INDICE

Introduzione

La seguente tesi esamina una delle tecnologie wireless più promettenti nel campo dell'identificazione, ossia la tecnologia RF-ID ed i problemi legati alla localizzazione, alla sicurezza e alla privacy degli utenti.

All'inizio della trattazione viene fatta una panoramica dei sistemi wireless (dall'inglese "senza fili"), focalizzando l'attenzione sulle più emergenti tecnologie come il 3G e 4G, ossia la terza e la quarta generazione delle comunicazioni mobili, la tecnologia Wi-Fi, il Wi-MAX, le reti Ad-Hoc MANET con la loro applicazione in ambito veicolare (le reti Ad-Hoc VANET) e la tecnologia di identificazione RF-ID, che è l'argomento della tesi.

La tecnologia RF-ID, dall'inglese Radio Frequency Identification, permette di identificare un qualsiasi oggetto in uno spazio circoscritto, grazie alle onde a radiofrequenza (RF). Lo scopo di questa tecnologia è quella di fornire informazioni su oggetti, animali e persone, attraverso i dispositivi a radiofrequenza e fa parte delle cosiddette tecnologie di autoidentificazione (AUTO-ID technology). Il codice a barre è un esempio di tecnologia di autoidentificazione in cui è richiesto un intervento umano per poter essere letto. L'RF-ID invece è stato creato in modo che il reader è in grado di comunicare con il tag (ossia l'etichetta), leggere i suoi dati e trasmetterli ad un computer senza alcun intervento umano.

L'RF-ID può essere utilizzato per monitorare ad esempio la sicurezza sul lavoro, il tracciamento di pratiche, l'assistenza e la manutenzione, l'identificazione degli animali, le biblioteche (come la rilevazione del patrimonio librario e il movimento dei libri), l'antitaccheggio e la rilevazione dei parametri ambientali.

I dispositivi RF-ID si dividono in due categorie, attivi e passivi. Gli RF-ID attivi hanno un trasmettitore ed una fonte di energia (ad esempio una batteria) propria per poter funzionare e sono in genere di lettura/scrittura, ossia i dati possono essere riscritti e/o modificati sul tag. Gli RF-ID passivi, invece, non sono in grado di trasmettere, ma riflettono al reader, attraverso un'antenna, le onde radio che esso gli invia. Gli RF-ID passivi sono molto più leggeri degli RF-ID attivi, meno costosi, e offrono una vita operativa illimitata. I sistemi RF-ID si distinguono, inoltre, anche per i loro range di frequenza:

A **bassa frequenza (da 30 KHz a 500 KHz):** sono utilizzati per letture brevi e hanno costi più bassi. Essi vengono utilizzati negli ambiti della sicurezza, nelle attività di monitoraggio, nell'identificazione degli animali e delle applicazioni;

- Ad **alta frequenza (da 850 MHz a 950 MHz e da 2.4 GHz a 2.5 GHz):** i sistemi offrono un range con letture a maggiore distanza e ad alta velocità e vengono utilizzati per applicazioni come le ferrovie e il monitoraggio automatizzato delle auto.

Un sistema RF-ID è composto da due elementi fondamentali, il tag e il reader, che comunicano attraverso dei segnali a radio frequenza (RF), per cui non c'è bisogno di un contatto fisico e che gli apparati siano vicini :

- I **tag o trasponder**: sono dei dispositivi a radiofrequenza di piccole dimensioni che permettono di trasmettere i dati.

- Il **reader**: è un ricetrasmettitore che ha la funzione di interrogare e ricevere le informazioni provenienti dai tag.

Negli anni '90 la tecnologia RF-ID inizia ad essere sempre più presente nelle applicazioni di massa. Un esempio è rappresentato dal pedaggio autostradale attraverso il Telepass, che permette il pagamento automatico dell'autostrada e rappresenta uno dei più famosi esempi di sistema RF-ID che da alcuni anni viene utilizzato nel nostro Paese.
L'evoluzione attuale di questa tecnologia è rappresentata dalle Smart Label che hanno rivoluzionato il commercio mondiale. Le dimensioni e i costi ridotti permettono inoltre di inserire questa tecnologia di identificazione su qualsiasi tipo di prodotto andando a sostituire man mano i codici a barre.
Nella tesi ho analizzato le problematiche relative alla localizzazione dei tag. Esistono diverse tecniche che vengono utilizzate, ma in base a questa scelta si possono avere dei limiti come l'eccessivo costo, la predisposizione dell'ambiente o la precisione che viene offerta. Le tecniche puramente basate sugli RF-ID, che non si servono quindi dell'aiuto di altre tecnologie di localizzazione, ricavano la posizione di un tag attraverso l'attenuazione del segnale ricevuto oppure attraverso il Time of

