Alma Mater Studiorum - Università di Bologna

Scuola di Scienze

Corso di Laurea Triennale in Informatica

Tecniche di localizzazione indoor per il tracciamento di oggetti: studio per un caso reale

Tesi di Laurea in Architettura degli Elaboratori

Relatore:
Chiar.mo Prof.
Vittorio Ghini

Presentata da:
Vittorio Lanzara

Sessione I
2012/2013

Introduzione

Nuovi sviluppi nella comunicazione wireless e nell'elettronica hanno permesso lo sviluppo di dispositivi poco costosi, poco energivori e multifunzione, piccoli in dimensione e in grado di comunicare a breve distanza. Collegati con tecnologie senza fili e disponibili in gran numero, questi sensori hanno offerto opportunità senza precedenti nel monitorare e controllare case, città, e l'ambiente. In aggiunta, i sensori wireless hanno anche una vasta gamma di applicazioni nella sicurezza, generando nuove capacità di riconoscimento e sorveglianza, unite ad altre finalità tattiche. La capacità di localizzazione di questi congegni poi è altamente studiata e ricercata, per applicazioni che vanno dal monitoraggio di incendi, della qualità dell'acqua e dell'agricoltura di precisione alla gestione di inventari, di sistemi anti intrusione, monitoraggio del traffico e di parametri medici. Da questo esteso panorama di utilizzi, è scaturita l'idea di un impiego di queste reti in un contesto particolare.
L'esperienza maturata in ambito fieristico mi ha portato a considerare una problematica da sempre sentita, ma che non ha mai trovato soluzioni soddisfacenti o definitive, che è quella della protezione dei beni dai rapinatori. In questo ultimo periodo, dove si assiste ad un progressivo ma repentino calo degli affari dovuto ad una congiuntura economica mondiale sfavorevole, il problema è più avvertito da chi, in vari settori, vede un sempre più basso margine di compensazione ai furti.

Il documento è stato organizzato nel modo seguente:

- descrizione dell'ambiente operativo, del problema che si vuole risolvere e delle caratteristiche che un eventuale sistema debba avere per dirimere in maniera efficiente tutte le questioni considerate (Cap. 1)

- overview sulle reti di sensori, breve enunciazione storica, descrizione delle caratteristiche e degli standard presenti attualmente, riferimenti alla tecnologia Rfid

(Cap. 2)

- analisi delle tecniche di localizzazione nelle Wireless Sensor Network, in particolare la distinzione tra reti basate su ancore e non, algoritmi più comuni utilizzati nell'individuazione della posizione di oggetti, tematiche di ranging e positioning (Cap. 3)

- studio delle caratteristiche del sistema in relazione alle tecnologie presenti sul mercato, tenendo in discrimine costi, dimensioni, eventuale connubio di più tecniche, limiti normativi e di tecnologia (Cap. 4)

- conclusioni e sviluppi futuri, con designazioni qualitative sulle debolezze riscontrate e indicazioni di progetto da tenere in osservazione (Cap. 5)

Indice Generale

Elenco delle figure

[XIV] Confronto WHART, ZigBee
T. Lennvall, S. Svensson, F. Hekland “A Comparison of WirelessHART and ZigBee for Industrial Applications”, IEEE 2008

[XV] Bluetooth
http://m.eet.com/media/1049270/Table1.gif

[XVI] Differenze Tag attivi e Tag passivi
http://www.csa.com/discoveryguides/rfid/images/attributes.jpg

[XVII] TOA
http://www.sensorwiki.org/lib/exe/fetch.php/sensors/ultrasound_echo_ranging2.jpg?w=&h=&cache=cache

[XVIII] TDOA
http://www.intechopen.com/source/html/16531/media/image5.png

[XIX] AOA
http://www.surehealth.it/wp-content/uploads/2012/01/SensoriUbisense1.png

[XX] RSSI
http://www.cisco.com/en/US/i/200001-300000/220001-230000/223001-224000/223329.jpg

[XXI] Equazione di Friis
http://lifetimepowerkit.com/wp-content/uploads/2009/01/friis-equation1-300x223.jpg

[XXII] MinMax
http://origin-ars.els-cdn.com/content/image/1-s2.0-S1474034610000984-gr2.jpg

[XXIII] Triangolazione
https://doc.novay.nl/dsweb/GetRendition/Document-12997/html/index153002.jpg

[XXIV] Struttura WSN
http://www.wavecomm.it/immagini/wsn2.jpg

[XXV] comparazione frequenze RFID
http://www.ibtechnology.co.uk/images/rfid_comparison_table.png

Capitolo 1

Il problema

1.1 Il caso studiato

Al giorno d'oggi, chi gestisce o dirige un negozio od un'attività commerciale, oltre a dover fare i conti con un fisco particolarmente esigente , deve far fronte ad una calamità che purtroppo pare sia in continuo aumento: i reati predatori. Il Sole24Ore, noto giornale economico, analizzando i dati del Ministero degli Interni relativi ai delitti denunciati all'autorità giudiziaria, ha constatato l´incremento di rapine, furti e scippi negli ultimi due anni, in un quadro delinquenziale non particolarmente rassicurante. Nel 2011 c'è stato un rovesciamento del trend rispetto agli anni precedenti, quando i reati registravano una decrescita; dal 2010 al 2011 sono infatti aumentati del 5,4%. In particolare, i reati per rapina hanno visto un´incremento del 20,1% nello stesso periodo considerato.

I negozi e gli esercizi commerciali in generale sono diventati meta di reato prediletta, rispetto al passato dove le banche attiravano la quota più alta d'intenti delinquenziali, poiché i furti sono aumentati del 16%, mentre le rapine del 24%. [1]

Il 2012 non è andato meglio, confermando l'infausto andamento dell'anno precedente: complessivamente, i reati sono aumentati dell'1,3%. In special modo, i reati contro il patrimonio hanno avuto incrementi considerevoli: i furti in casa (+15,5 per cento), gli scippi (+13 per cento) e i borseggi (+11 per cento). [2]

Il caso considerato fa riferimento ad un particolare ambito commerciale, quello dell'esposizione fieristica, dove i commercianti si riuniscono in quello che può essere ritenuto un grande magazzino dove ogni zona ha un proprietario.

Questo particolare situazione favorisce l'evento delittuoso, poiché in questo scenario si hanno diversi limiti e restrizioni a protezione sicura della merce degli espositori.

Tra questi :

- impossibilità di un sistema di antitaccheggio univoco
- poca resa delle telecamere di sorveglianza
- presenza di grande affollamento
- periodo di durata dell'evento breve
- ambienti con caratteristiche e disposizioni diverse

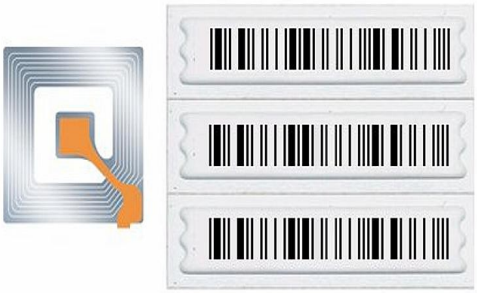
[I]

La presenza contemporanea di più espositori che intervengono su un´area relativamente piccola pregiudica un qualsiasi tipo di controllo condiviso e generalizzato volto alla prevenzione o determinazione di ruberie.
Esistono diversi sistemi che in questo frangente non possono essere utilizzati, quali :

Varchi elettromagnetici

Funzionano con tag RFID dotati di 1 bit di memoria e di una striscia ferrosa, che inviano un segnale all'antenna ricevente posta all'interno del varco. Se la frequenza del segnale captato

è uguale a quella memorizzata nel varco, allora non si attiverà alcun allarme, in caso di mismatch si avvierà una procedura di allerta (acustica, luminosa, etc). Il settaggio della frequenza viene effettuato al momento del pagamento del bene, tramite uno scanner presente alle casse. In Europa questo tipo di sistemi è molto diffuso, per via del basso costo dei tag, dovuto anche alla riusabilità degli stessi. Una limitazione significativa di questo tipo di tecnologia è il basso range dei varchi, la cui antenna deve essere a stretta distanza [II] dal tag. Nel contesto considerato, non è possibile utilizzare questo sistema, da una parte per un'ovvia impossibilità fisica di dislocamento dei varchi, che conterebbero 2 apparecchi per ogni espositore, dall'altra per l´estrema sconvenienza nell'installare un sistema cosi´ complesso per una durata media della manifestazioni che solitamente non supera i 10 giorni. Il motivo principale rimane comunque l'assoluta inefficienza di funzionamento, considerando il fatto che questi tag per essere attivati hanno bisogno di passare molto vicino al varco, cosa che in uno spazio aperto è di difficile realizzazione.



Varchi magneto-acustici

[III]

questo tipo di sistemi lavorano sempre con tag RFID passivi, ad 1 bit di memoria, ma a differenza dei precedenti è il varco ad iniziare la comunicazione, emettendo un segnale in AM a 58 kHz. Il tag risponde al segnale con un altro di una certa frequenza, che viene captato e processato da un apparecchio, il quale in base alla magnetizzazione o meno dell'etichetta fa partire o meno l´allarme. Rispetto al precedente, questo sistema ha un più ampio raggio di copertura. I difetti legati all'utilizzo di questo tipo di antitaccheggio sono gli stessi

rispetto al caso elettromagnetico.

Questi varchi, per avere un´efficacia, dovrebbero essere posti in tutte le entrate ed in tutte le uscite dell'ambiente espositivo, questione tecnicamente assai ardua calcolando l'ampia metratura e il numero delle aperture per il transito dei visitatori. Inoltre, ogni espositore si dovrebbe dotare i propri prodotti di un tag standard e riconosciuto dai rilevatori di ogni ente organizzatore di manifestazioni, i quali aderiscono ad un protocollo di intesa volto a proteggere i propri clienti: uno scenario di molto improbabile.

Telecamere di sorveglianza

[IV]

Questo tipo di soluzione non offre ampie garanzie, solitamente non hanno una funzione di feedback in real-time, ma vengono utilizzate negli esercizi commerciali principalmente come deterrenza e analisi del misfatto *a posteriori.* Per quanto riguarda la prima casistica, ragionando su grandi numeri, la dotazione di telecamere in ogni stand andrebbe a produrre molto probabilmente l´effetto opposto, ovvero la deterrenza all'acquisto. La tecnologia attuale consente però, a pari qualità, di disporre di telecamere miniaturizzate, nascondibili e quindi non percepibili dal cliente. Bisogna considerare il grande afflusso di persone presente davanti ai prodotti, la cui situazione genera difficoltà non sicuramente affrontabili con questa soluzione, quale l´associazione di una determinata mano ad un determinato volto. L'utilizzo di videosorveglianza comunque può essere considerato uno step propedeutico alla risoluzione del problema furto, poiché consente di imparare in che dinamica avviene l'azione, ma non è certamente la deliberazione definitiva.

Espositori bloccanti

Sono dei particolari tipi di fissaggio merce, e offrono una protezione prettamente fisica dal furto del bene. Vengono adoperati principalmente cavi in acciaio o a molla, con supporto calamitato o adesivo. Anche le vetrine o teche in vetro o in plexiglass fanno parte di questa categoria. I più recenti sono dotati di microswitch i quali, in caso di interruzione del circuito, vanno in allarme. Alcuni modelli prevedono l'utilizzo di Smart Card e segnalatori led, oltre che di una piccola unità di processamento dati che memorizza lo stato e la cronologia degli eventi registrati. [V]

Tra i sistemi elencati, è forse quello che da maggiori garanzie, avere un supporto fisico che si occupa della sicurezza del bene elimina quasi totalmente la necessità di un fattore psicologico di dissuasione o la manchevolezza del venditore nel caso in cui faccia errori dovuti a disavvedutezza. Nonostante abbia più pregi che difetti, questo sistema nel contesto considerato non troverebbe facile applicazione, a causa della grande quantità di oggetti che possono essere presenti sul banco. Potrebbe essere adoperato efficacemente su oggetti di valore, ma su alcuni settori merceologici (come ad esempio piante o fiori e botanica in generale, oppure tessuti, abbigliamento) non c'è convenienza nell'impiego.

Un ulteriore difetto che potrebbe pregiudicare la vendita è l'impossibilità del potenziale cliente di venire a contatto con l´oggetto d´interesse in caso fosse sotto chiave, o comunque venirne a contatto in maniera limitata nel caso fosse agganciato ad un espositore.

[VI]

Security e vigilanza

Esistono ditte specializzate che offrono un servizio di tutela del patrimonio, di sicurezza complementare integrata con quella delle forza pubblica. Questo tipo di soluzione viene usata maggiormente negli aeroporti, nelle stazioni ferroviarie, nei porti ed in tutti quei luoghi pubblici particolarmente sensibili dove si avverte la necessità d'una protezione più capillare. Nel caso esaminato, intervenire con risorse umane potrebbe sortire un effetto analogo di deterrenza a quello riscontrato sulle telecamere, oltre al costo considerevole che questo genere di soluzione comporta. Dal punto di vista dell'efficienza, a fronte di una vasta partecipazione di pubblico, si dovrebbe assumere un numero adeguato di personale, la qual cosa presenta aspetti antieconomici.

Le soluzioni analizzate non rispondono completamente all'esigenza di sicurezza avvertita in quel tipo di ambiente, nemmeno se combinate tra loro. Tali tecnologie e tecniche di prevenzione, al netto della sempre maggiore abilità dei malviventi alla sottrazione, non trovano adeguata applicazione nel contesto considerato; i limiti riscontrati hanno caratteristiche talmente condizionanti da pregiudicare un possibile utilizzo efficiente.

1.2 La soluzione proposta

Per far fronte a queste problematiche, comprendendo la necessità che ne scaturisce, si è pensato ad una metodologia d´intervento basata su una rete di sensori.

