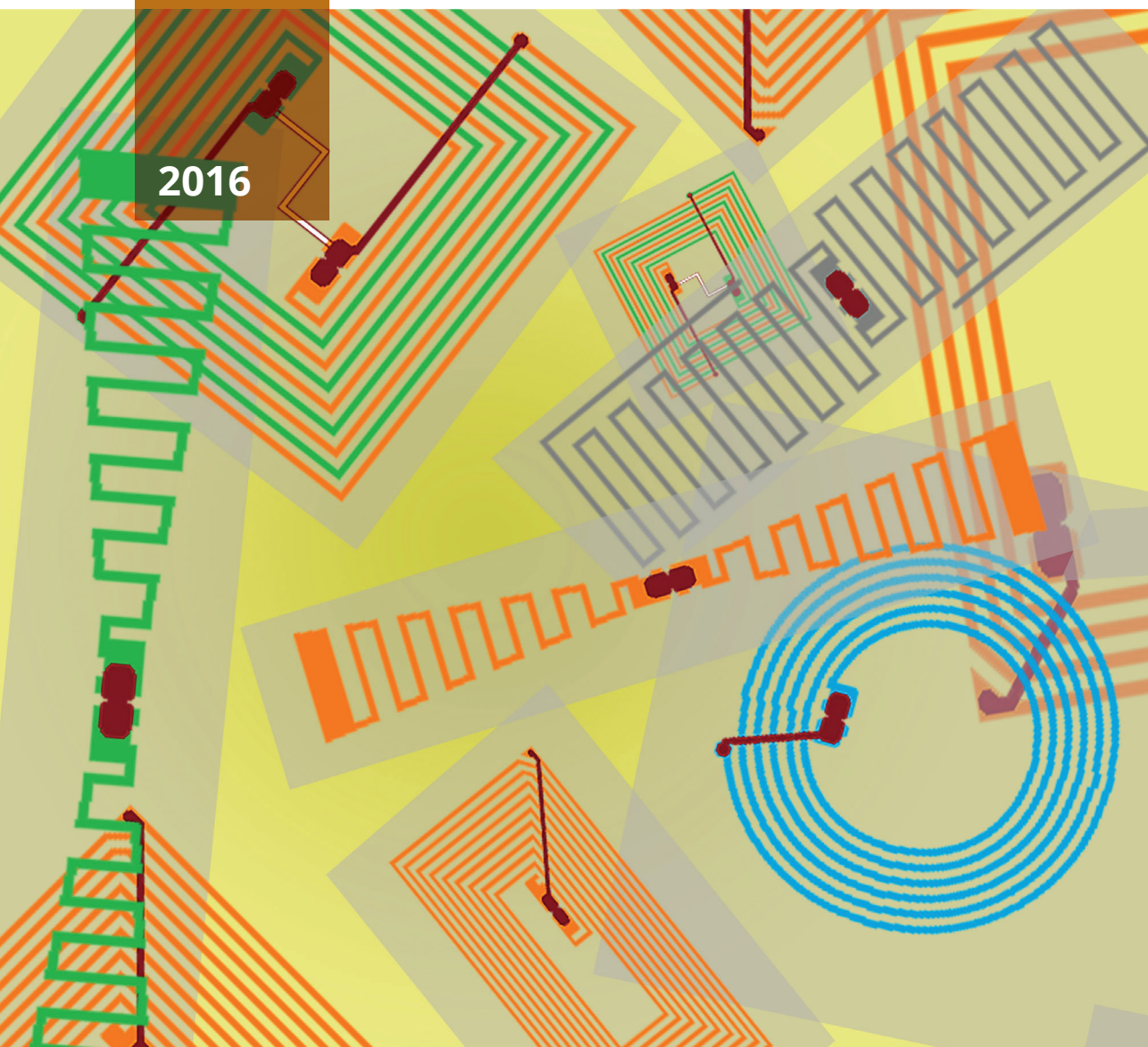
RFId *(Radio-Frequency Identification)* in applicazioni di sicurezza

INAIL

2016



RFId *(Radio-Frequency Identification)* in applicazioni di sicurezza

INAIL

2016

Pubblicazione realizzata da

Inail
Dipartimento innovazioni tecnologiche
e sicurezza degli impianti, prodotti e insediamenti antropici

Autori
Giovanni Luca Amicucci
Fabio Fiamingo

per informazioni
Inail - Dipartimento innovazioni tecnologiche
e sicurezza degli impianti, prodotti e insediamenti antropici
via Roberto Ferruzzi, 38/40 - 00143 Roma
dit@inail.it
www.inail.it

ISBN 978-88-7484-524-8

Tipolitografia Inail - Milano, gennaio 2017

Prefazione

Secondo quanto definito dal Testo Unico sulla Sicurezza del lavoro (d.lgs. 81/08 e s. m. i.) è fatto obbligo al datore di lavoro di provvedere affinché siano messe in atto le misure generali di tutela della salute e della sicurezza dei lavoratori nei luoghi di lavoro di cui all'art. 15 del Testo stesso.

In particolare il datore di lavoro deve provvedere affinché:
- sia effettuata una valutazione di tutti i rischi per la salute e la sicurezza e
- sia effettuata una riduzione dei rischi alla fonte, ad esempio:
  - con la limitazione al minimo del numero dei lavoratori che sono, o che possono essere, esposti a tali rischi;
  - con l'adozione prioritaria di misure di protezione collettiva rispetto alle misure di protezione individuale;
  - con la regolare manutenzione di ambienti, attrezzature e impianti, con particolare riguardo ai dispositivi di sicurezza, in conformità alle indicazioni dei fabbricanti.

Inoltre, le attrezzature di lavoro messe a disposizione dei lavoratori devono essere conformi alle specifiche disposizioni legislative e regolamentari di recepimento delle Direttive comunitarie di prodotto ad esse applicabili (d.lgs. 81/08, art. 70).
Tali attrezzature, che devono essere idonee ai fini della salute e sicurezza e adeguate al lavoro da svolgere o adattate a tali scopi, devono anche essere utilizzate conformemente alle disposizioni legislative di recepimento delle Direttive comunitarie (d.lgs. 81/08, art. 71).

I sistemi RFId (Radio-Frequency Identification) sono una tecnologia che permette il riconoscimento a distanza di un oggetto per mezzo di comunicazioni radio.
Un trasponder (Tag) è accoppiato all'oggetto che deve essere riconosciuto. Un apposito lettore (Reader) interroga i Tag per ricavare le informazioni di interesse.
Il Tag può assumere qualunque forma, può essere esposto agli agenti atmosferici o essere rivestito con il materiale più idoneo al tipo di utilizzo che se ne vuole fare.

I sistemi RFId permettono soluzioni innovative per raggiungere taluni degli obiettivi di salute e sicurezza richiesti dal Testo Unico.

L'Inail svolge attività di ricerca sull'argomento.

Il presente lavoro ha lo scopo di presentare:

- la tecnologia RFId, ed in particolare:
  - la filosofia di funzionamento;
  - i più comuni metodi di utilizzo;
  - alcune applicazioni di sicurezza;
  - alcune applicazioni in ambiente sanitario;
  - alcune criticità rilevate;
- altre tecnologie di comunicazione (Wi-Fi, UWB, Bluetooth LE, ZigBee, NFC) impiegabili (o già impiegate) per applicazioni molto vicine a quelle per cui sono utilizzati gli RFId.

Indice

1. I sistemi RFId

1.1. Introduzione

I sistemi RFId (*Radio-Frequency Identification*) sono una tecnologia che permette il riconoscimento a distanza di un oggetto per mezzo di comunicazioni radio.
Negli ultimi anni le tecnologie di identificazione automatica più diffuse sono state quelle dei codici a barre e delle carte a banda magnetica, tuttavia nei prossimi anni l'RFId potrebbe superarle poiché offre funzionalità più complesse, infatti:

- nei sistemi che utilizzano il codice a barre occorre mantenere una distanza minima tra l'oggetto e il lettore e far assumere all'etichetta la giusta orientazione rispetto al lettore; inoltre, l'etichetta su cui è riportato il codice a barre è di solito cartacea e quindi non in grado di tollerare rivestimenti od agenti esterni, come acqua o sporcizia, che possono degradarne il contenuto informativo;
- le carte a banda magnetica sono soggette a smagnetizzazione e a limitazioni della distanza di utilizzo analoghe a quelle dei codici a barre.

I sistemi RFId sono in grado di superare tutto ciò da grazie alle comunicazioni a radiofrequenza (RF).
In pratica all'oggetto che deve essere riconosciuto è accoppiato un trasponder (Tag) in grado di comunicare via radio le informazioni richieste da un apposito Reader. Ogni Tag può essere identificato in modo univoco grazie ad un codice memorizzato nel proprio microchip.
Il Tag può assumere qualunque forma si desideri, può essere esposto agli agenti atmosferici o essere rivestito con il materiale più idoneo al tipo di utilizzo che si vuole fare dell'oggetto su cui è applicato.
Un Tag può immagazzinare anche una cospicua quantità di dati e consentire operazioni di lettura e scrittura in tempo reale a distanza di alcuni metri.
Il fatto che un Tag possa essere letto a distanze superiori rispetto ad un codice a barre o ad una carta magnetica è un'intrinseca superiorità dei sistemi RFId rispetto a tali tecnologie.

1.2. Origini e sviluppo della tecnologia RFId

L'RFId non è una tecnologia recente. Nacque durante la Seconda Guerra Mondiale in seguito all'uso dei primi radar (*radio detecting and ranging* - rilevamento radio e misurazione di distanze) che non erano sofisticati come quelli attuali.
Il radar è costituito da un'antenna di trasmissione fortemente direzionale (in grado di emettere una serie di impulsi radio), da un impianto di ricezione (che sfrutta la stessa antenna), da un sistema di amplificazione e da uno schermo. L'antenna montata su un piano rotante invia verso l'oggetto cercato radioonde modulate a impulsi e riceve le onde riflesse dallo stesso (echi radar). Dal ritardo degli echi è possibile calcolare la distanza e conoscendo la posizione istantanea della rotazione dell'antenna ricevente, è possibile visualizzare sullo schermo un punto rappresentante l'oggetto.
Il ministero della difesa britannico non considerò soddisfacenti i primi radar, in quanto avrebbero dovuto non solo avvistare gli aerei nemici, ma anche identificare gli amici dai nemici, in modo da ottenere, in tempo reale, la situazione delle battaglie aeree. Fu ordinata, quindi, la progettazione di un sistema IFF (*Identification Friend or Foe* - identificazione amico o nemico). Il sistema consisteva in una scatola, montata sugli aviogetti inglesi, contenente una ricetrasmittente, denominata successivamente trasponder.
Quando il fascio di radioonde del radar colpiva l'aereo, il trasponder rispondeva sulla stessa frequenza, permettendo l'identificazione degli aerei amici sullo schermo del radar. La tecnologia fu estesa subito alle navi per identificarne la posizione e la velocità.
I primi trasponder, destinati solo a scopi militari, erano molto costosi e di notevoli dimensioni.
Le applicazioni militari favorirono lo sviluppo di tali tecnologie e delle loro funzionalità. La severità degli ambienti operativi e le elevate prestazioni richieste per gli apparati militari permisero di sviluppare prodotti altamente affidabili.
Poi, con lo sviluppo delle nuove tecnologie elettroniche, furono realizzati anche prodotti con alte prestazioni e costi adeguati all'utilizzo nel settore civile.
Verso la fine degli anni '60 ebbero inizio i primi usi civili, con la commercializzazione dei primi sistemi EAS (*Electronic Antitheft Surveillance* - sorveglianza elettronica antiladri), realizzanti funzioni antitaccheggio.
Tali sistemi utilizzano apparecchiature che permettono il rilevamento della presenza o dell'assenza del trasponder, gestendo pertanto un bit di informazione.
Negli anni '70 diverse grandi industrie americane del settore militare misero a punto applicazioni RFId civili utilizzando le tecnologie da essi sviluppate. Una di queste applicazioni era dedicata al controllo di oggetti e di mezzi in movimento ma non ebbe successo commerciale.
In realtà si riteneva la tecnologia non completamente matura, e per tale motivo non furono definiti standard ufficiali per L'RFId, lasciando la massima libertà di ricerca e sperimentazione.

Negli anni '80 la tecnologia RFId si diffuse su scala mondiale. Negli Stati Uniti l'interesse dei costruttori puntò sul controllo delle merci trasportate, dei mezzi di trasporto e degli accessi delle persone ad aree controllate. In Europa si puntò all'identificazione degli animali, alle applicazioni industriali e al controllo degli accessi in autostrada. Negli anni '90 iniziarono a svilupparsi degli standard internazionali condivisi ed i circuiti si miniaturizzarono sempre di più, permettendo una diminuzione drastica dei consumi di energia. Infatti, i trasponder potevano essere alimentati dalla stessa onda elettromagnetica generata dal lettore che li interrogava, rendendo inutile la presenza delle batterie. Ciò era favorito anche dalla possibilità di utilizzare memorie non volatili, in modo da non avere la necessità di una batteria per mantenere i dati. I progressi tecnologici degli ultimi vent'anni e il perfezionamento delle tecniche di produzione di massa hanno reso possibile la creazione di transponder di dimensioni ridottissime (anche pochi millimetri) a basso costo. La tecnologia RFId è stata quindi utilizzata in numerosi campi applicativi andando incontro ad un successo crescente, ad esempio, anche nel campo dell'identificazione personale (passaporti, patenti e carte d'identità RFId) e del pagamento elettronico.

1.3. Caratteristiche dei sistemi RFId

La tecnologia RFId si compone di tre elementi fondamentali: Tag, Reader e sistema di gestione.

- Il Tag è un trasponder (ricevitore e trasmettitore) a radiofrequenza, di piccole dimensioni, costituito da un circuito integrato (chip) con logica di controllo, da una memoria (normalmente la quantità di dati contenuti in un RFId è piuttosto modesta: da pochi bit a centinaia di byte o, al massimo a qualche kbyte) e da un ricetrasmettitore RF, connesso ad un'antenna. Il Tag è inserito in un contenitore, o incorporato in un'etichetta, una smart-card, una chiave, o integrato in apparati elettronici (orologi, telefonini). Il Tag permette la comunicazione di dati a breve raggio, senza contatto fisico. I dati contenuti nella memoria sono spesso limitati ad un unico codice (identificativo del Tag). Viceversa, alcuni Tag possono immagazzinare anche una notevole quantità di informazioni.
- Il Reader è un ricetrasmettitore controllato da un microprocessore, usato per interrogare i Tag e ricevere in risposta le informazioni in essi contenute.
- Il sistema di gestione (Management system) è un sistema informativo, connesso in rete con i Reader, che consente, a partire dai codici identificativi provenienti dai Tag, di ricavare tutte le informazioni disponibili associate a tali oggetti e di gestirle per gli scopi dell'applicazione.

1.3.1. Classificazione dei Tag

I Tag sono classificati, a seconda dell'alimentazione, in: passivi, semi-passivi e attivi.

- I Tag passivi ricavano l'energia per alimentare i propri circuiti interni dal segnale proveniente dal Reader. Una volta che ha decodificato il segnale del Reader, il Tag risponde riflettendo e rimodulando il campo incidente. I Tag passivi sono tipicamente dispositivi a basso costo e di piccole dimensioni che consentono di realizzare numerosi tipi di applicazioni, che spesso sono possibili proprio per le ridotte dimensioni dei Tag. Infatti, essendo costituiti solamente da un'antenna (tipicamente stampata) e da un circuito integrato (generalmente miniaturizzato), l'altezza dei Tag passivi può essere anche di poche centinaia di micron. Pertanto tali Tag possono essere inseriti in carte di credito, etichette adesive, bottoni, piccoli oggetti di plastica, fogli di carta, banconote e biglietti, dando vita ad oggetti parlanti.
- I Tag semi-passivi sono dotati di batteria utilizzata per alimentare la logica di controllo, la memoria ed eventuali apparati ausiliari, ma non il trasmettitore, comportandosi in trasmissione come Tag passivi, ciò consente di incrementare la durata della batteria e, di conseguenza, la vita del dispositivo.
- I Tag attivi sono alimentati a batteria e possono avere funzionalità molto complesse, limitate solo dalla durata della batteria.

Le informazioni che il Tag trasmette al Reader sono contenute in una certa quantità di memoria che ogni Tag contiene al suo interno. Le informazioni d'identificazione sono relative all'oggetto interrogato: tipicamente un numero di serie univoco, in qualche caso anche la copia dell'UPC (Universal Product Code) contenuto nel codice a barre ed altre informazioni (ad es.: date di produzione, composizione dell'oggetto).
In base al tipo di memoria i Tag sono classificati di tipo read-only o read-writable. Questi ultimi consentono, durante l'uso, oltre alla lettura, anche la riscrittura dell'informazione in essi memorizzata. In passato i Tag passivi erano principalmente di tipo read-only, sia perché la fase di scrittura richiede la disponibilità di una elevata quantità di energia che si ricava con difficoltà dal segnale ricevuto, sia perché le memorie riscrivibili hanno un costo relativamente elevato. I Tag passivi riscrivibili sono comunque in rapida diffusione.
Per i Tag attivi o semi passivi, oltre alla maggior quantità di memoria ed alla funzione di riscrivibilità della stessa, l'evoluzione tecnologica ha consentito di aggiungere funzioni che superano la semplice identificazione. Si ricordano, ad esempio, le funzioni di radiolocalizzazione (RTLS - *Real Time Location System* - sistema di localizzazione in tempo reale) o la misura di parametri ambientali attraverso sensori (ad es.: temperatura, movimento).

1.3.2. Caratteristiche dei Reader

Il Reader consente di leggere le informazioni contenute nel Tag, che si traducono in molti casi in un semplice identificativo, che, a differenza dei codici a barre, ha la particolarità di essere univoco nell'ambito del sistema informativo che realizza il

sistema di gestione. Entrando, quindi, in tale sistema informativo ed usando l'identificativo univoco come chiave di ricerca, si possono ricavare informazioni dettagliate (anche aggiornate nel tempo) sul particolare oggetto a cui il Tag è associato.
I Reader per Tag attivi sono progettati usando le più diverse tecnologie a radiofrequenza, in modo da consentire letture anche a distanza di parecchie centinaia di metri.
I Reader per Tag passivi (e semi passivi), invece, emettono segnali RF di tipo particolare, in grado di fornire ai Tag anche l'energia necessaria per la risposta. Per consentire di ricavare un'energia sufficiente, le distanze di lettura non sono elevate.

1.3.3. Frequenze di esercizio per i sistemi RFId

Le frequenze di comunicazione tra Reader e Tag dipendono sia dalla natura del Tag, sia dalle applicazioni e sono regolamentate allo scopo di limitare la potenza di emissione e di prevenire le interferenze. La regolamentazione, però, è divisa in base alle regioni geografiche ITU (Regione 1 = Europa, Africa, Medio Oriente fino all'Iraq, Unione Sovietica, Mongolia; Regione 2 = Americhe, Groenlandia e alcune isole del Pacifico; Regione 3 = parte rimanente dell'Asia e Oceania), con normazione diversa da regione a regione (specie per le frequenze più alte, di uso più recente). Ciò può comportare problemi di incompatibilità quando gli RFId viaggiano insieme alle merci alle quali sono associati, anche se, ad oggi, alcune bande di frequenza sono accettate in tutto il pianeta.
La scelta della frequenza di lavoro e il valore massimo della potenza irradiata dal Reader influiscono sulla distanza di funzionamento del sistema, sulle interferenze con altri sistemi radio, sulla velocità di trasferimento dei dati e sulle dimensioni dell'antenna.
I sistemi più moderni che usano frequenze più basse e Tag passivi sono in grado di trasmettere dati al massimo fino a distanze non superiori a un metro e mezzo.
I sistemi che usano frequenze più elevate e Tag attivi riescono ad avere distanze di funzionamento maggiori, anche se comunque limitate dal massimo valore consentito per la potenza irradiata.
Per sistemi a frequenza più alta le dimensioni delle antenne si riducono (Tag più piccoli) e la velocità di trasferimento dati cresce.
Una breve panoramica non esaustiva delle bande di frequenza più utilizzate per la realizzazione di sistemi RFId è riportata nell'Appendice I, esistono, comunque, anche altre frequenze utilizzabili quali 433÷435MHz in banda UHF (Ultra High Frequencies) bassa e 5,8GHz in banda SHF (Super High Frequencies).

1.3.4. Tipi di memorie impiegate nei Tag

La capacità di memoria del Tag, la velocità di accesso alla stessa, la durata tempo-

rale dei dati immagazzinati e l'eventuale possibilità di riscrittura degli stessi, sono caratteristiche fondamentali nelle applicazioni RFId.
Le memorie impiegate nei Tag sono dei seguenti tipi: ROM, PROM, EEPROM, SRAM e FRAM.
Una breve panoramica delle memorie più utilizzate per la realizzazione di sistemi RFId è riportata nell'Appendice II.

2. Princìpi di funzionamento degli RFId

2.1. Accoppiamento Reader-Tag nei sistemi passivi

La lettura di un Tag passivo (o semi-passivo) è diversa da una comunicazione dati bidirezionale. A differenza dei Tag attivi, i Tag passivi dipendono per la loro alimentazione dall'energia ricevuta dall'antenna. Infatti, essi non generano la frequenza portante per la trasmissione, ma re-irradiano, modulandola, una parte dell'energia ricevuta dal Reader che li sta interrogando. Ciò è possibile tramite variazione dell'impedenza dell'antenna del Tag.
Nei sistemi RFId, il diverso comportamento delle onde elettromagnetiche nei campi vicino e lontano, è importante (Appendice III).
Se la frequenza utilizzata è bassa, nelle normali condizioni operative è verificata la condizione $r << \lambda/(2\pi)$ ed il sistema RFId opera in condizione di campo vicino, in tal caso è possibile sfruttare il concatenamento dovuto all'induzione magnetica per lo scambio di informazioni, viceversa, alle frequenze più alte è verificata la condizione $r >> \lambda/(2\pi)$ ed il sistema RFId opera in condizione di campo lontano, in tal caso per lo scambio di informazioni sono utilizzate onde elettromagnetiche (costituite da campi elettrici e magnetici ortogonali tra loro e ortogonali alla direzione di propagazione e con ampiezze in rapporto costante).
Pertanto, per ricavare energia e comunicare con il Reader, il funzionamento dei Tag si basa su uno dei due seguenti principi fisici:

- accoppiamento induttivo o magnetico (in condizioni di *campo vicino*);
- accoppiamento elettromagnetico (in condizioni di *campo lontano*).

Il caso di funzionamento in condizione di campo vicino è paragonabile allo scambio di energia tra il primario ed il secondario di un trasformatore elettrico, mentre il caso di funzionamento in condizione di campo lontano si può paragonare ad un sistema di trasmissione e ricezione radio.
Nell'accoppiamento induttivo (figura 1) le antenne del Reader e del Tag sono costituite da spire.
Per distanze relativamente brevi rispetto alla lunghezza dell'onda emessa dall'antenna del Reader, nell'antenna del Tag prevalgono gli effetti della corrente indotta dal campo magnetico: in pratica l'antenna del Reader genera un flusso magnetico variabile nel tempo che si concatena con le spire dell'antenna del Tag dando origine, secondo la legge di Lenz, ad una corrente indotta.

Poiché l'accoppiamento tra Reader e Tag è simile a quello tra il circuito primario ed il circuito secondario di un trasformatore elettrico, il Tag è attivato dall'energia trasferita al secondario.
Per ottenere le condizioni di campo vicino alle distanze operative impiegate si fa ricorso alle bande con maggiore lunghezza d'onda (LF ed HF). La distanza operativa di Tag passivi basati sull'accoppiamento induttivo non supera di solito il metro.
Nell'accoppiamento elettromagnetico (figura 2) si sfrutta l'effetto di *backscattering* delle onde radio (il motivo del prefisso *back* serve a mettere in evidenza che le onde, dopo la riflessione, tornano indietro al Reader che le ha emesse). Per distanze relativamente lunghe, rispetto alla lunghezza dell'onda emessa dall'antenna del Reader, nell'antenna del Tag prevalgono gli effetti delle onde radio su essa incidenti: in pratica l'antenna del Tag riflette parte della potenza elettromagnetica ricevuta (attraverso una variazione di impedenza pilotata). Questa può essere rilevata dall'antenna del Reader.
Per ottenere le condizioni di campo lontano alle distanze operative impiegate si fa ricorso alle bande con minore lunghezza d'onda (UHF e SHF). La distanza operativa di Tag passivi basati sull'accoppiamento elettromagnetico è compreso tra 1 e 10 m, per distanze maggiori è necessario ricorrere a Tag attivi.

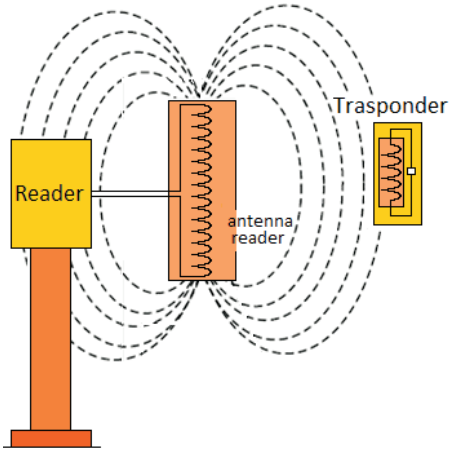


Figura 1: Accoppiamento induttivo o magnetico.

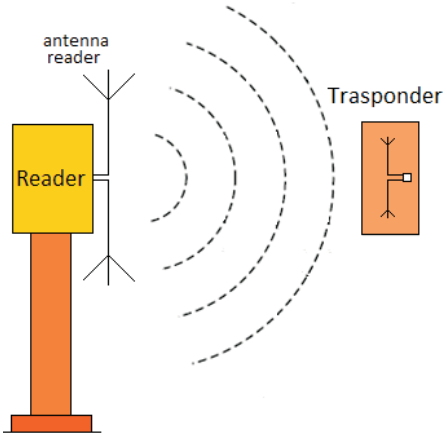


Figura 2: Accoppiamento elettromagnetico.

2.2. Principi di funzionameno dei Tag passivi

Come già anticipato, i Tag passivi dei sistemi RFId modulano la riflessione del segnale incidente attraverso la variazione dell'impedenza della propria antenna, ciò consente la comunicazione con il Reader.
I Tag passivi che operano a frequenze maggiori, usano tecniche a modulazione di

ampiezza simili a quelle dei Tag che operano a frequenza più bassa e ricevono ugualmente la loro potenza dal campo generato dal Reader.
La differenza consiste nel modo in cui l'energia è trasferita e nel tipo di antenna (antenne a spira in condizioni di campo vicino e antenne a dipolo in condizioni di campo lontano).
Quando il segnale emesso dal Reader incide sull'antenna del Tag (figure 3 e 4) una parte dell'energia è assorbita (attraverso un ordinario circuito con un raddrizzatore ed un condensatore), fornendo alimentazione alla logica di controllo del Tag.
La logica di controllo del Tag si attiva e decodifica il segnale di interrogazione del Reader. Poi, sulla base dei dati presenti nella memoria, modula l'impedenza dell'antenna del Tag, riflettendo all'indietro verso il Reader una piccola parte della potenza incidente.
L'energia ricavata dall'antenna del Tag è sicuramente troppo bassa per alimentare un trasmettitore. Per questo, per la comunicazione tra Tag e Reader, si sfrutta la modulazione d'impedenza dell'antenna del Tag.
Il Reader ha anche il compito non semplice di captare le conseguenti variazioni nel segnale riflesso. Infatti problemi potrebbero sorgere per il fatto che il segnale di risposta è modulato sulla stessa frequenza del segnale di interrogazione.
Il Reader decodifica il segnale riflesso tramite un rivelatore e trasmette i dati ricevuti alla propria logica di controllo.

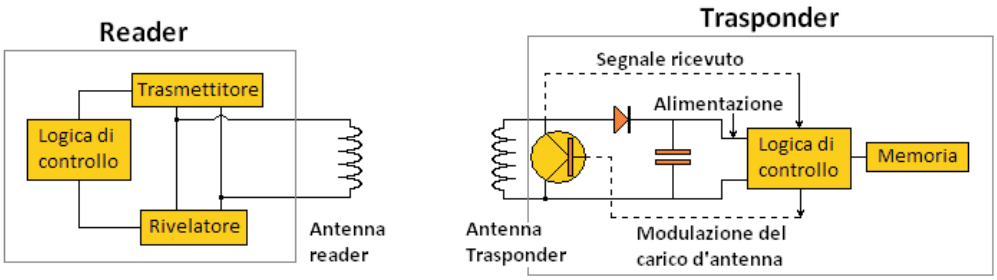


Figura 3: Principio di funzionamento di un Tag passivo ad accoppiamento induttivo.

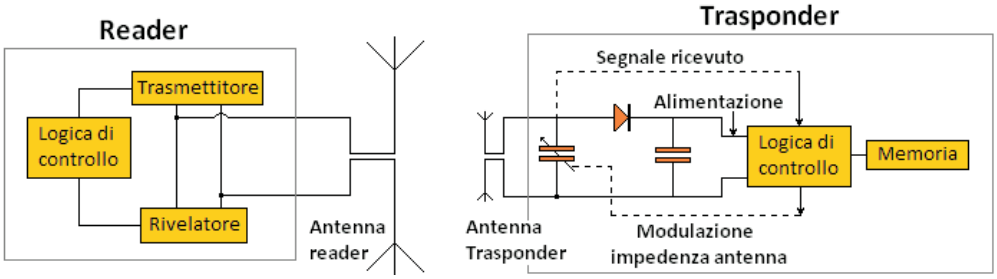


Figura 4: Principio di funzionamento di un Tag passivo ad accoppiamento elettromagnetico.

