Fonte: www.digitalbirmingham.co.uk

Zigbee: il wireless emergente

Il protocollo Zigbee si adatta a un ampio range di applicazioni, dalla domotica alla telegestione, dall'automazione alla gestione dei consumi energetici

Stefano Maggi

Non è certa l'origine del nome Zigbee, anche se alcuni sostengono che derivi dal movimento a 'zig-zag' delle api, che, passando di fiore in fiore, si trasmettono l'una l'altra l'informazione su dove trovare cibo. Zigbee è infatti un protocollo wireless che consente lo scambio di informazioni fra i nodi di una rete. Le reti wireless sono la naturale evoluzione di quelle 'wired', ossia cablate, e si sono sviluppate soprattutto a partire della metà degli anni '80 sotto il nome di Wlan, Wireless local area network.

Con la diffusione di dispositivi mobili di differente tipologia, poi, si è fatta via via più evidente la necessità di mettere a punto reti che fossero 'concentrate' attorno alla persona, estese per pochi metri in tutte le direzioni. Tali reti hanno quindi preso il nome di Wpan, Wireless personal area network, e sono regolate dallo standard Ieee 802.15. In particolare, sono stati definiti tre differenti classi di Wpan, sulla base della velocità di trasmissione, del consumo di energia e della qualità del servizio (QoS): Wpan con data rate elevato (Ieee 802.15.3), indicate per applicazioni multimediali che richiedono un elevato QoS; Wpan con data rate intermedio (Ieee 802.15.1/Bluetooth), adatte a una grande varietà di compiti, tra cui telefonini e cellulari, PDA e, in generale, applicazioni idonee alla comunicazione vocale (auricolari per cellulari); infine, Wpan con data rate basso (Ieee 802.15.4/LR-Wpan), particolarmente indicato in campo industriale, home automation, medicale e, in genere, per tutte quelle applicazioni che necessitano di un basso costo, di un basso consumo di potenza e di una velocità di trasmissione non elevata. In quest'ultima categoria rientra lo standard Zigbee.

Zigbee Alliance e Ieee 802.15.4

L'ultima tipologia di Wpan descritta nasce dallo sforzo congiunto di Ieee e della Zigbee Alliance. Quest'ultima individua un consorzio di oltre 80 società, in continuo aumento, il cui obiettivo è assicurare a breve la diffusione di Zigbee in un'ampia fetta del mercato wireless. La speranza dei promotori dello standard è realizzare chip sempre più integrati, conseguentemente più economici, che siano in grado di implementare l'intero protocollo. Chiaramente la sfida non è semplice, poiché si tratta di un mercato in gran parte saturato da tecnologie come Wifi (Ieee 802.11), Bluetooth, UWB e WirelessUSB.

I dispositivi Zigbee sono in grado di trasmettere fino a una distanza di circa 70 m in linea d'aria senza ostacoli e di circa 30 m all'interno di edifici, a seconda delle interferenze RF nell'ambiente in cui si trovano e del consumo di potenza richiesto dall'applicazione. Essi operano all'inter-

no di bande di frequenza libere da licenza, come ISM 2,4 GHz, UHF 915 MHz negli Stati Uniti e UHF 868 MHz in Europa. La velocità di trasferimento dati varia in base alla frequenza e va da un minimo di 20 kbps a 868 MHz a un massimo di 250 kbps a 2,4 GHz.
Il lavoro della 'task force' di Zigbee Alliance e Ieee è consistito nella definizione dell'intero stack del protocollo; in particolare, Ieee ha sviluppato i due layer più bassi, fisico e MAC, mentre l'Alleanza ha definito i layer superiori, cioè quello di rete e di applicazione, in maniera tale da garantire l'interoperabilità tra i prodotti di diverse case costruttrici (definizione dei profili).

