In campo ‘senza fili’

Quali requisiti deve presentare un protocollo wireless per essere adeguato all’uso in applicazioni industriali?

Riduzione dei costi e migliore manutenibilità sono i fattori primari che hanno spinto l’adozione delle reti wireless in ambito industriale

Fonte: www.networkswork.com

Mariano Severi

La rivoluzione wireless che ha caratterizzato le applicazioni consumer negli ultimi anni ha ormai raggiunto anche il settore industriale. La riduzione dei costi e la migliore manutenibilità della rete sono sicuramente i fattori trainanti. Come termine di confronto, basti pensare che, considerando le perdite legate all’inoperatività dell’impianto durante le necessarie operazioni, l’installazione di una connessione cablata può arrivare a costare fino a 10 mila euro per metro. La tecnologia wireless usa invece l’etere come mezzo di trasmissione, il che, in senso lato, non costa. Quali sono però i requisiti che deve rispettare un protocollo wireless per essere adeguato ad applicazioni in ambito industriale?

Caratteristiche imprescindibili

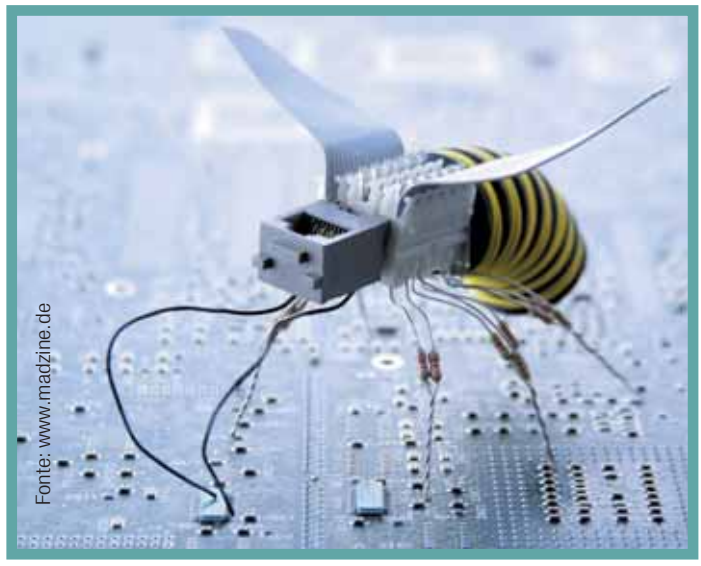
L’affidabilità della connessione è sicuramente un punto cruciale, tanto più se si considera che la trasmissione radio è più soggetta a errori rispetto a quella via cavo. Proprio per questo motivo, del resto, la tecnologia wireless viene impiegata nel settore industriale principalmente in applicazioni di allarme e monitoraggio, non per il controllo di processi critici. Per mitigare il problema e fornire un servizio affidabile, in ogni caso, la maggior parte dei protocolli impiega uno schema del tipo ‘listen before send’, ossia ‘ascolta prima di trasmettere’, in modo da favorire l’interoperabilità con altre reti eventualmente presenti nella stessa area, e un meccanismo ‘send/acknowlede/retry’, cioè ‘spedisci/convalida/riprova’, che consente di verificare la corretta ricezione del messaggio al nodo ricevitore.
Altro aspetto importante è quello della sicurezza della comunicazione, intesa nelle diverse accezioni di integrità, autenticazione e confidenzialità delle informazioni trasmesse; l’accesso all’etere non può essere bloccato, quindi la rete può essere soggetta a intrusioni non autorizzate. Molti dei protocolli supportano schemi di crittografia delle informazioni per assicurare la privacy della comunicazione; lo standard AES con chiavi a 128 bit è la soluzione più diffusa.
L’assenza di una connessione cablata, poi, comporta il più delle volte la necessità di alimentare i nodi a batteria o con sorgenti alternative (luce solare, vibrazioni, differenze di temperatura). L’adozione di soluzione di risparmio energetico diventa quindi cruciale; nel caso dell’alimentazione a batteria, il sistema deve disporre di un’autonomia dell’ordine di un anno almeno, per non incidere negativamente sui costi di manutenzione della rete.
Non è invece un fattore critico la capacità di trasmissione dati. Nelle applicazioni più tipiche, di gestione allarmi, monitoraggio della temperatura, lettura di codici a barre, controllo dello stato delle macchine, infatti, il traffico di un singolo nodo non supera l’ordine delle decine di kB al giorno.
Vediamo ora nello specifico quali standard hanno saputo meglio adattarsi a questi requisiti, trovando maggiore diffusione nel settore industriale.

