e 15 slot per layers che adottano OFDM.

Questa informazione è trasmessa dall'AP con una *beacon frame* che contiene informazioni sulla rete.

Nuovi meccanismi di protezione:

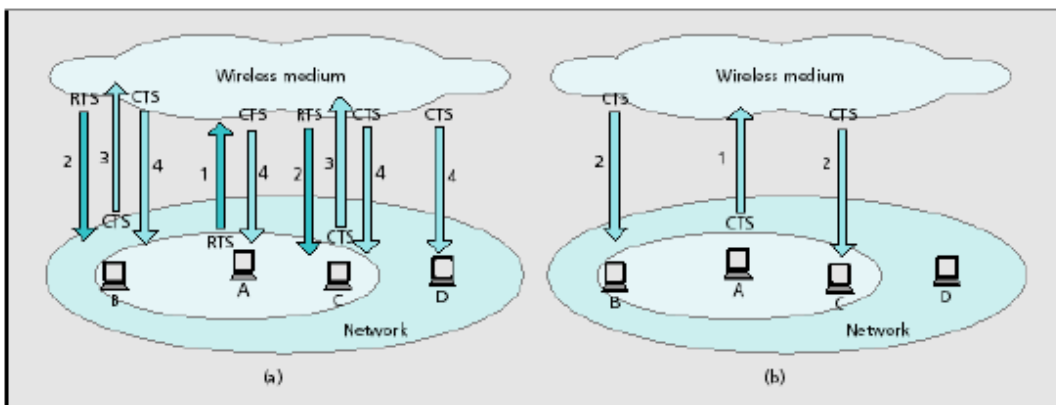
Sono necessari perchè in IEEE 802.11g ho a che fare con uno scenario variegato in cui le stazioni possono usare tecnologie e strati fisici diversi. I tipi di stazioni possibili sono:

1. Stazioni ERP: stazioni che operano in accordo con IEEE 802.11g puro (OFDM).
2. Stazioni non ERP: stazioni con IEEE 802.11b, che non supportano lo strato fisico esteso, ma con il firmware aggiornato per supportare il preambolo corto.
3. Stazioni non ERP che non supportano il preambolo corto.

Se l'AP impone uno strato fisico OFDM le stazioni non-OFDM non sono in grado di accorgersi delle stazioni OFDM che stanno comunicando. Bisogna concepire delle tecniche per evitare queste collisioni:

- Una soluzione potrebbe essere quella di usare DSSS-OFDM in modo che le stazioni non ERP sentono il canale occupato (e non trasmettono) anche se non possono ricevere il pacchetto OFDM.
- Un'altra soluzione potrebbe essere quella di utilizzare la tecnica RTS/CTS in DSSS per proteggere i pacchetti OFDM; usando il 4-way handshaking, le stazioni ERP riescono a capire se il canale è occupato. In questo modo si riesce anche a gestire meglio il problema del terminale nascosto.
- La soluzione alternativa, utilizzata in IEEE 802.11g, è il meccanismo CTS-to-self, che non risolve il problema del terminale nascosto (come mostra la seguente figura) ma riduce l'overhead perchè trasmette un solo pacchetto anzichè due; in pratica è un 3-way handshaking perchè chi deve trasmettere avverte soltanto gli altri mandando un CTS (che non viene ascoltato però dai terminali nascosti).

CTS-to-self

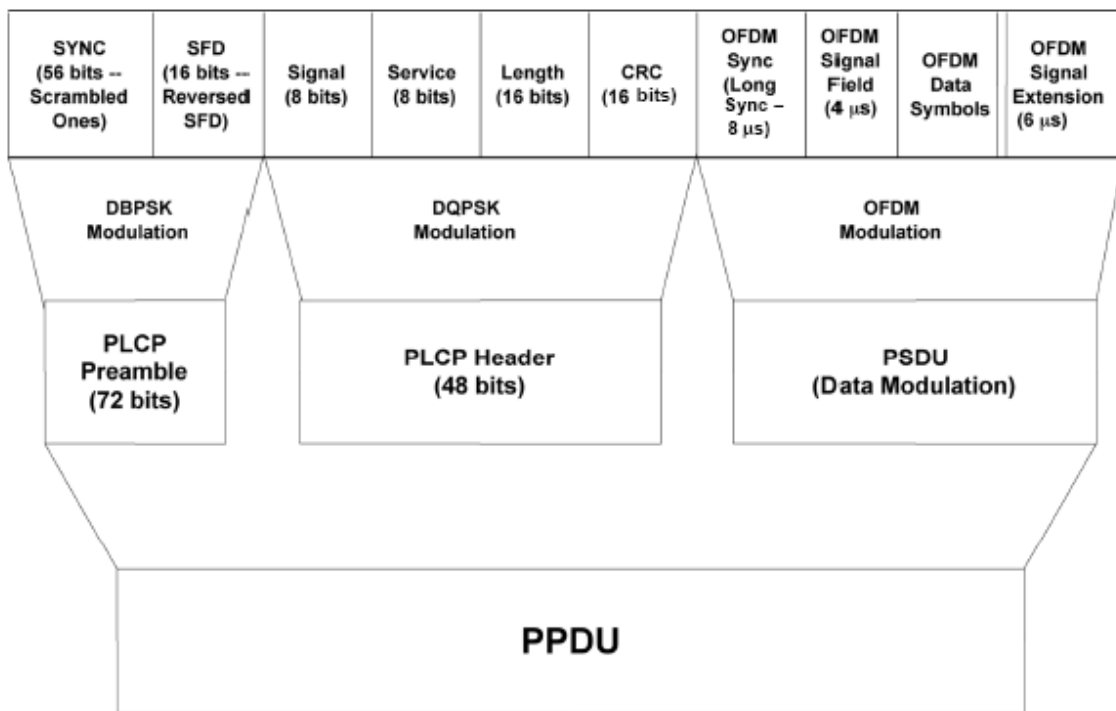


Spiegazione figura: La figura mostra le differenze tra le due tecniche RTS/CTS e CTS-to-self. Nello scenario (a) c'è la tecnica RTS/CTS. La stazione A deve comunicare con C --> A trasmette un RTS. Sia B che C sono nella copertura di A e quindi entrambe acquisiscono l'RTS. C manda un CTS perchè ha scoperto che A vuole comunicare con lui. La stazione D, che è fuori dalla copertura di A e quindi non ha ricevuto l'RTS, può acquisire il CTS e si accorge che la rete è impegnata --> superata la collisione da terminale nascosto. Lo scenario (b) illustra, invece, il meccanismo CTS-to-self. A deve comunicare ancora una volta con C ma in questo caso non manda un RTS ma un CTS nel medium. B vede il CTS e non trasmette. C capisce che è impegnato in tale comunicazione ma non può rispondere a sua volta con un CTS inverso poiché la procedura non lo prevede. Il problema è ora che D, che non è in copertura di A, non si accorge della trasmissione e può andare in collisione --> non è risolto il problema del terminale nascosto.

La frame PLCP:

IEEE 802.11g ha 4 differenti strati fisici e quindi 4 differenti frame per il PLCP. La frame per gli strati ERP-DSSS con preambolo lungo e corto sono del tutto identiche a quelle di 802.11b. La frame OFDM (per lo strato fisico ERP-OFDM) ed è del tutto identica a quella di IEEE 802.11a, ed è usata quando nella rete ci sono tutte stazioni abilitate con l'OFDM. La frame associata allo strato fisico DSSS-OFDM, con preambolo lungo e corto, hanno l'overhead (preambolo+header) del tutto identico a quello della frame della versione "b" e la parte dati trasmessa con OFDM, come si può osservare nella seguente figura, che fa riferimento al preambolo corto (la frame per preambolo lungo si differenzia solo per il campo sync, che è di 128 bit anziché 56).

Short preamble PPDU format for DSSS- OFDM(Optional)



4.2.3 Carrier Sensing

In IEEE 802.11 il sensing è complicato poichè la dinamica del segnale (cioè le possibili escursioni che la potenza ricevuta può subire) è molto ampia (a causa del fading) e l'interferenza può mascherare il segnale utile. Esso può essere eseguito sia a livello fisico che in maniera virtuale (a livello MAC).

Il sensing a livello fisico è eseguito attraverso il segnale CCA (Clear Channel Assesment) prodotto dal PLCP per stabilire se il canale è libero. Il CCA è basato sul sensing reale dell'interfaccia radio osservando i bit ricevuti o sul RSS (Received Signal Strenght). Osservare i bit ricevuti significa osservare il segnale a valle dell'operazione di demodulazione ed è dunque un'operazione più sofisticata rispetto al semplice confronto della potenza ricevuta con una soglia. Il sensing sui bit è più affidabile però, essendo un'operazione più sofisticata, è più lenta a causa dell'operazione di rivelazione dei dati. Decisioni basate sul RSS possono dar luogo a falsi allarmi o comunque a decisioni non corrette a causa della presenza di interferenze. Le soluzioni migliori combinano il sensing basato sul RSS con quello basato sui bit rivelati, ovvero se non supero una certa soglia posso dire che il canale è libero, se non la supero, prima di dire che il canale è impegnato, faccio il sensing sui bit.

Il sensing virtuale è basato sul segnale del vettore di allocazione della rete (NAV) che è associato al meccanismo di RTS/CTS o alla procedura PCF nello strato MAC. Il segnale NAV opera come un segnale per sentire il canale, per prevenire la trasmissione di dati in contesa per un tempo prestabilito. Contiene un campo lunghezza che definisce il tempo che deve trascorrere prima che il mezzo sia liberato.

4.3 Lo strato DL in IEEE 802.11x

Lo strato Data Link, come noto, è comune per tutte le versioni 802.11x. Esso comprende il sottostrato *LLC*, che si interfaccia al livello rete e si occupa dell'attivazione, gestione e rilascio della connessione, del controllo degli errori e del flusso, e fornisce i servizi punto-punto: senza connessione con/senza ACK, affidabile orientato alla connessione; e il sottostrato *MAC* che a sua volta si suddivide in *MAC management*, che si occupa del roaming in ESS, e della gestione della mobilità, della potenza e della sicurezza, e *MAC sublayer*, che si occupa del meccanismo di accesso e della frammentazione e il riassetto dei pacchetti.

4.3.1 Il sottolivello 802.11 MAC sublayer

Come già accennato, questo sottolivello gestisce il controllo dell'accesso e la segmentazione dei pacchetti. Il controllo dell'accesso alla rete avviene attraverso due modalità:

1. **Distributed Coordination Function (DCF)**. Accesso casuale senza gerarchia: tutte le Stazioni entrano in contesa per ogni trasmissione di pacchetto. E' fornito tramite due possibili procedure: *2-way handshaking* (opzione di default) oppure *4-way handshaking* (RTS/CTS), in cui prima di trasmettere si cerca di prenotare il canale con il meccanismo RTS/CTS.
2. **Point Coordination Function (PCF)**. Accesso controllato dall'AP, che assegna connessioni esenti da contese (l'AP manda il NAV con il quale indica che si può trasmettere senza contese. In realtà lo standard prevede che ci debba essere una fase PCF (cioè libera da contese) seguita da una DCF). Quindi qui l'AP ha una gerarchia da seguire.

