Reti di comunicazione standardizzate

Mariano Severi

La considerazione più semplice che viene in mente pensando alla realizzazione di reti di comunicazione è che una delle esigenze principali degli utenti in tutti gli ambiti di applicazione è certamente la mobilità. Non stupisce quindi la crescente diffusione dei sistemi di connessione senza filo (wireless) nelle reti LAN (Local Area Network); a ben vedere, la stessa evoluzione si è osservata nel settore della telefonia con la crescita esponenziale dei cellulari.

La rivoluzione mobile ora è anche nel settore networking con lo standard 802.11, la tecnologia wireless per le reti locali

Di seguito è riportata un'introduzione alla specifica Ieee 802.11 che rappresenta ormai lo standard universalmente adottato in questo settore.

Un po' di storia

Il primo esempio di connessione wireless per la trasmissione di dati si può far risalire al 1970, quando un gruppo di ricercatori dell'Università delle Hawaii, guidato da Norman Abramson, creò AlohaNet, una rete a stella di sette calcolatori dislocati sulle quattro isole dell'arcipelago e connessi mediante radio amatoriali. Nel 1979 Gfeller e Bapst sperimentarono la prima connessione a infrarossi; un anno dopo Ferret pubblicò un lavoro sull'applicazione di tecniche 'spread spectrum' per comunicazioni wireless.

La prima generazione di modem wireless viene sviluppata agli inizi degli anni '80; le prime applicazioni supportano data-rate di 9.600 bps su distanze di pochi metri. Agli inizi degli anni '90, invece, appaiono i primi prodotti sul mercato e la commissione Ieee 802.11 inizia il proprio lavoro di standardizzazione; nel 1991 si tiene il primo workshop per valutare le tecnologie alternative.

Nel 1999 al Macworld Expo a New York City, Steve Jobs presenta la soluzione AirPort di connettività wireless a Internet per gli iBook di Apple; per la prima volta la tecnologia wireless viene resa disponibile a utenti tradizionali a costi accessibili.

Vantaggi e svantaggi

Diversi sono i vantaggi delle reti LAN wireless (Wlan). Primo fra tutti è la mobilità per l'utente, con la possibilità di avere una connessione praticamente dovunque all'interno della zona coperta dalla rete; tale aspetto si traduce in una maggiore convenienza e facilità nell'utilizzo delle risorse della rete. In ambito lavorativo, ad esempio, questo può determinare una maggiore produttività del dipendente messo in condizione di lavorare nella locazione più congeniale a lui o all'attività svolta. Allo stesso modo, la continua diffusione delle Wi-Fi zone all'interno delle strutture pubbliche e private come aeroporti, alberghi, internet cafè e bar apre all'erogazione di nuovi servizi con migliaia di potenziali clienti interessati. D'altra parte, l'assenza di connessioni cablate rende più semplice l'installazione e la manutenzione della rete, riducendo nel contempo i costi associati; la struttura stessa è più flessibile, facilmente estendibile e aggiornabile. Si pensi alla difficoltà di cablare un edificio storico con forti vincoli ambientali e di conservazione e tutela del patrimonio; con una connessione wireless le barriere architettoniche diventano più facilmente superabili.

