Zanella Francesco 575344

Da 802.11g a 802.11n: innovazioni e ottimizzazioni

Indice

Indice delle figure

Indice delle tabelle

1. Introduzione

Questa tesi si propone di descrivere caratteristiche, potenzialità e innovazioni del nuovo standard IEEE 802.11n, rispetto al diffusissimo 802.11g. Si inizierà quindi descrivendo, nel capitolo 2, l'evoluzione dello standard 802.11 per poi analizzare, nel capitolo 3, tutte le caratteristiche dell'ultima versione.

IEEE 802.11 definisce uno standard per le reti WLAN sviluppato dal gruppo 11 dell'IEEE 802, in particolare per il livello fisico e MAC del modello ISO/OSI, specificando sia l'interfaccia tra client e base station (o Access Point) sia tra client wireless.
Wi-Fi, termine con cui si identificano in genere i dispositivi 802.11, indica l'approvazione del dispositivo stesso da parte della Wi-fi Alliance, che raccoglie numerosi costruttori di hardware (Cisco, Nokia, Intel, Broadcom, Philips, Asus, ecc.). L'organizzazione è nata con l'obiettivo di certificare l'interoperabilità di prodotti 802.11.
La famiglia 802.11 consta di quattro standard dedicati alla trasmissione delle informazioni, referenziati con le lettere a, b, g ed n (più 802.11p dedicato alla gestione tra autoveicoli); la sicurezza è stata inclusa in uno standard a parte: 802.11i; gli altri standard della famiglia (c, d, e, f, h, …) riguardano estensioni dei servizi base e miglioramenti di servizi già disponibili. Il primo standard largamente diffuso è stato il b, in seguito si sono diffusi lo standard a e soprattutto il g, ora si sta diffondendo il nuovo standard n.

1.1. Basi tecniche

Si illustrano ora alcuni concetti di base necessari per comprendere gli argomenti che verranno trattati nel seguito.

1.1.1. Bande ISM

ISM (Industrial, Scientific and Medical) è il nome assegnato dall'Unione Internazionale delle Telecomunicazioni (ITU) ad alcune bande di frequenze lasciate al libero impiego per le applicazioni che prevedono potenze EIRP (Equivalent Isotropic Radiated Power) estremamente limitate ed utilizzate all'interno di una proprietà privata (la normativa vieta l'attraversamento del suolo pubblico, anche se evidentemente questo concetto è inapplicabile date le caratteristiche intrinseche della tecnologia).
Le bande ISM sono state definite dal settore "Radiocommunication" dell'ITU nelle "Radio Regulations" 5.138 e 5.150. L'uso di queste bande può differire da stato a stato a causa di specifiche regolamentazioni nazionali. Le bande ISM definite a livello mondiale sono (Figura 1.1):

- banda dei 900 MHz (902-928 MHz)
- banda dei 2,4 GHz (2,400-2,4835 GHz)
- banda dei 5,8 GHz (5,725-5,850 GHz)

Recentemente tali bande sono state utilizzate senza bisogno di licenze per sistemi di comunicazione senza fili come le wireless LAN (IEEE 802.11b/g e Bluetooth operano nella banda dei 2,4 GHz, mentre IEEE 802.11a opera nella banda dei 5,8 GHz) (Figura 1.2).

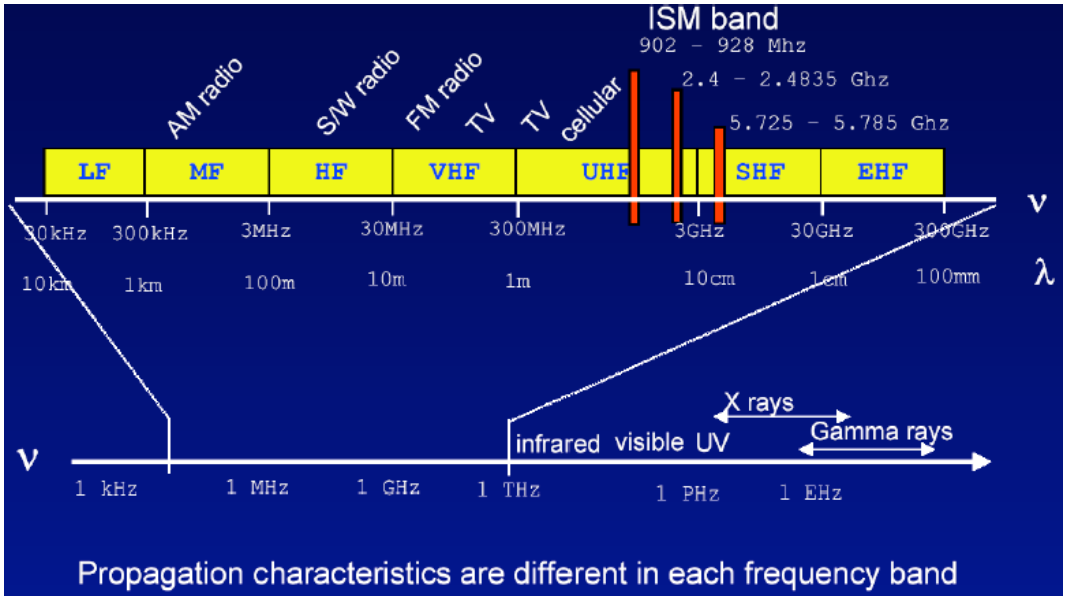

Figura 1.1: posizione delle bande ISM nello spettro elettromagnetico.

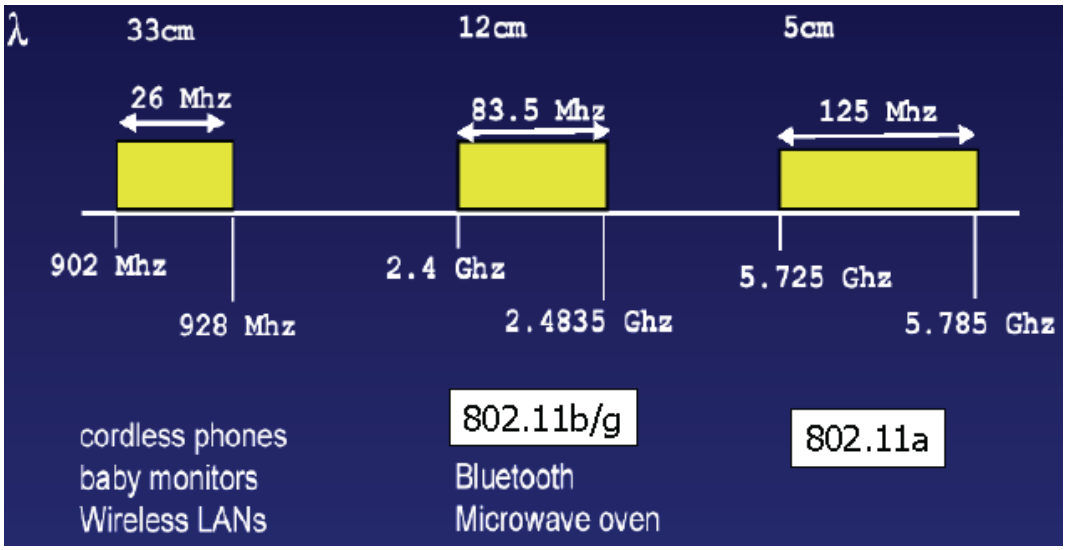

Figura 1.2: caratteristiche e utilizzazioni delle principali bande ISM.

1.1.2. Modello ISO/OSI

Il modello ISO Open Systems Interconnection (meglio conosciuto come ISO/OSI) è un insieme di standard per reti di calcolatori introdotto nel 1978 dall'International Organization for Standardization, il principale ente di standardizzazione internazionale; il modello definisce un'architettura logica di rete composta da una pila di **protocolli** suddivisa in 7 livelli, i quali insieme espletano in maniera logico-gerarchica tutte le funzionalità della rete.

Il modello ISO/OSI, concepito per reti di telecomunicazioni a commutazione di pacchetto, è costituito da una pila (o stack) di protocolli attraverso i quali viene ridotta la complessità implementativa di un sistema di comunicazione per il networking. In particolare ISO/OSI è costituito da strati (o livelli), i cosiddetti **layer**, che racchiudono uno o più aspetti fra loro correlati della comunicazione fra due nodi di una rete. I layers sono in totale 7 e vanno dal livello fisico (quello del mezzo trasmissivo, ossia del cavo o delle onde radio) fino al livello delle applicazioni (quello dei servizi utilizzati dagli utenti finali).

ISO/OSI realizza una comunicazione per livelli cioè, dati due nodi A e B, il livello n del nodo A può scambiare informazioni col solo livello n del nodo B attraverso un

protocollo: ciò conferisce modularità al sistema e semplicità di implementazione e reimplementazione (Figura 1.3). Ogni livello realizza la comunicazione col livello corrispondente su altri nodi usando il PoS (Point of Service) del livello immediatamente sottostante attraverso un'**interfaccia**, dunque ISO/OSI incapsula i messaggi di livello n in messaggi di livello n-1 (Figura 1.4).

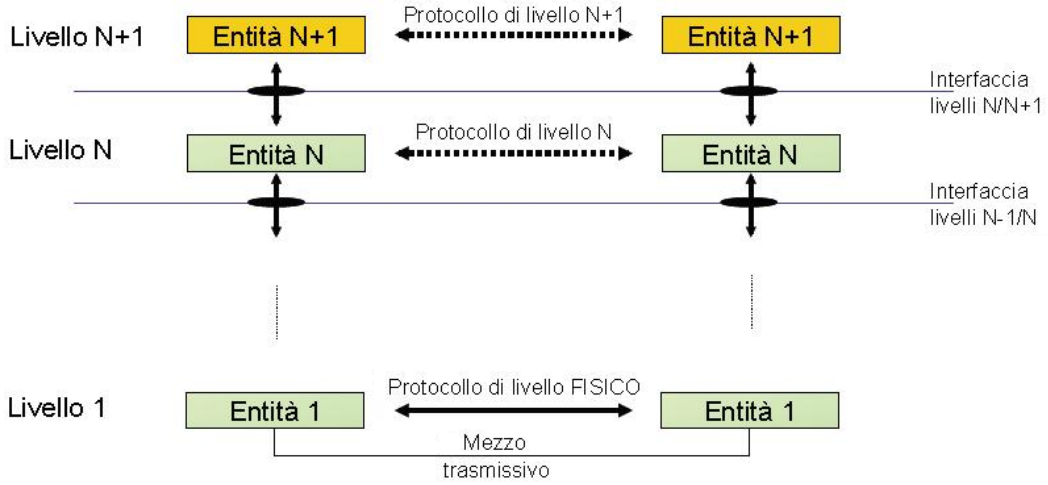

Figura 1.3: concetti di protocollo e interfaccia nel modello ISO/OSI.

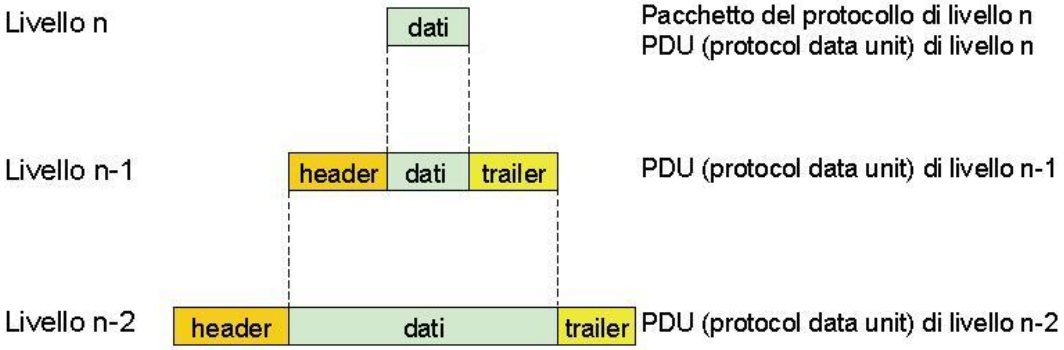

Figura 1.4: incapsulamento dei dati.

La Figura 1.5 illustra i 7 livelli definiti dal modello e le relative unità dati.

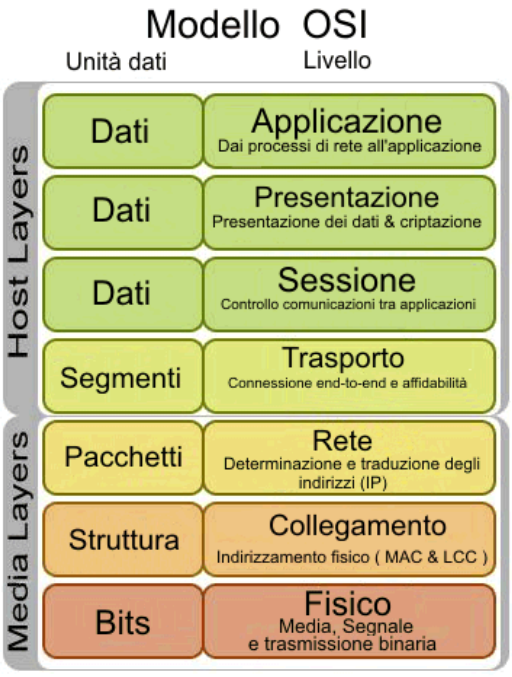

Figura 1.5: struttura logica del modello ISO/OSI.

Gli standard 802.11 trattano solo i primi 2 livelli e li suddividono in sublayer specifici illustrati in Figura 1.6.

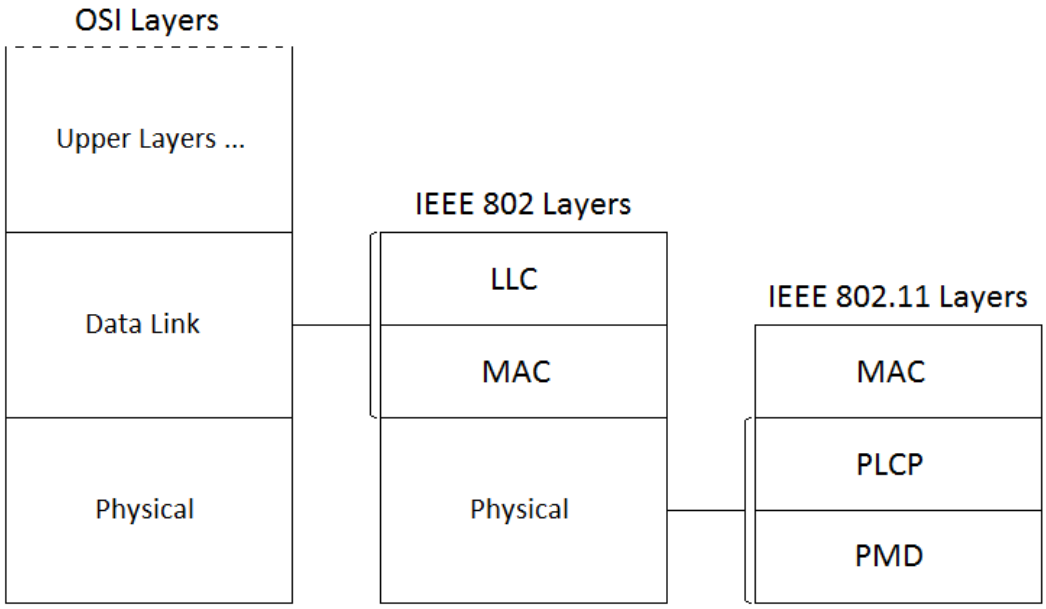

Figura 1.6: livelli specifici che interessano i diversi standard.

- **LIVELLO 1: Physical**

  Obiettivo: trasmettere un flusso di dati non strutturati attraverso un collegamento fisico, occupandosi della forma e del voltaggio del segnale. Ha a che fare con le procedure meccaniche ed elettroniche necessarie a stabilire, mantenere e disattivare un collegamento fisico.

  In questo livello si definiscono:

  - le tensioni scelte per rappresentare i valori logici;
  - la durata in microsecondi del segnale elettrico che identifica un bit;
  - la modulazione e la codifica utilizzata;
  - l'eventuale trasmissione simultanea in due direzioni;
  - la forma e la meccanica dei connettori usati per collegare l'hardware al mezzo trasmissivo.

  802.11 suddivide il livello fisico in PMD e PLCP sublayer che verranno descritti in seguito.

- **LIVELLO 2: Data Link**

  Obiettivo: permettere il trasferimento di dati attraverso il livello fisico. Consente l'invio di frame di dati con la necessaria sincronizzazione ed effettua un controllo degli errori e delle perdite di segnale. Tutto ciò permette di far apparire, al livello superiore, il mezzo fisico come una linea di trasmissione esente da errori di trasmissione.

  Questo livello si occupa principalmente di formare le trame da inviare attraverso il livello fisico, incapsulando il pacchetto proveniente dallo strato superiore in un nuovo pacchetto provvisto di nuovi header (intestazione) e tail (coda), che contengono anche sequenze di controllo. Questa frammentazione dei dati in specifici pacchetti è detta framing ed i singoli pacchetti sono i **frame**. Per il controllo d'errore di ogni frame ricevuto, il destinatario invia al mittente un pacchetto ACK (ACKnowledgement, conferma) contenente l'esito della ricezione: il mittente deve ripetere l'invio dei pacchetti sui quali il destinatario ha rilevato errori e che quindi non sono stati confermati. Per ottimizzare l'invio degli ACK, si usa una tecnica detta Piggybacking, che consiste nell'accodare ai messaggi in uscita gli ACK relativi ad una

connessione in entrata, per ottimizzare l'uso del livello fisico. I pacchetti ACK possono anche essere raggruppati e trasmessi in blocchi.
Questo livello si occupa anche di controllare il flusso di dati (controllo di flusso): in caso di sbilanciamento della velocità di trasmissione tra mittente e destinatario, il protocollo si preoccupa di rallentare l'invio dei dati del sistema più veloce adeguandolo alla capacità di ricezione del sistema più lento, minimizzando così le perdite dovute a sovraccarico.
Il livello data link si suddivide ulteriormente in due sottolivelli:

- LLC (Logical Link Control): è il sottolivello più alto; si occupa dell'interfacciamento con il livello superiore, del controllo di flusso e dell'ARQ (Automatic Repeat reQuest);
- MAC (Medium Access Control): è il sottolivello che interessa 802.11; si occupa del controllo dell'accesso al mezzo, dell'assemblaggio dei frame, dell'indirizzamento e del controllo d'errore.

2. Lo standard IEEE 802.11g

IEEE 802.11g-2003 è una revisione dello standard IEEE 802.11 che pur lavorando nella banda ISM dei 2,4 GHz come 802.11b estende il throughput a 54 Mbps utilizzando la tecnica di modulazione OFDM già implementata in 802.11a.

2.1. Physical layer

Le principali funzionalità che il livello fisico di 802.11 deve fornire sono (Figura 2.1):

a) scambiare frame con il livello MAC sotto la gestione della Physical Layer Convergence Procedure (PLCP);
b) usare una data modulazione per trasmettere e ricevere dati attraverso il mezzo fisico (in questo caso le radio frequenze) sotto il controllo del Physical Medium Dependent (PMD) sublayer;
c) fornire un'indicazione del Carrier Sense (rilevamento della portante) al livello MAC per verificare l'attività nel mezzo trasmissivo.

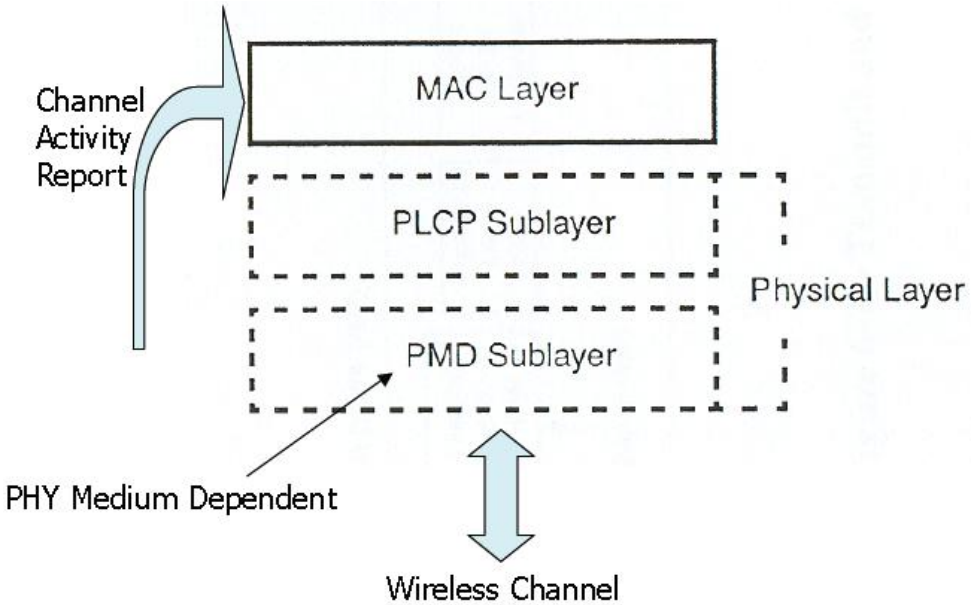

Figura 2.1: struttura e funzionalità dei sottolivelli di 802.11.

