Alla scoperta

La tecnologia ZigBee rappresenta un protocollo per reti wireless indirizzata per applicazioni d'automazione e controllo remoto.
Non si è certi sull'origine del suo nome, ma alcuni sostengono che derivi dal movimento a zig zag compiuto dalle api che passando di fiore in fiore trasmettono alle altre l'informazione su dove trovare cibo...

INTRODUZIONE ALLE WPAN

Le reti wireless sono la naturale evoluzione di quelle wired ed hanno visto il loro sviluppo a partire dalla metà degli anni ottanta con le cosiddette WLAN (Wireless Local Area Network).
Con lo sviluppo di dispositivi mobili di differente tipologia si è manifestata, poi, la necessità di realizzare reti che siano concentrate attorno alla persona e che quindi si estendano per pochi metri in tutte le direzioni.
Tali reti si chiamano WPAN (Wireless Personal Area Network) e sono regolate dallo standard IEEE 802.15. In particolare, sono definiti tre differenti classi di WPAN, sulla base della velocità di trasmissione, del consumo di energia e della qualità del servizio (QoS):

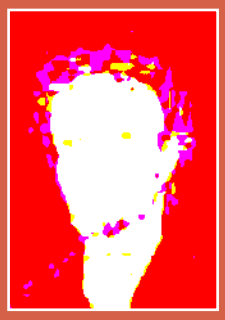
1. WPAN con data rate elevato (IEEE 802.15.3), indicate per applicazioni multimediali che richiedono un elevato QoS.
2. WPAN con data rate intermedio (IEEE 802.15.1/Bluetooth), indicate per una gran varietà di compiti tra cui telefoni cellulari, PDA ed in generale applicazioni adatte per comunicazioni vocali (es. auricolari per telefonini).
3. WPAN con data rate basso (IEEE 802.15.4/LR-WPAN), particolarmente indicate in campo industriale, home automation, medicale ed in generale per tutte quelle applicazioni che necessitano di un basso costo, consumo di potenza e velocità di trasmissione. E' in quest'ultima categoria che rientra lo standard ZigBee, oggetto del presente articolo.

Figura 1 Logo della ZigBee Alliance

ZIGBEE ALLIANCE E IEEE 802.15.4

La tecnologia ZigBee rappresenta un protocollo per reti wireless indirizzata per applicazioni d'automazione e controllo remoto. Non si è certi sull'origine del suo nome, ma alcuni sostengono che derivi dal movimento a zig zag compiuto dalle api che passando di fiore in fiore trasmettono alle altre l'informazione su dove trovare cibo.
Questo particolare tipo di WPAN nasce dallo sforzo congiunto di IEEE e della ZigBee Alliance (in Figura 1 è rappresentato il logo).
Quest'ultima è un consorzio di oltre 70 società (tra cui Motorola, Philips e Samsung) il cui obiettivo è quello di assicurare, a breve, la diffusione di ZigBee in un ampio settore del mercato wireless. La speranza dei promotori di ZigBee è di realizzare chip sempre più integrati e 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 Wi-Fi (IEEE

dello ZigBee



di Savino Giusto

802.11), Bluetooth e WirelessUSB. La Tabella 1 riporta un confronto dettagliato tra le principali tecnologie wireless esistenti, evidenziando le caratteristiche di ciascuna di esse.
I dispositivi compatibili con ZigBee sono in grado di trasmettere fino a un distanza di 75 metri, a seconda delle interferenze RF dell'ambiente in cui si trovano e del consumo di potenza richiesto dall'applicazione. Essi trasmettono all'interno della banda di frequenze senza licenza (2.4GHz, 915MHz negli Stati Uniti e 868MHz in Europa). La velocità di trasferimento dei dati è variabile in base alla frequenza e varia da un minimo di 20Kbps (@868MHz) ad un massimo di 250Kbps (@2.4GHz).

Il lavoro della task force ZigBee Alliance e IEEE è consistito nella definizione dell'intero stack; in particolare, la seconda ha sviluppato i due layer più bassi del protocollo (fisico e MAC), mentre la prima ha definito i layer superiori, cioè quello di applicazione e di rete, in maniera tale da garantire l'interoperabilità tra i prodotti di diverse case costruttrici. La Figura 2 propone i vari layer di cui è costituito lo stack ZigBee.

ZIGBEE VS. BLUETOOTH

La tecnologia che risulta più simile a ZigBee è sicuramente il Bluetooth. Pertanto si cercherà di evidenziare in cosa esse si differenziano, parlando dei limiti di Bluetooth che si è tenta-

Tecnologia	Parametro						
	Frequenza	Data rate	Range(m)	Rete	Complessità	Consumo	Applicazioni
ZigBee	868MHz (Europa) 915MHz (USA) 2.4GHz	20 kbits/s 40 kbits/s 250 kbits/s	10÷75m	Stella, peer- to-peer, mista	bassa	molto basso	Controllo di ambienti domestici e industriali, di sensori; giochi ed apparecchiature medicali
Bluetooth	2.4GHz	1 Mbits/s	10÷100m	Piconet	alta	medio	Auricolari, connessioni PC, portatili, cellulari
Wi-Fi	2.4GHz (802.11b) 5GHz (802.11)	11Mbits/s 54 Mbits/s	50÷100m	Punto Multipunto	alta	alto	WLAN, trasferimento file, collegamento ad Internet senza fili
UWB	3.1÷10.6GHz	100÷500 Mbits/s	<10m	punto punto	media	basso	Applicazioni multimediali (immagini e filmati)
UHF	260-470 MHz 902-928 MHz	10÷100 kbits/s	10m	punto punto	molto bassa	basso	Accesso remoto senza chiavi per apertura porte
Wireless USB	2.4GHz	62.5 kbits/s	10m	punto punto	bassa	basso	Periferiche PC
IrDA	Infrarosso	20-40 kbits/s	a vista	punto punto	bassa	basso	Collegamenti PC

Tabella 1 *Confronto tra la tecnologia ZigBee e quelle concorrenti*

to di superate con ZigBee.
Tra i punti critici di Bluetooth si ricordano il consumo di energia e la latenza. Il suo protocollo è relativamente complesso (circa 250Kbyte per implementare tutto lo stack e 131 primitive previste) in quanto deve inviare un volume di dati di controllo superiore rispetto ad altre soluzioni; questo provoca un aumento della latenza e quindi dei tempi di trasmissione, nonché una durata media della batteria bassa. Un altro punto a sfavore del Bluetooth è il costo.