1.2.1 Specifiche

Il sistema deve avere le seguenti caratteristiche:

- basso costo
- dimensioni contenute
- facilmente trasportabile
- adattabile ad ambienti differenti ed ostili
- installazione e dismissione veloce
- capacita' di localizzazione nodi nell'ordine dei centimetri
- scarsa influenza dalla presenza massiccia di esseri umani

Tenendo in considerazione la difficoltà di gestione di un sistema con queste peculiarità da parte di un unico soggetto (l'ente organizzatore dell'evento), si lascia al singolo partecipante il compito di occuparsi della sua struttura, acquisendo così ulteriori proprietà modulari ed adattive.

L'impianto deve poter funzionare anche in presenza di altri sistemi wireless concorrenti od avversi.
Il campo coperto è compreso tra una PAN ed una LAN, diciamo che per avere un buon risultato il raggio di copertura deve essere di 15/20 metri.

1.2.2 Descrizione del sistema [VII]

L'idea prevede la localizzazione di ogni oggetto posto sul banco, ma soprattutto è fondamentale conoscere lo spostamento che questo ha in tempo reale.
E' pacifico che un potenziale sottrattore infatti si allontani con la merce senza più tornare.
La conoscenza della posizione può essere utile per stabilire un contatto col nodo, attraverso un allarme sonoro, luminoso, o meglio ancora un raggio di luce che parte da un punto fisso e segue la merce in movimento.
Questo "punto fisso", ve ne può essere più di uno, non ha vincoli di dimensione, consumo di energia o mobilità in quanto verosimilmente posizionato lontano dalla zona "a rischio" e fissato saldamente al pavimento, ad una colonna etc. e alimentato tramite corrente elettrica.
Una volta stabilita con relativa certezza la direzione nella quale l'oggetto sta andando, si possono usare diverse tecniche di recupero per riappropriarsi del maltolto, che in questo scritto non verranno trattate.

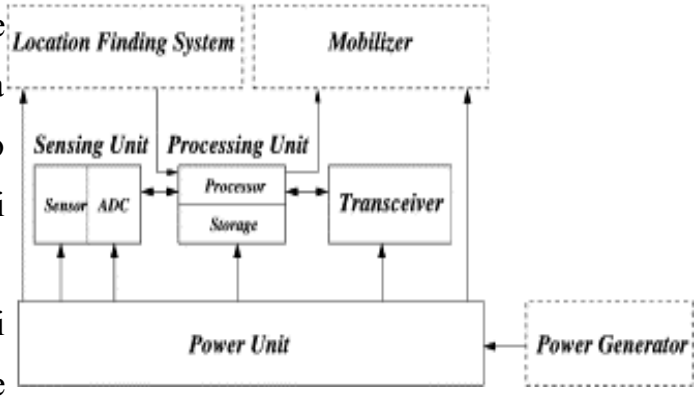
Per raggiungere questo obbiettivo, è necessario:

- ➔ rendere ogni oggetto un nodo della rete di sensori
- ➔ calcolare in maniera molto precisa la posizione del nodo
- ➔ approntare un meccanismo di allarme nel caso in cui il nodo esca da un certo raggio

Capitolo 2

Wireless Sensor Network

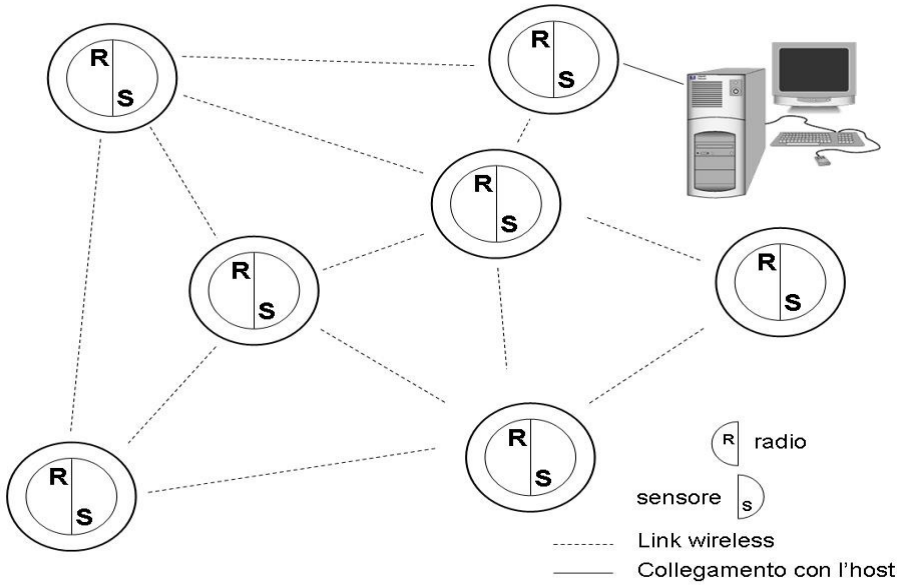
Con le ultime innovazioni in campo di comunicazione wireless, dell'elettronica digitale e dei microsistemi elettro-meccanici (MEMS), si sono riusciti a sviluppare sensori a basso costo, bassa potenza e multifunzione, che posseggono piccole dimensioni . Questi dispositivi vengono chiamati *mote* (muovere), nome coniato dai ricercatori che hanno iniziato a sviluppare, tra la fine del 1900 e l'inizio degli anni 2000, progetti importanti su reti di sensori. [VIII]



Un sensore può assolvere a diversi compiti, ed è composto fondamentalmente da un processore integrato, memoria interna od esterna, un modulo di alimentazione e un modulo di comunicazione (tipicamente un trasmettitore radio), oltre ad avere uno o più sensori per acquisizione dati.

2.1 Che cos'è una WSN

Una WSN è letteralmente una rete di sensori, in largo numero, distribuiti nello spazio, che sono disposti all'interno o comunque molto vicino all'avvenimento che si vuole monitorare. In questa rete, ogni nodo acquisisce e processa dati in maniera autonoma, per poi comunicare con gli altri nodi e trasmettere le informazioni ad un'unità centrale che elabora ciò che ha ricevuto.



[XXIV]

2.2 Cenni storici

Durante la guerra fredda, furono progettati negli Stati Uniti dei sistemi radar aviotrasportati per sorveglianza aerea, chiamati AWACS (Airborne Warning and Control System). In questa rete, i sensori erano costituiti dagli aerei stessi. Il primo velivolo dotato di questa tecnologia fu un Boeing 747, ed entrò in servizio nel 1977.

Nel 1978, in un workshop tenuto alla Carnegie Mellon University, intitolato ¨Proceedings of the Distributed Sensor Nets Workshop¨ , si posero le basi per l´identificazione dei componenti di una rete distribuita di sensori. In quella circostanza, si parlò di sensori acustici, moduli di processamento e comunicazione, e di software distribuito.

I primi passi nella ricerca sulle WSN vennero poi compiuti presso il DARPA (Defence Advanced Research Projects Agency) attorno al 1980, nell'ambito del programma DSN (Distributed Sensor Networks). Questo tipo di reti venne pensato come un insieme di nodi a basso costo distribuiti nello spazio, con prerogative di collaborazione tra sensori ma operanti in autonomia, nel quale le informazioni sarebbero dovute essere instradate verso i nodi con maggiore capacità di elaborazione di quel tipo di dato.

Una dimostrazione sull'applicazione di questi concetti venne effettuata nel 1984,

implementando un sistema di tracciamento per elicotteri, attraverso l´uso di un array di microfoni e di tecniche di astrazione e matching dei segnali generati, sviluppato dal Massachussets Institute of Technology (MIT).

Nonostante l´idea di fondo permanga tutt'oggi quasi intatta, all'epoca c´erano grosse limitazioni di carattere tecnologico che non erano in grado di superare. Un esempio è il collegamento che intercorre tra i sensori, ancora wired con protocollo Ethernet, che all'inizio degli anni 80 iniziò a prendere piede (la prima formulazione è datata 1976).

Un altro fattore fortemente limitante lo si trova nella dimensione dei nodi, eccessivamente ingombranti per molte tipologie d´applicazione.

Bisogna aspettare la fine degli anni 90 per avere migliorie significative, quando cioè vengono sviluppate nuove tecnologie di networking e di ridimensionamento dei componenti, oltre ad una flessione verso il basso del costo di tali dispositivi.

In questo nuovo scenario, la ricerca si apre anche a possibili applicazioni civili, creando una seconda generazione di sensori, i MEMS sopra citati, la cui naturale evoluzione sono gli attuali NEMS (Nanoscale Electromechanical Systems). La tecnologia ebbe un decorso talmente rapido tale da far stabilire, nel 2004, un obbiettivo commerciale piuttosto ambizioso: realizzare sensori MEMS con dimensione totale di 1 mm^3. [3]

La contemporanea creazione di standard è stata la chiave di svolta per la diffusione delle WSN: ZigBee, Bluetooth, WiMax, WiFi, RfId sono alcuni tra questi, che hanno permesso l'utilizzo di queste reti in maniera globale, riuscendo a connettere sempre più dispositivi in un'ottica applicativa sconfinata.

Mote Type	*WeC*	*René*	*René 2*	*Dot*	*Mica*	*Mica2Dot*	*Mica 2*	*Telos*
Year	1998	1999	2000	2000	2001	2002	2002	2004
							
Microcontroller								
Type	AT90LS8535		ATmega163			ATmega128		TI MSP430
Program memory (KB)	8		16			128		60
RAM (KB)	0.5		1			4		2
Active Power (mW)	15		15		8		33	3
Sleep Power (μW)	45		45		75		75	6
Wakeup Time (μs)	1000		36		180		180	6
Nonvolatile storage								
Chip		24LC256				AT45DB041B		ST M24M01S
Connection type		I^2C				SPI		I^2C
Size (KB)		32				512		128
Communication								
Radio		TR1000			TR1000		CC1000	CC2420
Data rate (kbps)		10			40		38.4	250
Modulation type		OOK			ASK		FSK	O-QPSK
Receive Power (mW)		9			12		29	38
Transmit Power at 0dBm (mW)		36			36		42	35
Power Consumption								
Minimum Operation (V)	2.7			2.7		2.7		1.8
Total Active Power (mW)		24			27	44	89	41
Programming and Sensor Interface								
Expansion	none	51-pin	51-pin	none	51-pin	19-pin	51-pin	10-pin
Communication	IEEE 1284 (programming) and RS232 (requires additional hardware)							USB
Integrated Sensors	no	no	no	yes	no	no	no	yes

2.3 Caratteristiche di una WSN [IX]

Le reti di sensori wireless presentano una moltitudine di proprietà che le rendono plasmabili a diversi campi applicativi, per ognuno di questi è necessario saper scegliere accuratamente quelle che meglio si adattano alla situazione considerata.

Hardware

Ogni nodo della rete è formato dall'interazione di 4 componenti fondamentali: un'unità di calcolo, un modulo di comunicazione, una sorgente di alimentazione ed un sensore.
L'unità di calcolo è un microcontrollore a bassa potenza, ha funzioni di storage, processing e poco altro. E' un componente molto limitato, in quanto al mote non sono richiesti calcoli di elevata complessità. Fa eccezione , ma non sempre è presente, nel mote di riferimento (o gateway), il quale è dotato di maggiore capacità computazionale poiché ha anche la funzione di collegamento tra la rete e l'utente che se ne serve.
Il modulo di comunicazione è quell'elemento che permette di interagire con gli altri nodi,

tipicamente opera attraverso radiofrequenza, ma esistono anche sistemi basati su banda infrarossa e su ultrasuoni. Nel nostro caso si considereranno segnali radio a banda larga.
La sorgente di alimentazione può essere dei tipi più disparati; attraverso l'applicazione delle tecniche di energy harvesting è possibili alimentare il dispositivo tramite energia solare, energia eolica, energia termica, energia prodotta da vibrazioni ed ancora energia raccolta da campi elettromagnetici. Oltre a questi, il mote può essere dotato di batteria oppure essere collegato alla rete elettrica.
Il sensore è il responsabile dell'acquisizione di grandezze fisiche, e della trasformazione del dato in un formato trasmissibile tramite il modulo di comunicazione; per fare questo si utilizza un convertitore analogico-digitale. Ogni mote può disporre di più sensori, per raccogliere informazioni su diverse grandezze quali temperatura, umidità, luminosità etc.
Il nodo così composto è studiato per far possedere alla rete una proprietà basilare per le reti wireless, ovvero l'indipendenza dall'intervento umano e la possibile assenza di un controllo centralizzato di gestione del riconoscimento e dell'interazione tra nodi.

Costo

E' un aspetto di essenziale importanza, poiché su questo si fonda la qualità della rete implementata. In linea generale, più una rete è popolata di nodi, maggiore sarà il suo grado di definizione.
Va da sé che il costo del singolo nodo ha conseguenze sull'intera rete, in quanto esiste una relazione diretta tra convenienza nell'investimento e task da raggiungere. Ci sono tipologie d'applicazioni, per esempio, che non richiedono l'uso di wireless ma potrebbero eseguire le loro funzioni con collegamenti tradizionali; qualora il costo di quel componente diventasse non più ammissibile, si abbandonerebbe tale strada.
Nel nostro campo d'interesse, la localizzazione dei nodi non può prescindere dall'uso di tecnologia senza fili; in caso quindi di costi elevati, ci sarebbero ripercussioni sulla densità

della rete, fattore che inficia la precisione nella misurazione della posizione.