2.1.1. PMD sublayer

Il sottolivello PMD è il più vicino al mezzo di trasmissione fisico, si occupa quindi della trasmissione vera e propria dei dati attraverso le radio frequenze.
Come è noto, per inviare un segnale tramite un'antenna, tale segnale deve essere prima modulato: andrà a modificare certe caratteristiche di un'onda portante che trasporterà l'informazione. La modulazione è necessaria per portare il segnale ad una frequenza idonea ad essere trasmessa da un'antenna sufficientemente piccola, e per poter trasmettere più segnali attraverso l'etere utilizzando portanti a frequenze diverse.
Nel seguito verranno analizzate le diverse modulazioni/codifiche che hanno permesso l'evoluzione dei diversi standard 802.11.

Una tecnica adottata in tutti gli standard 802.11 è l'uso di uno **scrambler** inserito all'inizio della catena di modulazione. Lo scrambler è un dispositivo che permette di randomizzare la sequenza di bit che arrivano dal livello superiore, raggiungendo due scopi:

- ✓ evitare la trasmissione di lunghe sequenze di zero o uno logici consecutivi che comprometterebbero la sincronizzazione in ricezione;
- ✓ fare in modo che lo spettro della potenza del segnale da inviare non dipenda direttamente dai dati originari, ma da altri quasi del tutto random con una Power Spectral Density più dispersa e quindi migliore.

Nel ricevitore si troverà un de-scrambler idoneo a ricostruire la sequenza di bit originaria.

2.1.1.1. 802.11: DSSS modulation

Il Direct Sequence Spread Spectrum (DSSS) è una tecnica di trasmissione a "frequenza diretta" a banda larga, nella quale ogni bit viene trasmesso come una sequenza prefissata di valori, detti chip. L'interfaccia DSSS utilizza un sistema con dispersione in banda base impiegando un chipping code (codice di dispersione): ogni bit trasmesso, prima di essere modulato, viene associato (attraverso una porta XOR) ad una sequenza a 11 bit detta sequenza di Barker (10110111000) che permette di semplificare di molto la sincronizzazione in ricezione ottenuta tramite correlazione (Figura 2.2). Questo sistema fornisce maggior robustezza contro ISI (InterSimbol Interference, interferenza d'intersimbolo), rumore e jamming; il suo punto debole è invece l'assenza di benefici contro l'interferenza tra canali adiacenti.

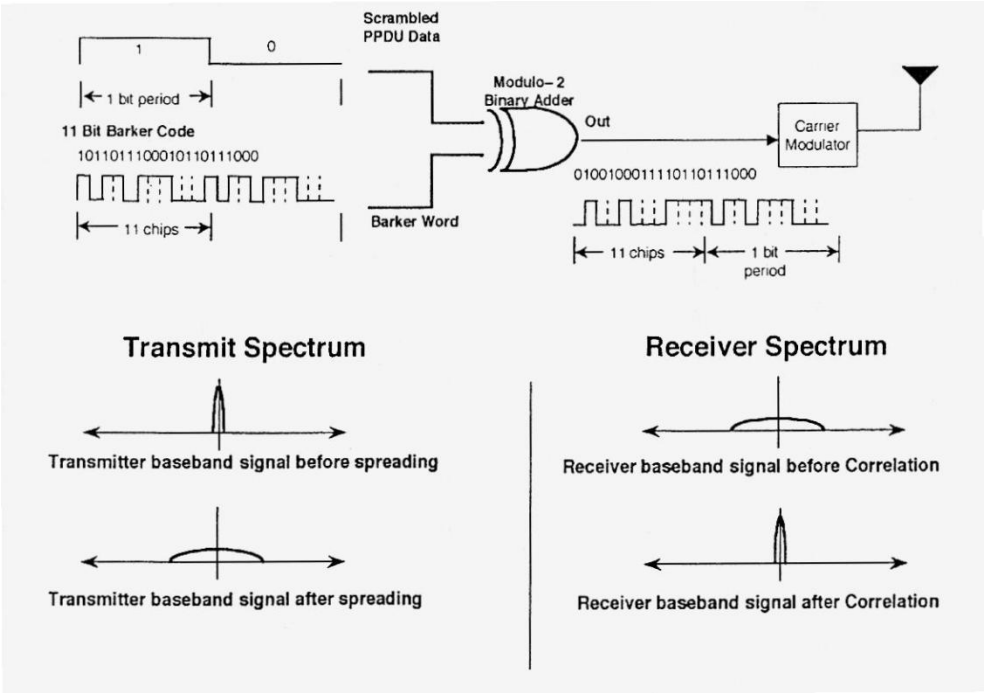

Figura 2.2: costruzione e benefici della DSSS modulation.

Nella versione originaria di 802.11 erano previsti 2 tipi di modulazione:

- ➢ DBPSK: Differential Binary Phase Shift Keying, in grado di trasmettere 1 bit per simbolo, arrivando ad una velocità di 1 Mbps.
- ➢ DQPSK: Differential Quaternary Phase Shift Keying, in grado di trasmettere 2 bit per simbolo, permettendo una velocità di 2 Mbps.

Il grande pregio della modulazione differenziale consiste nel fatto che non è richiesta in ricezione la ricostruzione della portante perché l'informazione è contenuta nella differenza di fase tra l'onda ricevuta nell'attuale periodo di simbolo (T_s) e il precedente (Figura 2.3).

DBPSK	
diff. di fase	simbolo
0°	0
180°	1

DQPSK	
diff. di fase	simbolo
0°	00
90°	01
180°	11
-90°	10

Tabella 2.1: bit associati alla differenza di fase nelle modulazioni DBPSK e DQPSK.

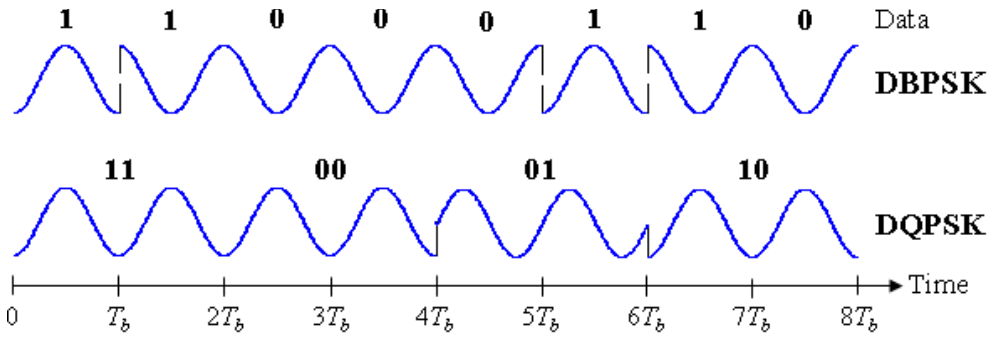

Figura 2.3: modulazione DBPSK e DQPSK (nel caso $T_S=2T_b$).

La struttura del modulatore (Figura 2.4) è quella del modulatore QAM alla quale ci si può ricondurre tramite i seguenti passaggi matematici:

- il segnale modulato DQPSK si può scrivere come

$$s(t) = V_0 \sum_{i=-\infty}^{+\infty} g(t - iT)\cos(2\pi f_0 t + a_i)$$

con V_0 componente continua (per distanziare i punti della costellazione), $g(t)$ imipulso base (teoricamente un rect, in pratica un coseno rialzato), T periodo di simbolo, f_0 frequenza della portante, e $a_i = a_{i-1} + \Delta a_i$ sfasamento secondo la modulazione differenziale (Δa_i porta l'informazione);

- Utilizzando la formula trigonometrica di addizione

$$s(t) = V_0 \sum_{i=-\infty}^{+\infty} g(t - iT)\cos(2\pi f_0 t + a_i) =$$

$$= V_0 \sum_{i=-\infty}^{+\infty} g(t - iT)\cos(2\pi f_0 t)\cos a_i - V_0 \sum_{i=-\infty}^{+\infty} g(t - iT)\sin(2\pi f_0 t)\sin a_i =$$

$$= v_I(t)\cos(2\pi f_0 t) - v_Q(t)\sin(2\pi f_0 t)$$

si evidenziano le due componenti della modulazione QAM: componente in fase $v_p(t)$ che moltiplica il coseno e componente in quadratura di fase $v_q(t)$ che moltiplica il seno

$$v_p(t) = V_0 \sum_{i=-\infty}^{+\infty} g(t - iT)a_{pi}$$

$$v_q(t) = V_0 \sum_{i=-\infty}^{+\infty} g(t - iT)a_{qi}$$

- In particolare a_{pi} e a_{qi} possono valere o 1 o 0 e vengono calcolati secondo la modulazione differenziata

$$a_{pi} = \cos a_i = \cos(a_{i-1} + \Delta a_i) = a_{p(i-1)} \cos \Delta a_i - a_{q(i-1)} \sin \Delta a_i$$
$$a_{qi} = \sin a_i = \sin(a_{i-1} + \Delta a_i) = a_{q(i-1)} \cos \Delta a_i - a_{p(i-1)} \sin \Delta a_i$$

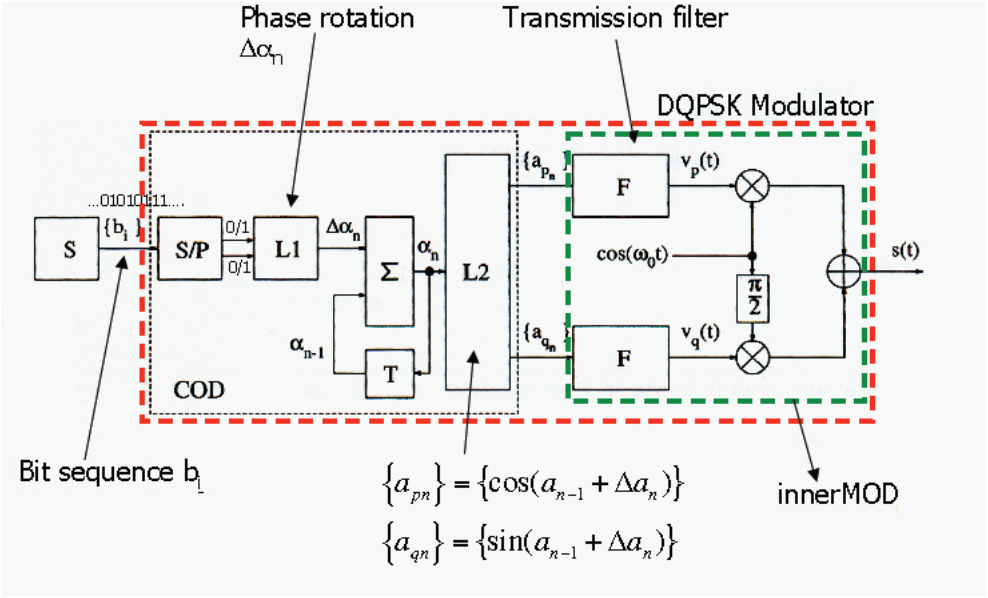

Figura 2.4: struttura del modulatore DQPSK.

L'occupazione di canale della DSSS modulation risulta di 22 MHz con una forma spettrale di un $|\mathrm{sinc}(x)|$ filtrato (Figura 2.5).

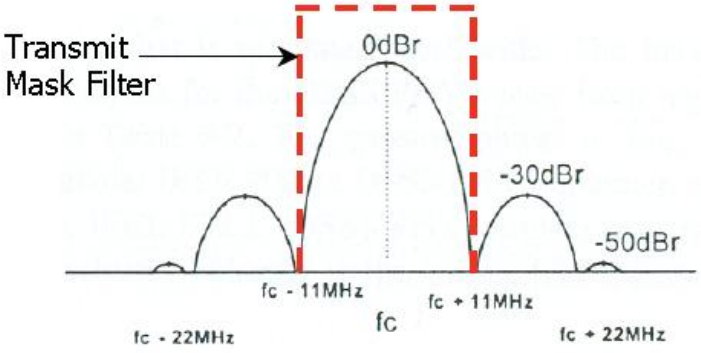

Figura 2.5: spettro del segnale modulato DSSS.

Il disturbo nella banda di un canale A generato da un canale adiacente B deve essere inferiore a -50 dB, si è scelta quindi una distanza minima di guardia pari a 25 MHz, per consentire l'interoperabilità nella stessa area di più dispositivi contemporaneamente (Figura 2.6).

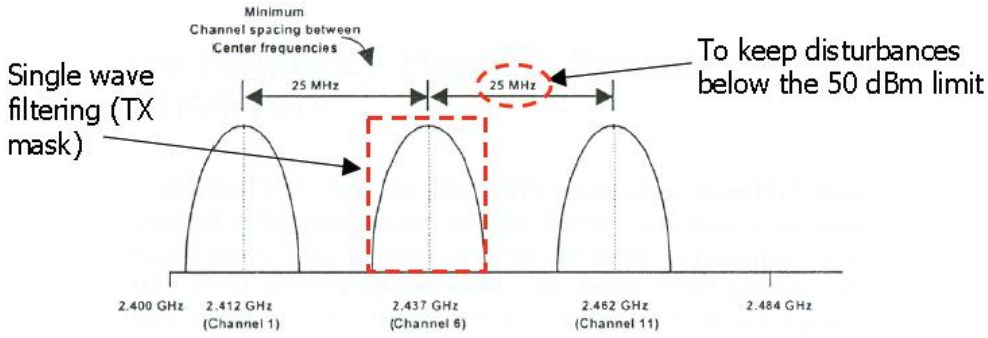

Figura 2.6: distanza di guardia tra canali adiacenti.

Nei 14 canali in cui è stata divisa la banda ISM dei 2,4 GHz si sono potuti ottenere 3 canali non sovrapposti (tra i primi 11 disponibili nella maggior parte del mondo, scelti quindi per i dispositivi commerciali) nei quali possono operare 3 diversi Access Point nella stessa area senza interferire eccessivamente (in Europa 3 gruppi da 3 canali, a scelta) (Tabella 2.2).

Commercial products

Channel Number	Frequency GHz	North America	Europe	Spain	France	Japan-MKK
1	2.412	X	X			
2	2.417	X	X			
3	2.422	X	X			
4	2.427	X	X			
5	2.432	X	X			
6	2.437	X	X			
7	2.442	X	X			
8	2.447	X	X			
9	2.452	X	X			
10	2.457	X	X	X	X	
11	2.462	X	X	X	X	
12	2.467		X		X	
13	2.472		X		X	
14	2.483					X

Tabella 2.2: canali disponibili nelle diverse aree mondiali nella banda dei 2,4 GHz (in rosso i 3 non sovrapposti).

In conclusione, la Figura 2.7 illustra lo schema completo del sottolivello PMD per 802.11.

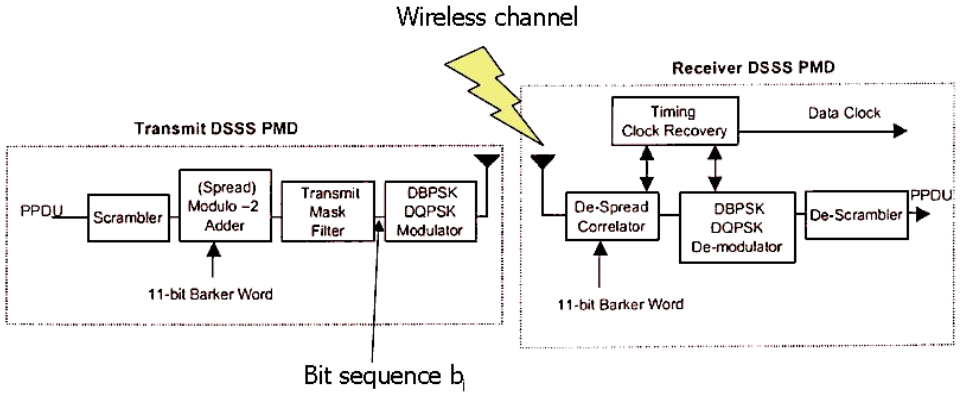

Figura 2.7: schema a blocchi del sottolivello PMD di 802.11.

2.1.1.2. 802.11b: CCK modulation

802.11b supporta le velocità di trasmissione 5,5 e 11 Mbps utilizzando la codifica CCK (Complementary Code Keying) mentre la tecnica di modulazione rimane la stessa di 802.11 e viene chiamata HR/DSSS (High Rate DSSS).

Nella codifica CCK vengono usate code-word con proprietà particolari per codificare i dati da inviare. Sia $\underline{c}^k = [{c_0}^k, {c_1}^k, \dots, {c_{N-1}}^k]$ la parola di codice binaria, con N la lunghezza della parola e $k = 1,2,\dots,K$ che identifica le diverse parole di codice. Chiamando $R_{kk}[j]$ l'autocorrelazione della k-esima

parola di codice (prodotto di correlazione tra la parola e la sua copia traslata di j), $\underline{c}^k$ deve rispettare la seguente proprietà:

$$\sum_{k=1}^{K} R_{kk}[j] = \begin{cases} KN & se\ (j \bmod N) = 0 \\ 0 & altrove \end{cases}$$

Il che significa che ogni ritardo j diverso da 0 offre un'autocorrelazione pari a 0 riducendo l'ISI, eccetto per ritardi multipli dell'intera parola di codice (NT_C) (nel caso di 802.11b si avrà $NT_C \cong 10 \div 50\ ns$ sufficiente per applicazioni indoor).
In 802.11b le parole di codice CCK sono lunghe 8 chip: $\underline{c} = [c_0, c_1, \dots, c_7]$ e sono espresse in funzione di quattro fasi $\varphi_1, \varphi_2, \varphi_3$ e φ_4:

$$\underline{c} = \left[e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, -e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1}\right]$$

φ_i può assumere i soli valori $[0, \pi/2, \pi, 3\pi/2] = [1, 1j, -1, -1j]$. Le code-words vengono trasmesse a 11 Mchip/s.

Rate 5,5 Mbps:
In una code-word di 8 chip, trasmessa a 11 Mchip/s, vengono inviati 4 bit d'informazione d_0, d_1, d_2, d_3, ciò comporta una velocità trasmissiva di 5,5 Mbps.

- d_0 e d_1 codificano φ_1 in base ad una modulazione DQPSK, come illustra la Tabella 2.3.

Dibit pattern (d0, d1) (d0 is first in time)	Even symbols phase change (+jω)	Odd symbols phase change (+jω)
00	0	π
01	π/2	3π/2 (–π/2)
11	π	0
10	3π/2 (–π/2)	π/2

Tabella 2.3: codifica della fase φ_1 per il rate 5,5 Mbps.

  La fase φ_1 cambia relativamente alla fase φ_1 del simbolo precedente come previsto nella Differential PSK.
- I rimanenti bit d_2 e d_3 codificano le altre 3 fasi φ_2, φ_3 e φ_4 :

$$\varphi_2 = (d_2 \cdot \pi) + \pi/2$$
$$\varphi_3 = 0$$
$$\varphi_4 = d_3 \cdot \pi$$

  Quindi i chip che si ottengono sono quelli indicati nella Tabella 2.4.

d2, d3	c1	c2	c3	c4	c5	c6	c7	c8
00	1j	1	1j	−1	1j	1	−1j	1
01	−1j	−1	−1j	1	1j	1	−1j	1
10	−1j	1	−1j	−1	−1j	1	1j	1
11	1j	−1	1j	1	−1j	1	1j	1

Tabella 2.4: codifica delle fasi φ_2, φ_3 e φ_4 per il rate 5,5 Mbps.

Riassumendo 2 bit (d_2 e d_3) selezionano la code-word e altri 2 bit (d_0 e d_1) modulano secondo DQPSK la parola di codice scelta.

Rate 11 Mbps:

In una code-word di 8 chip, trasmessa a 11 Mchip/s, vengono inviati 8 bit d'informazione $d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7$, ciò comporta una velocità trasmissiva di 11 Mbps.

- d_0 e d_1 codificano φ_1 esattamente come per la velocità 5,5 Mbps.
- Le coppie di bit di informazione (d_2, d_3), (d_4, d_5), (d_6, d_7) codificano rispettivamente le 3 fasi φ_2, φ_3 e φ_4 in base ad una QPSK, come illustrato in Tabella 2.5:

Dibit pattern [di, d(i+1)] (di is first in time)	Phase
00	0
01	π/2
10	π
11	3π/2 (−π/2)

Tabella 2.5: codifica delle fasi φ_2, φ_3 e φ_4 per il rate 11 Mbps.

Queste 2 tecniche di codifica sono molto potenti generando un set di $4^8 = 65536$ possibili parole di codice anziché $8^8 = 16777216$; ricevendo quindi $\underline{r} = [r_0, r_1, \ldots, r_7]$, simbolo affetto da AWGN (Additive White Gaussian Noise), il ricevitore sceglierà la parola di codice $\underline{c}$ che più si avvicina a $\underline{r}$ tra le 65536 valide, cioè quella che più minimizza la distanza euclidea:

$$d(\underline{c}, \underline{r}) = |\underline{c} - \underline{r}|^2$$

Per far ciò si utilizzano algoritmi efficienti come il Fast Walsh Transform.
Concludendo, per entrambe le velocità si genera una sequenza di "bit complessi" (complex spread sequence) che si possono interpretare come componente in fase e in quadratura e quindi trasmettere con lo stesso modulatore di 802.11.

2.1.1.3. 802.11a: OFDM modulation

OFDM (Orthogonal Frequency Division Multiplexing) è una modulazione di tipo **multi-portante**, che utilizza un numero elevato di sotto-canali ortogonali tra di loro. Ogni sub-carrier è modulata attraverso una modulazione di tipo convenzionale (ad esempio una QAM) con un basso symbol rate, in modo da mantenere un data rate simile agli schemi a singola portante; questo

permette di ridurre l'interferenza intersimbolica grazie ad intervalli di guardia di durata accettabile.
Il vantaggio principale dell'OFDM rispetto agli schemi a singola portante è dato dall'abilità di comunicare anche in condizioni pessime del canale, ad esempio nei casi in cui si presenta un'attenuazione ad alta frequenza oppure interferenze a banda stretta.

