Università di Pisa

DIPARTIMENTO DI INFORMATICA
Corso di Laurea Magistrale in
Sicurezza Informatica: Infrastrutture ed Applicazioni

Tesi di Laurea Magistrale

Sicurezza e Privacy nei Sistemi RFID

Relatore
Prof. Maurizio Angelo Bonuccelli

Controrelatore
Prof.ssa Anna Bernasconi

Candidato
Valentina Marconi

Anno Accademico 2014/2015

Al mio Babbo

Ringraziamenti

Desidero innanzitutto ringraziare il Prof. Bonuccelli e la Prof.ssa Bernasconi per i preziosi consigli e la disponibilità dimostrata.

Ringrazio il mio compagno Paolo per il grande supporto e mio figlio Filippo al quale ho un sottratto un po' della mia presenza, per la stesura di questa tesi.

Ringrazio i miei genitori, i miei fratelli e i miei suoceri, per il prezioso aiuto che mi hanno dato, è stato fondamentale per potermi dedicare allo studio.

Ringrazio i miei colleghi, in particolar modo Roberto e Rosanna, che mi hanno sopportato e supportato in questo periodo molto intenso, il mio capo Michele per la grande comprensione dimostrata.

Ringrazio il mio compagno di università Giacomo, figura fondamentale in questo corso di studi e mio compagno in varie attività di gruppo.

Per ultimo, ma primo per importanza, ringrazio mio Padre, mia guida, mio punto di riferimento, senza il suo aiuto non ce l'avrei mai fatta.

Indice

Introduzione

La tecnologia RFID (Radio Frequency Identification) [Finke2010], [Juels2006], [Impin2016], usata per l'identificazione a distanza, negli ultimi anni si sta affermando, grazie alle sue caratteristiche, in vari ambiti: commerciale, sanitario, controllo degli accessi e sicurezza.

L'impatto di questa tecnologia sarà notevole: si ipotizza che ogni prodotto nei prossimi anni sarà dotato di un tag RFID, e questo grazie agli enormi vantaggi che possono derivare dal suo utilizzo. Le più grandi aziende hanno adottato la tecnologia RFID per le loro catene di montaggio o per la loro logistica, garantendo la tracciabilità dei prodotti attraverso la catena di produzione e distribuzione.

L'identificazione implica l'assegnazione di un'identità univoca ad un oggetto che consenta di distinguerlo in modo non ambiguo. Il fine principale di questa tecnologia, pertanto, è l'acquisizione di informazioni su oggetti, animali o persone identificati, per mezzo di piccoli apparati a radiofrequenza [Talo2008].

I sistemi RFID sono composti da Radio Frequency (RF) *tag* o *transponder* e da RF *reader* or *transceiver*.

Il tag RFID viene attaccato all'oggetto da identificare automaticamente a distanza, esso è un piccolo microchip con una antenna, progettato per comunicazioni wireless.

È possibile realizzare tag RFID in vari formati: inseriti in etichette normalmente utilizzate nei capi di abbigliamento, sotto forma di adesivi da applicare sulle confezioni dei prodotti o all'interno di tessere formato carta di credito.

Il reader RFID ha una o più antenne che emettono onde radio e ricevono indietro un segnale dal tag, i reader sono collegati con un back-end database server attraverso una normale rete di computer, sono anche chiamati *interrogator* perché interrogano i tag.

L'area nella quale un interrogator fornisce energia sufficiente ad un tag passivo è detta *interrogation zone, read field* o *reader field*. I tag al di fuori della interrogation zone non ricevono sufficiente energia per rispondere riflettendo il segnale.

Il segnale che va da un reader al tag è chiamato *forward channel* mentre il segnale che va da

un tag al reader viene chiamato *backward channel*.

A differenza dei sistemi a codice a barre, in cui normalmente l'operazione di lettura richiede l'intervento dell'uomo e il tag deve essere visibile da parte del reader senza ostacoli interposti, nei sistemi RFID i tag non devono essere sulla linea di visibilità del reader, annullando i problemi di posizionamento, inoltre il reader ha la capacità di leggere centinaia di tag al secondo, permettendo di identificare tutti i prodotti presenti in un carrello della spesa.

In ambito commerciale, i sistemi RFID possono essere usati in varie fasi della catena di produzione e distribuzione, permettendo di avere un identificatore unico (serial number) per ogni singolo prodotto, a differenza dei codici a barre che ne identificano solamente le categorie. Per esempio in uno scaffale di un supermercato con 50 confezioni uguali, il codice a barre identifica la tipologia del prodotto ma non distingue tra le 50 confezioni. Il serial number dei tag RFID distingue ogni singola confezione, questa capacità, con l'ausilio di un database, viene utilizzata per tenere traccia del prodotto per tutto il suo ciclo di vita.

Un database potrebbe contenere attributi come:

1. Tipo di prodotto.
2. Produttore.
3. Acquirenti.
4. Percorso effettuato.

La tecnologia RFID è considerata, per la sua potenzialità di applicazione, una tecnologia "general purpose" e, dato i suoi benefici, presenta un elevato livello di "pervasività".

I sistemi RFID sono una delle principali tecnologie che fanno parte di Internet of Things (IoT).

Il concetto fondamentale di Internet of Things è legato alla possibilità di associare a qualsiasi cosa una piccola componente tecnologica capace di trasformare questo oggetto in un dispositivo intelligente e comunicante in modalità wireless. Internet of Things è la chiave dell'auto che ci permette di metterla in moto, aprire o chiudere le portiere in automatico, senza estrarre la stessa dalla propria tasca, ma è anche la chiavetta prepagata in cui in molti uffici il personale può comodamente prelevare bevande e snack da un distributore automatico.

Questa tecnologia ha introdotto anche nuovi problemi e tematiche legate alla sicurezza e alla

privacy, in questa tesi verrà prestata particolare attenzione a queste tematiche.

Nel primo capitolo viene esaminata la tecnologia dei sistemi RFID e le loro applicazioni, nel secondo capitolo vengono trattati protocolli di comunicazione tra tag e reader e le problematiche relative all'identificazione dei tag.

Nel terzo capitolo vengono esaminati gli attacchi che possono essere rivolti ai sistemi RFID. Dato il non trascurabile aspetto sociale legato alla possibile tracciatura fraudolenta di cose, persone e animali, nell'ultimo paragrafo del terzo capitolo vengono proposte le attuali posizioni del garante della privacy e della comunità Europea relativamente a questa tecnologia.

Nel quarto capitolo viene trattato il problema dell'autenticazione, aspetto fondamentale per la sicurezza di questi sistemi.

Capitolo 1 Tecnologia e Applicazioni

1.1 Tecnologia

Un sistema RFID (Fig.1) si basa su tre componenti [Finke2010], [Rom1990], [WEIS2003]:

- Il *Tag* o *Transponder* che è posizionato sull'oggetto da identificate.
- Il *Reader* o *Transceiver* che capace di leggere o inviare dati al tag.
- Un sistema di data processing che elabora i dati ottenuti dal reader chiamato *Back end Server*.

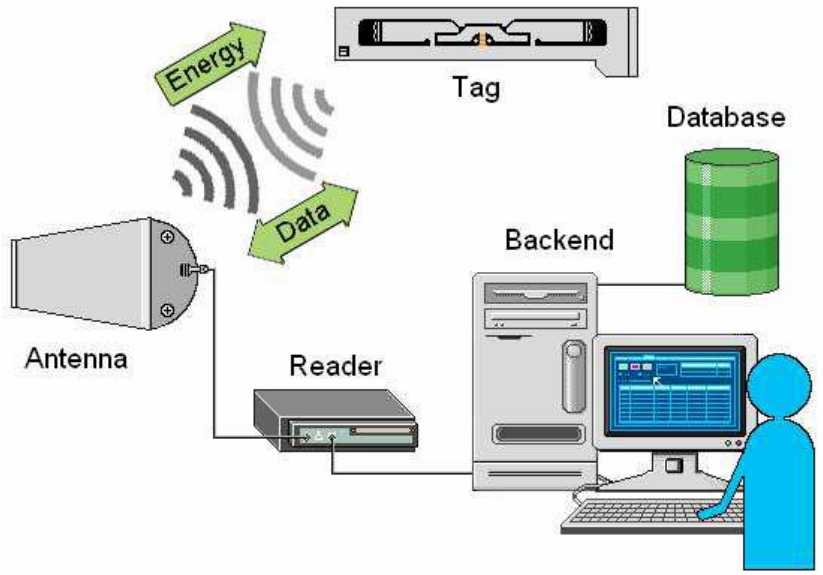

Figura 1 [Xiao2008]

Un RFID tag può essere passivo, semi-passivo o attivo.

I tag passivi non hanno un proprio alimentatore, essi ricevono la potenza necessaria per trasmettere dal segnale che gli viene inviato dal reader. I tag passivi, possono offrire particolari capacità di robustezza e resistenza a condizioni industriali estreme, il loro limite prestazionale risulta essere la limitata distanza di lettura e l'impossibilità di integrare sensori ausiliari. Questo tipo di Tag non è adatto ad applicazioni di localizzazione in tempo reale, per il fatto che la loro attivazione è legata alla presenza di un reader nel campo di azione.
Nonostante le loro limitate capacità computazionali, risultano essere la tipologia di Tag

maggiormente utilizzata, merito anche del loro ridotto costo.
In questa tesi prenderemo in considerazione solo sistemi RFID con tag passivi, che verranno approfonditi più avanti.

I tag attivi hanno un proprio sistema di alimentazione, di solito una piccola batteria al litio e sono computazionalmente più potenti. La batteria oltre ad alimentare i circuiti di ricetrasmissione, può servire per tenere attiva una memoria RAM nella quale si memorizzano i dati relativi al tag. Un'alimentazione interna permette di realizzare sistemi che lavorano con frequenze del segnale più elevate e che hanno un raggio di azione che va da 10 a 500 metri.
I tag attivi sono usati per l'identificazione automatica di oggetti in movimento, come le automobili lungo l'autostrada, per i quali la distanza di rilevamento è più lunga e non fissa. Alcuni tag attivi lavorano con un segnale di banda con frequenza attorno ai 900 MHz ed anche a frequenze più elevate dell'ordine dei GHz.
Nei tag attivi la trasmissione del codice di identificazione avviene in modo autonomo senza interrogazione da parte del reader.
Grazie alle batterie i tag rimangono sempre accesi, per questa caratteristica sono utilizzati quando c'è la necessità di realizzare dei sistemi di localizzazione in tempo reale. Il loro funzionamento può essere continuo o a intervalli di tempo regolari (Ping-Rate), variabili da 0,5 msec a 20 sec. per risparmiare la batteria. L'uso della batteria permette ai tag RFID attivi di montare ed alimentare anche dei sensori aggiuntivi, per esempio per la rilevazione della temperatura o della pressione. Gli svantaggi dei tag attivi sono la dimensione, di solito più ingombrante di quella dei tag passivi, le difficoltà di utilizzo in situazioni ambientali difficili, come quelli caratterizzati da temperature elevate proprio per la presenza della batteria, i maggiori costi di acquisto e di manutenzione o sostituzione della batteria,

I tag semi-passivi sono simili ai tag attivi, ma la batteria ha il solo scopo di mantenere in funzione i circuiti del microchip e non viene utilizzata per inviare un segnale al reader. I tag semi-passivi sono in uno stato dormiente fino a quando non sono "svegliati" dal segnale di un reader, come i tag passivi, riflettono modulato il segnale ricevuto. Come accennato, la batteria ha due utilizzi: alimentare sensori aggiuntivi, se il tag ne è provvisto, oppure aiutare il chip a "svegliarsi" tenendolo in uno stato di stand-by, inattivo ma acceso, questo per

conservare il più possibile l'energia della batteria.
Essendo la distanza di lettura dei tag passivi molto spesso limitata dalla difficoltà del chip a "svegliarsi", se non sufficientemente stimolato dall'energia del campo del reader, l'aiuto della batteria nei tag semi-passivi permette a questi ultimi di offrire distanze di lettura ben superiori.
A livello di prezzi, i tag semi-passivi si collocano in linea di massima tra i tag passivi e quelli attivi. La necessità di preservare la batteria può limitare l'utilizzo dei tag semi-passivi negli ambienti più difficili.
Esistono anche read-write tag in grado di memorizzare nuove informazioni sul microchip, essi vengono usati per contenitori riusabili, quando il contenuto cambia anche l'informazione nel tag cambia.

Come già detto in precedenza i componenti di un sistema RFID sono: il tag, il reader e il back end server. Il reader converte le onde radio ricevute in informazioni digitali che vengono passate al back end server. Il back end server, che normalmente è un database online, è necessario per raccogliere, filtrare, processare e gestire i dati del sistema RFID. Il back end memorizza informazioni, dati utili alla tracciabilità dei prodotti e informazioni necessarie per la gestione dei tag, è importante per una applicazione RFID poter raccogliere, gestire e analizzare i dati nella maniera più efficiente possibile. Un aspetto importante di questi sistemi è l'integrazione della tecnologia RF (Radio Frequency) con un back end server, che permette di effettuare opportune query sul database in base agli input ricevuti dal reader. Quando il tag di un oggetto viene interrogato, trasmette come identificatore un serial number, che sarà poi la chiave per identificare l'oggetto tramite accesso al back end database. Un aumento della sicurezza si ha inserendo nei tag solamente le informazioni sufficienti a identificare l'oggetto, recuperando quindi gli altri dati dal database, questo aumenterebbe la difficoltà di un eventuale attacco che ora dovrebbe essere rivolto sia al tag che al back end. Questo accorgimento non risulta però efficace nel contrastare la contraffazione di un tag, di fatto l'identificatore potrebbe essere intercettato durante la trasmissione ed utilizzato per creare un tag clone, il back end database non sarebbe in grado di distinguere il tag legittimo da un tag clonato contenente lo stesso identificatore.
Per limitare gli attacchi alla sicurezza del back end è necessario stabilire, per la comunicazione dei dati tra il tag ed il reader, un canale sicuro o la criptazione del segnale.

Il backend server può essere attaccato anche da virus, trasmessi da tag infetti, usando l'attacco *SQL Injection* e *Buffer Overflow* [Xiao2008], [Rieb2006].

1.1.1 I Tag Passivi

TAG passivi [Talo2008] sono sicuramente gli oggetti RFID più diffusi e molta cura viene dedicata alla loro costruzione per mantenere il loro costo contenuto.

In un TAG passivo si possono distinguere tre componenti principali:

- il chip
- l'antenna
- il substrato

Le seguenti sono immagini di alcuni tag passivi:

Figura 1 Bracciale Monouso Utilizzo generale, RFID Global

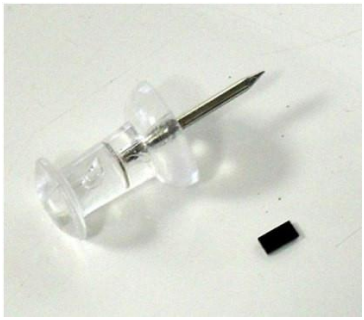

Figura 2 TITAN, un tag passivo UHF EPC global estremamente miniaturizzato, IDNOVA

Figura 3 HF Wet Inlay Etichetta adesiva in sintetico trasparente non stampabile, RFID Global

Figura 2 Badge PVC HF Badge RFID HF, RFID Global

Il chip si occupa di tutte le funzioni necessarie all'operatività del TAG, essenzialmente l'immagazzinamento dei dati, la conversione dell'energia RF ricevuta dall'antenna in alimentazione elettrica e la modulazione del segnale riflesso. La memoria del chip può essere read-only (RO), write-once read-many (WORM), oppure read-write (RW), vari tipi di memoria possono coesistere nello stesso chip. La capacità di memoria, può variare da un numero minimo di bit, 1 o 2 bit per segnalare la semplice presenza del TAG come misura antitaccheggio, fino a qualche migliaio di bit divisi in varie sezioni (RO, WORM, RW).
Oltre alle funzioni viste sopra, il chip può anche possedere capacita computazionali, le quali sono limitate dalla scarsità di alimentazione, ma sufficienti per qualche funzione di sicurezza e protezione dell'informazione.

L'antenna è collegata elettricamente al chip, le sue funzioni consistono nel raccogliere l'energia RF irradiata dal reader e di rifletterne una parte per trasmettere. Le prestazioni di un tag passivo, come la distanza operativa e la capacità computazionale, dipendono dalla capacità dell'antenna di raccogliere energia e di rifletterla, le sue dimensioni sono quindi molto importanti. Le frequenze alle quali opera l'antenna determinano la sua forma.

Il substrato fornisce il supporto fisico per l'assemblaggio del tag e permette di tenere insieme le sue componenti, può essere realizzato in film plastico, carta o altri materiali.

Le caratteristiche della trasmissione RF con tag passivi sono:

- Limitata capacità di tuning che significa che un tag non può filtrare delle frequenze non desiderate.
- Il forward channel è un segnale con una potenza superiore al backward channel, normalmente 5 volte maggiore. La potenza del forward channel deve essere superiore alla potenza necessaria per la trasmissione, perché il tag, essendo passivo, prende la sua energia dal segnale che riceve.
- Ci possono essere dei tag che non generano segnali perché non hanno la potenza necessaria, si limitano a riflettere una parte del segnale ricevuto, il reader usa l'onda riflessa come un'impronta per identificare l'oggetto legato al tag.
- I tag a basse frequenze (LF) operano a meno di 135 kHz.
- I tag alle alte frequenze (HF) operano nel range 6.765 - 27. 283 MHz.

- I tag a *Ultra High Frequency* (UHF) operano a 433 MHz e nel range 868-928 MHz.
- Infine i tag alle Micro frequenze operano nel range 2.45 -5.875 GHz.
- I tag UHF e Micro frequenze sono soggetti a più interferenze di quelli a basse frequenze.

1.1.2 I Reader

Il reader è l'elemento che nei sistemi RFID consente di assumere le informazioni contenute nel tag. Si tratta di un vero e proprio ricetrasmettitore, governato da un sistema di controllo e spesso connesso in rete con sistemi informatici di gestione, per poter ricavare informazioni dall'identificativo trasmesso dai tag.

Questo, infatti, specie nei tag passivi, è un semplice codice univoco che può essere usato come chiave di ricerca in un sistema informativo. In questo modo si possono ricavare dettagliate informazioni, aggiornate nel tempo, sul particolare oggetto a cui il tag è associato.

I reader per tag passivi e semi passivi, devono emettere segnali RF di tipo particolare, in grado di fornire al tag anche l'energia necessaria per la risposta. Le tecniche di comunicazione e trasferimento dati utilizzate nei sistemi RFID sono molto diverse tra loro, variano da applicazioni che prevedono la lettura a pochi centimetri di distanza, di tag passivi, ad applicazioni che prevedono letture di tag attivi a distanza di centinaia di metri.

Esistono reader fissi negli accessi ai magazzini, sui nastri trasportatori e negli scaffali e reader portatili, simili a quelli in uso per i codici a barre. Per quanto riguarda la diffusione, le installazioni di reader fissi rappresentano più dell'80% del totale a livello mondiale.

Per quanto riguarda l'uso delle frequenze, la maggior parte del mercato dei reader, sia in termini di fatturato che in termini di numero di unità, è rappresentato da reader HF. Però si prevede che il mercato dei reader UHF cresca molto più velocemente degli altri nel prossimo futuro**.**

1.2 Applicazioni RFID

Grazie alla grande flessibilità di interconnessione, i sistemi RFID si stanno affermando in vari ambiti, i tag vengono applicati a beni di consumo, ad animali, ad esseri umani e perfino alla spazzatura, portando vantaggi economici ed un impatto positivo sulla vita quotidiana. L'applicazione di questa tecnologia può portare vantaggi per esempio nella gestione dell'inventario di magazzini, nella gestione di biblioteche e nella gestione di forniture.