Consumo di energia

E' un aspetto cruciale, soprattutto in quei sistemi non provvisti di un'alimentazione costante e certa dei nodi. E' un aspetto legato al periodo di attività dei dispositivi, particolarmente decisivo in quei casi dove i nodi non sono fisicamente raggiungibili e non è possibile fornire un adeguato approvvigionamento energetico.
Il componente maggiormente energivoro, tra quelli visti, è il ricetramettitore, poiché la comunicazione è una delle funzioni che consumano più energia, comparato al processamento dei dati.[4] L'energia spesa per spedire 1 singolo bit è infatti circa la stessa impiegata per processare migliaia di istruzioni in un sensore. [5]
Poiché i sensori sono solitamente alimentati a batteria e possono operare incustoditi per lunghi periodi di tempo, massimizzare l'efficienza energetica è diventato uno dei temi di ricerca più attivi negli ultimi anni. Si sono sviluppati protocolli *power-aware* affiancati ai sistemi operativi dei dispositivi, basati su eventi statistici. Una quantità importante di energia può essere risparmiata facendo un forecast sul carico del nodo e sull'allocazione ottimale delle risorse. E' presente quindi un task scheduler nel core del SO, che gestisce le operazioni da effettuare sulla base dei limiti di tempo e di risorse. [6][7]
Il consumo di energia, inoltre, può rientrare nella vasta trattazione legata alla sicurezza delle reti di sensori. Esistono infatti alcuni tipi di attacchi, perpetrati da altre reti ostili, che mirano a far consumare ai nodi più energia di quanta non ne occorra, fiaccandone la densità e tentando d'impedire il corretto funzionamento e l'esecuzione del task prefissato.[8]

Ambiente

La rete può trovarsi ad operare in situazioni e luoghi ostili, e deve essere sempre capace di lavorare con uguale precisione ed affidabilità in ognuno di essi. E' possibile che nodi

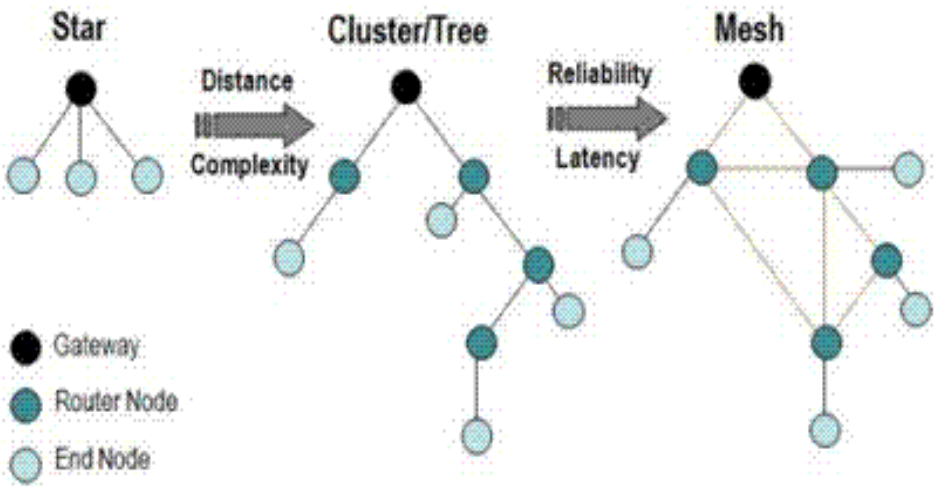
vengano persi in fase di deploying, o si guastino, o si ritrovino privi di energia.
In questi frangenti, un ruolo di primaria importanza lo ricopre il sistema centrale, che deve essere in grado di salvaguardare la consistenza ed il funzionamento della rete nonostante questo tipo di eventi. Oltre a ciò, in ambienti indoor potrebbero esserci difficoltà dovute alla natura del mezzo trasmissivo con il quale i nodi comunicano. La presenza di ostacoli, metalli, persone eccetera può provocare ritardi o perdita di informazioni. Anche in questo contesto ci può essere un problema di sicurezza, nel caso in cui nell'ambiente sia presente un'altra WSN che ha lo scopo di interferire con l'obbiettivo di quella che lecitamente insiste in quell'area. Un esempio è un attacco man-in-the-middle, dove con tecniche di disinformazione la rete attaccante si interpone nelle comunicazioni tra nodi e genera falsi messaggi. Ciò può avvenire non solo tramite attacco esterno, ma anche compromettendo una sottorete della WSN, riprogrammandola per effettuare azioni di disturbo.[8]

Topologia

Determinare la corretta struttura geometrica di una rete rappresenta un altro punto focale nell'efficienza di tutta l'architettura. Ci sono tre principali gruppi che si distinguono nella rappresentazione della geometria delle reti:

- - struttura a stella
- - struttura magliata
- - struttura ad albero

[X]

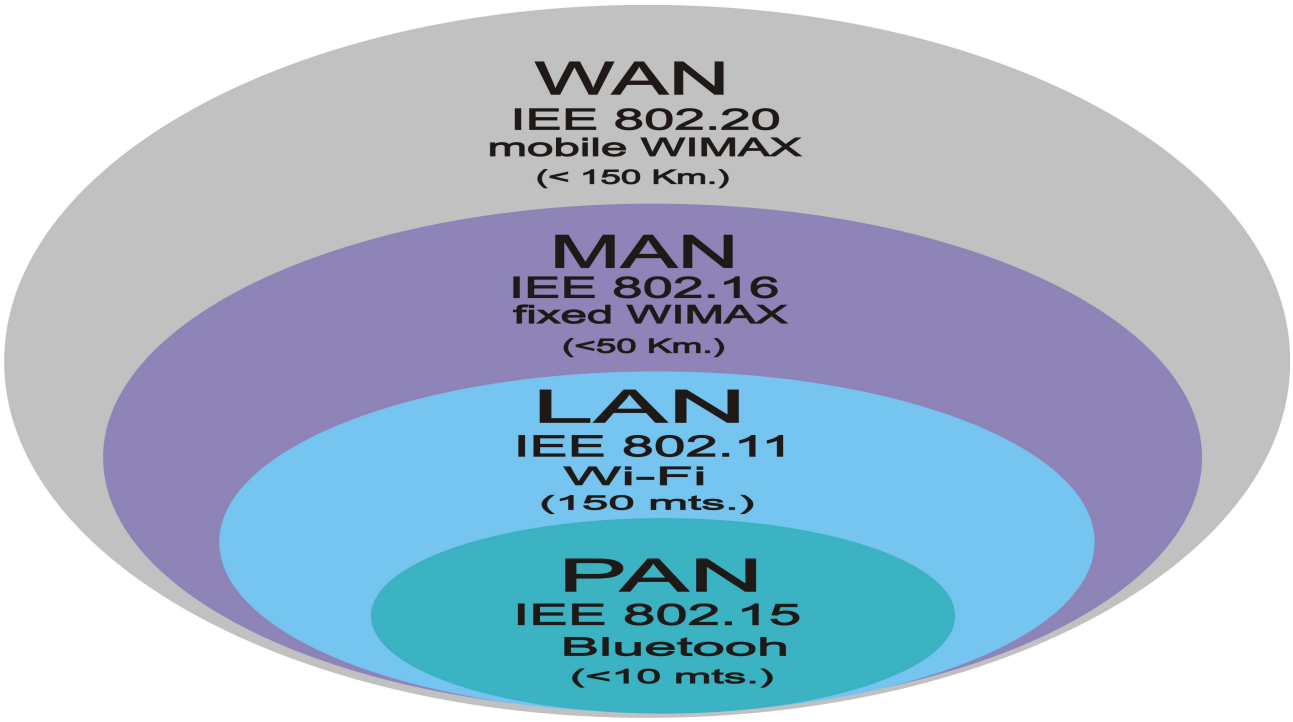


Come si vede in figura, le reti a stella sono centralizzate, ovvero hanno un nodo al quale fanno riferimento tutti gli altri nodi della rete. Ciò implica che il nodo centrale funge da coordinatore, nel caso due nodi della rete debbano comunicare, devono passare entrambi dal centro della rete, che distribuisce i messaggi smistandoli ai diversi destinatari. Può anche avere funzionalità di broadcast, non selezionando i destinatari ma inviando messaggi a tutta la rete. Il punto di forza ed allo stesso tempo quello di debolezza di questa topologia è proprio il nodo coordinatore: la sua presenza garantisce semplicità implementativa, ma in caso si guastasse tutta la rete non funzionerebbe. Nonostante ciò, le reti a stella sono molto affidabili, ed anche scalabili, nei limiti consentiti dal nodo centrale. Un fattore ulteriormente incrementale della scalabilità è la possibilità di collegare due reti a stella tramite i due nodi centrali. Oltre ad un più capillare aumento dei nodi, si ha una maggiore garanzia di sicurezza, in quanto in coincidenza di guasto una parte della rete rimarrebbe comunque operativa.

E' questo il caso delle reti ad albero, che si possono visualizzare come reti a stella interconnesse tra loro, in maniera gerarchica come la disposizione di rami e foglie, appunto, su un albero.

Infine abbiamo le reti mesh, più complesse delle prime due ed anche computazionalmente più impegnative. Queste reti sono anche dette *peer-to-peer,* punto a punto, poiché ogni modo è connesso con un altro senza intermediazioni. In realtà, bisogna distinguere due sottogeneri di reti mesh, ovvero quelle *completamente connesse* e quelle *non completamente connesse.* Le prime hanno collegamenti pari ai nodi raggiungibili da ciascun nodo, mentre le seconde hanno un numero inferiore di collegamenti. In entrambi i casi, si ha un'elevata fault tolerance, vista la grande quantità di collegamenti che convergono su ogni nodo, è possibile trovare percorsi alternativi nell'eventualità di guasti in alcuni punti della rete.

2.4 Classificazione di una WSN [XI]



A seconda dell'estensione dell'area geografica in cui sono dislocati i nodi, le reti sono suddivise in:

- BAN (*body area network*), detta anche rete corporea, si estende fino ad un metro. E' utilizzata per connettere dispositivi "indossabili" sul corpo umano.
- PAN (*personal area network*), ha un raggio di copertura di 10 metri, si riferisce alla comunicazione di piccoli dispositivi "da mano" quali smartphones, fa parte di questo tipo ZigBee, Bluetooth e Rfid.
- LAN (*local area network*), ha un raggio di copertura di qualche centinaia di metri, si riferisce a dispositivi collegati tra loro all'interno dello stesso luogo, come un'abitazione privata (in questo caso si parla di HAN, *home area network*), un'area aziendale, una scuola, un ufficio etc.
- MAN (*metropolitan area network*), copre un'ampia area metropolitana, in questo

caso i nodi si trovano all'interno di una città o raggruppa comuni limitrofi. Necessita di una struttura hardware di maggiore complessità.

- WAN (*wide area network*), connette reti di regioni e di nazioni, può compredere l'intero territorio nazionale od anche più stati.
- GAN (*global area network*), connette nodi dislocati in diversi continenti, tecnologicamente le più impegnative, si usano anche satelliti per interconnettersi, ha estensione mondiale; internet è un esempio di questa classe di reti.

2.5 Standard

Le reti di sensori wireless possiedono diverse caratteristiche uniche se rapportate alla loro controparte cablata, quali il vasto numero dei dispositivi coinvolti, la mobilita´ degli stessi, l ´installazione temporanea, la ridondanza delle componenti, e la topologia mutevole. Affiancate a queste, ci sono dei vincoli comuni per tutti i nodi: l´ambiente operativo, l ´ampiezza della banda di comunicazione, la capacita' di storage, la potenza di calcolo, il consumo di energia.

Su questa base, negli ultimi 15 anni alcune organizzazioni hanno lavorato per creare delle norme tecniche condivise, con lo scopo di rappresentare un punto di riferimento nella grande offerta che rappresenta il mondo delle reti wireless. Tra le molteplici organizzazioni, ricordiamo la IEEE (*Institute of Electrical and Electronics Engineers*) che si occupa del livello fisico e del livello MAC, e la IETF (*Internet Engineering Task Force*), che opera a livello network. Accanto a queste, la ISA (*International Society of Automation*) propone soluzioni a tutti i livelli. Nonostante tutto, in questo campo l´utilizzo di standard e´ molto minore rispetto ad altri sistemi computazionali, la presenza di specifiche proprietarie e definizioni fuori dalla norma è molto alta, la qual cosa crea una difficoltà di interazione tra sistemi con diverse caratteristiche. Rispetto a soluzioni proprietarie, i sistemi standardizzati presentano discreti vantaggi, quali:

- costi infrastrutturali più contenuti

- indipendenza da logiche di mercato applicate dai vendor
- maggior supporto in caso di problemi
- interoperabilita' tra sistemi con base comune

Ognuno di questi standard è organizzato su stacks, per fornire una descrizione astratta ed a livelli dell' architettura del protocollo di rete. Ogni livello dello stack e' una collezione di funzioni , ed ha il compito di fornire servizi al livello superiore, e di ricevere servizi dal livello sottostante.

Presentiamo qui alcuni standard attualmente dominanti, e che hanno rilevanza al fine della nostra ricerca:

2.5.1 IEEE 802.15.4

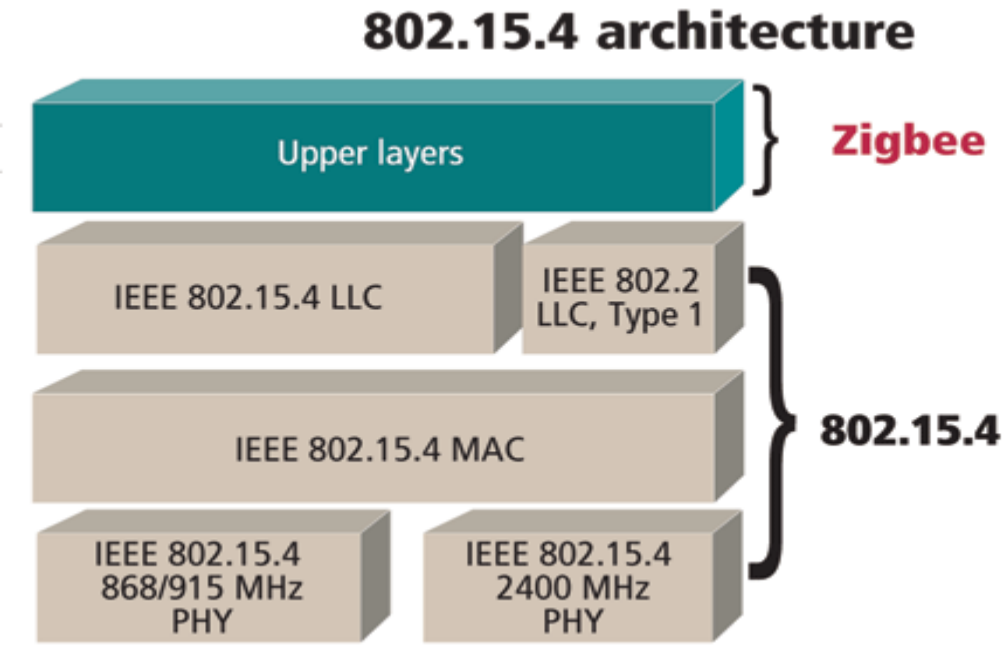
Come indica il nome, afferisce al gruppo di lavoro 802.15, la cui commissione norma le WPAN. Venne ratificato come standard nell'estate del 2003.
Questo standard specifica il livello fisico e il livello MAC di una rete wireless a corto raggio, che pone l´accento sulle seguenti proprietà:

- semplicità
- consumi contenuti
- costi contenuti
- basso data rate
- robustezza

La specifica definisce due tipi di nodo, ovvero gli RFD (*Reduced Function Device*) e gli FDD (Full Function Device). I primi sono device che possono comunicare solamente con nodi del secondo tipo, e non tra di loro, ragione per la quale vengono utilizzati solamente

nelle reti con topologia a stella. I secondi, al contrario, sono nodi pienamente operativi, non hanno limitazioni ed hanno funzioni di coordinamento rispetto agli altri nodi; per questo motivo, posso essere impiegati in ogni topologia di rete, e offrono la possibilità di costruire WSN dimensionalmente importanti e di complessità rilevante.