Rappresentazione geometrica dei segnali:
Può essere provato che un insieme di M segnali reali $S = \{s_1(t), s_2(t), \dots, s_M(t)\}$ definiti in $[0,T)$ con energia finita, può essere rappresentato come combinazione lineare di $N \leq M$ funzioni, base ortonormale:

$$s_i(t) = \sum_{j=1}^{N} s_{ij}\Phi_j(t) \quad ,con\ 0 \leq t < T$$
$$s_{ij} = \int_0^T s_i(t)\Phi_j(t)dt$$

Esempi di funzioni (approssimativamente) ortonormali che formano una base ortonormale dello spazio sono il seno e il coseno:

$$\Phi_1(t) = \sqrt{\frac{2}{T}}\cos(2\pi f_0 t)$$
$$\Phi_2(t) = \sqrt{\frac{2}{T}}\sin(2\pi f_0 t)$$

Sono ortonormali in quanto il prodotto scalare con se stessi vale 1 e tra loro vale 0:

$$\int_0^T [\Phi_1(t)]^2 dt = \frac{2}{T}\int_0^T \frac{1}{2}[1+\cos(4\pi f_0 t)]dt = 1 + \frac{\sin(4\pi f_0 t)}{4\pi f_0 t} \approx 1$$
$$\int_0^T \Phi_1(t)\Phi_2(t)dt = \frac{2}{T}\int_0^T \frac{1}{2}\sin(4\pi f_0 t)\,dt = \frac{-\cos(4\pi f_0 t)}{4\pi f_0 t} \approx 0$$
$$Con\ T\ periodo\ di\ simbolo\ e\ assumendo\ f_0 t \gg$$

Avendo quindi un segnale in banda base:

$$v(t) = \sum_k v_k(t-kT) = \sum_k \left(a_{pk} + j a_{qk}\right) g(t-kT) \qquad \text{(M-QAM)}$$

con $v_k(t)$ segnale analogico in banda base trasmesso in $[kT,(k+1)T]$ e $a_{pk} + j a_{qk} = \rho_k e^{j\theta_k}$ simbolo M-ario trasmesso in $[kT,(k+1)T]$ (ad esempio se $a_p, a_q \in \{-1,1\}$ si avrà una QAM), il segnale in banda passante sarà:

$$s(t) = \mathrm{Re}\left\{v(t)e^{j2\pi f_0 t}\right\} =$$
$$= \sum_k a_{pk}\, g(t-kT)\cos(2\pi f_0 t) - \sum_k a_{qk}\, g(t-kT)\sin(2\pi f_0 t)$$

In particolare si avrà in $[kT,(k+1)T]$:

$$s_k(t) = a_{pk}\cos(2\pi f_0 t) - a_{qk}\sin(2\pi f_0 t) = \\ = s_{pk}\cos(2\pi f_0 t) + s_{qk}\sin(2\pi f_0 t)$$

riportandosi così alla base ortonormale prima definita.
Usando una $g(t)$ diversa dal $\mathrm{rect}(t)$ si avrà:

$$s_k(t) = s_{pk}g(t-kT)\cos(2\pi f_0 t) + s_{qk}g(t-kT)\sin(2\pi f_0 t)$$

Si può provare che si ottiene una base ortonormale (approssimata) anche usando per $g(t)$ il coseno rialzato, realizzabile nella pratica.

Tecnica OFDM:
Si consideri un sistema con bitrate R e occupazione di banda $B = 1/T_S$ (T_S periodo di simbolo); il canale è affetto da un delay spread (ritardo di diffusione causato dai multipath) τ_M , quindi ha una banda di coerenza $B_C = 1/\tau_M$.
Se, come accade, $\tau_M \gg T_S$, gli echi del segnale trasmesso dovuti al multipath in un certo kT_S si ripercuoteranno anche nei periodi di simbolo successivi causando ISI; dal punto di vista delle frequenze $B_C \ll B$ quindi il fading prodotto dal canale influenza solo parte dello spettro del segnale (selective fading) causando distorsione.
Il principio base dell'OFDM è quello di suddividere B in N sistemi indipendenti modulati in parallelo (Figura 2.8); ogni sotto-canale avrà una banda $B_N = B/N$ e un bitrate $R_N = R/N$. Per $N \gg$ si saranno risolti i problemi precedentemente esposti, infatti $T_{SN} \ll \tau_M$ e $B_N = B/N \ll B_C$ quindi il canale influenzerà allo stesso modo tutta la banda del segnale (flat fading).

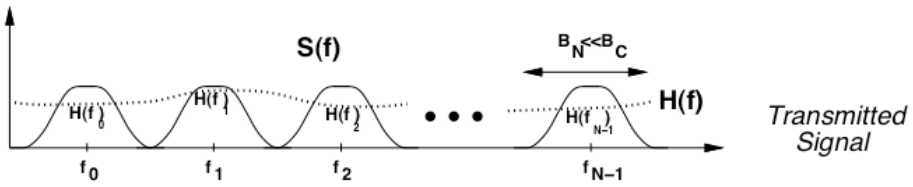

Figura 2.8: suddivisione del canale in N sotto-canali indipendenti.

Considerando una modulazione BPSK, i simboli s_k possono valere 1 o -1, sono quindi reali e non complessi:

$$s(t) = \mathrm{Re}\{v(t)e^{j2\pi f_0 t}\} = \\ = \sum_k a_{pk}\, g(t-kT)\cos(2\pi f_0 t) - \sum_k a_{qk}\, g(t-kT)\sin(2\pi f_0 t) = \\ = \textstyle\sum_k a_{pk}\, g(t-kT)\cos(2\pi f_0 t) \qquad (a_{qk} = 0 \text{ per BPSK})$$

La Figura 2.9 illustra lo schema del trasmettitore OFDM di base:

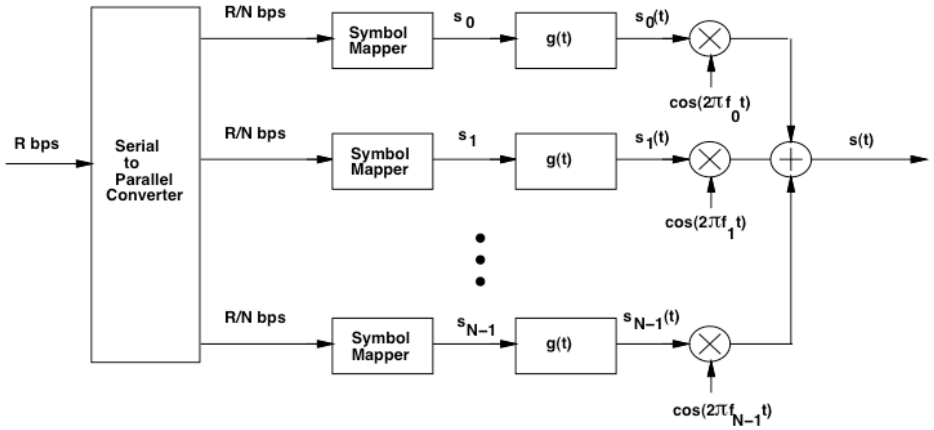

Figura 2.9: schema a blocchi del trasmettitore OFDM di base.

Il bitstream viene suddiviso in N sub-stream paralleli, ognuno dei quali viene modulato con una diversa portante (sub-carrier) f_n e occupa una banda B_N. Se $g(t)$ è un coseno rialzato, il periodo di simbolo del sotto-canale sarà $T_N = (1+\beta)/B_N$ (dove β è il coefficiente di roll-off del coseno rialzato), si avrà quindi una banda $B_N = (1+\beta)/T_N$.
I segnali modulati provenienti da tutti i sotto-canali vengono sommati assieme per formare il segnale da trasmettere:

$$s(t) = \sum_{i=0}^{N-1} s_i\, g(t) \cos(2\pi f_i t + \Phi_i)$$

Per non avere sovrapposizione di canali si impone:

$$f_i = f_0 + iB_N = f_0 + i\frac{(1+\beta)}{T_N} \qquad , i = 0,1,\dots,N-1$$

Il bitrate totale non è cambiato ma l'ISI è stata eliminata quasi del tutto.
Il ricevitore per questo tipo di modulazione viene costruito come illustrato in Figura 2.10:

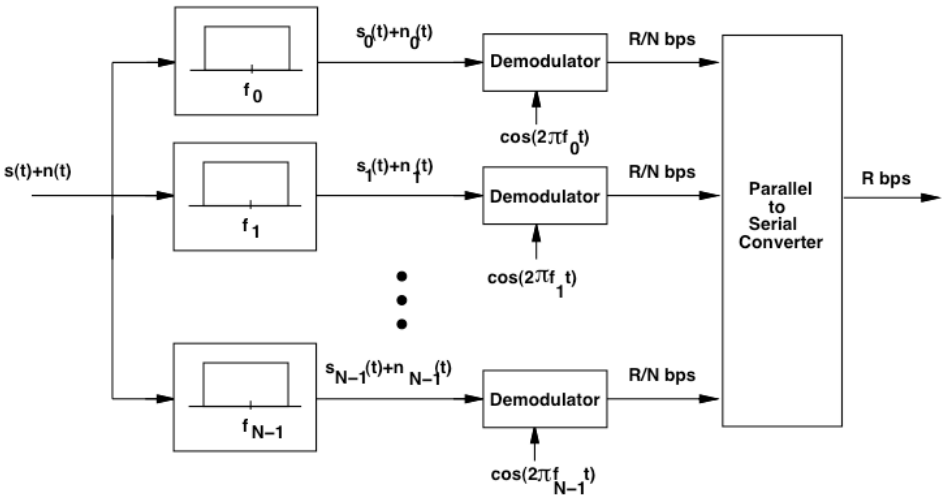

Figura 2.10: schema a blocchi del ricevitore OFDM di base.

Implementando in questo modo trasmettitore e ricevitore, sorge un problema: usando un impulso a coseno rialzato l'occupazione di banda totale risulta:

$$B = NB_N = \frac{N(1+\beta)}{T_N}$$

In un progetto reale ogni sotto-canale occuperà una banda ancora maggiore, perché $g(t)$ deve essere a tempo finito:

$$B = NB_N = \frac{N(1+\beta+\varepsilon)}{T_N}$$

Si avrà dunque uno spettro molto poco efficiente.
Si è trovata una soluzione sovrapponendo in parte i sotto-canali adiacenti, omettendo il coefficiente β nella distanza tra le portanti; si può provare che le portanti $\{\cos[2\pi(f_0 + i/T_N)t + \Phi_i] \quad , i = 0,1,\dots,N-1\}$ sono ancora ortogonali nell'intervallo $[0, T_N]$ quindi separabili dal demodulatore, e che le funzioni $\{g(t)\cos[2\pi(f_0 + i/T_N)t + \Phi_i] \quad , i = 0,1,\dots,N-1\}$ per un appropriato $g(t)$ formano ancora una base ortonormale.
Ora la frequenza dell'i-esima portante è imposta:

$$f_i = f_0 + \frac{i}{T_N} \qquad , i = 0,1,\dots,N-1$$

Di conseguenza l'occupazione di banda totale risulta:

$$B = \frac{N+\beta+\varepsilon}{T_N}$$

spettro molto più efficiente per $N \gg$.
Il ricevitore per questa versione è costruito nel modo illustrato in Figura 2.11:

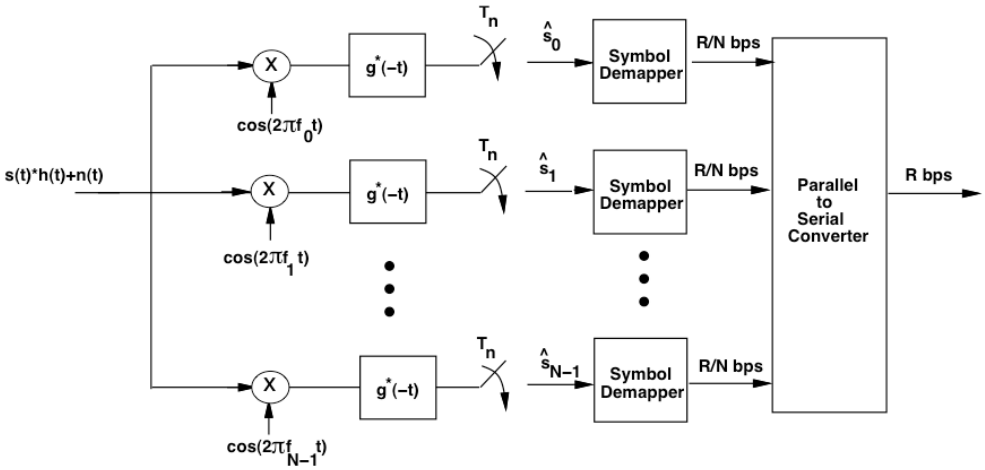

Figura 2.11: schema a blocchi del ricevitore OFDM nella versione con canali parzialmente sovrapposti.

Ottimizzazione dell'implementazione del trasmettitore:
Si è arrivati a definire il segnale trasmesso se i simboli sono reali (BPSK):

$$s(t) = \sum_{i=0}^{N-1} s_i\, g(t)\cos(2\pi f_i t + \Phi_i) \qquad f_i = f_0 + \frac{i}{T_N} \quad , i = 0,1,\dots,N-1$$

Se i simboli sono invece complessi (M-QAM, M-PSK), il coseno verrà sostituito da un esponenziale complesso e il segnale dovrà essere modulato in due componenti (in fase e in quadratura):

$$s(t) = \sum_{i=0}^{N-1} s_i \, g(t) e^{j(2\pi f_i t + \Phi_i)}$$

Si può provare che anche gli esponenziali formano una base ortonormale.
Trasmettendo tutti i segnali da uno stesso trasmettitore, essi sono sincronizzati quindi $\Phi_i = 0 \ , i = 0,1, \dots, N-1$, e nonostante lungo il canale vengano sfasati in modi diversi (lavorando su frequenze diverse), si può provare che l'ortogonalità al ricevitore è preservata.
Lo schema del trasmettitore per simboli complessi è quello illustrato in Figura 2.12:

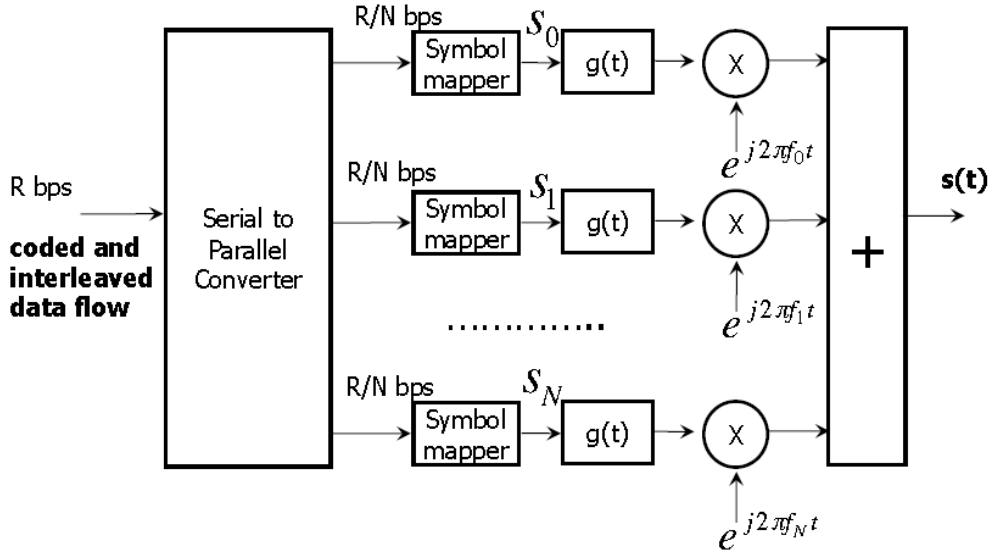

Figura 2.12: schema a blocchi del trasmettitore OFDM per simboli complessi.

Un trasmettitore costruito in questo modo è estremamente dispendioso in termini di costo (tanta circuiteria, N modulatori, N filtri) e di energia di alimentazione richiesta (N circuiti identici e indipendenti). Per far fronte a tale dispendio, osservando la formula del segnale da trasmettere (con $f_i = f_0 + i/T_N$):

$$s(t) = \sum_{i=0}^{N-1} s_i \, g(t) e^{j(2\pi f_i t)} = g(t) e^{j(2\pi f_0 t)} \sum_{i=0}^{N-1} s_i \, e^{j\frac{2\pi i t}{T_N}}$$

si è arrivati a notare la grande analogia con la **IDFT** (Inverse Discrete Fourier Trasform):

$$x[n] = \sum_{i=0}^{N-1} X[i] e^{j\frac{2\pi i n}{T}}$$

e quindi a semplificare trasmettitore e ricevitore utilizzando un circuito in grado di calcolare la trasformata di Fourier inversa e diretta, risparmiando notevolmente (Figura 2.13 - 2.14).

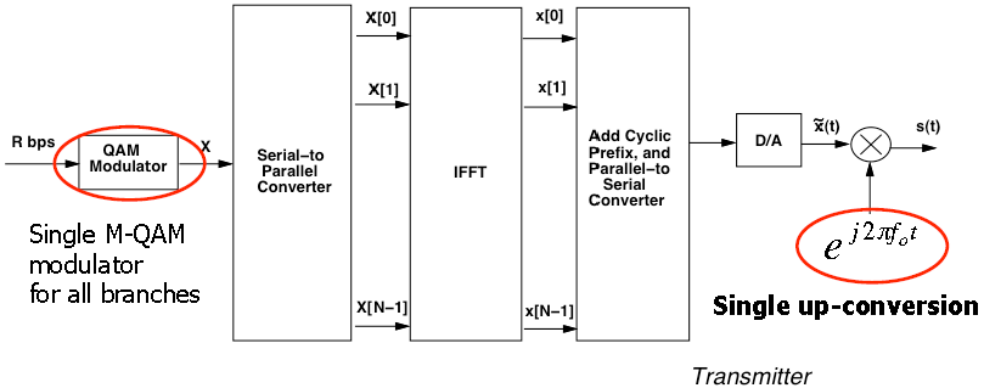

Figura 2.13: schema a blocchi del trasmettitore OFDM che utilizza la IFFT.

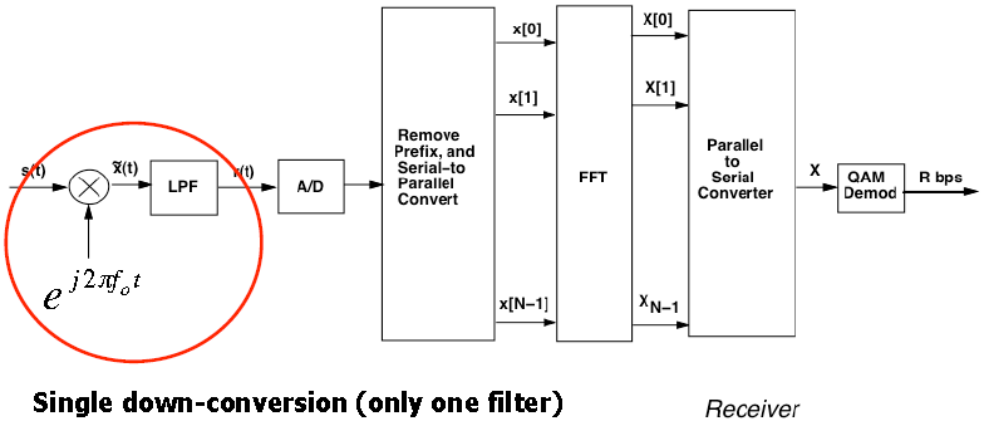

Figura 2.14: schema a blocchi del ricevitore OFDM che utilizza la FFT.

Il **Cyclic Prefix** a cui si riferisce la figura è un intervallo di guardia inserito all'inizio del simbolo OFDM per lasciar decadere gli echi del simbolo precedente, limitando l'ISI (Figura 2.15).

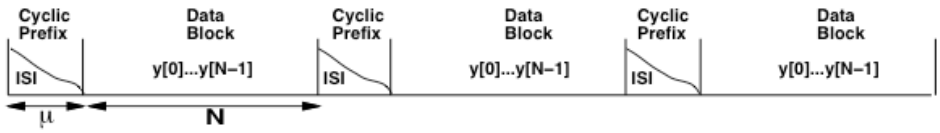

Figura 2.15: Cyclic Prefix tra i simboli OFDM.

Il Data Block è il **simbolo OFDM** formato dagli N "campioni OFDM", ognuno dei quali è modulato da una sub-carrier e generato da M bit in base al tipo di modulazione.

Interleaving:

L'interleaving è una tecnica utilizzata per disporre i dati in maniera non contigua, al fine di migliorare le prestazioni in caso di errori a raffica (error-burst). L'operazione inversa, che ricostruisce l'ordine originario, prende il nome di de-interleaving.

Avendo ad esempio 20 bit di dati da inviare, si può disporli in una matrice 5x4 scrivendoli in riga da sinistra a destra (Figura 2.16):

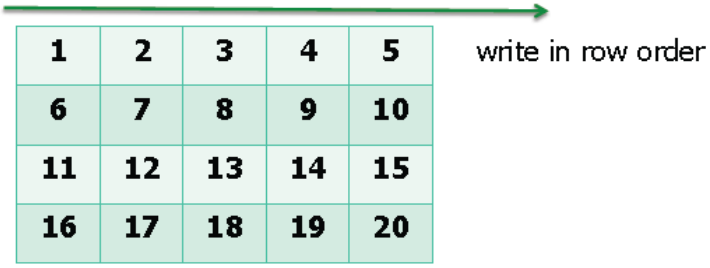

Figura 2.16: esempio interleaving, scrittura dei dati in una matrice per righe.