La tecnologia RFID appartiene alla categoria della identificazione automatica ed EPC

(Electronic Product Code) è un termine specifico per un intero sistema, che è pianificato per usare in maniera più efficiente le proprie risorse. L'EPC è un meta-code, la cui struttura dati è stata sviluppata in modo da indentificare risorse fisiche, come pallet e prodotti di consumo attraverso un serial number. Questo serial number può essere usato come chiave per accedere ad un database dove sono memorizzate maggiori informazioni.
Alcune caratteristiche delle RF usate sono:

- LF e HF sono impiegate per distanze <1.5m; sono usate per identificare animali, libri in biblioteche e serrature per auto; gestione bagagli sull'aereo e accesso nelle abitazioni.
- UHF e Microwave possono essere usate per distanze maggiori 1.5m; sono usate per identificare valigie, pallet, contenitori e per il controllo dell'accesso dei veicoli.

Il seguente è un esempio di implementazione di un sistema RFID per un ciclo di produzione e vendita di prodotti:

- Il produttore mette i tag con EPC su prodotti o nell'imballaggio per permettere, con la creazione di un database, il loro tracciamento fino al punto vendita.
- Il produttore usa gli EPC per organizzare la spedizione preparando gli imballaggi, pallet e notifiche di spedizione.
- Durante tutto il ciclo di distribuzione, i reader RFID memorizzano posizione e data per fornire informazioni sullo stato dei prodotti ai partner coinvolti nella filiera, queste informazioni sono accessibili da un server.
- Il punto vendita riceve in anticipo la notifica dell'avvenuta spedizione e al momento dell'arrivo, se richiesto, avvisare della avvenuta ricezione del prodotto identificato tramite EPC. Quando il prodotto viene venduto questa informazione viene registrata automaticamente.
- Nel punto vendita l'inventario del magazzino può essere gestito automaticamente, tramite le informazioni che confluiscono in un database, si conosce la quantità del prodotto venduta e, se la giacenza è sotto una certa soglia, si provvede a riordinare il prodotto.

I benefici di questo sistema dipendono dall'applicazione e dalle relazioni commerciali tra i partner; le previsioni e i vantaggi per il produttore sono diversi da quelli del punto vendita.

I produttori devono ridisegnare alcuni processi interni per trarre il maggior vantaggio possibile e la gestione dei tempi è fondamentale.
Per i produttori i benefici sono:

- Riduzione dei casi in cui venga fatta richiesta di un prodotto esaurito.
- Migliore utilizzo delle risorse, grazie alla maggiore visibilità delle stesse.
- Avendo più informazioni è possibile prendere decisioni in tempo reale.
- Maggiore prevenzione delle contraffazioni.
- Minor rischio di avere prodotti obsoleti.
- Riduzione delle spese di inventario.
- Minor lavoro di magazzino.
- Riduzione di rischio di esaurito a magazzino.
- Riordino automatico.
- Riduzione dei furti.
- Maggiore prevenzione delle contraffazioni.

Anche i consumatori possono trarre benefici dall'introduzione di un sistema RFID, questo dipende da come il sistema di tagging è stato implementato.
I benefici più comuni sono:

- Servizio migliore per la possibilità di un checkout più veloce, completando l'acquisto utilizzando una card in prossimità del RFID reader.
- Gli ordini possono essere più tempestivi e quindi il cliente ha più possibilità di trovare sempre i prodotti che desidera.
- Migliore gestione dei prodotti difettosi, possibilità di localizzare i prodotti difettosi prima che arrivino al consumatore.

Oltre ai vantaggi parliamo anche brevemente dei problemi da considerare nel caso si volesse implementare un sistema RFID. Anche se negli ultimi anni è diminuito, il maggior aspetto da considerare è il costo dei tag, altri costi non trascurabili sono: il software di gestione, l'eventuale integrazione con altri sistemi e l'adeguamento dell'intera organizzazione.

Anche la leggibilità dei tag ha degli aspetti da considerare con cura.

- Le frequenze e le distanze.

- L'ambiente dove operano i reader, occorre evitare interferenze con altre apparecchiature, umidità, vibrazioni e shocks.
- Il tipo di oggetti a cui applicare i tag, per esempio gli oggetti metallici riflettono le onde radio, mentre gli oggetti contenenti liquidi le assorbono.

La tecnologia RFID viene usata anche nello sport [www.idnova.com], LAPTRACK è il sistema di IDNOVA basato su tecnologia RFID UHF di ultima generazione per tracciare ordine e tempi di arrivo in competizioni sportive, quali ad esempio corse su strada, su pista, o gare campestri. Il tag UHF prevede possibilità di fissaggio alla scarpa, ma anche a caviglia (con banda in velcro) o alla bici, permette un facile e rapido fissaggio che non ostacola il movimento dell'atleta, è economico e quindi adatto anche per applicazioni usa e getta.

I sistemi RFID hanno permesso alle stazioni di servizio di carburante della "Love's Travel Stops", sparse in tutti gli USA [www.impinj.com], di rifornire i suoi clienti senza la necessità di usare carte di credito. Prima dell'introduzione del sistema RFID un cliente, solitamente camionisti, per essere autorizzato a rifornirsi di carburante doveva inserire la tessera in un lettore e digitare i suoi dati, eventuali errori avrebbero comportato la necessità di ripetere l'intera procedura e, in alcuni casi, l'intervento del personale dell'area di servizio, causando speco di tempo.

"Northwestern Memorial Hospital" [www.impinj.com] ha introdotto la tecnologia RFID per risolvere il problema delle medicine scadute, che comportava interruzioni di assistenza e perdita di denaro. Con il sistema RAIN l'ospedale ha automatizzato l'inventario delle medicine, assicurandosi che venissero usate prima della scadenza e quindi risparmiando su nuovi acquisti, permettendo anche che le medicine effettivamente usate fossero fatte pagare.

Infine altri esempi di impiego di sistemi RFID sono: i microchip obbligatori per i cani sono, le chiavette dei distributori automatici, il Telepass e le etichette dei capi di abbigliamento di alcuni marchi.

1.3 Standard EPC

L' EPC (Electronic Product Code) [EPC2013], [EPCGLO], [Fink2010] è un identificatore universale che assegna un'identità unica ad un oggetto fisico. Gli EPC sono codificati sui tag e possono essere usati per tenere traccia di ogni tipologia di oggetto. L' EPC può essere ciò che distingue due oggetti uguali, un solo EPC può fornire la data di produzione, l'origine ed il numero di lotto di un prodotto. In generale l'EPC consiste di un header di lunghezza

variabile ed una serie di altri campi la cui lunghezza, struttura e funzioni sono determinati dal contenuto dell'header. La lunghezza totale dell'EPC può andare da 64 a 256 bit. La Tabella 1 riporta un esempio di codifica di un EPC usando 96 bit, ci sono sei campi: Header, Filter value, Partition, Company prefix, Item reference e Serial number.

I campi Header, Filter, Partition, e Company prefix sono direttamente legati all'identità globale del prodotto, mentre il serial number rappresenta l'identità secondaria, cioè un numero che identifica univocamente un articolo.

Il campo Company prefix contiene un numero che identifica il produttore, che ha emesso il primo contenuto dell'EPC. Il campo Item reference descrive la classe del prodotto, infine il

Tabella 1 Esempio di codifica EPC con 96 Bit [Fink2010]

Header	Filter value	Partition	Company prefix	Item reference	Serial number
8 bit	3 bit	3 bit	20– 40 bit	4– 24 bit	38 bit
0011 0000					

L'EPC che è memorizzato su un tag, è la base del flusso di informazioni della EPCglobal Network, una rete di computer che viene usata per condividere, tra partners, i dati sui prodotti. Per esempio possono essere condivisi i dati sugli spostamenti dei prodotti durante tutto il loro ciclo di vita.

Una rete EPCglobal consiste nei seguenti componenti:

- Object Naming Service (ONS).
- EPC Discovery Services.
- EPC Information Services (EPCIS).
- EPC Security Services.

L'ONS è un servizio che permette di trovare, dato un EPC, le informazioni su di un oggetto, la ricerca restituisce, a chi ne ha fatto richiesta, un URL o un indirizzo IP per ottenere maggiori informazioni sull'oggetto associato all'EPC. L'ONS è paragonabile al DNS (Domain Name System) che è utilizzato in internet per la risoluzione di nomi dei nodi della rete in indirizzi IP. L'ONS è una istanza del Discovery Services.

Il Discovery Services è un gruppo di servizi che permettono la ricerca di dati relativi ad un particolare EPC nella EPCglobal Network, può essere paragonato ai motori di ricerca in internet.

L'EPCIS è uno standard progettato per rendere possibile la condivisione dei dati tra le imprese e all'interno delle imprese. Questa condivisione ha lo scopo di permettere ai partecipanti della rete una vista comune dei dati sull'oggetto, permettendo ad ogni impresa di definire le policy di accesso alle proprie informazioni.

L'EPC Security Services sono strumenti che permettono l'accesso sicuro alle informazioni della rete EPC rispettando i privilegi di accesso dei partecipanti.

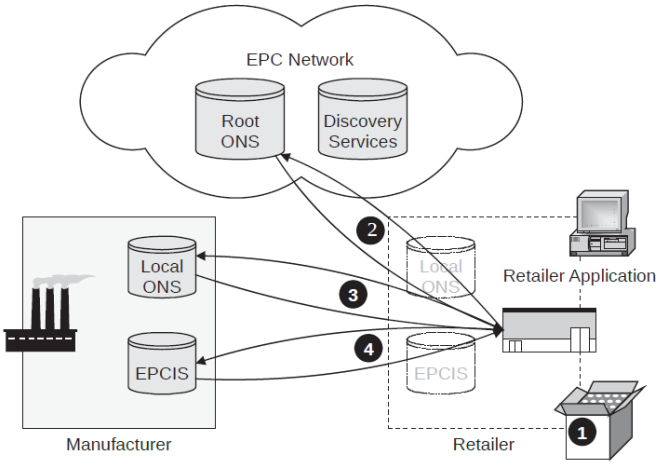

Figura 5 [Fink2010]

Il ciclo di vita di un EPC comincia nel momento della produzione, quando al prodotto viene attaccato un tag. Tutti i dati associati al prodotto come la data di produzione o la data di scadenza sono memorizzate nell' EPCIS del produttore e registrate con l'EPC Discovery Services. Dopo che il prodotto è arrivato nel punto vendita alcuni dati come la data di arrivo sono memorizzati nell'EPCIS locale del punto vendita e registrati con l'EPC Discovery Services. In un punto vendita, se si desidera accedere alle informazioni legate al prodotto, si devono compiere alcuni passi:

1. Si legge la company prefix che è nell'EPC.
2. Il prefix viene mandato al Root ONS che fornisce l'indirizzo IP dell'ONS locale del produttore.
3. All' ONS locale del produttore viene poi mandato l'item reference contenuto nell'EPC in modo da ottenere l'indirizzo IP dell'EPCIS del produttore.

4. Dal punto vendita, con l'item reference ed il serial number dell'EPC, si possono ottenere tutte le informazioni del prodotto con una richiesta all'EPCIS.

1.4 RFID e IoT (Internet of Things)

Recentemente i sistemi RFID sono stati proposti come una delle componenti principali nella costruzione dell'internet del futuro, cioè Internet of Things (IoT) [Atzori2010], [Bonuc2015], [Wel2009]. L'Internet of Things (IoT) è il paradigma che si sta rapidamente diffondendo nel mondo delle comunicazioni wireless, l'idea di base di questo concetto è l'interazione tra oggetti identificati univocamente, come cellulari, sensori e tag RFID, con lo scopo di raggiungere un obiettivo comune.

Internet of Things significa una world-wide network, basata su protocolli di comunicazione standard, di oggetti identificati senza ambiguità e interconnessi. L'idea di IoT avrà un grande impatto su molti aspetti della vita di tutti i giorni, nell'ambiente domestico come nell'ambiente industriale.

Nel contesto domestico si può citare la domotica, l'assistenza alle persone non autosufficienti e il supporto alla salute con la comunicazione medico paziente tramite l'informatica. Nel campo industriale l'impatto principale si ha sull'automazione, la logistica e il trasporto di beni e persone. La prima definizione di IoT deriva da Things oriented, dove le "things" erano oggetti semplici come RFID tag, per cui sono stati sviluppati strumenti web per la gestione dei dati. Il termine Internet of Things è stato usato per la prima volta da Auto-ID Labs, world-wide network di ricerca nel campo delle reti di RFID e delle tecnologie dei sensori.

Queste istituzioni hanno avuto come scopo primario la creazione di una IoT legata a EPCglobal, l'EPC è stato sviluppato per supportare l'uso di RFID in una world-wide network commerciale. Questi standard sono stati progettati per aumentare la visibilità degli oggetti, come la sua tracciabilità e la conoscenza del suo stato e posizione, questo è stato un passo avanti verso l'introduzione dell'IoT. L' IoT non è solo un sistema globale EPC con soli oggetti RFID, che sono solo una parte del sistema, esso implica un progetto più grande di un'identificazione di oggetti.

Partire da soluzioni RFID-centriche può essere positivo, perché gli aspetti più importanti della tecnologia RFID, cioè la tracciabilità e accessibilità fanno parte dell'IoT.

Internet of Things è un concetto in cui il mondo virtuale dell'Information Technology si integra con il mondo reale, in cui ogni cosa, incluso gli oggetti inanimati, hanno la loro

indipendente identità digitale, il mondo reale diventa più accessibile attraverso computer ed apparecchiature in rete, di questo ne beneficiano sia il business che la vita di tutti i giorni. L'internet of Things combina aspetti e tecnologie di diversi approcci e ricerche, coincidendo solo parzialmente con queste (Fig. 6).

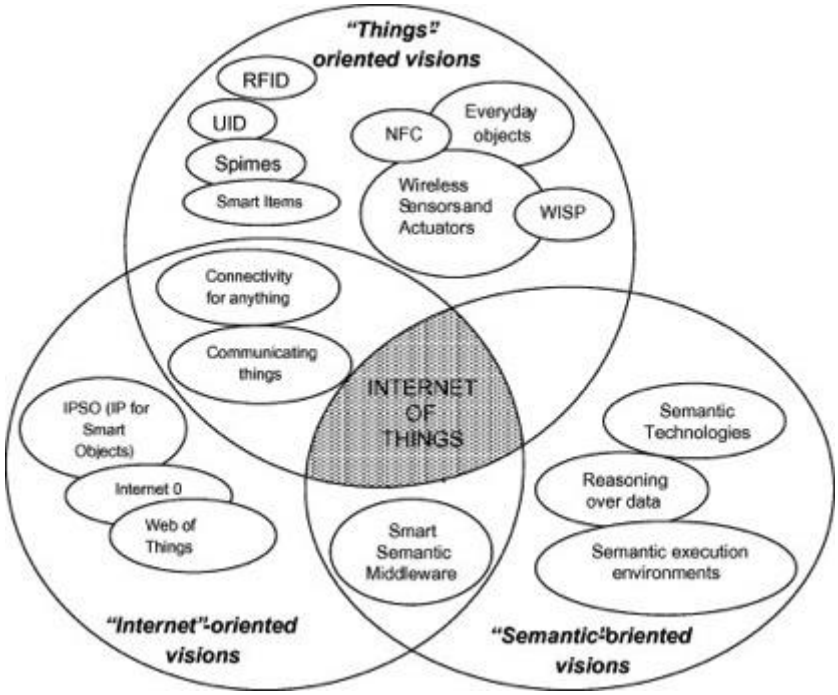

Figura 6 Internet of Things come convergenza di diversi campi di ricerca [Atzori2010]

Capitolo 2 Protocolli di comunicazione RFID

2.1 Il problema della collisione

Un sistema RFID è composto da un *Master Device* chiamato interrogator o reader e di un certo numero di *Slave Device* chiamati tag.

Un reader trasmette tramite un RF link in modo tale da raggiungere simultaneamente tutti i tag, per indirizzare un comando ad uno specifico tag (point-to-point communication) il Reader dovrà inviare un tagID insieme al comando. Allo startup o ad un cambio della configurazione i tagID non sono conosciuti, c'è quindi la necessità di identificarli tutti.

Ogni RFID reader ha intorno a sé un'area finita, chiamata *interrogation region*, entro la quale è possibile comunicare con i tag, quest'area si può definire come quella in cui un singolo tag può essere letto con successo, in assenza di interferenze da parte di altri tag o reader.

In un sistema RFID il reader dopo un'interrogazione deve riconoscere un tag, questo processo viene detto *Singulation*, è il metodo con il quale un RFID reader, nel proprio campo di azione (lettura), identifica, tra molti, un tag con uno specifico serial number. Questo è necessario perché, se diversi tag rispondono simultaneamente ad una interrogazione, potrebbero collidere e interferire (jam) tra di loro. In alcune applicazioni p essere presente più di un reader, un eventuale interrogazione simultanea potrebbe creare interferenze nei singoli processi di lettura dei tag.

Una collisione avviene quando due o più entità competono per la stessa risorsa, nella tecnologia RFID la strategia per risolvere questo problema è l'uso di protocolli anti-collisione. I protocolli anti-collisione usati in RFID sono simili ai metodi usati per risolvere i conflitti nelle comunicazioni multiple-access. Sono presenti però dei limiti di applicazione dei protocolli multiple-access ai sistemi RFID, i requisiti per costruire dei sistemi a basso costo, come i tag passivi, pongono delle limitazioni sulle dimensioni della memoria e la capacità computazionale, come l'incapacità di identificare eventuali tag vicini e tutte le trasmissioni che avvengono attraverso il canale. Questa limitazione è di importanza cruciale, perché la maggior parte dei protocolli per la risoluzione delle collisioni presuppone che il

tag venga a conoscenza di eventuali collisioni. L'uso di metodi del tipo CSMA (Carrier Sense Multiple Access) non sarebbe possibile, il CSMA è molto simile all'Aloha, ma in questa tecnica, ogni stazione può analizzare (ascoltare) il canale per rivelare o meno una trasmissione in corso, l'accesso al canale avviene solo se questo è risulta libero. Questo non elimina del tutto la probabilità di collisioni, occorre considerare i tempi di propagazione del segnale fra due stazioni, infatti potrebbe accadere che una stazione ascolti il canale e lo senta libero, perché il segnale di un'altra stazione non è ancora arrivato, inizi a trasmettere causando una collisione.

I protocolli per tag multipli si possono dividere in protocolli tree-based, che sono deterministici e protocolli stocastici come gli slot-aloha based. I protocolli tree-based a loro volta si dividono in binary tree ed in query tree. I protocolli Aloha sono protocolli tag-driven, mentre i protocolli tree-based sono reader-driven.

2.2 Identificazione con protocolli Aloha

2.2.1 Aloha puro

Il tipo di comunicazione che prevede la trasmissione dei dati da molti tag verso un reader è chiamato multi-access [Fink2010]. Diverse procedure sono state studiate con lo scopo di separare chi trasmette l'uno dall'altro e quindi di non collidere.

Esistono quattro procedure (Fig. 7):

- Space division multiple-access (SDMA).
- Frequency domain multiple-access (FDMA).
- Time domain multiple-access (TDMA).
- Code division multiple-access (CDMA).

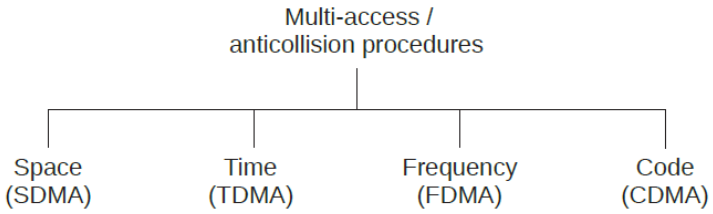

Figura 7 Procedure Multi-access e anti-collisione

Aloha è un protocollo che coordina l'accesso ad un canale di comunicazione condiviso di una rete, è un semplice protocollo time-division multiple-access (TDMA).

É stato sviluppato, originariamente per collegamenti radio, negli anni '70 da Abramson e i suoi colleghi [Abr1970], [Abr1977], [Metc1976], [Burd2004], [Wikipedia] della University of Hawaii. Un sistema di comunicazione condiviso come Aloha, ha bisogno di un metodo per gestire le collisioni, che si verificano quando due o più sistemi cercano di trasmettere contemporaneamente sullo stesso canale. Nel sistema Aloha una stazione trasmette ogni qualvolta i dati siano pronti per essere trasmessi, non prevede vincoli all'invio e quindi all'occupazione della banda di frequenze. Questo vuol dire che l'Aloha puro non controlla se il canale è già occupato prima di trasmettere, poiché ogni stazione agisce indipendentemente dalle altre, il successo è determinato unicamente dalla mancata collisione con altre trasmissioni.

