Il protocollo IEEE 802.11

1 - Introduzione

La descrizione del IEEE 802.11 consente di comprenderne i concetti fondamentali, il principio di funzionamento e molte delle ragioni che stanno dietro alle caratteristiche e ai componenti dello standard.

Anche se l'esposizione non sarà esaustiva di tutti gli argomenti e meccanismi compresi nello standard si tenterà di dare una descrizione degli elementi basilari in modo da comprendere le considerazioni che verranno sviluppate sulle applicazioni del protocollo sugli apparati Wireless LAN.

1.1- Architettura di rete

Componenti dell'architettura

L'architettura di una rete di comunicazione **wireless LAN 802.11** si fonda su una struttura cellulare, simile a quella dei sistemi di distribuzione per servizi di telefonia **GSM** (*Global System for Mobile communications*). Ciascuna cella è chiamata **Basic Service Area** (**BSA**). Un gruppo di stazioni situate all'interno di una BSA, in grado di comunicare tra di loro, formano un **Basic Service Set** (**BSS**). Ogni cella è controllata da una stazione base denominata **Access Point** (**AP**).

La maggior parte delle wireless LAN è formata da una molteplicità di celle dove i singoli Access Point sono interconnessi attraverso una qualche tipo di rete di distribuzione, che normalmente viene definita **Distribution System** (**DS**). Quello che si ottiene è chiamato **Extended Service Area** (**ESA**).

La rete di distribuzione è normalmente costituita da una dorsale **Ethernet** ed in certi casi è wireless essa stessa.

Il complesso delle diverse wireless LAN interconnesse, comprendenti differenti celle, i relativi Access Point e il sistema di distribuzione, viene visto come una singola rete 802 dai livelli superiori del **modello OSI** ed è noto nello standard come **Extended Service Set** (**ESS**).

L'equipment di rete può supportare due diversi tipi di wireless LAN:

- **AD HOC LAN** - Rete formata da un certo numero di stazioni, contenute in un'area limitata, e caratterizzata da facilità e rapidità di installazione, senza il supporto di una precedente infrastruttura.
- **INFRASTRUCTURE WIRELESS LAN** - Rete che include nodi speciali, gli Access Point, a ciascuno dei quali compete uno specifico BSS. Gli AP sono fra loro collegati tramite un Distribution System, normalmente in cavo, ma che potrebbe essere anche parzialmente wireless. Il sistema di distribuzione può fornire, inoltre, delle strutture adeguate (**Server**) per interfacciarsi con reti già esistenti.

Lo standard definisce anche il concetto di **Portal**. Un Portal è un dispositivo che permette l'interconnessione tra una rete LAN 802.11 e un'altra rete 802. Anche se lo standard non lo richiede espressamente, la maggior parte delle installazioni riuniscono l'Access Point e il Portal in un'unica entità fisica.

In Figura 1 è mostrato lo schema di una tipica rete LAN basata sul protocollo 802.11 comprendente i componenti descritti.

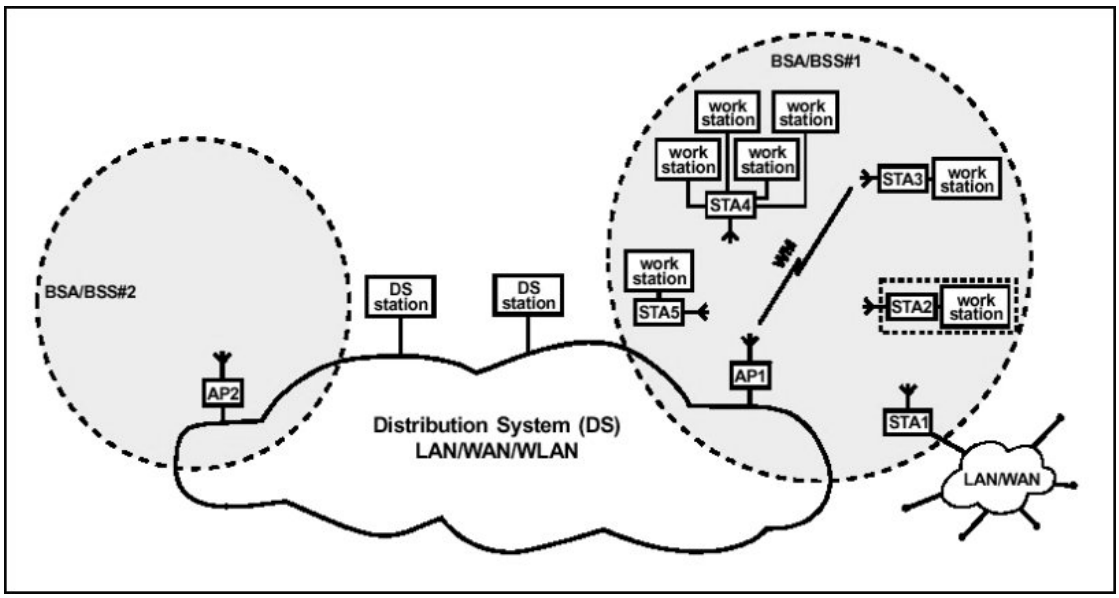

Figura 1 - Una tipica LAN 802.11

1. 2 - Gli Access Point

Gli Access Point sono dei nodi speciali a ciascuno dei quali compete uno specifico BSS.

Fra le funzioni degli AP:

AUTENTICAZIONE, ASSOCIAZIONE E RIASSOCIAZIONE. Gli AP consentono alle stazioni wireless di essere identificate e rimanere connesse alla rete pur spostandosi da una BSA ad un'altra.

POWER MANAGEMENT FUNCTIONS. Gli Access Point permettono alle stazioni wireless, e quindi **battery powered**, di operare in regime di consumo ridotto di potenza (*Power Save Mode*).

SYNCHRONIZATION FUNCTIONS. Assicurano che tutte le stazioni correntemente associate con l'AP siano sincronizzate su un clock comune. Il sincronismo fra le stazioni è indispensabile per sostenere servizi isocroni (**time bounded services**), per la gestione degli hop di frequenza e le funzioni di power management.

1.3 - Descrizione degli strati del protocollo

Come tutti gli altri protocolli 802.x, anche il protocollo 802.11 prende in considerazione i due livelli di MAC e livello fisico. Lo standard attualmente disponibile definisce un singolo livello MAC che può interagire con i seguenti tre livelli fisici, operanti a velocità variabili tra 1 e 3 Mbit/s:

- **Frequency Hopping Spread Spectrum (FHSS)** nella banda **ISM 2,4 GHz**

- **Direct Sequence Spread Spectrum (DSSS)** nella banda **ISM 2,4 GHz**
- **Trasmissione infrarossa**

<table>
<tr><td colspan="3">802.2</td><td>Data Link Layer</td></tr>
<tr><td colspan="3">802.11 MAC</td><td></td></tr>
<tr><td>FH</td><td>DS</td><td>IR</td><td>PHY Layer</td></tr>
</table>

Figura 2 - Stack IEEE 802.11

Inoltre il MAC 802.11 supporta alcune funzionalità aggiuntive, come la gestione della frammentazione delle **Protocol Data Unit**, la trasmissione dei pacchetti e la **gestione dell'acknowledge**.

Livello MAC

Il livello di MAC definisce due differenti metodi di accesso:

- **Distributed Coordination Function (DCF)** - La funzione di accesso al mezzo delle stazioni mobili e fisse (AP) è di tipo distribuita e fondata sull'algoritmo CSMA/CA.
- **Point Coordination Function (PCF)** - In questo caso la funzione di accesso opera in modo del tutto compatibile con lo svolgimento del CSMA/CA, tramite l'uso di un meccanismo di priorità d'accesso. Il suo impiego consente al protocollo di supportare **servizi time bounded** e in generale di tipo **contention-free**.

La banda trasmissiva che viene impiegata - 2.4 GHz ISM band - può essere sia **single-channel** che **multi-channel**. Nel primo caso non è possibile l'impiego della PCF qualora vi sono BSS che si sovrappongono; nell'altro l'uso della PCF è consentito solo se è garantito un adeguato isolamento fra i canali. L'utilizzo della DCF è valido in entrambe le situazioni.

La PCF può essere usata per implementare servizi che hanno requisiti temporali stringenti, come le trasmissioni audio o video. Questa funzione fa uso dell'elevata priorità d'accesso dell'Access Point. Utilizzando questa l'AP emette, secondo un **meccanismo di polling**, delle richieste alle stazioni per la trasmissione dati, quindi controlla l'accesso al mezzo. Allo scopo di consentire alle stazioni regolari di accedere al mezzo trasmissivo è prevista la norma in base alla quale l'AP deve lasciare abbastanza tempo per il Distributed Access all'interno della PCF.

Bisogna ribadire comunque che la PCF, svolta tramite l'AP, può essere realizzata solo in certi BSS. Infatti è necessario che non ci sia sovrapposizione tra le celle che operano sullo stesso canale radio; questa sovrapposizione è, invece, ininfluente se si opera con la funzione di accesso distribuita (DCF).