Zigbee

Protocollo per reti mesh wireless caratterizzate da basso volume di dati, costi contenuti e ridotta dissipazione di potenza, Zigbee è utilizzato principalmente per applicazioni di home e building automation, hospital care e telecomunica-

zioni. Lo standard è proprietario, ma è disponibile gratuitamente una licenza per scopi non commerciali. Si basa sullo standard Ieee 802.15.4, utilizzando schemi di modulazione Bpsk nella banda ISM a 868/915 MHz e Qpsk in quella a 2,4 GHz. Il raggio di copertura per un nodo è tipicamente compreso tra 10 e 75 m, con una potenza del segnale di 1 mW (0 dBm). La più recente specifica Zigbee Pro supporta trasmissioni su fino a 1.500 m.

Una rete Zigbee consiste di un insieme di Zigbee End Device (ZED), che comunicano con lo Zigbee Coordinator (ZC) o gli Zigbee Router (ZR). Questi ultimi sono nodi in grado di eseguire una generica applicazione utente e di instradare i messaggi attraverso la rete. Non è previsto, come accade in altri protocolli, che un nodo ZED operi come ponte per messaggi di dispositivi finali a esso contigui. Uno ZC, infine, è un nodo unico nella rete, che gestisce l'associazione di ZED e ZR a questa, oltre a essere depositario delle chiavi di sicurezza usate nella comunicazione. Sono supportate topologie di rete di tipo a stella e ad albero; nelle prime il nodo centrale è lo ZC. Il protocollo di costruzione della rete si basa su recenti algoritmi ('ad hoc on demand distance vector', neuRFon) per sistemi 'low speed'. La ricerca di un nodo può essere basata su comunicazione unicast o broadcast, a seconda delle informazioni disponibili.



Destinato a reti mesh wireless, caratterizzate da basso volume di dati, costi contenuti e ridotta dissipazione di potenza, il protocollo Zigbee si basa sullo standard Ieee 802.15.4

Sono supportate configurazioni di reti 'beacon' e 'non beacon enabled'. In quest'ultimo caso reti, il meccanismo di accesso al mezzo fisico è di tipo Csma/CA ('listen before send'); alcuni nodi sono costantemente attivi, mentre altri sono spenti, con un consumo di potenza quindi asimmetrico all'interno della rete. Un tale schema è favorito da un tempo di attivazione dei nodi piuttosto breve, inferiore tipicamente a 15 ms. Nelle reti 'beacon oriented', invece, utilizzate soprattutto in applicazioni più critiche, che richiedano bassa latenza nella trasmissione, è prevista la definizione di GTS (Guaranteed Time Slot), che evitano a priori il verificarsi di conflitti definendo precise finestre temporali di tra-

LO STANDARD IEEE 802.15.4

Ieee 802.15.4 è uno standard che copre i livelli fisici e di accesso al mezzo (MAC) definiti dal protocollo OSI nella realizzazione di reti Wpan. Definisce un'architettura a basso costo e ridotta dissipazione di potenza per la comunicazione tra dispositivi ovunque ubicati. È adottato da Zigbee, WirelessHart e MiWi e può essere usato con sistemi 6LoWpan per costruire soluzioni Wireless Embedded Internet.

Il livello fisico definisce le caratteristiche della trasmissione RF, gli algoritmi di selezione dei canali e le funzioni di gestione della potenza. Prevede trasmissioni nelle tre bande non soggette a licenza a 868,0-868,6 MHz, 902-928 MHz e 2.400-2.483,5 MHz. Le prime due sono usate rispettivamente in Europa e negli Stati Uniti, mentre la terza è adottata più o meno universalmente. La revisione originale pubblicata nel 2003 adotta uno schema di modulazione di tipo Dsss (Direct sequenze spread spectrum), che consente di ottenere data rate di trasmissione tra 20 e 40 kbps nelle bande a 8/915 MHz e 250 kbps in quella a 2.450 MHz. La revisione del 2006 ha successivamente esteso lo standard introducendo i diversi schemi di modulazione di tipo Bpks (Binary phase shift keying), Oqpsk (Offset quadrature phase shift keying) e ASK (Amplitude Shift Keying), consentendo così di raggiungere data rate tra 100 e 250 kbps, anche alle frequenze di 868/915 MHz. Prevede inoltre la possibilità di switching dinamico tra i vari livelli fisici. Ulteriori due livelli fisici sono stati introdotti dalla specifica Ieee 802.15.4 pubblicata nell'agosto 2007, che ha introdotto gli schemi CSS (Chirp Spread Spectrum) nella banda ISM e UWB (Ultra WideBand) nelle regioni al di sotto di 1 GHz, tra 3 e 5 GHz e tra 6 e 10 GHz. L'accesso al mezzo fisico è di tipo Csma/CA. Ai fini della sicurezza della comunicazione, il MAC contempla la definizione di liste di controllo di accesso per la restrizione della trasmissione a un gruppo di nodi autenticati. Il protocollo supporta configurazioni di rete di tipo 'peer to peer' e a stella. La comunicazione segue in genere uno schema di tipo 'request confirm/indication response' ed è previsto un meccanismo di ritrasmissione automatica del messaggio basato su timeout per la ricezione della conferma.

