ALMA MATER STUDIORUM -UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Scuola di Ingegneria e Architettura
Corso di laurea in Ingegneria Informatica

TECNOLOGIE RFID: DAL TAG AI SISTEMI BACK-END

Elaborata nel corso di: Elettronica dei Sistemi Digitali.

Tesi di laurea di:
THOMAS FARNETI

Relatore:
PROF. ALDO ROMANI

SESSIONE II

Anno Accademico 2012/2013

PAROLE CHIAVE

RFId

Identificazione

Middleware

Tag

Reader

Alla mia famiglia e a mia nonna,
che tanto ha sognato questo giorno.

Indice

Introduzione

I sistemi di identificazione tramite radiofrequenza hanno acquistato negli ultimi tempi una sempre maggiore importanza per il mondo produttivo, soprattutto nel settore della movimentazione delle merci, evolvendo verso applicazioni di tracciamento sempre più avanzate.

La tesi si propone di analizzare in dettaglio la tecnologia RFId, chiarendone gli aspetti fondamentali.

Il primo capitolo fornisce una breve introduzione alla RFId. Verranno quindi delineati i componenti fondamentali e si analizzeranno vantaggi e svantaggi della tecnologia.

Seguirà poi una serie di capitoli dedicati ai componenti fisici come tag antenne e reader dei quali verranno descritte in dettaglio le componenti fondamentali, i tipi e gli standard.

Dopo il layer fisico si passerà all'analisi del software che compone la tecnologia. In particolare si parlerà di Middleware e di Information Service analizzandone le caratteristiche e definendone un modello di uso comune..

Gran parte del materiale reperito da libri di testo, è stato poi unito alle conoscenze acquisite dal laureando durante la sua esperienza lavorativa nel settore RFId.

1 Introduzione alla RFId

1.1 Generalità e storia

RFID (Radio Frequency Identification) sta a indicare la funzione d'identificazione attraverso la radiofrequenza. L'identificazione implica l'assegnazione di un'identità univoca a un oggetto che consenta di distinguerlo in modo non ambiguo [1].

I primi rudimenti risalgono alla fine degli anni 30. Con il progredire dell'aviazione e degli armamenti ci si pose il problema dell'IFF (Identification Friend or Foe) ovvero identificare un velivolo nemico in avvicinamento in tempi rapidi e distinguendolo da quelli alleati.

La Luftwaffe risolse questo problema con un'ingegnosa manovra. Quando illuminati dal radar alleato, i piloti Tedeschi compievano un rapido rollio in modo da variare il segnale di ritorno riflesso dai loro Aeroplani. La conseguente modulazione dei segnali di ritorno nello schermo del radar permise agli operatori radar di identificare questi segnali come alleati.

Questo è il primo esempio [2] dell'uso della retrodiffusione passiva e di conseguenza della radiofrequenza per l'identificazione. Passiva si riferisce alla mancanza di un trasmettitore radio sull'oggetto da identificare; il segnale utilizzato per comunicare è un segnale radio trasmesso dalla stazione radar e ritrasmesso a esso dall'oggetto da identificare.

1.2 La struttura del sistema

Un sistema RFId, come mostrato in Figura 1.1 è sostanzialmente costituito da quattro elementi:

- **Tag** composto di un chip e un'antenna.
- **Antenna** che colloquia con quella del tag attraverso le onde radio.
- **Reader** che da una parte scambia dati con i tags RFId e dall'altra s'interfaccia a un sistema informatico cui è collegato.
- **Middleware** che s'interfaccia tra le applicazioni aziendali e i dati fisici raccolti attraverso i reader.

Figura 1.1 Struttura di un sistema RFId [3]

1.3 Vantaggi e Svantaggi

L'utilizzo della radiofrequenza garantisce una serie di vantaggi, ma allo stesso tempo pone dei limiti che durante lo sviluppo di un sistema, vanno compresi profondamente [4]

1.3.1 Visibilità diretta non richiesta

Questo è il più lampante e sicuramente il più importante vantaggio di questa tecnologia [4].

Se i codici a barre richiedono l'assoluta necessità di essere visibili, le etichette RFId non risentono di questo problema. Infatti, le onde radio che trasferiscono energia al tag ne trasmettono il contenuto d'informazione al sistema di lettura attraversando facilmente ogni superficie non metallica.

Queste caratteristiche portano quantomeno a tre vantaggi:

- **Efficienza,** poiché l'acquisizione dei dati può avvenire senza l'intervento umano
- **Flessibilità,** non essendo richiesta visibilità ottica.
- **Robustezza,** perché i tag possono essere inglobati direttamente nei pallet o nelle scatole ricevendone ulteriore protezione.

Come già anticipato però, le onde radio temono alcuni ostacoli tra i quali i metalli che ne impediscono l'attraversamento ed i liquidi che assorbono energia trasformandola in calore. Il metallo, oltre a schermare, può produrre anche effetti riflessivi fastidiosi creando zone d'ombra in cui le onde riflesse si elidono.

1.3.2 Letture simultanee multiple

Grazie a degli opportuni meccanismi di anticollisione, è possibile la lettura multipla e simultanea dei Tag.

Si prenda ad esempio la lettura di un pallet. Con un sistema Barcode occorrerebbe disassemblare il pallet e leggere scatola per scatola. Attraverso la radiofrequenza è possibile (se prese le dovute precauzioni) leggere simultaneamente il contenuto dell'intero pallet.

La lettura di un tag ovviamente è solo apparentemente contemporanea: il meccanismo di anticollisione consente al lettore di isolare di volta in volta con una e una sola etichetta RFId presenti nel campo di lettura. Terminata l'identificazione, il lettore passa all'etichetta successiva iterando il procedimento per tutte le etichette presenti. Ovviamente tutto ciò richiede un determinato tempo che dipende dal numero di tag presenti contemporaneamente.

1.3.3 Capacità di lettura e scrittura

Come si può facilmente immaginare una volta stampato un barcode è immodificabile. Ciò non avviene per i tag RFId i cui chip sono dotati di memoria che può essere riscritta un numero teoricamente infinito di volte garantendone maggiore accuratezza e flessibilità.

Ovviamente rispetto alle tecnologie Read-Only vi è un sostanziale aumento di costo che è tanto superiore quanto più grande è la capacità di memoria.

1.3.4 Vita e sopravvivenza

La sopravvivenza di un barcode è strettamente legata all'ambiente in cui opera. In ambienti particolarmente ostili può essere facilmente soggetto ad usura e sporco rendendone impossibile la lettura. Ciò non avviene per i tag RFId che potendo essere inglobati nel contenitore sono insensibili all'usura garantendone una durata pressoché illimitata [4].

1.4 Applicazioni

Come si può desumere dal nome, la tecnologia RFId ha un forte utilizzo in tutti gli ambiti nei quali è appunto richiesta l'identificazione di oggetti o persone. Si pensi ad esempio ai sistemi elettronici di raccolta pedaggi, i tag impiantati negli animali, gli "Ski pass" e perfino i sistemi di bloccaggio centralizzato dei veicoli.

Uno dei settori maggiormente influenzati dalla RFId è sicuramente quello della Grande Distribuzione Organizzata sia per i numeri sia per la forte correlazione con la tecnologia stessa. I tag sono principalmente usati come supporto dei codici identificatori universali

estendendo le informazioni contenute nei codici a barre (tipo di merce, produttore, ecc.). Con la riduzione progressiva dei costi si potrà applicare un tag RFId anche al singolo prodotto (item level tagging) rendendo accessibile a tutti gli attori della supply chain, una quantità di dati mai vista finora [1].

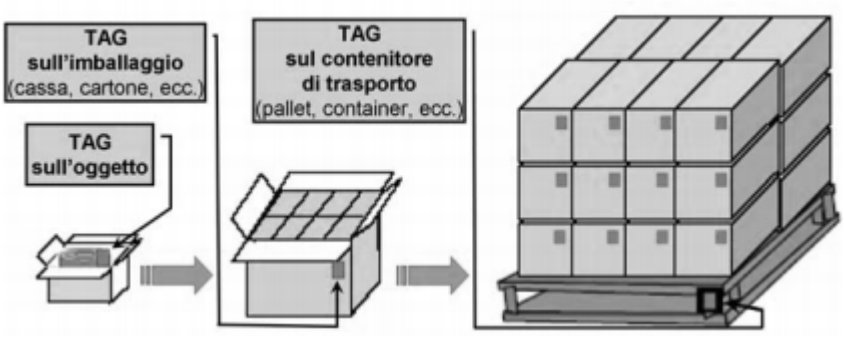

Figura 1.2 Esempio di Applicazione RFId [1]

2 Tags

2.1 Introduzione

In un sistema RFId gli elementi da indentificare e da tenere traccia sono contrassegnati con dei tag. Un tag è quindi la "Dolce metà" del sistema, perché contiene informazioni sull'articolo cui è collegato e ha la capacità di fornire le informazioni su richiesta.

2.2 Elementi Costitutivi di un Tag

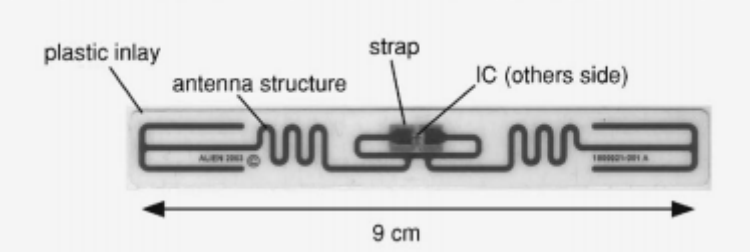

Figura 2.1 Elementi Costitutivi di un Tag [2].

Le funzionalità di un tag generalmente consistono nel:

- Memorizzare informazioni riguardo a un item.
- Elaborare la richiesta d'informazioni proveniente da un lettore.
- Preparazione e invio della risposta alla richiesta.

Per supportare queste funzionalità un tag è costituito da tre principali elementi:

- **Chip** utilizzato per generare o processare un segnale. Si tratta di un circuito integrato in silicio. Il chip è composto a sua volta dai seguenti componenti funzionali:
    - **Unità Logica** che implementa il protocollo usato per la comunicazione tag reader.
    - **Memoria** per lo storage dei dati.
    - **Modulatore** usato per modulare i segnali in uscita e demodulare i segnali in entrata.
    - **Power Controller** che converte l'alimentazione AC del segnale in ingresso in corrente continua per alimentare le parti del chip.

Per inviare e riceve segnali il chip è poi collegato a un'antenna.

- **Antenna** In un sistema RFID, l'antenna di un tag riceve il segnale (una richiesta d'informazioni) da un lettore e trasmette un segnale di risposta (informazioni d'identificazione) indietro al lettore. Solitamente è costituita di metallo o di un materiale a base di metallo. Sia reader sia tag sono dotati di antenna propria.
- **Substrato** cioè lo strato che ospita il chip e l'antenna. In altre parole, è la struttura di supporto per il tag. I substrati possono essere di diversi materiali come plastica, polietilene tereftalato (PET), carta, vetro ed epossidica. Il materiale del substrato può essere rigido o flessibile, in base all'utilizzo. I substrati per etichette RFID sono progettati per soddisfare le seguenti specifiche:
    - Dissipazione di accumulo di cariche statiche.
    - Resistenza in condizioni operative specifiche.
    - Protezione meccanica per IC, antenna e connessioni.
    - Superficie di stampa liscia.

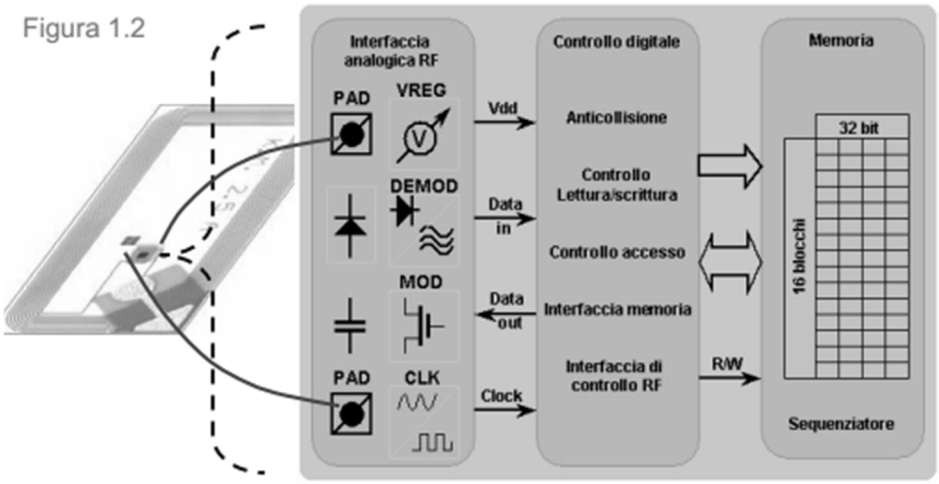

Figura 2.2 Schema di un Chip RFId [4]

2.3 Frequenze Operative

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.

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

- **In banda LF** (Low Frequencies) ed in particolare la sottobanda 120÷145 kHz. Si trova nella parte più bassa dello spettro RF, è storicamente la prima frequenza utilizzata per l'identificazione automatica e, ancora oggi, continua ad avere una presenza rilevante nel mercato. [2]
- **In banda HF** (High Frequencies) ed in particolare la sottobanda centrata su 13,56 MHz. È considerata la banda di frequenze "universale", usabile in tutto il mondo; questo ne ha fatta la banda più diffusa fino ad oggi [2].
- **In banda UHF** (Ultra High Frequencies), nella zona media le sottobande 865 ÷ 870 MHz in Europa – 902÷928 MHz in USA – 950 MHz in Asia. È la "nuova banda" per gli RFID per la logistica e la gestione dei singoli oggetti, con distanze operative significativamente maggiori di quanto non sia consentito da LF ed HF. Purtroppo la banda non è assegnata in modo uniforme nelle varie nazioni. [2]
- **In banda UHF, nella zona alta**, la sottobanda centrata su 2,4 GHz. Con caratteristiche simili all'UHF, permette un'ulteriore miniaturizzazione del TAG. Si tratta, però, di una banda molto affollata da altre tecnologie (WiFi, Bluetooth, ZigBee), con le quali è necessario convivere. Tuttavia, al di fuori dell'Europa, sono usati, su questa banda sia TAG passivi sia attivi, a standard ISO 18000-4. Esistono anche altre frequenze utilizzabili quali 433 ÷ 435 MHz in banda UHF bassa o 5,8 GHz in banda SHF (Super High Frequencies).