Figura 2 Stack ZigBee

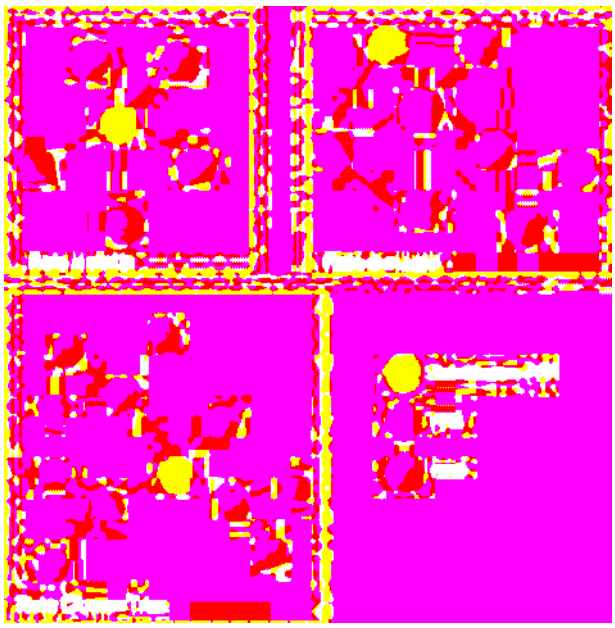


Figura 3 Topologie di reti

ZigBee può essere considerato come un potenziale concorrente anche nei progetti di periferiche per PC, in quanto riduce i costi e prolunga la durata delle batterie. Per l'implementazione dell'intero stack sono sufficienti 32Kbyte di memoria ROM, 8Kbyte di RAM ed un microcontroller a 8bit come un PIC o un 8051. Tutto ciò si rispecchia positivamente sul consumo (in quanto si trasmettono meno dati); un dispositivo ZigBee dovrebbe essere in grado di funzionare da 6 mesi a 2 anni con appena 2 batterie AA! La minor complessità si evince anche dall'esiguo numero di primitive (appena 30!).
I dispositivi ZigBee possono trasmettere con velocità almeno 1/4 inferiori rispetto al Bluetooth e ciò li rende inappropriati in tutti quei casi in cui la quantità di informazione diventa eccessiva. Come risvolto della medaglia si ha, però, la possibilità di utilizzare della logica di elaborazione più economica.
La possibilità di realizzare reti complesse è una delle qualità dello ZigBee, infatti è possibile (almeno in teoria) connettere tra loro oltre 60000 dispositivi con un unico coordinatore di rete, contro gli 8 device gestibili con il Bluetooth.
Riassumendo, dispositivi ZigBee risultano utili in tutte quelle applicazioni semplici, in cui il costo del singolo nodo diventerebbe più elevato della periferica ad esso collegato (es. un sensore) utilizzando il Bluetooth. Accensione di luci a distanza, rilevazione a distanza dei sensori per apparecchiature mediche, controllo wireless di sistemi di condizionamento e ventilazione, sensori di fumo e fuoco, termostati, controllo remoto di audio e video, sistemi di sicurezza e domotica sono solo alcune delle applicazioni che si prevede o che già utilizzano la tecnologia ZigBee.

IL PROTOCOLLO IEEE 802.15.4

Componenti di una rete ZigBee

Un sistema ZigBee consiste di differenti componenti, tra cui quello base è rappresentato dal dispositivo trasmittente che può essere:

- Dispositivo a piena funzionalità, FFD (Full-Function Device).
- Dispositivo a ridotta funzionalità, RFD (Reduced-Function Device).

Una rete ZigBee deve includere almeno un FFD, il quale può operare in tre modi diversi:
1. Coordinatore della PAN.
2. Coordinatore di una sotto-rete.
3. Dispositivo semplice.

Invece un RFD è previsto in applicazioni particolarmente semplici e che non necessitano di inviare grandi quantità di dati. Inoltre va ricordato che un FFD può parlare sia ad un altro FFD che ad un RFD, mentre un RFD può parlare solo ad un FFD.

Topologie di rete

La Figura 3 mostra le tre possibili topologie di reti che si possono realizzare con dispositivi ZigBee:
1. Topologia a stella
2. Topologia a maglia
3. Topologia cluster-tree.

Nella topologia a stella, la comunicazione è stabilita tra il dispositivo e il controllore del centro stella, detto coordinatore della PAN. Quest'ultimo in genere viene alimentato dalla rete elettrica (quindi non presenta vincoli stringenti sul consumo), mentre i restanti dispositivi funzionano a batteria. Applicazioni che utilizzano questo tipo di PAN sono domotica, periferiche per PC, giocattoli e giochi per PC. Dopo che un FFD si attiva per la prima volta, esso può stabilire la sua rete e diventare il coordinatore della PAN.
Anche nella topologia a maglia (detta anche peer-to-peer) esiste un unico coordinatore. Diversamente dalla stella, però, tutti i dispositivi possono comunicare con tutti gli altri. Applicazioni tipiche sono controllo industriale, monitoraggio e reti di sensori wireless.
Con questo tipo di rete è possibile utilizzare salti multipli per instradare un messaggio da un dispositivo all'altro nella rete e perciò tali reti sono particolarmente indicate in situazioni in cui la potenza del singolo dispositivo risulta limitata. L'affidabilità della trasmissione è garantita tramite percorsi multipli.
L'ultima topologia può essere considerata un caso particolare della precedente, in cui più dispositivi fungono da FFD ed un nodo può connettersi alla rete tramite di questi. Tra tutti gli FFD uno solo può fungere da coordinatore di rete. Quest'ultimo forma il primo cluster

PHY (MHz)	Banda di Frequenza	Chip rate (Kchip/s)	Modulazione	Bit rate (kbit/s)	Symbol rate	Symbol
868/915	868÷868.6	300	BPSK	20	20	Binario
	902÷928	600	BPSK	40	40	Binario
2450	2400÷2483.5	2000	O-QPSK	250	65.2	16 aryOrtogonale

Tabella 2 *Bande di frequenza e velocità*

Figura 4 *Bande di frequenze operative*

stabilendosi esso stesso come centro del cluster (CLH) con un identificativo (CID) pari a zero. A questo punto il coordinatore invia dei pacchetti broadcast per la sincronizzazione con tutti i dispositivi vicini.
Un dispositivo candidato può richiedere di unirsi alla rete tramite il CLH. Se il coordinatore lo permette, aggiunge questo device alla sua lista. Quest'ultimo a sua volta può agganciare alla rete altri nodi. Il vantaggio di questa struttura è quella di incrementare l'area coperta, con lo svantaggio però di incrementare la latenza dei messaggi trasmessi.