L'uso della tecnica di modulazione del backscatter in condizioni di campo lontano, introduce ulteriori problemi rispetto a quelli che si manifestano nei sistemi operanti in condizioni di campo vicino. Uno dei principali è dovuto al fatto che il campo emesso dal Reader, non è riflesso solo dall'antenna del Tag ma anche da tutti gli oggetti circostanti con dimensioni paragonabili alla lunghezza d'onda utilizzata. Tali campi riflessi (cammini multipli) si sovrappongono al campo principale e possono provocarne un affievolimento o perfino la cancellazione.
Comunque i Tag passivi ad accoppiamento elettromagnetico operano a distanze maggiori di quelli ad accoppiamento induttivo, con antenne più semplici e di dimensioni più contenute.

2.3. Antenne ed accoppiamenti

Nei sistemi RFId passivi, le antenne sono la fonte primaria di energia per i Tag, pertanto problemi di errato orientamento di tali antenne, rispetto alla polarizzazione del campo generato dal Reader, possono influire significativamente sulle prestazioni[1].
Ciò provoca sensibili riduzioni nella distanza operativa, fino ad arrivare al fallimento della lettura dei Tag orientati ortogonalmente rispetto al campo generato dal Reader.

- Per gli apparati con accoppiamento induttivo, che sono particolarmente sensibili all'orientamento delle antenne, l'orientamento ottimale per le spire delle antenne di Tag e Reader è quello che le porta ad essere parallele tra loro.
- Per gli apparati con accoppiamento elettromagnetico, il trasferimento ottimale di potenza tra Reader e Tag, avviene quando i vettori di massima intensità dei diagrammi di radiazione delle due antenne sono allineati.

Le antenne dei Tag ad accoppiamento elettromagnetico sono generalmente dei dipoli progettati anche per favorire il backscatter.
Per un soddisfacente trasferimento dell'energia, la lunghezza del dipolo deve essere pari a multipli di metà della lunghezza d'onda. In via ottimale dovrebbe essere uguale a $\lambda/2$. In realtà il dipolo è spesso costruito a $\lambda/4$ ed accordato con tecniche particolari.
Deviazioni da tali sottomultipli di lunghezza d'onda comportano significative perdite di prestazioni.
Per quanto riguarda il problema della polarizzazione, a volte si ricorre a Reader dotati di più antenne sistemate in posizione ortogonale tra loro. Questo minimizza la sensibilità alla polarizzazione.

1 Due importanti parametri, connessi alle antenne dei Tag che difficilmente le specifiche tecniche o gli standard forniscono, sono:
  - la sensibilità energetica (energizing sensitivity - ovvero l'energia del campo elettromagnetico necessaria al funzionamento del Tag);
  - la riflettività (reflectivity - ovvero il rapporto tra potenza incidente e riflessa dall'antenna del Tag).

2.3.1. Modello dell'accoppiamento induttivo

Il modello elettrico equivalente dell'accoppiamento induttivo Reader-Tag di un sistema RFId operante in condizione di campo vicino è mostrato in figura 5, dove il primario modella il Reader ed il secondario il Tag.

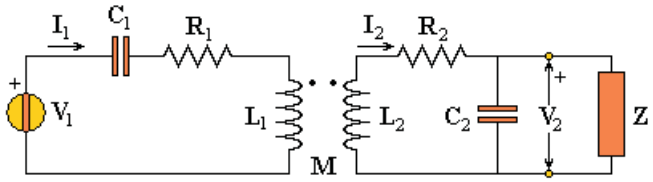


Figura 5: Circuito elettrico equivalente Reader-Tag in condizione di campo vicino.

La dimensione dell'antenna a spira del Tag è di solito scelta in modo da essere inferiore a un quarto della lunghezza d'onda, quindi è molto piccola, per non influenzare l'omogeneità del campo tra Reader e Tag.
Le equazioni di Kirkoff per il calcolo della tensione indotta dal Reader sul Tag (per $Z \approx \infty$) sono:

$$sMI_1 = \left(R_2 + sL_2 + \frac{1}{sC_2} \right) I_2$$

$$V_2 = \frac{1}{sC_2} I_2$$

dove s è la variabile di Laplace, sMI_1 è la forza elettromotrice indotta sul Tag dal campo magnetico generato dalla corrente I_1 che circola nel circuito del Reader.
La mutua induttanza M dipende dalla distanza tra le due spire, dall'angolo di orientazione reciproca, dalle dimensioni e dal numero delle spire, secondo la formula:

$$M = k \cdot \mu N_1 N_2 \pi \frac{b_1^{\,2} b_2^{\,2}}{2\left(r^2 + b_1^{\,2}\right)^{\frac{3}{2}}} \cos\alpha$$

dove:
- N_1 è il numero delle spire al primario (antenna del Reader),
- N_2 è il numero delle spire al secondario (antenna del Tag),
- α è l'angolo tra la normale alla superficie di una spira dell'antenna del Reader e la normale alla superficie di una spira dell'antenna del Tag,
- r è la distanza tra le spire,

- b_1 è il raggio delle spire del Reader,
- b_2 è il raggio delle spire del Tag,
- k è un fattore che tiene conto della non idealità dell'accoppiamento delle linee del campo magnetico.

L'autoinduttanza del Tag vale:

$$L_2 = \mu b_2 N_2^{\,2}\left[\ln\left(\frac{8b_2}{a_2}\right) - 1.75\right]$$

dove a_2 è il raggio del conduttore con cui sono realizzate le spire del Tag stesso.
La resistenza del Tag vale:

$$R_2 = N_2^{\,2}\frac{b_2}{a_2}\sqrt{\frac{\omega\mu}{2\sigma}}$$

dove:
- $\omega = 2\pi f$ è la pulsazione del segnale ed f è la sua frequenza,
- σ è la conducibilità del conduttore con cui sono realizzate le spire.

Per quanto riguarda il circuito del Reader si hanno le seguenti espressioni:

$$L_1 = \mu b_1 N_1^{\,2}\left[\ln\left(\frac{8b_1}{a_1}\right) - 1.75\right]$$

$$R_1 = N_1^{\,2}\frac{b_1}{a_1}\sqrt{\frac{\omega\mu}{2\sigma}}$$

dove a_1 è il raggio del conduttore con cui sono realizzate le spire del Reader.
La corrente I_1 del circuito del Reader può calcolarsi con la seguente equazione:

$$V_1 = \left(R_1 + sL_1 + \frac{1}{sC_1}\right)I_1 + sMI_2$$

Per massimizzare la potenza trasferita dal Reader al Tag, è necessario rendere risonanti entrambi i circuiti (la frequenza di risonanza è scelta in modo da coincidere con la frequenza di funzionamento):
- nel circuito del Reader è necessario massimizzare la corrente, in modo da massimizzare il flusso magnetico e quindi, poiché l'induttanza è fissata dalla realiz-

zazione fisica dell'antenna, è necessario aggiungere in serie una capacità C_1 tale che la reattanza dovuta a L_1 e C_1 tenda a zero alla frequenza di risonanza, in questo modo la corrente al primario è limitata solo dalla resistenza del circuito;

- nel circuito del Tag è necessario massimizzare la tensione V_2 di alimentazione del circuito elettronico (rappresentato con Z); l'induttanza è fissata anche in questo caso, ma è possibile inserire una capacità C_2 in parallelo, tale da rendere V_2 massima, in questo modo la tensione al secondario è limitata solo dalla resistenza del circuito.

In pratica, una volta fissata la geometria delle antenne, il conduttore con cui sono realizzate e la frequenza di risonanza f, se vale la condizione:

$$f < \frac{1}{2\pi}\frac{\sqrt{R_1 R_2}}{M}$$

è possibile scegliere

$$C_1 = \frac{1}{\omega^2 L_1} \quad \text{e} \quad C_2 = \frac{1}{\omega^2 L_2}$$

dove $\omega = 2\pi f$, per massimizzare il flusso magnetico emesso dal Reader e la tensione V_2 ricevuta dal Tag.

Dato un circuito con resistenza, induttanza e capacità in serie, è possibile definire un fattore di qualità Q pari a (dove ω è la pulsazione di risonanza tale che $\omega^2 = 1/LC$):

$$Q = \frac{\omega L}{R}$$

che indica il rapporto tra l'energia immagazzinata nei componenti reattivi e quella dissipata nella resistenza.
Per massimizzare il fattore di qualità si può ridurre la resistenza ed aumentare l'induttanza (la capacità è variata in modo da mantenere w pari al valore di risonanza/lavoro). Tuttavia i limiti di tale operazione sono dati dall'effetto che essa ha sulla banda passante, che diventa estremamente stretta, rendendo più difficile la comunicazione tra Reader e Tag. In fase di progetto, si cerca di trovare il giusto compromesso tra banda passante e potenza immagazzinata alla frequenza di lavoro.

2.3.2. Modello dell'accoppiamento elettromagnetico

Il modello elettrico equivalente dell'accoppiamento elettromagnetico Reader-Tag di un sistema RFId operante in condizione di campo lontano è mostrato in figura 6, dove il primo circuito modella il Reader ed il secondo il Tag.

Figura 6: Circuito elettrico equivalente Reader-Tag in condizione di campo lontano.

Il modello di figura 6 è basato sull'equazione di Friis (Appendice III) e su alcune considerazioni supplementari.
Nelle antenne reali non tutta la potenza P_a con cui è alimentata l'antenna viene poi irradiata (cioè contribuisce a P_i) ma vi sono delle perdite, dovute principalmente all'impedenza dei conduttori dell'antenna, al non perfetto isolamento dei supporti e all'assorbimento di oggetti metallici posti in prossimità dell'antenna. Di ciò si tiene conto col rendimento dell'antenna trasmittente η_t con (η_t<1):

$$\eta_t = \frac{P_i}{P_a}$$

In pratica si può pensare l'antenna come costituita da due resistenze, R_a e R_i, che tengono conto, rispettivamente della potenza dissipata e della potenza irradiata, in tal caso:

$$\eta_t = \frac{P_i}{P_a} = \frac{\frac{1}{2}R_i I^2}{\frac{1}{2}(R_i + R_a)I^2} = \frac{R_i}{R_i + R_a}$$

La potenza ricevuta dall'antenna ricevente vale:

$$P_r = p\eta_r \frac{\lambda^2}{(4\pi r)^2} G_r G_t (\eta_t P_a)$$

dove sono stati introdotti:
- il fattore di correzione *p* per le perdite dovute all'errata orientazione dell'antenna rispetto alla polarizzazione dell'onda trasmessa,
- il fattore η_r per le perdite dovute ad effetti di propagazione (multipath, scattering, ecc.) e di non perfetto adattamento tra l'impedenza dell'antenna ricevente Z_r ed il carico Z.

L'impedenza dell'antenna ricevente $Z_r = R_r + jX_r$ è di solito adattata all'impedenza di carico $Z = R + jX$ (ciò è ottenuto per $R_r = R$ e $X_r = -X$) in modo da avere su quest'ultima il massimo trasferimento di potenza:

$$P_Z = \frac{1}{2} R \cdot |I_r|^2 = \frac{1}{2} \frac{R \cdot |V_r|^2}{|Z + Z_r|^2} = \frac{1}{8} \frac{|V_r|^2}{R_r} = \frac{1}{2} P_r$$

dove

Si noti che della potenza ricevuta P_r, la metà P_Z è trasferita al carico e l'altra metà è dissipata sull'impedenza Z_r dell'antenna, cioè l'antenna del Tag re-irradia metà della potenza che riceve, ed è proprio con tale potenza, modulata tramite modulazione dell'impedenza Z_r che il Tag risponde alle interrogazioni del Reader.

3. Modelli di trasmissione dati per sistemi RFId

3.1. Introduzione

La comunicazione è l'insieme dei fenomeni che comportano la distribuzione di informazioni.
Essa si basa su alcuni elementi fondamentali:
- un'emittente (trasmettitore);
- un canale di comunicazione (necessario per trasferire l'informazione);
- il contenuto della comunicazione (l'informazione);
- un codice formale per la codifica e la decodifica delle informazioni;
- il destinatario della comunicazione (ricevente).

Nel caso di un'applicazione RFId, il Reader e i Tag e devono comunicare tra loro facilmente e senza disturbare altri sistemi radio o elettrici.
Allo scopo per ogni applicazione sono definiti i protocolli di comunicazione, cioè una serie di documenti normativi che descrivono tutti gli aspetti tecnici necessari per il processo di comunicazione, soprattutto quando l'applicazione richiede che dispositivi di fabbricanti diversi possano interoperare.
Le specifiche tecniche contenute nei i protocolli sono essenziali per garantire il successo di un'applicazione.
Le applicazioni di successo sono di solito basate su protocolli in grado di assicurare almeno i seguenti obiettivi principali:
- l'interoperabilità tra Reader e Tag (per l'interfacciamento di dispositivi di fabbricanti diversi);
- la capacità di operare senza interferire con le operazioni di altri apparati radio o elettrici.

Il rispetto del principio di non interferenza riguarda il livello fisico della comunicazione radio:
- bande di frequenze;
- larghezze di banda (all'interno delle bande permesse per un dato servizio);
- potenze radio di emissione (e condizioni ambientali in cui le emissioni avvengono: indoor, outdoor);
- non emissione di segnali spuri che costituiscano disturbo per altri sistemi.

Il dialogo tra Reader e Tag richiede comunque la definizione dei seguenti aspetti tecnici:

- Procedure per la costituzione dei link di comunicazione radio da Reader a Tag (forward link) e da Tag a Reader (return link);
  ⇒ tecnica di interrogazione messa in atto dal Reader;
  ⇒ procedure anti-collisione (al fine di ottimizzare la capacità di rilevare e classificare il maggior numero possibile di Tag all'interno dell'area operativa del Reader, nel minore intervallo di tempo).
- tipo di modulazione dei segnali;
- codifica dei dati;
- velocità di trasmissione dei dati (bit rate);
- formato ed impacchettamento dei dati.

Oltre a quanto visto possono essere necessarie indicazioni anche sui seguenti aspetti:

- la conformità al protocollo (il modo per valutare i prodotti di fabbricanti diversi);
- la forma e le caratteristiche fisiche dei contenitori dei Tag;
- le applicazioni particolari;
- i protocolli che specificano il modo in cui il sistema informativo deve processare dati e istruzioni.

3.2. Il modello OSI per la comunicazione tra dispositivi

Il modello OSI (*Open Systems Interconnection* [5]), strutturato su sette livelli (figura 7), è divenuto col tempo lo standard per modellizzare il processo di comunicazione tra due generici dispositivi (stazioni).

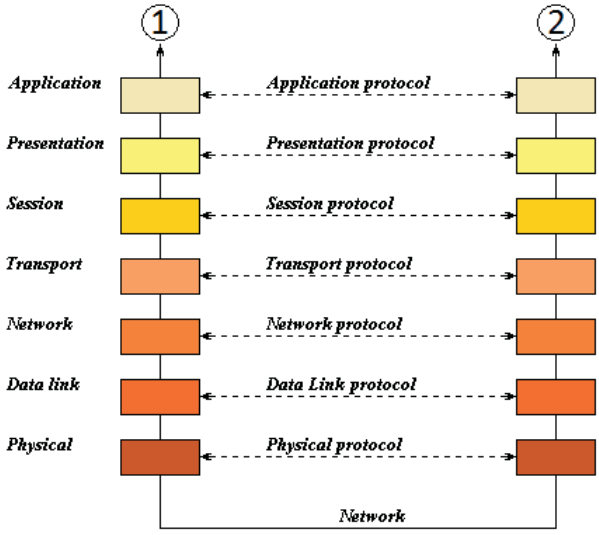


Figura 7: Modello OSI.

I livelli che compongono il modello sono indipendenti, gestiscono funzioni diverse e forniscono servizi ai livelli adiacenti (inferiore o superiore) tramite opportuni protocolli. Esistono, pertanto, interfacce diverse che interagiscono fra i livelli e che permettono la comunicazione tra le due stazioni. Un messaggio generato dalla stazione ① è elaborato di livello in livello, fino a raggiungere il livello fisico, per poi compiere il percorso a ritroso sui livelli della stazione ②; i livelli paritari di due stazioni sono, pertanto, virtualmente connessi tra loro. Nella tabella 1 sono riassunti i compiti dei sette livelli [3].

Tabella 1 - Funzione dei livelli del modello OSI [3]

Livello	Funzione
1. Fisico	modalità di trasmissione vera e propria dei dati
2. Dati	struttura dei dati
3. Rete	modalità di instradamento (routing)
4. Trasporto	divisione dei dati in pacchetti e qualità della comunicazione.
5. Sessione	organizzazione delle sequenze dei dati
6. Presentazione	interpretazione, cifratura, decifratura e compressione dei dati
7. Applicazione	protocolli al livello della particolare applicazione (struttura e significato dei messaggi che i due programmi nelle due stazioni si scambiano)

Anche i sistemi RFId possono essere rappresentati per mezzo del modello OSI, in particolare [6]:
- i livelli 1 e 2 rappresentano la modulazione e la codifica del segnale;
- il livello 3 rappresenta il processo di gestione dell'anticollisione;
- i livelli 4, 5 e 6 rappresentano il protocollo della comunicazione (rilevamento degli errori, correzione degli errori, sicurezza dell'accesso);
- Il livello 7 contiene gli effettivi servizi dell'applicazione RFId.

Le informazioni sono di tipo digitale (stato 1 o 0) ma sono trasmesse in un canale che utilizza una *portante* analogica modulata.

3.3. Modulazione della portante

La modulazione è l'operazione con cui il segnale contenente l'informazione (*modulante*) è combinato con un secondo segnale (*portante*) che ha le caratteristiche adatte alla trasmissione. In pratica la *modulazione* consiste nel far variare istante per istante una o più caratteristiche del segnale portante, sulla base del valore assunto dal segnale modulante. L'operazione inversa, che consiste nell'estrazione del segnale di partenza dal segnale modulato è detta *demodulazione*.

I sistemi RFId utilizzano un segnale modulante di tipo digitale e un segnale portante di tipo analogico. In relazione a ciò le modulazioni più usate sono la ASK, la FSK e la PSK.

ASK (*Amplitude Shift Keying*) [3]
Nella modulazione ASK l'ampiezza della portante sinusoidale è fatta variare in correlazione al segnale modulante digitale. Nel caso più semplice e più comune in corrispondenza dello zero logico il segnale modulato ha ampiezza zero o prossima allo zero, mentre in corrispondenza dell'uno logico ha ampiezza pari a quella della portante non modulata (figura 8). Questo metodo ha il vantaggio di trasmettere dati ad una velocità elevata con grande trasferimento di energia.

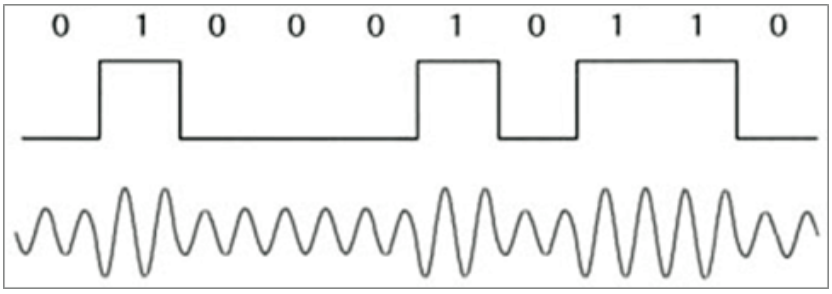


Figura 8: Modulazione ASK.

FSK (*Frequency Shift Keying*) [3]
Nella modulazione FSK l'ampiezza della portante sinusoidale rimane invece costante. Ciò che varia in correlazione al segnale modulante è la frequenza (figura 9). Questo metodo permette di utilizzare un ricetrasmettitore ancora relativamente semplice da realizzare e assicura un alto livello di immunità ai disturbi, ma non consente velocità di trasmissione molto alte.

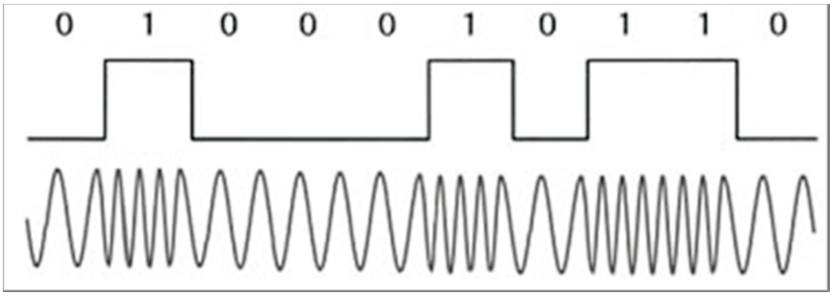


Figura 9: Modulazione FSK.

PSK (*Phase Shift Keying*) [3]
Nella modulazione PSK ampiezza e frequenza della portante sinusoidale restano costanti, mentre è la fase che cambia. Il metodo più semplice consiste nello scambio di fase della portante di 180° in corrispondenza dell'uno logico del segnale modulante (figura 10). Questo metodo assicura un buon livello di immunità ai disturbi e consente velocità di trasmissione elevate, ma richiede un ricetrasmettitore più complesso di quello necessario per il metodo precedente.

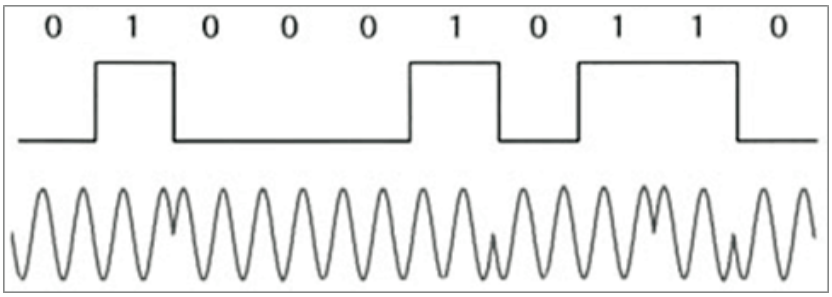


Figura 10: Modulazione PSK.

3.4. Codifica dei dati

La modulazione permette ai dispositivi RFId di trasmettere informazioni digitali per mezzo di onde elettromagnetiche. Negli ambienti in cui avvengono queste trasmissioni, però, spesso ci sono ostacoli che generano riflessioni. Le riflessioni si sommano in modo casuale al segnale, creando disturbi che possono ridurre la probabilità di una corretta interpretazione del segnale ricevuto da parte del circuito di demodulazione. Per evitare tali problemi si ricorre alla codifica dei dati.
Esistono numerosi metodi per effettuare tale codifica.
I più semplici ed i più utilizzati sono: NRZ, RZ, Manchester e Miller.

NRZ (*No Return to Zero*) [3]
Per la codifica NRZ (*No Return to Zero*) valgono le seguenti regole (figura 11):
- Lo stato digitale 1 è rappresentato con un segnale alto;
- Lo stato digitale 0 è rappresentato con un segnale basso.

Circuiti che realizzano tale codifica non sono complicati: i dati passano direttamente in uscita così come sono.
La robustezza agli errori è sufficientemente adeguata, anche se lunghe stringhe di 0 o di 1 possono causare la perdita del sincronismo.

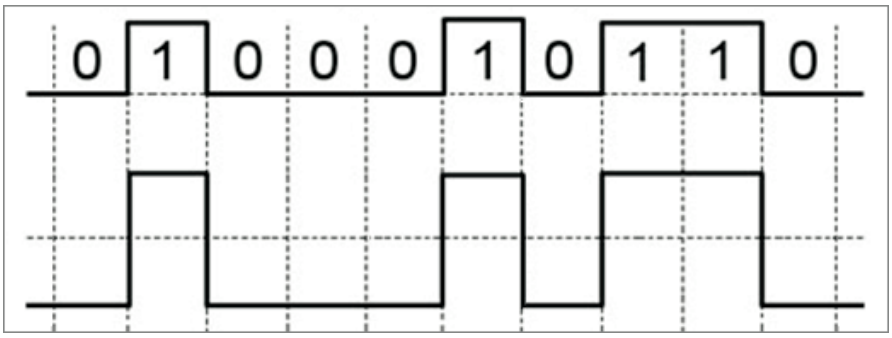


Figura 11: Codifica NRZ.

RZ (*Return to Zero*) [3]
Per la codifica RZ (*Return to Zero*) valgono le seguenti regole (figura 12):
- Lo stato digitale 1 è rappresentato con un segnale alto;
- Lo stato digitale 0 è rappresentato con un segnale basso;
- Ad ogni semiperiodo il segnale torna sempre a zero.

Come con la codifica precedente, non si ha una vera e propria codifica dei dati. Il ricevitore deve però distinguere tra 3 livelli, anziché tra 2, quindi la probabilità di errore è più grande rispetto al caso precedente. Il vantaggio però è che lunghe stringhe di 0 o di 1 non causano la perdita del sincronismo[40].

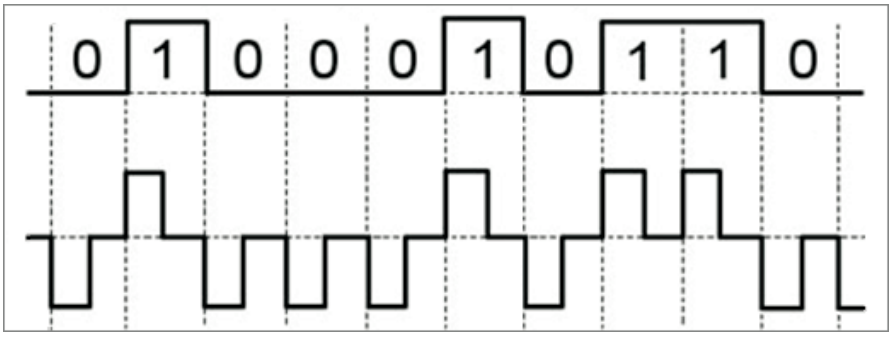


Figura 12: Codifica RZ.

Manchester [3]
Per la codifica Manchester valgono le seguenti regole (figura 13):
- Lo stato digitale 1 è rappresentato con una transizione al semiperiodo fra il segnale alto e il segnale basso;
- Lo stato digitale 0 è rappresentato con una transizione al semiperiodo fra il segnale basso e il segnale alto.

Come con la codifica precedente, anche con tale codifica lunghe stringhe di 0 o 1 non causano la perdita del sincronismo. Tuttavia, lavorando con solo due livelli, la robustezza agli errori è più alta. La codifica Manchester richiede un circuito più complicato rispetto a quelli per le codifiche RZ e NRZ.

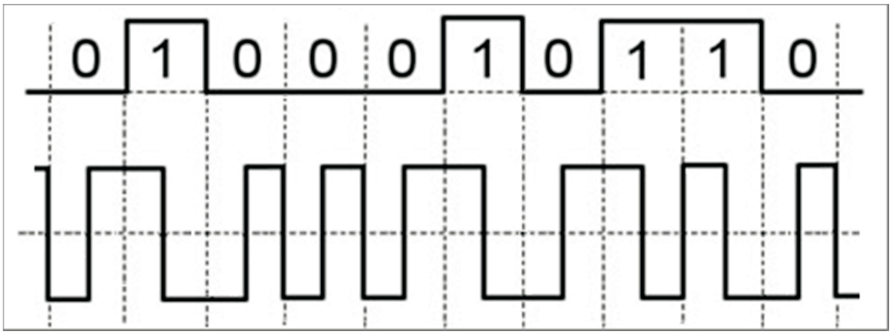


Figura 13: Codifica Manchester.

Miller [3]
Per la codifica Miller valgono le seguenti regole (figura 14):
- Lo stato digitale 1 è rappresentato mantenendo all'inizio del periodo il livello dello stato precedente e attuando una transizione al semiperiodo;
- Lo stato digitale 0 è rappresentato con uno dei due metodi seguenti:
  - Se lo stato precedente era un 1, viene mantenuto il livello per tutto il periodo;
  - Se lo stato precedente era uno 0, si ha una transizione all'inizio del periodo e poi si mantiene il livello costante per tutto il periodo.

Il metodo ha gli stessi vantaggi della codifica Manchester, ma richiede un circuito più complicato che necessita di memoria.

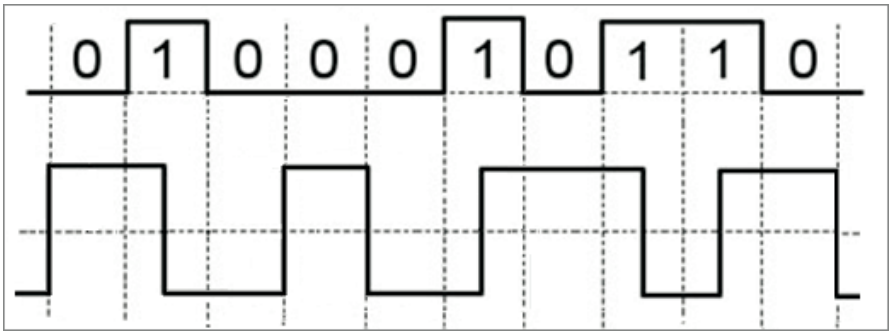


Figura 14: Codifica Miller.

Manchester modificata [3]
La codifica Manchester tradizionale è stata col tempo migliorata per mezzo della modulazione di una sottoportante durante il periodo di segnale basso (come si può notare dalla figura 15).

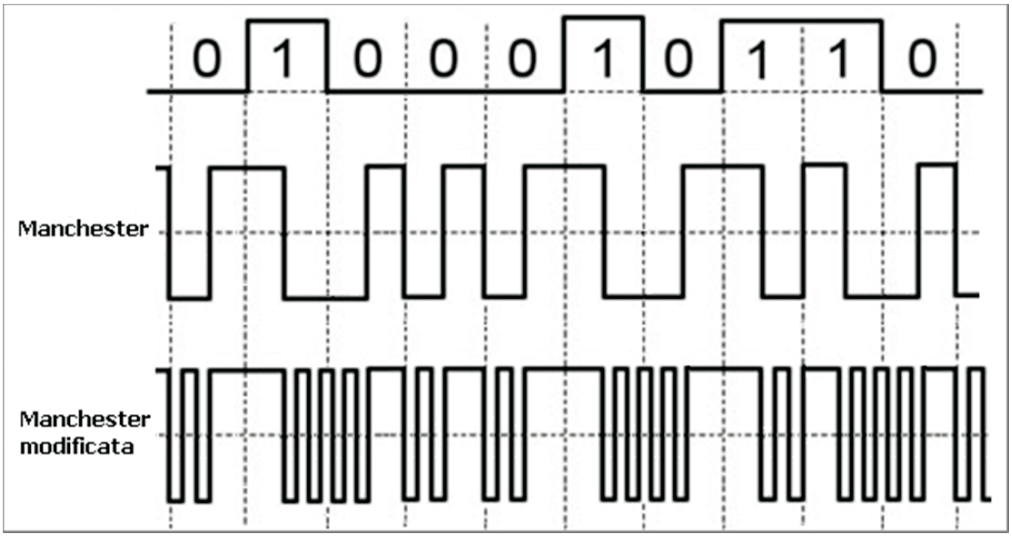


Figura 15: Comparazione tra le codifiche Manchester e Manchester modificata.