Gli svantaggi principali riguardano invece la sicurezza e l'af-

fidabilità della rete, l'area di copertura, la velocità di trasferimento dati. Utilizzando un mezzo di trasmissione come l'aria, accessibile a chiunque, infatti, la comunicazione wireless può facilmente essere intercettata. Del resto, per ridurre i costi delle apparecchiature degli utilizzatori, la potenza del segnale è piuttosto elevata rispetto al raggio di copertura. Con antenne a guadagno più elevato di quelle tipicamente utilizzate sarebbe quindi possibile ricevere il segnale anche al di fuori dell'area coperta dalla rete; i 'wardriver' sono apparecchiature in grado di localizzare una rete wireless ed eventualmente provare a violarla. Le trasmissioni wireless sono tipicamente codificate ma come è chiaro nessun sistema di crittografia è sicuro in assoluto; il primo sistema introdotto nel 1999 denominato WEP (Wired Equivalent Protocol) già del 2001 fu attaccato e oggi sono disponibili dei software che permettono di violarlo nel giro di qualche minuto. Per tali motivi, le applicazioni più recenti utilizzano un nuovo protocollo chiamato WPA (Wi-Fi Protected Access). Inoltre il livello di affidabilità di una rete wireless è peggiore rispetto a una connessione su cavo; la trasmissione con segnali radio è infatti maggiormente sensibile alle interferenze. In alcuni casi, poi, a causa delle riflessioni, si possono creare dei complessi fenomeni nella propagazione del segnale che ne influenzano la qualità e la capacità del ricevitore di ricostruire correttamente le informazioni. Per tali motivi, la copertura di una Wlan è quindi solo dell'ordine di decine di metri; su distanze maggiori devono essere utilizzati repeater o access point addizionali con, tuttavia, una crescita dei costi di istallazione. Non a caso per applicazioni su lungo raggio sono stati definiti protocolli diversi come il WiMAX.

La stessa velocità di trasmissione è inferiore rispetto a una comunicazione su cavo. Mentre ormai le connessioni su Ethernet raggiungono i 10 Gb, la nuova specifica 802.11n permette teoricamente di raggiungere 600 Mbps nella configurazione più complessa. Se nel caso di applicazioni per clienti tradizionali questo non rappresenta ancora un limite, si pensi invece all'erogazione di una connessione a Internet dove le velocità offerte dei provider, tipicamente inferiori di quanto reso disponibile dalla connessione wireless, possono diventare una limitazione nell'ambito di reti aziendali.

Introduzione alle reti 802.11

La figura 1 mostra uno schema di principio dell'organizzazione della famiglia di standard 802.11 che definisce le regole e le specifiche per tecnologie LAN; sono coperti il DataLink Layer e il Physical Layer del modello OSI. Il DataLink layer, in particolare, è diviso in LLC (Logic Link Layer) e MAC (Media Access Control). Quest'ultimo definisce le regole di accesso al mezzo fisico e le modalità per la comunicazione dei dati; i dettagli della trasmissione sono invece dichiarati nel Physical Layer.

Come mostrato in figura 1, la specifica 802.1 definisce i servizi di gestione della rete oltre a funzionalità accessorie come bridging (802.1d) e LAN virtuali (802.1q). La specifica 802.2 copre invece l'LLC mentre gli standard 802.3, 802.5 e 802.11 implementano MAC e Physical Layer. La 802.3 rappresenta la specifica per le reti Csma/CD legate allo stan-

