Andrea Sansalone

Studio e analisi delle tecnologie ICT finalizzate a favorire l'innovazione e la competitività dell'Euroregione Alpi-Mediterraneo, negli ambiti applicativi caratteristici del territorio

Novembre 2014

Sommario

Indice delle figure

1 INTRODUZIONE

L'Euroregione Alpi-Mediterraneo è un'area collocata al centro dell'Europa meridionale, tra l'arco alpino ed il Mar Mediterraneo, e raggruppa territori affini non solo da un punto di vista geografico, ma anche da quello culturale, storico ed economico. Essa rappresenta un'area strategica fondamentale per l'intera Europa meridionale e i numeri ne dimostrano l'importanza: una popolazione di 17 milioni di abitanti, un Pil complessivo che sfiora i 500 miliardi di euro con una spiccata capacità di esportare (il valore delle esportazioni pari a 110 miliardi di euro), un sistema economico costituito da 1,5 milioni di imprese tra industria, costruzioni, commercio, servizi e agricoltura di cui 1200 grandi imprese e oltre 100 reti d'impresa.

L'Euroregione nasce nel 2007 dalla volontà politica di alcune regioni italiane e francesi di cooperare strettamente per intensificare gli scambi nei comuni settori di competenza al fine di rafforzare legami politici, economici, sociali e culturali tra le loro rispettive popolazioni e operare in favore dello sviluppo sostenibile dell'insieme del territorio.

Con la creazione di tale struttura di cooperazione transnazionale, i governi regionali hanno iniziato un processo di coordinamento e concertazione dando l'avvio ad una serie di collaborazioni per lo sviluppo socio-economico del territorio e l'incremento della competitività delle sue imprese, attraverso iniziative coordinate, partenariati interregionali e cooperazioni strategiche. Per raggiungere tale obiettivo sono state individuate diverse aree tematiche prioritarie quali il turismo e la cultura, l'internazionalizzazione e l'innovazione delle reti d'impresa, il miglioramento del sistema dei trasporti e dell'accessibilità, l'ambiente, la prevenzione dei rischi e lo sviluppo sostenibile. In particolare spiccano le iniziative di collaborazione tra i Poli e i Distretti tecnologici del territorio transregionale finalizzate alla ricerca e all'innovazione in diverse aree tematiche.

In tale contesto si colloca il progetto europeo OCOVA AlpMedNet (Oggetti COmunicanti e VAlorizzazione ALPi-MEDiterraneo NETwork) che focalizza l'azione su tre territori della regione Alpi-Mediterraneo (Hautes-Alpes, Piemonte e Liguria), favorendo lo sviluppo dell'innovazione, il partenariato tra gli attori, la messa

in relazione dei bisogni degli utilizzatori, delle amministrazioni e dei singoli utenti con le offerte degli sviluppatori di soluzioni ICT basate su oggetti comunicanti e servizi mobile. Con tale azione si vogliono promuovere servizi legati alle Tecnologie dell'Informazione e della Comunicazione orientati al consumatore finale, sostenendo e promuovendo le imprese innovative italiane e francesi dei tre territori dell'area Alpi-Mediterraneo.

Oggi innovare e aumentare la propria competitività sul mercato significa sostanzialmente per le aziende passare all'adozione del paradigma Internet of Things nella propria logica di business.

L'Internet of Things (IoT) è un concetto tecnologico dal potenziale applicativo sconfinato, in grado di incidere su competività delle imprese, efficienza delle pubbliche amministrazioni e qualità della vita. L'IoT fa riferimento a un percorso nello sviluppo tecnologico in base al quale, attraverso la rete Internet, potenzialmente ogni oggetto dell'esperienza quotidiana acquista una sua identità nel mondo digitale. L'IoT si basa sull'idea di oggetti "intelligenti" tra loro interconnessi in modo da scambiare le informazioni possedute, raccolte ed elaborate.

I potenziali ambiti di applicazione dell'IoT sono innumerevoli: dai lampioni che regolano la loro luminosità sulla base delle condizioni di visibilità, ai semafori che si sincronizzano per creare un'onda verde per il passaggio di un mezzo di soccorso; dai dispositivi che consentono di rilevare una caduta di un anziano, agli elettrodomestici che regolano il loro ciclo di funzionamento sulla base del costo dell'energia; dalle vending machine che segnalano le necessità di rifornimento sulla base del consumo dei prodotti, ai sensosiri che monitorano le condizioni micro-ambientali per regolare l'irrigazione e l'uso di fitofarmaci in agricoltura. Tema interessante per l'ampiezza degli ambiti applicativi ma anche per la varietà e la dinamicità delle tecnologie abilitanti. Caratteristiche di standardizzazione, apertura, accessibilità dei dati, raggiungibilità degli oggetti intelligenti e multifunzionalità che rappresentano la pienezza del paradigma IoT.

L'IoT può avere impatti importanti sulle attività di imprese e pubbliche amministrazioni, oltre che modificare in meglio la vita delle persone: la velocità di diffusione nei vari ambiti dipenderà dall'esistenza di soluzioni tecnologiche

consolidate e dal bilancio tra valore dell'informazione e costo di creazione della rete di oggetti intelligenti.

Le tecnologie abilitanti per l' Internet of Things sono numerose e caratterizzate da diversi gradi di maturità. Tra queste spiccano in particolare due aree tecnologiche: RFID e WSN.

La tecnologia Radio Frequency Identification (RFID) esiste da molti anni ed è comunemente usata per identificare facilmente un oggetti mobili e per associare ad essi dati di vario genere, ponendo la comunicazione dati in radiofrequenza come alternativa ed evoluzione di altri sistemi di identificazione basati, ad esempio, su lettura ottica (codici a barre). I sistemi RFID più semplici sono caratterizzati da un modello di comunicazione passiva punto-punto; i cosiddetti tag RFID operano solo in presenza di un lettore e non possono comunicare direttamente tra loro. La quantità di memoria che equipaggia il singolo tag è minima e la sua unica funzionalità consiste nel rispondere quando interrogato. Al contrario, nei sistemi RFID attivi, i tag sono equipaggiati con batterie e sono dotati di una circuiteria più complessa. Questo permette di aumentare sia il raggio di azione, sia le capacità di elaborazione e di memorizzazione.

Le Wireless Sensor Networks (WSN) sono reti composte da dispositivi intelligenti miniaturizzati e dotati di sensori che cooperano per monitorare le condizioni dell'ambiente in cui operano. Questa tecnologia prevede l'impiego di nodi caratterizzati da costi molto ridotti, al fine di permetterne l'utilizzo anche in grandi quantità. Questo consente di ottenere una risoluzione delle condizioni ambientali con una granularità che può essere molto più fine rispetto a quella che caratterizza le tradizionali tecnologie di acquisizione dati. Un ambiente reale e complesso viene così trasformato in un sistema sensibile, intelligente e reattivo, garantendo nel contempo elevate capacità di adattabilità, gestione della complessità e tolleranza ai guasti. Le WSN permettono quindi di raccogliere informazioni con elevato livello di dettaglio in un area, anche molto vasta, tipicamente caratterizzata dall'assenza di infrastrutture per la comunicazione. Per questa ragione ogni nodo non è solo la sorgente del dato, ma costituisce anche parte dell'infrastruttura di trasporto. Per assolvere a questi compiti deve essere dotato di una certa complessità. Tipicamente, ogni nodo è composto da tre componenti, che sono: il sensore, il microcontrollore, il modem per la

comunicazione wireless. La gestione di questi dispositivi è affidata ad un firmware che deve essere ottimizzato in termini di occupazione di memoria e di efficienza nella gestione energetica dell'intero sistema. Dal momento che ogni nodo deve gestire in maniera autonoma la formazione ed il funzionamento della rete, il firmware può divenire anche piuttosto complesso. Esistono tuttavia alcuni "sistemi operativi" che semplificano la creazione del firmware e quindi la programmazione dei dispositivi.

Nei capitoli seguenti verranno descritte e analizzate nel dettaglio le tecnologie RFID e WSN e i relativi scenari di utilizzo.

2 LA TECNOLOGIA RFID

In questo capitolo verrà fornita una panoramica generale sui sistemi RFID (**R**adio **F**requency **ID**entification) partendo da alcune note introduttive, la storia e lo sviluppo di questi dispositivi, le parti che costituiscono il sistema, gli aspetti tecnici e di funzionamento, gli standard di riferimento, la presentazione di alcune evoluzioni come la soluzione tecnologica NFC, i molteplici settori applicativi in cui sono inseriti e verrà focalizzata infine l'attenzione sullo stato dell'arte.

2.1 INTRODUZIONE AI SISTEMI RFID

L'acronimo inglese RFID (Radio Frequency Identification) indica una tecnologia che consente l'identificazione attraverso una trasmissione a radiofrequenza; l'identificazione comporta l'assegnazione di un'identità univoca ad un oggetto che consenta di distinguerlo in modo non ambiguo.

Lo scopo principale di questa tecnologia è quello di assumere informazioni su oggetti, animali o persone, relativamente ad operazioni di ricerca, identificazione, selezione, localizzazione spaziale e tracciamento, mediante piccoli apparati a radiofrequenza.

Le componenti del sistema comunicano mediante segnali a radio frequenza, quindi senza necessità di contatto fisico (a differenza, ad esempio, delle carte a banda magnetica) e senza che gli apparati siano in visibilità reciproca.

Nata durante la Seconda Guerra Mondiale per effettuare il riconoscimento degli aerei amici, la tecnologia RFID oggi è in piena espansione, trovando riscontri positivi in innumerevoli settori, e porterà, in un futuro molto prossimo, significative innovazioni nella nostra vita quotidiana. Basti pensare che questa tecnologia è stata classificata dalla teoria economica come una delle General Purpose Technologies, ovvero tra quelle innovazioni duttili estremamente rare come l'elettricità o la macchina a vapore - ne sono state identificate solamente una ventina nel corso dell'intera storia umana - capaci di portare profonde modifiche sugli equilibri economici globali.

È stata messa a punto attraverso il progetto "Costumer Intelligence" dallo scienziato Nicholas Negroponte, portato avanti da uno dei più prestigiosi istituti di ricerca mondiale, l'MIT (Massachusetts Institute of Technology) di Boston, e sostenuto da grandi aziende multinazionali.

La comunicazione RFID si basa sui cosiddetti tag o "etichette intelligenti" dotati di un piccolo chip per la memorizzazione di informazioni e capaci di comunicare i dati raccolti ad appositi lettori in modalità wireless. La cosa sorprendente dei tag RFID è la straordinaria possibilità di unire, a dimensioni estremamente ridotte, capacità di memoria di chip decisamente grandi: argomento di rilevante interesse in quanto si è in grado di trasportare dati a costi zero, o meglio una volta implementate le etichette e l'infrastruttura necessaria, l'aggiornamento a livello di contenuto e la riutilizzazione, quando possibile, non prevedono ulteriori costi. Avere i dati del prodotto significa conoscere la sua provenienza, avere notizia delle trasformazioni subite e tante altre informazioni che oggi è difficile sapere o comunque tenerne traccia.

Questa tecnologia ha subito un lungo sviluppo nell'ombra, forse perché il codice a barre (Bar Code) ha guidato di fatto il mercato, visti i suoi costi quasi nulli e la capillare diffusione che ha trovato. Adesso però si sta procedendo verso una modifica di tale tendenza e le soluzioni di applicazione che si possono legare a questa tecnologia si sono moltiplicate. Quindi definire un solo campo applicativo di questa tecnologia, può risultare fuorviante, quanto riduttivo, anche se, ai suoi esordi, essa è nata e sviluppata principalmente nel campo logistico. Come vedremo nei paragrafi successivi, questa tecnologia lascia un ampio raggio di applicazioni data la sua estrema semplicità, ad esempio: sanità, pubblica amministrazione, trasporti, entertainment, lusso, largo consumo, alimentare, pagamenti, utility, settori manifatturieri, per citare solo i principali.

In particolare l'applicazione dell'identificazione automatica alle persone è estremamente interessante perché può permettere una reale interattività tra il mondo delle cose (la cosiddetta *Internet of the Things*) e gli esseri umani. Un essere umano con un trasponder RFID è riconosciuto automaticamente dai sistemi informativi che quindi possono inviargli informazioni personalizzate per le sue esigenze. La sicurezza dell'identificazione permette non solo di aumentare la sicurezza delle operazioni ma anche di evitare

comportamenti illegali, tuttavia è necessario considerare anche il rovescio della medaglia di questo fenomeno in quanto il controllo delle persone risulta in conflitto con il loro diritto alla privacy. Il problema ha diversi gradi di soluzione che dipendono dagli enti di garanzia (Authority della Privacy) e della volontà delle persone di accettare potenziali limitazioni al loro diritto alla privacy. In ogni caso l'impatto dell'RFID nei principali settori della vita umana sarà straordinario; soprattutto il mondo dei servizi pubblici e della sanità saranno notevolmente modificati. Tutto ciò in rapporto alle nostre decisioni riguardo alla disponibilità di ammettere "invasioni" nella nostra privacy: può essere che le riterremo accettabili durante un viaggio in crociera mentre risulteranno poco gradite o addirittura intollerabili in altri settori quale l'ambiente lavorativo piuttosto che quello medico, particolarmente delicato. In realtà il problema della privacy non nasce con questa tecnologia perché la tracciabilità degli oggetti e delle persone avviene già oggi con l'uso del cellulare o delle carte di credito.

Comunque, allo stato attuale, si può affermare che l'ostacolo maggiore che si oppone alla diffusione della tecnologia RFID consiste nella mancanza di uno standard universale ed aperto. I maggiori produttori offrono sistemi proprietari con il risultato che diverse aziende utilizzano linguaggi tra loro non compatibili per identificare i propri prodotti.

2.2 COMPONENTI E GESTIONE DI UN SISTEMA RFID

La tecnologia RFID è composta da tre elementi fondamentali (Figura 2.1):

- Reader
- Tag (o transponder)
- Antenna

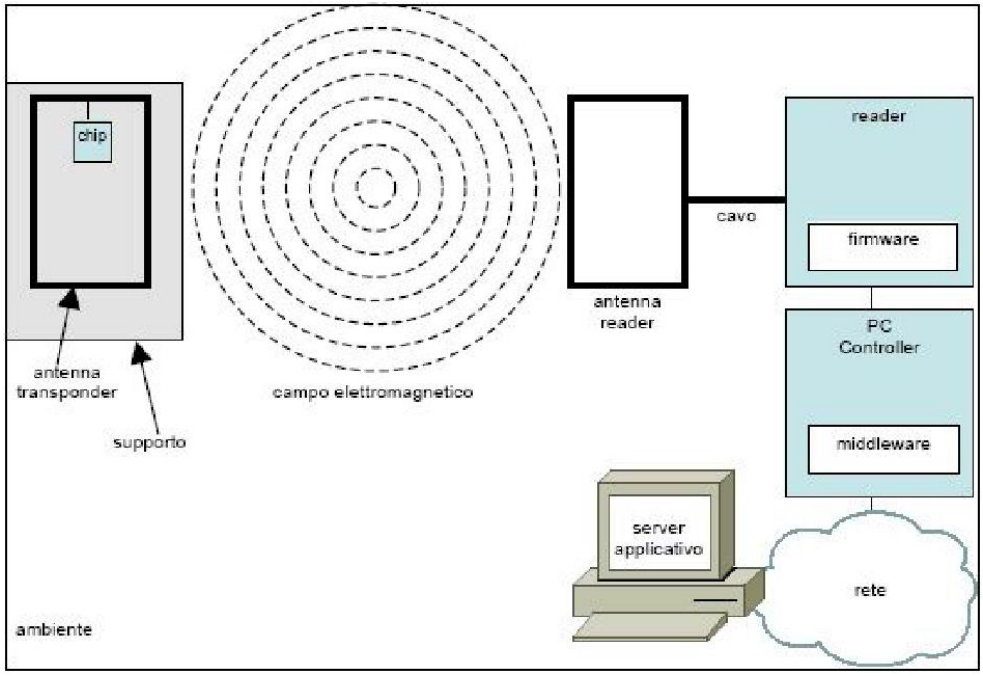

Figura 2.1 – Schema di un generico sistema RFID

In seconda analisi risulta essere di notevole importanza anche il *PC controller* (con relativo *Middleware*) il quale riceve in ingresso le letture del reader, per metterle in rete, dopo un'opportuna gestione, verso il server applicativo.

- Reader

  Il Reader, o lettore, è un ricetrasmettitore controllato da un microcontrollore ed è sostanzialmente usato per scambiare informazioni con i Tag. Questa comunicazione si instaura a partire dal Reader che interrogando il Tag, a seconda della tipologia del sistema, crea una connessione secondo cui il Tag si attiva e riesce a rispondere al Reader (chiamato anche "interrogator" o "controller" se distinto dalla sua antenna).

  Sono solitamente composti da una logica di controllo detta controller, incaricata della supervisione e gestione di tutte le applicazioni supportate, e da un'interfaccia di rete "*network interface*", dotata di interfacce di vario genere (porte seriali RS232/ RS422/RS485, Ethernet, schede digitali I/O, Fieldbus, Profibus, ecc.) e da una o più antenne per la ricezione (trasmissione) dei dati con i Tag. Solo nei sistemi più piccoli

o portatili le antenne sono integrate, in quanto una antenna esterna è sempre preferibile.

I lettori possono essere di tipo:

- ✓ Fisso (per postazioni di lettura pallets presso porte di carico/scarico, per nastri trasportatori, ecc.);
- ✓ Portatile (schede PCMCIA, ecc.);
- ✓ OEM, Original Equipment Manufacturer, (schede da integrare in altri dispositivi quali stampanti bar code o terminali di raccolta dati, automatismi, ecc.).

Sono ad esso delegate tutte le funzioni più importanti di un sistema RFID; deve essere in grado di gestire la corretta comunicazione anche tra più transponder contemporaneamente presenti nel raggio di azione delle antenne ad esso assegnate.

Rientra infatti nelle sue mansioni regolare le comunicazioni e, nel caso si verificassero, risolvere le eventuali collisioni. Come già accennato, gli standard per questa tecnologia prediligono soluzioni Reader in grado di acquisire dati provenienti da molteplici tipologie di Tag, operanti anche a frequenze diverse. Le normative sull'inquinamento elettromagnetico non sono omogenee tra le nazioni, e questo rende necessaria la supervisione diretta del Reader come regolatore delle potenze di emissione.

Con il termine "agile reader" EPCGlobal identifica quei lettori che possono leggere tipi diversi di Tag, di vari produttori, operando anche a frequenze differenti (ma sempre all'interno della propria banda di lavoro, es: la banda UHF); tali lettori sono talvolta definiti anche "frequency agnostic" e/o "protocol agnostic".

Il Reader svolge i suoi compiti in stretta sinergia con il PC controller: insieme gestiscono la memorizzazione e la condivisione dei dati. Possono essere inseriti in una rete LAN che consentirebbe l'acquisizione e lo scambio dei dati anche in maniera remota. Un lettore deve garantire la capacità di confrontarsi nel "mondo reale" con i disturbi alle trasmissioni causate da interferenze e dalla presenza di oggetti che riflettono, distorcono e assorbono le onde elettromagnetiche. In un settore come l'RFID dove gli standard non sono ancora stati completamente definiti,

un lettore dovrebbe garantire la possibilità di aggiornare facilmente il firmware per essere adattato ai nuovi standard in corso di emissione. Non meno importante, i lettori devono rispettare rigorosamente le normative internazionali che regolamentano le trasmissioni radio, e specifiche a seconda del paese nel quale si trovano ad operare.

- Tag

  Il transponder RFID è l'etichetta intelligente che è posta sugli oggetti da gestire, nella quale vengono riposte le informazioni.

  Elementi fondamentali del tag risultano essere (Figura 2.2):

  - ✓ Il chip/memoria ovvero il componente elettronico che ha la funzione intelligente di gestire tutta la parte di comunicazione e identificazione; i Tag sono disponibili in varie dimensioni, capacità di memoria, gamme e resistenze alle temperature a seconda dell'impiego a cui sono destinati.
  - ✓ L'antenna del Tag è il mezzo attraverso il quale lo stesso riceve ed invia le informazioni. Nel caso di Tag passivi essa rappresenta inoltre la fonte stessa da cui trarre l'alimentazione riposta in un condensatore.
  - ✓ Il supporto o packaging, ovvero il materiale di substrato (carta, PVC, resina, ecc.) su cui vengono depositati l'antenna, il chip e creato il relativo circuito. Successivamente, un ulteriore strato protettivo verrà riposto al fine di permettere una resistenza meccanica all'abrasione, urto e corrosione.

  Ciascun Transponder possiede un proprio codice identificativo (ID) univoco dato dall'azienda che lo produce (e che non può essere modificato, cancellato o copiato rendendo ogni Tag unico e impedendo ogni contraffazione) a cui si aggiunge un ulteriore codice identificativo progressivo "impresso" alla prima inizializzazione e assegnazione da parte dell'azienda proprietaria del bene.

  Elemento chiave consiste nel fatto che il Tag solitamente è fissato al dispositivo di trasporto o direttamente sul prodotto creando così un database remoto che si muove insieme al bene. A differenza dei suoi "concorrenti tradizionali" come il codice a

barre, un sistema RFID funziona anche se il transponder non è pulito e visibile o se sottoposto ad alte temperature (che possono mandare in crisi bande magnetiche e Smart card); essendo incapsulabile in strutture protettive (plastica, silicone, ecc.) sono anche maggiormente resistenti a degrado o usura, consentendo di prolungare il ciclo di vita dell'informazione.

Il suo range di lettura/scrittura può, però, essere influenzato dalla presenza di determinati metalli o liquidi, come descriveremo in seguito, che interferiscono o assorbono le onde emesse dal sistema. Ogni installazione pertanto va elaborata e realizzata singolarmente: sistemi ben progettati, prototipizzati ed installati possono sopperire a tali difetti.

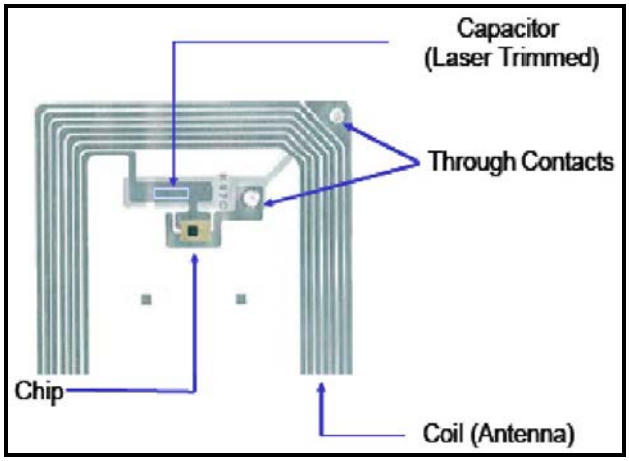

Figura 2.2 – Tag in cui si evidenzia la struttura

- Antenna

  L'antenna, che è la reale interfaccia fisica tra l'unità di controllo e i transponder, utilizza onde radio per leggere e scrivere dati su Tag, etichette, PCB (Printed Circuit Boards, schede a circuito stampato). Le antenne possono avere forme diverse per soluzioni particolari. Un esempio, sono le antenne che offrono varchi intorno a dispositivi di trasporto. Questi varchi (detti anche tunnel o porte) leggono o scrivono Tag/etichette/PCB, mentre questi vi passano attraverso.

La gestione del sistema è affidata ad un PC Controller, che permette di filtrare i dati ricevuti dal Reader. Infatti, immagazzinare tutte le informazioni sarebbe inutilmente oneroso, ridurrebbe in modo sostanziale le prestazioni del sistema; per ovviare a ciò, si utilizza un middleware dedicato, residente nel PC Controller, incaricato di elaborare i dati e di renderli comprensibili all'utente di livello superiore. I criteri di selezione dovranno essere mirati all'applicazione in oggetto, in modo da fornire le informazioni essenziali, prive di incoerenze e dati ridondanti. Il middleware compie anche una ricerca selettiva, che permette di ignorare tutte le letture dal resoconto dei dati, tranne quelle selezionate. In conclusione, possiamo affermare che il middleware si occupa non solo di ricevere dati e a trasformarli in un linguaggio più leggibile, ma aggiunge informazioni legate al contesto e all'utilizzazione futura dello stesso.

La gestione del sistema si dovrà occupare della risoluzione delle problematiche legate all'interconnessione di apparati Reader ipoteticamente anche diversi. In particolare consentirà ad un controllo di livello superiore la ricostruzione della fisionomia della rete LAN di lettori, senza richiedere una configurazione completa ad ogni accensione: al momento della connessione di un elemento, esso verrà immediatamente riconosciuto e gli sarà assegnata la sua mansione predefinita. Separando la componente fisica dalla parte logica dell'applicazione, il middleware garantisce l'interoperabilità del sistema e ne consente una futura evoluzione.

Questi concetti relativi alla gestione del sistema vengono comunque approfonditi nei due paragrafi successivi.

2.2.1 Middleware per la gestione dati del sistema

Un sistema RFID basato su questo schema di massima, produrrà nel tempo una certa mole di dati (letture dei vari codici dei tag). Perché questi dati siano comprensibili, è indispensabile rivederli e posizionarli ad un livello adeguato, mediante delle operazioni di pulizia (innanzitutto, l'eliminazione dei doppi), di verifica del contenuto (che è anche un miglioramento della qualità), di associazione per famiglie di prodotti o per azioni su cui insistono (aggregazione), ovvero, di associazione di questi dati agli eventi per i quali, a seconda delle circostanze e del contesto, essi rivestono particolare valore (gestione degli

eventi). A tutto questo serve il middleware RFID. Il middleware è quindi una componente fondamentale dell'architettura RFID presente sul PC controller connesso al reader. Esso permette di "pre-trattare" i dati di lettura per renderli assimilabili e comprensibili alle applicazioni di business. Il filtraggio dei dati è quindi una, ma non la sola, delle funzioni svolte da questo strato applicativo. È anche indispensabile, a questo livello, controllare ciò che accade all'interno del sistema di raccolta dati. Cioè, avere delle funzionalità di tipo "device management". Fra le altre importanti funzioni del middleware RFID c'è infatti quella di garantire l'interoperabilità dei lettori RFID, perché essi siano il più possibile plug & play, e il controllo di questi lettori, in modo da individuare al più presto gli eventuali malfunzionamenti e poter di conseguenza sostituire l'unità difettosa con un'altra omogenea. Questo consiste in particolare in una serie di meccanismi che, non appena si connette un lettore sulla rete, permettono di riconoscerlo automaticamente e di attribuirgli una funzione, senza necessità di ulteriori interventi. Il middleware insiste quindi tanto sul filtraggio dei dati, quanto sulla gestione integrale del sistema di acquisizione dei dati. Un punto sempre molto importante, ma spesso poco conosciuto quando si parla di middleware RFID, è che questo deve essere capace non soltanto di garantire una funzione di inserimento dei dati nell'ERP dell'azienda (sistema informativo dell'azienda), ma deve anche filtrare questi dati il più in alto possibile, al fine di evitare ogni possibile ridondanza, e anche di classificare tutti i dati temporanei affinché i dati inutili possano essere eliminati al più presto possibile: il che permette di evitare dei veri e propri colli di bottiglia dovuti a grandi quantità di dati da inviare e registrare nel sistema informativo. Infatti è impossibile pensare di immagazzinare tutti i dati provenienti dalle etichette, a meno di voler ipotecare in anticipo grandi quantità di spazio su disco, o subire tempi di attesa molto più lunghi in caso di ricerca di un dato. Piuttosto, si dovranno registrare le informazioni aggiuntive generate a partire da questi dati. E tuttavia anche questi genereranno del volume: è quindi fondamentale garantire una "pulizia di base" almeno per evitare i duplicati eliminando il più possibile i dati inutili, fuori contesto o già obsoleti. Questo spiega perché è stato necessario definire un certo numero di principi architetturali e standard applicativi, per permettere l'implementazione di questi sistemi. In questo contesto, per esempio, spiccano per razionalità i principi definiti da EPC Global:

definiti in origine per applicazioni di grande portata, si possono anche applicare ad ambienti di dimensioni più contenute. Tanto è vero che è stato anche possibile applicare questi principi architetturali sia in un contesto di ambiente aperto che chiuso, quest'ultimo, in generale, più facilmente gestibile da parte delle aziende. Questa architettura definisce soprattutto i principi di filtraggio, ma anche le regole di business che permettono di trasformare i dati grezzi, raccolti da portali o apparecchi di lettura mobile delle etichette RFID, in informazioni gestibili dalle applicazioni di business [3].

In pratica, il middleware permette di trasformare una semplice lettura di etichetta in un evento circostanziato. Il che, tradotto in linguaggio corrente, potrebbe avere la seguente forma: lettura del pallet X, contenente 12 articoli di referenza 28471927, alle 8.45, all'entrata del dock D, provenienti dal fornitore Martin, con sede a Tours, che devono essere rispediti nel giro di otto ore ai clienti con codice 342426 e 564235. In altri termini, il middleware non si accontenta di trasformare semplicemente un dato grezzo recuperato da un lettore o un portale in un formato leggibile dalle applicazioni di supply chain coinvolte, ma in più arricchisce questo dato, completandolo con informazioni di contesto, relazionate direttamente con gli eventi sopraggiunti nel ciclo di vita del prodotto e con l'uso che se ne intende fare. Altro punto interessante di questo sistema di architettura, è che esso evita di dover mettere in atto dei collegamenti punto a punto fra i dispositivi di lettura e le applicazioni di business. La non connessione diretta fra un il lettore RFID e l'applicazione evita che sia necessario un driver specifico per ciascun singolo utilizzo, fonte di problemi nel caso in cui si voglia far evolvere il proprio sistema, per esempio quando si deve passare da una generazione da lettori ad una successiva. Separando la parte fisica dalla parte logica dell'applicazione, il middleware ne garantisce in realtà l'interoperabilità e la possibilità di evoluzione.

Il secondo compito del middleware è quello di garantire la diffusione e l'integrazione delle informazioni di business derivate dai dati RFID in un sistema per sua natura non integrato. Il middleware giocherà allora una funzione comparabile a quella di un router o di uno scambio ferroviario, per poter dirigere le informazioni pertinenti verso l'applicazione corretta, in funzione dell'utilizzo che se ne deve fare. Inoltre, non si tratta di fare delle connessioni punto a punto fra i dati e le applicazioni, ma di appoggiarsi sul

concetto di EAI (Enterprise Application Integration) per permettere una circolazione fluida e pertinente dei dati di business fra le applicazioni aziendali, anche quando queste devono uscire dalle singole applicazioni, quando cioè questi dati devono essere condivisi con i sistemi informativi di altre aziende integrate nel processo della supply chain (come possono essere fornitori e distributori). In altri termini "routare" in modo adeguato questi dati presuppone due cose. Da una parte, bisogna classificare gli eventi che impattano sulle varie applicazioni, dall'altra determinare le applicazioni coinvolte, per poi scambiare con esse queste informazioni. Vi si ritrova quindi una doppia funzione: quella della gestione degli eventi e di arricchimento dei dati filtrati, e quella di indirizzamento delle informazioni così prodotte verso i processi di business coinvolti. Poiché le applicazioni che utilizzeranno i dati RFID sono diverse, e per i limiti delle funzionalità rete di cui dispongono i lettori, è necessario disaccoppiare lettori e applicazioni. I lettori producono eventi RFID, li inviano ai sistemi di messaggistica del middleware e sarà responsabilità di questi ultimi di inviare i messaggi ai loro destinatari corretti (cioè i processi di business). In un simile sistema di pubblicazione/diffusione, questo permette al lettore di non doversi occupare mai di chi siano i destinatari dei dati che egli ha raccolto. Allo stesso modo, le applicazioni non devono stabilire dei legami diretti con i lettori: non devono fare altro che specificare gli eventi che li riguardano, abbonandosi al sistema di messaggistica[3].

Da ciò derivano tre caratteristiche importanti del middleware:

- *Indirizzamento completo o indirizzamento parziale*: per lo più, le applicazioni non hanno bisogno che di un solo sottoinsieme di dati, non di tutti quelli che sono stati catturati. Questo sottoinsieme è generalmente specificato con l'identificatore dell'etichetta, e solo questa informazione è trasmessa all'applicazione per la quale il middleware effettua lo smistamento. In caso contrario, l'applicazione dovrebbe effettuare essa stessa questo smistamento sulla totalità dei dati, cosa che graverebbe non di poco sulla banda passante della rete e quindi sulle sue prestazioni.
- *Feedback dell'iscrizione*: se vi sono particolari criteri di accesso ai dati da parte delle applicazioni, può essere opportuno installare un meccanismo di gestione delle

autorizzazioni a livello dei lettori, e non di middleware. Si può quindi avere un meccanismo di "retroazione", di feedback, sui lettori stessi, per determinare quali sono le applicazioni interessate dai dati che essi producono. Tale feedback permette anche di gestire meglio i lettori e i loro settaggi: per esempio il fatto che un lettore debba distinguere e leggere solo una particolare categoria di tag, o che uno dei lettori debba essere semplicemente annullato per permettere a un altro lettore di disporre di tutta la banda passante. In questo caso, vi è un controllo dei dati che non si effettua più a livello del middleware, ma è portato a livello della trasmissione wireless. Sempre più spesso, quindi, i lettori integrano funzioni di controllo, e dispongono di interfacce programmabili per classificare i dati e le priorità da assegnare loro in funzione delle applicazioni interessate. Questo alleggerisce molto il lavoro del middleware, che può allora dedicarsi a compiti di arricchimento e non più alla gestione, sempre pesante, della banda passante disponibile fra l'hardware e le applicazioni aziendali.

- *Affidabilità*: certe applicazioni hanno tuttavia bisogno di ricevere immediatamente tutti i dati di flusso RFID. In questo caso, il meccanismo precedente non ha più affatto ragion d'essere. Ma se le applicazioni ricevono i dati a lotti, è indispensabile che il middleware assuma anche delle funzioni di coerenza dei dati, e anche di conservazione di questi dati fino a che l'applicazione coinvolta non ne richieda l'invio.

Quanto all'integrazione nei sistemi informativi, il suo obiettivo principale è far in modo che le applicazioni interessate accedano ai dati in modo ordinato, ovvero evitare le incoerenze nella trasmissione dei messaggi RFID verso i processi di business che ne devono fare uso. Ma l'integrazione deve anche fare in modo che le informazioni ricevute possano determinare delle azioni da intraprendere a livello di gestione: far sì che siano raccolti certi dati piuttosto che altri, aggiornare i contenuti delle etichette o determinare il momento in cui tali dati devono essere inviati, se subito o dopo un certo periodo di latenza. In altri termini, la comunicazione deve essere possibile in entrambi i sensi e questo significa che, nel middleware, saranno contemplati anche dei meccanismi di

reattività integrata e bi-direzionale, affinché chi gestisce l'azienda possa far sentire la sua voce a livello dei lettori, e non soltanto il contrario.

Un altro punto importante è quello della diffusione dei dati RFID. L'informazione raccolta da un lettore generalmente non interessa una sola applicazione, bensì un insieme di processi di business nell'azienda, anzi, anche al di fuori di questa, nelle aziende che fanno parte della sua rete di collaborazioni. Per questo i dati raccolti dovranno essere distribuiti a tutte quelle entità che saranno in grado di dimostrare quale sia il motivo per cui vi devono accedere. Per fare ciò, è importante che siano previsti tempi diversi di latenza e di conservazione dei dati, poiché la notifica della disponibilità di questi dati sarà diversa a seconda del tipo di applicazione. Vi saranno infatti applicazioni che necessitano di riposte immediate in quanto operano nel contesto di una interazione locale con gli oggetti fisici; il tempo di latenza, di conseguenza, sarà praticamente nullo. Altre, al contrario, non hanno niente a che vedere con la manipolazione del flusso dei dati, e possono benissimo ricevere questi dati a intervalli temporali predefiniti. Innanzitutto, per la maggior parte delle applicazioni è impensabile ricevere dati che non siano stati pre-trattati. Inoltre, possono anche esservi delle applicazioni che devono ricevere non tutti i dati, ma solo un loro sottoinsieme. Visto che l'RFID permette l'identificazione a diversi livelli, anche quello della categoria a cui l'oggetto appartiene, si potrà decidere con una certa libertà, evidenziando ciò che realmente l'applicazione intende raccogliere, potendo ovviamente arrivare a livelli di dettaglio molto elevati. Alcuni tag hanno sufficiente memoria per mettervi ben più di un semplice identificatore. In tal caso, il middleware deve poter fornire delle funzionalità di lettura-scrittura di questa memoria addizionale. Questa potrebbe essere utilizzata per registrare dei dati provenienti dalle applicazioni coinvolte, come per esempio la data di scadenza di un prodotto, ma anche per facilitare lo scambio dei dati nel caso in cui non sia disponibile l'accesso alla rete. La proliferazione dei lettori richiede che essi siano gestiti in un contesto di asset management. È una delle funzioni che più si vedono apparire su certi middleware; una funzione, indispensabile, poiché permette di gestire le disfunzioni e quindi le sostituzioni dei lettori, le modifiche di configurazione, le migrazioni dei sistemi e così via. Grande importanza riveste la protezione dei dati. Se il tag contiene un identificatore unico, che fa da puntatore verso

fonti di dati distribuite sulla rete e gestite dalle aziende, è molto importante sapere se una determinata applicazione è autorizzata ad accedere ad un determinato dato, e perché. Da qui la necessità, per il middleware, di garantire anche la gestione delle funzioni di verifica dei dispositivi connessi sulla rete (lettori RFID, applicazioni fornitore che accedono ad un database aziendale, terminali di lettura presso il distributore, ecc.). Effettivamente, è fondamentale conoscere in qualsiasi momento chi abbia questi diritti. Se il middleware può analizzare e identificare i dispositivi, i privilegi accordati a ciascun lettore sono verificati e, se il caso, approvati, nel momento in cui esso accede alla rete. D'altronde, seppure in un contesto in cui tutto, per definizione, deve essere tracciabile, bisogna poter distinguere fra dati pubblici e dati privati. Vi sono informazioni che non sono fatte per essere messe in mani qualsiasi, si pensi per esempio a ciò che riguarda determinati clienti o fornitori. È questa la ragione per cui cominciano ad apparire dei sistemi di identificazione "federali", che permettono, partendo da uno stesso identificatore posizionato nell'etichetta, in funzione del middleware che legge i dati, l'accesso soltanto a quella porzione di informazioni che sono di pertinenza dell'azienda in questione.

Le offerte di middleware distinguono spesso tre tipi di software:

- ✓ *edgeware*: posizionato all'estremità (edge, in inglese) dell'hardware e della rete aziendale, l'edgeware garantisce la gestione dei dati RFID a livello della loro acquisizione e del loro pre-filtraggio. È quello che si occupa anche della gestione delle periferiche e del loro aggiornamento, sia a livello dell'etichetta che del lettore;
- ✓ *gestione eventi*: arricchisce i dati grezzi associandoli al contesto della loro raccolta;
- ✓ *integratore*: formatta i dati in informazioni direttamente accessibili da parte delle applicazioni coinvolte;

Il tutto utilizza una componente comune, il sistema di messaggistica, che veicola i dati e tutte le richieste, sia a valle che a monte. La sincronizzazione dei dati è una dimensione supplementare che deve essere implementata nel middleware.

2.2.2 Rete e server applicativi

La rete rappresenta il punto di congiunzione tra il PC Controller ed i Server applicativi. Attraverso di essa vengono trasmessi i dati filtrati dal middleware, correlati da eventi e stati come data, ora, luogo, reader, di fondamentale importanza per la loro archiviazione e condivisione.

Tutti gli aspetti riguardanti gli impianti di rete sono quelli relativi all'esperienza dell'informatica tradizionale, ovvero comprendono tutti i relativi standard affermati fisici e di comunicazione.

I Server applicativi permettono invece di collegare ed integrare le informazioni dai confini dell'azienda all'ambiente operativo aziendale.

Punti fondamentali che si propongono di offrire sono:

- Miglioramento della gestione delle risorse e del capitale d'esercizio, fornendo funzioni di tracciabilità delle risorse stesse.
- Condivisione dati collaborativa all'interno dell'azienda e con i Business Partners con funzioni di tracciabilità e analisi dei trend.
- Aumento della produttività dei centri di distribuzione tramite l'acquisizione e la verifica automatizzate dei dati.
- Maggiore precisione dei dati per migliorare il servizio clienti.
- Aumento dei margini di guadagno con funzioni point-of-decision potenziate e più canali di vendita.
- Riduzione dei costi di ritiro, restituzione e riconciliazione grazie all'ottimizzazione di allocazione e pianificazione.
- Riduzione dei tempi di inattività grazie alla tecnologia RFID in costante evoluzione.

Molte società oggi si stanno impegnando in questa direzione, realizzando software sempre più efficienti e completi. Un esempio tra tutti è la Microsoft con "BizTalk Server", un sistema server che presenta grandi potenzialità nell'integrazione delle tecnologie RFID con i sistemi legacy già presenti all'interno dei sistemi informativi delle aziende retail. Il suo punto di forza è la sua capacità di orchestrare la comunicazione tra differenti sistemi utilizzando linguaggi e protocolli standard[4].

Un' altro esempio è proposto dalla Sun Microsystems con la piattaforma software per la gestione della problematica RFID chiamata "Java System RFID Software", basata sugli standard e sulla architettura EPC ed è costruita utilizzando la piattaforma Java Enterprise System ed il linguaggio Java J2EE. Per poter essere flessibile e garantire una futura interoperabilità la soluzione architetturale fa riferimento a degli standard aperti. Sun Microsystems ha scelto di sviluppare una soluzione RFID secondo le specifiche definite dall'Auto-ID center ed accettate dall'EPCGlobal. Componente fondamentale della soluzione Sun Java System RFID Software è l'RFID Information Server che interpreta/filtra e propaga le informazioni provenienti dai livelli inferiori verso i sistemi aziendali. E' una applicazione Java basata su application server che agisce da interfaccia per la ricerca e il recupero delle informazioni relative ad un transponder, gestisce l'osservazione e il monitoraggio dei dati associati ai tag, mappa le informazioni legate al tag verso strutture dati di livello superiore trasformando le osservazioni di basso livello provenienti dal mondo RFID in funzioni di business. L'RFID information server è in grado di recuperare le informazioni associate ad un tag sia da una base dati locale che da un repository esterno utilizzando unicamente le informazioni numeriche (es. codice EPC) presenti nel tag stesso. L'RFID information server realizza anche la funzione di track & trace degli eventi provenienti dall'event manager per certificare/validare le azioni RFID fornendo una nuova dimensione per gli aspetti di conformità e riconciliazione[5].

Una considerazione utile che vale la pena di evidenziare è che quando si sostituisce l'attività umana in un processo di identificazione di un oggetto usando la tecnologia RFID, il sistema deve necessariamente funzionare. Una abilità degli umani che una macchina difficilmente riuscirà a sostituire, per quanto potente possano diventare, è la capacità di improvvisare e pertanto di gestire le eccezioni. In caso di comportamento erratico o di dubbio un uomo in qualche modo può trovare delle soluzioni per poter aggirare i problemi. In caso di guasto, un sistema di identificazione RFID (dal transponder al server applicativo) semplicemente non funziona. Pertanto l'intero sistema e in particolare il PC Controller e i Server applicativi devono essere oggetto di un attento studio.

2.3 CLASSIFICAZIONE DEI SISTEMI RFID

I sistemi che utilizzano tecniche RFID sono molteplici. Una prima classificazione può esser fatta in base alle seguenti caratteristiche:

- Fonte di alimentazione
- Frequenze di lavoro
- Tipo di memoria
- Tipo di accoppiamento fisico

2.3.1 Fonte di alimentazione

I tag possono essere distinti, in primo luogo, per la gestione delle fonti energetiche. Esistono di tre diversi tipi: passivi, semi-passivi e attivi.

- **Passivi**: sono passivi quei tag che, non essendo dotati di una sorgente di alimentazione interna propria, lavorano con un'energia che viene ricavata dal campo elettromagnetico che li investe quando entrano nell'area di influenza dell'antenna del lettore, antenna che emette un campo di una determinata potenza. Quando tale campo investe l'antenna trasferisce a questa una quantità di energia che viene opportunamente gestita dal chip consentendo l'attivazione del tag. L'intensità del campo generato dal lettore decresce molto rapidamente all'aumentare della distanza ed è limitata dalle normative sui livelli di emissione RF del reader medesimo. Essa si fa quindi via via più debole fino al punto in cui l'energia che l'antenna del tag può raccogliere diventa insufficiente al suo funzionamento. La distanza massima per cui il reader riesce a riconoscere il tag viene definito "raggio d'azione" dell'accoppiamento lettore \ tag. Nei tag passivi il raggio d'azione può variare da alcuni centimetri a pochi metri, in particolare con la tecnologia odierna si riesce difficilmente a superare il limite degli 5 metri. I vantaggi di questo modello di tag riguardano il basso consumo e la capacità di gestire segnali RF affetti da rumore. In termini di potenza computazionale, non si va oltre una logica di base ed una macchina a stati in grado di eseguire semplici istruzioni. I tag contengono una certa quantità di memoria non volatile.

Naturalmente maggiore è la memoria maggiori sono le dimensioni del chip ed i relativi costi. Questa tipologia di tag è decisamente la più diffusa ed impiegata nelle applicazioni massive. I tag passivi sono solitamente dispositivi a basso costo e di piccole dimensioni che consentono di realizzare numerosi tipi di applicazioni, legate soprattutto alle particolari caratteristiche dimensionali del tag. Essendo infatti costituiti solamente da un'antenna (tipicamente stampata) e da un circuito integrato generalmente miniaturizzato, la dimensione dei tag passivi può essere anche di poche centinaia di micron. I tag, quindi, possono essere inseriti in carte di credito, etichette adesive, bottoni ed altri piccoli oggetti di plastica, fogli di carta, banconote e biglietti d'ingresso, generando così veri e propri oggetti "parlanti".

La Figura 2.3 illustra un tipico sistema RFID con Tag passivo; quest'ultimo è composto da un'antenna e un chip ASIC, entrambi con impedenza complessa. Il chip ottiene potenza dal segnale trasmesso dal Reader. Il Tag manda indietro informazioni cambiando la sua impedenza tra due stati, modulando in questo modo il segnale in backscattering, che è l'onda reirradiata dal Tag al Reader. I dati scambiati tra Reader e Tag possono utilizzare diverse modulazioni e schemi di codifica, come ad esempio ASK, PSK, codifica Manchester.

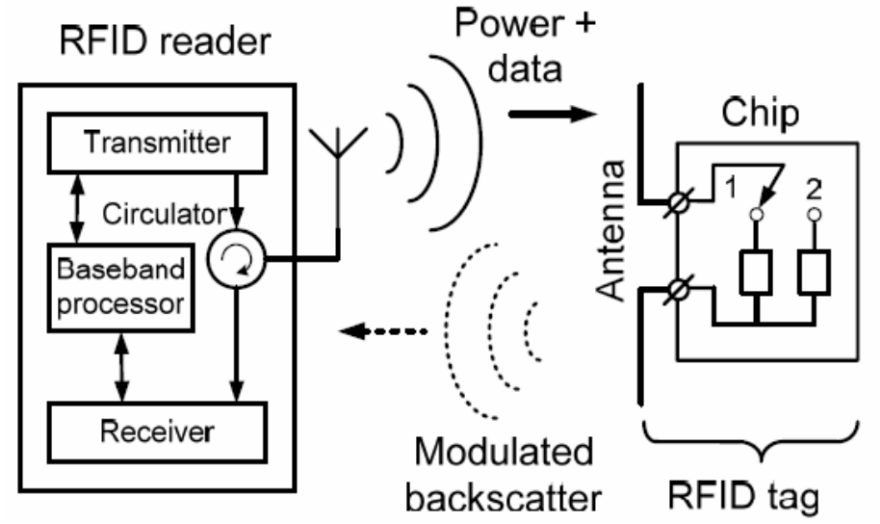

Figura 2.3 – Schema di funzionamento di un sistema RFID UHF

L'adattamento dell'impedenza tra l'antenna e il chip è molto importante in questi sistemi. Infatti influenza direttamente le potenzialità, come la profondità di lettura e di scrittura del Tag da parte del Reader.

La Figura 2.4 mostra lo schema a blocchi che descrive il funzionamento di un TAG passivo.

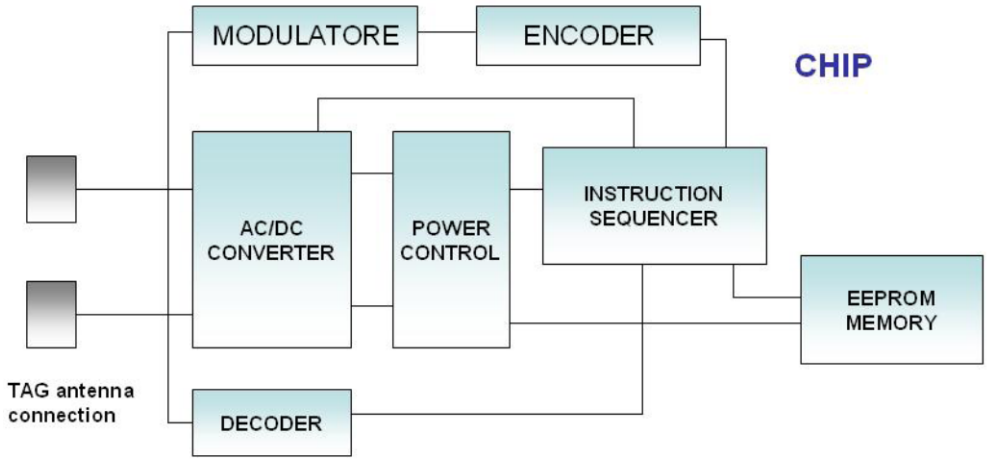

Figura 2.4 – Schema a blocchi di un TAG passivo

- **Semi-passivi**: i tag semi-passivi usano, come i tag passivi, il campo elettromagnetico generato dal segnale del reader come sorgente di energia per trasmettere, ma non per alimentare i propri circuiti. Nel tag infatti è inclusa una batteria, utilizzata però solo per alimentare il chip, non per comunicare con il reader. Questo consente al chip medesimo di realizzare funzioni più complesse e di operare anche quando il tag non riceve energia dal reader. Tuttavia la distanza operativa è limitata, come nei tag passivi, dal fatto che il tag non ha un trasmettitore integrato, ma è obbligato ad usare il segnale del reader per rispondere. Le distanze risultanti arrivano fino a 100 m. Alcuni tag semi-passivi "dormono" fino a quando vengono "risvegliati" da un segnale prodotto dal reader, il che consente di diminuire il consumo energetico. Il vantaggio dei tag semi-passivi è di poter montare memorie di maggior capacità e riscrivibili, nonché,

su alcuni modelli, sensori ambientali per misurare temperatura, pressione, movimento ecc. Usufruendo della fonte di energia della batteria i sensori possono compiere misure e conservarle in memoria con le informazioni temporali e restituirle all'interrogazione del reader, fornendo una storia della vita dell'oggetto a cui sono associati. La cosiddetta catena del freddo costituisce un'applicazione tipica per queste caratteristiche. La batteria con i suoi costi, la sua durata e le connesse problematiche di inquinamento, costituisce la principale criticità per questo tipo di tag. Alternativa alla disponibilità di una batteria può essere quella di ricavare energia dall'ambiente, attraverso piccole celle solari o sistemi inerziali che caricano accumulatori come in alcuni recenti orologi da polso.