Poiché i canali di comunicazione danno la possibilità di verificare (feedback) se il frame trasmesso è stato ricevuto correttamente oppure se si sono verificate collisioni, la stazione trasmittente ascolta il canale e determina il successo o l'insuccesso della trasmissione. Qualora non sia possibile ascoltare il canale, le stazioni si mettono in attesa di un riscontro (ack) da parte del ricevente. Se ci sono collisioni (o se l'ack non arriva entro un tempo di attesa stabilito), i frame corrotti vengono distrutti. Indipendentemente dal livello di corruzione dei dati; quando un frame è stato interessato da collisione, viene eliminato, in questo caso, la postazione mittente invia di nuovo il frame dopo un'attesa random e si rimette in ascolto sul canale (o attende un ack) fino a quando non stabilisce che il frame sia stato ricevuto correttamente.

Alcuni algoritmi si basano sulla storia recente delle collisioni della stazione, dopo n collisioni viene usato un ritardo di ritrasmissione pari ad un numero random di frame, calcolato in un intervallo da 0 a 2^n - 1. Per la prima collisione ci può essere un ritardo di 0 o 1 frame, dopo la seconda collisione, ci può essere un ritardo che va da 0 a 3 frame, dopo la terza collisione, il ritardo va da 0 a 7 frame e così via.

Quando il numero di ritrasmissioni aumenta il ritardo aumenta esponenzialmente, questo algoritmo è chiamato *Binary Exponential Backoff* [Metc1976].

Si ha *Starvation* quando una stazione non ha la possibilità di trasmettere un frame per un lungo tempo (anche illimitato) e quindi un tag non può essere identificato, questo rappresenta una criticità del protocollo Aloha.

La Figura 8 mostra un esempio di collisione tra frame in un protocollo Aloha, in cui abbiamo tre stazioni (tag) che si contendono l'accesso ad un canale condiviso. Tutte le stazioni trasmettono frame che si contendono l'accesso al canale, quando due frame tentano di occupare il canale allo stesso tempo, si verifica una collisione, entrambi i frame sono danneggiati e dovranno essere trasmessi di nuovo.

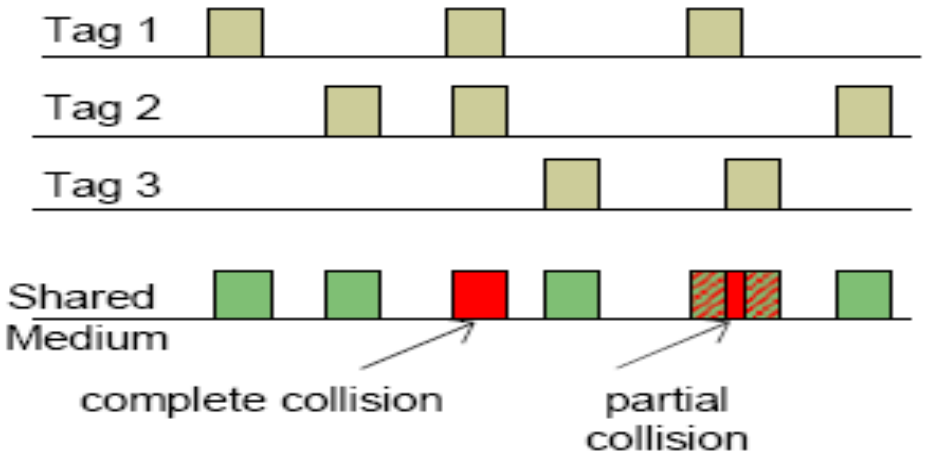

Figura 8 Collisione in Aloha puro [Burd2004]

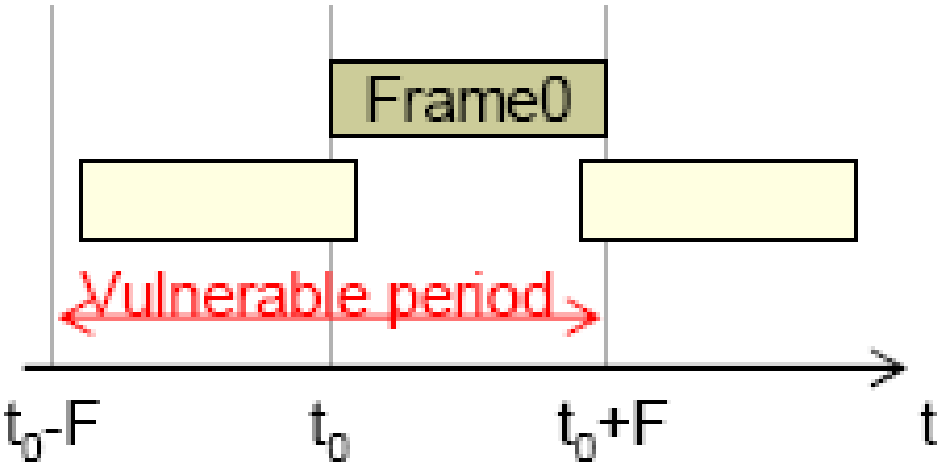

Figura 9 Periodo di vulnerabilità in Aloha puro [Burd2004]

Un'altra criticità del protocollo Aloha è l'intervallo di tempo durante il quale un frame è vulnerabile, cioè a rischio di collisione. Ogni tag che comincia la trasmissione nel periodo da $t0 - F$ a $t0 + F$ causerà almeno una collisione parziale (Fig. 10), è possibile quindi inviare un solo frame per ogni periodo di tempo pari alla durata di 2 frame.

2.2.1.1 Prestazioni del protocollo Aloha puro

La sequenza temporale della trasmissione dati in Aloha è mostrata in Fig. 10.

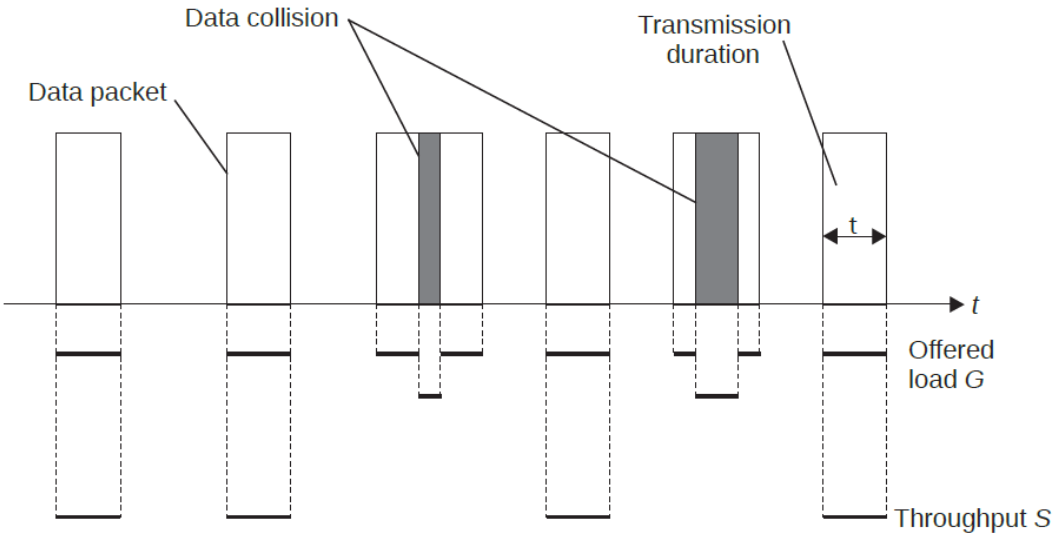

Figura 10 Definizione di offered load G e throughput di un protocollo Aloha: diversi tag trasmettono i loro dati ad istanti di tempo random. Quando c'è collisione il throughput S dei frame che collidono è zero.

Definiamo come *offered load G* [Finkenzeller2010] il numero di tag che trasmettono simultaneamente ad un certo istante di tempo *t0* che assume i valori *0, 1, 2, 3, ...* Il valore medio di offered load *G* è la media su un periodo di osservazione *T*, e si calcola usando la durata della trasmissione τ di un frame di dati:

$$G = \sum_{1}^{n} \frac{\tau_n}{T} \cdot r_n$$

Dove *n=1, 2, 3, ...* è il numero di tag nel sistema e r_n *= 0, 1, 2, . . .* è il numero di frame di dati che sono trasmessi dal tag *n* durante il periodo di osservazione *T*. Il throughput *S* è uno quando il periodo di osservazione corrisponde alla durata della trasmissione di un frame senza collisioni. *S* è zero quando c'è una collisione e ovviamente quando il frame non è trasmesso. Il throughput medio *S* di una trasmissione dato *G* come offered load è:

$$S = G \cdot e^{(-2G)}$$

Abbiamo il massimo della funzione S (Fig. 11) quando la sua derivata rispetto a G è zero.

$$\frac{dS}{dG} = e^{-2G} - 2G * e^{-2G} = 0 \text{ quando } G=\frac{1}{2}$$

Per valori di offered load $G > 0{,}5$ il numero di collisioni aumenta e il throughput S diminuisce, per valori di offered load $G < 0{,}5$ il sistema è poco utilizzato. Sostituendo nell'equazione S il valore $G = \frac{1}{2}$ ottengo il valore massimo $S = \frac{1}{2e} = 0.1839$, quindi una prestazione massima del 18.4%. Più dell 80% del sistema o canale di trasmissione resta inutilizzato. Il vantaggio dell'Aloha puro è la semplicità della sua implementazione che lo rendono adatto come protocollo anti-collisione per read-only tag.

2.2.2 Slotted Aloha

La performance dell'Aloha puro non è soddisfacente essendo la possibilità di collisioni alta. Per questo è stato sviluppato lo Slotted Aloha che riducendo le collisioni ne raddoppia la performance.

Questo nuovo protocollo divide il tempo del canale in intervalli discreti chiamati slot, dove uno slot corrisponde al periodo di tempo di un frame. Le stazioni possono mandare un frame solo all'inizio dello slot e solo un frame per slot. Se una stazione non riesce ad inserire un frame sul canale all'inizio dello slot, deve aspettare fino all'inizio del time slot successivo, il risultato è che il frame o collide o non collide affatto, le collisioni parziali sono eliminate. Questo metodo richiede, per prevenire le collisioni, che ci sia sincronizzazione tra i nodi che trasmettono. La figura seguente mostra un caso di collisione, usando lo Slotted Aloha.

Figura 11 Collisione nello Slotted-Aloha [Burd2004]

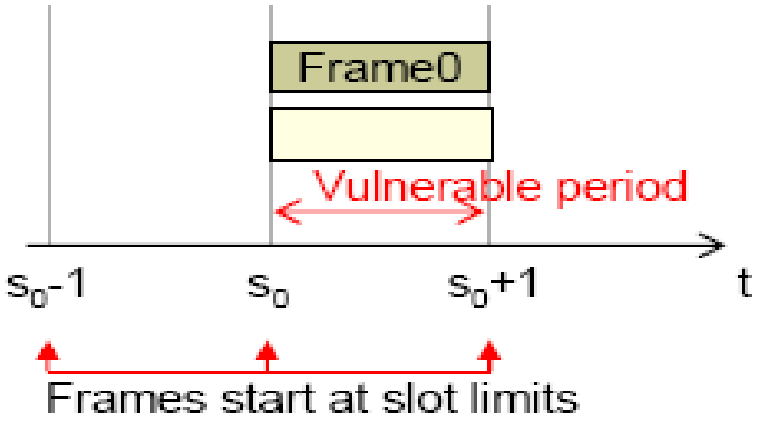

Figura 12 Periodo di vulnerabilità nello Slotted-Aloha[Burd2004]

Assumendo che la lunghezza dello slot sia la stessa del frame trasmesso, il periodo di vulnerabilità è pari alla lunghezza di un frame (Fig. 13), che è quindi la metà di quello dell'Aloha puro.

2.2.2.1 Prestazioni dello Slotted Aloha

Nell'Aloha puro il periodo di vulnerabilità cioè dove può avvenire una collisione è $T \leqslant 2\tau$. Nello Slotted Aloha questo tempo si reduce a $T = \tau$e la formula per il throughput [Fink2010] è:

$$S = G \cdot e^{(-G)}$$

Il throughput raggiunge il suo massimo $S = 0.3678$ per un offered load $G = 1$ (Fig.13). Le sue prestazioni quindi sono del 36.8% che è il doppio di quello dell'Aloha puro.

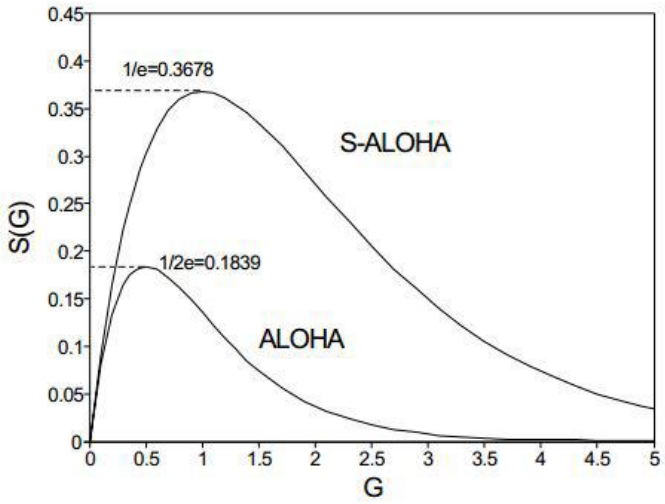

Figura 13 Performance Aloha e Slotted Aloha a confronto

Entrambi i protocolli sono instabili quando superano i valori: $G = 0.5$, per l'Aloha puro, e $G = 1$, per lo Slotted Aloha. Il throughput diminuisce tendendo allo zero perché si verificano molte collisioni ed il ritardo aumenta esponenzialmente (Fig. 14). Con l'aumento delle collisioni si incrementa il numero delle ritrasmissioni, che a loro volta aumentano la probabilità di avere collisioni.

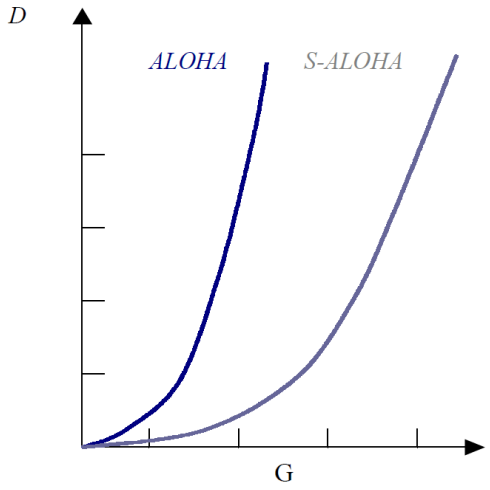

Figura 14 Ritardo medio D in funzione di offered load G

2.2.3 Frame-Slotted Aloha e Dynamic Frame-Slotted Aloha

Il Frame-Slotted Aloha protocol [Fink2010], [Burd2004] è un'estensione dello Slotted-Aloha, la divisione discreta del tempo viene organizzata raggruppando diversi slot in frame, dove ogni frame ha N slot.

Dopo che il reader ha fatto un'interrogazione con la sua richiesta ai tag, aspetta per un certo intervallo di tempo, questo intervallo viene diviso in un numero di slot che possono essere occupati dai tag per mandare la loro risposta. L'architettura degli slot non cambia, i tag trasmettono in uno slot selezionato in maniera random, tra gli *N* slot del frame ed una sola volta per frame, quando più tag selezionano lo stesso slot c'è collisione e i dati vanno persi. Con il semplice Slotted-Aloha un tag con un'alta frequenza di risposte colliderebbe con le risposte degli altri tag, i frame, raggruppando diversi slot insieme, limitano questo comportamento ripetitivo limitando il numero di messaggi che un tag può trasmettere ad uno per frame. Il lavoro di sincronizzazione ulteriore è dello stesso ordine di grandezza di quello dello Slotted-Aloha; il numero *N* di slot nel frame viene predefinito e messo come default nei tag.

Un'estensione del Frame-Slotted Aloha porta al Dynamic Frame-Slotted Aloha. Il

parametro *N*, cioè il numero di slot per frame, non è fisso ma può variare; il reader può aumentare o diminuire il numero *N* ad ogni richiesta. Il numero di slot può quindi seguire il numero di tag, può ridurre il numero di collisioni in un frame, aumentando il numero degli slot o diminuire il numero degli slot se questi sono vuoti.

All'aumentare dei tag il numero di slot necessari per identificarli aumenta esponenzialmente. Il numero degli slot ha un limite superiore e questo vuol dire che se il numero di tag è superiore al numero di slot disponibili nel frame, si verificherebbero sicuramente collisioni.

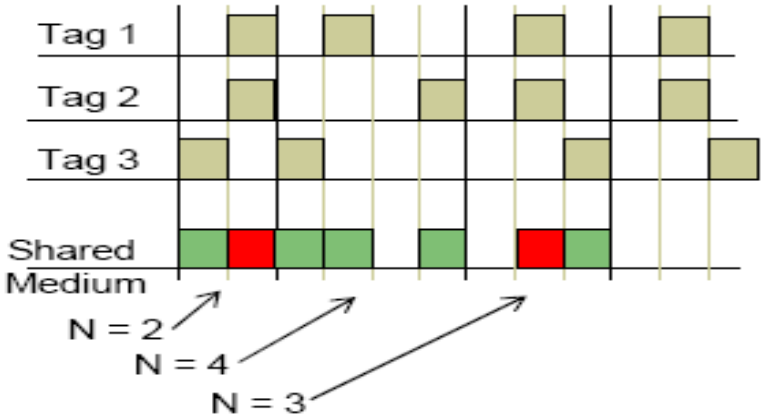

Figura 15 Dynamic Frame-slotted aloha [Burd2004]

2.2.4 Evoluzione dei protocolli Aloha

Sono stati studiati nuovi protocolli che migliorano l'efficienza dei protocolli Aloha fino a qui visti come il protocollo *Enhanced Dynamic Framed Slotted Aloha (EDFSA)* [Lee2005].

All'aumentare del numero dei tag viene aumentata la dimensione del frame, per ridurre la probabilità di collisione, poiché non è possibile incrementare il frame all'infinito, quando il numero dei tag supera una certa soglia le prestazioni del sistema iniziano a degradare. Questo protocollo fa una stima dei tag non letti e la compara con il numero soglia, se risulta maggiore divide i tag non letti in gruppi, permettendo solamente ad un gruppo di tag di rispondere.

Con questo protocollo il numero di slot che servono per leggere i tag aumenta linearmente e non esponenzialmente con l'aumentare dei tag. Le prestazioni del protocollo EDFSA [Bagn2009] non supera il 36,5% e scende al 34% quando il numero dei tag supera i 400.

2.2.4.1 Tree Slotted Aloha

Un altro protocollo Aloha migliorato è il Tree Slotted Aloha (TSA) [Bonuc2006]. TSA è una versione modificata dello Slotted Aloha che riduce il numero di collisioni nella

trasmissione. L'idea di base è quella di risolvere la collisione non appena si verifica, in Framed Slotted Aloha, due tag che non collidono in un frame possono collidere in quello successivo, con l'approccio usato dal TSA questa situazione non si verificherebbe. Tutti i tag selezionano uno slot per trasmettere il loro identificatore, generando un numero random, se c'è una collisione in uno slot, il reader trasmette la prossima interrogazione solo ai tag che hanno colliso in quello slot. I risultati di una simulazione mostrano come le prestazioni di questo approccio siano migliori del Framed Slotted Aloha e dei protocolli Query Tree Based in termini di numero di slot necessari per identificare tutti i tag. Il protocollo viene eseguito in diversi cicli di lettura del tag, un ciclo di lettura consiste in due step:

1. l reader trasmette una richiesta di dati specificando la dimensione del frame l_i.
2. Ogni tag seleziona lo slot, nel campo di lettura del reader, per la risposta, generando un numero random nel range $[l, \dots, l_i]$ e trasmette il suo identificatore in questo slot. Un reader identifica un tag quando riceve un identificatore senza collisioni.

