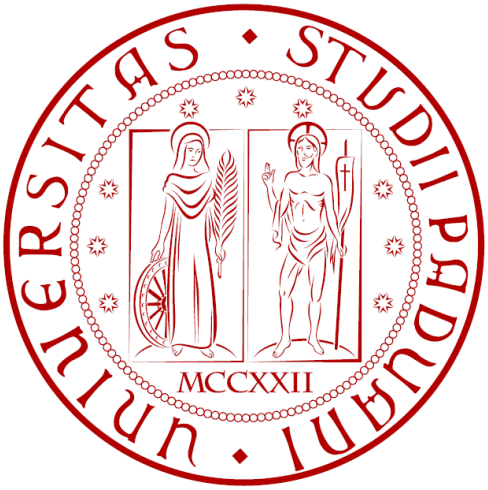
UNIVERSITÀ DEGLI STUDI DI PADOVA



Facoltà di Ingegneria

Corso di laurea in Ingegneria Elettronica

IWSN

Industrial Wireless Sensor Networks

Reti industriali wireless di sensori

Relatore: Prof. Stefano Vitturi

Laureando: Marco Dalla Rena

Anno Accademico 2011/12

Indice

Sommario

Obiettivo di questa tesina è quello di analizzare le reti wireless di sensori nel campo industriale e di dare uno sguardo d'insieme a quali sono i vantaggi, le possibili applicazioni e gli obiettivi di progettazione di una rete IWSN.
Nel seguito si presentano gli standard esistenti sul mercato che possono essere divisi in due principali gruppi:

1. Gli standard basati su IEEE802.15.4
2. Gli standard basati su IEEE802.15.1

dei quali si descrivono le caratteristiche, il grado di sicurezza ed affidabilità, le architetture di rete.

Introduzione

Al giorno d'oggi, le aziende necessitano sempre più di rendere efficiente la produzione, il monitoraggio ed il controllo processo, ed allo stesso tempo di restare in contenuti costi di implementazione, di schieramento e di manutenzione.
Tipicamente i sistemi industriali richiedono alta affidabilità e robustezza, dato che, il funzionamento di ogni singolo dispositivo o sensore utilizzato per il controllo ed il monitoraggio, è considerato fondamentale.
Il malfunzionamento di una qualsiasi unità potrebbe avere un enorme impatto sul processo, e nel caso peggiore causare pericolo o perdite economiche.
La tecnologia Wireless sembra essere una risposta a tali richieste, e nell'ultimo decennio ha avuto una notevole crescita, dapprima dal punto di vista sperimentale, fino a giungere all'applicazione odierna in molti processi produttivi.

Capitolo 1 – Reti IWSN

Le IWSN sono reti wireless che sono state adattate agli ambienti industriali come fabbriche, raffinerie, centrali elettriche, e vengono utilizzate per la misurazione, il controllo ed il monitoraggio. L'ambiente industriale è però caratterizzato da dure condizioni e notevoli interferenze, tali reti pertanto, devono essere robuste ed affidabili per poter rimpiazzare con successo le reti cablate. In alcuni casi si ha tutto l'interesse a sostituire le reti cablate, dato che le reti wireless presentano numerosi vantaggi. Vediamo quindi quali sono i vantaggi delle IWSN rispetto alle tradizionali reti, quali sono gli impieghi in ambito industriale, e le sfide tecniche da affrontare per venire incontro alle necessità industriali.

1.1 - Vantaggi

- Semplicità e dinamicità: le reti wireless sono capaci di avere un bacino d'utenze di molto maggiore rispetto ad una tradizionale rete LAN, ed inoltre lo sviluppo di tali reti, si sta orientando sempre più verso nodi che si organizzano autonomamente, in caso di caduta o aggiunta di un nodo ad esempio, senza l'intervento di operatori.
- Costi: esistono sicuramente mezzi trasmissivi con prestazioni migliori della trasmissione radio, in termini di immunità alle interferenze e banda, basti pensare alle trasmissioni in fibra ottica; ma il wireless ha il vantaggio di essere il più economico dato che le spese di installazione e disposizione dei nodi sono minime, vista la semplicità con cui tali dispositivi possono essere inseriti sul campo, ed in più c'è il notevole risparmio dato dal fatto che tali reti non richiedono cavi per la comunicazione.
- Flessibilità: grazie ai sensori in collegamento wireless è possibile effettuare misure in ambienti e posizioni in cui l'utilizzo di un sensore cablato sarebbe complicato, si pensi ad esempio ad ambienti corrosivi o a macchine in movimento.

1.2 - Applicazioni industriali

In generale la reti wireless possono essere utilizzate nel controllo processo in qualunque ambito industriale. Tuttavia, in alcune tipologie di industria, esistono delle applicazioni specifiche alle quali i sensori IWSN sono adibiti:

- Chimica: in questo tipo di industria possono essere utilizzati materiali pericolosi, sono necessari pertanto sensori che possano lavorare in ambiente

corrosivo e dove la presenza di cavi potrebbe essere problematica. I sensori installati controllano e monitorano la concentrazione di uno o più materiali, durante un processo chimico.

- Automobile: un' applicazione ancora in sviluppo ed in fase di sperimentazione, è quella di poter controllare all'interno di un automobile i parametri che ne permettono il corretto funzionamento tramite sensori (pressione gomme, livello olio, ecc.) e di poter comunicare con altre automobili al fine di prevedere code e conseguenti incidenti.
- Petrolio e gas: in tale tipo di industria i sensori sono utilizzati per il monitoraggio dell'integrità dei tubi e della pressione, del livello del combustibile a disposizione, della corrosione.
- Robotica: i robot sono dispositivi intelligenti in grado di percepire, calibrare, comunicare, misurare e se necessario ricalibrare per ottenere più accuratezza. Tali robot possono essere in grado di comunicare via wireless, trovando impiego nella realizzazione di sistemi intelligenti real-time, nell'automazione industriale.

1.3 - Le sfide tecniche da affrontare

- Risorse ristrette: la progettazione e l'implementazione delle IWSN è limitata da tre tipi di risorse: energia, memoria e capacità di elaborazione. Ciò è dovuto, in particolare, alle limitate dimensioni che tali sensori devono assumere.
- Topologia dinamica e dure condizioni ambientali: nell'ambiente industriale, la topologia e la connettività delle reti può fare la differenza, e se scelta male, può causare la perdita del collegamento con i nodi, dato che essi sono soggetti a interferenze RF, ambienti caustici e corrosivi, alta umidità, vibrazioni, sporcizia e polvere.
- Esigenze di qualità del servizio (QoS): data l'ampia varietà di applicazioni possibili per gli IWSN, è richiesto che ciascuna abbia un'adeguata qualità del servizio. Inoltre è importante anche la tempistica con cui i dati sono trasmessi ed elaborati, nei sistemi in cui è richiesto un controllo real-time, i cui dati devono avere tempi di latenza ridotti e predicibili.
- Ridondanza dei dati: le osservazioni dei sensori sono strettamente correlate nel dominio dello spazio e del tempo, sono quindi sovrabbondanti. Pertanto per limitare le trasmissioni e lo spreco di energia, i dati ridondanti devono essere ridotti tramite opportune elaborazioni.
- Errori nei pacchetti e capacità variabile dei collegamenti: contrariamente ai sistemi con reti cablate, la capacità raggiungibile (ovvero la quantità di dati trasferiti nell'unità di tempo in condizioni ottimali, misurata in kb/s) di un collegamento wireless dipende dal livello di interferenza percepito al ricevitore, ed alti bit error rate (tra 10^-2 e 10^-6) sono osservati nella

comunicazione. Inoltre i sistemi wireless presentano comunemente caratteristiche variabili nel tempo e nello spazio dovute all'ostruzione ed all'ambiente rumoroso; quindi la capacità e il ritardo di ogni collegamento dipendono dalla locazione dei nodi e variano continuamente , rendendo difficili le previsioni del QoS.

- Sicurezza: la sicurezza è senza dubbio uno dei requisiti più importanti nella progettazione del sistema, infatti non deve essere possibile alcuna intrusione esterna. Gli attacchi passivi consistono nel rilevare il traffico e scoprire il contenuto dei messaggi, gli attacchi attivi nella modifica e nell'interruzione del servizio, o addirittura nella cattura di un nodo. Il protocollo deve quindi essere immune a tali tipi di attacchi.
- Schieramento su larga scala e architettura ad hoc: alcuni sistemi IWSN contengono centinaia o addirittura migliaia di nodi, che potrebbero essere distribuiti in maniera casuale nell'ambiente. La rete deve essere pertanto gestibile, nonostante l'alto numero di utenze, ed organizzarsi autonomamente.
- Integrazione con internet ed altre reti: è di fondamentale importanza per lo sviluppo commerciale degli IWSN che essi possano interfacciarsi con internet ed altre reti, per salvare o per rendere accessibili i dati da qualunque postazione. Per realizzare questo bisogno, la rete IWSN dovrebbe essere integrata con architettura IP. La correnti piattaforme di reti di sensori utilizzano gateway in grado di connetterli ad Internet, tuttavia in futuro i sensori potrebbero avere connettività IP.

Capitolo 2 – Sviluppo di una IWSN

In questo capitolo si analizzano gli obiettivi di progettazione di una IWSN da un punto di vista generale, per poi scendere nel dettaglio ed avere un primo approccio tecnico, occupandosi dello sviluppo hardware, software, dell'architettura e del protocollo.

2.1 - Obiettivi di progettazione:

- Nodi con sensori a basso costo e di minime dimensioni: questi infatti sono parametri essenziali se si vuole creare una rete di nodi su larga scala. Da notare che devono essere tenuti in considerazione anche i costi di manutenzione, di installazione e di eventuali modifiche.
- Architettura scalabile e protocolli efficienti: è necessario sviluppare un'architettura flessibile e scalabile che può essere utilizzata per tutte le funzioni adibite alle IWSN all'interno della stessa infrastruttura. Un sistema modulare e gerarchico può migliorare la flessibilità, affidabilità e robustezza. In più, può essere richiesta la compatibilità con i sistemi esistenti, che operano ad esempio in Ethernet.
- Fusione dati e elaborazione locale: anziché trasmettere i dati grezzi, un nodo deve essere in grado di elaborare i dati autonomamente e trasmettere solo i dati necessari o richiesti, riducendo così la possibilità di sovraccaricare la rete.
- Progettazione efficiente delle risorse: è importante implementare un sistema che risparmi energia, dato che questo è uno dei dati di valutazione della qualità del servizio (QoS), in particolare viene considerato il tempo di vita della rete. Per migliorare tale tempo, si agisce su ciascun componente della rete, si utilizzano protocolli a basso consumo, modalità di risparmio energia nel livello MAC.
- Auto-configurazione e auto-organizzazione: vista la possibilità che i nodi vadano offline temporaneamente per guasti o altre ragioni, le reti IWSN hanno bisogno di architettura e protocolli auto-organizzanti, devono cioè lavorare in topologia dinamica; grazie a ciò, i nodi possono essere sostituiti, rimossi o modificati senza causare il malfunzionamento di tutta la rete.
- Operazioni di rete adattabili: l'adattabilità del sistema è importante perchè permette all'utente finale di creare nuovi tipi di operazioni e nuovi tipi di connettività.
- Sincronizzazione temporale: può essere richiesto che tutti i sensori debbano collaborare tra loro ed eseguire i compiti ad essi assegnati, ciò comporta che la sincronizzazione tra nodi sia una delle necessità chiave nella progettazione del protocollo che deve rispettare le necessità in termini di tempo delle

applicazioni, in particolare in quelle che effettuano un controllo real-time.