Zigbee e il protocollo Ieee 802.15.4

Lo standard Ieee 802.15.4, approvato nell'estate del 2003, definisce il protocollo di trasmissione a basso livello tramite comunicazione radio tra i diversi dispositivi che rientrano in una PAN (Personal Area Network). Le Wpan (Wireless PAN) vengono utilizzate per distribuire informazioni su distanze relativamente brevi e senza cavi di collegamento; le connessioni effettuate attraverso le Wpan riguardano piccoli ambienti e infrastrutture, il che favorisce lo sviluppo di soluzioni poco costose ed energeticamente efficienti per un'ampia gamma di applicazioni.
Lo standard definisce, più in particolare, le specifiche del livello fisico (PHY) e datalink (MAC), al fine di garantire una modalità di connessione wireless a basso data rate tra dispositivi fissi, portatili o mobili, che necessitano di un basso consumo di potenza, ovvero lunga durata delle batterie a bordo e che tipicamente lavorano in uno spazio operativo (POS-Personal Operating Space) dell'ordine di qualche decina di metri.
Il data rate deve essere sufficientemente elevato, in modo da consentire la connettività di periferiche interattive largamente diffuse, come quelle per PC, al contempo, però, vi deve essere la possibilità di ridurlo fino ai livelli tipici richiesti da sensori e da applicazioni orientate al controllo e all'automazione delle infrastrutture. Si perviene quindi, a una LR-Wpan (Low Rate Wpan), ovvero una rete di comunicazione semplice e a basso costo selettivamente orientata verso applicazioni a basso consumo e a throughput (quantità di informazione trasmessa) non elevato, principalmente caratterizzata da data rate di 250 kbps, 40 kbps e 20 kbps. A ciò si aggiungono operabilità in configurazione a stella o peer-to-peer, 16 bit o 64 bit d'indirizzo allocati, accesso al canale in modalità Csma-CA, completa definizione del protocollo per trasferimento dei dati.
E ancora basso consumo di energia, indicazione della qualità del canale e 16 canali nella banda attorno a 2,4 GHz, dieci canali nella banda attorno a 915 MHz, un canale a 868 MHz.

Diverse topologie di rete

Una LR-Wpan può includere due diversi tipi di dispositivi: FFD (Full Function Device) e RFD (Reduced Function Device). Un dispositivo del primo tipo può operare all'interno della rete secondo tre modalità: funzionando da coordinatore della rete, da coordinatore semplice, o da terminale di comunicazione. Un dispositivo FFD (coordinator e router) può dialogare con altri dispositivi di entrambe le categorie, mentre un RFD (end device) può comunicare direttamente solo con un FFD (si veda figura 2). L'inclusione di terminali RFD all'interno della rete è orientata ad applicazioni estremamente semplici, come interruttori di luce o sensori a infrarossi, che non necessitano dell'invio di grosse quantità di dati e possono, quindi, essere supportate attraverso minime risorse energetiche e limitate capacità di memoria.