2. - La tecnologia Spread Spectrum

2.1 - Generalità

Lo sviluppo delle WLAN, compreso lo standard 802.11, è essenzialmente basato sulle **tecnologie radio Spread-Spectrum** (**SS**). L'idea alla base di questa tecnologia è quella di utilizzare una banda più larga del necessario per fronteggiare ambienti ostili. In effetti, la teoria dell'informazione insegna che un modo per far lavorare un sistema con un rapporto segnale/rumore basso è quello di usare una banda larga.

L'allargamento di banda può essere ottenuto in due modi, che rappresentano le due versioni della tecnologia spread-spectrum. Il primo è quello di moltiplicare per una sequenza ad alto rate (**direct-sequence**), il secondo è quello di usare un certo numero di portanti radio “saltando” da una all'altra (**frequency-hopping**).

I vantaggi delle tecnologie spread-spectrum sono legati alla resistenza all'interferenza, alla possibilità di coesistere con altri sistemi e la resistenza ai cammini multipli. È chiaro che si richiede una banda più larga; inoltre, viene introdotta una maggiore complessità, per esempio legata al sincronismo.

L’utilizzo di una banda maggiore - nel senso di **banda spettrale** in Hz - rispetto ai segnali a banda stretta, per produrre un segnale più robusto e facile da rivelare, consente di ottenere un guadagno nel **rapporto Segnale/Rumore** (**S/N**).

Nel sistema il segnale viene diffuso (spread) su una banda molto più ampia di quella richiesta per trasmettere il segnale originale. Si sfrutta il concetto che, in un canale radio con rumore a banda stretta, se si incrementa la larghezza di banda del segnale trasmesso si incrementa la probabilità di riceverlo in modo corretto. L’incremento così ottenuto si definisce "**guadagno di prestazioni**" (**GP**) e descrive la fedeltà acquisita dal segnale al prezzo di una banda più ampia.

Graficamente, se la potenza del segnale viene rappresentata come l’area sotto la curva della banda spettrale, allora il segnale con equivalente potenza totale può avere una grande potenza di segnale concentrata in una piccola banda o una piccola potenza di segnale sparsa su una banda larga.

La distanza su cui le onde radio possono comunicare dipende dalla tecnica e dalla propagazione, specialmente in ambienti chiusi. L’interazione con i tipici oggetti presenti negli edifici, come muri, metalli e anche persone, può avere effetto sulla propagazione dell’energia del sistema.

La maggior parte dei sistemi WLAN utilizzano onde radio che penetrano muri e superfici interne. La distanza (raggio di copertura) per sistemi WLAN tipicamente varia tra 50-300 m. Variando la disposizione delle **Micro-Celle** si agisce sulla copertura e la mobilità via "**roaming**".

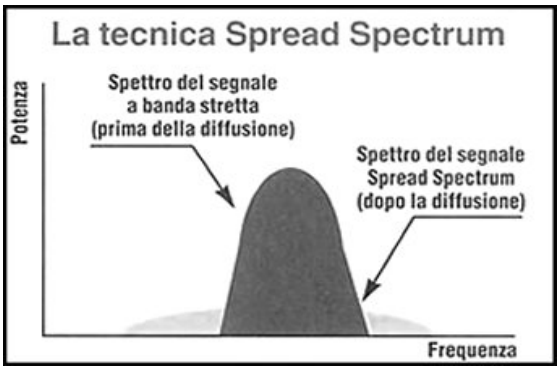

Figura 3 - Rappresentazione grafica dell'effetto della diffusione su potenza e banda spettrale del segnale

Come per le LAN cablate, il throughput dipende dalla predisposizione della **velocità di trasferimento dati** del prodotto. I fattori che ne determinano il valore reale sono la **congestione delle frequenze** (numero di utenti) e **fattori di propagazione** come distanza, interferenze da riflessione, tecnologia, latenze e colli di bottiglia sulle parti cablate. Gli utenti delle LAN tradizionali notano in particolare una differenza nei tempi di latenza. Le WLAN forniscono un trasferimento dati sufficiente alle applicazioni più comuni quali e-mail, accesso a periferiche condivise, data-base e applicazioni.

2.2 - Direct Sequence Spread Spectrum - Il metodo a sequenza diretta

Nel caso del direct sequence l'espansione dello spettro è ottenuta moltiplicando (o per meglio dire "correlando") la sequenza di informazione in banda base con una **sequenza PN**, detta propriamente di espansione, avente frequenza di simbolo molto maggiore (necessariamente almeno 10 volte) rispetto alla stessa sequenza di informazione.

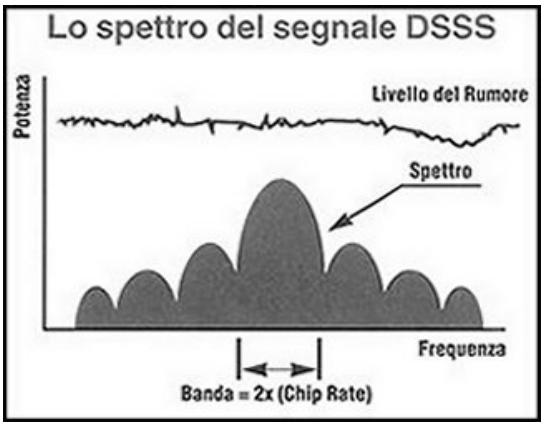

Figura 4 - Rappresentazione grafica di un segnale Direct Sequenze Spread Spectrum (DSSS) in termini di potenza e banda spettrale. Si nota che il rumore ha un livello superiore a quello del segnale

Il meccanismo produce l'effetto di distribuire lo spettro del segnale su una banda tanto più ampia quanto più lunga è la sequenza PN utilizzata (tecnicamente il trasmettitore si trova a dovere trasmettere, a parità di potenza, una maggiore "quantità di informazione"; questo incremento viene pagato con un maggiore impiego della risorsa radio).

In fase di ricezione, in cui il segnale viene moltiplicato per la stessa sequenza PN che ha prodotto l'espansione, il segnale utile verrà compresso nella sua banda originale.

La modalità di trasmissione e ricezione di questa tecnica è il motivo per cui si produce una drastica riduzione dello spettro di potenza dell'interferenza; tale riduzione avviene per effetto di una decisa resistenza al disturbo che lo stesso sistema produce per "sua natura"; per questo motivo i sistemi DS vengono definiti come i sistemi più robusti nei confronti delle interferenze.

La banda (larga) ottenuta con il **codice PN** permette una potenza di trasmissione del segnale sotto la soglia di rumore senza perdita di informazione. Ad un generico ricevitore, DSSS appare come rumore a larga banda di bassa potenza e viene ignorato dalla maggior parte dei ricevitori a banda stretta.

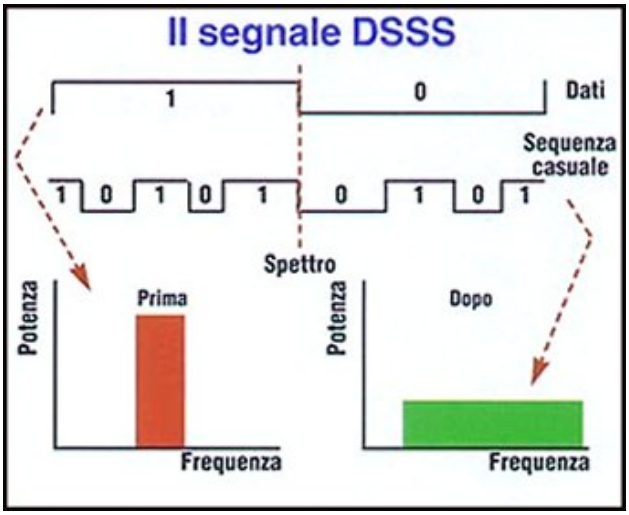

Figura 5 - Rappresentazione dell'effetto della codifica dei dati sulla banda e sulla potenza del segnale trasmesso nel caso del Direct Sequence Spread Spectrum (DSSS)

L'**operazione di despreading** nei sistemi che si servono della tecnica del direct-sequence riporta la densità spettrale del segnale al livello iniziale utilizzando la stessa sequenza usata per espandere. La cosa importante è che se si utilizza una certa sequenza per ricevere un segnale che è stato spedito con una sequenza diversa il despreading non avviene. Questo significa che, quando due utenti usano la stessa banda allargata contemporaneamente, con il despreading si riesce a isolare il segnale che interessa ricevere, lasciando invariato quello delle interferenze.

2.3 – Frequency Hopping Spread Spectrum - Il metodo a salto di frequenza

In questo caso l'espansione dello spettro è ottenuta facendo propriamente "saltare" il segnale, ovvero la porzione di banda che lo stesso occupa in banda base, su un certo numero di frequenze portanti, scelte in base ad una logica regolata da una sequenza PN (nota, come nel caso DS, solo al trasmettitore ed al ricevitore interessati alla comunicazione in atto).