4.3.1.1 DCF:

DCF è l'opzione di default dell'802.11 e si basa sul metodo **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance), ovvero, per prevenire le collisioni, quando una stazione può trasmettere non lo fa subito ma solo dopo un interframe space.

Il sensing avviene prima in maniera virtuale utilizzando il segnale NAV (Network Allocation Vector), che indica gli intervalli in cui il canale sarà occupato, e poi, attraverso il sensing reale ricorrendo al RSS (Received Signal Strength); se il meccanismo RSS rileva che il canale è libero, la stazione aspetta un tempo differente a seconda della tipologia di pacchetto da trasmettere. In particolare si usano tre differenti intervalli di spaziatura interframe, $SIFS < PIFS < DIFS$, a seconda della priorità del pacchetto da trasmettere (in tal modo si introduce una forma di priorità decentralizzata); i pacchetti a maggiore priorità sono gli ACK e i pacchetti RTS/CTS, che devono aspettare un SIFS (Short IFS); i DIFS sono usati dalle stazioni in modalità DCF mentre i PIFS da quelle in modalità PCF. In pratica, a differenza del CSMA/CA classico, quando una stazione può trasmettere lo fa dopo un intervallo dipendente dal tipo di pacchetto.

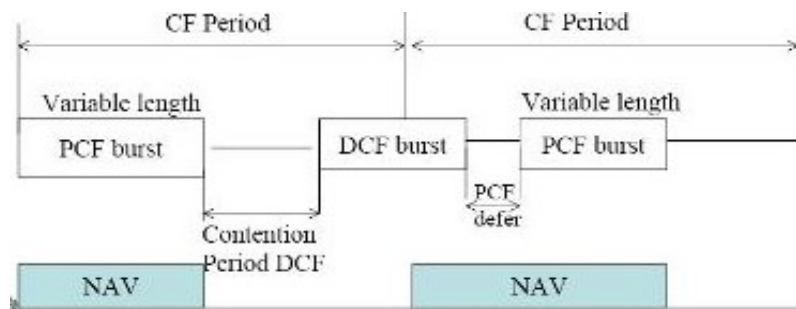
DCF gestisce anche le frame perse e/o errate: se la Stazione Tx non riceve l'ACK in un intervallo pari alla durata di un ACK + un intervallo SIFS, inizia la procedura di Back-off per una nuova trasmissione; ovviamente se l'ACK si perde la Stazione Rx riceverà due volte la stessa frame, ma sarà in grado di riconoscere che si tratta di un duplicato grazie al numero d'ordine della frame.

La procedura di accesso usata, come accennato, può essere la 2-way-handshaking (obbligatoria) oppure la 4-way-handshaking (opzionale); nel primo caso la procedura CSMA/CA è applicata a tutti i pacchetti, mentre nel secondo caso solo ai pacchetti ACK e RTS/CTS migliorando quindi le prestazioni quando si trasmettono pacchetti lunghi (in quanto si riduce la lunghezza delle frame coinvolte nel processo di contesa).

4.3.1.2 PCF:

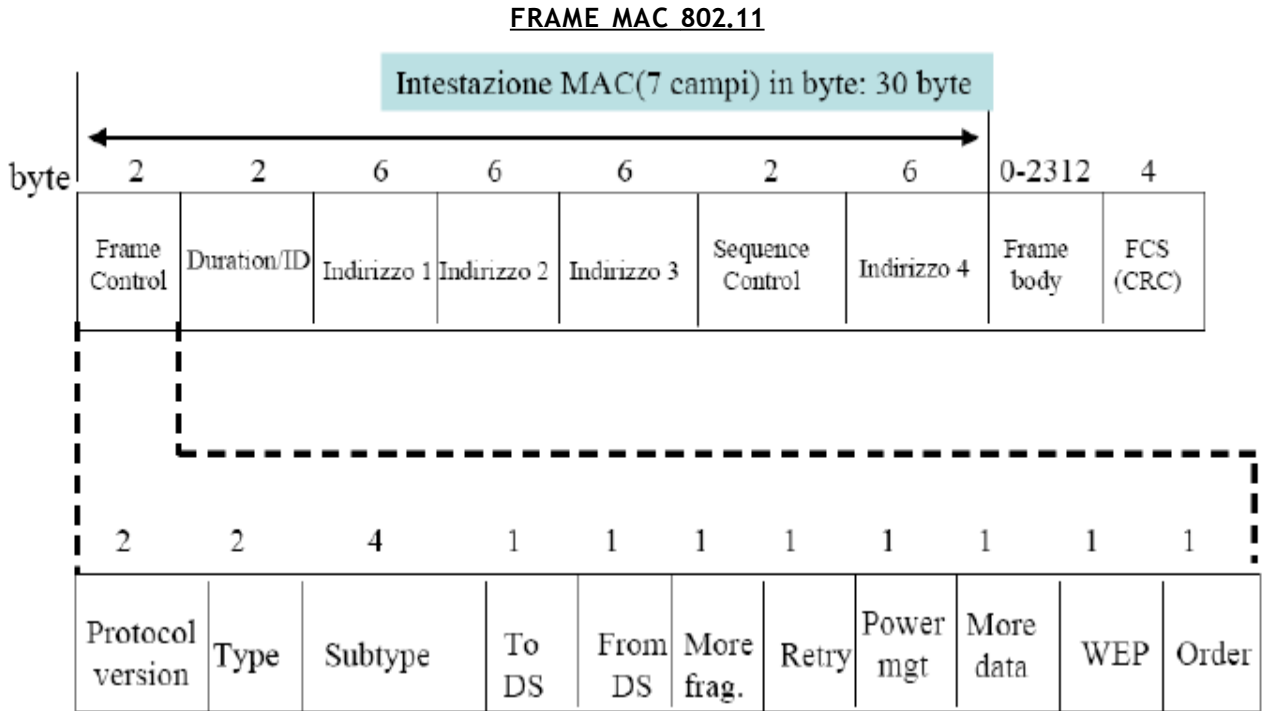
PCF è una procedura per reti infrastrutturate (ovvero richiede la presenza di un AP) che offre un servizio di trasferimento senza contese, ed è costruita sul DCF (che utilizza il CSMA) per erogare servizi senza contesa con latenza temporale limitata e trasmissioni asincrone, necessari per applicazioni che non tollerano ritardi, quali ad esempio la fonia e il video. Dovendo realizzare il *polling* ci sarà un sovraccarico, in quanto l'AP deve inviare delle frame per assegnare le slot alle Stazioni trasmittenti.

Il tempo è diviso in intervalli CF (Contention-Free); quando l'AP vuole assumere il controllo invia, dopo un PIFS, un segnale di beacon che arresta la trasmissione di tutte le stazioni ed indica la durata dell'intervallo CF; all'inizio di ogni periodo CF, l'AP invia il segnale NAV, che specifica la lunghezza dell'intervallo senza contesa (PCF burst) in cui la stazione abilitata dall'AP può trasmettere i propri dati; alla fine del NAV inizia un periodo di contesa DCF in cui le stazioni in modalità DCF si contendono un intervallo in cui trasmettere i propri dati (DCF burst). Dunque c'è un'alternanza di fasi PCF e DCF. La procedura è semiperiodica, in quanto l'inizio dei NAV è deterministico ma i periodi PCF possono prolungarsi.



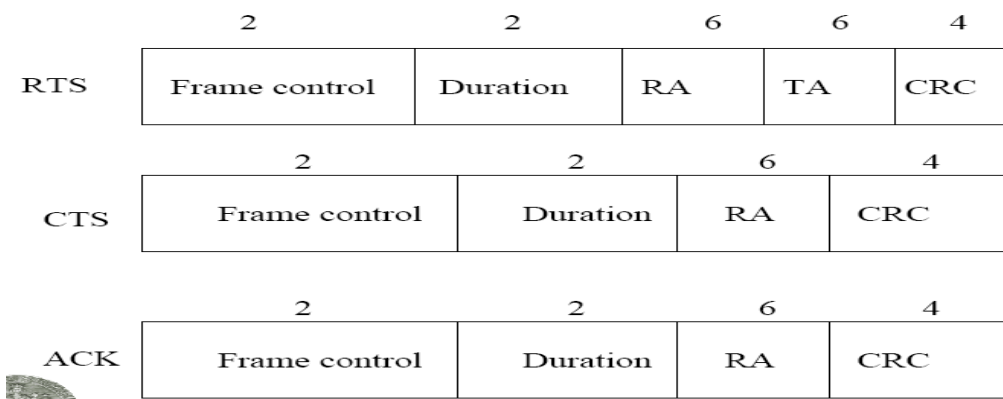
4.3.1.3 Formato della frame MAC

In 802.11 abbiamo tre tipologie di frame, frame di Gestione, di Controllo e Dati, che hanno la stessa struttura:



- **Frame Control:** informazioni di controllo da una stazione all'altra. Contiene 2 bit per la versione del protocollo, 2 bit per il tipo di frame (gestione, dati o controllo), 4 bit per il sottotipo di frame (ad ACK, CTS, etc.), 2 bit (From/To DS) per specificare se la frame è destinata a lasciare o meno il sistema di distribuzione che collega gli AP, 1 bit che indica se ci sono ulteriori frammenti della frame da inviare, 1 bit per indicare se si tratta di una ritx, 1 per mandare la stazione in basso consumo dopo la Tx (Pwr mgt), uno per indicare se devono essere inviati altri dati, uno per la cifratura e uno per indicare che le frame devono essere elaborate in ordine di arrivo.
- **Duration/ID:** intervallo di tempo in cui la Stazione può trasmettere (eventualmente identificativo della stazione che trasmette la frame);
- **Indirizzi 1,2,3,4:** vari indirizzi a seconda del formato (es. Indirizzi multicast, indirizzi di nodi o di gruppi di nodi, indirizzi AP);
- **Sequence control:** numero per la frammentazione + numero sequenziale di frame;
- **Frame body:** carico utile, cioè una MSDU (o NPDU) oppure informazioni di gestione o di controllo;
- **FCS (Frame Checks Sequence):** contiene il CRC (Cyclic Redundancy check) calcolato considerando l'intestazione e il corpo della frame.

Le frame RTS, CTS e ACK



Duration=durata della frame, RA/TA=indirizzo del Rx/Tx

4.3.2 Il sottolivello 802.11 MAC management

Questo sottostrato gestisce le procedure di associazione, riassociazione e dissociazione di un terminale presso un AP, la potenza e la sicurezza. Facciamo riferimento ad una mobilità interna al sistema di distribuzione che collega più AP (il sistema di distribuzione si fa carico della gestione della mobilità).

Gestione della mobilità:

L'AP invia periodicamente un beacon contenente il suo ID, un Timestamp (per consentire alle MS di sincronizzarsi con esso), i bit di power management (per mettere le MS in basso consumo) e per il roaming (From/To DS), ed il TIM (Traffic Information Map) che indica se l'AP ha dati da inviare ad una data MS. Le MS rilevano i segnali di beacon e cercano di associarsi all'AP il cui segnale di beacon ha il livello di potenza più alto.