- Tolleranza dei guasti e affidabilità: i dati devono essere trasferiti al nodo di controllo in maniera attendibile e nella stessa maniera, il nodo di controllo deve trasmettere i dati affidabilmente agli altri nodi (comandi, query, programmazione, assegnazione compiti, ecc.). Attualmente esistono metodi di verifica e correzione di ciascuno livello della comunicazione in grado di garantire il corretto funzionamento della rete.
- Progettazione specifica in base alle applicazioni: la progettazione deve variare in base al QoS richiesto e quindi anche al budget disponibile.
- Solida progettazione: il sistema deve essere robusto e sicuro, quindi la comunicazione ad ogni livello deve avvenire in maniera da non permettere intrusioni, catture di nodi ed altri tipi di disturbi tramite meccanismi quali l'autenticazione e la criptazione dei messaggi.

2.2 - Sviluppo hardware

Un nodo-sensore ha la funzione di rilevare, immagazzinare, elaborare e trasmettere i dati. L'architettura di quest'ultimo è composta da quattro principali componenti:

- I sensori: sono dispositivi che trasformano in grandezze misurabili (tipicamente grandezze elettriche) grandezze fisiche come temperatura, pressione, luce, suono, accelerazione, ecc. Il segnale analogico prodotto dal sensore è convertito in segnale digitale da un ADC e mandato al processore. Il campionamento, il condizionamento del segnale e la conversione ADC sono le principali cause di consumo di potenza.
- Il processore: l'unità di elaborazione che è generalmente molto piccola si occupa dell'elaborazione dei dati provenienti dal sensore, della gestione delle altre unità periferiche e del controllo del nodo.
- Il ricetrasmettitore: connette il nodo alla rete, trasmettendo e ricevendo i dati, ed ha quattro possibili stati (trasmissione, ricezione, idle, sleep). Nello stato Idle, ovvero lo stato di “attesa” c'è consumo rilevante, quasi quanto in stato di ricezione, quindi è conveniente spegnere il ricetrasmettitore nel caso non si stia trasmettendo né ricevendo.
- Risorse energetiche: il consumo di potenza è principalmente dovuto a tre funzioni, ovvero rilevamento, elaborazioni dati e comunicazione. Normalmente è la comunicazione quella che consuma in quantitativo maggiore, questo rende chiaro quanto è importante porre in stato di sleep il ricetrasmettitore ogni volta che è possibile, e quindi anche la sincronizzazione del sistema. Il tempo di vita di una rete dipende quindi dalle batterie, ed in caso di caduta di un nodo, la topologia e l'organizzazione della rete vengono modificati. Al momento sono in studio tecniche di raccolta dell'energia e sistemi per ridurre i consumi al

minimo (sleeping schedules, ottimizzazioni dinamiche e variazioni al clock). Di seguito viene mostrato un esempio di nodo di una rete (Figura 1), nel caso specifico si tratta di un sensore digitale di umidità e temperatura , prodotto da Telos; nella figura si può distinguere il modulo trasmettitore CC2420, il sensore (SHT11, prodotto da Sensirion), il microcontrollore (MP430 prodotto da Texas Instruments) inoltre come visibile, questo tipo di nodo può essere programmato via USB.
In Figura 2 è illustrato uno schema che riassume i principali componenti di un nodo sensore.

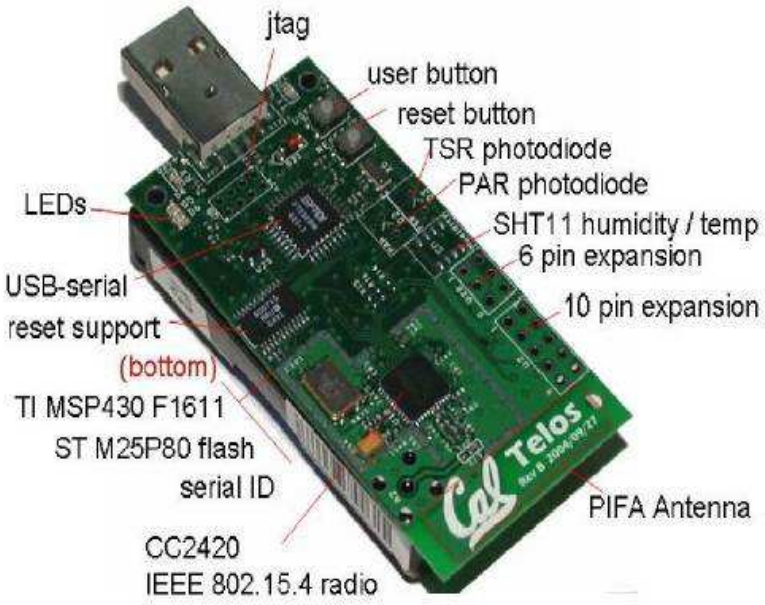


Figura 1

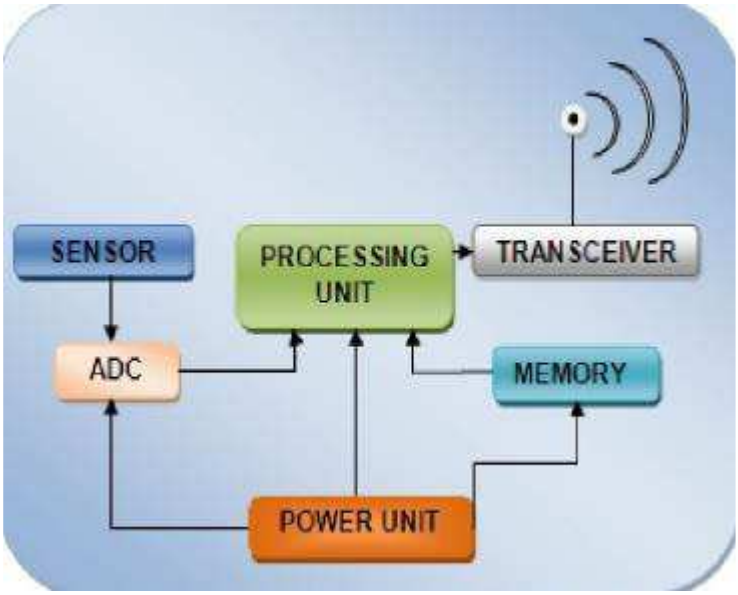


Figura 2

2.3 - Tecniche per la raccolta di energia

Nelle IWSN, per massimizzare il tempo di vita di una rete, oltre a puntare al minimo consumo, sono in studio anche tecniche per la produzione di energia elettrica all'interno dello stesso nodo; è infatti già stato dimostrato che è possibile creare sistemi che hanno durata illimitata basati su pannelli fotovoltaici, batterie e grandi condensatori.
La ricerca inoltre si sta focalizzando anche su altri modi per produrre energia, dalle onde radio, dalla conversione termoelettrica, dalle vibrazioni e dal corpo umano.
Sfortunatamente, dalle onde radio si ricava da un campo elettrico di 1 V/m solo 0,26 mW/cm^2 contro i 100 mW/cm^2 prodotti da una cella solare.
La conversione da fonti termoelettriche potrebbe invece non essere considerata appropriata all'ambiente di lavoro dei sensori, mentre la conversione in energia delle vibrazioni potrebbe essere molto interessante per le IWSN, essa si basa (generatore di potenza magnetico vibrazionale) sulla vibrazione di un magnete o di una bobina, e può produrre da decine di µW in un sistema microelettromeccanico fino a più di un mW in un sistema di grandi dimensioni.
Altri generatori vibrazionali sono basati su un capacitore le cui lamine, vibrando generano potenze dell'ordine di 10 µW.
Esistono infine metodi di produzione di energia basati su materiali piezoelettrici, che possono generare tra 100 e 300 µW a cm^3.

2.4 - Sviluppo software

2.4.1 - Api

Il software applicativo (API, Application Programming Interface) deve essere accessibile da una semplice interfaccia di programmazione personalizzata, sia per gli standard IWSN che per le specifiche richieste del cliente; questo permette anche rapidi sviluppi e installazioni della rete. Con un API adeguato, la basilare complessità della rete può essere trasparente all'utente finale esperto nelle specifiche applicazioni del cliente ma non in reti e comunicazioni wireless.
Dopo la disposizione sul campo, la gestione della rete e gli strumenti di servizio sono indispensabili; un esempio di tools di servizio potrebbe essere un display che mostra lo stato di connettività della rete e permette di regolare i parametri di un dato nodo. Gli strumenti di servizio possono però anche analizzare lo stato della intera rete trovando i nodi non funzionanti, fare upgrade di firmware e fare previsioni sul QoS.

2.4.2 - Il sistema operativo

Il sistema operativo nelle reti wireless di sensori è tipicamente meno complesso dei sistemi operativi general purpose; esso è un insieme di subroutine e si occupa del controllo e della gestione dei componenti hardware, nonchè nella gestione delle periferiche; inoltre nelle reti IWSN ha il difficile compito di trovare un compromesso tra consumo di energia e QoS
TinyOS è un esempio di sistema operativo per sistemi con piccoli nodi, basato sulla programmazione ad eventi: quando un evento esterno si presenta, come la ricezione di un pacchetto dati o la lettura del valore rilevato da un sensore, TinyOS segnala l'appropriato evento e lo gestisce secondo la procedura prevista (ovvero programmata); esso incorpora un'architettura di componenti base che minimizza il codice ed è dotato di una piattaforma flessibile che permette l'implementazione di nuovi protocolli di comunicazione, funziona con 178b di memoria e supporta comunicazioni, multitasking e codice modulare.
Inoltre spesso oltre al sistema operativo si fa ricorso ad un middleware, che permette una gestione più efficace: il middleware astrae il sistema come una collezione di oggetti estremamente distribuiti e permette alle applicazioni dei sensori industriali di generare richieste e compiti (query e task), raccogliere risposte e risultati e monitorare i cambi all'interno della rete.

2.5 - Architettura di sistema e progettazione del protocollo

2.5.1 - Architettura di rete

Nelle IWSN, progettare una rete scalabile è di primaria importanza, uno degli approcci più classici è schierare i sensori in maniera omogenea e programmare ciascuno di essi a compiere la maggior quantità di applicazioni possibile. Altrimenti, un alternativo modo di progettare è quello multistrato, ovvero di utilizzare elementi eterogenei, essi saranno suddivisi in elementi a basso utilizzo di potenza ed eseguiranno compiti semplici, ed elementi ad alto consumo di potenza come i gateway che eseguiranno compiti più complessi e non limitati in energia; questa architettura quindi, permette un consumo più sostenibile.

2.5.2 - Topologia di rete

Attualmente per le reti wireless sono utilizzate, per lo più, tre tipi di topologie

(illustrate in Figura 3): a stella (star), ad albero (tree) e mesh; ciascuna di queste tipologie ha delle proprietà che possono essere adeguate o meno alle esigenze applicative:

a)Star: è il tipo di rete più semplice ed il più utilizzato, consiste solo di dispositivi finali e di un nodo posto al centro della rete, detto Cluster o Hub, che li coordina; il principale svantaggio è che questa rete è solo two-hops, cioè la distanza percorsa dai dati può essere al massimo di due salti (dispositivo finale – hub – dispositivo finale), e questo è limitante in termini di copertura della rete; inoltre il punto debole della rete a stella è l'hub, che in caso di guasto, disabilita tutta la rete. I suoi vantaggi invece sono dati dall'alta scalabilità, possono infatti essere aggiunti nodi senza alcun problema, fino al limite gestibile dall'hub.

b)Tree: a differenza della rete a stella permette reti multi-hop e quindi un ampia copertura di rete, una sua limitazione è il fatto che i collegamenti vicini alla radice devono essere altamente scalabili dato che con l'ampliamento della rete potrebbero essere sottoposti ad alto traffico di comunicazione, e la caduta di uno di questi collegamenti disconnetterebbe tutta la parte di rete ad essa collegata. La latenza dei dati di questa topologia è più alta rispetto a quella a stella, a causa del numero di nodi da cui un dato deve passare e del più alto traffico in alcuni collegamenti come abbiamo già accennato.

c)Mesh: anche questo topologia permette la comunicazione multi-hop, ed ha inoltre il vantaggio di avere più direzioni per trasmettere un pacchetto da un nodo ad un altro, qualità che rende questo tipo di rete il più affidabile in assoluto, dato che in caso di caduta di nodi o collegamenti, la comunicazione può avvenire per vie alternative.