Il layer fisico (PHY)

Alla base della pila del protocollo ZigBee si trova il layer fisico (PHY), il quale fornisce due differenti servizi: quello dati e quello di gestione. Le caratteristiche principali implementate a questo livello sono attivazione e disattivazione del trasmettitore radio, rilevamento dell'energia (ED), indicazione della qualità del collegamento (LQI), selezione del canale, stima della disponibilità del canale (CCA), e trasmissione e ricezione dei pacchetti sul mezzo fisico (canale radio).
Lo standard offre due possibilità per la trasmissione/ricezione basate su differenti frequenze. Entrambi i metodi sfruttano la tecnica di modulazione DSSS (Direct Sequenze Spread Spectrum). Il tasso di trasmissione è di 250Kbps a 2.4GHz, 40Kbps a 915MHz e 20Kbps a 868MHz. Il tasso di trasmissione dati maggiore è da attribuirsi all'ordine dello schema di modulazione superiore. Frequenze più basse assicurano, invece, un range ed una sensibilità maggiore grazie alla minore attenuazione. Frequenze più alte garantiscono una velocità maggiore ed una latenza e duty-cycle minori. La Tabella 2 riporta le caratteristiche del livello fisico per ogni banda di frequenza utilizzata.

Nel range di frequenze tra 868÷868.6MHz esiste un solo canale, mentre ci sono 10 canali tra i 902.0MHz e 928.0MHz; infine tra le frequenze 2.4GHz e 2.4835GHz si trovano ben 16 canali (Figura 4).

Lo standard 802.15.4 supporta la possibilità di selezionare dinamicamente il canale, tramite una funzione di scansione che permette di cercare il frame di beacon (sincronizzazione) in una lista di canali utili.
La sensibilità del ricevitore (secondo le specifiche) deve essere pari a -85dB@2.4GHz e -92dB@868/915MHz; la maggiore sensibilità del ricevitore nella banda di frequenze più

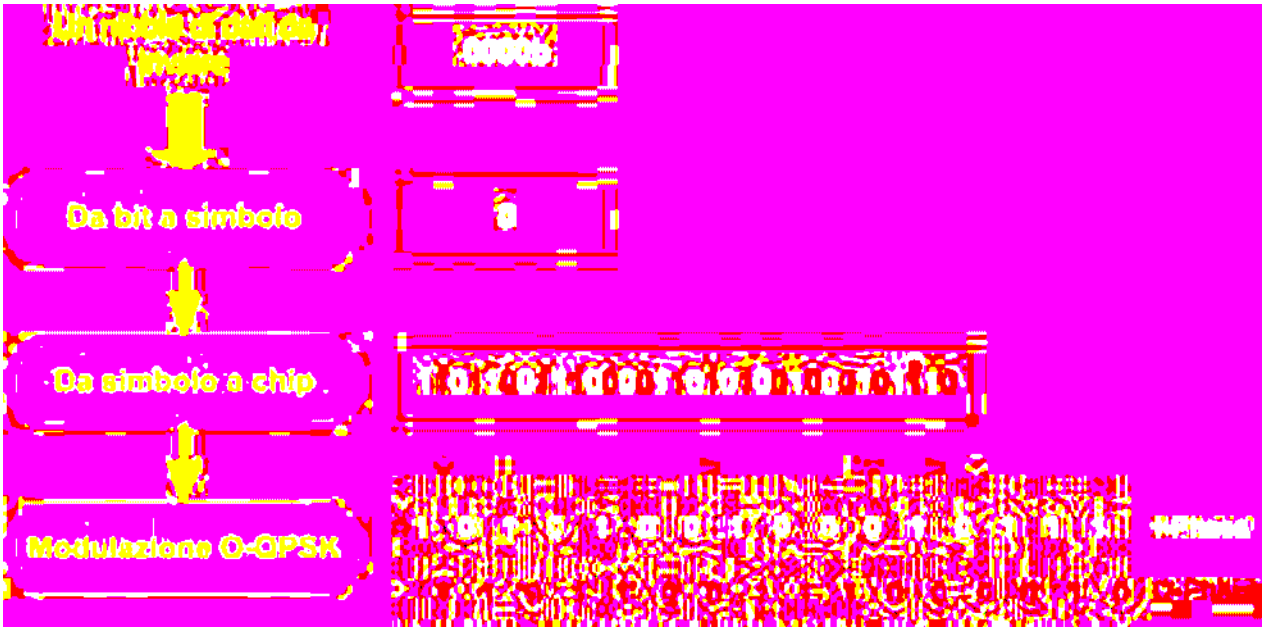


Figura 5 Processo di modulazione DSSS

bassa è dovuta al minore data rate. Il range operativo di ogni dispositivo dipende oltre che dalla sensibilità anche dalla potenza in trasmissione.
Con la modulazione DSSS un gruppo di bit è rappresentato mediate un unico simbolo; in particolare, nello standard in questione il gruppo è formato da 4 bit (detto nibble). Poiché con 4 bit le possibili combinazioni sono 16 (= 2^4) allora esistono 16 differenti simboli all'interno di una tabella numerata da 0 a 15, in cui a ciascun simbolo corrisponde una sequenza di 32 bit, detta chipping code. La Figura 5 illustra tale processo usando il chipping code per il simbolo 0.

Ciascun simbolo consiste, dopo tale processo, di 32 bits detti chips, il che comporta un notevole aumento nella frequenza del segnale, "spalmando" lo spettro del segnale iniziale su un ampio range di frequenze (è questo il concetto di modulazione DSSS). Dopo alcune operazioni di filtraggio per limitare la banda, i chips sono portati al modulatore. Per la trasmissione nella banda di frequenze superiore, il modulatore trasmette con un chipping rate pari a 2Mchip/s e poiché sono inviati 32 chips per ogni 4 bits di dati reali, il data rate effettivo è dato dalla seguente formula:

$$2x10^6(4/32) = 250 \text{ Kbps}$$

Oltre alle operazioni descritte sopra, un dispositivo che implementa il PHY deve essere capace di svolgere altri compiti, tra cui rilevamento dell'energia del ricevitore (ED).
Si tratta di una caratteristica utilizzata dal layer superiore network all'interno dell'algoritmo di selezione del canale. In pratica, l'ED è una stima del segnale ricevuto e nessun tentativo viene fatto per decodificare i bits ricevuti. Il tempo di ED è pari alla durata di 8 simboli e il risultato è riportato in una variabile intera di dimensione 8 bit (da 0x00 a 0xff). Il valore minimo è 0 ed indica una potenza ricevuta inferiore di 10dB ai valori di sensibilità del ricevutore specificati precedentemente.
Un'altra indicazione essenziale effettuata a questo livello è la qualità del segnale (LQI). Essa può essere effettuata utilizzando il parametro ED, una stima del rapporto segnale