Ciò ha aggiunto al metodo caratteristiche interessanti per la comunicazione tra Reader e Tag passivi, in particolare:
- il consumo di energia del Tag è minimizzato;
- si ha la capacità di inviare al Reader un segnale facilmente rilevabile;
- si ha la possibilità di mettere in atto una procedura di anticollisione (del tipo “Carrier Sense”);
- si ha una sincronizzazione automatica tra Reader e Tag.

Miller modificata [3]
La codifica Miller tradizionale è stata migliorata sostituendo la transizione del cambio di livello con un impulso generato da una sottoportante (come si può notare nella figura 16).

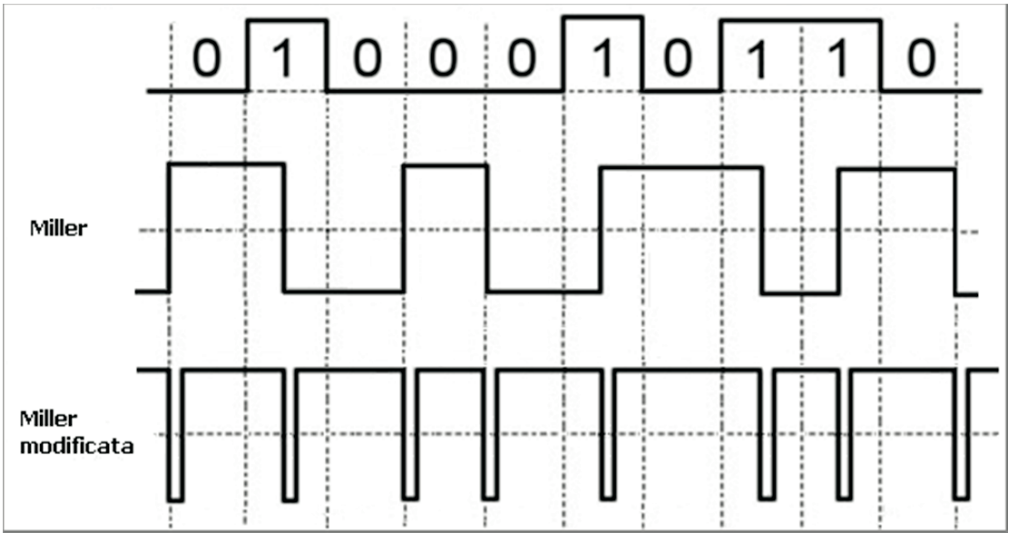


Figura 16: Comparazione tra le codifiche Miller e Miller modificata.

La codifica Miller modificata è molto efficace nella comunicazione tra Reader e Tag per le seguenti ragioni:
- l'energia trasmessa al Tag è massimizzata;
- il rapporto segnale/rumore è minimizzato;
- si ha una sincronizzazione automatica tra Reader e Tag.

La sincronizzazione automatica tra Reader e Tag è importante perché permette di ridurre gli errori di trasmissione in presenza di disturbi e accresce la velocità di trasmissione dei dati, soprattutto per i messaggi brevi. I vantaggi di una trasmissione più sicura sono pagati da una maggiore complessità circuitale del Tag rispetto a quella che si ha con codifiche più elementari.

3.5. Processo di anticollisione

La comunicazione non riesce se due o più Tag cercano di comunicare contemporaneamente. Quando ciò avviene, il messaggio ricevuto dal Reader, essendo la fusione di due o più messaggi è indecifrabile e si parla in tal caso di *collisione*.

Per gestire le collisioni esistono diversi metodi: i più semplici richiedono Tag di complessità circuitale relativamente ridotta, e quindi più economici, a discapito, però, della velocità di lettura.
Per velocità di lettura più alte si usano, invece, Tag più costosi, capaci di compiere le necessarie operazioni più complesse.
I protocolli di anticollisione effettivamente utilizzati nei sistemi RFId cercano di diminuire il più possibile l'attesa.
Esistono due famiglie di protocolli: stocastici e deterministici. Nella famiglia dei protocolli stocastici il momento in cui i Tag possono inviare i dati è scelto in modo casuale, invece nella famiglia dei protocolli deterministici tale momento è calcolato con tecniche precise [7].

Protocolli stocastici [3]
Negli anni '70 è nato il protocollo Aloha, per risolvere il problema della collisione che sorge quando più sorgenti radio, che condividono lo stesso canale di comunicazione, devono inviare ad un nodo centrale pacchetti di informazioni generati a istanti non prevedibili e le sorgenti sono indipendenti e senza la possibilità di comunicare l'una con l'altra. Tutti i protocolli stocastici derivano da tale protocollo.
Quando una sorgente ha qualcosa da trasmettere, lo fa immediatamente ed in caso di collisione attende un tempo casuale prima di ritrasmette i propri dati. In caso di ulteriori collisioni la procedura è ripetuta. In tal modo, il ritardo subito da un pacchetto dal momento in cui è stato inviato fino a quello in cui è ricevuto correttamente è abbastanza limitato.
La stessa situazione si presenta anche nei sistemi RFId: i Tag possono essere immaginati come sorgenti radio ed il Reader come il nodo centrale. In caso di traffico moderato la probabilità di collisione è ridotta e solo di rado si rende necessaria una nuova trasmissione. Viceversa, se il traffico diventa intenso le collisioni crescono e il continuo ingresso di nuovi pacchetti le moltiplica, rendendo il sistema instabile.
Per tale motivo il protocollo Aloha è stato modificato dando luogo a protocolli diversi.
Negli RFId a radiofrequenza le modalità in cui la lettura può avvenire sono due:

- Free access: secondo tale modalità i Tag inviano i propri dati appena entrano nella zona di trasmissione di un Reader e li ritrasmettono fino a che la lettura non va a buon fine;
- Blocked access: secondo tale modalità è il Reader che decide quando interrogare i Tag presenti nella sua zona, questi invia il segnale di inizio lettura che attiva i Tag presenti permettendo loro di partecipare al processo e da quell'istante gli altri Tag che entrano nella zona non sono abilitati a trasmettere.

I protocolli più utilizzati fanno parte tutti della tipologia Blocked access, e possono essere classificati in tre categorie: Pure, Slotted, e Framed (Appendice IV).

I protocolli deterministici [3]
A differenza dei protocolli stocastici, nei protocolli deterministici non esiste un metodo base: essi sono nati ognuno da idee diverse. Tuttavia è possibile attuare una classificazione in due categorie distinte (Appendice V):

- quella dei protocolli totalmente deterministici, cui appartengono i protocolli che risolvono le collisioni basandosi solo sul numero seriale (UId) del Tag;
- quella dei protocolli deterministici con elemento casuale, cui appartengono i protocolli che si servono di un generatore di numeri casuali posto sui Tag.

3.6. Rilevamento e correzione degli errori

Gli errori di trasmissione sono dovuti alla presenza di disturbi sul canale di comunicazione, che impediscono la corretta ricezione dei dati trasmessi. Gli ostacoli che un'onda elettromagnetica incontra durante la sua propagazione possono modificarla e può accadere quindi che dei bit 1 vengano trasformati in 0 e viceversa [3].

Durante la comunicazione possono verificarsi, di solito, tre tipi di errori [8]:

- Errori su un bit singolo (single-bit): coinvolgono un solo bit dell'unità dati il cui valore è trasformato da 1 a 0 o viceversa (figura 17). Tale tipo di errore è molto comune.

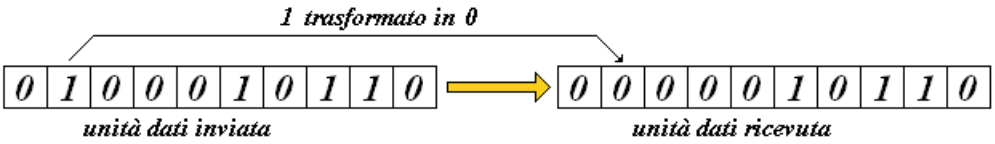


Figura 17: Esempio di errore single-bit.

- Errori su più bit (multiple-bit): coinvolgono due o più bit non consecutivi dell'unità dati, il cui valore è trasformato da 1 a 0 o viceversa (figura 18). Tale tipo di errore è relativamente comune.

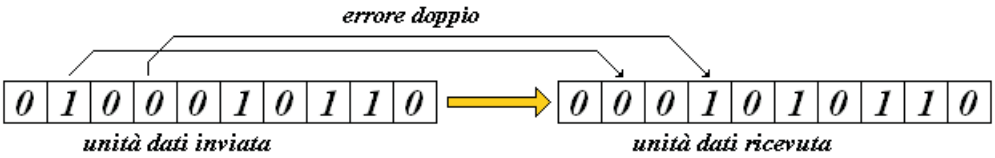


Figura 18: Esempio di errore multiple-bit.

- Errori a raffica (burst): coinvolgono due o più bit consecutivi dell'unità dati, il cui valore è trasformato da 1 a 0 o viceversa (figura 19). Tale tipo di errore non è comune.

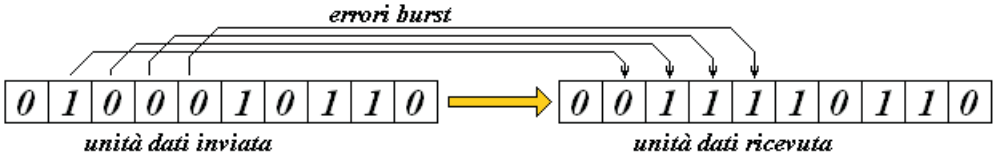


Figura 19: Esempio di errori burst.

Un metodo semplice per l'individuazione degli errori è quello di attuare un doppio invio per ogni unità di dati. Pertanto il ricevitore ha il compito di confrontare bit a bit le due copie della stessa unità. In tal modo, essendo infinitesima la probabilità di incontrare due errori sullo stesso bit, la trasmissione è molto affidabile, ma lenta: il tempo di trasmissione è più che duplicato, essendo necessario aggiungere anche il tempo per la verifica alla doppia durata della trasmissione. Si preferiscono, quindi, altri metodi che si basano sull'aggiunta sapiente di un numero limitato di bit di ridondanza. Appena il sistema ricevente si è accertato della corretta trasmissione, i bit supplementari sono eliminati (figura 20).

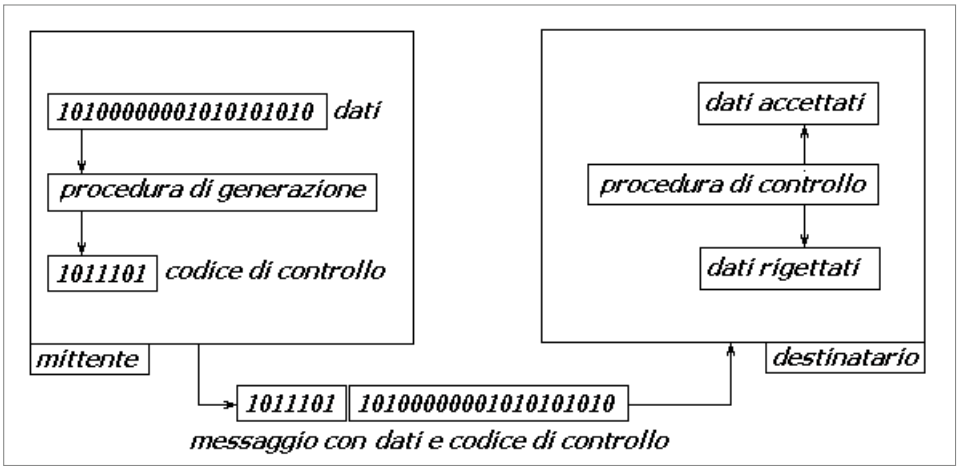


Figura 20: Rilevamento degli errori con l'aggiunta di bit di ridondanza.

Tre sono i principali algoritmi per il rilevamento errori che sfruttano la tecnica di ridondanza [8]:

- VRC (*Vertical Redundancy Check*), LRC (*Longitudinal Redundancy Check*), CRC (*Cyclic Redundancy Check*).
- Il VRC è il metodo più comune per il controllo d'errore: un bit è aggiunto all'u-

nità dati in modo che il numero di bit uguali a 1 dell'intera unità (bit supplementare compreso) sia pari o dispari. Nel primo caso si parla di *parity check* o controllo di parità (figura 21); nel secondo caso si parla di controllo di disparità. L'algoritmo VRC è molto facile da implementare ma ha alcuni limiti, infatti se un'unità ha un numero pari di bit invertiti l'errore non è rilevato.

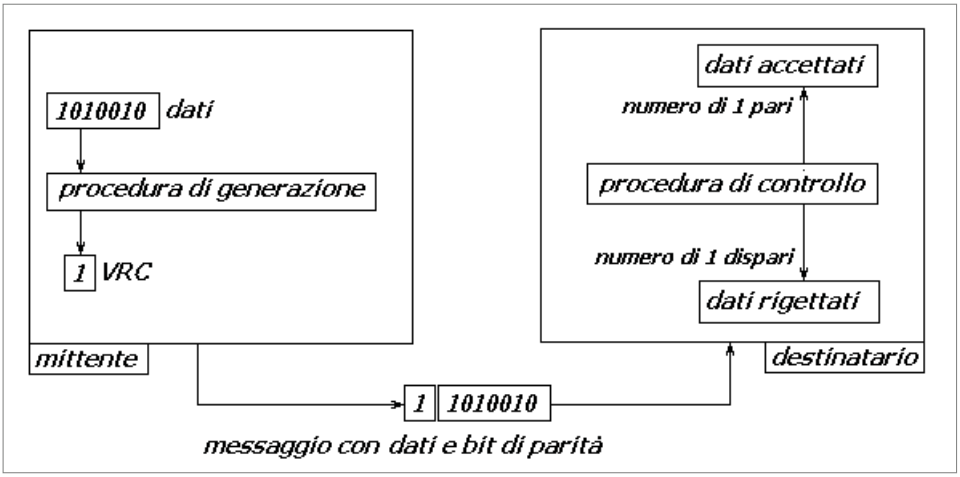


Figura 21: Algoritmo VRC con controllo di parità.

- L'algoritmo LRC è una sorta di VCR bidimensionale. Come nel VCR si ha l'aggiunta del bit di parità ad ogni unità dati, inoltre, ad ogni blocco composto da un numero prefissato di unità è aggiunta una unità supplementare che contiene i bit di parità associati alle sequenze di bit corrispondenti del blocco (figura 22). L'algoritmo LRC assicura maggiore affidabilità nell'individuazione degli errori di tipo multiple-bit e burst, ma può essere tratto in inganno da trasposizioni di byte.

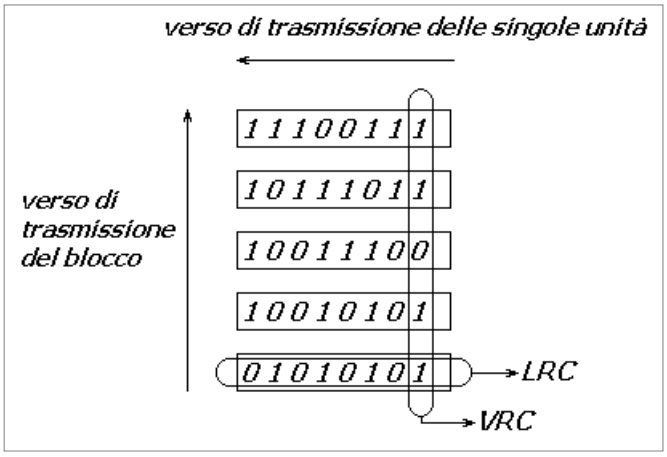


Figura 22: Algoritmo LRC.

- Nel metodo CRC i dati aggiunti ad ogni unità corrispondono al resto ottenuto dalla divisione dell'unità per un polinomio opportuno (detto *generatore*), di lunghezza dipendente dalla lunghezza dell'unità. Ad esempio, il generatore di un'unità lunga 9 bit potrebbe essere il polinomio $x^8 + x^5 + x^4 + x^3 + 1$, corrispondente all'unità 100111001. Il metodo CRC è molto affidabile nella trasmissione dei dati ed è utilizzato anche nei sistemi di registrazione su hard disk.

Quanto discusso finora riguarda il rilevamento degli errori, perché sia possibile la correzione è necessario aumentare il numero di bit di ridondanza, ciò soprattutto se sono previste comunicazioni con errori multipli o a raffica. Tuttavia una lunghezza eccessiva dell'unità dati, con conseguente riduzione della velocità di trasmissione è da evitare. Per questo, se sono rilevati errori, si preferisce, a seconda della complessità dell'algoritmo scelto e del tipo di errore, la ritrasmissione totale o parziale dell'unità in cui gli errori sono stati rilevati.

3.7. Sicurezza della comunicazione

In alcune applicazione può essere necessario garantire la sicurezza (security) della comunicazione tra Reader e Tag e ciò può essere fatto con metodi differenti, in funzione del grado di sicurezza richiesto.
Infatti è possibile:

- l'utilizzo di una password che permetta di identificare il Reader e il Tag (la password di identificazione del Reader può essere unica per tutti i Tag o specifica per ogni Tag), chiaramente l'adozione di numerose password rende più complesso l'utilizzo del sistema RFId;
- la codifica delle trasmissioni attraverso *chiavi* o polinomi o l'utilizzo di veri e propri sistemi di crittografia, naturalmente ciò ha un costo maggiore e riduce la velocità di comunicazione.

L'utilizzo di crittografia è limitato dalle leggi nazionali sulla sicurezza pubblica che impongono la possibilità di lettura da parte delle forze di Polizia, su richiesta delle autorità competenti.
Tra le applicazioni RFId che richiedono maggiore sicurezza vi sono le carte di credito *contactless* (in sostituzione di quelle *a strisciata*). Per eseguire il pagamento con tali carte è sufficiente avvicinare una carta dotata di Tag al POS dotato di Reader.

4. RFId in applicazioni di sicurezza

4.1. Uso in applicazioni di sicurezza

I Tag possono essere stampati o inseriti in oggetti di forma diversa (come ad esempio un badge identificativo) e quindi personalizzati con stampe di immagini, scritte, loghi, fotografie e codici a barre. Sui Tag possono essere registrate informazioni come: dati anagrafici, foto di riconoscimento, data e ora di transito, verso di transito e altre informazioni.
Prima di utilizzare un sistema RFId come parte di un sistema di controllo per un'applicazione di sicurezza, occorre conoscerne a fondo il funzionamento e comprendere il modo migliore per il suo impiego.
Un sistema RFId non può essere usato come barriera immateriale.
Una simile barriera è usata in un sistema di comando di una macchina per impedire l'accesso a zone pericolose. Il dispositivo entra in funzione quando un raggio ottico è interrotto dal passaggio di oggetti o parti del corpo di una persona. In pratica, nell'istante in cui il raggio è interrotto, il sistema di comando conosce la posizione di chi lo sta interrompendo, nell'intervallo di tempo che precede tale evento la barriera assume che non sussista nessuna situazione di pericolo, mentre vi è una probabilità non nulla che nell'intervallo di tempo successivo a tale evento possa presentarsi una situazione di pericolo, allora il sistema di comando avvia azioni che portano la macchina in uno stato sicuro.
Un sistema RFId non può conoscere la posizione di alcunché cui non sia stato in precedenza associato un Tag (riconosce la presenza del Tag all'interno della propria zona operativa). Per tale motivo non può mettere in sicurezza la macchina se eventuali soggetti sprovvisti di Tag entrano nella zona operativa del Reader, al limite potrebbe avviare azioni solo se soggetti che indossano un Tag entrano in tale zona operativa. Un tale uso non è sicuro in una barriera.
Viceversa un sistema RFId funziona molto bene per consentire l'accesso ad una zona pericolosa a persone che siano autorizzate (ad esempio dotate di Tag), quindi come chiave, o per consentire l'attivazione di taluni dispositivi (ad es.: un'attrezzatura di lavoro) solo da parte di un operatore noto (che indossi un Tag).
Anzi da questo punto di vista ha anche funzionalità superiori, in quanto il Tag è dotato di un identificativo, per cui può essere messa in atto una gerarchia di autorizzazioni. Ad esempio alcuni soggetti possono essere autorizzati ad accedere a

talune zone ed altri a zone diverse, oppure alcuni soggetti possono sbloccare alcune modalità di funzionamento di un'attrezzatura di lavoro, come il "modo di manutenzione", e altri no, e così via.
In molte applicazioni non è possibile utilizzare il sistema RFId come sicurezza principale, poiché protegge solo chi porta un Tag, ma è possibile utilizzarlo come sicurezza addizionale.
Infatti è più semplice (e naturale) il suo uso come "chiave" o come utensile per disattivare una barriera di sicurezza, o nel caso si debba accedere a qualche modalità operativa particolare (ad esempio: "modo di manutenzione", modo di addestramento", ecc.).

4.1.1. Uso come blocco di sicurezza aggiuntivo

In alcuni casi è ipotizzabile che si permetta il funzionamento di una macchina o apparecchiatura solo in presenza di operatori di macchina (es. una pressa o una TAC o altro). Tali attrezzature possono richiedere particolari procedure per assicurare la sicurezza propria o delle persone, impedendo ai non autorizzati il proprio utilizzo o arrestando il funzionamento se nell'area di lavoro non sia presente un operatore autorizzato.
Durante la manutenzione o altre operazioni (ad esempio l'addestramento) una macchina può azionare gli attuatori, spesso in modalità controllata (ad esempio con una velocità inferiore). Però anche in modalità controllata può sussistere un rischio residuo non trascurabile, soprattutto se ad avvicinarsi alla macchina possono essere soggetti terzi che non hanno niente a che fare con l'attività in corso.
Quando si presentano tali situazioni può essere in favore della sicurezza se il funzionamento degli attuatori, eventualmente in modalità controllata, possa essere attivato solo quando il personale autorizzato ad operare in quella particolare modalità (il manutentore, l'addestratore, ecc.), dotato di Tag, sia presente vicino alle parti in movimento.
Per tornare al funzionamento normale, invece, è preferibile essere certi della lontananza dalle parti pericolose del personale che prima si trovava ad operare all'interno della zona pericolosa (blocco di sicurezza che si disattiva solo quando il Reader non rileva più il Tag all'interno della sua zona operativa).
Si noti che, in quest'ultimo caso, il sistema RFId si comporta come una protezione aggiuntiva (infatti non è in grado di rilevare presenza o assenza di soggetti non dotati di Tag) che non dovrebbe esimere dall'uso di interblocchi o di ripari apribili solo con un utensile e da un consenso volontario per la riattivazione del funzionamento normale dell'attrezzatura di lavoro.

4.1.2. Uso come interblocco di sicurezza

I dispositivi di interblocco di un riparo di una macchina sono costituiti da un inter-

ruttore di posizione e da un attuatore che, all'apertura del riparo, aziona l'interruttore di posizione. Sono suddivisi dalla norma ISO 14119 [31] in 4 tipologie. Gli interblocchi di Tipo 4 "elettronici ad azionamento senza contatto con attuatori codificati" possono funzionare con attuatori magnetici, RFId o ottici.
In questo caso i sistemi RFId costituiscono l'attuatore che aziona l'interruttore di posizione quando il riparo è chiuso.
I sistemi RFId resistono agli urti ed alle vibrazioni e permettono elevate tolleranze di allineamento. Sono messi in commercio come sottosistemi con PFHD (probability of dangerous failure per hour - probabilità oraria di malfunzionamento pericoloso [32]) molto bassa (ad esempio tra 10^{-9} e 10^{-11} 1/h) ed alcuni hanno un sistema di test diagnostici integrato.

4.1.3. Uso come chiave di accesso ad un cantiere

Un sistema RFId può essere usato per consentire l'accesso in un cantiere, solo al personale che indossi i prescritti DPI: ad es. integrando opportuni Tag passivi su ogni DPI e posizionando all'ingresso del cantiere un Reader, in modo che l'accesso sia possibile solo a quei soggetti che presentino in ingresso la completezza della dotazione dei DPI.
Lo stesso discorso può essere applicato se il cantiere è suddiviso in zone ed in ogni zona vi è una prescrizione specifica per la dotazione di DPI, i Reader all'ingresso di ogni zona possono determinare se si hanno tutti i DPI necessari perché l'accesso sia consentito a quella particolare zona.
È possibile che i Tag associati a DPI dello stesso tipo abbiano lo stesso codice identificativo, tuttavia, data la versatilità dei sistemi RFId, è possibile che ciascun DPI abbia un codice identificativo univoco, che permetta di associarlo in via esclusiva ad un unico possessore. In tal caso è possibile conoscere istante per istante chi si trova all'interno di una zona specifica e se sta indossando i DPI previsti.
Alcune attrezzature di lavoro (dotate di Reader) potrebbero essere rese non attivabili se l'operatore non possiede particolari autorizzazioni e/o non indossa specifici DPI, e la verifica può essere fatta dal sistema di gestione dell'RFId (per mezzo dell'attivazione di un opportuno applicativo) sulla base del fatto che i DPI indossati (dotati di Tag univoco) sono esclusivi di uno specifico operatore.
Addirittura è possibile che terminali portatili svolgano sia la funzione di Reader per Tag passivi associati ai DPI (il Reader, indossato permanentemente dal soggetto che deve essere protetto dai DPI, può avvertire il lavoratore se questi dimentica o perde un DPI), sia la funzione di Tag attivo per un sistema di localizzazione tridimensionale dei lavoratori all'interno del cantiere.

4.1.4. Uso per la localizzazione dei lavoratori

L'RFId è una valida alternativa sia alle tecnologie di personal identification tradizio-

nali (badge, tesserini, ecc.), sia alle tecnologie basate sul riconoscimento degli attributi biometrici di un individuo. A differenza di tali tecnologie permette il riconoscimento anche "a distanza". L'identificazione tramite RFId distingue gli ingressi dalle uscite e verifica automaticamente l'elenco delle presenze all'interno di una determinata zona, permette l'avvio o l'arresto di dispositivi a seconda che il proprietario si trovi o meno nelle vicinanze.
Un sistema RFId che utilizzi Tag attivi può essere usato per realizzare una funzione di localizzazione tridimensionale dei lavoratori all'interno del luogo di lavoro (in presenza di almeno quattro Reader posizionati in modo da non giacere tutti sullo stesso piano).
Il sistema di localizzazione tridimensionale può essere utile per facilitare le operazioni di emergenza (ad esempio la localizzazione di un lavoratore disperso durante le fasi dell'esodo, quest'ultima funzione è facilitata dall'esistenza di un archivio storico dei dati, che permettere di rintracciare, presso l'ultima posizione registrata, il lavoratore disperso).

4.1.5. Uso come DPI aggiuntivo

Un sistema RFId può essere usato per bloccare il funzionamento di attrezzature in caso di caduta di operatori attraverso aperture al di là delle quali vi siano organi in movimento.
È questo il caso, ad esempio, di trebbiatrici, mietitrici, pompe idrovore, macchine per trucioli.
In tali attrezzature fieno, graminacee, sostanze liquide, legno entrano da un apposito ingresso durante il normale funzionamento. Tuttavia se avviene l'ingresso accidentale di un operatore è necessario fermare gli organi in movimento.
Al fine di proteggere tempestivamente gli operatori è possibile ricorrere ad un sistema RFId. I Tag passivi devono essere integrati sui vestiti o su fasce da indossare agli arti, al collo e al bacino, mentre il Reader è posto in corrispondenza dell'apertura la quale deve trovarsi a distanza sufficiente dalle parti in movimento (la zona operativa del Reader coincide con l'ingresso dell'attrezzatura).
Anche questa non è una sicurezza principale ma addizionale, infatti ha l'inconveniente di proteggere solo gli operatori che indossano i Tag e non eventuali terze persone.

4.1.6. Uso come inventario di sicurezza

Un sistema RFId può essere usato per controllare che alla fine di un certo lavoro, tutte le attrezzature di lavoro, dotate di Tag, rientrino negli appositi contenitori, dotati di Reader.
Un'applicazione può essere quella della localizzazione di un utensile o un'attrezzatu-

ra di lavoro, con particolare riguardo agli utensili e alle attrezzature la cui localizzazione potrebbe avere ricadute sulla sicurezza (ad esempio attrezzature pericolose). Ciò può essere ottenuto facendo in modo che alle entrate/uscite dai locali vi sia un Reader e sull'utensile o sull'attrezzatura vi sia un Tag.
L'applicazione tipica è quella del controllo dell'inventario degli utensili a fine lavoro, durante operazioni di lavoro svolte fuori sede o durante operazioni per cui sia importante (eventualmente per motivi economici) tale controllo: dei Tag passivi sono sistemati sugli utensili, un Reader in corrispondenza del contenitore degli utensili può segnalare a fine lavoro se qualche utensile non è stato riposto (indicando anche quale, grazie all'identificatore del Tag). Eventualmente un Reader mobile può essere passato sulla zona di lavoro per individuare gli utensili dispersi.
Un tale sistema non serve ad evitare l'adozione di procedure di qualità per il tracciamento degli utensili, ma può servire per accelerare le operazioni di inventario.
Il sistema RFId è utile per ricostruire anche la storia dell'utensile o dell'attrezzatura di lavoro in quanto, in un database aggiornato sulla base dei dati ricevuti dai Reader possono essere conservate informazioni su manutenzioni, verifiche ecc., che possono poi essere inviate sul terminale (telefonino, palmare o altro) dell'utilizzatore dell'utensile o dell'attrezzatura (il terminale può essere a sua volta dotato di Reader o di lettore di etichette o di q-code).
Interessante è l'applicazione di sistemi RFId nella manutenzione degli impianti chimici, dove si effettuano manutenzioni sulle valvole. Con una semplice lettura del Tag applicato direttamente su una specifica valvola può essere possibile ottenere la storia delle manutenzioni e riparazioni cui è stata sottoposta.

