Azzolini Riccardo 2020-09-29

Reti wireless IEEE 802.11 (Wi-Fi)

1 Vantaggi e svantaggi delle LAN wireless

Da quando sono state introdotte le LAN wireless, il numero di apparati connessi ad esse è aumentato in modo esponenziale. Ciò è avvenuto perché le reti wireless risolvono molti dei problemi delle soluzioni wired (cablate):

- i costi e tempi della posa in opera dei cavi;
- la degradazione delle prestazioni nel tempo, dovuta alla degradazione delle caratteristiche elettriche dei conduttori a causa degli agenti atmosferici;
- i costi di manutenzione dovuti alla rottura di cavi e connettori durante l'uso.

Più in generale, le motivazioni che possono rendere preferibile una LAN wireless sono:

- Motivazioni di ordine *logistico*: si riducono le difficoltà di cablaggio tra edifici separati da ostacoli (fiumi, laghi, ecc.), o in edifici di interesse storico/artistico, o ancora in ambienti a logistica complessa.
- Motivazioni di ordine *economico*: una rete wireless permette di riorganizzare o aggiungere facilmente uffici, e riduce i costi di manutenzione e sostituzione dei cavi in presenza dei guasti. Inoltre, anche quando si prevede la realizzazione di una LAN cablata, si può implementare una rete wireless temporanea prima della posa dei cavi.
- *Mobilità*: l'utente è libero di muoversi all'interno dell'area di copertura della rete senza perdere la connessione.
- *Scalabilità*: è facile aumentare il numero di dispositivi connessi (perché non bisogna posare nuovi cavi, ecc.).
- *Flessibilità*: in ogni momento possono essere collegati alla rete un numero variabile di utenti.

Le LAN wireless hanno però anche numerosi problemi:

- *Velocità di trasferimento dei dati*: nonostante l'evoluzione tecnologica, essa rimane sempre inferiore a quella delle reti cablate.

- *Inaffidabilità del mezzo trasmissivo*: il range e la velocità di trasmissione sono influenzate dalle interferenze elettromagnetiche (provocate da apparecchiature che emettono onde elettromagnetiche indesiderate) e dalle interferenze dovute a un "affollamento" della banda, cioè ad altre trasmissioni sulle stesse frequenze (interferenza co-canale) o su frequenze adiacenti. Gli standard delle reti wireless devono quindi essere progettati in modo da garantire il funzionamento dei protocolli di livello rete nonostante questa inaffidabilità.
- *Multipath fading in ricezione*: oltre al segnale trasmesso "in linea d'aria", alla stazione ricevente giungono spesso anche delle "copie" di tale segnale, dovute alla riflessione delle onde elettromagnetiche (tipicamente su pareti e oggetti metallici). Queste copie hanno intensità e tempi di arrivo diversi, per cui la loro sovrapposizione con il segnale originale può risultare problematica. Sistemi di ricezione più avanzati sono invece in grado di elaborare il segnale ricevuto in modo da sfruttare le riflessioni per migliorare la qualità della ricezione.
- *Sicurezza*: l'accesso al mezzo fisico condiviso è libero, quindi la rete deve essere protetta da appositi meccanismi di autenticazione (mentre per una rete cablata è difficile anche solo collegarsi al mezzo).
- *Consumo di energia*: la comunicazione su una rete wireless richiede energia, riducendo la durata delle batterie.
- *Area di copertura*: essa dipende dalle interferenze, dalla velocità di trasmissione e dalla potenza del segnale (dunque dal consumo di energia).
- *Salute*: l'emissione elettromagnetica deve essere limitata, perché un'eccessiva esposizione alle onde elettromagnetiche può essere dannosa per la salute.
- *Legislazione*: ogni nazione regolamenta l'occupazione delle frequenze.
- *Interoperabilità*: una rete wireless deve essere compatibile con apparati di produttori diversi. A tale scopo, esistono organismi che rilasciano certificazioni di conformità agli standard ("Wireless Fidelity", da cui deriva la sigla Wi-Fi).