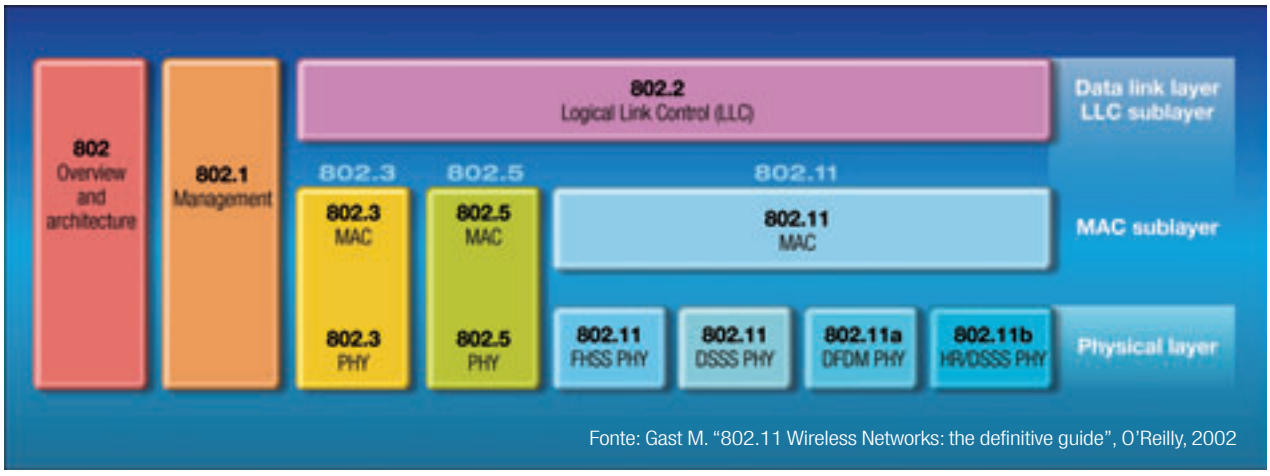

Figura 1 - Gli standard 802.11

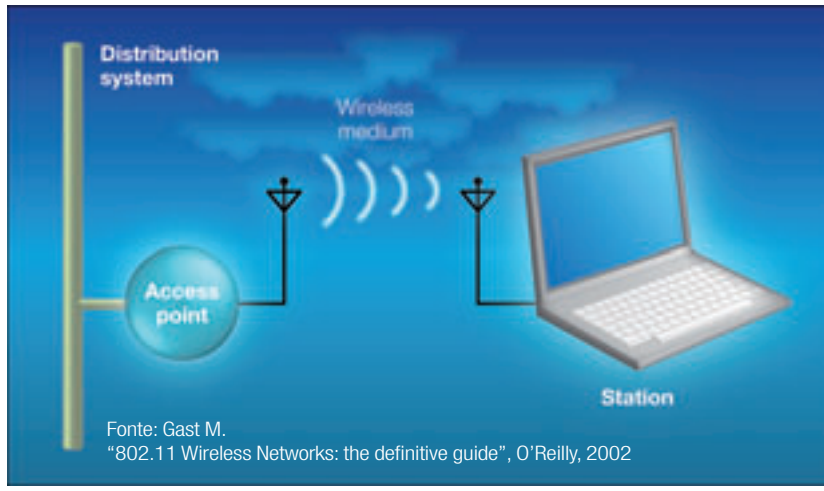

Figura 2 - Gli elementi di una rete 802.11

dard Ethernet; la 802.5 si riferisce alle reti Token Ring mentre la 802.11 copre le reti wireless (Wlan).
La figura 2 mostra uno schema di principio di una rete wireless. I componenti principali sono il sistema di distribuzione (distribution system), i punti di accesso (access point), il mezzo di trasmissione e le stazioni. Le stazioni, in particolare, sono i dispositivi dotati di interfaccia wireless, come computer portatili, desktop o PDA; i punti di accesso servono quindi a garantire la connessione delle stazioni tra loro e alla rete cablata; implementano funzionalità di bridging e identificazione, come vedremo in seguito. Il sistema di distribuzione è invece la dorsale di connessione dei diversi punti di accesso; tipicamente è basato sulla tecnologia Ethernet. Il mezzo di trasmissione è l'etere.
La configurazione base di una rete wireless è chiamata BSS (Base Service Set); è una semplice rete di stazioni connesse wireless tra loro all'interno di una area di copertura chiamata basic service area. La configurazione Independent BSS, in particolare, prevede che le stazioni comunichino mediante connessioni punto-punto, quindi senza necessità di un punto di accesso; tipicamente tali strutture vengono create per esigenze temporanee, come ad esempio scambio di dati in un gruppo di lavoro durante una riunione. Le reti Infrastructure BSS, invece, prevedono un punto di accesso attraverso il quale transita l'intero flusso di dati; tale punto di accesso riceve i messaggi dalle stazioni connesse e li invia ai rispettivi destinatari. Diversi sono i vantaggi di questa soluzione rispetto alla più semplice configurazione Independent BSS. L'area di servizio coperta dalla rete viene definita semplicemente dal raggio a partire dal nodo di accesso entro il quale è recepito il segnale e non dipende, invece, dalla posizione relativa dei due nodi in comunicazione. Nel caso di stazioni alimentate a batteria, inoltre, possono essere implementate delle soluzioni di risparmio della potenza. La stazione può essere accesa soltanto per certi intervalli di tempo nei quali offre connettività; nei periodi in cui è spenta il nodo di accesso cui è connessa, rilevando tale condizione, può memorizzare localmente i messaggi che vi dovevano essere inviati per spedirli solo quando la stazione diviene attiva.
Connettendo più Infrastructure BSS tra loro mediante una rete di distribuzione viene realizzata un Extended Service Set; le BSS possono eventualmente essere sovrapposte su una certa area, ma ogni stazione deve necessariamente fare parte di una sola di queste e quindi essere connessa a un solo punto di accesso. Lo standard non definisce una particolare tecnologia per la dorsale di connessione ma i servizi che deve fornire sono la distribuzione, che serve per distribuire i frame ricevuti dal punto di accesso alla destinazione corretta; l'integrazione con reti non 802.11 poiché i dettagli del servizio sono evidentemente specifici del particolare sistema di distribuzione e della rete cui si connette; l'associazione delle stazioni ai punti accesso in base alle informazioni di registrazione, infatti stazioni non associate non sono viste sulla rete analogamente a come i nodi Ethernet fisicamente non connessi via cavo non sono raggiungibili; gestione della riassociazione a un nuovo punto di accesso di una stazione mobile poiché in questo caso, il punto di accesso alla rete può cambia-