4.1.7. Rilevazione dei parametri ambientali

Una particolare applicazione dei sistemi RFId riguarda l'uso di Tag attivi equipaggiati con sensori in grado di rilevare i parametri climatici (temperatura, pressione, umidità, ecc.) dell'ambiente in cui sono immersi.
I parametri rilevati sono memorizzati in un'apposita memoria interna, fino a quando non sono scaricati da un operatore, dotato di apposito lettore.
In particolari realtà industriali, dove è necessario garantire regimi ambientali operativi controllati, i Tag, grazie alle dimensioni ridotte, possono essere collocati in punti scomodi delle attrezzature, dove è difficile portare il cavo necessario ad alimentare un apparecchio di misura, ed offrono, a costi contenuti, una soluzione affidabile e facilmente realizzabile.
Un'applicazione relativa alla catena del freddo è volta a controllare e mantenere a temperatura adeguata i prodotti durante le fasi della distribuzione (trasporto, immagazzinamento, allocazione presso i punti vendita) fino al momento della consegna, al fine di garantirne integrità e qualità.
I Tag incorporano un sensore di temperatura. Esistono due tipi di sensori: il primo tipo registra il picco della temperatura l'uscita da intervalli di temperatura prede-

finiti, il secondo tipo, invece, opera in modo continuo, monitorando nel tempo la temperatura. Anche per i sensori che operano in modo continuo è possibile programmare gli intervalli di misurazione della temperatura e memorizzarne i valori, in modo da ottenere un grafico nel tempo oppure identificare il momento (time stamp) di uscita dagli intervalli.
Il tipo di sensore utilizzato e la quantità di memoria necessaria influenzano il costo dei Tag.
Essendo Tag ad alto costo, e non quindi a perdere, occorre valutare anche il costo della logistica di rientro.
Grazie all'utilizzo di tali sistemi si può monitorare lo stato di conservazione di una sostanza senza aprire le confezioni e gestendo il dato per via informatica, prendendo centralmente le decisioni necessarie:

- eliminare il prodotto, o
- accelerare il trattamento di un processo, o altro.

5. Applicazioni mediche

5.1. Braccialetti RFId per l'identificazione e la localizzazione dei pazienti

È possibile associare un Tag passivo RFId ad un paziente per mezzo di un braccialetto.
Il numero contenuto nel Tag permette l'identificazione del paziente, la memorizzazione dei suoi dati e la sua localizzazione all'interno dei locali della struttura sanitaria.
L'identificazione positiva del paziente è utile per ridurre gli errori medici ospedalieri evitabili (ad esempio le disgrazie causate dall'uso improprio di medicinali sui ricoverati, i rischi di interventi chirurgici nelle sedi sbagliate sul paziente sbagliato, i rischi di trattamenti medici errati, ecc.).
Simili errori, oltre che influire direttamente sulla salute e la sicurezza degli interessati, hanno un costo per il servizio sanitario e per la collettività.
Per questo motivo i gruppi regolatori per l'assistenza sanitaria massima negli Stati Uniti hanno sviluppato il concetto delle "cinque regole della sicurezza medica": paziente giusto, medicina giusta, dosaggio giusto, percorso sanitario giusto e momento giusto.
L'identificazione non manuale del paziente per mezzo di braccialetti non trasferibili consente una serie di benefici:

- aiuta a migliorare l'efficienza del sistema (migliora la comunicazione e riduce gli errori di raccolta e immissione dei dati);
- aumenta la sicurezza del paziente, aiutando a realizzare la filosofia delle "cinque regole della sicurezza medica";
- la tecnologia consente un accesso veloce ai dati ed alla scheda clinica del paziente memorizzati all'interno del sistema informativo (per operazioni di lettura/scrittura e trasferimento);
- l'esecuzione della lettura è più veloce rispetto alla lettura di un codice a barre;
- a differenza dei codici a barre, la lettura può essere effettuata attraverso ed intorno al corpo umano, gli abiti, le coperte dei letti ed i materiali non metallici, senza disturbare il paziente;
- i Tag forniscono maggiore sicurezza sui codici a barre, che sono facili da copiare e da duplicare;
- esistono stampanti/programmatori a trasferimento termico per la stampa e la programmazione a richiesta dei braccialetti;

- posizionando dei Reader all'ingresso dei locali della struttura è possibile un approssimativo tracking del paziente.

5.2. Sistemi per la localizzazione di apparecchiature, pazienti e personale sanitario

Perché limitarsi alla sola identificazione del paziente, quando è possibile realizzare un approssimativo sistema di tracking, posizionando dei Reader all'ingresso dei locali della struttura sanitaria?
Una volta realizzato il sistema di tracking, perché limitarsi alla localizzazione dei soli pazienti, quando è possibile mettere dei Tag adesivi sulle apparecchiature (inclusi gli elettromedicali) o gli stessi tesserini identificativi del personale possono contenere dei Tag?
Realizzando il sistema di tracking (figura 23) sono possibili le seguenti funzionalità, che integrano ed estendono quanto già illustrato nel paragrafo precedente:

- localizzazione dei pazienti e stato del trattamento medico prescritto;
- gestione di eventuali casi acuti che dovessero presentarsi;
- registrazione della durata della permanenza di un paziente all'interno del Pronto Soccorso, del tempo speso all'interno dei reparti, del tempo speso in sala operatoria, del tempo totale di permanenza nella struttura sanitaria fino alla dismissione;
- l'analisi statistica periodica dei dati di pazienti con patologie simili registrati in tal modo nell'archivio storico della struttura sanitaria può permettere di migliorare la gestione dei pazienti e di verificare il raggiungimento di opportuni obiettivi di qualità;
- localizzazione degli elettromedicali all'interno dei locali della struttura sanitaria e loro individuazione in tempo reale;
- gestione delle emergenze (localizzazione dei pazienti e del personale sanitario durante le emergenze, incluso l'eventuale esodo);
- apposizione di Tag alle cartelle cliniche dei pazienti, in modo da evitare errori nella compilazione o lo smarrimento o lo scambio delle stesse;
- apposizione di Tag ai farmaci per la loro localizzazione;
- localizzazione dei lavoratori (personale medico, infermieristico e altri lavoratori) e dei pazienti all'interno delle strutture sanitarie per il trattamento delle malattie infettive, allo scopo di individuare e circoscrivere eventuali trattamenti necessari in caso di violazione del contenimento degli agenti patogeni.

L'ultimo uso possibile evidenziato mostra che a volte quella che può essere vista come una parziale rinuncia alla privacy potrebbe permettere di restringere i costi di trattamenti sanitari di emergenza in casi di quarantena (riducendo il numero delle persone che vi si debbono sottoporre).

Figura 23: Possibile posizione del Reader e situazione dei Tag in una sala operatoria.

5.3. Tracciamento dei ferri chirurgici in sala operatoria

Un'applicazione tipica può essere quella del controllo dei ferri chirurgici in una sala operatoria: dei Tag passivi sono sistemati sui ferri chirurgici, un Reader in corrispondenza del contenitore dei ferri può segnalare a fine operazione se qualche ferro non è stato riposto (indicando anche quale, grazie all'identificatore del Tag). Inoltre un Reader mobile può essere passato sul paziente appena operato per verificare che non siano rimasti ferri al suo interno dopo l'operazione.
Potrebbero esistere anche Tag certificati per essere posizionati sulle garze e sulle bende (a distanze prestabilite).
Un tale sistema non serve ad evitare l'adozione di procedure di qualità per il tracciamento dei ferri chirurgici e delle garze, ma può servire per avere un'informazione tempestiva (conoscere in tempo reale) sulla permanenza di corpi estranei all'interno del paziente.

5.4. Utilizzo di dispositivi attivi

In ambiente ospedaliero potrebbe essere utile usare anche dispositivi attivi.
Ad esempio è possibile ricorrere a dispositivi attivi per tracciare con precisione la posizione delle apparecchiature più costose o spostate di continuo, e utilizzare i dispositivi passivi solo per quelle apparecchiature meno costose per cui non è necessaria una localizzazione più precisa dell'identificazione della stanza.
Inoltre è possibile ricorrere ai dispositivi attivi, anche per il monitoraggio dei parametri vitali del paziente o per il monitoraggio delle terapie, ad esempio è possibile utilizzare:

- Tag attivi per il monitoraggio di parametri vitali (pressione del sangue, battito cardiaco, glicemia);
- Tag attivi per il monitoraggio di dispositivi impiantabili attivi (pacemaker, dispo-

sitivi per l'udito, dispositivi per la vista, dispositivi per il rilascio periodico di medicinali);
- Tag attivi per il monitoraggio delle condizioni ambientali cui il paziente è sottoposto.

L'uso delle tecnologie di monitoraggio può permettere un'estensione dei trattamenti e delle cure che possono essere somministrati presso l'abitazione del paziente, permettendo la riduzione dei costi di ospedalizzazione.
Ciò può essere utile soprattutto nel caso di pazienti cronici, di persone con ridotta mobilità, di persone anziane, di neonati. Per tali soggetti possono essere sufficienti Reader posizionati presso le abitazioni e collegati in rete col sistema informativo dell'azienda sanitaria, che sarebbe così in grado di registrare i dati monitorati.
I medici potrebbero accedere a tali dati a distanza, verificando la correttezza dei trattamenti e lo stato di salute dei pazienti.

5.5. Precauzioni nell'applicazione ai locali medici

In un ambiente sanitario le tecnologie wireless (RFId, Wi-Fi, Bluetooth, ZigBee, UWB) potrebbero essere una fonte di pericolo in quanto potenzialmente in grado di interferire con il funzionamento di dispositivi sensibili. Ciò potrebbe condurre a limitazioni d'uso variabili a seconda della tecnologia e dell'applicazione specifica.
Tuttavia studi e sperimentazioni possono essere condotti caso per caso in modo da trovare soluzioni sicure che permettano di non rinunciare alle ricadute positive delle nuove tecnologie.
Ad esempio sistemi RFId che ad una sperimentazione preliminare dovessero risultare in grado di interferire con dispositivi sensibili potrebbero essere mantenuti lontano da tali dispositivi piazzando i Reader nei luoghi dove la tecnologia è effettivamente utilizzata (stanze di servizio, porte che separano le ali dei vari reparti, porte delle stanze), che distino sufficientemente dai luoghi dove i dispositivi sensibili operano (le zone delle stanze di degenza, delle stanze di terapia intensiva, delle sale operatorie, dove sono le postazioni dei pazienti).

5.6. Soluzioni impiantistiche

Nei locali medici, ma anche in officine o altri ambienti di lavoro, possono aversi impianti di alimentazione con caratteristiche diverse all'interno dello stesso locale. Tali impianti servono ad alimentare utilizzatori che necessitano in modo specifico delle caratteristiche diverse.
Esistono molteplici soluzioni per fare in modo che le spine degli utilizzatori siano connesse nelle prese corrette: un codice di colori per prese e spine, prese e spine non intercambiabili, ecc.

I sistemi RFId possono essere d'ausilio anche in questo caso, fornendo un servizio dalle caratteristiche di sicurezza superiori, associando dei Tag (passivi) alle spine e dei Reader alle prese.
In tal modo il Reader può rilasciare il consenso per l'attivazione dell'alimentazione solo se la spina è stata inserita nella presa corretta. Inoltre è possibile riconoscere quando un utilizzatore è connesso all'alimentazione e monitorare i suoi consumi.
I dati dell'assorbimento di corrente e della tensione fornita possono essere immagazzinati in un database centralizzato, che può permettere così di risalire ai motivi dei malfunzionamenti degli utilizzatori per cause di alimentazione.

5.7. Uso per applicazioni di telemetria

Un sistema RFId basato su Tag attivi può essere usato per applicazioni di telemetria. I Tag attivi possono trasferire, oltre all'indicazione di presenza e posizione, anche alcuni dati biometrici (ad es.: pressione arteriosa, temperatura, battito cardiaco, elettrocardiogramma, elettroencefalogramma, dati accelerometrici) che potrebbe essere necessario monitorare per il controllo dello stato di salute di taluni pazienti o, al di fuori degli ambienti sanitari, durante applicazioni lavorative particolari.

6. Uso di un sistema RFId

6.1. Progettazione di un uso per un sistema RFId

Progettare l'uso di sistema RFId richiede una serie di passi.
Innanzi tutto devono essere chiare e ben specificate le finalità e le ragioni del ricorso al sistema RFId:

- Le finalità sono legate ai vantaggi che si intendono perseguire, ed è preferibile che siano espresse come specifica formale (tale specifica è bene che sia sottoposta ad un'analisi di coerenza e consistenza da parte di un soggetto esperto nell'uso dei sistemi RFId, in alternativa tale soggetto può redigere la specifica dopo un'intervista al committente del futuro sistema RFId, mirata ad appurare i risultati che si intendono ottenere);
- Le ragioni del ricorso sono, di solito, legate ad una serie di analisi comparative costi/benefici con altre tecnologie con cui si potrebbero realizzare le stesse finalità (se è più conveniente realizzare la stessa finalità con un'altra tecnologia più economica, allora è inutile l'uso degli RFId), tali analisi però devono tener conto anche dei possibili sviluppi futuri (taluni sistemi potrebbero non essere economicamente convenienti durante una prima fase di utilizzo, ma potrebbero divenirlo in una fase successiva con l'aggiunta di ulteriori funzionalità) e dell'eventuale esclusività (alcune funzionalità potrebbero essere realizzabili solo con la tecnologia RFId).

Per una migliore progettazione occorre tener presenti anche alcune caratteristiche degli RFId:

- il funzionamento si basa su caratteristiche fisiche ben definite (campi magnetici, in bassa frequenza, campi elettromagnetici, in alta frequenza);
- i Tag operanti in bassa frequenza hanno minori distanze operative e minori velocità di lettura; i Tag operanti in alta frequenza hanno maggiori distanze operative e maggiori velocità di lettura (ciò comporta che ai Tag operanti in alta frequenza siano riservate maggiori dotazioni di memoria o di funzionalità di sicurezza);
- il segnale è in grado di passare attraverso molti materiali, con l'eccezione dei metalli, inoltre si hanno attenuazioni importanti con i liquidi (acqua, alcool);
- vi è la possibilità di una lettura simultanea di più Tag;

- i Tag hanno di solito un formato piatto (etichetta, tesserino);
- allo stato attuale della tecnica, la progettazione dei Tag è relativamente semplice e la loro produzione è alquanto economica.

6.2. Scelta del sistema RFId

Una volta presa la decisione di ricorrere alla tecnologia RFId ed una volta nota la specifica formale delle finalità che si intendono ottenere si può procedere alla scelta del sistema da utilizzare.

Una serie di parametri devono essere valutati:
- standard trasmissivo adottato (variabile con la frequenza e con l'uso del sistema RFId):
  ⇒ 125/134 kHz (ISO11784/85) bassa frequenza;
  ⇒ 13,56 MHz (ISO15693, ISO14443) alta frequenza;
  ⇒ 868/915 MHz (EPC) frequenza ultra-alta;
- tipo di sistema:
  ⇒ passivo (in grado do ricavare energia dal campo magnetico incidente, ciò significa che i suoi Tag sono molto piccoli ed economici);
  ⇒ semi-attivo;
  ⇒ attivo;
- consumo di potenza:
  ⇒ periodicità di interrogazione dei Tag;
  ⇒ durata delle batterie dei Tag (se attivi o semi-attivi);
- distanza operativa (dipende dallo standard trasmissivo adottato e dalla passività o meno dei Tag);
  ⇒ prossimità (<10 cm);
  ⇒ vicinanza (<1 m);
  ⇒ lunga distanza (>1 m);
- dimensioni:
  ⇒ dimensione massima del Reader;
  ⇒ dimensione massima delle antenne;
  ⇒ dimensione massima dei Tag;
- materiali:
  ⇒ influiscono sulle prestazioni delle antenne;
  ⇒ alcuni come l'acqua interferiscono maggiormente al crescere della frequenza;
  ⇒ le strutture e gli ambienti metallici sono fonti di riflessioni e interferenze;
- tipo di involucro:
  ⇒ materiale dell'involucro(vetro, etichetta cartacea, scheda di plastica, altro);
  ⇒ possibilità di sovrastampa;
  ⇒ impermeabilità;
  ⇒ protezione da agenti chimici;

- memoria dei Tag:
  ⇒ dimensione [incluso l'UId (serial number)];
  ⇒ riscrivibilità dei Tag [R/W (Read/Write)];
  ⇒ riscrivibilità del programma del Tag [OTP (One Time Programmable) o altro];
  ⇒ multipage (pagine indipendenti);
  ⇒ segmentation/file structure;
  ⇒ durata (tempo di ritenzione dei dati memorizzati, che, anche per i Tag attivi, può essere slegata dalla durata delle batterie);
- funzionalità integrate e programmabilità:
  ⇒ tipo e quantità delle funzionalità operative già integrate nel sistema di gestione dei Reader;
  ⇒ possibilità di programmare nuove funzionalità operative.
- funzioni di sicurezza (security):
  ⇒ comunicazione non protetta;
  ⇒ lettura o scrittura protette da password;
  ⇒ autenticazione mutua;
  ⇒ comunicazione criptata;
  ⇒ autenticazione mutua con comunicazione criptata e lettura/scrittura protette da password;
- scala del sistema
  ⇒ quantità/costo dei Reader
  ⇒ quantità/costo dei Tag

il costo dei Tag incide anche sulla decisione di riutilizzo dei Tag stessi;

- altri requisiti:
  ⇒ robustezza dei Tag;
  ⇒ modalità di rilevamento anticollisione;
  ⇒ intervallo di temperature per l'operatività;
  ⇒ esperienza di sistemi radio (LF, HF, UHF) del progettista;
  ⇒ uso dell'involucro del Reader normalmente fornito dal fabbricante o sviluppo di un involucro con una forma appropriata.

6.3. Un esempio

6.3.1. Elenco delle funzionalità richieste

A titolo di esempio è possibile considerare un sistema per la localizzazione di apparecchiature, pazienti e personale sanitario, simile a quello descritto nel precedente paragrafo 5.2.
Il sistema deve permettere la localizzazione limitatamente al locale al cui interno si trova il Tag cercato. Ciò è possibile posizionando dei Reader all'ingresso dei locali della struttura sanitaria. I Tag consentono l'identificazione univoca di pazienti, personale sanitario e apparecchiature:

- i pazienti sono dotati di braccialetti identificativi contenenti appositi Tag;
- i lavoratori della struttura (medici, infermieri, tecnici e altri lavoratori) sono dotati di tesserini identificativi contenenti altri Tag;
- sulle apparecchiature (inclusi gli elettromedicali) sono apposti Tag adesivi.

I Reader sono connessi tramite rete al sistema informativo della struttura sanitaria. Opportuni applicativi gestiscono la localizzazione in tempo reale dei Tag e l'archivio storico.
Le principali funzionalità da perseguire sono le seguenti:

1. localizzazione dei pazienti e stato del trattamento medico prescritto;
2. registrazione della durata della permanenza di un paziente all'interno dei diversi locali di una struttura sanitaria (Pronto Soccorso, reparti, sala operatoria) e del tempo totale di soggiorno fino alla dismissione;
3. analisi statistica dei dati dei pazienti (con registrazione nell'archivio storico della struttura sanitaria, al fine di verificare il raggiungimento degli obiettivi di qualità);
4. localizzazione delle apparecchiature e degli elettromedicali all'interno dei locali della struttura sanitaria e loro individuazione in tempo reale;
5. apposizione di Tag alle cartelle cliniche dei pazienti in modo da evitare lo smarrimento o lo scambio delle stesse (riducendo in tal modo la probabilità di errori nella compilazione);
6. computo dell'orario di lavoro del personale sanitario (tramite avvicinamento dei tesserini identificativi ad appositi Reader posizionati all'ingresso della struttura sanitaria).

Oltre alle funzionalità attivate durante la prima fase, in una fase successiva potrebbe essere possibile attivare anche ulteriori funzionalità:

7. apposizione di Tag ai contenitori dei farmaci per la loro localizzazione;
8. gestione delle emergenze con localizzazione dei pazienti e dei lavoratori durante l'eventuale esodo (in caso di persone impossibilitate a lasciare la stanza, i componenti delle squadre di emergenza più vicini possono essere allertati); la localizzazione di emergenza potrebbe essere estesa anche ai visitatori, qualora fossero dotati di tesserini identificativi dotati di Tag durante la permanenza all'interno della struttura sanitaria;
9. reperibilità dei lavoratori all'interno della struttura sanitaria (i cui modi sono da definire in accordo con i sindacati);
10. localizzazione dei lavoratori e dei pazienti all'interno dei locali per il trattamento delle malattie infettive, allo scopo di individuare e circoscrivere i possibili trattamenti necessari in caso di eventuale violazione del contenimento degli agenti patogeni, tale funzionalità potrebbe essere estesa anche alla protezione dei visitatori, qualora fossero dotati di tesserini identificativi dotati di Tag durante la permanenza all'interno della struttura sanitaria.

6.3.2. Scelta delle principali caratteristiche del sistema

Al fine di conseguire le funzionalità elencate, la scelta più economica è quella di ricorrere a sistemi passivi operanti alla frequenza di 13,56 MHz.
È evidente che le funzionalità 1, 2, 4, 7, 8, 9 e 10, richiedono l'uso di Tag almeno di vicinanza (avendo cura, ad esempio, di posizionare i Reader per i Tag di vicinanza ai due lati delle porte dei locali, la cui ampiezza non può superare due volte la massima portata di ciascun Reader). La funzionalità 5, se eseguita con Tag di prossimità, richiede di dotare il personale di Reader di prossimità portatili o di passare le cartelle dotate di Tag in prossimità (<10 cm) dei rispettivi Reader per l'identificazione. La funzionalità 6 può essere eseguita utilizzando Tag di prossimità, ma ciò richiede di riacquistare i tesserini identificativi dei lavoratori se si dovesse decidere che devono essere attivate anche le funzionalità 8, 9 e 10.
Pertanto se le funzionalità 8, 9 e 10 non interessano, si possono usare Tag di vicinanza per i pazienti, per le apparecchiature ed eventualmente per i contenitori dei farmaci e Tag di prossimità per i tesserini identificativi dei lavoratori, mentre potrebbero essere usati Reader portatili e Tag di prossimità per le cartelle cliniche dei pazienti.
Viceversa se le funzionalità 8, 9 e 10 interessano (da subito o in futuro), conviene usare Tag di vicinanza anche per i tesserini identificativi dei lavoratori e dei visitatori.
Gli standard trasmissivi RFID a 13,56 Mhz che possono essere usati per il presente esempio sono contenuti nella ISO 15693, per i sistemi operanti in regime di vicinanza, e nella ISO 14443, per i sistemi operanti in regime di prossimità. In entrambe le norme sono previsti protocolli di rilevamento con gestione dell'anticollisione per il rilevamento multiplo.
In ogni caso i Tag cercati devono essere dotati di alimentazione passiva (ad induzione), mentre, come caratteristiche aggiuntive utili per l'esempio proposto, potrebbero essere cercati Tag dotati di:
- UId univoco a 64 bit;
- memoria con almeno 1024 bit, riscrivibile (100.000 cicli di scrittura per Tag);
- ritenzione del dato superiore a 10 anni.

Per quanto riguarda i Reader (di vicinanza) potrebbero essere cercati con le seguenti caratteristiche:
- potenza RF 0.5 W;
- modalità di rilevamento 3 D;
- velocità di rilevamento di circa 1 m/sec;
- altezza almeno di 170 cm;
- passaggio standard di 150 cm di ampiezza, con 2 Reader posizionati ai lati del passaggio;
- fissaggio a pavimento o a pedana;
- peso 10 Kg a elemento;
- alimentazione 12 Volt c.c. (con alimentatore interno per la conversione dalla tensione di 220 V c.a.).

7. Alcuni aspetti critici

7.1. Criticità di impiego

Nonostante il rapido successo, la tecnologia RFId presenta un certo numero di criticità rispetto alle caratteristiche ideali.
Esistono, infatti, alcuni problemi che costituiscono ancora un freno all'introduzione massiva degli RFId in taluni campi applicativi, anche se si spera che in un prossimo futuro potranno essere risolti con lo sviluppo tecnologico.
Un elenco breve e non esaustivo è il seguente:

- scarsa compatibilità "worldwide" (non uniformità di frequenze e potenze operative in tutto il pianeta);
- difficoltà nell'allestimento dell'applicazione (mancanza di sistemi "chiavi in mano", aspettative non realistiche indotte dagli integratori rispetto alle prestazioni effettive di Reader e Tag);
- mancata ripartizione dei costi sull'intera catena di distribuzione (produzione, trasporto, commercio);
- limiti fisici dei sistemi reali (scarsa distanza operativa, possibilità di fallimenti nelle operazioni di lettura, incompleta applicabilità su tutte le merci, bassa velocità di lettura-scrittura);
- scarsa flessibilità per la progettazione delle antenne con conseguenti limiti su forma, dimensioni e contenitori dei TAG;
- difficoltà ad ottenere fiducia dai consumatori (modesta sicurezza e protezione dei dati, impatto ambientale non trascurabile per alcuni tipi di Tag) e dalle aziende (alti costi del software applicativo, alto costo dei Tag, che viene percepito come il maggior fattore ostativo perché si somma al prezzo finale delle merci, limitata integrazione dei processi di "tagging" in alcuni dei processi aziendali, immaturità tecnica dei sistemi "middleware" che devono processare dati e istruzioni).

7.2. Pericoli per la privacy

Il ciclo di vita dei Tag supera spesso quello degli oggetti a cui il Tag è associato.
I Tag passivi, in particolare, non necessitando di batterie, hanno aspettativa di vita teoricamente infinita, e continuano a funzionare anche quando la catena di distri-

buzione è giunta al termine. Ciò significa che è teoricamente possibile continuare ad interrogare gli oggetti a cui i Tag sono associati, anche se sono ormai da tempo in possesso di proprietari privati, traendo da ciò informazioni sulle abitudini di tali persone.
Il problema non riguarda solo i Tag associati a singoli articoli di consumo, che non hanno un'associazione diretta con i dati personali dei proprietari, ma assume un carattere particolarmente preoccupante quando coinvolge altri oggetti abitualmente in possesso dei privati che invece possono consentire di risalire a dati personali (carte di pagamento o di accesso, passaporto elettronico, tessera sanitaria, chip biomedico[2], apparati elettronici, ticket, ecc.).
Per tali motivi, nel settore della logistica, lo standard EPC-Gen2 prevede che i Tag contengano solamente un unico codice (ovvero un numero di serie), cosicché la lettura di un Tag (posizionato su di un oggetto a fini di inventario) sia identica (trattandosi di una soluzione a breve raggio) a quella di un codice a barre e quindi non contenga alcuna informazione utile sull'identità del possessore, mentre diverso è il discorso per i chip che contengono informazioni sensibili.
Le aziende o organizzazioni di vario genere potrebbero comunque ancora acquisire informazioni indebite sulla clientela, ad esempio potrebbero realizzare indagini di mercato sui consumi delle singole persone, acquisendo informazioni al momento del pagamento elettronico.
Un altro problema che ricade sotto il campo della privacy è quello del tracking dell'individuo per mezzo di RFId.
Anche in questo caso il problema assume maggiore rilevanza in presenza di Tag che contengano a bordo informazioni personali che potrebbero essere soggetti a letture non autorizzate per finalità diverse da quelle originarie.
Tale problema però è, allo stato attuale della tecnologia RFId, alquanto sopravvalutato risultando più teorico che pratico.
Infatti, una limitazione proviene direttamente dalla piccola estensione delle zone di copertura dei Reader degli RFId. Le distanze di lettura dipendono fortemente dalle condizioni ambientali e dalle tecnologie utilizzate. In pratica le normative e i dispositivi attuali prevedono le seguenti portate operative:

- per i Tag passivi da 125 a 134.2 kHz, la distanza di lettura varia da quasi a contatto a circa 1 m;
- per i Tag a 13,56 MHz, la distanza di lettura varia da quasi a contatto a circa 1 m;
- per i Tag UHF passivi usati per la logistica (da 860 a 960 MHz), la distanza tipica prevista dalla normativa varia da 1 a 10 metri[3].

2 I chip biomedici sottocutanei servono per memorizzare talune informazioni e permettere, in caso di ricovero di emergenza, di attingere alla scheda sanitaria di un paziente. Sono informazioni personali e il chip è impiantato di solito su richiesta dell'interessato (alcuni Stati hanno approvato legislazioni preventive per vietare l'impianto di dispositivi sottocutanei senza consenso esplicito).

3 I Tag UHF sono quelli con la portata maggiore, tuttavia subiscono una limitazione della portata in presenza di acqua e, poiché il corpo umano è composto al 70% da acqua, l'ipotesi di utilizzarli (in forma cutanea) per il controllo degli spostamenti di una persona (pedinamento), anche se non impossibile, è poco efficace.