Per associarsi ad un AP la MS invia una frame di richiesta a cui l'AP risponde con una frame di risposta, con cui la MS acquisisce le informazioni contenute nel beacon. Dopo l'associazione vi è una fase di autenticazione, dopo la quale la MS può inviare e ricevere dati dall'AP. Man mano che la MS si sposta rileva diversi livelli del segnale di beacon dell'AP con cui è sincronizzata; quando il livello del segnale scende al di sotto di una certa soglia (detta soglia di handoff), la MS deve riassociarsi ad un altro AP; a tale scopo la MS può usare una scansione passiva, basata sull'ascolto dei segnali di beacon (la MS si sceglierà quello più forte), oppure una scansione attiva, basta sull'invio di probe request: ogni AP che rileva la probe request risponde con una probe response contenente le stesse informazioni del segnale di beacon, la MS sceglie l'AP con la probe request più

forte e gli invia una richiesta di riassociazione alla quale il nuovo AP risponde con una risposta di riassociazione contenente tutte le informazioni per la comunicazione. La notifica della riassociazione al vecchio AP non è standardizzata, la procedura IAPP prevede ad esempio che il nuovo AP comunichi l'avvenuta riassociazione con una richiesta di handoff al vecchio AP che risponde con una risposta di handoff.

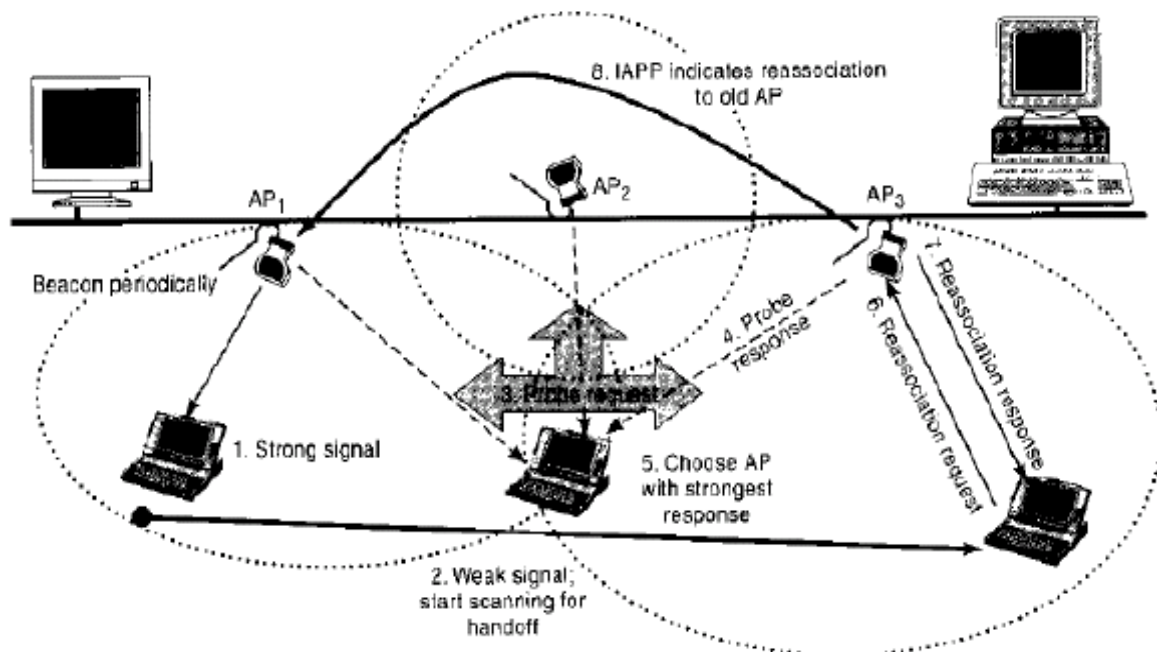
Nota: BSS (*Basic Service Set*) rappresenta l'insieme dei terminali che appartengono ad una BSA (*Basic Service Area*), che è la copertura dell'AP, cioè l'area in cui i terminali sono serviti da quell'AP piuttosto che da un altro. Un insieme di almeno due BSS, collegate tra loro dal sistema di distribuzione, costituisce un ESS (*Extended Service Set*).

Nota: L'handoff è la procedura che permette di garantire continuità del servizio quando una stazione mobile passa da una BSS ad un'altra BSS; essa ascolterà quale dei due segnali che riceve dalle 2 BSS è il più intenso e sceglierà di farsi servire dalla corrispondente BSS. La procedura di handoff è necessaria per mantenere aggiornata la rete e sapere istante dopo istante quale BSS sta servendo le varie MS.

Si noti che associarsi all'AP più forte non è sempre conveniente; dipende dal traffico, perchè ci può essere un effetto cattura oppure troppe contese da fare.

Si tenga presente che la riassociazione è una procedura più leggera rispetto alla prima associazione.

Nota: Si parla di handover orizzontale quando la MS si sposta all'interno di una stessa rete, di handover verticale se passa da una rete ad un'altra. Si noti che **Handover e Handoff sono termini equivalenti**.



Gestione della potenza e della sicurezza:

La gestione della potenza è necessaria perchè le MS funzionano tipicamente a batteria, e quindi occorre limitare i consumi per aumentare la durata delle batterie. Tramite il bit di power management del segnale di beacon l'AP indica alle MS di mettersi in uno stato di basso consumo (sleeping mode); le MS si risvegliano ogni tot ms e analizzano il campo TIM del beacon per capire se l'AP ha bufferizzato dati per esse; quando una MS apprende che l'AP ha dati da inviargli, invia ad esso un messaggio di OK e l'AP gli spedisce i dati al successivo risveglio.

Relativamente alla gestione della sicurezza, nello standard 802.11 le MS devono autenticarsi prima di accedere alla rete ma non è previsto un particolare schema di autenticazione: a seconda dell'applicazione si va dall'handshaking alla crittografia a chiave pubblica. Per la privacy dei messaggi si usa l'algoritmo WEP (Wired Equivalent Privacy), che è stato introdotto con la versione "1" del protocollo (2004).

Capitolo 5

Hiperlan 1 e 2

Hiperlan è sostanzialmente la versione europea di IEEE 802.11. La differenza sostanziale tra Hyperlan e IEEE 802.11 è che il primo è nato come rete voice-oriented mentre il secondo come data-oriented.

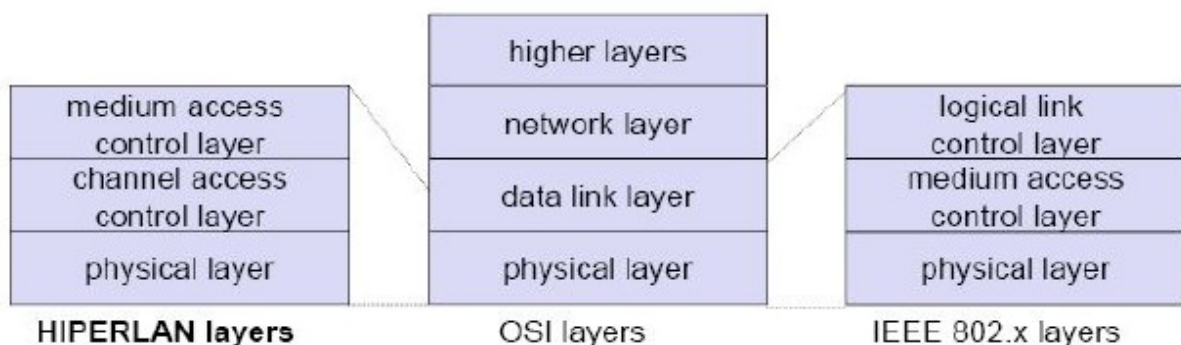
5.1 HIPERLAN 1

HIPERLAN 1 (**H**igh **P**ERformance **L**ocal **A**rea **N**etwork (type **1**)) è importante perchè ha introdotto delle soluzioni pioneristiche, ad es. ha proposto per la prima volta l'uso dei 5 GHz poi adottato anche da IEEE 802.11, il networking multihop (alcuni terminali fungono da bridge partecipando alla distribuzione dei pacchetti) e nonché l'uso dell'OFDM. In H1 l'enfasi è sul paradigma ad hoc.

5.1.1 Architettura protocollare

HIPERLAN 1 copre lo strato fisico e solo parte dello strato DL dello stack OSI, mentre 802.x copre sia strato fisico che DL.

Hiperlan 1 vs OSI vs IEEE

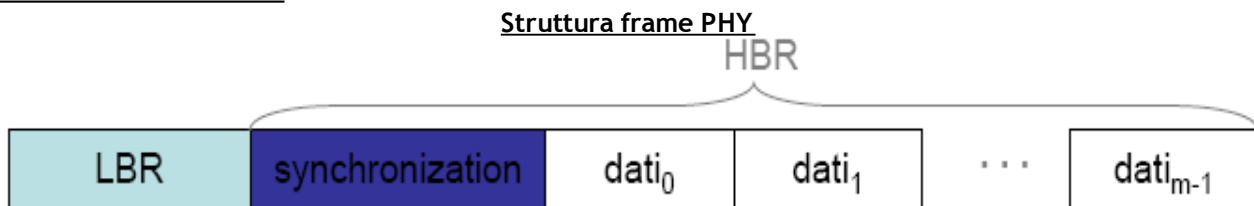


In particolare il livello DL è suddiviso in due sottostrati: **H-MAC**, che si occupa dell'accesso al mezzo, e **H-CAC**, che si occupa dell'accesso al canale. Questo perchè nello strato MAC di Hiperlan devo risolvere problemi legati alla qualità del servizio. In 802.11 per dare delle priorità uso le diverse Frame Interspace, in Hiperlan questa suddivisione non mi basta più perchè voglio che pacchetti di fonia siano accettati prima di pacchetti dati e ciò richiede uno strato MAC più complicato che in 802.x.

5.1.1.1 Livello fisico

Si occupa della modulazione, del framing, del controllo di errore e del channel sensing. Si usa una banda di 200MHz con spaziatura di 40MHz --> 5 canali. Per supportare velocità di 23.5Mbps il ricevitore usa un decisore basato su feedback (DFE) che elimina i bit già rivelati che hanno ISI con altri bit riducendo così parte dell'interferenza, per contro si ha un ritardo di trasmissione perchè la decisione non è presa immediatamente ma solo dopo la rivelazione dei bit.

Struttura della frame:



Sono previste due soluzioni, LBR (Low Bit-Rate) per velocità a 1.4Mbps usando FSK, e HBR per velocità di 23.5Mbps usando GMSK (la MSK è una modulazione a fase continua); si usano 450 bit per la sincronizzazione e il training e un massimo di 47 blocchi dati da 496 bit; per elevate velocità (>1.4Mbps) del terminale occorre ridurre il numero di blocchi dati (cioè accorciare la frame) per poter continuare a trascurare la tempo-varianza del canale e i problemi di sincronizzazione.