STANDARD ED EMENDAMENTI

Ieee 802.11-2007 è la revisione dello standard correntemente approvata. Di seguito sono elencati gli emendamenti (oltre a una breve descrizione e l'anno di pubblicazione) che sono stati emessi nel tempo come aggiornamento della specifica:

- *Ieee 802.11a: 54 Mbps, 5 GHz standard (1999)*
- *Ieee 802.11b: estensione per supportare data rate fino a 5,5 e 11 Mbps (1999)*
- *Ieee 802.11c: definizione delle procedure operative dei bridge; incluso in Ieee 802.1D standard (2001)*
- *Ieee 802.11d: estensione per roaming in ambito internazionale (2001)*
- *Ieee 802.11e: definizione dei servizi di Quality of Service (2005)*
- *Ieee 802.11f: Inter Access Point Protocol (2003)*
- *Ieee 802.11g: 54 Mbps, 2,4 GHz standard, compatibile con emendamento 802.11b (2003)*
- *Ieee 802.11h: estensione all'emendamento 802.11a per la gestione dello spettro e della potenza trasmessa nella banda a 5 GHz (2004)*
- *Ieee 802.11i: definizione dei protocolli di sicurezza (2004)*
- *Ieee 802.11j: estensione per il mercato giapponese (2004)*
- *Ieee 802.11-2007: nuova revisione dello standard che include emendamenti a, b, d, e, g, h, i e j (2007)*
- *Ieee 802.11k: gestione delle risorse radio per transizioni tra BSS (2008 - draft k)*
- *Ieee 802.11m: attività di manutenzione dello standard, correzioni, chiarimenti*
- *Ieee 802.11n: 2,4 e 5 GHz, architettura Mimo, 600 Mbps (2008)*
- *Ieee 802.11p: estensioni per accesso in ambienti veicolari (atteso per il 2009)*
- *Ieee 802.11r: transizioni veloci tra BSS (atteso per luglio 2008)*
- *Ieee 802.11s: ESS Extended Service Set per reti mesh (in fase di definizione - 2008)*
- *Ieee 802.11T: Wireless Performance Prediction (WPP), raccomandazioni su metodi di test e metriche (in fase di defiizione - 2008)*
- *Ieee 802.11u: interoperabilità con reti non-802 (in fase di definizione)*
- *Ieee 802.11v: gestione delle reti wireless (in fase di definizione)*
- *Ieee 802.11w: Protected Management Frames (maggio 2008 - draft 7)*
- *Ieee 802.11y: operabilità a 3.650-3.700 MHz in USA (aprile 2008 - draft 10)*
- *Ieee 802.11z: estensione Direct Link Setup (DLS) (in fase di definizione)*