La Figura 2.5 mostra lo schema a blocchi che descrive un TAG semi-passivo.

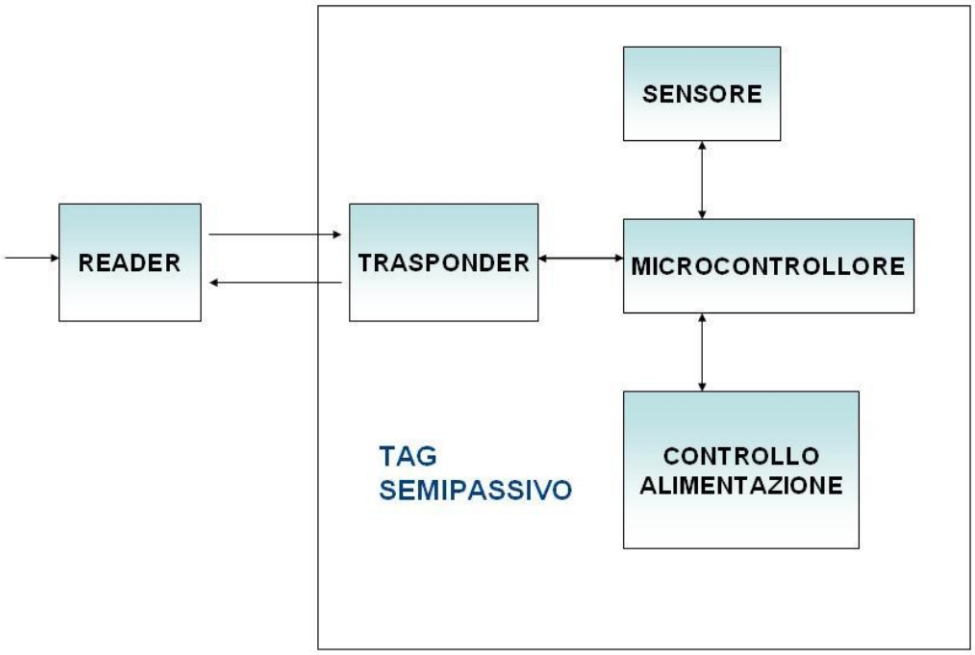

Figura 2.5 – Schema a blocchi di un TAG semi-passivo

- **Attivi**: i tag attivi sono dotati di una sorgente autonoma di alimentazione che fornisce energia sufficiente alla loro operatività, in questo modo tali trasponder risultano indipendenti infatti essi incorporano un ricevitore e un trasmettitore come i reader. Un tag attivo, inoltre, è capace di emettere a sua volta un certo

livello di energia per trasmettere al lettore le informazioni che contiene. Nei tag attivi contrariamente a quello che accade con quelli passivi, il tag può trasmettere emettendo un campo elettromagnetico la cui potenza è normalmente limitata solamente dalla necessità di ridurre i consumi per consentire una certa durata della batteria che li alimenta. Il primo vantaggio dei tag attivi è dato dalla distanza operativa (permettono distanze di lettura da qualche metro a 100 metri) molto superiore rispetto a quelli passivi e semi-passivi, in quanto equipaggiati con un vero trasmettitore alimentato da fonti di energia. La distanza raggiungibile è limitata unicamente dall'antenna e dall'energia disponibile nelle batterie. Altro vantaggio è che normalmente la memoria a bordo ha dimensioni più ampie di quella dei tag passivi e possono essere eseguite operazioni di lettura e scrittura su di essa. A volte i tag attivi hanno a bordo sensori di vario genere (temperatura, pressione, movimento, ecc.) che vengono usati, come si è detto, anche per i tag semi passivi. Questi apparati sono generalmente prodotti per frequenze elevate (UHF, SHF) e sono naturalmente dedicati ad applicazioni "di pregio", oppure in casi in cui il tag sia utilizzabile più volte. Sono impiegati per localizzazione di veicoli, tracciamento merci di alto valore, sistemi di pagamento elettronici, localizzazione veloce di oggetti riutilizzabili in campo aperto (quali ad esempio i pallets, ecc…).

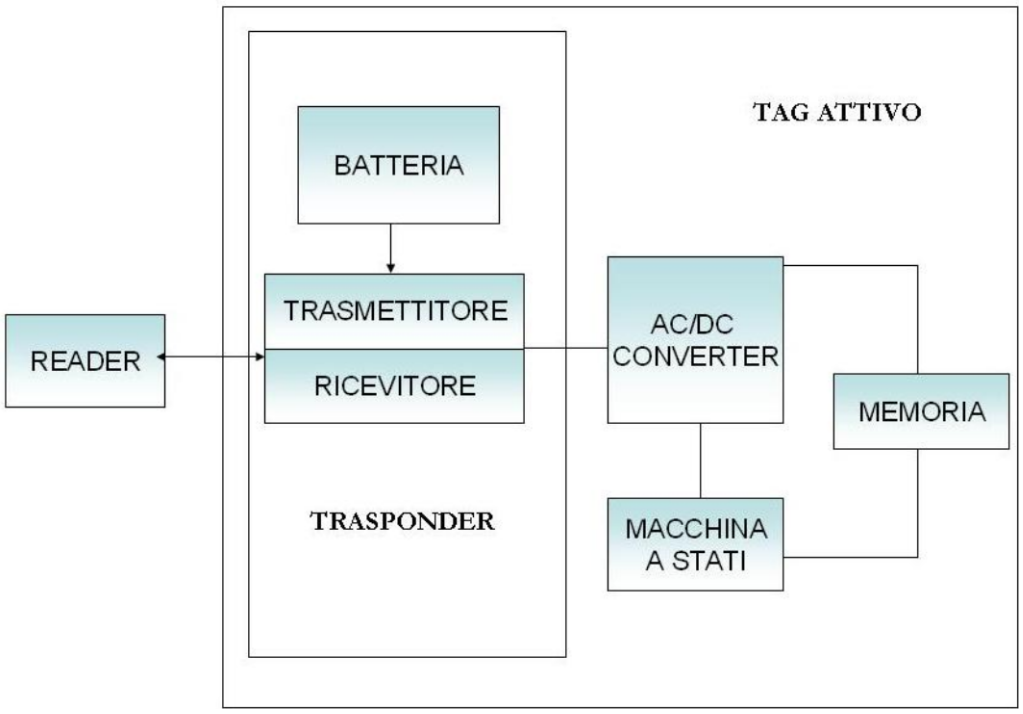

Figura 2.6 – Schema a blocchi di un TAG attivo

In sintesi i tag attivi:

- non devono essere alimentati dal campo emesso dal lettore per poter trasmettere i loro dati a differenza delle altre due tipologie che funzionano solo se immerse nel campo di interrogazione del lettore;
- emettono una quantità di energia sufficiente a far sentire la loro esistenza anche ad alcune centinaia di metri.

Per contro c'è da tener presente il costo consistente e l'ingombro recato dalle dimensioni.

La tabella seguente mostra invece una panoramica generale dei sistemi attivi, passivi e semipassivi, evidenziando vanataggi, svantaggi, le condizioni di lavoro, le applicazioni e le bande di frequenza in cui operano generalmente.

Tipo di TAG	Vantaggi	Svantaggi	Commenti
Passivi	- Tempi di vita elevati - Vasta gamma di forme - Flessibilità meccanica elevata - Costi ridotti	- Distanze limitate a 4-5 m (UHF) - Controllati rigorosamente da regolamentazioni locali	- E' la tipologia maggiormente utilizzata nei sistemi RFID - Bande: LF, HF o UHF
Semi-Passivi	- In grado di controllare sensori (temperatura, pressione, ecc.) - Non rientrano nelle rigorose normative per i TAG passivi	- Costi elevati a causa della batteria e degli involucri - Affidabilità limitata, per l'efficienza della batteria - Rischio ambientale per la presenza di prodotti chimici potenzialmente tossici nelle batterie	- Utilizzati principalmente in sistemi in tempo reale per tracciare materiali o dispositivi di elevato valore all'interno di un'azienda - Bande: UHF
Attivi	- Distanza operativa elevata		- Utilizzati nella logistica per il tracciamento di container su treni, camion, ecc. - Bande: UHF

Tabella 2.1 - Confronto tra le tre tipologie di tag con principali vantaggi e svantaggi

2.3.2 Frequenze di lavoro

Le frequenze di comunicazione tra Reader e Tag dipendono sia dalla natura del Tag, sia dalle applicazioni previste e sono regolate (per controllare le emissioni di potenza e prevenire interferenze) dai consueti organismi internazionali e nazionali. La regolamentazione, però, è divisa in regioni geografiche con normazione diversa da regione a regione, che comporta spesso incompatibilità, quando gli RFID viaggiano insieme alle merci alle quali sono associati.

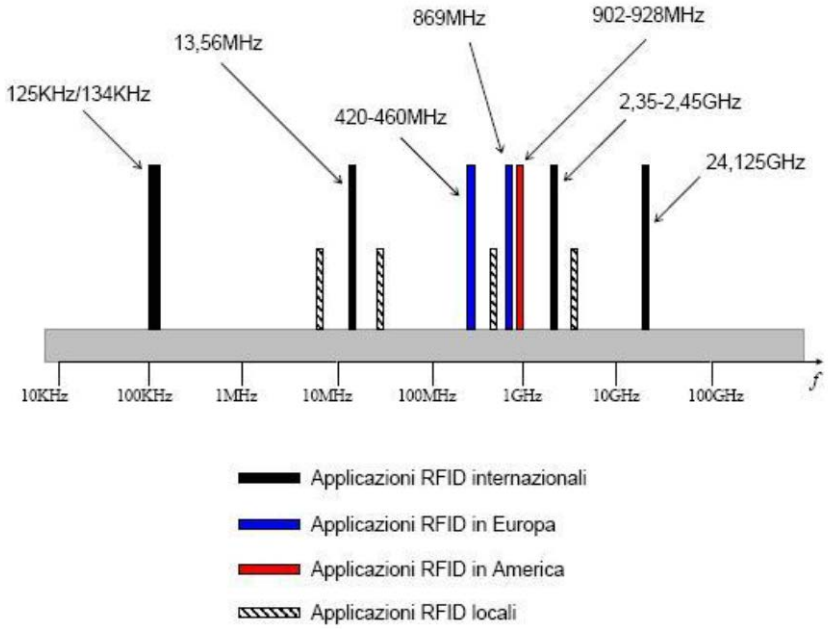

Figura 2.7 – Principali frequenze sfruttate per applicazioni RFID

Le porzioni di bande di frequenze più comunemente usate nella tecnologia RFID sono:

- LF-Low Frequency 125-145 kHz
- HF-High Frequency 13,56 MHz
- UHF Ultra High Frequency 865-930 Mhz
- MicroOnde:2,4 e 5,8 GHz

- **LF-Low Frequency 125-145 kHz**: questa è la frequenza utilizzata nella parte più bassa dello spettro RFID ed è stata storicamente la prima frequenza utilizzata per l'identificazione automatica e rimane ancora oggi significativamente presente sul mercato.

  Nel caso di tag passivi la distanza operativa (d) è all'incirca pari al diametro dell'antenna e varia da pochi cm al metro, al di là di questa portata la forza del campo si riduce molto rapidamente, in ragione di $1/d^3$, e l'energia captata dal tag per $1/d^6$.

  La frequenza di 125 kHz della portante è relativamente bassa e non consente velocità di trasmissione dei dati elevata.

  I tag a questa frequenza sono utilizzati principalmente nella tracciabilità animale per la bassissima influenza che l'acqua e i tessuti biologici hanno sulla trasmissione.

  Il trasponder protetto da un contenitore ceramico biocompatibile viene inserito nello stomaco dei bovini o, racchiuso in un contenitore di vetro, iniettato in zona sottocutanea negli animali di dimensioni più contenute.

  All'interno della banda LF in realtà sono due le frequenze operative più utilizzate:

  - 125,5 kHz nel settore automotive
  - 134,2 kHz tracciabilità animale

- **HF-High Frequency 13,56 MHz**: è la frequenza liberalizzata per uso RFID da tutti gli enti normatori mondiali e per questo ne ha fatto la frequenza più diffusa fino ai giorni nostri. Quasi unicamente di tipo passivo sono coperte da standard

ben assestati come l'ISO 14443 detto anche "proximity", che copre da 10 a 30 cm e l'ISO 15693 o "vicinity" che copre da 30 a 90 cm.

Sono diffusi nel settore del ticketing, del controllo accessi del personale, della tracciabilità dei bagagli nei sistemi aeroportuali e stanno per diventare comuni come sostitutivi intelligenti ed inviolabili delle schede magnetiche per le transazioni bancarie e come carte di credito. Le ultime generazioni di chip per questa tipologia di tag indirizzate all'identificazione automatica supportano come funzionalità quasi standard i meccanismi di anticollisione che consentono lettura/scrittura di più tag contemporaneamente.

A differenza dell'UHF e delle microonde il campo non è particolarmente influenzato dall'acqua e da tessuti biologici quali corpo umano. [6]

- **UHF-Ultra High Frequency 860-950 MHz**: l'evoluzione tecnologica dei semiconduttori che ha portato alla realizzazione di chip dal ridotto consumo energetico ha consentito la realizzazione di etichette RFID operanti a questa frequenza e con range di operazione decisamente più esteso di quanto non è consentito con LF e HF.

  A queste frequenze ci si scontra con problematiche più complesse rispetto a quelle riscontrabili con le frequenze inferiori: le strutture metalliche in prossimità dell'antenna possono riflettere le onde elettromagnetiche e, incontrandosi con l'onda diretta dell'antenna in opposizione di fase, possono generare degli spazi in cui il campo elettromagnetico risulta nullo; ne consegue che i tag in questa area risultano illeggibili.

  L'assorbimento da parte dell'acqua e di materiale organico delle onde elettromagnetiche si fa più consistente: l'efficienza di lettura in ambienti particolarmente umidi o con tag applicati a contenitori di liquidi può presentare problemi. [6]

  I tag operanti a queste frequenze possono essere di tipo passivo, semi-passivo o attivo.

- **Microonde 2,4-5,8 GHz**: a queste frequenze operano già le reti wireless come WLAN Bluetooth e tali frequenze sono ampiamente riconosciute a livello mondiale.

  Hanno caratteristiche molto simili all'UHF e grazie alla regola che l'antenna deve essere legata alla lunghezza d'onda consentono di ridurre la dimensione dell'antenna permettendo di conseguenza una ulteriore miniaturizzazione del tag.

La scelta della frequenza influisce ovviamente sul range di operatività del sistema, sulle interferenze con altri sistemi radio, sulla velocità di trasferimento dei dati e sulle dimensioni dell'antenna. I sistemi che usano frequenze più basse sono spesso basati su Tag passivi e sono in grado di trasmettere dati a distanze massime dell'ordine del metro e mezzo. Nei sistemi a frequenze più elevate, invece, oltre ai Tag passivi (con limitazioni a pochi metri delle distanze operative) sono diffusi Tag attivi che possiedono range operativi maggiori, sebbene limitati dai valori massimi di potenza irradiata stabiliti dagli organismi internazionali che regolano l'uso dello spettro radio.

	LF	HF	UHF media	UHF alta
Bande di frequenza	125 KHz & 134,2 KHz	13,56 MHz	865,6÷867,6; 868-869 MHz in EU 902÷928 MHz in USA 950 MHz in Japan	2.400÷2.483 MHz in EU 2.400÷2.500 MHz in USA
Standard ISO	18000-2	18000-3 mode 1/2 15693 14443 (typeA/B)	18000-6 type A/B/C	18000-4 mode 1/2
Standard EPCglobal	—	13,56 class 1	Class 0 Class 1 Class 1 Gen2	—
Accoppiamento	Induttivo (magnetico)	Induttivo (magnetico)	Elettromagnetico	Elettromagnetico
Alimentazione del TAG	Passivi Qualche TAG attivo	Nella stragrande maggioranza passivi	Passivi & attivi	Passivi & attivi
Distanza operativa	Tipica <0,5m Per TAG passivi si va dal 'contatto' fino a 70/80cm, dipendendo dalla potenza emessa dal lettore e dalla forma e dimensioni delle antenne. Nei sistemi con TAG attivi si possono raggiungere facilmente i 2m.	Tipica ≈1m Operatività fino a 1,2m in scrittura e 1,5m in lettura. La distanza operativa dipende dalla potenza emessa dal lettore e dalla forma delle antenne specialmente quella del tag: a superficie più grande corrisponde raggio d'azione più ampio	Tipica 2÷5 m, lettura TAG passivi in logistica. Distanza operativa influenzata dalle norme nazionali sulla potenza emessa: **In USA:** ≈4÷5m per Reader non regolamentati; ≈10m per apparati con licenza **In Europa:** ≈33cm per apparati limitati a 25 mW ≈1m per apparati limitati a 0,5 W ≈2m per apparati limitati a 2 W ≈ 100m se attivi	Tipica 1÷2 m Da 2 a 5m per tag passivi possono superare i 30-50m se attivi.
Capacità di Lettura/Scrittura	Disponibili TAG sia R/O che R/W	Disponibili sia del tipo R/O che R/W.	Generalmente R/W; disponibili R/O.	Disponibili sia R/O che R/W.
Capacità di Trasporto Dati	Da dispositivi R/O a bassa capacità (64bit) a dispositivi R/W con capacità fino a 2kbit	Generalmente di tipo R/W offrono capacità di memoria da 64 bit a decine di kbit. Spesso contengono 64 bit di codice unico identificativo scritto in produzione e quindi R/O.	Generalmente di tipo R/W offrono capacità di memoria che può variare da 64 bit fino ad alcuni kbit. Spesso contengono 64 bit di codice unico identificativo (UID) programmato durante la produzione e quindi R/O.	Sia passivi che attivi offrono capacità di memoria da 128 bit ad alcuni kbit (attivi).
Velocità trasferimento dati	Bassa velocità di trasferimento tipicamente da 0,2 a 1kbit/s.	Tipicamente nell'intorno di 25kbit/s.	Tipicamente nell'intorno di 28kbit/s ma esistono dispositivi quotati per 100kbit/s.	Tipici tra 100 e 250 kbit/s; max 1 Mbit/s. Dipendente dal dispositivo.
Letture Multiple	Disponibili sia per lettura singola che con meccanismi di anti-collisione.	Meccanismi anti-collisione per la lettura di circa 20/30 tag/s max; dipendendo dalle caratteristiche del sistema e dagli algoritmi impiegati.	Meccanismi anti-collisione per lettura di ~100 tag/s dipendendo da sistema ed algoritmi Per EPC Class1/Gen2, letture di 600 tag/s in EU e 1500 in USA.	Disponibili dispositivi per letture singole o multiple. 0,05 s per leggere alcune decine di TAG da 128 bit.
Formati	Disponibili in package e formati diversi: tipicamente incapsulati in vetro e/o ceramica per la tracciabilità animale (inserimento nello stomaco dei bovini) e in package plastici per usi industriali.	Vasta scelta, consente di coprire un gran numero di applicazioni. Il formato più diffuso è la cosiddetta "etichetta intelligente" che vede chip ed antenna integrate in una etichetta stampabile.	Vari formati per le diverse esigenze ambientali compresa l'applicabilità a unità metalliche. Uno dei formati più apprezzabili è la cosiddetta "etichetta intelligente" che vede chip ed antenna integrate in quella che appare una banale etichetta stampata.	Vari formati per le diverse esigenze ambientali compresa l'applicabilità a unità metalliche.
Costi	Dipendono in grande misura dal formato e dal tipo di applicazione che devono sostenere.	Meno costosi dei TAG LF Dipendono dal supporto fisico del TAG. Il costo minore è quello delle 'etichette intelligenti'; 40/60 €cent. legato anche alle quantità richieste.	Meno costosi dei TAG HF. Il costo minore è quello delle 'etichette intelligenti'; 20/40 €cent legato anche alle quantità richieste.	Essendo ancora un mercato di nicchia, quindi con volumi limitati, i costi sono tipicamente maggiori dell'HF ed UHF media.
Applicazioni	Identificazione animali, controllo accessi, identificazione veicoli immobilizer per auto, container, ecc.	Logistica (singoli oggetti) smart card biglietti smistamento bagagli	Logistica della filiera di fornitura (pallet) Logistica (singoli oggetti) Controllo bagagli	Logistica (asset tracking) Tool collection
Influenze ambientali	Propagazione agevole attraverso liquidi e tessuti organici. Sensibilità ad orientamento antenne	Praticamente Insensibili alla presenza di liquidi non conduttori e a tessuti organici.	Le prestazioni sono ridotte in presenza di metalli, liquidi, tessuti organici ed umidità.	Più sensibili dell'UHF media a metalli o liquidi
Caratteristiche generali	Antenne di grandi dimensioni costosi	Ottimi per applicazioni a distanza non grande e con limitato numero di TAG	Adatti per lunghe distanze o gruppi numerosi di TAG	Simili all'UHF media ma più rapidi in lettura
NOTE	Grande quantità prodotte a causa della tecnologia matura Tendono ad essere soppiantati dai TAG a frequenza maggiore	Attualmente i più disponibili ed i più diffusi perché di uso universale	Differenti frequenze e potenze nelle differenti regioni	Lavorano su banda molto affollata, convivendo con: ≡WiFI 802.11 B/G ≡Bluetooth ≡ZigBee

Tabella 2.2 - Confronto tra le caratteristiche delle diverse frequenze

2.3.3 Tipo di memoria

Una delle funzioni principali del chip è quella di trasportare le informazioni contenute in forma digitale in una porzione di memoria integrata nel medesimo componente.

Questa memoria oltre che essere caratterizzata dalla sua capacità ossia dalla quantità di bit che è in grado di contenere, si distingue in base alla tecnologia con cui è stata realizzata:

- **ROM**: acronimo di Read-only-Memory, ovvero memoria a sola lettura, prevede che le informazioni vengano definite al momento della produzione del dispositivo stesso.
- **PROM**: (Programmable-Read-Only-Memory) operano la tipica funzione Write-Once-Read-Many (WORM, di cui a volte prendono il nome), sono memorie di sola lettura. Le PROM contengono componenti elettronici il cui funzionamento è assimilabile a dei fusibili i quali possono essere bruciati secondo le esigenze per scrivere i dati richiesti. Sono scrivibili una sola volta e richiedono apparecchiature speciali per le operazioni di scrittura.
- **SRAM**: (Static Random Access Memory) consentono di mantenere le informazioni per un tempo infinito, sono molto veloci, consumano poco e quindi dissipano poca energia. La necessità di usare molti componenti, però, le rende molto costose e difficili da includere in un chip. Sono solitamente usate per le memorie cache, dove elevate velocità e ridotti consumi sono caratteristiche fondamentali. Vengono a volte impiegate nei tag attivi.
- **EEPROM** oppure **E2PROM**: Electrically Erasable Programmable Read- Only Memory. Hanno cicli limitati di lettura/scrittura, il che comporta un utilizzo dei tag limitato.

  La EEPROM (Electrically Erasable and Programmable ROM). A differenza di una semplice ROM è cancellabile e riscrivibile mediante opportune tensioni e correnti applicate ai MOSFET (i componenti base della memoria) che la compongono. Richiedono però voltaggi relativamente alti, hanno un consumo relativamente maggiore e tempi più lunghi per le operazioni di lettura/scrittura; richiedono anche una maggiore area di silicio sul chip e pertanto sono più costose. Le capacità di memoria EEPROM variano fino ad oltre 100 Kbyte e possono sopportare fino a 100.000 cicli di lettura/scrittura e possono conservare un dato scritto fino a 10 anni.
- **FRAM**: Ferroelectric RAM. Le FRAM costituiscono un notevole progresso rispetto alle EEPROM. Possono memorizzare dati per un lungo periodo di tempo, richiedono basso voltaggio ed offrono una grande resistenza ai cicli di

lettura/scrittura (numero illimitato di cicli lettura/scrittura) con alta velocità di scrittura. Tipicamente offrono velocità di trasferimento dati fino a 424 kbps; tempi rapidi di lettura e scrittura (meno di 200ns) e corrente estremamente bassa (alcuni μA); forniscono un'elevatissima affidabilità e tempi di conservazione dei dati superiori a 10 anni.

Tenendo conto della distinzione fatta è possibile un'altra classificazione delle etichette secondo il tipo di memoria; possiamo definirne tre tipi: Tag R/O, Tag R/W e Tag WORM.

- **Tag R/O: Read-Only**: utilizzando la tecnologia ROM, che ha il vantaggio di occupare a parità di informazioni memorizzate la minore area di silicio all'interno del chip e quindi di avere il minor costo possibile.
- **Tag R/W : Read-Write**: contrariamente ai tag precedenti questi sono realizzati con la tecnologia EEPROM ed offrono la possibilità di modificarne il contenuto.
  L'operazione di scrittura dei dati è molto laboriosa: è necessaria prima una operazione di cancellazione del blocco di memoria coinvolto dalla modifica dei dati e solo una volta che questa è avvenuta è possibile riscrivere i dati che devono essere conservati in quel particolare blocco. L'operazione di cancellazione di ogni singolo blocco può richiedere svariate decine di millisecondi e l'eventuale riscrittura di tutto il contenuto del tag può arrivare ad impiegare fino ad un secondo.
  Oltre al tempo di scrittura questo tipo di memoria richiede una quantità di energia decisamente superiore a quella necessaria durante la sola lettura. Nel caso di tag passivi questo si ripercuote sulla distanza operativa che ne risulta ridotta in modo significativo.
  Se nel caso della ROM l'informazione viene memorizzata in modo immodificabile all'interno del chip con un meccanismo che non subisce alterazioni con il tempo, nel caso della EEPROM l'informazione viene modificata iniettando od estraendo una certa quantità di cariche elettriche da una sorta di gabbia di contenimento.

Le operazioni di cancellazione e di scrittura causano un leggero deterioramento della struttura fisica della cella cosi le cariche in essa contenute tendono a sfuggire. Per questo motivo quando si parla di tag R/W vengono normalmente richiamanti due parametri :

- il numero di cicli di scrittura che possono essere supportati senza decadimento della funzionalità
- il tempo minimo garantito di mantenimento dei dati memorizzati, la tecnologia attuale consente di eseguire 100.000 cicli di scrittura e 10 anni di ritenzione dei dati.

- **Tag WORM**: Acronimo di Write Once Read Many, consentono la scrittura dei dati una sola volta dopo di che il meccanismo di scrittura viene bloccato ed il contenuto della memoria diviene immodificabile come nel caso dei tag R/O. L'unico vantaggio offerto da tale tecnologia è la programmabilità del codice identificativo che anziché essere forzato all'origine può essere deciso al momento della generazione dell'etichetta.

In passato i tag passivi erano principalmente di tipo read-only sia perché la fase di scrittura richiedeva la disponibilità di una quantità elevata di energia che si ricava con difficoltà dal segnale ricevuto, sia perché le memorie riscrivibili avevano un costo relativamente elevato. I tag passivi riscrivibili sono comunque in rapida diffusione. Per i tag attivi o semi passivi, oltre alla maggior quantità di memoria ed alla funzione di riscrivibilità della stessa, l'evoluzione tecnologica ha consentito di aggiungere, in alcuni casi, funzioni che superano di gran lunga la pura identificazione. Si ricordano ad esempio le funzioni di radiolocalizzazione (RTLS - Real Time Location System - posizione dell'oggetto che contiene l'RFID) o la misura di parametri ambientali attraverso particolari sensori (temperatura, movimento, ecc.). La differenza tra i due non è tanto nelle funzioni di memoria o negli eventuali sensori, quanto nel fatto che i tag attivi sono dei veri e propri apparati ricetrasmittenti mentre i tag semi passivi sfruttano la tecnologia di trasmissione dei tag passivi e pertanto necessitano di risorse di alimentazione modeste. Nei sistemi RFID i tag sono generalmente associati ad oggetti. Il protocollo di comunicazione tra

reader e tag è descritto in appositi standard. Le informazioni che il tag trasmette al reader sono contenute in una certa quantità di memoria che ogni tag contiene al suo interno. Le informazioni d'identificazione sono relative all'oggetto interrogato: tipicamente un numero di serie univoco, in qualche caso anche la copia dell'UPC (Universal Product Code) contenuto nel codice a barre ed altre informazioni (date di produzione, composizione dell'oggetto, ecc.).

Normalmente la quantità di dati contenuti in un RFID è piuttosto modesta (centinaia di byte o, al massimo qualche Kbyte). Ciò nonostante, la pervasività dell'uso dei tag e di opportune tecniche a radiofrequenza che consentono di interrogare e ricevere risposte da tutti i tag presenti in un particolare ambiente possono portare ad una "esplosione" della quantità di dati ottenibili [7].

2.3.4 Tipo di accoppiamento fisico

Abbiamo visto in precedenza la classificazione dei sistemi RFID in base alle frequenze di utilizzo, le quali si estendono dalla banda LF alle microonde. E' possibile però anche operare una distinzione di tali dispositivi in base al principio di funzionamento che verrà comunque approfondito nei paragrafi successivi.

- **Accoppiamento induttivo**

  I Tag induttivi LF seguono la norma dei trasformatori elettrici; il che richiede una particolare attenzione nell'orientamento delle antenne, pena una mancata lettura dei dati. Se impiegati in tecnologia passiva, sono caratterizzati da distanze di lettura comprese tra i 30cm e il metro, poiché il campo irradiato dalle antenne decresce molto velocemente. La scrittura delle etichette richiede un maggior quantitativo di energia e la massima lontananza consentita per questa operazione si riduce del 30÷50%. Le principali applicazioni sono l'automotive e il tracciamento animale. A tali frequenze la massima velocità di comunicazione è piuttosto bassa, circa 200 bit/sec, il che non consente l'impiego di sistemi per la lettura multipla di più Tag contemporaneamente. Il vantaggio dei sistemi RFID in LF è che la comunicazione non viene particolarmente disturbata da liquidi o tessuti organici.

La banda dei Tag induttivi HF è completamente liberalizzata e condivisa da tutti gli enti normatori mondiali; per questo motivo i Tag operanti a questa frequenza sono sicuramente i più diffusi. Si basano su standard mondiali condivisi, ad esempio l'ISO/IEC 14443, che ne semplificano l'interoperabilità e la progettazione. I costi delle etichette HF sono generalmente inferiori rispetto ai corrispettivi in ogni altra banda, ma dipendono fortemente dal supporto utilizzato. Sono disponibili differenti tipologie di packaging costruite con differenti materiali. Le dimensioni delle antenne ne determinano, a parità di potenza emessa dal dispositivo radiante del Reader, la sensibilità di lettura e la massima distanza operativa, che sono comunque comprese tra i 30cm e il 90cm per i dispositivi passivi. Come nel caso precedente, il corretto funzionamento è strettamente legato all'inclinazione dei componenti radianti. Rientrano in questa categoria le "Smart Card contactless", che ad oggi rappresentano il mercato più redditizio nel settore RFID. Le funzionalità offerte spaziano dalla capacità di memoria, che può andare dai pochi kilobyte e toccare oggi megabyte, alla disponibilità di algoritmi crittografici per effettuare transazioni sicure. Diffuse nel settore del ticketing, del controllo accessi del personale, della tracciabilità dei bagagli nei sistemi aeroportuali, stanno per diventare comuni come sostitutivi intelligenti ed inviolabili delle schede magnetiche per le transazioni bancarie (Bancomat) e come carte di credito.

- **Accoppiamento elettromagnetico**

  I Tag UHF che lavorano alle frequenze medie (860÷950MHz) ed alte (2,4GHz) hanno un chip a basso consumo energetico, nonostante consentano profondità di lettura maggiori rispetto alle precedenti tecnologie. L'accoppiamento Tag-Reader si svolge in maniera elettromagnetica, come avviene solitamente nei sistemi di radiocomunicazione.

  Un limite di queste tecnologie è l'incompatibilità delle frequenze. Inoltre, il fattore ambientale crea più problemi, poiché in prossimità di superfici metalliche, le onde magnetiche possono essere riflesse, ed in presenza di liquidi e tessuti organici assorbono energia con l'aumentare della frequenza.

È da sottolineare però la velocità di lettura, e la facoltà di rilevare molte informazioni in pochissimo tempo.

Nella tabella seguente viene mostrato un confronto per quanto riguarda il funzionamento dei TAG RFID, le loro problematiche e le loro prestazioni alle differenti frequenze operative: vengono evidenziate la sensibilità e l'orientamento delle antenne, la velocità di trasferimento dei dati fra TAG e Reader, la capacità di lettura di questi transponder in prossimità di ostacoli (ad esempio liquidi e metalli), il tradeoff fra le dimensioni dei TAG passivi e il loro assorbimento di energia attraverso l'adattamento di impedenza, i vantaggi e gli svantaggi per quanto riguarda le basse e le alte frequenze.

LF	HF	UHF media	UHF alta
Accoppiamento induttivo/campo M		Accoppiamento con campo EM (backscatter)	
Sensibilità ad orientamento ortogonale delle antenne			
Molto sensibili (mancate letture)		Sensibili (attenuazione; possibili mancate letture)	Poco sensibili
Velocità di trasferimento dei dati (TAG — Reader) Minore ◄——► Maggiore			
Velocità di lettura di gruppi di TAG Minore ◄——► Maggiore			
Capacità di lettura di TAG in prossimità di metalli o superfici bagnate Migliore ◄——► Peggiore			
Assorbimento da parte di liquidi,ovvero Capacità di lettura di TAG all'interno degli animali o coperti da acqua o ghiaccio Migliore ◄——► Peggiore			
Dimensione dei TAG passivi Dipende dall'energia captabile ◄——► Grande ◄ Dipende da frequenza e tipo di antenna ——► Piccola			
Assorbimento di energia Minore ◄——► Maggiore			

Tabella 2.3 - Confronto delle tecnologie RFID

2.4 PRINCIPI DI FUNZIONAMENTO DEI SISTEMI RFID

2.4.1 Equazioni di Maxwell

Per studiare i fenomeni fisici che sono legati alla trasmissione dei sistemi RFID è opportuno ricorrere alla teoria dei campi elettromagnetici, partendo dalle equazioni di Maxwell. Le equazioni di Maxwell mostrano come, in generale, sia possibile generare un campo elettromagnetico utilizzando delle sorgenti specifiche quali cariche e correnti.

Tali equazioni mostrano che per ottenere un campo di radiazione (elettromagnetico) è necessario che le sorgenti siano tempo varianti.

Consideriamo in particolare le due equazioni integrali inerenti le circuitazioni di campo magnetico ed elettrico:

La legge di Ampère-Maxwell:

$$\oint_c \mathbf{H}(\boldsymbol{r},t)\cdot d\boldsymbol{l} = \int_s \boldsymbol{J}_e(\boldsymbol{r},t)\cdot \boldsymbol{n}\, dS + \frac{d\phi_D}{dt} \tag{2.1}$$

Dove:

$$\phi_D = \int_c \boldsymbol{D}(\boldsymbol{r},t)\cdot \boldsymbol{n}\, dS \tag{2.2}$$

In forma differenziale:

$$\nabla \times \boldsymbol{H}(\boldsymbol{r},t) = \boldsymbol{J}_e(\boldsymbol{r},t) + \frac{\partial \boldsymbol{D}(\boldsymbol{r},t)}{\partial t} \tag{2.3}$$

Osserviamo come tale legge esprima il fatto che una corrente elettrica possa generare dei campi magnetici. Lo stesso effetto può essere osservato, in regime tempo-variante, se si considera la variazione di flusso del vettore **D** (corrente di spostamento).

La legge di Faraday:

$$\oint_c \boldsymbol{E}(\boldsymbol{r},t)\cdot d\boldsymbol{l} = -\frac{d\phi_B}{dt} \tag{2.4}$$

Dove:

$$\phi_B = \int_s \boldsymbol{B}(\boldsymbol{r},t)\cdot \boldsymbol{n}\, dS \tag{2.5}$$

In forma differenziale:

$$\nabla \times \boldsymbol{E}(\boldsymbol{r},t) = -\frac{\partial \boldsymbol{B}(\boldsymbol{r},t)}{\partial t} \tag{2.6}$$

I campi magnetici che variano nel tempo generano campi elettrici indotti.

Un campo elettrico può essere generato oltre che dalla distribuzione di carica elettrica, anche da un campo magnetico variabile nel tempo, in modo analogo un campo magnetico può essere generato, oltre che da una distribuzione di corrente elettrica anche da un campo elettrico variabile nel tempo. Quando si è in regime variabile nel tempo, campo elettrico e magnetico divengono l'uno la sorgente dell'altro.

Combinando insieme le equazioni di Maxwell si può ricavare l'equazione delle onde, che, in una regione priva di sorgenti, assume la forma:

$$\nabla^2 \mathbf{a}(r,t) - \varepsilon\mu \frac{\partial^2 \mathbf{a}(r,t)}{\partial t^2} = 0 \tag{2.7}$$

Tale equazione vale sia per **E** che per **H** sostituendo tali campi ad **a**.

Se la propagazione avviene in spazio libero il campo elettromagnetico si comporta localmente come un'onda piana, globalmente il campo assume l'andamento di un onda sferica, la propagazione avviene dal finito verso l'infinito, e in tale zona le ampiezze di campo elettrico e magnetico sono legate dalla relazione $|E| = \zeta |H|$ dove $\zeta = 377\Omega$ (o 120Π) è detta impedenza caratteristica del mezzo o impedenza d'onda.

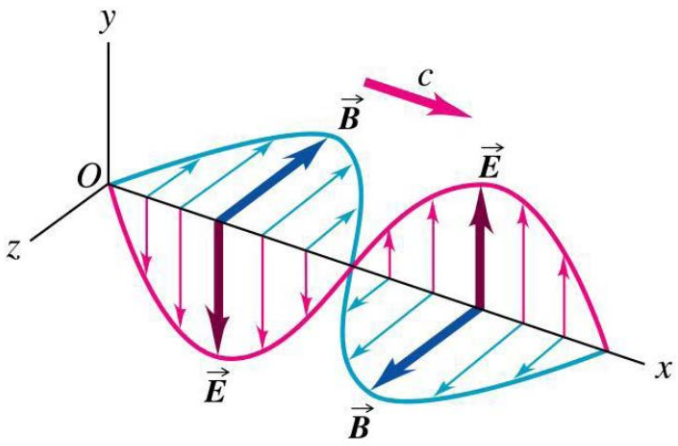

Figura 2.8 – Rappresentazione grafica della propagazione di un'onda elettromagnetica

2.4.2 Le antenne

Le antenne dei tag e dei reader, svolgono un ruolo di grande rilevanza nei si sistemi RFID passivi.

Infatti esse sono elementi in grado di irradiare o captare a seconda che siano usate in trasmissione o in ricezione.

La radiazione elettromagnetica di una sorgente come per esempio quella emessa da un'antenna non assume un comportamento omogeneo in tutto lo spazio, è necessario definire matematicamente il passaggio tra la zona di campo vicino e quella di campo lontano, mediante l'utilizzo delle seguenti formule:

1. $r > 10D$ (2.8)

2. $r > \frac{2D^2}{\lambda}$ (2.9)

3. $r > 10\lambda$ (2.10)

Dove D è il diametro della sfera di raggio minimo che racchiude l'antenna ed r è la distanza dalla sorgente.

Se tutte e tre le condizioni sono soddisfatte si parla di zona di far-field o campo lontano, altrimenti nel caso in cui si siano verificate le condizioni 1 e 3 ma non la 2 ci troviamo nella regione di near-field radiativo. Altrimenti si parla di near-field o campo vicino.

- **Campo vicino:** zona in cui la distribuzione angolare di campo varia al variare della distanza dalla sorgente. Non è assolutamente possibile assumere che il campo elettromagnetico sia descritto dalle condizioni di radiazione **E** ed **H** non sono perpendicolari, le relazioni di fase tra i campi sono fortemente variabili da punto a punto, i moduli di campo elettrico e magnetico non sono legati da una relazione semplice e nota.

La componente di energia reattiva prevale su quella attiva, se in vicinanza dalla sorgente:

$|\mathbf{E}| > \zeta\,|\mathbf{H}|$ la sorgente è di tipo elettrico (dipolo elementare)

$|\mathbf{E}| < \zeta\,|\mathbf{H}|$ la sorgente è di tipo magnetico (spira elementare)

Lo studio delle antenne in campo vicino è estremamente difficoltoso ed è praticamente impossibile.

- **Campo vicino di radiazione:** il comportamento del campo comincia a diventare quello richiesto dalle condizioni di radiazione, il fronte d'onda tutta via, non è perfettamente formato e la distribuzione angolare del campo elettromagnetico dipende ancora dalla distanza della sorgente.

- **Campo lontano:** zona in cui la distribuzione angolare di campo non dipende quasi più dalla distanza della sorgente. Il comportamento tende ad essere quello espresso dalle condizioni di radiazione, inoltre il fronte d'onda è perfettamente formato. In far-field il campo elettrico e il campo magnetico sono perpendicolari tra di loro ed alla direzione di propagazione.

2.4.3 Orientamento e polarizzazione

Da tener conto è l'orientamento e la polarizzazione del tag, fattori che incidono significativamente sulle prestazioni.

Gli apparati RFID che sfruttano l'accoppiamento induttivo, quindi funzionanti in campo vicino, sono particolarmente sensibili all'orientamento delle antenne che in questo caso sono assimilabili agli avvolgimenti primario e secondario di un trasformatore elettrico.

Gli apparati RFID che sfruttano invece l'accoppiamento elettromagnetico, quindi funzionanti in campo lontano, sia passivi che attivi, devono tener conto di due caratteristiche principali delle antenne sia del reader che del tag:

- **Diagramma di radiazione:** il diagramma di radiazione è una funzione matematica o una rappresentazione grafica che evidenzia le proprietà di radiazione delle antenne. Quelli più comuni sono riferiti alle ampiezze dei campi, all'intensità di radiazione o alla densità di potenza ed in particolare rappresentano queste grandezze normalizzate al loro valore massimo. Tali grafici sono spesso tridimensionali, in alcuni casi invece si preferisce mostrare sezioni lungo i piani coordinati o lungo piani di particolare interesse. E' spesso utilizzata la rappresentazione in forma polare.

  Sul diagramma di radiazione, è possibile individuare uno o più lobi di radiazione ovvero il profilo tridimensionale in cui si concentra il campo elettromagnetico emesso dall'antenna. Con un opportuno dimensionamento degli elementi dell'antenna si può ottenere un lobo di emissione più concentrato in un area limitata, questa capacità direzionale viene spesso sfruttata per restringere opportunamente il campo d'azione dell'antenna.

  La maggior parte delle antenne godono della proprietà di reciprocità, ovvero hanno lo stesso diagramma di radiazione sia quando irradiano sia quando ricevono, tale proprietà si applica anche alla polarizzazione.

- **Polarizzazione del campo elettromagnetico:** per polarizzazione s'intende l'orientamento del campo elettromagnetico emesso.

  Si ha polarizzazione lineare quando la direzione dei due vettori rimane inalterata e solo l'intensità e il verso cambiano secondo un andamento sinusoidale.

  Si ha polarizzazione circolare quando l'antenna è in grado di generare un campo in cui i vettori **E** ed **H** hanno modulo uguale e ruotano intorno all'asse normale ai due vettori.

  Si ha polarizzazione ellittica quando i due vettori **E** ed **H** ruotano attorno all'asse che indica la direzione di propagazione (come accade per la polarizzazione circolare) ma il loro modulo è diverso. Anche l'antenna del tag, generalmente a polarizzazione lineare, ha un suo orientamento il quale può condizionare l'accoppiamento con il campo incidente: a orientamento coerente corrisponde il massimo trasferimento di energia mentre con orientamento ortogonale si ha un accoppiamento trascurabile.

Il problema della polarizzazione nei sistemi RFID può essere superato anche con vari accorgimenti nella realizzazione dell'antenne del reader:

E' possibile costruire antenne con polarizzazione circolare. Questo consente al tag di trovare sempre un momento in cui l'orientamento dell'onda incidente sia favorevole al massimo accoppiamento; tale tecnica è utile per l'accoppiamento in alta frequenza (UHF).

Un'altra tecnica sfruttata in HF consiste nel posizionare antenne in diverse locazioni ovvero orientate secondo i tre assi ortogonali tra loro (X,Y,Z) creando cosi veri e propri portali.

In genere, per qualsiasi tipo di frequenza, le scelte adottate sono le seguenti: l'uso di due antenne a 90fl fuori fase l'una con l'altra o l'impiego di un tunnel di reader 3D.

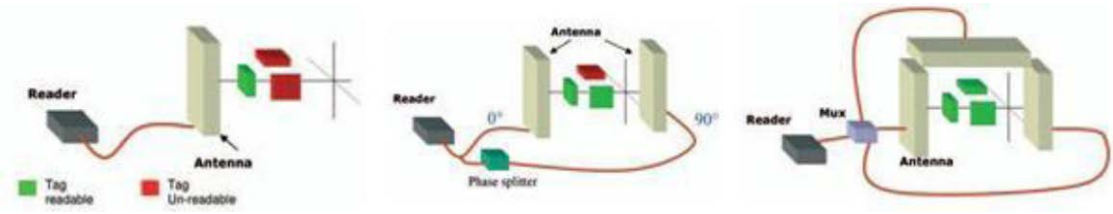

Figura 2.9 – Rappresentazione grafica di lettura con e senza tunnel di reader 3D

Se la polarizzazione lineare offre normalmente un raggio di azione più esteso la polarizzazione circolare rende il sistema più insensibile all'orientamento del tag ed una migliore distribuzione del campo elettromagnetico emesso, inoltre offre una migliore riflessione e superamento degli ostacoli.

2.4.4 Cenni di radiofrequenza

Il colloquio tra tag e lettore avviene per mezzo di un accoppiamento, definito per semplicità a radiofrequenza, ossia una propagazione delle onde elettromagnetiche. In realtà

nel caso del RFID i fenomeni fisici che consentono lo scambio di energia e di informazioni tra tag e lettore sono diversi a seconda della radiofrequenza operativa a cui si

opera. Per entrare nel problema si deve fare riferimento a due grandezze scalari, la frequenza "*f*" e la lunghezza d'onda "λ" che sono tra loro legate dalla relazione:

$$v = f \cdot \lambda \tag{2.11}$$

dove v rappresenta la velocità di propagazione delle onde elettromagnetiche nel mezzo trasmissivo. Per esempio nello spazio libero tale velocità è quella della luce: 300.000.000 metri al secondo. Facendo un rapido calcolo alle frequenze più usate dall'RFID :

a 125 KHz → 2.400 metri
a 13.56 MHz → 22 metri
a 868 MHz → 0,35 metri
a 2.45 GHz → 0,12 metri

E' semplice notare come a frequenze maggiori corrispondono lunghezze d'onda più piccole.

Utilizzando un'antenna ad esempio a dipolo per emettere un'onda elettromagnetica nello spazio con una radiazione ottimale, ossia per distanze rilevanti, occorre utilizzare una antenna che deve essere correlata alla lunghezza d'onda del segnale che si vuole trasmettere cioè al meglio pari almeno a $\frac{\lambda}{2}$ o ad un multiplo intero della lunghezza d'onda.

Nel caso di frequenze basse comprese nell'intervallo le LF (low frequency) 125 kHz e HF (high frequency) a 13.56 MHz, sarebbe impensabile realizzare antenne di grandi dimensioni per la trasmissione in far-field.

A queste frequenze si devono costruire antenne più piccole del valore della lunghezza d'onda, antenne che non sono in grado di generare un'onda elettromagnetica ma che sono comunque capaci di generare un campo o elettrico o magnetico a seconda della geometria d'antenna (es. dipolo o spira), che però date le dimensioni ridotte non è in grado di propagarsi liberamente a distanza, ma rimane strettamente legato alla prossimità

dell'antenna (campo vicino). Infatti le proprietà radiative e l'impedenza di una antenna dipendono dalla sua forma, dimensione (in termini di lunghezza d'onda) e dal materiale con cui è stata costruita. Nel caso di dipoli elementari, che sono antenne filiformi rettilinee di lunghezza molto inferiore a λ e percorse da corrente pressoché uniforme, il campo elettromagnetico prodotto in prossimità di tale antenna è prevalente di tipo elettrico (questa antenna ha un impedenza di tipo capacitivo, ed il campo magnetico non ha addendi che avanzano come $1/r^3$ al contrario di ciò accade per il campo elettrico), per questa ragione si dice che i dipoli elementari sono sorgenti di campo elettrico o sorgenti ad alta impedenza. Nel caso di spire elementari si tratta di antenne filiformi a forma circolare aventi un raggio di lunghezza molto inferiore a λ e il campo elettromagnetico prodotto in prossimità di tale antenna è prevalente di tipo magnetico (questa antenna ha un impedenza di tipo induttivo e il campo elettrico non ha addendi che vanno come $1/ r^3$ mentre ciò accade per il campo magnetico), per questa ragione si dice che le spire elementari sono sorgenti di campo magnetico o sorgenti a bassa impedenza. Quindi alle basse frequenza LF i trasponder sono accoppiati induttivamente nella maggior parte dei casi o elettricamente in rari casi. Le antenne utilizzate negli RFID induttivi non sono dei semplici avvolgimenti in aria, perché, per ottenere un segnale apprezzabile, occorrerebbero delle antenne a spira con un numero di avvolgimenti molto alto e con un diametro molto elevato. Antenne di questo tipo esistono e sono chiamate antenne a quadro o telaio , ma è possibile ridurre notevolmente la loro dimensione mediante l'inserimento al centro della spira di un materiale ferromagnetico, generalmente ferrite, il quale serve per convogliare più flusso magnetico all'interno dell'avvolgimento. Alle frequenze superiori UHF e microonde è valido l'uso del fenomeno propagativi delle onde radio (elettromagnetico).