rumore oppure una combinazione di entrambi. Tale valore è utilizzato nei layer superiori di rete o di applicazione e viene indicato come un valore intero ad 8 bit.
Infine, bisogna ricordare un'altra funzione svolta dal PHY, ossia la stima della disponibilità del canale (CCA), indispensabile per implementare gli algoritmi di CSMA-CA per la gestione delle collisioni. Prima di poter avviare una trasmissione, un dispositivo ZigBee deve accertarsi se un altro sta utilizzando il mezzo radio. Esistono tre possibili soluzioni per implementare tale funzione:

1. Energia oltre la soglia: il CCA riporta l'indicazione di mezzo occupato se il livello di energia ricevuto (ED) supera un prestabilita soglia.
2. Rilevamento della portante: il CCA riporta l'indicazione di mezzo occupato solo se rileva un segnale con le stesse caratteristiche fissate nel protocollo 802.15.4. Non è importante se tale segnale supera oppure no la soglia di energia.
3. Rilevamento della portante con superamento della soglia: si tratta dei due metodi combinati insieme; viene riportata l'indicazione di mezzo occupato se viene rilevata la portante e la sua energia supera la soglia.

Il layer MAC

Coordinamento dell'accesso al mezzo da parte del tranceiver, creazione ed instradamento dei pacchetti, generazione e riconoscimento dell'indirizzo, verifica del numero di sequenza dei pacchetti sono i principali compiti a cui è chiamato ad assolvere il livello MAC. Esso deve anche gestire il processo di rilevamento (discovery) da parte di un dispositivo di quelli ad esso vicini. Il tempo richiesto per far ciò è dell'ordine di 30ms, mentre le tecnologie concorrenti come USB o Bluetooth possono impiegare fino a 10s prima di poter iniziare ad utilizzare completamente di dispositivo.

Figura 6 I Quattro tipi di frame del layer MAC

Le principali funzioni del livello MAC sono sviluppate in software a differenza di quanto avviene per il PHY; esse sono scritte generalmente in linguaggio C e sono indicate con i nomi di setEncryption, sendPacket e packetReceived.
Esistono 4 possibili tipi di frame a livello MAC, come illustrato in Figura 6:

1. Frame di dati.
2. Frame ACK.
3. Frame di comando MAC.
4. Frame di beacon.

Il frame di dati è costituito al massimo da 104 bytes; esso è numerato per assicurare l'instradamento di tutti i pacchetti. Il campo Frame Check Sequence assicura che tutti i pacchetti siano ricevuti senza errori. Questo migliora notevolmente l'affidabilità in condizioni sfavorevoli di trasmissione.
Un altro frame molto importante è quello di ACK. Esso fornisce la conferma che il pacchetto inviato è stato ricevuto correttamente. Questa soluzione garantisce la consistenza dei dati, ma ovviamente aumenta la latenza. Essa può essere attivata o meno.
Il frame di commando MAC fornisce un meccanismo per il controllo e configurazione remota dei nodi client.
Infine, il frame di beacon ha il compito di "svegliare" i dispositivi client, i quali sono in ascolto del loro indirizzo e vanno in modalità sleep se non lo ricevono. I beacon sono importanti per le reti a maglia e cluster-tree per mantenere tutti i nodi sincronizzati senza la necessità che essi rimangano in ascolto per lunghi periodi di tempo, consumando così le batterie.
Trattandosi di una trasmissione in cui il mezzo (radio) è condiviso da tutti i dispositivi, è necessario disporre di qualche metodo di arbitraggio della trasmissione, affinché due dispositivi non inviino pacchetti contemporaneamente. Esistono due tecniche utilizzate: la CSMA-CA ed il beacon.
A differenza di quanto avviene nelle reti LAN su cavo (802.3), per le reti wireless è stata adottata la tecnica di accesso multiplo con rilevamento della portante ed eliminazione delle collisioni, CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance). In sostanza, significa che ogni dispositivo prima di iniziare una trasmissione deve ascoltare il mezzo e capire se è già in corso una trasmissione. Se c'è già un nodo che sta trasmettendo, allora sarà effettuata la ritrasmissione successivamente con un ritardo casuale.
La CSMA-CA viene adottata nelle reti ZigBee semplici di tipo peer-to-peer, come per esempio sistemi di sicurezza in cui il dispositivo è in modalità sleep per il 99,999% del tempo.
La seconda tecnica consiste nell'invio dal parte del coordinatore di un superframe (beacon) ad intervalli regolari di tempo (multipli di 15.38ms, fino a 252s).
Tra un beacon e l'altro ci sono 16 time slot di pari ampiezza in ciascuno dei quali è garantita l'assenza di collisione, come in Figura 7. Tutti i dispositivi si contendono i primi nove time slot. Gli ultimi slot temporali sono invece assegnati dal coordinatore ad un nodo speci-

Figura 7 Tecnica di accesso al mezzo mediante frame di beacon

fico e sono detti GTS (Guaranteed Time Slot). Nel caso un nodo debba trasmettere una grande quantità di informazione, il coordinatore può assegnargli anche più di un GTS. Tale struttura garantisce un banda dedicata ed una bassa latenza rispetto alla prima tecnica. Inoltre consente di ridurre notevolmente il consumo delle batterie, poiché ciascun dispositivo sa esattamente quando trasmettere ed è sicuro che non ci saranno collisioni.

ZIGBEE ALLIANCE

Il layer network

Il layer network (NWK) ha il compito di associare e dissociare i dispositivi al coordinatore, implementare la sicurezza ed instradare i frame alla loro destinazione (Figura 8).
Inoltre, l'NWK è responsabile della creazione di una nuova rete e dell'assegnazione di un indirizzo ai nuovi dispositivi associati.
Dal punto di vista del livello rete, i dispositivi ZigBee possono suddividersi in:

- Coordinatore (ZC): è unico per ogni rete; ha il compito di formare la rete ed agisce come router una volta che la rete si è costituita.
- Router (ZR): si tratta di un componente opzionale e si puo associare con lo ZC oppure con altri ZR; ha il compito di instradare i messaggi.
- End Device (ZED): si tratta di un componente opzionale e non partecipa al routing dei messaggi.