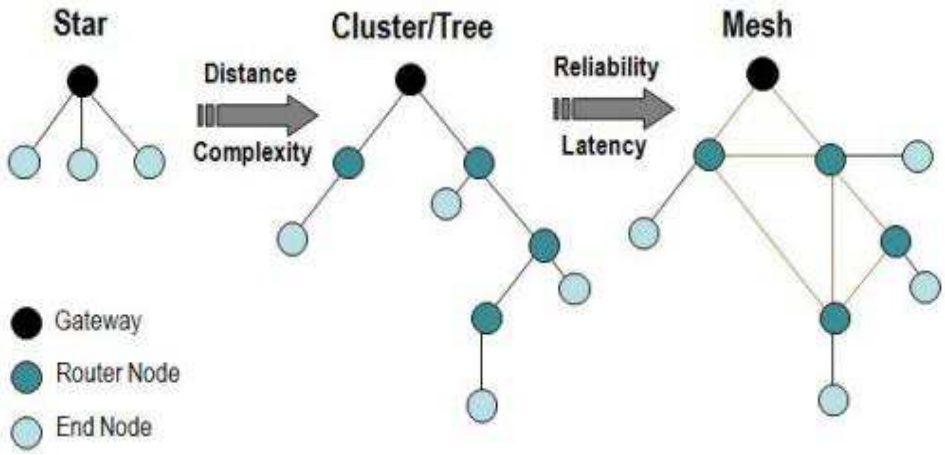


Figura 3

2.5.3 - Aggregazione e fusione dei dati

L'elaborazione dei dati grezzi prima della trasmissione, riduce la quantità della comunicazione e ne migliora l'efficienza. L'aggregazione e la fusione dei dati è un meccanismo localizzato per i dati in ingresso nella rete, infatti questi meccanismi riducono la lunghezza ed il numero dei pacchetti, eliminando la ridondanza dei dati. Se ad esempio un sensore intermedio riceve dei dati da più nodi sensori che hanno generato dati, anziché inoltrare i dati per intero, controlla la ridondanza tra di essi e li ricombina prima di trasmetterli. Questo sistema aiuta a raggiungere dense trasmissioni di dati.

Capitolo 3 - Gli standard basati su IEEE802.15.4

Dato che le reti IWSN sono attualmente in sviluppo, il processo di standardizzazione è ancora in atto, ed al momento, sebbene più compagnie stiano lavorando per sviluppare vari tipi di standard, non sono molti quelli già in commercio.
I principali standard sono ZigBee, WirelessHART, UWB, IEFT 6 LoWPAN, ISA100.11a, Bluetooth e bluetooth low energy.
Tutti gli standard elencati, ad eccezione del Bluetooth, utilizzano come livello fisico lo IEEE 802.15.4, e si differenziano per i livelli superiori (Network, Transport se presente, Application).

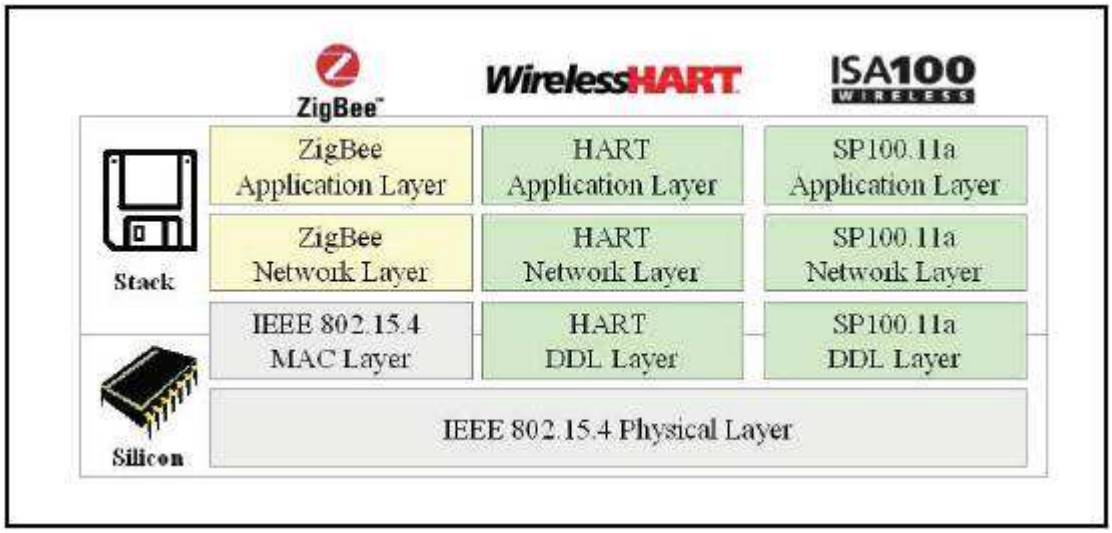


Figura 4

In questo capitolo, dopo una breve digressione sui livelli del modello OSI e sullo standard IEEE 802.15.4, introdurremo i quattro standard più significativi: ZigBee, ISA100.11, WirelessHART ed OCARI.

3.1 - Il modello ISO/OSI

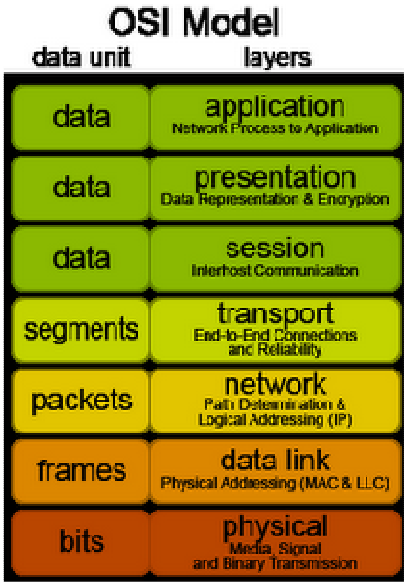


Figura 5

Il modello ISO/OSI è stato creato per semplificare l'implementazione delle reti di telecomunicazioni, ed è formato da uno stack di protocolli, ciascuno dei quali è detto livello o layer (Figura 5).
Tale modello inoltre, definisce quali sono i compiti di ciascun livello.
Lo scopo di ciascun livello è quello di fornire servizi ai livelli superiori, mascherando come questi servizi sono stati implementati; quindi, nella trasmissione di un dato, ciascun livello aggiunge delle informazioni (che poi saranno decodificate dallo stesso livello del nodo ricevente) fino a giungere al livello fisico che effettua la trasmissione.
Vediamo quali sono i livelli, e quali sono i loro compiti:

- Livello 1 – Physical: trasmette sequenze di bit sul canale di comunicazione.
- Livello 2 – Data Link (formato da due sottolivelli: MAC – Media Access Control, ed LCC – Logical Link Control): si occupa della trasmissione affidabile delle trame (frame) mediante l'inserimento di Frame Control Sequence (FCS).
- Livello 3 – Network: si occupa dell'instradamento dei messaggi (routing).
- Livello 4 – Transport: fornisce il trasferimento trasparente end-to-end dell'informazione (frammentazione del flusso in frame, correzione errori, prevenzione della congestione,ecc.).
- Livello 5 – Session: organizza il dialogo e la sincronizzazione tra due programmi applicativi e lo scambio di dati tra essi.
- Livello 6 – Presentation: gestisce la sintassi e la codifica dell'informazione da trasferire (es: traduzione in codice ASCIII).
- Livello 7 – Application: è il programma applicativo che si interfaccia con l'utente.

3.2 - Lo standard IEEE 802.15.4

Lo standard 802.15.4 viene approvato nell’estate del 2003 nella sua prima versione e definisce il protocollo di trasmissione a basso livello tramite comunicazione radio, quindi fornisce le specifiche per il funzionamento del livello fisico e del livello MAC; è stato concepito per regolamentare le reti WPAN (Wireless Personal Area Network) che hanno modeste dimensioni, di solito inferiori ai 30m.
Dal 2003 in poi ha avuto varie evoluzioni (802.15.4a – 2007, 802.15.4c – 2009, 802.15.4d – 2009) fino a giungere alla versione attuale.
In questo paragrafo si descrive lo standard analizzandone livello fisico, livello MAC ed infine la struttura di un suo superframe.
802.15.4 non nasce per trasportare dati multimediali come voce e video, ma come soluzione per la trasmissione di pacchetti dati di piccole dimensioni, esso è infatti adatto alla creazione di reti con basso data rate e raggiunge velocità di trasferimento dati di 250 kb/s.

3.2.1 - Livello fisico (PHY)

Il livello fisico 802.15.4 supporta 3 diverse frequenze operazionali:

- 2.4 GHz
- 915 MHz
- 868 MHz

e tre diversi data rate:

- 20 kb/s
- 100 kb/s
- 250 kb/s

La distanza coperta dalla trasmissione varia con il data rate e va da 10m a 100m
Ciascun data rate è ottenuto con una tipologia di trasmissione e modulazione diverse, come mostrato in tabella 1.

Tabella1

Data rate	**Trasmissione**	**Modulazione**
20 kb/s	Binaria	BPSK (Binary Phase Shift Keying)
100 kb/s	Binaria	GFSK (Gaussian Frequency Shift Keying)
250 kb/s	16 simboli ortogonale	O-QPSK (Offset Quadrature Phase Shift Keying)

Gli standard wireless quali ZigBee, WirelessHART e ISA100.11a utilizzano per lo più la banda di frequenza 2.4 GHz (2,4 – 2,4835 GHz) ed il data rate più alto (250 kb/s) in cui, dal lato trasmettitore, i dati sono divisi in gruppi da 4 bits, ciascun gruppo è poi codificato con uno dei 16 simboli disponibili e trasmesso con la modulazione O-QPSK via wireless, demodulato e decodificato al ricevitore, infine inviato al MAC.

3.2.2 - Livello data link

802.15.4 MAC supporta due tipi di topologie di rete:

- Star, in cui vi è un nodo coordinatore attraverso la quale passa ogni comunicazione.
- Peer to peer, in cui ciascun nodo comunica con un altro direttamente, senza intermediari.

e specifica due modalità di accesso al canale, per i nodi:

- Beacon enabled mode: un frame detto Beacon è trasmesso dal coordinator all'inizio di ogni superframe, tale Beacon, contiene informazioni sulla

sincronizzazione temporale, configurazioni di sistema ed una lista dei dispositivi che devono trasmettere dati al coordinator.

- Non Beacon enabled mode: ai dispositivi è permessa la trasmissione di dati in ogni momento, purchè necessario.