A oggi, alcune bande di frequenza (generalmente nelle LF o HF) sono accettate in tutto il pianeta. Un esempio per tutti è la banda dei 13,56 MHz, usata da molti TAG passivi incorporati essenzialmente nelle Smart card per controllo accessi, identificazione e

pagamenti, ma anche nelle etichette associate ad oggetti, quali controllo bagagli, lavanderie, biblioteche, ecc.

Per altre bande di frequenza, specie per quelle UHF di uso più recente, le allocazioni sono differenti da regione a regione, anche se gli standard garantiscono l'interoperabilità.

La scelta della frequenza di lavoro influisce sulla distanza (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. [1] 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 distanze operative maggiori. [1] Per sistemi a frequenza più alta, la velocità di trasferimento dati è generalmente maggiore mentre la dimensione delle antenne si riduce. Questo consente di costruire TAG più piccoli. [1]

Nome	Range Frequenze	Range Lung. d'onda	Frequenza ISM	Raggio Lettura
LF	30-300 kHz	10 km-1 km	<135 kHz	<50 cm
HF	3-30 MHz	100 m-10 m	6.78 MHz, 8.11 MHz, 13.56 MHz, 27.12 MHz	<3 m
UHF	300MHz-3GHz	1 m-10 cm	433 MHz, 869 MHz, 915 MHz	<9 m
Microwave	3GHz-300GHz	30 cm- mm	2.44 GHz, 5.8 GHz	>10 m

Tabella 2-1 Range operativi per sistemi RFId

La Tabella 2-1 mostra gli intervalli di frequenza radio che sono d'interesse per i sistemi RFID, insieme alle frequenze ISM.

2.4 Classificazione dei Tag per frequenze

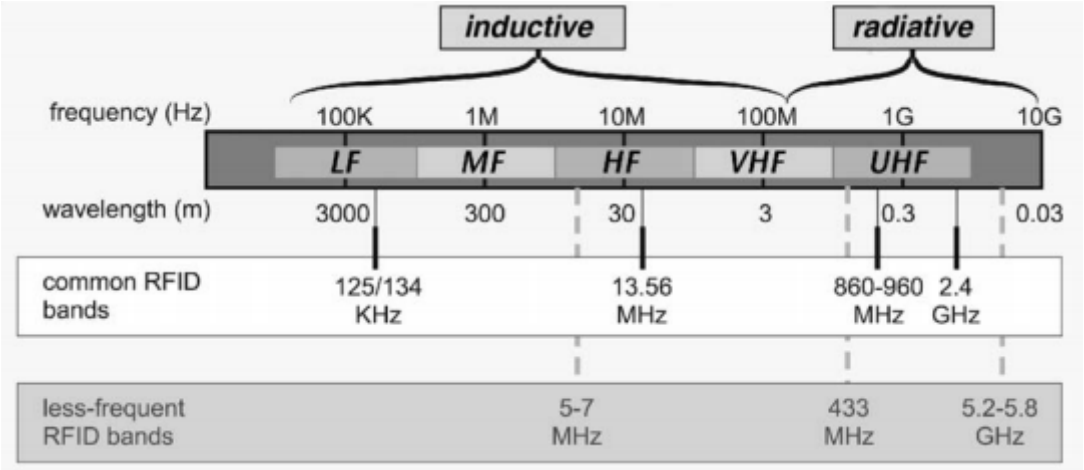

Figura 2.3 Banda di Frequenze RFId [2]

2.4.1 Tag Induttivi LF 120-145 KHz

La sottobanda operativa si trova nella parte bassa dello spettro RF, è storicamente la prima banda di frequenze utilizzata per l'identificazione automatica e rimane ancora oggi una presenza significativa nel mercato. L'accoppiamento Reader-TAG avviene per via induttiva, con lo stesso principio fisico dei trasformatori elettrici.

Nel caso di TAG passivi la distanza operativa è all'incirca pari al diametro dell'antenna del lettore e varia dai 30 cm al metro [1], oltre questa portata il campo si riduce molto rapidamente. Anche per questo motivo la distanza per poter eventualmente scrivere nella memoria, operazione che richiede un maggiore consumo di energia da parte del chip che equipaggia il TAG, è normalmente più bassa di quella di lettura; tipicamente è inferiore del 30÷50%.

Da notare che all'interno della banda LF in realtà sono due le frequenze operative più utilizzate:

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

La frequenza di 125kHz della portante è relativamente bassa e consente velocità massime di trasmissione dei dati nell'ordine del migliaio di bit al secondo [1]. A questa frequenza è meno diffuso il supporto di letture multiple ovvero di più TAG contemporaneamente presenti nel campo del lettore.

I TAG a una frequenza di 134,2 kHz sono utilizzati principalmente nella tracciabilità animale per la bassissima influenza che l'acqua ed i tessuti hanno sulla trasmissione. [1]

2.4.2 Tag Induttivi HF 13,56 MHz

La sottobanda di frequenze è riconosciuta da tutti gli enti normatori mondiali e questo ne ha fatto la banda più diffusa fino ai giorni nostri.

L'accoppiamento Reader-TAG avviene per via induttiva, come nei TAG LF.

La configurazione tipica prevede un'antenna formata da un avvolgimento normalmente in rame, ma è utilizzato anche l'alluminio, formato su un substrato piatto e ottenuto per incisione da un sottile foglio di metallo dello spessore di qualche decina (60-70) di μm, oppure depositato, sul medesimo substrato con inchiostri conduttivi. La dimensione ed il numero di spire determinano la sensibilità e la distanza operativa (insieme, ovviamente, alla dimensione ed alla potenza emessa dall'antenna del Reader).

I costi sono inferiori a quelli dei TAG LF ma strettamente dipendenti dal tipo di supporto e dalla dimensione, così come quelli dei Reader che godono di un buon livello di maturazione.

Le ultime generazioni di chip per questa tipologia di TAG supportano come funzionalità quasi standard i meccanismi anticollisione che consentono la lettura/scrittura di più TAG contemporaneamente presenti nel campo del Reader. A differenza di quanto avviene in UHF il campo RF a 13,56 MHz non è particolarmente influenzato dall'acqua o dai tessuti del corpo umano [1]. La banda HF è attualmente la più usata per le cosiddette "etichette intelligenti" (smart TAG) impiegate nella logistica e nella gestione degli oggetti, anche se, per quest'ultima applicazione si prevede che, a lungo termine, prevarranno i sistemi in banda UHF.

In questa frequenza operano anche le "Smart Card Contactless", ovvero carte intelligenti senza contatto che costituiscono il settore più tecnologicamente presidiato dai produttori di chip. Le funzionalità offerte spaziano dalla capacità di memoria, che può andare dai pochi Kb e toccare oggi anche il Mb, alla disponibilità di algoritmi crittografici per effettuare transazioni sicure. Quasi unicamente di tipo passivo, sono coperte da standard quali l'ISO/IEC 14443 – detto anche di 'proximity', che copre da 10 a 30 cm e l'ISO/IEC 15693, o di 'vicinity', per una distanza operativa da 30 a 90 cm. Diffuse nel settore del ticketing, del controllo accessi del personale, della tracciabilità dei bagagli nei sistemi aeroportuali, sono le Contactless Smart Card diventate comuni

come sostitutivi intelligenti ed inviolabili delle schede magnetiche per le transazioni bancarie (bancomat) e come carte di credito. Diversi stati le stanno introducendo come passaporto elettronico. [1]

2.4.3 Tag Elettromagnetici UHF 860-950 MHz

L'evoluzione tecnologica dei semiconduttori, che ha portato alla realizzazione di chip particolarmente parsimoniosi nel consumo energetico, ha consentito la realizzazione di etichette RFID operanti a questa frequenza e con distanza operativa decisamente più estesa di quanto non fosse consentito con LF ed HF.

L'accoppiamento Reader-TAG avviene per via elettromagnetica, come nei tradizionali sistemi di radiocomunicazione. Una distanza operativa di 3 metri è ormai standard, ma sempre più spesso estendibile verso cinque e più metri. Grazie a questo l'UHF media è destinata sicuramente a confermarsi come la banda regina della logistica e, soprattutto, della gestione degli oggetti. Tuttavia alcune problematiche, ad oggi in via di risoluzione, ne hanno rallentato l'introduzione.

- **Frequenze operative:** Usa, Europa e Asia si trovano a dover gestire frequenze diverse: le frequenze già occupate dalla telefonia cellulare, e quindi ormai immutabili, non consentono alle tre aree geografiche di utilizzare le stesse bande per le applicazioni RFID. Tuttavia i TAG passivi vengono spesso costruiti con accorgimenti che ne esaltano la capacità di rispondere a "larga banda", il che ne consente l'operatività su bande differenti (purché non troppo) al costo di un decadimento nelle prestazioni. Per i TAG attivi invece, se necessario gli apparati ricetrasmittenti vengono tarati su più frequenze (a scapito dei costi).
- **Standard di comunicazione:** sono necessari standard accettati dalla comunità internazionale per i protocolli di comunicazione tra Reader e TAG. Il problema è stato superato in tempi recenti dalla definizione del protocollo EPC "Class 1/Generation2" [6] e dalla relativa inclusione nello standard ISO/IEC 18000-6 Type C avvenuta nel luglio del 2006.
- **Potenze in trasmissione e larghezza delle bande di frequenza**: in Usa e in Europa esistono differenti limitazioni per la potenza massima emessa e, soprattutto, differenti larghezze della banda di frequenza UHF dedicata; ovvero esiste un maggior numero di canali sui quali i Reader possono operare per interrogare i TAG. In logistica, questo si traduce (per gli USA) in un vantaggio

competitivo (es. capacità di leggere rapidamente tutto il contenuto di una pallet) e di conseguenza un minore costo del servizio. Ciò avviene perché, potendo usufruire di un numero maggiore di canali, è possibile far operare contemporaneamente (nella stessa area) un maggior numero di reader, inoltre ciascun Reader opera a potenza leggermente maggiore (maggiore distanza operativa).

A queste frequenze ci si scontra con problematiche più complesse di quanto non si riscontri a frequenze inferiori:

- **Riflessioni:** le strutture metalliche in prossimità dell'antenna possono riflettere le onde elettromagnetiche; queste riflessioni possono, incontrandosi con l'onda diretta dell'antenna in opposizione di fase, generare degli spazi in cui il campo elettromagnetico risulta nullo. I TAG in queste aree sono illeggibili.
- **Liquidi:** l'assorbimento da parte dell'acqua delle onde elettromagnetiche si fa più consistente. L'efficienza di lettura in ambienti particolarmente umidi o con TAG applicati a contenitori di liquidi può diventare difficoltosa.

Essendo l'UHF media, grazie alla sua distanza operativa, la frequenza più utilizzata nella logistica, i rispettivi TAG dovrebbero arrivare, grazie all'esplosione attesa nei volumi di produzione, ad avere il costo più basso. La velocità di trasmissione risulta superiore a quella dei sistemi operanti a frequenze più basse. I sistemi, inoltre, sono in grado di gestire letture multiple contemporanee (anticollisione) arrivando alla lettura di più di 100 TAG al secondo. Le caratteristiche (tecnologiche e dell'algoritmo di anticollisione) di TAG conformi alle specifiche EPC/ISO Class1/Gen2 dovrebbero consentire, in linea teorica, la lettura di 600 (in Europa) e 1.500 (in USA) TAG/s che si presentino contemporaneamente al lettore. Il supporto da parte dei fornitori di tecnologia si va facendo via via più consistente, con un sempre maggior numero di fornitori e con ampliamento della possibilità di scelta sia sulle capacità di memoria dei chip che sulla possibilità di avere TAG passivi, attivi o semipassivi. [1]

2.5 Tag Passivi, Semi-passivi, Attivi

Le due caratteristiche principali che determinano le prestazioni e l'uso di un tag sono il tipo e la frequenza alla quale il tag opera. I tipi di tag sono determinati da due fattori: la capacità di avviare la connessione e la fonte di alimentazione. In base alla combinazione dei precedenti fattori sono definiti tre tipi di tag.

2.5.1 Tag Passivi

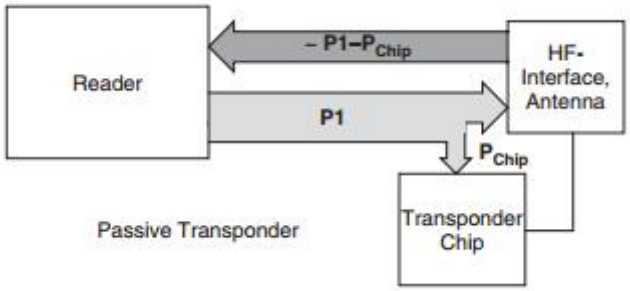

Figura 2.4 Schema tag Passivo [5]

È detto passivo un tag che non ha una propria sorgente di alimentazione, ad esempio una batteria, e quindi non può avviare la comunicazione. Risponde al segnale inviato dal lettore prendendo alimentazione dal segnale stesso. In altre parole, il segnale del reader sveglia il tag passivo. Il comportamento di un generico tag passivo è il seguente:

1. L'antenna riceve il segnale dal reader.
2. Il segnale è inviato al IC.
3. Una parte della potenza del segnale è utilizzata per alimentare l'integrato.
4. Il chip elabora il segnale in ingresso ed invia la risposta.