In trasmissione invece si leggeranno in colonna, dall'alto al basso, ottenendo un rimescolamento (Figura 2.17):

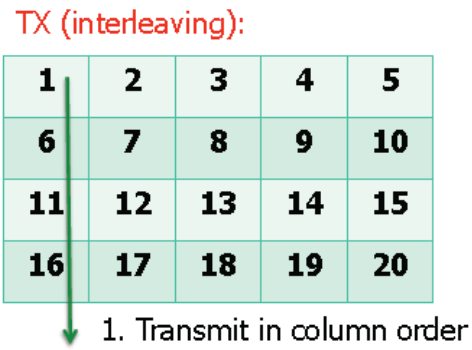

Figura 2.17: esempio interleaving, lettura dei dati dalla matrice per colonne.

Se la sequenza di bit trasmessi viene colpita da un error-burst lungo 6 bit (Figura 2.18),

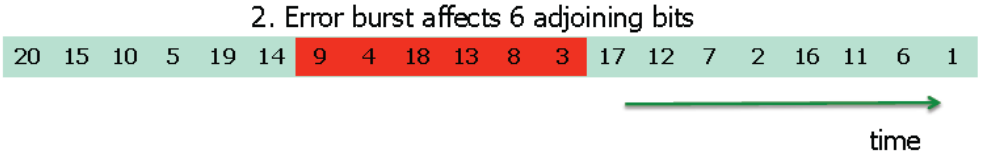

Figura 2.18: esempio interleaving, un error-burst colpisce 6 bit disordinati.

in ricezione verrà ricostruita la matrice e i bit errati si ritroveranno distribuiti e non contigui (Figura 2.19):

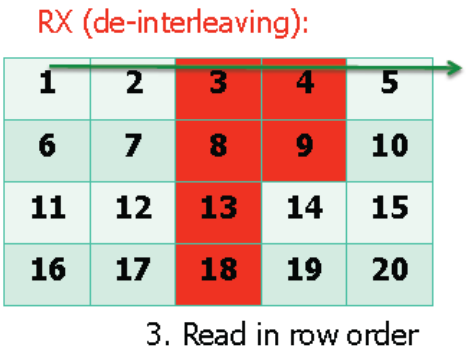

Figura 2.19: esempio interleaving, ricostruzione della matrice in ricezione che letta per righe distribuisce gli errori.

Questa tecnica è ancora più utile se ad ogni riga vengono associati dei bit ridondanti in grado di rilevare o addirittura correggere gli errori, come si può osservare nell'esempio analizzato al quale si sono aggiunti 2 bit ridondanti in grado di correggere fino a 2 errori per code-word (Figura 2.20):

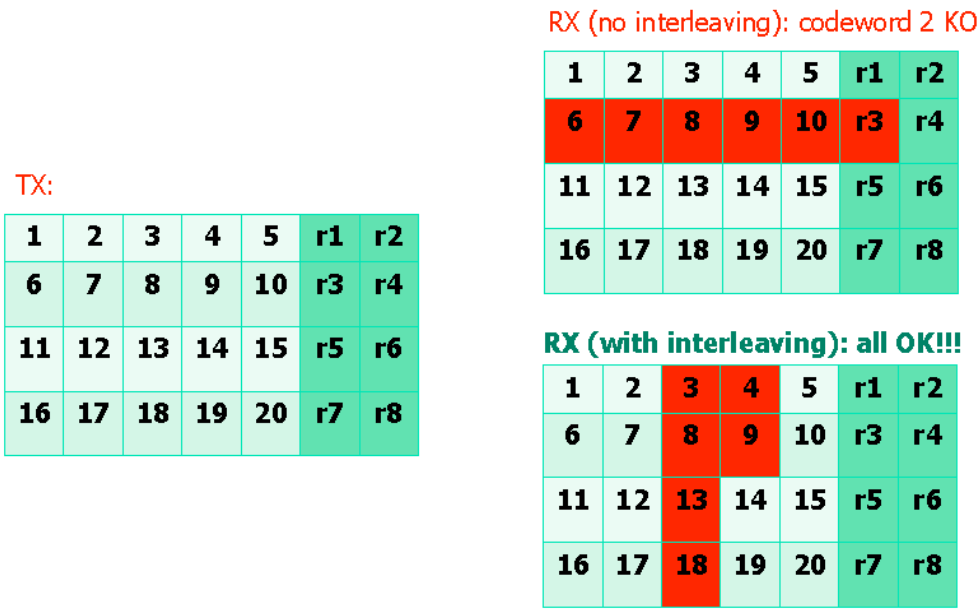

Figura 2.20: esempio in cui l'interleaving permette di correggere tutte le parole ricevute.

L'interleaving è una tecnica che accompagna perfettamente l'OFDM, in quanto i dati da inviare vengono prima codificati con l'interleaving come appena visto, e poi distribuiti sugli N sotto-canali, ottenendo così un interleaving sia nel tempo che nella frequenza, capace di evitare errori critici concentrati sia in un intervallo breve di tempo che in una banda molto ristretta.

Specifiche 802.11a:

IEEE 802.11a ha a disposizione canali larghi 20 MHz nella banda ISM dei 5 GHz. Utilizza una modulazione OFDM a N=64 sotto-portanti (1 campione OFDM per sotto-portante), di cui:

- 48 sono usate per i dati;
- 12 sono poste a zero per ridurre l'interferenza tra canali adiacenti;
- 4 sono "pilota" per la stima del canale.

Il Cyclic Prefix dura un tempo corrispondente a m=16 campioni OFDM, quindi il simbolo OFDM totale è costituito da 64+16=80 campioni OFDM.

Vengono usate inoltre 3 possibili codifiche convoluzionali FEC (Forward Error Correction) con rate $1/2, 2/3$ o $3/4$ data-bit/coded-bit.

Le modulazioni disponibili in ogni sotto-canale sono BPSK, QPSK, 16QAM, 64QAM (in un certo istante tutti i sotto-canali devono usare la stessa).

Chiamando T_S il "periodo di campionamento OFDM" (un campione OFDM ogni T_S secondi), ed essendo la banda totale disponibile $B = 1/T_S = 20\ MHz$, le 64 sotto-portanti risulteranno distanziate di:

$$B_N = \frac{20\ MHz}{64} = 312{,}5\ kHz$$

Il Cyclic Prefix, essendo lungo m=16 campioni OFDM, riuscirà ad eliminare l'ISI se il delay spread risulta avere un valore massimo di:

$$\tau_M < mT_S = \frac{m}{B} = \frac{16}{20\ MHz} = 0{,}8\ \mu s$$

più che sufficiente per un tipico ambiente indoor.
Includendo i dati e il Cyclic Prefix, ogni simbolo OFDM contiene 80 campioni OFDM; ciò comporta che la durata di un simbolo OFDM risulta:

$$T_N = 80T_S = 4\ \mu s$$

Il bitrate per ogni sotto-canale risulta:

$$R_N = \frac{\log_2 M}{T_N}$$

(BPSK:M=2→1bit/simbolo; QPSK:M=4→2bit/simbolo;
16QAM:M=16→4bit/simbolo; 64QAM:M=64→6bit/simbolo)

Il bitrate minimo si ha per:
- Modulazione BPSK;
- Rate di codifica $r = 1/2$.

$$R_{min} = 48 \cdot \frac{1}{2} \cdot \log_2 2 \cdot \frac{1}{4\ \mu s} = 6\ Mbps$$

Il bitrate massimo si ha per:
- Modulazione 64QAM;
- Rate di codifica $r = 3/4$.

$$R_{max} = 48 \cdot \frac{3}{4} \cdot \log_2 64 \cdot \frac{1}{4\ \mu s} = 54\ Mbps$$

Tra queste due velocità troviamo le intermedie elencate in Tabella 2.6, combinazioni di diverse modulazioni e codifiche:

Data rate [Mbps]	Modulation	Coding rate	Coded bits per sub-carrier	Coded bits per OFDM symbol	Data bits per OFDM symbol
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	16QAM	1/2	4	192	96
36	16QAM	3/4	4	192	144
48	64QAM	2/3	6	288	192
54	64QAM	3/4	6	288	216

Tabella 2.6: rate trasmissivi disponibili in 802.11a.

La banda ISM dei 5 GHz prevede 18 canali larghi 20 MHz, in ognuno dei quali si può usare l'OFDM. 802.11a prevede, come possiamo osservare in Tabella 2.7, 8 canali per applicazioni indoor (potenza massima 200 mW) e altri 4 per applicazioni outdoor (1 o 4 W).

36	5180 Mhz	200mW
40	5200 MHz	200 mW
42	5210 MHz	200 mW
44	5220 MHz	200 mW
48	5240 MHz	200 mW
50	5250 MHz	200 mW
52	5260 MHz	200 mW
56	5280 MHz	200 mW
58	5290 MHz	200 mW

60	5300 Mhz	200mW
64	5320 MHz	200 mW
149	5745 MHz	1000 mW
152	5760 MHz	1000 mW
153	5765 MHz	1000 mW
157	5785 MHz	4000 mW
160	5800 MHz	4000 mW
161	5805 MHz	4000 mW
165	5825 MHz	4000 mW

Tabella 2.7: canali disponibili nella banda ISM dei 5 GHz (verde=indoor, rosso=outdoor).

Due gruppi da 6 canali (4 indoor + 2 outdoor) non sono sovrapposti (Figura 2.21):

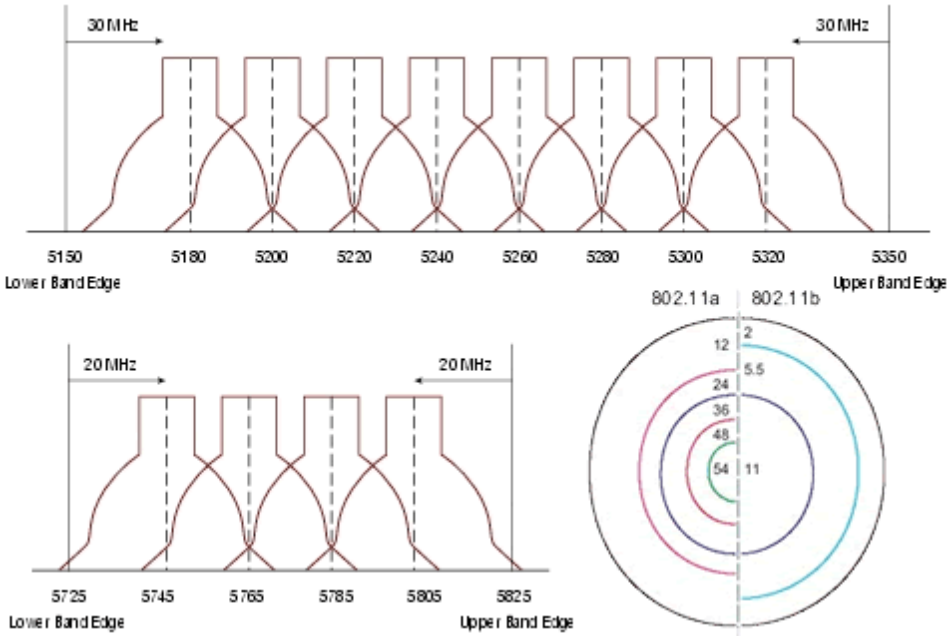

Figura 2.21: canali utilizzati da 802.11a e (schema circolare) confronto tra le velocità utilizzate da 802.11a e 802.11b in relazione alla distanza dall'Access Point.

2.1.1.4. 802.11g

Questo standard venne ratificato nel giugno del 2003, utilizza le stesse frequenze dello standard 802.11b, cioè la banda dei 2,4 GHz, ma fornisce una velocità nominale pari a 54 Mbps come quella dello standard 802.11a. È totalmente compatibile con lo standard b ma quando si trova a operare con periferiche b deve ovviamente prendere le dovute precauzioni per non entrare in conflitto col vecchio standard.

802.11g utilizza lo schema di modulazione OFDM per le velocità 6, 9, 12, 18, 24, 36, 48 e 54; quando però si trova a dialogare con dispositivi 802.11b commuta la modulazione in CCK per 5,5 e 11 Mbps e DBPSK/DQPSK+DSSS per 1 e 2 Mbps.

Dai 14 canali standardizzati nella banda ISM dei 2,4 GHz si sono ricavati 3 gruppi (utilizzabili singolarmente a scelta) di 3 canali non sovrapposti larghi 22

MHz e interspaziati di 25 MHz, come possiamo osservare nella Figura 2.22 e nella Tabella 2.8 (solo un gruppo per il Nord America: 1, 6, 11 per l'assenza dei canali 12 e 13; il canale 14 è disponibile solo in Giappone); in Europa si è riusciti a ricavare un gruppo di 4 canali non sovrapposti riducendo la larghezza a 20 MHz (1, 5, 9, 13) e ammettendo una leggera interferenza.

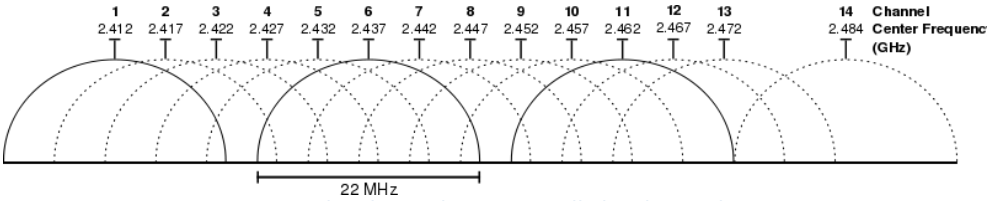

Figura 2.22: canali utilizzati da 802.11g nella banda ISM dei 2,4 GHz.

Channel	Center Frequency	Channel Width	Overlaps Channels
1	2.412 GHz	2.401 GHz - 2.423 GHz	2,3,4,5
2	2.417 GHz	2.406 GHz - 2.428 GHz	1,3,4,5,6
3	2.422 GHz	2.411 GHz - 2.433 GHz	1,2,4,5,6,7
4	2.427 GHz	2.416 GHz - 2.438 GHz	1,2,3,5,6,7,8
5	2.432 GHz	2.421 GHz - 2.443 GHz	1,2,3,4,6,7,8,9
6	2.437 GHz	2.426 GHz - 2.448 GHz	2,3,4,5,7,8,9,10
7	2.442 GHz	2.431 GHz - 2.453 GHz	3,4,5,6,8,9,10,11
8	2.447 GHz	2.436 GHz - 2.458 GHz	4,5,6,7,9,10,11,12
9	2.452 GHz	2.441 GHz - 2.463 GHz	5,6,7,8,10,11,12,13
10	2.457 GHz	2.446 GHz - 2.468 GHz	6,7,8,9,11,12,13
11	2.462 GHz	2.451 GHz - 2.473 GHz	7,8,9,10,12,13
12	2.467 GHz	2.456 GHz - 2.478 GHz	8,9,10,11,13
13	2.472 GHz	2.461 GHz - 2.483 GHz	9,10,11,12

Tabella 2.8: canali utilizzati da 802.11g (i colori evidenziano i 3 gruppi di 3 canali non sovrapposti).

Per concludere, la Tabella 2.9 confronta i 3 standard analizzati finora:

	802.11b	802.11a	802.11g
Standard approved	July 1999	July 1999	June 2003
Modulation	CCK	OFDM	OFDM & CCK
Maximum data rate	11 Mbps	54 Mbps	54 Mbps
Data rates	1,2,5.5,11 Mbps	6,9,12,18,24,36,48,54 Mbps	**CCK:** 1,2,5.5,11 Mbps **OFDM:** 6,9,12,18,24,36,48, 54 Mbps
Frequencies	2.4-2.497 GHz	5.15-5.35 GHz 5.425-5.675 GHz 5.725-5.875 Ghz	2.4-2.497 GHz

Tabella 2.9: confronto tra 802.11 a, b e g.

2.1.2. PLCP sublayer

Il compito principale del sottolivello PLCP è quello di interfacciare il livello MAC con il fisico; per far ciò esso crea un frame PPDU (PLCP Protocol Data Unit) che comprende le informazioni del livello fisico e del livello MAC (MPDU: MAC Protocol Data Unit).
Si esaminano ora i diversi frame previsti per i vari standard che hanno sempre cercato di restare compatibili con i precedenti.

2.1.2.1. 802.11

Il ricevitore utilizza il PLCP preamble per individuare un segnale in ingresso e per sincronizzare il demodulatore. Il PLCP preamble e header vengono sempre trasmessi alla velocità più bassa (1 Mbps) (Figura 2.23).

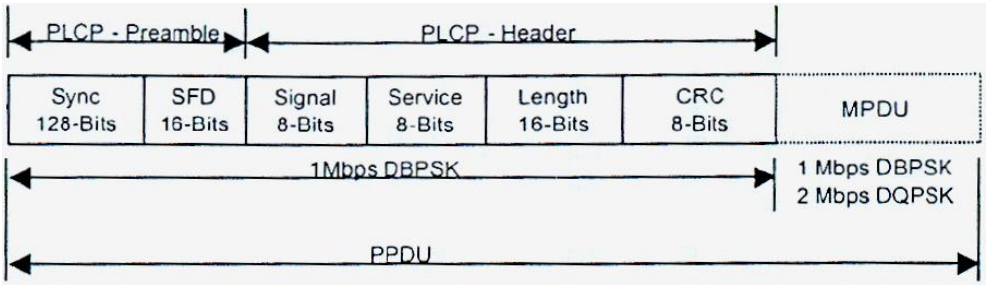

Figura 2.23: PPDU di 802.11.

Sync: contiene una stringa di 128 uno logici poi sottoposti a scrambling prima di essere trasmessi; è utilizzato dal ricevitore per sincronizzarsi con la portante prima della ricezione dei dati utili.
SFD: Start Frame Delimiter, indica la fine dei bit di sincronizzazione e l'inizio del PLCP header. Contiene il valore F3A0hex (1111001110100000bin).
Signal: indica la modulazione usata nella trasmissione del MPDU, contenendo la conseguente velocità divisa per 100 Kbps (DBPSK = 1 Mbps = 0Ahex, DQPSK = 2 Mbps = 1Ahex).
Service: campo lasciato libero per usi futuri, contiene 8 zero logici di default.
Lenght: contiene il tempo (in µs) necessario per trasmettere l'MPDU.
CRC: Cyclic Redundancy Check (Controllo a Ridondanza Ciclica) eseguito con l'algoritmo CCITT CRC-16 ed applicato al solo PLCP header, prima dello scrambling.
Un ulteriore campo CRC da 32 bit è incluso alla fine dell'MPDU per controllare i suoi eventuali errori, ma viene gestito dal livello MAC.

2.1.2.2. 802.11b

La struttura del frame è rimasta identica.
Nel campo Signal si possono inserire le due nuove velocità disponibili grazie al CCK (Tabella 2.10).

Signal value	Data rate
00001010	1 Mbps
00010100	2 Mbps
00111110	5,5 Mbps
01101110	11 Mbps

Tabella 2.10: velocità definite nel campo Signal.

Sono stati definiti i ruoli di 3 degli 8 bit del campo Service (Figura 2.24):
b2: posto a 1 quando la frequenza di trasmissione e il clock di simbolo usano lo stesso oscillatore locale;
b3: indica il tipo di codifica utilizzata: 0 per CCK, 1 per l'opzionale PBCC;
b7: utilizzato come estensione del campo Lenght che per rate maggiori di 8 Mbps diventerebbe ambiguo.

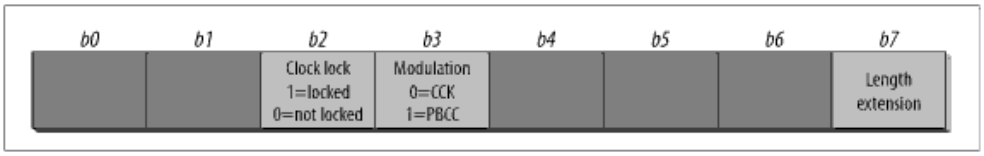

Figura 2.24: nuovo ruolo di 3 bit del campo Service.

Si è introdotta una nuova struttura opzionale (disponibile solo per le due nuove velocità) con uno short preamble, distinguibile per il campo Sync che contiene 56 zero logici e che permette di trasmettere il PLCP header a 2 Mbps (Figura 2.25).

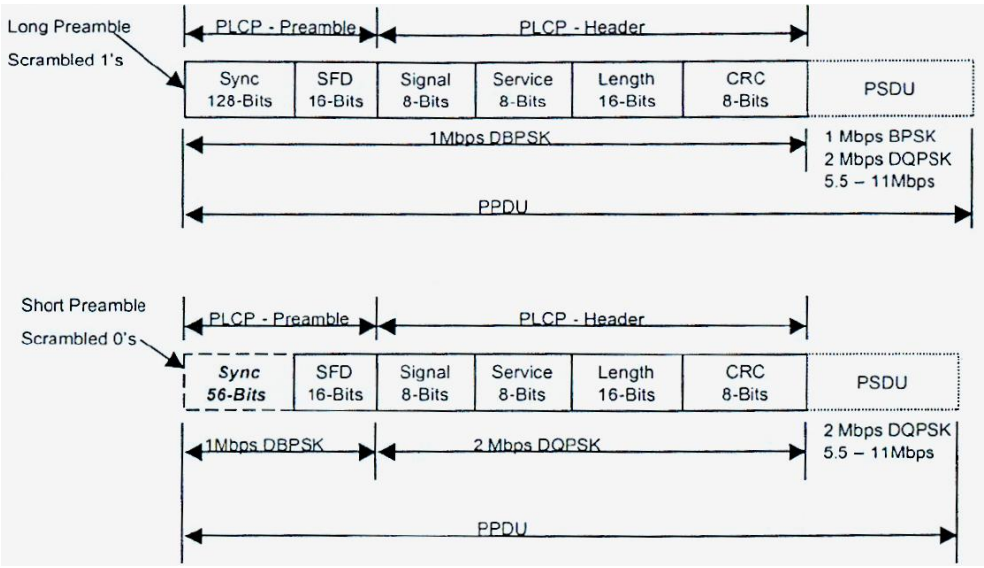

Figura 2.25: PPDU di 802.11b con Long e Short Preamble.