2 Standard IEEE 802.11

IEEE 802.11, noto con il nome commerciale **Wi-Fi**, è il principale standard per le reti LAN wireless. Nel corso degli anni, sono state definite numerose versioni di questo standard, ciascuna delle quali ha apportato modifiche in termini di velocità di trasmissione, qualità o sicurezza. Alcune versioni significative sono:

- 802.11, la versione originale, che funziona a una frequenza di 2.4 GHz e riesce a ottenere una velocità di 1–2 Mbps;
- 802.11b, che mantiene la stessa frequenza di 2.4 GHz ma aumenta la velocità massima a 11 Mbps;

- 802.11a, che funziona a 5 GHz, permettendo di raggiungere velocità fino a 54 Mbps;
- 802.11g, che ottiene una velocità di 54 Mbps pur lavorando a 2.4 GHz, grazie all'uso di una diversa tecnica di modulazione (OFDM, Orthogonal Frequency Division Multiplexing, la quale si basa su segnali *ortogonali*, che non producono interferenza tra di loro);
- 802.11e, che si occupa della gestione della qualità del servizio;
- 802.11i, che affronta i problemi di sicurezza.

3 Architettura di una rete Wi-Fi

I principali elementi e concetti di una rete LAN wireless basata sullo standard IEEE 802.11 sono i seguenti:

- **Station** (**STA**, stazione): ogni dispositivo che è in grado di comunicare usando il protocollo IEEE 802.11.
- **Basic Service Set** (**BSS**): un insieme di stazioni controllate da uno stesso access point.
- **Coordination Function**: la funzione logica che, all'interno di un BSS, assegna alle stazioni i diritti di trasmettere/ricevere. Si può avere o un accesso centralizzato, **Point Coordination Function** (**PCF**), oppure un accesso distribuito, **Distributed Coordination Function** (**DCF**).
- **Extended Service Set** (**ESS**): un insieme di BSS (ciascuna con un proprio access point) e LAN che viene visto come un'unica BSS dal livello LLC delle stazioni che vi fanno parte.
- **Distribution System** (**DS**): una dorsale cablata che interconnette BSS e LAN, formando un ESS.
- **Access Point** (**AP**): un dispositivo wireless che funge da punto di accesso a un distribution system. Esso è tipicamente dotato di una porta per la connessione alla LAN cablata (che costituisce il distribution system) e di un'antenna per la comunicazione wireless.

3.1 Tipologie di rete

Le reti Wi-Fi si distinguono in due tipi: reti **ad hoc** e reti **infrastructure** (con infrastruttura).

- Una rete "ad hoc" (che in latino significa "solo per questo scopo") è una rete wireless in cui non sono presenti access point. Ogni stazione può scambiare informazioni con le altre stazioni nella stessa rete (che prende il nome di **IBSS**, **Independent Basic Service Set**). L'architettura fortemente distribuita di questo tipo di rete la rende altamente flessibile, robusta, facile e veloce da realizzare, e praticamente indipendente dalle infrastrutture (non servono access point o reti wired). Il principale svantaggio è invece l'impossibilità di estendere la rete usando un distribution system.
- Una rete con infrastruttura corrisponde invece a un ESS, cioè a più BSS i cui access point sono interconnessi da un distribution system. Ciò permette la realizzazione di reti con un'estensione superiore alla massima distanza di trasmissione wireless: si possono sovrapporre più BSS per creare un'ampia area di copertura, e/o si possono interconnettere BSS distanti, ecc. Il fatto che la rete sia formata da più BSS è trasparente al livello LLC delle stazioni: ciascuna stazione può comunicare con stazioni in altri BSS, e anche spostarsi da un BSS a un altro senza perdere il segnale.

4 Tecniche di trasmissione

Al livello fisico, lo standard IEEE 802.11 può utilizzare le tecniche di trasmissione **frequency hopping** e **direct sequence**. Entrambe sono tecniche di tipo *spread spectrum* ("espansione dello spettro"), che diffondono il segnale su un intervallo di frequenze ampio, in modo da minimizzare l'effetto dell'interferenza da parte di altri dispositivi.