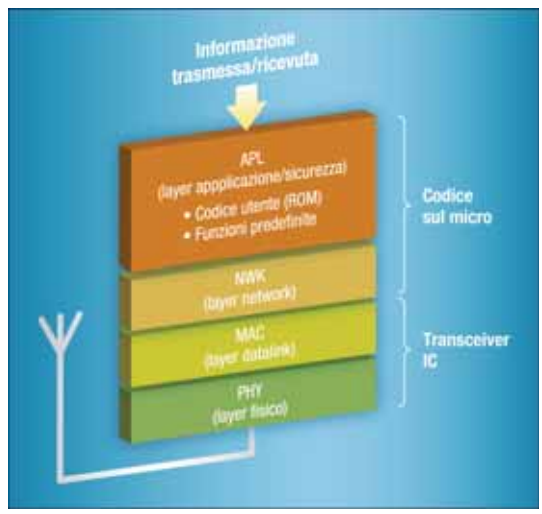

Fig. 1: I vari layer dello stack Ieee 802.15.4 Zigbee

Una Wpan è costituita da un minimo di due dispositivi operanti in una stessa POS; in ciascuna rete, uno solo di essi può configurarsi come 'PAN coordinator', che si occupa di iniziare, gestire e terminare la comunicazione tra le diverse periferiche. A seconda della particolare applicazione, una LR-Wpan può configurarsi in varie topologie (illustrate in figura 3).
In ogni caso, ciascun dispositivo interno alla rete possiede un indirizzo esteso a 64 bit, che può essere direttamente impiegato per la comunicazione; in alternativa si utilizza un indirizzo ridotto, attribuito dal PAN coordinator ogni volta che il dispositivo viene da esso rilevato.
Nella topologia a stella ciascun dispositivo può comunicare solo con il coordinatore, che controlla e gestisce ogni tipo di comunicazione all'interno della PAN e tipicamente è dotato di un'alimentazione fissa, mentre gli altri dispositivi sono dotati di batteria a bordo oppure alimentati da fonti energetiche innovative (mini pannelli solari, sistemi piezoelettrici ecc.). La topologia peer-to-peer differisce dalla precedente in quanto ciascun dispositivo può comunicare direttamente con un altro interno alla rete, a patto che questo rientri nella sua area operativa di copertura, senza ricorrere alla mediazione del coordinatore. Una tale topologia, quindi, si presta alla formazione di reti di comunicazione decisamente complesse, che coinvolgono potenzialmente un numero elevato di dispositivi. Essa è tipicamente rivolta ad applicazioni come il controllo e il monitoraggio industriale e ambientale, attraverso reti di sensori wireless, in aggiunta all'utilizzo in domotica.
La modalità di formazione di una PAN rientra nel livello di rete, o network layer. Nella formazione di una rete a stella ogni dispositivo FFD, dopo essersi attivato, può creare una propria rete diventandone un coordinatore 'locale'. Tutte le

reti a stella operano indipendentemente dalle reti simultaneamente attive, in quanto ciascuna di esse è contraddistinta da un identificatore PAN scelto dal coordinatore, in maniera tale da evitare conflitti già precedentemente presenti entro lo spazio operativo. Una volta scelto l'identificatore, il coordinatore può annettere alla propria PAN altri

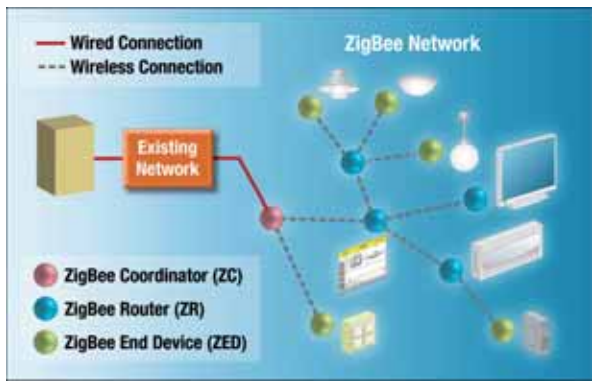

Fig. 2: Dispositivi di una rete Zigbee

dispositivi, siano essi di tipo FFD o RFD.
In una rete peer-to-peer, invece, ogni dispositivo può configurarsi come PAN semplicemente per essere il primo a comunicare su uno stesso canale. Un esempio di rete complessa fondata su una topologia peer-to-peer è il 'cluster-tree' (si veda figura 3). In questo caso, ogni dispositivo della rete può fungere da coordinatore, fornendo servizi ad altri dispositivi o coordinatori, anche al di fuori della propria sfera d'influenza. Soltanto uno di questi coordinatori locali, però, può configurarsi come coordinatore PAN, quello tipicamente dotato di maggiori risorse anche a livello computazionale.
Attraverso diversi nodi coordinatori (di questo tipo) risultano potenzialmente configurabili delle reti a struttura multicluster, il cui principale vantaggio è legato alla maggiore estensione della superficie coperta e al maggiore numero di nodi interagenti. Le caratteristiche di auto-configurabilità e d'interoperabilità permettono alla rete di modificarsi al variare delle condizioni operative e di auto-configurarsi, scegliendo dinamicamente i nodi e gestendone la connettività, a seconda dell'ambiente applicativo.
L'utilizzo di tecnologie magliate permette di massimizzare l'affidabilità complessiva della rete, garantendo la possibilità di instradare l'informazione su percorsi diversi. Inoltre, attraverso il processo di trasferimento dell'informazione 'hop-by-hop' tra i nodi, è possibile arrivare a un'estesa copertura del territorio, anche avendo a disposizione singoli collegamenti a portata limitata.