Gli RFID passivi o attivi possono operare o ad accoppiamento induttivo o elettromagnetico [8].

2.4.5 RFID ad accoppiamento induttivo

L'accoppiamento utilizzato nei tag a bassa frequenza come le LF e HF è nella maggior parte dei casi di tipo magnetico (e raramente elettrico) in quanto è d'obbligo lavorare in

condizioni di campo vicino. Questi sistemi si basano sul fatto che, per distanze piccole rispetto alla lunghezza dell'onda emessa dall'antenna, prevalgono gli effetti della corrente indotta dal campo magnetico che varia periodicamente nel tempo; il principio fisico che ne permette il funzionamento è lo stesso dei trasformatori in aria libera. Il campo magnetico generato dall'antenna del lettore, che svolge il compito di avvolgimento primario, si accoppia induttivamente con l'avvolgimento del secondario, che è rappresentato dall'antenna del tag.

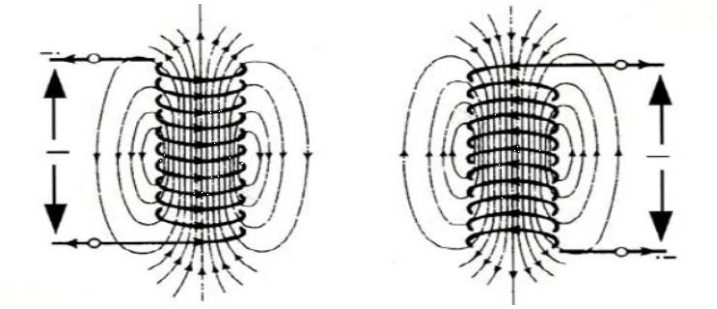

Figura 2.10 – Induttori accoppiati

Questo tipo di accoppiamento consente sia il trasferimento di energia verso il tag (come avviene nei trasformatori) sia lo scambio bidirezionale dei dati. A tali frequenze l'antenna del tag è rappresentata da un avvolgimento generalmente di rame. Essendo il campo magnetico un campo vettoriale, caratterizzato quindi da intensità direzione e verso, l'accoppiamento lettore – tag è dipendente dall'orientamento di quest'ultimo. Per ottenere accoppiamento massimo le spire dell'antenna del tag devono essere posizionate in modo tale da tagliare perpendicolarmente le linee di flusso del campo magnetico del lettore. Ne consegue che non è solo la distanza dell'antenna a condizionare l'attivazione o meno del tag, ma anche la posizione relativa; infatti tag molto vicini ma non allineati non captano sufficiente energia per attivarsi. Ciò vale anche per etichette HF (13.56 MHz). Esiste quindi una porzione di spazio, nell'intorno dell'antenna, in cui, a seconda dell'orientamento del tag, questo può ricevere o meno sufficiente energia dal campo che ne consenta l'attivazione. Questa porzione di spazio viene definita "lobo di emissione" dell'antenna; tale lobo dipende da diversi parametri tra cui la potenza emessa dall'antenna, dalla sensibilità del tag e dalla sua forma. Nel caso dei tag passivi la distanza operativa è all'incirca pari al diametro dell'antenna del lettore e varia dai 10 cm al metro; al di là di

questa zona il campo decade come $1/r^3$ e l'energia captata del tag $1/r^6$. Anche per questo motivo la distanza di scrittura, operazione che richiede un maggiore consumo di energia da parte del chip, e di norma più bassa di quella di lettura.

Comunicazione nei tag operanti alle frequenze LF ed HF

Questi tag usano l'accoppiamento induttivo tra antenne a spire accoppiate come un trasformatore elettrico (l'antenna del reader e quella del tag) per rifornire il tag di energia e trasmettere. Le due antenne sono, dal punto di vista elettrico, un circuito accordato LC (induttanza - condensatore). Alla frequenza di risonanza viene quindi massimizzato il trasferimento di energia tra reader e tag. A parità di altri fattori, un numero di spire minore genera una frequenza di risonanza maggiore (ad esempio per la frequenza di 13,56 MHz vengono tipicamente usate da 3 a 5 spire nelle antenne). La comunicazione tra reader e tag avviene modulando in ampiezza il campo magnetico generato dall'antenna del reader con il segnale digitale in banda base che deve essere trasmesso. Il circuito di ricezione del tag riconosce il campo modulato e decodifica, da questo, l'informazione trasmessa dal reader, è da tener presente che mentre il reader ha potenza per modulare e trasmettere il proprio campo il tag non ne ha.

La comunicazione inversa dal tag al reader si realizza quindi tramite accoppiamento induttivo, come in un trasformatore in cui l'avvolgimento secondario (antenna del tag) varia il proprio carico (modula) ed il risultato (modulato) è visto nell'avvolgimento primario (antenna del reader). Il chip del tag realizza questo effetto cambiando l'impedenza della propria antenna coerentemente con un segnale modulante ricavato dalla lettura dei dati contenuti nella propria memoria.

In effetti tutto ciò è più complesso in quanto se il segnale di risposta (modulato) ha la stessa frequenza del segnale di interrogazione del reader, sarà mascherato da questo e non facilmente rilevato a causa del debole accoppiamento tra reader e tag.

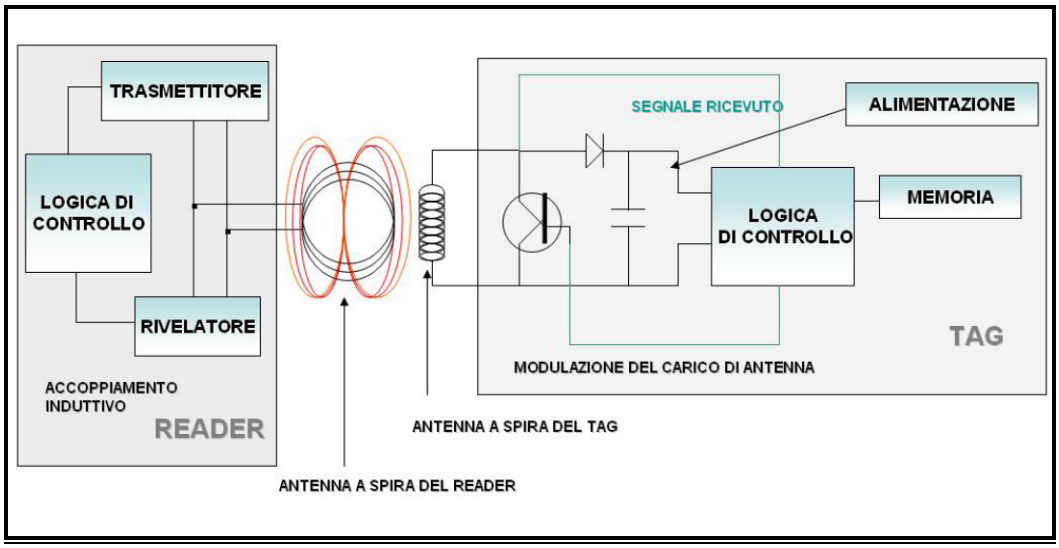

Figura 2.11 – Sistema TAG-Reader ad accoppiamento induttivo

In sintesi la sequenza di eventi nell'interrogazione del tag da parte del reader è la seguente:

1. La logica di controllo del reader invia i dati (dell'interrogazione) al trasmettitore che genera il segnale per l'antenna a spire.

2. La corrente nell'antenna del reader induce un campo magnetico pulsante che si concatena con l'antenna a spire del tag.

3. La corrente indotta viene rettificata ed accumulata in un condensatore, fornendo alimentazione alla logica di controllo del tag.

4. La logica di controllo del tag (alimentata) si attiva e decodifica il segnale di interrogazione del reader.

5. La logica di controllo del tag legge i dati nella sua memoria e, con questi, modula l'impedenza di antenna del tag medesimo.

6. Il reader percepisce (tramite il rivelatore) le variazioni d'impedenza dell'antenna del tag (essendo le spire del tag e del reader accoppiate come gli avvolgimenti di un trasformatore) e trasmette i dati ricevuti alla sua logica di controllo.

In dettaglio possiamo dire che una piccola parte del campo emesso penetra l'avvolgimento dell'antenna del tag che si trova ad una certa distanza dal reader.

Una tensione è generata nella bobina antenna del transponder dall'induttanza L_T. Questa tensione V_T è raddrizzata ed è impiegata come potenza di alimentazione per il data-

carrying device (microchip). Un condensatore C_R è connesso con la bobina antenna del reader, la cui capacità è scelta in modo da costituire con l'induttanza della bobina dell'antenna un circuito risonante parallelo con una frequenza di risonanza F_0 che corrisponde alla frequenza di trasmissione del reader .

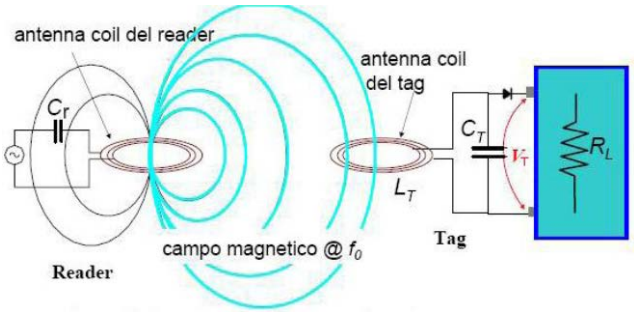

Figura 2.12 – Schema circuitale reader tag assimilabili a due circuiti RLC

L'avvolgimento dell'antenna del transponder e il condensatore C_T formano a loro volta un circuito risonante accordato sulla frequenza F_0 di trasmissione del reader.

$$F_0 = \frac{1}{2\pi\sqrt{L_T\, C_T}} \tag{2.12}$$

Un' analisi più accurata può essere svolta osservando la figura seguente:

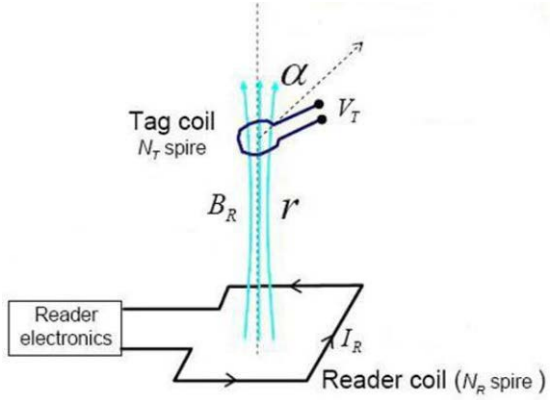

Figura 2.13 – Accoppiamento tra le spire del reader e tag

La densità del flusso magnetico generato dal reader B_R , fonte di alimentazione del tag è data dalla formula seguente nella quale viene messo in evidenza come tale densità dipenda

dalla corrente variabile I_R che percorre l'avvolgimento dell'antenna, dal numero di spire N_R della stessa, dal raggio a_R e dalla geometria con cui è realizzata e infine dalla distanza r tra essa e l'antenna del tag.

$$B_R(r) = \frac{\mu_0 (I_R N_R) a_R^2}{2\sqrt{(a_R^2 + r^2)^3}} \propto \frac{1}{r^3} \tag{2.13}$$

Supponendo la corrente I_R :

$$I_R = I_0 \sin \omega t \tag{2.14}$$

La tensione ai capi del tag sintonizzato è data da:

$$V_T = - N_T \frac{d}{dt} \iint B_R \, ds \tag{2.15}$$

Ovvero:

$$V_T = -K \frac{(I_R N_R) N_T \cos \alpha}{2\sqrt{(a_R^2 + r^2)^3}} Q_T \tag{2.16}$$

Dove:

$$K = \frac{1}{2} \mu_0 \, a_R^2 \omega \, S_T \sin \omega t \tag{2.17}$$

S_T rappresenta la superficie utile attraversata dal campo magnetico data dall'antenna del tag.

V_T può essere vista per semplicità del tipo: $V_T = V_0 \sin \omega t$

Il tag si attiva quando la tensione V_T raddrizzata, ed opportunamente stabilizzata, supera la tensione di soglia del chip, normalmente dell'ordine di qualche volt.

V_T (e quindi la distanza di lettura) aumenta quando:

- Aumenta il numero di spire nell'antenna del tag N_T o la frequenza ($\omega = 2 \pi f$)
- Angolo di accoppiamento $\alpha = 0$ (linee di flusso concatenate)
- Fattore di merito Q_T elevato (compatibilmente con la banda richiesta)

In conclusione l'efficienza del trasferimento di potenza tra reader e transponder è proporzionale alla frequenza operativa *f*, al numero di avvolgimenti *N*, alla superficie della bobina del transponder S_T, all'angolo relativo dei due avvolgimenti α e alla distanza tra le due bobine r.

In realtà l'accoppiamento di tipo trasformatore tra il primario, reader, e il secondario, transponder, è vero quando la distanza tra le due bobine r non supera la distanza tale da fuoriuscire dalla zona di campo vicino dell' antenna trasmittente (campo magnetico).

2.4.6 RFID ad accoppiamento elettromagnetico

Per ottenere le condizioni di campo lontano alle distanze operative e quindi realizzare una vera e propria comunicazione radio vengono impiegate le bande di frequenza con minore lunghezza d'onda come le UHF e SHF. I sistemi RFID che lavorano nelle frequenze UHF nell'intorno di 900Mhz e micro-onde, da 2,4 GHz in su fanno uso convenzionale della propagazione delle onde elettromagnetiche per comunicare dati e comandi e, nel caso di tag passivi, anche per fornire energia ai trasponder RFID. In questi sistemi l'antenna del lettore emette un campo elettromagnetico che si propaga, semplificando, come un fronte sferico. Questo campo assume la configurazione di un'onda elettromagnetica di forma sinusoidale con una certa frequenza, rappresentabile da due vettori **H** (campo magnetico) ed **E** (campo elettrico) tra loro ortogonali. I tag che vengono investiti da quest'onda elettromagnetica possono raccogliere parte dell' energia per lavorare. La quantità di energia disponibile in ogni punto del campo è legata alla distanza "r" dalla sua sorgente secondo l'andamento $1/ r^2$, ovvero in modo inversamente proporzionale al quadrato della distanza.

Comunicazione nei tag operanti in UHF e microonde

L'effetto Scattering: il fenomeno di scattering avviene quando un'onda elettromagnetica incide su delle irregolarità del mezzo in cui si propaga, e di conseguenza viene dispersa in modo casuale.

In sistemi come il radar o gli RFID passivi o semi-passivi sfruttano questo fenomeno, infatti un trasmettitore invia un'onda elettromagnetica ed un ricevitore rileva lo scattering generato da un oggetto sul quale l'onda incide.

Questo avviene quando un'onda elettromagnetica incide su un oggetto ed induce cariche oscillanti e correnti nell'oggetto e sulla sua superficie , di conseguenza, si genera un nuovo campo elettromagnetico.

Quando il trasmettitore ed il ricevitore sono un tutt'uno lo scattering viene chiamato backscatter. I sistemi RFID modulano il backscatter attraverso la variazione dell'impedenza della propria antenna, ciò consente la comunicazione con il reader.

I tag passivi che operano in UHF o a frequenze maggiori, usano tecniche a modulazione di ampiezza simili a quelle dei tag che operano a frequenza più bassa e ricevono ugualmente la loro potenza dal campo del reader, la differenza consiste nel modo in cui l'energia è trasferita e nell'antenna.

Come si è detto, il trasferimento di energia a queste frequenze avviene in condizioni di "campo lontano", ovvero a distanze a cui l'accoppiamento induttivo non è più l'effetto prevalente, si opera quindi con antenne a dipolo che catturano il campo elettromagnetico come nei tradizionali sistemi di radiocomunicazione.

Quando l'onda elettromagnetica emessa dal reader incide sull'antenna del tag una parte dell'energia viene assorbita per fornire potenza al tag,una piccola parte, invece, viene riflessa all'indietro verso il reader come backscatter.

L'energia ricavata dal campo elettromagnetico assorbito dall'antenna del tag è dell'ordine dei 200 μW, sicuramente troppo bassa per alimentare un trasmettitore. Per la comunicazione tra tag e reader, quindi, si sfrutta la modulazione dell'effetto backscatter.

Anche in questo caso la modulazione del backscatter è ottenuta tramite variazione d'impedenza dell'antenna del tag durante la trasmissione del segnale da parte del reader.

Il compito del reader è quello di captare le conseguenti variazioni nel segnale riflesso.

L'uso della tecnica della modulazione del backscatter in campo lontano, introduce problemi differenti da quelli che si manifestano nei sistemi a frequenza più bassa.

Uno dei maggiori problemi è dovuto al fatto che il campo emesso dal reader, non è riflesso solo dall'antenna del tag ma anche da tutti gli oggetti circostanti con dimensioni paragonabili alla lunghezza d'onda adoperata.

Questi campi riflessi si sovrappongono al campo principale emesso dal reader e possono provocarne lo smorzamento o perfino la cancellazione.

I tag passivi a frequenze elevate (UHF, SHF) inoltre, operano a distanze maggiori di quelli ad accoppiamento induttivo, con antenne più semplici e di dimensioni ridotte.

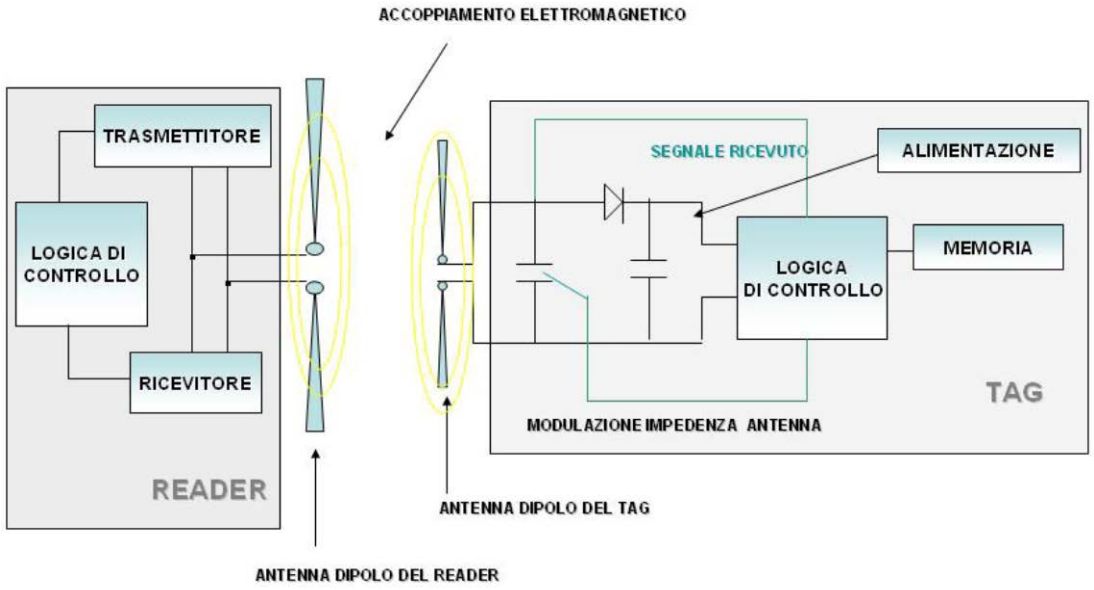

Figura 2.14 – Sistema TAG-Reader ad accoppiamento elettromagnetico

In conclusione, la sequenza di eventi nell'interrogazione in backscatter del tag da parte del reader può essere riassunta nei seguenti punti :

1. La logica di controllo del reader invia i dati (dell'interrogazione) al trasmettitore che genera il segnale RF per l'antenna a dipolo.

2. Il segnale si propaga nello spazio (campo lontano) ed è ricevuto dall'antenna a dipolo del tag.

3. L'energia del segnale ricevuto viene rettificata ed accumulata in un condensatore, fornendo alimentazione alla logica di controllo del tag.

4. La logica di controllo del tag (alimentata) si attiva e decodifica il segnale di interrogazione del reader.
5. La logica di controllo del tag legge i dati nella sua memoria e, con questi, modula l'impedenza di antenna del tag medesimo e, di conseguenza, modula il Backscatter.
6. Il reader riceve il segnale di Backscatter, lo decodifica tramite il ricevitore e trasmette i dati ricevuti alla logica di controllo.

Volendo fare uno studio energetico di questa situazione consideriamo che in un emettitore sferico, chiamato emettitore isotropico, l'energia è irradiata uniformemente in tutte le direzioni. [8]
Ad una distanza r la densità della radiazione S è calcolata come il rapporto tra la potenza trasmessa P_{EIRP} (EIRP sta per *effective isotropic radiated power*) e la superficie della sfera.

$$S = \frac{P_{EIRP}}{4\pi r^2} \tag{2.18}$$

Una ridotta parte di energia trasmessa viene riflessa e torna indietro all'antenna del trasmettitore.
E' la tecnica impiegata nella tecnologia radar che sfrutta questa riflessione per misurare la distanza e ricavare la posizione dei riflettori.
La regione di funzionamento tra reader e tag è quella per cui la potenza P_T ricevuta dall'antenna è maggiore della potenza minima P_{Chip} di attivazione del chip, ossia la sensibilità.
Nei tag ad accoppiamento elettromagnetico nell'ipotesi che l'antenna ricevente (del tag) sia adattata rispetto all'impedenza del chip e alla polarizzazione dell'onda incidente, la densità di potenza che investe l'antenna ricevente è:

$$S_{av} = \frac{P_{in}}{4\pi r^2} G_R(\vartheta_R, \varphi_R) \tag{2.19}$$

La potenza raccolta:

$$P_{Tag} = S_{av} A_{Tag}(\vartheta_R, \varphi_R) \tag{2.20}$$

L'area efficace del tag:

$$A_{Tag}(\vartheta_T, \varphi_T) = 4\pi \frac{G_{Tag}(\vartheta_T, \varphi_T)}{\lambda^2} \tag{2.21}$$

$$P_{Tag} = P_{in} G_R G_{Tag} \left(\frac{c}{4\pi r f}\right)^2 \tau \propto \frac{1}{r^2} \quad \text{(formula di Friis)} \tag{2.22}$$

La massima distanza di lettura tra reader e tag è quella per cui la potenza P_{Tag} ricevuta dall'antenna è uguale alla potenza minima P_{Chip} di attivazione del chip.

$$r_{max} = \frac{c}{4\pi f} \sqrt{\frac{P_{in} G_R G_{Tag}}{P_{chip}}} \tag{2.23}$$

Ove l'antenna del tag è adattata a quella del chip, ossia il massimo trasferimento di potenza incidente al chip si ha in caso di adattamento coniugato:

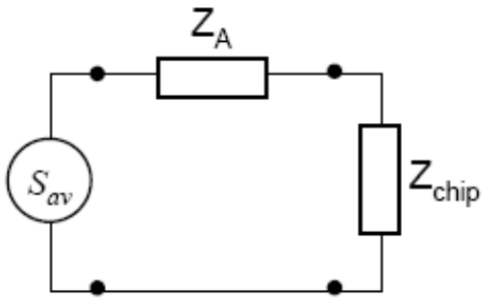

Figura 2.15 – Rappresentazione impedenza antenna e chip del tag

$R_A = R_{Chip}$ e $X_A = -X_{Chip}$ in realtà non è semplice adattare perfettamente l'antenna all'impedenza del chip, questo non perfetto adattamento viene tenuto conto dal coefficiente di trasmissione in potenza :

$$\tau = \frac{4 R_A R_{Chip}}{|Z_A + Z_{Chip}|} \leq 1 \tag{2.24}$$

La qualità dell'adattamento tra antenna e tag influenza la distanza di lettura, migliorando tale è possibile aumentare la distanza di lettura. Possiamo ricordare che la distanza di lettura quindi il raggio d'azione è influenzato principalmente da tre parametri, ossi la potenza emessa o irradiata dal lettore, il consumo del chip per poter funzionare, il tipo e la posizione delle antenne. [9]

2.5 STANDARD E NORMATIVE DI RIFERIMENTO

Esistono diversi enti ed iniziative che si pongono l'obiettivo di definire e diffondere degli standard che possano facilitare lo sviluppo e la diffusione dei sistemi interoperabili.
Gli standard sono accordi documentati che contengono specifiche tecniche od altri criteri precisi da utilizzare in modo consistente come regole, linee guida o definizioni di caratteristiche al fine di garantire che materiali, prodotti processi e servizi siano idonei allo scopo per cui sono stati creati.
Per quanto riguarda la tecnologia RFID il riferimento a specifiche tecniche deve prendere in considerazione quattro tipologie di standard:

- **Standard tecnologici:** che hanno a che fare con le caratteristiche, come l'interfaccia a radiofrequenza, il tipo di modulazione ed il protocollo per lo scambio dei dati, che devono essere comuni per garantire la compatibilità e l'interoperabilità in sistemi prodotti da costruttori diversi.
- **Standard dei dati:** che definisce la modalità con cui i dati sono strutturati sempre per soddisfare i requisiti di compatibilità ed interoperabilità.
- **Standard applicativi:** che si riferiscono al modo in cui la tecnologia viene utilizzata in applicazioni particolari per assicurarne un uno consistente.
- **Standard di conformità:** che fanno riferimento al modo in cui il sistema deve operare per essere accettabile nei confronti di criteri operativi particolari o criteri di salvaguardia per la salute pubblica.

Nel caso specifico di sistemi RFID si deve assicurare che i dati creati alla sorgente siano perfettamente comprensibili da chiunque li riceva.

Nel caso del RFID che opera utilizzando frequenze radio è necessario garantirne la conformità ai regolamenti ed alle normative che determinano l'uso dello spettro RF.
Questi aspetti normativi si aggiungono a quelli di base dello standard tecnologico e possono variare da paese a paese e cambiare nel tempo.
Gli enti standardizzatori più importanti con maggiore influenza su quest'area dell'identificazione automatica sono sostanzialmente due e si preoccupano di generare gli standard per la tecnologia RFID e si muovono in alcuni casi in collaborazione: **l**'international Standard Organizzation noto come ISO (International Standard Organisation) e EPC Global.
L'ISO nasce nel 1946 quando i delegati di 25 nazioni decisero di creare una nuova organizzazione il cui obiettivo fosse quello di facilitare il coordinamento internazionale per l'unificazione degli standard industriali.
Oggi l'ISO è composta da delegati in rappresentanza di 148 paesi, ha sede a Ginevra, e continua con estremo successo la sua attività gestendo la standardizzazione nei più svariati settori industriali.
L'EPC Global è invece una joint venture più recente tra EAN International e la Uniform Code Council (UCC) le due organizzazioni mondiali che ancora oggi garantiscono a livello globale il controllo e le assegnazioni dei numeri utilizzati nel più diffuso codice a barre e delle relative tecnologie a supporto della filiera di fornitura (supply chain) dei più ampi settori industriali. La loro unione con l'assorbimento dell'Auto-ID center, un progetto di ricerca accademico avviato presso il Massachusetts Institute of Technology (M.I.T.) affiancato da diverse università statunitensi e non, ha dato corpo ad EPC Global che è un'organizzazione privata ed è indipendente senza scopo di lucro per sviluppare le stesse funzioni che EAN ed UCC svolgevano per la tecnologia dei codici a barre ma portata verso la tecnologia RFID.

2.5.1 Standard ISO

Gli standard ISO sono stati sviluppati per garantire determinati obiettivi:

- Rendere lo sviluppo, la produzione e la fornitura di prodotti e servizi efficienti e sicuri.

- Facilitare il commercio tra i Paesi.
- Fornire i governi di una base tecnica per salute, sicurezza e legislazioni ambientali.
- Condividere migliorie tecnologiche e procedure di buona gestione.
- Salvaguardare i consumatori, e gli utenti in generale, dei prodotti e dei servizi.
- Fornire soluzioni a problemi comuni.

L'ISO è stata la prima a portare gli standard RFID nel mondo delle smart card sia a contatto che contactless

Due gli standard introdotti in questo settore:

- ISO/IEC 14443 (Identification Card Contactless integrated circuit card Proximity)

  Definisce lo standard per le carte senza contatto (Contactless Smart Card) operanti alla frequenza di 13,56 MHz in prossimità dell'antenna del Reader, a un massimo di 10 cm di distanza. Vengono descritti i requisiti fisici che le carte devono soddisfare (in termini di dimensioni e resistenza al danneggiamento), la potenza massima disponibile per la comunicazione RF, le interfacce e i protocolli di trasmissione e anticollisione.

  ISO/IEC 14443 fornisce due diversi tipi di codifica (A e B) del segnale: tutti e due gli schemi sono half-duplex e garantiscono una bit rate di 106 Kbits/s in entrambe le direzioni; i dati sono trasmessi modulando una sopportante a 847.5 KHz.

  Tipo A: il Reader comunica con la carta attraverso una modulazione d'ampiezza con indice di modulazione al 100% e codifica Miller Modificata; i dati della carta sono trasmessi al Reader usando la codifica Manchester, con modulazione OOK della sottoportante a 847.5 KHz. Il circuito integrato della carta deve essere progettato per immagazzinare sufficiente energia, poichè il campo RF non è costantemente generato, ma deve essere spento per brevi periodi, durante la trasmissione da parte del Reader.

  Tipo B: il Reader comunica modulando l'ampiezza della portante con indice di modulazione al 10% e codifica NRZ dei dati; la carta utilizza la modulazione

BPSK della sottoportante con i dati codificati NRZ-L. Il campo RF rimane costantemente attivo durante tutta la comunicazione.

- ISO/IEC 15693 (Identification Card Contactless integrated circuit card Vicinity)

  Fa parte di una serie di standard internazionali per la descrizione delle smart card senza contatto. Nelle sue varie parti lo standard si occupa della definizione delle dimensioni delle smart card, del protocollo di comunicazione Reader-card, della potenza utilizzata per la trasmissione, dell'interpretazione dei comandi ricevuti da una smart card per avere la sicurezza di selezionare la card giusta tra quelle presenti nel raggio di lettura del Reader.

  Le smart card operano alla frequenza di 13.56 MHz, una delle frequenze utilizzabili a livello mondiale nel settore industriale, scientifico e medico.

  Le smart card comunicano con il Reader modulando una o due sottoportanti a 450 KHz, con i dati codificati Manchester.

Successivamente ed espressamente per il mondo RFID sono stati emessi gli standard per il livello fisico sotto il protocollo ISO/IEC 18000 che definisce l'interfaccia di comunicazione via aria per le operazioni in radio frequenza per l'identificazione e la gestione di oggetti, specificandone i parametri alle varie frequenze operative (<135 KHz, 13.56 MHz, 2.45 GHz, 5.8 GHz, 860÷960 MHz, 433 MHz). Esso si si suddivide in:

- ISO/IEC 18000 Part 1-Generic Parameters for the air interface
- ISO/IEC 18000 Part 2- Parameters for Air interface communications < 135 KHz
  - Tipo A (FDX) 125 kHz e Tipo B (HDX) 134.2 kHz
- ISO/IEC 18000 Part 3- Parameters for Air interface communications at 13.56 MHz
  - Modo 1 basato sulla ISO 15693 con aggiunte varianti per migliorare la gestione di oggetti singoli.
  - Modo 2 è un interfaccia ad alta velocità
- ISO/IEC 18000 Part 4 – Parameters for Air Interface Communications at 2.45 GHz

- ISO/IEC 18000 Part 5 – Parameters for Air Interface Communications at 5.8 GHz
- ISO/IEC 18000 Part 6 – Parameters for Air Interface Communications at 860 to 930 MHz
    - Tipo A e Tipo B che differiscono sia per il tipo di codifica, modulazione ed anticollisione.
- ISO 18000/IEC Part 7 – Parameters for Air Interface Communications at 433 MHz

In particolare la direttiva ISO/IEC 18000-6 si occupa dei prodotti che operano nella banda 860÷960 MHz per applicazioni industriali, scientifiche e mediche (ISM band), fornendo i parametri tecnici per la comunicazione da Reader a Tag e viceversa, quali: frequenza operativa, occupazione di banda del canale, modulazione, duty cycle, codifica dei dati, bit rate.

La tabella seguente riassume le distinzioni delle frequenze di questa banda utilizzate dai diversi Paesi.

REGIONE	**FREQUENZA (MHz)**
GLOBALE	860-960
FCC - Federal Communication Commission (USA)	902-928
ETSI - European Telecommunication Standards Institute	868
GIAPPONE	950

Tabella 2.4 - Frequenze mondiali di rifermento per l'UHF

Inoltre, come si vede nell'elenco precedente, ISO/IEC 18000-6 descrive due tipologie di comunicazione:

Tipo A: usa una codifica Pulse Interval Encoding (PIE) per la comunicazione Reader-Tag e un protocollo anticollisione ALOHA adattivo;

Tipo B: per la comunicazione Reader-Tag usa la codifica Manchester, e il protocollo anticollisione adattivo ad albero binario (Adaptive Binary Tree).

NOTA: i Tag compatibili con lo standard EPC Global Class1 Gen2 trovano una loro controparte nella direttiva ISO/IEC 18000-6C.

L' ISO si è incaricata anche sul fronte logico ed applicativo definendo alcuni standard relativi:

- ISO/IEC 15961:2004 –Radio Frequency Identification for Item Management – Data protocol: application Interface.
- ISO/IEC 15962:2004 Radio Frequency Identification for Item Management-Data Protocol: data encoding rules and logical memory functions.
- ISO/CD 17363 Supply chain application for RFID Freight containers
- ISO/WD 17364 Supply chain application for RFID Transport units
- ISO/WD 17365 Supply chain application for RFID Returnable transport items
- ISO/WD 17366 Supply chain application for RFID Product packaging
- ISO/CD 17367 Supply chain application for RFID Product tagging

Ci sono gli standard espressamente sviluppati per la tracciabilità animale:

- ISO 14223/1:2003 RFID of Animals, Air Interface
- ISO 11785:1996 RFID of Animals, Technical concept
- ISO 11784:1996 RFID of Animals, Code Structure

2.5.2 Standard EPCglobal

Nei laboratory di Auto-ID center è stata avviata nel 1999 l'attività di ricerca e di sviluppo per la definizione di una architettura standard aperta allo scopo di creare una rete globale di oggetti fisici definite un internet delle cose.
Questo obiettivo è raggiungibile attraverso la tecnologia RFID che diventa il mezzo per collegare in modo trasparente gli oggetti alla rete globale: la EPC Global Network.
Quest'ultima è composta da cinque componenti:

- Electronic Product Code (EPC) un "codice a barre " elettronico che identifica il produttore, il prodotto, la versione ed il numero di serie di ogni singolo oggetto.
- Un sistema di identificazione o "System ID " composto da un'etichetta elettronica, o tag, e da un lettore (reader).
- L'EPC MiddleWare il software che consente lo scambio di informazioni tra il lettore ed il sistema informativo a cui si collega;
- Un "discovery Service" una rete di nodi di servizio hardware e software in grado di trovare i dati correlati con quello specifico codice EPC
- Un servizio EPC che consente agli utilizzatori di scambiare dati basati sul codice EPC.

NOTA: L'Electronic Product Code (EPC) è una famiglia di schemi di codifica creati come successori dei codici a barre. L'EPC è stato introdotto come metodo di tracciamento di beni a basso costo in tecnologia RFID, che garantisce un codice univoco per ogni Tag. I Tag EPC sono stati progettati per identificare ogni singolo prodotto, non solo classe e produttore come accade usando i codici a barre. L'EPC si integra con gli schemi di codifica esistenti e ne definisce di nuovi laddove necessario. Tutti i codici EPC contengono un header che individua lo schema di codifica che è stato utilizzato; a sua volta questo valore definisce la lunghezza, la struttura e il tipo dell'EPC. Inoltre, lo schema di codifica contiene un numero seriale che può essere utilizzato per identificare univocamente un oggetto.

Le specifiche definite dall'EPCglobal in termini di air interface e codifica dei dati sono le seguenti:

- 900 MHz Class 0 Radio Frequency Identification Tag Specification

  In questo documento viene definita l'interfaccia di comunicazione ed il protocollo di comunicazione alla frequenze di 900 MHz (UHF) per Tag detti di Classe 0.
- 13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification

  Interfaccia e protocollo per tag di clase 1 nella banda dei 13.56 MHz (HF).

- 860 MHz 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & logical Communication Interface Specification
  Interfaccia e protocollo per tag di classe 1 nella banda 860 – 930 MHz (UHF)

La categorizzazione in classi fa riferimento alla funzionalità base dei tag con questo schema:

- Classe 0 passivi Read Only
- Classe 0+ con lo stesso protocollo della classe 0 ma riscrivibili
- Classe 1 passivi Write Once Read Many, il codice viene scritto una prima volta dall'utente e poi diventa immodificabile.

La classificazione EPC prevede cinque classi ma le due appena riportate rappresentano le più significative anche se vengono rese obsolete dalla Classe 1/ generazione 2 mentre le classi 2, 3, 4, 5 non sembrano rilevare particolari interessi.
Le specifiche della classe 1/ generazione 1/ generazione 2 comunemente richiamate con il termine Gen2 sono state sviluppate per superare le limitazioni presentate dalle specifiche precedenti [10].

EPC Global Class1 Gen2

Nel dicembre 2004, EPCglobal ha emesso uno standard per TAG operanti nelle banda UHF media, che promette la diffusione massiva di TAG passivi a basso costo ed alte prestazioni. Si tratta dei cosiddetti Class 1 Generation 2 (EPC Gen2) RFID.
Lo standard Gen2 (EPCglobal & ISO/IEC 18000-6 Type C) definisce una classe di TAG passivi, operanti in backscatter nelle frequenze 860÷960 MHz ed in modalità HDX (Half Duplex).
Il Reader trasmette l'interrogazione al Tag modulando la portante a 860÷960 MHz; il Tag riceve dal campo RF la potenza necessaria ad alimentarsi (il Reader continua ad inviare la portante per fornire energia al TAG durante la risposta) e decodifica il segnale del Reader, rispondendo all'interrogazione modificando il segnale in backscattering. Il sistema è ITF (Interrogator Talks First), per cui il Tag modula il coefficiente di riflessione della propria

antenna solo dopo aver ricevuto il comando da parte del Reader. Inoltre, essendo le comunicazioni half-duplex, mentre il Reader parla, il Tag ascolta, e viceversa.

La Classe 1 descrive i dispositivi passivi (Tag o labels, etichette), dotati delle seguenti caratteristiche:

- Un identificativo EPC (Electronic Product Code).
- Un Tag Identifier (Tag ID o TID).
- Una funzione che permetta di disabilitare permanentemente il Tag (Kill).
- Accesso protetto da password (opzionale).
- Memoria utente (opzionale).

Nelle bande consentite a livello regionale, i sistemi hanno a disposizione 50 canali di 500 kHz a 4 W di potenza negli USA (902÷928 MHz) e 10 canali di 200 kHz a 2 W (più 5 a bassa potenza) in Europa (865÷868 MHz). Da ciò deriva una rilevante diversità di approccio tecnico al problema della possibile presenza di un numero rilevante di Reader nel medesimo ambiente operativo, che si concretizza nell'uso di tecniche di "Frequency Hopping" oppure di "**L**isten **B**efore **T**alk" – **LBT**.

Pur nell'estrema semplicità dell'elettronica associata ad un TAG passivo, un TAG Gen2 riesce a realizzare una macchia a stati finiti abbastanza complessa in cui i comandi ricevuti dal Reader possono provocare, a seconda dello stato corrente della macchina (TAG), risposte (al Reader) e transizioni di stato (della macchina – TAG) differenti.

La complessità della macchina a stati del TAG è dovuta alla necessità di integrare in essa tutte le funzioni del transponder medesimo; dalla generazione di sottoportanti in modulazione, agli algoritmi anti-collisione, alle procedure di sicurezza, ecc.

Vengono ora elencati alcuni aspetti chiave per i quali lo standard Gen2 ha identificato soluzioni di maggiore efficienza rispetto alle normative precedenti:

- **Modulazioni e codifiche:** lo standard prevede l'impiego da parte del TAG delle modulazioni ASK e PSK in modo indifferente
- **Memoria:** lo standard prevede una capacità di memoria non troppo dissimile dai TAG di classe 1 (EPCglobal). Da 96 a 512 bit di memoria nel TAG contro i precedenti 64÷96 (comunque sufficienti a contenere l'EPC). L'aspetto più

interessante consiste nella segmentazione della memoria per contenere maggiori informazioni rispetto al semplice EPC e nella protezione della memoria.

- **Bitrate vs. identificazione dei TAG:** in genere si riconosce ai TAG Gen2 una velocità superiore alle generazioni precedenti. I bitrate ammessi sono
  Reader =>TAG 26,7÷128 kbit/s;
  TAG=>Reader 5÷640 kbit/s.
  La velocità di lettura è in funzione di diverse variabili che comprendono la potenza d'uscita, la densità dei TAG e l'ambiente operativo a radiofrequenza.
- **Affidabilità:** sono previsti miglioramenti essenziali rispetto ai precedenti. Le nuove caratteristiche mirano all'eliminazione di falsi positivi in lettura e in generale all'ottenimento di maggiore affidabilità nella lettura medesima.
- **Raggio di copertura:** bisogna comunque ricordare che il massimo raggio di copertura è principalmente funzione della potenza irradiata. Poiché i limiti per tale potenza sono differenti per gli USA, l'Europa e il Giappone, ci si dovrà aspettare valori differenti tra queste aree.
- **Sicurezza:** i TAG conformi allo standard Gen2 sono protetti da manomissioni. Il cosiddetto "cloaking", infatti, consente di configurare i TAG in modo tale che prima di rispondere a qualunque interrogazione necessitano di ricevere una password dal Reader. Le Password possono essere anche richieste per scrivere i TAG o disabilitarli. Altro requisito di sicurezza supportato dallo standard e particolarmente richiesto è la possibilità di disabilitare definitivamente ("killing") i TAG in modo tale che i loro dati non possano più essere accessibili.
- **Costi:** una delle maggiori spinte che hanno guidato lo sviluppo dello standard Gen2 è stato quello di avere a disposizione una tecnologia RFID con costi tali da poter essere introdotta convenientemente nelle operazioni previste nelle catene di distribuzione. Lo standard Gen2 raggiunge un compromesso tra costo e funzionalità supportate, che dovrebbero condurre alla fabbricazione di prodotti competitivi in termini di prezzo che soddisfino le esigenze di applicazioni massive.

Memoria TAG secondo lo standard EPCglobal

L'organizzazione della memoria secondo lo standard EPC è divisa in quattro blocchi fondamentali, che contengono da zero a più "parole ". Essi sono:

a) **Memoria riservata:**

   Contiene la password per accedere al banco di memoria ("access password") e la password per distruggere il TAG una volta esaurita la sua funzione("kill password").

b) **Memoria EPC:**

   Contiene il CRC (Cyclic- Redundancy-Check per il controllo dei dati che vengono trasmessi da ricevitore a trasmettitore e da trasmettitore a ricevitore), contiene il PC (il Protocollo di Controllo che dà informazioni sul livello fisico; è contenuto nel banco 1 insieme al codice elettronico del prodotto) e il codice EPC che identifica l'oggetto a cui il TAG è attaccato. La quantità di memoria che viene riportata sui datashit (in genere 96 bit) si riferisce univocamente all'EPC. Gli altri banchi non sono compresi e rappresentano quella parte di memoria del TAG che in realtà è riservata.

c) **Memoria TID:**

   Contiene l'identificativo del TAG.

d) **Memoria Utente:**

   Opzionale. Permette all'utente di inserire in questa parte di memoria informazioni in più sul prodotto specifico o sul tipo di applicazione che occorre realizzare.

La figura seguente mostra appunto questa partizione. L'occupazione dei banchi varia a seconda della quantità di memoria disponibile.

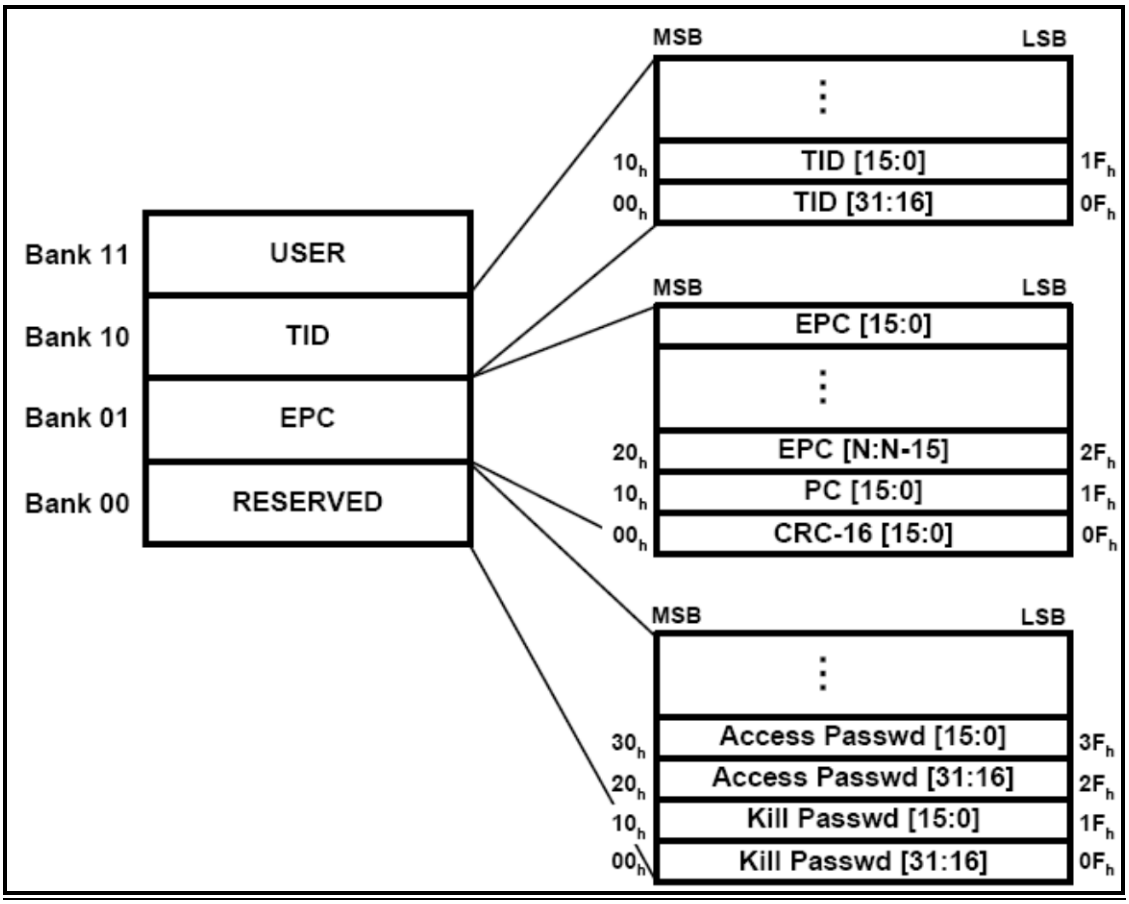

Figura 2.16 – Partizione della memoria del TAG secondo lo STANDARD EPC

2.5.3 Le organizzazioni normatrici

Non esiste un vero ente normatore internazionale, in quanto l'attribuzione e la regolamentazione delle frequenze radio dipendono dalla sovranità nazionale. È quindi sempre necessario, per ciascun utente, verificare che i prodotti che sta utilizzando rispettino le leggi in vigore. Per semplificare, si potrà dire che gli organismi di regolamentazione stabiliscono la frequenza o la banda di frequenza (come nel caso dell'UHF), la potenza di emissione, e il tempo massimo di comunicazione fra etichette e lettori.

Nota importante: Per quanto concerne la potenza, conviene precisare che questo termine può dar adito ad una confusione, poiché vi sono diversi tipi di accoppiamento fra etichetta e lettore, a seconda del tipo di frequenza. Per le basse e le alte frequenze, fino a

13,56 MHz, si tratta di un accoppiamento induttivo, e si dice che il sistema funziona in "campo vicino". Si parlerà quindi di intensità massima di campo, che si esprime in dBμA/m (decibel-microampère per metro).

Nelle altre frequenze (UHF, microonde) l'accoppiamento è elettromagnetico, e si dice che funzioni in "campo lontano". Si parlerà allora di potenza massima di emissione, esprimendo tale potenza in Watt. Ma attenzione: questa unità cambia a seconda delle zone geografiche. In Europa, l'unità è il Watt calcolato in ERP (Effective Radiated Power), in America l'unità è sempre il Watt, ma in questo caso calcolato in EIRP (Equivalent Isotropic Radiated Power). Il rapporto fra le due unità è il seguente: 1 W ERP = 1,62 W EIRP. Di conseguenza, quando si confrontano i livelli massimi autorizzati in queste due regioni, bisognerebbe utilizzare la stessa unità. Così facendo i 2 Watt ERP autorizzati dalla nuova norma europea di cui parleremo più avanti, corrispondono in realtà a 2 x 1,62 cioè a 3,24 Watt EIRP, che si potranno così comparare ad esempio ai 4 Watt EIRP ammessi negli Stati Uniti. Il lettore attento dovrà fare attenzione a quale unità sia effettivamente utilizzata in ciascun Paese.

In Europa, sono il CEPT (Comitato Europeo Poste e Telecomunicazioni), e i suoi organismi associati, l'ETSI (European Telecommunications Standard Institute) e l'ERC (European Radiocommunications Commitee), gli enti incaricati di proporre le norme comunitarie di riferimento che i Paesi europei saranno poi liberi di applicare o no, a seconda del caso. Secondo questi enti, la RFID viene considerata all'interno dei dispositivi "Short Range Device". Esistono già un certo numero di testi (vedi tabelle CEPT ed ETSI), in particolare il documento CEPT/ERC 70-03.

In particolare, nel settembre 2004, l'ETSI ha pubblicato la norma EN 302-208 che concerne specificamente l'UHF, e che autorizza una potenza di 2 Watt ERP nella banda di frequenza 865,6 – 867,6 MHz.

ORGANISMO	NORME	OBJECT
CEPT	CEP/ERC 70-03	Recommendation relating the use of short range devices (SRD)
	CEPT T/R 60-01	Low-power radiolocation equipment for detecting movement and for alert (EAS)
	CEPT T/R 22-04	Harmonisation of frequency bands for Road trasport Information Systems (RTI)
ETSI	EN 300/220	Electromagnetic compatibilità and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1000 MHz frequency range with power levels ranging up to 500 mW
	EN 300/330	Electromagnetic compatibilità and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 KHz to 25 MHz andinductive loop systems in the frequency range 9 KHz to 30 MHz
	EN 300/440	Electromagnetic compatibilità and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range
	EN 302/208	Electromagnetic compatibilità and Radio spectrum Matters (ERM); Radio Frequency Identification Equipment operatine in the band 865 MHz to 868 MHz with power levels up to 2 W

Tabella 2.5 - Le norme europee emesse da CEPT ed ETSI

2.5.4 Considerazioni sulla privacy

Gli RFID introducono alcune problematiche a livello di privacy.