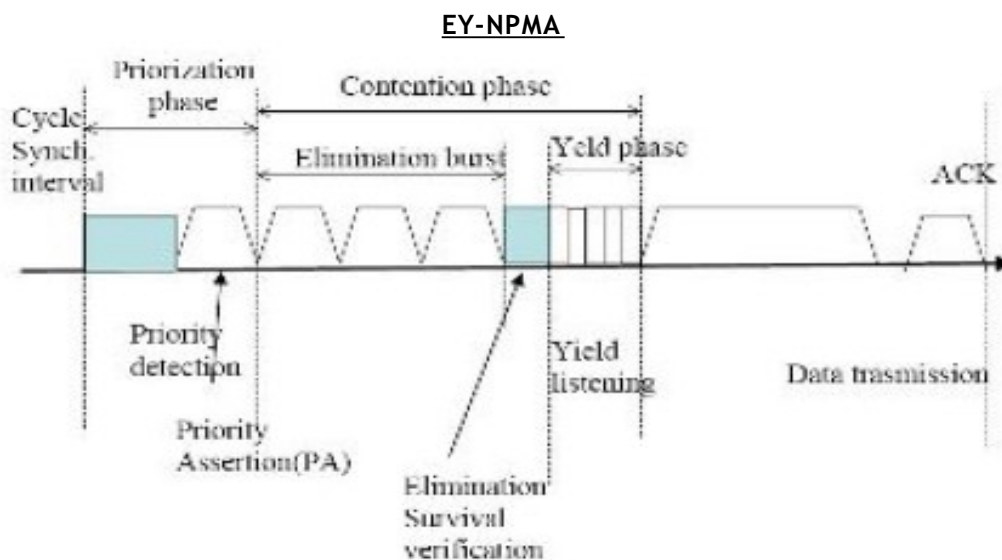
5.1.1.2 Livello Data Link

Come accennato, il livello DL si suddivide in due sottostrati: CAC e MAC.

Livello CAC:

Il livello CAC offre un servizio di Tx dati senza connessione allo strato MAC, ogni pacchetto ha sei campi indirizzi (mittente, destinatario, vicini Rx, vicini Tx (per il multihop)) ed ha associata una priorità tra 0 (alta) e 4 (bassa) (tale priorità CAC è assegnata dallo strato MAC in base alla priorità MAC e al tempo di vita residuo del pacchetto), il protocollo di accesso è del tipo "**ascolta prima di parlare**". Il cuore del sottostrato CAC è la procedura in tre fasi per l'accesso al canale **EY-NPMA** (**E**limination-**Y**ield **N**on-preemptive **P**riority **M**ultiple **A**ccess), che è simile a CSMA/CA:

1. **Priorization**: In questa fase vengono selezionati i nodi con maggiore priorità di trasmissione. Se il canale è impegnato inizia la fase di *priority detection*, ovvero un intervallo di un certo numero di slot, in cui ogni stazione ascolta per un numero di slot pari alla sua priorità (ad es. chi ha priorità 2 ascolterà per 2 slot prima di tx) dopodiché se sente il canale libero Tx un burst per notificare la sua priorità, altrimenti si ritira. Al termine di questa fase avremo un certo numero di stazioni che hanno annunciato la loro priorità (*priority assertion*).
2. **Contention**: I nodi selezionati nella fase 1 si contendono l'accesso al canale. Questa fase prevede due sottofasi:
 - *elimination*: le stazioni sopravvissute alla prima fase scelgono una slot casuale in cui Tx un burst e si mettono in ascolto fino a tale slot; se una stazione, nella slot scelta, sente una trasmissione si ritira, altrimenti trasmette il suo burst notificando così di aver vinto la contesa; i terminali che sentono questo burst si autoeliminano;
 - *yield*: la stazione superstita aspetta ancora un tempo random prima di trasmettere (perché è possibile che due stazioni con la stessa priorità hanno scelto la stessa slot); se non ascolta altre trasmissioni finalmente può trasmettere.
3. **Transmission**: il nodo superstita trasmette.



Il vantaggio di un algoritmo così complesso è che la probabilità di collisione è $< 3\%$.

Livello MAC

Il livello MAC offre un servizio senza connessione per trasportare frame da un nodo sorgente ad uno (o più) nodi destinatari. Offre un supporto alla QoS assegnando ad ogni pacchetto una priorità (0=alta/1=bassa) e un tempo di vita; sulla base della priorità e del tempo di vita residuo il livello MAC assegna un livello di priorità CAC tra 0 e 4.

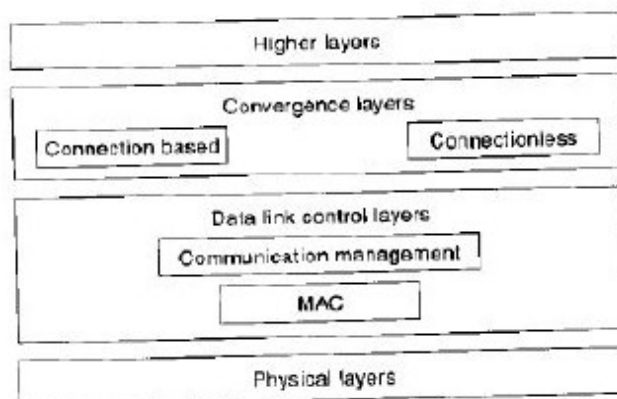
Inoltre offre un servizio di crittografia e di Power-saving: un nodo (p-saver) annuncia che ascolta solo in certi intervalli di tempo; alcuni nodi vicini (p-supporter) trasmettono i loro dati verso p-saver solo in quegli intervalli.

5.2 HIPERLAN 2

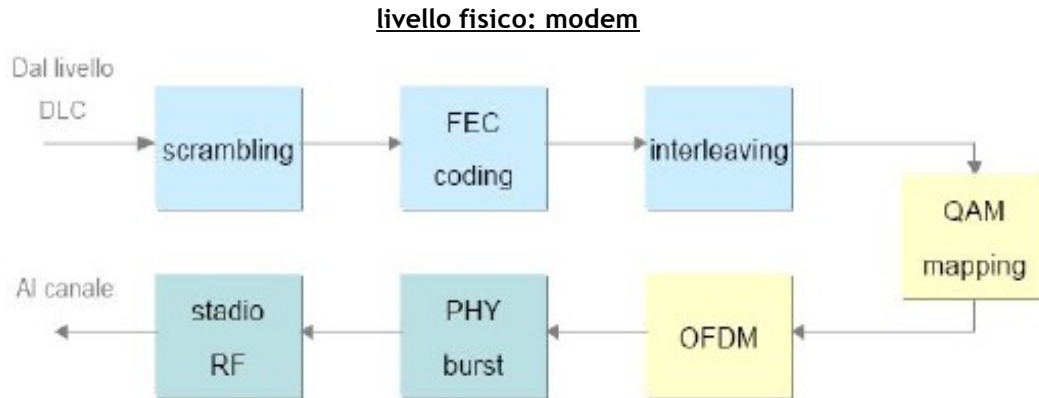
HIPERLAN 2 fornisce sia servizi orientati alla connessione che servizi connectionless; estende il paradigma ad hoc di HIPERLAN 1 prevedendo anche lo schema centralizzato con AP; il MAC è basato su TDMA/TDD, cioè l'accesso al canale non è più distribuito ma centralizzato (facilitando il supporto alla QoS); prevede anche handover verticale IP-based garantendo interoperabilità con Ethernet, UMTS, connessioni punto-punto (es. dial-up modem) e reti ATM-based; e usa OFDM con link adaptation, cioè a seconda della qualità del canale la velocità di trasmissione viene automaticamente modificata da 6 a 54 Mbps.

5.2.1 Architettura protocollare

H2 prevede tre strati, lo strato **Fisico**, che è simile a quello di IEEE 802.11a, lo strato **DLC**, che fornisce un link logico tra l'AP e la MS e si occupa dell'accesso al mezzo e della connessione, e lo strato di **Convergenza multipla**, che si occupa di mappare i pacchetti dei protocolli superiori (ATM, UMTS, Ethernet) in pacchetti per il DLC garantendo l'interoperabilità.



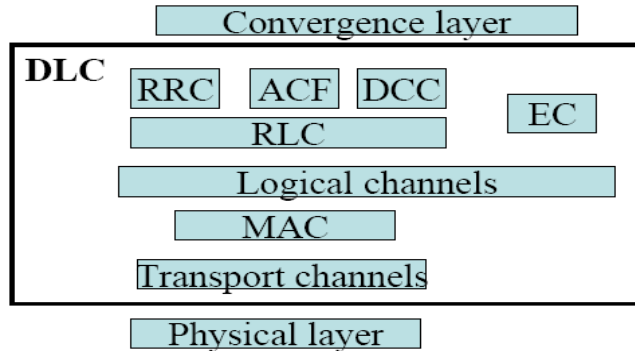
5.2.1.1 Livello fisico



Il livello fisico è del tutto simile a quello di 802.11a. I dati provenienti dal livello DLC vengono sottoposti allo scrambling (di lunghezza 127 con $S(x) = x^7 + x^4 + 1$ per whitening) per decorrelare i simboli che vanno a pilotare il codificatore; poiché il FEC può correggere errori solo su 4-5 bit si usa l'interleaving (con profondità 1 simbolo OFDM) per spalmare burst di errori su più flussi informativi; la scelta del mapping (BPSK, QPSK, 16QAM, 64QAM) dipende dalla qualità del canale: le opzioni di mapping/codifica forniscono la capacità multirate, cioè tramite diverse costellazioni e tassi di codifica si possono ottenere diverse velocità. Poiché si usa l'OFDM (con le stesse specifiche di 802.11a), occorre usare oscillatori stabili per evitare ICI (nello stadio RF). Diversi PHY mode (5 tipi) possono essere negoziati sulla base della QoS e della qualità del collegamento (link adaptation).

Note: Lo scrambling serve a rendere piatto lo spettro del segnale noise-like; in pratica fa uno sbiancamento dello spettro (poi in Rx occorre ricolorare); scrambling=strapazzamento: cerca di decorrelare i campioni, in modo che il FEC veda sempre lo stesso tipo di segnali. Per il FEC si usa tipicamente un codice convoluzionale, ovvero codice ad albero (N.B. non è un codice a blocco) in cui il codificatore associa ad ogni bit d'informazione in ingresso un certo numero di bit in uscita, che dipenderanno dai bit in ingresso e da un certo numero di bit precedenti memorizzati in un buffer (memoria convoluzionale); più è grande il buffer più la codifica è complessa ma tanto più il codice è robusto (cioè in grado di correggere gli errori); si usano differenti schemi di puncturing per ottenere diversi tassi di codifica ma limitare la complessità. Il FEC può correggere errori solo su 4-5 bit, per questo si usa l'interleaving. L'interleaving si usa per correggere burst di errori introdotti dal canale nelle situazioni di peggior funzionamento e che non possono essere corretti col FEC: con l'interallacciamento riesco a spalmare il burst di errori su più trame e a correggerle col codice convoluzionale. Nello stadio RF la stabilità degli oscillatori è necessaria perchè, facendo OFDM, le frequenze nelle sottoportanti potrebbero interferire.