La Tabella 3 riporta lo schema di un tipico frame a livello NWK, mentre la Tabella 4 mostra un dettaglio del campo di controllo.

Il procedimento con cui vengo instradati i pacchetti attraverso i vari router è basato su un tabella di routing contenuta all'interno dei ZR, il cui schema è riportato in Tabella 4.

Quando arriva un pacchetto, viene estratto

Figura 8 Stack ZigBee con dettaglio del layer network

Ottetti: 2	2	2	1	1	Variabile
Controllo del frame	Indirizzo destinazione	Indirizzo sorgente	Broadcast radium	Numero di sequenza broadcast	Payload
	Campi per il routing				
Intestazione protocollo NWK					Payload

Tabella 3 Dettaglio del frame di controllo

CENTRO FIERA del GARDA
MONTICHIARI (BS)

COMUNE DI MONTICHIARI · PROVINCIA DI BRESCIA · REGIONE LOMBARDIA

2/3 SETTEMBRE 2006

27ª

- Elettronica
- Video
- Strumentazione
- Componentistica
- Hi-Fi
- Computer
- Esposiz. Radio d'Epoca
- Filatelia

13° RADIOMERCATINO di PORTOBELLO

ORARIO CONTINUATO:
SABATO 9.00 - 18.30 - DOMENICA 9.00 - 17.30

CENTRO FIERA DEL GARDA
Via Brescia, 130 - 25018 MONTICHIARI (BS) - Tel. 030 961 68 - 961 042 - fax 030 962 946

Bits: 0-1	2÷5	6-7	8	9	10÷15
Tipo di frame	Versione protocollo	Percorso di rilevamento	Riservato	Sicurezza	Riservato

Tabella 4 Schema della tabella di instradamento

Nome campo	Dimensione	Descrizione
Destination address	2 bytes	Indirizzo a 16 bit del router di destinazione
Status	3 bits	Lo stato del router
Next-hop address	2 bytes	Indirizzo a 16 bit del salto successivo verso la destinazione

Tabella 5 Collegamento di un dispositivo alla rete

l'indirizzo di destinazione e se presente all'interno della tabella di routing, descritta in Tabella 5, allora si effettua il prelievo dell'indirizzo successivo. Come si nota in Figura 9, la formazione di una nuova rete da parte di un coordinatore è originata con una richiesta dal layer applicazione ed è poi gestita a livello network e MAC. La Figura 10 mostra invece la richiesta di un nodo ZigBee di legarsi ad una rete.

Il layer applicazione

Il layer applicazione è costituito dai driver e dal codice, contenuti nella ROM del microcontrollore.
La Figura 11 mostra lo schema competo di un nodo ZigBee, in cui vengono evidenziati, oltre al blocco relativo all'alimentazione, anche quelli inerenti il transceiver, il microcontrollore e l'interfaccia utente (rappresentata da un visualizzatore o da un sensore).
Il transceiver implementa il layer fisico, ossia si occupa della modulazione del segnale come descritto in precedenza. All'interno della ROM del microcontrollore è presente l'implementazione del livello MAC, NWK e applicazione. Tali due blocchi sono connessi tra loro mediante un interfaccia seriale sincrona ad alta velocità come per esempio SPI o I^2C. I sensori comunicano con il micro tramite le linee analogiche, le quali si occupano di convertire il segnale in digitale.

La sicurezza dei dati

Secondo lo standard, un nodo ZigBee può operare sia in modalità sicura che non sicura. Ovviamente, non implementando la sicurezza dei dati si ottiene un codice più leggero. Sono previsti 4 differenti servizi di sicurezza:

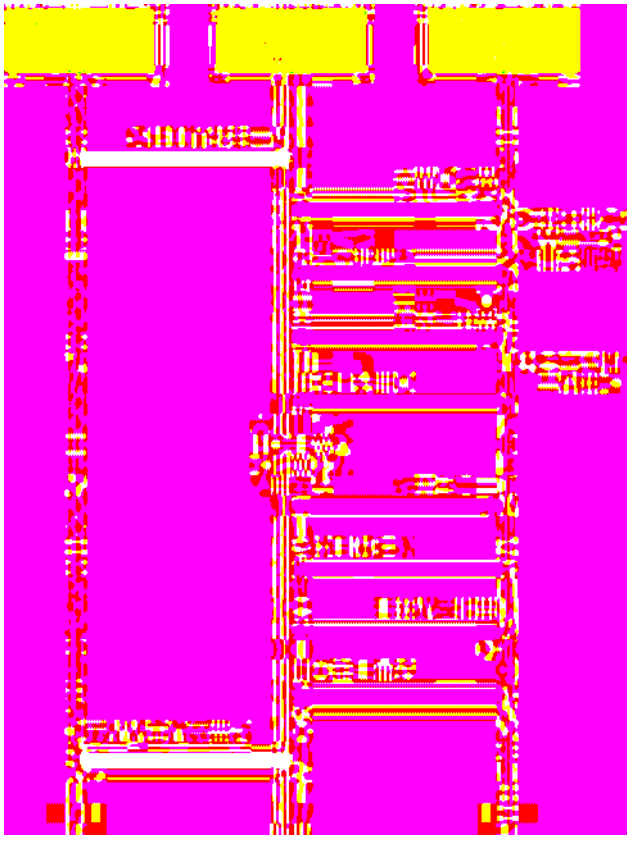


Figura 9 Formazione di una rete da parte del coordinatore

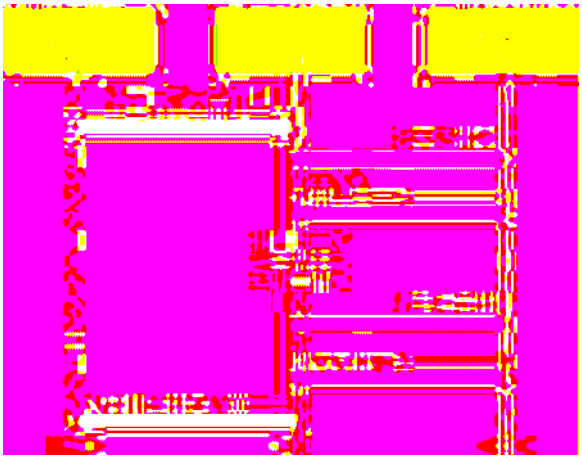


Figura 10 Richiesta di unione da parte di un nodo

1. Controllo degli accessi. Ogni dispositivo deve mantenere un lista di tutti i potenziali trasmettitori. In questo modo un dispositivo non autorizzato non può accedere ad una rete ZigBee.
2. Codifica dei dati. I dati non sono trasmessi in "chiaro", ma codificati mediante una chiave di crittografia posseduta solo dai componenti la rete.
3. Rinnovo sequenziale. Ogni frame viene confrontato con il precedente per evitare che ci siano ripetizioni.
4. 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.