Questi problemi frenano la diffusione di questa tecnologia: in questo paragrafo analizzeremo le problematiche relative alla privacy e vedremo le possibili soluzioni.

Le etichette RFID sono utilizzate in moltissimi settori per razionalizzare i sistemi di spedizione e stoccaggio, tenere traccia di componenti e apparecchiature, e autenticare i prodotti venduti. Sebbene nella maggior parte dei casi l'impiego delle etichette RFID sia limitato a livello di colli o pallet all'interno di magazzini e impianti di produzione, alcune aziende stanno iniziando a sfruttare questa tecnologia sulle confezioni dei singoli prodotti. Un esempio lo si trova nel settore farmaceutico, dove le etichette RFID possono aiutare a proteggere i consumatori dai medicinali contraffatti.

Il ciclo di vita dei TAG, supera spesso e di gran lunga quello degli oggetti ai quali sono associati. Specie i TAG passivi, che non necessitano di batterie, hanno aspettativa di vita teoricamente infinita.

I TAG, infatti, continuano a funzionare anche quando la catena di distribuzione è giunta al termine, ciò significa che è possibile continuare ad interrogare gli oggetti da tempo in possesso di proprietari privati, traendo da ciò informazioni sulle abitudini di vita degli utenti.

In realtà, in modo più pragmatico, il dibattito su RFID e privacy tende a focalizzarsi principalmente sulle applicazioni di TAG a singoli articoli di consumo e ad oggetti abitualmente in possesso di privati (carte di pagamento o di accesso, apparati elettronici, ticket, ecc.). In particolare, anche se l'etichettatura elettronica di singoli articoli non è ancora massivamente diffusa, la potenziale minaccia connessa con questa tecnologia agita timori connessi al fatto che le aziende, che inglobano questo tipo di sistemi nei loro prodotti, possano acquisire informazioni indebite sulla clientela.

A livello normativo, in Italia, il Garante per la Privacy ha pubblicato in data 9 marzo 2005 un provvedimento dedicato alle applicazioni RFID, una sorta di documento "attuativo" basato sulla ben nota legge 196 sulla privacy (" Codice in materia di protezione dei dati personali"). Il documento, che si può considerare un risultato soddisfacente e completo, parte da una rigorosa suddivisione fra applicazioni che richiedono il trattamento dei dati

personali – intendendo con questi tutto ciò che identifica o rende identificabile una persona – e sistemi che non lo fanno: solo nel primo caso, quindi, sarà necessario informare il titolare e richiedere il suo consenso all'utilizzo di queste informazioni. La RFID rientra in questi obblighi solo se i tag riguardano il trattamento dei dati personali: sarà quindi il caso di una carta fedeltà, non di una qualsiasi applicazione di supply chain o di magazzino. Il documento del Garante disciplina quindi l'uso della RFID per la gestione dei dati personali secondo una serie di principi basati in definitiva sui diritti e sulle libertà fondamentali della persona.

La soluzione che si sta mettendo in atto, per la gestione degli oggetti, è la possibilità di disattivare permanentemente i TAG al termine della catena di distribuzione, ovvero quando gli oggetti sono entrati in possesso dell'utente finale. Questa opzione viene denominata "Killing": alcuni TAG passivi (in particolare quelli aderenti allo standard EPC) riservano un'area di memoria dedicata, che serve proprio a questa funzione e alla quale si accede attraverso una password predefinita.

2.6 PROBLEMATICHE DI SICUREZZA

La diffusione degli RFID per identificazione elettronica, porta inevitabilmente ad un fiorire di nuove tecniche fraudolente, sfruttando il fatto che si tende a considerare le tecnologie "sicure" solo perché sono "nuove" anche quando effettivamente sicure non sono. L'acquisizione fraudolenta di dati o la loro alterazione o distruzione viene facilitata e non contrastata dall'uso di tecnologie che non richiedono né il contatto fisico, né la visibilità degli apparati. Basterà pensare che l'alterazione di etichette cartacee è operazione per nulla semplice ed inattuabile su larga scala, mentre un hacker esperto potrebbe, grazie alle tecnologie RFID, alterare in pochi minuti tutte le date di scadenza degli alimenti nelle etichette elettroniche in un supermercato, generando caos tra i clienti e disastrosi danni commerciali all'esercizio. Purtroppo, le misure di sicurezza attuabili sono, specie per i tag passivi, piuttosto deboli e si limitano alla protezione dei campi della memoria tramite password. Esistono soluzioni molto efficienti, basterebbe interfacciare le etichette con i metodi di crittografia comunemente usati nelle transazioni finanziarie come contro questi metodi richiedono però una capacità elaborativa attualmente incompatibile con tag passivi

a basso costo. Probabilmente l'impossibilità di implementare complessi processi di elaborazione nei tag passivi permarrà anche nel medio termine, le etichette elettroniche, pertanto, andranno saggiamente considerate come tali e non come documenti certificati [8].

2.6.1 Minacce alla sicurezza (threats)

L'acquisizione o l'alterazione illecita dei dati contenuti nei tag RFID può avvenire sia attraverso interrogazioni fraudolente degli RFID con reader non autorizzati sia mediante intercettazione, tramite ricevitori radio, durante una lettura degli stessi da parte di un reader autorizzato. Questo può essere realizzato sia mediante reader o ricevitori a lungo raggio sia, ad esempio, occultando un reader connesso ad un PC in un posto qualsiasi in prossimità dei tag in movimento lungo la linea di produzione oppure utilizzando un dispositivo portatile.

INTERCETTAZIONI (EAVESDROPPING):

L intercettazioni assumono particolare importanza e costituiscono il tipo di attacco più comune. Per intercettare un segnale l'hacker attaccante usa, ovviamente, un ricevitore ed una antenna. Il primo problema da risolvere sarà quindi la ricevibilità dei segnali, il secondo sarà interpretare il loro significato. La decodifica sarà un problema se la trasmissione è criptata, altrimenti la domanda principale sarà quanto deve essere vicino l'hacker per ricevere un segnale RF utilizzabile, visto che gli apparati operano generalmente in prossimità. Per effettuare questo tipo di attacco bisogna tener conto di un elenco di fattori quali:

- Potenza emessa dall'apparato sotto intercettazione.
- Sensibilità e capacità di decodifica del ricevitore dell'hacker (che può essere più alta di quella dei comuni reader, consentendo intercettazioni a distanze maggiori di quelle operative degli apparati commerciali).
- Caratteristiche dell'antenna dell'hacker (geometria, libertà di movimento, ecc.)

- Caratteristiche del campo RF emesso dall'apparato sotto intercettazione (geometria dell'antenna, effetto schermante dei contenitori o del circuito stampato del tag).
- Caratteristiche dell'ambiente (presenza di muri o masse metalliche, livello di rumore di fondo, ecc.).
- Modo di operare dell'apparato sotto intercettazione (in modalità passiva generalmente è molto più difficile da intercettare in quanto opera con un minimo campo EM).

A proposito del fatto che i tag passivi siano meno esposti alle intercettazioni di quelli attivi va ricordato che, nei sistemi con tag passivi di prima generazione, a volte il reader "ripete" a scopo di verifica (trasmettendolo ad alta potenza), l'EPC ricevuto dal tag. Questo vanifica il vantaggio contro le intercettazioni dei tag passivi. Il problema viene superato, nei tag passivi Gen2. In ogni caso le misure efficaci contro le intercettazioni sono essenzialmente due: - Minimizzazione della propagazione "inutile" dei segnali radio. - Allestimento di un "canale sicuro".

DISTURBO DELLA COMUNICAZIONE E ALTERAZIONE DEI DATI:

In questo tipo di attacco, l'hacker tenta di modificare i dati in transito in modo che vengano ricevuti alterati. L'alterazione, però, è intesa solo come disturbo della comunicazione, non essendo l'hacker in grado di interpretare i dati ed alterarli in modo da farli apparire come una falsa informazione.

Il disturbo viene in genere realizzato trasmettendo a tempo debito nelle frequenze corrette. Il momento opportuno può essere calcolato dall'hacker attraverso lo studio del sistema di modulazione e codifica del sistema sotto attacco. Questo tipo di attacco non è complesso da realizzare ma non permette all'hacker di manipolare i dati in transito, si tratta essenzialmente di un disturbo al servizio, attuabile per breve tempo e funzionale ad azioni di altro tipo. La contromisura per questo tipo di attacco è l'ascolto da parte di un sistema indipendente di controllo, attrezzato meglio di un reader commerciale, non tanto per ricostruire i dati corretti, ma per percepire la situazione e dare l'allarme. Una variante a questo tipo di attacco è l'alterazione dei dati, anche in questo tipo di attacco, l'hacker

tenta di modificare i dati in transito in modo che vengano ricevuti alterati. L'alterazione, in questo caso, è attuata per far sì che i dati vengano ricevuti come validi (ancorché manipolati). La fattibilità di questo attacco dipende dall'indice di modulazione utilizzato da chi trasmette, e dalla conseguente tecnica di decodifica.

ATTACCO DEL TERZO ESTRANEO:

Nella situazione classica dell'attacco da parte di un terzo estraneo due apparati che stanno scambiandosi dati (Apparato A e Apparato B) sono ingannati da un terzo estraneo (hacker) attraverso una conversazione a tre. Durante l'attacco i due apparati non sono consapevoli di non parlare tra loro, bensì con l'hacker che simula, alterandoli, i dati di entrambi.

Se il canale non è protetto, l'attacco del terzo estraneo ha buone possibilità di riuscire. Nel caso dell'allestimento di un "canale sicuro" (che se instaurato correttamente vanificherebbe l'attacco), i due apparati dovrebbero concordare una chiave segreta che useranno per criptare i dati generando un canale sicuro. Tuttavia l'hacker può concordare una chiave con l'apparato A ed una con l'apparato B continuando ad intercettare le comunicazioni ed alterare i dati.

Le tecniche di attacco del terzo estraneo si manifestano come:

- **Tracciamento illecito:** una delle questioni principali relative alla sicurezza nell'ambito dell'uso dei sistemi RFID, se i tag possono essere letti arbitrariamente, è il cosiddetto tracciamento illecito dei tag, per mezzo del quale, oltre alla privacy personale sulla localizzazione, può anche essere violata la sicurezza industriale.

  In particolare lo spionaggio industriale dall'interno della catena di distribuzione può essere favorito in quanto i tag contengono una varietà di dati che vanno dal semplice EPC a informazioni più articolate sul prodotto (ad esempio il tipo di sangue contenuto in un campione). In tale ambito si prefigurano quindi rischi sia di sabotaggio industriale cioè alterazione (cancellazione / modifica) dei dati dei tag usando un apparato portatile, sia di spionaggio industriale cioè furto di informazioni per conoscere quanti e quali tipi di prodotti sono fabbricati nell'azienda spiata.

- **Clonazione o furto degli ID:** si tratta di duplicazioni non autorizzate: le informazioni contenute in alcuni tag RFID possono essere acquisite a distanza e senza che il proprietario ne venga a conoscenza. È possibile quindi acquistare tag simili e scriverli con i dati autentici (copiati), creando quindi la possibilità di contraffazione di prodotti che si suppone siano protetti da tag. Questa è una problematica fondamentale per i tag contenuti nelle carte di accesso o nei sistemi di pagamento senza contatto, così come per i passaporti RFID e le card di
  identificazione; ma anche per semplici articoli di consumo protetti da marchi di origine, che possono essere sostituiti da merce contraffatta.
- **Violazione della privacy:** l'"invisibilità" e "silenziosità" dei tag così come dei reader è considerata una delle maggiori minacce alla privacy portate dalla tecnologia RFID. Infatti esiste la possibilità di raccogliere informazioni riguardanti un certo prodotto e, in dipendenza dalle circostanze, anche della persona che porta quel prodotto, senza informare la persona stessa e senza averne il suo consenso.

  Un'applicazione RFID può acquisire una grande mole di dati. Se un prodotto dotato di tag è, per esempio, pagato con una carta di credito, è possibile collegare l'ID che identifica univocamente quel prodotto con l'identità dell'acquirente. Inoltre, cogliendo l'occasione, sarebbe possibile interrogare tutti i tag associati agli oggetti e agli abiti che il cliente porta con sé in quell'istante, arricchendo la banca dati del venditore con informazioni preziose. I dati così ottenuti possono essere utilizzati per creare un profilo della persona. Tale profilo può esser utilizzato per vari scopi, come per valutare l'importanza di un consumatore per una certa azienda. La difficoltà di ottenere una situazione di serenità sugli usi possibili degli RFID è il motivo per cui molte tra le aziende produttrici di articoli e tra le organizzazioni di vendita al minuto, pur avendo in programma l'introduzione di RFID nei loro prodotti, non danno nessuna pubblicità all'evento e, in qualche caso, vincolano gli installatori dei sistemi alla riservatezza.

  In teoria, sarebbe anche possibile la localizzazione geografica ed il tracciamento di una persona attraverso i tag RFID che porta con sé. Questo diventa maggiormente significativo se le applicazioni sono integrate in sistemi estesi. Per esempio il sistema

EPC Global crea identificatori dei prodotti dotati di tag unici a livello mondiale, pertanto, l'individuazione, in un determinato luogo, anche di un solo oggetto di sicura appartenenza ad una persona, fornisce l'informazione che, con buona probabilità, la persona si trovi in quel luogo. Quest'ultima ipotesi, tuttavia, non è ancora realizzabile in quanto, necessitando di un incrocio di molte informazioni contenute in molte banche di dati differenti. Incrocio vietato dalle leggi di tutti i paesi civili. La soluzione al problema della violazione della privacy, comunque, è stata già trovata ed è in commercio. Le etichette RFID UHF di recente fabbricazione (i cosiddetti Gen2), hanno la possibilità di essere disabilitate definitivamente con un comando. Ciò rimuove tutte le possibilità di tracciabilità post vendita degli oggetti. Esistono alcuni aspetti ambientali che influenzano la propagazione e, di conseguenza, la comunicazione tra tag, reader che incidono sull'attacco da parte di eventuali hacker.

- **Disabilitazione totale (killing) o parziale (clipping) di tag:** il principale provvedimento per assicurare la privacy (e quindi la sicurezza) dell'utente privato, parte dal principio che, una volta acquistata la merce, cessa l'interesse a rendere disponibili le informazioni contenute nel tag. Un provvedimento estremamente efficace (per l'utente) è quindi la possibilità di disabilitazione permanente del tag medesimo. La funzione, chiamata "Killing" è stata realizzata nei tag UHF Gen2 e se ne prevede l'implementazione all'uscita dei punti vendita al dettaglio.

  Una possibilità alternativa alla disabilitazione irreversibile del tag è il cosiddetto "clipping" cioè l'operazione che consente di ridurre la distanza operativa del tag a pochi cm mediante la rimozione parziale (strappo fisico) della sua antenna. Questa operazione consente di incrementare significativamente la privacy senza compromettere completamente la funzionalità del tag. Risulta utile qualora l'utente possedesse elettrodomestici (frigoriferi, lavatrici, ecc.) in grado di sfruttare le informazioni dei tag lette da pochi centimetri di distanza. Tale approccio, pur possedendo un grado di sicurezza limitato, offre alcune caratteristiche interessanti, in particolare:

  - è l'utente che può operare direttamente la scelta di ridurre la distanza operativa del tag;

- fornisce una conferma "fisica" di tale operazione;
- consente un successivo utilizzo del tag per applicazioni con problematiche di privacy limitate.

Per contrastare le tecniche di attacco da parte di un terzo estraneo esiste la possibilità di utilizzare **tag a chiave simmetrica:** questo tipo di tag possiede capacità elaborativa sufficiente a produrre funzioni di crittografia simmetrica. In particolare i tag sono dotati di una funzione che genera una versione criptata (detta funzione "hash") di un testo in chiaro. Il testo criptatato si genera combinando una chiave segreta con il testo in chiaro. Per le proprietà della funzione di criptazione (funzione "hash") l'unico modo per risalire al testo in chiaro è possedere la chiave segreta. La gestione del sistema è generalmente centralizzata, nel senso che il Sistema di Gestione possiede le chiavi segrete di tutti i tag e le distribuisce, quando necessario, ai reader. La procedura prevede che il sistema risolva i problemi di autenticazione, scongiurando ogni pericolo di clonazione del tag. Infatti, non venendo mai trasmessa la chiave segreta, l'unico modo per rompere la sicurezza sarebbe quello di effettuare attacchi fisici al tag o al Sistema di Gestione. Questo costituisce anche un limite del sistema dovendo le chiavi segrete di ogni tag (miliardi di chiavi differenti) essere note a tutti i sistemi di gestione nella catena di distribuzione oppure circolare in rete. In entrambe i casi non essendo chiaro da chi debbano essere gestite.

2.7 ELABORAZIONE E TRASMISSIONE DEL SEGNALE

2.7.1 Codifica dei dati

La codifica è l'alterazione delle caratteristiche di un segnale per renderlo più adatto ad una applicazione. Nel tag e nel reader, i dati da trasmettere devono essere codificati in modo da generare un segnale unipolare binario che verrà usato per la modulazione. Esistono numerose tecniche di codifica, ognuna con caratteristiche differenti relativamente all'occupazione spettrale in banda base, alla complessità di codifica/decodifica, alla difficoltà di ricostruire la temporizzazione in ricezione, alla sensibilità ai disturbi e all'energia trasferita. In particolare, i sistemi basati su tag passivi impongono vincoli

piuttosto restrittivi sui parametri di scelta della codifica. La codifica dei dati un'operazione critica per molte applicazioni RFID, soprattutto data la necessità di massimizzare il trasferimento di potenza per l'alimentazione del tag.

Di fondamentale importanza è tener conto che nella trasmissione dal reader verso il tag deve essere massimizzata l'energia nel segnale, per fornire la maggior energia possibile al tag e nella trasmissione dal tag verso il reader deve essere minimizzata l'energia nel segnale, per la scarsità di energia disponibile; l'ampiezza del segnale deve essere comunque tale da consentirne la rilevazione da parte del reader. Generalmente vengono usate codifiche basate sulla durata degli impulsi (PIE - Pulse Interval Encoding) oppure basate sulle transizioni (Manchester, Miller, FM0). I metodi di codifica denominati Manchester (Bi-Phase-L) e Pulse Interval Encoding (PIE) sono i più utilizzati nelle comunicazioni dai reader verso i tag massimizzando l'energia del segnale. Una caratteristica importante di questi metodi di codifica è che, essendo basati sulle transizioni, forniscono una sequenza codificata "auto-temporizzata" tale da consentire di ridurre drasticamente, nei tag passivi, la circuiteria necessaria per la sincronizzazione. I metodi Miller ed FM0 invece vengono impiegati nella comunicazione dai tag passivi verso i reader, minimizzando l'energia del segnale, grazie alla loro proprietà di possedere la componente spettrale a frequenza zero nulla. Nei metodi di codifica viene definita la durata temporale minima dell'impulso. Tale intervallo temporale è denominato TARI (ISO/IEC 18000-6 Type A Reference Interval).

Codifica Manchester

Nella codifica Manchester ogni bit viene segnalato da una transizione. La codifica Manchester fornisce un modo semplice per codificare sequenze binarie arbitrarie senza mai avere lunghi periodi di tempo privi di transizioni di segnale, il che permette di prevenire la perdita della sincronizzazione del clock, oppure errori di bit. Assicura infatti che la componente a frequenza zero del segnale codificato sia zero. La codifica di ogni bit occupa un intervallo di tempo predefinito "time slot" diviso in due metà, chiamate mezzo bit. Uno zero è codificato con una assenza di modulazione nel primo mezzo bit ed una

modulazione nel secondo mezzo bit. Viceversa un bit uno è codificato con una modulazione nel primo mezzo bit ed una non modulazione nel secondo mezzo bit.

Codifica PIE

La codifica di tipo PIE (Pulse Interval Encoding) è basata su un TARI predefinito. I bit zero ed uno così come simboli speciali quali Start Of Frame (SOF) ed End Of Frame (EOF) sono composti da un numero differente di periodi TARI. Conseguentemente, a parità del numero di simboli da codificare, la lunghezza della sequenza codificata risulta variabile. Il valore TARI rappresenta anche l'ampiezza d'impulso minima presente nel segnale modulato, fattore importante per determinare la larghezza di banda del segnale trasmesso: più basso è il valore TARI, più elevata sarà l'occupazione di banda del segnale.

Codifiche MILLER e FM0

Nella comunicazione tag verso il reader sono richieste pertanto codifiche con una componente spettrale a frequenza zero nulla o con energia molto bassa tale da non interferire con il segnale ricevuto e da minimizzare l'emissione
di energia da parte del tag. Le codifiche di tipo Miller e FM0 godono di tale proprietà. Nel caso della codifica di Miller la codifica di ogni bit occupa un intervallo di tempo predefinito "time slot" diviso in due metà, chiamate mezzo bit.
Un bit a uno è codificato con una transizione da assenza di modulazione a presenza di modulazione o viceversa tra i due mezzi bit del simbolo. Un bit a zero è codificato invece continuando la presenza o l'assenza di modulazione come nel precedente mezzo bit oppure invertendo tale stato ovvero si può affermare che si ha un'inversione di fase in banda base nel caso di due zero consecutivi. Nella codifica FM0 invece si ha un'inversione di fase in banda base ad ogni inizio di simbolo ed inoltre la codifica del simbolo zero ha un'inversione tra il primo mezzo bit ed il secondo. [8]

2.7.2 Modulazioni

Nella comunicazione tra reader e tag e viceversa, vengono usate tecniche di modulazione semplici che richiedono bassa complessità circuitale e in cui l'ampiezza, la fase o la frequenza, vengono variate in accordo con l'informazione trasportata da un segnale unipolare binario. Poiché le caratteristiche di propagazione del segnale dipendono in maniera essenziale dalla frequenza operativa, i sistemi RFID che operano sulle bande LF, HF e UHF utilizzano codifiche e modulazioni differenti, i tre tipi di modulazione più comuni sono:

- **ASK** (Amplitude Shift Keying), modulazione d'ampiezza binaria, il segnale modulante (binario) causa la variazione tra due ampiezze della portante. Se la minore delle due ampiezze è 0, la modulazione è chiamata On-Off Keying (OOK). La modulazione ASK può inoltre essere di tipo Double Side Band- Amplitude Shift Keying (DSB-ASK) oppure Single Side Band-ASK (SSB-ASK). Le modulazioni digitali di tipo ASK sono inefficienti da un punto di vista dell'occupazione spettrale per un prefissato bitrate. La modulazione DSB-ASK, infatti, è la tecnica meno efficiente in termini di occupazione spettrale, ma la più semplice da realizzare tramite il meccanismo On – Off (On and Off Keying - OOK) della portante.Un approccio per incrementare l'efficienza spettrale è l'impiego della tecnica banda laterale unica, SSB-ASK .

- **Phase Reversal ASK** (PR-ASK) nella quale il segnale modulante (binario) causa lo spostamento di fase di 180fl della portante. Simile alla cosiddetta BPSK (Binary Phase Shift Keying) prevede che la rivelazione avvenga sulla base dell'ampiezza del segnale ricevuto, e non della fase, così da ottenere un segnale in banda base simile a quello ricavato ad una modulazione ASK. Una tecnica per la quale è possibile minimizzare i requisiti di rapporto segnale rumore in una banda stretta e contemporaneamente massimizzare la potenza trasmessa al tag è la cosiddetta PR-ASK nella quale la fase del segnale trasmesso varia di 180fl ogni volta che viene inviato un simbolo.

- **FSK** (Frequency Shift Keying), il segnale modulante (binario) causa lo spostamento della portante tra due frequenze. La modulazione FSK permette di utilizzare un ricetrasmettitore relativamente semplice da realizzare ed assicurare un alto livello di immunità ai disturbi, ma non consente velocità di trasmissione molto alte avendo a disposizione potenze estremamente limitate.

  Le tecniche di modulazione adoperate in ambiente RFID, devono soddisfare criteri di efficienza sia per l'occupazione spettrale (rapporto bit/Hertz) sia per potenza necessaria alla trasmissione (rapporto segnale/rumore). A questo si aggiunge la necessità di trasferire potenza elettrica al tag in modo continuo.

Modulazione READER → tag nei sistemi passivi

La modulazione reader verso tag deve assicurare che il tag riceva energia sufficiente, che possa facilmente effettuare la rivelazione e che il segnale del reader rispetti le regolamentazioni sulla potenza massima e sull'ampiezza di banda. Se la codifica e la modulazione non consentono al segnale di trasportare abbastanza energia, il tag passivo non è in grado di funzionare. Inoltre il ricevitore del tag deve essere sia semplice che in grado di sincronizzare il segnale. Per ottenere ciò lo schema di codifica (del reader) deve consentire (al tag) il recupero della sincronizzazione. Infine la probabilità di errore nei dati deve essere bassa, pena il fallimento della comunicazione. Nei sistemi LF il reader utilizza prevalentemente la modulazione FSK, per esempio con variazioni tra i due valori di 125 e 134kHz per rappresentare i dati binari trasmessi al tag. Nei sistemi HF e UHF il reader usa prevalentemente la modulazione ASK.

A bordo della maggior parte dei tag passivi sono realizzati ricevitori molto semplici con l'utilizzo di una potenza di alimentazione estremamente bassa. Un tipico circuito è il "rivelatore ad inviluppo".

Modulazione tag → READER nei sistemi passivi

Dato che il tag non è equipaggiato con un trasmettitore ma si limita a modulare il carico (nell'accoppiamento induttivo) o il backscatter (nell'accoppiamento elettromagnetico), va rilevato che entrambe queste tecniche permettono la variazione in ampiezza o in fase della

portante re-irradiata, in dipendenza della loro implementazione. Come conseguenza del livello estremamente basso del segnale modulato dal tag relativamente a quello emesso dal reader, si verificano difficoltà nella ricezione del segnale da parte di quest'ultimo. I due segnali infatti, quello del reader e quello del tag, avrebbero la stessa frequenza. Per consentire al reader di rilevare più agevolmente il segnale del tag viene spesso usata, nel processo di modulazione del tag, una sottoportante che sposta lo spettro del segnale modulato dal tag lontano dalla frequenza della portante (generata dal reader). Questa sottoportante è rilevabile con maggior facilità dal reader medesimo attraverso opportuno filtraggio. La risposta dei tag passivi all'interrogazione del reader si basa su opportuna "modulazione" del segnale ricevuto. La potenza disponibile per essere ritrasmessa al reader risulta quindi estremamente ridotta e conseguentemente il livello del segnale di risposta è più simile al rumore di fondo che a quello del segnale emesso dal reader. I differenti metodi di modulazione utilizzati possono essere classificati a seconda che i segnali di risposta siano o meno nella stessa banda del segnale ricevuto:

- **tecniche in banda:** in cui la variazione del carico o il backscatter interessano direttamente la frequenza portante emessa dal reader.
- **tecniche fuori banda:** in cui la variazione del carico o il backscatter interessano una sottoportante, generata dal tag, che si discosta dalla portante emessa dal reader.

Una problematica delle tecniche in banda è che il reader ed il tag non possono trasmettere dati contemporaneamente. Durante la trasmissione del tag, infatti, il reader deve inviare una frequenza non modulata al solo scopo di alimentare il tag medesimo (HDX) oppure il tag deve sfruttare energia accumulata (SEQ). Inoltre vi è un periodo di tempo necessario affinché il sistema transiti dallo stato in cui trasmette il reader a quello in cui trasmette il tag e viceversa. Da ultimo, per confinare la risposta dei tag nella banda di lavoro, la velocità dei dati trasmessi dal tag deve essere mantenuta approssimativamente uguale alla velocità del reader e quindi relativamente bassa. Questa caratteristica è realizzata tipicamente con una codifica digitale in banda base che risulta essere meno robusta al rumore rispetto a tecniche alternative. Ricordando che le emissioni dei tag possiedono livelli di potenza estremamente bassi, l'uso delle tecniche fuori banda determina indubbi

vantaggi nella progettazione di un sistema RFID; reader e tag, infatti, possono trasmettere dati contemporaneamente (FDX). In tal modo si realizza un sistema full duplex eliminando anche i periodi di tempo necessari al sistema per invertire il senso della trasmissione. Infine, migliorando il rapporto segnale/rumore, un reader può ricevere segnali di backscatter da tag disposti a distanze più elevate rispetto a quelle ottenibili da sistemi con risposta in banda. In conclusione si può affermare che le metodologie di risposta di backscatter in banda pongono ostacoli alla progettazione dei reader che invece vengono minimizzati nelle tecniche fuori banda.

Sistemi RFID FDX, HDX e SEQ

La comunicazione e il trasferimento di energia tra reader e tag avviene secondo uno dei seguenti schemi: full duplex (FDX), half duplex (HDX) and sequential (SEQ).

- Nel **sistema FDX** il trasferimento dati dal reader al tag (down-link) avviene contemporaneamente al trasferimento dati dal tag al reader (uplink), mentre il trasferimento di energia dal tag al reader è continuo, indipendentemente dal verso di trasferimento dei dati.

- Nel **sistema HDX** il trasferimento dati dal reader al tag (down link) si alterna al trasferimento dati dal tag al reader (uplink), mentre il trasferimento di energia dal tag al reader è anche in tal caso continuo (attraverso una portante non modulata), indipendentemente dal verso di trasferimento dei dati.

- Nel **sistema SEQ** il trasferimento di energia dal reader al tag avviene invece (contemporaneamente al trasferimento dati dal reader al tag) in periodi temporali determinati, mentre il trasferimento dati dal tag al reader avviene negli intervalli intercorrenti tra i precedenti, sfruttando energia accumulata dal tag.

Risulta evidente che la scelta di uno degli modi di comunicazione sopra citati sia vincolata in maniera determinante dalle tecnologie RF utilizzate. In particolare l'utilizzo di tecniche

di comunicazione fuori banda rende possibile la realizzazione di sistemi FDX, che invece è preclusa dall'uso di tecniche in banda [8].

2.7.3 Protocolli anticollisione nella comunicazione Reader↔Tag

Quando si lavora in ambienti con molteplicità di tag o reader che operano nello stesso tempo, sorgono i classici problemi di conflitti tra apparati nelle comunicazioni wireless. Il problema presenta due aspetti speculari:

- Tutti i tag risponderebbero contemporaneamente ad una interrogazione di reader ricevuta correttamente.
- I singoli tag dovrebbero rispondere contemporaneamente a tutti i reader che li hanno interrogati. Naturalmente in queste condizioni la comunicazione non può avvenire con successo, pertanto vanno presi provvedimenti affinché nessuno di questi due casi si verifichi.

In questo caso essi replicherebbero alle interrogazioni tutti nello stesso momento. Questo provocherebbe inevitabilmente collisioni e perdite di dati. È quindi necessario implementare nei tag algoritmi anti collisione, in modo che le loro risposte possano essere ordinate temporalmente e riconosciute individualmente. Il numero di tag che può essere identificato all'interno della distanza operativa di un reader dipende dal bitrate dei tag (che dipende anche dalla frequenza operativa) e dal protocollo anticollisione. Una volta che il singolo tag è stato identificato, il reader può indirizzarlo singolarmente e compiere operazioni su di esso senza interferire con i tag vicini. Tra le operazioni più comuni, se il tipo di tag lo permette, vi è la scrittura di parti della memoria, oppure la predisposizione del protocollo anti-collisione affinché tenga in standby il tag per un po' di tempo, onde non interferire con altri tag non ancora identificati. Devono essere attuate tecniche di sincronizzazione tra reader affinché non si verifichino interrogazioni contemporanee in un ambiente in cui sono presenti più reader. Problemi legati alla disponibilità di banda ed alle potenze impiegate hanno condotto Europa e Stati Uniti a definire due approcci completamente differenti alla sincronizzazione tra reader. Tali approcci vanno sotto il nome di "Listen Before Talk - LBT" in Europa e "Frequency Hopping" negli USA. Esistono due classi fondamentali di protocolli anti-collisione, derivati direttamente dalle

tecnologie delle wireless LAN, la classe dei protocolli deterministici e quella dei protocolli probabilistici. Nell'ambito dei protocolli che gestiscono le "collisioni" tra trasmissioni simultanee da una molteplicità di tag, il cosiddetto "Binary Decision Tree" appartiene alla classe dei protocolli deterministici mentre i cosiddetti "ALOHA" e "slotted ALOHA" appartengono alla classe dei protocolli probabilistici. Mentre il protocollo "Binary Decision Tree" è realizzato dal reader attraverso interrogazioni ripetute dei tag, i protocolli "ALOHA" e "slotted ALOHA" sono realizzati dai tag per rispondere ad una interrogazione da parte del reader. Il protocollo "Binary Decision Tree" ha l'obiettivo di identificare tag con identificatori uguali ad un prefissato numero binario. Il protocollo di tipo probabilistico ALOHA (sviluppato dall'Università delle Hawaii) prevede che il tag trasmetta il proprio messaggio e se il messaggio non va a buon fine il tag effettua un nuovo tentativo di trasmissione, autonomamente (dopo avere atteso un certo periodo di tempo) o a seguito di una nuova interrogazione da parte del reader. I tentativi di trasmissione proseguono fino a che la trasmissione del messaggio va a buon fine. Il protocollo "slotted ALOHA" prevede invece una sorta di discretizzazione degli istanti in cui i tag possono iniziare a trasmettere un pacchetto di dati. Questo comporta che se non vi è collisione nell'istante iniziale, il pacchetto sicuramente non subirà collisione durante la sua trasmissione. I protocolli ALOHA sono relativamente veloci nell'identificazione di un particolare tag nell'ambito di un insieme numeroso. Inoltre una maggiore efficienza può essere raggiunta con l'impiego aggiuntivo di tecniche di tipo Listen Before Talk (LBT). Queste prevedono che il reader verifichi che il canale di trasmissione sia libero prima di effettuare un'interrogazione, evitando così di interrompere una trasmissione in corso.

Un parametro essenziale per le prestazioni di un sistema RFID ad alta densità di tag è la velocità di identificazione ovvero la rapidità con la quale un reader identifica ciascuno dei tag che ricade nel proprio raggio d'azione. Se la velocità di identificazione è sufficientemente alta, si dovrebbe pervenire ad una prestazione molto richiesta, consistente nella lettura "in movimento" delle etichette, ad esempio prodotti contenuti in una pallet in transito su carrello o di bagagli su un nastro trasportatore. In mancanza di protocolli complessi (tag di prima generazione), la velocità di identificazione dipende essenzialmente da due fattori: l'efficienza del protocollo anticollisione ed il bitrate

prodotto dal tag. Il processo di identificazione nei tag passivi più moderni (Gen2 nelle bande UHF) avviene anche combinando il protocollo anticollisione (Slotted ALOHA) con una tecnica di "selezione" che divida in due parti la popolazione dei tag sulla base di determinate caratteristiche, limitando di conseguenza il numero di tag che possono collidere. Altri metodi efficaci consistono nel:

- "mettere a dormire" (put to sleep) per qualche tempo i tag che hanno risposto, evitando che interferiscano con la comunicazione verso gli altri. Questo modo di operare, però, crea problemi in quanto più lettori che operano nella stessa area, non possono sapere se un tag è stato "silenziato" da un altro reader.
- Generare delle risposte tronche da parte dei tag che risultino più veloci, trasmettendo solo una parte dell'identificativo o dell'EPC. Questa tecnica trova impiego in ambienti dove tutti i tag posseggano identificativi con parti comuni. Sfruttando queste possibilità i costruttori possono realizzare varie strategie di identificazione.
- **Listen Before Talk & Adaptive Frequency Agility:** nella tecnica LBT il reader deve ascoltare prima di trasmettere verificando che altri apparati non stiano già occupando il canale prescelto. Se il canale è occupato il reader deve attendere oppure tentare l'occupazione di un altro canale scelto tra un insieme di canali disponibili nel caso in cui si sia adottata la cosiddetta opzione di "Adaptive Frequency Agility" – AFA. La normativa europea definisce occupato un canale su cui sia presente un segnale di:

  -96 dBm se la potenza dell'interrogazione sia di 2 W

  -90 dBm se la potenza dell'interrogazione sia di 500 mW

  -83 dBm se la potenza dell'interrogazione sia di 100 mW

  Nell'ambito dell'impiego delle tecniche LBT/AFA, un uso più efficiente e mediamente equidistribuito tra i contendenti dei canali disponibili viene raggiunto imponendo un limite sul tempo massimo in cui il reader può occupare uno stesso canale e sul tempo minimo che deve attendere prima di rioccupare lo stesso canale (se disponibile). Per aumentare la capacità del lettore di operare in ambienti con congestione, rumori o interferenze, si può anche prevedere l'uso di uno di

quattro differenti rate di codifica per sotto-portante per variare la larghezza di banda del canale.

- **Frequency Hopping:** la tecnica utilizzata negli USA è basata sul salto di frequenza che consente di ottenere un elevato grado di efficienza. I trasmettitori in contesa non possono occupare una frequenza per più di un periodo di tempo molto ridotto (meno di mezzo secondo). Tuttavia, al termine di tale periodo di tempo, non devono necessariamente spegnersi (come nel caso del "Duty Cycle") ma sono obbligati a saltar su una frequenza differente con scelta casuale. L'effetto complessivo è che tale metodo risulta molto efficiente sia nel caso in cui sia presente un solo reader, sia in quello in cui siano presenti più reader. Nel primo di questi due casi è consentito all'unico reader presente di avere un tasso di utilizzazione della banda del 100% fino al completamento della sua emissione (che però avviene saltando su frequenze diverse). Nel secondo caso in cui sono presenti più trasmettitori, poiché le frequenze sono occupate in maniera casuale l'accesso diventa una questione di media probabilistica che si traduce in un'uniforme ripartizione tra tutti i trasmettitori dell'uso delle frequenze e della probabilità di trasmettere su una frequenza già occupata. In situazione di affollamento un reader costretto a saltare di frequenza troverà, con probabilità elevata, la nuova frequenza occupata e sarà costretto a riprovare fino a che non troverà una frequenza disponibile. Per assicurare buone prestazioni,è necessario assicurare un'ampia banda disponibile divisa in numerosi canali. Prove effettuate anche su pochi canali, sembrano mettere in evidenza che il modello fornisca prestazioni migliori del modello LBT. La modalità Frequency Hopping non porta a grandi complicazioni sia sul lato tag che su quello reader.

  Il tag, infatti, opera come un riflettore passivo (backscatter) intrinsecamente a larga banda, non risente pertanto dei salti della frequenza di interrogazione.

  La sezione ricevente del reader, per parte sua, recepisce automaticamente ogni cambio di frequenza del segnale emesso, in quanto la conversione di frequenza nel ricevitore condivide lo stesso oscillatore locale del trasmettitore. Le due tecniche di LBT e Frequency Hopping prevedono entrambe delle regole per limitare

l'occupazione del singolo canale radio. Queste procedure, che limitano il ciclo di lavoro di un trasmettitore su un singolo canale vanno sotto il nome di "Duty Cycle". La tecnica basata sul "Duty Cycle" prevede che un trasmettitore possa emettere ininterrottamente per non più di un breve periodo di tempo, al termine del quale dovrà spegnersi per consentire l'accesso alla frequenza da parte di altri trasmettitori in attesa. Per continuare la trasmissione dovrà attendere un certo periodo prima di tentare nuovamente di accedere alla frequenza [8].

2.8 CARATTERISTICHE DEI TAG

A questo punto entriamo nel dettaglio delle caratteristiche dei Tag, differenziati per tipologia e frequenza di utilizzo.

2.8.1 Tag passivi per frequenze HF

- Frequenza operativa: 13.56 MHz.
- Stardard di riferimento: ISO/IEC 15693–ISO 14443 A/B.
- Disponibili nelle versioni Read Only, Read/Write.
- Velocità trasferimento dati tipica: 106 Kbit/s.
- Distanza di lettura: a seconda della dimensione dell'antenna si stima la massima distanza di lettura compresa tra 0.1 m e 1.5 m, fino a un massimo di circa 1.8 m usando antenne a varco; la distanza di scrittura è tipicamente inferiore.
- Capacità di letture multiple: fino a 30÷50 Tag/s a seconda del modello e del protocollo anticollisione utilizzato dal Reader.
- Memoria: tipicamente da 32 a 64 bits di memoria riservata per il TID, ai quali vanno aggiunti opzionalmente fino a 10 Kbits di memoria programmabile.
- Dimensioni: variabili nel range (15÷200 mm) × (15÷150 mm) / Ø (7÷50 mm), con uno spessore che varia da 0.8 mm per le Smart Labels a 20 mm per i Tag inseriti in contenitori plastici.
- Temperatura di utilizzo: da −40 a un massimo di +120 flC.

- Applicazioni: i Tag inseriti all'interno di un'etichetta plastificata o di carta, adesiva e stampabile (o termo-trasferibile), sono tipicamente in uso per applicazioni di tracciabilità (pallets, contenitori riutilizzabili anche sottoposti a cicli di lavaggio), antitaccheggio, logistica, gestione di magazzini, librerie e biblioteche; i Tag inseriti in contenitori platici o di vetro, resistenti all'acqua, sostanze chimiche, acidi e oli, sono utilizzati in magazzini, strutture sanitarie, servizi alberghieri e industriali per il controllo dell'accesso di veicoli, l'autenticazione, la gestione di attività di tracciamento oggetti e la logistica.

  Il mercato dei Tag passivi HF ha poi sviluppato le forme più svariate per i packages, in funzione degli specifici obiettivi degli utenti: rivetti di acciaio inossidabile per la tracciabilità dei prodotti dal settore alimentare fino a quello dei prodotti in pelle; viti in acciaio per controllare l'efficienza dei pali dell'illuminazione stradale, identificare cassonetti per la raccolta dei rifiuti urbani, monitorare apparecchiature in esterno; adesivi speciali per l'impiego a contatto di superfici ostili o metalliche; bags in poliestere per l'identificazione dell'abbigliamento nelle lavanderie industriali (un singolo Tag garantisce la resistenza a oltre 70 cicli di lavaggio).

2.8.2 Tag semi-passivi per frequenze HF

- Frequenza operativa: 13.56 MHz.
- Standard di riferimento: ISO/IEC 15693.
- Memoria: equipaggiano memorie di dimensione variabile a seconda delle applicazioni (diversi Kbytes di memoria EEPROM).
- Tensione di alimentazione: 3.9÷6 Vdc, tipicamente batteria al litio ricaricabile (autonomia 500h), o supercapacità ricaricabile (autonomia 24h).
- Sensori di temperatura (ad es. range di misura da -40 flC a +70 flC, accuratezza: ±1 flC, risoluzione: 0.03125 flC) e di accelerazione/vibrazione interni (es.: range di misura da -6g a 6g , errore zero-g ±10%).

- Dimensioni: variabili, caratterizzati da un contenitore profondo alcuni centimetri per permettere l'alloggiamento dei sensori e delle batterie.
  Peso: <100 gr.
- Temperatura di utilizzo: da -40 flC a +70 flC.
- Applicazioni: impiegati nella logistica per il controllo del mantenimento della temperatura costante e per la verifica dello storico delle sollecitazioni meccaniche subite dai prodotti trasportati; controllo delle condizioni termiche durante le fasi di produzione e distribuzione di prodotti facilmente deperibili (ad es. nel settore alimentare e farmaceutico).

2.8.3 Tag passivi per frequenze UHF

- Frequenze operative: 865÷928 MHz, 2.45 GHz.
- Standard di riferimento: EPC Global Class1 Gen2/ISO 18000–6B compatibili.
- Memoria disponibile: varia a seconda dello standard e del modello. Tipicamente i Tag sono equipaggiati con 96 bits di memoria EPC, 32/64 bits di memoria TID; opzionalmente possono possedere una memoria utente fino a 1728 bits
- Dimensioni: variabili nei range (6÷150 mm) × (12÷210 mm); per i Tag incapsulati lo spessore del contenitore varia tra i 3 mm e alcuni centimetri.
- Capacità di letture multiple: fino ad alcune centinaia di Tags/s, in dipendenza dal tipo di Tag e di Reader utilizzato.
- Temperatura di utilizzo: da -40flC a +85flC.
- Applicazioni tipiche: tracciamento di pallet, contenitori metallici, contenitori plastici riutilizzabili (RPC), commercio al dettaglio, gestione della supply chain in genere, attività di logistica e magazzino (inventory management) e controllo della qualità, gestione di strutture sanitarie, servizi alberghieri e industriali, operazioni di pagamento delle tariffe autostradali e controllo di accesso ad aree protette. A seconda delle caratteristiche del contenitore offrono resistenza a sostanze chimiche, acidi e oli, basso assorbimento di acqua e permeabilità al vapor acqueo. I packages sono realizzati in maniera tale da adattarsi alle diverse superfici, offrendo isolamento dai metalli e dai materiali riflettenti in genere.

- Distanza di lettura: la tabella successiva mostra le performance, in termini di range di lettura, di alcuni tipi di Tag, a contatto con diverse superfici: plastica, metallo (contatto diretto, a distanza di 15 e 30 mm con interposizione di materiale isolante), vetro, cartone, compensato, e in spazio libero.

  I Tag che sono stati presi in considerazione per queste misurazioni sono:

  - Tag per container (1.82 cm × 8.82 cm × 0.43 cm).
  - Tag per container incapsulato in contenitore isolante plastico (3.25 cm × 10.49 cm × 3.17 cm).
  - Tag per container incapsulato in contenitore metallico (1.49 cm × 20.95 cm × 0.45 cm).
  - Tag specifico per RPC (Contenitori Plastici Riutilizzabili) (2.15 cm × 8.82 cm × 4.69 cm).
  - Intelligent ID Card: Tag specifico per applicazioni di monitoraggio a lungo raggio dell'accesso ad aree protette (5.39 cm × 8.57 cm × 0.07 cm).
  - Sticker Tag per parabrezza: ottimizzato per le operazioni di pagamento di pedaggio autostradale, o per regolamentare l'accesso a zone di parcheggio (4.59 cm × 7.89 cm × 0.12 cm).
  - Tag per applicazioni free-space (4.59 cm × 7.89 cm × 0.12 cm).

  Tutti i Tag funzionano alla frequenza di 915 MHz (Stati Uniti). Inoltre sono riportati i risultati delle stesse misurazioni eseguite su tre Tag funzionanti alla frequenza di 2.45 GHz, progettati appositamente per minizzare le dimensioni del dispositivo:

  - Free Space Tag: ottimizzato per l'utilizzo in spazio libero (0.59 cm × 2.99 cm × 0.5 cm).
  - Metal Mount Tag: progettato per l'applicazione su superfici metalliche o riflettenti in genere, e dotato di una limitata flessibilità (0.95 cm × 8.12 cm × 0.72 cm).
  - Metal Mount Insert: il cuore del prodotto precedente, adatto ad essere incapsulato in diversi tipi di contenitori (0.95 cm × 8.12 cm × 0.12 cm).

Materiale:	Plastica	Metallo: contatto	Metallo: 15 mm	Metallo: 30 mm	Vetro	Cartone	Compensato	Spazio Libero
Tag funzionanti alla frequenza di 915 MHz (read range in metri)								
Tag per container	1.40	0.15	0.15	0.30	2.50	1.10	1.85	1.10
Tag per container: contenitore plastico	2.95	0.10	0.25	0.60	1.55	2.80	2.50	4.00
Tag per container: contenitore metallico	3.85	3.00	2.50	2.80	4.00	4.00	3.70	4.00
Tag RPC	3.00	0.30	1.10	1.55	1.25	2.00	2.15	1.85
Intelligent ID Card	1.10	0	0	0.10	0.50	2.30	0.45	2.80
Tag per parabrezza	1.00	0	0	0.75	3.70	1.00	1.70	1.00
Tag per free-space	1.25	0	0	0.15	1.25	3.40	3.00	3.75
Tag funzionanti alla frequenza di 2.450 GHz (read range in centimetri)								
Free Space	56	0	0	15.25	13	40.5	43	40.6
Metal Mount I.	61	0	28	51	18	48	40.6	45.7
Metal Mount	53	96.5	110	127	38	71	51	71

Tabella 2.6 - Distanze di lettura per diversi tipologie di Tag UHF a contatto con differenti materiali

2.8.4 Tag semi-passivi per frequenze UHF

- Frequenze operative: 860÷960 MHz, 2.45 GHz.
- Standard di riferimento: EPC Global Class3.

- Memoria disponibile: tipicamente 64 Kbits.
- Operazioni consentite: Read Only, Read/Write.
- Dimensioni: variabili in relazione alla forma del package; in genere <10 cm per lato e alcuni centimetri di spessore.
- Durata della batteria: 3÷5 anni.
- Velocità di trasferimento dati tipiche: 8, 32, 48 Kbits/s (Reader-Tag), 2, 8, 32 Kbits/s (Tag-Reader).
- Distanza di lettura: 0÷100 m.
- Applicazioni: tracciamento e controllo di pallets e container in condizioni ambientali sfavorevoli, in presenza di liquidi, metalli e superfici riflettenti in genere, laddove l'impiego di Tag passivi, anche per il loro ridotto range di lettura, sarebbe impraticabile.

2.8.5 Tag attivi per frequenze UHF

- Frequenze operative: l'intera banda UHF con la possibilità di adattarsi alle normative in materia dei vari paesi.
- Memoria: da 64 byte a 8 KB (espandibile a 32 KB).
- Dimensioni: variabili, a seconda del package. In genere misurano alcuni centimetri di lato e hanno uno spessore che varia da pochi millimetri a qualche centimetro. Il peso può raggiungere anche alcune centinaia di grammi.
- Distanza di lettura: da 6 m fino a 100 m a seconda dei modelli
- Letture multiple: capacità di lettura fino a 100 Tag/s, identificazione simultanea di 2000 Tag.
- Durata della batteria: 5-6 anni, grazie anche al protocollo di comunicazione che prevede il controllo della trasmissione da parte della specifica applicazione, evitando lo scambio continuo di dati (comunicazione on-demand), e alla progettazione specifica per il bassissimo consumo di energia (prodotti broadcast).
- Applicazioni: identificazione automatica, tracciabilità e rintracciabilità, localizzazione di persone e beni anche tramite comunicazione wireless tra i vari

dispositivi, capaci di realizzare la triangolazione 'on-board', controllo di temperatura (tramite i sensori di cui il Tag è equipaggiato). La versione broadcast dei Tag attivi permette la memorizzazione statica dei dati e la loro trasmissione continua a intervalli programmabili (ping rate), senza alcuna richiesta proveniente dal controller.