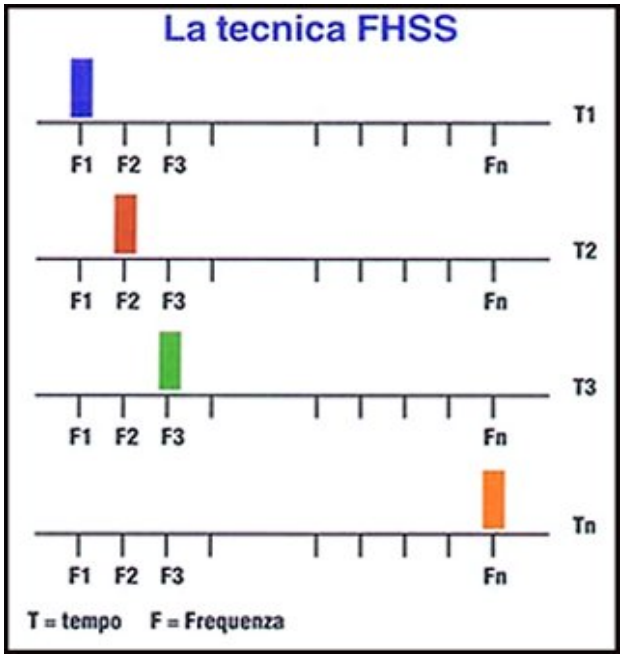

Figura 6 - Diagramma temporale che rappresenta la sequenza delle frequenze generate (F1, F2,...Fn) negli istanti T1, T2,...Tn quando si utilizza la tecnica FHSS

Si può dire che il segnale modula, nel corso del tempo di salto, una portante sempre diversa. Appare quindi evidente che un sistema frequence hopping di fatto non altera in alcun modo la distribuzione spettrale del segnale originale, contrariamente a quanto avviene nel caso DS, pertanto trasmettitore e ricevitore avranno sempre a che fare con segnali che possiamo a tutti gli effetti definire a banda stretta.

Per evitare le possibili interferenze il salto di frequenza (**Frequency Hop**) avviene su una differenza di frequenze. Fondamentalmente, la stringa di dati in ingresso viene spostata in frequenza, su una banda più ampia, di un valore determinato dalla sequenza PN (o **codice di diffusione PN**).

Il trasmettitore FHSS è pertanto un sintetizzatore di frequenza controllato da un **generatore di pseudo-rumore** (PN). La frequenza istantanea trasmessa salta da un valore all'altro pilotata dall'ingresso pseudo-casuale del codice PN. Variando istantaneamente le frequenze, si ottiene uno spettro che è effettivamente diffuso su una gamma di frequenze. In questo sistema, il numero di frequenze discrete determina la banda del sistema. Quindi il guadagno dipende, in modo proporzionale, dal numero delle frequenze scelte per una certa velocità di trasmissione.

L'effetto dei continui salti del segnale da una portante all'altra, caratterizzante il meccanismo di funzionamento della tecnica FH, determina un maggiore impiego di banda, rispetto all'impiego "strettamente necessario" che caratterizzerebbe un sistema a banda stretta.

Un fattore che caratterizza il sistema FHSS è la velocità alla quale avvengono i salti (hop/sec). Il tempo minimo richiesto per cambiare la frequenza dipende dalla velocità dell'informazione, dalla quantità di ridondanza utilizzata e dalla distanza dalla prima sorgente di interferenza.

La sequenza di hopping è definita canale.

Ad un ricevitore generico, FHSS appare come un breve impulso di rumore.

Il sistema FH determina la riduzione dell'effetto delle interferenze attraverso una forma di evasione; in altri termini si ha che in questo caso il sistema sfugge continuamente al disturbo, ma lo subisce completamente nei periodi in cui il segnale modulante va ad allocarsi attorno ad una frequenza portante affetta da un qualsiasi tipo di disturbo.

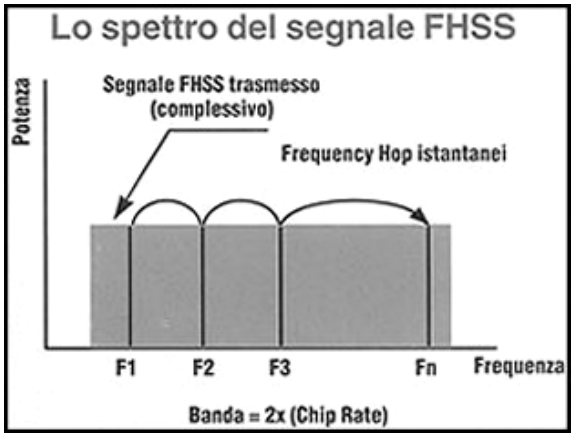

Figura 7 - Rappresentazione grafica dello spettro complessivo di un segnale FHSS a causa della sequenza di frequenze generate (per es. F1, F2... Fn)

Questa tecnica di evasione sarà tanto migliore quanto maggiore è la frequenza di salto. A tale proposito occorre ricordare che si distinguono **sistemi FH lenti** (**SFH**) e **FH veloci** (**FFH**), proprio per discriminare la velocità con cui vengono compiuti i salti in frequenza; allo stato attuale i sistemi FFH, decisamente superiori, non hanno tuttavia trovato una larga diffusione a causa della elevata complessità che li caratterizza. Tale complessità è da imputare alla necessità del ricevitore di espletare tutte le sue funzioni (demodulazione, decodifica, amplificazione ecc.), mantenendosi sempre e comunque sincronizzato con i salti del segnale che deve recuperare; questo problema, già rilevante per i sistemi SFH, diventa quasi ingestibile nel caso FFH.

2.4 - Osservazioni

Per come viene realizzato il processo di espansione e recupero dell'informazione (compressione del segnale nella banda originale) possiamo dire che i sistemi Direct Sequence, rispetto ai sistemi Frequency Hopping, garantiscono sicuramente una maggiore resistenza ai disturbi ed alle interferenze. Quindi, a prescindere da qualsiasi tipo di considerazione economico-commerciale, i sistemi a spettro espanso Direct Sequence si presentano come la soluzione migliore, rispetto ai sistemi Frequency Hopping, in quanto fanno meglio ciò per cui sono stati introdotti.

In secondo luogo è importante ricordare che quando si parla di "minore complessità" dei sistemi Frequency Hopping, si fa spesso riferimento alla maggiore diffusione della componentistica richiesta per la loro realizzazione (essi trattano effettivamente segnali a banda stretta); trascurando che, da un punto di vista strettamente fisico, il processo FH comporta notevoli problematiche relative alla gestione e recupero dell'informazione. Tali problematiche incidono significativamente sulle prestazioni dello stesso sistema, che infatti si presenta sicuramente più lento (si pensi ai tempi di salto da una frequenza all'altra) e difficile da gestire (si pensi alle difficoltà di Roaming).

Viceversa i sistemi Direct Sequence rappresentano sicuramente qualcosa di più sofisticato (e quindi di più costoso), ma garantiscono una maggiore efficienza e gestibilità.

Naturalmente un confronto dettagliato non può non tenere conto di una serie di fattori ulteriori che, in base alle diverse esigenze, potrebbero in qualche modo condizionare, sia in un senso che nell'altro, le conclusioni di carattere tecnico riportate.

3 - CSMA/CA

3.1 - Metodo di accesso base

Il meccanismo di accesso base, **Distributed Coordination Function** (**DCF**), è basato sul meccanismo di accesso multiplo con rilevamento della portate e prevenzione delle collisioni (*Carrier Sense Multiple Access with Collision Avoidence* o in forma più compatta **CSMA/CA**).

I protocolli CSMA sono ben noti nell'industria e il più popolare è sicuramente l'Ethernet che però è basato su un meccanismo di rilevamento delle situazioni di collisione sul canale di comunicazione (**CSMA/CD**, *Collision Detection*).

Un protocollo CSMA lavora nel modo seguente: quando una stazione vuole trasmettere ascolta il canale di trasmissione; se il canale è occupato la stazione rinvia la trasmissione ad un momento successivo (una delle altre stazioni connesse sul medesimo mezzo sta trasmettendo); se invece si rileva che il mezzo è libero, alla stazione è consentito trasmettere.

Questi tipi di protocolli sono molto efficienti se il mezzo di trasmissione non è pesantemente caricato in quanto le stazioni possono trasmettere con un ritardo minimo. Vi è però la possibilità che più stazioni rilevando contemporaneamente che il mezzo trasmissivo è libero comincino a trasmettere simultaneamente. In questo caso, ovviamente, si verifica una situazione di collisione sul mezzo radio. Questa situazione di collisione deve essere rilevata in modo che i pacchetti possano essere ritrasmessi direttamente dal livello di MAC senza interessare i livelli superiori dello stack protocollare, cosa questa che produrrebbe significativi ritardi a livello di trasmissione dei singoli pacchetti.