re in funzione della posizione della stazione stessa e della potenza del segnale ricevuto. La procedura di riassociazione viene iniziata dalla stazione mobile e non dal punto di accesso; al termine della procedura, il sistema di distribuzione utilizza le informazioni di registrazione per riassociare correttamente la stazione al nuovo punto di accesso; segue la dissociazione, per terminare un'associazione corrente nel momento in cui la stazione si disconnette dalla rete; al termine della procedura eventuali dati presenti nel sistema di distribuzione e inerenti al nodo dissociato sono eliminati.
Tra i servizi che devono implementare, invece, le singole stazioni vi è l'autenticazione, che serve a scopo di sicurezza della stazione che richiede l'associazione alla rete: in realtà alcuni punti di accesso sono configurati per autenticazioni 'open system' il che implica l'autenticazione, in definitiva, di ogni nodo che faccia richiesta di associazione alla rete. Vi è poi la deautenticazione per terminare una relazione di autenticazione della stazione precedentemente stabilita; ancora, la privacy, per proteggere la rete con il supporto di sistemi di cifratura delle informazioni, e infine Msdu delivery, per l'invio di dati (MAC Service Data Unit) al destinatario.
I primi servizi servono a gestire le procedure di autenticazione della stazione richiedente la connessione alla rete; i servizi di privacy quindi implementano gli algoritmi di cifratura delle informazioni per evitare il furto delle informazioni e l'infiltrazione di nodi non ammessi. I servizi Msdu (MAC Service Data Unit) delivery, invece, servono all'invio di dati al destinatario.

STANDARD DI WIRELESS NETWORKING

Protocollo 802.11	Data di emissione	Frequenza (GHz)	Throughput (Mbps)	Dati (Mbps)	Modulazione	Primo input (m)	Primo output (m)
–	1997	2,4	00,9	2		~20	~100
a	1999	5	23	54	Ofdm	~35	~120
b	1999	2,4	04,3	11	Dsss	~38	~140
g	2003	2,4	19	54	Ofdm	~38	~140
n	2009	2,4, 5	74	248		~70	~250
y	2008-06-23	3,7	23	54		~50	~5.000

Fonte: Gast M. "802.11 Wireless Networks: the definitive guide", O'Reilly, 2002

Il layer fisico

Nel modello standard OSI, il layer fisico definisce tutte le specifiche che riguardano le interfacce del dispositivo con il mezzo di trasmissione. Come accennato in precedenza, lo standard 802.11, in particolare, definisce diversi livelli fisici in funzione della applicazioni; la tabella elenca quelli attualmente supportati.
La versione originale dello standard pubblicata nel 1997, in particolare, specificava trasmissioni nella banda a 2,4 GHz riservata alle applicazioni industriali e medicali con segnali a infrarossi (IR) o utilizzando metodi spread spectrum di tipo frequency-hopping (FH) o direct-sequence (DS); erano supportati data rate di 1 e 2 Mbps.
Nel 1999 fu emesso l'emendamento 802.11a che spostava le trasmissioni alla banda dei 5 GHz e adottava tecniche Ofdm che consentono di ridurre gli effetti di multipath e migliorare l'efficienza spettrale. Lo standard supporta fino a 52 sottoportanti, di cui 48 per i dati e quattro riservate; la banda utilizzata per canale è 20 MHz, con una durata di simbolo di 4 ms. Le modulazioni adottate sono Bpsk, Qpsk, 16 QAM o 64 QAM. Il data rate massimo è fino a 54 Mbps che corrisponde a una capacità netta di trasferimento dati di circa 20 Mbps.
Nello stesso anno fu emessa anche la specifica 802.11b; utilizzando modulazione CCK nella banda originaria a 2,4

WI-FI ALLIANCE

Nell'Agosto 1999 3Com, Aironet (ora Cisco), Harris Semiconductor (ora Intesil), Lucent Technology (ora Agere), Nokia e Symbol Technologies crearono il consorzio no profit Weca (Wireless Ethernet Compatibility Alliance) per certificare l'interoperabilità e favorire la diffusione di sistemi e apparati compatibili con lo standard Ieee 802.11b. Interbrand Corporation (nota società di consulenza creatrice di marchi famosi come AT&T, Microsoft, Lexmark, Sony ecc.) con ciò successivamente il termine Wi-Fi e il noto logo in stile 'yin-yang' per il consorzio che dal 2000 ha quindi modificato la propria denominazione in Wi-Fi Alliance. Sebbene non fosse assolutamente nelle idee dei promotori, il termine Wi-Fi è stato confuso fin dagli inizi come acronimo di wireless fidelity, pur non avendo questo un significato preciso. Tale interpretazione è esplicitamente scoraggiata oggi dal consorzio.
La Wi-Fi Alliance conta attualmente oltre 320 membri, includendo i principali produttori di sistemi 802.11, e ha sede ad Austin, in Texas. Dal 2000 a oggi, oltre 4.000 prodotti sono stati certificati. La certificazione assicura l'interoperabilità dal punto di vista della trasmissione radio e del formato dei dati dei dispositivi, oltre ad accertare la conformità dei protocolli di sicurezza implementati e verificare (ove supportati) i servizi di QoS e gestione della potenza come definiti dalle corrispondenti clausole dello standard 802.11.