2.9 CONSIDERAZIONI SULLA SCELTA TECNOLOGICA

In questo paragrafo vengono fornite le indicazioni di massima da seguire nella realizzazione di un progetto RFID.

La scelta della tecnologia da utilizzare risulta essere un punto cruciale nella realizzazione di un sistema RFID perfettamente funzionante in un dato ambiente operativo. Da essa ne dipendono la buona riuscita del progetto, il corretto funzionamento in ogni circostanza anche in presenza di disturbi, la possibilità di sfruttarne appieno le potenzialità offerte. Per questo motivo l'affermarsi di normative sempre più precise e scrupolose, danno la sicurezza di effettuare scelte corrette a chi vuole fare di questa nuova tecnologia un punto di forza della propria impresa. Quanto studiato e sperimentato permette di poter indicare quelli che sono alcuni aspetti importanti da tenere sotto attenta considerazione :

- **Materiali con cui il Tag deve operare:** come verrà osservato nei test effettuati in laboratorio, il materiale con cui il tag è posto a contatto può essere fonte di forte degradazione delle prestazioni, pertanto la scelta delle frequenze deve tenere conto di questo aspetto pena il completo fallimento del sistema. Maggiore sarà la frequenza operativa e tanto maggiore sarà l'influenza subita da metalli e liquidi.
- **Distanze operative attese:** nella fase di progettazione devono essere stabilite le aspettative di funzionamento in termini di distanze di lettura/scrittura poiché ad ogni tecnologia ed ancor più nel particolare ad ogni package corrispondono raggi di copertura molto differenti. Tendenzialmente maggiori con l'aumentare della frequenza e della dimensione delle antenne.

- **Ambiente del sistema:** questo aspetto và analizzato profondamente in fase di progetto perché una delle principali cause di problemi (e spesso non può neppure essere eliminata) è proprio la presenza di forti disturbi in radio frequenza, che vanno ad occupare una banda fondamentale come quella di trasmissione della portante o dei toni di modulazione dei tag, rendendo di fatto la comunicazione impossibile.
- **Necessità di sola identificazione dell'oggetto o bagaglio dati:** talvolta è sufficiente la sola identificazione dell'oggetto o della persona per mezzo del codice identificativo, anche perché scelte di sicurezza possono rimettere i database in appositi server destinati a questo utilizzo. Altre volte si decide di realizzare un insieme di dati che accompagnano l'etichetta e che possono essere modificati durante il percorso. La scelta del tag deve rispecchiare tali necessità, andando ad analizzare i datasheet del produttore scelto per trovare il più adatto in termini di capacità di immagazzinamento dati ovvero dimensione della memoria.
- **Velocità richieste:** ogni utilizzo di tag RFID prevede quantomeno la loro lettura (e probabilmente scrittura) in un contesto più ampio di identificazione automatica. La velocità con cui tali operazioni vengono effettuate varia a seconda delle frequenze utilizzate, del Reader usato, dei tag scelti. Nel progetto si deve individuare con precisione il tempo minimo di permanenza dell'etichetta nell'area di illuminazione dell'antenna, in modo da poterne permettere l'attivazione e la lettura (o scrittura) senza che essa vi fuoriesca prima che il processo sia concluso. A tal fine vengono forniti nei datasheet i tempi teorici minimi di un dato tag.
- **Sicurezza e anticollisione:** un aspetto che può essere estremamente importante quando il sistema RFID viene sviluppato come controllo agli accessi, pagamento automatico di prodotti, o ogni altra applicazione che possa prevedere la totale ed unica identificazione del tag senza possibile manomissione da terze parti, anche in un contesto di presenze multiple. Ogni tecnologia si attiene a standard differenti che offrono prestazioni in termini di sicurezza e anticollisione che vanno analizzati caso per caso in modo da trovare quella che risulta più adatta al progetto in fase di realizzazione.

- **Costi**: vanno analizzati in funzione dell'obiettivo che si vuole raggiungere e sono costituiti oltre che progetto e certificazioni varie, principalmente dall' hardware e software scelto (il costo dei tag và da pochi centesimi di euro a diverse decine di euro). Una scelta attenta di una frequenza piuttosto che un'altra, di un Reader aggiornabile (ad esempio nel firmware), possono costituire un'arma vincente poiché in un ambiente in continua espansione come l'RFID sbagliare tecnologia può significare trovarsi nel giro di qualche tempo con un sistema ormai obsoleto.
- **Tecnologie proprietarie o standard liberi:** può capitare che una particolare soluzione proprietaria rispecchi in modo più preciso alle esigenze di progetto. Questa scelta può trovare motivo quando il sistema è costruito per operare singolarmente o in condizioni particolari che ne vincolano le scelte. Quando le condizioni lo permettono, e soprattutto quando deve entrare a fare parte di un progetto ben più ampio le scelte sarebbe opportuno ricadessero su standard liberi, ovvero standard di fatto che trovano impiego anche presso i partner commerciali correlati. Molte soluzioni offrono compatibilità multiple pertanto vanno preferite.
- **Modifica radicale o integrazione**: il sistema RFID progettato può rappresentare un tentativo radicale di modifica dell'assetto produttivo o gestionale di un'impresa, o il tentativo di assorbire la tecnologia per cause esterne, talvolta dettate dal mercato. Le scelte su quale frequenza utilizzare vengono condizionate fortemente da questo perché se in una totale modifica possono essere fatte valutazioni più precise in termini RFID, nell'integrazione devono essere osservati tutti gli aspetti dovuti alla compatibilità con le apparecchiature presenti, i database, le interfacce offerte dai vari dispositivi già istallati (sia software che hardware).
- **Normative vigenti:** rispettare scrupolosamente le normative vigenti nel paese di istallazione o dei paesi dove risiedono i partner commerciali, può spesso vincolare le scelte.

In generale si possono riassumere per ogni frequenza operativa i seguenti aspetti evidenziando dove possibile un tag idoneo tra quelli testati:

9-135KHz: accoppiamento di tipo induttivo (magnetico), hanno un raggio operativo per transponder passivi che varia dal "contatto" fino ai 2 metri, dipendente dal lettore e dalla forma delle antenne. Nei sistemi con transponder attivi si possono superare i 2 metri. Sono disponibili sia nel tipo read only che read write. La capacità di trasporto dati varia da 64 bit fino a 2Kbit. Hanno bassa velocità di trasferimento dati, generalmente da 200 bit/sec fino a 1 Kbit/sec. Il tempo di lettura dipende dalla quantità dei dati da trasferire e dalla velocità di trasmissione attiva. Per un transponder da 96 bit a 1 Kbit/sec occorrono circa 0,10 sec per la lettura. Sono disponibili sia per letture singole che con meccanismi anticollisione. Presenti in diversi formati e package, dalle capsule in vetro ai boli ceramici per la tracciabilità animale, dalle etichette ai dischi "rinforzati" per l'identificazione dei prodotti o di mezzi meccanici (treni, macchine, ecc…). Questa classe di frequenze si riferisce agli standard ISO 11784/85 e ISO 14223. Generalmente utilizzata per la rintracciabilità animale (Glass 23 mm), il controllo accessi (LF Card), l'identificazione di veicoli, treni o container (Disk 30mm), immobilizer per auto (KeyRing, Wedge), lavanderie (Glass 32 mm), ecc… La comunicazione attraverso liquidi e/o tessuti organici non è ridotta significativamente. I transponder sono particolarmente sensibili all'orientamento.

13,56MHz: accoppiamento induttivo (magnetico), sono principalmente di tipo passivo con un raggio attivo massimo di 1,5 metri per la lettura, inferiore per la scrittura. Le distanze dipendono dal Reader, dalle sue antenne, nonché dalla dimensione dell'antenna del tag. Sono disponibili sia del tipo read only che read write, spesso di questo ultimo tipo con memoria che varia da 64 bit a decine di Kbit. Dispongono di un codice identificativo che può essere soltanto letto. Hanno una velocità di trasferimento del dato di circa 25 Kbit/sec, che risulta essere estremamente efficiente poiché nel caso tipico per trasferire 512 bit occorrono 0,02 secondi. Sono sempre forniti con meccanismo anticollisione per un massimale in lettura di 50 tag, dipendente dal software impostato e dalle caratteristiche delle antenne del lettore. Sono prodotti in una vastissima varietà e consentono di poterli applicare praticamente ovunque e per qualsiasi applicazione. Il formato più comune è la "smart label" dove etichetta e transponder sono integrate. Questa classe di frequenza si riferisce agli standard ISO 18000-3, ISO 14443 A/B e ISO 15693. Le applicazioni vanno

da servizi logistici, controllo accessi (ISO Card Badge, Key Fob), ticketing (Tag-it, Tag-ISO), lavanderia (Laundry Tag), tracciabilità prodotti (Tag-ISO, Smart Label), controllo di produzione, videostore (Tag-it, Tag-ISO), ecc… Sono mediamente sensibili a liquidi e a tessuti organici, vengono influenzati nelle prestazioni dalla presenza di metallo nelle vicinanze.

300-1200MHz: accoppiamento di tipo elettromagnetico, generalmente i transponder UHF sono utilizzati in forma passiva ed operano in intervalli fino a 3 metri o più, in modalità lettura, dipendente dalla configurazione del sistema. Il raggio operativo è influenzato dalla regolamentazioni di potenza, in Italia attualmente tale tecnologia, con potenze superiori a 25 mW ERP, è vietata, se non espressamente autorizzata dal ministero competente. Sono disponibili sia in sola lettura che lettura/scrittura, con una memoria da 64 bit fino a decine di Kbit. Dispongono di un codice identificativo che può essere solo letto. La velocità di trasferimento dati è di circa 28 Kbit/sec, ma iniziano ad essere commercializzati dispositivi da 100 Kbit/sec. Il tempo di lettura con 28 Kbit/sec e 512 bit di dato da trasferire è di circa 0,02 secondi. Sono sempre forniti con meccanismo anticollisione per un massimale in lettura di circa 100 transponder contemporanei dipendente dal software impostato e dalle caratteristiche del lettore e delle antenne. Le nuove specifiche EPC Class1/Gen2 consentiranno una lettura di circa 100-1500 transponder/sec. Sono prodotti in una grande varietà e consentono di poterli applicare anche ad unità metalliche. Il formato più comune è la "smart label" dove etichette e tag sono integrate. Questa classe di frequenze si riferisce agli standard EPC Class0, Class1, Class1/Gen2 e ISO 18000-6. Le applicazioni vanno dalla tracciabilità dei pallets, logistica della filiera e di fornitura, pedaggi autostradali, bagagli (USA), ecc… Le prestazioni sono notevolmente ridotte in presenza di metalli, liquidi, tessuti organici ed umidità.

2,4 o 5,8GHz: accoppiamento di tipo elettromagnetico, il raggio operativo nel caso passivo è al massimo di qualche metro, nel caso attivo possono raggiungere anche i 50-70 metri. Sono disponibili in sola lettura o lettura/scrittura con memoria da 128 bit a decine di Kbit. La velocità di trasferimento dati è estremamente elevata, posso arrivare anche a 1 Mbit/sec in casi particolari. Tipicamente intorno a 100-250 Kbit/sec. Il tempo di lettura risulta pertanto piuttosto ridotto, per esempio a 100 Kbit/sec occorrono 0,03 secondi per

leggere 32Kbit, bastano 0,05 secondi per leggere alcune decine di transponder da 128 bit. Sono disponibili sia dispositivi a letture singole che con anticollisione. I formati sono diversi, comprendono anche particolari realizzazioni per l'applicabilità su metalli. Lo standard di riferimento è ISO 18000-4. Indispensabili quando la lettura deve essere eseguita su oggetti in movimento estremamente veloci (come il telepass sulle autostrade italiane). L'utilizzo tipico sono il pagamento pedaggi, il controllo accessi e la logistica veicolare. Le prestazioni sono fortemente ridotte in presenza di liquidi, metalli, tessuti organici e umidità.

Operata la scelta di quale frequenza utilizzare nel sistema RFID osservati tutti gli aspetti presentati in precedenza, occorre anche determinare il migliore posizionamento del transponder in funzione della sua sensibilità al materiale dell'oggetto. Alcuni punti da seguire sono:

- Determinare se il materiale da imballaggio della parte esterna sia RF trasparente: se il materiale da imballaggio è un contenitore di cartone, è RF trasparente. Se l'imballaggio contiene il metallo, non è RF trasparente. Occorre prediligere imballaggi dei quali si conosce la bassa influenza per l'etichetta, ottenendo le migliori prestazioni in termini di letture corrette o occorre sopperire con opportune sintonizzazioni o etichette fatte specialmente per il metallo.
- Se il materiale da imballaggio è RF trasparente: aprire il contenitore e controllare visivamente il contenuto. Quel che è probabile trovare è una varietà di materiali riflettenti ed assorbenti. Per esempio, aprendo una cassa di deodorante, l'etichetta sul deodorante dovrebbe essere di tipo idoneo per metalli poiché il flacone renderebbe invisibile una semplice etichetta, inoltre la massa del prodotto è un liquido contenente ossido di alluminio. Il tappo e le valvole sono tutti di plastica e può esserci spazio libero nella parte superiore o materiale da imballaggio per proteggerli.
- Determinare dove il prodotto è posizionato sulla piramide RFID (fig 3.14): per l'esempio del deodorante, con l'uso di etichette per metallo, posizionerebbero il prodotto flacone (metallo) nell'angolo in basso a destra della piramide perché si è

in presenza di materiali molto riflettenti. La combinazione di liquido e di alluminio sarebbe vicino alla zona centrale nella parte inferiore perché presente sia assorbimento che riflessione. Occorre osservare e posizionare tutti i materiali presenti.

- Determinare dove il contenuto è posizionato sulla piramide RFID (fig 3.14): allineare tutte le posizioni in zone differenti dell'oggetto nella piramide RFID ottenendo un indicazione media di come l'insieme (il singolo prodotto o tutta la scatola) si comportano in RF.
- Effettuare una fase di test cercando il posto più idoneo per il posizionamento del Tag: per esempio, sulla cassa del deodorante, la posizione certamente più idonea sulla singola latta è quella che si trova sul tappo plastico poiché non influenza negativamente la RF, mentre per l'intera scatola resta certamente la parte superiore perché presenta al di sotto una zona d'aria, con materiali plastici e da imballaggio che isolano l'etichetta dal metallo. In molti casi è sufficiente lo strato di cartone.

Il posizionamento dell'etichetta può essere effettuato in modo automatico o manuale dal personale addetto, ma resta un punto da non sottovalutare perché spesso è la causa della mancata identificazione del prodotto [7]. I test condotti in laboratorio hanno dimostrato come a 13,56 MHz la presenza di oggetti non metallici non costituisca alcun problema per l'identificazione, tuttavia soltanto dell'attenuazione, ma l'etichetta a contatto del metallo non viene riconosciuta, e a estrema vicinanza abbatte le distanze di lettura.

3 WIRELESS SENSOR NETWORKS

Le reti di sensori wireless (*Wireless Sensor Networks*) costituiscono un'importante area di ricerca di questi ultimi anni. Grazie alle loro caratteristiche, prime fra tutte le piccole dimensioni e la comunicazione via radio, vengono ampliate le possibilità offerte rispetto alle reti tradizionali, che devono invece tener conto dei limiti imposti dalle connessioni via cavo. Si sono aperti di conseguenza nuovi scenari e nuove necessità, ai quali è corrisposto un sempre maggiore sforzo nello sviluppo di nuove architetture hardware e software. La capacità di questo tipo di rete si è ampliata in termini di numero, mobilità, configurabilità e indipendenza dei suoi nodi (fisicamente detti *piattaforme*). Si è, così, sentita l'esigenza di poter disporre da un lato di dispositivi a basso costo e consumo, dall'altro di strumenti software che consentissero di sfruttarne appieno le caratteristiche.

Questo capitolo presenta una visione generale delle reti di sensori wireless; vengono infatti messe in evidenza le loro caratteristiche, con particolare attenzione all'architettura di un singolo nodo, lo stato dell'arte delle piattaforme hardware e software disponibili per realizzarle, con particolare attenzione al sistema operativo TinyOS[1], punto di riferimento per tutti i programmatori di questo settore, e infine viene offerta una panoramica degli ambiti in cui possono essere impiegate.

3.1 CONCETTI GENERALI

L'evoluzione delle tecnologie per le comunicazioni radio ha consentito la nascita di una nuova concezione di rete. Rispetto a quelle tradizionali che vedono le loro capacità di impiego limitate dalla presenza fisica del cavo necessario al collegamento dei loro nodi, le reti di sensori wireless possono essere utilizzate nei campi più disparati e in ambienti prima considerati inaccessibili: dal monitoraggio ambientale di zone remote alla ricostruzione di un campo di battaglia o al controllo remoto dei dati fisiologici di un paziente (per citare alcuni esempi).

Figura 3. 1 – Nodi sensore disposti in un bosco e su di un campo di battaglia

L'enorme varietà di applicazioni possibili e l'assenza di vincoli nel loro posizionamento porta cambiamenti non solo nella topologia delle reti ma anche nella struttura fisica dei suoi nodi e negli algoritmi che li gestiscono. Nella progettazione di questo tipo di reti, infatti, si devono affrontare nuovi tipi di scenario dovuti ad un numero molto maggiore di nodi possibili (anche migliaia), alla flessibilità del loro collegamento, alla libertà di movimento e posizionamento. E' possibile infatti realizzare reti composte da nodi distribuiti con elevata densità nella zona che si vuole monitorare in grado di comunicare tra di loro attraverso trasmissioni wireless. L'aumento delle capacità della rete nel suo insieme ha come conseguenza una notevole riduzione dell'importanza del singolo nodo, la cui funzione si limita alla semplice osservazione del fenomeno con pochissima elaborazione. I dati raccolti vengono infatti inviati ad una stazione base, passando da un nodo ad un altro, ed infine trasferiti, via internet o via satellite, verso un centro di raccolta. Si possono prevedere anche altre configurazioni, più o meno complesse, composte da più stazioni base, eventualmente mobili, o addirittura completamente isolate.

In generale i nodi sono dispositivi piccoli e a bassa potenza (alimentati a batterie), di conseguenza nella valutazione delle prestazioni l'efficienza energetica assume un'importanza pari alla bit error rate, dato che essa è legata al tempo di vita dei sensori e quindi al tempo di vita della rete.

Ogni nodo è composto essenzialmente da due parti: la prima riguarda il sensore vero e proprio (ossia il dispositivo in grado di rilevare grandezze fisiche come temperatura, umidità, pressione, accelerazione, posizione), mentre la seconda consiste in un transceiver per le trasmissioni radio e un microprocessore per l'elaborazione delle informazioni.

Le caratteristiche tipiche di una rete di sensori e in particolare di un singolo nodo verranno comunque approfondite durante la trattazione.

3.2 CARATTERISTICHE DELLE RETI DI SENSORI WIRELESS

Le reti di sensori si differenziano tra di loro per vari aspetti, e per ogni specifica applicazione è necessario scegliere la soluzione più opportuna tenendo conto delle numerose caratteristiche: scalabilità, costi, ambiente, topologia di rete, componenti hardware e consumo energetico.

Scalabilità

E' la proprietà della rete di poter modificare il sistema per poter includere nuovi sensori aggiunti in un secondo momento.

Questa proprietà è essenziale sia perchè ogni nodo ha generalmente una vita limitata, sia perchè è possibile aggiungere ulteriori nodi per rimpiazzare quelli guasti. La densità della rete quindi può variare anche velocemente a seconda del tipo di applicazione e della particolare condizione, pertanto ogni singolo sensore deve essere in grado di adattarsi nel tempo alla particolare situazione.

Costo

Questo parametro assume un ruolo molto importante nelle reti di sensori dato che sono formate da un numero molto grande di nodi. Infatti se il costo del componente wireless è maggiore rispetto ai sensori tradizionali allora l'impiego della tecnologia wireless potrebbe non essere più giustificabile, o comunque, per applicazioni in cui il wireless è indispensabile come nel caso della localizzazione, il costo dei nodi influirà sulla densità della rete e quindi sulla precisione raggiungibile.

Ambiente

I nodi devono poter essere inseriti in qualsiasi ambiente e devono essere in grado di sopportare condizioni di lavoro molto ostili.

Nel problema della localizzazione, ad esempio, bisogna tener presente proprio questi fattori perchè il basso costo di ogni singolo sensore può permettere l'utilizzo di un numero elevato di nodi per cui la rete è in grado di fornire un maggior numero di informazioni. Il software che gestirà la rete deve poter avere la possibilità di aggiungere o eliminare un nodo senza compromettere il funzionamento dei restanti; inoltre deve tenere presente in che modo l'ambiente può influire sulla rete; infatti, esisteranno dei problemi dovuti alle riflessioni e agli assorbimenti che in campo libero non si avrebbero.
Di seguito saranno evidenziati altri aspetti importanti relativi alla topologia della rete e la scelta opportuna in base alle necessità dell' applicazione.

Topologia della rete

E'un fattore molto importante perchè è in grado di determinare quale sarà il tipo di comunicazione tra i nodi che comporranno la rete; inoltre anche il posizionamento dei motes (o sensor nodes) permetterà di impiegare nel miglior modo ogni informazione.
I nodi sensore sono essenzialmente statici, cioè posti in posizioni precise che non evolvono nel tempo. Ma bisogna ricordare che la topologia può cambiare per esempio se un nodo si spegne a causa della mancanza di energia o se viene aggiunto un nuovo nodo.
Tutte le osservazioni fatte portano a valutare l'utilizzo di "topologie funzionali di rete" e di protocolli di routing che garantiscano l'affidabilità della rete anche in corrispondenza dell'aggiunta/rimozione dei nodi stessi.
In prima approssimazione è possibile classificare le topologie di rete in tre diversi gruppi: reti a stella, reti mesh o peer to peer ed infine reti ad albero (Figura 3.2).

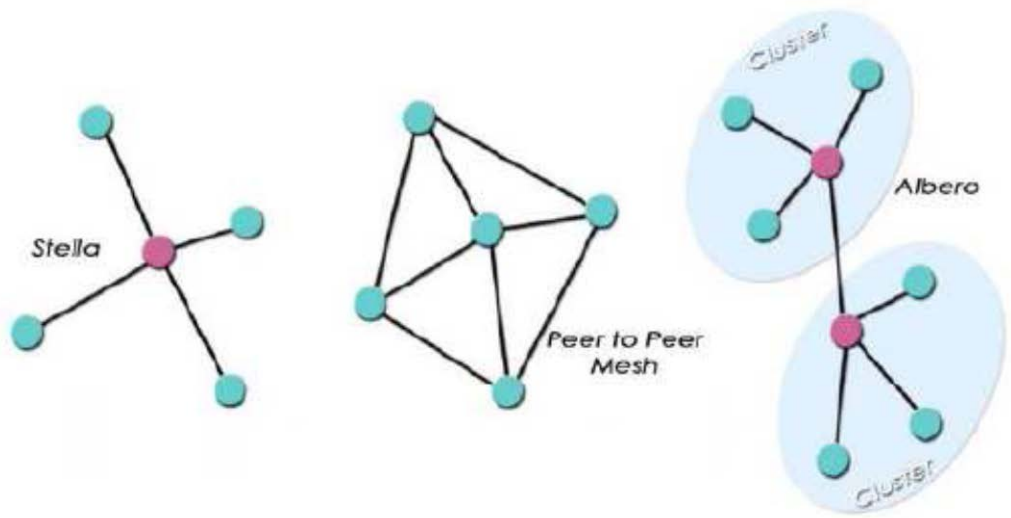

Figura 3.2 – Classificazione della topologia di rete

Nella topologia a stella si può individuare un nodo centrale, dotato di funzionalità di coordinatore: esso viene definito coordinatore della rete o centro della rete a stella, tutti gli altri nodi fanno riferimento a questo nodo centrale. Ciò implica che, affinchè due nodi possano comunicare fra loro, è necessario che entrambi comunichino con il coordinatore della rete. Questa topologia risulta essere la più semplicemente implementabile, consente l'impiego di protocolli poco onerosi da un punto di vista computazionale per i nodi semplici; ciò pone questa tipologia di rete in primo piano nel caso in cui sia possibile progettare un nodo che non abbia particolari requisiti in termini di potenza ed invece più nodi che debbano essere alimentati da unità di potenza limitata. è questo il caso, ad esempio, delle periferiche di input di un personal computer: sarà infatti possibile progettare un nodo centrale collegato al computer che possa essere alimentato dal computer stesso (es. mediante bus USB), ed invece diverse periferiche come mouse o tastiere alimentate a batteria. Generalmente il coordinatore delle reti a stella è in grado anche di funzionare da bridge verso altri sistemi di connessione: è proprio questo il caso dell'esempio appena fatto poichè il coordinatore funge da bridge fra il bus USB e la rete WSN.

La topologia di rete a stella però viene superata in funzionalità dalle reti di tipo peer to peer o mesh, reti cioè in cui il ruolo del coordinatore non è essenziale, dato che ogni

dispositivo è in grado di connettersi con tutti gli altri. In questo modo è possibile realizzare dei percorsi ridondanti che, da un lato consentono di aumentare l'affidabilità della rete, ma dall'altro richiedono l'implementazione di algoritmi di routing più complessi.

Infine abbiamo la topologia ad albero in cui diversi cluster costituiti da gruppi di nodi possono interconnettersi in modo simile ad una diramazione delle foglie su un albero. Ciascun cluster, infatti, è dotato di un nodo principale che rappresenta il punto di accesso per la sottorete in questione. Il vantaggio di questa topologia rispetto alle reti mesh è la riduzione dei percorsi di comunicazione possibili e ciò consente lo sviluppo di sistemi di gestione meno complessi.

Risulta quindi fondamentale la scelta di una opportuna struttura, che sia in grado di poter comunicare le informazioni in maniera efficiente senza perdere dati o avere eccessiva ridondanza.

Consideriamo ad esempio un'applicazione dedicata alla localizzazione. L'idea che un nodo debba raccogliere le informazioni e inviarle a un PC potrebbe suggerire di utilizzare una rete di tipo a stella, ma il problema che risalta immediatamente è che per la natura del sistema di localizzazione il nodo coordinatore non può invece essere che il nodo mobile, il quale ha necessità di comunicare con tutti i nodi fissi per stabilire la sua posizione. Questo comporterebbe però la necessità di effettuare l'elaborazione delle informazioni a bordo del nodo mobile e poi utilizzare un altro nodo come bridge verso il PC con un sovraccarico di uno dei collegamenti radio, nonchè una perdita di robustezza dovuta al fatto che il nodo principale sarebbe quello in movimento e quindi più a rischio di interruzioni nelle comunicazioni. Inoltre, non potendo i nodi fissi comunicare tra di loro, sarebbe loro impossibile utilizzare tutte le informazioni disponibili per ricalibrare la rete e compensare i problemi dovuti all'ambiente circostante.

Si preferisce quindi impiegare una topologia di tipo mesh in cui ogni nodo conosce tutte le informazioni relative agli altri ed è in grado di trasmetterle al nodo base in modo che il pc avendo le conoscenze sull'intera struttura possa elaborare tutti i dati per localizzare il mote mobile.

Ogni nodo quindi deve inviare un messaggio broadcast all'intera rete; tutti gli altri nodi in quell'istante saranno in fase di ascolto e potranno acquisire le informazioni sulla potenza con la quale ognuno riceve il nodo che sta trasmettendo. Quando tutti i nodi della rete avranno trasmesso le loro informazioni ciascun nodo avrà tutti i dati relativi ad ognuno degli altri nodi e potrà a sua volta ritrasmetterle. Il nodo centrale dovrà essere considerato come un nodo particolare ed avrà bisogno di un firmware diverso, perchè oltre alle funzionalità degli altri nodi avrà il compito di trasmettere al pc tutti i messaggi che riceve; questo perchè sarà poi quest'ultimo ad effettuare i calcoli relativi alla localizzazione.
Se l'area da coprire è estesa, si può pensare di utilizzare una rete ad albero che permetta di tenere il contatto tra tutti i nodi, individuando dei nodi centrali che devono poter comunicare al nodo base principale (ossia quello collegato al pc) le informazioni. Ogni cluster dovrà essere di tipo mesh per avere, come detto sopra,la massima duttilità.

Componenti hardware

Un nodo di una rete di sensori wireless è composto essenzialmente da quattro componenti fondamentali (vedi Figura 3.3):

Unità computazionale

E' una piccola unità per l'immagazzinamento dei dati, la loro elaborazione, la trasmissione e la gestione dei percorsi di routing con gli altri nodi. Nel nostro specifico caso si occupa principalmente di una semplice elaborazione dei dati e della gestione della comunicazione di essi all'intera rete. Di fatto le risorse di calcolo utilizzate sono limitate.

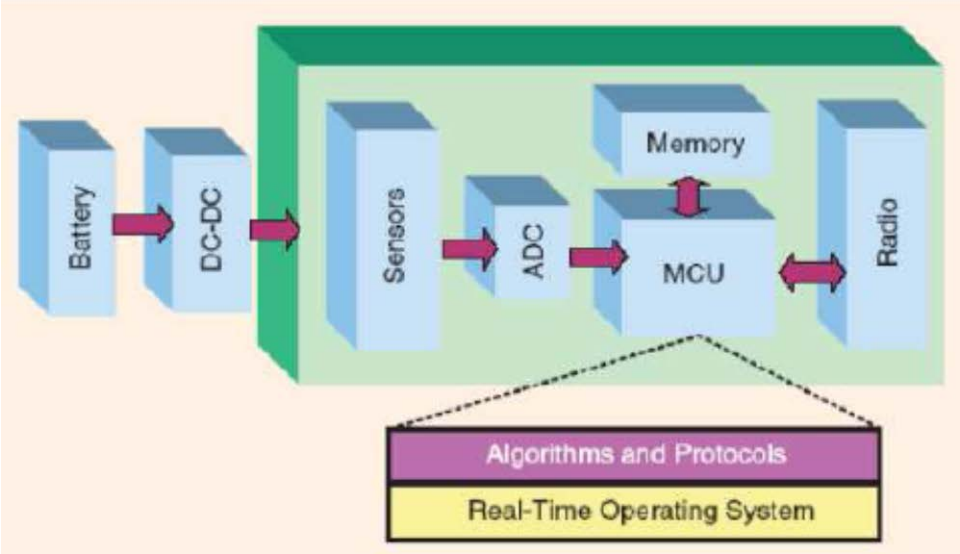

Figura 3.3 – Componenti hardware di un mote

Unità transceiver

E' il componente che connette il sensore alla rete attraverso radiofrequenza.

Unità energetica

Si può impiegare una fonte solare, delle batterie o la rete elettrica. Principalmente, siccome l'ambiente di studio sarà un ambiente indoor, i nodi fissi potranno essere alimentati attraverso la rete elettrica diminuendo i problemi legati al risparmio energetico, mentre il nodo mobile sarà necessariamente alimentato attraverso batterie.

Unità sensing

E' la parte del sensore vero è proprio; è in realtà divisa in due parti: la prima comprende il sensore mentre la seconda è costituita dal convertitore ADC per convertire il valore fornito dal sensore in un valore digitale da trasmettere.

Consumo Energetico

Questo è il parametro più importante dei motes, dato che determina il tempo di vita del sensore, infatti una volta che le batterie sono esaurite il nodo può essere considerato morto, a meno che non si abbia la possibilità di sostituirle.

Le tre operazioni che provocano consumo d'energia sono:

- *Sensing*: potenza necessaria per effettuare la rivelazione della grandezza;
- *Communication*: potenza necessaria per la trasmissione a radio frequenza; delle tre è sicuramente quella che causa maggior dispendio energetico;
- *Processing*: l'energia spesa per processare i dati.

3.3 ARCHITETTURA DI UN SINGOLO NODO

Analizziamo ora maggiormente nel dettaglio le caratteristiche in termini di architettura di un singolo nodo.

La riduzione dei compiti di ogni singolo nodo, o piattaforma, si è riflessa in una semplificazione della sua struttura, generalmente composta da un microcontrollore, un modulo di comunicazione, dei sensori, un modulo di memoria non volatile e una batteria. Gli obiettivi che si cerca di raggiungere con una configurazione di questo tipo sono:

- **ridotte dimensioni:** aumentano la possibilità di integrazione delle reti e accrescono di fatto il numero di ambiti in cui possono essere utilizzate (fino ad arrivare alle applicazioni più quotidiane come nel controllo di forni a microonde o di videoregistratori);
- **basso costo:** data l'enorme quantità di sensori che alcune applicazioni richiedono, il costo per unità non dovrebbe pesare sul costo complessivo della rete;
- **basso consumo:** per sfruttare al meglio l'assenza di collegamenti fisici ogni nodo ha una fonte indipendente di alimentazione, diventa quindi cruciale per la sua longevità ridurre i fabbisogni energetici.

Grande interesse, al momento, è rivolto alla riduzione dei consumi; in primo luogo perché i progressi nella miniaturizzazione e nei protocolli di comunicazione hanno permesso già di raggiungere livelli soddisfacenti per i primi due punti, in secondo luogo perché determina un fattore essenziale come l'indipendenza del sensore. Le ricerche hanno indirizzato i loro sforzi innanzitutto nel miglioramento dell'hardware, da un lato tentando di aumentare la capacità delle batterie a parità di dimensioni (argomento che

coinvolge in realtà più settori) e dall'altro progettando dispositivi che richiedano piccolissime potenze.

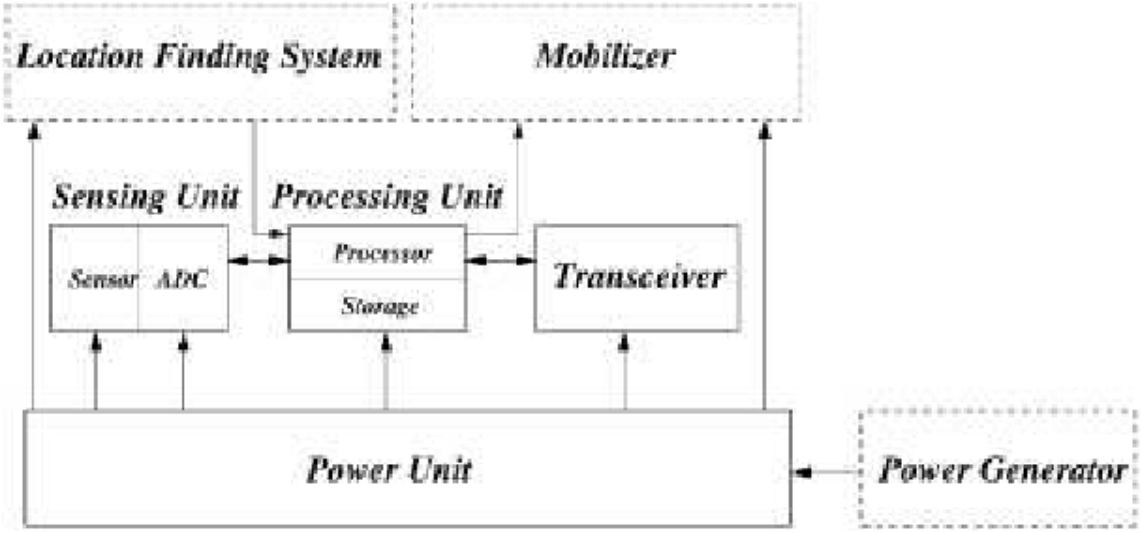

Figura 3.4 – Tipica struttura di un nodo sensore

Particolare attenzione è stata dedicata al microcontrollore per il ruolo centrale che riveste all'interno delle attività della piattaforma. Questo dispositivo riunisce in sé tutti i circuiti necessari a realizzare un completo sistema digitale programmabile (e per questo spesso fondamentale per la realizzazione di sistemi embedded), permettendo al progettista di disporre in un unico chip di un vero e proprio computer a basso costo. Le sue capacità di elaborazione e memorizzazione sono ridotte, ma nel contempo possiede una numerosa serie di periferiche. Un solo microcontrollore può essere in grado di comunicare con diversi dispositivi (per esempio attraverso moduli USART, I2C, SPI, CAN), effettuare conversioni analogico-digitali, generare onde PWM (utile per esempio per il pilotaggio di motori elettrici), oltre a possedere strumenti per la temporizzazione, comparazione, gestione degli interrupt. Queste caratteristiche lo rendono molto adatto per compiti di controllo dove è richiesta molta connettività e poca elaborazione. Nelle reti di sensori, infatti, vengono usati per coordinare le attività del singolo nodo come quando acquisire il dato, iniziare la comunicazione radio, attivare/disattivare la piattaforma. Visto l'elevato numero delle funzioni a cui assolve, disporre di microcontrollori a basso consumo diviene

fondamentale per le prestazioni di una piattaforma e di conseguenza di tutta la rete. Il raggiungimento di risultati soddisfacenti richiede un grosso sforzo in fase di progettazione, in quanto ogni particolare dell'architettura del microcontrollore influisce sulla potenza assorbita [2]. Di seguito vengono elencati i più importanti.

Power Management

Nelle attività di controllo è molto facile che il sistema resti in attesa di un evento senza assolvere a nessun compito. Per evitare di sprecare energia inutilmente, i microcontrollori sono in grado di spegnere il sistema (modalità *sleep*), alcuni addirittura solo le parti inutilizzate, quando questo è inattivo e riattivarlo quando necessario.

Wakeup Time

Meno tempo impiega il dispositivo a riattivarsi, maggiori saranno le condizioni in cui può permettersi di entrare in modalità *sleep* sfruttando anche intervalli molto brevi. Il fattore determinante è la velocità necessaria all'oscillatore primario per stabilizzarsi; sono state adottate in questo senso diverse soluzioni:

- scollegare nelle attese l'oscillatore primario dal microcontrollore, cosicché da mantenere attivo, quindi sempre pronto, il primo e spegnere il secondo;
- permettere l'inizio dell'esecuzione anche ad oscillatore non stabilizzato;
- utilizzare il meccanismo chiamato *Two-Speed Start-up*, che prevede l'utilizzo all'avvio di un oscillatore interno a basso consumo, meno preciso ma più pronto, e il passaggio all'oscillatore esterno quando quest'ultimo è stabile.

Clock Scaling

Alcuni microcontrollori sono in grado di cambiare dinamicamente la frequenza operativa così da avere un'ulteriore grado di libertà nella gestione dei consumi. Le tecniche utilizzate sono sostanzialmente due:

- oscillatore ad alta frequenza e divisore;
- oscillatore a bassa frequenza e moltiplicatore.

La prima soluzione consente di far lavorare il dispositivo con minori frequenze e consumi, ma mantiene l'oscillatore a pieno regime. La seconda viceversa permette l'utilizzo di un oscillatore a bassa frequenza e potenza, quindi in linea di principio preferibile. Il moltiplicatore, però, a differenza del divisore ha un consumo non trascurabile oltre ad avere bisogno di un certo tempo di assestamento per ogni cambio di frequenza; particolare che aumenta i tempi morti del microcontrollore.

Gestione della memoria

E' importante nell'ambito dei consumi perché più velocemente gli accessi in memoria vengono eseguiti, minore è il *duty cycle* (ossia la percentuale di tempo in cui il dispositivo rimane attivo). Innanzitutto un'architettura di tipo Harvard, per la sua capacità di eseguire un'operazione di lettura e scrittura contemporaneamente, è preferibile ad una di tipo Von Neumann. Altrettanto influente è la varietà e il tipo di indirizzamento, per esempio determina se il puntatore è in grado di accedere all'intera memoria in un sola istruzione.

Visto, inoltre, il ruolo predominante che riveste la gestione degli interrupt nelle attività di un sensore wireless, un'attenzione particolare va rivolta alla loro efficienza. Nel servire una richiesta di interrupt, spesso è necessario salvare un certo numero di registri e flag per mantenere traccia dell'esecuzione corrente. Siccome il codice necessario per evadere la richiesta è normalmente molto breve, il cambio di contesto può costituire la parte predominante del tempo richiesto dall'interruzione e una sua gestione efficiente non è secondaria. La soluzione migliore sarebbe quella di avere due set di registri separati, in modo da evitare le operazioni di salvataggio e completare il cambio di contesto con una singola istruzione.

Meno lineare è la scelta sulla gestione dello stack, che può essere dinamica o statica. La prima è la classica coda LIFO e richiede un indirizzamento indiretto nella forma *base* + *offset*. Nella seconda le locazioni di memoria vengono assegnate ai dati al momento di compilazione, dove viene determinato quali variabili possono condividere una locazione. Entrambe le soluzioni hanno i loro vantaggi e svantaggi. Uno stack dinamico consente una più ampia libertà nella programmazione (per esempio le funzioni possono essere

rientranti), ma richiede un'architettura più complessa che non tutti i microcontrollori posseggono. In uno stack statico gli accessi in memoria sono più efficienti, ma gli strumenti a disposizione del programmatore sono limitati; non è possibile, per esempio, l'uso di funzioni rientranti o ricorsive.

Set di istruzioni

Una maggiore complessità delle istruzioni disponibili permetterebbe una maggiore capacità di elaborazione del nodo con la conseguenza di potenziare la rete, ma soprattutto di ridurre al minimo i dati da trasmettere via radio; operazione questa molto dispendiosa in termini di consumo energetico. Purtroppo il potenziamento del set di istruzioni incide molto sul costo finale del dispositivo; tanto che la maggior parte dei microcontrollori operano su parole di otto bit, il numero di registri *general-purpose* è scarso, il calcolo in virgola mobile inefficiente.

3.4 PIATTAFORME DISPONIBILI PER WSN

In questo paragrafo viene presentata una breve panoramica delle piattaforme disponibili sul mercato e supportate dal sistema operativo TinyOS, che analizzeremo più avanti.

3.4.1 La piattaforma Renè

Renè è un'evoluzione della piattaforma *weC*, riprogettata per l'uso come base sperimentale e di sviluppo. Prodotta nel 2000 è composta da un microcontrollore, diversi sensori e attuatori, un ricetrasmettitore radio, un coprocessore e una memoria esterna.

Microprocessore

La piattaforma è basata sul ATMEL 90LS8535 [3]. Ha un architettura di tipo Harvard a 8 bit con indirizzamento a 16 bit. E' provvista di 32 registri general-purpose a 8 bit, una memoria flash da 8 KB e 512 bytes di memoria dati di tipo SRAM. Il microprocessore integra un certo numero di timer e contatori, che possono essere configurati in modo da generare degli interrupt a intervalli regolari, e un convertitore analogico/digitale per

interfacciarsi con i sensori. E' regolato da un oscillatore a 4 MHz e richiede un'alimentazione di 3 V.

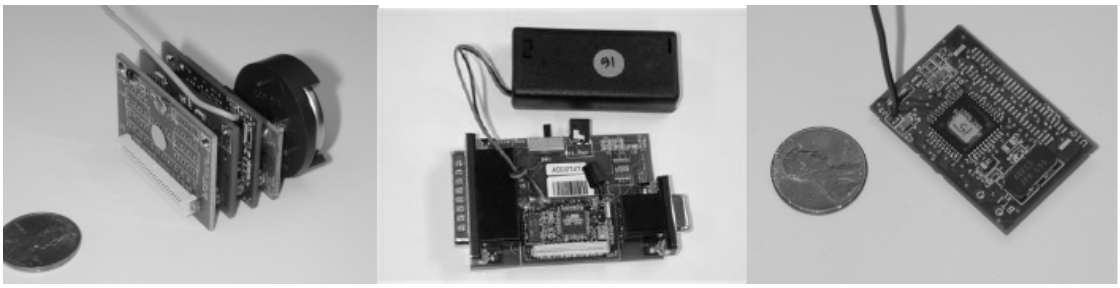

Figura 3.5 – Nodo sensore Renè

Memoria esterna

In appoggio alla memoria interna del microcontrollore, la piattaforma monta una EEPROM 24LC256 capace di contenere 32 kilobytes di dati. Per la connessione usa un bus I^2C.

Sistema radio

Il sistema radio è composto dal un ricetrasmettitore RF a 916.50 MHz (TR1000 [4]), un'antenna, oltre a una serie di componeti discreti necessari a configurare alcune caratteristiche come sensibilità e potenza. Utilizza una modulazione OOK con rate fino a 19.2 Kbps, anche se nella *Renè* si arriva al massimo a 10 Kpbs. Prevede tre modalità di funzionamento configurabili attraverso segnali di controllo: trasmissione, ricezione e *power-off*. La radio è sprovvista di buffer, per cui ogni bit deve essere processato dal microcontrollore. Soffre, inoltre, del fenomeno di jitter in trasmissione.

Coprocessore

La piattaforma è stata provvista di un coprocessore AT90LS2343 [5], soprattutto per permettere la riprogrammazione remota: attraverso la rete si trasmettono i dati necessari, dopodiché il coprocessore effettua un *reset* del microprocessore e lo riprogramma prelevando il codice dalla memoria esterna. Il componente AT90LS2343 possiede una

memoria programma tipo flash da 2 KB, 128 bytes di memoria sia SRAM che EEPROM per i dati.

Periferiche I/O

Sono presenti tre led, che possono essere usati per rappresentare valori binari o indicare lo stato della piattaforma, e un sensore di luce collegato all'ADC interno.

3.4.2 La piattaforma Mica

Mica è una piattaforma importante nel mondo delle reti di sensori perché rappresenta il primo dispositivo che si avvicina alle caratteristiche richieste da un nodo wireless. La piattaforma Mica è basata sulla Renè: continua ad avere un microcontrollore centrale che controlla tutta l'attività e il coprocessore AT90LS2343 per la riprogrammazione, ma in più gode dell'aiuto di acceleratori hardware per aumentare il bit rate della trasmissione radio e la reattività del sistema. Le dimensioni sono abbastanza contenute (3.16 x 5,72 cm, paragonabili a due pile AA) ed è la prima piattaforma su cui è stato sviluppato il sistema operativo TinyOS.

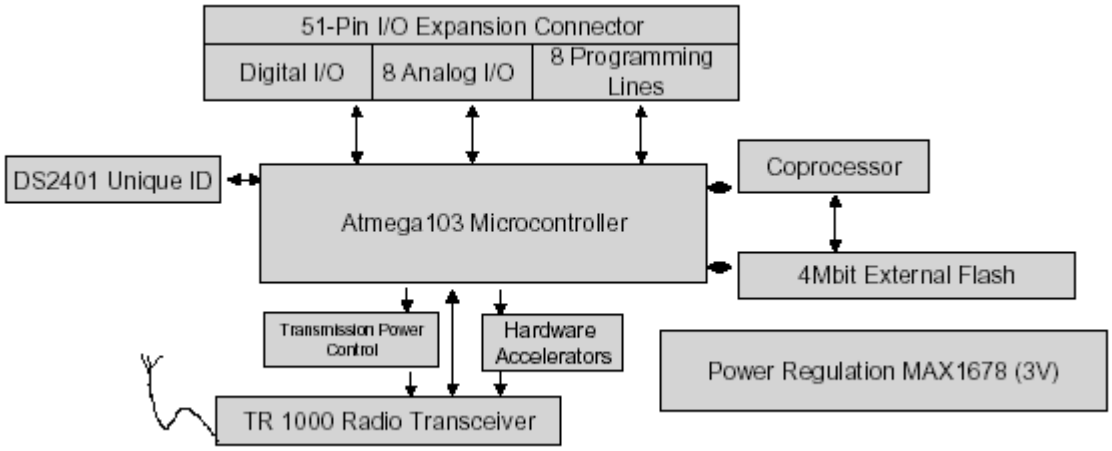

Figura 3.6 – Diagramma a blocchi della piattaforma Mica

Microcontrollore

Il microcontrollore costituisce un grosso passa avanti rispetto alla Renè e può essere o un Atmel ATMEGA103L [6] o ATMEGA128 [7]. Ha un architettura Harvard a 8 bit e indirizzamento a 16 bit, una memoria programma da 128 Kbyte di tipo flash, 4 Kbyte di RAM statica, un convertitore analogico-digitale a 8 canali con risoluzione 10 bit, tre timer hardware, 48 registri general-purpose, diverse linee di I/O, una modulo di comunicazione UART e un'interfaccia SPI. Dispositivo a bassa potenza prevede sei modalità di funzionamento per una migliore gestione dei consumi: Idle, ADC Noise Reduction, Power-save, Power-down, Standby, Extended Standby.

Memoria esterna

Mica è dotata di una più capiente flash AT45DB041B [8] da 128 Kbyte con interfaccia SPI, in grado quindi di riprogrammare la memoria interna da 128 Kbyte del microprocessore.

Sistema radio

Rispetto alla Renè viene utilizzato lo stesso componente radio, il TR1000, ma con modulazione ASK. La vera e sostanziale differenza, che consente un netto miglioramento, è nell'interfacciamento con l'aiuto di acceleratori hardware e un dispositivo per il controllo della potenza.

La gestione bit a bit della comunicazione da parte del microprocessore, a causa della mancanza di un buffer dedicato nel TR1000, è estremamente inefficiente, con la conseguenza di un deterioramento del bit rate e del risparmio energetico. Per sgravarlo da questo compito si sono aggiunti dei convertitori seriale-parallelo come buffer di appoggio, che permettono di raggiungere bit-rate fino a 40 Kbps con un'occupazione minore del controllore Atmel, assolvendo al compito di acceleratori hardware.

Grazie alla migliore efficienza della comunicazione, il microcontrollore può gestire anche altri aspetti come minimizzare la potenza utile ad una corretta trasmissione attraverso, per esempio, misurazioni sul rapporto segnale/rumore.

Periferiche I/O

Per donare flessibilità al collegamento con le periferiche esterne, la piattaforma monta un connettore a 51 pin collegati con le uscite dell'ATMEGA. La soluzione permette di collegare a seconda delle esigenze un sensore diverso. Sono disponibili attualmente una dozzina di sensori per il rilevamento della temperatura e pressione atmosferica, della luminosità, di campi magnetici, della luminosità, delle vibrazioni, a infrarossi e acustici. Anche questa piattaforma è dotata di tre led, uno verde, uno giallo e uno rosso.