Nel caso dell'Ethernet questa situazione di collisione è rilevata dalla stazione trasmittente la quale entra in una fase di ritrasmissione basata su algoritmo di posticipo della trasmissione denominato **Binary Exponential Backoff Algorithm**, il quale fissa arbitrariamente un tempo di ritrasmissione al termine del quale viene nuovamente testato il mezzo trasmissivo.In caso di nuove collisioni, il tempo di ritrasmissione viene aumentato con logica esponenziale.

Mentre questo meccanismo di rilevamento della collisione è un'ottima idea nel caso di wired LAN, è assolutamente esclusa la sua adozione nel caso in cui il mezzo trasmissivo sia il canale radio per due ragioni principali:

- L'implementazione di un meccanismo di rilevamento della collisione richiederebbe l'immediata implementazione di capacità di trasmissione e ricezione **Full Duplex**. Questo approccio porterebbe ad un significativo incremento del prezzo degli apparati. Inoltre, la vicinanza del trasmettitore e del ricevitore in una stazione, maschera la presenza di segnali provenienti da altre stazioni più lontane.

- In un ambiente wireless non è possibile assumere che una stazione sia in grado di sentire l'attività di tutte le altre (questa ipotesi è alla base dello schema di rilevamento della collisione). In quest'ottica se una stazione che vuole trasmettere rileva la non occupazione del mezzo, non necessariamente significa che il mezzo sia libero attorno all'area di ricezione.

Allo scopo di superare questi problemi, l'802.11 utilizza un **meccanismo di collision avoidance** unito ad uno **schema di positive acknowledge**.

3.2 - Positive acknowledge

Il funzionamento dello schema di positive acknowledge è il seguente:

- Una stazione che vuole trasmettere testa il mezzo trasmissivo. Se il mezzo è occupato la trasmissione verrà deferita. Se il mezzo è libero per un certo tempo, denominato **Distributed Inter Frame Space** (**DIFS**) nello standard, la stazione effettua la trasmissione.
- La stazione ricevente controlla il campo **CRC** (*Cyclic Redundancy Check*) del pacchetto ricevuto e invia un **pacchetto di acknowledgement** (**ACK**). La ricezione di questo pacchetto indica alla stazione trasmittente che non si è verificata nessuna situazione di collisione. Se la stazione che ha iniziato la trasmissione non riceve l'acknowledgement allora ritrasmetterà il pacchetto fintanto che non riceve un pacchetto di acknowledge. E' comunque fissato un numero massimo di ritrasmissioni oltre il quale il pacchetto viene buttato via.

Quando una stazione vuole trasmettere usa, quindi, un **meccanismo di rilievo della portante** (Carrier Sense) per determinare se il livello di energia del segnale nella banda trasmissiva è sopra una certa soglia.

3.3 - Virtual Carrier Sense - RTS/CTS Exchange

Allo scopo di ridurre la probabilità che si verifichi una situazione di collisione tra due stazioni a causa della impossibilità di ciascuna stazione di sentire tutte le altre, lo standard definisce un meccanismo denominato **Virtual Carrier Sense**.

Una stazione che vuole trasmettere innanzitutto procede alla trasmissione di un breve pacchetto di controllo denominato **RTS** (*Request To Send*) che contiene l'identificativo della sorgente e della destinazione oltre alla durata della successiva trasmissione relativa al pacchetto RTS e al rispettivo ACK. La stazione di destinazione risponde (se il mezzo è libero) con un pacchetto di controllo denominato **CTS** (*Clear To Send*) con la stessa informazione relativa alla durata di trasmissione.

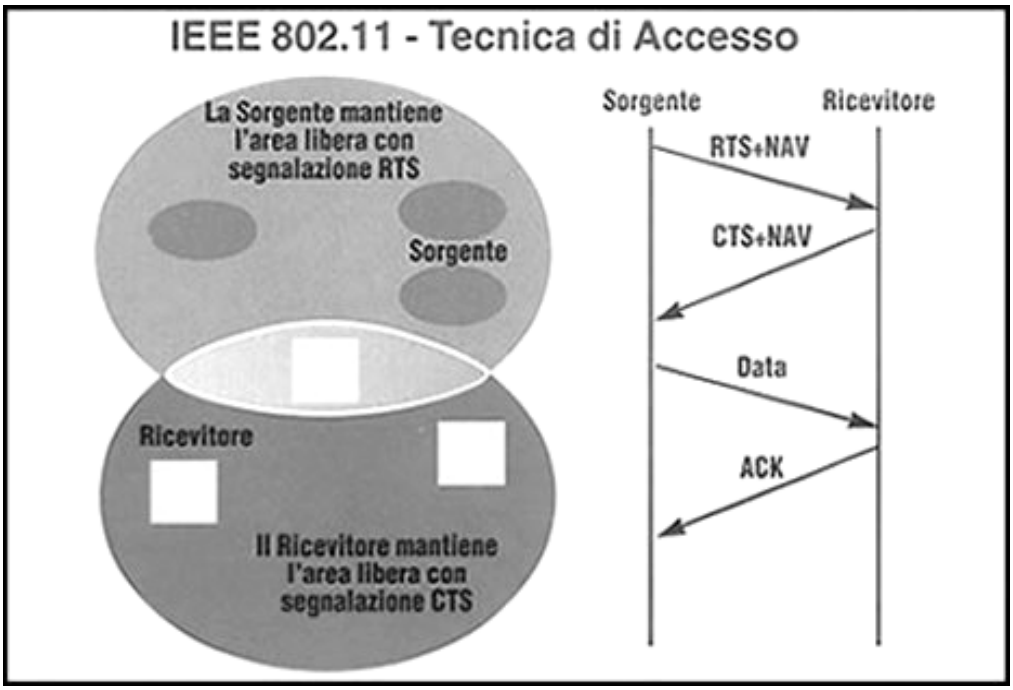

Figura 8 - Tecnica di Accesso

Tutte le stazioni, ricevendo sia un RTS sia un CTS, settano l'indicatore Virtual Carrier Sense (chiamato **NAV** che sta per ***Network Allocation Vector***), per un certo tempo ed utilizzano questa informazione insieme con il **Physical Carrier Sense** al momento in cui vanno a effettuare la rilevazione di occupazione del mezzo.

3.4 - RTS/CTS Exchange

Questo meccanismo riduce la probabilità di collisione su un'area di ricezione che è nascosta all'interno dell'intervallo di tempo necessario alla trasmissione dell'RTS poiché la stazione sente il CTS e definisce il mezzo come occupato fino alla fine della trasmissione. L'informazione relativa al tempo di trasmissione protegge inoltre l'area del trasmettitore dalle collisioni durante l'ACK da parte di quelle stazioni che sono fuori dall'area di visibilità della stazione che deve fornire l'acknowledge.

Bisogna inoltre osservare che a causa delle ridotte dimensioni dei pacchetti RTS e CTS, il meccanismo riduce anche l'overhead dovuto alla collisione, poiché non è necessaria la ritrasmissione dell'intero pacchetto dati. Questo è vero se il pacchetto dati è significativamente maggiore rispetto all'RTS.

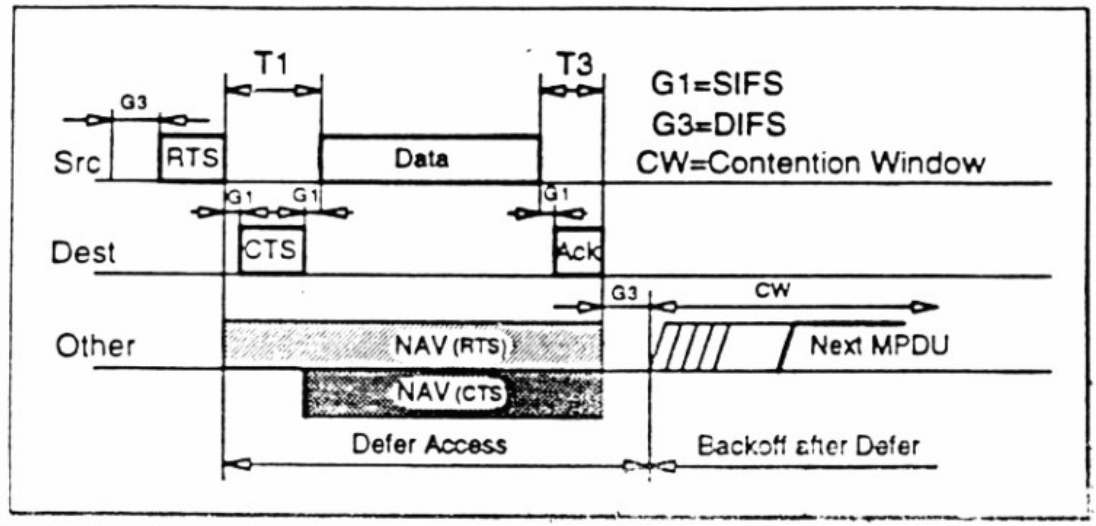

Figura 9 – MPDU: RTS/CTS/DATA/ACK

Per questo motivo lo standard prevede una variante in cui se il pacchetto è breve può essere trasmesso senza la transazione RTS/CTS.