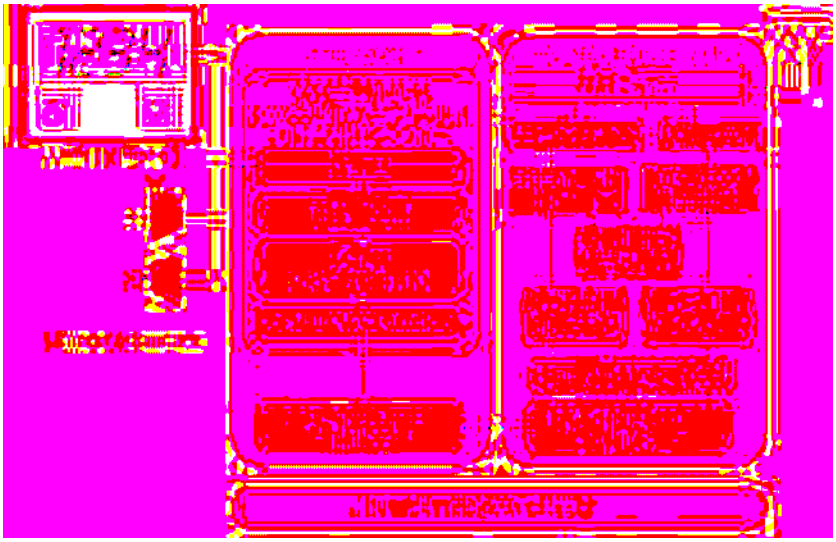


Figura 11 Diagramma completo di un nodo ZigBee

IL PROBLEMA DEL LOW POWER: LE SOLUZIONI

Il problema del ridotto consumo, come è stato ribadito più volte nel corso dell'articolo, è uno dei punto di forza dello standard ZigBee; si evidenzieranno ora le soluzioni adottate per ottenere questo risultato:

- Duty-cycling. Tale tecnica prevede la riduzione percentuale del tempo in cui un nodo risulta attivo.

Parametro			Prodotto				
			ZMD4410 (ZMD)	AT86RF210 (Atmel)	EM2420 (Ember)	MC13192 (Freescale)	CC2420 (Chipcon)
Banda di frequenza			868MHz 915MHz	868MHz 915MHz	2.4GHz	2.4GHz	2.4GHz
Interfaccia di controllo			SPI/Parallela	SPI	SPI (20MHz)	SPI (8MHz)	SPI (10MHz)
Sicurezza			AES-128	AES-128	CRC e AES-128	AES-128	AES-128
Range			~100m	~100m	~75m	~75m	~75m
Caratteristiche RF			≤40 kbps	≤40 kbps	250kbps OQPSK	250kbps OQPSK	250kbps OQPSK
Package			7mm x 7mm, 48 QLP			5mmX5mm, QFN 32	7mmX7mm, 48 QLP
Temperatura operativa			-40ºC ÷ +85ºC				
Tensione			2.4V	1.8V ÷ 3.6V	1.8V ÷ 3.3V	2.0V ÷ 3.4V	2.1V ÷ 3.6V
Consumo di corrente	Modalità	Sleep	2µA	1µA	0,5µA	<1µA	<1µA
		TX	32mA	20.7mA	20.7mA	30mA	17.4mA
		RX	28mA	14.5mA	19.7mA	37mA	18.8mA
Sensibilità in ricezione			-100dBm	-95dBm	-92dBm	-92dBm	-95dBm
Potenza di uscita			1mW	4mW	1mW	1mW	1mW

Tabella 6 Caratteristiche tecniche di alcuni transceiver commerciali

Pin I/O del PIC	Pin del CC2420
RB0 (input)	CC2420: FIFO
RB1 (input)	CC2420:CCA (non usato)
RB2 (input)	CC2420: SFD
RB3 (input)	CC2420: FIFOP
RC0 (output)	CC2420: CSn
RC1 (output)	CC2420: VREG_EN
RC2 (output)	CC2420: RESET
RC3 (output)	CC2420: SCK
RC4 (input)	CC2420: SO
RC5 (output)	CC2420: SI

Tabella 7 *Linee utilizzate per l'interconnessione del PIC con il chip CC2420*

Figura 12 *PICDEM Z di Microchip*

Lo standard prevede un valore massimo di 1%, anche se esistono applicazioni in cui si può scendere molto al di sotto di tale limite (un esempio su tutti: il monitoraggio di sensori, in cui si può ridurre il duty-cycling anche fino a 10ppm). L'utilizzo di intervalli di inter-beacon permettono di ridurre il tempo di attività dei dispositivi.

- Spaziamento tra canali. Nel caso di banda a 2.4GHz si ha uno spacing di 5MHz contro i 2MHz strettamente necessari. Questo permette ai sintetizzatori di frequenza di lavorare con riferimenti frequenziali più alti e ridurre quindi il tempo di assestamento.
- Chip-sequence. La codifica dell'informazione tramite le sequenze di chip, pur peggiorando la banda, consente un guadagno in termini di sensitività. In questa maniera è possibile ridurre la potenza trasmessa a parità di BER (Bit Error Rate).
- Bassa potenza trasmessa. Ovviamente riducendo la potenza si riduce conseguen-

