Uno sguardo alle più importanti tecnologie wireless

Andre Schmitz
Field applications engineer
Green Hills Software

Questo articolo fornisce una descrizione di diverse tecnologie - Wi-Fi, Bluetooth, NFC e così via – utilizzate per la comunicazione wireless e ne presenta alcuni scenari applicativi nell'ambito dei sistemi embedded

I moderni sistemi embedded sono spesso progettati per interfacciarsi in qualche modo con l'ambiente esterno. Queste interfacce possono essere utilizzate per controllare il sistema embedded, per ricevere da esso i dati di misura, oppure come mezzo di comunicazione. In passato, queste interfacce erano cablate, come accade ad esempio nel caso delle tecnologie CAN, Ethernet, USB o RS232. I moderni dispositivi tendono invece ad avere interfacce di tipo wireless, ad esempio basate su Wi-Fi, Bluetooth oppure NFC. Queste tecnologie hanno caratteristiche differenti per quanto riguarda portata, velocità di trasmissione e mobilità. Questo articolo fornisce una descrizione di diverse tecnologie nel settore della comunicazione wireless e ne presenta alcuni scenari applicativi nell'ambito dei sistemi embedded. Verrà inoltre prestata particolare attenzione alla realizzazione software dei relativi stack di protocollo e all'importanza della sicurezza.

Scenari applicativi

In futuro, lo scambio di dati da e verso un dispositivo embedded avverrà probabilmente attraverso un'interfaccia wireless. Un medico in ospedale porterà con sé un terminale elettronico per memorizzare le cartelle cliniche dei suoi pazienti. Questo terminale sarà sincronizzato con le stanze di degenza oppure con un server centrale, tramite collegamenti wireless. Saranno inoltre presenti sistemi di pagamento wireless, che naturalmente dovranno essere protetti da usi impropri e da intercettazioni illegali. Oggi è normale leggere email, accedere alla rete aziendale o navigare in Internet ovunque ci si trovi. Inoltre, nell'ambito della domotica, il numero dei cavi presenti nell'edificio può ridursi significativamente se molti dispositivi elettronici, lampade e interruttori verranno collegati sfruttando la tecnologia wireless. Dal punto di vista software è importante riuscire a integrare perfettamente e in modo affidabile questa tecnologia nel sistema embedded e impedire a chiunque un accesso non autorizzato alle informazioni confidenziali.

Specifiche

In quasi tutti i casi la trasmissione wireless è effettuata tramite radiazioni elettromagnetiche di diversa frequenza. L'interfaccia radio delle diverse tecnologie differisce nei seguenti parametri:

- Portata massima e velocità massima di trasmissione – definizione degli scenari possibili
- Potenza di trasmissione – ha effetto sulla durata delle batterie
- Mobilità – quanto velocemente può muoversi il terminale
- Duplex – a divisione di tempo oppure a divisione di frequenza
- Cifratura – sicurezza dalle intercettazioni
- Modulazione

Le potenzialità del terminale dipendono dall'hardware e dal software installato. Il terminale è l'oggetto in cui girano gli stack di protocollo in cui i dati vengono generati, ricevuti e immagazzinati e in cui risiede la robustezza del sistema. Ciò influenza non solo la "safety" (ossia il fatto che il sistema sia affidabile e stabile), ma anche l'effettiva "security" (sicurezza informatica) del sistema (ossia la capacità di resistere agli attacchi). Nessuno vorrebbe un sistema di pagamento senza contatto soggetto ad attacchi o veder finire le cartelle cliniche nelle mani di persone non autorizzate.
Un elemento chiave della sicurezza informatica è, naturalmente, la cifratura dei dati che viaggiano lungo l'interfaccia radio.