Il comportamento del protocollo segue una struttura ad albero, il nodo radice è il frame nel primo ciclo di lettura, indichiamo con l_0 la dimensione del frame, con N_i indichiamo il numero di tag che trasmettono il loro l'identificatore nello slot i, dove $i \leqslant l_0$, $N_i \geqslant 2$, $\sum_i N_i = n$, con n uguale al numero di tag passivi. Se $N_i \geqslant 2$vuol dire che c'è una collisione nello slot i. Alla fine di ogni ciclo di lettura, il reader comincia un nuovo ciclo per ogni slot in cui si è verificata una collisione, questo corrisponde ad aggiungere nuovi nodi all'albero come figli di un nodo padre, che rappresenta il ciclo di lettura precedente; verrà aggiunto un figlio per ogni slot del nodo padre oggetto di collisioni. Per ogni ciclo di lettura precedente, i tag memorizzano lo slot nel quale hanno trasmesso il loro identificatore ed aumentano di uno il proprio contatore di livello dell'albero, così da poter sapere quando saranno coinvolti nelle trasmissioni successive. Il TSA, a differenza del protocollo Framed Slotted Aloha, non è memoryless, infatti il tag deve memorizzare lo slot usato nella trasmissione ed il livello dell'albero. La quantità di memoria necessaria ai tag per queste memorizzazioni e di pochi bit.

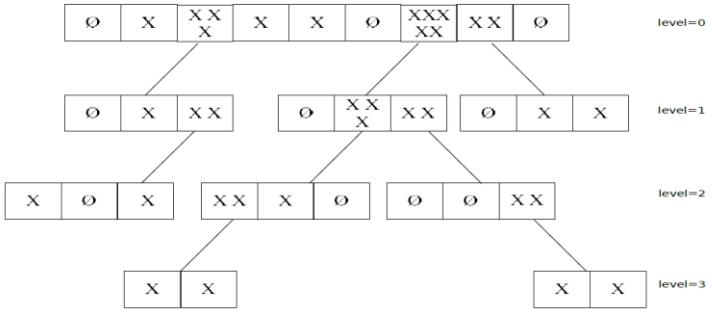

Figura 16 Esempio di esecuzione del protocollo TSA, [Bonuc2006]

L'efficienza del sistema è definita come il rapporto tra il numero di tag ed il numero di slot necessari perché vengano identificati tutti. Per il TSA questo rapporto è 0.4344, quindi la sua prestazione è del 43.4%, dato teorico, che è superiore agli altri protocolli Aloha fino a qui esaminati, anche se [Bagn2009] si riduce al 42% effettivo. Le prestazioni del TSA non scendono sotto il 38% anche per reti con tanti tag (meno di 1000).

Il protocollo TSA è stato ulteriormente migliorato con il protocollo Dy_TSA (Dynamic TSA) [Mase2008]. Il TSA spende quasi metà del tempo necessario risolvere le collisioni. Questo dipende dalle operazioni del TSA ed in particolare dal modo di stimare il numero di tag che collidono. È stato osservato che nel caso di reti di grandi dimensioni il TSA stima in difetto e di molto questo numero, il Dynamic Tree Slotted Aloha utilizza la conoscenza acquisita durante i cicli di lettura per aggiustare la stima del numero dei tag che collidono, così facendo adatta la lunghezza dei cicli di lettura al numero attuale dei tag che ancora richiedono di essere identificati.

2.3 Identificazione con protocolli basati su alberi di decisione

2.3.1 Alberi Binari

Se guardiamo al comportamento del protocollo Aloha (ad eccezione del TSA) notiamo che non tenta di risolvere le collisioni nel momento che accadono, questi tentativi sono rimandati nel tempo con la speranza che le cose si mettano a posto, in questo modo il sistema può diventare instabile. Nei sistemi multi-access sono stati introdotti un tipo di algoritmi chiamati *Tree-Search algorithm* od anche *Collision Resolution Protocol* (CRP) [Capeta1979], [Mass1981], che possono essere usati per la RFID arbitration e che cercano di risolvere le collisioni non appena queste si verificano. I nodi di questi alberi corrispondono ai tag e trasmettono in time slot quando sono interrogati da un reader, il

reader riconosce se c'è stata una collisione quando più tag trasmettono nello stesso time slot. In questo caso per time slot si intende l'intervallo di tempo in cui si svolge un'interrogazione di un reader e le eventuali risposte da parte dei tag. Il reader manda sempre un feedback informando i tag se 0 frame, 1 frame o più di un frame sono stati trasmessi nello slot precedente. Questi feedback corrispondono rispettivamente ad un idle slot, ad una identificazione o ad una collisione. Questo feedback è necessario perché il tag deve tenere traccia della sua posizione nella ricerca e deve sapere a quale sottoinsieme appartiene e quando poter trasmettere, questo può essere implementato con un contatore [Bertse1992]. In questo tipo di algoritmi o protocolli le collisioni si risolvono, essendo alberi binari, dividendo il set dei nodi che collidono in due sottoinsiemi. I nodi nel primo sottoinsieme trasmettono nel primo time slot mentre i nodi nell'altro sottoinsieme aspettano fino a quando la collisione tra i nodi del primo sottoinsieme è risolta, se nel primo sottoinsieme si verifica un'altra collisione in nodi verranno ulteriormente suddivisi. La procedura verrà ripetuta ricorsivamente fino a quando non ci sono più collisioni. Le operazioni del protocollo ad albero binario possono anche essere descritte in termini di stack, che è la descrizione standard per un tree-search o tree-traversal. Quando si verifica una collisione l'insieme dei tag che collidono viene diviso ed ogni sottoinsieme viene inserito (pushed) in uno stack (ogni elemento di uno stack è un sottoinsieme di nodi). Il sottoinsieme al top dello stack (quello inserito per ultimo) è rimosso ed i tag che appartengono al sottoinsieme sono abilitati a trasmettere. Ogni tag può sapere quando trasmettere se conosce in quale posizione dello stack è il sottoinsieme a cui appartiene, utilizzando il contatore. Quando un tag è coinvolto in una collisione, viene generato un numero random che può assumere due valori 0 o 1, i tag vengono raggruppati in due sottoinsiemi, quelli che hanno generato 0 e che mettono il loro contatore a 0, e quelli che hanno generato un 1 e che mettono il loro contatore ad 1. Ad ogni collisione il contatore del tag viene incrementato di 1 e decrementato di 1 per ogni successo o stato idle, il tag trasmette quando il suo contatore è zero.

In questi protocolli i nuovi dati che arrivano al sistema non vengono trasmessi se è in corso la risoluzione delle collisioni. L'intervallo di tempo in cui la collisione viene risolta è chiamato *collision resolution interval* (CRI). Se in questo intervallo il numero di arrivi nel sistema è mediamente minore del numero di collisioni risolte il sistema si può definire stabile.

I protocolli anti-collisione tree-based possono avere un ritardo nell'identificazione del tag anche maggiore dei protocolli del tipo Aloha, ma non hanno il problema detto starvation, dove il ritardo è molto lungo. L'implementazione di un protocollo di ricerca ad un albero binario [Fink2010] richiede che la precisa posizione dei bit nella collisione venga riconosciuta dal reader. Un protocollo di ricerca binario consiste in una sequenza predefinita di interazioni (comando e risposta) tra un reader e diversi tag (transponder) con lo scopo di poter essere in grado di selezionare un qualsiasi tag appartenente ad un gruppo, anche di grandi dimensioni. Per la realizzazione del protocollo c'è bisogno di un insieme di comandi che possono essere eseguiti dal tag (transponder) (Tab. 2).

Tabella 2 Comandi eseguiti dal Tag (Transponder) per il protocollo di ricerca binari.

REQUEST(SNR)	This command sends a serial number to the transponder as a parameter. If the transponder's own serial number is ***less than*** (or equal to) the received serial number, then the transponder sends its own serial number back to the reader. The group of transponders addressed can thus be preselected and reduced
SELECT_(SNR)	Sends a (predetermined) serial number (SNR) to the transponder as a parameter. The transponder with the identical transponder address will become available for the processing of other commands (e.g. reading and writing data). This transponder is thus selected. Transponders with different addresses will thereafter only respond to a REQUEST command
READ_DATA	The selected transponder sends stored data to the reader. (In a real system there are also commands for authentication or writing, debiting, crediting, etc.)
UNSELECT	The selection of a previously selected transponder is cancelled and the transponder is 'muted'. In this state, the transponder is completely inactive and does not even respond to a REQUEST command. To reactivate the transponder, it must be reset by temporarily removing it from the interrogation zone of the reader (= no power supply)

Ogni tag ha un unico identificatore o serial number (Tab. 3), nel nostro esempio usiamo un 8-bit serial number che garantisce l'unicità dei tag fino ad un massimo 256.

Tabella 3 Serial number dei transponder (Tag) usati nell' esempio

Transponder 1	10110010
Transponder 2	10100011
Transponder 3	10110011
Transponder 4	11100011

Assumiamo di avere 4 transponder, la prima iterazione del nostro protocollo comincia con il reader che trasmette il comando REQUEST (≤11111111). Il serial number 11111111 è il più alto possibile, i serial number dei transponder che sono nel campo di lettura del reader hanno un valore minore o uguale a 11111111, perciò a questo comando rispondono tutti i transponder (Fig.17).

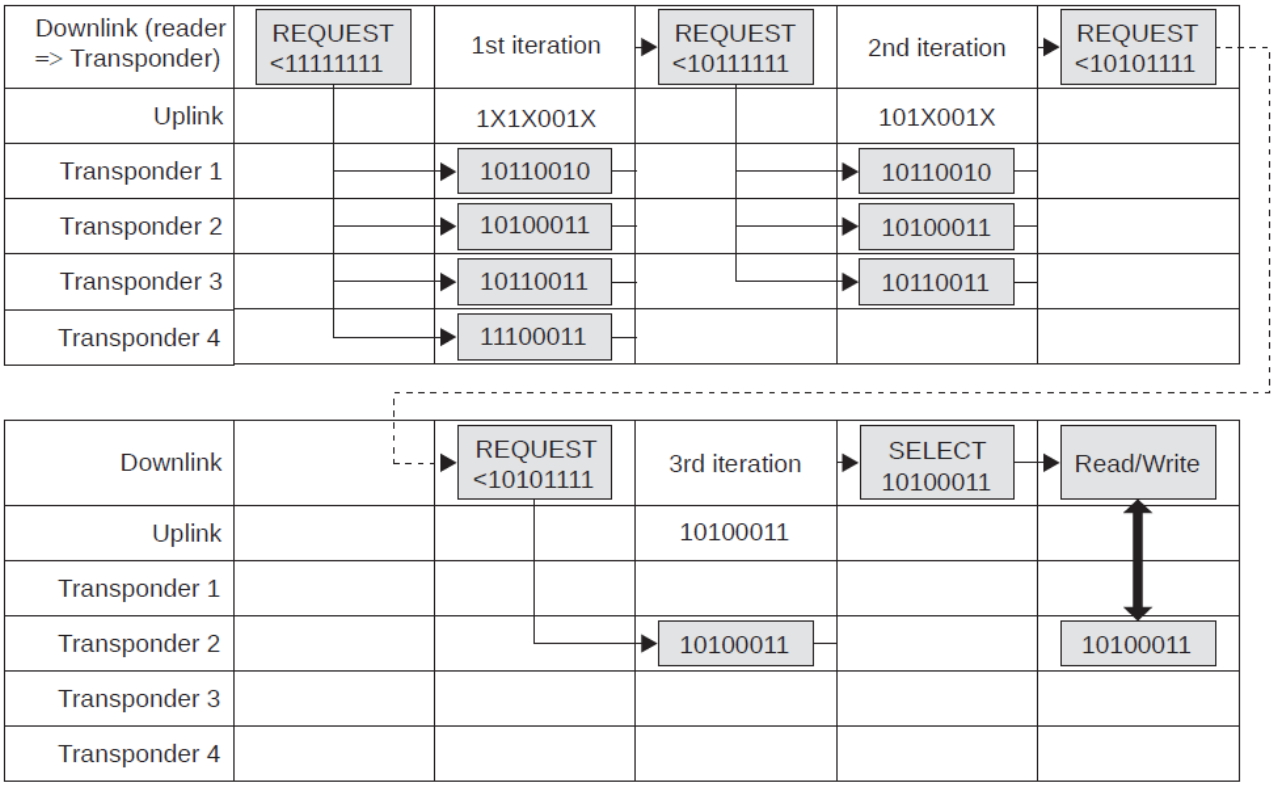

Figura 17 . I serial number che sono trasmessi dai transponder al reader in risposta al comando REQUEST collidono. Dopo alcune iterazioni il protocollo porta ad una situazione finale dove un solo transponder risponde.

La sincronizzazione di tutti i tag, in modo tale che tutti trasmettano esattamente allo stesso tempo il loro serial number è cruciale per il funzionamento del protocollo di ricerca binaria. In questo modo si riesce a capire quali bit collidono. Nelle posizioni dei bit 0,4,6 del serial number ricevuto c'è stata una collisione (X) come il risultato della sovrapposizione delle differenti sequenze dei bit delle risposte dei transponder. Se c'è stata una collisione significa che ci sono uno o più transponder nel campo di lettura del reader, la sequenza di bit ricevuta dal reader è 1X1X001X e fa presupporre che ci siano 8 tag (Tab. 4). Il bit 6 è il più alto bit nel quale è avvenuta una collisione nella prima iterazione, questo significa che c'è almeno un tag nei range $SNR \geqslant 11000000$, $SNR \leqslant 10111111$.

Decidiamo arbitrariamente di continuare la ricerca per $SNR \leqslant 10111111$ (1st iteration, Fig.

17), mettendo il bit 6 a 0 e quelli in posizione più bassa tutti a 1. Il reader trasmette ora il comando REQUEST (≤ 10111111) e i tag 1,2 e 3 che soddisfano questa condizione, rispondono trasmettendo il loro serial number. In questa risposta 101X001X la sequenza di bit mostra che c'è collisione al bit 0 e al bit 4, questo indica la possibile esistenza di quattro tag ancora da identificare.

Tabella 4 Possibili serial number (tag) dopo l'elaborazione dei dati ricevuti tenendo conto delle collisioni (X). I serial number con asterisco sono effettivamente esistenti.

Bit number:	7	6	5	4	3 2 1	0
Received data in the reader	1	**X**	1	**X**	001	**X**
Possible serial number A	1	**0**	1	**0**	001	**0**
Possible serial number B*	1	**0**	1	**0**	001	**1**
Possible serial number C*	1	**0**	1	**1**	001	**0**
Possible serial number D*	1	**0**	1	**1**	001	**1**
Possible serial number E	1	**1**	1	**0**	001	**0**
Possible serial number F*	1	**1**	1	**0**	001	**1**
Possible serial number G	1	**1**	1	**1**	001	**0**
Possible serial number H	1	**1**	1	**1**	001	**1**

Come nella precedente iterazione mettiamo arbitrariamente il bit 4 a 0 e quelli in posizione più bassa tutti a 1, quindi il comando per la terza iterazione è REQUEST (≤ 10101111).
Il tag che soddisfa questa condizione è solo il numero 2 (10100011) che perciò è l'unico che risponde alla richiesta del reader (Fig. 18). A questo punto abbiamo selezionato un serial number valido e non è necessaria un'ulteriore iterazione.

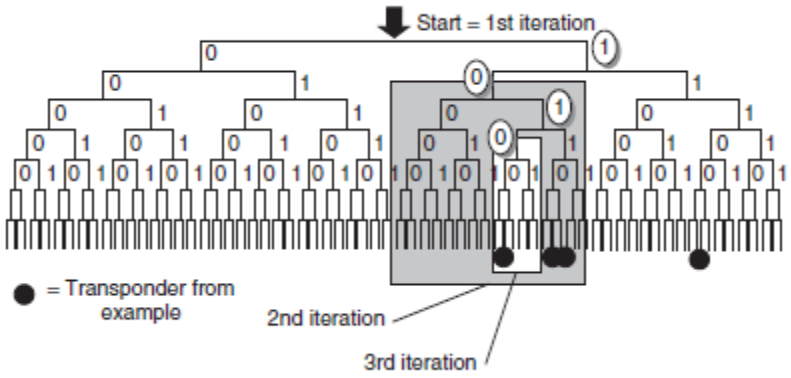

Figura 18 Identificazione del transponder 2 alla terza iterazione.

Il reader trasmette il comando SELECT(10100011) indirizzato al tag 2, seguito da eventuali comandi di read o write, il tag 2 è l'unico a rispondere, tutti gli altri tag sono silenti.

Finite le operazioni di read o write, il tag 2 può essere disattivato con il comando UNSELECT e da questo momento non risponderà ai comandi REQUEST seguenti. Eliminando i tag identificati si riducono il numero delle iterazioni necessarie per identificare i rimanenti tag. In questo caso ripetendo la procedura si identificheranno i tag 1,3 e 4.
Lo pseudo codice della procedura di identificazione potrebbe essere il seguente:

```
while true:
send REQUEST(maxSNR)
receive(SNR)
while SNR contains 'X':
replace highest 'X' with '0' and set all lower bits '1'
send REQUEST(SNR)
receive(SNR)
foundTag(SNR)
send SELECT(SNR) ...
send UNSELECT
```

2.3.2 Alberi binari dinamici

Nella ricerca binaria descritta precedentemente, i serial number sono trasmessi con la loro lunghezza massima. In pratica i serial number dei tag possono arrivare fino a 10 byte di lunghezza, quindi per identificare un tag bisogna trasmettere una grossa quantità di dati [Fink2010]. Esaminando i dati durante la trasmissione possiamo vedere che (Fig. 19):

- I bit del comando che vanno da $(X-1)$ a 0 non contengono nessuna informazione in più per il tag, dal momento che sono tutti a 1.
- I bit da N a X del serial number trasmesso dal tag come risposta, non contengono nessuna informazione in più per il reader, dal momento che sono già conosciuti e prestabiliti.

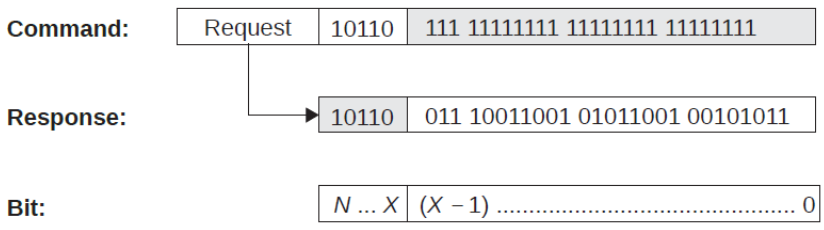

Figura 19 In grigio i bit che sono ridondanti sia nel comando che nella risposta. X è la più alta posizione del bit in cui è avvenuta una collisione nell'iterazione precedente

Si può migliorare il protocollo di ricerca non trasmettendo i bit ridondanti, nel comando REQUEST il reader manda solo la parte $(N - X)$ del serial number, tutti i tag rispondono alla richiesta del reader trasmettendo i bit dei loro serial number da $(X - 1)$ a 0. I tag sono informati del numero di bit che ricevono, con il parametro NVB (number of valid bits) nel comando REQUEST. La sequenza delle iterazioni e i serial number dei tag è la solita usata nel precedente protocollo, ma la quantità dei dati trasmessi si riduce fino al 50%.
La Figura 20 mostra il funzionamento di questo protocollo.