L'acronimo PSDU sta per Physical layer Service Data Unit e rappresenta il contenuto del PPDU che deve essere inviato.

2.1.2.3. 802.11a

Lavorando in un'altra banda di frequenze, il frame PLCP di 802.11a può avere una struttura diversa dalle precedenti, descritta nella Figura 2.26.

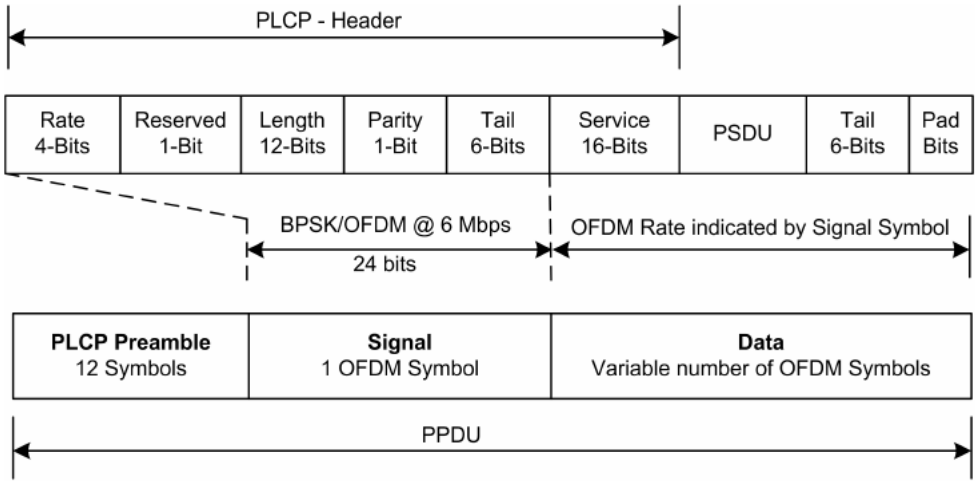

Figura 2.26: PPDU di 802.11a.

PLCP preamble: 12 simboli che indicano al ricevitore di prepararsi a ricevere il segnale OFDM in ingresso.
Rate: identifica la velocità con cui verranno inviati i dati.

Rate value	Data rate
1101	6 Mbps
1111	9 Mbps
0101	12 Mbps
0111	18 Mbps
1001	24 Mbps
1011	36 Mbps
0001	48 Mbps
0011	54 Mbps

Tabella 2.11: velocità definite nel campo Rate.

Reserved: settato a zero logico.
Lenght: indica il numero di ottetti contenuti nel frame.
Parity: bit di controllo di parità positiva sui 3 campi precedenti.
Tail: contiene 6 zero logici.
Service: 7 bit sono posti a zero logici e servono per sincronizzare il descrambler del ricevitore, i restanti 9 bit sono lasciati ad usi futuri (zeri logici di default).
Tail: 6 zeri logici per permettere al ricevitore di eseguire funzioni di processo del segnale.
Pad bits: contiene il numero di bit necessari a portare la lunghezza del frame ad un valore multiplo dei bit codificati nel simbolo OFDM.

2.1.2.4. 802.11g

802.11g utilizza la banda ISM dei 2,4 GHz come 802.11 e 802.11b, deve quindi restare necessariamente retrocompatibile con i dispositivi che lavorano con gli standard precedenti, pur utilizzando la OFDM modulation. Per far ciò PLCP preamble e header sono rimasti inalterati e la parte di controllo OFDM è stata inserita nel PSDU.

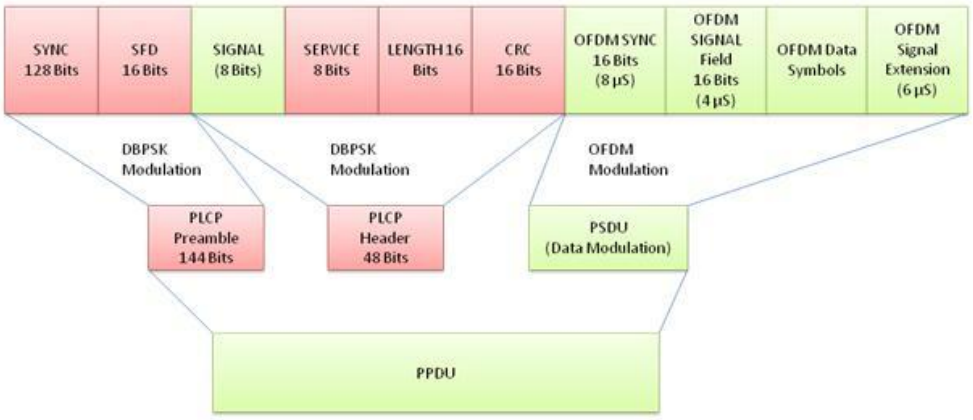

Figura 2.27: PPDU di 802.11g.

Anche qui è previsto uno short preamble opzionale costruito allo stesso modo di 802.11b.

2.2. MAC layer

Il sottolivello MAC (Medium Access Control) si occupa del controllo dell'accesso al mezzo, dell'assemblaggio dei frame, dell'indirizzamento e del controllo di errori. Deve riuscire, con le sue funzionalità, a fornire i seguenti servizi:

Servizi di stazione (devono essere garantiti da tutte le stazioni connesse alla rete):

- AUTENTICAZIONE: (Figura 2.28) E' il meccanismo utilizzato in una rete Wi-Fi per stabilire se un client ha il permesso di accedere ai servizi della rete e comunicare con gli altri client. Questo servizio deve garantire un livello di sicurezza elevato, al pari di una rete cablata. Ciò vuol dire che ogni client che richiederà l'accesso alla rete dovrà superare vari controlli di sicurezza prima di essere accettato. Ad esempio si protegge la rete con una password e solo i client che la conoscono saranno autenticati, oppure si utilizza un sistema di filtraggio dell'indirizzo MAC della scheda di rete.
- DEAUTENTICAZIONE: E' il servizio necessario per deautenticare dalla rete un client che ne ha fatto richiesta all'Access Point.
- SEGRETEZZA: Questo servizio è importante per garantire confidenzialità alle trasmissioni tra i vari client cifrando ogni messaggio. Se il traffico non fosse cifrato, chiunque si mettesse in ascolto sulle frequenze radio della trasmissione potrebbe tranquillamente leggere i dati scambiati tra mittente e destinatario.
- TRASMISSIONE: Servizio che garantisce la trasmissione, a livello MAC, tra due client della rete.

Servizi di distribuzione (di pertinenza esclusiva dell'Access Point):

- ASSOCIAZIONE: (Figura 2.28) Per poter inoltrare un pacchetto all'interno della rete l'Access Point deve conoscere la posizione della stazione di destinazione. Quando una stazione entra nel raggio di azione di un Access Point notifica a quest'ultimo la sua presenza.
- RIASSOCIAZIONE: Questo tipo di servizio consente ad una stazione di cambiare associazione da un AP ad un altro.
- DISASSOCIAZIONE: E' l'antitesi del servizio di Associazione. Questo servizio consiste nel notificare la fine di una associazione e viene eseguito dalla stazione prima di effettuare lo spegnimento. Nel caso in cui si abbia necessità di spengere l'Access Point per aggiornamento o manutenzione, quest'ultimo invierà una notifica di disassociazione a tutte le stazioni a lui connesse.
- DISTRIBUZIONE: E' uno dei servizi più importanti svolti dall'Access Point e consiste nello smistare i frame che lo raggiungono verso le stazioni di destinazione se esse appartengono

alla rete oppure verso l'Access Point che serve la rete nella quale si trova la stazione di destinazione.

- INTEGRAZIONE: Consente la traduzione dei frame dello standard 802.11 in altri formati compatibili con altri standard appartenenti alla famiglia degli standard 802. Sostanzialmente se ci immaginiamo una rete wireless con un Access Point interfacciato con una LAN, tutti i frame inviati da una stazione wireless e diretti ad una stazione appartenente alla LAN cablata verranno tradotti affinchè le stazioni appartenenti alla LAN cablata, che utilizza uno standard diverso dall'802.11, interpretino correttamente il frame ricevuto.

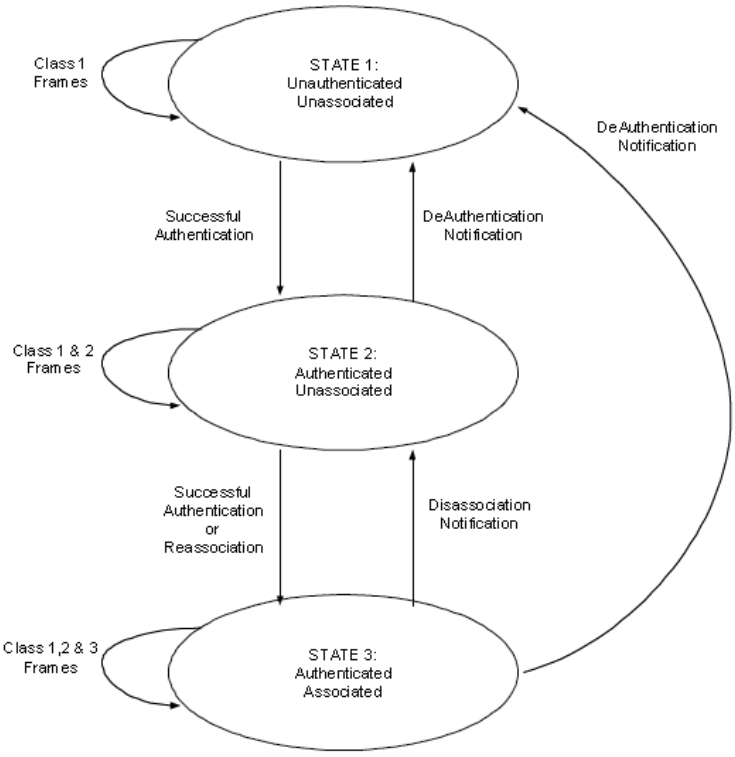

Figura 2.28: relazione tra stati di autenticazione e associazione.

La funzionalità più complicata che il livello MAC deve implementare nella tecnologia wireless è quella della modalità di accesso al mezzo, in quanto presenta numerose problematiche, la prima delle quali è l'impossibilità di utilizzare la classica CSMA/CD (Carrier Sense Multiple Access / Collision Detection), il cui principio di funzionamento è il seguente:

- CSMA: una stazione che desidera trasmettere si mette in "ascolto" del canale, se lo trova libero (non ci sono altre trasmissioni in corso) trasmette, se lo trova occupato ritarda la trasmissione;
- CD: la stazione che sta trasmettendo riconosce la collisione, si ferma e inizia la fase di ritrasmissione secondo un algoritmo di random backoff.

Nelle WLAN non è possibile utilizzare questa modalità di accesso al mezzo per due ragioni: l'implementazione richiederebbe una trasmissione di tipo full-duplex (trasmissione e ricezione contemporanea) con costo significativamente superiore, e in ambito wireless non si può garantire che tutte le stazioni si possano "sentire" l'un l'altra (assunzione base del CD).
Per questo si sono progettate delle modalità di accesso al mezzo proprie per le reti wireless, sempre basate sul CSMA: la **DCF** (Distributed Coordination Function) e le più evolute **PCF** (Point Coordination Function) e **HCF** (Hybrid Coordination Function).

2.2.1. Distributed Coordination Function

Ogni stazione prima di trasmettere "ascolta" il canale (CSMA): se il canale rimane libero per un tempo **DIFS** (Distributed InterFrame Space) trasmette, altrimenti inizia il **random**

backoff time. Il backoff timer esegue il conto alla rovescia solo mentre il canale è libero, se viene rilevata una trasmissione si interrompe momentaneamente per essere riattivato, dopo un DIFS, col canale nuovamente libero. La stazione che aveva trovato il canale occupato può riprovare a trasmettere non appena il suo backoff timer arriva a 0 (Figura 2.29).

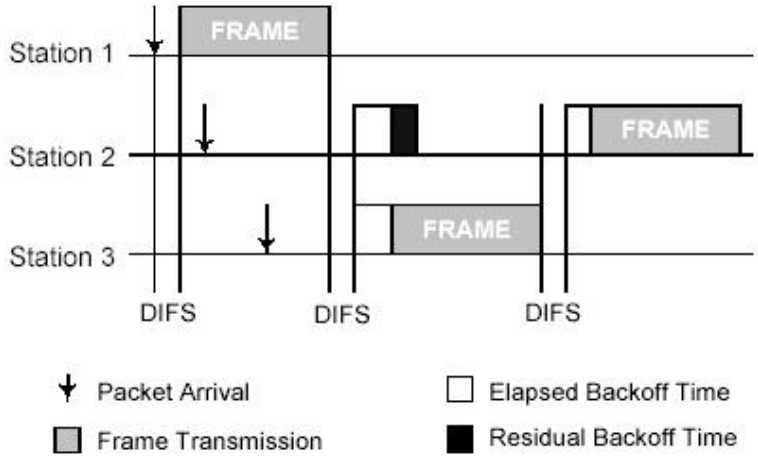

Figura 2.29: esempio di occupazione del canale trasmissivo regolato dalla DCF.

Il backoff time viene scelto come variabile aleatoria uniforme $U[0, CW-1]$, dove CW è la Contention Window che segue le seguenti regole (Figura 2.30):

$$CW(1) = CW_{min} = 32 \quad ,al\ primo\ tentativo\ di\ trasmissione\ fallito$$
$$CW(n) = \min(2 \cdot CW(n-1), CW_{max}) \quad ,al\ n-esimo\ tentativo\ fallito$$

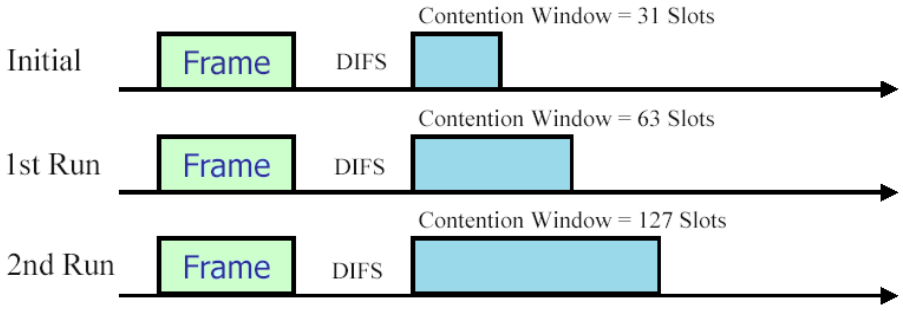

Figura 2.30: scelta della Contention Window.

Non implementando il Collision Detection, può succedere che due o più stazioni trasmettano simultaneamente senza che nessuno se ne renda conto, perché le antenne lavorano in half-duplex e non riescono quindi a rilevare altre trasmissioni mentre trasmettono. Questa situazione viene corretta da 802.11 prevedendo un pacchetto ACK (ACKnowledgement) che la stazione ricevente deve inviare alla trasmittente quando e se riceve correttamente il pacchetto. L'ACK viene inviato dopo un tempo **SIFS** (Short InterFrame Space) minore di DIFS (Figura 2.31).

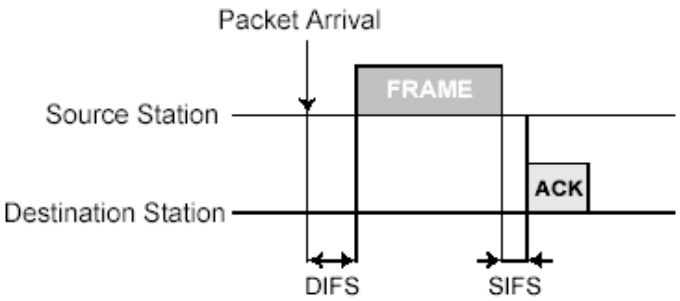

Figura 2.31: Utilizzo del ACK nella DCF.

La stazione ricevente controlla il pacchetto ricevuto tramite un CRC: se il Controllo a Ridondanza Ciclica fallisce l'ACK non viene inviato, e se la stazione trasmittente non riceve l'ACK il pacchetto viene ritenuto perso. Prima di poter ritrasmettere, dopo un evento di pacchetto perso, la stazione trasmittente deve aspettare un tempo **EIFS** (Extended InterFrame Space).

2.2.2. Hidden and exposed terminal problem

Si esamini una situazione di questo tipo:

- 3 stazioni A, B e C;
- solo B è nel range di trasmissione di A;
- solo B è nel range di trasmissione di C;
- A e C sono nel range di trasmissione di B;
- si sottolinea che A e C non riescono a "sentirsi".

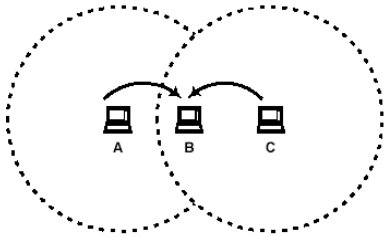

Figura 2.32: hidden terminal problem.

Può insorgere il seguente problema, chiamato "del terminale nascosto" (**hidden terminal problem**) (Figura 2.32):

1. A sta trasmettendo a B;
2. C vuole trasmettere a B;
3. secondo la DCF C sente il canale libero per un tempo DIFS quindi trasmette provocando una COLLISIONE in B.

Per ovviare a questa situazione si ricorre ad un meccanismo **RTS/CTS**:

1. la stazione che desidera trasmettere, che trova il canale libero, invia un breve pacchetto di controllo di richiesta di trasmissione RTS (Request To Send) che contiene anche la durata totale della trasmissione (Figura 2.33);

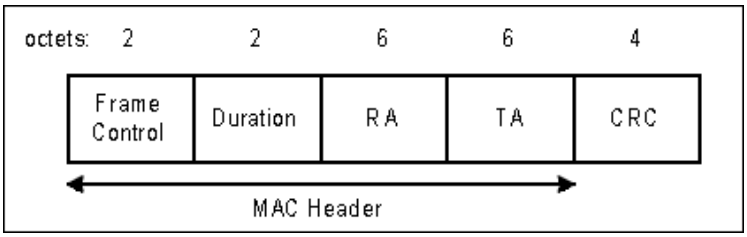

Figura 2.33: struttura del pacchetto di controllo RTS.

RA: Receiver Address;
TA: Trasmitter Address, chi invia il RTS;
Duration: durata totale della trasmissione in µs, dati+CTS+ACK+3SIFS;

2. la stazione destinazione, se sente anch'essa il canale libero, risponde, dopo un SIFS, con un breve pacchetto di controllo CTS (Clear To Send) contenente anche'esso la durata della rimanente trasmissione (Figura 2.34);

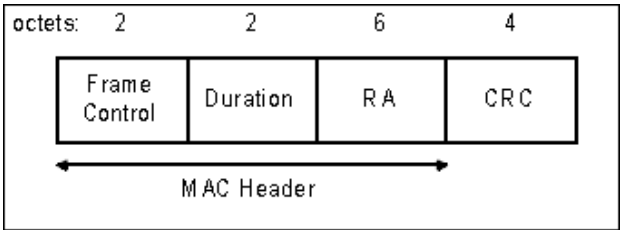

Figura 2.34: struttura del pacchetto di controllo CTS.

RA: Receiver Address, copiato dal TA del RTS;
Duration: durata della rimanente trasmissione in μs, dati+ACK+2SIFS;

3. le altre stazioni, ricevendo il RTS inviato dal mittente, il CTS inviato dal destinatario (che viene sentito anche dalle stazioni che non sono nel range di trasmissione del mittente, ma in quello del destinatario) o entrambi i pacchetti, attivano il loro VIRTUAL CARRIER SENSE indicator: **NAV** (Network Allocation Vector) cioè una portante virtuale che dura per il tempo indicato nei pacchetti RTS/CTS (Figura 2.35).

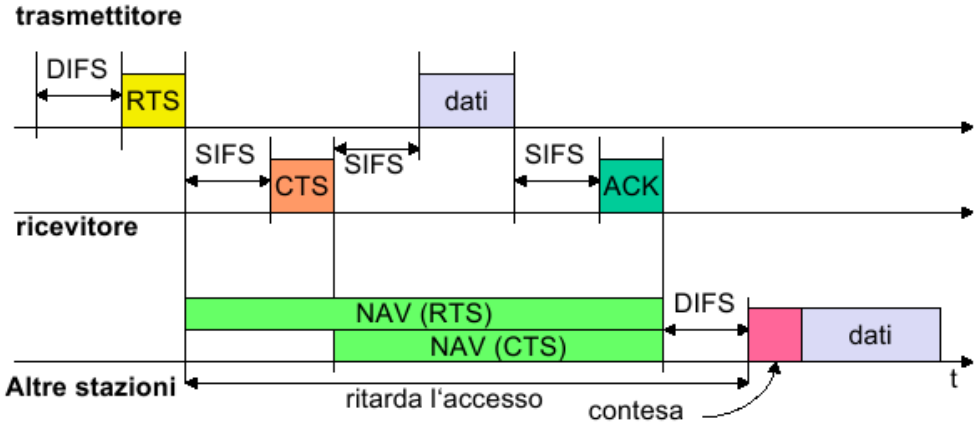

Figura 2.35: esempio di occupazione del canale trasmissivo completo di meccanismi RTS, CTS e NAV.