Tale comportamento è controllato in ogni stazione da un parametro detto **RTS Threshold**.

Attraverso lo scambio di trame RTS/CTS la stazione trasmittente e quella ricevente dichiarano agli altri nodi della rete il loro intento di occupare il mezzo per una certa durata, e li invitano pertanto ad astenersi dal trasmettere durante questo periodo. In tal modo si possono prevenire eventuali disfunzioni del protocollo nel caso in cui ci fossero delle **stazioni hidden**, ovvero che non ricadono nella copertura radio della stazione trasmittente, o per temporanei "**fading**" del segnale radio; l'**RTS/CTS Exchange** funge, in questo caso, da meccanismo di protezione dal rischio di collisione.

La Figura 9 descrive i messaggi scambiati tra **Sorgente** e **Destinazione**, durante un **trasferimento dati directed** (ovvero *non broadcast*), con l'impiego dell'opzione RTS/CTS.

Le stazioni non indirizzate rilevano l'RTS o il CTS fissando o aggiornando il NAV, che può ritenersi, quindi, indicativo, in modo anticipato, dello stato del mezzo per l'immediato futuro.

E' opportuno osservare che, nel caso di *directed frame*, lo scambio di trame RTS/CTS accresce la **robustness** del protocollo nel caso di stazioni hidden.

3.5 - Fragmentation e Reassembly

I protocolli per reti LAN utilizzano pacchetti aventi dimensioni di diverse centinaia di bytes. Ci sono però molte ragioni che spingono all'utilizzo di pacchetti di dimensioni minori in un contesto wireless LAN:

- A causa dell'elevato **Bit Error Rate** di un collegamento radio, la probabilità che un pacchetto sia corrotto durante la fase di trasmissione aumenta all'aumentare della dimensione del pacchetto.

- Nel caso in cui un pacchetto ricevuto contenga errori di qualsiasi natura e debba essere ritrasmesso, l'**overhead** introdotto dal processo di trasmissione decresce con la dimensione del pacchetto.
- In un sistema Frequency Hopping non è garantita la continuità del mezzo trasmissivo a causa dei salti di frequenza. Riducendo la dimensione del pacchetto diminuisce la probabilità che la trasmissione sia posticipata dopo il tempo di pausa (**dwell time**).

E' impensabile, comunque, introdurre un nuovo protocollo che non possa trattare pacchetti di una certa dimensione; così l'organismo di standardizzazione ha deciso di aggiungere un semplice **meccanismo di frammentazione e riassemblaggio** al livello di MAC. Il meccanismo è costituito da un semplice **algoritmo Send-and-Wait** che non consente ad una stazione di trasmettere un nuovo frammento finché non sia verificata una delle seguenti situazioni:

- ricezione di un ACK per il frammento precedentemente trasmesso
- decide che il frammento è stato ritrasmesso troppe volte ed elimina tutta la frame.

3.6 - Inter Frame Spaces

Lo standard definisce quattro tipi di spazi tra le frame (**Inter Frame Spaces**), che sono utilizzate per fornire differenti priorità:

- **SIFS** - ***Short Inter Frame Space***. E' utilizzato per separare trasmissioni che appartengono ad un singolo dialogo (**Fragment-Ack**) ed è il più piccolo spazio tra le frame possibile. C'è sempre al più una stazione che trasmette ad un dato istante di tempo, prendendosi dunque la priorità sulle altre. Questo valore è fissato per il livello fisico ed è calcolato in modo tale che la stazione trasmittente possa essere in grado di commutare il suo modo di funzionamento alla ricezione e decodificare il pacchetto entrante.
- **PIFS** - ***Point Coordination IFS***. E' usato dall'Access Point (o dal Point Coordinator) per guadagnare l'accesso al mezzo prima di ogni altra stazione. Questo valore è pari al SIFS più uno *slot time*.
- **EIFS** - ***Extended IFS***. E' il più lungo IFS ed è usato da una stazione che ha ricevuto un pacchetto di cui non è stata in grado di comprendere il contenuto. Questo è necessario per proteggere la stazione (la quale non comprende l'informazione di durata necessaria per il virtual carrier sense) da collisioni con i futuri pacchetti appartenenti al dialogo corrente.
- **DIFS** - ***Distributed IFS***. E' l'Inter Frame Space utilizzato per una stazione che vuole iniziare una nuova trasmissione. E' calcolato come PIFS più uno slot time.

3.7 - Exponential Backoff Algorithm

Quello del backoff è un metodo ben noto per risolvere il contenzioso tra differenti stazioni che vogliono accedere contemporaneamente al mezzo trasmissivo. Il metodo richiede che ciascuna stazione scelga un numero casuale (n) compreso tra 0 e un dato numero e aspetti per questo numero di slot prima di accedere al mezzo, effettuando

comunque il controllo sulla portante per vedere se qualche altra stazione ha avuto accesso al mezzo in precedenza.

Lo **slot time** è definito in modo tale che la stazione sia sempre capace di determinare se un'altra stazione ha avuto accesso al mezzo all'inizio del precedente slot. Questo consente di ridurre notevolmente la probabilità di collisione.

Il Backoff è detto esponenziale poichè ogni volta che la stazione sceglie uno slot per la trasmissione e si verifica una collisione, verrà aumentato in maniera esponenziale il massimo valore per la selezione casuale dello slot di trasmissione.

L'802.11 definisce un algoritmo di backoff esponenziale che deve essere eseguito nei seguenti casi:

- quando la stazione testa il mezzo prima della prima trasmissione del pacchetto e il mezzo è occupato
- dopo ciascuna ritrasmissione e
- dopo una trasmissione che ha avuto successo.

Il solo caso in cui il meccanismo non è utilizzato è quando la stazione decide di trasmettere un nuovo pacchetto e il mezzo viene rilevato libero per un tempo maggiore di DIFS (Distributed Inter Frame Space).

In Figura 10 una schematizzazione del meccanismo di accesso al mezzo.

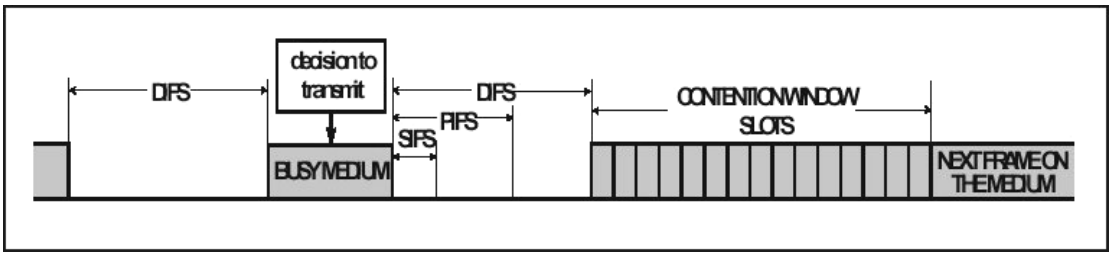

Figura 10 - Meccanismo di Accesso al mezzo radio

Il vantaggio di questo approccio consiste nel fatto che le stazioni che hanno perduto la precedente contesa, dopo il successivo DIFS, riprendono lo scorrimento del **backoff timer** da dove era rimasto. In questo modo è probabile (non certo) che esse abbiano un ritardo d'accesso inferiore rispetto alle stazioni che entrano in backoff per la prima volta.

3.8 - Procedure di recupero

E' possibile distinguere diversi eventi che comportano delle procedure di recupero.

Quando dopo la trasmissione di un RTS non viene ricevuto nessun CTS, entro un predeterminato **CTS_TimeOut**, allora una nuova Request To Send viene generata seguendo opportunamente il **meccanismo di backoff**.

Lo stesso criterio (**Access Backoff**) viene seguito per la mancata ricezione di Ack entro una fissata **Ack_Window** dopo che sia stata trasmessa una **trama unicast**.

I tentativi di recupero continuano fino a quando un **RE_TRANSMIT_COUNTER** non raggiunge un **RE_TRANSMIT_LIMIT**.

Le cause di una mancata ricezione della trama CTS possono essere diverse. Può verificarsi una collisione con un'altra trama RTS o DATA, un fading del segnale trasmesso, oppure può accadere che in quel frangente la remote station abbia attiva la Carrier Sense o il NAV, e quindi deve rimandare la trasmissione.

Quando, invece, nessun Ack viene rilevato in tempo utile, allora questa situazione può essere causata da errore nei dati (essendo previsto solo un meccanismo di acknowledgement positivo) oppure per eventuali collisioni. La procedura di recupero, a seguito di un mancato Ack, comporta la ritrasmissione dell'intero **MPDU** (*RTS/CTS; DATA; Ack*).