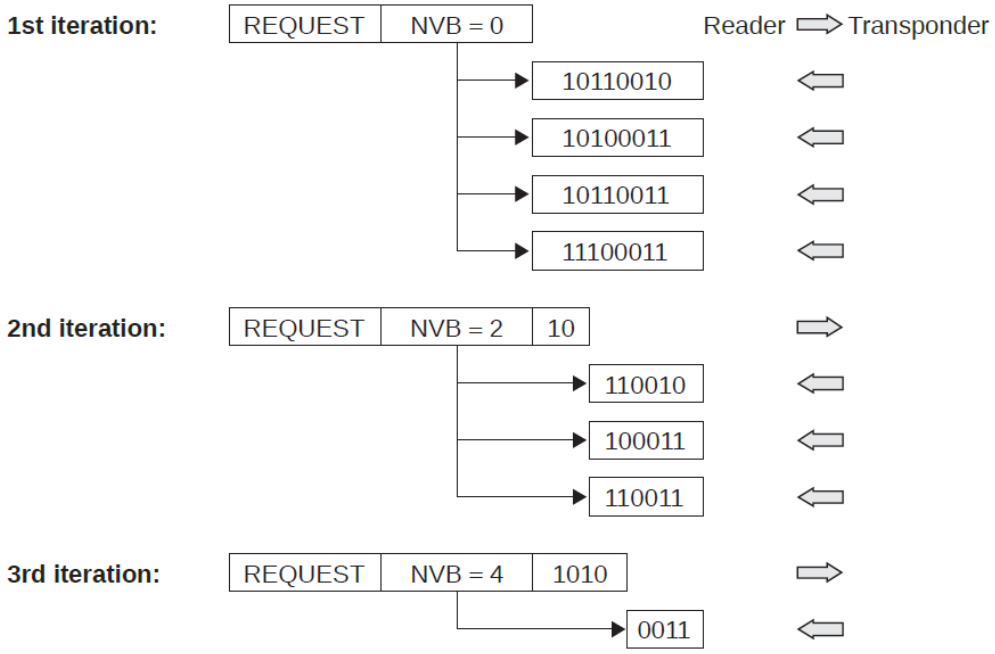

Figura 20 Il protocollo di ricerca binaria dinamica non trasmette i bits ridondanti dei serial number. La trasmissione dei dati si riduce anche del 50%

Vediamo ora lo pseudo-codice di un protocollo di ricerca binario [Bonuc2007].
Il reader implementa l'identificazione in maniera ricorsiva suddividendo l'insieme dei tag che trasmettono una risposta, ogni tag ha un counter inizialmente a zero, solo i tag con il counter a zero possono rispondere all'interrogazione (query) del reader. Dopo ogni trasmissione dei tag il reader notifica il risultato della query: collisione, identificazione o nessuna risposta. Quando si verifica una collisione ogni tag con counter a zero incrementa il proprio contatore con un numero random binario (0,1). Gli altri tag incrementano di uno il loro contatore. In questo modo l'insieme dei tag che hanno risposto è diviso in due sottoinsiemi. Dopo una trasmissione senza collisioni tutti i tag decrementano il loro contatore di uno.

Pseudo-code of BS protocol

Reader procedure:

```
channelStatus = 2;
whilechannelStatus > 1) do
broadcast(query);
receiveAnswers;
broadcast(channelStatus);
if (channelStatus = = 1) then tagIdentification();
```

Tag procedure:

```
identified = false; myCounter = 0;
while (not identified) do
     receive(query);
      if (myCounter = = 0) then sendAnswer;
      receive(channelStatus);
      if (channelStatus > 1) then
          if (myCounter==0) then
                myCounter + = rand()%2;   //collisione
          else myCounter++;
        if (channelStatus < = 1) then      //nessuna collisione
           myCounter--;
     if receivedIDrequest then
          send myID;
          identified = true;
```

La prestazione del protocollo ad albero binario è del 34% [Bagn2009].

2.3.3 Query-Tree

Il protocollo Query-Tree [Law2000], [Zhou2004], [Abra2002] è memoryless, cioè il tag non deve ricordarsi delle operazioni eseguite nel corso delle interrogazioni. La risposta di un tag dipende dall'interrogazione attuale e non tiene conto delle interrogazioni passate. I tag non mantengono informazioni di stato e non comunicano tra di loro, rispondono semplicemente alle interrogazioni del reader. Il solo calcolo richiesto ai tag è quello di confrontare il proprio identificatore con la stringa della interrogazione del reader. In questo protocollo invece di mandare un bit ad ogni interrogazione, il reader manda una stringa di n bit prefix (prefisso) che sarà confrontata con i primi n bit dell'identificatore dei tag.

L'algoritmo può essere descritto come segue [Abra2002]:

a) Il reader trasmette una stringa prefix p, inizialmente viene inviato un unico bit, 0 o 1.
b) Tre possibili casi si possono presentare in base alla risposta dei tag:

- più di un tag ha p come prefix: tutti i tag che hanno p come prefix manderanno una risposta. All'inizio del processo di identificazione è più probabile che più di un tag abbia lo stesso prefix e quando le risposte trasmesse dai tag raggiungono simultaneamente il reader si verifica una collisione.
- Esattamente un tag ha p come prefix: il reader riceve una risposta specifica (identificatore) dal tag e così il tag viene identificato.
- Nessun tag ha p come prefix: se nessun tag ha p come prefix il reader non riceve nessuna risposta dai tag.

c) Prepara un'altra stringa p aggiungendo 0 o 1 come appropriato, questa sarà la prossima stringa da mandare ai tag.

d) Ripetere gli step da a) a c), che costituiscono un ciclo, fino a quando tutti i tag sono identificati.

Dopo ogni ciclo il reader informa i tag trasmettendo l'identificatore del tag che è stato identificato nel ciclo precedente, così il tag identificato non trasmetterà nei prossimi cicli.
Adesso illustriamo il protocollo con un esempio e assumiamo di dover identificare i quattro tag: 010, 011, 101 e 111. La Tab. 5 descrive i passi eseguiti dal protocollo. Per identificare i 4 tag, il reader deve mandare la stringa prefix 9 volte.

Tabella 5 Comunicazione tra il reader e i tag nel protocollo QT.

Step	Query	Response
1	[a] (Empty String)	Collision
2	0	Collision
3	1	Collision
4	00	No response
5	01	Collision
6	10	101
7	11	111
8	010	010
9	011	011

Il protocollo QT genera un albero binario, ad ogni messaggio trasmesso dal reader corrisponde un solo nodo dell'albero. L'arco che connette i nodi contiene la stringa prefix trasmessa. I nodi in nero sono i tag che sono stati identificati dal reader. I nodi in grigio indicano i tag che hanno colliso e i nodi in bianco indicano che nessun tag ha risposto. Le stringhe in rosso sono gli identificatori dei tag da identificare.

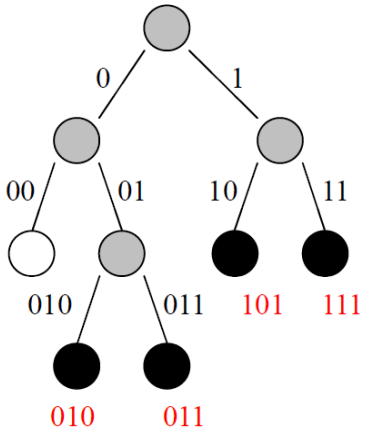

Figura 21 Esempio di protocollo Query Tree

Ci sono stati miglioramenti al protocollo QT per ridurre il tempo di esecuzione, il più importante si chiama *Query Tree Improved (QTI)* [Law2000], [Bagn2009], la variazione usata si chiama *Short Cutting* e cerca di evitare le interrogazioni che producono collisioni che nell'albero corrispondono a nodi interni. Supponiamo che una interrogazione con un prefix p produca una collisione. Alla prossima interrogazione la stringa p viene allungata con 0 o 1 e se dopo l'interrogazione con prefix p0 non abbiamo nessuna risposta dai tag (nessun string match) allora concludiamo che ci sono almeno due tag con stringa p1. Il reader salta l'interrogazione con prefix p1 perché ci saranno sicuramente collisioni e passa direttamente alle interrogazioni con stringhe p10 e p11.
Le prestazioni del protocollo QTI è di circa del 37% [Bagn2009].

2.4 Altre Problematiche

Ci sono dei protocolli [Bonuc2015] che cercano di risolvere problemi diversi da quelli fino a qui visti e che richiedono una appropriata esecuzione del polling di tutti o parte dei tag: *Information Collection*, *Exact Missing*, *Probabilistic Missing* e *Cloned Tags Warning*.

2.4.1 Information Collection

Dopo la rivoluzione nell'industria introdotta dall'uso dei codici a barre, le tecnologie RFID rivoluzioneranno la gestione dei magazzini e dell'inventario [Chen2011]. I tag permettono di identificare gli oggetti in un ambiente wireless, il prossimo passo sarà trovare altri benefici da questa infrastruttura. Per esempio attraverso l'aggiunta, ai tag, di sensori per raccogliere informazioni in tempo reale sullo stato degli oggetti o sull'ambiente dove questi oggetti sono dislocati. Da qui la necessità di avere protocolli efficienti per raccogliere

informazioni dai tag.

Questo rappresenta una problematica che non viene gestita dai protocolli esistenti.

2.4.2 Missing Tags

Il problema *Missing Tag* riguarda il monitoring frequente, quindi nel minor tempo possibile, di grandi insiemi di tag; esso è stato trattato in due versioni [Li2010], [Luo2012]:

- La prima chiamata *Exact Missing*, si propone di trovare esattamente tutti i tag mancanti. Attaccando un tag ad un oggetto, il proprietario può periodicamente monitorarli per determinare quali tag e quindi quali oggetti sono presenti, verificando cosi che non ci siano stati furti.
- La seconda versione è chiamata *Probabilistic Missing* e si propone di verificare se un insieme di tag è intatto o no. Per intatto si intende che tutti i tag sono presenti allo stesso tempo nel campo di lettura del reader. Il problema può essere risolto con una certa tolleranza, cioè viene tollerato che possano mancare meno di m tag. Se mancano meno di m tag l'insieme di tag viene considerato intatto.

2.4.3 Cloned Tags Warning

Il *Tag Cloning* [Juels2006] è una minaccia per sistemi RFID. In un attacco Tag cloning si produce una replica esatta di un tag legittimo, con lo scopo di contraffare oggetti in un punto vendita o passaporti. Anche in questo caso il tempo è il parametro più importante perché l'attacco deve essere segnalato tempestivamente, sono quindi necessari nuovi e più efficienti protocolli.

Capitolo 3 Sicurezza e Privacy

La gestione della sicurezza che riguarda l'accesso a delle risorse si basa su tre azioni:

- Identificazione
- Autenticazione
- Autorizzazione

L’identificazione è il processo che associa ad una entità fisica un identificativo univoco all’interno del sistema, che può essere una username o un ID. L’identificazione è necessaria per associare ad un preciso utente le azioni fatte su un sistema o gli accessi ad una risorsa.

Non è sufficiente dichiarare di essere un utente e di aver associato un ID e necessario provare la propria identità attraverso il processo di autenticazione, che spesso si basa sull’inserimento di una password.

Infine l'autorizzazione definisce diritti o privilegi sulle risorse del sistema.

Con la tecnologia RFID sorgono un certo numero di problemi di sicurezza e privacy che potrebbero ridurre sostanzialmente i benefici della tecnologia. Questo evidenzia che una nuova e più sofisticata tecnologia non presuppone maggior sicurezza.

Con i sistemi RFID la lettura non richiede una line-of-sight, ciò determina un progresso rispetto alla lettura dei codici a barre, ma può facilitare azioni fraudolente sui dati perché non c'è contatto fisico, né visibilità delle apparecchiature. Rispetto ai precedenti sistemi i tag contengono più informazioni, questo vantaggio pone anche maggiori problemi legati alla sicurezza e alla privacy, come avvantaggiare la concorrenza sleale.

I tag rispondono alle interrogazioni senza avvisare il sistema, così se il range lo permette, letture clandestine sono possibili.

I tag emettono dei serial number che sono trasmessi ai reader vicini e quindi segnalano la loro posizione anche ad eventuali intrusi. L'acquisto con una carta di credito rende possibile creare un’associazione tra il cliente e i prodotti acquistati, questo può essere usato per studi di mercato anche senza il consenso del cliente. I tag come quelli EPC contengono altre informazioni come un codice prodotto e l’identificativo del produttore, questo comporta il rischio che queste informazioni vengano utilizzate per effettuare inventari clandestini.

Gli aspetti vulnerabili di un sistema RFID sono:

- La trasmissione wireless tra tag e reader, che è oggetto della maggior parte degli attacchi fraudolenti.
- Le limitate risorse dei tag: la potenza e la memoria dei tag passivi economici limitano l'applicazione di misure di sicurezza.
- Le dimensioni minuscole dei tag, i quali potrebbero essere trasportati da persone a loro insaputa.

Ci sono attacchi che generano problematiche relative alla privacy:

- Il tagging di prodotti individuali, che per esempio permettono un veloce e automatico controllo del magazzino, presenta come problema di privacy la lettura non autorizzata dei tag. In assenza di protezioni sarebbe possibile conoscere i beni acquistati da una determinata persona, il loro prezzo e altre informazioni, creando quindi un profilo cliente non autorizzato.
- L'identificazione di documenti elettronici e contactless smart card, comporta rischi per la privacy, la lettura dei tag porta alla conoscenza di dati personali del proprietario del documento, permettendo così la clonazione del documento stesso, oppure la tracciabilità dei movimenti.

Un fattore, che deve essere necessariamente preso in considerazione, è la fiducia del cliente, tutte le misure intraprese per creare un sistema sicuro devono essere accompagnate anche da un’appropriata informazione, in modo che la percezione che il cliente ha del livello di sicurezza e privacy sia adeguata e rassicurante.

3.1 Attacchi e Contromisure

Esaminiamo ora le maggiori minacce alla sicurezza [Rott2009], [Xiao2008], [Rieb2006] messe in campo contro i sistemi RFID. Le principali tipologie di minacce sono relative all’acquisizione o l’alterazione illecita dei dati contenuti nei tag. Questo può avvenire sia attraverso interrogazioni fraudolente con reader non autorizzati, sia mediante intercettazione, tramite ricevitori radio, durante una lettura degli stessi da parte di un reader autorizzato. Può succedere che un tipo di attacco sia un atto preparatorio per un altro attacco, per esempio una intercettazione può essere usata per una clonazione di un tag, questa potrebbe essere seguita da un attacco del tipo *man-in-the-middle*, che può portare ad un accesso non

autorizzato al sistema.

Nella prossima figura vengono rappresentate le varie tipologie di attacco, i componenti del sistema interessati e i paragrafi in cui l'argomento viene trattato:

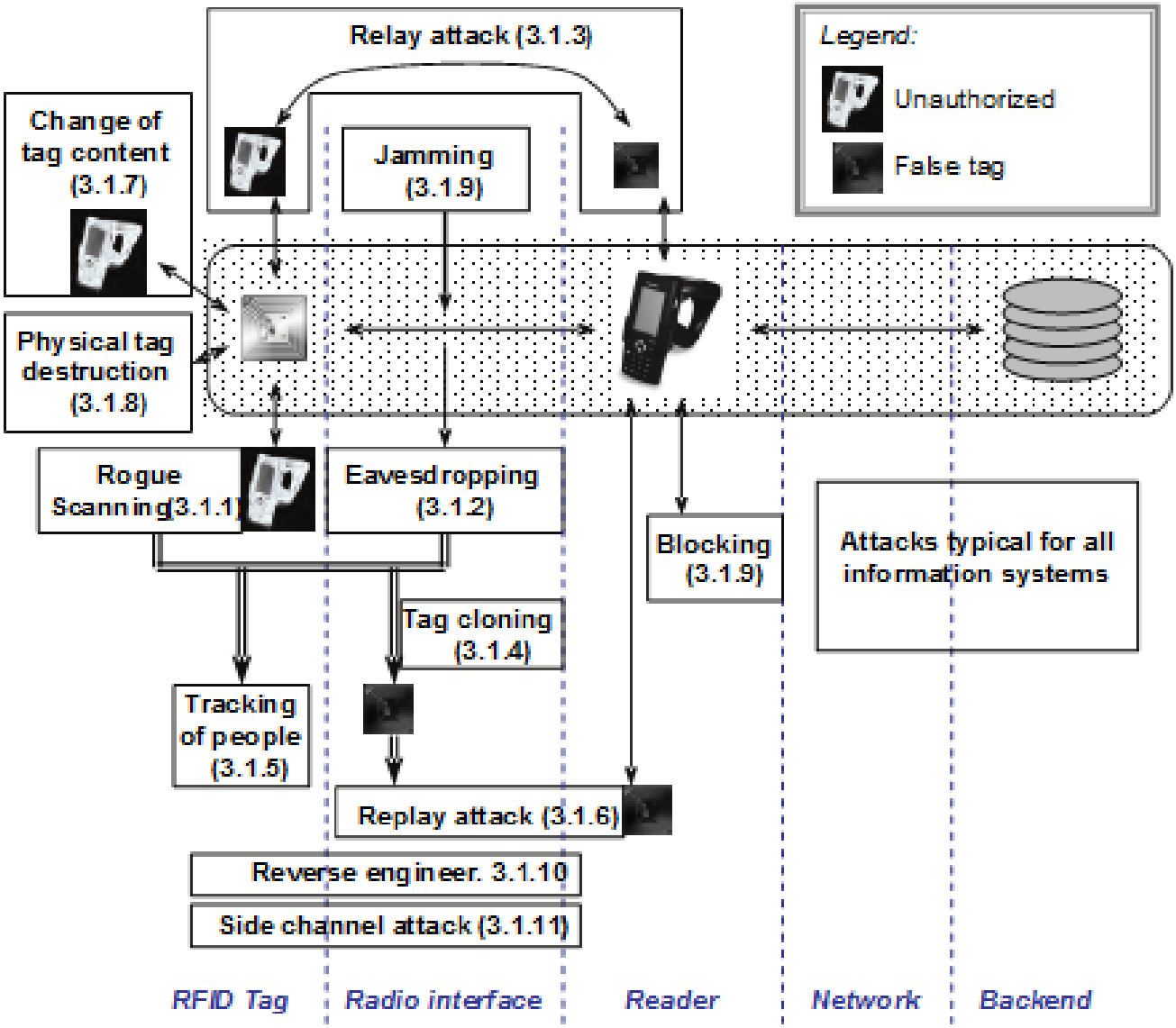

Figura 22 Attacchi ai sistemi RFID, con indicato i paragrafi in cui vengono trattati.

3.1.1 Lettura Fraudolenta del Tag

Un reader non autorizzato ed occultato, oppure un reader portatile, possono essere usati per leggere le informazioni di un tag. La distanza a cui un reader può leggere può andare diverse volte oltre la distanza standard per la comunicazione. La distanza standard per leggere un passaporto elettronico o una card è di 10 cm, con un reader che legga fino a 25 cm è possibile leggere una card dalla tasca di una persona.

Alcune delle contromisure attuabili:

- L’utilizzo di tag a corto raggio, dove è possibile, rende più difficile la lettura fraudolenta.
- Schermatura dei tag con un materiale anti-skimming (alluminio).
- Spostare le informazioni sensibili nel database del server.

3.1.2 Intercettazione (Eavesdropping)

Eavesdropping è una intercettazione fraudolenta di dati in una trasmissione wireless, in un sistema RFID tra un tag ed un reader. L'eavesdropping è una azione passiva, l'aggressore è difficile da individuare perché non emette alcun segnale, infatti non avrà bisogno di energizzare il tag che già riceve energia da un reader legittimo.

Questa aggressione ha due fasi:

1. La ricezione del segnale.
2. L'interpretazione o decodificazione del segnale.

I sistemi RFID sono vulnerabili a questo tipo di attacco soprattutto quando usano algoritmi anti-collisione, poiché il reader invia al tag tutto o parte del serial number.

il reader trasmette con una potenza più alta di quella del tag, quindi le informazioni inviate dal reader vengono intercettate anche a lunga distanza.

Alcune delle contromisure attuabili:

- Minimizzare la distanza di propagazione del segnale.
- Criptazione di dati trasmessi tra il tag e il reader.

3.1.3 Relay Attack (Man-in-the-middle Attack)

L’attacco del tipo *man-in-the-middle* si ha quando, in una connessione tra un reader ed un tag, un terzo estraneo si intromette nella trasmissione ingannando i componenti del sistema. Durante l’attacco i due tag e reader legittimi inconsapevolmente non parlano tra loro, bensì con l’aggressore che simula, alterando i dati di entrambi.

Per contrastare questo attacco è fondamentale la tipologia di protocollo di autenticazione utilizzato.