GHz, lo standard supporta un data rate fino a 11 Mbps su distanze fino a 30 m o di 1 Mbps fino a 90 m. Adottando protocolli TCP o UDP, la capacità di trasferimento dati che si ottiene è 5,9 e 7,1 Mbps rispettivamente.
Il successivo emendamento 802.11g, adottato a partire dal 2003, estende la capacità di trasmissione nella stessa banda fino a 54 Mbps (corrispondente a un 'throughput' di circa 19 Mbps). Per trasmissioni a 6, 9, 12, 18, 24, 36, 48 e 54 Mbps la modulazione supportata è Ofdm; per trasmissioni a 5,5 e 11 Mbps sono invece impiegate tecniche CCK mentre per connessioni a 1 e 2 Mbps sono adottati metodi Dbpsk/Dqpsk. Come tutti gli standard operanti a 2,4 GHz, anche la specifica 802.11b soffre tuttavia di problemi di interferenza legati all'elevata occupazione della banda; nella stessa banda operano ad esempio forni a microonde, dispositivi bluetooth, telefoni cordless.
L'ultimo emendamento approvato in ordine di tempo è l'802.11n, emesso in versione draft numero 4 nel maggio 2008. Rispetto alle precedenti versioni prevede una architettura Mimo (Multiple Input Multiple Output) che utilizza più trasmettitori e antenne per ottenere migliori prestazioni e definisce canali a 40 MHz raddoppiando, quindi, la larghezza di banda. Grazie all'architettura Mimo, lo standard supporta tecniche di multiplexing spaziale (Spartial Division Multiplexing) con la trasmissione simultanea di più flussi di dati (fino a quattro) in un solo canale spettrale e channel bonding con l'utilizzo in parallelo di due canali che non si sovrappongono per trasmettere i dati di una singola sorgente. Lo standard è specificato per operare in entrambe le bande a 2,4 e 5 GHz con modulazioni compatibili con quelle previste dagli emendamenti precedenti. Una configurazione con quattro antenne e quattro trasmettitori, con larghezza di banda di canale di 40 MHz, utilizzando modulazione Ofdm dovrebbe consentire teoricamente un throughput di 600 Mbps.

Il layer MAC

In base al modello OSI, il MAC è lo strato del protocollo che controlla l'accesso al mezzo fisico per la trasmissione dei dati. Il MAC definito dallo standard 802.11, in particolare, è un adattamento del protocollo Ethernet alla trasmissione in aria dei dati con i problemi a essa inerenti. Mentre l'Ethernet si basa, infatti, su un protocollo di tipo Csma/CD (Carrier Sense Multiple Access with Collision Detection), la 802.11 adotta uno schema Csma/CA (Carrier Sense Multiple Access with Collision Avoidance). Il primo schema tende a rilevare eventuali collisioni nell'accesso alla rete, verificando, ad esempio mentre si trasmette, che i dati ricevuti siano uguali a quelli trasmessi; nel caso di collisione la trasmissione viene interrotta e dopo un tempo di attesa viene inviato un messaggio per indicare la volontà di riprendere la comunicazione e quindi inibire l'invio di dati da parte degli altri nodi. Nello schema Csma/CA, invece, si cerca a priori di evitare collisioni in quanto rappresentano uno spreco di banda per la trasmissione; d'altra parte, per ridurre i costi delle apparecchiature, tipicamente i transceiver wireless non hanno la possibilità di ricevere mentre trasmettono, rendendo quindi difficile proprio il rilevamento delle eventuali collisioni.
Nello schema Csma/CA, il nodo che intende spedire dati deve rilevare preventivamente se il mezzo di comunicazione è disponibile; la condizione prevista è che non siano stati ricevuti messaggi nel precedente intervallo di tempo Difs (nel caso di messaggi con errore il tempo di attesa è definito dal parametro Eifs). Quindi il nodo invia un messaggio sulla rete per istruire le altre stazioni a non accedere al mezzo fisico; la trasmissione quindi può iniziare seguendo un semplice schema di richiesta e autorizzazione (RTS/CTS). Per evitare collisioni, ogni messaggio inviato contiene un campo NAV (Network Allocation Vector) che indica la quantità di tempo per la quale il mezzo dovrà essere considerato riservato alla stazione trasmittente; le stazioni in ascolto devono implementare un contatore del tempo trascorso per evitare di accedere alla rete quando il mezzo è ancora riservato. I messaggi inviati dalla stazione trasmittente devono essere separati tra loro da un tempo definito dal parametro Sifs.
All'interno del MAC del protocollo 802.11 le funzioni di connessione Csma/CA sono gestite dai servizi DCF (Distributed Coordination Function); il PCF