Le principali caratteristiche di un tag passivo sono:

- **Posizionamento** in quanto il tag dipende interamente dal lettore per la sua alimentazione e deve trovarsi all'interno della zona di interrogazione per ottenere abbastanza energia per elaborare la risposta.
- **Range e Dimensione** essendo sprovvisti di batteria i tag passivi tendono ad avere una dimensione minore ed un range di lettura più ridotto rispetto ai tag attivi.
- **Durata** non dovendo rimpiazzare la batteria hanno una durata elevata.

- **Frequenza Operativa** generalmente i tag passivi operano nelle frequenze LF Hf UHF.
- **Costo** ridotto dato la loro semplicità

2.5.2 Tag Semi-passivi

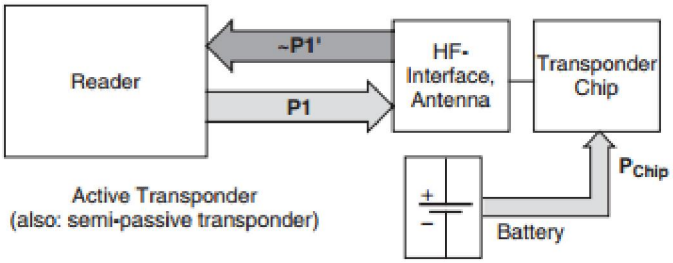

Figura 2.5 Schema Tag Semi-Passivo [5]

Un tag semi-passivo è dotato di batteria ma non avvia la comunicazione. È attivato dal segnale del lettore e utilizza la propria batteria per alimentare i circuiti. Dato che come quelli passivi sfrutta l'energia del lettore il loro modo di operare è praticamente identico. In compenso dovendo contenere una batteria è di dimensioni maggiori ed ha una durata inferiore. Questi tag hanno il vantaggio di produrre un segnale di risposta più forte con un raggio di lettura molto ampio. In alcuni casi la batteria può essere utilizzata per alimentare dei piccoli sensori.

2.5.3 Tag Attivi

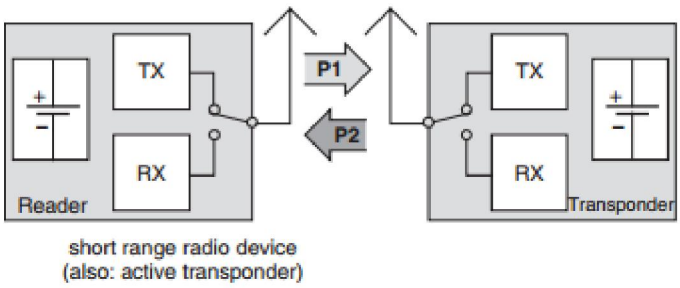

Figura 2.6 Schema Tag Attivo [5]

Un tag attivo è dotato di batteria e non utilizza l'alimentazione del segnale del lettore. Il vantaggio dei TAG attivi è dato dalla distanza operativa molto superiore rispetto a quelli passivi e semi-passivi, poiché equipaggiati con un vero trasmettitore alimentato da fonte di energia. La distanza raggiungibile è limitata solo dall'antenna e dall'energia

disponibile nelle batterie. A volte i TAG attivi hanno a bordo sensori di vario genere (temperatura, pressione, movimento, ecc.) che sono usati, come si è detto, anche nei TAG semi passivi. Sono generalmente prodotti per frequenze elevate (UHF, SHF) e sono naturalmente dedicati ad applicazioni “di pregio”, oppure in casi in cui il TAG sia riusabile più volte.

3 Accoppiamento Tag-Reader nei sistemi Passivi

A differenza degli apparati di tipo attivo, i TAG passivi dipendono per la loro alimentazione dall'energia a radio frequenza che ricevono. I TAG passivi, inoltre, non generano la frequenza portante che usano per la trasmissione. Piuttosto essi re-irradiano, modulandola, una parte dell'energia trasmessa dal Reader che li sta interrogando. Questo fa riferimento alla possibilità di modulare un segnale generato dal Reader tramite la variazione dell'impedenza dell'antenna del TAG che trasforma l'antenna medesima da assorbente a riflettente. Tale processo è molto simile all'uso di uno specchio e della luce solare per segnalazioni luminose a distanza [1]. Per ricavare energia e comunicare con il Reader, il funzionamento dei TAG passivi si basa su uno dei due principi fisici seguenti: accoppiamento Induttivo ed accoppiamento Elettromagnetico.

3.1 Accoppiamento induttivo

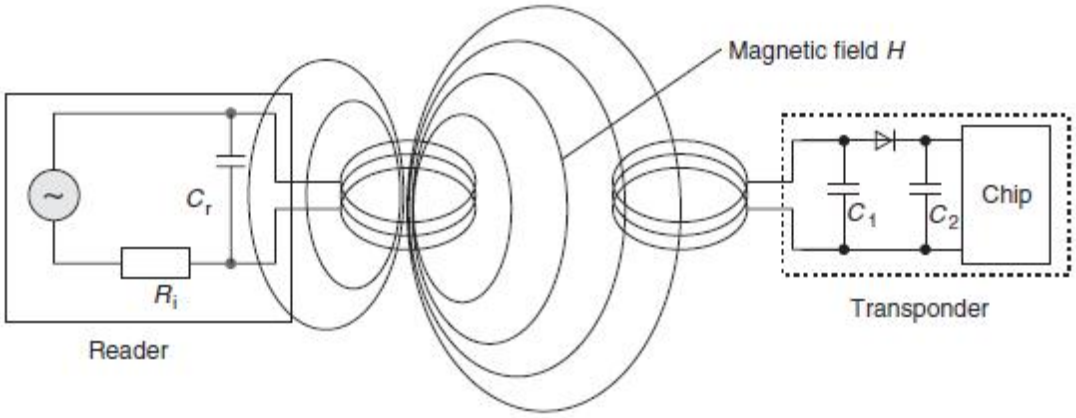

Figura 3.1 Schema accoppiamento induttivo Tag-Reader [5].

3.1.1 Alimentazione per transponder passivi

Un transponder induttivamente accoppiato comprende un dispositivo elettronico di trasporto dati, di solito un unico microchip, e una bobina di grande superficie o un loop conduttore che funge da antenna.

I transponder ad accoppiamento induttivo sono quasi sempre azionati passivamente. Ciò significa che tutta l'energia necessaria per il funzionamento del microchip deve essere fornita dal lettore.

A questo scopo, l'antenna del lettore, genera un forte campo elettromagnetico ad alta frequenza, che penetra la sezione trasversale dell'area della bobina e la zona attorno alla bobina stessa. Poiché la lunghezza d'onda della banda di frequenza utilizzata (<135 kHz: 2400 m, 13,56 MHz: 22,1 m) è di molte volte maggiore della distanza tra antenna del lettore e transponder, il campo elettromagnetico può essere trattato come un semplice campo magnetico alternato in relazione alla distanza tra Transponder e antenna.

Una piccola parte del campo emesso penetra l'antenna a bobina del transponder, che è una certa distanza dalla bobina del lettore. Una tensione Ui viene generata nell'antenna del transponder per induttanza. Questa tensione viene raddrizzata e serve come alimentazione per il dispositivo di trasporto dati (microchip).

Un condensatore Cr è collegato in parallelo con la bobina dell'antenna del lettore. La capacità di questo condensatore è stata selezionata in modo che funzioni con l'induttanza della bobina della bobina per formare un circuito risonante con una frequenza di risonanza corrispondente alla frequenza di trasmissione del lettore. Correnti molto elevate possono essere generate nella bobina dell'antenna del lettore mediante l'aumento della risonanza nel circuito risonante parallelo, che può essere utilizzato per generare le intensità di campo richiesti per il funzionamento del transponder remoto.

La bobina dell'antenna del transponder e il condensatore C1 formano un circuito risonante sintonizzato sulla frequenza di trasmissione del reader. La tensione U alla bobina del transponder raggiunge un massimo dovuto all'aumento della risonanza nel circuito risonante parallelo.

La disposizione delle due bobine può anche essere interpretata come un trasformatore nel qual caso vi sia solo un accoppiamento molto debole tra i due avvolgimenti. L'efficienza del trasferimento di potenza tra la bobina dell'antenna del redear e del trasponder è proporzionale alle frequenza operativa f, al numero degli avvolgimenti n, all'angolo relativo tra le due bobine e alla loro distanza.

3.1.2 Modulazione di carico

Come descritto in precedenza, i sistemi ad accoppiamento induttivo si basano su un accoppiamento simile a quello dei trasformatori tra la bobina primaria nel lettore e la bobina secondaria nel transponder. Questo è vero quando la distanza tra le bobine non supera $\lambda/2\pi$ in modo che il transponder si trovi nel campo vicino dell'antenna trasmittente.

Se un transponder risonante è posizionato entro il campo magnetico alternato dell'antenna del lettore, il transponder trae energia dal suddetto campo. La retroazione risultante del transponder sull'antenna del lettore può essere rappresentata come l'impedenza trasformata ZT nella bobina dell'antenna del reader.

La commutazione on off di un resistore di carico all'antenna del transponder determina un cambiamento nell'impedenza ZT e quindi cambiamenti di tensione all'antenna del reader. Questo ha l'effetto di una modulazione di ampiezza della tensione UL alla bobina dell'antenna del reader dal transponder remoto. Se la temporizzazione con cui la resistenza di carico viene accesa e spenta è controllata dai dati, questi dati possono essere trasferiti dal transponder al lettore. Questo tipo di trasferimento viene chiamato modulazione di carico.

Per recuperare i dati al lettore, la tensione all'ingresso dell'antenna è rettificata. Questo rappresenta la demodulazione di un segnale modulato in ampiezza.

Se il transponder lascia il campo vicino il trasformatore di accoppiamento tra antenna del lettore e antenna del tag è perduto con la transizione nel campo lontano. Pertanto, la modulazione del carico non è più possibile

Questo non significa che la trasmissione di dati dal transponder al lettore non sia più possibile. Con la transizione nel campo lontano il meccanismo dell'accoppiamento a retrodiffusione diventa efficace. In pratica, la trasmissione dei dati al lettore di solito non riesce a causa della bassa efficienza delle antenne dei transponder (cioè il basso guadagno dell'antenna) nel campo lontano.

3.2 Accoppiamento Elettromagnetico

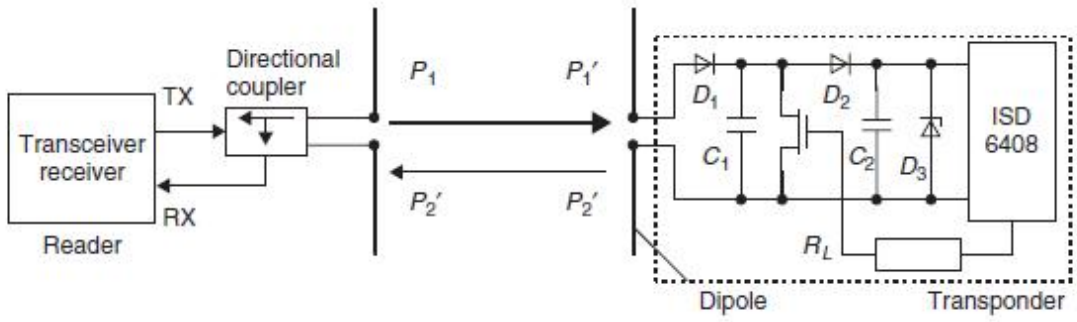

Figura 3.2 Principio operativo di un transponder Backscatter [5].

3.2.1 Retrodiffusione Modulata

Sappiamo dal campo della tecnologia radar che le onde elettromagnetiche vengono riflesse da oggetti di dimensioni superiori a circa la metà della lunghezza d'onda. L'efficienza con cui un oggetto riflette onde elettromagnetiche è descritto dalla sua sezione radar. Oggetti che sono in risonanza con il fronte d'onda che li colpisce, come avviene per le antenne alla frequenza appropriata ad esempio, hanno una sezione radar riflessa particolarmente ampia.

La potenza P1 è emessa dall'antenna del lettore ed una piccola parte raggiunge l'antenna del transponder. La potenza P1 è fornita alle connessioni dell'antenna come tensione RF e dopo essere rettificata dai diodi D1 e D2 può essere utilizzata come tensione di attivazione per la disattivazione o attivazione del risparmio energetico, nel caso di tag dotati di batteria. La potenza ottenuta può anche essere sufficiente per alimentare il tag per brevi intervalli.

Una porzione dell'antenna P1 in arrivo viene riflessa dall'antenna e restituita come potenza P2. Le caratteristiche di riflessione dell'antenna possono essere influenzate alterando il carico collegato all'antenna. Per trasmettere i dati dal trasponder al reader, una resistenza di carico connessa in parallelo con l'antenna viene acceso e spento in tempo con il flusso di dati da trasmettere. L'ampiezza della potenza P2 riflessa dal trasponder può essere quindi modulata (retrodiffusione modulata).

La potenza P2 riflessa dal transponder viene irradiata nello spazio circostante. Una piccola porzione viene prelevata dall'antenna del lettore. Il segnale riflesso viaggia dunque all'indietro nella connessione dell'antenna del lettore e può essere disaccoppiato

mediante un accoppiatore direzionale e trasferito al ricevitore d'ingresso del reader. Il segnale in avanti del trasmettitore, che è più forte, è in larga misura soppresso dall'accoppiatore direzionale.

Il rapporto tra potenza trasmessa dal lettore e potenza di ritorno dal transponder (P1/P2) può essere stimata utilizzando l'equazione radar.