Dato che l'aggressore ritrasmette l'informazione senza il bisogno di interpretarla, un protocollo di autenticazione con password fissa non protegge contro questo tipo di attacco. La massima distanza tra un tag legittimo ed il reader dell'aggressore, chiamato anche *leech*, deve essere molto corta (50 cm), ma la distanza tra un reader legittimo ed un apparecchio

dell'aggressore che simula un tag, chiamato anche *ghost*, può essere molto più lunga, anche 50 m.

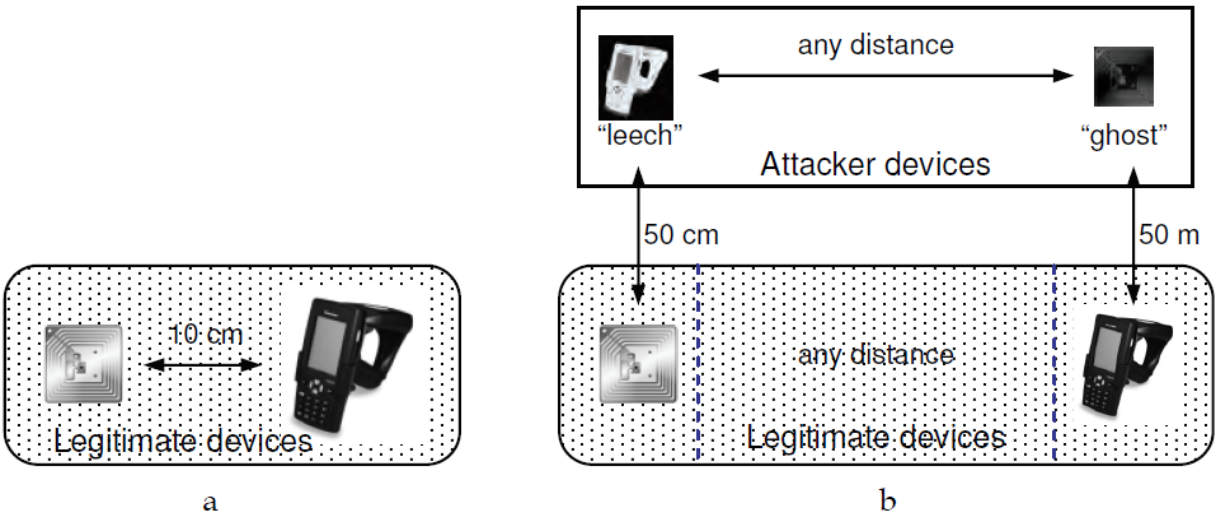

Figura 23 Una comunicazione legittima (a) ed un Ralay Attack (b).

Alcune delle contromisure attuabili:

- l'uso di tag a corto raggio.
- Schermatura di tag con alluminio, quando non sono in uso.
- L'uso di protocolli *Distance-bounding*, dove un'entità (verifier) stabilisce un limite superiore alla sua distanza da un'altra entità (prover). La distanza è calcolata dopo uno scambio di messaggi tra il verifier ed il prover. Il verifier manda una challenge al prover, il quale prover risponde con una response dopo il tempo necessario alla elaborazione del messaggio ricevuto.

3.1.4 Clonazione del tag (Spoofing)

In relazione alla tecnologia RFID, spoofing si verifica quando un tag falsificato impersonifica un tag legittimo, guadagnando quindi un vantaggio illegittimo.

La clonazione di un Tag è un attacco di tipo spoofing, in cui il malintenzionato acquisisce i dati da un tag valido e ne crea una copia non autorizzata.

Può essere utilizzato un tag vuoto, un tag riscrivibile o un'apparecchiatura che ha le solite funzionalità.

Un esempio di clonazione di un tag si ha quando un malintenzionato acquisisce i dati relativi ad un prodotto a basso costo presente in un negozio per poi caricarli su un altro tag, che verrà associato ad un oggetto simile ma molto più costoso.

La clonazione permette di superare i controlli di accesso o fare una transazione al posto del legittimo proprietario.
Una contromisura si ha implementando un protocollo di autenticazione RFID e crittografia dei dati, che aumenta la complessità e il costo tecnologie necessarie per un attacco di successo [Xiao2008].
È necessario applicare anche contromisure di tipo fisico, utilizzando delle strutture fisiche non clonabili incorporate negli involucri degli oggetti, la cui rimozione ne comporterebbe la distruzione.
Tuyls e Batina [Tuyls2006], propongono di utilizzare *Physical Unclonable Functions* (PUFs), come unità di memoria sicure dove salvare le chiavi segrete sui tag.
Gli autori hanno affermato che sia l'attacco fisico sia quello basato sull'attacco del protocollo di comunicazione tra Tag e Reader può essere impedito.

3.1.5 Tracciamento delle persone

Il tracciamento fraudolento si verifica quando un aggressore segue i movimenti di persone attraverso tag RFID, questo avviene con la lettura diretta dei tag, oppure con l'intercettazione fatta vicino ad un reader legittimo.
Alcune delle contromisure attuabili:

- l'uso di tag a corto raggio.
- la loro schermatura.
- l'autenticazione dei reader.
- disabilitare i tag quando non sono in uso.

3.1.6 Replay Attack

Nel caso di un replay attack l'aggressore si impadronisce dell'identità di un'altra persona, ripetendo la stessa sequenza di autenticazione di una persona autorizzata. Un replay attack può essere fatto utilizzando un clone di un tag legittimo, oppure ritrasmettendo da un computer il segnale intercettato. Per portare avanti questo tipo di attacco bisogna ottenere l'informazione che viene trasmessa da un tag durante un'interrogazione. Una contromisura a questo tipo di frode è impedire le intercettazioni e la lettura non autorizzata del tag, per esempio con l'autenticazione del tag con un challenge-response protocol.
Se il protocollo è progettato bene la chiave necessaria per preparare la risposta non può essere dedotta dai dati della dalla trasmissione wireless.

3.1.7 Modifica fraudolenta del contenuto dei tag

La modifica del contenuto di un tag o di alcuni attributi di un oggetto falsifica il suo profilo, per esempio ad una persona illegittima potrebbe essere consentito l'accesso ad un sistema come lo si potrebbe impedire ad una persona legittima.

Il contenuto dei tag può essere modificato inserendo codice "maligno" (*Code Insertion*), con lo scopo di far eseguire lo stesso sui server di back end.

Una tipologia di attacco che ne deriva è la *SQL Injection*, che prevede l'inserimento nei dati del tag di codice SQL capace di compromettere seriamente il database di back end.

I limiti di archiviazione di dati nel tag non comportano un limite a questo tipo di attacco, è infatti possibile provocare danni al database con pochi caratteri in input.

Ad esempio iniettando:

```
;shutdown--
```

Tale istruzione provocherebbe lo spegnimento del database utilizzando solamente 12 caratteri [Rieb2006].

I tag riscrivibili possono essere portatori di malware, in questo tipo di tag il contenuto della memoria può essere protetto disabilitando temporaneamente la capacità di scrittura (funzioni lock e permalock in EPC standard).

Per prevenire attacchi di tipo di Code Insertion occorre escludere la possibilità di interpretare i dati del tag come comandi.

3.1.8 Distruzione fisica del tag

La distruzione fisica di un tag si può attuare riscaldandolo con le microonde o colpendolo con un martello. Queste azioni fraudolente vengono attuate per esempio quando un tag viene usato come protezione contro il furto. Il tag RFID di un passaporto elettronico, potrebbe essere l'obiettivo di questa azione da parte del proprietario, per paura che gli venga rubata l'identità, anche se il tag RIFD non funziona il passaporto è ritenuto valido.

3.1.9 Blocking

Il *Blocking* viene eseguito con un tag con funzione bloccante, che simula la presenza di enorme numero di tag e causa un rifiuto del servizio (*denial of service*), cioè rispondere alle interrogazioni dei reader.

Se infatti un TAG con funzione bloccante decide di rispondere affermativamente a ogni

domanda del reader, farà sembrare che siano presenti tutti i TAG possibili, rendendo l'operazione di lettura estremamente lunga e complessa.
Il blocking dei tag può essere utilizzato anche come strumento di protezione per la privacy [Juels2003], ad esempio, un tag può essere settato in fase di "blocking" al momento dell'acquisto dell'oggetto a cui è associato.

3.1.10 Reverse Engineering

Il *Reverse Engineering* indica un metodo per scoprire la struttura dei circuiti e perfino i valori del voltaggio, in punti diversi del circuito mentre è in uso. L'obiettivo è conoscere gli algoritmi di funzionamento o le chiavi di criptazione, informazioni necessarie per la clonazione dei tag. Questo tipo di attacco richiede un alto livello di conoscenza ed esperienza e l'uso di strumenti costosi e sofisticati.
Alcune delle contromisure attuabili:

- Inserimento di strutture *Dummy*, che hanno il solo scopo di depistare.
- Schermatura dei chip, soprattutto la memoria il cui contenuto potrebbe essere criptato.

3.1.11 Side Channel Attack

Il *Side-Channel Attack* è un attacco basato su informazioni ottenute dall'implementazione fisica di un sistema criptato, non fa ricorso quindi a vulnerabilità negli algoritmi oppure ad un brute-force attack, cioè provando ogni combinazione di passwords fino a trovare la password corretta. Per esempio le informazioni sui tempi, il consumo di energia, le emissioni elettromagnetiche o persino il suono possono fornire informazioni che possono essere usate per capire il funzionamento del sistema ed esporlo ad un attacco fraudolento.

3.2 Privacy e aspetti sociali dell'uso della tecnologia RFID

3.2.1 Il Garante della Privacy a proposito di RFID

Il garante per la protezione dei dati personali [Gara2005] ha individuato delle garanzie necessarie per affrontare un uso pervasivo della tecnologia RFID nella società. Sappiamo che l'utilizzo di tale tecnologia può risultare utile, ad esempio, per garantire una migliore gestione dei prodotti aziendali, per incrementare la rapidità di operazioni commerciali anche a vantaggio dei consumatori, per rintracciare l'origine di prodotti particolarmente delicati, per controllare accessi a luoghi riservati e per altri usi nei luoghi di lavoro.
Tuttavia, determinati impieghi della tecnologia RFID possono costituire una violazione del

diritto alla protezione dei dati personali ed avere serie ripercussioni sull'integrità e la dignità della persona, anche perché, per le ridotte dimensioni e l'ubicazione delle "etichette intelligenti" e dei relativi lettori, il trattamento dei dati personali può essere effettuato all'insaputa dell'interessato. In particolare l'impiego della tecnologia RFID, da parte di soggetti privati o di soggetti pubblici, può determinare forme di controllo sulle persone, limitandone le libertà. Potrebbero, ad esempio, raccogliersi innumerevoli dati sulle abitudini di un individuo a fini di profilazione, tracciare i percorsi effettuati da quest'ultimo o verificare prodotti (vestiti, accessori, medicine, prodotti di valore) dallo stesso indossati o trasportati. In alcune ipotesi, l'impiego della tecnologia RFID può essere finalizzato esclusivamente al tracciamento di prodotti, per garantire una maggiore efficienza nel processo di produzione industriale. In particolare, nel caso in cui tali sistemi siano impiegati da produttori o distributori solo all'interno di una catena di distribuzione, l'informazione contenuta su ciascuna etichetta come stato di conservazione, stabilimento di produzione, sussistenza di difetti, appartenenza a partite avariate, ecc. è relativa ai soli produttori o distributori. Questo tipo di trattamento di dati non pone particolari problemi di liceità. In altri casi, invece, può comportare il trattamento di dati personali relativi a terzi, persone fisiche o giuridiche, enti o associazioni. Infatti, le "etichette" potrebbero contenere esse stesse dati personali, o essere impiegate in modo tale da rendere comunque identificabili gli interessati attraverso il raffronto con altre informazioni. I sistemi informativi cui esse sono collegate possono permettere, di individuare la posizione geografica di chi detiene l'etichetta o l'oggetto su cui essa è apposta, con considerevoli ripercussioni sulla libertà di circolazione delle persone. La tecnologia RFID può essere inoltre usata nelle tecniche di impianto di microchip sottocutaneo, anche su individui: l'inserimento di microprocessori sottopelle, pone il delicato problema dei diritti delle persone e rende quindi necessaria la predisposizione di particolari cautele. Ulteriori pericoli per gli interessati possono derivare, dalla possibilità che terzi non autorizzati "leggano" i contenuti delle etichette o intervengano sugli stessi (mediante, ad esempio, "riscrittura"). Si deve tenere anche conto che lo sviluppo tecnologico può comportare un aumento della potenza dei sistemi RFID, rendendo possibile una "lettura" delle etichette a distanze sempre maggiori; il progressivo contenimento dei costi di produzione dei dispositivi in questione agevola la crescita dell'impiego di tali tecniche di identificazione. È quindi necessario che l'implementazione e l'utilizzo di questa tecnologia, nel caso di trattamento di dati personali, avvenga nel rispetto dei principi dettati

dal Codice, delle libertà, dei diritti fondamentali e della dignità degli interessati. A garanzia degli interessati, si propongono pertanto alcune prime misure che devono essere adottate da parte di coloro che, a diverso titolo, si avvalgano di tecniche fondate sulla tecnologia RFID. Tali misure si applicano ai casi in cui si trattino dati personali relativi a terzi identificati o identificabili; non valgono invece nei casi, che non pongono particolari problemi sul piano della protezione dei dati, in cui la tecnologia sia utilizzata, ad esempio, in una catena di distribuzione aziendale al solo fine di garantire una maggiore efficienza del processo di produzione. Si possono proporre ulteriori misure che potrebbero rendersi necessarie in relazione a specifici trattamenti di dati personali effettuati mediante tecnologia RFID, anche in vista dell'evoluzione rapida e costante di questa tecnologia. Il suo utilizzo può comportare condizionamenti e vincoli per gli interessati, è necessario quindi assicurare il rigoroso rispetto di tutti i principi dettati dal Codice, in particolare:

Principio di necessità

I sistemi di RFID devono essere configurati in modo tale da evitare l'utilizzo di dati personali o l'identificabilità degli interessati, quando non siano strettamente necessarie in relazione allo scopo. Tale valutazione deve essere condotta tenendo presente che nella maggior parte degli impieghi, ad esempio nella catena di distribuzione di prodotti, non è necessario trattare dati personali relativi a terzi.

Liceità

Il trattamento mediante RFID è lecito solo se si fonda su uno dei presupposti che il Codice prevede per soggetti pubblici, per soggetti privati ed enti pubblici economici. L'utilizzo di tali tecniche deve svolgersi anche nel rispetto di altre leggi e regolamenti a seconda del loro settore di impiego. In ambito lavorativo, l'uso di tecniche RFID deve in particolare rispettare il divieto di controllo a distanza del lavoratore.

Finalità e qualità dei dati

Il titolare può trattare dati personali esclusivamente per scopi determinati,
espliciti e legittimi. I dati possono essere inoltre utilizzati soltanto in termini compatibili con la finalità per la quale sono stati originariamente raccolti, devono essere conservati per il tempo strettamente necessario a perseguire tale finalità, decorso il quale devono essere cancellati o resi anonimi. l titolare deve curare la pertinenza e non eccedenza, l'esattezza e l'aggiornamento dei dati personali.

Proporzionalità

Il titolare deve verificare il rispetto del principio di proporzionalità in tutte le diverse fasi del

trattamento. I dati trattati e le modalità del loro trattamento, anche con riferimento alla tipologia delle infrastrutture di rete adoperate, non devono risultare sproporzionati rispetto agli scopi da prefissare. Non risulta di regola giustificato il trattamento che comporti il funzionamento delle etichette apposte su prodotti acquistati dall'interessato anche fuori dell'esercizio commerciale, a meno che ciò sia necessario per fornire un servizio specificamente e liberamente richiesto dall'interessato stesso.

Informativa

Il titolare del trattamento, nel fornire agli interessati la prescritta informativa precisando anche le modalità del trattamento, deve indicare la presenza di etichette RFID e specificare che, attraverso i sistemi connessi, è possibile raccogliere dati personali senza che gli interessati si attivino al riguardo. Analogamente, deve essere segnalata mediante informativa, l'esistenza di lettori in grado di "attivare" l'etichetta (lettori che possono comunque essere presenti solo in quanto strettamente necessari in rapporto alla finalità del trattamento).

Chiara evidenza deve essere data anche alle modalità per asportare o disattivare l'etichetta, o per interrompere in altro modo il funzionamento del sistema RFID. L'informativa potrebbe essere altresì fornita attraverso appositi avvisi, agevolmente visionabili nei luoghi in cui le tecniche RFID sono adoperate, con un formato ed un posizionamento tale da risultare chiaramente visibile. La presenza di avvisi non esime i titolari del trattamento dall'apporre un'idonea informativa sugli oggetti o sui prodotti recanti le "etichette intelligenti", qualora le stesse rimangano attive dopo che è stato reso possibile associarle con dati relativi a terzi identificati o identificabili, in particolare al di fuori dei luoghi (ad esempio esercizi commerciali) in cui si fa uso della RFID.

Trattamento da parte di privati: il consenso

In generale, l'utilizzo della tecnologia RFID che implichi un trattamento di dati personali da parte di privati può essere effettuato solo con il consenso dell'interessato, a meno che ricorra un altro presupposto equipollente del trattamento.

Esercizio dei diritti

Il titolare del trattamento deve agevolare l'esercizio, da parte dell'interessato, dei diritti secondo il Codice, semplificando le modalità e riducendo i tempi per il riscontro al richiedente. Già nella fase di progettazione delle tecnologie, i produttori di sistemi RFID dovrebbero opportunamente predisporre modalità idonee a garantire agli interessati un agevole esercizio dei diritti.

Disattivazione o rimozione delle etichette

agevole, la rimozione o la disattivazione delle etichette RFID al momento dell'acquisto del prodotto su cui è apposta l'etichetta o al termine dell'utilizzo del dispositivo.

Le etichette devono essere posizionate in modo tale da risultare, per quanto possibile, facilmente asportabili senza danneggiare o limitare la funzionalità del prodotto o dell'oggetto a cui si riferiscono (ad esempio, disponendone la collocazione sulla sola confezione).

Impianto sottocutaneo di microchip

L'impianto sottocutaneo di microchip in esseri umani solleva problematiche, particolarmente delicate, che hanno già indotto altre autorità garanti in Europa a considerarlo inaccettabile sul piano della protezione dei dati. Anche nei casi in cui un limitato impiego di microprocessori sottocutanei è stato permesso (ad es., negli Stati Uniti: Food and Drug Administration, 12 ottobre 2004), sono stati comunque messi in evidenza i potenziali rischi di tali operazioni, sia per la salute dei soggetti, che si sottopongono all'impianto, sia per la sicurezza dei dati personali trattati. Gli impianti sottocutanei di microchip devono ritenersi in via di principio esclusi, in quanto contrastanti, con riferimento alla protezione dei dati, con il principio di dignità, ferme restando le altre norme dell'ordinamento a garanzia dell'integrità fisica e dell'inviolabilità della dignità della persona, contenute anche nella Carta dei diritti fondamentali dell'Unione europea. Fatte salve le previsioni della normativa sulla protezione dei dati e le prescrizioni del presente provvedimento, l'impiego di microchip sottocutaneo può essere quindi ammesso solo in casi eccezionali, per comprovate e giustificate esigenze a tutela della salute delle persone, in stretta aderenza al principio di proporzionalità, e nel rigoroso rispetto della dignità dell'interessato. L'interessato dovrebbe poter essere in grado di ottenere di regola, in qualunque momento e senza oneri, la rimozione del microchip e l'interruzione del relativo trattamento dei dati che lo riguardano. I titolari del trattamento devono inoltre predisporre modalità di impianto e di impiego delle etichette sottocutanee tali da garantire la riservatezza circa la presenza delle stesse etichette nel corpo dell'interessato. I trattamenti di dati sensibili, oltre che effettuati nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, devono essere, ove prescritto, preventivamente autorizzati dal Garante. Il Garante si riserva di prescrivere ai titolari del trattamento, ai sensi dell'art. 17 del Codice, di sottoporre alla verifica preliminare di questa Autorità (anche con eventuali provvedimenti di carattere

generale) i sistemi di RFID destinati all'impianto sottocutaneo che, in quanto tali, presentano rischi specifici per i diritti, le libertà fondamentali e la dignità degli interessati.