5.2.1.2 Livello DLC



Il livello DLC gestisce l'accesso al mezzo e la comunicazione. Si occupa in particolare della formazione delle frame per i canali logici e di trasporto. I canali logici specificano la semantica dell'informazione trasportata e sono associati ai canali di trasporto che specificano il formato dell'informazione, tramite il protocollo MAC (che usa il TDMA/TDD).

I canali logici sono usati per implementare 4 operazioni della rete:

1. **Radio link control (RLC)** (trasporto per RRC, DCC e ACF).
2. **Radio resource control (RRC)** (handover, dynamic frequency selection, sleeping mode and power saving operation).
3. **DLC connection control (DCC)** (setup/release/modify della connessione, join/leave multicast e broadcast).
4. **Association Control function (ACF)** (associazione e dissociazione, scambio chiavi, autenticazione).

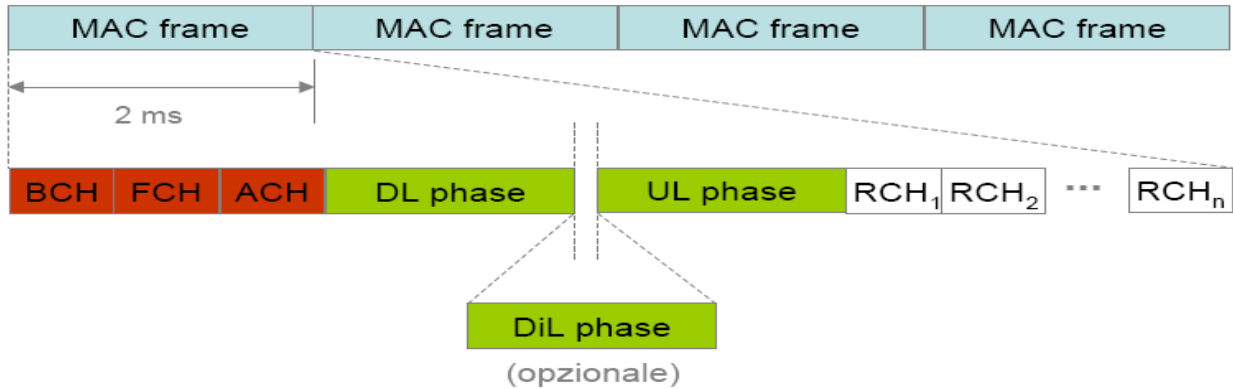
Il DLC supporta anche un meccanismo di error control (EC) sui canali logici.

Rispetto ad Hiperlan 1 manca il CAC perchè qui l'accesso è TDD/TDMA e la gestione delle contese è a carico dell'AP (diversamente anche da 802.11 dove col DCF non c'è questo aspetto gerarchico dell'AP). Questo perchè H2 è una rete voice-oriented, e i requisiti stringenti sul ritardo spingono verso una tecnica TDMA. L'AP effettua uno scheduling centralizzato per assegnare dinamicamente le risorse, supportare la QoS e fornire trasmissioni collision-free.

Si usa la tecnica di accesso random ALOHA con prenotazione ad uno specifico canale.

Per supportare la QoS H2 cambia la periodicità dei segnali trasmessi; ad esempio si possono assegnare tre periodi, quello più lungo per la Tx dei messaggi broadcasting, quello medio per la Tx dei pacchetti dal terminale a minore priorità, e quello più corto per la Tx dei pacchetti dal terminale a maggiore priorità.

Formato frame MAC:



Ogni frame dura 2 msec ed è costituita dai seguenti campi:

- **BCH** = Broadcast Channel: usato per il controllo risorse radio.
- **FCH** = Frame CHannel: usato dall'AP per comunicare ad un terminale le risorse date.
- **ACH** = Access feedback Channel: usato dall'AP per informare una MS di una precedente collisione nel tentativo di accesso.
- **RCH** = Random CHannel: usate dalle MS per richiedere assegnazione di risorse; sono le slot di contesa in cui le stazioni cercano di Tx.
- **DL phase** = traffico downlink (AP --> MS). **UL phase** = traffico uplink (MS --> AP).
- **DiL phase** = traffico direct link (MS --> MS) (opzionale).

Quando una MS vuole trasmettere invia una richiesta di risorse all'AP usando uno dei canali RCH; se si verifica una collisione l'AP lo notifica nel canale ACH della frame successiva e la MS usa l'algoritmo BBE per la ritrasmissione, altrimenti l'AP comunica le risorse assegnate alla MS (UL, DL, DiL) inviando una resource grant nel canale FCH.

Associazione e riassociazione:

La MS ascolta il BCH di differenti AP e sceglie quello con la migliore qualità radio. Per entrare nella rete la MS manda una richiesta di associazione all'AP scelto, che risponde col proprio MAC-ID. Dopo l'associazione vi è l'autenticazione ed uno scambio per la crittografia. Dopo l'associazione la MS può richiedere un Dedicated Control Channel (DCCH) per effettuare il setup di una connessione DLC. Per la disassociazione la MS notifica all'AP che non vuole più comunicare, oppure l'AP realizza che la MS non è più attiva e la elimina dalla rete liberando tutte le risorse ad essa assegnate.

Per la riassociazione (handover) la MS può usare uno scanning passivo, ascoltando i canali BCH degli AP, oppure attivo, usando segnali di probe. La MS può passare le info della connessione al nuovo AP, oppure può passare al nuovo AP solo l'ID del vecchio AP, nel qual caso il passaggio delle info avviene via rete fissa senza sprecare risorse wireless.

Capitolo 6

Reti Personali Wireless

Le W-PAN sono una soluzione per la copertura di una area limitata, che richiede bassi costi e consumi di energia. Tali reti operano nella banda a 2.4GHz (possibilità di interferenza con dispositivi IEEE 802.11), e sono tipicamente usate per connettere unità/periferiche, per realizzare reti ad hoc, o per fare da bridge tra reti eterogenee.

6.1 La tecnologia Bluetooth 802.15

Una rete Bluetooth è una rete ad hoc in cui un nodo può assumere la funzione di *master* o di *slave*. Il master fornisce il timing (il clock) e la sequenza di salti per la tecnica FHSS, gli slave devono sincronizzarsi (N.B. le stazioni possono avvicinarsi come Master).

Una rete formata da un unico master e al massimo 7 slave attive è detta piconet; un insieme di piconet interconnesse forma una scatternet, nella quale ci saranno nodi che sono master in una piconet e slave in un'altra (o in altre) piconet. Una unità può "saltare" da una piconet ad un'altra.

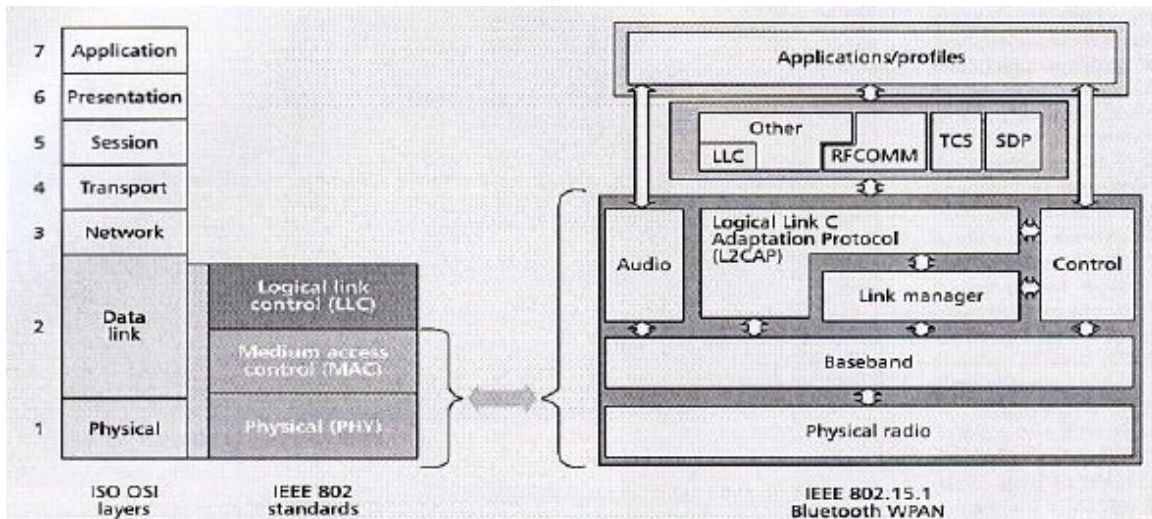
Bluetooth ricorre a trasmissione di pacchetti mediante polling. Tutte le comunicazioni possono avvenire tra slave e master utilizzando TDD con l'esclusione di connessioni dirette tra slave e slave (il che non rende possibile il multihop se non attraverso il master).

Il master può trasmettere solo in slots "pari" mentre la slave può trasmettere solo in slots "dispari".

6.2 Lo stack protocollare di BT

BT è una suite di protocolli divisi in tre gruppi logici:

1. Il protocollo Trasporto
2. Il protocollo Middleware
3. Il gruppo Applicazioni.



Il **protocollo Trasporto** si occupa della localizzazione reciproca dei dispositivi BT e della gestione dei link fisici e logici con lo strato Middleware e con le applicazioni. Esso include:

- lo strato **RF** (fisico), che si occupa di tutte le specifiche del modem;
- lo strato **Bandabase** (fisico), che abilita la connessione fisica wireless in RF tra i dispositivi; in particolare, definisce come dispositivi cercano gli altri dispositivi e come essi si connettono tra loro. In questo strato sono definite le regole *master/slave*, le *sequenze FHSS*, e i tipi di pacchetti;
- il **Link manager** (MAC), è responsabile del processo di instaurazione della connessione tra i dispositivi; si occupa del consumo di potenza, della QoS e della sicurezza;
- lo strato di adattamento **L2CAP** (MAC), durante una connessione adatta i protocolli degli strati superiori per la trasmissione in bandabase; fornisce servizi senza connessione e orientati alla connessione agli strati superiori, e si occupa della segmentazione e il riassemblaggio delle unità dati dei livelli superiori;
- lo strato **Controllo** (MAC), fornisce un'interfaccia di comando per lo strato Link Manager e Baseband per tenere conto dei differenti hardware coinvolti;
- lo strato **Audio** (MAC), interfaccia direttamente le applicazioni al baseband per la trasmissione dei pacchetti audio.

Il **protocollo Middleware** interfaccia le applicazioni al gruppo trasporto, e contiene un'interfaccia a radiofrequenza **RFCOMM**, che emula una porta seriale e consente di utilizzare standard già esistenti (come PPP, TCP/IP, WAE/WAP), il protocollo **TCS** (Telephony Control Specifications), che serve per la telefonia, e **SDP** (Service Discovery Protocol), che interfaccia il middleware alle applicazioni.

Alcuni esempi di applicazioni (**gruppo Applicazioni**), sono *vCard su BT*, *WAP su BT*, e *Cordeless Telephone su BT*.