[XII]



1) Livello fisico (PHY)

E´ il primo livello (quello alla base) del modello ISO/OSI accettato in tutto il mondo. Si occupa della trasmissione dei dati, e fa da interfaccia per l´accesso ad ogni livello del modello, oltre a tener traccia di informazioni sulla rete alla quale afferisce. In piú, ha il controllo del modulo radio di trasmissione/ricezione del nodo, ne regola l´accensione e lo spegnimento; ha quindi un ruolo decisivo rispetto al consumo energetico del nodo. Inoltre, gestisce la selezione del canale di trasmissione e tutte le funzioni legate alla modulazione e all´analisi dei segnali. Su queste differenze sono stati creati 4 sottolivelli, 3 dei quali

utilizzano un approccio di trasmissione a frequenza diretta (DSSS), mentre l'altro concerne un tipo di trasmissione a diffusione parallela dell'informazione (PSSS).

Questo livello opera su tre bande libere differenti, ciascuna in modalita' differenti, in base all´area geografica nella quale ci si trova.

868-868.6 Mhz: viene utilizzata principalmente nel continente europeo, fino al 2006 si aveva a disposizione un solo canale, dopo si sono triplicati. Il data rate é di 20 Kbps, dopo la revisione del 2006, e´ arrivato fino a 100 Kbps. E' richiesta una sensibilitá del ricevitore di -92 dBm, ed il raggio di copertura ottimale per il funzionamento é di 1 km.

902-928 Mhz: viene utilizzata in Oceania e nel Nord America, aveva 10 canali disponibili fino al 2006, ora ne ha 13. Anche il data rate é stato incrementato: da 40 Kbps a 250 Kbps. Per quanto riguarda sensibilitá e raggio di copertura, valgono gli stessi valori della banda 868.

2400-2483,5 Mhz: viene utilizzata in tutto il mondo, nella revisione del 2006 non ha subito pressoché modifiche, ha un data rate di 250 Kbps, e 16 canali. Il ricevitore deve avere una sensibilitá di -85 dBm, con raggio di copertura ottimale di 220m.

Oltre a queste frequenze, all'interno dell'IEEE si sta valutando l'adozione delle nuove bande 314-316 Mhz, 430-434 Mhz, 779-787 Mhz in Cina, e la banda 950-956 Mhz per il Giappone; l'iter per questa operazione e' cominciato nel 2009, quando e' stata rilasciata dai gruppo di lavoro la prima bozza di modifica dello standard.

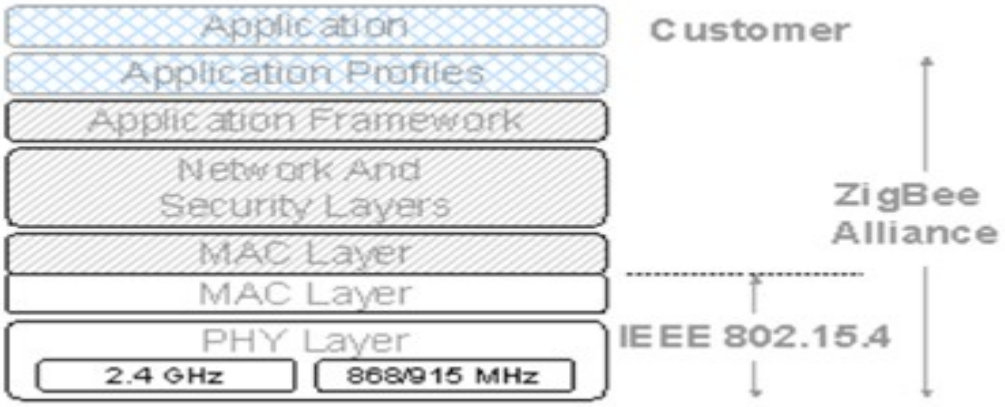
2) Livello MAC

E' il secondo livello del modello ISO/OSI, ha il compito di gestire l'accesso multiplo dei nodi al canale trasmissivo, per regolare il quale viene impiegato il protocollo CSMA/CA nel

caso wireless (se la rete e' cablata si utilizza un altro protocollo, il CSMA/CD). Questo algoritmo prevede l'ascolto sul canale prima di ogni trasmissione, a ridurre la probabilita' di collisione con eventuali segnali entranti.
Oltre a questo, viene controllata la sequenzialità dei pacchetti in entrata ed in uscita, creati ed instradati, ed ha delegata la funzione di rilevamento dei dispositivi vicini.
Questo livello supporta fino a 65536 nodi, grazie all'impiego di indirizzamento a 16 bit, e prevede algoritmi di cifratura dati, basati su AES-128, per quelle reti che scambiano dati particolarmente sensibili.
Ci sono due tipi di meccanismi di accesso consentiti, uno ordinato ed uno casuale:
in quello ordinato e' eliminata l'eventualita' di collisioni, in quanto e' stato stabilito a priori l'ordine di priorita' per il canale, che viene pertanto occupato da uno ed un solo segnale alla volta. Diverso e' il caso dell'accesso casuale, nel quale possono intervenire sulla trasmissione piu' nodi contemporaneamente, ed e' necessario quindi adottare delle tecniche per abbassare piu' possibile il numero di collisioni verificabili. Queste determinano, oltre alla perdita di dati trasmessi, anche un spreco di banda e di energia dei nodi.

Andiamo ora ad analizzare quali specifiche definiscono i livelli superiori di questo standard:

2.5.2 ZigBee [XIII]



La ZigBee Alliance e´ un gruppo di compagnie (oltre 200) che ha sviluppato e mantiene lo standard ZigBee. L'obbiettivo e' quello di fornire flessibilita', mobilita' e facilita' d'uso agli utenti, tramite la diffusione di apparecchi affidabili, low cost, low power, wireless e appartenenti ad una specifica aperta. Definisce i livelli applicazione e network sopra 802.15.4, e consente alle applicazioni di quest'ultimo di essere in grado' di supportare reti magliate.

Il nome deriva dall'attinenza del protocollo al comportamento di gruppo delle api. La comunita' di questi insetti infatti e' numericamente importante, e fonda la propria sopravvivenza, tra le altre cose, anche sulla comunicazione tra i vari membri che la compongono, nella ricerca di cibo e nella selezione del luogo migliore per porre l'alveare. La tipica peculiarità di volare a zig-zag inoltre ispira la prima parte del nome del protocollo.

La tecnologia definita da ZigBee opera nella fascia WPAN, e si prefigge d´essere piu´ semplice e meno costosa rispetto alle altre che insistono sulla stessa fascia d´utilizzo, come ad esempio Bluetooh.

Questo tipo di reti possiede facilita' d'installazione, un trasferimento dati affidabile ed un corto raggio di copertura, che consenta una ragionevole consumo di energia.

Il protocollo e' basato su un algoritmo AODV (Ad-Hoc on Demand Distance Vector), ovvero le attivita' di instradamento, di ricerca e di comunicazione punto-punto sono

consentite, cosi' come le gia' citate reti mesh. E' un algoritmo computazionalmente semplice, non occupa eccessiva memoria e non genera traffico se non quando se ne fa richiesta (cio' avviene quando un percorso tra due nodi e' sconosciuto e bisogna creare un cammino).

Ci sono tre tipi di dispositivi ZigBee:

1) **Coordinatore**: attiva e controlla la rete, memorizza informazioni sulle connessioni e, in caso di tramissioni criptate, puo' funzionare da Trust Centre e possedere le chiavi di sicurezza. All'interno di una rete, puo' essercene soltanto uno.

2) **Router**: estendono la copertura della rete, evitano dinamicamente gli ostacoli che trovano sul percorso, e forniscono cammini alternativi in caso di congestione o guasto. Possono connettersi al coordinatore o ad altri router, e possono avere dispositivi figli.[9]

3) **Dispositivi Finali**: inviano e ricevono messaggi, ma non fanno attivita' di routing. Devono essere connessi al coordinatore od a un router, altri dispositivi non li supportano, nemmeno figli. Richiedono un basso quantitativo di memoria, per questo sono i piu' economici rispetto ai primi due tipi.[9]

Per economizzare il consumo di batteria, i dispositivi finali, secondo standard, trascorrono la maggior parte della loro vita in sleep mode, attivandosi solamente in caso debbano inviare o

ricevere dati. Coordinatore e router, per il ruolo che ricoprono, hanno la regola di rimanere sempre accesi, ma non hanno vincoli di consumo in quanto connessi ad alimentazione fissa (tipicamente una presa elettrica).
In materia di consumi, la potenza minima di funzionamento e' stabilita in – 3 dBm, per ogni banda di frequenza del protocollo. Queste si differenziano nella potenza massima di trasmissione:

- ➔ nella 868 mhz il limite massimo consentito e' 14 dBm (25mW)
- ➔ nella 915 Mhz il limite e' di 30 dBm (1 W), eccezion fatta per i sistemi costruiti interamente su integrati (SoC), per i quali la potenza massima e' fissata in 10 dBm
- ➔ nella 2.4 Ghz si hanno 10 dBm di picco, anche se tipicamente il carico e' di 0 dBm

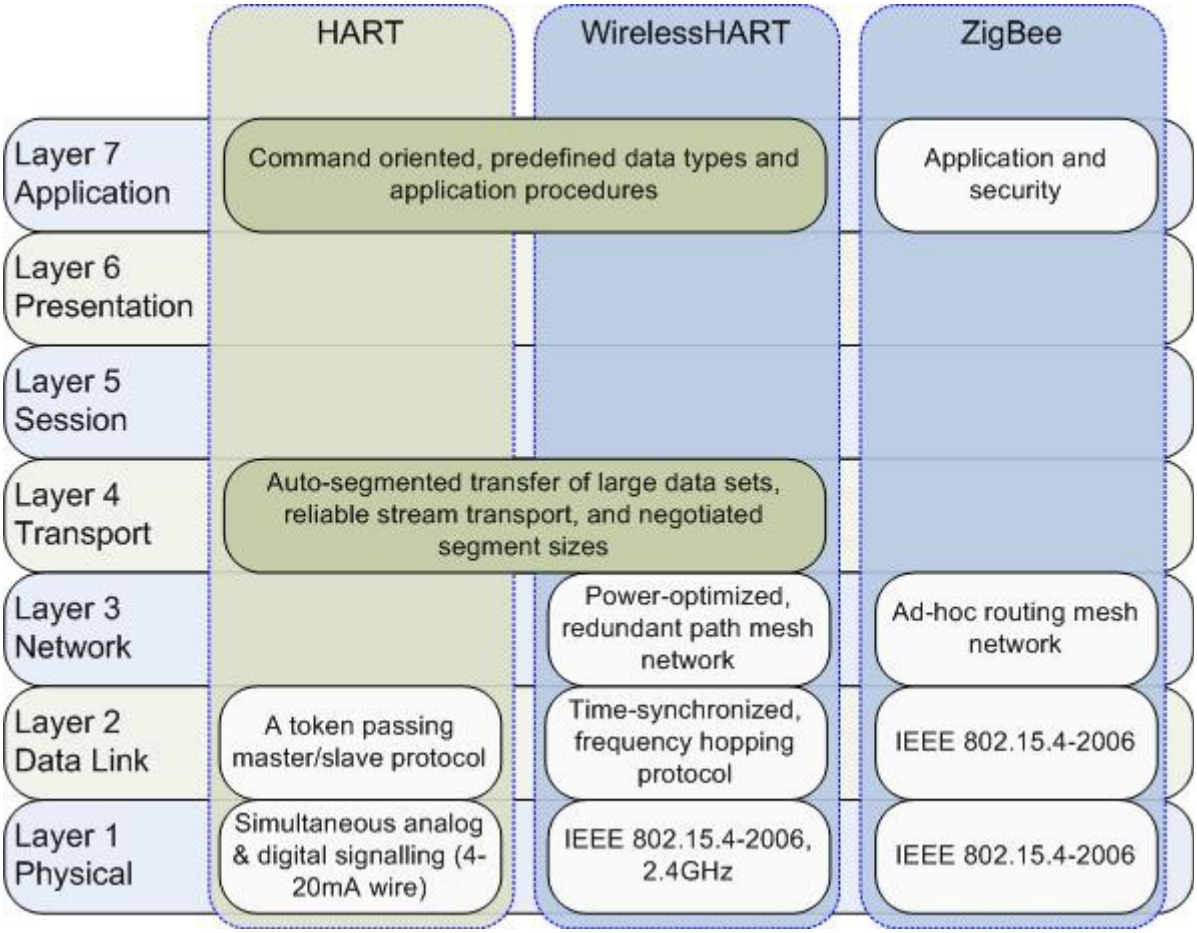
Sul piano della sicurezza, ZigBee fa uso di meccanismi di safety presenti in 802.15.4 cui si accennava poco prima, come algoritmi di crittografia avanzati (AES a 128 bit).
E' bene ricordare che un nodo ZigBee può, secondo lo standard operare in condizioni di sicurezza o meno: nel secondo caso, si avrà un codice più snello a discapito di eventuali attacchi subiti.
Esistono 4 diversi servizi di sicurezza nelle reti ZigBee:

- Codifica del segnale. Ogni messaggio immesso nella rete viene criptato tramite una chiave posseduta solamente dai componenti della rete.
- Controllo degli accessi. Ogni nodo memorizza una lista di possibili interlocutori, tagliando fuori ogni dispositivo tentasse di accedere alla rete illecitamente.
- Coerenza dei dati. In ogni pacchetto in trasmissione viene effettuato un controllo d'integrità, attraverso il quale è possibile risalire a modifiche non autorizzate.
- Rispetto della sequenza. Ogni frame viene confrontato col precedente, in modo da non creare ripetizioni nelle trasmissioni.