Pertanto, in virtù della portata limitata della comunicazione wireless dei Tag, per il tracking è necessario un numero enorme di lettori sparsi su un territorio con lievitazione dei costi relativi.
Vale la pena di osservare che il tracking visivo assicura la copertura di distanze maggiori con migliore accuratezza, e che le forze dell'ordine, se incaricate dall'autorità giudiziaria, possono accedere ben più facilmente ai dati degli operatori di telefonia mobile per seguire gli spostamenti di persone ricercate o soggette ad indagine.
Discorso diverso può essere quello del tracciamento degli spostamenti del personale di un'azienda, all'interno dell'azienda stessa, per mezzo delle tessere RFId di riconoscimento ed accesso. In tal caso anche Tag passivi da 125 a 134.2 kHz o da 13,56 MHz potrebbero essere utilizzati. Posizionando i Reader in corrispondenza delle porte delle stanze è possibile un grossolano posizionamento del personale (presenza o assenza all'interno della stanza). L'economicità dipende dal numero degli ambienti che si intendono controllare. Naturalmente l'effettiva realizzabilità è legata agli accordi sindacali e all'accettazione da parte del personale interessato.

7.3. Pericolo di diffusione di informazioni commerciali

Una particolare attenzione merita la sicurezza dei dati scambiati, soprattutto quelli relativi all'etichettatura elettronica. Infatti, poiché i product code sono molto diffusi in ambito commerciale come identificatori di prodotti (catene produttive e gestione di magazzino), la violazione della segretezza della comunicazione wireless di risposta dei Tag (e la vendita al mercato nero dei dati relativi ai prodotti) costituisce un rischio per l'attività produttiva e commerciale delle aziende, con danni economici potenzialmente rilevanti e un possibile guadagno per le aziende competitrici.

7.4. Rischi per la salute

È necessario evitare esposizioni indebite per durata e potenza di esseri umani ai campi elettromagnetici[4]. Esistono limiti opportuni che dipendono dalla frequenza e devono essere verificati di caso in caso a seconda dell'applicazione specifica.

4 L'International Agency for Research on Cancer (IARC) ha classificato i campi elettromagnetici a radiofrequenza come "possibilmente cancerogeni per gli esseri umani (Gruppo 2B)" (una categoria usata quando "un'associazione causale è considerate credibile, ma la casualità, il pregiudizio o l'incertezza, non possono essere esclusi con ragionevole confidenza"), a tal proposito occorre precisare che gli studi che hanno portato a tale classificazione riguardavano principalmente il rischio associato alla telefonia mobile più che il rischio associato all'uso di altre tecnologie.

Analizzando opportunamente i parametri necessari al funzionamento (frequenza del segnale, ampiezza/potenza, durata dell'esposizione) è possibile che la maggior parte delle attuali applicazioni RFId siano realizzabili senza problemi per la salute, soprattutto se i dispositivi hanno una sufficiente distanza dal corpo.
Nel caso di chip biomedici impiantati è utile valutare anche i seguenti rischi:

- reazioni avverse dei tessuti;
- migrazione del Tag dalla zona dell'impianto;
- guasto del Tag;
- rischi per la salute del paziente durante esami di risonanza magnetica.

Appendice I
Frequenze di esercizio per i sistemi RFId

A.I.1. Tag induttivi in banda LF (sottobanda da 120 kHz a 145 kHz)

La banda LF (Low Frequency) si trova nella parte più bassa dello spettro radio ed è storicamente la prima banda utilizzata per l'identificazione automatica. Sistemi RFId operanti con tali frequenze sono tuttora diffusi sul mercato.
L'accoppiamento tra Reader e Tag avviene per via induttiva tramite antenne a spira.
Nel caso di Tag passivi la distanza operativa è pari, all'incirca, al diametro dell'antenna del lettore e varia dai 30 cm al metro. Al di là di questa portata il campo si riduce molto rapidamente con la terza potenza della distanza.
La distanza per poter eventualmente scrivere nella memoria, operazione che richiede un elevato consumo di energia, è normalmente più bassa di quella di lettura.
In banda LF la frequenza della portante è relativamente bassa e consente velocità massime di trasmissione dei dati dell'ordine del migliaio di bit al secondo che possono però scendere in alcuni casi.
In tale banda è meno diffuso il supporto di letture multiple, ovvero di più Tag contemporaneamente presenti nel campo del lettore.

A.I.2. Tag induttivi in banda HF (sottobanda a 13,56 MHz)

La sottobanda centrata sui 13,56 MHz della banda HF (High Frequency) è utilizzata in tutto il mondo per applicazioni RFId.
L'accoppiamento tra Reader e Tag avviene per via induttiva, come nei sistemi LF.
La realizzazione tipica prevede un Tag con un'antenna formata da un avvolgimento metallico (rame, alluminio, argento), ottenuto per incisione da un sottile foglio di metallo (dello spessore di poche decine di micron), oppure per deposizione di inchiostri conduttivi su di un substrato. La dimensione ed il numero di spire, insieme alla potenza emessa dall'antenna del Reader, determinano la sensibilità e la distanza operativa del sistema.
I costi sono inferiori a quelli dei Tag LF ma strettamente dipendenti dal tipo di supporto e dalla dimensione, così come i costi dei Reader.

Le ultime generazioni di Tag per l'identificazione automatica supportano meccanismi di anticollisione dei messaggi, che permettono la lettura di più Tag presenti contemporaneamente nel campo del Reader.
A differenza di quanto avviene nella banda UHF il campo elettromagnetico a 13,56 MHz non è particolarmente influenzato dalla presenza di acqua o dai tessuti del corpo umano.
La banda HF è attualmente la più usata per le cosiddette etichette intelligenti (*smart tag*) impiegate nella logistica e nella gestione degli oggetti ma anche per le *smart card contactless*.
Le smart card sono quasi unicamente di tipo passivo, offrono una notevole capacità di memoria (da pochi kilobyte al megabyte) e algoritmi crittografici per effettuare transazioni sicure. Sono diffuse nel settore del ticketing, del controllo accessi del personale, della tracciabilità dei bagagli nei sistemi aeroportuali e stanno per diventare comuni come sostituti delle schede magnetiche per le transazioni bancarie (bancomat) e come carte di credito. Diverse nazioni stanno facendo prove per introdurle come passaporto elettronico.

A.I.3. Tag elettromagnetici in banda UHF media (sottobanda da 860 a 950 MHz)

La banda UHF (Ultra High Frequency) media è una banda usata dagli RFId per la logistica e per la gestione degli oggetti, con distanze di funzionamento decisamente più estese di quanto non sia consentito dalle frequenze LF ed HF. Per tale scopo sono usate le sottobande: 865÷870 MHz nella Regione ITU 1 (Europa ed Africa); 902÷928 MHz nella Regione ITU 2 (America del Nord del Centro e del Sud); 950 MHz nella Regione ITU 3 (Estremo oriente e Oceania).
L'accoppiamento tra Reader e Tag avviene per via elettromagnetica, come in un tradizionale sistema di radiocomunicazione. La distanza operativa può arrivare a 3-5 m.
Le dimensioni fisiche dell'antenna del Tag ed il rispettivo diagramma di radiazione variano con la lunghezza d'onda di lavoro del segnale utilizzato. Alla frequenza di 870 MHz la lunghezza d'onda è di circa 34,4 cm ed un'antenna a mezz'onda è lunga circa 17,2 cm, mentre un'antenna ad un quarto d'onda è lunga circa 8,6 cm, sono possibili anche antenne più corte a scapito di una riduzione dell'efficienza di trasmissione, con riduzione delle distanze operative.
Alcuni problemi hanno rallentato la diffusione di RFId operanti in banda UHF media.

- Le frequenze sono diverse a seconda della Regione ITU, poiché le frequenze già occupate dalla telefonia cellulare non consentono di utilizzare le stesse bande anche per applicazioni RFId. Per superare la difficoltà i Tag passivi possono essere costruiti con capacità di rispondere a *banda larga*, in modo da consentirne l'operatività su bande differenti (a scapito di un decadimento nelle prestazio-

ni). Invece i Tag attivi possono essere costruiti con apparati ricetrasmittenti sintonizzabili su più frequenze di lavoro (a scapito dei costi).
- Standard comuni per i protocolli di comunicazione tra Reader e Tag sono stati definiti solo recentemente.
- Nelle diverse Regioni ITU esistono limitazioni differenti per la massima potenza irradiabile. Nel settore della logistica, ciò può tradursi in un vantaggio competitivo per le nazioni che si trovano nelle Regioni in cui sono consentite potenze più alte. Infatti, ad una potenza maggiore corrisponde una maggiore distanza operativa e di conseguenza un diverso costo del servizio (ad es.: tutto il contenuto di un pallet potrebbe essere letto con un'unica operazione).

A queste frequenze si incontrano anche problemi di propagazione delle onde elettromagnetiche:
- se le strutture metalliche in prossimità dell'antenna riflettono le onde, allora le onde riflesse, incontrando l'onda diretta in opposizione di fase, possono generare degli spazi in cui il campo elettromagnetico è nullo, in tali aree i Tag non sono leggibili;
- le onde elettromagnetiche alle frequenze della banda UHF media subiscono un assorbimento consistente da parte dell'acqua, pertanto la capacità di lettura può essere ridotta in ambienti particolarmente umidi o se i Tag sono applicati a contenitori di liquidi.

Comunque, alcune caratteristiche tecniche stanno rendendo i sistemi RFId operanti in banda UHF media sempre più appetibili.
La velocità di trasmissione è superiore a quella dei sistemi operanti a frequenze più basse. I sistemi, inoltre, sono in grado, grazie a protocolli anticollisione, di gestire letture multiple contemporanee, arrivando alla lettura di più di 100 Tag al secondo (con le nuove specifiche si può arrivare anche ad alcune volte tali valori). Sta crescendo il numero dei fornitori di tali sistemi ed il supporto che sono in grado di offrire ai possibili acquirenti, inoltre si registra un ampliamento della scelta della capacità di memoria dei chip e della possibilità di avere sistemi che utilizzano Tag passivi, semipassivi o attivi.

A.I.4. Tag elettromagnetici in banda UHF alta e in banda SHF (sottobanda 2,4 GHz)

La banda UHF alta [ed in particolare la sottobanda centrata su 2,4 GHz] ha caratteristiche simili alla banda UHF media, consentendo, però, un'ulteriore riduzione delle dimensioni dell'antenna e quindi del Tag (per il legame tra le dimensioni dell'antenna e la lunghezza d'onda). Si tratta, comunque, di una banda molto affollata da altre tecnologie (Wi-Fi, Bluetooth, ZigBee).
Ovviamente al La riduzione delle dimensioni dell'antenna comporta comunque

una riduzione della capacità di captare energia dal campo elettromagnetico incidente. Tuttavia antenne molto compatte consentono di dirigere il campo elettromagnetico con maggiore precisione, ottenendo aree di lettura molto ristrette e direzionali.
Le funzionalità non si discostano da quelle dei Tag UHF attivi, semi-passivi e passivi, con memoria da pochi bit (64/96 bit per una semplice etichetta di ID) a diversi kbyte.

Appendice II
Memorie impiegate nei Tag

A.II.1. Memorie ROM (Read Only Memory)

Memorie di sola lettura. Sono programmate in fabbrica attraverso fotoincisione durante la realizzazione del chip. Occupano, a parità di dati registrati, la minore area di silicio all'interno del chip, risultando le più economiche.

A.II.2. Memorie PROM (Programmable Read Only Memory)

Realizzano la tipica funzione WORM (Write Once Read Many). Sono memorie di sola lettura. Le PROM contengono componenti elettronici che possono essere modificati dal processo di scrittura dei dati. Sono scrivibili una sola volta e richiedono apparecchiature speciali per le operazioni di scrittura.

A.II.3. Memorie EEPROM (Electrically Erasable Programmable Read Only Memory)

Le EEPROM, a differenza delle ROM, sono cancellabili e riscrivibili con l'applicazione di opportune tensioni ai componenti che le compongono. Sopportano, però, un numero limitato di cicli di lettura/scrittura (fino a 100.000), il che comporta un riutilizzo limitato dei Tag che le contengono.
Hanno un consumo relativamente alto e tempi lunghi per le operazioni di lettura/scrittura. richiedono anche una consistente area di silicio sul chip e, pertanto, sono costose.
Le capacità delle memorie EEPROM variano, potendo arrivare fino ad oltre 100kbyte. I dati possono essere conservati fino a 10 anni.

A.II.4. Memorie FRAM (Ferroelectric Random Access Memory)

Le FRAM costituiscono un notevole progresso rispetto alle EEPROM. Possono memorizzare dati per un lungo periodo di tempo, richiedono basse tensioni ed

offrono grande resistenza ai cicli di lettura/scrittura, con alta velocità di scrittura. Offrono velocità di trasferimento dei dati fino a 400 kbps, tempi rapidi di lettura e scrittura (meno di 200 ns), correnti estremamente basse (alcuni μA). Sono molto affidabili e hanno tempi di conservazione dei dati superiori a 10 anni.

A.II.5. Memorie SRAM (Static Random Access Memory)

Consentono di mantenere le informazioni per un tempo infinito, sono molto veloci, dissipano poca energia. La necessità di usare molti componenti, però, le rende molto costose e difficili da includere in un chip. Sono solitamente usate per le memorie cache, dove elevate velocità e ridotti consumi sono caratteristiche fondamentali. Vengono impiegate soprattutto nei Tag attivi.

Appendice III
Propagazione dei campi elettromagnetici

A.III.1. Campi emessi da un dipolo ideale infinitesimo

Analizzando le soluzioni delle equazioni di Maxwell per un dipolo ideale si ottengono le espressioni analitiche per i campi elettrico e magnetico, in funzione della corrente che attraversa il dipolo (i simboli fanno riferimento alla figura A.1 dove il dipolo di lunghezza *dl*, con *dl*<<λ, è posto nell'origine del sistema di riferimento e diretto lungo l'asse *z*):

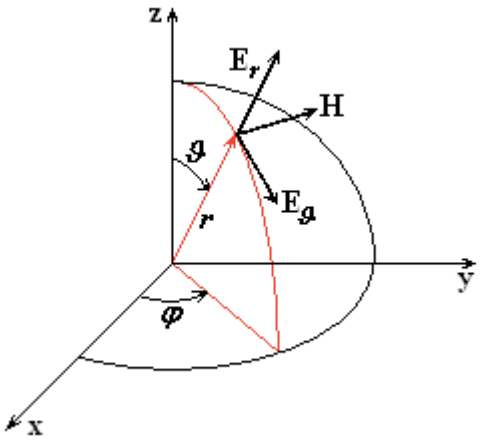


Figura A.1: Campi elettrici e magnetico emessi da un dipolo idea.

$$E_r = \eta \frac{Idl}{2\pi r^2} \cos\vartheta \left(1 - j\frac{\lambda}{2\pi r}\right) e^{-j\frac{2\pi}{\lambda}r} e^{j\omega t}$$

$$E_\vartheta = \eta\, j \frac{Idl}{2\lambda r} \sin\vartheta \left(1 - j\frac{\lambda}{2\pi r} - \frac{\lambda^2}{4\pi^2 r^2}\right) e^{-j\frac{2\pi}{\lambda}r} e^{j\omega t}$$

$$H = j\frac{Idl}{2\lambda r} \sin\vartheta \left(1 - j\frac{\lambda}{2\pi r}\right) e^{-j\frac{2\pi}{\lambda}r} e^{j\omega t}$$

Quando ($r<\lambda/(2\pi)$) le componenti del terzo ordine in ($1/r$) prevalgono ed a questa distanza il campo elettrico diminuisce con il cubo del raggio mentre il campo magnetico diminuisce con il quadrato del raggio. Tale situazione si chiama condizione di *campo vicino* (*near field*).
Al contrario, a grande distanza dal dipolo ($r>>\lambda/(2\pi)$) si ha:

$$E_r \approx 0$$
$$E_\vartheta \approx \eta\, j \frac{Idl}{2\lambda r} \sin\vartheta\, e^{-j\frac{2\pi}{\lambda}r} e^{j\omega t}$$
$$H \approx j \frac{Idl}{2\lambda r} \sin\vartheta\, e^{-j\frac{2\pi}{\lambda}r} e^{j\omega t}$$

e si vede che prevalgono le componenti del primo ordine in ($1/r$), inoltre il campo elettrico, il campo magnetico ed il vettore che va dall'origine al punto considerato sono ortogonali tra loro, il campo elettrico ed il campo magnetico diminuiscono entrambi con l'inverso della distanza ed il rapporto delle loro ampiezze è costante ($\eta=\sqrt{\mu_0/\varepsilon_0}=120\pi$). Tale situazione si chiama condizione di *campo lontano* (*far field*).

A.III.2. Campi emessi da una spira ideale infinitesima

Nel caso di spira ideale le equazioni di Maxwell forniscono le seguenti soluzioni per i campi elettrico e magnetico, in funzione della corrente che attraversa la spira (i simboli fanno riferimento alla figura A.2 dove la spira di raggio b, con $b<<\lambda$, è posta nell'origine del sistema di riferimento con asse diretto lungo l'asse z):

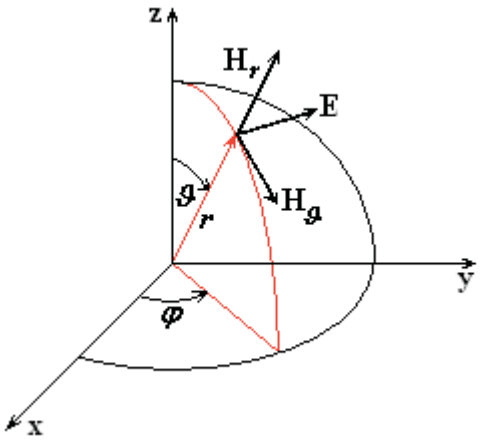


Figura A.2: Campi elettrico e magnetici emessi da una spira ideale.

$$H_r = j\left(\frac{2\pi}{\lambda}\right)\frac{I\pi b^2}{2\pi r^2}\cos\vartheta\left(1 - j\frac{\lambda}{2\pi r}\right)e^{-j\frac{2\pi}{\lambda}r}e^{j\omega t}$$

$$H_\vartheta = -\left(\frac{2\pi}{\lambda}\right)\frac{I\pi b^2}{2\lambda r}\sin\vartheta\left(1 - j\frac{\lambda}{2\pi r} - \frac{\lambda^2}{4\pi^2 r^2}\right)e^{-j\frac{2\pi}{\lambda}r}e^{j\omega t}$$

$$E = \left(\frac{2\pi}{\lambda}\right)\eta\,\frac{I\pi b^2}{2\lambda r}\sin\vartheta\left(1 - j\frac{\lambda}{2\pi r}\right)e^{-j\frac{2\pi}{\lambda}r}e^{j\omega t}$$

Il segno meno nell'espressione di *H,* indica che nella realtà il campo è orientato in verso opposto rispetto all'orientazione che ha in figura 2.
Quando ($r<\lambda/(2\pi)$) le componenti del terzo ordine in ($1/r$) prevalgono ed a questa distanza il campo elettrico diminuisce con il quadrato del raggio mentre il campo magnetico diminuisce con il cubo del raggio(*campo vicino - near field*).
Al contrario, a grande distanza dalla spira ($r>>\lambda/(2\pi)$) si ha:

$$H_r \approx 0$$

$$H_\vartheta \approx -\left(\frac{2\pi}{\lambda}\right)\frac{I\pi b^2}{2\lambda r}\sin\vartheta\, e^{-j\frac{2\pi}{\lambda}r}e^{j\omega t}$$

$$E \approx \left(\frac{2\pi}{\lambda}\right)\eta\,\frac{I\pi b^2}{2\lambda r}\sin\vartheta\, e^{-j\frac{2\pi}{\lambda}r}e^{j\omega t}$$

e si vede che prevalgono le componenti del primo ordine in ($1/r$), inoltre il campo elettrico, il campo magnetico ed il vettore che va dall'origine al punto considerato sono ortogonali tra loro, il campo elettrico ed il campo magnetico diminuiscono entrambi con l'inverso della distanza ed il rapporto delle loro ampiezze è costante (η), (*campo lontano - far field*).

A.III.3. Trasferimento di potenza per mezzo di campi elettromagnetici

Poiché in condizione di campo lontano i campi elettrico e magnetico sono ortogonali tra loro ed ortogonali alla direzione di propagazione e le rispettive ampiezze sono legate, la conoscenza di uno solo dei due campi è sufficiente a descrivere completamente anche l'altro. In tale caso non si parla più distintamente di campo elettrico e di campo magnetico, ma di un'unica entità denominata *campo elettromagnetico*, che si propaga per onde (*onde elettromagnetiche*).
Alle onde elettromagnetiche è associato un flusso di energia nella direzione di propagazione. In un dato istante, la potenza che attraversa l'unità di superficie nor-

male alla direzione di propagazione è detta *densità di potenza* ed è calcolabile dal modulo (*N*) del *vettore di Poynting*:

$$\vec{N} = \vec{E} \times \vec{H} \qquad (\mathrm{W/m^2})$$

$\vec{N}$ ha direzione normale al piano dei vettori $\vec{E}$ ed $\vec{H}$ ed il suo verso coincide con quello di propagazione dell'onda (il modulo è uguale al prodotto dei valori istantanei del campo elettrico e magnetico.
Quando la corrente nell'antenna varia nel tempo con legge sinusoidale, allora anche le ampiezze dei campi sono sinusoidali e le informazioni energetiche sono ricavate utilizzando il valor medio in un periodo della densità di potenza, N_m, al posto della densità di potenza istantanea, *N*.
Si hanno allora le seguenti relazioni:

$$N_m = \frac{1}{2} EH = \frac{1}{2} \frac{E^2}{\eta} = \frac{1}{2} \eta H^2$$

$$E = \sqrt{2 \eta N_m}\ ; \qquad H = \sqrt{\frac{2N_m}{\eta}}\ ;$$

dove *E* ed *H* sono le ampiezze massime rispettivamente del campo elettrico e del campo magnetico.

Un'antenna che irradia la stessa potenza in tutte le direzioni è detta *antenna isotropa*.
La potenza P_i emessa dall'antenna isotropa può essere messa in relazione con la densità di potenza N_m. Infatti a distanza *r* dall'antenna la potenza si distribuisce su una superficie sferica di raggio *r*. Nel caso di campi sinusoidali nel tempo ed in condizione di campo lontano si ottengono le seguenti relazioni per i valori medi nel periodo della potenza P_i e della densità di potenza N_m:

$$N_m = \frac{P_i}{4\pi r^2}$$

$$E = \frac{1}{r} \sqrt{\frac{\eta P_i}{2\pi}}\ ; \qquad H = \frac{1}{r} \sqrt{\frac{P_i}{2\pi \eta}}\ .$$

In pratica, l'intensità del campo irradiato dalle antenne reali varia con la direzione. È possibile allora costruire un *solido di radiazione*, riportando, con origine nell'an-

tenna e per ogni direzione, ampiezze proporzionali al rapporto tra le intensità di campo radiato e il valore dell'intensità del campo nella direzione di radiazione massima.
I *diagrammi di radiazione* sono le curve che si ottengono sezionando il solido di radiazione con opportuni piani passanti per l'origine.
Il *guadagno G* di un'antenna nella direzione di massima radiazione è definito come il rapporto tra la potenza che dovrebbe essere irradiata da un'antenna isotropa e la potenza dell'antenna in esame perché si abbia lo stesso campo ad una determinata distanza nella direzione di massima radiazione. Poiché l'antenna isotropa irradia con uguale intensità in tutte le direzioni, il guadagno può essere definito anche come il rapporto della densità di potenza irradiata nella direzione di massima radiazione e la densità di potenza media irradiata. In tal senso, il guadagno indica la *direttività* dell'antenna, cioè la capacità dell'antenna di irradiare l'energia concentrandola in una data direzione (per questo è detto anche guadagno di direttività).
Tenendo conto del guadagno G_t (l'indice *t* indica un'antenna trasmittente), i campi in un punto a distanza *r* dall'antenna, nella direzione di massima radiazione valgono:

$$E = \frac{1}{r}\sqrt{\frac{\eta G_t P_i}{2\pi}}; \qquad H = \frac{1}{r}\sqrt{\frac{G_t P_i}{2\pi\,\eta}}.$$

L'*area efficace* di un'antenna ricevente è definita come rapporto tra la potenza P_u disponibile all'uscita dell'antenna (cioè quella fornita dall'antenna al carico), quando questa è orientata nella direzione di massima ricezione, e la densità di potenza N_m dell'onda incidente:

$$A_e = \frac{P_u}{N_m}$$

Area efficace e guadagno G_r (l'indice *r* indica un'antenna ricevente) dell'antenna sono legati dalla relazione:

$$G_r = \frac{4\pi\, A_e}{\lambda^2}$$

Le precedenti relazioni consentono di calcolare la potenza disponibile all'uscita dell'antenna ricevente (equazione di Friis), nello spazio libero, a distanza r da un'antenna trasmittente che irradi la potenza P_i (le antenne sono orientate nelle rispettive direzioni di massima ricezione e di massima radiazione):

$$P_u = A_e N_m = A_e \frac{G_t P_i}{4\pi\, r^2} = \frac{\lambda^2 G_r}{4\pi} \cdot \frac{G_t P_i}{4\pi\, r^2} = \frac{\lambda^2}{(4\pi\, r)^2} G_r G_t P_i$$

A.III.4. Fenomeni che influenzano la propagazione delle onde elettromagnetiche

Nell'atmosfera terrestre, a causa dell'indice di rifrazione dell'atmosfera, le onde elettromagnetiche viaggiano ad una velocità dipendente dalla frequenza e sono soggette ad attenuazione, riflessione, rifrazione, diffrazione, diffusione e rumore:

- L'*attenuazione* è la riduzione della potenza del segnale dovuta alla distanza tra trasmettitore e ricevitore e alle proprietà fisiche del mezzo in cui si propagano le onde; è possibile distinguere tra:
  - *l'attenuazione isotropica* da spazio vuoto, dovuta a fattori geometrici (distanza r), che in potenza va come $1/r^2$;
  - *l'attenuazione supplementare* del mezzo reale (diverso dallo spazio vuoto), che si somma all'attenuazione isotropica.
- La *riflessione* avviene alla superficie di separazione tra due mezzi, quando vi è una netta variazione dell'indice di rifrazione: i due mezzi possono essere ad esempio aria ed un altro materiale o due masse d'aria con caratteristiche fisiche diverse (diversa densità e/o concentrazione di vapore acqueo).
- La *rifrazione* si ha ugualmente alla superficie di separazione tra due mezzi, e consiste in una riduzione di potenza (infatti la potenza dell'onda incidente si ripartisce tra l'onda riflessa e l'onda rifratta, che è quella che penetra nel secondo mezzo) associata ad una variazione del percorso, rispetto alla direzione dell'onda incidente (in funzione del rapporto tra gli indici di rifrazione).
- La *diffrazione* è un fenomeno fisico dovuto alla natura *ondulatoria* dell'onda[5], per cui questa può propagarsi oltre un ostacolo di dimensioni inferiori od uguali alla propria lunghezza d'onda mentre viene bloccata da un ostacolo molto più grande.
- La *diffusione (scattering)* è un fenomeno fisico dovuto alla disomogeneità del mezzo in cui l'onda si propaga: ad esempio grazie alle disomogeneità dell'atmosfera le onde elettromagnetiche sono diffuse nelle varie direzioni e l'orizzonte diviene sorgente di onde che possono raggiungere un ricevitore che si trovi oltre l'angolo visivo del trasmettitore.
- Il *rumore* ha natura variabile e aleatoria nel tempo, con effetti sulla qualità del radiocollegamento, andandosi a sommare al segnale utile informativo. È suddiviso in:
  - *rumore interno* al sistema, dovuto al rumore termico dei componenti circuitali dell'emettitore e del ricevitore (se ne tiene conto attraverso la potenza di rumore $N_0=kTB$ dove k è la costante di Boltzmann, T la temperatura equivalente di rumore e B la banda di frequenza passante del ricevitore),
  - *rumore esterno* al sistema (detto semplicemente *disturbo*), dovuto ad altre sorgenti di radiazione, naturali e artificiali, come la radiazione cosmica (di fondo e diretta) e il rumore termico di altri oggetti fisici.

5 Infatti, ad un dato istante, ogni punto del fronte di un'onda è sorgente di onde dalla cui interferenza risulta il fronte d'onda per l'istante successivo.

L'attenuazione supplementare, detta anche *fading* (evanescenza), ha natura aleatoria e variabile nel tempo, a causa delle variazioni delle caratteristiche fisiche del canale radio. Il fading può essere *costante* oppure *selettivo* al variare della frequenza (nel caso di fading selettivo si ha una distorsione del segnale a cui si può porre rimedio con opportuni equalizzatori).
In generale è possibile distinguere tra:

- *fading statico*, dovuto all'assorbimento da parte dell'ossigeno e del vapore acqueo atmosferico (per lo più in corrispondenza di determinate frequenze di assorbimento corrispondenti alle rispettive risonanze molecolari). In tali bande ovviamente non è consigliabile trasmettere alcuna potenza elettromagnetica. Le bande complementari utili alla trasmissione sono comunemente note come *finestre trasmissive*.
- *fading scintillante*, dovuto allo scattering particellare e caratterizzato da bassi livelli di attenuazioni e valor medio nullo nel tempo.
- *fading per cammini multipli* (*multipath fading*), dovuto alle riflessioni, causate dal suolo o da ostacoli, che generano cammini multipli seguiti dall'onda elettromagnetica nel suo percorso e la cui ricombinazione in fase è aleatoria nel tempo, generando variazioni di potenza nel ricevitore in conseguenza di interferenza costruttiva o distruttiva.
- *fading* da *precipitazioni*, dovuto alla pioggia, è funzione dell'intensità di precipitazione ed aumenta fortemente con la frequenza dell'onda elettromagnetica.
- *fading* da *effetto condotto*, dovuto alla formazione di *condotti atmosferici* , causati da anomalie nella distribuzione verticale dell'indice di rifrazione per variazione delle condizioni meteorologiche (es. inversioni termiche), nei quali rimane confinato il segnale elettromagnetico, che subisce forti attenuazioni per riflessione sulle pareti del condotto stesso.
- *fading* per *diffrazione* dovuto alla presenza di ostacoli fisici.