4.1 Frequency hopping

La tecnica di frequency hopping consiste nel trasmettere il segnale su una sequenza pseudo-casuale di frequenze. Tale sequenza non viene comunicata sulla rete, ma è invece generata indipendentemente dal mittente e dal ricevente, utilizzando lo stesso algoritmo inizializzato con lo stesso *seme* (noto solo a mittente e ricevente). Così, le due stazioni comunicanti sono in grado di "saltare" da una frequenza all'altra in maniera sincronizzata.

Oltre a rendere la comunicazione più resistente alle interferenze, questa tecnica introduce anche un certo grado di sicurezza, perché eventuali altre stazioni che potrebbero cercare di ascoltare la comunicazione sono ostacolate dal fatto di non conoscere il seme, e quindi la sequenza di frequenze su cui avviene la trasmissione.

Per il frequency hopping, lo standard IEEE 802.11 definisce 79 canali, ciascuno ampio 1 MHz, e stabilisce che il cambio di frequenza (*hop*) debba avvenire almeno ogni 0.4 secondi. Un eventuale pacchetto perso viene ritrasmesso al successivo hop.

4.2 Direct sequence

Con la tecnica direct sequence, ogni bit di un frame da trasmettere è rappresentato da molteplici bit nel segnale trasmesso, facendo l'OR esclusivo (XOR) con una sequenza di bit generata in modo pseudocasuale (usando un seme noto solo al mittente e al ricevente, come nel frequency hopping); la sequenza di bit trasmessi (il risultato dell'OR esclusivo) è chiamata *chipping sequence*. In questo modo, si ottiene un segnale più resistente al rumore, e anche più difficile da interpretare per eventuali altre stazioni (che non conoscono il seme della sequenza pseudocasuale), a costo di una certa ridondanza, che riduce la velocità massima possibile (perché appunto ogni bit di dati è rappresentato da più bit nel segnale trasmesso).

Ad esempio, per trasmettere i bit 1010 usando una chipping sequence a 4 bit:

1. ciascun bit dei dati viene replicato 4 volte:

   $$1111\,0000\,1111\,0000$$

2. si genera una sequenza di bit pseudocasuale, come ad esempio:

   $$0100\,1011\,0101\,1001$$

3. viene calcolata e trasmessa la chipping sequence, l'OR esclusivo delle sequenze ottenute ai punti 1 e 2:

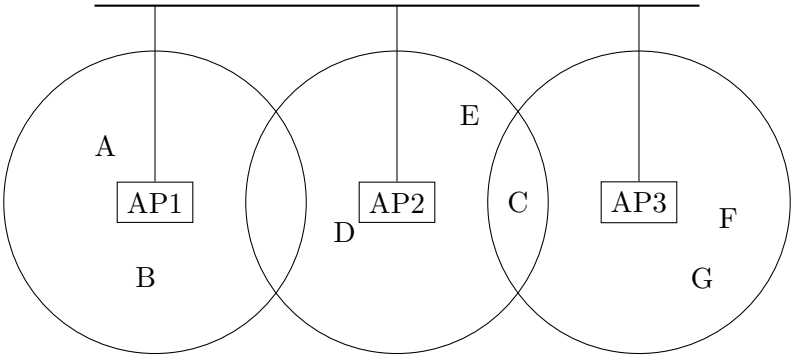
   $$\begin{array}{l} 1111\,0000\,1111\,0000 \\ 0100\,1011\,0101\,1001 \\ \hline 1011\,1011\,1010\,1001 \end{array} \text{ XOR}$$

4. il ricevente, eseguendo l'operazione inversa, risale ai bit di dati originali.