4 Antenne

Un ruolo di grande rilevanza nei sistemi RFID passivi, è giocato dalle antenne del TAG e del Reader. Le antenne sono la fonte primaria di energia per i TAG ed i problemi di orientamento e polarizzazione, influiscono significativamente sulle prestazioni e le problematiche connesse.

4.1 Materiali e tecniche di produzione

Per quanto riguarda i materiali di costruzione, le antenne sono generalmente realizzate in metallo inciso, o con deposizione sul substrato d'inchiostro conduttore. Una tecnologia alternativa prevede un'antenna in filo di rame applicata direttamente sul substrato. A volte, per TAG ad accoppiamento induttivo a bassa frequenza (LF) sono impiegati avvolgimenti in filo su nucleo ferromagnetico. Le prime due tecniche sono impiegate sia per TAG ad accoppiamento induttivo che elettromagnetico, la terza trova applicazione prevalente per TAG ad accoppiamento induttivo, la quarta è, come detto, è principalmente riservata alle basse frequenze (LF).

La maggior parte delle antenne per TAG passivi, sia di tipo elettromagnetico che di tipo induttivo, sono prodotte chimicamente incidendo sottili lastre di rame o di alluminio. In seguito le antenne così ottenute vengono laminate al substrato del TAG. I limiti di questo processo di produzione sono il costo, la lentezza e le condizioni ambientali dato l'utilizzo di acidi [2].

Una tecnologia competitiva è la stampa delle antenne con inchiostro conduttivo. Questa è basata sull'impiego di colle (inchiostri) che contengono un'alta concentrazione di particelle d'argento. Questo processo tuttavia è attualmente ancora costoso ed i suoi limiti sono costituiti dalla bassa conduttività elettrica degli inchiostri, dalle proprietà deboli di adesione, dalla mancanza dell'esattezza di stampa dovuta alla corrosione delle particelle d'argento [2].

4.2 Antenne per Tag ad accoppiamento Elettromagnetico

Le antenne dei TAG ad accoppiamento elettromagnetico sono generalmente dei dipoli progettati anche per favorire il Backscatter.

Per un trasferimento ottimale dell'energia, la lunghezza del dipolo deve essere pari a sottomultipli della lunghezza d'onda. In via ottimale dovrebbe essere uguale a $\lambda/2$, il che comporta (per la banda UHF media) una dimensione intorno ai 16 cm. In realtà il dipolo è spesso costruito a $\lambda/4$, accordandolo con varie tecniche, comunque deviare da questi sottomultipli di lunghezza d'onda comporta gravi perdite di prestazioni [2].

Esistono due importanti parametri per definire le prestazioni delle antenne:

- **Sensibilità energetica** indica l'energia del campo EM necessaria al funzionamento del TAG.
- **Riflettività** indica il rapporto tra potenza RF incidente e riflessa dall'antenna del TAG.

Per quanto riguarda il problema della polarizzazione a volte si opera per rendere i TAG UHF meno sensibili alla polarizzazione del campo EM ricorrendo ad una antenna con due dipoli sistemati in posizione ortogonale

4.3 Antenne per Tag ad accoppiamento Induttivo

Per quanto riguarda il dimensionamento delle antenne a spire, i fattori di maggior influenza sono costituiti dall'area dell'antenna a spire e dal numero di spire.

La tensione indotta ai capi dell'antenna del TAG è, infatti, direttamente proporzionale al numero di spire ed al flusso del vettore induzione magnetica. Quest'ultimo, a sua volta, è calcolato sull'area della spira. Poiché generalmente l'area che complessivamente può occupare l'antenna costituisce un vincolo di progetto, l'aumento del numero di spire è limitato. dalla conseguente riduzione dell'area all'interno delle spire medesime. Con le tecnologie produttive standard presenti sul mercato, non è possibile "giocare" molto sul numero di spire e sulla distanza tra di esse [2].

Questo perché un'antenna stampata occupa già di per sé un certo spessore sul foglio che risulta maggiore rispetto, ad esempio, a quello occupato da un antenna a filo. Quando si aumenta il numero di spire, l'area all'interno dell'antenna si riduce rapidamente; non è quindi possibile spingersi oltre un certo limite.

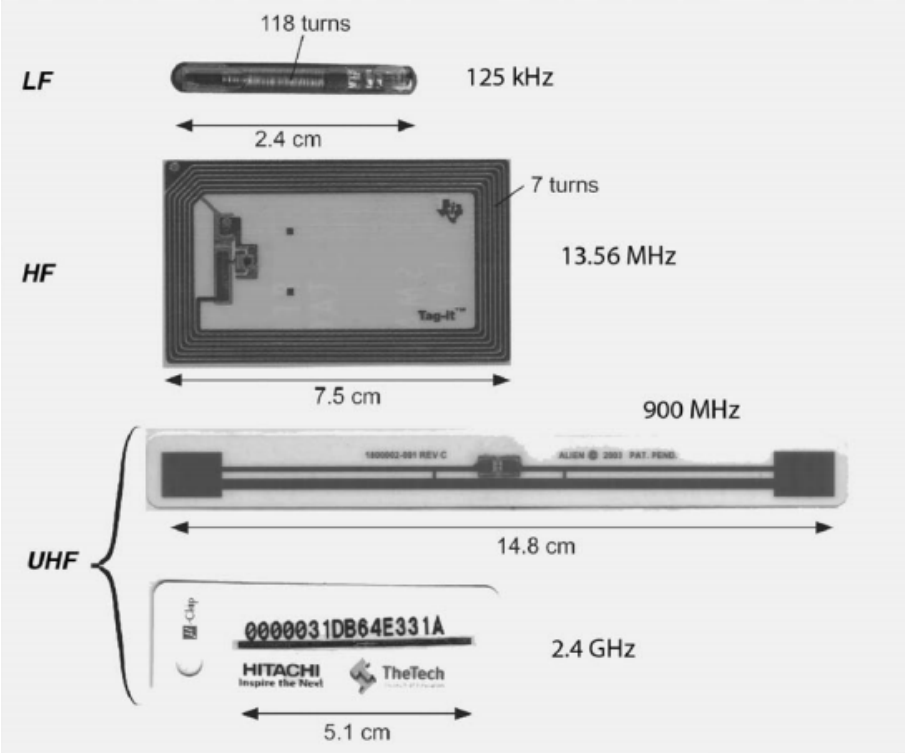

Figura 4.1 Esempi di antenne per differenti frequenze operative [2].

4.4 Accoppiamento induttivo nei tag UHF

Una nuova tecnologia per TAG passivi UHF deriva dallo sfruttamento dell'accoppiamento induttivo in campo vicino, analogamente a quanto avviene per i TAG HF.

L'intensità del campo magnetico diminuisce rapidamente con la distanza; l'accoppiamento induttivo, prevale quindi a brevi distanze (una o due lunghezze d'onda) mentre in "campo lontano" prevale la propagazione del campo elettromagnetico. Tuttavia, entrambe le tipologie di radiazione esistono indipendentemente dalla frequenza operativa [2].

I TAG HF (13,56 MHz) operano generalmente con accoppiamento induttivo perché, a queste lunghezze d'onda, la distanza operativa del "campo vicino" raggiunge e supera il metro; mentre i TAG UHF (860 - 960 MHz) operano generalmente con accoppiamento elettromagnetico in "campo lontano" raggiungendo distanze operative maggiori.

L'antenna dei TAG ad accoppiamento induttivo è realizzata con spire.

Secondo la legge di Faraday si evince che l'effetto dell'accoppiamento magnetico, in condizioni di campo vicino, cresce all'aumentare della frequenza. In particolare nella

banda UHF è circa 60 volte maggiore rispetto alla banda HF [1]. Naturalmente, viste le diverse lunghezze d'onda, per sfruttare l'effetto "campo vicino" bisogna operare, nella banda UHF, a distanze molto più piccole che nella banda HF.

Sfruttando questo fatto, si è visto che i TAG UHF, se dotati di opportuna antenna ed operando in prossimità (qualche cm), possono ricavare dall'accoppiamento induttivo una quantità di energia analoga rispetto a quella dei TAG HF.

In pratica è possibile utilizzare antenne di piccole dimensioni costituite da un'unica spira che possono essere realizzate, ad esempio, mediante processi di stampa con inchiostri conduttivi (a costi contenuti).

Tutto ciò garantisce elevati read/write rate a distanze operative di alcuni cm impiegando gli stessi reader utilizzati per le letture a distanza.

Un altro vantaggio dell'operare in UHF con accoppiamento induttivo è quello di rendere il funzionamento del TAG non influenzato dalla vicinanza o addirittura dall'immersione in liquidi [4], circostanza che rende tale tipologia di TAG adatta per l'impiego in applicazioni in cui sia richiesta questa caratteristica. Inoltre è possibile progettare un antenna che in vampo vicino sfrutti la presenza delle superfici metalliche alle quale il tag può essere fissato. Tale possibilità è in genere preclusa operando in banda HF [3].

Infine, per operare anche a distanze maggiori della stretta prossimità, uno stesso TAG UHF può essere dotato di due antenne distinte per operare sia in campo vicino che in campo lontano.

5 Readers

Un interrogatore RFID è 'elemento che raccoglie le informazioni dai tag e le invia a un sistema Host. Il processo di raccolta delle informazioni dai tag è chiamata lettura delle etichette, e per questo motivo un interrogatore è anche chiamato reader.

L'obiettivo di un sistema RFID è quello di identificare e rintracciare articoli, che si realizza mediante codifica gli articoli con tag e la raccolta delle informazioni riguardanti gli oggetti dai tag. Un interrogatore è al centro di quest'azione.

Dalla prospettiva di un interrogatore, il processo di raccolta dati è eseguito come segue:

1. L'interrogante riceve una richiesta d'informazioni dal sistema Host.
2. L'interrogante invia la richiesta d'informazioni a un tag all'interno della sua zona d'interrogazione.
3. Il tag risponde con le informazioni richieste.
4. L'interrogatore invia le informazioni raccolte al sistema Host.

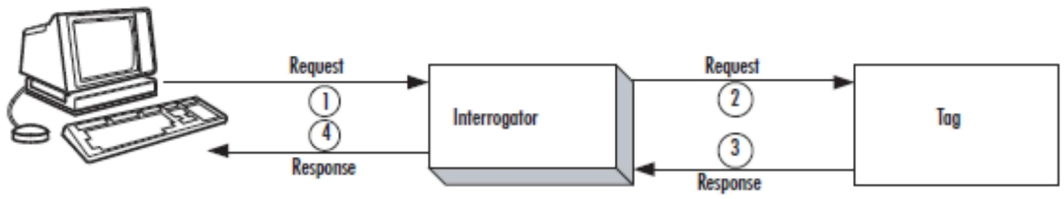

Figura 5.1 Ruolo del reader nel processo di raccolta delle informazioni.

5.1 Elementi Costitutivi di un Reader

Un interrogatore è composto dai seguenti elementi:

- Un modulo RF, chiamato anche un ricetrasmettitore, che modula i segnali RF in uscita e demodula i segnali RF in arrivo.
- Un'unità di controllo ed elaborazione dei segnali
- Un elemento di accoppiamento che comunica con i tag tramite segnali RF (Antenna)
- Un'interfaccia per comunicare con il sistema Host.

Con questi elementi di base, gli interrogatori sono disponibili in varie tipologie.

5.2 Tipi di Reader

Gli interrogatori sono disponibili in varie tipologie per soddisfare le svariate esigenze applicative. Tutti questi tipi sono classificati nelle due categorie seguenti:

- **Read-Only** Leggere le informazioni di sola lettura memorizzata (programmata) nel tag. Tutti quegli interrogatori che possono leggere solo le informazioni dal tag e non possono scrivere le informazioni al tag sono chiamati a sola lettura.
- **Read and Write** Interrogatori che possono scrivere informazioni in un tag oltre a leggerle.

5.2.1 Reader Fissi

Reader a montaggio fisso sono interrogatori montati in punti specifici attraverso i quali gli articoli con tag sono tenuti a passare. Trasportatori, porte di carico e punti vendita al dettaglio sono alcuni esempi di tali luoghi.

Qualsiasi elemento con tag, che passa attraverso la zona di interrogazione viene analizzato, cioè l'interrogatore legge le informazioni dal tag attaccato all'item. Il vantaggio di un interrogatore fisso è che i tag vengono letti (in altre parole, gli elementi vengono scansionati) automaticamente. Lo svantaggio di un interrogatore fisso è l'ambiente in cui opera. Particolari condizioni ambientali come temperatura, umidità, vibrazioni, e materiali come metalli possono inficiare la capacità di scansione del reader. È necessario prendere atto di tali condizioni, durante il montaggio di un interrogatore-per esempio, ponendo l'antenna lontano da metalli.

5.2.2 Handheld Reader

I reader palmari sono interrogatori portatili quindi contengono tutti gli elementi di base, inclusi l'antenna e il software applicativo, in un unico device. Le informazioni raccolte dai tag vengono memorizzate nel reader e successivamente trasferite in un sistema di elaborazione dei dati, se l'applicazione lo richiede.

Interrogatori palmari offrono la massima flessibilità. Un utente può portare l'interrogatore vicino all'elemento taggato e raccogliere le informazioni. questi interrogatori sono progettati con un campo vicino di lettura/scrittura. La portata di lettura di un interrogatore palmare è inferiore a quella di un interrogatore fisso. Questi reader possono essere utilizzati per applicazioni quali il monitoraggio e la scansione di oggetti in ambito medico, negli uffici, e nella vendita al dettaglio.