Questo meccanismo comporta evidenti vantaggi oltre alla riduzione del rischio di collisioni, dovuti al fatto che i pacchetti RTS/CTS sono molto più corti dei pacchetti dati: le collisioni (possibili anche tra i pacchetti di controllo) vengono individuate più velocemente, il numero di bit danneggiati da scartare sono molti meno e di conseguenza sono meno i bit da ritrasmettere rispetto ad una ritrasmissione di un intero pacchetto dati (lungo 512-1024 byte).

Utilizzando questa nuova tecnica, si potrebbe verificare la seguente situazione:

- 4 stazioni A, B, C e D;
- solo B è nel range di trasmissione di A;
- solo A e C sono nel range di trasmissione di B;
- solo B e D sono nel range di trasmissione di C;
- solo C è nel range di trasmissione di D;
- si sottolinea che D non “sente” A e B;

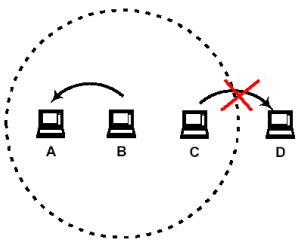

Figura 2.36: exposed terminal problem.

Tale situazione potrebbe portare al problema "del terminale esposto" (**exposed terminal problem**) (Figura 2.36):

1. B sta trasmettendo ad A dopo aver completato l'handshake RTS/CTS;
2. C, captando il RTS inviato da B, avvia la sua portante virtuale;
3. C vuole trasmettere a D ma ritarda la sua trasmissione fino al termine del NAV.

C ha ritardato la sua trasmissione anche se poteva trasmettere senza provocare collisioni: D non avrebbe sentito ciò che stava trasmettendo B, e A non avrebbe sentito ciò che avrebbe trasmesso C. Il throughput si è ridotto per ridurre il rischio di collisioni quando non era necessario.

Questo problema non viene risolto da 802.11 privilegiando una riduzione di rischio di collisione a una riduzione di throughput.

2.2.3. Point Coordination Function

Per sostenere un minimo di QoS (Quality of Service), quindi dare la possibilità ad una stazione con dati ad alta priorità di trasmettere subito, un Access Point (AP) può assumere un controllo più rigoroso sull'andamento delle trasmissioni e lo fa utilizzando il **PIFS** (PCF InterFrame Space) più breve del DIFS. In questo caso l'AP svolge il ruolo di Point Coordinator (PC) supportando la Point Coordination Function (PCF): in occasione dell'invio dei pacchetti Beacon (pacchetti che l'AP invia ad intervalli regolari per rendersi visibile ai terminali che volessero connettersi a lui) può dare inizio ad un periodo libero da contesa **CFP** (Contention-Free Period), in cui annuncia un NAV tale da inibire la trasmissione di tutte le altre stazioni. Al CFP segue un normale **CP** (Contention Period) in cui vige la DCF; si crea così un super-frame (Figura 2.37).

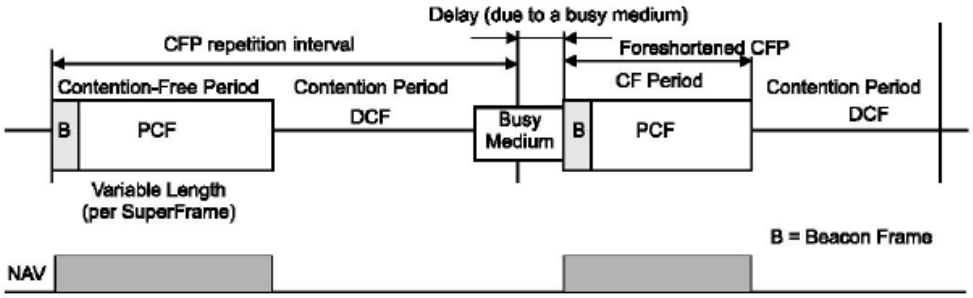

Figura 2.37: regolazione del canale trasmissivo con il super-frame creato dalla PCF.

La trasmissione del Beacon, che dovrebbe avvenire ad intervalli regolari, può essere posticipata a causa della occupazione del mezzo trasmissivo, ed in tal caso ha luogo dopo che è trascorso un PIFS dal momento in cui il mezzo è libero.

La durata del CFP può essere minore del previsto, in tal caso viene tramessa una trama di controllo CF-End, che fa terminare il NAV.

Durante il CFP, il PC invia messaggi di CF-Poll a rotazione verso le stazioni, interrogandole riguardo alla disponibilità di dati da trasmettere. In questo modo, anche in presenza di traffico sostenuto proveniente/destinato da/a tutte le stazioni, si riesce a garantire una certa equità di trattamento per le diverse stazioni (Figura 2.38).

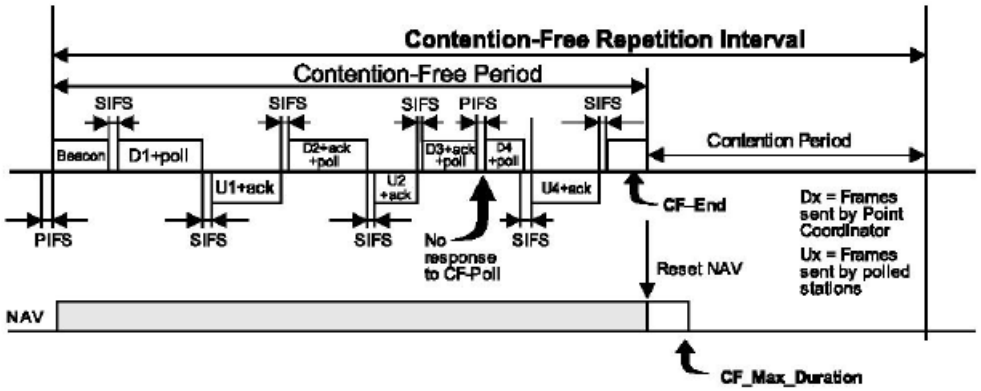

Figura 2.38: esempio di occupazione del canale trasmissivo regolato dalla PCF, in un CF Repetition Interval.

2.2.4. Hybrid Coordination Function

Lo standard IEEE 802.11e-2005 migliora la DCF e la PCF con una nuova funzione di coordinamento: la Hybrid Coordination Function (HCF). 802.11e definisce un set di miglioramenti per la QoS su reti wireless ed è ritenuta di importanza assoluta per applicazioni sensibili al ritardo come VoIP o streeming multimedia.
La HCF definisce due metodi di accesso al mezzo simili rispettivamente alla DCF e alla PCF: il **EDCA** (Enhanced Distributed Channel Access) e il **HCCA** (HCF Controlled Channel Access). Entrambe definiscono delle categorie di traffico, ad esempio una e-mail apparterrà ad una classe a bassa priorità mentre una conversazione VoIP apparterrà ad una classe ad alta priorità.

2.2.4.1. Enhanced Distributed Channel Access

Con il EDCA il traffico ad alta priorità ha maggiore probabilità di essere inviato prima rispetto al traffico a bassa priorità; una stazione che vuole inviare dati ad alta priorità, infatti, deve aspettare in media un tempo minore. In pratica questo viene realizzato con una diversificazione della CW e del tempo **AIFS** (Arbitration InterFrame Space) in relazione alla priorità: il traffico ad alta priorità avrà una CW e un AIFS più corti, scelti in base alla Tabella 2.12.
Il EDCA prevede inoltre un accesso contention-free in un tempo chiamato **TXOP** (Transmit Opportunity) nel quale la stazione può inviare tutti i pacchetti che riesce. Il TXOP massimo è rispettato severamente: se un pacchetto dovesse sforare, deve essere frammentato e finito di trasmettere al TXOP successivo. Questa tecnica, oltre a dare la possibilità di trasmettere più dati video o voce di seguito, riduce il problema delle stazioni a basso rate fornendo loro un tempo dedicato.

AC	CWmin	CWmax	AIFSN	Max TXOP
Background (AC_BK)	31	1023	7	0
Best Effort (AC_BE)	31	1023	3	0
Video (AC_VI)	15	31	2	3,008ms
Voice (AC_VO)	7	15	2	1,504ms
Legacy DCF	15	1023	2	0

Tabella 2.12: caratteristiche assegnate alle diverse categorie di traffico.

AC: Access Category.
TXOP=0: limitato a un singolo MPDU.

L'obiettivo della QoS è di preservare i dati ad alta priorità rispetto a quelli a priorità più bassa; ci sono però alcune situazioni in cui è necessario proteggere i dati anche da altri dati della stessa classe. Il EDCA fornisce l'Admission Control, per il quale l'AP pubblica la banda disponibile nei Beacon, cosicché le stazioni possano controllarla prima di aggiungere altro traffico.

2.2.4.2. HCF Controlled Channel Access

Il HCCA lavora in maniera molto simile alla PCF, con la differenza che il CFP, chiamato in questo caso **CAP** (Controlled Access Phase), può iniziare in qualsiasi momento del periodo tra due Beacon e non necessariamente all'inizio. Il CAP viene iniziato dall'AP, che prende il ruolo di Hybrid Coordinator (HC) in qualsiasi momento necessiti di inviare o ricevere dati in maniera libera da contesa. Nel resto del tempo (CP) tutte le stazioni funzionano in modalità EDCA.

L'ulteriore importante differenza con la PCF consiste nel fatto che, durante il CAP, l'HC non interroga tutte le stazioni una alla volta (round-robin), ma processa le informazioni inviategli dai client sulla lunghezza delle loro code di ogni classe di traffico per scegliere chi e per quanto tempo interrogare (il TXOP viene deciso dall'HC).

Il HCCA è considerato la più avanzata e complessa funzione di coordinamento, pochi AP in commercio infatti lo implementano. La Wi-Fi Alliance ha reso obbligatori solo il EDCA con il solo TXOP, il resto è facoltativo.

3. Lo standard IEEE 802.11n

Lo standard IEEE 802.11n-2009 è stato approvato dopo anni di studi e 8 versioni intermedie (la draft 2.0, approvata nel 2007, è stata implementata nei dispositivi di parecchie case produttrici senza aspettare la versione definitiva).
802.11n, pur lavorando su entrambe le bande ISM finora utilizzate (2,4 e 5 GHz), prevede un set di nuove tecniche e miglioramenti dei livelli fisico e MAC che accrescono radicalmente il throughput dei dispositivi, l'affidabilità delle comunicazioni e la distribuzione della copertura. I suoi punti di forza sono:

- la tecnica **MIMO** (Multiple Input Multiple Output), che sfrutta le diverse antenne dei dispositivi per aumentare affidabilità e bitrate;
- i canali larghi **40 MHz**, che portano più dati aumentando il bitrate;
- l'accrescimento dei **rate di modulazione**;
- la riduzione dell'**intervallo di guardia**;
- la **Frame Aggregation**, che riduce l'overhead unendo più pacchetti insieme;
- il **RIFS** (Reduced InterFrame Space), che riduce l'overhead quando non è possibile usare il Frame Aggregation;
- il miglioramento del **Power Saving** per i client;
- la robusta **retrocompatibilità**, che permette la coesistenza di dispositivi a, b, g e n finchè non avverà il completo passaggio a 802.11n, evento che porterà ulteriori miglioramenti ora utilizzabili solo in greenfield (zone con soli dispositivi n).

3.1. MIMO

Multiple Input Multiple Output (MIMO) è il cuore di 802.11n ed è la tecnica principale che permette di ottenere rate trasmissivi fino a dieci volte superiori a 802.11a/b/g pur lavorando nello stesso spettro. Sfruttando le antenne multiple dei dispositivi, MIMO migliora le situazioni con un difficile ambiente per le Radio Frequenze (RF) (muri spessi, stanze piccole, …) nonché quelle che richiedono un alto throughput o QoS.

In un collegamento radio classico single input single output, il parametro che descrive quanto è buona la comunicazione, e quindi quanta informazione è possibile trasportare, è il Rapporto Segnale/Rumore **SNR** (Signal to Noise Ratio), tipicamente espresso in deciBel (dB), che esprime quanto è più potente il segnale rispetto al disturbo al ricevitore.
MIMO riesce ad accrescere molto il SNR, e una volta raggiunto il valore minimo per garantire lo scambio rapido di dati, tutto il SNR addizionale può essere utilizzato per aumentare il rate, aumentare la distanza o, in più piccola parte, entrambi.

In un tipico ambiente indoor (abitazioni, uffici, strutture pubbliche, …) è raro che un'onda radio segua il percorso dritto e più breve dal trasmettitore al ricevitore; spesso le due antenne non sono in LOS (Line Of Sight), cioè non si vedono direttamente, per via di ostacoli (muri, porte, …) che possono attenuare il segnale fino a rendere la sua potenza comparabile a quella del rumore, quindi indecifrabile dal ricevitore.
Fortunatamente le onde radio possono seguire altri percorsi per arrivare al ricevitore, infatti molte superfici (arredamento metallico, porte metalliche, tubi, …) riflettono l'onda elettromagnetica. La riflessione, che aiuta a raggiungere il ricevitore, ha purtroppo anche un lato molto negativo: gli infiniti percorsi che l'onda può seguire riflettendosi (**multipath**) fanno si che al ricevitore arrivino molte copie del segnale diradate nel tempo (prima arriverà la porzione di onda che ha seguito il percorso più breve e via via le altre), distorcendo il segnale complessivo. Inviando lo stesso segnale su due antenne diverse, senza utilizzare le tecniche MIMO, il fenomeno viene amplificato ulteriormente (Figura 3.1).

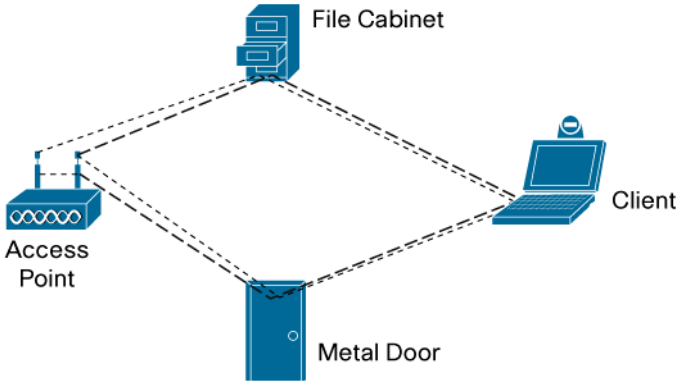

Figura 3.1: multipath creato da 2 antenne trasmissive.

Le copie della stessa onda che arrivano al ricevitore possono poi creare interferenza costruttiva o distruttiva (se in opposizione di fase) in maniera pressochè casuale rispetto a frequenza e posizione dell'antenna: **multipath fading**, un esempio nel grafico di Figura 3.2.

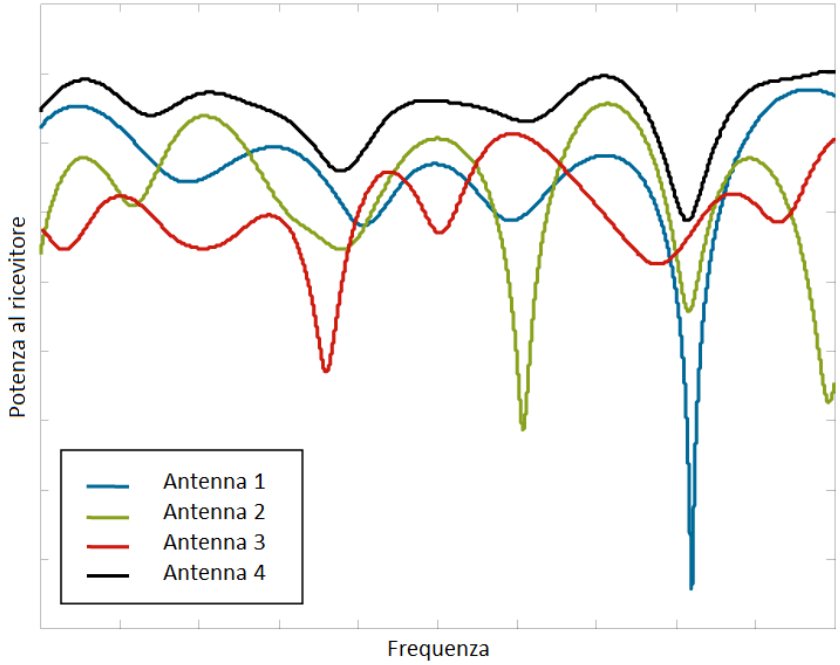

Figura 3.2: esempio di canale soggetto a multipath fading.

Un dispositivo che utilizza le avanzate tecniche MIMO invia segnali diversi contemporaneamente sulle diverse antenne, traendo vantaggio dal multipath. I segnali possono essere adeguate modificazioni della stessa informazione per aumentare l'affidabilità, o informazioni totalmente diverse per aumentare il throughput. Ciascun segnale viene inviato da una singola antenna che usa la propria catena RF (dispositivo che porta il segnale in banda base ad una RF adatta ad essere trasmessa o viceversa). Visto lo spazio esistente tra due antenne diverse, ogni segnale segue un percorso RF (una per antenna) e riceverà in ognuna di esse segnali con percorsi multipath indipendenti, che processerà e combinerà insieme o sfrutterà per ricevere più informazioni contemporanamente. Le potenti funzioni che il MIMO riesce ad implementare sono (Figura 3.3): diverso prima di arrivare all'antenna ricevente. Anche il ricevitore, se possiede più antenne, avrà più catene

- utilizzare più antenne trasmittenti che inviano la stessa informazione per accrescere il SNR al ricevitore;
- utilizzare più antenne riceventi per accrescere il SNR combinando i segnali multipli con l'**equalizzatore MIMO**;
- utilizzare più antenne trasmittenti e riceventi per inviare più segnali (**spatial stream**) allo stesso tempo e nello stesso spettro realizzando lo **Spatial Division Multiplexing** (SDM).

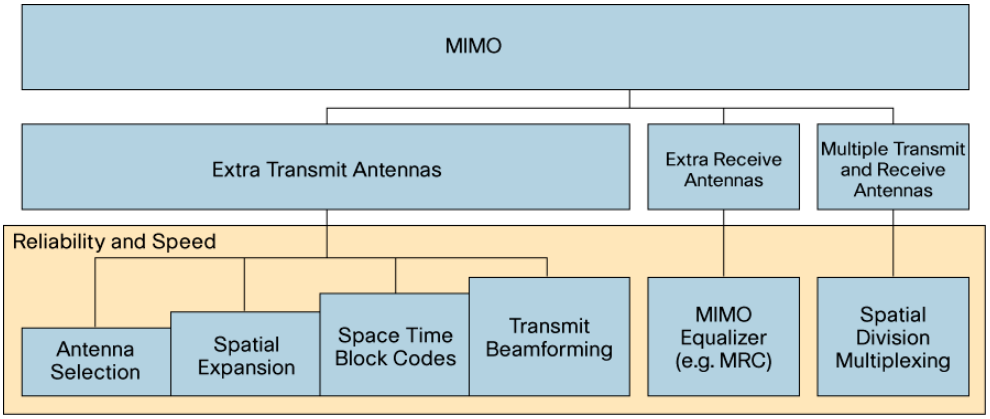

Figura 3.3: tecniche MIMO in base alla disponibilità di antenne addizionali.

Un collegamento MIMO è descritto dal numero di antenne che utilizza in trasmissione e in ricezione, e viene indicato generalmente in questo modo: TxR, con T numero di antenne trasmittenti e R riceventi; ad esempio 3x2 rappresenta un link con 3 antenne in trasmissione e 2 in ricezione. 802.11n permette un massimo di 4 spatial stream (4x4), si avranno poi tutte le combinazioni intermedie tra 1x1 e 4x4.
La potenza della tecnica e la complessità di realizzazione cresce passando dalle molteplici antenne trasmissive, all'equalizzatore MIMO, fino allo SDM, quindi un link 2x3 (2 spatial stream SDM + 1 equalizzatore MIMO) è migliore di un link 3x2 (2 spatial stream SDM + 1 antenna trasmittente addizionale). 802.11n definisce, come si è appena visto, un set di tecniche trasmissive in base al numero di antenne trasmittenti e riceventi, dando priorità allo SDM per poi migliorare il link con le ulteriori antenne disponibili.

3.1.1. Uso delle antenne trasmittenti per accrescere il SNR

Avendo a disposizione più antenne trasmittenti che spatial stream (SDM), si può migliorare il SNR al ricevitore sfruttando le antenne trasmittenti addizionali utilizzando diverse tecniche riportate di seguito in ordine di potenza e complessità decrescenti: il **transmit beamforming**, lo **Space Time Block Coding** (STBC), la **Spatial Expansion** (SE, anche chiamata cyclic delay diversity) e la **selezione dell'antenna**.

3.1.1.1. Transmit beamforming

Quando si ha a disposizione più di una antenna trasmittente, il transmit beamforming è il metodo per coordinare i segnali inviati da ogni antenna affinchè la ricezione sia radicalmente migliorata. Questa tecnica era stata creata originariamente per link 2x1 in presenza di numerosi ostacoli e superfici riflettenti, ma è stata adattata anche a tutte le altre situazioni MIMO-OFDM. Il transmit beamforming applicato a link 2x1 riesce ad accrescere il SNR di 3-6 dB (in base al rate).