Lo standard IEEE 802.11 adotta una chipping sequence a 11 bit, e definisce per il frequency hopping 11 canali da 22 MHz, parzialmente sovrapposti tra di loro (solo 3 di questi canali sono completamente non sovrapposti). In caso di interferenza, si cambia il canale su cui avviene la comunicazione.

5 Distribution system

Per permettere la mobilità (libero spostamento) delle stazioni tra BSS diverse e la connessione ad altre reti (prima tra tutte, la rete Internet), si utilizzano degli access point connessi a un distribution system (infrastruttura di rete fissa).



Ogni stazione si associa a un particolare access point, e può comunicare anche con le stazioni associate ad altri access point, tramite il distribution system. Ad esempio, nello schema riportato sopra, se A vuole comunicare con F:

1. A invia un frame (con indirizzo MAC di destinazione impostato a quello di F) al suo access point, AP1;
2. AP1 inoltra il frame ad AP3 attraverso il distribution system;
3. AP3 trasmette il frame ad F.

5.1 Tecnica di scanning

La tecnica usata da una stazione per selezionare un access point è detta **scanning**, e prevede quattro passi:

1. la stazione invia un frame di **probe**;
2. tutti gli access point alla portata della stazione rispondono con un frame di **risposta al probe**;
3. la stazione seleziona uno degli access point (tipicamente quello con la migliore qualità del segnale ricevuto) e invia a esso un frame di **richiesta di associazione**;
4. l'access point selezionato risponde con un frame di **conferma di associazione**.

Questo protocollo è utilizzato:

- quando la stazione si unisce alla rete;
- quando la stazione essa diventa "scontenta" dell'access point a cui è attualmente associata, ad esempio perché si sta allontanando fisicamente da esso, e quindi il segnale risulta indebolito.

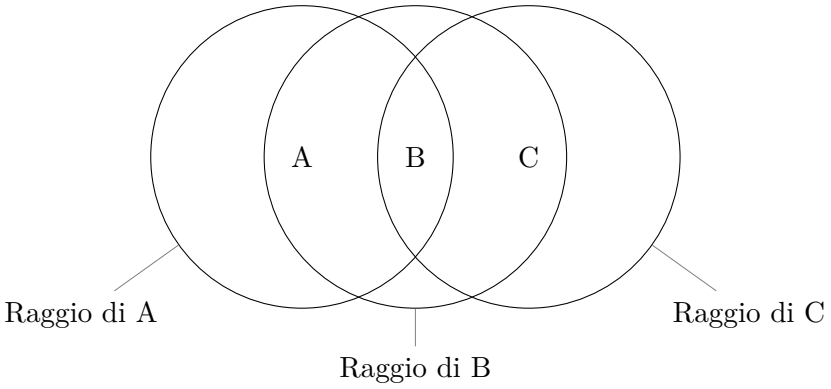
In questo secondo caso, se la stazione decide di passare a un nuovo access point, invia a esso una richiesta di associazione, e il nuovo access point manda a sua volta una notifica del cambiamento al vecchio access point, attraverso il distribution system.

6 Controllo di accesso al mezzo condiviso

Al livello MAC, lo standard IEEE 802.11 impiega un protocollo di accesso al mezzo condiviso che, come per Ethernet (IEEE 802.3), è di tipo ad accesso casuale con rivelazione del canale e delle collisioni. Tale protocollo presenta però degli accorgimenti in più, resi necessari dal fatto che non tutti i nodi sono sempre alla portata l'uno dell'altro; in particolare, bisogna risolvere i problemi dei **nodi nascosti** e dei **nodi sovraesposti**.

6.1 Problema dei nodi nascosti

Si consideri uno scenario in cui sono presenti tre nodi (stazioni wireless): A, B e C. A e C sono entrambe nel raggio di copertura di B, ma non sono invece l'una nel raggio di copertura dell'altra.