2.5.3 WirelessHART

E' uno standard nato dalle deficienze di ZigBee in ambito industriale. Nel 2004 e nel 2005 infatti, ZigBee era candidato ad irrompere nel panorama industriale, ma alcuni testi effettuati sul campo hanno rilevato delle incompatibilità ambientali. L'industria richiedeva connessioni sicure ed affidabili, ma la vulnerabilità al multipath fading, dovuto all'utilizzo di un singolo canale di trasmissione, ha creato l'esigenza di utilizzare un altro protocollo.
La differenza tra i due protocolli è essenzialmente questa: *Frequency Hopping Spread Spectrum* (FHSS) permette a WirelessHART di "saltare" tra i 16 canali definiti nello standard 802.15.4 per evitare interferenze. In più, è dotato di un meccanismo, il *Clear Channel Assessment*
(CCA), che certifica la pulizia di un canale, e di un'opzione chiamata *Blacklisting,* che consente di disabilitare alcuni canali.
Un'altra importante differenza è nei device: mentre alcuni tra quelli di ZigBee hanno funzioni ridotte, tutti quelli di WirelessHART possiedono uguali proprietà; sono infatti tutti in grado di effettuare routing. Questa caratteristica permette un'installazione, un deployment ed un'espansione della rete più semplice rispetto a ZigBee.
Come suggerisce il nome, WirelessHart deriva dal protocollo digitale HART (*Highway Addressable Remote Transducer*) per comunicazioni bidirezionali tra un'applicazione ed uno strumento. Il primario uso di WHART è infatti quello di accedere a dispositivi dotati di HART, inseriti in sistemi che invece non supportano tale protocollo, e di monitorare le condizioni e le performance di tutti quegli strumenti non raggiungibili via cavo a causa degli alti costi.
Lo standard è stato disegnato secondo le seguenti caratteristiche:
- dev'essere semplice da usare e da installare
- deve autogestirsi e in caso di guasti autoripararsi
- dev'essere flessibile, ovvero deve supportare diverse applicazioni

- dev'essere scalabile, adattarsi a piccoli ed a grossi impianti
- dev'essere affidabile, sicuro
- deve supportare ed interfacciarsi con la tecnologia HART esistente



[XIV]

2.5.4 IEEE 802.15.4a

E' uno standard che nasce a seguito del precedente descritto, viene rilasciato nel 2007 e prevede l'aggiunta di due ulteriori livelli fisici rispetto all' IEEE 802.15.4-2006, che di base ne proponeva 4.

I due nuovi livelli usano CSS (Chirp Spread Spectrum) e UWB (Ultra Wide Band); il primo offre un data-rate massimo di 2 Mbps e piu' robustezza, con un range di parecchie misure piu' alto

rispetto allo standard che l'ha generato (che si attesta sui 10 metri). L'implementazione fatta dalla Nanotron riesce ad operare con una distanza tra i dispositivi nell'ordine delle centinaia di metri [11], operante sulla banda 2450 Mhz ISM.
Il secondo utilizza per trasmettere una serie di impulsi a radiofrequenza molto ridotti, nell'ordine dei nanosecondi, che non richiedono un processamento di frequenza intermedio, poiche' lavorano su baseband, la qual cosa riduce la complessita' hardware e il consumo di energia.
Generalmente, a causa della brevita' degli impulsi, minori di 1 ns, l'ampiezza di banda del segnale trasmesso e' sull'ordine del Ghz o maggiore.[12] Lo standard prevede 3 bande: sotto il Ghz, tra 3 e 5 Ghz e tra 6 e 10 Ghz.

2.5.5 Bluetooth

Bluetooth e' uno standard (802.15.1) ed un protocollo di comunicazione pensato per bassi consumi e corto raggio d'azione, economico e sicuro. Venne inizialmente sviluppato da Eriksson, per soddisfare l'esigenza di eliminare i collegamenti via cavo tra i telefoni prodotti e i vari accessori (cuffie, auricolari etc.) Nel 1994 si avvio' un primo studio di fattibilita', nel 1998 si costitui' il SIG (Special Interest Group), un' associazione di aziende quali Ericsson, Nokia, IBM, Toshiba e Intel, e nel 1999 si arrivo' ad una prima specifica (la versione 1.0), seguita nel corso di un decennio da altre release fino ad arrivare all'attuale 4.0.
Il protocollo prevede un range che va da 1 a 100 metri, caratteristica che gli consente di implementare delle LAN wireless sebbene l'intento iniziale fosse quello del corto raggio (PAN). Come WirelessHART, comprende la tecnologia FHSS, con la differenza che Bluetooth fa hopping su 79 canali invece di 16. Un'altra caratteristica comune tra i due e' la frequenza operativa, 2.4 Ghz ISM. Presenta tuttavia alcune limitazioni che pregiudicano l'uso di questa tecnologia in diverse applicazioni, quale la scarsa resa energetica (la batteria ha autonomia nell'ordine di giorni) e il numero di nodi supportati dalla rete, solamente 7. Il bit rate varia da 1 a 3 Mbps, a seconda della configurazione dei dispositivi.

Di seguito una tabella riassuntiva: [XV]

Frequency band	2400 … 2483.5 MHz
Number of channels Channel spacing Channel frequencies	79 1 MHz f = 2402 + k MHz (k=0,…,78)
Output TX power	Class 1 100 mW Class 2 2.5 mW Class 3 1 mW
Modulation type Modulation index Symbol rate	Binary, Gaussian FSK (BT = 0.5) 0.28 … 0.35 1 Msymb/s
Media access scheme	Frequency-hopping (FH-)CDMA
Hop frequency Slot time Multiplexing scheme	1600 hops/s 625 µs Time division duplex (TDD)
Required RX sensitivity	-70 dBm @ 0.1% BER

2.5.6 RFID

La tecnologia Rfid ha origini lontane, un suo predecessore lo si puo' trovare all'epoca della seconda guerra mondiale (i trasponder IFF usati dagli Alleati), ma la sua attivita' di normazione e' relativamente recente.

Principalmente due organizzazioni se ne occupano: EPCGlobal, un'associazione privata, e ISO, l'ente mondiale di standardizzazione che si interessa di svariati settori, primariamente tecnologici.

La prima pone attenzione sui processi logistici e sulla catena di distribuzione, mentre la seconda ha interesse di piu' ampio respiro, vertente tutta la parte di gestione degli elementi che costituiscono il sistema. Progressivamente si sta arrivando ad una convergenza tra i due standard, nonostante ci siano ancora diverse controversie da appianare, quali i differenti

approcci normativi a riguardo della proprieta' intellettuale.

Un sistema Rfid e' composto fondamentalmente da:

1) Reader: e' un apparecchio di lettura e/o scrittura, dotato di un microprocessore che controlla un ricetrasmettitore che ha funzioni d'interrogazione e ricezione informazioni dai TAG

2) TAG (o trasponder): e' un chip digitale che possiede un certo numero di informazioni sull'oggetto a cui e' applicato, e' provvisto di un'antenna che gli permette di comunicare con il reader o di alimentarsi in caso si tratti di etichetta passiva.
   Possono essere di tipo *read-only* o *read-writeable,* ossia possono consentire, durante il loro uso, oltre alla lettura, anche la modifica o la riscrittura dei dati presenti.

3) Sistema informativo: collegato al reader, serve per la gestione e l'elaborazione dei dati collezionati, ma non sempre e' presente.

→ Classificazione dei TAG per sorgente di alimentazione [XVI]

RFID Tag Attributes

	Active RFID	Passive RFID
Tag Power Source	Internal to tag	Energy transferred using RF from reader
Tag Battery	Yes	No
Availability of power	Continuous	Only in field of reader
Required signal strength to Tag	Very Low	Very High
Range	Up to 100m	Up to 3-5m, usually less
Multi-tag reading	1000's of tags recognized – up to 100mph	Few hundred within 3m of reader
Data Storage	Up to 128Kb or read/write with sophisticated search and access	128 bytes of read/write

Tag Attivi: sono alimentati a batterie, dispongono quindi di energia propria, grazie alla quale possono attivarsi senza avere un reader nelle vicinanze. Sono sempre accesi, salvo politiche di risparmio della batteria, ed emettono continuamente un segnale di identificazione, che consente una localizzazione costante. Questo comportamento li rende abili a creare sistemi di localizzazione in tempo reale (RTLS), ma allo stesso tempo pregiudica la loro vita media, inferiore rispetto a quella degli altri tipi di tag. Il fatto di possedere una fonte di alimentazione autonoma permette loro di avere feature aggiuntive rispetto ai passivi: possono incorporare diversi tipi di sensori che appunto richiedono una fonte di approvvigionamento energetico che i passivi non hanno.

Solitamente sono dotati di antenna piccola e multidirezionale, che lavora su frequenze nell'ordine del Gigahertz (tra i 900 Mhz e i 5,8 Ghz), che consente una range di lettura nell'ordine delle decine di metri (fino a 200m). A questa distanza di lettura elevata sono affiancati algoritmi di anticollisione elevati, per il riconoscimento contemporaneo di centinaia di tag.

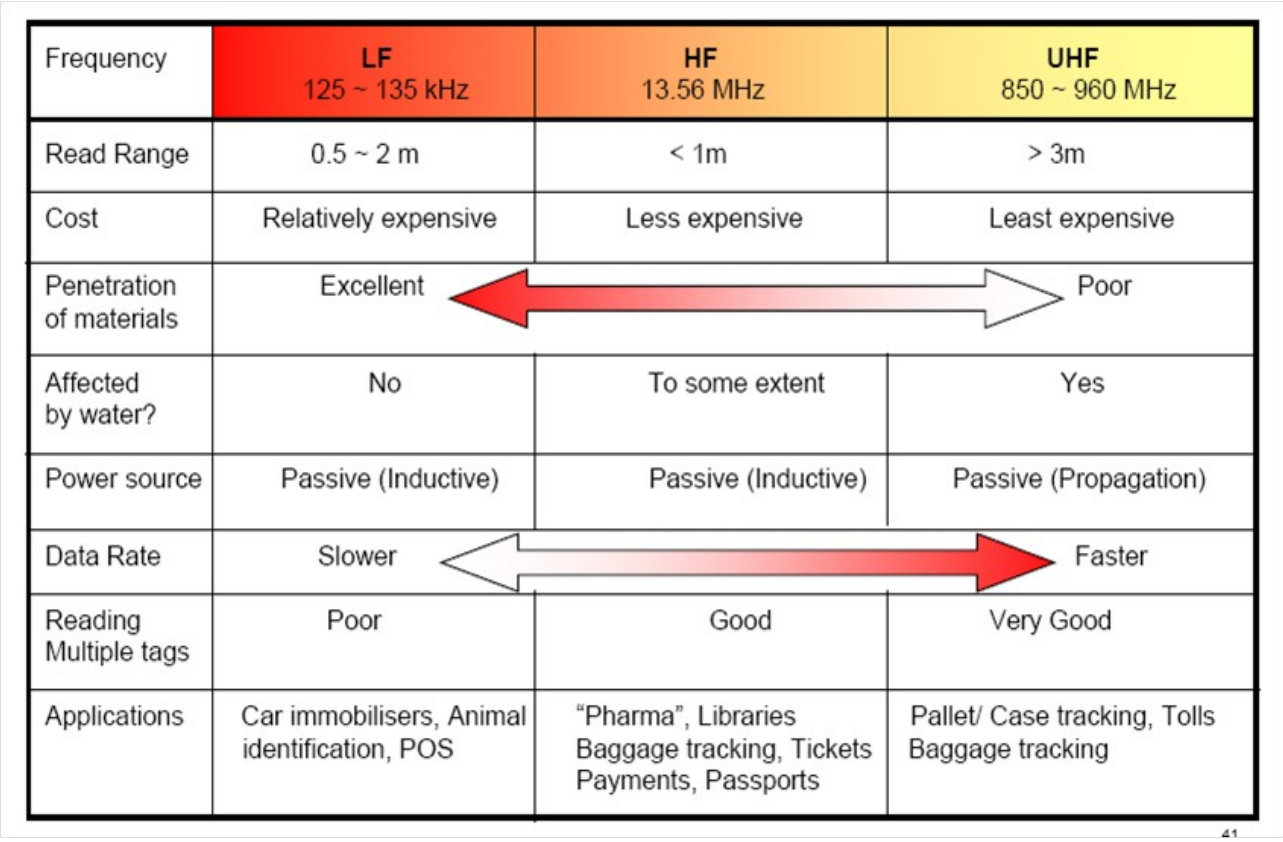
Gli svantaggi riscontrabili in questi tag, oltre ai cicli di vita piu' bassi, sono la manutenzione e il costo della batteria, che incidono significativamente sulla differenza di prezzo che

intercorre tra tag passivi e tag attivi, e le dimensioni dei dispositivi, piu' ingombranti proprio a causa del circuito d'alimentazione. La presenza della batteria, inoltre, puo' rivelarsi controproducente in quegli ambienti che le causano sofferenze d'utilizzo (alte temperature etc.).