Per comprendere come lavora il transmit beamforming bisogna pensare ai segnali come onde; considerando un collegamento 2x1, all'antenna ricevente le due onde verranno sommate insieme: in base alla differenza di percorso arriveranno in fase o in opposizione di fase, rispettivamente sommandosi (**interferenza costruttiva**) o sottraendosi (interferenza distruttiva). L'obiettivo del transmit beamforming è proprio quello di far arrivare le onde in fase, in modo da sommarsi positivamente, come osservabile in Figura 3.4.

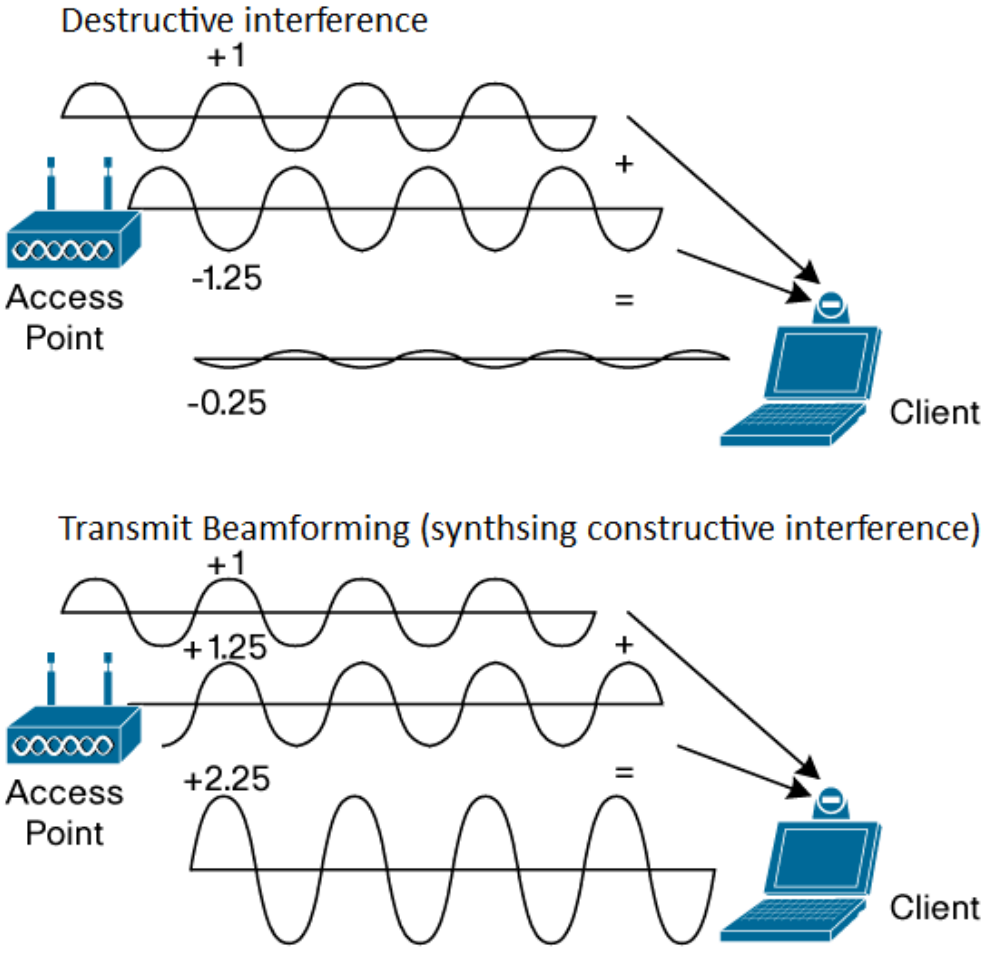

Figura 3.4: interferenza distruttiva e costruttiva (obbiettivo del transmit beamforming).

Il transmit beamforming non si può implementare semplicemente nel trasmettitore, dato che quest'ultimo necessita di continue informazioni sul segnale ricevuto dal ricevitore (soprattutto se il client si sposta nello spazio); 802.11n definisce il protocollo che trasporta questo tipo di informazioni. Vista la complessità di realizzazione, la prima generazione di dispositivi n non implementava questa tecnica.

È importante osservare che il transmit beamforming non è applicabile a trasmissioni broadcast o multicast, non potendo ottimizzare le fasi di più apparati riceventi contemporaneamente; non riesce quindi a migliorare l'area di copertura di un AP che dipende dalla trasmissione dei Beacon inviati in broadcast.

3.1.1.2. Space Time Block Coding

Lo Space Time Block Coding (STBC) utilizza le antenne addizionali per inviare, in tempi successivi, una versione riordinata dei dati inviati dalla prima antenna per poter correggere gli eventuali errori. È possibile utilizzare lo STBC in collegamenti 2x1, 3x2, 4x2 e 4x3 ma solo il 2x1 è certificato dalla Wi-Fi Alliance. I dati vengono divisi in blocchi di dimensione M (il numero di bit che forma un simbolo OFDM), dopodiché, ad esempio in un collegamento 2x1, i blocchi vengono duplicati in due stream (uno per antenna): il primo viene inviato, il secondo viene diversamente ordinato e inviato subito dopo il primo (Figura 3.5). Il throughput viene dimezzato (perché vengono inviati due volte gli stessi dati) ma moltissimi errori vengono corretti confrontando le due stringhe; per avere un errore dovrebbero infatti essere compromessi

entrambi i percorsi multipath in tempi differenti, situazione molto poco probabile.

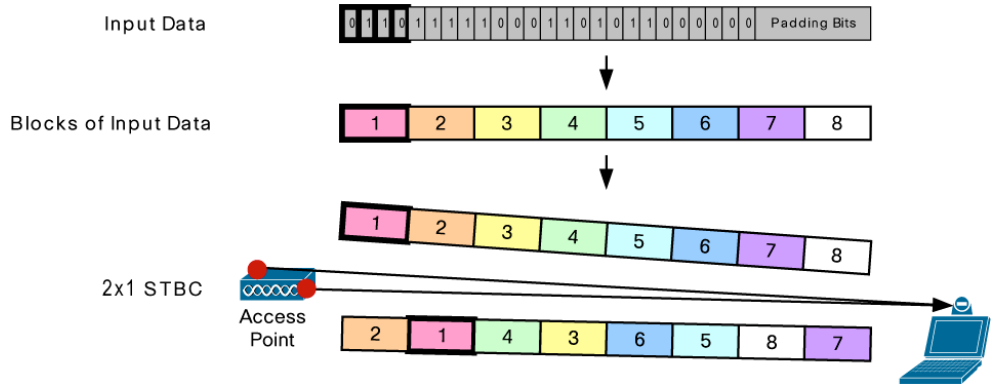

Figura 3.5: Space Time Block Coding in un collegamento 2x1.

Osserviamo che lo STBC può lavorare sia in unicast che in broadcast/multicast non essendoci settaggi individuali per ogni ricevitore. Essendo però una tecnica di livello fisico, può essere utilizzata in broadcast/multicast solo se tutti i client la supportano: non può essere usata in presenza anche di un solo dispositivo a/b/g, n draft 2.0 e n che non la implementa (essendo opzionale).

3.1.1.3. Spatial Expansion

La Spatial Expansion (SE), anche chiamata cyclic delay diversity, è un metodo rudimentale per mappare i diversi spatial stream sulle diverse antenne trasmittenti. La SE fa in modo di evitare di trasmettere, non intenzionalmente, troppa energia su un unico percorso multipath casuale per antenna, che potrebbe essere affetto da multipath fading (interferenza distruttiva a certe frequenze). La SE è molto utile in situazioni in cui ostacoli e riflessioni creano pochi echi al ricevitore (ci sono pochi percorsi possibili). Questa tecnica agisce appunto creando echi artificiali del segnale con le antenne addizionali in modo che il ricevitore veda un canale medio buono anche quando il percorso dell'antenna principale è affetto da multipath fading che attenua di molto il segnale.
La SE è applicata "alla cieca": senza riscontri dei ricevitori, indipendentemente dalla situazione attuale del canale, i suoi benefici sono quindi modesti per situazioni generiche.

3.1.1.4. Selezione dell'antenna

La selezione dell'antenna è una tecnica usata principalmente negli AP a/b/g con più antenne che tipicamente hanno una sola catena RF e non possono quindi utilizzare le tecniche viste finora. Usando misure di PER (Packet Error Rate) o di potenza del segnale ricevuto, si determina quale sia la migliore antenna trasmittente da usare con un determinato client.
Questa tecnica è un debole strumento in confronto alle tecniche precedenti, oltretutto la scelta dell'antenna può richiedere la trasmissione di molti pacchetti di controllo.

3.1.2. Equalizzatore MIMO

L'equalizzatore MIMO è la tecnica complementare del transmit beamforming, infatti permette al ricevitore di combinare al meglio i diversi segnali ricevuti sulle antenne multiple. Nel caso di un singolo spatial stream in un link 1x2 (Figura 3.6), l'equalizzatore MIMO è meglio conosciuto come Maximum Ratio Combiner (MRC).

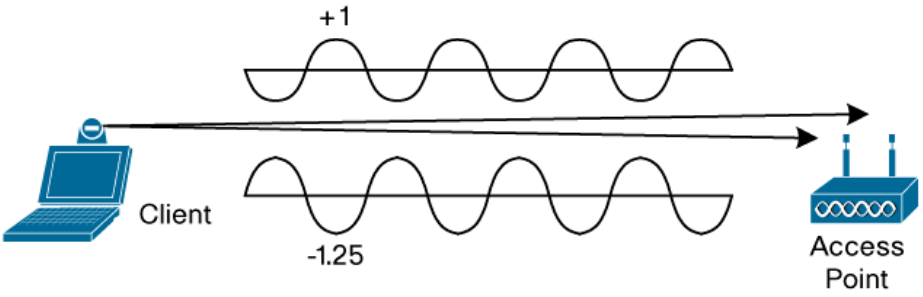

Figura 3.6: collegamento 1x2.

Prendendo come esempio il link 1x2, la singola antenna trasmittente invia il segnale che sarà riflesso e attenuato dai diversi ostacoli, percorrendo strade molteplici (multipath). Il segnale arriva ad una antenna del ricevitore e, in base al percorso che ha seguito, i suoi echi possono creare interferenza costruttiva o distruttiva. Se il ricevitore possiede una seconda antenna, anch'essa riceverà il segnale che però, vista la distanza tra le due antenne, avrà seguito un percorso diverso. È poco probabile che entrambi i percorsi abbiano provocato interferenza distruttiva, quindi la **spatial diversity** ha fatto in modo che, combinando matematicamente i due segnali ricevuti dalle due antenne, il SNR sia cresciuto.

3.1.3. Spatial Division Multiplexing

Lo Spatial Division Multiplexing (SDM) è la tecnica che permette ad ogni coppia di antenne (trasmittente/ricevente) di trasmettere, nel proprio spatial stream, la propria informazione, diversa da quella delle altre coppie. Può essere utilizzata per link 2x2, 3x3, 4x4 duplicando, triplicando e quadruplicando il bitrate (ogni antenna ulteriore da un singolo lato della trasmissione può essere usata per una delle precedenti tecniche), è quindi questa la tecnica che permette a 802.11n di incrementare così drasticamente il rate trasmissivo rispetto ai precedenti standard.

Raggiungere la velocità massima, comunque, diventa sempre più difficile con il crescere degli spatial stream: è richiesto un SNR sempre più elevato, i dispositivi devono essere molto vicini e le trasmissioni sono sempre più sensibili a interferenze di altri dispositivi vicini o non-Wi-Fi. Un'implementazione diretta dei rate più alti richiede un SNR superiore a 35 dB e una distanza inferiore a 6 metri, quindi per l'uso "enterprise" lo SDM deve essere supportato da metodi ausiliari per incrementare il SNR come antenne addizionali oltre agli spatial stream per usare l'equalizzatore MIMO o il transmit beamforming, correzione di errori, ricevitore ottimale e assenza di interferenza non-Wi-Fi.

La Wi-Fi Alliance per 802.11n draft 2.0 certificava fino a due spatial stream per lo SDM; per la revisione finale di 802.11n ne ha testati e certificati tre che già risultano di difficile uso al momento attuale visti l'elevato SNR richiesto e la maggioranza di dispositivi a/b/g installati.

3.2. Miglioramenti del physical layer

Oltre alla novità della tecnologia MIMO, 802.11n prevede numerosi miglioramenti sulla parte radio per accrescere il throughput effettivo delle WLAN. I più importanti riguardano la larghezza dei canali, i rate di modulazione e l'intervallo di guardia.

3.2.1. Canali da 40 MHz

802.11 e 802.11b usano canali larghi 22 MHz e distanti 25 MHz l'uno dall'altro; 802.11a e g usano canali larghi 20 MHz (essendo 802.11g un'estensione di b anch'esso spazia di 25 MHz). Il bitrate per larghezza di banda è un'importante misura dell'efficienza di un canale radio ed è chiamata **efficienza spettrale** (misurata in bit al secondo per hertz). L'efficienza spettrale di 802.11b è 0,5 bit al secondo per hertz (11 Mbps in 22 MHz), quella di 802.11a e g è 2,7 bit al secondo per hertz (a 54 Mbps).

Alcuni produttori di dispositivi a e g erano riusciti a fornire ai loro acquirenti velocità di 108 Mbps, pur utilizzando la medesima tecnologia OFDM: semplicemente usavano due canali adiacenti allo stesso tempo, coniando la tecnica **channel bonding**. L'efficienza spettrale resta la stessa ma avendo a disposizione una larghezza di banda doppia il bitrate del collegamento raddoppia.

802.11n non solo mette a disposizione canali da 40 MHz (oltre a quello standard da 20 MHz), ma prevede anche l'uso della parte di spettro che era adibita ad evitare l'interferenza tra canali adiacenti, ricavando 4 ulteriori sub-carrier (Figura 3.7). Passando quindi da un canale da 20 MHz ad uno da 40 MHz il rate è più che duplicato e l'efficienza spettrale aumenta leggermente grazie alle portanti addizionali.

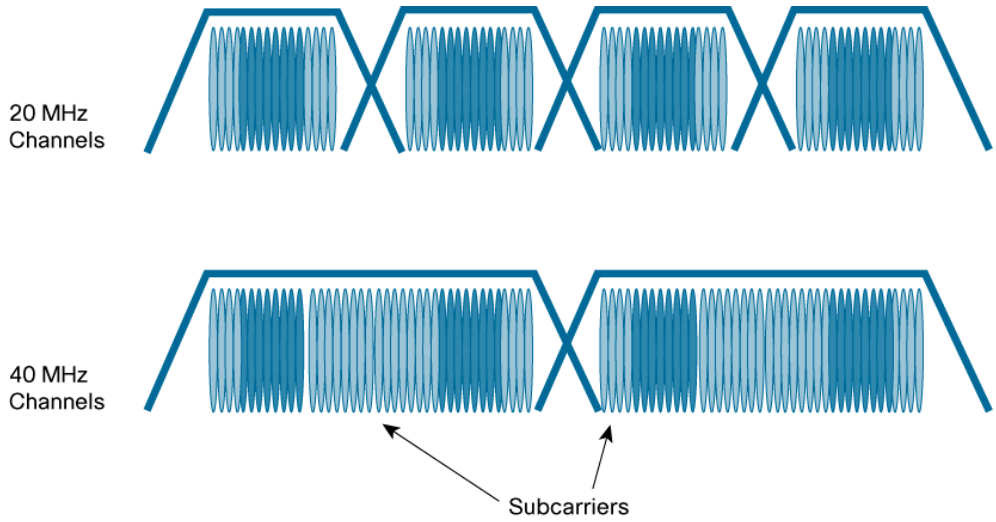

Figura 3.7: confronto tra canali da 20 e 40 MHz.

3.2.2. Rate di modulazione superiori

In 802.11a e g un simbolo OFDM dura 4 µs, inclusi 800 ns di intervallo di guardia. Alla velocità più alta (54 Mbps) ogni simbolo trasporta 216 bit di dati e 72 bit di correzione d'errore (coding rate 3/4), per un totale di 288 bit in un simbolo OFDM distribuiti in 48 sub-carrier; ogni sub-carrier, infatti, è modulata 64QAM quindi è in grado di trasportare 6 bit per simbolo (6x48=288).

802.11n continua la scalata al miglioramento della modulazione e dell'efficienza spettrale come tutte le evoluzioni di 802.11; utilizza anch'esso la tecnica OFDM con un periodo di simbolo di 4 µs, ma incrementa il numero di sub-carrier in ogni canale da 20 MHz da 48 a 52, inoltre prevede un nuovo coding rate: 5/6. Questi due miglioramenti portano ad una velocità massima pari a 65 Mbps; usando lo SDM si raggiungono velocità

elevatissime quali 130, 195 e 260 Mbps rispettivamente per 2, 3 e 4 spatial stream (2, 3 e 4 antenne in trasmissione e ricezione); l'efficienza spettrale raggiunge i 13 bit al secondo per hertz.
Usando i nuovi canali da 40 MHz, 802.11n incrementa il numero delle sub-carrier a 108 (52+52+4). Ciò porta a dei rate esorbitanti: 135, 270, 405 e 540 Mbps rispettivamente per 1, 2, 3 e 4 spatial stream. L'efficienza spettrale sale a 13,5 bit al secondo per hertz grazie alle 4 sub-carrier addizionali.
Nei rate elencati finora era sottointesa la **equal modulation**, cioè ogni spatial stream modula le proprie sub-carrier allo stesso modo degli altri (ad esempio tutte 64QAM). 802.11n dà la possibilità di scegliere la modulazione di ogni singolo spatial stream (**unequal modulation**) incrementando a dismisura il numero di rate utilizzabili; sfortunatamente ciò ha pochi vantaggi pratici in quanto sarebbe richiesto molto feedback dal ricevitore per scegliere le modulazioni multiple ottimali.

3.2.3. Intervallo di guardia ridotto

Come già visto, l'intervallo di guardia è la parte di tempo del simbolo OFDM lasciata vuota per limitare l'ISI, cioè per lasciar decadere gli echi multipath del simbolo precedente prima di inviare il simbolo successivo (Figura 3.8). Una sovrapposizione di simboli ridurrebbe di molto il SNR.

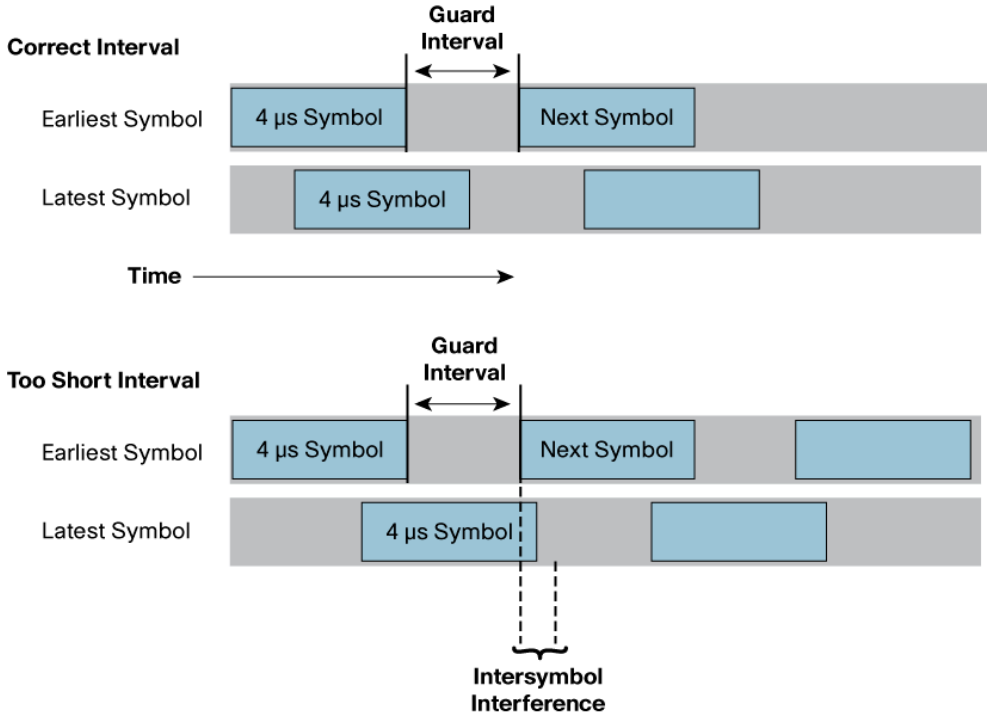

Figura 3.8: esempio di intervallo di guardia sufficiente e non sufficiente ad evitare l'ISI.

802.11n, così come fanno a e g, utilizza un intervallo di guardia standard lungo 800 ns, permettendo differenze di percorso fino a 800 piedi. In ambienti multipath in cui la differenza tra i percorsi multipath tra trasmettitore e ricevitore non è così elevata, 802.11n prevede un **intervallo di guardia ridotto** a 400 ns. Ciò riduce l'overhead del simbolo OFDM e abbassa la sua durata da 4 µs a 3,6 µs, aumentado il rate. Per i canali da 20 MHz le velocità massime raggiungibili in base agli spatial stream disponibili sono 72, 144, 216 e 288 Mbps, per quelli da 40 MHz 150, 300, 450 e 600 Mbps.

3.3. Miglioramenti del MAC layer

L'aumento del rate radio non è il solo elemento da migliorare per accrescere le prestazioni delle WLAN. C'è una quantità significativa di overhead fisso nel protocollo di livello MAC per ogni frame trasmesso che, alle più alte velocità, potrebbe addirittura superare i dati. 802.11n introduce dei cambiamenti nel livello MAC che mirano a ridurre questo overhead.