5.3 Operare in ambienti ad alta densità

Interrogatori e tag sono due elementi principali di un sistema RFID. Quando un sistema contiene più tag e interrogatori può sorgere una condizione chiamata ambiente denso.
Ci sono due tipi di ambienti ad alta densità:

- **Dense Reader** in cui più interrogatori operano in stretta vicinanza l'uno all'altro.
- **Dense Tag** in cui più tag sono nella zona d'interrogazione in modo che più di un tag può ottenere lo stesso segnale dall'interrogatore.

Ambienti densi possono ostacolare le prestazioni del sistema RFID attraverso effetti come le collisioni.

5.4 Collisioni

5.4.1 Collisioni tra interrogatori

Queste collisioni occorrono in ambienti in cui operano due o più reader dove la zona di lettura di uno si sovrappone a quella dell'altro.
In generale possono verificarsi due tipi di problema:

- **Letture Multiple** Sue reader le cui zone di lettura si sovrappongono, possono leggere lo stesso tag. In base all'applicazione, queste letture duplicate possono causare problemi. Come analogia, si pensi di contare qualcosa più volte quando si suppone sia contata una sola volta. Una delle soluzioni a questo problema è di programmare il sistema RFID in modo che un tag con un dato ID univoco sia letto una sola volta.
- **Interferenza del Segnale** Quando le zone d'interrogazione di due lettori si sovrappongono i segnali dei due reader che attraversano la zona possono collidere l'uno con l'altro. Una delle soluzioni a questo problema è che i lettori utilizzino la tecnica TDMA eseguendo le letture in tempi frazionati diversi, riducendo così la probabilità di collisioni.

5.4.2 Collisioni tra tag

Le collisioni tra tag occorrono quando due o più tag cercano di rispondere contemporaneamente alla richiesta d'informazioni da parte di uno stesso lettore. Le risposte multiple potrebbero confondere l'interrogatore rendendolo incapace d'identificare uno dei tag e di conseguenza l'oggetto a essi collegato.

Oltretutto in un ambiente denso di tag può verificarsi un effetto di shadowing in cui un elemento etichettato oscura il segnale di un medesimo tag nascosto dietro ad esso. Per ovviare a questi problemi sono stati così introdotti del protocollo anticollisione.

5.4.3 Protocolli di anticollisione

La soluzione al problema delle collisioni risiede appunto nei protocolli di anticollisione che possono essere suddivisi in due categorie: aloha-based e tree-based.

5.4.3.1 Protocolli Aloha-Based

L'obiettivo fondamentale è quello di leggere un solo tag alla volta. Per far ciò sono usati i due schemi seguenti:

- **Time-slotted Aloha.** In questo schema, un interrogatore mantiene l'invio periodico di una richiesta di ID. Un tale interrogatore è chiamato un faro. Quando un'etichetta riceve la richiesta, seleziona in modo casuale uno slot in cui risponde con il suo ID. Se l'interrogante riconosce l'ID, inizia la comunicazione col tag per ottenere le informazioni richieste. Terminata la comunicazione con quel tag, ricomincia l'invio di comandi di richiesta a cui un altro tag può rispondere, e così via. Se due o più tag ottengono lo stesso comando di richiesta dall'interrogatore, la speranza è che l'algoritmo di selezione casuale generi diverse fasce orarie per le loro risposte, evitando così la collisione. Da notare la possibilità che i due tag possano scegliere (a caso) la stessa fascia oraria. In questo caso ci sarà una collisione. Quindi, quest'approccio riduce le collisioni, ma non le elimina.
- **Frame-slotted Aloha**. Questo schema è un'estensione precedente dove al posto della scelta casuale del tempo di slot viene selezionato uno specifico slot all'interno di un frame nel quale il tag può rispondere. Si riducono così ulteriormente le collisioni.

I protocolli aloah-based riducono, ma non eliminano il problemi di collisione. Inoltre può verificarsi una situazione detta "starvation" in cui il tag rimane silente per lungo tempo a causa di altri tag che ciclicamente "rubano" slot validi per la trasmissione.

5.4.3.2 Protocolli Tree-based

Questo tipo di protocolli offrono una soluzione al problema della starvation. Si utilizza un algoritmo che divide il gruppo di etichette in collisione in due sottogruppi

iterativamente fino a quando il lettore riconosce gli ID dei tag senza collisioni. Questo può essere fatto in due modi diversi:

- **Binary Decision Tree**. Per supportare il protocollo, i tag devono poter gestire un contatore e implementare un generatore di numeri casuali. I tag che collidono sono ripartiti secondo un numero selezionato in modo casuale. I tag che selezionano 0 trasmettono il loro ID all'interrogatore. Se più tags selezionano 0 e quindi rispondono, l'interrogatore continua a camminare lungo l'albero fino a quando risponde solo un tag. Quando ciò accade, l'interrogatore stabilisce la comunicazione con quel tag per ottenere le informazioni richieste.
- **Query Tree.** Il protocollo utilizza un algoritmo, in cui il reader invia una query con un prefisso e le etichette che hanno l'ID che combina con il prefisso rispondono.

I protocolli basati su alberi risolvono il problema della starvation, ma possono creare ritardi identificativi lunghi. Quindi, l'obiettivo fondante di tutti i protocolli di anticollisione è selezionare solo tag in un momento in cui il lettore può comunicare.

6 Standard RFId

La standardizzazione dei suoi prodotti è una delle questioni più importanti che ogni settore emergente deve affrontare. Di seguito sono riportati i vantaggi di avere standard di settore:

1. Dato che tutti i fornitori seguono lo stesso standard per la fabbricazione di dispositivi, norme tecniche garantiscono l'interoperabilità dei dispositivi. Questo avvantaggia il consumatore e consente ai fornitori di sviluppare una sana competizione. [6]
2. Poiché gli organismi di normazione non servono gli interessi di un solo fornitore, gli standard generalmente definiscono la piattaforma più efficiente su cui un settore può operare e progredire. [6]
3. Gli standard generalmente riducono i costi e la facilità d'implementazione. [6]
4. Gli Standard sviluppano la fiducia dei consumatori nella tecnologia. Diverse organizzazioni sono state coinvolte nello sviluppo di standard per la tecnologia RFID, l'ISO ed EPCglobal sono le due prominenti. [6]

6.1 Standard ISO

L'ISO è un organismo internazionale composto di rappresentanti di organismi nazionali di normalizzazione. Fondata il 23 febbraio 1947, quest'organizzazione definisce gli standard in tutto il mondo industriale e commerciale, che vengono comunemente chiamati gli standard ISO.

I primi standard RFID realizzati per TAG passivi a bassa frequenza e comprendono:

1. Gli standard sui TAG per identificazione degli animali
    - **ISO 11784** Radio frequency identification of animals - Code structure.
    - **ISO 11785** Radio frequency identification of animals - Technical concept
2. Protocolli per l'interfaccia radio per TAG RFID usati nei sistemi di pagamento, smart cards senza contatti e carte di prossimità:
    - **ISO/IEC 10536** Close-Coupling Smart Cards.
    - **ISO/IEC 14443** Proximity-Coupling Smart Cards.

- **ISO/IEC 15693** Vicinity-Coupling Smart Cards.

3. Metodi per il test e la conformità di TAG e Reader RFID a uno standard (ISO/IEC 18047).
4. Metodi per il test delle prestazioni di TAG e Reader RFID (ISO/IEC 18046).

6.2 Standard EPCglobal

L'Auto-ID Center presso il Massachusetts Institute of Technology (MIT), lavorando in collaborazione con i leader del settore e le istituzioni accademiche di tutto il mondo, ha progettato un sistema per portare i benefici della tecnologia RFID per la supply chain globale. Questo sistema comprende l'Electronic Product Code (EPC), la tecnologia RFID, e il software di supporto basato su standard EPCglobal, e viene indicato come rete EPCglobal. . La rete comprende elementi come EPC, il sistema d'identificazione per i tag EPC e lettori, e Object Name Service (ONS) La rete EPCglobal fornisce le seguenti cinque principali servizi:

- Assegnazione di numeri di identificazione univoci agli elementi che consentano loro di essere identificati. I numeri EPC consentono il monitoraggio a livello di elemento.
- Rilevamento e identificazione degli articoli. Tag EPC e lettori lo rendono possibile.
- La raccolta e filtraggio dei dati. L'EPC Middleware fornisce servizi che facilitano lo scambio di dati tra i lettori dell'EPC e sistemi informativi aziendali, come i database. Solo i dati sugli eventi d'interesse saranno memorizzati.
- Esecuzione di query e archiviazione dei dati. Questo servizio consente diverse applicazioni aziendali in esecuzione in luoghi diversi per lo scambio e la condivisione data. Questo significa che i partner commerciali possono interrogare e scambiare dati tra di loro.
- Individuazione d' informazioni. Si tratta di un servizio di discovery per individuare i repository per i dati EPC richiesti.

EPC è una famiglia di schemi di codifica per Gen 2 tag. È progettato per soddisfare le esigenze dei vari settori, mentre allo stesso tempo garantisce l'unicità di tutti i tag EPC-compatibili, chiamato tag EPC. Schemi di codifica contengono un numero di serie, chiamato numero EPC, che può essere utilizzato per identificare univocamente un

oggetto .L'EPC è un numero strutturato, composto da più campi, come mostrato nella Tabella 6-1.

Nome Campo	Descrizione	Esempio
Header	Identifica lunghezza, tipo, struttura versione e generazione di EPC	015
EPC Manager	Identifica la compagnia	35000
Object class	Indentifica il prodotto	213761
Serial number	Indentifica lo specifico item del dato prodotto	210000000

Tabella 6-1 Campi di un numero EPC

EPCglobal Network-compliant sotware e hardware utilizzeranno i protocolli di dati standard EPCglobal e quindi useranno numeri EPC Manager. Quindi i numeri EPC Manager emessi da EPCglobal sono necessari se le aziende si impegneranno con i partner commerciali al di fuori le loro operazioni interne.

Un esempio di un numero EPC è mostrato in Figura 5.1. Campi aggiuntivi possono essere utilizzati anche come parte del numero di EPC per codificare e decifrare correttamente le informazioni da sistemi di numerazione diversi nelle loro native forme.

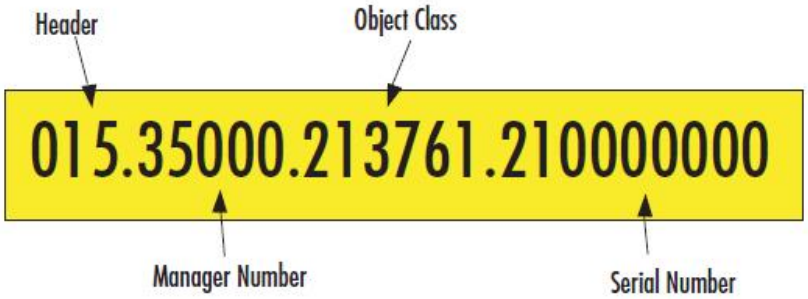

Figura 6.1 Struttura di un numero EPC [6].

6.3 Near-Field Communication

A prima vista, NFC non è un sistema RFID, ma un interfaccia dati wireless tra dispositivi, simile al Bluetooth. Tuttavia, NFC ha diverse caratteristiche che sono di interesse in relazione ai sistemi RFID.

La trasmissione di dati tra due interfacce NFC utilizza campi magnetici ad alta frequenza alternati nel gamma di frequenze 13,56 MHz. Il raggio di comunicazione tipico per la trasmissione dei dati NFC è di 20 cm perché la rispettiva controparte di comunicazione si trova nel campo vicino dell'antenna trasmittente; quindi la comunicazione viene detta in campo vicino (near-field) [5].

L'interfaccia NFC ha un trasmettitore 13,56 MHz e un ricevitore 13,56 MHz che vengono alternativamente collegati all'antenna. L'antenna è progettata come una bobina di grande superficie o spira.

Per la comunicazione tra due interfacce NFC, la singola interfaccia può assumere diverse funzioni, ossia quella di un iniziatore NFC (master) o di un obiettivo NFC (slave).

La comunicazione è sempre avviata dal master NFC. Inoltre, la comunicazione NFC distingue tra due diverse modalità operative, l'attivo e la modalità passiva.

6.3.1 Modalità Attiva

Per trasmettere i dati tra due interfacce NFC in modalità attiva una delle interfacce NFC attiva il suo trasmettitore e funziona quindi come l'iniziatore NFC. La corrente ad alta frequenza che scorre nell'antenna induce un campo magnetico alternato il quale si diffonde intorno all'anello antenna. Parte del campo magnetico indotto scorre attraverso il loop dell'antenna dell'altra interfaccia NFC che si trova nelle vicinanze. Poi una tensione U è indotta nel loop dell'antenna e può essere rilevata dal ricevitore dell'altra interfaccia NFC. Se l'interfaccia NFC riceve i segnali e i corrispondenti comandi di un iniziatore NFC, questa interfaccia NFC adotta automaticamente il ruolo di un bersaglio NFC. Per la trasmissione dei dati tra le interfacce NFC, l'ampiezza del campo magnetico alternato emessa è modulata (modulazione ASK), simile alla trasmissione di dati tra lettore RFID e tag.

Tuttavia, la differenza tra un target NFC in modalità attiva e un RFID transponder consiste nel fatto che il campo magnetico alternato deve alimentare il transponder con

energia tale per azionare il microchip. In contrasto con ciò, il dispositivo elettronico contenente l'interfaccia NFC fornisce energia all'interfaccia stessa.

La direzione di trasmissione è invertita per inviare dati dal target NFC al master NFC. Ciò significa che il target NFC attiva il trasmettitore e l'iniziatore NFC passa in modalità di ricezione. Entrambe le interfacce NFC alternativamente inducono campi magnetici in cui i dati sono trasmessi solo dal trasmettitore al ricevitore.