È possibile distinguere diversi tipi di propagazione per le onde elettromagnetiche:

- *Propagazione per onda diretta*: si verifica quando il ricevitore è nella visuale del trasmettitore. È il tipo di radiopropagazione più diffuso, specie nei ponti radio. È utilizzato con le bande VHF, UHF, SHF e EHF (nelle bande VHF e UHF la diffrazione consente anche il superamento di ostacoli).
- *Propagazione per onda ionosferica*: sfrutta la riflessione elettromagnetica da parte della ionosfera (lo strato atmosferico ionizzato conduttore distante un centinaio di chilometri dal suolo terrestre) permettendo la propagazione oltre la semplice portata ottica tra trasmettitore e ricevitore ovvero oltre i limiti imposti dalla curvatura terrestre. È utilizzata con la banda HF. Al giorno d'oggi è scarsamente utilizzata.
- *Propagazione per onda superficiale*: sfrutta l'effetto guidante della superficie terrestre all'interfaccia con la strato atmosferico, consentendo anche lunghi percorsi. Poiché l'attenuazione del terreno cresce con la frequenza delle onde, è utilizzata con le bande VLF e LF. Dato che la superficie del mare genera una

minore attenuazione, le onde superficiali sono utilizzate soprattutto per comunicazioni nautiche e con sommergibili.

- *Propagazione per effetto condotto*: sfrutta la formazione di condotti atmosferici per l'onda elettromagnetica grazie all'inversione dell'indice di rifrazione dell'aria in particolari condizioni atmosferiche. Non è tuttavia pienamente affidabile in quanto la formazione dei condotti si manifesta in maniera aleatoria nel tempo.
- *Propagazione per onda riflessa*: si verifica quando il terreno o altri ostacoli riflettono l'onda verso il ricevitore. Quando l'onda elettromagnetica segue più percorsi dal trasmettitore al ricevitore si chiama *multipropagazione* (*multipath*). In tal caso, a causa della ricombinazione con fase generalmente diversa delle varie onde in ricezione dovute al differente cammino percorso la potenza in ricezione è soggetta a fading aleatorio (almeno nel caso di trasmissioni radiomobili).
- *Propagazione per scattering troposferico*: si verifica quando la troposfera (lo strato atmosferico più basso e denso, distante una decina di chilometri dal suolo terrestre) grazie alla diffusione reindirizza una piccola parte dell'energia delle onde verso il ricevitore, anche se non in vista. È utilizzata con la banda HF.

Appendice IV
Protocolli anticollisione stocastici

I protocolli anticollisione stocastici più utilizzati sono del tipo Aloha, tipologia Blocked access, e possono essere classificati in tre categorie: Pure, Slotted, e Framed (figura A.3) [3].

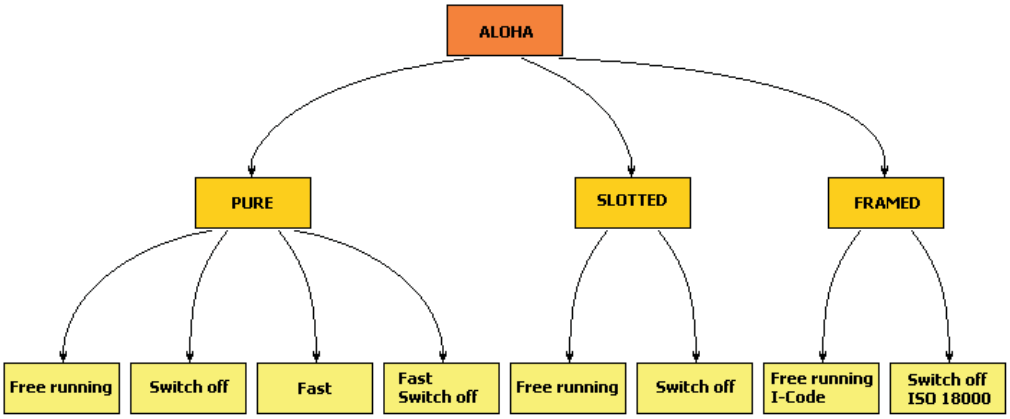


Figura A.3: Classificazione dei protocolli Aloha.

A.IV.1. I protocolli Aloha Pure

A.IV.1.1. Aloha Pure Free Running

Nel protocollo Aloha Pure Free Running il Reader comunica con i Tag quando deve iniziare e terminare la lettura. Durante tale intervallo di tempo ogni Tag comunica ripetutamente il proprio codice ad intervalli casuali (figura A.4). Se il numero di Tag da gestire è basso, la probabilità di collisione è ridotta e solo raramente è necessaria una nuova trasmissione. Tuttavia, se il numero di Tag è alto, le collisioni sono frequenti e il continuo ingresso di nuovi pacchetti le moltiplica rendendo instabile il sistema [3].

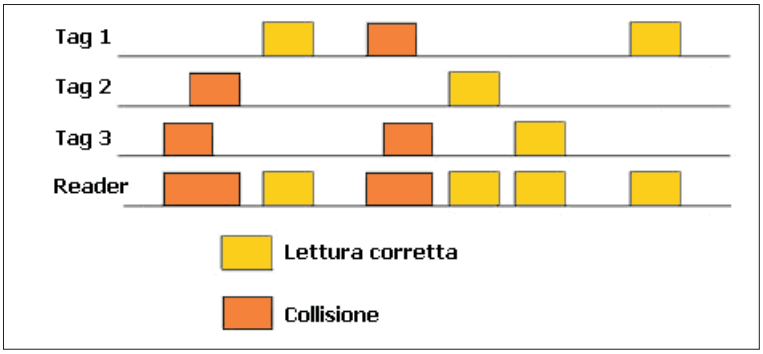


Figura A.4: Protocollo Aloha Pure Free Running.

A.IV.1.2. Aloha Pure Switch Off

Il protocollo Aloha Pure Switch Off (figura A.5) è un miglioramento rispetto al metodo precedente. I Tag tentano di inviare il proprio codice in modo casuale, ma continuano a farlo solo finché i dati non sono stati letti correttamente. Quando ciò avviene, il Reader manda un segnale di ACK (acknowledgement) al relativo Tag che da quel momento cessa di prendere parte al processo di lettura. Operando in tale maniera il rischio di collisioni diminuisce col passare del tempo, ed è possibile gestire anche centinaia di Tag [3].

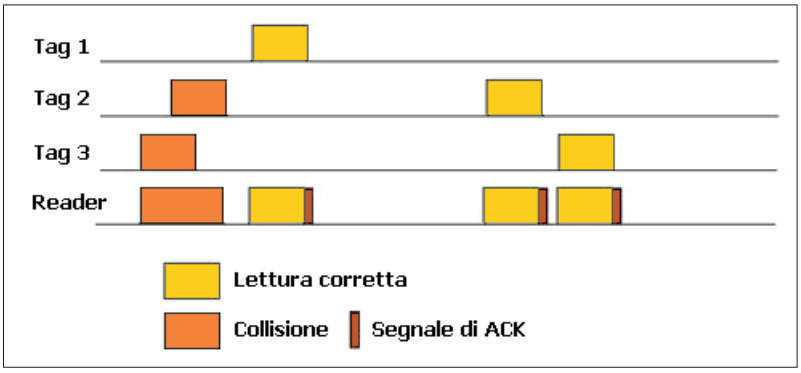


Figura A.5: Protocollo Aloha Pure Switch Off.

A.IV.1.3. Aloha Pure Fast

Questo protocollo (chiamato anche Carrier Sense) prevede un segnale di Mute che, al contrario dell'ACK, è inviato appena un Tag comincia a trasmettere ed è indirizzato a tutti i Tag ad eccezione di quello che sta trasmettendo. Tale segna-

le blocca le azioni dei Tag per un tempo pari alla durata di uno slot, mandando sicuramente a buon fine la lettura dell'unico Tag rimasto attivo in trasmissione (figura A.6). Questo protocollo assicura una buona gestione delle collisioni, anche se richiede un Reader più complesso. Infatti, per essere in grado di leggere e contemporaneamente di inviare il segnale di Mute, il Reader deve disporre di due antenne [3].

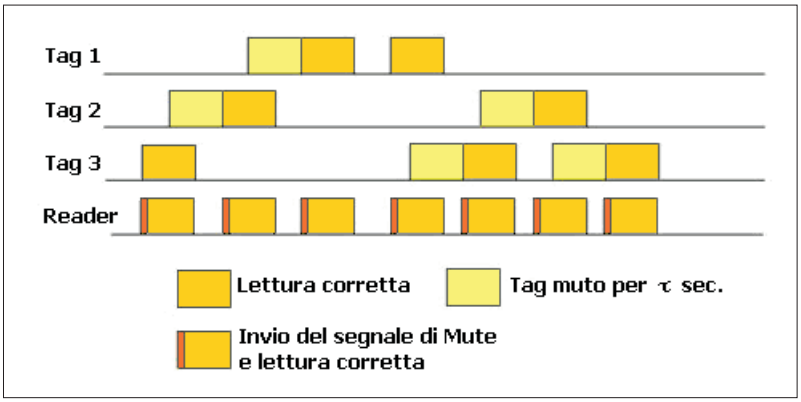


Figura A.6: Protocollo Aloha Pure Fast.

A.IV.1.4. Aloha Pure Fast Switch Off

Il protocollo Aloha Pure Fast Switch Off è la combinazione dei due metodi precedenti. Il Reader comunica con i Tag attraverso segnali di ACK e di Mute (figura A.7). Ciò richiede una notevole complessità circuitale e costi maggiori, che sono ripagati da un tempo di comunicazione più breve rispetto a quello dei metodi precedenti, soprattutto in presenza di centinaia di Tag [3].

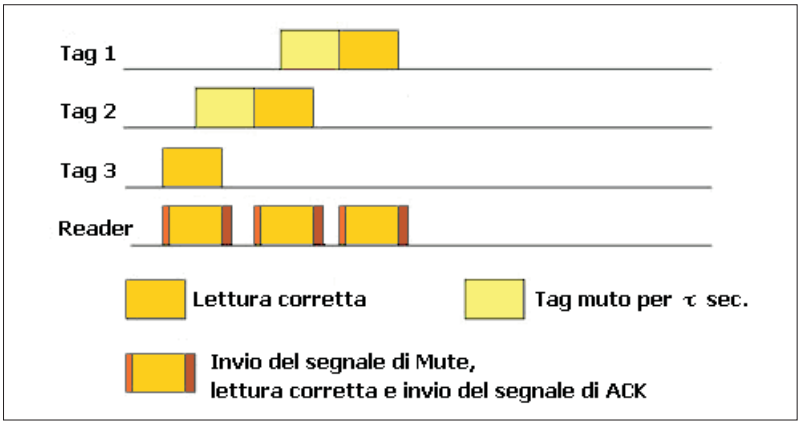


Figura A.76: Protocollo Aloha Pure Fast Switch Off.

A.IV.2. I protocolli Aloha Slotted

A differenza dei protocolli Aloha Pure, in cui si ha una comunicazione asincrona, l'Aloha Slotted prevede invece una comunicazione sincrona, grazie alla discretizzazione del tempo in slot temporali della durata di un pacchetto.
Il Reader comunica con i Tag all'inizio di ogni nuovo slot e ciascun Tag, in modo casuale, decide se trasmettere oppure no in tale slot:

- nel caso in cui non sia inserito nessun altro segnale di comunicazione, il protocollo assume il nome di Aloha Slotted Free Running;
- se il Reader invece prevede il segnale di ACK, si ha la modalità Aloha Slotted Switch Off.

L'Aloha Slotted Switch Off permette una buona velocità di comunicazione, anche se l'Aloha Pure Fast Switch Off è più veloce [3].

A.IV.3. I protocolli Aloha Framed

I protocolli Aloha Framed sono anch'essi sincroni: lavorano con i frame, cioè con insiemi di slot. Il numero di slot che compongono un frame solitamente non è fisso, ma è comunicato dal Reader ai Tag ed è scelto secondo criteri di massimizzazione della velocità di lettura. Ogni Tag invia i propri dati durante uno slot ancora casuale, ma tale invio accade solo una volta ogni frame, in modo da limitare le possibili collisioni. I metodi principali di Aloha Framed sono due: I-Code e ISO 18000 [3].

A.IV.3.1 I-Code

Il funzionamento di questo protocollo è analogo a quello del protocollo Aloha Slotted Free Running, solo che invece di lavorare con gli slot, lavora con i frame. Il numero di slot di un frame è variabile ed è scelto per mezzo di una stima dei Tag presenti nel campo. La stima è calcolata dal Reader in base al numero di collisioni e di successi rilevati. Alla fine di ogni frame, il numero di slot del frame successivo è nuovamente dimensionato. Ovviamente la stima non avviene per il primo frame che ha una dimensione prestabilita [3].

A.IV.3.2 ISO 18000 (Aloha Framed Switch Off)

Questo protocollo è uno dei due protocolli contenuti nello standard ISO 18000-6. Il funzionamento di tale algoritmo è analogo a quello dell'Aloha Slotted Switch Off, con l'organizzazione degli slot in frame. Le caratteristiche sono quelle del protocollo I-Code, con in aggiunta l'utilizzo del segnale di ACK. Grazie ad esso le prestazioni migliorano notevolmente: in caso di numerosi Tag (anche migliaia) è il protocollo più rapido, anche se è quello che richiede la comunicazione più intensa tra Reader e Tag [3].

Appendice V
Protocolli anticollisione deterministici

A differenza dei protocolli stocastici nei protocolli deterministici non esiste un metodo base, ma metodi derivanti da idee diverse. È possibile, comunque, una classificazione in due categorie:
- la categoria dei protocolli totalmente deterministici;
- la categoria dei protocolli deterministici con elemento casuale.

A.V.1. Time Division Multiple Access

Uno dei metodi di base sfrutta la tecnica TDMA (Time Division Multiple Access), che prevede che ad ogni Tag sia assegnato un preciso slot temporale nel corso del quale trasmettere i propri dati. L'assegnazione dello slot è fatta in base alle ultime due cifre del UId del Tag. Visto che ogni Tag può inviare i propri dati solo durante lo slot a lui assegnato, il rischio di collisioni si riduce. In realtà, è facile trovare in commercio Tag con le ultime due cifre dell'UId identiche. Inoltre, operare con tale metodo equivale a ritardare il momento della lettura di un numero di slot proporzionale al numero dei Tag. Ciò rende inutilizzabile il protocollo per scarsa efficienza, tranne che nel caso in cui il numero dei Tag sia molto basso [3].

A.V.2. Binary Search

Il protocollo di ricerca binaria è un protocollo deterministico molto utilizzato. Per un corretto funzionamento, ha bisogno di due elementi:
- la sincronizzazione sui bit di codice risposti contemporaneamente da più Tag interrogati dal Reader;
- un livello di logica sul Tag che permetta di individuare se il codice inviato dal Reader è di valore maggiore, o minore, rispetto a quello posseduto dal Tag.

Codice da trovare

1	0	1	0	0	0	1	1

1° passo

Richiesta del Reader	1	1	1	1	1	1	1	1
Risposta dei Tag	1	0	1	1	0	0	1	0
	1	0	1	0	0	0	1	1
	1	0	1	1	0	0	1	1
	1	1	1	0	0	0	1	1
Risultato	1	X	1	X	0	0	1	X

2° passo

Richiesta del Reader	1	0	1	1	1	1	1	1
Risposta dei Tag	1	0	1	1	0	0	1	0
	1	0	1	0	0	0	1	1
	1	0	1	1	0	0	1	1
Risultato	1	0	1	X	0	0	1	X

3° passo

Richiesta del Reader	1	0	1	0	1	1	1	1
Risposta dei Tag	1	0	1	0	0	0	1	1
Risultato	1	0	1	0	0	0	1	1

Figura A.8: Funzionamento del Binary Search in caso di quattro Tag presenti. Dopo il 3° passo il Tag con il corrispondente UId è identificato e disattivato.

Il funzionamento dell'algoritmo è illustrato nella figura A.8: ad ogni passo dell'algoritmo il Reader invia un numero e, in modo sincronizzato, i Tag che hanno un UId di valore inferiore o uguale a tale numero trasmettono il proprio codice identificativo. Al primo passo dell'algoritmo il Reader invia ai Tag il massimo numero possibile. Ad esempio, se i Tag hanno un UId a 8 bit, il numero inviato dal Reader è 255, cioè 11111111. I Tag verificano di avere il proprio UId minore o uguale a 255 e lo inviano. Grazie alla sincronizzazione dei Tag, il Reader riesce ad individuare i bit sui quali è avvenuta una collisione. Questo significa che alcuni Tag hanno UId che differiscono tra loro per quei determinati bit. A questo punto il Reader invia un codice che restringe il campo dei Tag che possono rispondere. Per fare ciò prende il vecchio codice e, a partire dal primo bit più significativo su cui si è riscontrata una collisione, pone a 0 tale bit. Si procede così finché non rimane un solo Tag a rispondere. Il codice di quel Tag è quindi identificato dal Reader, che successivamente lo disabiliterà.
La ricerca riprende dall'ultima richiesta precedente alla scoperta del codice e termina quando il Reader scopre l'UId dell'ultimo Tag rimasto [3].

A.V.3. Stack ISO 18000

Questo protocollo fa parte dei protocolli deterministici con elemento casuale. È uno dei protocolli riconosciuto dallo standard ISO 18000-6.
L'algoritmo necessita dei seguenti due elementi:

- un generatore di numeri casuali sui Tag, che possa assumere solo i valori 0 o 1;
- un contatore su ogni Tag, che è aggiornato durante lo svolgimento dell'algoritmo; quando il contatore assume un valore maggiore di zero il Tag non è abilitato a inviare il proprio UId.

Il funzionamento dell'algoritmo è illustrato dal diagramma di figura A.9.
Il Tag può assumere uno dei seguenti stati:

- WAIT (attesa): il Tag non può inviare il proprio UId. Il Reader può provocare l'incremento o il decremento del contatore. Quando il contatore raggiunge il valore zero il Tag passa allo stato ACTIVE.
- ACTIVE: (attività): il Tag invia il proprio UId. Se non si verificano collisioni il Tag passa allo stato SLEEP, altrimenti rimane nello stato ACTIVE (nel caso il generatore casuale fornisca come risultato 0) oppure ritorna allo stato WAIT (nel caso il generatore casuale fornisca come risultato 1).
- SLEEP (Tag disattivato): il Tag non può più partecipare alla sessione di lettura.

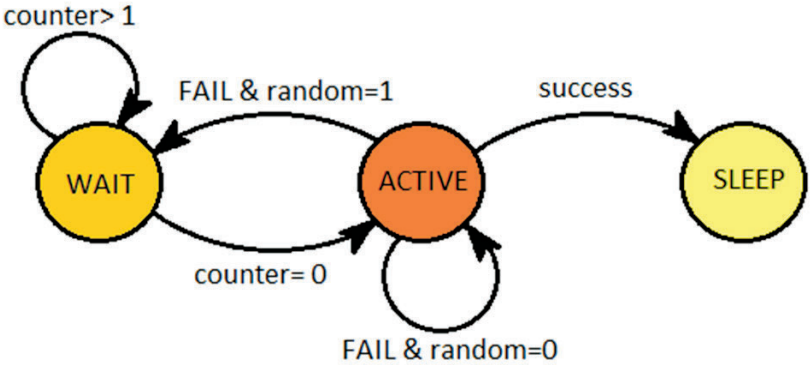


Figura A.9: Diagramma degli stati di un Tag funzionante con protocollo Stack ISO 18000.

Quando il Reader inizia la lettura in blocked access, tutti i Tag che partecipano alla sessione azzerano il proprio contatore e inviano al Reader il proprio UId. Ogni volta che il Reader rileva delle collisioni invia un segnale di FAIL che provoca l'incremento dei contatori dei Tag. Invece, ogni volta che rileva una corretta comunicazione oppure non rileva nessun traffico invia un segnale di SUCCESS che provoca il decremento dei contatori dei Tag. Se il SUCCESS si è verificato in seguito al successo della trasmissione di un Tag, il Reader ne acquisisce l'UId e lo disattiva.
L'algoritmo ha termine quando sono stati letti tutti gli UId dei Tag e non si ha più traffico verso il Reader, perché tutti i Tag sono stati bloccati nello stato di SLEEP [3].

Appendice VI
Altre tecnologie utilizzabili per sistemi wireless

Sono qui contenuti alcuni cenni a tecnologie di comunicazione (Wi-Fi, UWB, Bluetooth LE, ZigBee, NFC) impiegabili (o già impiegate) per applicazioni che potrebbero rientrare negli scopi del presente lavoro (cioè potrebbero essere usate per realizzare Tag attivi ad alte prestazioni). Tali tecnologie sono utilizzate con successo anche nel settore delle reti di sensori ed attuatori. In particolare, esiste una certa vicinanza tra tali tecnologie e il mondo degli RFId attivi, soprattutto per applicazioni "closed loop" (applicazioni in cui il Tag è recuperabile e riutilizzabile).
Infatti si assiste sempre più spesso alla migrazione degli RFId attivi dalla semplice funzione di identificazione automatica a funzioni legate al mondo delle reti di sensori.
Le potenzialità sono enormi, basti pensare, ad esempio, alle funzionalità di una rete mesh che consenta di comunicare con i nodi, attraverso altri nodi: in ambito logistico potrebbe essere possibile la comunicazione con i container di un intero porto senza disseminare lo stesso di Reader connessi in rete.
La tabella seguente mostra una comparazione tra i diversi sistemi wireless considerati nei prossimi paragrafi.

Tabella A.1 - Comparazione delle diverse tecnologie Wireless [2]

	Tecnologie Wireless				
Proprietà	**Wi-Fi**	**Bluetooth LE**	**ZigBee**	**UWB**	**NFC**
Frequenza	802.11 a/b/g/n (2,4÷5 GHz)	2,4 Ghz	2,4 Ghz	3,1÷10,6 GHz	13,56 GHz
Data Rate	802.11b (11Mb/s) 802.11a/g (54Mb/s) 802.11n (250Mb/s)	1Mb/s	20÷250Kb/s	100÷250Mb/s	100÷400Kb/s
Raggio di azione (m)	50÷100	10	50÷100	10	0,1
Topologia	Punto-Multipunto	Ad hoc	Stella, Peer-to-Peer, Cluster-tree	Punto-punto	Punto-punto
Complessità	Alta	Alta	Media/Bassa	Media	Bassa
Consumo	Alto	Medio	Molto basso	Basso	Basso/Nullo (passive-mode)
Applicazioni	Wireless LAN, trasferimento dati	Collegamenti ad hoc: audio o dati	Controllo accessi e ambienti, domotica reti di sensori, applicazioni biomediche	Telerilevamento, reti di controllo, RFid, trasferimento dati	Ticketing, sistemi di autenticazione e sicurezza, RFid

Wi-Fi, Bluetooth LE e ZigBee, seppur con potenze decisamente inferiori, operano nella stessa banda di frequenze usata dai forni a microonde per la cottura del cibo (2,45 GHz).

A.VI.1. Dispersione di spettro

I sistemi di comunicazione *Spread Spectrum* (a dispersione di spettro) sono basati su una tecnologia di modulazione nata in ambito militare durante la seconda guerra mondiale ed esclusa dalle applicazioni civili fino alla fine degli anni '80. Recentemente, grazie alla riduzione dei costi, hanno trovato applicazione nell'ambito delle comunicazioni a corto raggio.
La dispersione di spettro utilizza segnali la cui potenza è distribuita su di una banda di ampiezza molto maggiore rispetto a quella necessaria per inviare l'informazione con una modulazione tradizionale ("a banda stretta").

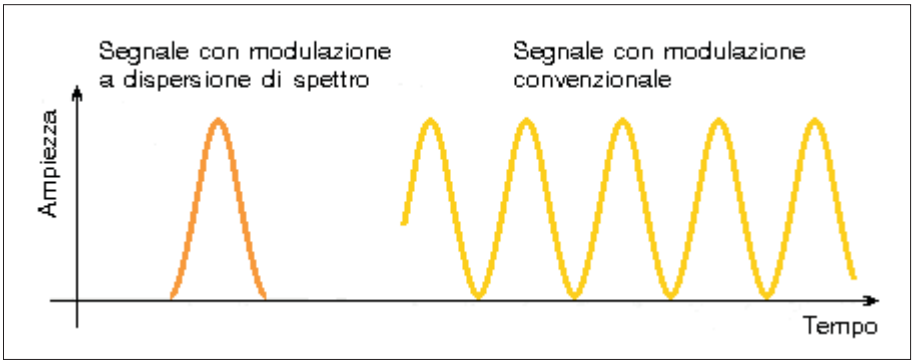


Figura A.10: Confronto tra modulazione convenzionale e dispersione di spettro in termini di forma d'onda.

Poiché il segnale a banda stretta e quello a dispersione di spettro (figura A.10) trasportano le stesse informazioni e la quantità di potenza è la stessa, necessariamente la densità di potenza del segnale che utilizza la dispersione di spettro è molto più bassa (figura A.11).

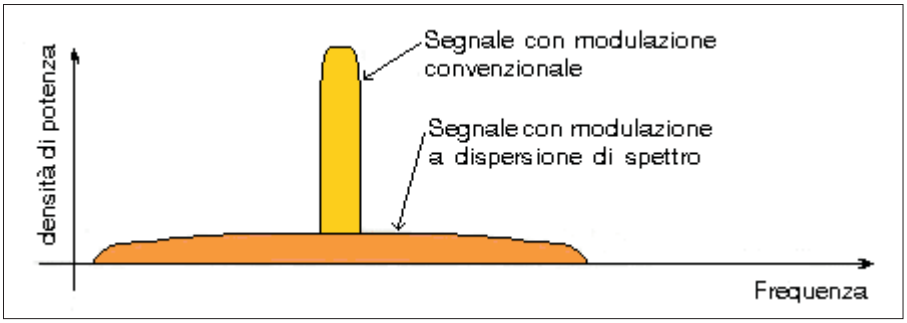


Figura A.11: Confronto tra modulazione convenzionale e dispersione di spettro in termini di occupazione di banda e di livello di densità di potenza.

L'incremento della banda avviene introducendo una certa pseudocasualità nel codice utilizzato per la trasmissione.
La larghezza della banda, la densità di potenza ridotta e la pseudocasualità del codice, rendono il segnale simile ad un rumore gaussiano (rumore di fondo), cosa che rende il segnale a dispersione di spettro di difficile intercettazione da parte di ricevitori estranei al sistema (tale caratteristica è la ragione dell'uso militare).
La similitudine al rumore di fondo fa sì che le comunicazioni a dispersione di spettro possano coesistere con comunicazioni di tipo tradizionale che occupino la stessa banda. Ciò rende possibile l'utilizzo delle stesse frequenze per applicazioni diverse che non interferiscano tra loro.
Le due tecniche più utilizzate per la modulazione a dispersione di spettro sono la *Direct Sequence* (DS) e la *Frequency Hopping* (FH).
Nella Direct Sequence una sequenza binaria pseudocasuale con periodo inferiore alla durata del singolo bit dei dati da trasmettere viene moltiplicata in XOR con la sequenza dei bit dei dati da trasmettere [2].
Ciò ha l'effetto di aumentare l'ampiezza di banda del segnale trasmesso. Il segnale in uscita ha una banda la cui larghezza dipende dalla sequenza pseudo casuale, centrata sulla frequenza dell'oscillatore locale del modulatore. Per demodulare il segnale e decodificare i dati trasmessi, il ricevitore opera sul segnale ricevuto ripetendo le stesse operazioni del trasmettitore con la stessa sequenza pseudocasuale(figura A.12).

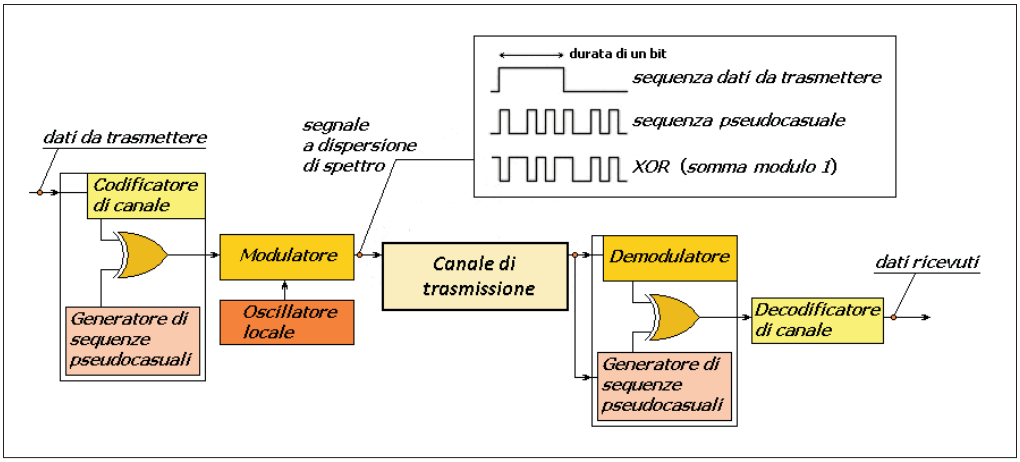


Figura A.12: Dispersione di spettro con tecnica Direct Sequence (DS).

Nella Frequency Hopping, i dati da trasmettere possono essere modulati a banda stretta o a banda larga. All'atto della trasmissione la frequenza portante del modulatore *salta* tra una lista di frequenze predeterminate generata in modo pseudocasuale [2].
Ciò è ottenuto pilotando con la sequenza pseudocasuale un sintetizzatore di frequenza (con funzione di oscillatore locale del modulatore).
Il ricevitore deve saltare tra i canali utilizzando la stessa sequenza usata in trasmissione (figura A.13).