Inoltre Il MAC del 802.15.4 permette l'utilizzo di reti con 2 tipi di dispositivi: FFD (Full Function Device) ed RFD (Reduced Function Device)

3.2.3 - Struttura di un superframe

Il superframe consiste di due parti principali: periodo attivo e periodo inattivo; la durata di questi due periodi è controllata dal coordinatore tramite il settaggio di due paramentri (BO – Beacon Order, SO – Superframe Order).
Il periodo attivo è dedicato alla trasmissione e ricezione dei dati e consiste di due parti, la cui durata è ancora regolata dal coordinatore per massimizzare le prestazioni: CAP (Contention Access Period) e CFP (Contention Free Period). Durante il CAP i nodi accedono al canale grazie al protocollo CSMA/CA , di cui si parlerà in seguito. Il CFP invece è riservato dal coordinatore ai dispositivi con applicazioni real-time ed è composto da GTS (Guaranteed Time Slots).
Durante il periodo inattivo, tutti i dispositivi sono in modalità “sleep” per risparmio energetico.

3.2.4 - CSMA/CA+GTS

Come già detto, 802.15.4 utilizza durante la fase CAP il CSMA/CA e riserva ai GTS la fase CFP.
Il CSMA/CA (Carrier Sense Multiple Access Collision Avoidance) è un ben collaudato metodo di accesso multiplo, utilizzato appunto per la trasmissione su un canale condiviso da più dispositivi; prima di iniziare la trasmissione, ciascun nodo verifica l’assenza di altro traffico sul canale (rilevando la presenza della portante), se il canale è libero, il dispositivo inizia la trasmissione, in caso contrario deve attendere un tempo casuale e poi riascoltare il canale. Questo metodo è applicabile in celle con pochi dispositivi finali, dato che il CSMA viene usato per flussi di dati senza ordine di priorità e senza garanzie temporali.
Il fatto che le richieste siano fatte in ordine casuale nel CSMA/CA implica un rischio di collisione tra dispositivi finali della stessa cella, che potrebbero iniziare la trasmissione nello stesso istante.
Per risolvere questo problema è stato introdotto il CFP che fornisce slot dedicati ciascuno ad un dispositivo, chiamati GTS (guaranteed time slot).Nella pratica il

dispositivo finale richiede al coordinatore un allocazione GTS durante il prossimo superframe, se le dimensioni massime del CFP non sono state raggiunte, il timeslot può essere assegnato; inoltre se un dispositivo finale non utilizza il suo GTS entro un dato tratto di tempo, tale GTS è automaticamente soppresso.
Questo metodo di accesso mostra molti vantaggi sia in termini di tempi di ritardo sia in termini energetici (un dispositivo finale può essere messo in sleep eccetto durante il suo GTS).

3.2.5 - Sviluppi futuri

E' importante segnalare che è in avanzata fase di studio una nuova versione di questo standard, denominata IEEE 802.15.4e, basata su meccanismi di accesso multiplo di tipo TSCH (Time Slotted Channel Hopping), in grado di garantire una maggiore robustezza alle interferenze elettromagnetiche esterne e ridotte probabilità di collisione dei dati.

3.3 - ZigBee

Zigbee è uno standard di comunicazione wireless basata sulla specifica IEEE802.15.4, a cui vengono aggiunti i livelli Networtk ed Application (Figura 6), che saranno descritti in seguito.

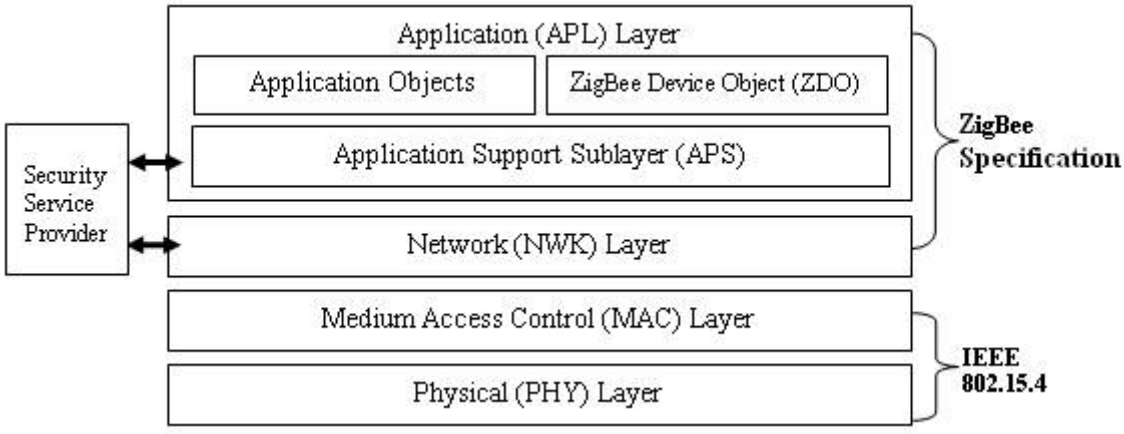


Figura 6

ZigBee 1.0 è stata approvato a dicembre 2004 ed è disponibile ai membri della ZigBee Alliance (all'epoca formata da poco più di 100 aziende), nel 2007 viene messa a punto con lo sviluppo e l'approvazione di ZigBee PRO.
ZigBee ha trovato ampio utilizzo nel campo industriale, in particolare nella comunicazione di sistemi embedded con un consumo molto basso di potenza, campo in cui può essere considerato senza dubbio la tecnologia wireless più utilizzata,

questo perchè presenta caratteristiche adatte all'impiego industriale, qui elencate:

- Propone uno stack protocollo leggero (32Kb – 64 Kb) per le applicazioni che richiedono un basso data rate e bassa latenza.
- Permette una alta efficienza energetica, infatti la durata della batteria di un nodo varia da pochi mesi fino a svariati anni, dato che ciascun nodo assorbe meno di 10µA in modalità sleep e può tornare in modalità attiva in meno di 300µs.
- Supporta più topologie di rete (star, tree, mesh), sebbene la star resti la più utilizzata.
- Garantisce alta affidabilità e sicurezza.

ZigBee opera nelle frequenze radio assegnate per scopi industriali, scientifici e medici (ISM), come specificato da 802.15.4: 868 MHz, 915 MHz e 2.4 GHz; la banda 2,4 GHz in particolare è suddivisa in 16 canali, da 5 MHz ciascuno; inoltre ha una copertura di 10m ed un data rate che va da 10 Kb/s fino a 250 kb/s, limite imposto da 802.15.4.

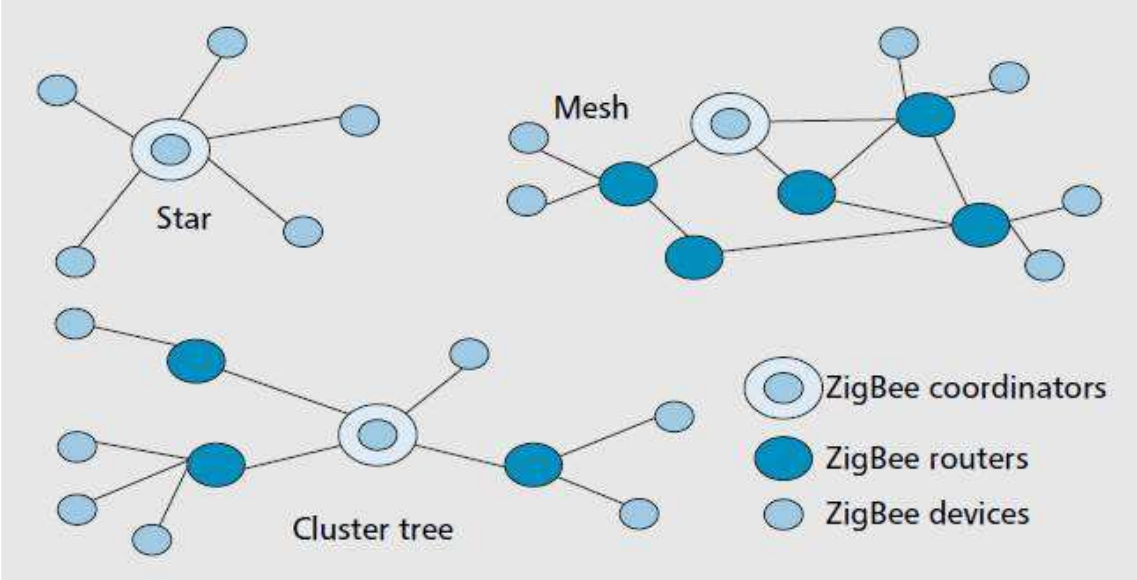


Figura 7

I dispositivi ZigBee possono essere di tre tipi, come possiamo vedere in figura 7:

1. ZigBee Coordinator (ZC): ha funzione di radice nel caso di topologia ad albero ed hub nel caso di topologia a stella; in ogni rete può essercene solo uno e ha compiti di gestione, di controllo ed è dotato di memoria per il salvataggio dei dati.
2. ZigBee Router (ZR): funzionano appunto da router, passando i dati da e verso altri dispositivi, vengono in particolare utilizzati per estendere le reti. Nelle reti

ad albero, lo ZR trasferisce dati e messaggi di controllo attraverso la rete utilizzando un indirizzamento gerarchico.

3. ZigBee End Device (ZED): sono i meno costosi e possono svolgere solo funzioni elementari quali trasmettere i propri dati e comunicare con gli ZC o ZR.

ZigBee ha però una limitazione importante per quanto riguarda la mobilità dei dispositivi, infatti la rimappatura della rete richiede un tempo elevato (fino a 10s), pertanto non è possibile utilizzare questo standard in reti dalla topologia instabile, e tanto meno con nodi in movimento.

3.3.1 - Livello Network

I compiti del livello Network nelle specifiche ZigBee sono di seguito elencati:

- Indirizzamento dei pacchetti dati dal nodo sorgente a quello destinazione.
- Connessione e disconnessione dei nodi alla rete.
- Configurazione di nuovi dispositivi connessi alla rete.
- Assegnazione indirizzo a tutti i nodi della rete e riconfigurazione in caso di modifiche alla topologia della rete.
- Scoperta delle vicinanze, necessaria per l'indirizzamento.

Ciascun nodo di una rete ZigBee è identificato con un indirizzo unico di 64 bit, come previsto da IEEE802.15.4, a cui viene aggiunto un indirizzo per le comunicazioni interne alla rete di 16 bit.
Per quanto riguarda l'indirizzamento di un pacchetto dati ed il calcolo del percorso da seguire, ZigBee prevede 3 tipologie di indirizzamento:

- Indirizzamento gerarchico: viene calcolato un percorso ad albero della rete in cui il coordinatore (ZC) funge da root, pertanto il frame contenente i dati risale l'albero dal nodo sorgente fino allo ZC, se il nodo destinazione si trova su tale percorso avrà già ricevuto i dati, altrimenti il coordinatore provvede a far riscendere il pacchetto nell'albero fino a destinazione.
- Indirizzamento gerarchico con RREQ: questo tipo di indirizzamento deriva dal più conosciuto AODV (Ad hoc Ondemand Distance Vector) e ciascun percorso non passa necessariamente per il coordinatore. Ci sono due comandi in questo protocollo: route request (RREQ) che viene generato dal nodo sorgente e inoltrato di nodo in nodo fino al raggiungimento del nodo destinazione; route reply (RREP) che viene generato dal nodo destinazione una volta ricevuto il pacchetto e ripercorre il percorso al contrario.
- Trasmissione dati source-routed: ciascun nodo, dopo la prima trasmissione ad un nodo, memorizza una tabella (source-routed-table) che indica il percorso più breve per il raggiungimento di ciascun altro nodo ed utilizza la suddetta tabella per le successive trasmissioni.