Flight, ossia il tempo necessario ad un segnale radio emesso da un reader, per raggiungere il tag e ritornare alla fonte.
Le tecniche di prossimità, sono altre tecniche meno complesse dal punto di vista matematico e largamente utilizzate. Il loro vantaggio è quello di avere ottime performance a costi ragionevoli, ma possono essere utilizzate soltanto per applicazioni semplici.
Inoltre, esistono anche altre tecniche di localizzazione che riguardano la localizzazione non RF-ID based e la localizzazione RF-ID based. La differenza sta nel fatto che la localizzazione non RF-ID based si basa sul tempo di arrivo dei segnali mentre la localizzazione RF-ID based è simile alla localizzazione del Wi-Fi, in quanto indica la distanza attraverso la potenza del segnale a radiofrequenza RF.
Tra i sistemi di localizzazione non RF-ID based ho trattato l'active badge, l'active bat, il radar, il GPS e le WLAN. La scelta di un sistema anziché un altro deve essere fatta in base allo studio dei vantaggi e degli svantaggi a cui si va incontro. Se ad esempio in un ufficio sono presenti numerosi ostacoli oppure quest'ultimo è esposto alla luce del sole, non è conveniente usare il sistema di localizzazione active badge poiché i raggi infrarossi possono essere bloccati. I costi dell'infrastruttura sono un'altra importante caratteristica da considerare, in quanto se il loro costo è elevato bisogna orientarsi verso altri sistemi che offrono le stesse caratteristiche ma a costi inferiori. Altra caratteristica da considerare è se l'oggetto da localizzare si trova all'aperto oppure se si necessita di una certa mobilità. Questo determina se è conveniente o meno usare dispositivi GPS o le WLAN.
Se inizialmente la tecnologia era focalizzata sul settore dell'alimentazione e su settori di largo consumo, man mano si sta espandendo ad un'ampia casistica di settori industriali come il settore farmaceutico, tessile, settore sanitario e delle amministrazioni pubbliche. Una delle applicazioni RF-ID più comuni è la gestione del magazzino. Identificare ogni contenitore e ogni scaffale di un magazzino con i tag riduce gli errori nei prelievi e permette di identificare con precisione la merce.
La tecnologia RF-ID può essere utilizzata anche per la gestione della biblioteca. Il tag RF-ID memorizza le informazioni sugli elementi della libreria, come il titolo di un libro, che poi vengono letti da un reader RF-ID, senza doverli salvare in una

database separato. Il vantaggio del loro utilizzo è che i tag RF-ID sono leggibili attraverso un suono, quindi non c'è bisogno di aprire la copertina di un libro.
Altra applicazione importante è quella che viene utilizzata nei centri sanitari, ad esempio per localizzare i pazienti, il personale, le forniture e le attrezzature in modo da migliorarne il servizio, ridurne i costi e i rischi. Per cui anche in questo caso risulta molto utile. Attraverso l'algoritmo di localizzazione LANDMARC si riesce a monitorare i pazienti infettivi e permette di ridurre il numero di operatori sanitari in modo da garantire una risposta tempestiva in caso di emergenza.
Gli algoritmi per la localizzazione RF-ID sono usati per modellare matematicamente la variazione dei segnali a radiofrequenza RF nello spazio. Teoricamente si può applicare un modello di propagazione che calcola la distanza in base all'intensità del segnale o al tempo di arrivo. Nella realtà, non si utilizza questo modello perché ci sono dei fenomeni, come il fading, ossia la distorsione di un segnale che giunge a destinazione sotto forma di un certo numero di repliche, e l'assorbimento, che riducono la potenza del segnale. Per questo motivo, si utilizzano altri metodi, come ad esempio l'analisi statistica, per calcolare il rapporto tra segnale e distanza, oppure dei metodi che permettono di localizzare gli oggetti direttamente senza dover andare a considerare la propagazione del segnale. Tra questi metodi è stato utilizzato un algoritmo che fornisce un'efficiente localizzazione 3D, basato sulla potenza del segnale a radiofrequenza RF per tenere traccia dei tag mirati (target tag) attraverso una matrice di tag. Altro algoritmo trattato ha come scopo quello di dividere la regione di interesse in piccole griglie costituite da nodi-sensori, che sono posti sui vertici della griglia stessa. Attraverso questa griglia, i nodi da localizzare, detti blind nodes, possono essere facilmente determinati confrontando i valori dei vari RSSI, ossia i valori di potenza dei segnali ricevuti. Gli altri algoritmi calcolano le coordinate del nodo di destinazione in base alle distanze che ci sono tra il nodo di destinazione ed i nodi di riferimento, che hanno coordinate note, o due punti vicini, in cui più è piccola la differenza tra l'intensità del segnale dei due punti, e più un oggetto può essere localizzato dai suoi vicini, oppure un'altra metodologia è quella in cui viene utilizzata un'area di comunicazione generica per rilevare se il nodo di destinazione è nella regione oppure no. Sono stati trattati anche algoritmi sulla calibrazione che usano, invece, delle tecniche basate sul tempo.