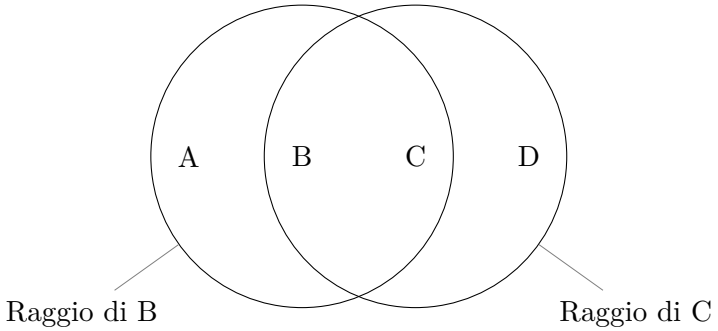


A causa della distanza, A non sente le trasmissioni di C, e viceversa. Per questo, A e C sono detti **nodi** (reciprocamente) **nascosti**.

Se A e C tentassero di inviare dati simultaneamente verso B, causerebbero una collisione in ricezione (perché i segnali di entrambe sono ancora abbastanza forti da interferire tra loro quando raggiungono la stazione B). Il problema è che *né A né C sarebbe in grado di rilevare tale collisione*, perché ciascuna delle due stazioni "sentirebbe" solo il proprio segnale, e non quello trasmesso dal nodo nascosto, che genera l'interferenza.

6.2 Problema dei nodi sovraesposti

In questo scenario ci sono quattro stazioni wireless (A, B, C e D), disposte nel modo seguente:



Si suppone che B stia trasmettendo ad A, e che C (il **nodo sovraesposto**) desideri trasmettere dati a D. Sentendo la trasmissione di B, C pensa di dover aspettare, ma in realtà potrebbe trasmettere subito senza provocare interferenze:

- C non interferirebbe con la stazione A perché quest'ultima è fuori dal raggio di copertura di C;
- C non interferirebbe con B perché questa sta trasmettendo, non ricevendo;
- D riceverebbe la trasmissione di C senza interferenza perché è fuori dal raggio di copertura di B.

6.3 CSMA/CA

Per risolvere i problemi dei nodi nascosti e dei nodi sovraesposti, lo standard IEEE 802.11 usa un protocollo di accesso al mezzo chiamato **CSMA/CA**, **Carrier Sense Multiple Access with Collision Avoidance**:

1. Prima di inviare i dati, il mittente attende che il canale sia libero (come nel CSMA/CD usato da Ethernet), poi trasmette un frame **Request To Send** (**RTS**, "richiesta di trasmissione").
2. Il ricevente risponde con un frame **Clear To Send** (**CTS**, "permesso di trasmissione").
3. Il mittente invia il frame dati.
4. Il ricevente invia un ACK per confermare di aver ricevuto il frame.

Questo protocollo risolve i problemi sopra citati nel modo seguente:

- Ogni nodo nel raggio di copertura del ricevitore riceve il frame CTS dunque sa che deve aspettare trasmettere, onde evitare interferenze. Questo funziona ugualmente anche se il mittente è un nodo nascosto (perché il CTS è appunto trasmesso dal ricevente).

- Un nodo sovraesposto riceve l'RTS ma non il CTS, quindi sa di essere fuori dal raggio di copertura del ricevente, ovvero di poter trasmettere contemporaneamente senza provocare interferenze.

Il frame RTS contiene un campo (*Network Allocation Vector*, NAV) che indica la lunghezza del frame dati da trasmettere, e tale valore viene replicato anche nel CTS, in modo che tutti i nodi situati nel raggio di copertura di almeno una delle stazioni comunicanti sappiano quanto durerà la trasmissione (e quindi quanto tempo devono attendere prima di poter a loro volta trasmettere, se non sono nodi sovraesposti).

Nonostante il nome "Collision Avoidance", rimane inevitabilmente la possibilità di collisione tra due frame RTS inviati contemporaneamente. Perciò, se un nodo invia un RTS e poi non riceve un CTS, suppone che si sia verificata una collisione, e prima di riprovare a trasmettere aspetta per un tempo determinato in base all'algoritmo di **binary exponential backoff** (come nel CSMA/CD).