3.3.2 - Livello Application

Il livello Application (APL) ZigBee consiste di due sottolivelli: APS (Application Support Sublayer) e ZDO (ZigBee Device Object).
APS ha la responsabilità di rilevare le richieste ed i bisogni di ciascun nodo e di inoltrare messaggi tra i dispositivi della rete
Lo ZDO invece definisce il ruolo di ogni nodo all'interno della rete (ZC, ZR, ZED), determinando quali e quanti nodi ci sono sulle rete e stabilendo una relazione stabile tra di essi; inoltre deve anche rispondere alle richieste di ciascun nodo (rilevate dal APS).

3.3.3 - Architettura di un nodo

Come visto nel cap.2 un nodo ha la funzione di collezionare i dati richiesti e di trasmetterli al coordinatore; nel caso specifico dello standard ZigBee un nodo è composto da cinque parti:

- modulo sensore: contiene il sensore, il circuito di elaborazione del segnale ed il convertitore ADC
- modulo MCU: è l'unità di elaborazione, nelle versioni recenti ZigBee utilizza un controllore MSP430F149 (Prodotto dalla texas Insutruments) a 16 bit che ha un bassissimo consumo, un bus dati non espandibile, frequenza di clock 8 MHz, un convertitore A/D a 12 bit e può gestire 16 interrupt veloci.
- modulo ricetrasmettitore: Zigbee utilizza un trasmettitore CC2420 o CC2530 (prodotti dalla Texas Instruments) che permette di criptare il segnale trasmesso ed effettua un controllo checksum sulla trasmissione.
- modulo di memoria
- modulo di potenza: è composto da una o più batterie.

Segue uno schema esemplificativo di un nodo ZigBee con sensore di temperatura DS18B20 (Figura 8) ed una fotografia di un generico nodo ZigBee (Figura 9):

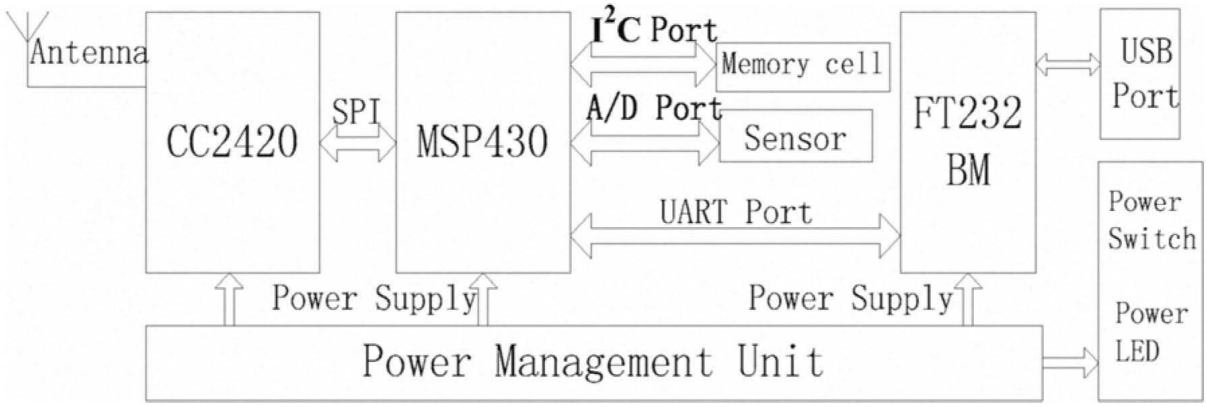


Figura 8

Figura 9

3.3.4 - Sistemi di sicurezza in ZigBee

Per rendere sicura la comunicazione tra dispositivi, ZigBee opera su ciascun livello; infatti sono già previsti sistemi al livello MAC per controllare l'integrità di un messaggio trasmesso e la possibile ritrasmissione, specificati dallo standard IEEE802.15.4; in aggiunta a ciò, ZigBee effettua altri controlli d'integrità ed inoltre cripta ciascun messaggio secondo uno standard internazionale detto AES-128 (Advanced Encryption Standard, basato su algoritmi a chiave simmetrica, a 128 bit), applicandolo al livello network ed ancora il livello Application può inserire un ulteriore encrypting generando una coppia di chiavi.
ZigBee è considerato generalmente un sistema molto sicuro per la sua applicazione.

3.4 - WirelessHART

WirelessHART è uno standard per reti di sensori wireless sviluppato dal 2004 dalla HART Communication Foundation (HCF) ed è stato approvato dalla IEC nel recente 2010 e si basa sull'utilizzo del protocollo HART (Highway Addressable Remote Transducer Protocol).
WirelessHART come i precedenti standard è basato sull'utilizzo di IEEE802.15.4 di cui utilizza il livello fisico e MAC, opera esclusivamente alla frequenza di 2.4 GHz per le trasmissioni; tipicamente una rete WirelessHART è di tipo mesh, tuttavia lo standard è in grado di supportare anche reti a stella.
Esistono tre tipi di dispositivi in una rete WirelessHart:

- WirelessHART Field Device: sono i dispositivi che operano sul campo, quali sensori ed attuatori
- WirelessHART Gateway: fanno da ponte tra i dispositivi di campo ed il WNM, possono essere utilizzati per conversioni di protocollo. In ogni rete può esserci uno o più gateways, inoltre più gateway aumentano l'affidabilità della rete.
- WirelessHART Network Manager: è unico nella rete e ha compiti di gestione, monitoraggio dello stato della rete, mappatura della rete, gestione delle “routing tables”.

3.4.1 - Livelli Network e Transport

I livelli Network e Transport cooperano per rendere efficace e sicura la comunicazione tra due dispositivi finali (field device); in particolare nello standard WirelessHART due protocolli di indirizzamento sono possibili:

- Graph routing: un grafo è un insieme di percorsi che collega ciascun nodo ad un qualunque altro. Il WNM crea tale grafo e lo trasmette a ciascun dispositivo che lo utilizza per trasmettere i dati, inserendo nell'header del pacchetto un ID che indica il nodo destinazione.
- Source routing: in questo caso invece, un nodo indica nell'header una lista ordinata dei nodi che deve attraversare il pacchetto per giungere alla sua destinazione, ogni nodo per cui il pacchetto passa rimuove dall'header il proprio indirizzo e manda al prossimo della lista fino a che la destinazione non è stata raggiunta.

3.4.2 - Livello Application

In WirelessHART il livello Application ha il compito di decifrare il contenuto dei messaggi dei dispositivi di campo, estrarne il numero del comando, eseguire il comando e generare una risposta.
Inoltre tale layer deve monitorare e segnalare lo stato della rete e dei dispositivi.

3.4.3 - Sistemi di sicurezza in WirelessHART

WirelessHART è notoriamente uno standard molto sicuro, anch'esso, come ZigBee utilizza AES a 128 bit come metodo di encrypting, a cui il livello network aggiunge altre chiavi di sicurezza; quattro chiavi possibili sono definite in WirelessHART:

- Public keys: utilizzate per generare il MIC (Message Integrity Code) dai dispositivi che accedono alla rete
- Network keys: sono condivise da tutti i dispositivi della rete ed utilizzate per generare il MIC dai dispositivi esistenti
- Join keys: ogni dispositivo è provvisto di una join key unica, che serve per l'accesso alla rete e l'autenticazione
- Session keys: generata dal WNM, è unica per ciascuna coppia di nodi ed è utilizzata per la trasmissione di dati tra i due.

3.5 - ISA100.11a

ISA100.11a è uno standard per reti wireless sviluppato dalla International Society of Automation (ISA), approvato e rilasciato a settembre 2009.
ISA100.11a punta ad ottenere le performance necessarie per il monitoraggio periodico ed il controllo di processi, dove latenze dell'ordine dei 100ms possono essere tollerate in generale, con poche eccezioni.
ISA100.11a adotta i livelli fisico e MAC dello standard IEEE802.15.4 ed opera esclusivamente nelle frequenze ISM 2.4 GHz, adottando la velocità massima (250 kb/s) e utilizzando solo 16 canali.
L'architettura di ISA100.11a ha più livelli di quella ZigBee, in essa il DMAP (Device Management Application Process, una speciale applicazione utente che ha la funzione di gestire, monitorare, configurare la rete) accede direttamente ai livelli Data-Link, Network, Transport ed Application.
ISA100.11a è stato progettato in particolare per le applicazioni sul campo industriale (field); fisicamente una rete ISA è composta da tre tipologie di dispositivi, come si può vedere nella figura 10:

- DL (Data Link subnet): include i dispositivi I/O ed i dispositivi di indirizzamento, cioè tutti i dispositivi che operano sul campo come sensori ed attuatori.
- BN (Backbone Network): include tutti i dispositivi che fanno parte della rete dorsale, ovvero routers, gateways e la dorsale stessa.
- MN (Manager Network): ne fanno parte i dispositivi che controllano il sistema wireless e che si interfacciano con l'operatore.

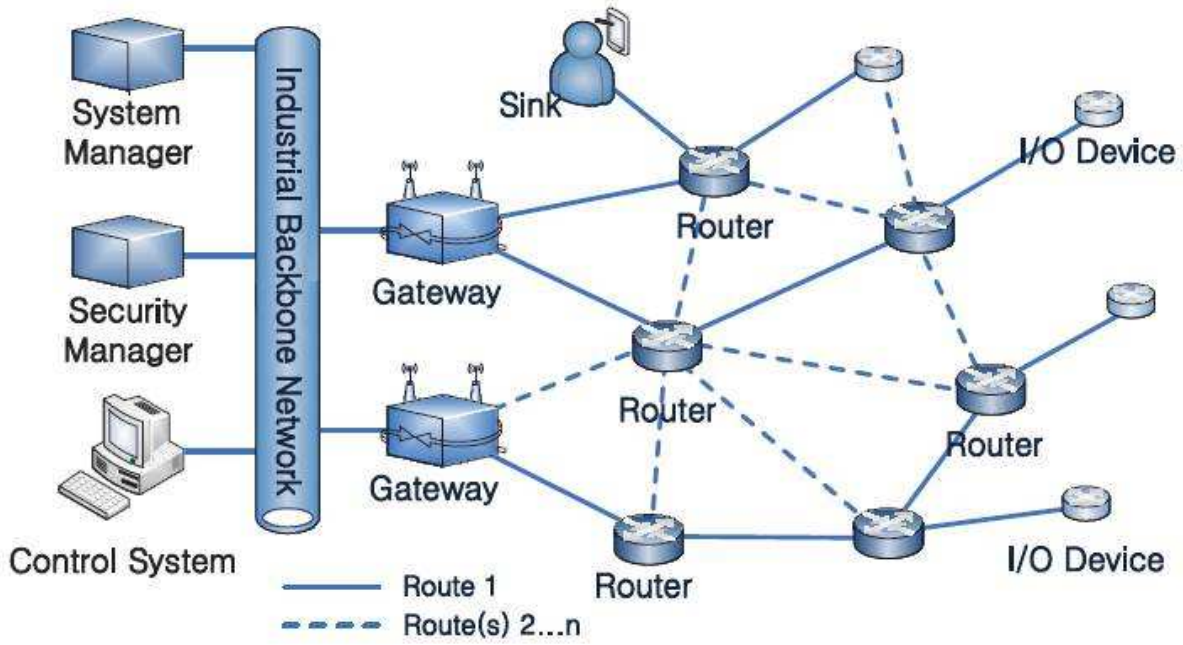


Figura 10

La sincronizzazione tra i dispositivi è effettuata da un nodo detto System Manager, appartenente alla categoria MN.
L'indirizzamento dei dati ed il percorso da seguire per una trasmissione sono controllati dal MN, che dota ciascun dispositivo di una “routing table”, come avviene in ZigBee; ciascun dato proveniente dal campo può passare direttamente al gateway (one hop) o servirsi anche di un router (multihop).
Durante il ciclo globale, a ciascun dispositivo DL è assegnato un timeslot che varia tra 10ms e 12ms, la cui durata è stabilita dal MN nel momento in cui il dispositivo DL accede alla rete.
In ISA100.11a ciascuna operazione di trasmissione può essere effettuata in tre modi:

- slotted channel hopping: ogni timeslot usa differenti canali radio per completare una trasmissione (con possibilità di acknowledgement opzionale), questo metodo è quello predefinito dal MN e permette una forte riduzione dei disturbi dovuti alle interferenze radio .
- slow channel hopping: un certo numero di timeslot (solitamente tra 100ms e

400ms) è raggruppato e trasmesso su un unico canale; questo metodo è preferito nel caso di dispositivi lenti o con problemi di sincronizzazione
- metodo ibrido: è una combinazione dei due precedenti.