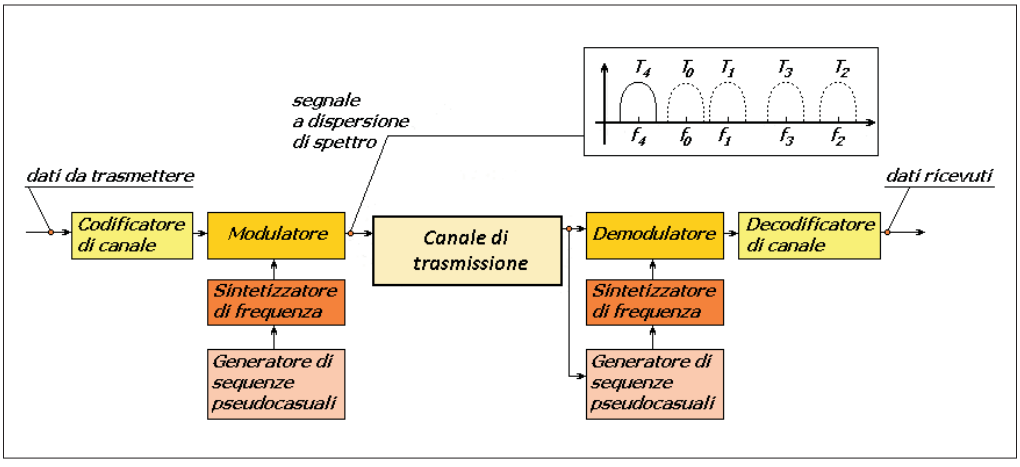


Figura A.13: Dispersione di spettro con tecnica Frequency Hopping (FH).

Nella dispersione di spettro la larghezza di banda e la potenza del segnale hanno minore importanza rispetto ad altri aspetti più significativi della comunicazione, quali l'accesso multiplo e la robustezza alle interferenze.
In particolare, la trasmissione DS è una soluzione molto robusta per via della sua ridondanza (trasmette contemporaneamente diverse copie dei dati originali, il fattore di ridondanza al suo interno è chiamato *guadagno di processo*[6]) con cui si possono risolvere alcuni dei problemi che caratterizzano i canali wireless:

- le interferenze da rumore così come quelle derivanti da altri segnali sono minimizzate in ricezione, non contenendo la chiave del codice pseudocasuale (in pratica, il ricevitore ignora i segnali o i disturbi che non corrispondono alla rivelazione effettuata con la chiave pseudocasuale);
- le interferenze da cammini multipli (dovuti alla riflessione) sono ignorate, poiché i ritardi di propagazione dei cammini multipli sono tali da porre fuori sincronismo i segnali riflessi.

Poiché la trasmissione DS fornisce immunità agli errori di trasmissione (dovuti a interferenze o a basso rapporto S/N), in questo momento, è la più diffusa (ad es. è impiegata in ZigBee e Wi-Fi, che utilizzano impulsi modulati con tecnica Phase Shift Keying (PSK)).

A.VI.2. Tecniche Spread Spectrum per RFId

Nei sistemi a corto raggio, possono essere impiegate tecniche di modulazione Spread Spectrum in banda UHF [2].
Nei sistemi RFId con Tag passivi a basso costo le tecniche Spread Spectrum sono spesso utilizzate in maniera differente da quanto visto nel paragrafo precedente. Infatti per ottenere una vera modulazione DS o FH è necessaria una elevata complessità del Tag. Invece, nei sistemi reali, quest'ultimo continua, come di consueto, a lavorare modulando il backscatter, con la differenza che l'antenna ha una larghezza di banda che copre la banda del segnale Spread Spectrum. In tal modo il Tag è in grado di ricevere tutta la potenza proveniente sia da un segnale a banda stretta che salta tra le frequenze con tecnica FH sia da un segnale a banda larga generato con tecnica DS.
In entrambi i casi, però, i segnali devono essere modulati in ampiezza dal Reader per consentire al Tag di operare il backscatter.
Esistono anche sistemi RFId con Tag attivi basati su tecnologia UWB (trattata nel paragrafo A.VI.4), utilizzati spesso per sistemi di radiolocalizzazione in tempo reale (per la localizzazione si rimanda all'Appendice VII).

6 guadagno di processo = $10 \log \left(\frac{\text{bit rate sequenza pseudocasuale}}{\text{bit rate sequenza dati}} \right)$

A.VI.3. Sistemi Wi-Fi

Il *Wi-Fi* è una tecnologia che consente a terminali di utenza di collegarsi tra loro attraverso una rete locale in modalità wireless (WLAN) basandosi sulle specifiche dello standard IEEE 802.11.
La rete Wi-Fi è concettualmente paragonabile a una rete a copertura cellulare a piccola scala (locale), con dispositivi di ricetrasmissione radio come gli Access Point (AP) in sostituzione delle tradizionali stazioni radio base delle reti radiomobili (architettura client-server).
Per aumentare la zona di connettività di un singolo access point e poter coprire così una data area si usano comunemente più AP (e relative celle di copertura) collegati tra loro tramite cablaggio in rete locale. L'interfaccia radio AP-utente costituisce la rete di accesso, mentre la LAN cablata che collega tutti gli AP rappresenta la rete di trasporto. Le celle di copertura degli AP sono spesso parzialmente sovrapposte per evitare buchi di copertura del segnale, mentre la parte cablata è generalmente una rete Ethernet. I singoli AP hanno il compito d'inviare in broadcast alle stazioni ricetrasmittenti wireless nel loro raggio di copertura l'SSID che identifica la rete o le reti che stanno servendo.
La rete totale così ottenuta può essere connessa alla rete Internet per il tramite di un router usufruendo dei relativi servizi di Internet.
Sono possibili anche soluzioni architetturali senza dorsale cablata che collegano direttamente in maniera wireless gli Access Point consentendo loro una comunicazione come sistema wireless distribuito ovvero con scambio di informazioni interamente tramite le interfacce radio pur con una perdita in efficienza spettrale del sistema oppure architetture completamente wireless senza alcun AP (modello di architettura Peer-to-Peer) con ciascuna stazione base che riceve/trasmette direttamente da o verso altre stazioni.
La differenza del Wi-Fi con le altre reti a copertura cellulare risiede soprattutto nei protocolli di comunicazione che ridefiniscono i livelli fisico e di collegamento, per la parte radio, e il livello di trasporto, per la parte cablata.
In particolare dato che la trasmissione di ciascuna stazione avviene alla stessa frequenza operativa (2,4 o 5 GHz) per evitare collisioni in ricezione si utilizza il protocollo di accesso multiplo CSMA/CA.
I protocolli Wi-Fi consentono anche di adattare la velocità di trasmissione nella tratta wireless di accesso in funzione della distanza della stazione mobile ricetrasmittente dall'AP, minimizzando le perdite di trasmissione.
Le coperture delle antenne sono fondamentalmente di due tipi: omnidirezionali e direttive.
Con antenna omnidirezionale è possibile coprire fino a una distanza di 100 metri teorici (uso domestico) se non vi è alcuna barriera in linea d'aria (potenza di trasmissione di 100 mW). In presenza di muri, alberi o altro il segnale decade a circa 30 metri. Tuttavia, con più antenne direzionali, dal costo inferiore, la copertura potrebbe salire a 1 km.

Esistono varie classi di Wi-Fi con prestazioni diverse (come specificato nello standard IEEE 802.11), le principali sono:
- classe a ⇒ 54 Mb/s (5 GHz);
- classe b ⇒ 11 Mb/s (2,4 GHz);
- classe g ⇒ 54 Mb/s (2,4 GHz);
- classe n ⇒ 450 Mb/s (2,4 GHz e 5 GHz);
- classe ac ⇒ 3 Gb/s (5 GHz).

In Europa e nella gran parte del mondo, la banda Wi-Fi vede la presenza massiva di apparati radio LAN, tra cui primeggiano quelli con tecnologia Wi-Fi descritti nello standard IEEE 802.11a/g/n (nella banda 2.400-2.483,5 MHz)
In ambienti in cui siano già installate, per vari motivi, reti Wi-Fi ed in cui è programmato l'impiego di un numero non esorbitante di Tag attivi, può essere conveniente usare Tag che comunichino rispettando lo Standard Wi-Fi. In questo caso la funzione di Reader può essere svolta dal software di rete per mezzo della wireless LAN.
Nelle bande Wi-Fi potrebbero operare in Europa anche sistemi RFId non conformi allo standard Wi-Fi, sia con Tag attivi che passivi. In Europa infatti la banda 2.446 ÷2.454 MHz è tra quelle in cui possono operare i sistemi RFId. E questi potrebbero utilizzare tecnologie (protocolli, modulazioni, ecc.) differenti dal Wi-Fi.

A.VI.4. Sistemi UWB (Ultra Wide Band)

Con il termine UWB (*Ultra Wide Band*) si indica una tecnologia sviluppata per trasmettere segnali modulati a dispersione di spettro su bande molto larghe, dell'ordine di 500 MHz o più [2]. La normativa è caratterizzata da alcune differenze tra Stati Uniti ed Europa (frequenze assegnate comprese tra 3,1 e 10,6 GHz).
La tecnologia UWB opera con le seguenti caratteristiche:
- trasmissione per mezzo di onde radio;
- impulsi di durata estremamente ridotta, da poche decine di picosecondi a qualche nanosecondo, formati da pochi cicli dell'onda portante, e quindi con spettro risultante estremamente largo (in ogni istante la larghezza di banda è uguale o superiore al 20% della frequenza centrale di lavoro oppure è uguale o superiore a 500 MHz);
- segnale "mimetizzato" con il rumore di fondo, poiché un generatore di sequenze pseudocasuali è usato per generare impulsi ad intervalli di tempo casuali; inoltre, la potenza di trasmissione è talmente bassa che i segnali sono percepiti sotto la soglia del rumore da apparati che operano con altri tipi di modulazione sulle stesse bande (non si hanno quindi interferenze con altre trasmissioni modulate tradizionalmente);
- "Duty Cycle" limitato, per evitare interferenze con altre trasmissioni a modulazione tradizionale;
- resistenza alle interferenze per cammini multipli, a causa della brevità dell'im-

pulso che minimizza il problema dell'interferenza tra il segnale diretto e quelli riflessi durante il percorso (particolarmente adatto ad applicazioni di radiolocalizzazione - Real Time Location);
- capacità di penetrazione attraverso gli ostacoli (pareti o corpo umano);
- comunicazioni con capacità fino a circa 1/2 Gbit/s a distanza di qualche metro (high bit rate PAN).

La potenza media della trasmissione risente del valore di picco della potenza, cioè della potenza di ogni impulso, ma anche del duty-cycle del segnale, legato alla frequenza di ripetizione degli impulsi (Pulse Repetition Frequency - PRF).
La potenza di ogni impulso è strettamente legata al limite imposto dalla normativa sui valori della densità spettrale di potenza radiata isotropicamente (Equivalent Isotropically Radiated Power - EIRP), media e di picco. La possibilità di codificare i simboli informativi utilizzando impulsi di brevissima durata (molto inferiore alla durata del tempo di simbolo) permette di garantire alla comunicazione importanti caratteristiche, quali:
- valori di potenza media molto ridotti, per il fatto che di solito la durata T_p dei singoli impulsi utilizzati per codificare un simbolo è molto inferiore alla durata T_s del simbolo stesso: $T_p << T_s$;
- data-rate elevato[7], anche se una parte dell'occupazione di banda è dovuta alla codifica e non al contenuto informativo;
- alta capacità di penetrazione del segnale attraverso gli ostacoli, grazie all'ampio intervallo di frequenze in esso contenute;
- comunicazione difficilmente intercettabile perché codificata.

Nell'ambito dei sistemi di trasmissione UWB vi sono due opposte metodologie per limitare la densità spettrale di potenza:
- la prima è quella adottata dai sistemi short-range, high data-rate, in cui la frequenza di ripetizione degli impulsi è mantenuta elevata (la quantità di informazione inviata nell'unità di tempo è massimizzata): la frequenza di ripetizione degli impulsi assume perciò valori elevati e il rispetto dei limiti della densità spettrale di potenza radiata isotropicamente è garantito dalla riduzione della potenza dei singoli impulsi, con conseguente diminuzione del raggio di copertura spaziale della comunicazione.
- la seconda è quella adottata dai sistemi long-range, low data-rate, in cui è ridotta la frequenza di ripetizione degli impulsi, in modo da permettere la trasmissione di impulsi di potenza più elevata, al fine di garantire la massima distanza di copertura del segnale (anche centinaia di metri).

7 La capacità del canale radio in termini di bit-rate è data dalla formula di Shannon:

$$C = B \log_2 (1 + SNR)$$

dove C è la capacità del canale in bit/s, B è la banda del segnale trasmesso, e SNR è il rapporto segnale-le-rumore.

Rientrano nei sistemi che fanno uso della prima metodologia i sistemi di comunicazioni in cui sia necessario garantire un'elevata velocità di trasferimento dell'informazione (che può arrivare fino all'ordine dei Gb/s), con un raggio di copertura del segnale che non supera la decina di metri. Tali prerogative sono proprie delle reti wireless personali (WPAN, Wireless Personal Area Network), usate per lo streaming di dati o lo scambio veloce di informazione tra più utenti.
Appartengono ai sistemi che fanno uso della seconda metodologia ambiti applicativi come le reti di sensori (sensor network) in cui non sono richiesti alti data-rate ma può essere utile garantire un buon campo di copertura, oppure sistemi di identificazione a distanza di Tag:

- applicazioni logistiche (ad es.: il tracking di pacchi);
- applicazioni di security (ad es.: la localizzazione degli accessi ad aree controllate);
- applicazioni mediche (ad es.: il monitoraggio di pazienti);
- applicazioni domestiche (ad es.: comunicazione tra locali domestici, monitoraggio di infanti);
- applicazioni di sicurezza (ad es.: localizzazione di vittime di valanghe);
- applicazioni militari (ad es.: comunicazioni non intercettabili).

Alcune delle tecniche di modulazione più comuni utilizzate nei sistemi UWB sono riassunte nella tabella A.2.

Tabella A.2 - Confronto tra tecniche di modulazione UWB [2]

Modulazione	Codifica	Vantaggi	Svantaggi
On-Off Keying (OOK)	L'assenza e la presenza dell'impulso rappresentano rispettivamente i bit "0" e "1"	Semplice e realizzabile con trasmettitori a bassa potenza	Altamente sensibile al rumore; sincronizzazione critica soprattutto per trasmissioni di lunghe sequenze di 0 e 1
Pulse Amplitude Modulation (PAM)	Due livelli d'ampiezza rappresentano i bit "0" e "1"	Trasmettitori semplici (gli impulsi hanno la stessa polarità)	L'attenuazione nel canale radio la rende simile alla OOK
Pulse Position Modulation (PPM)	Codifica basata sulla posizione dei treni di impulsi trasmessi in una finestra temporale	Meno soggetta ad errori di decodifica rispetto a PAM o OOK	Necessita di sincronizzazione della temporizzazione estremamente precisa, drift o jitter possono determinare codifiche inaffidabili
Bi-Phase Shift Keying (BPSK)	I bit "1" e "0" sono rappresentati da impulsi di polarità opposta	Meno sensibile alla distorsione dato che la differenza tra i due livelli è il doppio dell'ampiezza di un impulso	Maggiore complessità nella realizzazione del trasmettitore (per gli impulsi di polarità differente)

Nell'ambito dell'applicazione delle tecnologie UWB a sistemi del tipo PAN (*Personal Area Network*) che operano con trasmissioni a corto raggio sono stati sviluppati metodi di trasmissione complessi nei quali l'intera banda disponibile per le emis-

sioni dei dispositivi UWB si suddivide in un certo numero di sotto bande (ciascuna delle quali di larghezza pari a circa 500 MHz), che sono opportunamente gestite in maniera coordinata per massimizzare le prestazioni della comunicazione.
Le molteplici proposte ricevute in ambito normativo IEEE (802.15.3a task group - TG3a) sono state fatte progressivamente convergere verso due approcci differenti:
- Direct Sequence UWB;
- Multi-Band OFDM.

Il sistema Direct Sequence UWB, conosciuto anche come "Direct Sequence Code Division Multiple Access" (DS-CDMA), può operare in due bande indipendenti: la prima da 3,1 GHz a 4,85 GHz (banda bassa), la seconda da 6,2 GHz a 9,7 GHz (banda alta) [2].
All'interno di ciascuna banda sono supportati fino a 6 canali con codici di accesso e frequenze di lavoro univoche. Un dispositivo conforme allo standard deve supportare obbligatoriamente i canali da 1 a 4 che sono quelli a frequenze più basse, mentre il supporto dei canali da 5 a 12 è opzionale.
Il sistema è basato sull'uso di due possibili tipi di sequenze:
- BPSK (binary phase shift keying), in cui il bit di dati determina semplicemente con quale polarità (+/-) è trasmesso il relativo codice della lunghezza desiderata.
- 4-BOK o Q-BOK (*Quaternary Bi-Orthogonal Keying*), in cui ogni simbolo trasferisce due bit di dati. La configurazione di ogni coppia di bit corrisponde ad uno tra due codici e ne determina anche la polarità.

Differenti velocità di trasmissione sono ottenute attraverso l'uso di codici a lunghezza variabile (da 1 a 24). Sono previste *codifiche con correzione d'errore* (FEC) convoluzionali aventi rapporti di 1/2 o di 3/4.
Le velocità di trasmissione supportate dal sistema sono di 28, 55, 110, 220, 500, 660, 1000 e 1320 Mbit/s.
Il supporto del metodo BPSK è obbligatorio mentre per il 4-BOK è obbligatoria la trasmissione ma la ricezione è opzionale (comunque la complessità aggiuntiva per la generazione di segnali 4-BOK rispetto a quanto già previsto per il BPSK è bassa).
Il sistema Multi-Band OFDM (Orthogonal Frequency Division Multiplexing) impiega di 122 sottoportanti non adiacenti ma sparse sulle varie bande [2]. Per semplicità circuitale, le sottoportanti sono modulate solo con tecnica QPSK.
Le velocità di trasmissione supportate dal sistema sono di 53,3, 55, 80, 106,67, 110, 160, 200, 320, e 480 Mbit/s. In particolare la capacità di trasmettere e ricevere alle velocità di 53,3, 106,67, 110, e 200 Mbit/s è una caratteristica che tutti i dispositivi devono obbligatoriamente possedere.
Sono previste *codifiche con correzione d'errore* (FEC) convoluzionali aventi rapporti di 1/3, 11/32, 1/2, 5/8, o 3/4.
Il sistema utilizza un *codice tempo-frequenza* (TFC) per l'interleaving dei dati codificati su 3 bande di frequenza (chiamate gruppo di bande). Sono definiti quattro gruppi di bande con tre bande ciascuno e un gruppo con 2 bande. Ciascuna banda

ha un'ampiezza di 528 MHz. Sono anche definiti 4 possibili TFC per i 4 gruppi (1÷4) di 3 bande ciascuno e 2 TFC per il gruppo 5 composto di 2 bande, in modo da poter avere 4 canali logici per banda (2 per la banda 5) per un totale di 18 canali logici separati (figure A.14 e A.15).

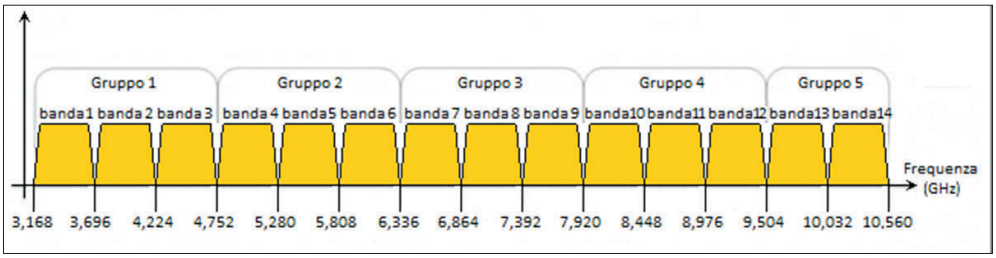


Figura A.14: Bande di frequenza per un sistema Multi-Band OFDM.

È obbligatorio che tutti i dispositivi siano in grado di operare in Modo 1 (gruppo delle prime tre bande a frequenza più bassa), il supporto degli altri gruppi di bande è opzionale.
I gruppi di bande così definiti sono dedicati a classi di applicazioni differenti (ad es. a lungo e corto raggio).
Per poter leggere i dati, il dispositivo ricevente deve essere sincronizzato con la trasmissione, conoscendo a quali intervalli di tempo e su quali frequenze i dati saranno trasmessi. Se il ricevente non è sincronizzato, non può distinguere una trasmissione OFDM dal rumore di fondo.

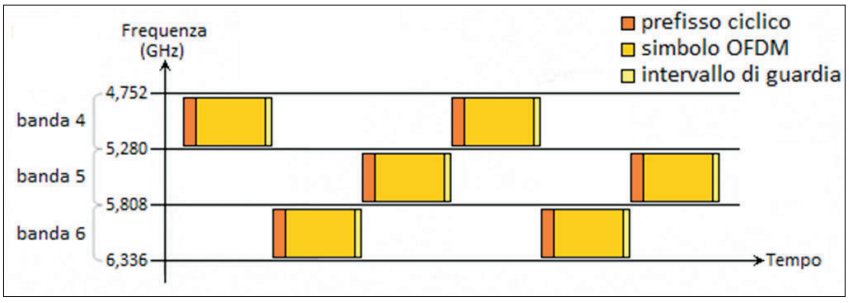


Figura A.15: Intervalli di tempo e frequenze nella trasmissione dei dati (due periodi temporali relativi ad uno dei codici TFC), in un sistema Multi-band OFDM.

A.VI.5. Sistemi Bluetooth LE

Bluetooth Low Energy (nota anche come Bluetooth LE e commercializzata come Bluetooth Smart) è una tecnologia radio digitale progettata per consumi considerevolmente bassi e portate brevi (10 metri - Wireless Personal Area Network).
È nata per lavorare fianco a fianco e come complemento di Bluetooth. Come Bluetooth e Wi-Fi, opera nella banda ISM (industriali, scientifici e medicali) dei 2,4 GHz, con una velocità di trasmissione del livello fisico di 1 Mb/s, simile a quella del Bluetooth, ma adotta una modulazione più semplice.
Il nome originario della tecnologia era Wibree. La tecnologia è stata inclusa nello standard Bluetooth nel 2010 con l'adozione del Bluetooth Core Specification Version 4.0.
In realtà Bluetooth LE non è compatibile all'indietro con la tecnologia Bluetooth originale ("Classic"), infatti la specifica Version 4.0 prevede che i dispositivi implementino l'uno o l'altro o entrambi i sistemi, condividendo la stessa antenna.
Nel 2011 è stato chiarito dal Bluetooth Special Interest Group (SIG) che:

- Bluetooth Smart Ready indica un dispositivo dual-mode, compatibile sia col Bluetooth Classic che col Bluetooth LE;
- Bluetooth Smart indica un dispositivo compatibile solo col Bluetooth LE, in grado di interagire solo con altri dispositivi Smart o con dispositivi Smart Ready.

La tecnologia Bluetooth LE, avendo cercato di superare i problemi di consumo e di complessità circuitale del Bluetooth Classic, estendendo la connettività locale a dispositivi di piccole dimensioni e di costi più contenuti, potrebbe essere impiegata per realizzare apparati con funzioni RFId.
Lo strato di collegamento (link layer) minimizza il consumo (nello stato "idle"), realizza un semplice meccanismo per la scoperta dei dispositivi presenti nel raggio di copertura radio e fornisce un servizio di trasferimento dati punto-multipunto affidabile, con funzionalità avanzate e crittografia dei dati.

A.VI.6. Sistemi ZigBee

ZigBee è una tecnologia nata con lo scopo di realizzare Wireless Personal Area Network più economiche di altre, soprattutto di quelle Bluetooth (che è per questo corsa ai ripari con la specifica di Bluetooth LE).
ZigBee fa uso di piccole antenne digitali a bassa potenza e basso consumo basate sullo standard IEEE 802.15.4. Lo standard individua una serie di profili applicativi che permettono di realizzare comunicazioni specifiche per diversi profili tipici del campo delle Wireless Sensor Network. I profili spaziano dal mondo dell'energia (Smart Energy) al mondo della domotica (Home Automation). In particolare, l'accento è posto sulla definizione di Wireless Mesh Network economiche, autoconfiguranti e autogestite che possano essere utilizzate per scopi quali il controllo indu-

striale, le reti di sensori, la domotica, e le telecomunicazioni, con consumo energetico tale da poter funzionare per uno o due anni sfruttando le batterie incorporate nei nodi.
Nel 2014 è stato annunciato un nuovo protocollo chiamato ZigBee 3.0, che ingloberà diversi profili applicativi oggi non interoperabili fra loro. Una volta rilasciato questo protocollo (che andrà a sostituire la specifica ZigBee PRO 2007) vi saranno di fatto solo 2 domini principali, uno per la Smart Energy e uno per l'Home Automation.
ZigBee opera nelle bande ISM (868 MHz in Europa, 915 MHz negli Stati Uniti e 2,4 GHz in tutto il mondo), ma ad oggi le uniche vere implementazioni disponibili sul mercato sono quelle a 2,4 GHz, in quanto in tale banda, la stessa utilizzata da Wireless LAN generiche come Wi-Fi e Bluetooth, nonché da qualche Tag RFId passivo, è possibile installare gli apparati in maniera libera, senza richiedere autorizzazioni.
Altri punti di forza di ZigBee sono la semplicità, che implica anche un basso costo per chip, e la crescita del numero massimo di apparati che possono essere connessi, rispetto ad altre reti.
La produzione di componenti elettronici che implementano funzioni di ZigBee e permettono la realizzazione di apparati più o meno conformi è iniziata già a partire dal 2004. I profili di applicazione, i programmi di certificazione e le specifiche complete ZigBee sono state rese disponibili nel giugno 2005.
I primi prodotti ZigBee sono apparsi nei settori dell'anti-intrusione e dei telecomandi per domotica dove esistevano solo prodotti proprietari, con scarse funzioni di rete e non integrabili con altri prodotti di terze parti.
ZigBee opera su distanze brevi (raggio teorico tra i dieci e i settantacinque metri) e con una modesta banda passante (al massimo 250 kb/s - low bit rate PAN). Questo perché l'obiettivo che si sono posti i suoi progettisti non è stato quello di operare con dispositivi "veloci", quali apparati di rete tradizionali, computer o terminali mobili, quanto, piuttosto, quello di operare con reti a basso bit rate che colleghino oggetti che non richiedono velocità, avendo poche informazioni da scambiare, a cui fornire la capacità di integrarsi in una rete. Questi oggetti hanno, piuttosto, bisogno di consumare poca energia e di funzionare per lungo tempo (mesi o anni) con le batterie incorporate. Il consumo elettrico limitato è stato possibili proprio grazie alla scelta di avere una banda ridotta e uno scarso raggio di azione.
Sfruttando lo standard ZigBee è possibile integrare un Tag su ogni sistema di comando, per quanto semplice esso sia (interruttore della luce, condizionatore, ventola, sistema di riscaldamento, serratura, uscita di emergenza, serranda automatica, sensori ambientali, allarmi, sbarra di uscita). In tal modo è possibile monitorare e controllare lo stato di tali sistemi in maniera centralizzata sia in ambiente domestico che in ambienti commerciali o industriali.
Le caratteristiche di ZigBee sono:
- Interfaccia radio di alto livello:
  ⇒ frequenza operativa universale: 2,4 GHz - 16 canali;

  - ⇒ modulazione: Direct Sequence Spread Spectrum;
  - ⇒ codifica: orthogonal QPSK (due bit per simbolo), nella banda 2,4 GHz;
- Elevata autonomia (specie dei nodi terminali, progettati per operare con batterie dalla durata variabile da tre mesi a tre anni, con conseguente riduzione dei costi di gestione della rete):
  - ⇒ applicazioni a bassissimo duty-cycle <0,1%;
  - ⇒ protocollo di accesso al canale di tipo beaconing network, oppure CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), (alto throughput e bassa latenza, per apparati che operano con basso duty-cycle come i sensori);
- Possibilità di realizzare reti Mesh (reti in cui i dispositivi possono divenire nodi di smistamento delle informazioni), caratteristica che estende la portata della rete, aumenta l'affidabilità e soprattutto la resistenza a interferenze e guasti di apparati, essendo possibile modificare i percorsi della comunicazione a seconda delle condizioni al contorno:
  - ⇒ topologie multiple di rete: Peer-to-Peer, Star, Mesh, Hybrid (Mesh-Star);
  - ⇒ gran numero di apparati collegabili: 18 miliardi di miliardi di dispositivi (indirizzamento a 64 bit);
  - ⇒ possibilità di avere più reti indipendenti nella stessa area: 65.535 reti;
- Limitata velocità di trasmissione (poiché una rete di sensori ed attuatori non necessita di banda larga):
  - ⇒ bit rate lordi disponibili all'interfaccia aerea: 250 kb/s a 2,4 GHz; 40 kb/s a 915 MHz; 20 kb/s a 868 MHz;
- Alta sicurezza del collegamento: sono incluse funzioni di autenticazione e crittografia simmetrica (AES-128) tra apparati, sia a livello di rete, che a livello MAC (Media Access Control - il secondo livello del modello ISO/OSI), che a livello applicativo:
  - ⇒ Tre livelli gerarchici di chiavi: Master Keys, Network Keys, Link Keys;
  - ⇒ Protocollo con PDU confermate (Fully hand-shaked protocol) per l'affidabilità della trasmissione;
- Operatività in un raggio tipico di circa 50 metri (da 5 a 500 m in base all'ambiente).

ZigBee opera con un'organizzazione gerarchica in cui sono definiti tre livelli di apparati:
- ZigBee Coordinator - ZC (detto anche *Controller*): è il dispositivo più "intelligente", costituisce la radice della rete ad albero e può operare come ponte verso altre reti, inoltre inizializza la rete, gestisce i vari nodi e opera la raccolta dati; ne esiste uno solo per ogni rete, contiene le informazioni sulla rete e le chiavi di sicurezza;
- ZigBee Router - ZR (detto anche *Full Function Device* - FFD): è un dispositivo che agisce come router intermedio, passando i dati da e verso altri dispositivi, di fatto non ha differenze hardware con un ZC e opera in modo identico, se non per il fatto che viene lasciato al Coordinator il ruolo di inizializzare la rete;
- ZigBee End Device - ZED (detto anche *Reduced Function Device* - RFD): è un dispo-

sitivo che include solo le funzionalità minime per dialogare con il nodo padre (Coordinator o Router), non può trasmettere dati provenienti da altri dispositivi; pertanto richiede il minor quantitativo di memoria e risulta più semplice ed economico, destinato agli oggetti (interruttori, TV, radio, lampade, elettrodomestici, ecc.) .