6.2.1 Il livello fisico di BT (Baseband)

Usa una banda di 80Mhz nella banda a 2.4Ghz, il TDD, grazie al quale non c'è una sezione radio destinata unicamente alla ricezione ed una destinata alla trasmissione ma un unico chip che commuta da Tx a Rx (ogni unità trasmette e riceve a slot alternate), e il FHSS: 79 canali da 1MHz, modulazione 2-GFSK (1Mbps), slot di 625µsec (dunque 625 bit, visto che Tx a 1Mbps), e hopping-rate di 1600 hop/s (Fast-FHSS).

Ad ogni piconet (master) è una specifica sequenza di 32 salti, determinata dall'identità della piconet e dal clock del master. I 79 salti di 1 MHz sono suddivisi in due gruppi: salti "pari" e "dispari"; ad ogni completamento di una sequenza di 32 salti si avvicenda una nuova sequenza di salti ottenuta shiftando (in avanti) di 16 salti la precedente. Quando cambia il clock e/o l'identificativo cambia il pattern di salti.

Per proteggere l'informazione si introduce FEC sull'header, e opzionalmente sul payload.

Nota: Si tenga presente che in BT possono esserci anche 20-30 piconet nella stessa area; a differenza di IEEE 802.11, in cui nella stessa area possono esserci al più 2-3 BSS.

6.2.2 Il livello MAC di BT (Link Mgr e L2CAP)

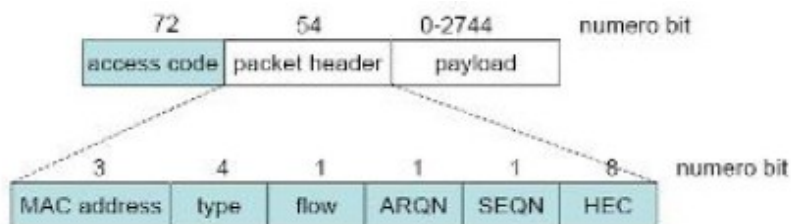
Il MAC è un meccanismo FH-CDMA/TDD che impiega un polling per stabilire un link: la TDD evita l'interferenza cross-talk tra Tx e Rx; il FH con slot di 625µsec garantisce maggiore tolleranza all'interferenza; è un CDMA perchè ogni piconet usa un codice diverso (non usa DSSS/CDMA perchè richiede il controllo centralizzato di potenza, per evitare il fenomeno near-far, e, quindi, non è compatibile con BT che vuole fornire reti ad hoc). Il metodo di accesso in ogni piconet è TDMA/TDD. La condivisione del mezzo è ottenuta attraverso un polling gestito dal Master.

Tale livello offre 2 tipologie di servizio:

1. **Synchronous Connection-Oriented (SCO):** servizio simmetrico, punto-punto, tipicamente voce, trasmissione *single-slot*, velocità costante a 64 kbps, nessuna ritrasmissione (per evitare la latenza temporale), accesso: con prenotazione.
2. **Asynchronous Connectionless Link (ACL):** simmetrico/asimmetrico, punto-multipunto, tipicamente dati; trasmissione *multislot* (1,3,5 slot), max velocità 721/57.6 kb/s (asimm.), 432.6 kb/s (simm.), accesso: *polling* da parte del master (implicito o con pacchetti di *poll*), cioè è il master a destinare le risorse agli slave che ne hanno fatto richiesta.

6.2.3 Formato delle frame

La frame BT dura 1,3 o 5 slot a seconda del tipo di pacchetto ed ha il seguente formato:



- **Access Code.** Serve per la sincronizzazione ed è formato da: *Preambolo* (4), *Word di sincronizzazione* (64 bit: sequenza PN con buone proprietà di auto e mutua correlazione), *Coda* (4 opzionale). Gli Access code possono essere di 3 tipi:
 1. *Channel AC*: identifica la piconet, cioè il Master.
 2. *Device AC*: identifica una Slave; è utilizzato per procedure speciali come il paging, e non include i bit di coda.
 3. *Inquiry AC*: ha due possibili varianti:
 - *General*, per scoprire nuove unità entro il raggio di azione.
 - *Dedicated*, per scoprire solo le unità che condividono speciali caratteristiche (fax, stampanti, etc.).
- **Packet header.** I 18 bit ripetuti per tre volte: FEC (codice a ripetizione:1/3); è formato da: Indirizzo MAC (fino a 7 slave), tipo pacchetto (16 possibili pacchetti), controllo flusso, ARQN/SEQN (per comunicare l'ACK / per ordinare i pacchetti), controllo di errore (HEC).
- **Payload.** Differenti payloads specificati da differenti codici di pacchetto; ciò consente di realizzare differenti tipologie di applicazioni (voice-oriented, data-oriented); il M può usare per ogni S uno dei possibili formati.

I 4 bit del campo *Type* dell'Header consentono di specificare 16 formati di pacchetto per il payload:

- 6 *Asynchronous Connectionless (ACL)* per la Tx di pacchetti dati protetti **DM1**, **DM3**, **DM5**, e non protetti **AUX1**, **DH1**, **DH3**, **DH5**; sono numerati a seconda del numero di slot che utilizzano.
- 3 *Synchronous Connection Oriented (SCO)* per la Tx di pacchetti voce **HV1**, **HV2**, **HV3** (HV=High Voice); sono numerati con livelli di qualità crescenti: i pacchetti HV1 sono spediti con cadenza di uno ogni sei slot, HV2 ogni 4 slot, HV3 ogni due slot.
- 1 *Applicazioni di integrazione voce/dati*, pacchetti voce/dati **DV**;

- 4 *Pacchetti di controllo*; pacchetti di controllo baseband **Null**, **Poll**, **ID**, **FHS**. Il pacchetto **ID** occupa metà slot e trasporta l'access code e il codice del tipo di pacchetto (è utilizzato prima di stabilire una connessione per comunicare un indirizzo); i pacchetti **NULL** e **POLL** sono usati per gestire il polling e si differenziano per il fatto che NULL non richiede l'ACK mentre POLL lo richiede; il pacchetto **FHS** trasporta l'access code, ovvero le informazioni per la sincronizzazione.

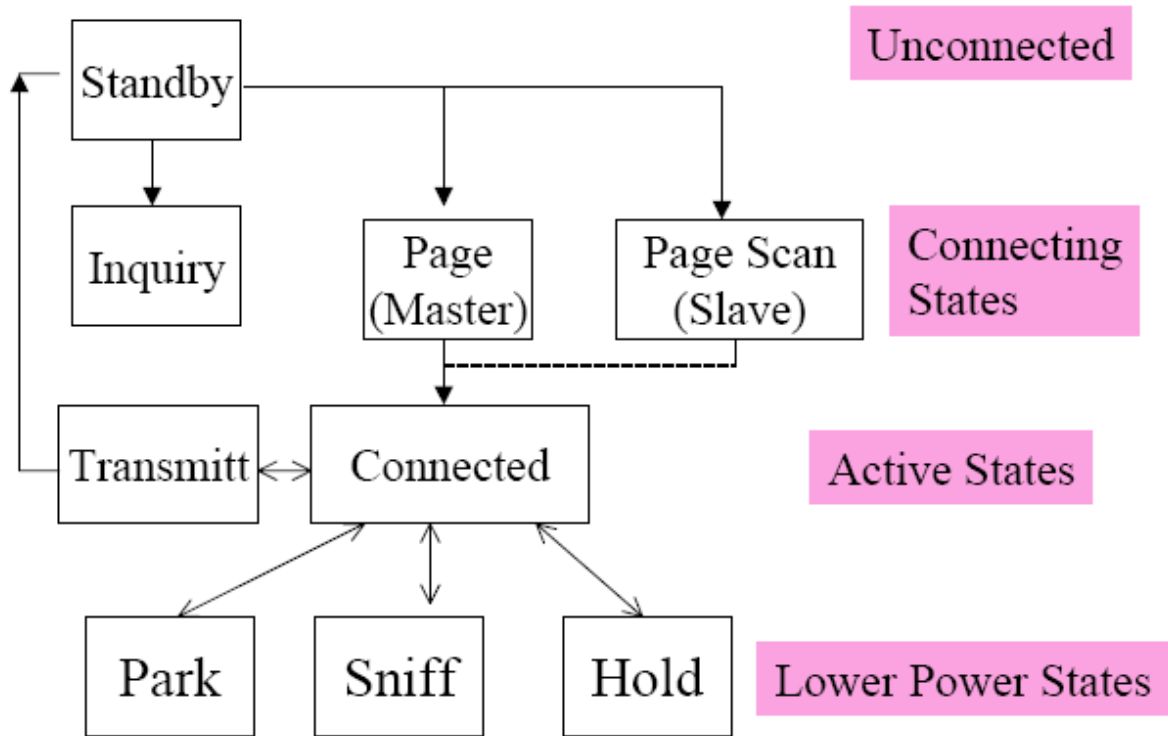
6.3 Gestione della connessione

Ricordiamo che in una piconet possono esserci al più 7 slave attive; inoltre, possono esserci al più 255 nodi in uno stato di “*park*” (cioè precedentemente attive ma ora costrette a rilasciare le risorse) se si usa un indirizzamento diretto, mentre con una modalità di indirizzamento indiretto non ci sono limiti.

La specifica BT stabilisce che l'inizializzazione della rete avviene mediante un unico algoritmo di *inquiry* (ricerca) e *paging*:

All'inizio della formazione della piconet, tutti i componenti sono nello stato **SB** (Stand by, stato di non connessione); poi, uno dei componenti inizia una procedura *inquiry*, diventa Master (se scopre almeno un terminale) e registra tutti i terminali **SB** che così diventano S; l'identificazione e il timing di tutte le S è eseguito mediante i pacchetti FHS (che trasportano le info di sincronizzazione). Una connessione inizia con un messaggio di **PAGE** con cui il Master spedisce il suo timing e la sua identità alla Slave. Quando la connessione è stabilita (stato attivo **connected**), la sessione di comunicazione inizia (si passa nello stato attivo **Trasmit data**) ed alla fine la S può essere rimandata nello stato **SB**, oppure in uno stato di basso consumo **Park**, **Sniff** o **Hold**. **Park** è uno stato in cui la slave restituisce il suo indirizzo attivo, che sarà assegnato ad un altro nodo, ma resta sincronizzata alla rete e, occasionalmente, ascolta il traffico del M per acquisire i messaggi in broadcasting. **Sniff** è uno stato in cui il nodo si sveglia per la trasmettere i suoi dati in una slot predefinita per poi ritornare in modalità sleeping fino alla prossima slot di sniff. **Hold** è uno stato di basso consumo in cui non è previsto nessun trasferimento di dati, ed è usato quando vi sono molte piconet interconnesse.