E' giusto ricordare, che come previsto dallo standard IEEE802.15.4 ciascuno dei tre metodi utilizza il CSMA/CA per l'accesso al canale.
Tuttavia, il punto di forza dello standard ISA100.11a può essere considerato la flessibilità nella gestione dei dispositivi, infatti ISA100.11a differisce da 802.15.4 per quanto riguarda i superframes a livello di DL: come sappiamo un superframe è costituito da una sequenza di timeslots ed ha una durata fissa in tutti gli standard; Isa100.11a permette al NM di far variare la durata di un superframe da dispositivo a dispositivo; questa configurazione flessibile aiuta a gestire diverse classi di traffico; generalmente un superframe di bassa durata significa bassa latenza per i dati ma maggiore occupazione di banda e consumo energetico.

3.6 - OCARI

OCARI (Optimization of Communication for Ad hoc Reliable Industrial networks project) è uno standard wireless sviluppato da un consorzio di aziende quali:

- Électricité de France
- DCNS
- LATTIS
- LIMOS
- INRIA
- Telit-RF Technologies
- LRI

L'OCARI è stato creato per essere utilizzato principalmente in centrali elettriche e navi da guerra, partendo dalle specifiche ZigBee e completando o modificando le funzioni che non corrispondono alle richieste applicative.
OCARI utilizza, come gli altri standard, il livello fisico IEEE 802.15.4, opera alla frequenza di 2.4 GHz, mentre i livelli superiori sono propri di OCARI ed introducono delle novità fondamentali qui sotto elencate:

- Un livello MAC proprio con metodi di accesso deterministici dei nodi alla rete, in grado di garantire una bassissima latenza ai pacchetti, chiamato MaCARI.
- Un sistema di indirizzamento (routing) molto efficiente dal punto di vista energetico, detto EOLSR.
- Un sistema di coordinazione e sincronizzazione tra i nodi, finalizzato al risparmio energetico, detto SERENA.

Tuttavia, OCARI è dotato anche di altre caratteristiche innovative, quale il supporto della mobilità dei nodi (alla velocità del passo umano) e di applicazioni HART.
Le reti OCARI (di cui è visibile un esempio in Figura 11) prevedono tre tipi di nodi che danno alla rete una struttura gerarchica:

- Workshop (o Cluster) Coordinator (FFD): ha il compito di inizializzare e gestire la rete, quindi assegna gli indirizzi e funziona da gateway verso la rete di comunicazione dorsale dell'infrastruttura. Solitamente è unico nella rete. Il dominio Workshop è lo spazio entro cui un unico Workshop Coordinator riesce a ricevere il segnale a potenza sufficiente.
- Cell Coordinator (CC): ha il compito di coordinare una cella, quindi comunica con i dispositivi finali della sua stessa cella, tramite una topologia a stella, e con il Workshop, mandando in dati in modalità push, o nel caso di sistemi con costrizioni temporali in modalità tree.
- Dispositivi finali (RFD): tali nodi sono quelli che sono a diretto contatto con il sensore-attuatore e non possono comunicare tra loro, ma solo con il Cell Coordinator, che se necessario reindirizza i pacchetti al nodo destinatario. I dispositivi finali hanno limitate risorse energetiche e possono svolgere solo funzioni elementari, a differenza degli altri due tipi che sono full function.

Nella rete vi è inoltre anche un nodo chiamato Time Server che fa da sorgente di clock e quindi si occupa della sincronizzazione di un dominio Workshop.

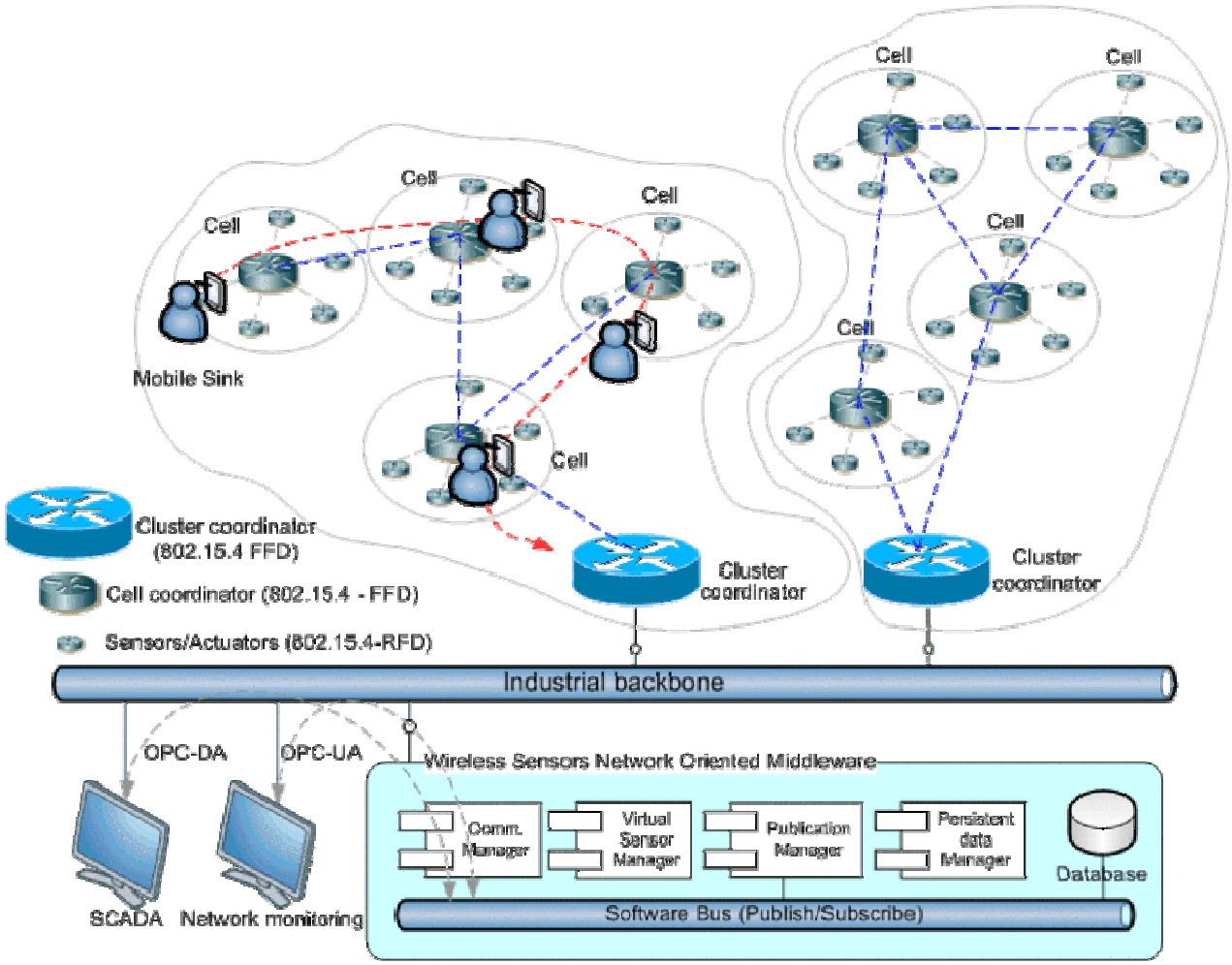


Figura 11

3.6.1 - MaCARI

Un MAC deterministico deve garantire l'accesso al canale radio ad ogni dispositivo ogni determinato periodo di tempo (ciclo globale), ed affichè tale MAC possa essere definito efficiente dal punto di vista energetico, deve porre in modalità sleep più a lungo possibile ogni dispositivo; MaCARI è stato progettato trovando un compromesso tra questi due bisogni, ed inoltre permette anche l'indirizzamento multihop.
Per comprendere completamente il funzionamento del protocollo MaCARI, dobbiamo studiarlo sotto due punti di vista, cioè il punto di vista globale (intercelle) e quello intracelle; infatti MaCARI ha diversi protocolli per le due tipologie di comunicazione.

3.6.2 - Protocollo globale

Nel MaCARI i frames possono essere indirizzati direttamente o indirettamente al nodo destinazione, viene infatti calcolato uno spanning tree della topologia della rete , che funge appunto da percorso, e che ha come radice il nodo Cell Coordinator che deve indirizzare il pacchetto.
Il ciclo globale della comunicazione, gestito dal coordinatore della rete (Workshop) è suddiviso in tre distinte fasi temporali: la sincronizzazione, le attività pianificate, le attività non pianificate.
La sincronizzazione parte dal nodo Time Server che trasmette un segnale, tale segnale è passato da un nodo all'altro (hop by hop), ed infine, ogni CC ripete il segnale ad un tempo prestabilito dal Workshop. Alla fine di questa fase tutti i nodi della rete sono sincronizzati e può iniziare la trasmissione.
La seconda fase, quella in cui si svolgono le attività pianificate, è suddivisa in più intervalli (slot), ciascuno dei quali è assegnato ad una cella. Durante uno slot, sono in modalità attiva il Workshop, il CC della cella in questione, e tutti i suoi dispositivi finali, mentre tutti gli altri dispositivi della rete sono in sleep; quando questo intervallo sta per terminare, il CC, dopo aver raccolto i dati dagli RFD, comunica con il Workshop in modalità polling/selecting.
Durante la fase di attività non pianificate, il MaCARI gestisce l'attività dei nodi in accordo con le richieste del SERENA (SchEdule RoutEr Nodes Activity) e la trasmissione dei frames avviene osservando il protocollo di indirizzamento a risparmio energetico EOLSR; durante questo periodo gli spazi temporali sono assegnati secondo dei colori, ovvero durante un dato slot tutti i nodi di un certo colore possono trasmettere simultaneamente ed in maniera indipendente, senza incorrere in collisioni; quindi l'assegnazione dei colori ai nodi ha funzione di coordinazione, cioè di fare in modo che tutti i nodi di uno stesso colore, possono trasmettere nello stesso

momento.
Abbiamo visto quindi, come il protocollo risulti deterministico, visto che durante la seconda fase (attività pianificate) a ciascun cella e dispositivo è dedicato un spazio predeterminato.
Per quanto riguarda l'efficienza energetica, con il MaCARI, durante la sincronizzazione una cella può entrare in sleep non appena riceve il segnale atteso, durante la fase di attività pianificate, tutti dispositivi finali di una cella possono restare in sleep eccetto durante lo slot assegnato, mentre durante la fase di attività non pianificate la gestione dipende dal protocollo SERENA.