Sicurezza e affidabilità

Uno dei principali vantaggi di Zigbee rispetto ad altre tecnologie wireless di prossimità è l'elevato livello di sicurezza che viene supportata a livello di collegamento fra due nodi di rete, nonché a livello rete e a livello applicativo. I servizi di sicurezza forniti da Zigbee includono meccanismi e protocolli per la generazione e il trasporto sicuro delle chiavi, per la protezione dei frame e per la gestione dei dispositivi. In particolare, la protezione dei dati è garantita da algoritmi di crittografia avanzati (AES a 128 bit) e da meccanismi d'integrità e di autenticazione per la protezione da eventuali attacchi provenienti da dispositivi non autorizzati, che tentano di accedere alla rete o al contenuto informativo trasmesso. È definito anche un concetto di 'trust center' per la gestione centralizzata della sicurezza, a livello di politiche e di aggiornamento delle chiavi.
Secondo lo standard, un nodo Zigbee può operare sia in modalità sicura, sia non sicura. Ovviamente, non implementando la sicurezza dei dati si ottiene un codice più leggero.

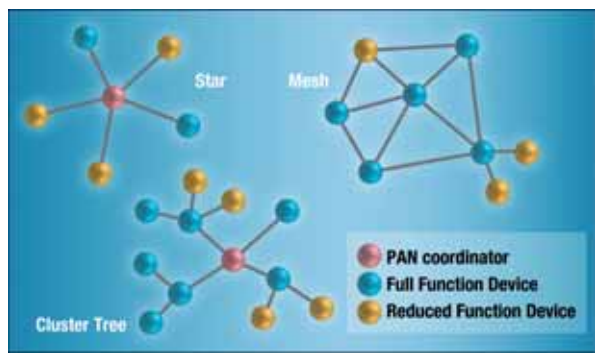

Fig. 3: Principali topologie di rete previste dallo standard Ieee 802.15.4

Sono previsti quattro servizi di sicurezza, di cui il primo è il controllo degli accessi, per cui ogni dispositivo deve mantenere una lista di tutti i potenziali trasmettitori. In questo modo, un dispositivo non autorizzato non può accedere a una rete Zigbee. Il secondo servizio di sicurezza riguarda la codifica dei dati, per cui i dati non sono trasmessi in chiaro, ma codificati mediante una chiave di crittografia posseduta solo dai componenti di rete. Il terzo meccanismo di controllo è definito come rinnovo sequenziale, ossia ogni frame viene confrontato con il precedente per evitare che vi siano ripetizioni. Infine, viene controllata l'integrità dei frame: sui bit di tutto il frame viene calcolato un 'check', tramite il quale è possibile risalire a modifiche del frame da parte di nodi non autorizzati. Per garantire l'interoperabilità tra prodotti di fornitori diversi, la Zigbee Alliance prevede la creazione di profili pubblici applicativi standard. Il primo profilo che è stato standardizzato è relativo all'automazione domestica, o 'home automation', per il controllo degli impianti d'illuminazione, riscaldamento e condizionamento e di altri sensori/attuatori utilizzati in ambito residenziale. Altri profili applicativi già standardizzati sono quelli relativi ai servizi 'smart energy', per il controllo energetico e la gestione efficiente dei consumi, e 'commercial building automation', ossia automazione industriale. Sono invece in fase di standardizzazione i profili per 'telecom application', telecomunicazioni, e 'personal healthcare', in ambito sanitario/medico. ■