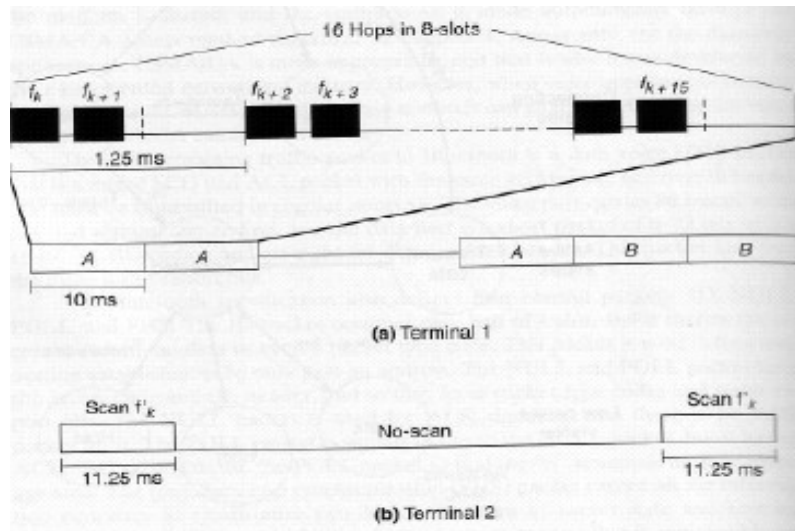
Dunque un nodo BT può essere in uno degli stati mostrati nella seguente figura:



6.3.1 Paging ed Inquiry in Bluetooth

Procedura di sincronizzazione tra due terminali:

Le procedure di paging ed inquiry si basano sul seguente meccanismo di ricerca tra due terminali che non sono sincronizzati, ma che conoscono entrambi l'indirizzo di un Master.



I due terminali conoscono l'indirizzo di 48 bit di un Master in base al quale possono generare un comune pattern di 32 hops e una sequenza PN comune per l'access code di tutti i loro pacchetti. T1 Tx in broadcast 2 pacchetti ID (ognuno occupa mezza frame), contenenti l'access code comune, su 2 frequenze diverse f_k e f_{k+1} e ascolta la risposta nella slot successiva; se T2 non risponde, T1 tenta con altre 2 frequenze, al max per 8 volte (quindi per 10ms, visto che la frame dura 1,25ms); quindi in 10ms Tx 16 frequenze; se dopo gli 8 tentativi T2 non risponde, T1 assume che sta dormendo e ritrasmette lo stesso set di frequenze (A). Se T2 ancora non risponde, T1 assume che non ha usato questo set di frequenze per la scansione e ripete il broadcasting usando le altre 16 frequenze. T2 è nello stato sleeping e si sveglia periodicamente per 11.25 msec effettuando la scansione del canale con una delle frequenze associate al suo access code; quando tale frequenza coincide con una delle 16 usate da T1 si ha un picco all'uscita del correlatore di T2 che segnala a T1 l'avvenuta sincronizzazione. A seconda del tipo di operazione (paging o inquiry), T2 può fare una verifica con una seconda scansione per avere una conferma della sincronizzazione alla stessa frequenza oppure ad una frequenza differente .

Procedura di paging:

E' usata per la ricerca di terminali il cui indirizzo è noto.

1. Come nella procedura di sincronizzazione tra due terminali, in questo caso il Master esegue un broadcasting ripetendo su due frequenze il pacchetto ID che trasporta l'access code del terminale da coinvolgere nella piconet.
2. Nella slot successiva ascolta la risposta e, in caso negativo, ripete la procedura, utilizzando altre due diverse frequenze, fino a coprire le prime 16 frequenze del pattern (in 8 slot, cioè 10 msec).
3. Lo Slave effettua la scansione per 11.25 msec con una delle 32 frequenze del suo pattern di hop, poi va in sleeping mode e al risveglio effettua una nuova scansione.
4. Quando le frequenze coincidono si avrà un picco all'uscita del correlatore sliding dello Slave che a questo punto notifica al Master con il suo pacchetto ID l'avvenuta sincronizzazione.
5. Il Master arresta il broadcasting dei pacchetti ID e invia un pacchetto FHS contenente il suo ID e le informazioni di timing, a cui lo Slave risponde con un altro pacchetto ID in accordo al timing del Master. La connessione è allora stabilita e lo Slave entra a far parte della piconet per lo scambio di informazioni.

Procedura Inquiry:

La procedura Inquiry si esegue quando si vogliono trovare terminali con indirizzo non noto ed è simile a quella di paging, ma in questo caso i terminali destinatari possono essere più di uno, e questo può generare collisioni quando rispondono più terminali. Per evitare tali collisioni, ogni terminale che rileva il picco aspetta un tempo random prima di eseguire una seconda scansione; solo quando rileva per la seconda volta il picco invia al Master la sua identità e il suo timing tramite il pacchetto FHS. In tal modo il Master acquisisce tutti gli ID e i clock nel suo raggio di copertura.

Capitolo 7

Reti Wireless Ad Hoc

Mobile Ad hoc NETWORK (MANET)

Le reti ad hoc sono reti in cui le comunicazioni avvengono terminale-terminale sulla base di un protocollo di tipo peer to peer. Questo comporta tutta una serie di nuove problematiche, ad esempio relative al routing: visto che non c'è l'access point, tutti i terminali devono collaborare all'instradamento dei pacchetti mediante degli algoritmi multihop.

Una rete ad hoc comporta diversi vantaggi: è costruita sulla base di una specifica applicazione e allestita sulla base delle risorse dei nodi disponibili; si evitano i costi ed i tempi di installazione di una rete infrastrutturata; può essere facilmente disinstallata o riconfigurata; e può presentare grande robustezza grazie alla sua natura distribuita, ridondanza dei nodi e assenza di punti centralizzati che possono andare fuori servizio.

Per contro si ha una limitazione delle prestazioni, dovuta all'uso del paradigma di routing multihop e di controllo distribuito.

Le reti ad hoc possono essere usate per molteplici applicazioni: scambio di dati tra portatili, palmari, PDA etc; per la realizzazione di reti domestiche; per eliminare i cavi delle connessioni tra componenti come stampanti, mouse, telefoni cellulari, etc; per controllare impianti a distanza mediante sensori ed attuatori interconnessi attraverso link wireless; per realizzare reti di sensori per il monitoraggio e il controllo di ambienti casalinghi, o per il monitoraggio di risorse (idriche, energetiche, etc).

Idealmente una rete ad hoc dovrebbe essere avere un'adeguata flessibilità per adattarsi alle più differenti applicazioni. Questa capacità di adattamento può essere conseguita ricorrendo ad un paradigma cross-layer adattivo.

Problematiche di progetto:

Per assicurare la scalabilità in reti con un grande numero di nodi, si usano algoritmi basati sul controllo distribuito che si adattano alle condizioni locali sfruttando l'auto-organizzazione, la gestione della mobilità e il routing distribuito. Ma i protocolli distribuiti consumano una significativa quantità di potenza per l'elaborazione locale e lo scambio di messaggi e, quindi, un trade-off interessante riguarda la quantità di elaborazione rispetto a una soluzione centralizzata. Questo trade-off è particolarmente interessante nel caso di reti di sensori con sensori relativamente vicini che acquisiscono segnali fortemente correlati, per i quali un processing locale può dar luogo ad un risparmio significativo di risorse di comunicazione.

Un'ulteriore criticità delle reti ad hoc riguarda i requisiti di energia. Infatti, esiste un trade-off tra la durata per trasmettere un bit e il consumo di energia: quanto più la durata del bit aumenta tanto minore è l'energia spesa per la trasmissione, ma tanto maggiore è l'energia spesa nella circuiteria. Trade-off nella modalità *sleeping*: tale modalità fa risparmiare energia rispetto alla *Stand-by* ma complica il routing, la gestione ed il controllo della rete.

7.1 Architettura protocollare e progetto degli strati

Nelle reti ad hoc il paradigma dell'architettura a strati non può essere pienamente rispettato, perchè richiedono una forte interdipendenza tra gli strati (esigenza di crosslayer), e il layering può dar luogo ad inefficienze.

1. Lo strato **Fisico** riguarda la trasmissione dei bit. Le scelte fatte in questo strato influenzano le scelte degli strati superiori; ad esempio, il livello di potenza influenza gli strati superiori: diminuisce il PER (Packet Error Rate), aumenta il livello di interferenza nei confronti degli altri nodi e quindi il rate di ritrasmissione. Il livello di potenza influenza anche il numero di hop: più basso è il livello maggiore sarà il numero di hop. L'adozione di tecnologia MIMO fa diminuire il PER e quindi avvantaggia gli strati superiori (accesso, networking, trasporto). La potenza va ottimizzata rispetto a tutti gli strati che influenza.
2. Lo strato di **Accesso** definisce come i nodi condividono le risorse. I metodi più diffusi per le reti ad hoc sono le varie versioni di ALOHA, CSMA e i vari metodi basati sullo scheduling. Il controllo di potenza è effettuato perchè la potenza di trasmissione di un nodo influenza i SNR di tutti i nodi --> occorre minimizzare la potenza di Tx di tutti i nodi. Si usa un algoritmo distribuito che aumenta o riduce la potenza Tx a seconda che il SNR è al di sotto o al di sopra di una certa soglia.

3. Lo strato **Networking** è responsabile della connessione end-to-end. Le principali funzionalità dello strato sono:

- **Neighbor discovery**: scoperta dei vicini quando si entra nella rete. La procedura di ND inizia con un segnale di probe con un livello iniziale di potenza. Se la potenza non è sufficiente a stabilire $N \geq 1$ connessioni con i nodi vicini si ripete il segnale di probing con un livello superiore di potenza. La procedura continua finchè non si stabiliscono N connessioni o si raggiunge il massimo livello di potenza consentito. Se N e/o P_{max} sono piccoli, la rete può formarsi in maniera disconnessa: piccoli cluster di nodi che non possono comunicare tra di loro. Se N e P_{max} sono grandi la rete sarà pienamente connessa, ma molti nodi trasmetteranno con livelli di potenza eccessivi rispetto a quelli strettamente necessari --> Spreco di risorse e aumento dei livelli di interferenza. Una volta che la rete è pienamente connessa, si può adottare l'algoritmo distribuito per la ricerca dell'allocazione delle potenze tra i nodi per garantire i SNR target.
- **Routing**: come i pacchetti sono instradati per arrivare a destinazione. Gli algoritmi di routing per le MANET si possono classificare in:
 - **Flooding**: il pacchetto è Tx ai nodi vicini che lo inoltrano ai loro vicini, e così via fino alla destinazione. Ok per reti con pochi nodi ed elevata mobilità.
 - **Reattivi**: l'instradamento avviene solo se un nodo chiede di Tx pacchetti; non occorre mantenere tabelle di routing non in uso corrente, ma si ha un maggior ritardo nella consegna dei pacchetti.
 - **Proattivi**: si distinguono in centralizzati, source driven, e distribuiti. In quelli centralizzati ogni nodo invia le info sul canale e sulla topologia della rete ad un'entità centrale che computa le tabelle di routing per tutti i nodi e le trasmette ai nodi stessi (OK per reti con pochi nodi). In quelli source-driven ogni nodo riceve informazioni sulla intera rete e determina il miglior percorso per inoltrare i suoi pacchetti verso la destinazione, che invia periodicamente all'entità centrale. In quelli distribuiti ogni nodo riceve da suoi vicini le loro informazioni di connettività, sulla base delle quali calcola le tabelle di routing; ogni nodo determina, quindi, il prossimo hop nel percorso basandosi su informazioni locali (Ok per reti con molti nodi ed elevata mobilità).
- **Allocazione dinamica delle risorse**: come la banda e la potenza sono distribuite nella rete. Tipicamente questa funzionalità è svolta da più strati e ricorrendo anche al paradigma cross-layer.

