**Data Link Layer Wireless LAN**

**Frequency Hopping Spread Spectrum**

Utilizza 79 canali ad 1 MHz. Il nostro segnale rimbalza da una frequenza all’altra secondo una specifica sequenza pseudocasuale nota a trasmettitore e ricevitore. Grazie alla sequenza pseudocasuale, questa tecnologia è anche abbastanza sicura e assicura solidarietà nel multipath fadding ( il segnale viene riflesso e dopo un tempo torna indietro nella frequenza di trasmissione e cambiando frequenza non avremo sovrapposizioni ). Le velocità però sono limitate, sotto i 10 Mbps.

**Direct Sequence Spread Spectrum**

Utilizza la tecnica del chipping. Ogni bit viene convertito in una serie di bit ridondanti detti chip ed il segnale trasmesso è l’or esclusivo dei bit dati combinati con una sequenza pseudocasuale. Il segnale ottenuto risulta essere un segnale trasportato in un range di frequenza molto più ampio allargando così lo spettro. Per ogni bit di dati si usa una sequenza fissa per codificare il bit con una sequenza di 11 chip.

Riusciamo ad arrivare anche fino a 300 Mbps o addirittura fino ad 1 Gbps.

Nella condivisione del mezzo trasmissivo o canale nelle LAN individuare una collisione è abbastanza semplice, oltre al problema della propagazione del segnale che prima o poi arriva comunque, nelle reti wireless LAN c’è anche la problematica del range di propagazione. Ogni stazione ha il proprio range di propagazione in cui oltre i segnali non arrivano e ci potremmo trovare in due casi tipici:

**CSMA stazione nascosta**

* Come esempio consideriamo tre stazioni A, B e C tali che B sia a portata di A e di C, ma A e C non possano rilevare le rispettive trasmissioni
* Se C sta trasmettendo dati a B, A non potra’ rilevare l’occupazione del canale in quanto e’ fuori portata
* A iniziera’ a trasmettere ed il suo segnale arrivera’ a B interferendo con i dati che C sta’ trasmettendo
* Questo e’ detto problema della stazione nascosta

**CSMA stazione esposta**

* Se nelle stesse ipotesi supponiamo che A stia trasmettendo verso un’altra destinazione, e che B desideri inviare dati a C
* B ascolta il canale e lo trova occupato, quindi non trasmette
* In realta’ il canale sarebbe disponibile (nella ipotesi che la destinazione della trasmissione di A sia fuori dalla portata di B) perche’ in C i segnali non interferirebbero
* Questo e’ il problema della stazione esposta

MCMA

Il protocollo MACA (Multiple Access with Collision Avoidance) tenta di risolvere il problema nel seguente modo:

* il trasmettitore A invia un piccolo frame (RTS: Request To Send) al ricevitore B
* il frame RTS contiene la richiesta di trasmettere un frame a B, specificandone la lunghezza
* il ricevitore B trasmette un piccolo frame di conferma (CTS: Clear To Send) ad A, con le stesse informazioni del RTS
* quando A riceve il CTS trasmette il frame di dati a B

Tutte le stazioni che ricevono il frame RTS sanno che

* B rispondera’ con un CTS
* in seguito A trasmettera’ un frame di dati di lunghezza specificata in RTS
* Queste stazioni attenderanno senza trasmettere un tempo sufficiente alla trasmissione dei dati
* Le stazioni nascoste non vedono il frame RTS, ma vedono il frame CTS, quindi sanno che
* trasmesso il CTS B dovra’ ricevere il frame di dati, di lunghezza specificato nel CTS

Queste stazioni attenderanno senza trasmettere per il tempo necessario alla trasmissione del frame di A (che loro non vedranno in quanto nascoste, ma sanno che ci sara’)

* Collisioni saranno possibili se un frame RTS venisse trasmesso contemporaneamente verso una destinazione collocata nel campo di ricezione dei due trasmittenti: i due frame andranno perduti
* In questo caso la stazione che non riceve il CTS dopo un timeout applica l’algoritmo di backoff esponenziale binario e ritenta

Collisioni su wireless: CA

Collision Avoidance: viene utilizzato nelle reti wireless poiche il CD non può dare sicurezza che ogni WT ascolti tutte le altre WT

**Funzionamento**

* Tx ascolta il canale – Carrier Sense (CS)
* Se Tx trova il mezzo libero per un tempo DIFS (Distribuited Inter Frame Space) trasmette
* Tx trasmette un breve messaggio di controllo RTS (Request to Send)

– Lunghezza del MSG  
– Mittente e Destinatario

* L’AP riceve l’RTS e risponde, dopo un tempo SIFS, con un breve messaggio CTS (Clear to Send)

CSMA/CA

CA = Collision Avoidance.

Cerca di evitare le collisioni o comunque di ridurne la possibilità.

Ogni host, prima di inizializzare effettivamente la trasmissione, avvisa il destinatario il quale se risponderà affermativamente (con un pacchetto ACK) darà il via alla comunicazione. In caso contrario, il mittente riproverà dopo un tempo arbitrario.