Azzolini Riccardo 2020-10-01

Bluetooth

1 Bluetooth

Il **Bluetooth** è una tecnologia per la realizzazione di reti **PAN** (**Personal Area Network**) wireless, basate su onde elettromagnetiche a radiofrequenza. Una PAN è una rete con un raggio di copertura molto corto, pensata per collegare dispositivi fissi e portatili dislocati su (o nei pressi di) una singola persona (ad esempio un computer, una stampante, un telefono, ecc.).

Il progetto Bluetooth è nato nel 1998, con la formazione di uno Special Interest Group tra Ericsson e altre grandi aziende. Successivamente, esso è stato standardizzato come **IEEE 802.15**.

2 Piconet e scatternet

Una **piconet** è una rete Bluetooth costituita da al più 8 dispositivi: un **master** e al massimo 7 **slave**. Il master è l'entità centrale che gestisce l'allocazione delle risorse tra i vari slave. Un dispositivo può funzionare sia come master che come slave:

- all'interno della stessa piconet, il suo ruolo può cambiare nel tempo;
- se esso appartiene contemporaneamente a più piconet, può agire da master in alcune di esse e da slave in altre.

Due o più piconet "sovrapposte" (che hanno dispositivi in comune) possono essere collegate tra loro, formando una **scatternet**. La funzione di *bridge* (collegamento) tra due piconet viene svolta da un dispositivo che appartiene contemporaneamente a entrambe le reti (e potrebbe indifferentemente essere un master in entrambe, uno slave in entrambe, oppure un master in una e uno slave nell'altra).

Le scatternet permettono di realizzare reti Bluetooth con più di 8 dispositivi e con una più ampia area di copertura, ma in pratica non sono praticamente mai usate: se serve una rete "grande", risulta più pratico il Wi-Fi.

3 Caratteristiche del canale radio

Bluetooth opera alla frequenza di 2.4 GHz, e usa la tecnica di accesso al canale **Frequency Hopping Spread Spectrum** con **Time Division Duplexing** (**FHSS/TDD**).

- Il frequency hopping è analogo a quello impiegato dal Wi-Fi: sono definiti 79 canali da 1 MHz (situati alle frequenze $(2402 + k)$ MHz, per $k = 0, 1, \ldots, 78$), e si salta (hop) da uno all'altro in base a una sequenza pseudocasuale. Il canale viene dunque suddiviso in *time slot*: per ogni time slot si salta alla frequenza successiva nella sequenza pseudocasuale. Tutti i dispositivi Bluetooth appartenenti a una stessa piconet saltano tra le frequenze in modo sincronizzato, così da rimanere sempre in grado di comunicare l'uno con l'altro.
- Il time division duplexing è usato per la fase di trasmissione alternata master/slave.

3.1 Classi di potenza

I dispositivi Bluetooth si classificano in tre **classi di potenza**, in base alla potenza massima del segnale trasmesso, che determina la copertura della rete:

- la *classe di potenza 1* fissa una potenza massima in uscita di 20 dBm = 100 mW, che permette una copertura di circa 100 m;
- la *classe di potenza 2* ha una potenza massima in uscita pari a 4 dBm $\approx$ 2.5 mW, con una copertura di circa 10 m;
- la *classe di potenza 3*, infine, prevede una potenza massima di 0 dBm = 1 mW, che limita la copertura a circa 10 cm.

4 Tipi di link

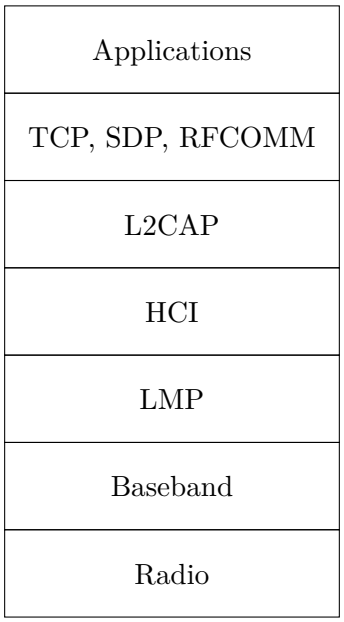
Tra il master e gli slave di una piconet possono essere stabiliti due diversi tipi di link: **SCO** e **ACL**.

- Un link SCO è un collegamento di tipo point-to-point tra il master e un singolo slave nella piconet, che fa uso del canale radio all'interno di time slot riservati, e può quindi essere considerato una connessione a commutazione di circuito.
- Un link ACL è invece un collegamento point-to-multipoint tra il master e tutti gli slave di una piconet. Per questo link non vengono riservati time slot, quindi la connessione realizzata è una a commutazione di pacchetto. I pacchetti ACL non sono indirizzati verso uno specifico slave, ma sono invece leggibili da ogni slave (cioè sono di fatto pacchetti broadcast).