4. Lo strato di **Trasporto** si occupa delle funzioni end-to-end del recupero dell'errore, della ritrasmissione, del riordinamento e del controllo di flusso. Gli stessi meccanismi a livello di link non sono infallibili. Lo strato trasporto fornisce ulteriore protezione nei confronti degli errori. I pacchetti possono arrivare non in ordine a causa del multipath del routing, lo strato trasporto li consegna in ordine allo strato applicazione. L'uso di TCP comporta nelle reti ad hoc elevata inefficienza, perché è stato concepito per reti cablate, nelle quali la perdita di pacchetti è attribuita a problemi di congestioni nei nodi, mentre nelle reti wireless la perdita dei pacchetti è dovuta principalmente all'inaffidabilità del canale. Inoltre nello scenario wireless la capacità di un link dipende da tutte le interferenze associate ai nodi esistenti, e non solo dalle interferenze *presenti* nel link; flussi di traffico assegnati ad un link causeranno interferenza su altri link e quindi modificheranno le capacità e i ritardi degli altri link. Questa forte interdipendenza tra controllo di flusso, routing e allocazione delle risorse rende necessario l'approccio cross-layer.
5. Lo strato **Applicazione** genera i dati da consegnare allo strato Trasporto ed elabora i dati ricevuti da esso. Esso opera una compressione dei dati, la correzione e il mascheramento degli errori. Maggiore è la compressione (minore ridondanza) minore è il data rate richiesto alla rete, ma maggiore è la vulnerabilità agli errori introdotti dalla rete. La ridondanza può essere anche introdotta attraverso una codifica a descrizione multipla, che è una forma di compressione che introduce descrizioni multiple dei dati originali. Questa diversità a livello di Applicazione può essere combinata con la diversità a livello di networking (multipath di rete) dando luogo ad un cross-layer tra strato Network e Applicazione: le differenti descrizioni sono inviate su differenti percorsi.

La QoS (end-to-end data rate o ritardi) ovviamente non può essere garantita da una rete ad hoc; i diversi strati fanno del loro meglio (best-effort come Internet): per favorire qualcuno occorre sfavorire qualcun altro.

7.2 Limiti della capacità e limitazioni sull'energia

Limiti della capacità:

Si dimostra che il throughput (in bits/sec) totale cresce col numero di nodi, e quindi il data-rate per nodo decresce al crescere del numero di nodi, perchè i nodi intermedi usano la maggior parte delle loro risorse per inoltrare pacchetti di altri nodi, e quindi restano risorse insufficienti per spedire i propri dati.

Limitazioni dell'energia:

Quasi sempre i nodi di una rete ad hoc operano con batterie, che in molti casi (reti di sensori) non possono essere ricaricate o sostituite. Le limitazioni in energia condizionano fortemente le operazioni in hardware, la potenza disponibile in trasmissione e il signal processing. Bisogna introdurre tecniche che minimizzano i consumi energetici nel processing necessario in tutti gli strati e l'ammontare di informazione di controllo da scambiare tra i nodi. Le modalità di sleep devono essere ottimizzate, perchè il risparmio che con esse si ottiene è pagato in termini di complicazioni a livello di routing e accesso. La limitazione in energia rende ancora più necessario l'uso di un approccio cross-layer.

A livello **fisico** occorre minimizzare il tempo di Tx; utilizzare modulazioni multisimbolo piuttosto che binarie può portare a risparmi notevoli in applicazioni short-range, a distanze maggiori il consumo per la trasmissione è dominante, e quindi costellazioni con pochi simboli e velocità inferiori (tempi di Tx più elevati) sono più convenienti. La tecnologia MIMO può dar luogo ad un risparmio di energia se la dimensione della costellazione è ottimizzata rispetto alla distanza; infatti, in questo caso, poichè i MIMO possono sostenere data rate più elevati, si riducono i tempi di trasmissione e il sistema può essere, quindi, per più tempo in stato di riposo (sleep).

A livello di **accesso** per aumentare il risparmio di energia occorre diminuire le collisioni, e quindi le ritrasmissioni, e ottimizzare le potenze. Se i nodi devono trasmettere lunghi messaggi, l'accesso random non è attraente poichè possono verificarsi molte collisioni. In questi casi il canale va assegnato in maniera più sistematica attraverso uno scheduling di trasmissione.

Anche le politiche di **routing** possono determinare risparmi del consumo dell'energia, se tutti i nodi della rete sono coinvolti uniformemente nel carico di trasmissione.

L'ottimizzazione dell'energia deve essere fatta lungo tutti gli strati della rete, e può essere basata sui requisiti dell'applicazione.

Capitolo 8

Reti MESH

Le reti **MESH** sono realizzate con una combinazione di nodi fissi e mobili interconnessi tra di loro con link wireless per formare una rete ad hoc multihop. Come nelle MANET le apparecchiature di utente hanno una parte attiva, cioè possono operare da **terminali di utente** ma anche da **router** per altri nodi, estendendo così la copertura della rete. L'interesse per queste reti è dovuto alle enormi possibilità che esse offrono per l'integrazione e l'interoperabilità di reti eterogenee (ad esempio si prevede di integrare Wi-Fi e WiMax per fornire connessioni su lunghe distanze). La tecnologia delle reti MESH è considerata la soluzione più attraente dal punto di vista economico per la realizzazione di reti wireless **scalabili** a larga banda su larga scala

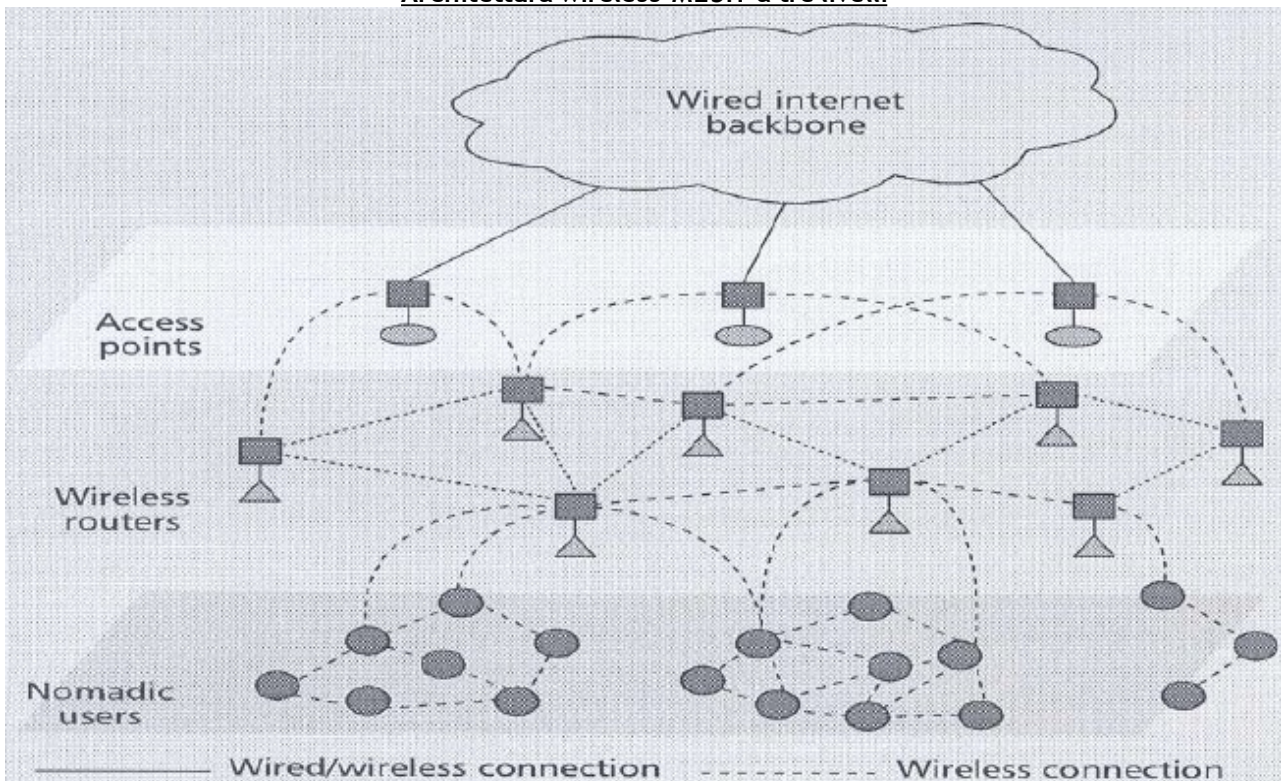
La tecnologia Mesh può essere usata ad esempio per costruire sistemi di trasporto intelligente, applicazioni per Pubblica Sicurezza, per fornire accesso pubblico a banda larga in aree di difficile accesso e/o scarsamente popolate.

Architettura:

Una rete MESH è una rete interamente wireless che impiega comunicazioni multihop per inoltrare traffico e per ricevere traffico da punti di accesso Internet di reti fisse.

A differenza delle MANET, le MESH introducono una gerarchia nell'architettura, rappresentata da nodi dedicati (**wireless routers**) dotati di accesso wired a larga banda ad Internet e che forniscono comunicazioni wireless per lo scambio di dati tra utenti e/o tra AP. La maglia realizzata tra i wireless routers e gli AP ad Internet fornisce un servizio di smistamento del traffico dal nodo di origine al punto di accesso fisso da cui può essere distribuito ad una rete fissa. L'architettura wireless assicura elevata scalabilità e costi contenuti per lo sviluppo dell'accesso capillare wireless ad alta velocità ad Internet.

Architettura wireless MESH a tre livelli



Vantaggi:

La soluzione MESH comporta diversi vantaggi:

1. **Riduzione dei costi di installazione**, perchè il numero degli AP è notevolmente ridotto.
2. **Scalabilità**, grazie al ruolo cooperativo dei terminali mobili, che consente estensione della copertura a livello micro/pico-cellulare, e alla tecnica del Multihop per comunicazioni su lunghe distanze grazie ai nodi wireless intermedi (poichè i link intermedi sono brevi la velocità di trasmissione si mantiene elevata).
3. **Affidabilità**, grazie alla presenza di percorsi ridondanti tra end-points del backbone wireless, e alla presenza di una molteplicità di possibili destinazioni (es. ogni punto di uscita verso la wired Internet).
4. **Autogestione**, grazie alla modalità peer-to-peer che garantisce l'auto-riconfigurabilità e l'auto-cicatizzazione. Il setup della rete è automatico e trasparente per l'utente; quando un nuovo nodo entra nella rete, esso usa tutte le sue funzionalità di tipo "meshing" per scoprire automaticamente i wireless routers e il percorso migliore verso la rete fissa.

Parecchi Gruppi IEEE stanno lavorando alle definizioni di specifiche per reti MESH.