LA TRASMISSIONE SPREAD SPECTRUM

Le tecniche spread spectrum sono modi di trasmissione di un segnale che utilizzano una banda passante maggiore della larghezza dello spettro dell'informazione. Conosciute fin dagli inizi del secolo (la prima trattazione è riportata nel testo 'Wireless Telegraphy' di Zenneck del 1908), sono tipicamente utilizzate per trasmissioni in bande non licenziate, come nel caso dei sistemi 802.11 operanti nell'ISM (Industrial, Scientific and Medical band). Disperdendo la potenza del segnale, non sono intercettabili dai classici ricevitori a banda stretta e possono essere confuse come rumore di fondo. Tra i vantaggi principali vi sono minore distorsione e migliore immunità alle interferenze. Per questo sono spesso state utilizzate nei sistemi militari; l'utilizzo commerciale è iniziato soltanto nei primi anni '80.
Lo standard 802.11 prevede le seguenti tecniche spread spectrum: FH (Frequency Hopping), DS (Direct Sequence) e Ofdm (Orthogonal Frequency Division Multiplexing). Nei sistemi FH, ad esempio, la frequenza della portante viene variata in maniera casuale seconda una sequenza pseudo random; le tecniche DS, invece, utilizzano una modulazione di fase di un segnale sinusoidale mediante codici pseudo casuali aventi durata inferiore al periodo di bit. i metodi Ofdm, invece, dividono la banda disponibile in canali utilizzando questi per la codifica e la trasmissione in parallelo di diverse componenti del segnale.

Figura 3 - La struttura di un frame 802.11

(Point Coordination Function) invece consente di trasferire informazioni senza entrare nella procedura di contenzioso del bus per applicazioni in tempo reale. Pifs è il tempo che un nodo deve attendere dopo la ricezione di un messaggio per poter inviare propri dati.

La figura 3 mostra la struttura di un frame come prevista dallo standard 802.11; per ogni campo è riportata la lunghezza corrispondente in byte. Il campo Frame Control, in particolare, specifica la versione di protocollo utilizzata, il tipo di messaggio tra quelli consentiti, l'eventuale destinazione di questo al sistema di distribuzione, se il messaggio è stato frammentato o se si tratta di una ritrasmissione. Il Duration/ID field invece contiene, in condizioni normali, il NAV richiesto dalla stazione trasmittente. Fino a quattro diversi campi di indirizzo sono quindi inclusi successivamente, con significato diverso a seconda del tipo di messaggio; servono a specificare la sorgente e il destinatario del messaggio, la stazione trasmittente o quella ricevente o, nel caso di presenza di diverse Wlan nella stessa area, la BSS cui la stazione è associata. Il campo Sequence Control Field serve per gestire la frammentazioni dei messaggi del più alto livello e il rigetto al nodo ricevente di eventuali frame duplicati. Il Frame Body o Data Field contiene invece i dati del messaggio utente; l'LLC dello standard 802.11 supporta fino a 2.296 byte con 8 byte di header per frame. Il Frame Check Sequence, infine, contiene i campi di controllo (CRC) che permettono di verificare l'integrità e la correttezza del frame ricevuto. ■