Standard aperto pubblicato da Hart Communications Foundation, WirelessHart porta il protocollo Hart nel mondo wireless

smissione per i nodi. Tali finestre sono definite sulla base dei messaggi periodici inviati dai router. L'intervallo di beacon varia, ad esempio, tra 15.26 ms e 251.65824 in una comunicazione a 250 kbps. La sicurezza della rete è assicurata da un meccanismo di cifratura mediante chiavi a 128 bit. È possibile definire una chiave per l'intera rete o per ogni singolo link. In questo secondo caso, le chiavi sono derivate da una 'master key' che ne controlla la corrispondenza con il canale di comunicazione; possono essere acquisite mediante pre-installazione, accordo o trasporto. Un nodo della rete è designato come 'trust center' e demandato alla distribuzione delle chiavi; gli altri nodi accetteranno soltanto messaggi originati con chiavi fornite da esso.

WirelessHart

Standard aperto, pubblicato nel 2007 dalla HCF (Hart Communications Foundation), WirelessHart porta il protocollo Hart nell'ambito del wireless. Adotta il livello fisico definito dallo standard Ieee 802.15.4, utilizzando modulazione Dsss nella banda a 2,4 GHz. Basandosi su un protocollo di comunicazione piuttosto diffuso (esistono oltre 24 milioni di dispositivi Hart nel mondo) rappresenta una soluzione stabile, correntemente supportata, caratterizzata da tempi d'integrazione ridotti e rischi contenuti.

Una rete WirelessHart consiste di un insieme di nodi wireless connessi tra loro mediante gateway che ne gestiscono la comunicazione con le applicazioni host; un manager definisce lo schedule delle trasmissioni, controlla il routing dei messaggi e monitora lo stato di attività della rete. La configurazione di rete è di tipo mesh ridondata, con ogni nodo in grado di funzionare come router per i messaggi dei nodi contigui. Tale soluzione estende l'area coperta della rete senza necessità di incrementare la potenza del segnale e assicura maggiore affidabilità, consentendo diversi cammini alternativi per la trasmissione di un messaggio da e verso i gateway. Per ridurre i problemi d'interferenza adotta, come tutte le altre tecnologie che operano nella banda ISM, tecniche di 'channel hoping', variando il canale di comunicazione tra i 16 diversi definiti dal livello fisico. La connessione tra i nodi è stabilita entro finestre temporali fisse e predefinite, il che garantisce una comunicazione non soggetta a collisioni, scalabile ed efficiente in potenza. La configurazione della rete è definita in modo da assicurare appropriati QoS per i diversi messaggi.

Per quanto concerne gli aspetti di sicurezza della comunicazione, lo standard WirelessHart adotta uno schema di cifratura dei messaggi con chiavi a 128 bit e a rotazione e prevede codici di verifica dell'integrità delle informazioni per ogni messaggio. L'accesso alla rete avviene mediante un meccanismo di autenticazione. L'adozione, come abbiamo visto, di algoritmi di channel hopping nella selezione del canale rende poco efficaci gli attacchi che tendano a impedire la comunicazione saturando un certo canale.

La definizione di uno schema di comunicazione sincrono consente la realizzazione di soluzioni a bassa dissipazione di potenza. I nodi, o al limite la sola sezione a radiofrequenza, possono eventualmente essere spenti nei periodi in cui non è previsto che trasmettano. Il protocollo, poi, prevede interessanti capacità di risparmio energetico nella gestione stessa della comunicazione. Tra queste, ad esempio, la funzionalità di 'Smart Data Publishing' consente la trasmissione dei dati solo in presenza di variazione delle condizioni di processo o su esplicita richiesta dell'utente ed eredita una modalità di comunicazione a 'burst' propria dal protocollo Hart. I servizi di 'Notification by Exception' consentono infine di notificare all'utente una richiesta d'intervento per un nodo o l'occorrenza di certi eventi, evitando la necessità di interrogare costantemente i nodi stessi per rilevare lo stato di salute complessivo della rete.