Si possono realizzare reti a topologia Mesh, in cui sottoreti a stella (uno ZR che coordina diversi ZED) si interfacciano mediante collegamenti diretti fra ZR.
Sono possibili due modalità operative distinte:
- in modalità Beacon Enabled i Router (ZR) comunicano sulla rete dei beacon a intervalli regolari per confermare la loro presenza agli altri nodi; tra un beacon e l'altro gli altri nodi (ZED) possono cambiare modalità per risparmiare energia, abbassando il duty cycle; per questioni di economia energetica il sistema cerca di funzionare minimizzando il tempo di attività dei sistemi, ma intervalli di beaconing lunghi richiedono una temporizzazione precisa, che comporta aumenti di costo;
- in modalità Non-Beacon Enabled è utilizzato un meccanismo di accesso al canale di tipo unslotted CSMA/CA (il terminale verifica che il canale sia libero prima di trasmettere e ritrasmette in caso di collisione), che rende asimmetrico l'impiego della potenza da parte dei dispositivi;, infatti i Router (ZR) hanno i ricevitori sempre accesi (e questo provoca consumo energetico) mentre gli altri nodi (ZED) sono spenti per la maggior parte del loro tempo e si attivano per trasmettere in presenza di uno stimolo esterno (consumando energia solo nel momento della trasmissione, poi, al termine, ricevono il segnale di "acknowledge" e tornano inattivi).

A.VI.7. Sistemi Contactless NFC (Near Field Communication)

La tecnologia NFC (*Near Field Communication*) è derivata dalla tecnologia degli RFId e da quella delle smartcard. Le specifiche sono emesse dall'NFC Forum, nato nel 2004.

Le caratteristiche più importanti degli NFC sono:
- comunicazione a corto raggio (fino a 10 cm);
- superamento sia della distinzione tra Reader e Tag, sia di quella tra apparati attivi e passivi;
- integrazione nello stesso chip delle funzioni di una smartcard senza contatto e di un Reader;
- frequenza operativa 13,56 MHz (come le smartcard) e compatibilità opzionale con le carte ISO/IEC 14443 o ISO/IEC 15693;
- comunicazione a bit rate moderato (velocità massima di 424 kbit/s).

Le principali applicazioni comprendono:
- transazioni per ticketing (realizzate con un palmare o un telefono cellulare del-

l'utente a cui è associato un NFC che si interfaccia con obliteratrici di biglietti, parchimetri o altri dispositivi, dotati anch'essi di NFC);
- pagamenti sicuri (utilizzando i dati della carta di credito o della SIM per telefonia mobile);
- comunicazioni di vario genere tra apparati elettronici.

Gli NFC non sono progettati per operare in rete di dispositivi o per la trasmissione di grandi moli di dati, ma per consentire un opportuno scambio dati tra Tag a basso costo (ad es. etichette RFId) e dispositivi elettronici (ad es. palmare o telefoni cellulari).
Un dispositivo NFC può interrogare come un Reader ed essere interrogato come un Tag e, quando opera come Tag, può funzionare in modalità attiva o passiva. Pertanto la comunicazione può operare in modi diversi. Il modo in cui i dati sono trasmessi dipende da ciò.
Nella comunicazione tra NFC, oltre alla modalità attiva e passiva, un dispositivo può gestire due differenti (ed intercambiabili) ruoli:
- *initiator*, che invia un messaggio ("*message*");
- *target*, che invia una risposta ("*reply*") al messaggio);

dove "message" e"reply" sono le due primitive fondamentali per la comunicazione. Questo significa che il dispositivo 1 manda un messaggio ad un dispositivo 2 che deve rispondere. Non è possibile che il dispositivo 2 invii dati al dispositivo 1 senza ricevere prima un messaggio da questo.
I ruoli non sono entrambi compatibili con tutte le modalità operative. Nella modalità operativa passiva, i dati delle "reply" sono inviati nella modalità consueta dei Tag passivi ad accoppiamento induttivo (modulazione del carico dell'antenna ricevente). Il messaggio inviato da un initiator può essere ricevuto da una molteplicità di target, ma l'initiator seleziona il target da cui vuole la risposta, gli altri non risponderanno. Non sono infatti previsti messaggi broadcast che provochino la risposta contemporanea di più target.
I dati sono sempre codificati col metodo Manchester.
La modulazione dipende dalla velocità di trasmissione e dalla modalità operativa. Per 106 kbit/s è usato un indice di modulazione pari al 100% (l'ampiezza del segnale modulato varia da zero all'ampiezza massima della portante) ed è modulata una sottoportante. Per velocità superiori, è usato un indice di modulazione pari al 10% ed è modulata la portante a 13,56 MHz.
Gli NFC possono essere utilizzati per l'accoppiamento di apparati (Device Pairing), grazie alle funzionalità dell'NFC per l'autenticazione rapida e sicura.
Infatti, lo scambio di informazioni fra dispositivi, tramite il contatto o l'avvicinamento a una distanza di pochi cm, genera la configurazione di una rete peer-to-peer senza la necessità di ulteriori passaggi di abilitazione. I dispositivi possono poi comunicare a distanze molto maggiori con protocolli più veloci quali Wi-Fi o Bluetooth, data la minore capacità dell'NFC rispetto a questi.

A.VI.8. Disattivazione intenzionale di dispositivi

Un aspetto critico che interessa soprattutto i dispositivi attivi riguarda la possibilità di disattivare intenzionalmente a distanza un dispositivo, ad esempio con un aggiornamento del software o disattivando un servizio necessario per il funzionamento del dispositivo stesso.
In un mondo che si appresta ad avere automobili che si guidano da sole, dispositivi medici o altri dispositivi necessari per la salute e la sicurezza delle persone controllati a distanza, la possibilità di disattivare simili dispositivi a scopi commerciali (la scadenza di un abbonamento) pone seri interrogativi proprio riguardo alla salute e alla sicurezza.

A.VI.9. Rischi per la salute

La maggior parte delle tecnologie wireless considerate finora (Wi-Fi, Bluetooth LE, Zigbee, NFC) hanno bassi livelli di potenza, variabili però con la tecnologia. Ad esempio i comuni router Wi-Fi emettono a potenze di norma non superiori a 100 milliwatt, molto inferiori a quelle dei telefoni cellulari (1 watt circa, in standby).
Il Wi-Fi ha un'enorme diffusione negli uffici e negli ambienti domestici. A proposito di questi ultimi ambienti, data la concentrazione abitativa nelle città, è possibile che all'interno di un appartamento le emissioni del Wi-Fi possano raggiungere valori di densità di potenza paragonabili con quelli della telefonia mobile.
Tuttavia, la maggior parte delle agenzie nazionali di salute pubblica non vede alcun motivo per cui il Wi-Fi non dovrebbe continuare a essere utilizzato, anche se le stesse agenzie aggiungono anche il consiglio di prendere precauzioni, come con i telefoni cellulari, in attesa di ulteriori studi che approfondiscano la situazione.

Appendice VII
La localizzazione indoor

A.VII.1. Sistemi di localizzazione indoor

Un sistema di localizzazione indoor (indoor positioning system - IPS) è un sistema per localizzare oggetti all'interno di edifici utilizzando agenti fisici diversi (segnali elettromagnetici, acustici, ottici). I diversi agenti fisici sono usati per ottenere una stima della distanza dell'oggetto di interesse (terminali, Tag) da una serie di nodi (stazioni, Reader) collocati in posizione nota. Esistono diversi sistemi sul mercato, ognuno con standard proprio.
Dai primi anni '90 la localizzazione di persone e oggetti per usi civili è stata resa accessibile ad un vasto bacino di utenti grazie al sistema satellitare GPS (Global Positioning System), utilizzato in seguito sempre più diffusamente grazie alla costante riduzione delle dimensioni dei suoi terminali.
Il GPS è basato su di una costellazione di satelliti in orbita che inviano informazioni in broadcasting verso i terminali mobili sulla terra. Dalle informazioni ricevute i terminali mobili sono in grado di ricavare indicazioni sulle coordinate geografiche, sull'altitudine rispetto al livello del mare e sull'orario.
Attualmente accanto allo statunitense GPS è attivo anche il sistema russo GLONASS, mentre sono allo studio altri sistemi, tra cui l'europeo Galileo.
Il GPS consente la localizzazione di terminali mobili con la precisione di pochi metri, per i dispositivi più economici, ma si possono raggiungere anche precisioni inferiori al metro, in applicazioni militari.
Rimane in ogni caso fondamentale per il corretto funzionamento, che il terminale GPS riceva informazioni da almeno quattro dei satelliti della costellazione (visibilità satellitare), per la determinazione delle coordinate spaziali.
In mancanza di visibilità satellitare la localizzazione non può avvenire. È il caso, ad esempio, degli ambienti chiusi (localizzazione indoor).
All'interno di tali ambienti il segnale è degradato a causa dell'attenuazione dovuta all'assorbimento causato dai materiali da costruzione e a causa delle riflessioni (cammini multipli). In realtà problemi simili si hanno per tutti i sistemi di localizzazione indoor basati su onde elettromagnetiche.
Nonostante i problemi tecnici, localizzare con una sufficiente accuratezza una persona o un oggetto all'interno di un ambiente chiuso può essere, a volte, molto utile, se non addirittura necessario (si pensi alla gestione delle emergenze o alla

dislocazione dei macchinari in un ambito produttivo o degli elettromedicali in un ambito ospedaliero).
Pertanto, negli ultimi anni si è cercato di sviluppare dei metodi di localizzazione indoor di tipo non GPS, sfruttando le informazioni ottenibili da segnali radio utilizzati per le comunicazioni tra dispositivi, in modo da determinare la posizione di terminali mobili all'interno di ambienti chiusi. Una simile opportunità è stata possibile grazie anche al continuo sviluppo dei sistemi di comunicazione wireless, per la telefonia cellulare o per l'accesso ad internet, che ha portato ad un notevole aumento della distribuzione geografica delle reti wireless basate su tali sistemi.
Un sistema RFId può essere usato per la localizzazione?
In realtà la distanza di lettura degli RFId passivi è generalmente limitata.
I Tag attivi, invece, usano una batteria per alimentare la circuiteria e trasmettere il segnale, ciò consente distanze operative notevolmente superiori, benché ancora limitate.
Nei prossimi paragrafi sono illustrati metodi per utilizzare la tecnologia RFId o le tecnologie trattate nell'Appendice VI come sistemi di localizzazione.

A.VII.2. Real-time locating systems

Intorno alla fine del millennio, è nato il concetto di sistema di localizzazione in tempo reale (Real-time locating systems - RTLS), relativo a sistemi in grado di identificare e tracciare oggetti in tempo reale (mostrandone la posizione sullo schermo di un PC), di solito all'interno di un edificio o di un'area confinata (tali sistemi non sono stati studiati per fornire coperture globali come il GPS).
La tecnologia si è sviluppata determinando la posizione di Tag, applicati ad oggetti o indossati dalle persone, rispetto a Reader in posizione nota (di solito opportunamente distribuiti e spaziati all'interno dell'area da coprire e a seconda della precisione richiesta).
Sistemi RTLS sono usati nella localizzazione di prodotti (automobili) lungo la catena di montaggio, di merci in un magazzino, di elettromedicali in un'azienda sanitaria.
Alcuni usi possibili sono i seguenti:
- localizzazione di oggetti all'interno di un'area;
- generazione di notifiche quando uno degli oggetti ha lasciato l'area;
- identificazione di oggetti multipli che occupano la stessa locazione (ad es. lo stesso pallet);
- localizzazione di clienti all'interno di un esercizio commerciale, per la consegna dei beni acquistati;
- localizzazione di detenuti all'interno dei luoghi di correzione, allo scopo di ottimizzare la presenza del personale di controllo e di verificare gli accessi in aree controllate;
- verificare la permanenza di personale all'interno di aree soggette ad evacuazione di emergenza, al fine di ottimizzare eventuali operazioni di soccorso;

- tracciamento (con indicazione temporale) di persone o oggetti all'interno di un "processo" (ad esempio la durata della permanenza di un paziente all'interno del Pronto Soccorso, il tempo speso all'interno della sala operatoria, il tempo totale di permanenza nella struttura sanitaria fino alla dismissione), allo scopo di migliorare il "processo" stesso;
- localizzazione dei pazienti nelle strutture sanitarie e gestione di eventuali casi acuti che dovessero presentarsi;
- localizzazione dei lavoratori all'interno delle aziende.

L'ultimo uso evidenziato può essere vista come una parziale rinuncia alla privacy del lavoratore, ma potrebbe essere di estrema utilità in caso di situazioni di emergenza (ad esempio durante l'esodo di una struttura potrebbe essere utile sapere che non vi siano più lavoratori all'interno di zone pericolose).

A.VII.3. Tecniche di localizzazione

Localizzare un dispositivo all'interno di una rete richiede lo scambio di segnalazioni tra il dispositivo da localizzare (nodo target) e alcuni nodi di riferimento di cui è nota la posizione. Le tecniche di localizzazione si distinguono per il parametro utilizzato per la stima della distanza: angolo di arrivo, attenuazione del segnale ricevuto, ritardo di propagazione.

A.VII.3.1. Localizzazione per mezzo dell'angolo di arrivo del segnale

Per localizzare un nodo in uno spazio bidimensionale si possono misurare gli angoli di arrivo (Angle of Arrival - AoA) di segnali che giungono ad almeno due ricevitori. Gli angoli sono quelli formati, rispetto ad una direzione predeterminata, dalle rette di congiunzione del nodo target con i nodi di riferimento (figura A.16). L'angolo di arrivo può essere determinato misurando la differenza temporale di arrivo (Time Difference of Arrival - TDoA) dello stesso segnale ad antenne diverse dello stesso array. Altri ricevitori invece, basati su array di antenne fortemente direzionali, determinano l'angolo di arrivo individuando l'antenna che ha ricevuto il segnale.

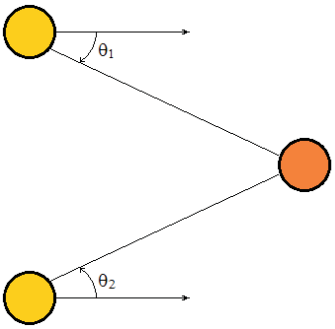


Figura A.16: Localizzazione attraverso stime angolari. La valutazione della posizione planare del nodo target avviene stimando gli angoli (θ_1 e θ_2) formati, rispetto ad una direzione di riferimento, dalle congiungenti dei nodi localizzatori con il nodo target.

A.VII.3.2. Localizzazione per mezzo dell'attenuazione del segnale ricevuto

Per misurare la distanza da un nodo è possibile misurare l'attenuazione subita dal segnale radio, infatti questa dipende dalla distanza percorsa. L'indicazione della potenza del segnale ricevuto (Received Signal Strength Indication - RSSI) permette di ricavare una stima della distanza tra trasmettitore e ricevitore, poiché la densità di potenza ricevuta decresce con l'inverso del quadrato della distanza (in condizioni di campo lontano e se non devono essere considerate altre cause di errore).
Tale metodo di localizzazione necessita, però, di una valutazione affidabile dei parametri che caratterizzano la propagazione del segnale attraverso il canale radio.
Purtroppo all'interno degli edifici, a causa delle riflessioni e dell'assorbimento dei muri, il metodo perde in accuratezza. Per ridurre l'incertezza si ricorre anche al filtraggio stocastico dei dati.
Per localizzare un nodo target in uno spazio bidimensionale si possono misurare le distanze del nodo da altri tre nodi di riferimento (figura. A.17).

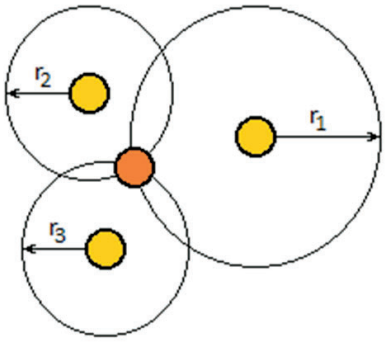


Figura A.17: Localizzazione attraverso stime di distanza. La valutazione della posizione planare del nodo target avviene stimando la distanza del nodo target rispetto a tre nodi di riferimento, in base all'attenuazione subita dal segnale o al suo ritardo di propagazione.

A.VII.3.3. Localizzazione per mezzo del tempo di arrivo o del ritardo di propagazione del segnale

Il tempo di arrivo (Time of Arrival - ToA) è il tempo impiegato dal segnale per giungere dal trasmettitore al ricevitore. Assumendo costante la velocità di propagazione del segnale (nel caso di mezzo omogeneo ed isotropo), il tempo di arrivo del segnale consente la misura della distanza tra i due nodi. La combinazione di tre o più misure, rispetto ad altrettanti nodi di posizione nota, consente la localizzazione (triangolazione) del target.
I sistemi che usano il tempo di arrivo, di solito ricorrono a complessi meccanismi di sincronizzazione per fare in modo che la sorgente temporale su cui sono basati i sensori sia affidabile.
Se due nodi hanno uno stesso clock di riferimento, il ricevitore può misurare il ritardo di propagazione che il segnale, inviato dal trasmettitore all'istante concordato, impiega ad attraversare la tratta radio che separa i due nodi.
La precisione del sincronismo tra i nodi può limitare la massima accuratezza. Se può essere garantita la sincronizzazione solo tra due nodi localizzatori, si può comunque garantire una stima differenziale del ritardo di propagazione (Time Difference of Arrival - TDoA).
La stima differenziale, permette di ridurre l'incertezza della posizione del bersaglio ad una regione spaziale che è un iperbole con i fuochi sui due localizzatori.
Per stabilire la posizione puntuale del trasmettitore, anche in questo caso è necessario un terzo localizzatore.
Nel caso non ci sia sincronizzazione tra i due nodi localizzatori, una stima del ritardo andata-ritorno (ritardo di propagazione), dal trasmettitore ai due nodi, può essere utilizzata per misurare la distanza relativa.
Nei locali indoor l'accuratezza dei metodi che utilizzano il tempo di arrivo risente spesso di problemi dovuti ai numerosi cammini multipli, per via delle riflessioni causate dai muri, dalle aperture e dagli infissi. Tali effetti possono essere ridotti ricorrendo a tecniche basate sulla diversità spaziale o temporale.

A.VII.3.4. Localizzazione per mezzo di tecniche miste

Spesso si ricorre a più tecniche di localizzazione contemporaneamente: le stime ottenute con una tecnica sono integrate o corrette con quelle ottenute con un'altra, al fine di migliorare la precisione complessiva. Ad es.:

- forme d'onda di durata brevissima possono essere utilizzate in congiunzione con le tecniche di localizzazione basate sulle stime angolari, queste sono influenzate negativamente dalle riflessioni multiple, ma l'alta risoluzione temporale (minima durata, cioè banda ampia) delle forme d'onda di durata brevissima permette di eliminare il problema dell'interferenza tra il segnale diretto e quelli riflessi (multipath): il segnale diretto, infatti, è tanto breve da essere ricevuto ed elaborato ben prima che arrivino i segnali riflessi;

- la localizzazione per mezzo dell'attenuazione del segnale può essere resa più precisa con le informazioni sulla posizione del trasmettitore che si ottengono utilizzando anche le stime temporali.

A.VII.4. Esempi

A.VII.4.1. Wi-Fi positioning system

Il Wi-Fi- positioning system (WPS) si basa sull'indicazione della potenza del segnale ricevuto (RSSI).
L'SSID (service set identifier, è il nome con cui una rete Wi-Fi o in generale una WLAN si identifica ai suoi utenti) e il MAC address (Media Access Control - il secondo livello del modello ISO/OSI) del punto di accesso sono inviati ad un database in cui è registrata la posizione geografica del ricevitore, ciò permette la localizzazione dei dispositivi che si mettono in contatto con i ricevitori.
L'accuratezza dipende dal numero di ricevitori la cui posizione è registrata nel database. Possibili fluttuazioni del segnale possono ridurre tale accuratezza, che è in grado comunque di raggiungere una precisione di 3 - 5 m metri (fortemente dipendente dalle condizioni ambientali).

A.VII.4.2. Prossimità con sistemi Bluetooth

Sulla base delle specifiche tecniche del Bluetooth, tale sistema può essere usato per indicazioni di prossimità indoor e non di localizzazione, anche se sistemi di micro-mappatura indoor basati sul Bluetooth o su Bluetooth LE sono stati realizzati.

A.VII.4.3. Metodo dei passaggi obbligati

Quando un sistema RFId non permette di calcolare la potenza del segnale ricevuto o l'angolo di arrivo del segnale, una stima della localizzazione può essere comunque ottenuta sfruttando le pur minime possibilità offerte dal sistema. Ad esempio è possibile ricorrere a passaggi obbligati. I Reader, posizionati in prossimità dei passaggi registrano la presenza dei Tag. Conoscendo la posizione dei Reader lungo un determinato percorso è possibile conoscere la traiettoria dell'oggetto a cui il Tag è associato (metodi simili possono essere applicati alle catene di montaggio, ai "processi" di produzione, allo smistamento di merci in un magazzino, allo smistamento di pacchi postali, allo smistamento bagagli in aeroporto).

A.VII.4.4. Griglia di Reader

Il metodo precedente può essere esteso fino a comprendere una griglia di Reader a corto raggio che ricopre un'area di interesse. Il Reader attivato fornisce una stima della posizione del Tag di interesse.

A.VII.4.5. Mobile phone tracking

È possibile tracciare la posizione di un terminale mobile per telefonia utilizzando informazioni ottenute da diverse stazioni radio base vicine. Il processo non richiede una chiamata attiva, è sufficiente l'emissione di un segnale di roaming da parte del terminale.
Il sistema misura la potenza ricevuta dalle diverse stazioni radio base vicine e, sulla base della conoscenza della posizione di queste è in grado di avere stime delle distanze utilizzabili per triangolare il terminale. I sistemi più avanzati possono aggiungere anche l'informazione del settore per diminuire il numero di informazioni necessarie (il settore più la distanza) per ottenere una stima (grezza) della posizione.
In ambiente urbano, con alta densità di stazioni radio base vicine (micro-celle, con molti settori), si possono raggiungere precisioni di 50 m. Il sistema Assisted GPS (A-GPS) integra le informazioni del GPS con quelle della rete per ricavare la posizione.

A.VII.4.6. Near-field electromagnetic ranging

Il Near-Field Electromagnetic Ranging (NFER) è una tecnologia radio che utilizza le proprietà dei campi elettrico e magnetico vicini, per calcolare la distanza da un'antenna.
Vicino all'antenna i campi elettrico e magnetico emessi (campi vicini) sono sfasati di 90°. Lontano dall'antenna (campi lontani) lo sfasamento si riduce a zero. Se il ricevitore, trovandosi nella zona di campo vicino, è in grado di misurare separatamente i campi elettrico e magnetico e può comparare le rispettive fasi, ciò può essere utilizzato per stimare la distanza dal trasmettitore.
A seconda della frequenza usata (comunque al di sotto dei 30 MHz), il metodo può avere una risoluzione variabile da 30 cm (frequenze più alte) a 300m (frequenze più basse).
La tecnologia offre i seguenti vantaggi:
- non sono richiesti segnali modulati, pertanto possono essere usati anche segnali in banda base, con banda arbitrariamente piccola;
- non è richiesta una precisa sincronizzazione tra diversi nodi fissi;
- lo sfasamento tra i campi resta immutato anche se i segnali sono traslati in banda base

Il metodo è più efficiente alle frequenze più basse (zone di campo vicino più estese), però in tal caso le antenne, che di solito operano a mezz'onda o a un quarto d'onda, sono più grandi, con gli svantaggi che ne conseguono (l'uso di antenne più corte riduce significativamente il guadagno e, conseguentemente, ciò limita la distanza di funzionamento).

A.VII.4.7. Localizzazione con sistemi UWB

La localizzazione basata su stime angolari non è ottimale nel caso di sistemi Ultra Wide Band (UWB):
- le antenne direttive precludono la possibilità che il sistema sia a basso costo;
- in presenza di ostacoli si hanno cammini riflessi che rendono difficoltosa la stima della direzione di arrivo del cammino principale.

Neanche la localizzazione basata su stime dell'attenuazione è ottimale nel caso di sistemi UWB:
- a causa della breve durata degli impulsi inviati, è possibile ottenere, per le distanze misurate, un'accuratezza teorica molto elevata, ma, l'accuratezza reale è notevolmente inferiore, in quanto limitata dalla minima distanza spaziale che può produrre un'attenuazione misurabile;
- è necessaria la scelta di una modulazione degli impulsi che non preveda operazioni di codifica tali da alterare l'energia delle forme d'onda: in tal senso, sono da preferire alla PSM (Pulse Shape Modulation) altri tipi di codifica dell'informazione, come la PPM o la BPSK.

Ciò fa preferire, nei sistemi UWB, strategie di localizzazione che si basano sul tempo di arrivo:
- l'accuratezza del posizionamento spaziale del target rispetto ai nodi, si può migliorare aumentando la banda effettiva del segnale (per esempio l'utilizzo di un impulso di banda pari a 1,5 GHz può garantire un'accuratezza di localizzazione pari al centimetro, con un rapporto segnale-rumore, SNR, di 0 dB).

In termini di accuratezza i sistemi UWB raggiungono teoricamente una precisione di 15-30 cm.
Pertanto, se è necessario che la localizzazione indoor abbia una precisione inferiore ad un metro, allora utilizzare tali sistemi è una soluzione tecnologicamente efficace.
Le caratteristiche dei sistemi UWB permettono i seguenti vantaggi:
- alta precisione di localizzazione del dispositivo che sta trasmettendo (dell'ordine dei centimetri), grazie alla brevissima durata di ogni singolo impulso;
- dispositivi Tag attivi con basso consumo energetico e quindi con lunga durata operativa (da 1 a 5 anni).

Appendice VIII
Riferimenti

[1] D.Lgs. del 9 Aprile 2008 n. 81 e successive modificazioni ed integrazioni "Attuazione dell'articolo 1 della legge 3 agosto 2007 n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro"

[2] AA.VV., RFId Tecnologie per l'innovazione, Fondazione Ugo Bordoni, 2006 - Sez. I, RFId Tecnologia e Applicazioni, di P. Talone e G. Russo.

[3] http://www.mondorfid.com/index.asp

[4] G. L. Amicucci, F. Fiamingo, I sistemi RFid in applicazioni di sicurezza, "Costozero", n. 6, luglio 2012, pp. 48-49, Ed. del Mediterraneo.

[5] ISO 7498, Information Processing Systems - Open Systems Interconnection - Basic Reference Model - The Basic Model - Security Architecture - Naming and addressing - Management framework

[6] L. Battezzati, J. L. Hygounet, RFID - Identificazione automatica a radiofrequenza, Ulrico Hoepli Editore, Milano, 2003

[7] C. Patierno, Viaggio nel mondo RFID, http://punto-informatico.it, 2004

[8] G. Holzmann, Design and Validation of Computer Protocols, Prentice Hall, Englewood Cliffs (NJ), 1991

[9] Gea Lab, Breve storia dell'RFID, http://www.rfid-lab.it

[10] E. Cerroni, RFID: La Tecnologia dei Sistemi a Radio Frequenza, http://www.i-dome.com, 2004

[11] S. Petrizzelli, Protocolli di linea, http://www.sandropetrizzelli.it, 2001

[12] F. Buffa, Modulazioni numeriche, http://www.ilmondodelletelecomunicazioni.it

[13] P. Ciaccia, D. Maio, Lezioni di Basi di Dati, Litopress Esculapio, Bologna, 2000

[14] ISO/IEC 18000-6:2004, Information technology - Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz, 2004

[15] ISO/IEC 14443, Identification cards - Contactless integrated circuit(s) cards -

Proximity cards - Physical characteristics, Radio frequency power and signal interface - Initialization and anticollision - Transmission protocol,

[16] ISO/IEC 15693, Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Physical characteristics - Air interface and initialization - Anticollision and transmission protocol,

[17] F. Cascetta, M. De Luccia, Sistemi di identificazione personale, http://www.mondodigitale.net, 2004

[18] G. Bianchini, RFID: Tecnologia e impatto sulla privacy, http://camp.olografix.org, 2004

[19] Gea Lab, Le memorie dei transponder, http://www.rfid-lab.it

[20] Accenture, White Paper - Radio Frequency Identification (RFID), 2001

[21] D. M. Dobkin, T. Wandinger, A Radio-Oriented Introduction to Radio Frequency Identification, High Frequency Electronics, 2005

[22] Tektronix, Radio Frequency Identification (RFID) Overview, 2004

[23] Atmel, Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards, http://www.atmel.com/images/doc2056.pdf

[24] AA.VV., Using ISO 15693 Compliant RFID Tags in an Inventory Control System, https://www.ieee.org/education_careers/education/standards/using_iso_15693_compliant_rfid_tags.pdf

[25] W.R. Smythe, Static and Dynamic electricity, McGraw Hill, 1950.

[26] Clayton R. Paul, Introduction to electromagnetic compatibility, John Wiley & Sons, 2006.

[27] F. Buffa, Propagazione, http://www.ilmondodelletelecomunicazioni.it

[28] A. Montanari, Misure elettroniche, Ed. Cupido, 1989.

[29] E. Walk Standard RFID per la logistica: la situazione attuale, http://www.rfid.it, 2004

[30] EVB Elektronik, RFId selection Guide, https://cdn-shop.adafruit.com/datasheets/rfid+guide.pdf

[31] ISO 14119, Safety of machinery - Interlocking devices associated with guards - Principles for design and selection

[32] ISO 13849-1:2015, Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design