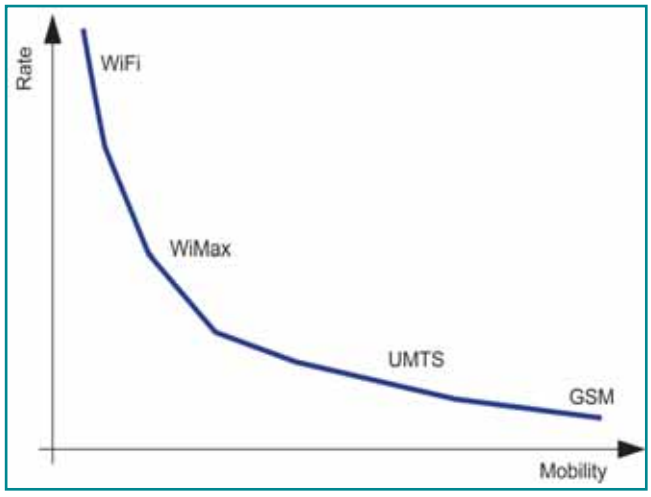

Fig. 1 - Velocità di trasmissione in funzione della mobilità nelle tecnologie wireless

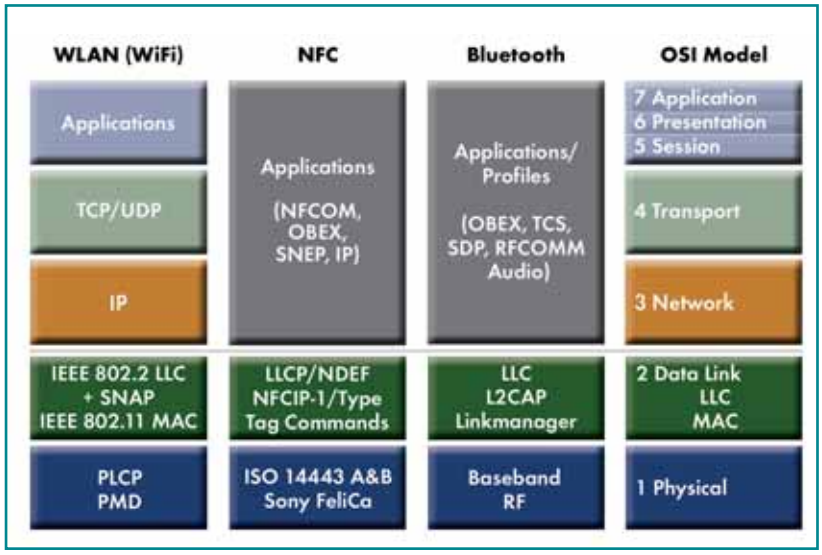

Fig. 2 - Confronto tra le diverse tecnologie wireless in relazione al modello OSI [4]

Tuttavia, ancora più importante è l'uso di sistemi di controllo degli accessi (autenticazione), di memorizzazione sicura dei dati, di moduli software ben separati e, se necessario, l'impiego della virtualizzazione per integrare software già esistenti e potenzialmente non sicuri. Infine, occorre mantenere il consumo di potenza entro limiti ragionevoli.

PAN – Personal Area Network

Nelle comunicazioni su brevi distanze, bande di frequenza e intervalli di potenza vengono utilizzati per trasmettere segnali alla distanza di qualche metro. Si tratta principalmente di bande di frequenza soggette a licenza, disponibili a basso costo.

L'impiego della tecnologia a infrarossi (IrDA) nella trasmissione dei segnali sta diventando obsoleto. Tecnologie più interessanti sono Bluetooth (IEEE 802.15.1) e NFC – Near Field Communication (ISO/IEC 14443), che verrà descritta più avanti in questo articolo. Oltre a queste, vi sono molte altre tecnologie, più o meno specifiche per determinate applicazioni, come ad esempio ONE-NET, Z-Wave o Wireless USB.

Uno standard piuttosto interessante è ZigBee (basato su IEEE 802.15.4), principalmente utilizzato nel settore degli elettrodomestici, della videosorveglianza e della domotica. ZigBee punta a realizzazioni a basso costo, con una banda limitata (20-250 kbit/s), una portata rispettabile (10-75 m) e un consumo di potenza molto basso (1 mW).

LAN – Local Area Network

Per portate fino a qualche centinaio di metri, vi sono due standard molto conosciuti. Uno è la tecnologia wireless LAN (WiFi - IEEE 802.11a, b, g, n) che può essere considerata la sostituzione indispensabile dell'Ethernet cablata. L'altro è lo standard DECT (ITU IMT-2000). È noto nella telefonia wireless e può anche essere utilizzato nelle reti locali.