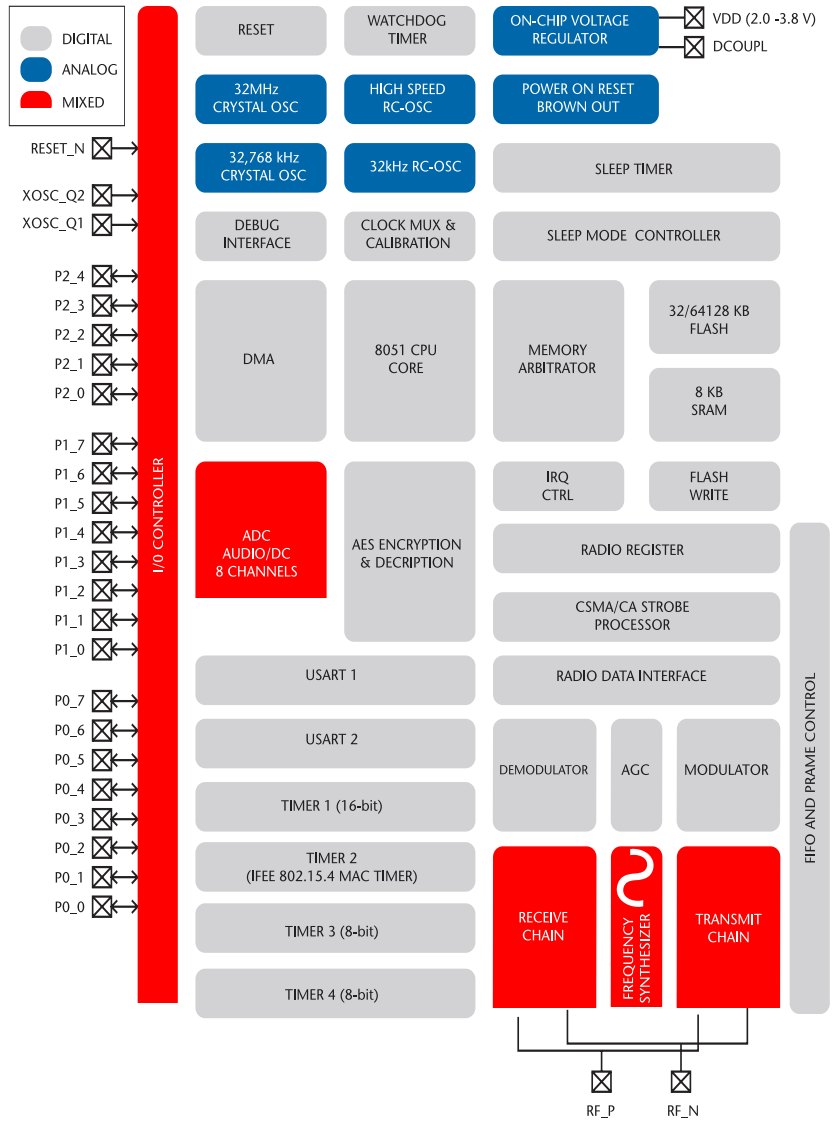


Figura 13 *Struttura interna del chip CC2430*

UN CONTROLLORE ALTERNATIVO

COMFILE
TECHNOLOGY

CUBLOC™

GAMMA DI CONTROLLORI PROGRAMMABILI IN BASIC E LADDER LOGIC CON AMBIENTE DI SVILUPPO GRATUITO.

www.comfiletech.com

Codice MIP 253091

Inware
Providing Innovation

INWARE Srl Via Cadorna, 27/31 - 20032 Cormano (MI) Tel: 0266504794 - Fax: 0266508225 - www.inware.it

temente la superficie coperta. Questo problema però è stato aggirato prevedendo le topologie di rete a maglia. Una osservazione è tuttavia doverosa: i transceiver attuali permettono di scendere anche sotto 1mW, ma questo non da un grosso vantaggio dal punto di vista del consumo poiché l'elettronica che si interfaccia con il chip RF (microcontrollore) di solito non consuma meno di 10mW.

- Riduzione del periodo di ascolto in CSMA-CA. Il periodo di accensione del ricevitore può essere ridotto fino a pochi slot temporali, prima di iniziare la trasmissione dei frame, nel caso di applicazioni a basso traffico.
- Semplicità del protocollo. Un protocollo semplice, come quello di ZigBee, permette di ridurre notevolmente la quantità di informazione trasmessa e ricevuta.

LO STATO DELL'ARTE

Alcune possibili soluzioni per implementare il trasmettitore/ricevitore secondo lo standard IEEE 802.15.4 sono di seguito riportate (vedi anche tabella 6):

- ZMD4410 di ZMD (http://www.zmd.de/)
- AT86RF210 di Atmel (http://www.atmel.com/)
- EM2420 di Ember (http://www.ember.com/)
- MC13192 di Freescale Semiconductor (http://www.freescale.com/)
- SmartRF CC2420 di Chipcon (http://www.chipcon.com/)
- ML7065 di OKI Semiconductor (http://www2.okisemi.com/)
- JT24Z001 di Jennic (http://www.jennic.com/)

Tra i vantaggi della tecnologia ZigBee si trova sicuramente la semplicità di implementazione del protocollo, rendendo sufficiente l'utilizzo di un micro ad 8 bit come PIC, AVR o altri basati su 8051.

Una soluzione di facile utilizzo è lo stack ZigBee di Microchip (scaricabile gratuitamente dal sito www.microchip.com) che presenta le seguenti caratteristiche:

- Supporto del chip CC2420.
- Supporto per RFD e coordinatore di rete
- In modalità coordinatore, implementa la memorizzazione dei nodi vicini.
- Supporto di reti a stella
- Supporto con la maggior parte dei PIC18
- Realizzazione di codice modulare per l'aggiunta/rimozione di specifici moduli.

Come è già stato detto più volte nel corso dell'articolo, un dispositivo ZigBee deve utilizzare un numero ridotto di risorse del microcontrollore; questo vincolo è soddisfatto osservando, in Tabella 7, le linee utilizzate per la comunicazione con il transceiver (appena 10 linee!).

Per ridurre il time to market Microchip offre una scheda di valutazione, la PICDEM Z, che permette di effettuare gli eventuali test per lo sviluppo della propria applicazione. La Figura 12 mostra un'immagine di tale evaluation board.

Quelle presentate fin qui sono soluzioni ibride, il chip CC2430 della Chipcon rappresenta invece una soluzione SoC (System on Chip) per ZigBee, ossia interamente integrata. Essa combina il trasmettitore/ricevitore CC2420 con un micro di tipo 8051, dotato di 8KB di RAM. Questa soluzione integrata richiede pochi componenti esterni, risulta facile da