6.3.2 Modalità Passiva

Anche nella modalità passiva, l'iniziatore NFC induce un campo magnetico alternato per trasmettere dati al target NFC . L'ampiezza del campo è modulato tramite modulazione ASK. Tuttavia, dopo aver trasmesso un blocco di dati , il campo non viene interrotto , ma continua ad essere emesso in modo non modulato . Il target NFC è ora in grado di trasmettere dati al master NFC generando una modulazione di carico . Il metodo di modulazione carico è noto anche dai sistemi RFID .

Usando questo metodo per interfacce NFC offre una serie di vantaggi e opzioni interessanti ad uso prati . Così i diversi ruoli delle due interfacce NFC all'interno della comunicazione possono essere negoziate e modificate in qualsiasi momento. Un'interfaccia NFC con alimentazione debole, ad esempio con una batteria a bassa capacità , in grado di negoziare e adottare il ruolo di target NFC al fine di risparmiare energia mediante la trasmissione di dati tramite la modulazione del carico.

L'interfaccia NFC target è anche in grado di stabilire , in aggiunta ad altre interfacce NFC, la comunicazione verso transponder passivi compatibili (ad esempio secondo la norma ISO / IEC 14443) che il target alimenta e che , attraverso la modulazione del carico, può trasmettere i dati per l'interfaccia NFC. Questa opzione consente a dispositivi elettronici dotati di interfacce NFC , come ad esempio i telefoni cellulari NFC , di leggere e scrivere su diversi transponder , come le etichette intelligenti o tickets. L'interfaccia NFC in questo caso si comporta come un lettore RFID , questa opzione è denominata anche " modo lettore "

Se un'interfaccia NFC è situa vicino a un lettore RFID compatibile il lettore NFC è anche in grado di comunicare con un lettore. Qui, l'interfaccia NFC adotta il ruolo di un target NFC e può trasmettere dati al lettore con modulazione di carico. Questa possibilità consente a lettori RFID di scambiare dati con un dispositivo elettronico con interfaccia NFC come ad esempio i telefoni cellulari NFC . Dal punto di vista del

lettore, il dispositivo elettronico si comporta come una smart card contactless, questa opzione è anche chiamata "modalità card".

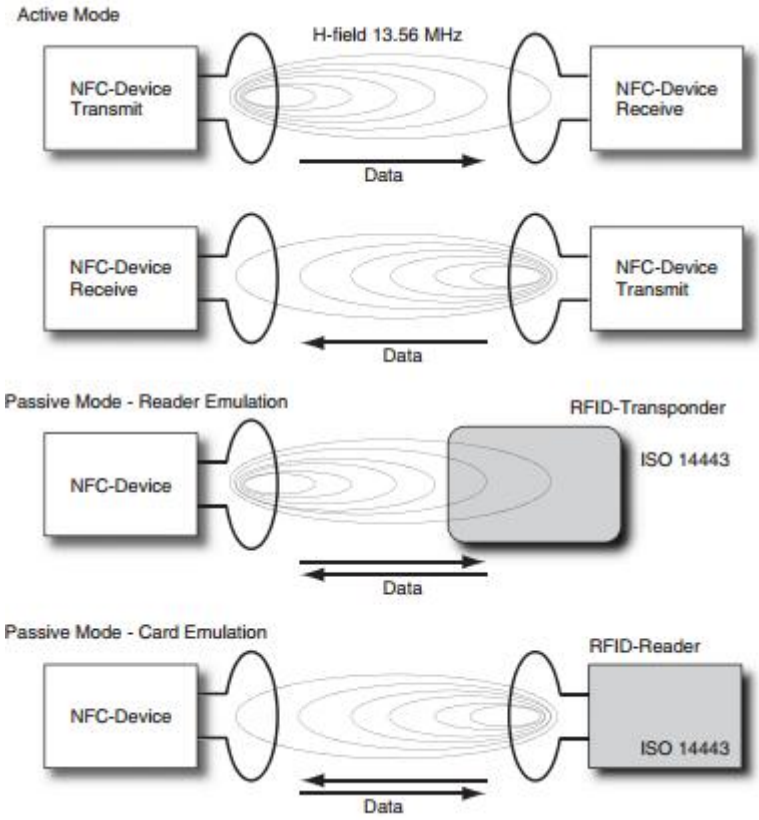

Figura 6.2 Modalità di un dispositivo NFC

7 Middleware RFId

7.1 Motivazioni

Ci sono tre motivazioni principali dietro l'uso di un Middleware RFID:

1. Incapsulare le applicazioni dalle interfacce dei dispositivi.
2. Elaborare le informazioni grezze catturate da lettori e sensori in modo che le applicazioni vedano solo gli eventi rilevanti, ad alto livello, riducendo così il volume d'informazioni da elaborare.
3. Fornire un'interfaccia a livello di applicazione per la gestione dei reader e l'interrogazione delle informazioni.

La maggior parte dei Middleware RFID disponibili oggi fornisce queste funzionalità. La Figura 7.1 mostra gli elementi principali del Middleware RFID.

Figura 7.1 Elementi di un Middleware RFId.

7.1.1 Reader Interface

Consideriamo come le applicazioni possano interfacciarsi con i reader e altri sensori dell'infrastruttura fisica. Una possibilità è di avere ogni applicazione legata alla specifica API di ciascun lettore. Questo però può funzionare solo per scenari banali dato che una tipica impresa è obbligata ad usare un mezza dozzina di lettori diversi [3]. La maggior parte delle aziende trarrebbe vantaggio lasciando che siano i fornitori di software specializzati a tenere il passo con le API e scrivere driver personalizzati o interfacce reader. Una reader interface fornisce i mezzi per eliminare i capricci dei diversi lettori ed esporre un'unica interfaccia astratta per le applicazioni.

7.1.2 Filtraggio eventi

Un tipico distributore RFID-enabled o rivenditore con diversi di negozi avrà centinaia, se non migliaia di lettori. Questo può portare a milioni di letture RFId al secondo. Esponendo informazioni grezze da parte dei lettori e sensori ad applicazioni aziendali sarebbe simile a cercare di bere acqua con un idrante. Oltre al volume di dati, le

informazioni grezze necessitano di ulteriore elaborazione per essere significative per le applicazioni aziendali. Data la fisica delle comunicazioni a radio frequenza, le attuali tecnologie producono tassi di lettura che potrebbe essere 80-99 % accurate in ambienti commerciali [3]. Questo significa che se ci fossero 100 tag vicino a un lettore, sarebbero probabilmente registrate tra 80 e 99 etichette per ogni ciclo di lettura. Dato che i tassi di lettura non sono al 100 % accurati, un elemento che viene rilevato in un ciclo di lettura potrebbe essere perso durante il prossimo. Consideriamo di avere un'applicazione smart shelf che si integra con il sistema di controllo del magazzino. Immaginiamo di passare ciascuna delle letture grezze dal sistema smart shelf al sistema d'inventario. Se così fosse, il sistema di controllo del magazzino, oltre ad essere impantanato dall'enorme volume di dati in entrata, si sarebbe dovuto adeguare continuamente alle osservazioni fluttuanti provenienti dai lettori di smart shelf.

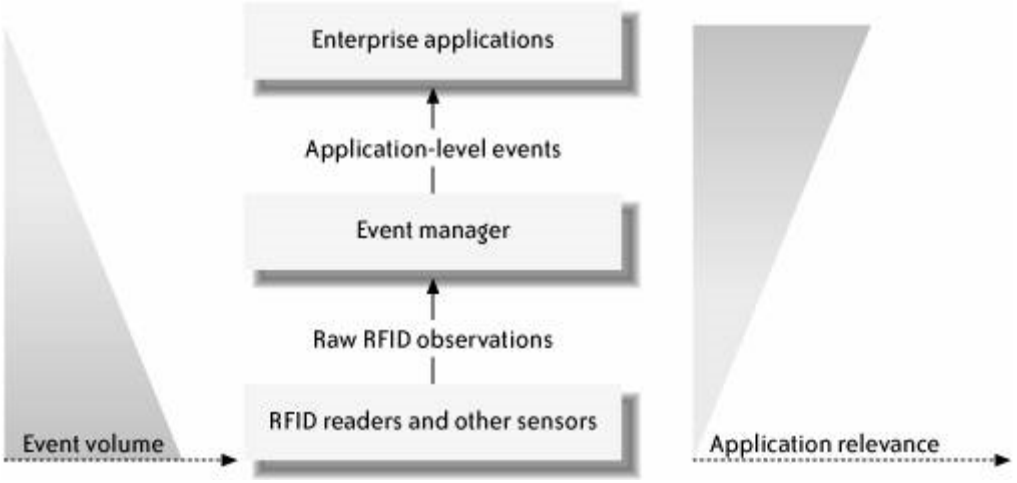

Figura 7.2 Volume eventi e rilevanza attraverso layer differenti di un sistema RFId

Come mostrato in Figura 7.2, le informazioni grezze provenienti da lettori RFID e sensori mancano del contesto a livello di applicazione. Più elaborazione deve essere fatta per mappare queste informazioni ad eventi più grossolani che sono significativi per le applicazioni. Ad esempio, un'applicazione di gestione degli ordini vorrebbe sapere quando l'inventario in-store per un elemento particolare scende sotto la soglia. Come si può immaginare, un sistema di gestione degli ordini non sarebbe minimamente interessato a sapere se i lettori RFID sono impiegati nel monitoraggio delle voci nei negozi, per non parlare di quanti lettori ci sono per ogni negozio e in che

configurazione. Esporre un sistema di gestione per ogni scansione di un lettore RFID senza alcun filtraggio a livello di applicazione sarebbe inutile e controproducente. Di conseguenza, vi è necessità di un Middleware che non può solo consolidare, aggregare e filtrare informazioni provenienti da lettori e sensori, ma che fornisca un contesto a livello di applicazione. Come si può vedere, questo richiede un po' di elaborazione delle informazioni RFID grezze prima di essere inviate alle applicazioni. Il processo di appianare le informazioni provenienti da lettori e sensori si chiama filtraggio eventi. Il componente che fornisce le funzioni di filtraggio evento viene chiamato il gestore eventi.

7.2 Architettura Logica

RFID e altre tecnologie di telerilevamento forniscono un livello di automazione che non era possibile in precedenza con tecnologie come codici a barre che necessitano dell'intervento umano. Tuttavia, questo livello di automazione richiede che i lettori e sensori siano monitorati e gestiti in remoto. Una soluzione Middleware che opera ai bordi è più adatta per il monitoraggio e la gestione dei dispositivi. Così, oltre alle funzioni sopra descritte, una soluzione Middleware RFID dovrebbe anche fornire, o almeno integrarsi con, un'interfaccia di gestione e monitoraggio.

Più dati e più transazioni significano un maggiore carico sulla rete, server e storage. Le applicazioni aziendali sono generalmente impiegate in centri dati, quindi esponendole direttamente alle letture RFID non solo sforzerà le applicazioni, ma introdurrà anche un ritardo di elaborazione. Pertanto, fatta eccezione per le applicazioni banali, è necessario pianificare l'utilizzo di un Middleware RFID tra le applicazioni e i dispositivi ai margini del sistema. Questo Middleware dovrebbe, come minimo, incapsulare le peculiarità dei tipi di lettori disponibili dalle applicazioni e permettere loro di concentrarsi su eventi, a livello di applicazione significativi senza essere bombardati da informazioni grezze collegate in parte ai lettori. Come accennato in precedenza, tale Middleware dovrebbe anche fornire monitoraggio remoto e funzionalità di gestione.

La Figura 7.3 mostra un modello concettuale di Middleware RFID. Il Middleware riceve informazioni grezze da una o più fonti di dati. Una sorgente di dati può essere qualsiasi sensore che raccoglie i dati dal mondo fisico, come un lettore RFID o un sensore di temperatura. Dopo aver ricevuto le informazioni da parte dei lettori, la

componente event-manager aggrega, trasforma, o filtra tali informazioni preparandole al consumo da parte delle applicazioni. Oltre a rendere le informazioni RFID più rilevanti per le applicazioni, l'Event Manager aiuta a ridurre il volume di dati che devono elaborare.

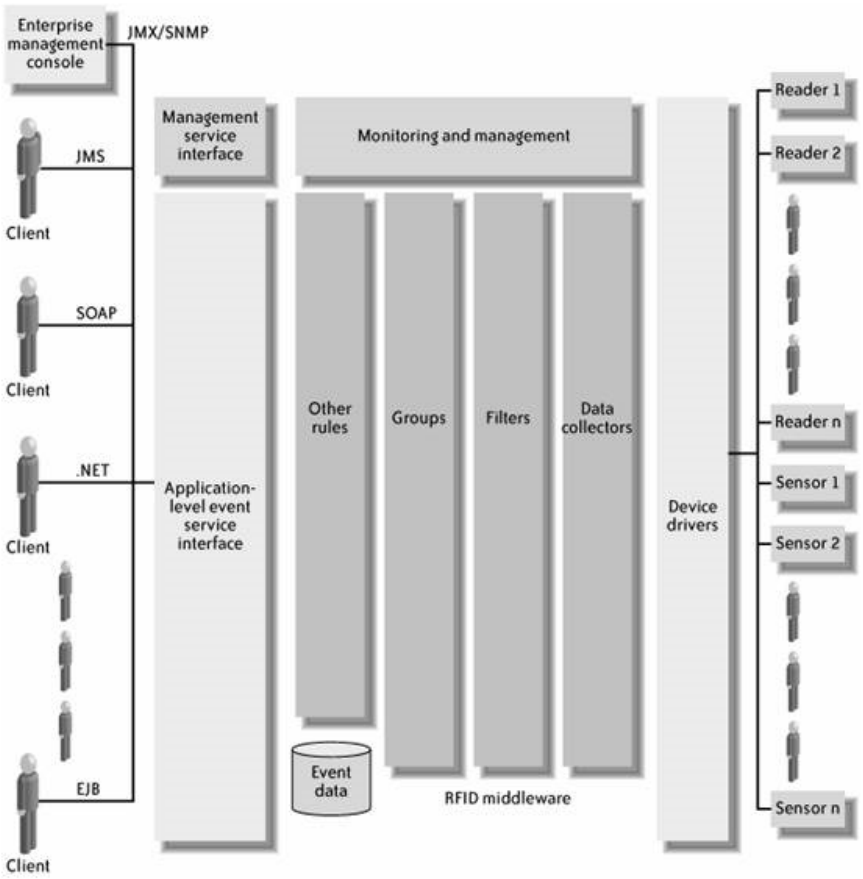

Figura 7.3 Architettura concettuale per un Middleware RFId [7]

Come mostrato nella Figura 7.3, un Middleware RFID è in grado di supportare: ricerca, provisioning, monitoraggio e gestione dei reader. Fornisce la raccolta dei dati, la traduzione, l'aggregazione, il filtraggio e meccanismi di raggruppamento; supporta interfacce service-oriented che utilizzano standard come Java, J2EE,. NET, e web service.