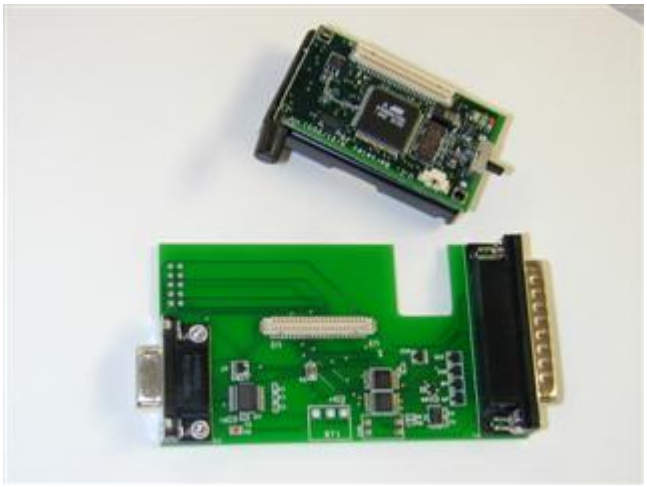

Figura 3.7 – Piattaforma Mica (in alto) e programmatore (in basso)

3.4.3 Le piattaforme Mica2 e Mica2Dot

Mica2 e Mica2Dot sono due piattaforme identiche alla Mica, ma con prestazioni molto più elevate grazie al ricetrasmettitore CC1000 [9] della Chipcon. Progettato per applicazioni che richiedono un basso consumo di energia, ha un raggio d'azione che può arrivare fino ad un centinaio di metri. Utilizza la codifica Manchester, la modulazione FSK, un protocollo MAC del tipo CSMA/CA, supporta bande di frequenza a 315, 433, 868 e 915 Mhz ed è in grado di lavorare a frequenza comprese tra 300 e 1000 MHz. Il sistema radio può lavorare in quattro distinte modalità: transmit, receive, idle e sleep. Questo significa che mentre trasmette non è in grado di ricevere.

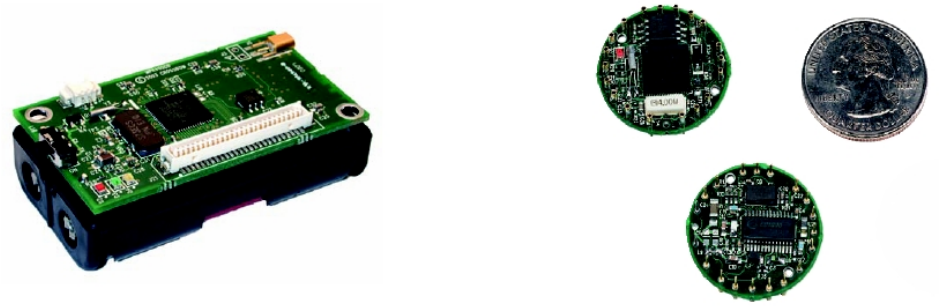

Figura 3.8 – Piattaforme Mica2 (a sinistra) e Mica2Dot (a destra)

Più che nel basso consumo, sicuramente non secondario, il vero punto di forza del CC1000 è il completo supporto hardware delle operazioni di trasmissione e ricezione. Il compito del microprocessore, infatti, si limita al trasferimento sul buffer del ricetrasmettitore del byte da trasmettere; la codifica, decodifica, sincronizzazione e verifica vengono fatte dal componente della Chipcon. Il lavoro del microprocessore si alleggerisce notevolmente con il vantaggio abbassare il duty-cycle, mantenendo allo stesso tempo alti bit-rate (fino a 40 Kbps).

3.4.4 La piattaforma MicaZ

Anche questa piattaforma differisce dalla Mica solamente per il sistema radio, basato sul componente *CC2420* [10] della Chipcon. Compatibile con lo standard 802.15.4 e con il protocollo *ZigBee*, lavora sulla banda di frequenze intorno ai 2.4 GHz. Utilizza una modulazione O-QPSK sfruttando la tecnica *digital direct sequence spread spectrum*, che portano ad un data-rate effettivo di 250 Kbps. Provvede al supporto hardware per quanto riguarda la codifica, decodifica, verifica dei dati da trasmettere o ricevuti, oltre alla possibilità di crittografarli (AES con chiave a 128 bit). Anch'esso, come il CC1000, riduce il compito del microcontrollore ad un semplice trasferimento di dati su di un bus SPI.

3.4.5 La piattaforma Telos

La piattaforma Telos merita particolare attenzione non tanto per le periferiche in dotazione, tra cui una memoria esterna da 128 Kbyte e un CC2420, quanto per il microcontrollore *MSP430* [11] della *Texas Instrument*. Rispetto al ATMEGA128L può

essere considerato un passo evolutivo in più; riesce, infatti, ad associare una buona capacità di elaborazione con una notevole diminuzione dei consumi. Una caratteristica chiave è la rapidità di commutazione dalla modalità attiva alla *sleep* (meno di 100 μs); inoltre è stato progettato in modo che le periferiche possano funzionare mentre il clock di sistema è disabilitato: le operazioni di conversione A/D, le comunicazioni seriali e il trasferimento dei dati alla radio possono procedere mentre il nucleo è spento. In totale sono previste sei modalità di funzionamento.

Possiede un architettura Von Neumann a 16 bit, un convertitore *ADC* a 12 bit con un sample-rate di 100 campioni al secondo oltre le solite periferiche per la temporizzazione e la comunicazione.

Figura 3.9 – Piattaforme MicaZ (a sinistra) e Telos (a destra)

3.4.6 La scheda Microchip PicDem Z

PicDem Z è un kit dimostrativo, commercializzato dalla Microchip, per illustrare l'uso del protocollo *ZigBee* [12] attraverso il ricetrasmettitore CC2420. Data la funzione prettamente sperimentale, la componentistica presente è molto essenziale e consta principalmente di un microcontrollore pilotato da un oscillatore al quarzo a 4 MHz, un sensore di temperatura, due led, due switch e ovviamente il sistema radio; la dotazione è facilmente espandibile grazie alla basetta forata con i collegamenti per ogni piedino del microcontrollore già realizzati e pronti per l'uso.

Microcontrollore

Il microcontrollore in dotazione è un PIC18LF4620 prodotto dalla Microchip.

Un microcontrollore o microcontroller, detto anche computer single chip è un sistema a microprocessore completo, integrato in un solo chip. I microcontroller sono la forma più diffusa e più invisibile di computer. Comprendono la CPU, un certo quantitativo di memoria RAM e memoria ROM (può essere PROM, EPROM, EEPROM o FlashROM) e una serie di interfacce di I/O (input/output) standard, fra cui molto spesso bus. Le periferiche integrate sono la vera forza di questi dispositivi: si possono avere convertitori ADC e convertitori DAC multicanale, timer/counters, numerose porte esterne bidirezionali bufferizzate, comparatori, PWM. I microcotrollori hanno un set di istruzioni di tipo RISC (Riduced Instruction Set Computer) ovvero sono caratterizzati dall'avere poche istruzioni molto veloci e semplici da eseguire, tutte della stessa lunghezza e con lo stesso formato in modo da poter utilizzare una struttura di controllo di tipo pipeline, ovvero una sorta di catena di montaggio a più stadi.

La capacità di calcolo è in realtà molto limitata ma in compenso la velocità di clock varia da 1 a 100MHz. La capacità di memorizzazione è anch'essa piuttosto bassa poiché tutto ciò che serve deve essere presente all'interno del chip.

Potrebbe sembrare che dei componenti così siano buoni solo per scopi dimostrativi o piccoli giocattoli ma in realtà è vero il contrario. Se analizziamo il funzionamento di un qualsiasi apparato elettronico che ci circonda, dal cellulare alla televisione, ci rendiamo conto di come tutto il lavoro svolto da tali oggetti sia ripetitivo e prefissato. Non è importante quindi che la memoria sia vastissima, non quanto la velocità e la mancanza di errori. Sembra una cosa scontata presupporre un programma stabile e privo di errori ma troppo spesso si viene smentiti. Si pensi ad esempio ad un cartellone pubblicitario gestito da un PC con un sistema operativo tipo Windows o Linux, il primo errore di lettura o interruzione di corrente potrebbe portare ad un blocco del sistema che neanche un reset forzato sarebbe in grado di ripristinare. I microcontrollori in genere hanno il codice da eseguire in memoria ROM (non cancellabile e non modificabile) e la relativa semplicità interna limita o annulla gli errori hardware. Dal 1990 in poi questi componenti sono stati impiegati in ogni sorta di apparecchio ed oggi sono utilizzati anche in ambienti dinamici molto complessi come potrebbe essere la gestione di una automobile. Ciò sembra contraddire quanto scritto sopra ma basta dividere il problema auto in tanti piccoli

sottoproblemi semplici per ottenere la soluzione; ecco così che un microcontrollore gestisce l'ABS, un altro gli airbags, un terzo controlla la combustione e così via.

Negli ultimi anni i microcontrollori sono stati prodotti sempre su più larga scala per permetterne l'uso anche in apparecchiature a basso costo; l'abbattimento dei prezzi ha anche favorito il diffondersi dei microcontrollori fra gli hobbisti e sono nati così modelli molto economici dalle prestazioni magari non elevatissime ma sufficienti a sostituire delle enormi reti logiche grazie alla loro estrema versatilità, alla semplicità di installazione e alla velocità di programmazione.

Il PIC18LF4620 si presenta come un chip nero di forma rettangolare di 40 pin.

L'acronimo PIC significa Peripheral Interface Controller e la sigla che lo segue è utile per capire le potenzialità e le caratteristiche dell'oggetto infatti le prime 2 cifre identificano sempre la famiglia (nel nostro caso 18), l'ultimo numero rappresenta il modello (4620) mentre le lettere poste fra i due numeri possono esserci o meno e identificano diverse versioni dello stesso chip. Nel caso specifico "LF" significa che la memoria interna è di tipo flash e la tensione di alimentazione deve variare in un range compreso fra 2,0V e 5,5V, una flessibilità rara visto che di solito l'alimentazione è fissa a 5 V ±0,5V.

Il microcontrollore in questione dispone di un'architettura Harvard a 8 bit e indirizzamento a 8 bit, una memoria programma da 64 Kbyte di tipo flash, una *SRAM* da 4 Kbyte, una *EE*PROM da 1 Kbyte, 1 registro general-purpose, un convertitore A/D da 10 bit, comparatori, generatore PWM, contatore timer con prescaler a 16 bit chiamato WDT (watchdog timer), diverse linee di I/O e moduli di comunicazione SPI, I2C ed EUSART.

Nello schema in Figura 3.10 sono riportate le linee di ingresso/uscita per ogni piedino. Si notano subito gli ingressi per l'alimentazione (pin 11, 12, 31, 32), la linea MCLR (utilizzata per resettare il chip) e le connessioni OSC1 e OSC2 sui pin 13 e 14 che sono utilizzate per collegare l'oscillatore che darà il clock al sistema.

Inoltre esso può, tramite un software di controllo interno, scrivere sulla propria area di memoria. Uno dei vantaggi più evidenti di una memoria flash è la semplicità di scrittura e cancellazione poiché ciò avviene tramite opportuni valori di tensione ed è quindi possibile riprogrammare il tutto senza togliere l'integrato dallo zoccolo. Questo tipo di memoria

inoltre consente fino a 1000000 di riscritture e i dati si conservano, in mancanza di refresh, fino a 40 anni.

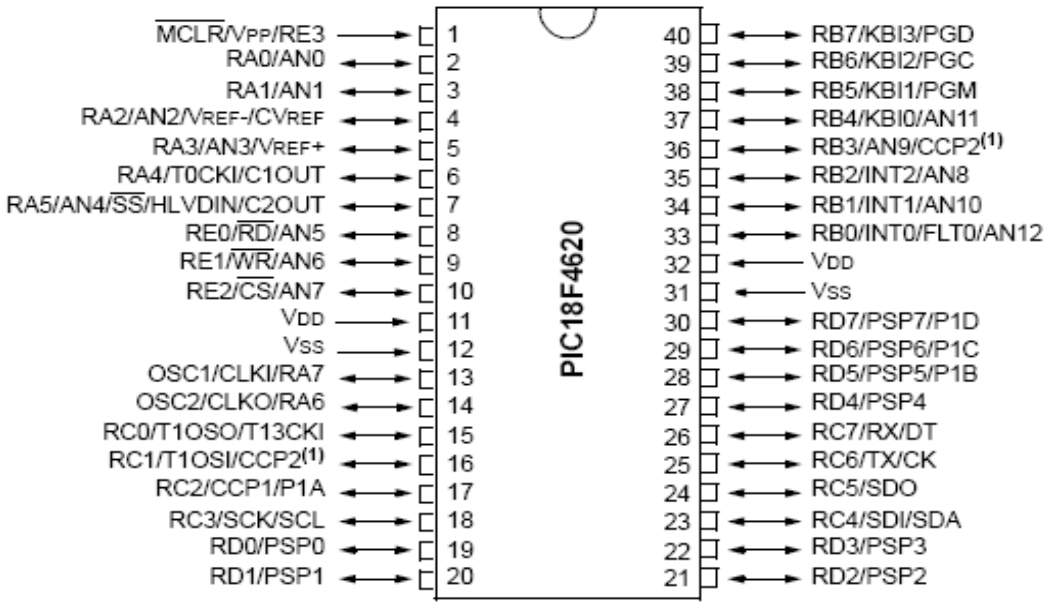

Figura 3.10 – Il microcontroller PIC18LF4620

A fronte di una capacità di elaborazione piuttosto limitata, soprattutto a causa dell' architettura *load/store* dotata di un unico registro, grazie alla tecnologia *nanoWatt* richiede un assorbimento di corrente veramente ridotto. Per una migliore gestione dei consumi è stata dotata di:

- Tre modalità di funzionamento: *Run*, *Idle* (nucleo spento, periferiche attive), *Sleep*.
- Meccanismo *Two-Speed Start-Up*.
- Ingresso per un oscillatore secondario a 32 kHz.
- Moltiplicatore sull'oscillatore primario.
- Oscillatore interno a basso consumo, con un range di frequenze selezionabili compreso tra 31 kHz e 8 MHz.

Il basso consumo e il basso costo, nonostante le basse prestazioni computazionali, fanno del PIC un componente da tenere in considerazione per le reti di sensori, soprattutto in

tutti quei casi in cui ai nodi sono richiesti compiti più di monitoraggio che di elaborazione.

Apparato di trasmissione e ricezione

I segnali da trasmettere, così come quelli ricevuti hanno bisogno di essere convertiti ed adattati al fine di essere utilizzati. Affinché si possano inviare informazioni via etere è necessario che queste vengano modulate per mezzo di un altro segnale detto "portante". Nel nostro caso la portante è una onda elettromagnetica di forma sinusoidale operante alla frequenza di 2,4 GHz . Il motivo per cui si utilizza la modulazione risiede nel fatto che i segnali rappresentanti le informazioni da trasmettere sono in prevalenza di natura passa-basso (il loro contenuto spettrale è concentrato per lo più a basse frequenze), mentre i canali trasmissivi che più comunemente si utilizzano sono di natura passa-banda. Occorre quindi convertire in frequenza, mediante tale operazione, lo spettro del segnale elettromagnetico rappresentante l'informazione e, dopo averlo eventualmente amplificato, trasmetterlo mediante un'antenna. Ovviamente il ricevitore dovrà compiere un lavoro inverso ovvero, dopo aver captato la trasmissione ed aver ripulito il segnale dai disturbi presenti, recuperare il messaggio di partenza mediante un'operazione detta di demodulazione. E' necessario che il trasmettitore ed il ricevitore abbiano la stessa ed identica portante e che siano al corrente del tipo di modulazione operata dall'altro apparecchio. Esistono infatti molti tipi di modulazione che si dividono in due grossi sottogruppi a seconda del tipo di segnale che abbiamo la necessità di modulare: le "modulazioni analogiche" e le "modulazioni digitali". Le prime si usano se il segnale in banda base è analogico mentre le seconde si usano per segnali binari, cioè tali da assumere solo due possibili valori (esempio 0 o 1, -1 o +1). Le modulazioni analogiche più usate sono la modulazione di ampiezza (AM) e la modulazione di frequenza (FM) mentre tra quelle digitali le più conosciute sono la modulazione digitale di ampiezza (ASK), la modulazione digitale a spostamento di frequenza (FSK) e la modulazione digitale di fase (PSK).

All'interno della scheda PICDem Z la funzione di modem (modulazione/demodulazione) nonché quella di antenna è demandata al chip CC2420 (Figura 3.11).

Figura 3.11 – Il chip CC2420

Esso riceve da un bus a otto linee i bit da inviare e, prima di modularli, li codifica in maniera tale che resistano meglio al rumore e non diano origine ad errori di trasmissione. Il procedimento usato per irrobustire le informazioni consiste nella sostituzione di ogni blocco di 4 bit con una stringa pseudo-casuale predefinita lunga 32 bit (chiamati "chip" vedi Figura 3.12); ciò giova all'affidabilità della connessione ma costa parecchio in termini di velocità poiché un singolo byte in ingresso comporta 8 byte da spedire e ciò significa che è necessaria una velocità di trasmissione pari a 2 Mchips/s per ottenere i 250 Kbps previsti dallo standard.

Simboli (b_0,b_1,b_2,b_3)	Valore in chip ($c_0,c_1 \ldots c_{31},c_{31}$)
0 0 0 0	11011001110000110101001000101110
1 0 0 0	11101101100111000011010100100010
. . . .	. . . . .
0 1 1 1	10010110000001110111101110001100
1 1 1 1	11001001011000000111011110111000

Figura 3.12 – Stringa pseudo-casuale

Dallo schema a blocchi seguente (Figura 3.13) si noti che la modulazione usata è la O-QPSK(Offset Quadrature Phase-Shift Keying). Nella O-QPSK, ogni chip pari di una

sequenza viene modulato sulla fase I (in phase) ed i chip dispari sulla fase Q (quadrature). Per formare l'offset tra la fase I e la fase Q, la fase Q deve essere ritardata di Tc rispetto alla fase I, dove Tc è l'inverso del chip rate (Figura 3.14).

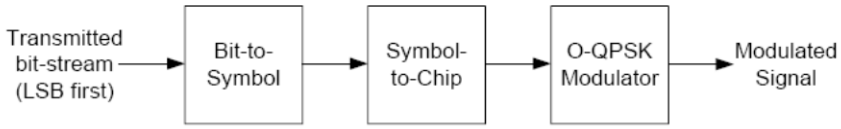

Figura 3.13 – Schema a blocchi

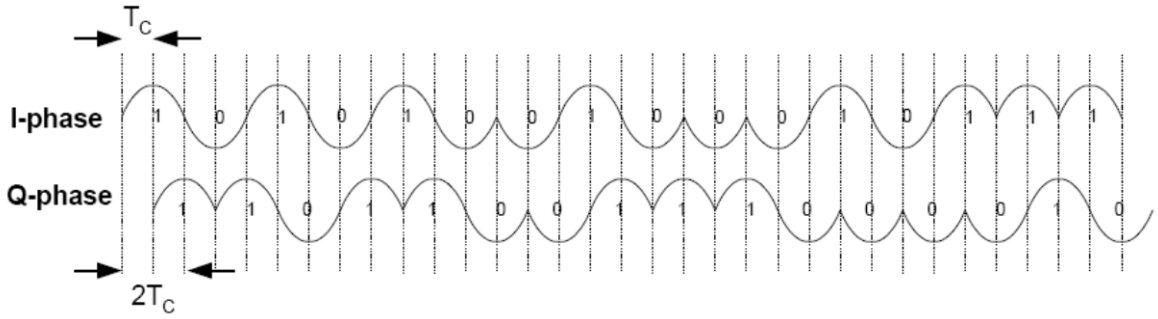

Figura 3.14 – Modulazione O-QPSK

Periferiche di I/O

Sulla piattaforma sono presenti due led di colore verde utili per la rappresentazione di uscite digitali o di stato, due switch per la simulazione di ingressi digitali e un sensore di temperatura *TC77* [13] della Microchip. Quest'ultimo componente è interessante perché, similmente al CC2420, contiene in sé tutti i circuiti necessari alla rilevazione e alla conversione digitale del dato, che deve semplicemente essere letto dal microprocessore attraverso il bus SPI. Il sensore prevede anche due modalità di funzionamento: *continuos mode* (sempre attivo) e *shut-down* (il convertitore interno viene spento). Purtroppo nella configurazione di fabbrica non è prevista una memoria esterna; le sue capacità di collezione dei dati in maniera permanente, o almeno a lungo termine e in assenza di

alimentazione, sono limitate alla sola EEPROM interna, ma soprattutto non è possibile la riprogrammazione remota.

Figura 3.15 – La scheda PICDEM Z

Il protocollo ZigBee

Voluto da un consorzio industriale per colmare l'assenza di un protocollo di comunicazione per applicazioni wireless a bassissima potenza, ZigBee opera sullo standard IEEE 802.15.4 traendo vantaggio dalla tecnica Direct Sequence Spread Spectrum.

Lo standard ZigBee definisce un meccanismo di comunicazione paragonabile a quello fornito dal sistema operativo TinyOS (**Error! Reference source not found.**).

Come è stato già detto, Microchip è stato uno dei primi produttori a proporre soluzioni hardware/software per ZigBee. Ha lanciato infatti ad inizio del 2005 un kit dimostrativo comprendente :

- ZigBee software Stack che supporta nodi RFD, FFD Coordinator
- PIC18L4620, una MCU con memoria Flash da 64 KB con robuste periferiche integrate, in tecnologia a bassissimo consumo

- Ricetrasmettitore a radio frequenza con antenna, realizzato su schedina separata per ottenere una maggiore flessibilità che supporta la banda di frequenza dei 2,4GHz a mezzo di un modem RF CC2420 Chipcon (Figura 3.16)
- Connettore di interfaccia ICSP™ e MPLAB ICD2
- Interfaccia RS232
- Regolatore da 9 a 3,3 Volt DC
- Sensore di temperatura (Microchip TC77, LED, e switch per supportare le dimostrazioni)

Microchip fornisce agli sviluppatori uno Stack progettato appositamente per assistere lo sviluppo di applicazioni che implementano il protocollo ZigBee. La libreria dello Stack fornisce un' interfaccia indipendente dal livello fisico. Essa permette di "portare" facilmente le applicazioni da un trasmettitore a radio frequenze ad un altro senza dover ricorrere a significativi cambiamenti nel codice sorgente dell' applicazione. Lo Stack Microchip è stato progettato per evolversi con le specifiche del protocollo wireless ZigBee, che analizzeremo in dettaglio più avanti (3.6).

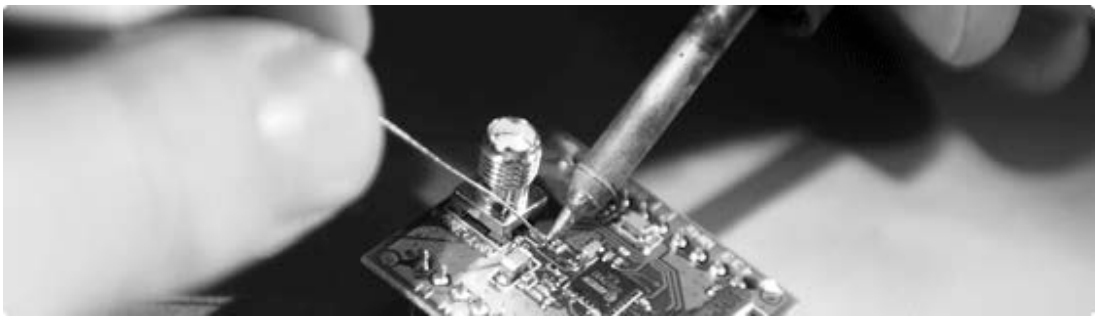

Figura 3.16 – *Il modem RF CC2420 Chipcon*

3.5 SISTEMI OPERATIVI PER LE PIATTAFORME WSN

Disporre di strumenti per limitare il dispendio energetico, anche se fondamentale, non è sufficiente; determinante è anche il modo in cui vengono utilizzate. Parallelamente allo sviluppo di nuove soluzioni hardware, si è sentito il bisogno di una piattaforma software che venisse in aiuto alla programmazione.

Le caratteristiche che deve avere un sistema operativo per piattaforme di sensori wireless sono:

- **semplicità:** a causa delle limitate risorse hardware, l'uso di configurazioni tradizionali (memoria virtuale, processore virtuale, contest-switching) diventa proibitivo.
- **flessibilità:** le applicazioni per le piattaforme sono molto legate all'hardware, che oltretutto può variare da nodo a nodo (per esempio montando sensori diversi); sarebbe perciò importante poter disporre di un sistema flessibile.
- **basato sugli eventi:** diversamente dai calcolatori tradizionali, i sensori wireless sono usati per il monitoraggio e controllo dell'ambiente circostante piuttosto che per elaborazioni general-purpose; è più adatto, quindi, un sistema pilotato da eventi esterni piuttosto che da processi interattivi o batch, anche perché permette di spegnere il microcontrollore nelle fasi di inattività.
- **affidabilità:** a seconda del contesto in cui viene utilizzata la rete, può succedere che il nodo rimanga isolato per mesi prima di poter essere controllato dall'operatore; diventa importante, perciò, ridurre il più possibile la probabilità di errori run-time, che manderebbero in stallo il microprocessore.

3.6 LO STANDARD IEEE 802.15.4 ED IL PROTOCOLLO ZIGBEE

In questo capitolo si parla del protocollo ZigBee della sua nascita delle sue potenzialità e delle miriadi di possibili applicazioni. Viene illustrata la suddivisone delle competenze tra IEEE, ZigBee Alliance ed utente finale (OEM). Si analizzano i vari tipi di reti (stellari o magliate), le tipologie e le gerarchie dei nodi; infine vengono descritti i meccanismi di scambio dati di ZigBee, i nodi endpoint delle reti a stella, le interfacce, i cluster, gli attributi ed i profili, le tabelle di binding ed i formati dei frame ZigBee.

3.6.1 Premessa sulle reti wireless

Le reti wireless sono e saranno sempre più una importante forma di connessione per molte attività, soprattutto per le imprese. Il mercato per i dispositivi wireless è stimato in crescita. Il giro d'affari, di 300 milioni di dollari nel 1998, è passato ad 1,6 miliardi nel 2005. Le reti wireless vengono installate soprattutto negli aeroporti, nelle università, nei parchi pubblici delle grandi città. Un tempo, a causa del prezzo degli apparecchi wireless, questa tecnologia veniva utilizzata solo in caso di condizioni in cui l'uso di cavi era difficile o impossibile.

Mano mano che i prezzi sono diminuiti, però, le WLAN sono entrate anche nelle case, permettendo la condivisione di dati e della connessione Internet tra i computer di una famiglia. Le reti locali Wireless possono utilizzare come mezzo trasmissivo le onde radio, la luce infrarossa o i sistemi laser.

Le onde radio vengono utilizzate dalle reti tipo Wi-Fi cioè reti che devono coprire ambienti eterogenei dove le diverse postazioni da collegare non sono necessariamente visibili, infatti possono essere separate da muri o da intercapedini. Le reti basate su infrarosso vengono utilizzate per collegare dispositivi visibili direttamente, sono lente e spesso utilizzano apparecchi dedicati, infatti sono in disuso e sostituite quasi totalmente dai dispositivi Bluetooth. Le reti basate su Laser vengono utilizzate normalmente per collegare sottoreti costruite utilizzando altre tecnologie. Il Laser viene utilizzato per la sua elevata velocità di trasmissione. Un tipico esempio è il collegamento delle reti di due edifici vicini. Il laser ha il problema di essere sensibile alle condizioni esterne e alle vibrazioni infatti anche queste tipologie di dispositivi sono considerati in disuso e quasi sempre sostituiti da collegamenti via onde radio.

Agli albori delle reti per computer e nei primi anni della loro diffusione si è assistito ad un crescente caos provocato principalmente dalla mancanza di norme e di uno standard comune. La troppa libertà ha portato molte aziende a creare dei propri standard con la conseguente nascita di decine di protocolli differenti e non compatibili fra loro. Da subito è iniziata una lotta fra i produttori al fine di conquistare il maggior numero di utenti che si è risolta solo quando i leader del mercato si sono accordati ed hanno definito dei protocolli comuni.

Ultimamente stanno prendendo sempre più piede le WPAN (wireless personal area network) ovvero delle piccole reti che utilizzano le onde radio al posto degli usuali cavi. Esse sono caratterizzate da una bassa potenza di trasmissione e da velocità non elevatissima che le rende ideali per periferiche a basso consumo o con ridotta autonomia come palmari, cellulari, notebook, ecc. Il fenomeno è in piena espansione e, seppur ci sia chi scommette sulla totale scomparsa dei fili entro pochi anni, si è già registrata una prima battuta d'arresto all'utilizzo smodato delle WPAN. Il primo problema riscontrato è quello legato alle qualità del collegamento, ovvero la resistenza alle interferenze, la qualità del segnale e la sua stabilità poiché, soprattutto con le reti basate su infrarosso è importante l'orientazione fra i trasmettitori. Un altro inconveniente prevedibile, trascurato sull'onda del successo ma riscoperto con l'uso quotidiano, è l'autonomia delle periferiche senza fili. Un mouse, ad esempio, ha un cavo che lo collega al PC e che oltre a trasferire le informazioni sul movimento provvede all'alimentazione della periferica stessa; l'eliminazione di quest'ultimo significa l'utilizzo di batterie ed un maggior dispendio energetico al fine di inviare un segnale radio. Ad oggi il più famoso esempio di WPAN è rappresentato dal Bluetooth anche se l'IEEE (**I**nstitute of **E**lectrical and **E**lectronic **E**ngineers) ha creato il gruppo 802.15 con l'intento di sviluppare altri protocolli (ad esempio ZigBee) al fine di standardizzare e ottimizzare questa interessante tipologia di rete.

Le reti wireless, seppur più comode e flessibili, presentano però degli inconvenienti che sono raggruppabili in cinque categorie: mobilità, interferenze, riservatezza dei dati, consumo di potenza e throughput.

- **Mobilità:** La libertà di movimento è la massima aspirazione di una rete wireless ma comporta delle grandi problematiche nella gestione della comunicazione. Innanzi tutto il segnale radio è, al contrario di quello su cavo, soggetto a rifrazioni e ciò porta ad un effetto eco che disturba e sfasa la comunicazione. Un altro problema è legato alla tecnologia costruttiva di una rete wireless. Succede infatti che per limitare le potenze trasmesse si utilizzino più ripetitori che gestiscono solo una piccola porzione della superficie da coprire (detta cella) ed un apparecchio mobile che si sposta nell'ambiente deve poter passare da un trasmettitore ad un altro in maniera

trasparente e senza perdite.

- **Interferenze:** Il problema delle interferenze può essere dovuto a problemi interni od esterni. Se due apparecchi wireless tentano di comunicare simultaneamente si verifica una sovrapposizione di segnali che li rende entrambi incomprensibili (problema interno) oppure si può ottenere una comunicazione disturbata a causa di un oggetto che nulla ha a che fare con le comunicazioni senza fili come ad esempio un forno a microonde (problema esterno).
- **Riservatezza:** Una rete cablata è abbastanza riservata poiché è difficile, per un malintenzionato, collegarsi alla rete fisicamente ed è altresì facile controllare gli accessi. Le reti wireless comunicano in aria e ciò permette a chiunque di "ascoltare" quanto passa sul canale. Per risolvere il problema sono stati introdotti degli algoritmi di protezione e crittografia a vari livelli che però riducono le prestazioni ed alzano il costo della rete.
- **Consumo:** Mentre i dispositivi fissi sono normalmente alimentati dalla tensione di rete, gli apparati wireless sono alimentati a batteria e dovranno essere quindi progettati per ottimizzare l'efficienza energetica.
- **Throughput:** Le reti wireless, a causa dei limiti fisici e di banda disponibile, sono sempre svantaggiate rispetto alle reti cablate anche se, ad oggi, esistono protocolli e tecnologie in grado di assottigliare il divario tra le due.

Nota: reti PAN (802.15)

Le reti PAN (Personal Area Network) sono reti wireless a corto raggio che si contrappongono alle reti WAN (Wide Area Network) di grande estensione geografica. Oltre allo standard ZigBee fanno parte della famiglia PAN altri due standard principali, Bluetooth e UWB (UltraWide Band). Essi, anche se appartengono alla stessa famiglia, hanno caratteristiche tra di loro molto diverse.

La PAN è gestita da un coordinatore e puμo comprendere due tipologie di dispositivi:

- FFD (Full Function Device): sono dispositivi in grado di effettuare il routing, hanno bisogno di una memoria interna e possono fungere da coordinatori (sono tipicamente alimentati dalla rete);

- RFD (Reduced Function Device): sono in grado di disattivarsi e non possono fare il routing (tipicamente sono alimentati a batteria);

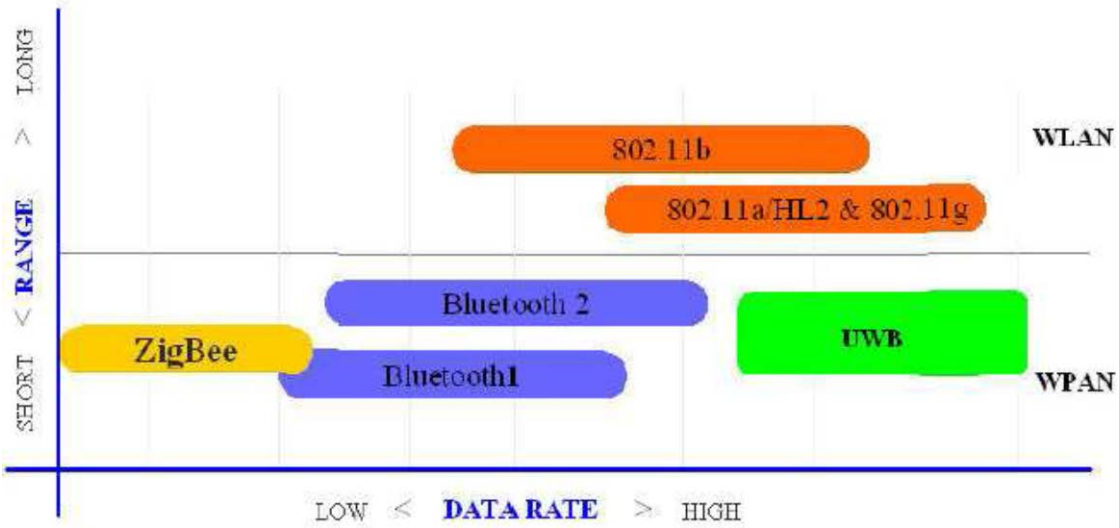

Figura 3.17 – Caratteristiche degli standard Wireless

3.6.2 Le specifiche IEEE 802.15.4

Il protocollo ZigBee usa le specifiche IEEE 802.15.4 per implementare il Medium Access Layer (MAC) ed il Livello Fisico (PHY).

Una rappresentazione grafica delle aree di responsabilità tra la IEEE standard, Zigbee Alliance e lo User è rappresentata nella Figura 3.18.

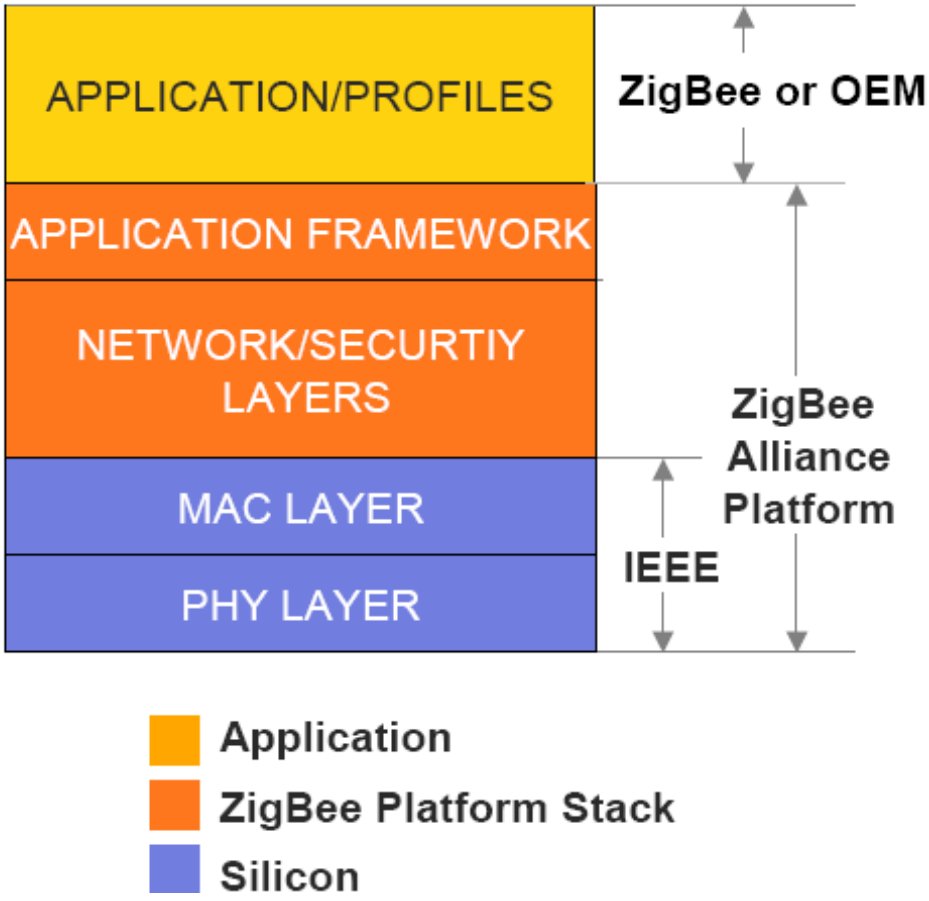

Figura 3.18 – Una rappresentazione grafica delle aree di responsabilità tra lo standard IEEE , Zigbee Alliance e lo User

3.6.3 Caratteristiche della IEEE 802.15.4

- Interfaccia radio DSSS (**D**irect **S**equence **S**pread **S**pectrum)
- Schema IEEE MAC e autoconfigurazione
- Accesso basato su tecnica CSMA-CA (**C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance)
- Power management per assicurare bassi consumi
- Basso costo rispetto a soluzioni Bluetooth

- Frequenze: 16 canali nella banda ISM (2,4 GHz), 10 canali nella banda 915 MHz, 1canale nella banda 868 MHz
- Portata minore di 100 metri
- Basso bit rate: 20 Kbit/s a 868 MHz, 40 Kbit/s a 915 MHz, 250 Kbit/s a 2,4 GHz
- Disponibilità di chipset

La bit rate del protocollo dipende dalla frequenza operativa selezionata, ma in realtà il vero data throughput è minore di quello nominale esposto sopra, in quanto vengono introdotti ritardi durante le fasi di incapsulamento del frame e di gestione dei dati.

La lunghezza massima di un pacchetto MAC IEEE 802.15.4 è di 127 byte.

Ogni pacchetto comprende oltre ai dati utili un' intestazione (header) ed un valore a 16 bit per il CRC. Il valore del CRC serve per verificare l'integrità del frame una volta ricevuto.

In aggiunta, le IEEE 802.15.4 forniscono un meccanismo di trasferimento dati con riconoscimento (Acknowledged). Con questo metodo, tutti i frames con uno speciale flag ACK settato sono riconosciuti dal loro ricevitore. Questo meccanismo si assicura che un frame sia di fatto inviato. Se il frame è trasmesso con un flag ACK settato e il riconoscimento non è ricevuto entro un certo periodo di tempo (time-out), il trasmettitore riproverà la trasmissione per un numero finito di volte prima di generare un errore. E' importante notare che la ricezione di un riconoscimento indica semplicemente che un frame è stato ricevuto correttamente dal livello MAC . Non indica però che il frame sia stato processato correttamente. E' possibile che il livello MAC del nodo ricevente riceva e riconosca un frame correttamente, ma per mancanza di risorse, questo possa venire scartato dai livelli superiori. Come risultato, molti dei livelli superiori e delle applicazioni richiedono ulteriori risposte ai riconoscimenti.

3.6.4 Le origini di ZigBee

I primi studi su ZigBee risalgono al 1998 da parte della Motorola ma è solo con la versione V0.2 (rilasciata alla fine del 2000) che sono iniziati gli studi del IEEE (*Institute for Electric and Electronic Engineering*). Nel 2002 nasce ZigBee Alliance, un'associazione di

compagnie (Motorola, Mitsubishi, Honeywell ecc.) che lavorano insieme per realizzare prodotti di basso costo, bassa potenza e corto raggio per la monitorizzazione ed il controllo. La pubblicazione dello standard dell'IEEE 802.15.4 riguardante i primi due livelli del protocollo ZigBee è del 1° ottobre 2003. La prima versione dei livelli superiori è del 12 dicembre 2004, ma lo standard sui livelli superiori è ancora oggi riservato ai membri della ZigBee Alliance (Figura 3.18).

ZigBee è un nome di fantasia, (richiama il volo di uno sciame di api, per dare l' idea di una rete costituita da tanti nodi piccoli e cooperanti), che il comitato dei produttori ha scelto per questa tecnologia, progettata con l' obiettivo di realizzare reti di sensori wireless a bassa velocità, basso costo, bassissimo consumo energetico, elevata affidabilità, per applicazioni di monitoraggio remoto, domotica e building automation, nei mercati industriali e consumer. Si prevede che lo standard ZigBee sarà largamente utilizzato per connettere non solo sensori, videocitofoni, sistemi d'allarme e strumenti per l'automazione domestica, ma anche micro-sensori per monitorare e controllare le reti e ogni tipo di impianto. Infatti, degli oltre otto miliardi di micro-sensori inseriti ogni anno in tutti i prodotti, meno del 2% può essere attualmente connesso in rete mentre per le applicazioni industriali e domestiche sarebbe utile collegarne almeno il 20%. Grazie ai consumi ridotti, un sensore Zigbee può funzionare da 2 a 5 anni con due sole batterie alcaline AA. Lo standard IEEE 802.15.4, presentato in forma ufficiale a fine 2004, prevede 16 canali nella banda radio di 2,4 GHz (la stessa banda di Bluetooth, di WiFi e dei forni a microonde) e una velocità di trasmissione dei dati da 20 a 250 Kbps fino a 75 metri di distanza. Un dispositivo ZigBee deve avere un errore di frequenza rispetto al centro del canale di al massimo ± 40 ppm. Il trasmettitore deve essere capace di trasmettere almeno a -3 dBm ed il livello di input massimo di segnale accettabile per il ricevitore deve essere maggiore o uguale a -20 dBm.

Per queste potenzialità lo Zigbee è considerato da alcuni osservatori "la prossima vera rivoluzione nel wireless". Dopo i primi progetti pilota nel 2005, nel 2006 si prevede la crescita di ZigBee nel settore dell'automazione delle abitazioni e nel settore industriale. A partire dal 2007, l'integrazione in un'ampia gamma di prodotti di largo consumo. Secondo

le previsioni dei principali analisti di mercato, gli oggetti con ZigBee a bordo venduti nel mondo saranno 80 milioni entro la fine del 2006 e 150 milioni nel 2008.

3.6.5 Il protocollo ZigBee

Lo scopo del protocollo ZigBee è quello di fornire il supporto per reti *wireless* a basso consumo di energia e corto raggio. Questa tecnologia consente il rimpiazzo di cavi di collegamento tra dispositivi realizzando un collegamento radio. Sensori, spie luminose, impianti di condizionamento, segnalatori di posizione a breve raggio, tutti questi dispositivi possono far parte di un unico sistema ZigBee. Oltre a sostituire i cavi, ZigBee può agire da collegamento verso reti preesistenti (ovvero agire da *bridge*) oppure può essere visto come un sistema per realizzare piccole reti ad hoc quando ci si trova lontano da altre infrastrutture di rete.

Come abbiamo già visto, il protocollo è strutturato su cinque livelli (Figura 3.19): quelli superiori sono stati definiti dalla *ZigBee Alliance* mentre il livello MAC (Media Access Control) e il livello PHY (Fisico) sono definiti dallo standard IEEE 802.15.4.

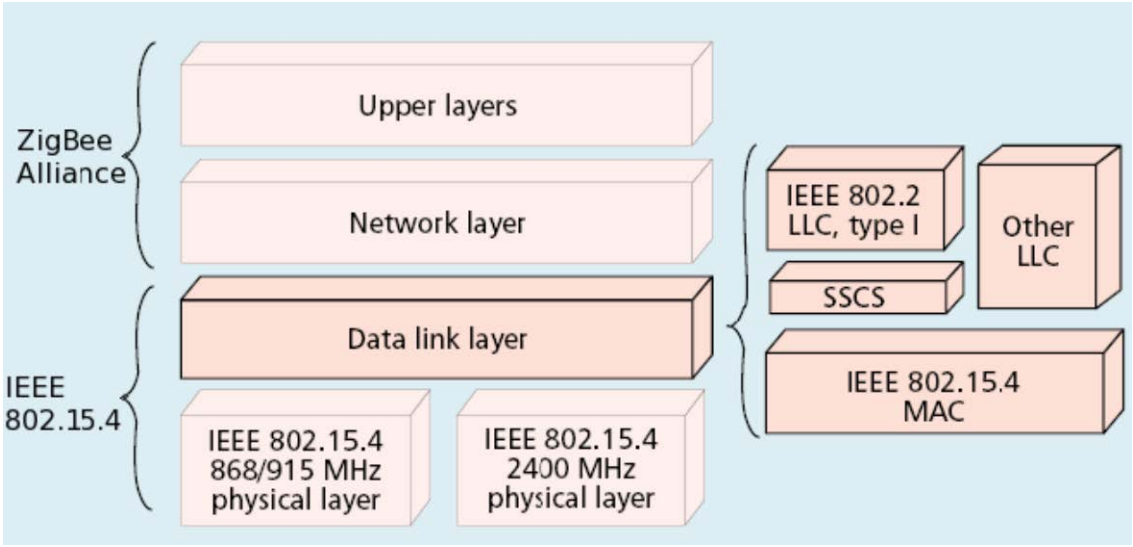

Figura 3.19 – Livelli del protocollo ZigBee

Il protocollo ZigBee individua i seguenti tipi di dispositivi logici all' interno di una rete: i Coordinatori, i Routers e le End Devices.

I Coordinatori inizializzano una rete, controllano i nodi della rete, mantengono informazioni sui nodi della sua PAN (Personal Area Network). I Routers prendono parte alla rete instradando-smistando i messaggi tra nodi accoppiati. Le End Devices agiscono nella rete come nodi terminali e possono essere un RFD o un FFD.

Un RFD è il più piccolo e il più semplice nodo ZigBee. Esso infatti implementa solo un set ridotto dei servizi ZigBee. Il coordinatore è una variante speciale di una Full Function Device che implementa un set più vasto di servizi ZigBee.

Una rete IEEE 802.15.4/ZigBee richiede almeno un dispositivo FFD come coordinatore, mentre tutti gli altri dispositivi possono essere RFD per ridurre i costi. Un dispositivo RFD è implementato usando la minima quantità di memoria RAM e ROM possibile ed è progettato per essere un semplice nodo trasmettitore e/o ricevitore in una rete più grande. Con una dimensione dello stack ZigBee ridotta è richiesta meno memoria ottenendo così un circuito integrato meno costoso. I dispositivi RFD dello Zigbee sono generalmente alimentati per mezzo di una batteria. Un dispositivo RFD può cercare reti disponibili, trasferire dati dalla sua applicazione quando necessario, stabilire se ci sono dati in attesa di essere trasferiti , richiedere dati dal coordinatore della rete e rimanere inattivo per lunghi periodi di tempo per ridurre il consumo di energia. Un dispositivo RFD può colloquiare solo con un dispositivo FFD, cioè un dispositivo con sufficiente risorse di sistema per effettuare il routing della rete. Un FFD può servire come coordinatore della rete, coordinatore di link o come dispositivo di comunicazione. Qualunque FFD può colloquiare con qualsiasi altro FFD e RFD. I FFD rivelano altri FFD e RFD per stabilire comunicazioni e tipicamente sono alimentati via cavo.

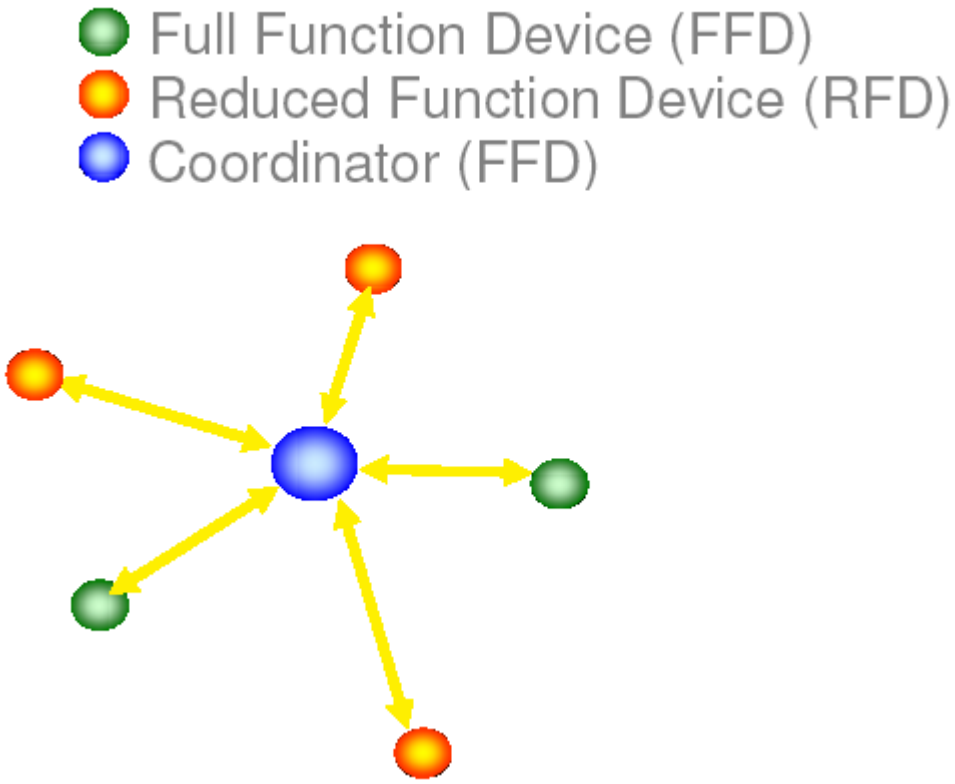

Figura 3.20 – *Esempio di rete wireless ZigBee*

Riassumendo, in corrispondenza della classificazione vista prima avremo tre differenti tipi di dispositivo ZigBee:

- **ZigBee Coordinator:** E' il dispositivo più "intelligente" tra quelli disponibili, costituisce la radice di una rete ZigBee e può operare da ponte tra più reti. Ci può essere un solo Coordinator in ogni rete. Esso è inoltre in grado di memorizzare informazioni riguardo alla sua rete.
- **ZigBee Ro**uter: Questi dispositivi agiscono come router intermedi passando i dati da e verso altri dispositivi.
- **ZigBee End Device:** Includono solo le funzionalità minime per dialogare con il suo nodo parente (Coordinator o Router). E' il dispositivo che richiede il minor quantitativo di memoria e quindi risulta spesso più economico rispetto ai ZR o ai ZC.