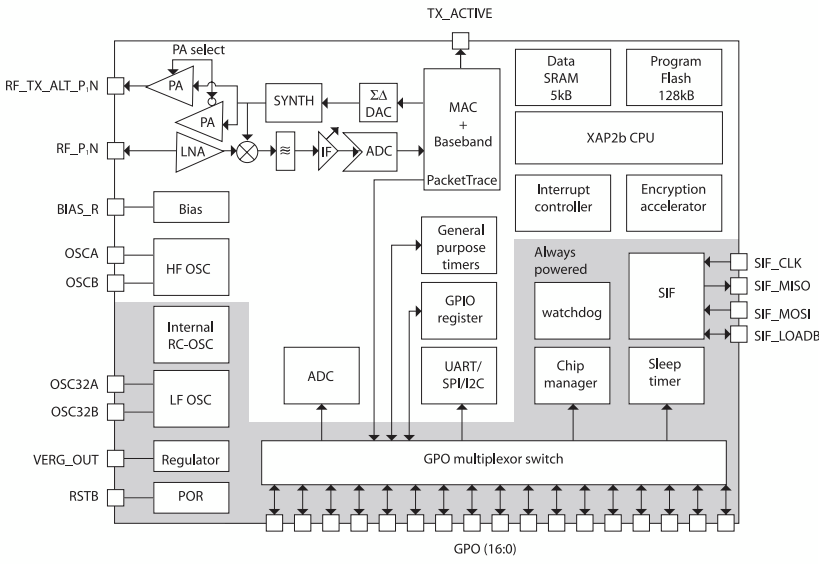


Figura 14 Struttura interna del chip EM250

Parametro		Prodotto	
		CC2430	EM250
Caratteristiche generali	Corrente modalità sleep (µA)	max 0.9	max 1
	Corrente RX (mA)	27	35.5
	Corrente TX (mA)	25	33
	Temp.operativa	-40° to +85° C	-40° to +85° C
	Tensione (V)	2.0 ÷ 3.6	2.1 ÷ 3.6
	Package	48QLP	48QLP
Caratteristiche RF	Data rate (kbps)	250	250
	Frequenza (MHz)	2400 ÷ 2485 16 canali	2400 ÷ 2485 16 canali
	Sensibilità RX (dBm)	-94	-97
	Potenza TX (dBm)	-24 ÷ 0	-32 ÷ 3
Caratteristiche micro	ROM (KB)	32,64,128	128
	RAM (KB)	8	5
	Frequenza clock (MHz)	32	24
	Core	8051 / 8-bit	XAP2b / 16-bit
	ADC	8-14 bit	12 bit
	Porte di comunicazione	UART/SPI	UART/SPI/I2C
	Coprocessore AES	presente	presente
	Pin I/O general-purpouse	21	17

Tabella 8 *Confronto tra due soluzioni integrate della Chipcon ed Ember*

implementare ed economica. Il core viene fornito in differenti modelli secondo la necessità di memoria ROM: CC2430-F32 (32KB), CC2430-F64 (64KB) e CC2430-F128 (128KB). Il CC2430 include anche caratteristiche avanzate come DMA, timers, co-processore per crittografia AES-128, ADC a 8-14 bit, USART, sleep-mode timer, Power-on-Reset e 21 pins I/O programmabili.
Insieme all'hardware viene fornito il protocollo ZigBee (Z-stack) ed il compilatore/debugger. Il kit di valutazione utilizzato per il test delle applicazioni è lo SmartRF04EB. Una rappresentazione dettagliata dei blocchi interni di questo modello è riportata in Figura 13.

L'altra soluzione interamente integrata è rappresentata dal chip della Ember, EM250, basato un processore a 16 bit con una frequenza di clock pari a 24MHz. Notevole risulta la disponibilità di memoria ROM (128KB) e di RAM (5KB). La Figura 14 illustra lo schema a blocchi interno dell'EM250.
Le caratteristiche di tale chip sono riassunte nella Tabella 8 per un confronto tra i due modelli.

PROSPETTIVE FUTURE PER ZIGBEE

Affermare oggi se ZigBee diventerà domani uno standard diffuso come Bluetooth o Wi-Fi è davvero una scommessa. E' certo però che per essere utile uno standard di comunicazione radio deve essere facilmente disponibile, economico e comprensibile. Per uno sviluppo davvero capillare è poi indispensabile che si interfacci ad un microcontrollore con poche linee di comunicazione I/O e siano disponibili economici sistemi di sviluppo. Queste sono caratteristiche possedute dalla tecnologia ZigBee.
Ne sono passati di bit sulle reti Ethernet da quando Bob Metcalfe ideò questa tecnologia,

modificando nei primi anni '70 l'architettura Alohanet basata sull'utilizzo delle onde radio. Oggi lo stesso Metcalfe è uno dei più fermi sostenitori di ZigBee ed è schierato in prima linee nel suo sviluppo con la società Ember.

Figura 15 Esempio di applicazione ZigBee: Raymarine LifeTag

Figura 16 Esempio di applicazione ZigBee: sensori di livello dell'acqua

Figura 17 Esempio di applicazione ZigBee: illuminazione degli appartamenti

Metcalfe ha rivelato l'esistenza di un "problema" di ZigBee: "Ha un numero enorme di applicazioni potenziali.
Bluetooth, ad esempio, ha trovato la sua killer application connettendo il cellulare all'auricolare o all'auto; esso risulta quindi facile da commercializzare perchè ci sono poche tipologie di clienti e di applicazioni... per ZigBee si parla invece di 'zilioni' di applicazioni: sistemi di controllo domestici (illuminazione, riscaldamento, allarmi), controllo remoto di veicoli (ad esempio un'imbarcazione), telelettura dei contatori (elettricità, gas), controllo industriale (raffinerie) e così via. E quella che ora si sta portando avanti è appunto la ricerca di una killer application per una prima diffusione di ZigBee ad alti volumi".
Una possibile killer application è quella commercializzata dalla società Raymarine, specializzata nello sviluppo di attrezzature elettroniche per la navigazione. Una di queste si chiama LifeTag e prevede l'utilizzo di una stazione base che comunica con tag indossabili dalle diverse persone che si trovano a bordo di una imbarcazione.
Qualora qualcuno dovesse allontanarsi di una decina di metri, evidenziando un degrado di segnale (ad esempio dovuto a una caduta in mare), si attiverà automaticamente un allarme. In Figura 15 è riportata un'immagine del dispositivo descritto.
Un altro possibile campo applicativo è rappresentato dai sensori di livello dell'acqua (Water Level Sensing), di cui la Figura 16 riporta uno schema generale. L'idea è quella di installare i dispositivi ZigBee in posti non coperti dalla rete GSM e sigillarli con il relativo sensore e le batterie all'interno delle cisterne che si vuole monitorare.
Le potenzialità di ZigBee sono sfruttate anche nella realizzazione di impianti di illuminazione domestica (Figura 17).
Essi possono ridurre i costi di installazione poiché eliminano la necessità della stesura dei cavi elettrici. Termostati e condizionatori possono, così, essere posti in qualunque punto dell'abitazione.

Codice MIP253078