Un altro problema dei sistemi RF-ID sono le collisioni tra tag e reader. Per questo sono stati implementati due algoritmi anticollisione che attraverso un calcolo probabilistico riescono ad evitare che vi siano interferenze:

1. Eliminazione delle interferenze Reader-to-Tag;
2. Eliminazione delle interferenze Reader-to-Reader.

Le altre problematiche che ho analizzato nella tesi riguardano la Sicurezza e i rischi connessi alla Privacy degli utenti.

Nell'ambito delle telecomunicazioni, le problematiche relative alla sicurezza dello scambio dei dati durante un processo di comunicazione, riguardano tutte le tecnologie e i tipi di comunicazione, incluse le tecnologie e le comunicazioni wireless. Quest'ultime, rispetto alle comunicazioni cablate, sono maggiormente esposte a diverse tipologie di attacchi in quanto condividono lo stesso mezzo, ossia l'etere. Per cui al fine di garantire che un sistema sia sicuro, è importante ridurre al minimo tali minacce. I fattori che permettono di fare questo sono la riservatezza (confidentiality), l'integrità (integrity) e la disponibilità del sistema (availability).

Il problema dei tag RF-ID è che sono dei dispositivi che possono solo ascoltare e rispondere, in quanto non ha importanza chi invia il segnale con la richiesta. Questo mette in primo piano i rischi di accesso non autorizzato e la modifica dei dati delle variabili. Per cui i tag non protetti possono essere vulnerabili a diversi tipi di attacchi come l'eavesdropping, il data spoofing, l'analisi del traffico e il cloning fisico, attacchi Denial of Service (*DoS*), gli attacchi Replay e la clonazione dei tag non autorizzata.

Parallelamente ai problemi legati alla sicurezza, esistono altri tipi di problemi legati alla violazione della Privacy delle persone, in quanto i tag anche dopo la vendita dei beni, continuano ad operare sugli oggetti che sono in possesso degli acquirenti, spesso ignari. Da qui deriva l'origine degli attacchi alla privacy. Il loro scopo è il tracciamento o le informazioni personali di una persona che possiede il tag.

Tutto questo succede perché un'applicazione RF-ID può contenere una grande quantità di dati. Se un prodotto dotato di tag viene, per esempio, pagato con una carta elettronica, è possibile collegare l'ID che identifica univocamente quel prodotto con l'identità dell'acquirente. Nei sistemi RF-ID un approccio alla sicurezza è l'utilizzo dell'autenticazione. Questo metodo effettua sempre una

comparazione tra il codice di autenticazione atteso e il codice effettivamente ricevuto, che può essere ottenuto tramite diverse procedure come l'utilizzo di:

- Password o PIN;
- Codici di autenticazione dei messaggi (HMAC);
- Firme Digitali.

Per la sicurezza e la privacy personale, sono stati trattati protocolli di sicurezza basati sulle catene di hash, come l'OSK e due dei suoi miglioramenti: OSK/AO e OSK/BF, inoltre sono stati presentati i protocolli O-RAP e la sua evoluzione O-FRAP, che attraverso dei meccanismi query/replay e acknowledgment garantiscono l'autenticazione tra tag e reader. Inoltre sono state fatte delle comparazioni tra diversi protocolli, come OSK e O-RAP, al fine di evidenziarne i vantaggi e le differenze. Alcuni protocolli recenti riescono a ridurre la complessità del reader memorizzando i tag segreti in una struttura speciale, come un albero, una griglia, ecc, ma presentano il problema della tracciabilità. Altro protocollo è quello relativo alla crittoanalisi, basato sempre sulle funzioni hash, e che fornisce l'autenticazione reciproca di tag e reader.

Infine è stato citato un protocollo di autenticazione ultra-leggero (ultra-lightweight authentication protocol). Questa famiglia di protocolli sono basati sull'uso di pseudonimi per garantire l'anonimato dei tag. Per far questo viene utilizzato un indice-pseudonimo da un reader autorizzato per recuperare le informazioni associate a un tag. Inoltre, la chiave viene divisa in diverse sottochiavi, che sono condivise tra i tag e i reader legittimi, al fine di scambiare messaggi nella fase di autenticazione.

Il mercato RF-ID in Italia, inizialmente ha visto registrare un elevato tasso di crescita, ridimensionandosi poi in un secondo momento. La liberalizzazione delle frequenze UHF ha avuto effetti contrastanti, in quanto da un lato vi è stato un notevole aumento dei progetti RF-ID nei settori del trasporto e della logistica con un incremento pari ad una percentuale del 62%, dall'altro la disponibilità dell'UHF ha ridotto la necessità di ricorrere ai più costosi RF-ID attivi, che prima rappresentavano una scelta obbligata in alcune situazioni. Gli anni successivi al 2009 hanno visto il rafforzarsi di queste tendenze anche nei settori in cui l'investimento rappresentava un rischio per l'impresa, e per questo sono stati avviati ugualmente alcuni grandi progetti.