Una rete wireless ZigBee può assumere diversi tipi di configurazioni.

Una configurazione a rete a stella (star network) consiste in un nodo coordinatore ("master") ed una o più end devices ("slaves"). In una rete a stella, tutte le end devices comunicano solo con il coordinatore. Se una end device deve trasferire dei dati verso un' altra end device, manda prima i suoi dati al coordinatore che li invia al corretto end device ricevente.Oltre alla rete a stella, una rete ZigBee può assumere diverse configurazioni tra le quali citiamo il peer-to-peer, il cluster tree o la mesh (rete a maglia). L'architettura di rete a maglia permette ai dati e ai messaggi di controllo di essere trasferiti da un nodo l'altro attraverso più vie. Questa interessante proprietà rende questa tipologia di rete molto diffusa e migliora l'affidabilità dei dati. Questa capacità peer-to-peer può essere usata per costruire reti grandi e geograficamente sparse dove piccole reti sono collegate assieme per formare una rete "cluster tree" . Le reti di tipo cluster e mesh sono anche dette reti multi-hop, grazie alle loro abilità di instradare pacchetti attraverso diversi nodi , mentre la configurazione a stella è definita come rete a single-hop.

Come in ogni rete, una rete ZigBee è una rete di tipo multi-access, una rete nella quale ogni nodo presente abbia uguale accesso al mezzo di comunicazione. Esistono due tipi di meccanismi per implementare il multi-access. In una rete abilitata di tipo beacon, ai nodi è permesso trasmettere solamente in predefiniti intervalli temporali (time slots). Il coordinatore periodicamente inizia con un superframe identificato come beacon frame e al quale tutti i nodi presenti nella rete devono sincronizzarsi. Ad ogni nodo è assegnato uno specifico intervallo (slot) nel superframe nel quale gli è permesso ricevere e trasmettere i suoi dati. Un superframe può anche contenere uno slot in comune durante il quale tutti i nodi competono per accedere al canale.

La versione corrente dello Stack Microchip supporta solamente reti a stella di tipo non beacon.

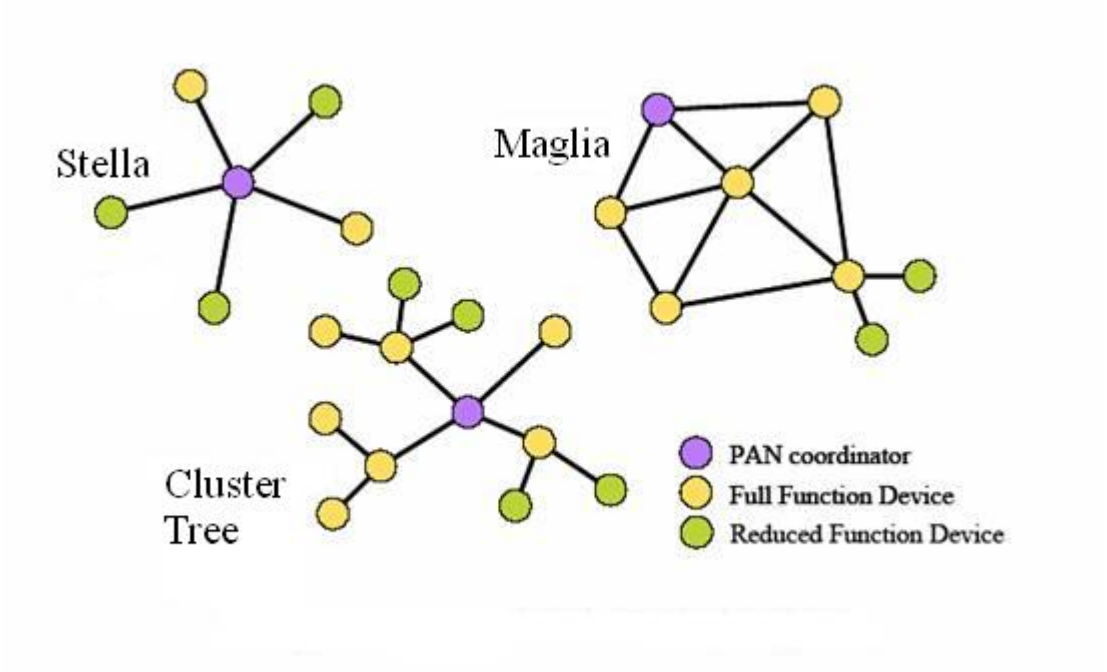

Figura 3.21 – *Topologia delle reti ZigBee*

3.6.6 Network Association

Le reti ZigBee possono essere costruite ad-hoc, ciò significa che si tratta di una rete autoconfigurante "non" gerarchica nella quale i nodi possono assumere la capacità di instradamento selettivo. Vantaggi di una configurazione "ad-hoc:

- Natura intrinseca di propagazione wireless: variabilità della connettività anche in presenza di nodi statici
- Auto adattività della rete al variare delle condizioni operative
- Design dei protocolli di rete per l' adattamento a condizioni variabili
- Affidabilità: distribuzione delle informazioni su diversi percorsi.

In una rete a configurazione di tipo stella, le end devices cercano sempre una rete prima di iniziare un trasferimento dati. Una nuova rete è sempre stabilita da un coordinatore. Durante la fase di inizializzazione, un coordinatore cerca altri coordinatori vicini e se non ne trova , realizza una propria rete e seleziona un univoco identificatore PAN ID a 16 bit. Una volta stabilita la nuova rete, una o più end devices possono associarvisi. La decisione di permettere o negare la nuova associazione alla rete dipende dal coordinatore.

Quando la rete è formata, è possibile che per via di cambiamenti fisici, più reti possano sovrapporsi e sorgano conflitti di PAN ID. In questa situazione, un coordinatore inizierebbe una procedura di risoluzione dei conflitti PAN ID e l'altro cambierebbe il proprio PAN ID o canale ed istruirebbe tutte le sue end devices per i necessari cambiamenti. Un coordinatore può memorizzare tutte le associazioni della rete in una memoria non volatile, chiamata neighbor table. Per procedere alla connessione ad una rete, una end device deve eseguire la procedura di notifica orfano per trovare la rete alla quale era precedentemente associata o eseguire la procedura per inserirsi in una nuova rete. Nel primo caso , il coordinatore riconoscerà una end device precedentemente associata esaminando la propria neighbor table. Una volta associata ad una rete , una end devices può scegliere di dissociarsi dalla rete eseguendo la procedura di rimozione. Se richiesto, un coordinatore può iniziare una procedura di rimozione per forzare un nodo a lasciare la rete. La versione dello Stack ZigBee che ho utilizzato supporta solo la procedura di rimozione richiesta da end devices.

3.6.7 Meccanismi di scambio dati di ZigBee

In questo paragrafo vengono descritti i meccanismi di scambio dati di ZigBee, i nodi endpoint delle reti a stella, le interfacce, i cluster, gli attributi ed i profili, le tabelle di binding ed i formati dei frame ZigBee.

3.6.7.1 Endpoints, Interfacce, Clusters, Attributi e Profili

Secondo il protocollo ZigBee, un nodo è definito come un insieme di descrizioni ed applicazioni di un dispositivo indipendente le quali risiedono nella stessa unità. Un tipico nodo ZigBee può supportare diverse funzionalità. Per esempio, un nodo di Input/Output può avere diverse porte di I/O analogiche e digitali. Alcune porte di input digitali possono essere usate da un nodo controllore remoto e le altre da un altro nodo. Queste disposizioni permettono di creare una vera rete di controllo distribuita. Per facilitare il trasferimento di dati tra i nodi di I/O ed i due nodi controllori, le applicazioni in tutti i nodi devono mantenere diversi collegamenti tra i dati. Per ridurre i costi , un nodo ZigBee

usa solo un canale radio e diverse enpoints/interfacce per creare collegamenti virtuali o canali. Un endpoint è definito come un particolare componente all' interno di una unità. Un nodo ZigBee supporta 31 endpoints (numerati da 0 a 31) e 8 interfacce (numerate da 0 a 7). L' endpoint 0 è riservato solo per il broadcast. In questo modo si ha un totale di 30 endpoints disponibili per le applicazioni. Per ogni endpoint sono disponibili un totale di 8 interfacce. Quindi , in realtà, un' applicazione può disporre fino a 240 canali virtuali in un unico canale fisico.

Un tipico nodo ZigBee può anche disporre di molti attributi. Un attributo è definito come un' entità dato che rappresenta una quantità fisica o uno stato. Per esempio, un nodo I/O contiene diversi attributi chiamati input_digitale_#1 , input_digitale_#2 , input_analogico_#1 ed output_analogico_#1. Ogni attributo avrà un determinato valore. Per esempio, l' attributo input_digitale_#1 potrà valere 1 o 0. Un insieme di attributi è chiamato Cluster. Ad ogni cluster è assegnato un unico cluster ID nell' intera rete. Ogni cluster può avere fino a 65536 attributi.

Il protocollo ZigBee definisce un termine chiamato profilo. Un profilo è sinonimo di descrizione di un' applicazione distribuita. Un profilo descrive un' applicazione distribuita in termini di pacchetti che deve gestire e di azioni che deve eseguire. Un profilo è descritto usando un 'descrittore', che altro non è che una complessa struttura di diversi valori. E' il profilo che permette ai dispositivi ZigBee di essere interoperabili. La ZigBee Alliance ha definito molti profili standard, tra i quali citiamo la gestione remota di interruttori, e la gestione di sensori ottici. Qualsiasi nodo che si conformerà ad uno di questi profili standard sarà interoperabile con altri nodi che implementano lo stesso profilo.

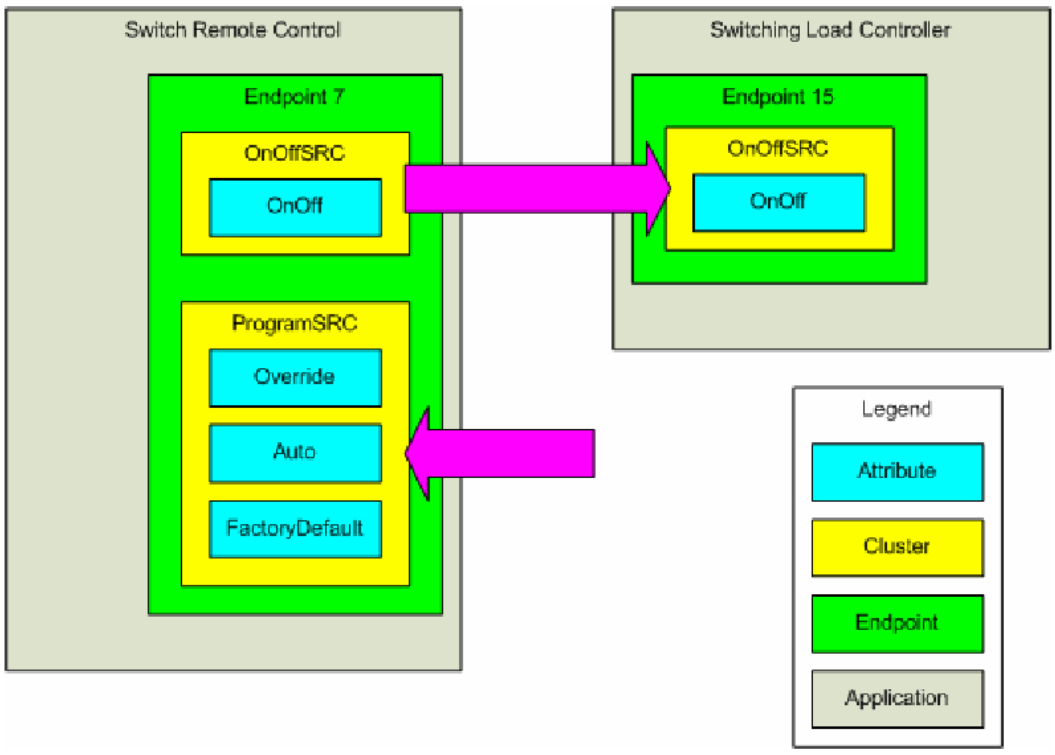

Figura 3.22 – Applicazioni, Endpoint, Cluster e Attributi

Le applicazioni in Figura 3.22 mostrano un tipico esempio di implementazione di un profilo per l' automazione domestica (domotica). L' applicazione Switch Remote Control gestisce un endpoint che utilizza due Cluster (OnOffSRC e ProgramSRC) entrambi già definiti dalle specifiche ZigBee. Il cluster OnOffSRC descrive tutte i dispositivi che gestiscono un interrutore remoto (switch). L' applicazione Switch Remote Control potrebbe controllare l' accensione o lo spegnimento di una lampadina locata in un nodo remoto. L'applicazione utilizza l' attributo OnOff che descrive lo stato del dispositivo interruttore. Il valore di questo attributo è rappresentabile ad esempio da una variabile booleana (On,Off) oppure da un intero che può descrivere i diversi stati che può assumere l' interrutore. Oltre ai due stati già descritti si potrebbe definirne un terzo denominato TOGGLE che permette di invertire lo stato già impostato nell' attributo OnOff del dispositivo Switch Remote Controller. L' applicazione che controlla lo stato dell' attributo riceve dal nodo coordinatore lo stato da impostare e lo elabora. La figura

mostra che l' endpoint 7 gestisce oltre allo stato dell' interruttore anche un cluster denominato ProgramSRC. Questo cluster utilizza tre diversi attributi. E' interessante notare che in questo caso l'endpoint 7 può solo ricevere informazioni riguardo questo cluster. E' possibile attribuire ad ogni endpoint dei cluster in ingresso e in uscita. L' endpoint gestirà in modo differente i due cluster. Un terzo nodo potrebbe essere il responsabile della trasmissione di questi attributi. Potrebbe ad esempio interpretarsi come una richiesta di informazioni da un nodo elaboratore che fornisce le informazioni sullo stato di tutti i dispositvi presenti in una casa. Questo attributo verrebbe gestitito dal Switch Remote Control che controlla il valore assegnato all' attributo Auto dal terzo nodo e decidere di elaborarlo nel modo più appropriato. E' necessario però che ogni endpoint abbia eseguito un binding con il nodo con cui dovrà interagire.

3.6.7.2 Endpoint Binding

Come menzionato precedentemente, in una rete a stella un end device deve sempre comunicare con un coordinatore. Quest' ultimo è responsabile dell' instradamento dei pacchetti inviati da un end point di un nodo ad un altro end point nel dispositivo ricevente. Quando viene stabilita una nuova rete, al coordinatore deve essere comunicato come creare un collegamento tra un endpoint sorgente ed un endpoint destinazione. Il protocollo ZigBee definisce una speciale procedura chiamata endpoint binding. Come parte del processo di binding, un nodo gestore remoto di rete / dispositivo può chiedere al coordinatore di modificare la sua binding table. Il nodo coordinatore mantiene una binding table che essenzialmente contiene un collegamento logico tra due o più endpoints. Ogni collegamento è definito univocamente dal suo endpoint sorgente e dall' identificatore del cluster (cluster ID). Per esempio, se i dati input_digitale_#1 del nostro nodo I/O devono essere inviati al canale_controllo_#1 del nodo controllore, si deve chiedere al coordinatore di creare una riga nella tabella di binding nella quale si specificherà che input_digitale_#1 del nodo I/O sarà l'enpoint sorgente mentre canale_controllo_#1 del nodo controllore sarà l'endpoint destinazione. Creata la riga nella tabella di binding, ogni volta che il nodo I/O invia dati dal suo endpoint input_digitale_#1, il node coordinatore esaminerà la propria tabella di binding ed

instraderà il pacchetto all' endpoint canale_controllo_#1 del nodo controllore. Sia input_digitale_#1 sia canale_controllo_#1 condividerranno un identificatore cluster in comune. In funzione di come viene creata la tabella di binding, e possibile realizzare un multicast di dati da un endpoint a più endpoint su più nodi.

Il protocollo ZigBee definisce uno speciale oggetto software chiamato ZigBee Device Object (ZDO), il quale fornisce i servizi di binding oltre a molte altre funzioni. Solo lo ZDO eseguito su un coordinatore fornisce i servizi di binding. Un gestore remoto di rete / dispositivo lancerà una speciale richiesta di binding diretta al ZDO (endpoint 0) per creare o modificare una riga nella tabella di binding. In questo modo è possibile che un pc che esegue un software di emulazione nodo possa gestire una rete ZigBee. Nelle applicazioni ho implementato un meccanismo di binding semplice ed elementare basato su eventi e procedure a stati finiti. Questo meccanismo permette ad ogni nodo di inviare la propria richiesta di binding all' oggetto ZDO (endpoint 0) del nodo coordinatore.

3.6.7.3 Formati dei frame ZigBee

Il protocollo Zigbee definisce due formati per i frame: il Key Value Pair (KVP) ed il Message (MSG). Entrambi sono associati con un cluster ID, ma i frame KVP sono stati progettati per trasferire un' informazione associata ad un attributo usando una struttura fissa, mentre i frame MSG trasferiscono l' informazione senza usare strutture (si passerà in questo caso un puntatore ai dati e la loro dimensione). Il profilo per le applicazioni specificherà quale formato per il frame dovrebbe essere usato per trasferire quale informazione e la struttura di eventuali frame MSG. Per via di differenze nel formato, un cluster non può contenere entrambe le strutture dei frame. Esaminando le note applicative dello Stack ZigBee ho cercato di capire quale fosse il formato più conveniente per scambiare informazioni tra due nodi. La conclusione è che dipende dal tipo di dato da trasmettere. Se si desidera scambiare una serie di dati, ad esempio molti attributi, in un'unica sessione converrebbe utilizzare il formato MSG. Trasmettere molti dati con un formato KVP è possibile ma impiegherebbe più tempo ed impiegherebbe molte risorse del nodo controllore (ad esempio l' occupazione di un canale) a scapito degli altri nodi. La differenza più marcata sembra comunque riguardare l' utilizzo degli attributi. Il formato

KVP è fortemente legato alla definizione di attributi e di cluster mentre il formato MSG permette di utilizzare un livello di astrazione maggiore lasciando più libertà nella gestione dei dati allo sviluppatore. Per trasmettere un dato con il formato MSG è necessario fornire solo la lunghezza dei dati ed i valori. Per implementare la mia applicazione ho utilizzato il formato KVP perchè è semplice da usare, non richiedendo l'utilizzo di puntatori ne allocazione di memoria per i dati. Inoltre dovendo trasmettere dei singoli tipi di dato il formato KVP mi garantiva una minore elaborazione in fase di ricezione in quanto necessita solo di riconoscere il cluster e di verificare che l' attributo ricevuto sia effettivamente quello richiesto.

3.6.8 Applicazioni ZigBee

Le possibili applicazioni dello standard ZigBee sono molteplici, tra cui: Monitoring (reti di sensori, controllo merci), Building Automation (sicurezza, lettura automatica di contatori, controllo luci e accessi, sistema di condizionamento HVAC...), Controllo Salute (monitoraggio pazienti...), Industrial Automation (controllo fasi di lavoro per ottimizzare i processi, gestione energia...), Consumer Electronic (TV, VCR, DVD/CD...), PC e Periferiche (mouse, tastiera...) e Home Automation (sicurezza, HVAC, controllo luci e accessi, sistema di irrigazione...).

3.6.9 ZigBee VS Bluetooth

Dopo aver visto le potenzialità e le caratteristiche dello standard ZigBee viene da pensare subito ad un'altra tecnologia che da anni è entrata nelle nostre case e nelle nostre tasche (in tutti i cellulari di ultima generazione) e che sembra simile a questa: Bluetooth.

Il paragone fra ZigBee e Bluetooth è utile solo se prima si capisce per cosa sono stati ideati i due protocolli. Anche se entrambi possono essere usati per le medesime applicazioni è pur vero che ognuno di essi presenta dei punti di forza e delle debolezze. Il più grande problema di ZigBee è la velocità di trasmissione e la relativamente piccola distanza di propagazione mentre Bluetooth paga principalmente un consumo di energia molto elevato. I punti di forza di una tecnologia sono i difetti dell'altra ed ecco così che

ZigBee brilla per la sua lunga autonomia mentre Bluetooth garantisce elevate velocità di trasmissione. Ciò chiarisce che un confronto fra le due tecnologie è quasi impossibile e sarebbe come confrontare, se pensassimo in termini automobilistici, una piccola utilitaria con una Ferrari: la prima è lenta ma consuma poco mentre la seconda è velocissima ma richiede molto più carburante per uno stesso tragitto.

Alla luce di ciò non è possibile scegliere quale dei due è meglio ma solo pensare a ciò che intendiamo realizzare e valutare se uno di essi presenta più vantaggi rispetto all'altro. Inizialmente il Bluetooth era utilizzato nella comunicazione fra sensori e centraline di raccolta dati poiché sembrava già un buon compromesso in grado di offrire bassi consumi e discreta velocità. L'avvento di ZigBee ha soppiantato la vecchia tecnologia poiché i sensori sono alimentati da pacchi di batterie che sarebbe utile ottimizzare ed inoltre, poiché i sensori non devono trasmettere grandi moli di dati, non è necessaria una grande banda di trasmissione.

Un campo in cui al momento ZigBee non sembra riuscire a incidere è proprio quello dei cellulari poiché se da un lato c'è la necessità di allungare la durata delle batterie, dall'altro ci si scontra con la velocità di trasmissione richiesta fra apparecchi mobili. Si preferisce infatti che un cellulare possa scambiare foto e messaggi in maniera rapida piuttosto che risparmiare energia ed impiegare 8 volte tanto.

Di seguito una tabella riassuntiva puramente indicativa che tiene conto della media dei consumi di alcune piattaforme Bluetooth rispetto ad alla media di piattaforme ZigBee.

Modalità	***Assorbimento Bluetooth***	***Assorbimento ZigBee***
Sleep	4 mA	1 μA
Trasmissione	17 mA	17 mA
Ricezione	20 mA	19,7 mA

Si nota subito che a far la differenza non è tanto il consumo durante la trasmissione o la ricezione bensì il consumo in stato Sleep. Se torniamo agli esempi precedenti e consideriamo nuovamente il caso del sensore che deve, su richiesta della centralina, spedire un'informazione e tornare in standby, è ovvio che la scelta cada su ZigBee poiché consuma 4000 volte di meno. Il caso del cellulare è invece opposto poiché la trasmissione

Bluetooth è attivata dall'utilizzatore solo quando serve e non esiste quindi la fase di standby.

Un altro aspetto che finora non è stato preso in considerazione poiché non legato direttamente alle prestazioni dei protocolli ma che si rivela importantissimo per l'uso di tutti i giorni è il fattore sicurezza.

Poiché personalmente non siamo in grado di analizzare i due protocolli e non possiamo quindi notare le differenze a basso livello abbiamo preso spunto da pubblicazioni di altri ricercatori (chiaramente esplicitati nel seguito).

Per quanto riguarda ZigBee, durante la fase di handshake, si verifica che la comunicazione non sia sicura poiché non è ancora stata definita la chiave simmetrica da utilizzare per la connessione (la chiave simmetrica è l'unico meccanismo messo a disposizione da ZigBee). L'algoritmo AES utilizza la modalità CTR per generare la chiave di sessione (che viene cambiata frequentemente). La chiave di sessione è a sua volta utilizzata per cifrare i pacchetti da inviare. La chiave di sessione, però, è costruita a partire da un'altra chiave simmetrica che i due dispositivi devono conoscere al momento di iniziare il procedimento di autenticazione e/o cifratura. Ogni nodo possiede una chiave simmetrica per ogni ACL entry riferito ad un altro nodo della rete. Se questa è conosciuta a priori dai dispositivi, tutti gli algoritmi di cifratura successivi possono considerarsi sicuri.

Cambiando protocollo, e passando quindi a Bluetooth, una falla nella sicurezza è nota dall'Aprile 2004 e si ha nella fase di handshake iniziale, nel momento in cui le unità si accordano sulla chiave simmetrica a 128 bit da usare. Durante questa fase tutta la sicurezza si appoggia su un codice PIN (Personal Identification Number) immesso dall'utente. Dovendo essere immesso manualmente si usano per il PIN cifre decimali e ciò equivale a non sfruttare a pieno la potenza dei 16 byte della chiave. Immettendo infatti una chiave di 16 byte si avrebbero 65536 combinazioni possibili mentre usando la base decimale si utilizzano solo 4 cifre (con 5 cifre avremmo 99999 combinazioni, non rappresentabili con 16 byte) e quindi 9999 combinazioni. Sfruttando questo difetto se si riescono a trovare due dispositivi in fase di handshake è possibile trovare il PIN in un range di 9999 combinazioni possibili. Essa poteva sembrare una falla accettabile poiché questa procedura viene effettuata solo una volta e per un arco di tempo molto ridotto.

Nel Giugno del 2005 però i ricercatori Y. Shaked e A. Wool hanno trovato un sistema per cui è possibile far ripetere la fase di handskake ad un dispositivo già autenticato. Questa forzatura si basa sul BD_ADDR che ogni dispositivo Bluetooth ha e deve condividere pubblicamente. L'attacco, a detta dei ricercatori, è possibile in una frazione di secondo e con una macchina di media potenza [25].

In conclusione si può affermare che per il protocollo Bluetooth esiste almeno una falla che ne compromette l'affidabilità. Per quanto riguarda ZigBee non si conoscono ancora problemi di sicurezza ma questo avviene principalmente perchè il protocollo è molto giovane, non molto impiegato ed in più presuppone che gli sviluppatori dei livelli superiori provvedano a completare la parte di sicurezza non implementata al livello MAC. La parte di sicurezza che non viene implementata al livello MAC per ZigBee è proprio la fase di handshake. Se questa non sarà prevista dal protocollo e ci si limiterà a registrare su ogni nodo un numero finito di chiavi simmetriche per un altrettanto numero finito di nodi con cui comunicare, il protocollo è da considerarsi sicuro. In tale caso, però, il protocollo sarebbe notevolmente limitato. Viceversa, se si permette di aggiungere nuove ACL entry e quindi nuove chiavi di sicurezza per ogni dispositivo che viene scoperto durante la vita di un nodo, il problema dell'handshake rimarrebbe anche per ZigBee ancora da risolvere.

4 SCENARI APPLICATIVI

Di seguito vengono presentate applicazioni sia consolidate sia sperimentali delle tecnologie RFID e WSN. La finalità è quella di offrire spunti di innovazione da utilizzare negli ambiti applicativi caratteristici dell'area Alpi-Mediterraneo.

4.1 APPLICAZIONI RFID

La tecnologia RFID è applicata in moltissimi settori anche totalmente eterogenei, quali ad esempio:

- Logistica:
  - Stoccaggio e spedizioni delle merce
  - Identificazione pallets, stazioni di lavoro
  - Gestione rifiuti
  - Magazzini automatici
  - Ronde di sorveglianza

- Industriale:
  - Robotica e automazione
  - Controllo nei processi di produzione
  - Gestione dati nel controllo qualità
  - Lavanderie industriali
  - Identificazioni utensili nelle macchine automatiche
- Automotive:
  - Immobilizzatori per auto, motocicli, barche con transponder implementato nella chiave di accensione
  - Sistemi di sicurezza
  - Controllo del parco auto e loro manutenzione
  - Localizzazione di automezzi

- Anticontraffazione:
    - Etichette con transponder implementato contro la contraffazione di beni di lusso
    - Identificazione passaporti e/o documenti personali
    - Certificati di origine
- Agro-alimentare, animali e piante:
    - Identificazione animali con transponder iniettato (normativa ISO 11784/11785)
    - Controllo filiera e qualità agro-alimentare
    - Registrazione e controllo caratteristiche di origine
    - Protezioni prodotti tipici e anti contraffazione
    - Identificazione univoca animali e piante
    - Automazione macelli
    - Controllo migrazione
- Controllo accessi e ticketing:
    - Sistemi di controllo a "mani libere"
    - Aperture porte, cancelli, serrande garage
    - *Building* automation
    - Sistemi di controllo accessi
    - Gestione parcheggi
    - Gestione documentale e archivi storici
    - Carte prepagate
    - Sistemi di pagamento per autobus, ferrovie telefono
    - Erogazione di servizi sul territorio
    - Distributori automatici
    - Abilitazione a computer, stampanti, copiatrici

Presentiamo di seguito un insieme dei principali scenari applicativi per le tecnologie basate su RFID, tenendo conto sia delle applicazioni e dei progetti in corso, sia di quelli attesi in prospettiva.

4.1.1 Sanità

Il settore sanitario è ancora caratterizzato da una netta prevalenza di progetti sperimentali, che vanno a toccare diversi ambiti, con particolare attenzione alla gestione del rischio clinico per la prevenzione degli errori. Avendo come riferimento il paziente e la sua condizione clinica, alcune applicazioni sono: la corretta associazione tra paziente e percorso di cura, l'accesso ai dati presenti sulla cartella clinica, il monitoraggio del percorso clinico del paziente in pronto soccorso, la localizzazione, la tracciabilità e la gestione inventariale di dispositivi medici (elettrobiomedicali, come i defibrillatori, e non, come i letti). L'autenticazione di un farmaco attraverso un'etichetta RFID consente, oltre a tracciare il prodotto, di proteggersi dalle contraffazioni e di migliorare l'efficienza dei processi, velocizzando e semplificando il ricevimento e la consegna della merce.

Mentre l'esperienza ha ridimensionato i dubbi circa le potenziali interferenze tra i dispositivi RFID e le apparecchiature mediche, il principale ostacolo che caratterizza questi progetti è la limitata estensione funzionale delle applicazioni, che tendono ad essere focalizzate su una singola fase del percorso clinico del paziente, e la difficoltà a personalizzarle in relazione alla specifica esigenza dell'utente.
Le frequenze utilizzate sono UHF/HF a seconda dell'applicazione (UHF: monitoraggio del trasporto dei farmaci; HF: scaffali delle farmacie ospedaliere).
Vediamo alcuni esempi di sistemi attualmente in uso o in sperimentazione presso diverse strutture mediche:

- Braccialetti RFID funzionanti in tecnologia HF (13.56 MHz) per consentire la corretta identificazione tra madri, neonati e rispettive cartelle cliniche.
- Informatizzazione dell'intero ciclo di gestione del farmaco nell'ambito delle attività di reparto: attraverso un sistema wireless le richieste pervengono alla farmacia ospedaliera che movimenta i farmaci sfruttando le etichette intelligenti di

cui sono stati dotati dalle stesse aziende produttrici. Al momento della somministrazione gli operatori possono controllare la corretta associazione farmaco – paziente, confrontando i dati contenuti su un braccialetto RFID di cui è dotato il paziente nella fase di accettazione.

Gli Standard utilizzati sono: EPC Class1 Gen2 (UHF) e ISO 15693 (HF). Si prediligono etichette dalle dimensioni ridotte, come il modello Mini che misura 24 mm x 24 mm (UHF); anche per le smart label in tecnologia HF si preferiscono le misure contenute, tra 15 e 45 mm per lato.

Figura 3.23 – Esempi di Braccialetti RFID e farmaco con Tag inserito nell'etichetta

4.1.2 Pubblica amministrazione

In questo settore le applicazioni sono principalmente focalizzate su due ambiti specifici: l'identificazione dei cittadini e la gestione dei beni di valore. Per quanto riguarda il primo, è già stato portato a compimento il progetto "passaporto elettronico", mentre sono in fase di emissione le Carte Nazionali dei Servizi, che permettono ai cittadini di usufruire

dei servizi forniti dalla pubblica amministrazione, per via telematica. Nell'ambito della gestione dei beni di valore delle amministrazioni, le applicazioni più interessanti riguardano l'inventariazione dei beni, la certificazione delle operazioni di manutenzione appaltate a società esterne, la localizzazione in tempo reale, mediante tag RFID attivi, del bene e della persona che ne è responsabile.
Di notevole interesse appare anche la gestione documentale per conoscere il posizionamento di un documento, seguirne l'iter amministrativo, e stabilirne l'eventuale possibilità di consultazione da parte di terzi.

Alcuni esempi di applicazioni e di sperimentazioni in corso:

- Il passaporto elettronico è stato sviluppato dagli stati membri dell'International Civil Aviation Organization (ICAO), che prevede l'impiego di chip RFID ISO 14443 con una memoria minima di 64 Kbyte, per la memorizzazione e la trasmissione dei dati (dati anagrafici e l'immagine del volto).
- La CNS nasce con tecnologia a contatto conforme allo standard ISO 14443, per applicazioni ad elevata velocità di transazione (ticketing per trasporto pubblico locale, pagamento parcheggi...); si prevede la possibilità di utilizzare tecnologie contactless RFID.

4.1.3 Trasporto Pubblico locale

In questo settore, si trovano applicazioni per quanto riguarda bigliettazione elettronica e support operation. La bigliettazione elettronica, o ticketing, ha già avuto molti riscontri in diversi settori, ma principalmente nel settore dei pubblici servizi. Ad esempio ATM Milano, ATAC Roma, ATAF Firenze, e molti altri. Nei casi appena elencati, abbandonati gli abbonamenti e i biglietti ordinari, ci si è rivolti ad una tecnologia RFID, che prevede carte nominali e supporti magnetici a basso costo, allo scopo di ridurre le spese di manutenzione e offrire un servizio più rapido e personalizzato ai passeggeri (differenziando la gamma delle offerte). A Venezia è già stato realizzato un progetto full contactless per quanto riguarda ACTV, l'azienda che gestisce i trasporti pubblici. Questo

progetto non ha avuto riscontro in altre città in quanto risulta complessa la realizzazione di un'integrazione tariffaria e di coordinamento delle diverse organizzazioni.
Altre realizzazioni si possono trovare nel campo del support operations. Ad esempio, sperimentazioni sulla tracciabilità dei vagoni della metropolitana, di componenti costosi sui veicoli dedicati ai trasporti pubblici locali, o localizzazione/identificazione di mezzi nei depositi, volta a facilitare manutenzione e gestione logistica di posizionamento.

Alcuni esempi di applicazioni e di sperimentazioni in corso:

- ACTV Venezia che ha sviluppato un metodo di ticketing elettronico che si basa sull'utilizzo di chip RFID ISO 14443 B, utilizzando smart card CD21 per abbonamenti e MiFare UltraLight per biglietti di corsa semplice. Per limitare il costo i chip-on-paper sono stati resi ricaricabili (limite massimo di 10 volte) e validi per un anno.
- Altre applicazioni sono compatibili con gli standard ISO 14443 A – B, ISO 15693 e utilizzano etichette adesive dalle dimensioni più svariate con frontali in carta o sintetici.

4.1.4 Education ed Entertaiment

Questo è un settore dai più svariati scenari applicativi, con interesse rivolto in particolare all'identificazione delle persone. Come scenari principali, si denotano quattro regioni di interesse: ticketing contactless, pagamenti, support operations, gestione degli asset e integrazione in dispositivi di guida multimediale, e infine abilitazione della fruizione di servizi nei luoghi di divertimento.
Per quanto riguarda il primo scenario, come esempio applicativo si può citare l'utilizzo di RFID in comprensori sciistici per l'accesso ad impianti sportivi, come difesa dalla falsificazione dei biglietti per accedere alla struttura.
Nel settore dei pagamenti, la tecnologia RFID è stata finora utilizzata in luoghi chiusi, come discoteche, cinema, villaggi turistici e Resort.

Il support operations e la gestione degli asset impiegano gli RFID specialmente in ambito bibliotecario, nell'identificazione degli elementi arborei nei parchi naturali, nella conservazione e gestione del patrimonio artistico. Sono disponibili inoltre delle guide multimediali che si attivano nelle zone di interesse, in modo da avere la descrizione degli elementi degni di attenzione nei luoghi più diversi, che vanno dai musei ai siti archeologici, dalle manifestazioni temporanee agli spazi cittadini.
Nell'ultima sfera applicativa, che concerne i luoghi di divertimento, alcuni progetti in fase di sviluppo sono focalizzati sulla localizzazione di persone all'interno del parco giochi.

Alcuni esempi di applicazioni e di sperimentazioni in corso:

- Accesso agli stadi (con riferimento allo stadio Barbera di Palermo): è stato sviluppato un progetto in tecnologia RFID con SmartCard contacless (MiFare), abbinata al codice a barre per il controllo anticontraffazione.
- Musei (con riferimento al progetto "Il museo si racconta"-Padova): include 4 musei, di cui 3 indoor, in cui si utilizzano 80 tag passivi HF ISO 15693 che danno informazioni culturali in prossimità dei beni esposti, e un orto botanico, in cui si utilizzano 15 tag attivi in prossimità di piante storiche.
- Biblioteche: vengono utilizzate etichette adesive a basso costo, disponibili in vari formati (in genere tra i 5 – 10 cm per lato) a frequenze HF, per il controllo automatico, in entrata e in uscita, di libri, CD, DVD, videocassette, documenti. Il prestito, la restituzione e la visibilità in tempo reale delle risorse disponibili possono essere facilmente gestiti dotando gli scaffali dei negozi e delle biblioteche di dispositivi per la lettura.

Figura 3.24 – Biblioteca gestita tramite tecnologia RFID

4.1.5 Lusso e Moda

In questi ambiti, l'utilizzo della tecnologia RFID ha come obiettivi l'anticontraffazione dei prodotti e l'agevolazione nelle attività logistiche, e recentemente l'interazione consumatore-punto vendita. Nel primo caso, il risultato si ottiene principalmente tramite applicazioni per la tracciabilità dei prodotti; il secondo, invece, prevede l'automatizzazione delle attività di smistamento merci, e la messa in opera di un servizio che esegue un check-out automatico dei prodotti acquistati. Nell'ultimo caso gli obiettivi principali sono: la riduzione dei tempi di servizio, e la distribuzione di agevolazioni fiscali, memorizzando gli acquisti di ciascun cliente ed eventualmente altri dati.

La difesa dei marchi concerne sia l'abbigliamento sia altri campi come la cosmesi e la profumeria.

Alcuni esempi di applicazioni e di sperimentazioni in corso:

- Attività logistiche (con riferimento al progetto Ceseca-comune di Capannori e di ICR Cosmetics): per tenere traccia dei prodotti è stato sviluppato un sistema con tecnologia RFID HF e UHF, che rappresenta il metodo migliore poiché consente di

memorizzare dati direttamente sul tag, e di identificarlo poi agevolmente tramite il suo codice univoco (TID). Gli standard di riferimento sono Class1 Gen2, ISO 15693, ISO 14443A (standard di prossimità per la lettura di card a pochi centimetri di distanza dal reader, impiegato dai prodotti NFC – near field communication) e i modelli più utilizzati sono: Web, ShortDipole, DogBone per la tecnologia UHF, etichette adesive e non, con frontale in carta o sintetico e dimensioni ridotte (15 x 15 mm, BullsEye Ø 35 mm) per la tecnologia HF. I tag vengono poi rimossi dai capi d'abbigliamento all'atto dell'acquisto al dettaglio (non sono progettati per resistere ai cicli di lavaggio).

- Check-out automatico dei prodotti acquistati (con riferimento al progetto di Beta 80 Group): attraverso l'inserimento di tag RFID a 13,56 MHz sui prodotti, in cui vengono salvate tutte le specifiche (codice univoco, taglia, colore, tipo, marca, prezzo…), è possibile effettuare un'identificazione automatica.

4.1.6 Trasporto merci

L'aiuto che la tecnologia RFID può apportare in questo settore si focalizza su due problematiche inerenti sempre l'identificazione: dei mezzi di trasporto o delle unità di trasporto standard, oppure di "colli" all'interno delle reti dei corrieri. Nello specifico, nel primo ambito, si utilizzano queste tecnologie con l'obiettivo di tracciare il mezzo di trasporto, in particolare su gomma, e il suo carico, in modo da memorizzare prenotazioni, automatizzare il controllo degli accessi, verificare la posizione dei veicoli per l'imbarco. La catena di fornitura si avvale ampiamente delle tecnologie RFID per etichettare pallet, casse e contenitori da trasporto a rendere (RTI – Returnable Transit Items; RPC – Reusable Plastic Container), come le cassette di plastica utilizzate per gli alimenti freschi. I sistemi basati su RFID garantiscono la tracciabilità dei beni e il controllo delle risorse disponibili attraverso l'elaborazione di dati acquisiti in tempo reale. Applicazioni per il traffico su rotaia o interportuale, come ad esempio l'identificazione di container, casse mobili ed altre unità di trasporto per facilitarne i processi di carico/scarico, sono state studiate maggiormente all'estero.

Inoltre, la tecnologia RFID, offrendo una precisione di gran lunga superiore ai codici a barre, e la possibilità di trasmettere una maggiore quantità di dati in tempo reale, viene utilizzata per la gestione dei bagagli, riducendo i casi di smarrimento, e velocizzando la localizzazione dei bagagli smarriti.

Figura 3.25 – Nastro aeroportuale dotato di Tag UHF

Nel settore postale l'impiego di tag RFID per etichettare gli articoli permette di monitorarne lo smistamento e la consegna, senza interrompere il ciclo di lavorazione. I tag garantiscono letture multiple di articoli lungo la catena di trasporto e offrono scarsa sensibilità all'orientamento fisico degli oggetti da monitorare (si pensi alle lettere in un sacco o in una cassetta postale).

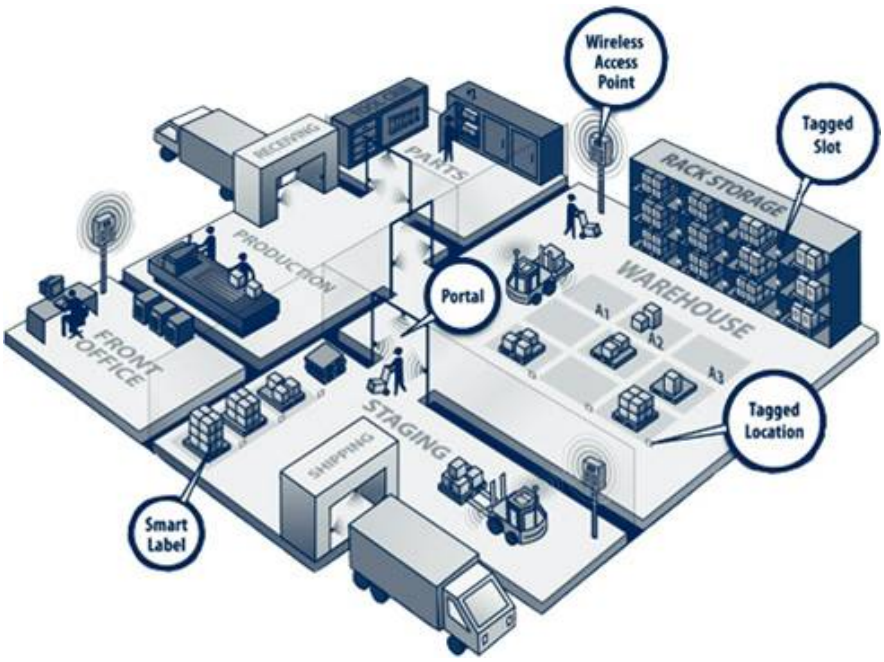

Figura 3.26 – Magazzino gestito attraverso sistema completo RFID

Alcuni esempi di applicazioni e di sperimentazioni in corso:

- Ambito portuale: si utilizzano gli RFID per tenere traccia dei mezzi di trasporto e dei container e si basano su tag attivi a 2,45 GHz o 433 MHz
- Niinivirta transport: quest'azienda di spedizioni nazionali ed internazionali ha utilizzato una tecnologia RFID con tag HF passivi, ma sta effettuando degli studi per poter migliorare le prestazioni attraverso un approccio con tag UHF che a parità di distanza e affidabilità di lettura hanno costo unitario inferiore.
- Nel settore postale si predilige l'utilizzo di tag RFID, soprattutto Web e Dogbone, che sono compatibili con lo standard EPC Class1 Gen2 per frequenze UHF.

4.1.7 Largo consumo

In Italia, lo sviluppo di progetti che utilizzano la tecnologia RFID in questo settore è marginale. All'estero per quanto riguarda i grandi distributori la sperimentazione ha preso campo senza grossi problemi a beneficio di molte aziende.

Per quanto riguarda il nostro paese, i progetti hanno interessato direttamente la sezione dei produttori; tre esempi importanti sono i seguenti: la lavorazione delle carni, il made in Italy, la filiera del fresco.

Nel primo caso, l'impiego di tecnologia RFID permette di tracciare la carne allo scopo essere certi della sua provenienza, e potere in qualsiasi momento risalire ai processi di lavorazione che ha subito. Nell'ambito del made in Italy, si intende fornire al consumatore finale una garanzia dell'autenticità del bene e poterlo valorizzare a seconda della provenienza. Per quanto riguarda la filiera del fresco, si possono monitorare i prodotti lungo la catena logistico-produttiva.

Un esempio di applicazioni e di sperimentazioni in corso:

- Grande distribuzione (riferimento a Wal-mart): si utilizzano RFID con tecnologia EPC per rendere più efficiente la distribuzione dei prodotti.

4.1.8 Tracciabiltà e anticontraffazione nell'alimentare

In questo settore, largamente collegato al precedente, l'impiego dei tag RFID è volto all'identificazione univoca e al tracciamento degli animali di allevamento e dei prodotti agricoli. Questo permette di verificare provenienza, garantendo l'origine dei prodotti e contribuire nell'organizzazione della parte relativa alla distribuzione finale dei prodotti. Per quanto riguarda la tracciabilità degli animali, ogni specie è tutelata da una distinta legge di applicazione.

Alcuni esempi di applicazioni e di sperimentazioni in corso:

- Consorzio Qualità Bovina (Coldiretti di Milano e Lodi): si utilizzano tre applicazioni RFID per ottenere un'efficace tracciabilità alimentare lungo l'intera filiera. La prima consta in apparecchiature plug&play per utilizzare tag a 134,2 KHz ISO 11784/11785 per l'identificazione automatica nell'allevamento. Come secondo aspetto, per la tracciabilità si usa un sistema basato su tag HF a 13,56 MHz read only,

situati ad esempio sui ganci dei macelli. Infine si installano tag HF passivi a 13,56 MHz read only per ricostruire l'intera storia della carne

- SDAG Gorizia: l'uso dei tag verte al tracciamento animale e fa affidamento a transponder passivi e conformi alle norme ISO 11784 e11785 (LF a 134,5 KHz).

Figura 3.27 – Bovino dotato di Tag LF

4.1.9 Logistica interna

L'avvento di questa tecnologia è recente e ancora in via di sviluppo e può fornire supporto alla logistica nel settore manifatturiero per l'identificazione dei prodotti, specialmente di grande valore, e per operatori logistici conto terzi, un campo ancora quasi inesplorato.

Figura 3.28 – Portale UHF per il tracciamento delle merci

Come esempio di applicazioni e di sperimentazioni in corso si riporta:

- Identificazione materiale (Antolini Luigi): si utilizzano tag RFID passivi a 13,56 MHz i cui codici permettono di identificare i blocchi di pietra, mentre le informazioni in memoria registrano le caratteristiche importanti e le note per la lavorazione.

4.1.10 Utility

Gli ambiti più ricchi di applicazioni: la raccolta di rifiuti solidi, che prevede la disposizione di tag LF standard ISO 18000 per abilitare l'applicazione della tariffa di igiene ambientale, e l'identificazione/localizzazione dei mezzi e dei dipendenti, che è utile ai fini della sicurezza sul lavoro.

Alcuni esempi di applicazioni e di sperimentazioni in corso:

- Identificazione di mezzi e dei dipendenti, settore petrolifero: un progetto prevede l'utilizzo di tag Ultra Wide Band per la localizzazione dei dipendenti.
- Raccolta di rifiuti solidi (Fiemme Servizi): il sistema fa affidamento su tag LF passivi che sono applicati su ogni contenitore in dotazione a ciascuna famiglia; sul mezzo pubblico di raccolta sono installati dei lettori per l'identificazione automatica dei cassonetti ad ogni svuotamento, mentre un sistema di comunicazione di raccolta dati

wireless fornisce le informazioni una volta rientrati in magazzino. Questo metodo deve far fronte a qualche criticità: i tag devono essere talvolta sostituiti a causa degli impatti, altre volte sono stati danneggiati da una non corretta installazione, in altri casi, vi sono dei problemi di lettura dovuti alla presenza di ghiaccio.

4.1.11 Settori manufatturieri tradizionali

Gli ambiti principali si concentrano in applicazioni di asset management per il settore della meccanica, dove si cerca di identificare contenitore e contenuto, automatizzare e controllare i processi, e nel settore logistico in genere, per la gestione delle spedizioni di prodotti finiti, componenti e sottosistemi, che prevedono il tracciamento ed il monitoraggio dei beni.

Un esempio di applicazioni e di sperimentazioni in corso:

- Honda Italia Industriale: si installano tag a 13,56 MHz su ogni lotto in arrivo per la localizzazione di materiali di grado A e componenti critici di cui l'azienda è direttamente responsabile.
- Nel settore petrolifero si stanno cercando soluzioni con tag attivi per monitorare i barili e facilitare il controllo della sicurezza in situazioni ambientali particolarmente ostili.

4.1.12 Gestione dei pagamenti

In questo settore l'applicazione delle tecnologie RFID è ancora agli inizi, poiché non vi è un importo fisso da saldare. Tra gli esempi disponibili citiamo le nuove carte di credito contacless, che per piccoli pagamenti non richiedeono neanche la firma della ricevuta o l'inserimento del PIN, e la convergenza tra le tecnologie RFID e gli apparati di telefonia cellulare, con il fine di effettuare pagamenti per mezzo di strumenti di grande diffusione, attraverso interrogazioni ed identificazioni in radiofrequenza.

Alcuni esempi di applicazioni e di sperimentazioni in corso:

- Carte di credito contacless (Visa Contactless, Paypass-Mastercard, ExpressPay-American Express…): rendono più rapidi i pagamenti, effettuati avvicinando la carta ad un lettore RFID. Per pagamenti inferiori a 25$ non è richiesta alcuna autenticazione, poiché la sicurezza è garantita al pari dei tradizionali supporti; gli apparecchi a cui si avvicina la carta ad almeno 10 cm, come da standard ISO14443, processano una carta per volta, evitando errori di transazione.

Figura 3.29 – Carta di credito equipaggiata con tecnologia contactless

- RFID e gli apparati di telefonia cellulare: il sistema è attivo soprattutto in zone orientali e utilizzano tecnologia Felica per applicazioni di ticketing per il trasporto pubblico e micro-pagamenti attraverso il borsellino elettronico. Quest'ultima applicazione potrebbe essere usata in Europa tramite tecnologia NFC, simile e compatibile con Felica per il Giappone.