3.2.2 La Commissione Europea a proposito di RFID

IL Tema RFID è stato discusso anche nella Commissione delle comunità Europee di Bruxelles [ComEu2007], che ha condotto una consultazione pubblica nel 2006 i cui risultati sono stati sono stati riportati nel documento a cui facciamo riferimento.

Nonostante la tecnologia RFID fosse pronta sotto il profilo tecnologico e commerciale, è sorta la necessità di istituire un quadro giuridico e politico chiaro e stabile per convincere gli utilizzatori ad accettare questa nuova tecnologia. In tale quadro si sono affrontare le seguenti questioni:

- Le conseguenze etiche.
- La necessità di proteggere la vita privata e la sicurezza.
- La gestione delle basi dei dati d'identificazione RFID.
- La disponibilità dello spettro radio
- L'elaborazione di norme internazionali armonizzate.
- Le preoccupazioni per le conseguenze sanitarie e ambientali.

Per affrontare tali sfide la Commissione ha avviato un'ampia consultazione pubblica, nell'ambito della quale sono stati condotti cinque seminari tematici specialistici e una consultazione in linea, svoltasi nel periodo luglio-settembre 2006, alla quale hanno contribuito 2190 partecipanti. La fase di consultazione si è conclusa in ottobre con un seminario aperto nel corso del quale sono stati presentati i primi risultati della consultazione.

Nel corso del dibattito pubblico sulla tecnologia RFID sono emerse gravi preoccupazioni in merito alla possibilità che essa possa mettere in pericolo la riservatezza della vita privata, si è evidenziata l'inquietudine dei cittadini, i quali vedono la tecnologia RFID come potenzialmente "invadente" ed esprimono la necessità di prevedere misure adeguate di tutela della vita privata.

Sono emersi timori sul possibile inasprimento della sorveglianza, in particolare sul luogo di lavoro, paventando forme di discriminazione, di esclusione e licenziamenti

È apparso evidente che l'attuazione di sistemi RFID deve essere accettabile dal punto di vista sociale e politico, ammissibile dal punto di vista etico e permessa da quello giuridico.

Questa tecnologia potrà assicurare la realizzazione dei numerosi vantaggi economici e sociali che promette, solo se saranno messe in atto garanzie efficaci per la protezione dei dati, la tutela della vita privata e gli aspetti etici collegati, i quali sono alla base del dibattito sull'accettazione della tecnologia RFID da parte dei cittadini.

L'unione Europea sta tutt'ora mostrando enorme interesse verso la tecnologia RFID e la sua applicazione nell'Internet of Things.
Nel 2010 viene redatto un testo [ComEu2010] che ha come oggetto "Internet of things", dove vengono ribaditi alcuni punti emersi nel precedente dibattito:

- La diffusione dell'internet degli oggetti consentirà una migliore interazione tra persone e oggetti e tra gli oggetti stessi, che può tradursi in vantaggi enormi per i cittadini dell'UE, a patto che siano rispettate la sicurezza, la protezione dei dati e la vita privata.
- È necessario condividere l'attenzione alla protezione dei dati personali e della vita privata nonché alla "governance" dell'internet degli oggetti, in quanto è possibile conquistare una più ampia accettazione sociale soltanto col rispetto della vita privata e la protezione dei dati personali, accompagnati dall'apertura e dall'interoperabilità;
- Chiede di incoraggiare tutte le parti interessate, europee e internazionali, ad affrontare le minacce correlate alla ciber-sicurezza, di spronare gli Stati membri ad attuare tutte le disposizioni internazionali esistenti in materia, compresa la Convenzione del Consiglio d'Europa sulla ciber-criminalità;
- Negli standard di prossima pubblicazione dovrebbero essere prese in considerazione le questioni relative alla sicurezza e alla vita privata, detti standard dovranno definire diverse caratteristiche di sicurezza volte a garantire la riservatezza, l'integrità o la disponibilità dei servizi;
- Se il ricorso ai chip RFID può essere efficace nella lotta alla contraffazione, nel prevenire le sottrazioni di neonati dai reparti maternità, nell'identificazione degli animali, ecc., esso può anche rivelarsi pericoloso e sollevare problemi di etica per i cittadini e la società, in relazione ai quali si dovranno trovare le necessarie salvaguardie;
- La tecnologia RFID e altre tecnologie correlate all'internet degli oggetti per l'etichettatura intelligente dei prodotti e dei beni di consumo e per i sistemi di

comunicazione tra gli oggetti e le persone possono essere utilizzate ovunque e sono in pratica invisibili e silenziose, si chiede, di conseguenza, che la suddetta tecnologia sia l'oggetto di ulteriori e più approfondite valutazioni da parte della Commissione europea, concernenti in particolare:

- l'impatto ambientale dei chip e del loro riciclaggio;
- la vita privata e la fiducia degli utenti;
- i maggiori rischi in tema di ciber-sicurezza;
- la presenza di chip intelligenti in un determinato prodotto;
- il diritto al silenzio dei chip, che garantisce l'autonomia e il controllo da parte dell'utente;
- le garanzie per i cittadini riguardo alla protezione durante la raccolta e l'elaborazione dei dati personali;
- lo sviluppo di una struttura e di un'infrastruttura di rete aggiuntive per le applicazioni dell'internet degli oggetti e l'hardware;
- la garanzia della miglior protezione possibile dei cittadini e delle aziende dell'UE da tutti i tipi di attacchi informatici online;
- l'impatto dei campi elettromagnetici sugli animali, in particolare gli uccelli presenti nelle città;
- l'armonizzazione degli standard regionali;
- lo sviluppo di standard tecnologici aperti e l'interoperabilità tra diversi sistemi; e sia oggetto, se del caso, di una regolamentazione specifica a livello europeo;

Nel 2015 viene costituito l'AIOTI, che sarà il principale organo di consultazione della Commissione Europea nella preparazione delle future politiche di ricerca, innovazione e standardizzazione nell'Internet of Things Innovation.

L'Europa punterà molto sull'Internet of Things, mettendo a disposizione bandi di finanziamento dedicati nel 2016 e nel 2017.
Il ruolo dell'AIOTI è stato essenziale nella progettazione dei futuri Pilot su larga scala, che

saranno oggetto di finanziamento in Horizon 2020, programma di finanziamento per la ricerca e l'innovazione.

Le tematiche relative all'Iot per cui la Commissione ha lanciato i bandi sono:
- Pilot 1: Ambienti di vita intelligenti per l’invecchiamento sano
- Pilot 2: Agricoltura intelligente e Sicurezza alimentare
- Pilot 3: Tecnologie indossabili per ecosistemi intelligenti
- Pilot 4: Zone di riferimento nelle città europee
- Pilot 5: Veicoli autonomi in ambienti connessi

Hanno ricevuto finanziamenti anche dodici progetti di ricerca presentati dall'Ateneo Pisano, tra cui quello proposto dal professor Giuliano Manara, del dipartimento di Ingegneria dell'Informazione, intitolato "EMERGENT. Chipless multisensor Rfid for green networks", che si occuperà di sensori innovativi basati su Tag Rfid a basso impatto ambientale

Capitolo 4 Protocolli di Autenticazione

Con l'introduzione su larga scala di sistemi RFID, sono sorti problemi di sicurezza e privacy [Jants2006], [Leht2006]. Tra questi la possibilità di tracciare dei tag senza che il proprietario ne sia consapevole, oppure la capacità di clonare i tag per creare delle contraffazioni. L'autenticazione permette ad una parte (verifier) di certificare l'identita della controparte (prover o cleimant).

In un sistema RFID, la possibilità di autenticare reader e tag ricopre un ruolo fondamentale garantendo sicurezza e privacy, la sola identificazione non e sufficiente a garantire che l'identità acquisita corrisponda a quella legittima.

Le tecniche di autenticazione, qualora non eliminassero la contraffazione, ne aumenterebbero le difficoltà rendendola meno conveniente economicamente.

Sono richiesti protocolli che soddisfino i requisiti di sicurezza dei sistemi RFID rispettando le loro restrizioni, come la limitata capacità delle batterie o la necessità di costruire dei tag a basso costo, che non permetterebbero l'implementazione di molte delle primitive crittografie.

Un protocollo di autenticazione è un processo real-time, che garantisce che la parte autenticata sia operativa nel momento dell'esecuzione del protocollo. Le tecniche di autenticazione si basano su qualcosa di conosciuto dall'entità che viene interrogata, come una password o una chiave segreta.

Gli schemi convenzionali con la password fissa sono vulnerabili al replay-attack, quando chi attacca registra la password trasmessa su un canale, la può replicare in un altro momento ed accedere al sistema, per questo motivo questi schemi di autorizzazione viene detto *weak-authorization.*

Il protocollo maggiormente diffuso e il *challenge-response [Men2006], [Rana2006]*, l'idea del protocollo (Fig.24) è che una entità (claimant o prover) da prova della sua identità ad un'altra entità (verifier), dimostrando la conoscenza di un segreto, notoriamente associato a quella entità (claimant).

La response viene generata a fronte di una challenge che varia nel tempo e dipende sia dal segreto dell'entità che dal challenge. La challenge è tipicamente un numero random e segreto chiamato nonce. L'uso del nonce previene il replay-attack perché se la response viene intercettata durante una esecuzione dell'autenticazione, non dovrebbe fornire all' intruso informazioni utili per una successiva autenticazione, in quanto le challenge successive differiscono l'una dall'altra. Per questo il protocollo challenge-response viene chiamato *strong-authentication*

1. Reader choses a challenge, x, which is a random number and transmits it to the reader.
2. The label computes $y = e_K(x)$ and transmits the value y to the reader (here e is the encryption rule that is publicly known and k is a secret key know only to the reader and the particular label).
3. The reader then computes $y' = e_K(x)$.
4. Then the reader verifies that $y' = y$.

Figura 24 Challenge-response protocol

4.1 Protocolli Hash Based

4.1.1 Funzione Hash

Una funzione hash [Men2006], [Jants2006] è una funzione computazionalmente efficiente, che ha come input stringhe binarie di lunghezza arbitraria e come output stringhe binarie di lunghezza fissa chiamate valori hash, questa è una definizione basilare, perché per essere usata in crittografia sono necessarie altre caratteristiche:

1. Deve essere una *one-way function*: per ogni elemento $x \in X$ è computazionalmente facile calcolare $f(x)$, ma per la maggior parte degli elementi $y \in Y$ è computazionalmente difficile determinare un x tale che $f(x) = y$.
2. Le buone funzioni hash dovrebbero essere *collision resistance*, teoricamente significa che non ci dovrebbero essere due messaggi m_1 e m_2 tali che $h(m_1) = h(m_2)$, ma dal momento che c'è un numero infinito di input ma un numero finito di output, le collisioni sono inevitabili. In pratica però, collision resistance significa che è computazionalmente molto improbabile trovare collisioni.
3. Una funzione hash dovrebbe essere random e quindi dovrebbe essere computazionalmente difficile distinguere tra una funzione hash e una funzione

random.

Anche se difficile da invertire una funzione one-way hash non necessariamente protegge le informazioni, per esempio: supponiamo di avere una funzione one-way hash h', poi definiamo una seconda funzione hash $h(x||y) == h'(x)||y$.

L'output di h è difficile da invertire perché è difficile invertire h', la cui seconda parte però è una informazione non protetta. Vedremo nel paragrafo 4.1.3 che il tag trasmette una coppia $(r, hash(tagID||r))$, se la funzione h fosse definita come sopra si avrebbe $(r, hash(tagID)||r)$ e quindi ci sarebbero informazioni non protette. Nonostante queste incertezze le funzioni hash in pratica proteggono le informazioni in maniera sufficiente.

4.1.2 Protocollo Hash Lock

Bisogna considerare che i tag passivi RFID non hanno le risorse computazionali per implementare le tradizionali operazioni crittografiche di controllo di accesso, gli *hash lock* [WEI2003] sono semplici meccanismi di controllo di accesso basati su funzioni one-way hash adatti alle risorse dei tag passivi. Assumiamo che i tag reader abbiano una connessione sicura con il back-end database, ll reader-to-tag, o forward channel, può trasmettere con un segnale forte abbastanza da arrivare anche a 100m ed essere intercettato da un eavesdropper fino a quella distanza. Il tag-to-reader o backward channel è relativamente più debole, la sua trasmissione può essere ricevuta dal reader e quindi anche da un eavesdropper solo nel corto raggio (circa 3m). Generalmente si assume che un eavesdropper può intercettare, senza essere scoperto, solo la trasmissione del forward channel , come mostrato dalla Fig. 25.

Figura 25 Forward vs. Backward Channels: Il reader può rilevare solo il tag che è nel backward range, ma non il tag in rosso. Un eavesdropper che è distante può intercettare il forward channel ma non le risposte del tag.

Ogni tag abilitato alla funzione hash ha una porzione della sua memoria riservata ad un temporaneo *metaID* e può operare in uno stato *locked* o *unlocked*. Per mettere un tag in lock, il proprietario del tag salva, come metaID del tag, la funzione hash di una random key :

$metaID = hash(key)$, per effettuare questa operazione è possibile utilizzare il canale RF o un canale fisico diretto per maggiore sicurezza.
Dopo il locking di un tag il proprietario salva sia la key che il metaID nel back-end database, sarà poi possibile l'accesso ai dati utilizzando il metaID come chiave. Quando il tag riceve un metaID entra nello stato di lock. Mentre è in lock il tag risponde a tutte le interrogazioni con il metaID soltanto e non offre nessun'altra funzionalità.
I passi della sequenza del protocollo sono descritti nella Fig.26.

1. Reader R seleziona a random *key* e calcola *metaID := hash(key)*
2. R scrive *metaID* su Tag T.
3. T entra in locked state.
4. R salva la coppia *(metaID,key)* nel backend database.

Figura 26 Protocolli di locking a hash lock.

Un unlocked tag offre la sua completa funzionalità ad ogni reader nel suo raggio di azione.
Per mettere un tag nello stato di unlock, il proprietario ottiene il metaID interrogando il tag e poi usa questo valore come chiave per recuperare la key dal backend database. Il proprietario trasmette la key al tag, il quale calcola una funzione hash e la paragona con il metaID memorizzato, se sono uguali il tag si mette in stato di unlock accettando le interrogazioni da parte dei reader. L'unlocking di un tag corrisponde ad una autenticazione. Lo stato di unlock dovrebbe durare solo il tempo necessario per eseguire una funzione e ritornare subito nello stato di lock, questo per prevenire accessi indesiderati al tag. Il protocollo è descritto nella Fig.27.

1. Reader R interroga Tag T per il suo *metaID*
2. R looks up *(metaID,key)* dal backend database.
3. R manda *key* a T.
4. If *(hash(key) == metaID)* , T unlocks se stesso.

Figura 27 Protocollo di unlocking a hash lock.

Questo protocollo previene l'accesso al tag da parte di reader non autorizzati perché è difficile invertire una funzione one-way hash. Tentativi di spoofing possono essere rilevati ma non prevenuti. Un aggressore potrebbe interrogare un tag per ottenere il suo metaID,

tramite un replay attack, gli sarebbe possibile autenticarsi al reader impersonando il tag leggittimo. Il reader ha la possibilità di verificare la correttezza dei dati contenuti nel tag (come l'identificatore) con quelli nel backend database, se non tutto è corretto, viene lanciato un alert che indica un attacco in corso. Dal momento che il *metaID* viene usato come identificatore ci potrebbe essere un pericolo per la privacy, rendendo tracciabili gli individui.

4.1.3 Protocollo Random Hash lock

È stato sviluppato un nuovo metodo per cui un tag quando è interrogato non risponde in maniera prevedibile a reader non autorizzati, ma allo stesso tempo il tag sia identificabile da un reader legittimo. Nel nuovo metodo oltre alla one-way function viene usato anche un generatore di numeri random. Un tag può essere locked con una semplice istruzione del reader, nessun protocollo è necessario. Per mettere un tag in stato unlocked un reader manda una semplice interrogazione, i tag rispondono a questa interrogazione generando un nonce random r, poi il tag usa una funzione hash del nonce concatenato con il tagID, in fine risponde al reader con la coppia $(r, hash(tagID||r))$.

Quando il reader legittimo riceve la coppia $(r, hash(tagID||r))$, esegue una ricerca esaustiva di tutti i tagID conosciuti. I tagID vengono usati per calcolare la funzione $hash(tagID||r)$ fino a quando non si trova lo stesso valore ricevuto dal tag, a quel punto il tagID è individuato. Si assume quindi, che il reader deve sin dall'inizio conoscere tutti i tag disponibili. Il reader può mettere il tag in stato di unlock trasmettendo il tagID individuato, oppure lasciare il tag in lock se lo scopo era solo quello di autenticare il tagID

1. Reader R interroga il Tag T.
2. T genera un nonce random *r* e calcola *hash(tagID||r)*.
3. T trasmette *(r,hash(tagID||r))* al reader R.
4. R calcola $hash(tagID_i || r)$ per tutti i $tagID_i$ conosciuti.
5. Quando R trova che $hash(tagID_j ||r) == hash(tagID || r)$, R trasmette $tagID_j$ a T.
6. T unlocks se stesso se riceve $tagID_j == tagID$.

Figura 28 Protocollo random hash unlock

Questo schema non è pratico per un gran numero di tag, che richiedono molte letture al secondo e quindi molte ricerche esaustive del database. L'autenticazione è proporzionale al numero di tag e non è efficiente, la sua complessità è O(N). Anche se questo schema può

essere sufficiente in pratica non è teoricamente robusto. La definizione della funzione one-way stabilisce solo la difficolta di invertire l'output della funzione, non prevede nulla sulla segretezza, è quindi possibile che alcuni dati siano rivelati

4.2 Protocollo Tree Based

In un protocollo di autenticazione *tree-based* [Dimi2006], partiamo con un albero le cui foglie contengono tutti i possibili indentificatori dei tag $t_1, t_2, \dots, t_n$. Gli archi dell'albero contengono secret keys create durante il setup del sistema. Ogni tag t_i parte già con le keys corrispondenti al cammino dalla radice alla fogliat_i. Se d è la lunghezza di questo cammino, k_i^1,k_i^2,….,k_i^d rappresentano le secret keys lungo il cammino fino a t_i, allora il protocollo per interagire con i reader è mostrato in Fig.29.

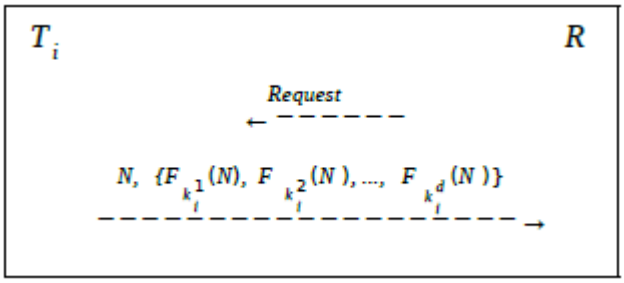

Figura 29 Protocollo di autenticazione

Il tag, quando interrogato, genera un numero random N (nonce) e calcola $\{F_{k_i^1}(N),F_{k_i^2}(N),\dots,F_{k_i^d}(N)\}$ dove $F_K(r)$ è il risultato di una funzione pseudo-random F con una chiave k e input r. In pratica un tag sceglie un numero random e calcola i valori $F_{k_i^j}(N)$ per tutte le secret key a partire dal nodo radice fino a t_i. Con l'aiuto del backend database possiamo autenticare un tag usando un algoritmo del tipo tree walking. Il backend database ha memorizzato i valori $N, \{f^1, f^2, \dots, f^d\}$ dove ogni $f^j = F_{k_i^j}(N)$ e dal momento che conosce anche le secret keys di tutti i nodi, può calcolare il cammino che porta al tag t_i seguendo la seguente procedura:

1. Considerate le chiavi k_l^1 e k_r^1 che sono associate agli archi che partono dalla radice. Così k_l^1e k_r^1 sono le prime chiavi associate al sottoalbero di sinistra e di destra. Si calcola $F_{k_l^1}(N)$ e $F_{k_r^1}(N)$ che sono paragonate con il valore ricevuto f^1, se f^1 è uguale a $F_{k_l^1}(N)$il tag appartiene al sottoalbero di sinistra, altrimenti appartiene a quello destro.