Risulta allora opportuno prevedere differenti limiti di ritrasmissione in base ai casi.

4. - Metodi di accesso ad un BSS

4.1 - Cenni sullo Scanning

Le stazioni che desiderano porsi in rete con un Basic Service Set (BSS) devono trovare (**Scanning**) le altre stazioni appartenenti a quel BSS ponendosi in ascolto nel canale appropriato e sincronizzando i propri timers con il resto del BSS.

Se la stazione ha individuato un esistente BSS e vuole accedervi ha bisogno di acquisire la sincronizzazione relativa alle informazioni dall'Access Point.

La stazione può acquisire questa informazione in uno dei seguenti modi:

- **PASSIVE SCANNING** - La stazione aspetta di ricevere una **Beacon Frame** dall'Access Point. La Beacon è una frame periodicamente inviata dall'Access Point contenente l'informazione relativa al sincronismo di trasmissione dei dati.
- **ACTIVE SCANNING** - La stazione tenta di localizzare un Access Point attraverso la trasmissione di una **Probe Request Frame** e attende che un Access Point risponda con frame **Probe Response**.

Lo **Scanning Passivo** è praticabile solo quando il numero di canali da indagare è ristretto oppure è breve il **Beacon Interval** relativo a ciascun canale. Per il resto entrambi i metodi sono validi e la scelta tra uno o l'altro viene effettuata in funzione di esigenze di consumo o di incremento delle prestazioni.

4.2 - Meccanismi di Autenticazione e Associazione

Il **Processo di Autenticazione** viene eseguito non appena una stazione ha localizzato un Access Point e ha deciso di unirsi alla corrispondente Base Service Set (BSS).

In questa fase la stazione e l'Access Point effettuano uno scambio di informazioni in modo da verificare la relativa conoscenza di una data Password.

Quando le stazioni si sono autenticate inizia il **Processo di Associazione**.

In questa seconda fase le informazioni scambiate hanno lo scopo di definire le caratteristiche della stazione e le capacità offerte dalla BSS. Tutto ciò consente al DSS, ovvero all'insieme degli AP, di ottenere informazioni circa l'attuale posizione della

stazione espressa come appartenenza ad una particolare BSS ovvero come associazione ad un determinato Access Point.

Si osserva che una stazione è in grado di trasmettere o ricevere informazioni solo dopo che il processo di associazione si è positivamente concluso.

4.3 - Roaming

Il **Roaming** è il processo che consente lo spostamento di una stazione da una cella (o BSS) ad un'altra senza perdita di connessione. Questa funzione è simile a quella che viene realizzata nei sistemi di telefonia cellulare, con due differenze fondamentali:

- Su un sistema LAN, basato su un sistema di trasmissione a pacchetti, la transizione da una cella ad un'altra deve essere realizzata tra la trasmissione di un pacchetto e quella del successivo; al contrario di quanto accade in un sistema per telefonia in cui il processo deve avvenire durante lo svolgimento di una comunicazione. In una LAN, quindi, il processo risulta sicuramente di più semplice implementazione.
- Su un sistema per il trasferimento della voce una temporanea sconnessione può non avere un effetto significativo, mentre in un ambiente basato sul pacchetto questa momentanea interruzione della connessione porta ad una significativa riduzione delle prestazioni, in quanto è necessario operare delle ritrasmissioni gestite, però, dai livelli superiori dello stack protocollare.

Lo standard 802.11 non definisce come il roaming debba essere realizzato, ma definisce un modo di funzionamento base. La stazione in movimento, attraverso il meccanismo di Passive Scanning o quello di Active Scanning, rileva quali Access Point sono disponibili per la connessione; in funzione del livello del segnale ricevuto dagli AP decide a quale è più conveniente associarsi e attraverso un meccanismo di re-associazione, definito dallo standard, può eliminare l'associazione dal vecchio AP e associarsi a quello nuovo. Il processo di re-associazione consta di uno scambio di informazioni tra i due AP interessati allo scambio di utente, attraverso il **distribution system**, quindi senza appesantire la comunicazione attraverso il canale radio.

4.4 - Mantenimento della sincronizzazione

I nodi inclusi in un Basic Service Set hanno la necessità di conservare una certa sincronizzazione che è necessaria per mantenere la sincronizzazione nei salti di frequenza e per la realizzazione di altre funzioni come il risparmio energetico.

In una infrastruttura basata su BSS si provvede pertanto all'aggiornamento del clock delle singole stazioni in accordo con un dato meccanismo.

L'Access Point trasmette periodicamente una Beacon Frame. Questa frame contiene il valore del clock interno dell'Access Point al momento della trasmissione. Si osservi che questo rappresenta il momento in cui la trasmissione viene realizzata e non il momento in cui la frame viene inserita nella coda di trasmissione. Poiché anche questa frame viene trasmessa utilizzando la regola CSMA, la trasmissione può essere significativamente ritardata. La stazione ricevente controlla il valore del proprio clock al

momento della ricezione del segnale e lo corregge mantenendo la sincronizzazione con l'orologio dell'Access Point.

Questo meccanismo è di fondamentale importanza perché previene lo slittamento del clock che si può verificare dopo alcune ore di funzionamento del sistema.

Si osserva che il raggiungimento della sincronizzazione non richiede un protocollo sincrono. Una tale scelta richiederebbe un dominio del tempo partizionato in intervalli regolari e in modo tale che certe trasmissioni si verificassero ad istanti prefissati. Tale viene scartato perché non compatibile con il metodo d'accesso previsto per le reti wireless, il CSMA/CA.

5 - Sicurezza in una Rete IEEE 802.11

5.1 - Wireless e sicurezza

La tecnologia wireless ha radici nella tecnologia militare e quindi i criteri di sicurezza sono stati considerati sin dall'inizio.

Nonostante la tecnologia radio con segnali in banda larga sia estremamente difficile da demodulare per un ricevitore involontario, a livello di traffico della WLAN sono state comunque adottate soluzioni per la sicurezza.

Per quanto riguarda lo standard IEEE 802.11 è stato definito un insieme di funzioni denominate "**security services**" e il meccanismo che è stato implementato dal comitato che ha sviluppato lo standard è denominato **WEP** (***Wired Equivalent Privacy***).

Gli scopi fondamentali di questo meccanismo sono:

- Prevenire l'accesso alle risorse di rete da parte di apparecchiature Wireless LAN simili. Una qualunque stazione che intende comunicare deve dimostrare attraverso un meccanismo di autenticazione la conoscenza della chiave di autenticazione correntemente in uso. Tale meccanismo è simile a quello attuato nelle **wired LAN**, nel senso che colui che vuole entrare nel sistema deve immettere i permessi utilizzando la chiave fisica allo scopo di connettere la propria **workstation** alla LAN.
- Impedire la cattura del traffico wireless LAN da parte di entità esterne. Questa operazione viene realizzata mediante l'**algoritmo WEP**, che è generatore di numeri pseudocasuali inizializzato per mezzo di una chiave segreta. Questo **PRNG** produce in uscita una sequenza chiave di bits pseudo-casuali di lunghezza uguale al più grande pacchetto consentito dal sistema che viene combinata con i pacchetti in uscita o in entrata producendo il pacchetto effettivamente trasferito in aria.

5.2 - WEP - Wired Equivalency Privacy

Il WEP è un semplice algoritmo su **RC4 RSA** che ha le seguenti proprietà:

- **Notevole robustezza** - Un attacco brutale a questo algoritmo è difficoltoso perché ciascuna frame è inviata con un vettore di inizializzazione che riavvia il PRNG per ciascuna frame.

- **Mantenimento della sincronizzazione** - L'algoritmo di re-sincronizzazione è eseguito per ogni messaggio. Questo è necessario per lavorare in un **ambiente connection-less** dove i pacchetti possono andare persi (quello che tipicamente accade in tutte le LAN).

A livello di sistema, il Wired Equivalency Privacy si pone l'obiettivo di una protezione uguale o migliore rispetto alle reti cablate. La chiave di abilitazione - **Current Key** - viene definita per una singola stazione, mentre la funzione per l'accesso alla rete è garantita dall'Access Point.

Se si vuole vedere un limite nel meccanismo lo si trova a livello di protocolli di autenticazione e di distribuzione delle chiavi, il cui sviluppo è lasciato all'implementazione.

A livello dei dati utente esiste una cifratura opzionale "station to station", che si basa sull'algoritmo proprietario **RC4** di **RSADS**. Esso sfrutta una chiave segreta cifrata di lunghezza variabile a 40 bit, abbastanza efficiente per velocità di 1 Mbps. Per allungare la vita delle chiavi viene utilizzato un vettore di inizializzazione (**IV**) da 24 bit. Il controllo di integrità viene ottenuto con le tecniche **CRC32** e **ICV** a 12 bit.