Sia il master che gli slave possono partecipare contemporaneamente a un link SCO e un link ACL (ad esempio, si potrebbe utilizzare un link ACL per inviare informazioni di controllo a tutti gli slave nella piconet, e un link SCO per scambiare dati con uno specifico slave). Non possono invece essere stabiliti contemporaneamente più link per tipo nella stessa piconet, perché il master è in grado di gestire al massimo un link SCO e un link ACL.

5 Pila protocollare

Le reti Bluetooth utilizzano una pila protocollare (*Bluetooth protocol stack*) che è diversa dalla pila TCP/IP:



- Il livello fisico, chiamato semplicemente livello **radio** per via dell'unico mezzo fisico previsto, definisce i requisiti dei dispositivi ricetrasmittenti (transceiver).
- Il livello **baseband**, al quale si trova il protocollo *link controller*, gestisce i link ACL e SCO, la creazione della piconet, la selezione dei salti di frequenza e la correzione degli errori.
- **LMP**, *Link Management Protocol*, gestisce principalmente il setup del link e l'**autenticazione**.[1]
- *HCI*, *Host Controller Interface*, fornisce al livello superiore un'interfaccia di comando per il baseband controller e il link manager.

[1] L'autenticazione è l'accertamento dell'identità degli attori della comunicazione, ed è uno dei requisiti fondamentali della sicurezza.

- *L2CAP*, *Logical Link Control And Adaptation Protocol*, fornisce ai livelli superiori dei servizi di trasporto dati connection-oriented e connectionless.
- *RFCOMM* implementa un'emulazione delle porte seriali sopra il livello L2CAP.
- **SDP**, *Service Discovery Protocol*, permette di specificare quali servizi siano attivi e determinare le loro caratteristiche. Così, mediante un'operazione di *binding*, un dispositivo può trovare un servizio che soddisfi i propri requisiti.

6 Creazione della piconet

Per definizione, il master è il dispositivo che inizia la creazione della piconet, cioè la connessione verso uno o più slave. Una volta creata la piconet, i ruoli di master e slave possono però essere scambiati.

Un dispositivo Bluetooth può trovarsi in due stati principali: *stand-by* e *connessione*. Il passaggio dallo stato di stand-by a quello di connessione avviene tramite 7 sotto-stati: page, page scan, inquiry, inquiry scan, master response, slave response e inquiry response.

6.1 Procedura di inquiry

1. Un dispositivo che vuole scoprire altri dispositivi (il master) entra nello stato di **inquiry**, mentre un dispositivo che vuole essere scoperto entra nello stato di **inquiry scan**.
2. Il dispositivo che si trova nello stato di inquiry invia in broadcast (quindi su un link di tipo ACL) un **inquiry message**. Esso non contiene informazioni sul dispositivo che l'ha inviato, se non al più la classe di potenza a cui esso appartiene.
3. I dispositivi in stato di inquiry scan possono opzionalmente rispondere all'inquiry message con un messaggio di **inquiry response**. Il dispositivo in inquiry colleziona queste risposte, acquisendo così gli indirizzi e i clock di tutti i dispositivi che rispondono.
4. Infine, i dispositivi passano allo stato di connessione, completando la creazione della piconet. Successivamente, come già detto, il ruolo di master potrebbe passare a un dispositivo diverso da quello che ha iniziato la procedura.

Durante questa procedura, l'accesso al canale avviene su 32 frequenze appositamente riservate, secondo una sequenza di salto ben nota.

7 Confronto tra Bluetooth e Wi-Fi

Le tecnologie Bluetooth (802.15) e Wi-Fi (802.11) presentano numerose differenze, tra cui alcune delle principali sono:

- Accesso: nel Bluetooth può essere punto-punto (SCO) o punto-multipunto (ACL), mentre nel Wi-Fi è sempre punto-punto.
- Frequenza radio: il Bluetooth opera a 2.4 GHz, mentre il Wi-Fi può operare sia a 2.4 GHz che a 5 GHz.
- Frequenza di cifra: 1 Mbps per il Bluetooth (nelle sue prime versioni), rispetto ad esempio a 11 Mbps per l'802.11b.
- Tecnica spread spectrum: il Bluetooth usa FHSS (frequency hopping), mentre il Wi-Fi può usare FHSS o, più comunemente, DSSS (direct sequence).
- Profilo (funzione dei dispositivi connessi): il Bluetooth supporta molti diversi tipi di dispositivi, mentre in una rete Wi-Fi si hanno solo stazioni LAN e access point.
- Autenticazione: il Bluetooth ha sempre previsto l'autenticazione dei dispositivi che si connettono alla rete, mentre per il Wi-Fi questa è stata aggiunta solo con lo standard 802.11i.
- Copertura: per il Bluetooth è tipicamente minore di 10 m, mentre per il Wi-Fi può superare i 100 m.
- Gestione della mobilità: nel Bluetooth è responsabilità del master, mentre nel Wi-Fi se ne occupa la stazione mobile.