3.3.1. Frame aggregation

Ogni frame trasmesso da un dispositivo 802.11 ha un overhead fisso dovuto al radio-preamble, al radio-header e ai campi di controllo del livello MAC che limitano il throughput effettivo anche per rate molto elevati (Figura 3.9).

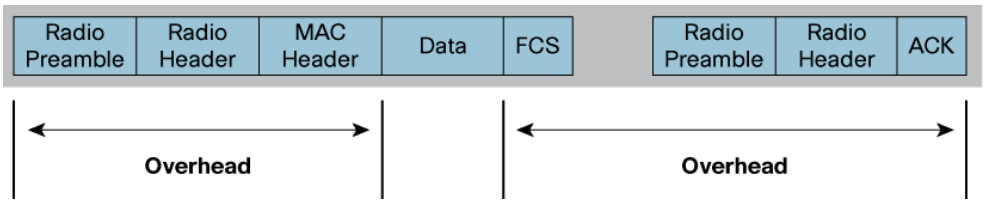

Figura 3.9: overhead in 802.11.

Per ridurre l'overhead, 802.11n introduce il **frame aggregation** cioè l'unione dei dati di più frame in un'unica trasmissione. Sono previsti due metodi di aggregazione: la **MAC Service Data Unit** (MSDU) **aggregation** e la MAC **Protocol Data Unit** (MPDU) **aggregation**. Entrambi i metodi riducono l'overhead ad un singolo radio-preamble e radio-header per tutti i frame aggregati, portando benefici specialmente nella trasmissione di numerosi pacchetti di piccole dimensioni (come voce, TCP ACK, …). La dimensione massima dei frame è aumentata da 4 a 64 kB in 802.11n per accomodare questi lunghi frame uniti.

Un ulteriore importante vantaggio portato dalla frame aggregation è il fatto che avendo meno frame da inviare il numero delle potenziali collisioni e il tempo perso dal backoff vengono significamente ridotti.

Una limitazione della frame aggregation consiste nel fatto che tutti i frame uniti in una trasmissione devono avere la medesima destinazione. Un'altra limitazione consiste nel fatto che tutti i frame da aggregare devono essere pronti nel trasmettitore allo stesso momento; ritardare l'invio per aspettare ulteriori frame da aggregare ridurrebbe i vantaggi. Una terza limitazione consiste nel fatto che i lunghi frame possono subire danneggiamenti dal **channel coherence time**, un fattore che dipende da quanto velocemente i terminali si muovono nello spazio: più velocemente si muovono, più deve essere corto un frame per arrivare senza corruzioni; in altre parole il tempo della trasmissione deve essere più corto del channel coherence time.

3.3.1.1. MAC Service Data Unit aggregation

Nei terminali (AP o client), i frame generati ai livelli superiori sono originariamente nel formato Ethernet; per essere trasmessi via radio, devono quindi essere prima tradotti in frame 802.11. La MSDU aggregation raccoglie i frame Ethernet con la stessa destinazione e li incapsula in un unico frame 802.11 con un unico radio e MAC header (Figura 3.10).

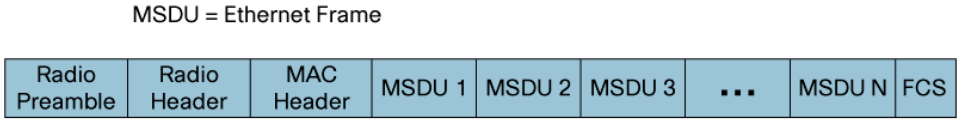

Figura 3.10: MAC Service Data Unit aggregation.

La MSDU aggregation è la modalità di aggregazione più efficiente per frame di dimensione fino al massimo concesso da questa tecnica (3839 o 7935 byte in base alla capacità del client), perché l'header Ethernet è più corto dell'header 802.11 (sarà chiaro il perché analizzando la MPDU aggregation).
Con la MSDU aggregation il frame totale è criptato tutto allo stesso modo e una sola volta (solo un header di criptazione), usando l'associazione di sicurezza instaurata col destinatario.
Una restrizione della MSDU aggregation consiste nel fatto che tutti i frame costituenti devono appartenere allo stesso livello QoS (non si possono ad esempio aggregare frame voce con frame best-effort).

3.3.1.2. MAC Protocol Data Unit aggregation

La MPDU aggregation è leggermente diversa dalla MSDU infatti invece di raccogliere frame Ethernet, li traduce prima in frame 802.11 e poi riunisce tutti quelli con la stessa destinazione. Non serve un ulteriore incapsulamento, tranne quello radio, in quanto ogni frame costituente ha già il suo header MAC 802.11 (Figura 3.11).

RP = Radio Preamble
RH = Rapid Header
MH = Mac Header
FCS = Frame Check Sequence

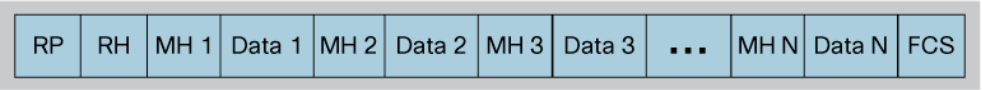

Figura 3.11: MAC Protocol Data Unit aggregation.

Si comprende che la MPDU aggregation è meno efficiente della MSDU per frame costituenti di lunghezza piccola e media, in quando l'header Ethernet è più corto dell'header 802.11. L'efficienza è ulteriormente ridotta dal fatto che ogni costituente viene criptato individualmente, quindi viene aggiunto overhead (un header di criptazione per ogni costituente). D'altro canto la MPDU aggregation può creare frame totali lunghi fino a 65535 byte quindi è preferibile per situazioni con molti frame di grandi dimensioni, disponibili per l'aggregazione.
Come la MSDU aggregation, la MPDU aggregation richiede che tutti i frame costituenti appartengano al medesimo livello QoS.

3.3.1.3. Block acknowledgement

Secondo il protocollo MAC 802.11 ad ogni frame 802.11 inviato ad un singolo destinatario (non broadcast o multicast) deve corrispondere una conferma di avvenuta ricezione da parte del ricevente: un ACKnowledgement.
La MSDU aggregation non richiede cambiamenti in questo ambito perché il frame complessivo è un unico normale frame 802.11, quindi richiede un solo ACK.
Per la MPDU non è così semplice: ogni costituente è un frame 802.11 al quale deve corrispondere un ACK individuale. Per soddisfare questa necessità 802.11n prevede un block acknowledgement: tutti gli ACK pronti per la trasmissione (quelli corrispondenti a frame arrivati senza errori) vengono aggregati in un unico frame e inviati al trasmettitore originario. Questo permette un semplice e rapido meccanismo di ritrasmissione selettiva dei soli

frame ricevuti con errori. In situazioni con elevato error rate questa ritrasmissione selettiva permette un throughput effettivo molto maggiore di quello della MSDU aggregation perché quest'ultima in caso di errori dovrebbe ritrasmettere l'intero frame aggregato.

3.3.2. Reduced InterFrame Space

Quando la frame aggregation non è utilizzabile, 802.11n prevede un altro meccanismo per ridurre l'overhead. Come già visto, 802.11e, l'estensione per la QoS, permette ad un trasmettitore di inviare un burst di frame separati da un SIFS durante la sua transmit opportunity, senza l'utilizzo del random backoff.
802.11n migliora questo meccanismo specificando un interframe space ancora più breve: il **RIFS** (Reduced InterFrame Space) che riduce i tempi morti (non occupati da trasmissione) nella transmit opportunity.
I due aspetti negativi del RIFS sono la minor efficienza della frame aggregation per trasmissioni allo stesso destinatario e l'utilizzo limitato al solo greenfield, cioè in assenza di dispositivi a/b/g nel range di trasmissione.

3.4. Power saving

Una catena RF richiede molta potenza; con la tecnologia MIMO si utilizzano fino a quattro catene RF, richiedendo fino al quadruplo della potenza. È evidente quindi che 802.11n ha dovuto introdurre dei miglioramenti anche nell'ambito del **power management**. Si sono introdotte due estensioni ai meccanismi originali e all'**automatic power save delivery** introdotto da 802.11e: lo **Spatial Multiplexing power save** e il **Power Save Multi-Poll**.

3.4.1. Spatial Multiplexing power save

Lo Spatial Multiplexing (SM) power save permette ai client 802.11n di spegnere tutte le proprie catene RF tranne una che resta in ascolto. Può avere due metodi di funzionamento: statico (static) o dinamico (dynamic).
Con lo static SM power save un client lascia accesa solo una catena RF diventando equivalente ad un client a o g. L'AP al quale è associato il client viene informato (con un nuovo tipo di pacchetto di controllo) che quest'ultimo sta lavorando con una sola catena RF, il primo dovrà quindi utilizzare un solo spatial stream finchè il client non lo informa di aver riattivato le sue catene RF addizionali.
Nel dynamic SM power save il client con una sola catena RF attiva, abilita tutte le catene RF alla ricezione del RTS dopodichè invia il CTS; al termine della ricezione può tornare in modalità basso consumo.

3.4.2. Power Save Multi-Poll

Il Power Save Multi-Poll (PSMP) è un meccanismo di polling che lavora insieme al HCCA: durante il CFP l'AP può interrogare un client in qualsiasi momento, quindi tutti i client dovrebbero essere sempre pronti a ricevere; con il PSMP l'AP inizia le trasmissioni inviando uno schema dei tempi destinati al downlink, uplink, broadcast, multicast e unicast, il client può così determinare immediatamente quando deve stare attivo e di conseguenza quando può entrare in modalità risparmio energetico.
Il PSMP non è un effettivo Unscheduled Automatic Power Save Delivery (U-APSD) definito in 802.11e, perché è pilotato dall'AP e perché richiede che il client resti attivo per ricevere lo schema PSMP.

3.5. Retrocompatibilità

La retrocompatibilità di 802.11n rispetto ai dispositivi a/b/g è un aspetto importantissimo del nuovo standard, dato che i nuovi dispositivi dovranno coesistere per lungo tempo con i vecchi non compromettendone il funzionamento. Per questo motivo 802.11n prevede due metodi di funzionamento: il **mixed-mode** in presenza di vecchi dispositivi e il **greenfield-mode** in assenza di essi.

In mixed-mode è previsto un meccanismo di protezione simile a quello già utilizzato in 802.11g: viene utilizzato un formato di pacchetto chiamato **HT-mixed,** che inizia con un preamble e un header radio decifrabili da qualsiasi dispositivo 802.11 legacy che informano della presenza e della durata della trasmissione in atto, e continua con preamble e header radio specifici di 802.11n che precedono i dati (Figura 3.12).

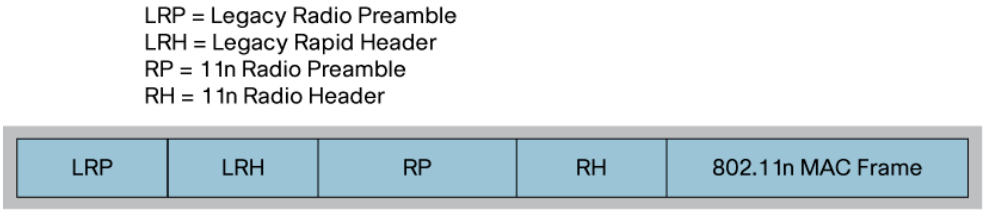

Figura 3.12: formato del pacchetto HT-mixed.

È necessario utilizzare oltre ai legacy preamble e header un ulteriore meccanismo di protezione già definito in 802.11g: il **CTS-to-self** che comunica ai dispositivi con standard precedenti quando possono trasmettere e quando devono effettuare un random backoff. Il CTS-to-self permette ai nuovi dispositivi di trasmettere un CTS destinato a se stessi che include le informazioni di durata della prossima trasmissione, attivando così la portante virtuale dei vicini; ovviamente il CTS deve essere trasmesso con rate ricevibili dai vecchi dispositivi.

Questi meccanismi di protezione richiedono maggiore overhead ad ogni trasmissione, quindi una riduzione del throughput effettivo non eliminabile in presenza di dispositivi pre-n.

In assenza di dispositivi con vecchi standard, 802.11n può lavorare al massimo delle sue potenzialità utilizzando il formato di pacchetto **HT-greenfield** che elimina i legacy preamble e header riducendo l'overhead di 12 µs.

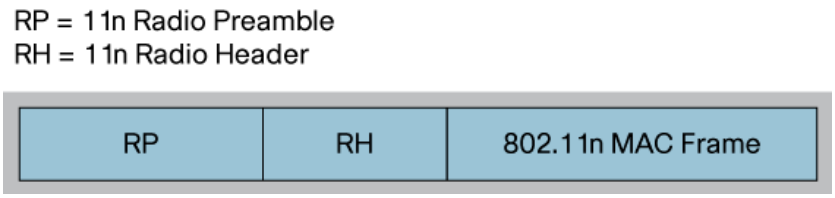

Figura 3.13: formato del pacchetto HT-greenfield.

Per utilizzare 802.11n in greenfield-mode si può pensare di riservare parte dello spettro solo ad esso. Nella banda dei 2,4 GHz ci sono pochi canali e molti dispositivi (b e g); nella banda dei 5 GHz ci sono invece molti canali in molte parti del mondo, quindi si può pensare di riservare qualche canale al solo 802.11n per utilizzarlo in greenfield-mode.

Uso dei canali da 40 MHz nella banda dei 2,4 GHz:

In molte parti del mondo la banda dei 2,4 GHz fornisce 3 o 4 canali non sovrapposti per l'utilizzo di 802.11b/g. L'uso dei canali da 40 MHz in questa banda pone molteplici problemi:

- i dispositivi legacy lavorano comunemente nei canali 1, 6 e 11; questo vale per canali distanziati di 25 MHz, mentre il mixed-mode preamble fornisce protezione solo ai canali distanziati di 20 MHz;
- una bassa percentuale di dispositivi funzionano nei canali intermedi (2, 3, 4, …) per i quali il mixed-mode preamble non funziona e il CTS-to-self può aiutare solo parzialmente;

- alcuni studi hanno rilevato che l'uso dei canali da 40 MHz di 802.11n nella banda dei 2,4 GHz può limitare altri sistemi che utilizzano questa stessa banda (come Bluetooth e Zigbee).

Per questi motivi 802.11n pone dei limiti molto restrittivi sull'uso dei canali da 40 MHz nella banda ISM dei 2,4 GHz: i dispositivi n non possono usare i canali da 40 MHz se sono presenti dispositivi pre-n in uno qualsiasi dei canali sovrapposti al loro. Devono quindi scansionare regolarmente i vari canali e fermare l'uso dei 40 MHz non appena venga rilevato un AP b/g che lavora in un canale sovrapposto al proprio o una trasmissione di un sistema non 802.11.
È evidente che nella pratica un canale da 40 MHz nella banda dei 2,4 GHz potrà essere usato molto raramente in situazioni non greenfield, anche perchè in tali situazioni, con i limiti imposti, questa banda permetterebbe 1 solo canale da 40 MHz affiancato da un solo canale da 20 o 25 MHz; oltretutto, con i CTS-to-self inviati a 1 o 2 Mbps, il canale da 40 MHz risulta meno efficiente di due canali da 20 MHz.

3.6. Migrazione

La migrazione verso 802.11n è ben avviata, anche grazie alla draft 2.0 che è stata adottata da molti costruttori ancora prima dell'approvazione della versione definitiva. 802.11n è già lo standard di default degli adattatori wireless dei laptop ed è implementato in praticamente tutti i dispositivi mobili di ultima generazione (smart-phone, pocket PC, …). La **pianificazione** della migrazione, soprattutto nell'ambito dello spettro radio, resta comunque essenziale.
La banda dei 2,4 GHz è larga non più di 100 MHz e molto meno in alcuni paesi del mondo. I dispositivi 802.11b e g, che lavorano nella stessa banda, sono i più diffusi al momento e per quanto riguarda questa banda, molto stretta, non si può fare molto altro che aspettare l' "estinzione" dei dispositivi pre-n. Come si è già osservato, ora è possibile sfruttare insieme solo un canale da 40 MHz e uno da 20 MHz (quando si erano riusciti a ricavare 4 canali da 20 MHz non sovrapposti), tuttavia in questa banda la situazione non migliorerebbe di molto neanche con il raggiungimento del greenfield totale, in quanto si trova difficoltà ad affiancare anche solo due canali da 40 MHz senza sovrapporli: non c'è banda a sufficienza.
La banda ISM dei 5 GHz è stata aperta in gran parte del mondo e riesce a contenere molti più canali permettendo una migliore pianificazione, anche per quanto riguarda i canali da 40 MHz.
In questa banda sono infatti possibili due metodi di migrazione: il primo è, anche in questo caso, quello di aspettare la dismissione dei dispositivi 802.11a o la loro sostituzione con dispositivi n, e durante il tempo richiesto operare in mixed-mode; il secondo è quello di riassegnare i canali dei dispositivi 802.11a in modo da lasciarne un gruppo libero dove 802.11n possa lavorare tranquillamente in greenfield mode.

Nell'ambito della migrazione si devono considerare anche altri due importanti aspetti dal punto di vista hardware: il primo riguarda maggiormente le strutture domestiche, il secondo quelle industriali.
In ambito domestico gli AP sono oggi tipicamente collegati con una rete cablata Ethernet che supporta fino a 100 Mbps. I dispositivi pre-n possono riversare nella rete Ethernet fino a 108 Mbps nominali che con le varie inefficienze si riducono a 50-60 Mbps. I nuovi dispositivi n, con un singolo collegamento dual-band (un canale da 20 MHz nei 2,4 GHz e uno da 40 MHz nei 5 GHz), possono iniettare nella loro rete Ethernet picchi di 300-400 Mbps, rendendo la rete cablata un collo di bottiglia. Un'altra necessità per sfruttare a pieno 802.11n diventa quindi l'upgrade delle reti cablate domestiche da 100 Mbps a **1 Gbps**.
Per quanto riguarda gli ambienti industriali, ci potrebbero essere problemi di migrazione nelle reti in cui è stato scelto di utilizzare la **PoE** (Power over Ethernet) o 802.3af, cioè l'alimentazione dei dispositivi attraverso la rete Ethernet piuttosto che attraverso quella elettrica (i telefoni VoIP sono un esempio tipico di questo utilizzo). Rispetto alle precedenti

versioni, tutte le tecnologie adottate in 802.11n richiedono decisamente molta potenza in più. Per ovviare a questo problema è stato definito lo standard 802.3at (802.3 è Ethernet) che permette di fornire fino a 30 W di potenza ai dispositivi. In alternativa qualche produttore ha provato a rinnovare i chipset affinchè richiedano potenza al di sotto del limite del vecchio standard.

4. Conclusioni

Riassumendo, i benefici introdotti dallo standard 802.11n rispetto alle versioni precedenti derivano da due grandi processi:

- il processo di **innovazione** che ha portato alla tecnologia MIMO accrescendo enormemente il throughput e il SNR raggiungibile dal collegamento radio, grazie alle complesse tecniche Spatial Division Multiplexing, equalizzatore MIMO e transmit beamforming;
- il processo di **ottimizzazione** del livello fisico, che ha introdotto i canali da 40 MHz, i rate di modulazione superiori e l'intervallo di guardia ridotto, e del livello MAC, che ha portato alla frame aggregation e al Reduced InterFrame Space.

Alcune osservazioni possono scaturire osservando i router wireless certificati 802.11n in vendita nei grandi magazini: i più economici montano una sola antenna, il che impedisce l'applicazione delle tecniche MIMO; gli apparecchi di fascia leggermente superiore con 2 antenne non parlano nelle specifiche di tecniche MIMO, cosa che fa supporre che lavorino come gli apparecchi pre-n con 2 antenne; tutti evidenziano nella voce "dual band" il "pregio" di poter selezionare la banda ISM in cui il router lavorerà, anziché lavorare su entrambe le bande contemporaneamente come permette lo standard; i dispositivi con 3 antenne che implementano le tecniche MIMO sono molto costosi e si trovano solo in negozi specializzati. Si presume e si spera che le aziende e i grossi enti, adoperino i dispositivi che implementano a pieno le potenzialità di 802.11n.
I laptop, tutti ormai certificati 802.11n, montano di norma, sulla scheda di rete wireless, una sola antenna confidando nel fatto che almeno il router possieda più antenne addizionali, il che impedisce che le potenzialità dello standard vengano sfruttate a pieno. Per chi ne avesse l'esigenza, si possono trovare in commercio schede wireless esterne con più antenne, per PC sia fisso che portatile.
Si è osservato invece che i dispositivi outdoor messi a disposizione da alcuni comuni (ad esempio Venezia-Mestre) e disseminati nei punti di interesse della città, sono tecnologicamente molto avanzati e possiedono spesso 4 o 5 antenne.

Per concludere si può dire che IEEE 802.11n si prospetta di migliorare drasticamente l'esperienza delle WLAN, incrementando in misura mai raggiunta il throughput, l'affidabilità e la robustezza della rete, nonché la copertura dei punti morti. Come è stato osservato però, per sfruttare al meglio le potenzialità del nuovo standard è essenziale il passaggio completo di tutte le reti WLAN a dispositivi certificati 802.11n.

Bibliografia

- “Medium Access Control in Wireless Networks”, Hongyi Wu, Yi Pan Editors, biblioteca DEI ;
- “WLAN - 802.11 a,b,g and n”, National Instruments, http://zone.ni.com/devzone/cda/tut/p/id/7131#toc0 ;
- “802.11n: The Standard Revealed”, Cisco Systems White Paper;
- “A Technical Tutorial on the IEEE 802.11 Protocol”, Pablo Benner, BreezeCOM ;
- http://en.wikipedia.org ;
- http://it.wikipedia.org ;
- http://infocom.uniroma1.it/alef/802.11/on_desk/accesso.html .