L'algoritmo RC4 è esportabile dagli USA ed è operativo dal 1994.

6 - Frame IEEE 802.11: tipi e struttura

L'unità informativa base scambiata dal protocollo tra differenti entità MAC è una trama (*frame*). Un completo **MAC Protocol Data Unit** (**MPDU**) può consistere di una sequenza di frame tra loro correlate e scambiate tra due **MAC entities**, per es. **RTS/CTS/DATA/Ack** oppure **DATA/Ack**. In questi casi la relazione fra le frame è indicata tramite un campo **MPDU ID** interno all'*header* della trama.

Tre sono in generale i tipi fondamentali di frame:

- **Data Frames** - usati per la trasmissione dei dati;
- **Control Frames** - usati per il controllo dell'accesso al mezzo (es. RTS, CTS e Ack);
- **Management Frames** - trasmessi come le Data Frames per lo scambio di informazioni di controllo, ma non sono passati ai livelli superiori dello stack protocollare (esempio le Beacon Frames).

Ciascun tipo di frame è poi suddiviso in differenti sottotipi, in base alla specifica funzione. In Figura 11 sono mostrati i componenti che compongono le frame definiti dallo standard 802.11.

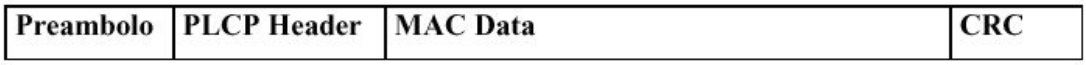

Figura 11 - Formato di un frame

Preambolo

Questo campo è dipendente dal livello fisico e comprende:

- **Synch**: una sequenza di 80 bit di 1 e 0 alternati che è utilizzata dalla circuiteria del livello fisico per selezionare l'appropriata antenna (se è utilizzata la diversità)
- **SFD**: è il delimitatore di inizio frame (*Start Frame Delimiter*) che consiste di una configurazione binaria di 16 bit modello 0000 1100 1011 1101, che è usata per definire la temporizzazione della frame.

PLCP Header

L'Header PLCP è sempre trasmesso a 1Mbit/s e contiene informazioni logiche utilizzate dallo strato fisico per decodificare la frame. Consiste dei seguenti campi:

- **PLCP_PDU Length Word**: rappresenta il numero di bytes contenuti nel pacchetto. Questa informazione è essenziale per lo strato fisico allo scopo di rilevare correttamente la fine del pacchetto.
- **PLCP Signaling Field**: Correntemente contiene solo l'informazione relativa alla velocità di trasmissione codificata in incrementi di 0,5 Mbit/s da un 1 Mbit/s a 4,5 Mbit/s
- **Header Error Check Field**: è un campo di 16 bit che viene utilizzato per la rilevazione d'errore.

MAC Data

La Figura 11 mostra il tipico formato della frame di MAC. I campi indicati in figura non sono presenti in tutti le frame così come verrà descritto successivamente.

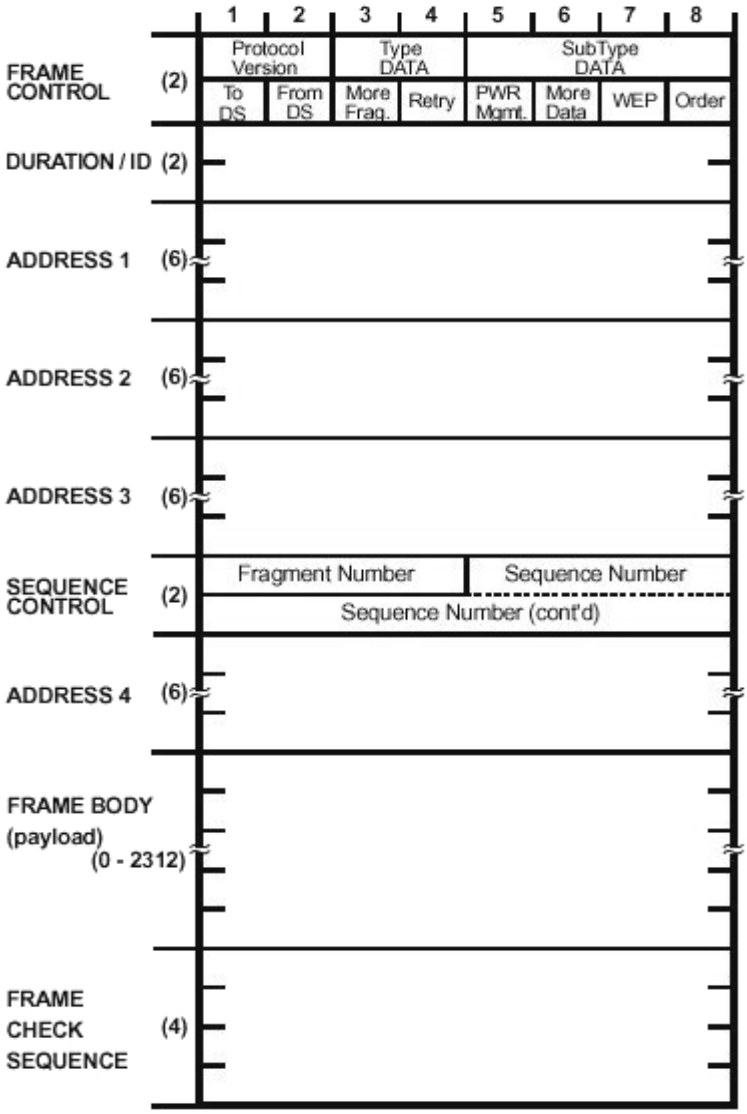

Figura 12 - Formato della Frame di MAC

Campo Frame Control

Il campo Frame Control contiene le seguenti informazioni (Figura 13):

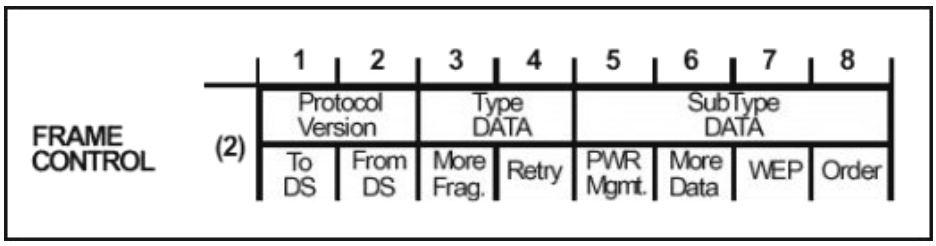

Figura 13 – Struttura del campo di controllo della Frame

- *Protocol Version:* Questo campo consiste di 2 bits che sono invarianti sia per dimensione sia per posizionamento nelle successive versioni dello standard 802.11 e saranno utilizzati per riconoscere le future versioni quando queste saranno disponibili. Nella versione attualmente disponibile dello standard questo valore è fissato a 0.

- *Type e Subtype*: Questi 6 bits definiscono il tipo e il sottotipo della frame.
- *ToDS*: Questo bit è posto al valore 1 quando la frame è indirizzato all'AP allo scopo destinato ad essere trasferito ad una stazione collegata al Distribution System, compresi i casi in cui la stazione di destinazione è nella stessa BSS e l'AP funziona da semplice ripetitore per la frame. In tutti le altre frame questo bit è posto al valore 0.
- *FromDS*: Questo bit è posto al valore 1 quando la frame è ricevuta dal Distribution System.
- *More Fragments*: Questo bit è posto al valore 1 quando più frammenti appartenenti alla stessa frame seguono il frammento corrente.
- *Retry*: Questo bit indica che il frammento corrente è la ritrasmissione di un frammento precedentemente trasmesso. Questo è utilizzato per riconoscere le trasmissioni duplicate delle frame che si possono verificare quando un pacchetto di Acknowledgment va perso.
- *Power Menagement*: Questo bit serve per cambiare lo stato da Power Save a Active e viceversa.
- *More Data*: Questo bit è utilizzato per il Power Menagement ma viene sfruttato anche dall'Access Point per indicare che ci sono molte frame memorizzate e indirizzate a questa stazione. La stazione può decidere di utilizzare questa informazione per continuare il **Polling** o anche per commutare il modo di funzionamento in Active.
- *WEP*: Questo bit indica che il corpo della frame è codificato in accordo con l'algoritmo WEP.
- *Order*: Questo bit indica che la frame è stata inviata con **Stricly-Order service class**. Questa classe di funzionamento è definita per utenti che non possono accettare cambi di ordinamento tra **frames Unicast e frames Multicast** (l'ordinamento delle frames Unicast a uno specifico indirizzo è sempre mantenuto).