Esistono diverse implementazioni di questa architettura logica. I questa tesi si è stata proposta la più utilizzata cioè la specifica Application Level Events di EPCglobal. La specifica ALE definisce un'interfaccia lettore-neutro per la ricezione, filtraggio e raggruppamento di eventi da parte dei lettori RFID.

7.3 Application Level Events

La specifica ALE è lo standard d'interfaccia a livello di applicazione sviluppata da EPCglobal per consentire ai client di ottenere informazioni EPC filtrate e consolidate da una varietà di fonti. L'interfaccia ALE consente ai client di impostare i metodi di elaborazione degli eventi e richiedere eventi filtrati in forma di report. La specifica ALE fornisce un mezzo per spingere l'elaborazione data EPC più vicino alla fonte. Lo fa attraverso la definizione di un'interfaccia di servizio e di un modello di interazione tra client ALE e server ALE. Tuttavia, la specifica ALE non detta come l'interfaccia di servizio deve essere implementata o dove può essere distribuita. Per esempio, un servizio ALE può essere implementato da solo, su un lettore, o su un cluster di server di applicazioni. Fino a quando le esigenze specifiche dell'interfaccia ALE sono soddisfatte, il servizio sarà considerato "EPCglobal ALE specification-compliant".
I principali vantaggi della specifica ALE includono:

- **Standard per la gestione eventi** La specifica ALE fornisce un'interfaccia lettore-neutro per la ricezione, il filtraggio e raggruppamento eventi da lettori RFID. Le applicazioni che utilizzano il Middleware ALE-compliant non devono avere i driver di periferica per i singoli lettori e non devono utilizzare le loro interfacce di programmazione proprietarie.
- **Estensibilità**.
- **Separazione dell'interfaccia dall'implementazione** La specifica ALE fornisce un'interfaccia tra clienti e RFID Middleware, lasciando i dettagli d'implementazione per i venditori.

8 RFId Information Service

Una delle promesse di RFID è che i partner commerciali saranno in grado di raccogliere e condividere automaticamente informazioni di monitoraggio riguardante gli elementi della loro supply chain. Per la realizzazione, le aziende devono accordarsi su quali, quando e come queste informazioni saranno raccolte, dove e come verranno memorizzate, e, infine, dove e come accedervi.
Naturalmente, l'infrastruttura utilizzata per la condivisione di informazioni RFID deve anche fornire le funzionalità di sicurezza che ci si aspetta in architetture orientate ai servizi, come l'autenticazione e l'autorizzazione.
La standardizzazione rispetto alla struttura e al significato dei dati RFID, l'attuazione di meccanismi che raccolgono e condividono informazioni di interesse reciproco, sono in grado di ridurre il time to market e il costo della condivisione delle informazioni per i partecipanti di una filiera [3].

8.1 L'EPCglobal Network

EPCglobal prevede una rete di servizi di dati EPC-enabled che è utilizzata dai partner commerciali per consentire le informazioni di monitoraggio real-time su articoli nelle loro catene di approvvigionamento e prende il nome di EPCglobal network. L'EPCglobal Network introduce alcuni componenti dedicati, come ad esempio il Naming Service Object (ONS) e gli EPC Information Services (EPCIS).
L'EPCglobal Network si propone di fornire dati in tempo reale sulle singole voci, mentre si muovono attraverso una catena di fornitura globale. Centrato intorno alla tecnologia RFID EPC e, e sulla base dell'infrastruttura Internet esistente, la rete EPCglobal offre il potenziale per una maggiore efficienza e precisione nel monitoraggio di prodotti tra partner commerciali.
L'EPCglobal Network si compone di cinque servizi principali:

1. **Assegnazione d'identità uniche**. Il tracking degli item non è possibile senza la capacità di identificarli univocamente. Qui è dove l'Electronic Product Code entra in gioco.

2. **Individuare e identificare gli elementi.** Il sistema d'identificazione è costituito da tag EPC e lettori. L'EPC fornisce uno schema di codifica per i tag RFID in modo da identificare i produttori di un articolo, categoria di prodotto e il numero di serie univoco. Il tag è applicato a un oggetto, sia durante il processo di fabbricazione o da qualche parte lungo la catena di approvvigionamento.
3. **Raccolta e filtraggio eventi.** Il Middleware EPC fornisce le specifiche per i servizi che permettono lo scambio di dati tra i lettori dell'EPC e dei sistemi informativi aziendali.
4. **Archiviazione e l'interrogazione eventi.** L'EPC Information Service consente agli utenti di scambiare dati EPC con i partner commerciali. La specifica EPCIS si propone di fornire gli standard per la cattura e l'interrogazione dei dati EPC.
5. **Individuazione d'informazioni EPC.** Per consentire ai partner commerciali di condividere le osservazioni EPC, è necessario fornire servizi di ricerca in grado di individuare i repository per i dati EPC richiesti. L'ONS, come specificato ora, è essenzialmente un servizio di ricerca EPC.

Figura 8.1 illustra la rete EPCglobal. Come si vede, i lettori RFID raccolgono informazioni su oggetti con etichetta RFID mentre si muovono attraverso la catena di approvvigionamento.

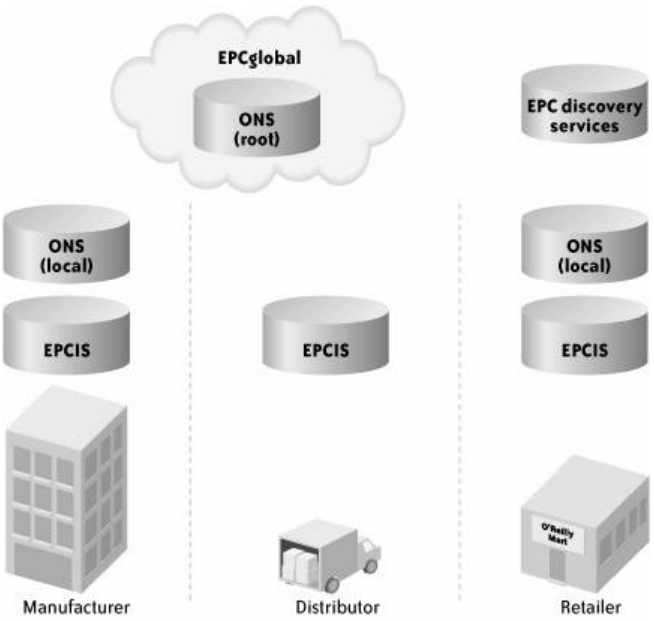

Figura 8.1 EPCglobal Network

I lettori passano queste osservazioni al Middleware RFID dopo qualche filtraggio rudimentale. Il Middleware RFID riceve i dati dai lettori filtrandoli e raggruppandoli secondo le necessità delle applicazioni a valle. L'event manager aggiunge informazioni sulla posizione alle osservazioni filtrate. Secondo la concezione EPCglobal,network le informazioni filtrate (o eventi) dai gestori di eventi sono poi passate a un server EPCIS locale. Il server EPCIS registra le osservazioni EPC per un uso successivo. L Object Naming Server mantiene una mappatura tra EPC e i server EPCIS che conservano le informazioni su di loro. Proprio come il DNS opera per gli indirizzi IP, l'ONS funziona in modo gerarchico per fornire un servizio di ricerca globale.

Allo stesso modo, altri partner commerciali in un negozio della catena di fornitura memorizzano informazioni EPC sul loro server EPCIS locale. Un EPC però identifica solo un'entità. Altre informazioni su un tipo di prodotto, il produttore, e così via non fanno parte dell'EPC. Quando un'applicazione ha bisogno di conoscere la sorte di un particolare EPC o ha bisogno di altre informazioni su un EPC, interrogherà un server ONS locale. Se un server EPCIS locale è in grado di fornire le informazioni necessarie, l'ONS ritorneranno informazioni sulla sua ubicazione (indirizzo IP e la porta). In caso contrario, utilizzerà la gerarchia globale di ONS per individuare un server EPCIS che le può fornire.

Occorre ricordare che, al momento della scrittura, la rete EPCglobal è una visione. Sviluppare servizi dati sicuri, scalabili e affidabili non è banale. Mettere un accordo commerciale in essere, avendo i componenti di sicurezza necessarie, sviluppando i mezzi per autenticare i partner commerciali, e limitando l'accesso di un richiedente per solo le informazioni che è autorizzato è un processo complicato.

9 Sicurezza nei Sistemi RFId

9.1 Zone di Sicurezza

Come con qualsiasi sistema distribuito, per definire una strategia di sicurezza per i sistemi RFID, cominciamo trattando tutte le richieste di accesso come se fossero provenienti da potenziali agenti di minaccia. Figura 9.1 mostra uno schema di come un tipico sistema RFID può essere suddiviso in zone di sicurezza distinte.

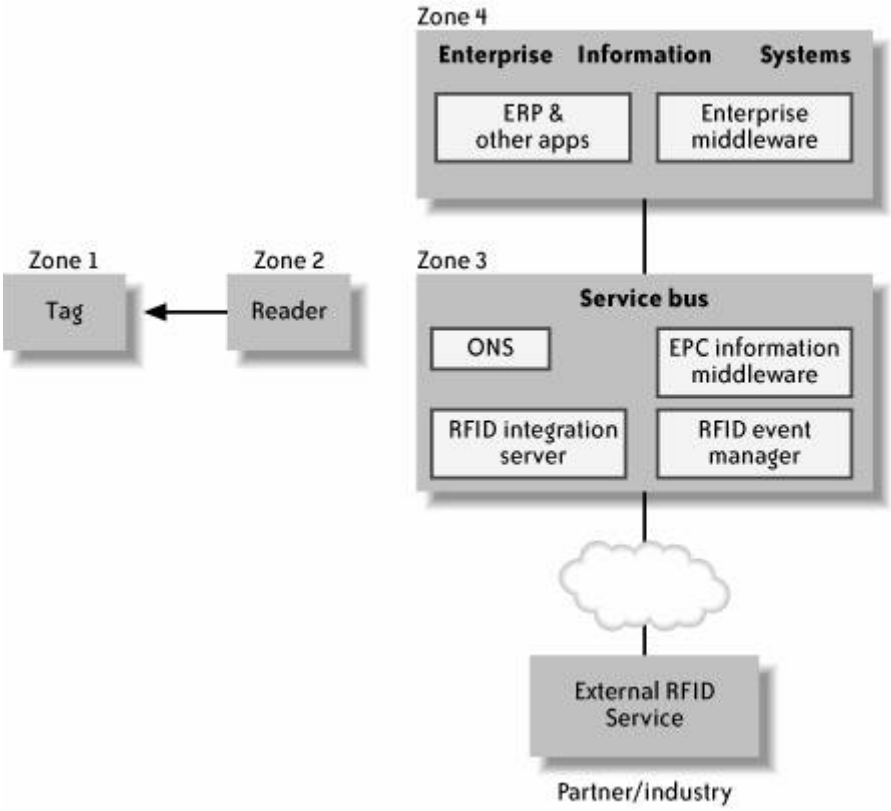

Figura 9.1 Zone di Sicurezza nei Sistemi RFId [8]

Ogni zona assume una certa dose di fiducia per i componenti al suo interno e diffidenza per eventuali outsider. Partendo dal basso a sinistra, si può vedere che tag e lettori comunicano tramite onde radio. Il lettore si collega al RFID service bus, che contiene uno o più dei seguenti elementi: EPC event manager, server ONS, server EPCIS e server d'integrazione RFId. Il server d'integrazione RFID si connette ad altri sistemi informativi aziendali, sia a livello d'infrastruttura (ad esempio Directory, Identity

Management, ecc.) che a livello di applicazione (come un Enterprise Resource Planning o ERP). Il server d'integrazione RFID si collega anche a fornitori di servizi RFID esterni, come ONS di un settore e server EPCIS o server di integrazione RFID di un partner.

9.2 Zona 1 : Tag

9.2.1 Vulnerabilità

Ci sono tipicamente due aree di vulnerabilità:

- I dati sul tag sono memorizzati in chiaro. L'aggiunta di crittografia per i tag richiede spazio aggiuntivo e circuiti sui chip RF. Questo significa costi aggiuntivi [8] (in un ambiente di vendita al dettaglio / della catena di fornitura che è molto attenta ai costi).
- Senza la supervisione fisica, chiunque nei locali con accesso al tag può rimuovere o scambiare un tag con un altro.