Tag Passivi: sono il tipo piu' economico, in quanto non hanno una fonte di alimentazione elettrica propria, e si attivano col campo elettromagnetico del lettore. Il principio secondo il quale tag e reader possono comunicare e' l'induzione magnetica; una volta entrato nel campo magnetico del reader, il tag reirradia il segnale ricevuto dal reader, sottoponendolo prima a modulazione e riflettendolo con la propria antenna. Il segnale modulato e riflesso in risposta al reader viene quindi decodificato dallo stesso. Le distanze nelle quali questo avviene variano da alcuni centimetri fino a pochi metri, a seconda della frequenza operativa.
Questo e' un limite prestazionale che, unito alla mancanza di possibili sensori ausiliari, rende questo tipo di tag molto vincolati.
Montano un'antenna monodirezionale e di discrete dimensioni, che opera su basse frequenze.

Tag BAP: utilizzano una fonte di energia per alimentare solamente alcune componenti del tag, quali il microchip e gli eventuali sensori ausiliari, ma non il trasmettitore. Questo componente infatti viene alimentato con lo stesso principio che impiegano i tag passivi, tramite induzione. La batteria incorporata ha due funzioni: alimentare la circuiteria e aiutare il chip a rimanere in uno stato di standby, inattivo ma comunque acceso; questa carica aggiuntiva permette di ampliare il raggio di lettura, se il campo elettromagnetico del reader non basta, interviene la batteria onboard a provvedere all'attivazione del trasmettitore. In mancanza di interrogazioni, il tag può pertanto rimanere a lungo operativo, ma permane ad ogni modo il vincolo di non poter iniziare una comunicazione. Il range non è più limitato dalla parte del tag, come avviene in quelli passivi, ma dalla parte del reader, il quale pone come distanza di copertura la sensibilità di ricezione della sua antenna.

→ Classificazione dei TAG per frequenza operativa



Frequency	**LF** 125 ~ 135 kHz	**HF** 13.56 MHz	**UHF** 850 ~ 960 MHz
Read Range	0.5 ~ 2 m	< 1m	> 3m
Cost	Relatively expensive	Less expensive	Least expensive
Penetration of materials	Excellent ←		→ Poor
Affected by water?	No	To some extent	Yes
Power source	Passive (Inductive)	Passive (Inductive)	Passive (Propagation)
Data Rate	Slower →		← Faster
Reading Multiple tags	Poor	Good	Very Good
Applications	Car immobilisers, Animal identification, POS	"Pharma", Libraries Baggage tracking, Tickets Payments, Passports	Pallet/ Case tracking, Tolls Baggage tracking

41

[XXV]

Le diverse bande di frequenze presentano caratteristiche diverse e sono quindi indicate per applicazioni differenti. In generale, al crescere della frequenza crescono la distanza di lettura e la quantità di informazioni che si possono trasferire nell'unità di tempo, e il numero di letture simultanee effettuabili. Diminuiscono invece la capacità di resistenza alle condizioni operative, i costi e la grandezza fisica del tag. Le onde a bassa frequenza si comportano come le onde radio di uno stereo: riescono a superare ostacoli come muri o acqua, ma vengono fermate dai metalli.

Quelle ad alta frequenza, al contrario, hanno una degradazione nelle prestazioni di lettura se a contatto con liquidi, che determinano un assorbimento del segnale, o con metalli, i quali

tendono a deviare le onde radio.

Le frequenze LF inferiori ai 135 kHz sono storicamente le prime ad essere impiegate per l ´identificazione automatica, ed ancora oggi vedono un vasto utilizzo, poiche' sono disponibili in praticamente tutti i paesi industrializzati, Nord America, Europa e Giappone su tutti. Hanno il fastidioso svantaggio di essere dimensionalmente piu' impegnative rispetto all´antenna del reader, mentre i tag necessitano di piu' spire nella bobina per ricevere il segnale.

La banda HF, e piu´ precisamente la sottobanda riferita a 13.56 Mhz, e´ la frequenza standard per i tag della tecnologia Rfid in praticamente tutti i paesi del mondo: e´ infatti la piú diffusa in Nord America, Australia, Europa e Giappone. Lo standard ISO 14443 e 15693 regola l´utilizzo di questa banda nelle Smart Card, ma trova applicazione anche nel controllo bagagli, nelle biblioteche, nelle lavanderie etc.

La banda UHF in zona media (850-960 Mhz) hanno il vantaggio di funzionare con antenne di ridotte dimensioni, adatte per dispositivi portatili. E' la banda piu´ recentemente introdotta nei sistemi Rfid, e non si e' ancora arrivati ad una frequenza di lavoro standardizzata comune per tutti i paesi: in Europa vengono usate le sottobande 865-870 Mhz, in USA 902-928 Mhz e in Asia 950 Mhz. La distanza operativa e' nettamente superiore, in alcune circostanze con i tag passivi si arriva fino a 10 metri di range.

La banda UHF in zona alta (2.45 Ghz) e´ detta anche ¨a microonde¨, e´ stata standardizzata da ISO 18000-4, al di fuori pero' del continente europeo. Questa frequenza risulta parecchio affollata a causa delle altre applicazioni e tecnologie che la popolano, delle quali abbiamo gia' discusso (Bluetooth, ZigBee, WiFi), e con le quali e´ obbligatorio convivere. Appartengono a questa fascia anche alcuni dispositivi di uso comune, che potrebbero creare interferenze, come per esempio i cordless e i forni a microonde. Esiste anche un´altra frequenza per le microonde, quella a 5,8 Ghz, che ha il vantaggio di avere dispositivi con antenne di ridottissime dimensioni e range di lettura elevati, ma che deve operare in condizioni LOS (*line of sight*), poiche´ soffre particolarmente la presenza di ostacoli tra il lettore e il tag. Ha lo svantaggio di non essere presente negli Stati Uniti.

Capitolo 3

Tecniche di Localizzazione Indoor nelle WSN

La capacita' di localizzare un nodo all´interno di una rete ha sempre attratto considerevoli interessi di ricerca, la flessibilitá di questo tipo di network ne permette l´uso in varie situazioni, dagli impianti industriali alla domotica privata, dal controllo del traffico a sistemi antintrusione.[9]
Sebbene la localizzazione di un nodo in una rete puo´ sembrare un semplice problema di ordine matematico, a livello pratico ci sono diverse considerazioni da fare. Tra queste, la scelta della struttura di rete ha un feedback diretto col numero di nodi raggiungibili direttamente, che nel caso migliore (tutti i nodi raggiungibili) vanno a formare una rete magliata.
Considerata la vastita' di argomenti e letteratura presenti, si e' scelto di illustrare solamente le tecniche piu´ vicine alla risoluzione del problema posto.

3.1 Caratteristiche del sistema di posizionamento

Esistono due principali tipologie di reti che si differenziano per la presenza o meno di nodi di riferimento:

- **Anchor Based WSN**

Nelle reti anchor based, sono presenti alcuni nodi (*anchors*), dei quali si conosce esattamente la posizione, ottenuta usando o un sistema GPS (qualora nell'ambiente fosse possibile) oppure installando questi nodi in punti di coordinate note. Questi nodi ancora,

inseriti in un contesto di coordinate assolute, mandano informazioni sulla propria posizione in broadcast a tutti i nodi circostanti raggiungibili, i quali per la maggior parte non conoscono la propria posizione: sono detti nodi *non anchor*.
La stima della distanza tra nodi ancora e nodi non ancora può avvenire tramite interazione diretta (Single -hop) oppure tramite interazione indiretta (Multi-hop).
su reti anchor based la posizione di ogni nodo poggia su un sistema di riferimento assoluto, e questa caratteristica è di vitale importanza se l'informazione deve essere condivisa con altri dispositivi al di fuori della rete, oltre ad avere una propagazione minore di errori di misura rispetto a reti anchor free.

- **Anchor Free WSN**

Nelle reti senza nodi ancora le informazioni vanno trasmesse in broadcast, in questo tipo di rete però non c'è un sistema di posizionamento assoluto, non esistono nodi ancora ma particolari nodi che determinano un riferimento posizionale relativo, è infatti comunicata agli altri nodi la posizione "locale". Rispetto alla soluzione con ancore, quella senz'ancore presenta il vantaggio di poter disporre i nodi a piacimento, nessun nodo ha necessità di conoscere la propria posizione, fermo restando che la posizione di ogni nodo rimane valida solo all'interno della rete, proprio per il fatto d'essere definita localmente.
Le moderne trasmittenti radio, delle quali i nodi della rete sono provvisti, possono variare la loro potenza di trasmissione, e possono quindi raggiungere la loro destinazione attraverso un gran numero di piccoli "balzi" (multi hop), oppure tra mite un piccolo numero di grandi "balzi" (single hop).

3.2 Fasi della localizzazione

In ogni algoritmo, e´ facile individuare due fasi comuni che compongono il processo di localizzazione: stima delle distanze tra i nodi (ranging) e stima della posizione dei nodi

(positioning).

→ Ranging (stima della distanza)

Una volta definita una rete di sensori, per attuare la localizzazione di un nodo è necessario conoscere la distanza che li separa. In base al tipo di stima effettuata, le tecniche di ranging si dispongono su due gruppi:

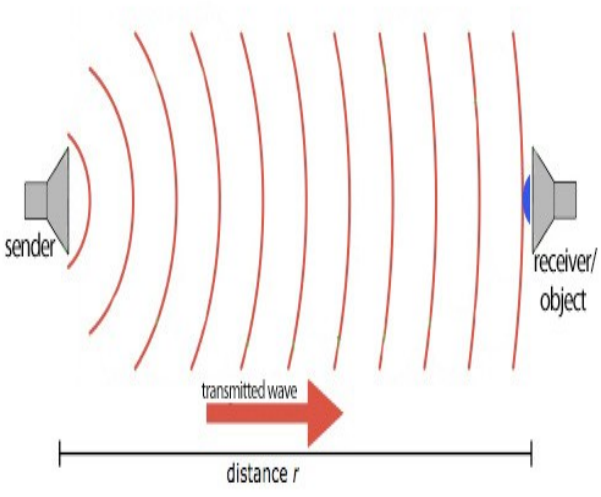
- *Range Based*

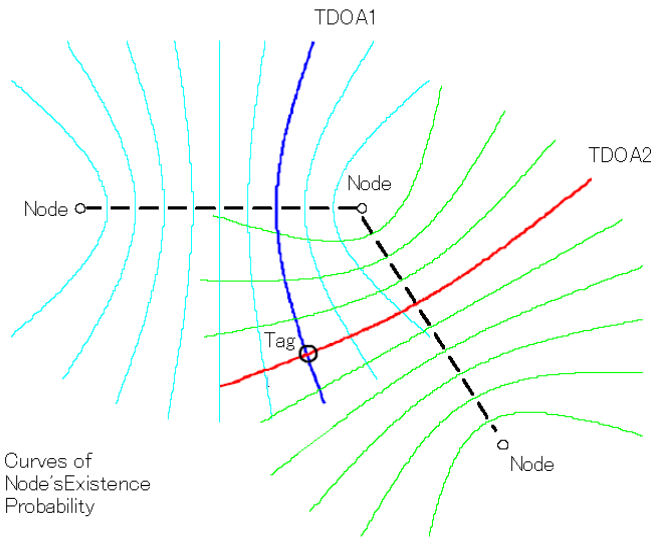
- *Range Free*

La prima metodologia si basa sulla distanza euclidea tra i diversi sensori,
mentre la seconda prescinde dal concetto euclideo, fornendo una misurazione alternativa. [23]

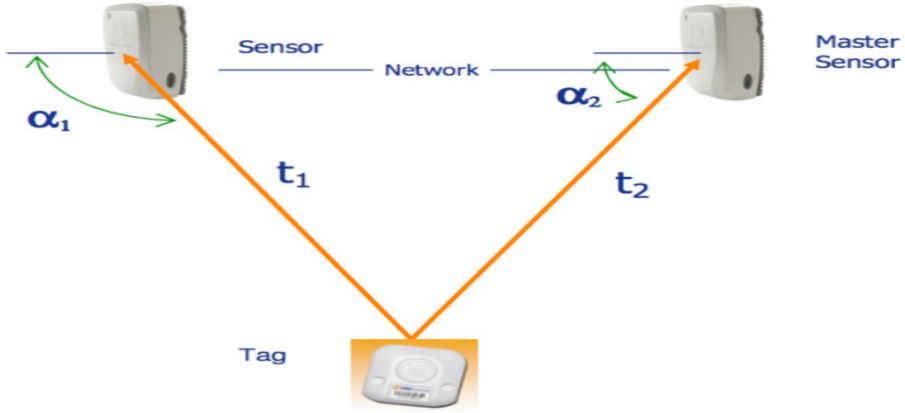
Nel primo gruppo rientrano i seguenti metodi, più comunemente diffusi:

- **Time Based**, nei quali viene misurato il tempo di arrivo del segnale inviato dagli anchors (Time of Arrival) oppure la differenza dei tempi di arrivo di più segnali (Time Difference of Arrival). E' fondamentale conoscere la velocità di propagazione del segnale trasmesso, di qualunque segnale si tratta (ottico, radio, sonoro, ad ultrasuoni etc.) [XVII] [XVIII]



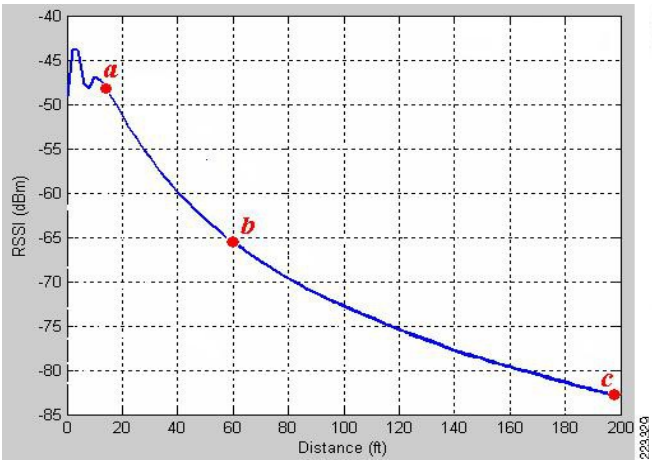


– **Angle of Arrival**, viene utilizzata la distanza angolare rispetto al segnale trasmesso dall'anchor, per il calcolo è necessario ricorrere ad algoritmi trigonometrici quale la triangolazione. E' uno dei metodi più costosi dal punto di vista infrastrutturale, limite compensato però da un 'accuratezza maggiore rispetto, per esempio, a tecniche meno costose quali RSSI. Negli ultimi anni, sono stati apportate diverse migliorie per questo metodo, riassunte in [13]. [XIX]



– **RSSI**, *Received Signal Strength Indicator*, si basa sul potere di trasmissione dell'ancora, il ricevente misura la potenza del segnale ricevuto, tipicamente in dBm, e si calcola la perdita di propagazione. Con questi dati è possibile ricavare una stima della distanza tra i due dispositivi, utilizzando l'equazione di Friis.