3.6.3 - Protocollo intracelle

Esaminiamo ora il protocollo di comunicazione che viene utilizzato per la comunicazione tra i dispositivi finali ed il CC, all'interno di una stessa cella; esso prevede quattro opzioni, due delle quali non verranno descritte perchè già trattate nei paragrafi precedenti:

1. CSMA/CA
2. CSMA/CA + GTS
3. CSMA/CA + GTS(n): l'allocazione statica di un GTS può essere eccessiva in alcuni casi, ad esempio per un sensore di temperatura un intero GTS può essere troppo lungo, quindi si potrebbe pensare di allocare diversi servizi al dispositivo finale a seconda del tipo di comunicazione. In questo metodo di accesso, un GTS è dedicato al dispositivo finale in accordo con la periodicità con cui ha bisogno di trasmettere i dati al CC, se n=0 in ogni superframe, se n=1 ogni 2 superframes, ed in generale ogni 2^n superframes.

Sicuramente questo metodo può essere considerato più efficiente del precedente nella gestione delle risorse.

4. CSMA/CA + GTS(n) + PDS: un inconveniente che si può presentare nella precedente opzione è dato dal fatto che la GTSrequest deve essere fatta necessariamente dal dispositivo finale in modalità CSMA/CA durante il CAP; tale richiesta non è garantita, quindi tale opzione non è completamente deterministica. Per alcuni critici sensori che richiedono un alto QoS, può essere opportuno dedicare uno slot iniziale, detto PDS (Previously Dedicated Slot), che è di fatto un GTS dedicato a priori, che il dispositivo può utilizzare anche per richiedere uno o più successivi GTS.

3.6.4 - NwCARI

Il livello Network del protocollo OCARI prende il nome di NwCARI ed è costituito da due moduli: EOLSR e SERENA, già accennati, qui descritti in dettaglio.

3.6.4.1 - EOLSR

EOLSR è un'estensione del protocollo OLSR (già utilizzato in altri standard), è stato sviluppato dal concetto di EMPR (Energy according MultiPoint Relays) e consiste principalmente di due funzionalità:

- scoperta delle vicinanze: ogni nodo router acquisisce la conoscenza di tutti i nodi alla distanza rispettivamente di uno o due salti scambiando con essi periodici messaggi; seleziona quindi i nodi distanti un salto come EMPR in maniera da poter ricoprire anche i nodi distanti due salti.
- diffusione nella topologia: un nodo selezionato come EMPR manda un messaggio di controllo di topologia nella rete; questo messaggio è inoltrato se e solo se è il primo ricevuto.

La funzione di queste due operazioni è quella di avere una mappatura aggiornata della rete e delle posizioni dei nodi.
Il metodo EOLSR, a differenza dell'OLSR, nel momento in cui seleziona i nodi EMPR, tiene conto anche della autonomia residua dei nodi, escludendoli se essa è bassa. Il percorso per la trasmissione è poi scelto scegliendo il più economico in termini di consumi energetici per spedire un pacchetto, tenendo conto anche dell'energia persa in trasmissione, ricezione ed interferenze.

3.6.4.2 - SERENA

SERENA (SchEdule RoutEr Nodes Activity) è una strategia per il risparmio energetico, che come spiegato precedentemente, che entra in funzione durante la terza fase del ciclo globale.
Come sappiamo un nodo, per risparmiare energia deve essere in modalità sleep ogni qual volta è possibile, deve però essere awake per trasmettere e ricevere, quindi c'è bisogno di coordinazione tra i nodi. SERENA crea questa coordinazione come segue: un nodo è in modalità awake solo durante il suo slot e durante gli slot concessi ai suoi vicini (one hop). Gli slot sono assegnati in base al colore di un nodo ed al suo traffico.
Per evitare collisioni, un nodo colora se stesso se e solo se tutti i nodi a più di due salti con una più alta priorità sono già colorati, scegliendo il primo colore disponibile con priorità più bassa.
Da notare che quando i nodi si muovono ci possono essere conflitti di colore e due nodi che sono distanti uno o due salti potrebbero avere lo stesso colore, tali conflitti devono essere rilevati e risolti, quindi il nodo con maggiore priorità deve mantenere il suo colore mentre gli altri devono variare.

Sicuramente si può dire che i due metodi permettono un notevole risparmio energetico data la prolungata permanenza negli stati di idle e sleep, e permettono quindi un maggiore utilizzo di potenza nella trasmissione e nella ricezione. Quantificando l'utilizzo del EOLSR allunga il tempo di vita di un nodo del 40%, del SERENA del 195% e l'utilizzo combinato di entrambi del 275%.

3.6.4.3 - Le strategie per l' efficienza energetica di OCARI

Nel protocollo OCARI l'algoritmo di indirizzamento seleziona un percorso per la trasmissione hop by hop, escludendo i nodi con un basso livello di carica residua della batteria, quindi quando un nodo ha un basso livello di batteria residua, esso viene utilizzato solo per operazioni di base ed elementari, per evitare la sua caduta. Per essere però al corrente del livello di carica residua in una batteria, bisogna conoscere il costo in termini di energia di ogni operazione effettuata dal nodo; questo è uno degli obiettivi del protocollo di indirizzamento OCARI, cioè di dare un valore noto alla batteria iniziale e poi di sottrarre i valori delle operazioni compiute dal nodo di volta in volta, in maniera da poter monitorare il tempo di vita rimanente, attraverso una funzione esponenziale (questa operazione è svolta da un modulo detto Energy Service Provider).

Capitolo 5 – La tecnologia WISA

WISA (Wireless Interface for Sensors and Actuators) è un concetto di sistema sviluppato dalla multinazionale svizzera-svedese ABB, che fornisce un sistema di comunicazione wireless (WISA-COM) ed un sistema di alimentazione wireless (WISA-POWER).
WISA è l'unico standard per reti wireless industriali a basarsi su IEE802.15.1, del quale si darà una descrizione; WISA è stato presentato ed applicato per la prima volta nel 2002 ed ha trovato sempre più largo utilizzo nell'automazione industriale.

4.1 - Lo standard 802.15.1

Lo standard 802.15.1, comunemente chiamato Bluetooth, definisce un metodo di trasmissione a corto raggio, sicuro e veloce, per la comunicazione di dispositivi in reti WPAN e ha conosciuto grande popolarità negli ultimi anni anche nel campo della telefonia e dell'informatica; esso è stato sviluppato da Ericsson nel 1998 e poi formalizzato da un consorzio di aziende, detto SIG (Bluetooth Special Interest Group, di cui fanno parte IBM, Intel, Toshiba, Nokia, la stessa Ericsson e molte altre aziende); nel corso dell'ultimo decennio è stato modificato più volte, aumentando la propria efficienza e sicurezza in particolare, fino a giungere alla versione attualmente in uso: Bluetooth 4.0, approvata a luglio 2010.
Bluetooth opera alla frequenza di 2.4 GHz e la sua trasmissione copre un raggio che può arrivare fino a 100m: esistono infatti 3 classi di dispositivi Bluetooth che hanno una copertura che va da 1m (classe 3) fino a 100m (classe 1), ovviamente una copertura maggiore comporta una potenza di trasmissione maggiore.
Nelle tabelle 2 e 3 sono indicate le classi con relative potenze di trasmissione e le frequenze a cui Bluetooth opera nei principali paesi industrializzati:

Power Class	Maximum Output Power (Pmax)
1	100 mW (20 dBm)
2	2.5 mW (4 dBm)
3	1 mW (0 dBm)

Power classes

Tabella 2

Country	Frequency Range	RF Channels
Europe* & USA	2400 - 2483.5 MHz	f = 2402 + k MHz
Japan	2471 - 2497 MHz	f = 2473 + k MHz
Spain	2445 - 2475 MHz	f = 2449 + k MHz
France	2446.5 - 2483.5 MHz	f = 2454 + k MHz

Tabella 3

Bluetooth può raggiungere elevate velocità di data rate (fino a 1 Mb/s nella prima versione, 3 Mb/s nella più recente) ed utilizza la modulazione DQPSK (Differential Quadrature Phase Shift Keying) shiftata di 45° a 2 Mb/s ed una 8DPSK a 3 Mb/s.
La dimensione dei pacchetti dati trasmessi, nello standard 802.15.1 è variabile, ciascun pacchetto può occupare un numero differente di time slots (la durata di ciascun time slot è di 625µs).
Per mitigare le interferenze create dalla coesistenza con altri protocolli che operano nella banda ISM, Bluetooth utilizza un sistema innovativo, detto FHSS (Frequency Hopping Spread Spectrum), secondo cui i dati sono divisi e trasmessi in 79 bande da 1 MHz ciascuna, situate nel range di frequenze 2402-2480 MHz
Tuttavia, lo standard 802.15.1 ha una importante limitazione: ciascun Master può connettersi con un massimo di 7 Slaves (tale rete è detta Piconet); per questo motivo è stato ideato il concetto di Scatternet, ovvero un insieme di Piconet che operano sulla stessa area; ciascuna Piconet mantiene il proprio Master, e può interagire con le altre.
Nelle ultime versioni, Bluetooth presenta innumerevoli caratteristiche ed opzioni, tra cui c'è anche la possibilità di trasmettere utilizzando 802.11, dove richiesto, per aumentare il data rate fino a 24 Mb/s e quindi poter trasmettere anche segnali video in streaming.

4.2 - WISA-COM

Il protocollo di comunicazione WISA è stato progettato su misura per la comunicazione dei sensori nel campo industriale, opera nelle frequenze ISM (2,4 Ghz) e permette lo scambio di dati a 32 bit in entrambe le direzioni.
Una rete WISA ha topologia a stella, il cui nodo master è la stazione base (o base station), che a sua volta è gestita dal master del bus di campo (ovvero il PLC), collegato ad essa via cavo.
Il metodo di accesso al canale utilizzato da WISA è il TDMA (Time Division Multiple Access), simile al CSMA in quanto anch'esso divide un frame in più slot, di cui alcuni sono utilizzati per il downlink (comunicazione con i sensori) ed altri per l'uplink (comunicazione con gli attuatori).

Figura 12

La stazione base, visibile in figura 12, ha 4 canali per comunicare uplink ed uno downlink contemporaneamente. A ciascuno slave è dedicato uno slot esclusivo di 128 o 64 µs su uno dei quattro canali uplink, mentre il downlink è diviso in maniera che otto slave dividono uno slot di 128 µs; inoltre essa è in grado di ricevere segnali forti e deboli in slot uno successivo all'altro sulla stessa frequenza, se la loro differenza è fino a 59 dB, ed ha una forte resistenza alle interferenze dei canali adiacenti.
Tutti i nodi sono posti in modalità sleep, eccetto durante lo slot ad essi dedicato; la stazione base invece, è in sleep solo quando non deve trasmettere e consuma in tale modalità 1 mA, mentre in fase di trasmissione/ricezione il consumo sale a 45 mA.
In conclusione, WISA-COM presenta numerosi vantaggi rispetto ai protocolli esistenti in commercio (ZigBee, ISA100.11a, ecc), qui riassunti:

- Numero di nodi: una singola stazione base WISA permette il collegamento di 120 slave a input singolo o 60 slave a IO multipli .
- Bassa latenza: il tempo di risposta di un nodo è di 2 ms, nel caso limite in cui i nodi da gestire siano 120 a input singolo.
- TER (Telegram Error Rate) minore di 10^-9, un valore talmente basso da poter essere comparato ai sistemi cablati.
- Alta immunità alle interferenze create dai nodi della stessa rete o dalle altre reti wireless presenti sul campo.