WAN – Wide Area Network

Nel caso di tecnologie che coprono diversi chilometri, le bande di frequenza utilizzate devono di norma essere ottenute tramite una licenza.

Un'eccezione è la cosiddetta Muni-WiFi, che impiega una rete di punti di accesso WiFi distribuiti per impostare una WAN urbana virtuale. Una vera tecnologia WAN è WiMax (IEEE 802.16), ad esempio. Utilizza una velocità di trasmissione di 35-144 Mbit/s e raggiunge una distanza massima di 50 km.

Per quanto riguarda le WAN, occorre parlare degli standard di comunicazione radiomobile, come GPRS con velocità di trasmissione di 56-114 kbit/s, UMTS-TDD (ITU IMT-2000) con velocità di trasmissione fino a 7,2 Mbit/s o HSPA con velocità di trasmissione fino a 42 Mbit/s. Vi sono molte altre tecnologie come LTE, iBurst, WiBro e EVDO, ad esempio.

Wireless LAN

Wireless LAN (IEEE 802.11) solitamente sostituisce la rete Ethernet al livello fisico delle comunicazioni ed è pertanto principalmente utilizzato nella trasmissione di traffico TCP/IP. Tipicamente, i terminali trasmettono con potenze di 25-30 mW, mentre il massimo consentito per legge è pari a 100 mW nei paesi europei e pari a 300 mW negli USA. La tabella 1 illustra le velocità e i le portate di diverse tipologie di WLAN.

Agli albori del WiFi, la cifratura e l'autenticazione si basavano sulla tecnologia WEP (Wired Equivalent Privacy) che oggi si è rivelata non sicura. Nel 2003 è stata sostituita dalla WPA (Wi-Fi Protected Access) o dalla WPA2 (IEEE 802.11i) rispettivamente [1].

Utilizza un handshake a 4 vie per l'autenticazione e lo scambio delle chiavi. In alternativa, WiFi supporta l'uso di un server RADIUS per l'autenticazione, l'autorizzazione e l'accounting.

Tabella 1 - Caratteristiche della famiglia IEEE 802.11 [2]

Standard	Frequenza	Bit-rate nominale	Bit-rate tipico	Distanza massima
IEEE 802.11a	5 GHz	54 MBit/s	~27 MBit/s	15 m – 30 m
IEEE 802.11b	2,4 GHz	11 MBit/s	~5 MBit/s	30 m – 90 m
IEEE 802.11g	2,4 GHz	54 MBit/s	~22 MBit/s	30 m – 90 m
IEEE 802.11n	5 / 2,4 GHz	600 MBit/s	~144 MBit/s	90 m – 180 m

Bluetooth

Esattamente come per la WLAN, Bluetooth trasmette nella banda dei 2,4 GHz e utilizza una banda complessiva di 83,5 MHz con 79 canali. Ciò fornisce una velocità massima di trasmissione per canale pari a 1 Mbit/s con Bluetooth 1.1 o pari a 2-3 MBit/s rispettivamente con Bluetooth 2.0 e EDR (Enhanced Data Rate) [4]. La portata e la potenza di trasmissione identificano 3 classi distinte come illustrato in tabella 2.

Comunicazione a distanza ravvicinata

Nella ricerca di una tecnologia wireless a corto raggio, NFC (ISO/IEC 18092:2004) appare un valido candidato. Fisicamente, la NFC si basa sullo standard ISO/IEC 14443 (a 13,56 MHz), utilizzata anche nei dispositivi RFID. La portata è solitamente inferiore a 20 cm e le velocità di trasmissione possibili sono anch'esse molto piccole e pari a 106, 212, 424 o 848 kbit/s [4]. Anche la potenza di trasmissione è molto bassa ed è possibile realizzare dispositivi NFC in grado di operare in modalità passiva, ossia senza un'alimentazione autonoma. In questo caso, essi catturano l'energia necessaria dal campo a RF tramite induzione. La NFC supporta diverse modalità di trasmissione dati, tra cui una cifratura basata sulla tecnologia Mifare (Philips) o Felica (Sony), ad esempio. Tutto ciò rende la NFC un candidato perfetto per i sistemi di pagamento senza contatto di prossima generazione.