[XX] [XXI]



How much power is available?

Simplified Friis Equation

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi R} \right)^2$$

P = Power
G = Gain
λ = wavelength
R = Distance
r = Receive
t = Transmit

Nel secondo gruppo, i più diffusi sono:

- **PiT** (*Point in Triangulation*), il nodo che vuole fare self-localization sceglie 3 ancore intorno a sé, e simula uno spostamento in una posizione arbitraria. Se tutte le ancore si allontanano rispetto alla direzione dello spostamento, significa che il nodo si trova al di fuori del triangolo formato dalle stesse, e dovrà ripetere l'operazione con altre ancore. In caso contrario, se nello spostamento simulato c'è un avvicinamento ad un'ancora, significa che il nodo è all'interno di detto triangolo, e la sua posizione viene approssimata al baricentro.

- **Centroid**, viene utilizzato unicamente in ambito Anchor-Based, basandosi proprio sulla posizione certa delle ancore. Le ancore presenti nel raggio di copertura del nodo da localizzare fanno da vertici per una figura geometrica della quale verrà calcolato il centroide, che corrisponderà alle coordinate del nodo non ancora.

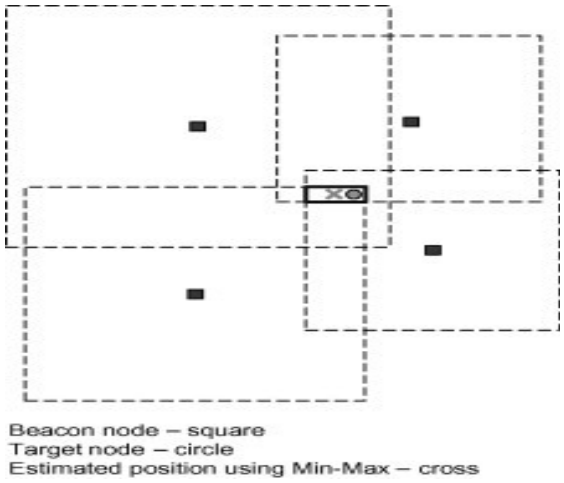
- **DV-Hop**, è una tecnica che usa parzialmente la distanza euclidea tra nodi, viene inclusa in questa categoria perchè viene espressa la distanza come numero di hops. Una volta calcolata la distanza euclidea tra due nodi, questa la si divide per il numero di “balzi” che il segnale ha effettuato.

→ Positioning (Calcolo della Posizione)

Sono presenti svariate tecniche di positiong, differenti tra loro per applicazione su topologie di reti differenti, accuratezza, costo computazionale.
Vengono riportati qui i più comuni:

- **Bounding Box** – detto anche MinMax, è un metodo che vede la posizione del nodo

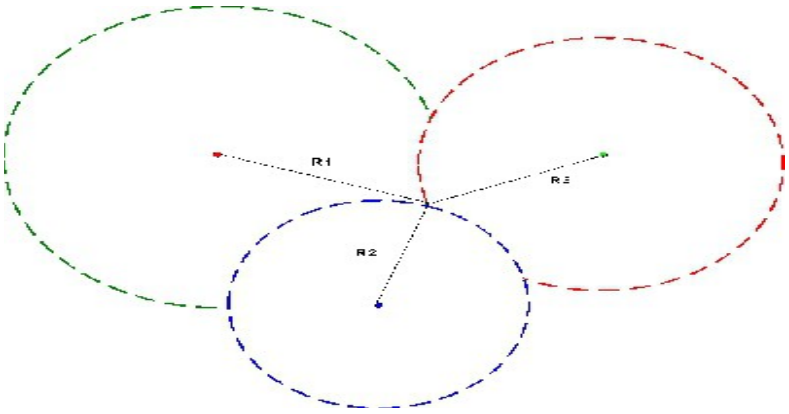
da rilevare come il baricentro dell'intersezione dei quadrati aventi centro nelle ancore e lato pari al doppio della distanza fra nodo e ogni ancora. E' un metodo poco accurato, poco soggetto ad errori di misura e agevolmente scalabile.



[XXII]

- **Triangolazione** – si utilizza in AOA, calcola le coordinate del nodo a partire dalla conoscenza dell'angolo di provenienza del segnale, necessita di almeno 3 ancore e quindi di 3 segnali distinti che raggiungono il nodo da localizzare. Si basa per il calcolo su trigonometria.

- **Laterazione** – ogni ancora funge da centro di una circonferenza, costruita con raggio pari alla distanza stimata (tramite RSSI) dal nodo non-ancora. Anche in questo caso, se si pensa al caso bidimensionale sono necessarie tre ancore. L'intersezione di queste circonferenze identifica la posizione del nodo cercato. [XXIII]



- **Prossimità** – vengono scandite le ancore attorno ad un nodo non-ancora, se nel raggio di copertura ne è presente una sola viene utilizzata la sua posizione come posizione del nodo non-ancora, in caso contrario viene assegnato il valore medio delle coordinate dei nodi ancora presenti.

Capitolo 4

Studio di fattibilita' del sistema

Analizzando le tecnologie descritte, si vuole capire se attualmente ne esiste una in grado di soddisfare tutti i requisiti posti nel Capitolo 1, considerando tematiche fondamentali quali la distanza di lettura, le dimensioni fisiche delle apparecchiature, la precisione di localizzazione, gli algoritmi piu' adatti, l'affidabilita' e la sicurezza.

4.1 Costi

L' ampia offerta di sistemi si riflette su una variegata disponibilita' di prezzi, alcuni troppo elevati per i nostri scopi, altri invece che potrebbero rivelarsi interessanti, posto che sia sempre valido l'aforisma di Samuel Johnson “Qualunque somma tu abbia, spendi meno.”
Ci si riferisce solamente al costo del dispositivo che va applicato agli oggetti, in quanto reale parametro di confronto se moltiplicato per il numero di oggetti da controllare (da poche decine ad piu' di un centinaio).

ZigBee: il costo di questi dispositivi e' stato stimato (nel 2005) di 1,10 $, solamente per il modulo di ricetrasmissione, in grossi quantitativi. A questo poi andrebbe aggiunto il costo di un microcontrollore, ma gia' per il modulo wifi la spesa sarebbe eccessiva. Il modulo CC2430, utilizzato da molti per applicazioni di localizzazione, ha un costo all'ingrosso tra i 3,3$ e i 3,9$, a seconda della quantita' di memoria flash e ram disponibile a bordo[15].

Bluetooth: il prezzo per moduli di questo tipo e' contenuto, si attesta sotto i 3$, andando anche a migliorare le prospettive di lancio (avvenuto nel 1998) che invece ipotizzava un

prezzo all'ingrosso dai 4$ ai 6$. Sempre a titolo esemplificativo, il modulo della National LMX9830 ha un costo al dettaglio di 6,80$ [14].

Rfid: in questa tecnologia, ci sono diversi fattori che fanno oscillare il prezzo dei tag, tra i quali: dimensioni piu' o meno ridotte, resistenza alle basse temperature, quantita' di memoria, raggio di copertura eccetera. In linea di massima, si puo' stabilire una forbice di 0,10 – 10 euro, su volumi d'acquisto importanti. Prezzi che sono in continuo calo, e che dovrebbero, secondo alcuni [13], sfondare il muro dei 5 cent per tag.

4.2 Dimensioni

La questione spaziale non e' trascurabile, se si vuole avere il piu' ampio campione di materiale etichettabile. Anche in questo caso, il discrimine e' sul nodo mobile della rete, ovvero l'oggetto sul quale si vuole applicare il sensore, mentre nessun tipo di vincolo si considera nel “lettore”, se non quello di essere trasportabile. Tutte le tecnologie analizzate, ad ogni modo, dispongono di lettori portatili che non interferiscono in nessuna maniera con l'applicazione in esame.
In questa dinamica, il tag Rfid passivo si rivela la scelta piu' sensata, giocando a suo favore l'assenza di una batteria che ne appesantisce e amplifica l'ingombro.

4.3 La tecnologia Rfid

Posti costo e dimensioni dei dispositivi vincoli non negoziabili per l'applicazione da realizzare, concentriamo la disamina sui chip Rfid, che offrono costi e dimensioni nettamente più convenienti rispetto alle altre tecnologie. In particolare, si andranno a discutere limiti e proposizioni relative all'interazione tra questi chip e UWB, tecnologia

risultata tipicamente adatta ai nostri scopi.

4.3.1 Effetti sulle persone

E' stato effettuato una valutazione empirica sulle risultanze dell'interazione tra Rfid e corpo umano [16]. Nell'esperimento, condotto alla facolta' di Ingegneria di Ladkrabang, ci sono in totale 44 tag su un muro, a 60cm di distanza l'uno dall'altro. Il reader e' stato posizionato a (120, 180 e 240) cm dal muro, e sono state condotti dei test sia con reader su treppiede che imbracciato dall'uomo. Se il reader e' mantenuto dall'uomo, il numero di tag rilevati decrementa, possiamo quindi affermare che il corpo umano ha un qualche tipo d'influenza sul riconoscimento dei tag.
Per ogni misurazione, sono state considerate 20 locazioni, con reader posizionato a 116 cm o 177 cm dal suolo. Le potenze di trasmissione utilizzate sono 26 dBm e 30 dBm.
I risultati ci dicono che la stima dell'errore è più alta nel caso umano, dal quale deduciamo che l'accuratezza diminuisce; all'aumentare della potenza di trasmissione, l'errore si abbassa.
Il numero di tag percepiti su treppiede è quindi superiore di quello umano, a riprova del fatto che il corpo offre una schermatura per questo tipo di onde.
Cosa accade invece quando un segnale UWB attraversa un corpo umano? In uno studio apparso su IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS [19], si nota come anche quest'onda venga in qualche modo assorbita: c'è un decremento di 23,6 dB rispetto alla stessa misurazione effettuata in ambiente senza riverberi, avvertito però solamente con un angolo di incidenza del raggio compreso tra 180° e 240°; è quindi stabilita una corrispondenza tra performance del sistema e angolo di arrivo del segnale. Il fatto curioso che emerge da questo studio avviene in un ambiente affetto massicciamente da multipath, un piccolo ufficio con rumore di fondo a -102 dBm, ininfluente per la banda considerata. In questo esperimento si riduce la distanza tra ricevitore e trasmettitore a 3,14

m, contro i 5 m del caso precedente. Si è misurata una differenza di 6,8 dBm rispetto ad ambiente neutro, dovuta, si pensa, ad una minore dipendenza dalla variazione dell'angolo di incidenza segnale\corpo.
Il comportamento inconsueto di UWB in ambiente con multipath rappresenta uno dei vantaggi di questa tecnologia, che ottiene risultati significativamente migliori laddove i tradizionali sistemi di comunicazione presentano grossi limitazioni.

Un ulteriore esperimento effettuato [20], e che lascia ben pensare, è stato condotto ponendo diversi tipi di antenne UWB nelle strette vicinanze di una superficie metallica. I risultati, anche in questo caso, sorprendono: è stato mostrato che la propagazione dell'energia di backscatter è maggiore, in un'antenna monostatica, quando è posta nell'intorno di un oggetto metallico. Questo effetto è dovuto alle caratteristiche della banda ultra larga, che si contrappongono a quelle già note dell' UHF, che fiaccano il range di lettura in presenza di metalli.

4.3.2 Coesistenza UHF/UWB

Come confermato da Cruz et al. in un recente articolo apparso nel gennaio di quest'anno [17], la pulsazione UWB non è in grado di alimentare il chip del tag, che deve forzatamente attivarsi tramite un onda UHF. La proposta è stata quella di progettare un tag con due facce, nell'una saldato il chip Rfid con la porta UHF, nell'altra l'antenna UWB. I risultati di questo prototipo sono relativamente positivi: ha le stesse prestazioni dei normali tag passivi, ha una range di 4 m indoor e 8 m in campo aperto, ma possiede un'antenna in grado di trasmettere ad altissime frequenze. Questa antenna ha dato esiti simili ad un'antenna stand-alone, dimostrando che UHF e UWB possono coesistere sullo stesso chip, opportunamente settati, senza interferire. Anche le performance di localizzazione si sono rivelate favorevoli: la stima dell'errore è compresa tra 2 cm e 6,5 cm.
Un risultato simile, ma senza proporre un design d'antenna, è stato riscontrato da Amitz et al.[18], i quali specificano che la funzione delle bande UHF debbano essere impiegate

solamente per l'alimentazione e la comunicazione col tag, mentre dall'antenna UWB viene lanciato un segnale a banda larga, che viene ricevuto dal tag, modulato e rispedito al reader. Dal momento che sia il ricevitore che il trasmettitore a banda larga si trovano sullo stesso chip, si ha un processamento del segnale più semplice, in quanto non è necessario praticare alcuna sincronizzazione. Questa soluzione è compatta e di basso impatto infrastrutturale, poiché le operazioni che il tag deve compiere con il segnale UWB sono solamente quelle di backscattering, le quali non necessitano di energia aggiuntiva e arrecano minime modifiche di design rispetto ai tag UHF.