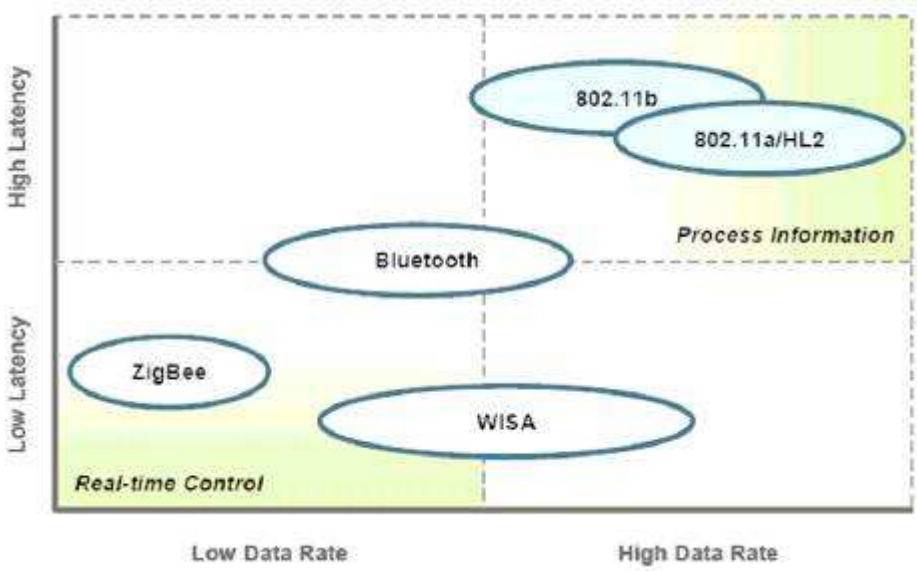


Figura 13

4.3 - WISA-POWER

WISA-POWER è un innovativo sistema di alimentazione dei nodi che sfrutta l'accoppiamento tra due avvolgimenti; esso utilizza un campo magnetico alternato alla frequenza di circa 120 kHz.
Per funzionare ha bisogno che i nodi da alimentare siano circondati da un loop primario (Figura 14), che genera un campo magnetico della potenza di migliaia di milliwatt , mentre all'interno di ciascun nodo vi è l'avvolgimento secondario che quindi fornisce la potenza necessaria al funzionamento.

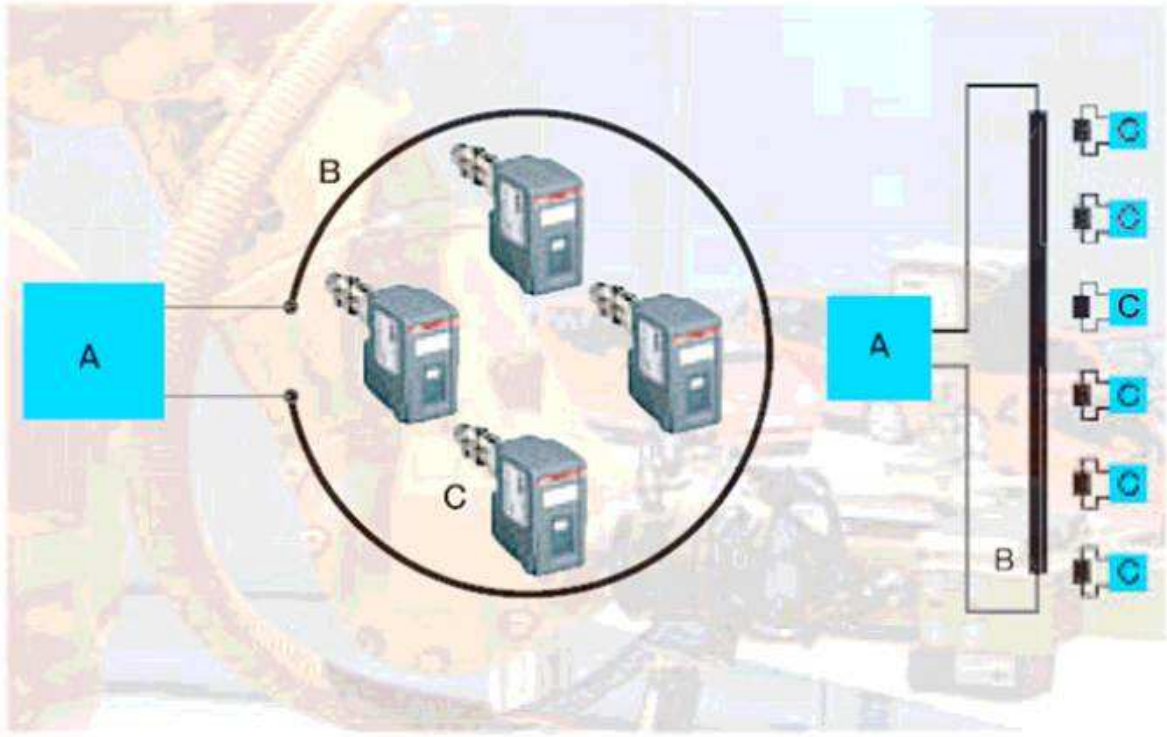


Figura 14

Nella pratica gli avvolgimenti, sia primario che secondario, sono tre, e non uno, questo perchè, in caso di nodi rotanti ,o più in generale in movimento, non si può sapere a priori l'orientamento dei sensori.
Nella figura 15 si può vedere un nodo WISA, in cui è visibile l'avvolgimento secondario.

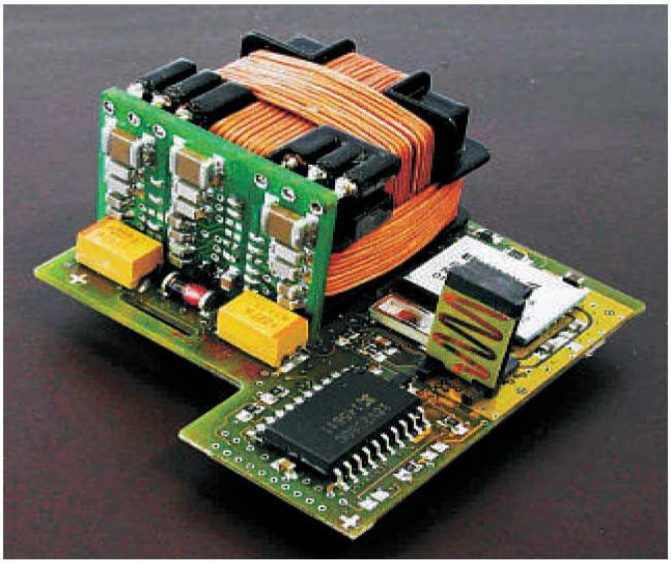


Figura 15

Conclusioni

Abbiamo visto in questa tesi quanto la tecnologia wireless stia crescendo, e le molte opzioni disponibili sul mercato.
Tuttavia, non si crede che il wireless possa rimpiazzare in tempi brevi le reti cablate; la sua principale funzione resta, per il momento, quella di collegare zone non raggiungibili via cavo ed ambienti ostili, per monitorarli.
I motivi per cui tale rimpiazzo non può avvenire sono due: la mancanza di affidabilità del mezzo trasmissivo e la ristrettezza della banda.
Il collegamento wireless infatti, può interrompersi facilmente, ad esempio a causa di ostacoli fisici e richiedere ritrasmissioni numerose, che in ambito industriale non sono accettabili.
Per quanto riguarda la ristrettezza della banda, il problema è l'esiguo numero di segnali che può essere trasmesso nella porzione di banda utlizzabile; da questo punto di vista sono stati fatti numerosi progressi negli ultimi anni grazie a tecniche avanzate di modulazione, tuttavia il canale radio resta limitato, per cui le trasmissioni wireless devono essere in numero ridotto.
Attualmente, la ricerca è concentrata sulla risoluzione di questi due limiti e non è prevedibile quali risultati saranno ottenuti nei prossimi anni.
Il contributo del wireless nel campo industriale è comunque da considerarsi importante e si prevede per i prossimi anni una crescita del mercato, come è avvenuto nell'ultimo decennio.

Bibliografia

[1] Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches
Vehbi C. Gungor, Member, IEEE, and Gerhard P. Hancke, Senior Member, IEEE

[2] Which Wireless Technology forIndustrial Wireless Sensor Networks? The Development of OCARI Technology
Khaldoun Al Agha, Marc-Henry Bertin, Tuan Dang, Alexandre Guitton, Pascale Minet, Thierry Val, and Jean-Baptiste Viollet

[3]Integration of aWireless I/O Interface for PROFIBUS and PROFINET for Factory Automation
Jimmy Kjellsson, Anne Elisabeth Vallestad, Richard Steigmann, and Dacfey Dzung

[4]Wireless Sensor Networks for Industrial Applications
Xingfa Shen , Zhi Wang, and Youxian Sun

[5]Industrial Control using Wireless Sensor Networks
Kamran Khakpour M.H Shenassa

[6]Wireless Sensor Networks for Industrial Processes
M. Antoniou, M.C.Boon, P.N.Green, P.R.Green and T.A.York

[7]Industrial Wireless Sensor Networks and Standardizations -The Trend of Wireless Sensor Networks for Process Automation
Li Zheng

[8]Industrial Utilization of Wireless Sensor Networks
Shanmugaraj.M, R.Prabakaran, V.R.Sarma Dhulipala

[9]Performance evaluation of the SERENA algorithm to SchEdule RoutEr Nodes Activity in wireless ad hoc and sensor networks
Saoucene Mahfoudh and Pascale Minet

[10]WISA – Wireless Interface for Sensors and Actuators in Industrial Applications
Peter Vikström

[11]Improving Power Efficiency of Bluetooth Systems with EDR Packets and Efficient Channel Coding
M. A. M. Mohamed El-Bendary, A. E. Abu El-Azm, N.A.El-Fishawy, M. A. R. El-Tokhy, and F. Shawky

[12]A Cross-Layer Mechanism for Solving Hidden Device Problem in IEEE 802.15.4 Wireless Sensor Networks
Hsueh-Wen Tseng, Shan-Chi Yang, Ping-Cheng Yeh, and Ai-Chun Pang

[13]Performance Evaluation of IEEE 802.15.4 Based IPMAC Network
Tarique Haider, Mariam Yusuf

[14]IEEE 802.15.4 PHY Analysis: Power Spectrum and Error Performance
Priyanka Gupta, Stephen G. Wilson

[15]Performance Evaluation of Priority CSMA-CA - Mechanism on ISA100.11a Wireless Network
Nguyen Quoc Dinh, Sung-Wook Kim, and Dong-Sung Kim

[16]Network Management in WirelessHART Network for Industry Application
Zuo Yun, Ling Zhihao, Liu Luming

[17]WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control
Jianping Song, Song Han, Aloysius K. Mok

[18]When HART Goes Wireless: Understanding and Implementing the WirelessHART Standard
Anna N. Kim, Fredrik Hekland, Stig Petersen, Paula Doyle

[19]WirelessHART versus ISA100.11a
Stig Petersen and Simon Carlsen

[20]Remote-controlled Home Robot Server with Zigbee Sensor Network
Jae-Min Choi, Byeong-Kyu Ahn, You-Sung Cha and Tae-Yong Kuc

[21]Voice Communications over ZigBee Networks
Chonggang Wang and Kazem Sohraby, Rittwik Jana, Lusheng Ji, and Mahmoud Daneshmand

[22]Study on Security of Wireless Sensor Network Based on ZigBee Standard
Bin Yang

[23]Study on Electrical Switching Device Junction Temperature Monitoring System Based on ZigBee Technology
Zhang Gang, Liu Shuguang

[24]802.15.4 - IEEE Standard for information technology