Tabella 2 - Classi del segnale Bluetooth [3]

	Potenza	Portata
Classe I	100 mW	100 m
Classe II	2,5 mW	10 m
Classe III	1,0 mW	10 cm

Mobilità

In generale, il concetto di mobilità ha senso unicamente con le reti LAN e WAN. In una PAN, la mobilità è limitata dal breve raggio della tecnologia sottostante. La regola pratica è che più è alta la velocità di trasmissione più la mobilità del terminale è ridotta. La figura 1 mostra tale dipendenza in maniera schematica per alcuni esempi di tecnologie selezionate.

Integrazione software

Il fine principale dell'integrazione software è solitamente la corretta realizzazione dei rispettivi stack di protocolli. La 2 illustra la corrispondenza tra le tecnologie WLAN, NFC e Bluetooth con il modello di riferimento OSI. La parte principale di questi protocolli riguarda i livelli 1 e 2. Per NFC e Bluetooth, l'assegnazione dei livelli non è ovvia, in particolare per i livelli 3-7. Soprattutto con Bluetooth, si definisce solitamente un'interfaccia HCI (Host Control Interface) che serve da interfaccia tra lo stack dell'host e il controller Bluetooth.

Nell'applicazione embedded questa esplicita differenziazione tra la CPU dell'host e il controller non sempre è valida. Quando si integrano i protocolli nel software embedded, occorre rispettare gli standard di tali protocolli. La conformità allo standard deve essere verificata mediante validazioni e collaudi di interoperabilità. Tuttavia, è importante notare che ciò non è sufficiente per garantire la sicurezza informatica del sistema. Il sistema operativo (OS) sottostante e l'architettura del sistema vanno scelti in modo che possano consentire un funzionamento affidabile e sicuro del software. È obbligatorio separare parti critiche, come quelle che gestiscono i dati sensibili, dalle sezioni meno critiche, come ad esempio l'interfaccia utente. Inoltre il sistema operativo deve garantire memoria, allocazione temporale della CPU e altre risorse hardware ai singoli moduli software separatamente. Un sistema operativo a microkernel aumenterebbe l'affidabilità e la sicurezza, mettendo la maggior parte del codice nella modalità utente e riducendo l'ammontare di codice critico nel kernel. Maggiore è la quantità di codice che lavora in modalità kernel, maggiore è il rischio che un bug del software faccia andare in crash l'intero sistema o apra le porte a un attacco esterno.

Tutto ciò può essere ottenuto utilizzando un kernel di separazione, che separa e garantisce le risorse ed esegue i driver in modalità utente. La virtualizzazione non è un requisito per avere un sistema sicuro. Tuttavia, la virtualizzazione può "arricchire" un dispositivo già sicuro con una varietà di altre caratteristiche.

In definitiva, nel progettare un dispositivo embedded con tecnologia wireless, occorre tenere in considerazione i parametri fisici e realizzare e verificare correttamente i protocolli di comunicazione. La cifratura dei dati trasmessi e un controllo sicuro degli accessi di per sé non garantiscono una comunicazione wireless sempre sicura. Il software embedded del terminale va progettato in modo che sia sicuro e protegga i dati sensibili da un loro impiego scorretto.

RIFERIMENTI

[1] http://de.wikipedia.org/wiki/Wi-Fi_Protected_Access
[2] http://en.wikipedia.org/wiki/IEEE_802.11
[3] M. Hietanen, T. Alanko (2005-10). "Occupational Exposure Related to Radiofrequency Fields from Wireless Communication Systems" (PDF). XXVIIIth General Assembly of URSI - Proceedings. Union Radio-Scientifique Internationale.
http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7(01682).pdf.
[4] Christian Unhold, "Bluetooth und NFC", September 2008, http://www.scribd.com/doc/8527369/Bluetooth-und-NFC