4.1.13 Altri casi applicativi

Altri spunti di applicazione della tecnologia RFID possono essere i seguenti:

Montaggio meccanico: l'identificazione delle componenti da serrare con degli avvitatori controllati da computer in una linea di montaggio può essere effettuata direttamente

dall'avvitatore e non da un lettore di codice a barre riducendo il tempo necessario agli operatori.

Logistica interna: all'interno di ogni stabilimento è immediato immaginare come vengano attaccati transponder a colli, pallet, ecc. per tracciare in tempo reale gli spostamenti e le fasi di lavorazione per migliorare qualità, controllo e ridurre costi di gestione del magazzino. Esistono transponder che, oltre a fare quanto illustrato in precedenza, sono in grado di rilevare e registrare eventuali forti accelerazioni cui vengono sottoposti. In questo modo si può sapere se un collo è caduto durante una fase della lavorazione o del trasporto.

Controllo accessi: dall'auto all'ufficio, in modo trasparente. E' possibile stabilire quali varchi possono essere attraversati dal singolo individuo, quante volte, a distanza di quanto tempo, ecc. Una persona che entra in una stanza può essere riconosciuta e quando si avvicina ad un computer, questo, riconoscendolo, gli può presentare il suo ambiente di lavoro (Desktop del PC), eventualmente richiedendogli un codice di identificazione stile bancomat (PIN: Personal Identification Number).

Controllo integrità: un container potrebbe essere sigillato con un transponder che cessa di funzionare se il container viene aperto. In questo modo una gru che prelevi da un treno o da una nave un container, senza alcun bisogno di ispezione visiva umana è in grado di determinare se il container è stato aperto e quindi, richiedendo una nuova ispezione doganale, deve essere depositato in un'area di ispezione specifica. Il numero di operazioni effettuate dalle gru, in questo modo, si dimezza.

Controllo Ronde: un metodo assai semplice per il controllo delle ronde di vigilanza è il notissimo bigliettino che queste lasciano presso gli immobili che visitano. Questo meccanismo non consente di tracciare effettivamente il numero di visite compiute e i relativi orari, per poter assicurare il cliente che quanto stabilito nel contratto sia stato mantenuto. Se il luogo da visitare è attrezzato con un transponder il personale di ronda può essere dotato di un lettore tascabile che registra l'ora di ogni effettiva visita, ottenendo quindi la certezza dell'attività svolta.

Ambito Sanitario: esiste una normativa che impone di lavare la biancheria dei reparti infettivi separatamente dall'altra con un procedimento specifico. Il fornitore deve

certificare la completa sterilità di un telo od un camice, secondo specifici processi in autoclave. La soluzione è possibile mediante l'apposizione di tag RFID a 134kHz in un lembo del telo o del camice è possibile tracciare (scrivendo nel tag) tutti i processi di sterilizzazione a cui è sottoposto e tracciare il personale che ne è venuto in contatto durante gli stessi (attraverso apposite antenne e varchi). Questo permette, nel caso di un processo di sterilizzazione fallito la sua ripetizione solo sui capi non correttamente processati. La scelta del tag RFID ottimale ricade su etichette a 134kHz, motivata dalla presenza di acqua e dalla elevata resistenza ad emissioni x-ray (fino ad emissioni doppie di quanto possa assorbire una persona in un anno).

Vantaggi oggettivi immediati:

1) Possibilità di certificare la qualità della merce fornita;
2) Scarto immediato del materiale non conforme, riduzione dei costi di ri-trattamento;
3) Gestione in realtime del lavorato;
4) Applicazioni di filiera, è possibile fornire al cliente i dati dei tag apposti nel materiale per permettere la sua gestione interna;

Costi immediati: Circa 1€ a tag, costo dell'infrastruttura informatica e del SW. Rientri economici: Miglioramento delle procedure di gestione, riduzione degli errori (e le relative cause a carico della struttura), dimostrazione e certificazione di qualità dei materiali forniti. Non è possibile alcuna soluzione alternativa valida (etichette non utiizzabili, inchiostri facilmente degradabili ecc...)

Riconoscimento certo dei materiali emoderivati: con l'utilizzo di etichette RFID sarebbe possibile realizzare una inventariazione automatica delle forniture di emoderivati, una gestione in real-time del magazzino con l'identificazione immediata (con comunicazione tempestiva anche su materiale già consegnato) di materiale non idoneo e una certificazione della corretta conservazione. È possibile risolvere in poco tempo il problema applicando delle etichette su ogni sacca di emoderivato, inoltre è possibile fornire al personale dei palmari idoneamente equipaggiati, che si interfacciano in un database unico in modalità wireless, ottenendo tutte le informazioni in realtime (tutte le informazioni sull'emoderivato selezionato o in alternativa, dove trovarlo in magazzino). Inoltre questo sistema permette

di riordinare le scaffalature e ritrovare con un semplice "scan" materiale erroneamente collocato, oltre che permettere di gestirne lo stato di conservazione "loggando" con appositi varchi gli orari di ingresso ed uscita dal magazzino. È possibile inserire dei dati non modificabili nell'etichetta stessa che permette il funzionamento anche con il database offline. La scelta dei transponder ottimale sono le etichette ISO 15693 B + Badge ISO 15693 B, scelta obbligata per il formato etichetta e per mantenere uno standard utilizzabile a livello mondiale Vantaggi oggettivi immediati:

1) Catalogazione dell'uso degli emoderivati automatico;
2) Gestione automatica del magazzino;
3) Riduzione degli errori di trasfusione (sopratutto in caso di emergenza);
4) Gestione dello stato di conservazione in modo automatico;
5) Log delle consegne del materiale automatico (a chi è fornito per la somministrazione il materiale);

Vantaggi secondari:

1) Applicazioni di filiera, cioè i fornitori potranno fornire con gli emoderivati anche il relativo database e condividerlo con più strutture, fornendo alert in tempo reale;

Costi immediati: Circa 50/80 cent€ ad etichetta (ISO 15693 B), costo dell'infrastruttura informatica, costo del SW. È possibile calare il SW in ambienti informatici già più avanzati, riducendo i costi dell'implementazione.

Rientri economici: Miglioramento delle procedure di gestione, riduzione degli errori (e le relative cause a carico della struttura), dimostrazione e certificazione di qualità degli emoderivati.

Distribuzione di farmaci: In ogni ospedale c'è un problema di identificazione dei pazienti e di somministrazione a loro dei farmaci corretti, farmaci che vengono preparati prima del giro in corsia per ogni paziente presente. Questa pratica è soggetta ad errori manuali, talvolta con conseguenze nefaste. Si può dotare ogni paziente di un braccialetto con un transponder e dotare un carrello di un lettore che quando viene avvicinato al paziente apre automaticamente lo scomparto corrispondente all'interno del quale era stata messo il farmaco specifico per quel paziente.

Armi: Se un utente avesse un transponder in un anello ed ogni arma fosse dotata di un lettore si potrebbe evitare che le armi venissero usate da persone diverse dei legittimi titolari. In alcuni paesi ove è assai sentito il problema del controllo degli armamenti presso la popolazione, è allo studio la possibilità di realizzare un registro delle armi legalmente detenute con un transponder che contiene, oltre al codice identificativo inalterabile, i dati anagrafici del titolare e la sua fotografia codificata digitalmente e cifrata in modo irriproducibile da malintenzionati.

Capi abbigliamento: transponder possono essere inseriti nelle etichette in poliammide dei capi di abbigliamento. Quando un cliente entra nel camerino, il camerino riconosce cosa ha indosso ed è in grado di suggerire abbinamenti su un display al suo interno. Gli ingombranti e macchinosi chiodi magnetici che fanno suonare i varchi di uscita dai negozi al loro passaggio possono essere sostituiti con transponder ed antenne di dimensioni assai inferiori senza deturpare l'estetica dei punti vendita. Dotando ogni scaffale di una antenna è possibile conoscere cosa vi è appoggiato sopra e quindi realizzare un inventario permanente in tempo reale, senza intervento umano, riuscendo a sapere in Italia cosa è presente in ogni punto vendita del mondo.

Anticontraffazione: beni di lusso possono essere dotati di transponder che, essendo univoci, possono dimostrare l'originalità di un prodotto, senza alcun dubbio.

Tracking documenti: Alcuni produttori hanno iniziato a produrre risme di carta, molto costose per adesso, i cui fogli contengono un transponder. Se la copertina di ogni fascicolo fosse realizzata con questa carta e gli armadi degli archivi fossero dotati di antenne, non esisterebbe più il problema di ritrovare una pratica...

Quando si parla di radiofrequenza molti rivolgono un pensiero anche ad aspetti legati alla riservatezza delle informazioni personali ed alla propria salute. Da un punto di vista elettromagnetico, i transponder passivi vengono letti/scritti da antenne che generano campi elettromagnetici almeno tre ordini di grandezza inferiori (un millesimo) di quelli generati dai telefoni cellulari... Il tema della privacy è un po' più delicato o, quantomeno, la risposta non è così immediata. Innanzitutto ricordiamo che esistono vari soggetti che di noi sanno dove andiamo, cosa compriamo, quando, come è composto il nostro nucleo

famigliare, per chi lavoriamo, quanto consumiamo, ecc… e questi soggetti sono banche e società che gestiscono le carte di credito. Migliaia di persone all'interno di queste organizzazioni hanno accesso a queste informazioni ma ciò non ci frena nell'usare la nostra tessera bancomat, i nostri assegni o la nostra carta di credito. Moltissimi di noi hanno registrato il proprio profilo presso il servizio Passport di Microsoft, magari in modo ignaro, semplicemente perché usano il programmino di messaggistica istantanea Messenger che appare di frequente in modo spontaneo sulle nostre scrivanie. In questo modo Microsoft è in possesso di una enorme quantità di informazioni circa i siti che consultiamo, gli amici cui mandiamo messaggi ed i siti che consultano loro. Una paura che si rileva diffusamente quando si parla di transponder è dovuta al fatto che la lettura non avviene con un gesto evidente, esplicito, come nel caso dei pagamenti di cui sopra, ma in modo automatico, trasparente, e alcuni temono, di nascosto. Bisogna ricordare che le distanze di lettura sono abbastanza modeste e che i transponder non contengono dati aggregati ma solo codici che sono portatori di significato solo per chi li ha prodotti. Anche se un terzo fosse in grado (ammesso e non concesso) di leggere il codice 11023465772887778 scritto in un transponder attaccato ad una maglietta di Benetton (società tra le prime ad essere stata oggetto di reazioni da parte di opinione pubblica preoccupata), questo codice significherebbe ben poco a costui. Per Benetton potrebbe significare il lotto di produzione, la data, la fabbrica, il lotto di cotone utilizzato, il suo produttore, lo spedizioniere utilizzato, i magazzini attraversati, il negozio di vendita, ecc. Tutte queste informazioni saranno assai ben protette, grazie a meccanismi di cifratura, per evitare che un concorrente di Benetton ne possa venire a conoscenza semplicemente leggendo e decifrando un'etichetta. Questo già avviene, ad esempio per le carte di credito, la cui riproduzione altrimenti sarebbe un fatto talmente banale da minarne alla base il funzionamento del sistema. Non vi è possibilità pratica che un transponder inserito in un oggetto utilizzato da un individuo sia utilizzabile per tracciare i suoi comportamenti ed abitudini, abbinandolo alla sua identità, nemmeno da parte del soggetto che gestisce le identità degli individui, cioè lo Stato, anche se facesse carte di identità con transponder. Alla base di questa affermazione c'è il fatto, come si desume da questo documento, che

ogni utilizzo dell'RFID si basa su Transponder specificatamente realizzati ed utilizzati per ogni singola applicazione.

4.2 APPLICAZIONI WSN

Le reti di sensori possono essere implementate utilizzando una vasta tipologia di sensori come sensori sismici, magnetici, termici, infrarossi, acustici, radar, gps, in grado di monitorare una ampia classe di grandezze fisiche.
Alcune delle principali applicazioni delle reti di sensori wireless possono essere classificate come di seguito.

Applicazioni ambientali

Possiamo distinguere in questa categoria: *monitoraggio di strutture* (rilevare e localizzare danni in costruzioni, ponti, aerei e navi), *monitoraggio dell'ambiente naturale* (sistemi di prevenzione degli incendi, ricerche meteorologiche e geofisiche, in particolare studio di zone pericolose, come vulcani o zone a rischio sismico, studi scientifici su flora e fauna, controllo dell'inquinamento, controllo in ambito agricolo delle colture per permettere un intervento in tempo reale con trattamenti opportuni al fine di debellare insetti o prevenire altre situazioni critiche).

Applicazioni mediche

Alcuni esempi in questo campo possono essere la trasmissione dei parametri fisiologici dei pazienti all'interno degli ospedali, attività diagnostiche, somministrazione di medicinali, personal healthcare ed altro.
Altra applicazione interessante è il controllo remoto di persone anziane per prevenire situazioni di pericolo quali per esempio una caduta o uno sbalzo improvviso delle pulsazioni cardiache. In queste situazioni, utilizzando un sistema di localizzazione, sarebbe possibile individuare la posizione dell'individuo e rendere più semplice, tempestivo ed efficace l'intervento dei soccorsi.

Applicazioni domotiche

Si può pensare di inserire i sensori sia nei componenti di elettronica di consumo sia nella categoria delle innovazioni, per esempio per il controllo dei sistemi HVAC (Heating, ventilation and air conditioning): si tratta di sistemi in grado di regolare la temperatura di ogni stanza sulla base di diversi sensori, che potrebbero essere migliorati tenendo conto anche della posizione degli esseri umani determinata da un sistema di localizzazione.

Applicazioni industriali

Un altro ambito di interesse per le reti di sensori wireless sono il monitoraggio in ambiente industriale e l'automazione industriale. Le caratteristiche delle WSN consentono infatti di realizzare svariate applicazioni in questo settore ma tutte rivolte al controllo dei processi produttivi.

Applicazioni commerciali

In questa categoria si considerano problemi di car tracking (rilevamento della posizione e del movimento di veicoli, controllo del traffico), rilevamento del furto di auto, museo interattivo (possibilità di interagire con gli oggetti esposti, servizio di localizzazione all'interno del museo), in cui la localizzazione è uno dei punti determinanti dell'applicazione stessa.

Applicazioni di localizzazione

Le applicazioni di localizzazione si dividono in due filoni principali: localizzazione statica e tracking. La prima è più legata alle reti di sensori, in quanto oltre ad avere una misura di un parametro fisico è utile sapere da quale punto quel dato proviene, e se i sensori sono in grado di autolocalizzarsi si semplifica la fase di installazione della rete, in quanto non c'è la necessità che un operatore misuri a mano la posizione del nodo, ma sarà il nodo stesso a farlo. In questo caso la localizzazione viene eseguita solo all'inizio dell'attività della rete, e in seguito può essere necessario ripeterla solo se si vuole verificare che non ci siano stati spostamenti. Questa situazione in genere prevede che nella rete ci siano pochi nodi fissi

posizionati a mano e usati come riferimento per un gran numero di altri nodi che saranno invece sparsi e dovranno essere localizzati in modo automatico. Altro problema è invece per le applicazioni di tracking, in cui un buon numero di nodi fissi con posizione nota al momento dell'installazione serve da riferimento per i nodi mobili, la cui utilità è in genere legata principalmente alla possibilità di essere localizzato istante per istante, in modo da seguirne gli spostamenti: in questo caso la localizzazione va effettuata ripetutamente, con un intervallo di campionamento che sarà un compromesso tra quello che sarebbe richiesto per poter rilevare i movimenti più veloci e le necessità di risparmio energetico dovute soprattutto al nodo mobile.

4.3 SCENARI APPLICATIVI DI CONVERGENZA

Esistono anche esempi di utilizzo congiunto di tecnologie WSN e RFID che valorizzano le peculiarità tipiche di entrambe le tecnologie, quali ad esempio la potenza di elaborazione dei nodi delle WSN e l'economicità dei tag RFID, al fine di sfruttarne meglio la complementarietà e le sinergie. Nel seguito ne riportiamo una selezione che riteniamo particolarmente significativa per la varietà di combinazioni tra soluzioni WSN e RFID che vi viene presentata.

4.3.1 Agricoltura intelligente

Nel settore agricolo in generale, e in quello vinicolo in particolare, si ha necessità di acquisire informazioni da usare come supporto a decisioni immediate. Chi gestisce la coltivazione deve poter conoscere in ogni istante ciò che sta accadendo in termini di grandezze ambientali misurate (temperature, umidità, precipitazioni, ecc.) e di operazioni effettuate dagli addetti (irrigazione, irrorazione con pesticidi, raccolta prodotti, ecc.).

Raccogliere queste informazioni presenta varie difficoltà. Una coltivazione vitivinicola insiste sicuramente su di un'area di dimensione anche molto elevata, non dotata di infrastrutture di comunicazione o per la fornitura di energia elettrica. Per trasportare i dati

acquisiti da un nodo periferico fino ad una stazione base occorrerebbe quindi disporre di nodi di acquisizione in grado di comunicare a grandi distanze con la minor spesa energetica possibile, in quanto l'alimentazione proviene soltanto dalle batterie od, eventualmente, dall'ambiente (per esempio: energia solare). Per quanto riguarda il tracciamento delle attività svolte, ai problemi di comunicazione e di approvvigionamento energetico si somma il fatto che gli operatori del settore agricolo non sono dotati di un profilo propenso al data entry effettuato con sistemi tradizionali (per esempio: PDA), ne' possono essere distolti dalle loro attività.

Una possibile soluzione a questi problemi consiste in un uso congiunto di WSN e RFID. Per esempio, volendo monitorare l'attività di irrorazione con pesticidi, si può pensare di creare una rete di nodi fissi dislocata lungo i filari del vigneto e di dotare l'irroratore di un tag RFID che permetta la sua identificazione. Se la rete è in grado di leggere il tag diviene possibile tracciarne l'attività di irrorazione, che diventa l'input della rete di sensori. In modo simile, equipaggiando con tag RFID gli opportuni attrezzi, può essere localizzata e registrata l'attività di potatura, di raccolta, o di sarchiatura. Se il tag che equipaggia l'attrezzo utilizzato dall'operatore è sufficientemente capiente in termini di memoria, si può pensare di utilizzarlo come contenitore mobile per trasportare dati verso la stazione base. In questo modo è possibile risolvere anche i problemi relativi al trasferimento dati verso la stazione base, creando un meccanismo di trasporto di tipo data mule. In particolare, dal momento che i tag da dedicare al trasporto dati saranno sensibilmente più costosi degli altri, si può pensare di applicarli solo su agenti che si muovono frequentemente all'interno della coltivazione. Questi potrebbero essere gli operatori stessi, ma anche animali domestici o i mezzi agricoli.

In questo esempio, il tag RFID diviene sia "sensore di utilizzo" (un determinato oggetto), sia meccanismo di trasporto nell'ambito di una infrastruttura di tipo WSN i cui nodi esplicano la funzione di acquisizione dati. Le operazioni svolte sono complementari e gli ambiti di intervento ben definiti.

4.3.2 *Parcheggio intelligente*

Si tratta di un lavoro proposto da gruppo di ricerca del Consorzio CREATE-NET di Trento [4] come esempio di applicazione di monitoraggio ambientale. Gli Autori descrivono un sistema informativo sviluppato su area urbana che supporti gli automobilisti nella ricerca di un parcheggio libero.

Nello scenario considerato, ogni parcheggio della città è dotato di un sensore in grado di fornirne lo stato (libero oppure occupato) e la posizione geografica. Ogni automobilista che aderisce al servizio è dotato di un dispositivo portatile che può comunicare sia con il sensore che con gli altri utenti. Gli utenti, muovendosi attraverso la città, raccolgono informazioni sullo stato dei parcheggi che incontrano lungo il loro tragitto. L'informazione è memorizzata all'interno dei loro dispositivi, insieme all'istante di acquisizione. Quando due utenti si incontrano, i dati vengono scambiati e le informazioni memorizzate all'interno dei loro dispositivi vengono aggiornate. A questo punto l'utente può interrogare il proprio dispositivo per conoscere la posizione dei parcheggi liberi nelle immediate vicinanze.

In questo esempio il tag RFID diviene anche sensore e lettore, praticamente può essere considerato come un nodo WSN. L'aumento della complessità e delle potenzialità del tag, seppur con fini diversi, è presente anche nel prossimo esempio.

4.3.3 *Tracciabilità di semilavorati in un contesto industriale*

Questo esempio descrive un progetto sviluppato da Infineon Technologies in Villach, Austria [5], in cui si utilizzano in maniera combinata RFID attivi, RFID passivi e tecniche di localizzazione basate su segnali ultrasonici, tipicamente utilizzate nell'ambito di WSN. L'obiettivo finale consiste nel tracciare in tempo reale la posizione di wafer di silicio semilavorati all'interno dello stabilimento di produzione. Gruppi di wafer vengono trasportati per mezzo di speciali contenitori equipaggiati con tag RFID attivi che permettono di identificarne in ogni momento il contenuto e la posizione. In questo modo è possibile ottimizzare gli spostamenti dei semilavorati, tenerne traccia ed inviare i lotti presso gli opportuni processi di lavorazione. Ogni contenitore è inoltre equipaggiato con

un tag passivo che viene utilizzato sia a scopo di verifica incrociata del funzionamento del tag attivo, sia per mantenere la compatibilità con segmenti di processo che utilizzano la tecnologia passiva.

Per mezzo degli RFID attivi è possibile effettuare una localizzazione grossolana della posizione del contenitore semplicemente misurando la potenza del segnale ricevuto dall'antenna durante la comunicazione. Questo tipo di soluzione è molto impreciso, a causa delle riflessioni a cui sono soggette le onde elettromagnetiche, specialmente in un ambiente complesso quale un impianto industriale. Per ottenere una localizzazione più fine si è preferito utilizzare una tecnica che fa uso di ultrasuoni. Per questo scopo il soffitto dell'impianto è stato dotato di nodi di tipo WSN che periodicamente emettono un segnale sonoro combinato con un impulso RF. I tag attivi che si trovano sui contenitori sono interfacciati con un nodo WSN che riceve sia il segnale sonoro che l'impulso RF. Calcolando la differenza tra i tempi di arrivo dei due segnali, il tag attivo conosce il tempo di volo dell'ultrasuono inviato da ogni emettitore e lo registra all'interno della propria memoria . Questi valori vengono poi letti dall'antenna RFID che provvede a trasferirli verso un server centrale che genera e memorizza l'informazione di localizzazione di ogni singolo contenitore.

In questo scenario, la tecnologia RFID permette di identificare un grande numero di tag in maniera efficiente, sia dal punto dell'affidabilità, sia del costo e trae vantaggio dall'integrazione con il WSN al fine di ottenere una localizzazione precisa. Il tag RFID, attivo, diviene molto complesso e tende ad assomigliare, concettualmente, al nodo di unaWSN. Nell'esempio che segue vediamo il processo opposto: un nodo WSN che viene semplificato fino a trasformarsi in un tag RFID passivo.

4.3.4 Tag sensore di movimento

Uno degli aspetti più critici delle WSN è l'approvvigionamento energetico. Le caratteristiche più importanti per un nodo di questo tipo, cioè basso costo, dimensioni ridotte e comunicazione wireless, mal si coniugano con questo aspetto. Tipicamente le soluzioni a questo problema si cercano nella tecnologia delle batterie, oppure si studia la

possibilità di ricavare energia dall'ambiente. Il lavoro di Intel Research e dell'Università di Washington presentato in [6] percorre invece una via diversa, basata sulla tecnologia utilizzata dai sistemi RFID passivi.

Viene presentato come esempio un accelerometro ad un bit, completamente passivo, basato sull'accoppiamento di due diversi transponder ad una unica antenna per mezzo di un interruttore al mercurio. Quando il tag viene scosso, o semplicemente spostato, l'interruttore commuta l'antenna del tag su uno o sull'altro transponder. In questo modo la risposta del tag, cioè l'identificativo inviato all'antenna, varia a seconda a seconda della posizione del tag. Dal momento che ogni tag può inviare solo due identificativi all'antenna è sempre possibile ricavare, in presenza di più tag, quale ha subito un movimento. Usando lettori in grado di coprire aree ampie con elevate velocità di lettura è possibile pensare di catturare il movimento dei tag, quindi degli oggetti su cui possono venire applicati, anche in ambienti complessi ed in presenza di numerosi tag.

Le applicazioni proposte per il sensore di movimento spaziano dal settore della cura degli anziani che vivono soli, dove potrebbero essere utilizzati per monitorarne lo stato di salute attraverso l'analisi dell'uso degli oggetti della vita quotidiana, alle applicazioni di training, in cui potrebbero essere utilizzati per registrare e verificare la corretta esecuzione di operazioni manuali (per esempio: manutenzione di apparati, operazioni chirurgiche).

Questo è un esempio in cui la tecnologia RFID accorre in aiuto alle WSN per risolvere il problema dell'approvvigionamento energetico ed apporta un contributo talmente determinante da fare quasi scomparire gli aspetti di WSN. Nell'ultimo esempio vediamo invece come RFID e WSN possono completarsi al meglio mantenendo le proprie identità e peculiarità.

4.3.5 Logistica delle merci deperibili

In [7] l'Università di Bremen propone un progetto di container intelligente da utilizzare per il trasporto di merce facilmente deperibile, quali i prodotti ortofrutticoli. Questo tipo di prodotto risente molto delle condizioni ambientali a cui è sottoposto durante il trasporto e può essere soggetto a cambiamenti di stato: un monitoraggio attento

permetterebbe di minimizzare eventuali perdite dovute ad alterazione dello stato di conservazione. Una soluzione per ottenere questo risultato potrebbe essere quella di utilizzare dei sensori intelligenti da applicare a lotti di merce per registrare le condizioni durante tutto il trasporto. Tuttavia questa soluzione richiederebbe di utilizzare una quantità di oggetti molto costosi, di cui una percentuale dei quali potrebbe facilmente andare smarrita o rompersi durante il trasporto. Una possibile alternativa consiste nel realizzare un container intelligente, cioè dotato di una rete di sensori che effettui un monitoraggio continuo e puntuale delle condizioni ambientali al suo interno e memorizza queste informazioni su tag RFID applicati direttamente sulle derrate alimentari. In questo scenario, la parte più costosa del sistema è applicata ad un oggetto assolutamente riutilizzabile quale è il container, non vi sono problemi di alimentazione, in quanto vi è spazio in abbondanza per le batterie, o addirittura può essere possibile accedere a sorgenti di alimentazione. E' inoltre possibile utilizzare sensori più complessi e costosi di quelli applicabili direttamente sulle derrate alimentari. D'altra parte l'uso di tag semplici e, quindi, di basso costo sui prodotti, permette una livello di etichettatura più profondo, nonchè la compatibilità con infrastrutture già esistenti.

Bibliografia

CAPITOLO 2

[1] Abi Research , "Global RFID Market to Reach $5.3 Billion This Year", RFID Forecasts RFID & Contactless Research Service, novembre 2008, disponibile in rete: http://www.abiresearch.com/media.jsp

[2] L. Battezzati, Jean-Louis Hygounet, "RFID Identificazione automatica a radiofrequenza", Hoepli 2008

[3] Collection Data, articolo: "Middleware RFID: professione intermediario" di Michel Rousseau 11-05-2006

[4] http://www.microsoft.com/italy/stampa/speciali/smau/mbs/scheda_RFID.mspx

[5] http://www.sun.com/software/solutions/RFID

[6] "The battle between HF and UHF RFID" tratto da "Microwave Journal" vol.51.No.5

[7] Patrick J.Sweeney, "RFID for Dummies", Wiley Publishing, Inc. 2005

[8] Paolo Talone, Giuseppe Russo, Fondazione Ugo Bordoni, "RFID TECNOLOGIA E APPLICAZIONI"

[9] Gaetano Marrocco "La tecnologia RFID"

[10] Franco Musiari RFID "Introduzione alla tecnologia delle etichette intelligenti"

[11] "Boot Loader Reference Guide for Series 4000 Reader" http://www.ti.com/RFID

[12] "S4100 MFR Module DataSheet" http://www.ti.com/RFID

[13] "Tag-it Transponder Protocol Reference Manual" http://www.ti.com/RFID

[14] "Base Aplication Protocol Reference Guide" http://www.ti.com/RFID

[15] "TagTracker v2.1 User Manual" http://www.databrokers.net/

[16] "PIRF Lite version 2.0 User Manual" http://www.databrokers.net/

[17] K. Finkenzeller, "RFID Handbook: Fundamental and Application in contactless Smart Cards and Identification" , 2nd ed, Chichester, Wiley and Sons Ldt, 1999

CAPITOLO 3

[1] TinyOS Reference Website, *http://www.tinyos.net* /.

[2] Ciaràn Lynch and Fergus O' Reilly, "Processor Choice For Wireless Sensor Networks," Workshop on Real World Wireless Sensor Networks, RealWSN 2005, Stockholm, Sweden, 20-21 June 2005.

[3] Atmel Corporation, "AT90S/LS8535 Datasheet," 2001. Disponibile in rete: http://www.atmel.com /atmel /acrobat /doc1041.pdf.

[4] RF Monolithics Inc., "TR1000 Data Sheet," 1999. Disponibile in rete: http://www.rfm.com /products /data / tr1000.pdf.

[5] Atmel Corporation, "AT90S2323/LS2323/S2343/LS2343 Datasheet," 2001. Disponibile in rete: http://www.atmel.com /atmel /acrobat /doc1004.pdf.

[6] Atmel Corporation, "ATMega103(L) Datasheet," 2001. Disponibile in rete: http://www.atmel.com /atmel /acrobat /doc0945.pdf.

[7] Atmel Corporation, "ATMega128 Datasheet," Rev. 2467I-09/03, 2003.

[8] Atmel Corporation, "AT45DB041B Datasheet," 2001. Disponibile in rete: http://www.atmel.com /atmel /acrobat /doc1938.pdf.

[9] Chipcon, "CC1000 Single Chip Very Low Power RF Transceiver," 2002. Disponibile in rete: http://www.chipcon.com /files /CC1000_Data_Sheet_2_1.pdf.

[10] Chipcon, "2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver," Rev. 1.3, 2005. Disponibile in rete: http://www.chipcon.com /files /CC2420_Data_Sheet_1_3.pdf.

[11] Texas Instruments, "MSP430X13x, MSP430X14x Mixed Signal Microcontroller User Guide," Rev. F., 2003. Disponibile in rete: http://focus.ti.com/lit/ds /symlink/msp430f133.pdf.

[12] ZigBee Alliance Official Website, *http://www.zigbee.org*.

[13] Microchip Technology Inc., "Thermal Sensor with SPI Interface," 2002. Disponibile in rete: http://ww1.microchip.com /downloads /en /DeviceDoc /20092a.pdf.

[14] D. Gay, P. Levis, D. Culler, and E. Brewer, "nesC 1.1 Language Reference Manual," May 2003.

[15] D. Gay, P. Levis, R. Von Behren, M. Welsh, E. Brewer, and D. Culler, "The nesc language: A holistic approach to networked embedded systems," in Proc. ACM SIGPLAN 2003 conference on Programming language design and implementation, June 2003, pp. 1-11.

[16] VxWorks 5.4 Datasheet, http://www.windriver.com /products /html/vxwks55_ds.html.

[17] Microsoft Windows CE, http://www.microsoft.com /windowsce /embedded.

[18] PalmOS Sofware 3.5 Overview, http://www.palm.com /devzone /docs/palmos35.html.

[19] QNX Overview, http://www.qnx.com /literature /whitepapers /archoverview.html.

[20] Creem, http://members.dodo.net.au /~void /old /creem.htm.

[21] pOSEK, http://www.isi.com /products /posek /index.htm.

[22] Ariel, http://www.microware.com/ProductServices/Techologies/ariel_technology_brief.html.

[23] A. Dunkels, B. Grönvall, and T. Voigt, "Contiki – a Lightweight and Flexible Operating System for Tiny Networked Sensors," In Proceedings of the First IEEE Workshop on Embedded Networked Sensors, Tampa, Florida, USA, November 2004.

[24] S. Dulman, and P. Havinga, "Operating System Fundamentals for EYES Distributed Sensor Network," PROGRESS Workshop, Utrecht, the Netherlands, October 2002.

[25] http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05

[26] PERL Reference Website, *http://perl.com* /

[27] Ciaràn Lynch and Fergus O' Reilly, "PIC-based TinyOS Implementation," in Proc. 2nd European Workshop on Sensor Networks, Instanbul, Feb 2005, pp. 378-385.

[28] Hans-Jörg Körbert, Housam Wattar, Gerd Scholl, and Wolfang Heller, "Embedding a Microchip PIC18F452 based commercial platform into TinyOS"

CAPITOLO 4

[1] www.tinyos.net

[2] R. Shah, S. Roy, S. Jain, W. Brunette, Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks , IEEE SNPA Workshop, May 2003

[3] Carreras, I. Chlamtac, I. Woesner, H. Zhang, H., "Nomadic sensor networks", Proceeedings of the Second European Workshop on Wireless Sensor Networks, 2005

[4] Thiesse, F.; Fleisch, E.; Dierkes, M.; LotTrack: RFID-based process control in the semiconductor industry, Pervasive Computing, IEEE, Volume 5, Issue 1, Jan.-March 2006 Page(s):47 – 53

[5] M. Philipose et al., Battery-Free Wireless Identification and Sensing, IEEE Pervasive Computing, 2005

[6] Jedermann, R. and Lang, W.: Mobile Java Code for Embedded Transport Monitoring Systems. In: Grote, C. and Ester, R. (eds.): Proceedings of the Embedded World Conference 2006, February 14-16, Nuremberg, Germany. Vol 2., pp. 771-777. Franzis Verlag, Poing

Miscellanea bibliografia su RFID

- P. Talone, G. Russo, "RFID Tecnologia e applicazioni", Fondazione Ugo Bordoni e Federcomin, 2006, disponibile in rete: http://www.rfid.fub.it/.
- S. J. Orfanidis, "Electromagnetic waves and antennas", novembre 2002, disponibile in rete: http://www.ece.rutgers.edu/~orfanidi/ewa/.
- M. Parodi, Dispense del corso "Sistemi elettrodinamici per l'energia", A.A. 2007/2008
- Fondazione Guglielmo Marconi, Giornata di studio "Dalle tecnologie alla applicazioni dei sistemi RFID", Villa Griffone, Pontecchio Marconi, Bologna, Maggio 2008, documentazione disponibile in rete http://www.fgm.it/site/index.php.
- F. Fuschini,C. Piersanti, F. Paolazzi, G. Falciasecca, "Electromagnetic and system level co-simulation for RFId radio link modeling in real environment.", 2007, http://www.eucap2007.org/.
- F. Fuschini,C. Piersanti, F. Paolazzi, G. Falciasecca, "Analytical Approach to the Backscattering from UHF RFID Transponder", IEEE Antennas and Wireless propagation letters, vol. 7, 2008.
- P. V. Nikitin, K. V. S. Rao, S. F. Lam, V. Pillai, R. Martinez, and H. Heinrich, "Power Reflection Coefficient Analysis for Complex Impedances in RFID Tag Design", IEEE Transactions on microwave theory and tecniques, vol. 53, no. 9, Settembre 2005.

- P. V. Nikitin, K. V. S. Rao, S. Lazar, "An Overview of Near Field UHF RFId", 2007 IEEE International Conference on RFID, Marzo 2007.
- Rapporto 2007 Osservatorio RFId, "RFId: alla ricerca del valore.", Giugno 2007, http://www.osservatori.net/web/osservatori/rfid/rassegna.
- R. Firenze, "Studio dei sistemi RFId e loro caratterizzazione sperimentale", Università degli Studi di Genova, Settembre 2006.
- I. Damonte, "Valutazione sperimentale delle caratteristiche di sistemi RFID", Università degli Studi di Genova, 2007.
- K. V. S. Rao, P. V. Nikitin, F. Lam, "Antenna design for UHF RFID Tags: a review and a practicle application", IEEE Transaction of antennas and propagation, Vol.53, no. 12, Dicembre 2005.
- P. V. Nikitin, K. V. S. Rao, "Theory and measurement of backscattering from RFID Tags", IEEE Antennas and Propagation Magazine, 2006.
- P. V. Nikitin, K. V. S. Rao, "Differential RCS of RFID Tags", Electronics letters, vol. 43, no. 8, Aprile 2007.
- P. V. Nikitin, K. V. S. Rao, F. Lam, "Impedance Matching Concepts in RFID Transponder Design", Automatic Identification Advanced Technologies, 2005.
- C. Turner, "Backscatter modulation of impedance modulated RFID Tags", Febbraio 2003.
- C.C. Yen , A. E. Gutierrez, D. Veeramani, D van der Weide, "Radar cross section analysis of Backscattering RFID Tags", IEEE Antennas and wireless propagation letters, vol. 6, 2007
- P. H. Cole, B. Jamali, D. Ranasinghe, "Coupling relations in RFID Systems", Auto-Id Centre University of Adelaide, Giugno 2003.
- "Passive RFID Basics", disponibile in rete all'indirizzo http://ww1.microchip.com/downloads/en/AppNotes/00680b.pdf
- Klaus Finkenzeller, "RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition", WILEY 2003
- Heinrich, Rfid and Beyond, Wiley, Indiana 2005.
- B. Forouzan, "I protocolli TCP/IP", McGraw-Hill 2001

- U. Karthaus, M. Finscher, "Fully Integrate passive UHF Transponder IC with 16.7-µm Minimum RF Imput power", "IEEE Journal of solid-state Circuits", vol.38, October 2003
- CAEN RFID, "Introduction to RFID technology", Application Note, http://www.caen.it/rfid/index.html
- G. De Vita, G. Iannaccone, "*Design Criteria for RF Section of Long Range passive RFID Systems.*" , Proc. NORCHIP 2004, Oslo, Norway, Novembre 2004
- Roy Want, *"Quando gli oggetti parlano"*, Le Scienze febbraio 2004
- Mantelero, Identificatori a radio frequenza (RFID) e controllo capillare dei dati personali: il rischio di un "mondo nuovo" per il consumatore?, in Contratto e Impresa Europa, 2004.
- Provvedimento del 9 marzo 2005 http.//www.garantedellaprivacy.it/
- RFID: Normative e standard http://www.simet.com/Ita/news/download/data_collection_RFID_normative.
- Seminario: "Dalle tecnologie alle applicazioni dei sistemi RFID", Pontecchio Marconi (BO) 14 Maggio 2008.
- "EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Comunication at 860MHz-960MHz,Version 1.0.9", EPCglobal Inc™.
- "Programmer's Reference Manual Basic Reader Interface", Intermec.
- Tesi di laurea: "Valutazione sperimentale delle caratteristiche di sistemi RFID", Irene Damonte Università degli studi di Genova
- Presentazione: "Real Time Location System", Prof. Carlo Maria Medaglia, 16 Aprile 2008.
- "A Tracking Algorithm in RFID Reader Network", Wei Jiang , Dan Yu, Yan Ma, Computer Society.
- "Combined AOA/TOA UWB localization", Stefan Galler, Waldemar Gerok, Jens Schroeder, Kyandoghere Kyamakya, and Thomas Kaiser.

- "Localization via Ultra-Wideband Radios [A look at positioning aspects of future sensor networks]", Sinan Gezici, Zhi Tian, Georgios B. Giannakis, Hisashi Kobayashi, Andreas F. Molisch,H. Vincent Poor, and Zafer Sahinoglu.
- "Real Time Enterprise: dalla micro alla macro localizzazione", Cesare Borretti, Sales Consultant, Oracle Italia.
- "Securing RFID with Ultra-wideband Modulation", Pengyuan Yu, Patrick Schaumont and Dong Ha, Virginia Tech and Electrical and Computer Engineering Department. Blacksburg, VA 24061.
- Ulaby Fawwaz T, "Fondamenti di campi elettromagnetici. Teoria e applicazioni", McGraw-Hill Libri Italia 2006
- Collection Data, articolo: "Middleware RFID: professione intermediario" di Michel Rousseau 11-05-2006
- "Random samplin Algorithm in RFID Indoor Location System", Bao Xu, Wang Gang
- Andrea Boaretto, "Tecnologie di prossimità come meccanismo di engagement"
- Orlando Mario, "Bluetooth, tecniche trasmissione dati". Disponibile online all'indirizzo http://www.alfredomartinelli.info/viewart.php?idart=103
- Enrico Amedeo, "Uml, imparare a descrivere sistemi orientati agli oggetti graficamente e in modo standard"
- Ferrante Angelo, "Market Basket Analysis"
- Edsger Dijkstra, "L'algoritmo di Dijkstra". Disponibile online all'indirizzo http://it.wikipedia.org/wiki/Algoritmo_di_Dijkstra
- MVC. Disponibile online all'indirizzo http://it.wikipedia.org/wiki/Model-View-Controller
- Rich Client Platform. Disponibile online all'indirizzo: http://wiki.eclipse.org/index.php/Rich_Client_Platform
- Il protocollo LLRP. Disponibile online all'indirizzo http://www.llrp.org/
- http://www.macitynet.it/macity/aA26721/index.shtml.
- AnnikaPaus. Near Field Communication in Cell Phones. Seminararbeit Ruhr-Universitat
- Bochum, 2007.

- Viktor Nilsson Erik Rolf. Near Field Communication (NFC) for Mobile Phones. Lund University, August 2006.
- Klemens Breitfuss Ernst Haselsteiner. Security in near _eld communication (NFC). Printed handout of Workshop on RFID Security RFID, Philips Semiconductors, 06 July 2006.
- Java APIs for Bluetooth. http://www.jcp.org/en/jsr/detail?id=82.
- Sun Microsystems Inc. Java Card 2.0 API.
- Qusay H. Mahmoud. Wireless Application Programming with J2ME and Bluetooth. Sun
- Microsystems Inc, February 2003.
- Steven P. Miller. What is RFID? Purdue University.
- Nokia. Nokia 6131 NFC Technical product description.
- Nokia. White Paper Near Field Communication.
- FORUM NOKIA. Bluetooth Technology Overview. Version 1.0, April 4, 2003.
- FORUM NOKIA. Nokia 6131 NFC SDK: User's Guide. Vers on 1.1, July 3, 2007.
- FORUM NOKIA. MIDP: Bluetooth API Developer's Guide. Version 2.0, October 31st, 2006.
- Hilty Kohler Kelter Ullmann Wittmann Oertel, Wolk. Security Aspects and Prospective Applications of RFID Systems. Bundesamt fr Sicherheit in der Informationstechnik, Bonn, 11 January 2005.
- Ed Ort. Writing a Java Card Applet. Sun Microsystems Inc.
- Francesco Prato. Near Field Communication (NFC) Marketing Introduction.
- Terry R Sherman. How Radio Frequency Identi_cation (RFID) works. 5/8/2003.
- Steffen Steinmeier. The Near Field Communication (NFC) Technology Roadmap. NXP Semiconductors, March 2006.
- RFID Handbook, http://www.rfid-handbook.com/
- http://www.Zebra.com/
- http://www.jltrfid.com/
- http://www.nec.it/
- http://en.wikipedia.org/wiki/Main_Page

- http://www.upmraflatac.com/
- http://www.impinj.com/
- http://www.intermec.com/
- http://www.alientechnology.com/
- RFID Journal, http://www.rfidjournal.com
- http://www.eurochip.com/
- http://www.rfiditalia.com
- http://newsrfid.com
- www.bioblog.it
- http://www.eximia.it
- http://www.microsoft.com/italy/stampa/speciali/smau/mbs/scheda_rfid.mspx
- http://www.sun.com/software/solutions/rfid

Miscellanea bibliografia su WSN

- Microchip Technology Inc., "PicDem Z demostration kit user's guide," 2004. Disponibile in rete: http://ww1.microchip.com /downloads /en /DeviceDoc /51524a.pdf.
- Microchip Technology Inc., "PICMicro 18C MCU Family Reference Manual," 2000. Disponibile in rete: http://ww1.microchip.com /downloads /en /DeviceDoc /80214a.pdf.
- Microchip Technology Inc., "PIC18F2525/2620/4525/4620 Data Sheet," 2004. Disponibile in rete: http://ww1.microchip.com /downloads /en /DeviceDoc /39626b.pdf.
- Ciaràn Lynch and Fergus O' Reilly, "PIC-based TinyOS Implementation," in Proc. 2nd European Workshop on Sensor Networks, Instanbul, Feb 2005, pp. 378-385.
- Hans-Jörg Körbert, Housam Wattar, Gerd Scholl, and Wolfang Heller, "Embedding a Microchip PIC18F452 based commercial platform into TinyOS,"
- Microchip Technology Inc., "PIC16F87X Datasheet," Revision C, 2000. Disponibile in rete: http://ww1.microchip.com /downloads /en /DeviceDoc /30292c.pdf.

- Microchip Technology Inc., "18FXX2 Data Sheet", 2002.
- Microchip Technology Inc., "Thermal Sensor with SPI Interface," 2002. Disponibile in rete: http://ww1.microchip.com /downloads /en /DeviceDoc /20092a.pdf.
- Microchip Technology Inc., "MPLAB C18 C Compiler User's Guide," 2005. Disponibile in rete: http://ww1.microchip.com/ downloads /en /DeviceDoc /MPLAB_C18_Users_Guide_51288j.pdf
- Microchip Technology Inc., "PIC18 Configuration Settings Addendum," 2005, pp. 188-191. Disponibile in rete: http://ww1.microchip.com /downloads /en /DeviceDoc/51537A.pdf.
- Microchip Technology Inc., "MPLAB IDE User's Guide," 2006. Disponibile in rete: http://ww1.microchip.com /downloads/en /DeviceDoc /51519B.pdf.
- GNUPIC Project Website, http://www.gnupic.org
- Atmel Corporation. ATmega128 Data-Sheet, 2003. http://www.atmel.com.
- Paramvir Bahl and Venkata N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. INFOCOM, (2):775{784, 2000.
- N. Bulusu, J. Heidemann, and D. Estrin. Gps-less low cost outdoor localization for very small devices. Technical report, University of Southern California, Computer science department, April 2000. citeree. iso. psi. edt/bulusu00gpsless.html.
- Crossbow. MPR/MIB Users Manual. http://www.xbow.com.
- Lance Doherty, Kristofer S. J. Pister, and Laurent El Ghaoui. Convex position estimation in wireless sensor networks. In First ACM International Workshop on Wireless Sensor Networks and Application, In Proceedings IEEE INFOCOM. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society, 2001.
- Deborha Estrin, Tommy Tran, Nirupama Bulusu, and John Heidemann. Self-configuring localization system: design and experimental evaluation. ACM transactions on embedded computer system, TDB, pages 1{31, 2004.
- Charalampos Fretzagias and Maria Papadopouli. Cooperative location sensing for wireless network. University of North Carolina at Chapel Hill, Departement of computer science, 2004.

- I. Guvenc, C. T. Adballah, M. Jordan, and O. Dedeoglu. Enhancement to rssi based indoor tracking systems using kalman filters. Technical report, International Signal Processing Conference (ISCP) and Global Signal Processing Expo (GSPx), March 2003.
- Tian He, Chengdu Huang, John A. Stankovic, Brian M. Blum, and Tarek Abdelzaher. Range-free localization schemes for large scale sensor networks. Technical report, University of Virginia, Departement of computer science, June 2003.
- Tian He, Chong Liu, and KuiWu. Sensor localization with ring overlapping based on comparison of received signal strength indicator. In Proceedings of the 1st IEEE international Conference on Mobile ad-hoc and sensor system (MASS04), Florida, October 2004. Fort Lauderdale.
- J. Hightower, C. Vakili, G. Borriello, and R. Want. Design and calibration of the SpotOn ad-hoc location sensing system. Computer Science and Engineering, 2001.
- Jeffrey Hightower and Gaetano Borriello. A survey and taxonomy of location system for ubiquitous computing. Computer Science and Engineering, University of Washington, Seattle, WA 98195, Box 352350, September 2001. UW-CSE 01-08-03.
- J. S. Kenney and A. Leke. Power Amplifier Spectral Regrowth for Digital Cellular and PCS Applications. Microwave J., October 1995.
- Koen Langendoen and Niels Reijers. Distributed localization in wireless sensor networks: a quantitative comparison. Computer Networks, (43(4)):499{518,2003.
- Chong Liu and Kui Wu. Performance evaluation of range-free localization methods for wireless sensor networks. In Proceedings of 24th IEEE International Performance Computing and Communications Conference (IPCCC2005), Phoenix, Arizona, April 2005.
- John H. Mathews. Modules for Numerical Methods and Numerical Analysis: Least Squares Line Fitting. http://mathews.ecs.fullerton.edu /n2003/LeastSqLineMod.html, 2004.
- Miodrag Potkonjak, Alberto Sangiovanni, Vincentelli Farinaz Koushanfar, and Sasa Slijepcevic. Ad-Hoc Wireless Networking, chapter Location Discovery in Ad-hoc Wireless Sensor Networks. ACM Press, 2003.

- Nissanka B. Priyantha, Anit Chakraborty, and Hari Balakrishnan. The Cricket location-support system. Mobile Computing and Networking, pages 32{43, 2000.
- B. S. Rao and H. F. Durrant-Whyte. Fully decentralised algorithm for multi-sensor kalman filtering. In Control Theory and Applications, volume 138, pages 413{420, Phoenix, Arizona, September 1991. IEEE Proceedings D.
- Chris Savarese, Jan M. Rabaey, and Koen Langendoen. Robust positioning algorithms for distributed ad-hoc wireless sensor networks. In Proceedings of the General Track, pages 317{327, Berkeley, CA, USA, 2002. USENIX Annual Technical Conference, USENIX Association.
- A. Savvides, H. Park, and M. Srivastava. The bits and °ops of the n-hop multilateration primitive for node localization problems. In First ACM International Workshop on Wireless Sensor Networks and Application, Atlanta, GA., September 2002.
- Andreas Savvides, Chih-Chieh Han, and Mani B. Strivastava. Dynamic finegrained localization in ad-hoc networks of sensors. In Mobile Computing and Networking, pages 166{179, 2001.
- Standard IEEE 802.15.4. Wireless Medium Access Control(MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).
- R. Want, J. Hightower, and G. Borriello. SpotOn: An indoor 3d location sensing technology based on rf signal strength. Technical report, Seattle, WA, February 2000.
- Roy Want, Andy Hopper, Veronica Falcao, and Jon Gibbons. The active badge location system. Technical report, Cambridge CB2 1QA, ORL, 24a Trumpington Street, 1992.
- Kiran Yedavali, Bhaskar Krishnamachari, Sharmila Ravula, and Bhaskar Srini-vasan. Ecolocation: A sequence based technique for rf localization in wireless sensor network. Technical report, University of Southern California, LA, CA, 2004. USC CENG 2004-16.