4.3.3 Limiti

Ci sono vincoli di varia natura che frenano , almeno per ora, l'attuazione di un sistema come quello descritto. Possiamo dividerli in due macro aree:

- Limiti normativi
- Limiti tecnologici

System Type Part 15	GPR, Wall-Imaging 15.509	Drywall Imaging 15.510 (C)	(D)	Surveil-lance Systems 15.511	Medical Imaging 15.513	Vehicular Radar 15.515	Indoor General 15.517	Hand-Held Portable 15.519
UWB band, GHz	<10.6	<0.96	1.99 to 10.6	1.99 to 10.6	3.1 to 10.6	22 to 29	3.1 to 10.6	3.1 to 10.6
Frequency Band, GHz	Emissions Limits							
<0.96	15.209 General Limits							
0.96 to 1.61	-65.3	-65.3	-46.3	-53.3	-65.3	-75.3	-75.3	-75.3
1.61 to 1.99	-53.3	-53.3	-41.3	-51.3	-53.3	-61.3	-53.3	-63.3
1.99 to 3.1	-51.3	-51.3	-41.3	-41.3	-51.3	-61.3	-51.3	-61.3
3.1 to 10.6	-41.3	-51.3	-41.3	-41.3	-41.3	-61.3	-41.3	-41.3
10.6 to 22	-51.3	-51.3	-51.3	-51.3	-51.3	-61.3	-51.3	-61.3
22 to 29	-51.3	-51.3	-51.3	-51.3	-51.3	-41.3	-51.3	-61.3
29 to 31	-51.3	-51.3	-51.3	-51.3	-51.3	-51.3	-51.3	-61.3
>31	-51.3	-51.3	-51.3	-51.3	-51.3	-61.3	-51.3	-61.3

Range 0.03 to 0.96 GHz: peak and average detector, 120-kHz RBW
Range >0.96 GHz: dBm/MHz EIRP, rms average detector, 1-MHz RBW

Nella tabella sono riportati i limiti imposti dalla *Federal Communications Commission* (FCC), negli Stati Uniti, sui dispositivi UWB. Questa normativa ha dato l'impulso, nel 2002, ad occuparsi della banda ultra larga. Nel dicembre 2004 ci fu una revisione, dello standard, che portò nuovi dispositivi a farne parte.

La FCC ha definito, per ognuno dei sistemi autorizzati, uno spettro di emissione del livello di potenza, espresso in EIRP (*Equivalent Isotropic Radiated Power),* come riportato in tabella.

L'unione Europea arrivò ad una regolamentazione più tardi, il 21 febbraio del 2007, modificando poi l'assetto nei primi mesi del 2008.

In questo documento sono state approvate tutte le regole stabilite dall'FCC, anche se dello spettro originariamente dedicato ne viene usato solo una parte.

In Europa il limite massimo di -41,3 dBm/mhz Eirp viene applicato solamente sulla banda di frequenze comprese tra 6 e 8,5 Ghz.

Per quanto riguarda la banda UHF, i limiti sono dipendenti dalla nazione e dalla frequenza : in Europa i dispositivi che trasmettono su 2,4Ghz non possono superare i 100mW (corrispondenti a 20 dBm), mentre in USA, sulla stessa frequenza, si hanno 4W (36 dBm) come soglia massima.

Alzando la frequenza operativa, in Europa gli apparati Hiperlan Outdoor (5.4-5.7GHz) sono limitati a 30dBm, pari ad 1W, mentre per i dispositivi a corto raggio non specifici a 5.8GHz hanno il limite di 25mW pari a circa 14dBm.
In USA, il range di limitazione per la banda 5Ghz è compreso tra 50 mW (17 dBm) e 4 W (36 dBm).

I limiti tecnologici maggiori sono rappresentati dal forte condizionamento agli ostacoli che questo sistema oppone. Le onde UHF risentono pesantemente di metalli e acqua, ma sono comunque necessarie per alimentare il tag passivo che altrimenti non avrebbe potenza, e tra quelle analizzate offrono il maggior raggio di copertura. Utilizzare onde a bassa frequenza LF o HF, migliorerebbe sicuramente l'aspetto del *non-line of sight* in termini di penetrazione dei materiali, ma darebbe risultati scarsissimi sulla distanza reader-tag.
Come abbiamo visto, anche le onde UWB sono condizionate dalla componente umana, ed è un vincolo che può pregiudicare fatalmente la precisione nella localizzazione.
Inoltre, il raggio di copertura massimo è modesto in maniera eccessiva, 10 metri per l'applicazione considerata non sono sufficienti, a questi bisogna sottrarre gli errori di misura e l'influenza degli ostacoli, nell'esperienza pratica la riduzione sarebbe notevole ed inutilizzabile allo scopo.
Qualora i limiti normativi ponessero emissioni meno castigate, probabilmente il problema del ranging troppo corto potrebbe essere aggirato aumentando la potenza in uscita del segnale dal reader, in modo tale da coprire distanze accettabili per il tipo di applicazione esaminata.

Capitolo 5

Conclusioni e Sviluppi Futuri

Con il quadro attuale, molti problemi sono stati risolti grazie all'impiego sempre crescente di reti di sensori, le quali permettono di raggiungere obbiettivi sempre più ambiziosi con strumenti che uniscono basso impatto economico a sofisticatezza. Il periodo che stiamo vivendo offre una varietà di risorse amplissimo, impossibile da vagliare approfonditamente
Lo scopo principale è stato quello di creare una soluzione ad un problema che prevede una gestione non facile delle informazioni e della loro trasmissione, e si è tentato di farlo con tecnologie economiche, come le reti di sensori.
Infatti, data l'estensione della tematica trattata non è stato possibile entrare nei dettagli di tutti gli aspetti, mentre altri non sono stati nemmeno toccati.
Uno su tutti, la sicurezza, che entra in gioco in più parti del sistema, negli algoritmi di localizzazione, nella protezione fisica dei dispositivi, nella difesa delle informazioni.
C'è infatti l'aspetto della sicurezza nelle reti di sensori, che è più critico da risolvere rispetto agli altri problemi. Attaccare una WSN richiede difatti meno complicazioni rispetto, per esempio, ad una rete LAN. Questo è dovuto alla semplicità dei dispositivi con i quali la rete di sensori è formata, dotati di protocolli di sicurezza più blandi, proprio per mantenere quel criterio di economicità e di computazione leggera che questo tipo di meccanismi si prefiggono. Un malintenzionato potrebbe senza troppe difficoltà intercettare i dati spediti dai nodi o, ancora peggio, effettuare della manomissione di dati. Questo può avvenire in più modi: il malevolo potrebbe sostituire il nodo con un altro che spedisce dati falsi oppure potrebbero alterare fisicamente i sensori in modo da sfalsare le rilevazioni.
Infine, si potrebbero provare nuovi protocolli nella WSN in grado di migliorare ulteriormente l'efficienza energetica e diminuire la casistica di messaggi persi. Oltre a ciò, è

opportuno procedere all'implementazione del meccanismo di allarme e pensare a come migliorare certi aspetti secondari, come il metodo di applicazione dei tag agli oggetti ed il loro eventuale riuso.

Oggi, in commercio, aziende che propongano sistemi con queste caratteristiche non ce ne sono, vale la pena però menzionare un progetto che, se attuato, potrebbe costituire un'ottima base d'implementazione. Si tratta della TagArray [25], una compagnia formata e fondata da Kourosh Pahlavan e Farokh H. Eskafi, che promette “prestazioni attive ad un prezzo passivo”. Secondo quanto da loro scritto, il sistema costa 100 volte meno ed è 20 volte più piccolo di GEN2 (un sistema rfid della EPCGlobal) ed ha una precisione di 5-7cm a 100m, con 1000 tag letti al secondo. Nel loro progetto, indicano come misura del substrato del tag 4cm x 8cm, che sarebbe una misura accettabile, e frequenza nella banda dei 915 Mhz, che permette di avere meno resistenza agli ostacoli.

Attualmente lo sviluppo non è completo, e stanno cercando partner strategici per riuscire a portare il prototipo sul mercato.

Bibliografia

[1] Daniela Caruso ¨Furti e rapine in aumento con la crisi, Milano e Rimini in testa¨
http://www.fanpage.it/furti-e-rapine-in-aumento-con-la-crisi-milano-e-rimini-in-testa/
20 agosto 2012

[2] ilVelino/AGV NEWS ¨Reati, l´anno nero di furti e scippi¨
http://www.ilvelino.it/it/article/orenove7-reati-lanno-nero-di-furti-e-scippi/366986cd-c0f0-456a-89d8-211e9fa4dc92/
17 giugno 2013

[3] M. Welsh, D. Malan, B. Duncan, T. Fulford-Jones, S. Moulton, ‘‘Wireless Sensor Networks for Emergency Medical Care,’’ presentato alla GE Global Research Conference, Harvard University and Boston University School of Medicine, Boston, MA, Mar. 8, 2004.

[4] C. Schurghers, V. Raghunathan, S. Park, and M. Srivastava.
“Energy-Aware Wireless Microsensor Networks”. IEEE Signal Proc Mag. , 2002

[5] W. J. Kaiser and G. J. Pottie. “Wireless Integrated Network Sensors”. CACM. , 2000

[6] P. Spanos, V. Raghunathan, and M. Srivastava. “Adaptive Power fidelity in Energy Aware Wireless Embedded Systems”. IEEE REAL. 2001

[7] A. Demers, F. Yao, and S. Shenker. “A Scheduling Model for Reduced CPU Energy”. FOCS. , 1995

[8] A. Czarlinska, W. Luh, and D. Kundur. “G-E-M sensor networks for mission critical

surveillance in hostile environments”

[9] G. Mao, B. Fidan, B.D.O. Anderson “Wireless Sensor Network Localization Techniques”

[10] Lennvall, T. ; Svensson, S. ; Hekland, F. “A Comparison of WirelessHART and ZigBee for Industrial Applications” Factory Communication Systems, 2008.

[11] http://www.nanotron.com/EN/CO_techn-css.php

[12] D. Dardari, R. D'Errico, C. Roblin, A. Sibille, M.Z. Win “Ultrawide Bandwith RFID: The Next Generation?”

[13] Kevin Ashton “Whither the five-cent tag?” Rfid Journal, 21 feb 2011
http://www.rfidjournal.com/articles/view?8212

[14] Bluetooth costo
http://www.ti.com/product/lmx9830#this

[15] Zigbee costo

[16] N. Pathanawongthum, P. Cherntanomwong “Empirical Evaluation of RFID-based Indoor Localization with Human Body Effect” APCC, 2009

[17] C.C. Cruz, J.R. Costa, C.A. Fernandes “Hybrid UHF/UWB Antenna for Passive Indoor Identification And Localization Systems” IEEE Transactions on Antennas and Propagation, 2013

[18] D. Amiz, U. Muehlmann, K. Witrisal “UWB ranging in passive UHF RFID: proof of

concept” 22 giugno 2010

[19] T.B. Welch, R.L. Musselman, B.A. Emessiene, P.D. Gift, D.K. Choudhury, D.N. Cassadine, S.M. Yano “The Effects of the Human Body on UWB Signal Propagation in an Indoor Environment” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 20, NO. 9, DECEMBER 2002

[20] F. Guidi, A. Sibille, D. Dardari, C. Roblin “UWB RFID Backscattered Energy In The Presence Of Nearby Metallic Reflectors”, 5th EUCAP

[21] V. Chawla, D.S. Ha “An Overview of Passive RFID” IEEE Applications and Practice, settembre 2007

[22] V. Heiries, K. Belmkaddem, F. Dehmas, B. Denis, L. Ouvry, R. D'Errico “UWB Backscattering System for Passive RFID Tag Ranging and Tracking” ICUWB 2011

[23] H. Suo, J. Wan, L. Huang, C. Zou “Issues and Challenges of Wireless Sensor Networks Localization in Emerging Applications” ICCSEE 2012

[24] T. Sanpechuda, L. Kovavisaruch “A Review of RFID Localization: Applications and Techniques” ECTI-CON 2008

[25] TagArray http://www.isa.org/Content/Microsites530/Computer_Tech__Division/Home528/Passive_Wireless_Sensor_Workshop/PWSW_2012/8-1TagArrayPWST_June_2012.pdf

Ringraziamenti

In questi lunghi anni di studio ho incontrato davvero tante persone, colleghi, docenti, ognuno dei quali ha lasciato un segno. Chi più, chi meno ha trasmesso qualcosa di sé, difficile sarebbe ricordarli qui tutti, a coloro che sono stati presenti in questo percorso vanno tutti i miei ringraziamenti.

In particolare, vorrei ringraziare il Professor Vittorio Ghini, che ha sempre agito con professionalità e perizia, dispensando sempre ottimi consigli. Lo ringrazio per la disponibilità dimostrata, per la comprensione, manifestata da un rapporto con gli studenti che si eleva rispetto alla mera didattica accademica. Ringrazio anche il resto dei docenti, i quali, salvo qualche rara eccezione, hanno sempre agito con competenza nei riguardi delle loro discipline.

Ringrazio i miei genitori, per avermi sempre supportato e mai condizionato, per essere stati sempre pronti a dare una mano in caso di bisogno, e per avermi lasciato quella libertà necessaria a fare quelle scelte che oggi mi portano a questo punto.

Senza di loro, questo obbiettivo molto probabilmente non sarebbe stato raggiunto.

Ringrazio i nonni, gli zii e gli altri parenti, per l'affetto incondizionato e la fiducia riposta, prezioso nutrimento per la stima di sé e antidoto formidabile contro lo scoraggiamento che in alcuni momenti può essere avvertito.

Nella vasta fauna di colleghi con i quali in otto anni mi sono confrontato, preparato e accostato, ne sento di ringraziare particolarmente due, Vincenzo Ferrari e Andrea Mancini, con i quali ho attraversato intensi periodi di studio ed emozionanti esperienze di vita extra universitaria. Li ringrazio per la loro amicizia, per il loro affetto, per essere stati presenti nei momenti di maggiore necessità, in maniera incondizionata e leale.

In ultimo, ringrazio i membri della Balla Bolognese, della quale faccio parte da quando ero matricola, i quali mi hanno trasmesso quel profondo senso di fierezza e di gioia che l'appartenenza al nostro Ateneo è meritevole di suscitare.