Duration/ID

Questo campo ha due significati diversi in base al tipo di frame:

- In messaggi di **Power Save Poll** questo campo rappresenta l'identificativo della stazione
- In tutti le altre frame questo campo rappresenta il valore di durata utilizzato per il calcolo del **NAV**

Address Fields

Una frame può contenere al più 4 indirizzi come definito dai campi ToDS e FromDS definiti nel campo Control:

- Address-1: è sempre l'indirizzo del destinatario. Se ToDS è a 1 questo è l'indirizzo dell'AP, mentre se è a 0 questo rappresenta l'indirizzo del destinatario finale.

- Address-2: è sempre l'indirizzo di colui che effettua la trasmissione. Se FronDS è a 1 questo è l'indirizzo dell'AP mentre se è a 0 è l'indirizzo della stazione.
- Address-3: in molti casi è l'indirizzo mancante. Se una frame ha il campo FromDS al valore 1 Address-3 rappresenta l'indirizzo della vera sorgente della frame. Se ToDS i invece a 1 il valore in questo campo identifica l'indirizzo di destinazione.
- Address-4: è usato in casi particolari dove è presente un Distribution System completamente wireless e la frame è stata trasmessa da un AP ad un altro. In questo caso sia ToDS sia FromDS sono a 1 così sia l'indirizzo di destinazione sia l'indirizzo della vera sorgente della frame sono mancanti.

La seguente tabella riassume l'utilizzo dei vari indirizzi in funzione del valore di ToDS e FromDS.

ToDS	FromDS	Address1	Address2	Address3	Address4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	**1**	**RA**	**TA**	**DA**	**SA**

Tabella 1 – Significato dei campi indirizzo

Sequence Control

Questo campo è utilizzato per rappresentare l'ordine di differenti frammenti che appartengono ad una stessa frame e di controllare la duplicazione dei pacchetti. E' in realtà costituito da due sottocampi, **Fragment Number** e **Sequence Number**, che definiscono la frame e il numero del frammento nella frame.

CRC

Il CRC è un campo di 32 bit contenete un **Cyclic Redundancy Check** (**CRC**) a 32 bit.

6.1 - Formato della Frame più comuni

Formato della Frame RTS

La frame RTS ha una struttura come quella mostrata in Figura 14.

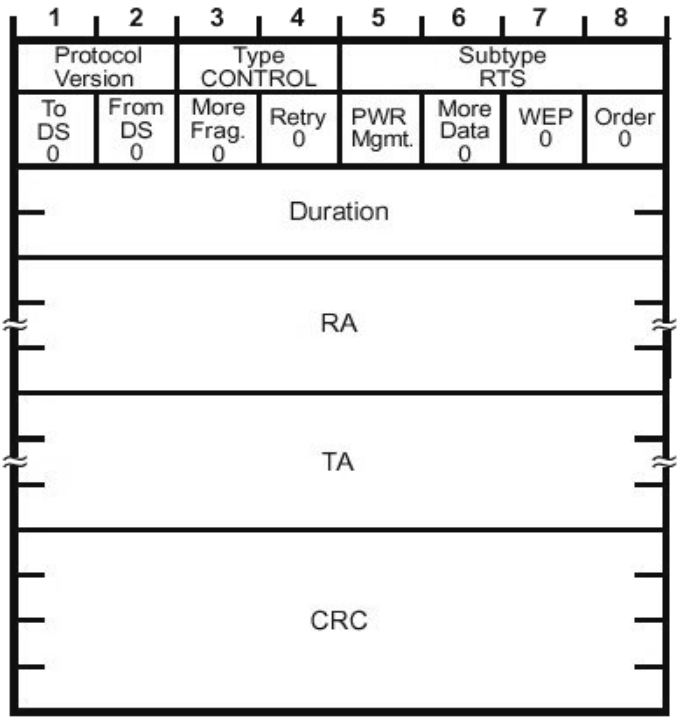

Figura 14 – Formato della Frame RTS

L'**RA** della frame RTS è l'indirizzo della **STA** (*station*) che è designata come immediata destinataria della successiva frame dati o di Management.

Il **TA** è l'indirizzo della STA che ha trasmesso la frame RTS.

Il campo **Duration** contiene il tempo, espresso in microsecondi, richiesto per trasmettere la successiva frame dati o Management, più una CTS, più una frame ACK, più tre intervalli SIFS.

Formato della Frame CTS

La struttura della frame nel caso della Clear To Send è mostrata in Figura 15.

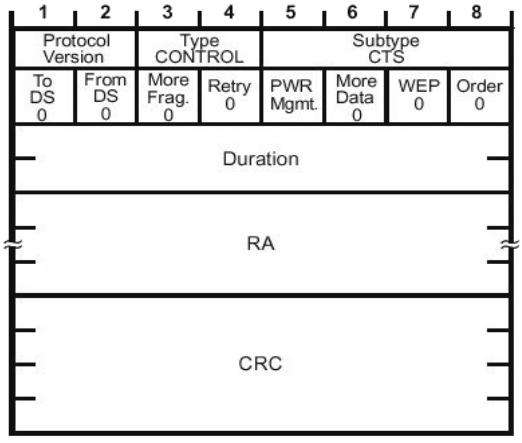

Figura 15 – Formato della Frame CTS

Il campo **Receiver Address** (**RA**) della CTS è copiato dal campo **Transmitter Address** (**TA**) della frame RTS immediatamente precedente del quale il CTS rappresenta la risposta.

Il valore Duration è il valore ottenuto dal campo Duration della frame RTS immediatamente precedente, meno il tempo, espresso in microsecondi, richiesto per trasmettere la frame CTS e il suo intervallo SIFS.

Formato della Frame ACK

La frame ACK ha la struttura mostrata in Figura 16.

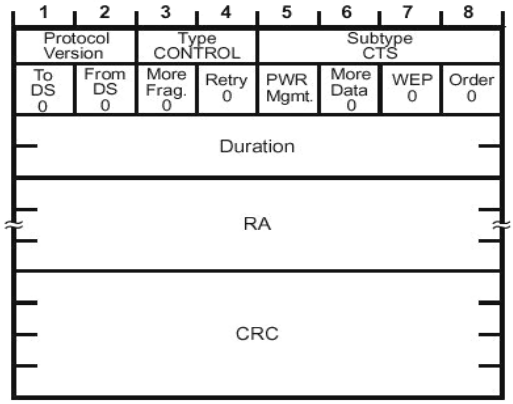

Figura 16 – Formato della Frame ACK

Il campo Receiver Address della frame ACK è copiato dal campo Address-2 della frame immediatamente precedente. Se il bit More Fragment era settato a 0 nella precedente frame, il valore del campo Duration è posto a 0, altrimenti il valore è ottenuto dal campo Duration della precedente frame meno il tempo in microsecondi richiesto per trasmettere la frame ACK e il suo intervallo SIFS.

7 - Power Management

7.1 - Generalità

Una stazione mobile in una rete wireless dovrà sostenere un certo consumo di potenza, sia in trasmissione che in ricezione. Mentre nessuna riduzione di potenza è possibile quando si deve trasmettere, degli adeguati accorgimenti possono essere presi per evitare che i ricevitori delle stazioni siano "**power on**" per tutto il tempo, come sarebbe necessario se essi dovessero essere pronti a recepire una frame che può sopraggiungere in qualunque istante.

I **meccanismi di power saving** sono quindi mirati a fare in modo che i ricevitori delle stazioni mobili siano "**on**" solo quando strettamente necessario.

Innanzitutto occorre che le stazioni informino l'AP di competenza se esse desiderano operare in **power conserving mode**. In questo caso l'AP non trasmette arbitrariamente (cioè in qualunque istante) le trame alle stazioni, ma le "bufferizza" e li trasmetterà solo a tempo debito.

Le stazioni per le quali vi è del traffico immagazzinato sono elencate in una **Traffic Indication Map**, o **TIM**, che è periodicamente generata dall'AP come un elemento interno del Beacon. Una stazione potrà accertarsi che una frame è immagazzinata per essa nell'AP, ascoltando i TIM, e in caso positivo, procedere in modo da assicurarsi che la trama sia correttamente ricevuta.

7.2 - Power Save Mode

I Beacons (con i TIMs) sono periodicamente generati dall'AP, intervallati da un **Beacon Interval**. Le stazioni possono individualmente scegliere quanto frequentemente ascoltare i Beacons (e quindi i TIMs), sulla base di un parametro **Listen Interval**, ovviamente multiplo del Beacon Interval, e dal quale dipende in maniera significativa il target power/performance raggiunto dalla stazione.

Le stazioni possono inoltre scegliere due vie per acquisire le **frame buffered** nell'AP:

- ***POWER SAVE POLLING MODE*** (**PSP**) - Le stazioni operano trasmettendo una breve poll frame all'AP, che risponderà inviando le rispettive trame bufferizzate;

- ***POWER SAVE NON-POLLING MODE*** (**PSNP**) - Le stazioni si pongono in ascolto secondo Listen Interval più lunghi, e quindi solo di alcuni TIMs, chiamati DTIMs, a seguito dei quali l'AP trasferirà le frame buffered senza attendere l'arrivo di un **poll**.