ISA 100.11a

Standard aperto multi-funzionale per reti wireless di sensori e attuatori, ISA 100.11a è stato ufficialmente riconosciuto con una specifica approvata nel maggio 2009, rilasciata solo di recente al pubblico. Adotta il livello fisico a 2,4 GHz definito nella revisione del 2006 dello standard Ieee 802.15.4, con modulazione di tipo Dsss. La scelta di un solo livello fisico favorisce l'interoperabilità tra i produttori di apparecchiature, al fine di semplificare la diffusione dello standard. Impiega uno schema di channel hopping

Fra i protocolli nati per applicazioni consumer, ma largamente impiegati anche in ambito industriale figura Bluetooth

analogamente a quello previsto dal protocollo WirelessHart; la stessa tecnica, del resto, è usata nelle apparecchiature militari per migliorare l'affidabilità della comunicazione in condizione di congestione del mezzo fisico. L'accesso a quest'ultimo è deciso sulla base di uno schema Tdma (Time divsion multiplex access) nelle modalità 'slotted channel hopping', 'slow channel hopping' e 'ibrida', che consentono di definire 'time slot' flessibili e configurabili; lo schema adottato all'interno del protocollo WirelessHart, descritto in precedenza, invece, si basa su finestre temporali di durata fissa di 10 ms. Il formato dei frame è in accordo alle raccomandazioni Ietf RFC 4944 (IP based); il livello di rete dello standard definisce i servizi d'indirizzamento e routing, oltre alle procedure di internetworking. Sono supportate configurazioni di rete a stella, adottate soprattutto in applicazioni critiche che richiedano tempi di risposta ridotti, e mesh, caratterizzate da maggiore affidabilità e tolleranza ai problemi d'interferenza. Diversamente dalle reti 'multi hop', che tendono a ripetere uno stesso messaggio più volte, soprattutto nelle strutture di dimensioni più ampie, i sistemi ISA 100.11a tentano di inoltrare quanto prima il messaggio a una dorsale di distribuzione primaria a elevata qualità, riducendo drasticamente l'uso del canale radio. Ne consegue una sostanziale riduzione della potenza dissipata, fondamentale soprattutto nelle applicazioni con alimentazione a batteria. L''application sublayer' definisce i servizi che realizzano l'integrazione dei nodi con le applicazioni host mediante gateway. Fondamentali sono le funzionalità di 'tunneling' rese disponibili per la traslazione di protocolli generici. Questi vanno da un semplice 'basic tunneling', che consente di inglobare i dati utente generici in un frame ISA 100.11a e trasportarli tra due nodi utilizzando il livello fisico del protocollo, a soluzioni complete di 'extended tunneling', che permettono, ad esempio, di connettere mediante gateway a una rete ISA 100.11a un sistema di controllo per bus Devicenet, Profibus, FF, Hart o anche proprietario. Per quanto concerne gli aspetti di sicurezza, anche ISA 100.11a prevede la cifratura delle informazioni ai livelli 'data link', per ogni hop della rete, e di 'trasporto', mediante chiavi simmetriche e non (pubbliche). L'autorizzazione della comunicazione è basata sull'identità dei nodi e uno schema di relazioni tra essi definito all'interno della rete.

Le alternative: WiFi e Bluetooth

Esistono anche alcuni protocolli nati principalmente per applicazioni consumer, che vengono utilizzati anche in ambito industriale. WiFi, ad esempio, è un protocollo per reti Wlan (Wireless local area network). Il livello MAC è definito dalla specifica Ieee 802.11. Opera nelle bande a 2,4 GHz e 5 GHz, con modulazione Dsss e Ofdm. Assicura un troughput tipico compreso tra 27 Mbps su distanze fino a 30 m (per la specifica 802.11a) e 144 Mbps su fino a 180 m (per la revisione 802.11n, che adotta uno schema 'Mutiple input multiple output'). Il livello LLC è specificato dallo standard Ieee 802.2. Gli aspetti di sicurezza sono invece definiti dai protocolli WEP (Wired Equivalent Privacy), ormai superato, e WAP (WiFi Protected Access). Bluetooth, invece, è uno standard di comunicazione a corto raggio per reti Wpan (Wireless personal area network). Definisce uno stack di protocolli che vanno dal livello LMP (Link Management Protocol) a quello Avdtp (Audio/visual data transport protocol). Adotta, nella soluzione base, modulazione Gfsk (Gaussian frequency shift keying) nella banda ISM, dove definisce fino a 79 canali con larghezza di banda di 1 MHz; supporta fino a 1.600 variazioni di canale al secondo. La potenza di segnale è compresa tra 1 mW, per applicazioni di classe 3, e 100 mW, per applicazione di classe 1. Il data rate di trasmissione nominale è fino a 3 Mbps nella versione 2.0. Prevede uno schema di correzione degli errori nella comunicazione in banda base di tipo FEC (Forward Error Correction) 1/3 rate o ARQ (Automatic Repeat Request). Infine, implementa algoritmi basati sullo schema di cifratura a blocchi Safer+ nella gestione degli aspetti di confidenzialità del messaggio, autenticazione dei nodi e derivazione delle chiavi. ■