9.2.2 Agenti di Minaccia

Gli Agenti di minaccia comprendono chiunque abbia accesso fisico ai tag e la necessità, capacità e voglia di studiare ed eventualmente modificare il loro contenuto.
Gli scenari di alcune minacce possono essere i seguenti:

- Qualcuno con accesso fisico ad un tag è in grado di leggerne i contenuti attraverso l'analisi in un ambiente di laboratorio, utilizzando sonde, radiografie, e simili. Si noti che, essendo necessari sia l'accesso fisico ai tag che un ambiente di laboratorio di tipo controllato, attacchi come questi sono difficili da realizzare su scala massiccia. Inoltre, la minaccia di snooping non riguarda unicamente i sistemi RFID. I barcode ad esempio hanno etichette "Human-Readable" quindi il loro contenuto può essere facilmente determinato. La minaccia maggiore, nei sistemi RFId, deriva dalle loro informazioni di monitoraggio. La minaccia diventa grave se qualcuno ottiene un codice EPC e lo usa per interrogare un server EPCIS per i dati di monitoraggio associato al codice.
- Un agente può simulare un tag valido (ad esempio, forzando una lettura mentre il prodotto non è presente / rubato) o scambiare un tag RFID a un elemento più costoso con uno di basso prezzo. Anche questo tipo di minaccia non avviene

unicamente nei sistemi RFId. Risulta altrettanto facile, se non più facile, fare lo stesso scambio con le etichette di codici a barre. La differenza è che i codici a barre richiedono una scansione supervisionata, il che significa che tale cambiamento ha più probabilità di essere rilevato.

- Qualcuno con accesso a un magazzino può rubare una cassa e attaccare il tag RF su un altra. Questa cassa restante ora avrà due tag e può essere identificata dai lettori come due casse distinte. Dato che i sistemi RFID si basano su processi automatizzati (possibilmente senza inventario umano), il furto può passare inosservato per qualche tempo e sarà difficile individuare quando e dove si è verificato.
- Possono verificarsi modifiche non autorizzate delle informazioni memorizzate su un tag RFID riscrivibile.

9.2.3 Contromisure

Per i problemi appena elencati ci sono diverse contromisure che possono essere adottate:

- Fornire un adeguato controllo di accesso per i locali fisici.
- Implementare sorveglianza della merce taggata.
- Richiedere un controllo accessi rigoroso alle informazioni ricavabili da un EPC.
- Separare il codice EPC da ogni informazione che è sensibile alla società o ai consumatori, introducendo un ulteriore livello d'informazione che dovrebbe essere violato in modo da utilizzare il codice EPC.
- Utilizzando tag riscrivibili soli se necessari e con un adeguato controllo d'accesso (fisico crittografico).

9.3 Zona 2: RFId Reader

Lettori RFID sono normalmente collegati ad una rete interna Ethernet utilizzando connessioni sia cablate o wireless.

Generalmente sono soggetti alle seguenti vulnerabilità:

- Traffico dati non criptato tra tag e reader.
- Non è possibile autenticare i tag.

9.3.1 Vulnerabilità

Le vulnerabilità derivanti comprendono lo spoofing, attacchi DoS e attacchi di protocollo.

9.3.2 Agenti di Minaccia

Gli agenti di minaccia comprendono chiunque sia collegato alla stessa rete (come ogni nodo collegato a una rete, un lettore è aperto a tutti gli agenti di minacce di rete), e qualcuno con un dispositivo wireless sniffer e la conoscenza del protocolli lettore.
Le possibili minacce possono essere le seguenti:

- Se un lettore è connesso a una rete wireless, è vulnerabile a un nodo maligno che è in grado di accedere al punto di accesso wireless. Sia lettori via cavo sia wireless sono vulnerabili ad attacchi basati sulla rete. La minaccia di rete più probabile è un attacco DOS.
- Qualcuno con uno sniffer RF e una comprensione adeguata dei protocolli potrebbe controllare la comunicazione tra reader e tag spiando i movimenti di magazzino. La comunicazione dal lettore al tag RFID si chiama "canale di andata", mentre l'eco di ritorno dal tag RFID per il lettore è chiamato "canale di ritorno". In generale, il canale in andata usa molta più potenza e ha un raggio più lungo (fino a 10 m) rispetto al canale inverso (circa 3 metri). Qualcuno potrebbe monitorare il canale in avanti più facilmente del canale inverso.
- Un attacco DoS può verificarsi quando un intruso disturba la comunicazione tag reader con un rumore casuale.
- Un tag bloccante universale può essere utilizzato anche per lanciare un attacco DoS.
- Con l'identificazione delle persone in base agli oggetti da essi trasportati, qualcuno è in grado di monitorare la sorte di tali individui. Quando questa informazione è legata ad altri item mappati alle varie posizioni, il curiosare può costruire un profilo molto dettagliato delle abitudini di acquisto, la salute e lo stile di vita degli individui tracciati.

9.3.3 Contromisure

Possono essere adottate le seguenti contromisure:

- Implementare un accesso alla rete adeguato, usando firewall, intrusion detection systems, network sniffers, ed altro. Meccanismi di controllo degli accessi fisici possono essere messi in atto per limitare l'accesso ai locali.
- EPCglobal ha un gruppo di lavoro sulla sicurezza (parte del Gruppo di Azione Software), co-presieduta da VeriSign e ConnecTerra [7], che sta lavorando sulle specifiche per le comunicazioni EPCIS sicure.
- EPCglobal sta lavorando su una infrastruttura di sicurezza che definirà quali network partecipanti verranno autenticati. Questo molto probabilmente comporterà il concetto diffuso di certificati digitali rilasciati da un'autorità attendibile. Inoltre, l'ONS è una directory "autorevole" di servizi di informazione che possono essere consultati per garantire che una query EPCIS proviene da una fonte attendibile. [8]

9.4 Zona 4: Sistemi Informativi Aziendali

I sistemi informativi aziendali comprendono sistemi aziendali quali directory, gestione delle identità, controllo degli accessi e sistemi di messaggistica, così come tutti i sistemi di back-end che saranno i "consumatori" di dati RFID. Sistemi back-end includono i sistemi ERP.

9.4.1 Vulnerabilità

I volumi delle transazioni e dei dati che i sistemi RFID richiedono possono sopraffare l'infrastruttura di rete esistente. Le aziende corrono il rischio di dover memorizzare un largo numero informazioni impreviste o potenzialmente sensibili.

9.4.2 Agenti di Minaccia

Gli agenti di minaccia possono essere spie aziendali od intrusi. Alcune esempi di minacce possono essere:

- La gestione individuale degli elementi potrebbe portare all'acquisizione di informazioni più preziose di quello che l'infrastruttura di stoccaggio è progettata per proteggere. Le informazioni in un sistema potrebbero essere utili per tracciare individui se collegate ad informazioni in altri sistemi. Gli intrusi

possono valutare queste informazioni più di quanto una società si renda conto sotto investendo nella sicurezza a causa di questa percezione errata.

- I sistemi informativi aziendali sono più suscettibili ad essere esposti a volumi di dati molto più alti con i sistemi RFId che con i sistemi a codici a barre.

Conclusioni

Dopo aver analizzato nei vari capitoli della tesi gli aspetti fondanti dell'RFId è bene concludere con un'analisi sulle criticità e opportunità per lo sviluppo di questa tecnologia.

Il mercato attualmente si trova a dover affrontare una serie di problematiche che anche se potrebbero essere risolte in futuro attraverso lo sviluppo tecnologico, oggi rappresentano ancora un freno all'introduzione su vasta scala dell'Rfid.

Uno dei primi problemi è la compatibilità a livello mondiale, dovuta alla non uniformità di frequenze operative e potenze di trasmissione. Un'ulteriore criticità è rappresentata dalla difficoltà per le aziende di allestire l'applicazione, e questo per mancanza di offerta di sistemi pronti all'uso e degli alti costi del software.

Attualmente, inoltre, sono considerate ancora modeste le prestazioni di tag e reader rispetto alle specifiche o alle aspettative dell'applicazione: infatti è ancora scarsa la distanza operativa, mentre è più elevata la possibilità di fallimenti nelle operazioni di lettura. I tag, inoltre, hanno ancora dei limiti di applicabilità su alcune forme di prodotti o tipologie di merci.

Fermo restando che tutte queste osservazioni siano valide, uno dei problemi dell'Rfid è anche quello di dimostrare il reale valore aggiunto che porta, e che quindi ne giustifichi l'investimento, specie se si confronta con tecnologie ormai consolidate come i codici a barre.

A parte gli esempi di chi vanta indiscutibili vantaggi con l'utilizzo di questa tecnologia, forse la via migliore per approcciarla potrebbe essere quella di non puntare al contesto aziendale per l'introduzione dell'RFId, ma, come accaduto per i codici a barre, coinvolgere nel processo tutta la catena distributiva, ripartendo i costi e condividendo i benefici tra tutti gli attori. Così facendo, l'attenzione non sarebbe concentrata sulle prestazioni di tag e reader, quanto sulla funzionalità di sistemi di gestione e middleware e, soprattutto, sulla loro accessibilità da parte di tutti gli attori della catena.

Esistono infatti diverse applicazioni in cui questo approccio è risultato vincente. Si pensi ad esempio al "tagging" di due milioni di manoscritti e libri presenti nella Biblioteca Vaticana che ha risolto i problemi di prestito ed inventario dei volumi.

Guardando al futuro: più intelligente, più piccolo, più economico e più veloce sono le tendenze ricorrenti nelle tecnologie informatiche. Non ci vuole molto coraggio per prevedere lo stesso nel settore dell'identificazione a radiofrequenza.

L'attesa è che l'evoluzione tecnologica porterà a tag dal costo sempre più ridotto che faranno parte di sistemi più gestibili e più interconnessi. Cosa più importante è prevedere che la tecnologia RFID produrrà alcune "killer application" entro i prossimi tre cinque anni che saranno tanto inaspettate e innovative, quanto l'introduzione del World Wide Web nel 1990 [3].

"Un computer in ogni casa" recitava non troppi anni fa Bill Gates. Con la continua evoluzione dell'elettronica stampabile si arriverà allo stesso per gli RFId. Si potranno così realizzare antenne e persino chip tramite stampanti a inchiostro conduttivo, con una conseguente riduzione di costi.

Ringraziamenti

Credo sia ormai di rito iniziare i ringraziamenti dalla propria famiglia. Questo perché sono le persone che più mi hanno aiutato e supportato per arrivare fin qui. Senza di loro avrei fatto ben poco. Spero di poter ripagare in futuro tutti gli sforzi e i sacrifici che avete fatto e fate per me.

Ringrazio il mio relatore Aldo Romani che tra i suoi tanti impegni ha trovato il tempo per seguirmi e soprattutto per leggersi il mattone interminabile che ho scritto.

Se si parla di RFId non può che venirmi in mente l'azienda per la quale lavoro da ormai 5 anni. Studiare e lavorare non è stato semplice, ma se alla fine sono riuscito a portare avanti le due cose lo devo all'estrema disponibilità del presidente Marino Bandini. Ha creduto in me fin dal primo giorno dove ho timidamente varcato la soglia del suo ufficio. Spero di essere sempre all'altezza dell'investimento che ha fatto su di me.

Ovviamente non posso non citare i due nasi più importanti della Ceracarta cioè Massimo e Stefano. Ringrazio Stefano per rendere le mie giornate in ufficio più sopportabili e ringrazio Massimo per i consigli e per le sue frasi tipiche come "C'è solo un ingegnere in questo ufficio!" che mi hanno spronato a terminare questo percorso.

Ringrazio Valentina e Beatrice per l'affetto per gli utili consigli e per la loro disponibilità.

Ringrazio Alessandro e tutte le donne dei vari uffici della Ceracarta che in 5 anni ancora non ho ancora imparato!.

Ringrazio tutti gli operai della fabbrica! Nonostante alcuni di loro presentino una dubbia sessualità abbiamo spesso lavorato fianco a fianco e anche se sovrastati di lavoro hanno sempre trovato tempo ogni qual volta gli chiedessi un favore.

Infine ringrazio tutti i miei amici. Ovviamente non posso non partire da Enrico. Dovrei scrivere una pagina solo per lui e forse non basterebbe per ringraziarlo a pieno. Credo sarei perso se certe volte non ci fosse. Devo a lui la perdita di gran parte della mia sanità mentale ma per conto devo render grazie a lui se per certi versi sono la persona che sono. Spero di poter assistere presto alla sua laurea.

In quanto a perdita di sanità mentale non posso dimenticarmi di Sacco e Jeppy e tutti gli amici delle serate underground. Perdere neuroni assieme a voi sarà sempre un piacere!

Ringrazio i ragazzi del Rotaract. Anche loro come altri si sono subiti i miei strippi le mie paturnie e nonostante fossi un pazzo squilibrato mi hanno pure concesso di fare il presidente. Ma chi è più pazzo? Il pazzo o chi lo segue?

Ringrazio le tre grazie che hanno condiviso in parte il mio percorso di studi. Mi mancano molto le nostre giornate sue libri di Analisi e le strippate con la Lu che non riusciva a vedere le funzioni come le vedevo io!

Ringrazio anche le persone inutili per le quali ho sprecato una marea tempo credendo in qualcosa che in realtà non esisteva. Proprio quando pensavate di avermi affossato mi avete solamente dato più carica e più forza. Ricordate sempre che rispetto a me siete vetro contro acciaio.

Bibliografia

[1] G. R. Paolo Talone, RFId Fondamenti di unatecnologia silenziosamente pervasiva, Fondazione Ugo Bordoni, 2008.

[2] D. Dobkin, The RF in the RFID, Newnes, 2008.

[3] B. G. Himanshu Bhatt, RFID Essentials, O'Reilly, 2006.

[4] A. Italia, RFID Introduzione alla tecnologia delle etichette intelligenti, AIM Italia, 2006.

[5] K. Finkenzeller, RFID HANDBOOK, Wiley, 2010.

[6] D. P. Sanghera, RFID+, Syngress, 2007.

[7] «EPCglobal®,» [Online]. Available: http://www.gs1.org/epcglobal.

[8] B. H. A. M. D. Frank Thorton, RFID Security, Syngress.