2. Assumiamo di aver stabilito il cammino fino al nodo di livello j. Ora consideriamo le chiavi k_l^j e k_r^j associate agli archi che partono da quel nodo. Di nuovo si calcola $F()$ usando queste chiavi ed input N e poi paragonando il valore con f^j. A seconda del risultato si procede con il sottoalbero di sinistra o di destra.
3. Si ripete il passo 2 fino a quando non si raggiunge un nodo foglia (tag). Se ad ogni punto del processo il valore ricevuto f^jnon è uguale a nessuno dei due risultati, il processo si ferma e il tag è rifiutato.

Dovrebbe essere chiaro che un tag valido verrà riconosciuto in un tempo proporzionale alla profondità dell'albero e non dal numero dei nodi floglia (tag) e quindi il processo è efficiente, la sua complessità è O(log N), esamineremo ora i possibli attacchi a questo protocollo.

I tag in questo protocollo non trasmettono nessun codice fisso (sempre uguale), quindi l'eavesdropping non è un problema fino a quando F non rivela nessuna informazione sulle chiavi. Se la lunghezza delle chiavi è scelta bene nessun brute force attack può essere rivolto alle chiavi.

Il protocollo fin qui descritto risulta vulnerabile ad attacchi di tipo Cloning o Spoofing, questa problematica viene risolta con la seguente evoluzione del protocollo (Fig. 30).

Un reader sceglie un nonce N_Re lo trasmette insieme ad una richiesta di lettura. Il tag genera il proprio nonce N_Te valuta la funzione pseudo-random con input $r = N_T \parallel N_R$usando le chiavi del cammino k_i^j. Chiaramente l'attacco precedente non funziona più perchè il reader specifica un nonce N_Re un aggressore non ha il controllo sulla scelta di N_R, per questo motivo una replica del messaggio verrebbe intercettata e rifiutata dal reader legittimo.

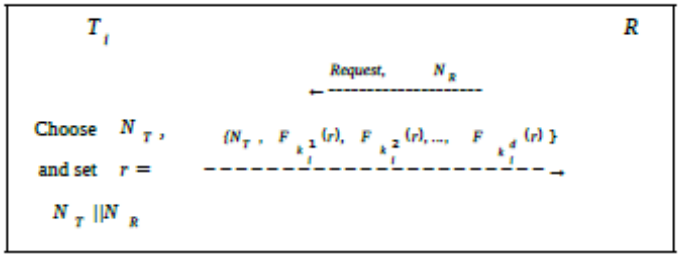

Figura 30 Versione migliorata del protocollo

Si potrebbe pensare che il tracking non sia possibile, dal momento che i tag rispondono con diversi nonce ogni volta e che il valore della funzione F non è prevedibile. Però i tag condividono le secret keys, quindi se un tag è compromesso può rivelare informazioni sugli

altri tag, vedi Fig.31.

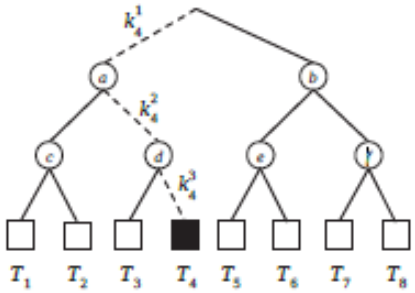

Figura 31 Un tag (T_4) compromesso

Ci sono 8 tag come nodi foglia, il cammino tratteggiato corrisponde alla sequenza delle secret keys che portano all'identificatore del tag T_4 e che sono memorizzate nel tag stesso. Si vede che la chiave k_4^1 è in comune ai tag T_1,T_2,T_3e T_4, la chiave k_4^2è in comune a T_3e T_4e solo la chiave k_4^3 appartiene a T_4. Supponiamo ora che T_4 sia compromesso in modo tale che l'aggressore possa accedere alle secret keys memorizzate nel tag. Vediamo quali problemi questo può comportare, guardando alla figura precedente ci rendiamo conto che solo i tag che condividono lo stesso cammino sono in pericolo di rivelare delle informazioni. Dal momento che ogni tag ha almeno la chiave dell'ultimo livello diversa dalle altre, vediamo che la privacy è assicurata, perché nessun aggressore può prevedere il valore di F con quella chiave e impersonificare il tag con il reader. Per ridurre la possibilità di attacchi che possano compromettere i tag [Lu2007] ha proposto un protocollo che aggiunge alla autenticazione tree-based un dynamic key-updating con il quale le chiavi condivise dell'albero sono periodicamente aggiornate.

4.3 Protocollo Group Based

Nei protocolli di autenticazione *group-based* [Saka2013], [Avoin2007], [Hoqu2011] i tag sono divisi in gruppi disgiunti, un reader assegna due chiavi ad ogni tag, una chiave unica sk ed una chiave di gruppo gk. La risposta del tag consiste di due componenti criptati da gk e sk. Un reader prima prova tutte le chiavi di gruppo per decodificare il primo componente che contiene il group ID al quale il tag appartiene. Dopo il reader applica le chiavi uniche associate con il gruppo, per decodificare il secondo componente in modo tale da verificare l'autenticità del tag. Nell'autenticazione group-based se alcuni tag sono compromessi i tag negli altri gruppi sono intatti. In Fig.32 i tag sono divisi in 4 gruppi contenenti ciascuno 2 tag, se il tag 3, che ha come chiavi sk3 a gk2 è compromesso, anche l'identità del tag 4 con

chiave sk4 è compromessa, gli altri tag rimangono comunque indistinguibili. Con questo protocollo l'efficienza dell'autenticazione è bassa.

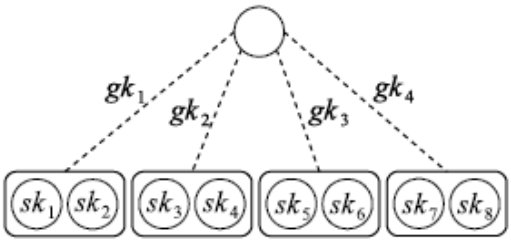

Figura 32 Protocollo group-based

4.4 Protocollo Skip-Lists Based

Le *Skip list* [Pugh1990], [Saka2013] sono strutture dati probabilistiche formate da una gerarchia di liste concatenate di sottosequenze di elementi (Fig.33). Queste liste addizionali permettono di percorrere la lista con efficienza, paragonabile a quella di un albero bilanciato. Al livello più basso (livello 2) la lista contiene tutti i nodi ordinati in ordine crescente delle loro chiavi. Un nodo nella lista ad un livello i > 0 compare nel livello i-1 con probabilità p. Il numero medio di liste in skip list è $\log_{1/p}N$ dove N è il numero di elementi dell'input. Le operazioni di search, insert e delete sono eseguite in $O(\log_{1/p}N)$ dal momento che il numero di passi in ogni lista concatenata è in media $1/p$. Teoricamente le skip lists dovrebbero essere un'alternativa agli alberi bilanciati.

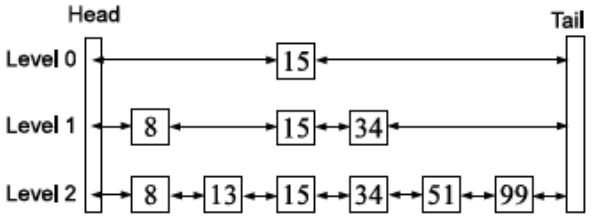

Figura 33 Skip list

Per esempio nella figura precedente per trovare la chiave 13 si parte dalla lista al livello più alto. La lista al livello 0 ha solo un nodo quello con chiave 15, dal momento che 13 < 15 passiamo con la ricerca al livello 1 sulla sinistra. Al livello 1 troviamo il nodo con chiave 8 che è minore di 13, perciò passiamo al livello 2 verso la parte destra. Al livello 2 troviamo il nodo con chiave 13.

Il protocollo di autenticazione basato sulle *Randomized Skip-Lists* (RLSA) è stato proposto da [Saka2013] e consiste di quattro componenti:

1. Key issuing (inizializzazione).
2. Private authentication.
3. Key-updating.
4. System maintenance.

Durante la fase *key issuing* il sistema genera le skip list, i tag sono casualmente assegnati ai nodi del livello più basso. Una chiave unica ed un insieme di chiavi di gruppo sono assegnate ad ogni tag partendo da un nodo nella lista in fondo fino alla lista al livello più alto. Durante l'autenticazione un reader legge le chiavi di gruppo per ridurre lo spazio della ricerca della corrispondente chiave unica del tag, partendo dalla lista al top fino a quella in fondo. Il meccanismo di *key-updating*, che aggiorna le chiavi dei tag e delle skip list, rende RSLA meno vulnerabile.

Il *system maintenance* si occupa della registrazione dei tag e la loro rimozione. L'idea chiave di RSLA è lo spostamento casuale in una lista ad ogni livello e le dipendenze tra le liste. Questo rende lo schema basato sulle skip lists più sicuro delle soluzioni esistenti, mantenendo allo stesso tempo la performance dei protocolli tree-based.

4.4.1 Costruzione delle Skip List

Prendiamo in considerazione un sistema RFID con N tag ed un reader connesso con un canale sicuro ad un back-end server e vediamo come si costruiscono le skip list [Saka2013]. Indichiamo con L_i la lista del livello i e con v_i un nodo i, un nodo ha puntatori ai nodi sulla sinistra e sulla destra nella stessa lista che indichiamo con $v_i.sin e$ con $v_i.des$. Il puntatore alla sinistra del primo nodo e il puntatore alla destra dell'ultimo nodo sono null, inoltre i puntatori ai primi e agli ultimi nodi delle liste L_i sono memorizzati in $L_i.head$ e $L_i.tail$. Generiamo skip list che contengono $\eta + 1$ liste, dove l'altezza delle skip list $\eta = \lceil \log_k N \rceil$ ed N il numero di tag, ogni lista L_i contiene 2^i nodi. Possiamo quindi assegnare tutti i tag ai nodi del livello più basso, se ci sono più nodi che tag qualche nodo non sarà associato ad un tag. Dato il numero di tag N e k=2, viene creata una lista L_η con k^η nodi. Il nodo v_i viene aggiunto alla lista $L_{\eta-1}$ se $i \bmod k = 0$. Per ogni livello j $(0 \leqslant j \leqslant \eta - 1)$, un nodo v_i è aggiunto alla lista L_j se $i \bmod k^{\eta-j}=0$, questo processo è ripetuto da η a 0. La lista al livello più alto ha sempre un nodo cioè $L_0 = \{v_0\}$, dal momento che il numero di nodi nella lista al

livello più basso è k^{η}. Ogni nodo nella skip lists ha un insieme di chiavi. Definiamo $v_i.key[j]$ come la variabile per memorizzare la chiave dei nodi v_i per il livello j. Se v_i non compare in L_j, $v_i.key[j]$ è vuota. Assumiamo che il tag t sia assegnato a v_i, la chiave unica sk_t del tag t è memorizzata in $v_i.key[\eta]$. Denotiamo con $gk_{i,j}$ la chiave di gruppo memorizzata in $v_i.key[j]$, se v_i compare in L_j tutti i nodi in skip lists hanno una chiave unica in $v_i.key[\eta]$ e chiavi di gruppo per il livello j ($1 \leq j \leq \eta - 1$) in $v_i.key[j]$. Non assegniamo nessuna chiave al nodo nella lista al livello più alto L_0 dal momento che L_0 ha solo un nodo, così $v_0.key[0]$ è vuota. Le skip lists sono strutture dati semplici che possono essere usate al posto degli alberi bilanciati. Gli algoritmi skip list sono facili da implementare, da modificare e da estendere, inoltre sono veloci come gli algoritmi ottimizzati dei balanced tree. Con l'uso delle skip list, a differenza degli alberi bilanciati, il link tra i nodi allo stesso livello, può essere utilizzato per rotazioni random senza dover cambiare la struttura dati.

Elencheremo ora quali sono gli aspetti negativi delle skip list:

- Ogni operazione o sequenze di operazioni nelle skip lists possono richiedere un tempo maggiore di quello atteso, anche se la probabilità che possa essere significativamente maggiore è trascurabile.
- Le skip lists richiedono più spazio dei balanced tree perchè richiedono più puntatori per nodo.
- Ci sono molte più implementazioni ottimizzate per i balanced tree che per le skip list.

4.4.2 Key Issuing

In RSLA il tag *t* ha tre variabili: la chiave unica sk_t, un insieme di chiavi di gruppo GK_t ed un insieme di numeri random R_t. Nel processo key issuing ogni tag *t* è assegnato in maniera casuale ad un nodo $v_i$nella lista di più basso livello L_η. Partendo da v_i il *key issuer* attraversa le liste fino alla lista al top L_0 spostandosi sulla sinistra di $r_j$nodi ad ogni L_j($1 \leq j \leq \eta - 1$), dove r_j è casualmente scelto tra 0 e $|L_j|$-1 (ad esempio 2^j-1). Così facendo la chiave del nodo selezionato per ogni livello è assegnata a un tag.

L'algoritmo in pseudo codice è descritto nella Fig 34.

Algorithm 1 Key Issue

```
1: /* Key Issuer does following */
2: Issuer locates all tags t to node v_i
3: /* For each tag i Key Issuer does following */
4: for for each tag t in the system do
5:     KeyIssue(i, v_i)
6: end for
7: /* The function to assign keys to Tag t */
8: KeyIssue(t, v_i)
9: /* v_i is the current node */
10: R_t = φ /* Initialize the random numbers list */
11: GK_t = φ /* Initialize the grop keys list */
12: / * At the lowest level list L_η */
13: sk_t ← v_i.key[η]
14: v_i ← v_m where m = i − (i mod k)
15: for (j from η − 1 to 1) do
16:     /* Random shifting by r and add a group key */
17:     r ←(uniform)— [0, |L_j| − 1]
18:     Add r to R_t
19:     v_i ← shift to the left by r
20:     Add v.key[j] to GK_t
21:     /* Move to upper level */
22:     v_i ← v_m where m = i − (i mod k^(η−j+1))
23:     j = j − 1
24: end for
```

Figura 34 Algoritmo Key Issuing

Vediamo un esempio dell'algoritmo key issuing:

Consideriamo un sistema RFID con 8 tag che usa skip lists con k=2 e η=3 per le assegnazioni delle chiavi, come mostrato in Fig.35, i tag sono assegnati ai nodi in L_3.

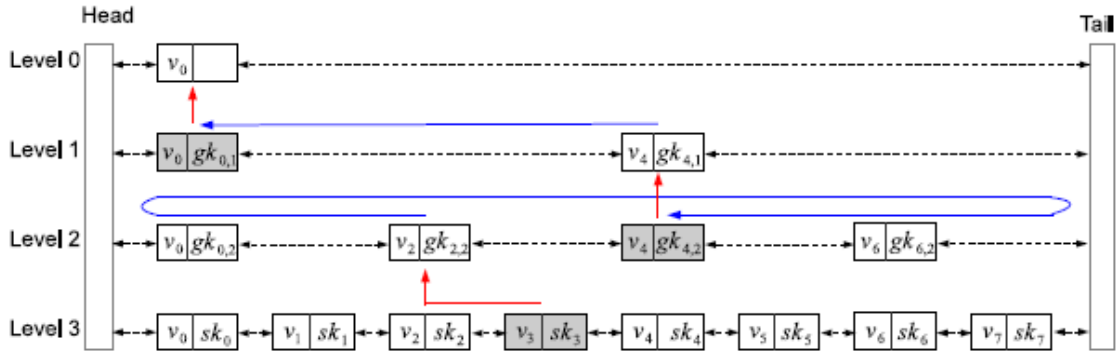

Figura 35 Esempio di key issuing.

Vediamo ora come il key issuer assegna le chiavi di gruppo e numeri random ad un tag, per esempio tag 3. Partendo da v_3 il key issuer attraversa la skip list fino alla lista al top. Per prima cosa il tag 3 recupera sk_3 memorizzato in $v_3.key[3]$ e il puntatore si sposta al livello 2 attraverso v_2. Poichè v_3 non compare in L_2, il puntatore punta a v_2 $((3-3\ mod\ k)=2)$ e

dopo si sposta al livello 2. Il key issuer casualmente seleziona $r_2 = 3$ ed il puntatore si sposta a sinistra di 3, nello stesso tempo 3 viene sommato a R_3. Il puntatore punta ora a v_4 in L_2. Il key issuer assegna $gk_{4,2}$ memorizzata in $v_4.key[2]$ al tag 3. Questo processo continua fino a quando il key issuer non raggiunge L_0. Supponiamo che il tag 3 selezioni r_1= 1 al livello L_1, esso ottiene sk_3, GK_3=$\{gk_{0,1}, gk_{4,2}\}$ e R_3=$\{1,3\}$.

4.4.3 Autenticazione

Dopo aver generato le chiavi il reader può comunicare in modo sicuro con i tag, in questo protocollo di autenticazione il reader invia un'interrogazione con un nonce n_r, il tag crea una risposta con nonce n_t che poi viene decodificata dal reader.

Lo pseudo codice dell'algoritmo che crea la risposta del tag è descritto in Fig.36.

Algorithm 2 ReplyToReader(n_r)

1: /* Assume Tag t has sk_t, GK_t, and R_t */
2: /* where $GK_t = \{gk_1, gk_2, ..., gk_{\eta-1}\}$ */
3: /* and $R_t = \{r_1, r_2, ..., r_{\eta-1}\}$ */
4: Generate nonce n_t
5: **for** i from 1 to $\eta - 1$ **do**
6: $\beta_i.hash \leftarrow H(gk_i||r_{i-1}||n_t||n_r)$ /* r_0 = empty */
7: $\beta_i.num \leftarrow E(gk_i, r_i)$
8: Add β_i to β
9: **end for**
10: $\beta_\eta.hash = H(sk_t||r_{\eta-1}||n_t||n_r)$
11: reply n_t and β

Figura 36 Risposta del tag al reader

Assumiamo che il sistema abbia un tag t con chiave unica sk_t, un insieme di chiavi di gruppo $GK_t = \{gk_1, gk_2, \ldots, gk_{\eta-1}\}$ ed un set di numeri random $R_t = \{r_1, r_2, \ldots, r_{\eta-1}\}$. Indichiamo con $\beta = \{\beta_1, \beta_2, \ldots, \beta_\eta\}$ β la risposta del tag dopo l'interrogazione del reader, dove β_i $(0 \leq i \leq \eta)$ consiste nel valore hash $\beta_i.hash$ ed un numero $\beta_i.num$ criptato ad ogni livello i. Le righe da 5 a 9 dell'algoritmo di risposta del tag descrivono come β_i $(0 \leq i \leq \eta - 1)$ è calcolato dalle chiavi di gruppo. Il valore hash $\beta_i.hash$ è ottenuto con $H(gk_i \parallel r_{i-1} \parallel n_t \parallel n_r)$ con la base r_0=empty, cioè $\beta_1.hash=H(gk_1 \parallel n_t \parallel n_r)$ perché non c'è rotazione in L_0. Il motivo per cui includiamo il numero del livello precedente r_{i-1} in $\beta_i.hash$ è per rafforzare la dipendenza tra i livelli e tenere alta l'anonimità. L'anonimità può essere usata per misurare il grado di sicurezza [Diaz2002], è definita come una condizione in cui non si è identificati quando si è parte di un insieme anonimo, un insieme anonimo è un insieme di tutti i possibili tag le cui risposte non sono distinguibili. Un caso di poca

anonimità è quello dell'approccio tree-based nel caso in cui un tag è compromesso e quindi le risposte dei tag possono essere messe in correlazione usando le chiavi dei tag compromessi. Il numero random r_i è criptato con $E(gk_i, r_i)$ e assegnato a $\beta_i.num$. Per l'ultimo elemento β_η il valore hash $\beta_\eta.hash$ è definito da $H(sk_t \parallel r_{\eta-1} \parallel n_t \parallel n_r)$ dove la chiave unica è usata come descritto alla riga 10 dell'algoritmo *ReplayToReader* e $\beta_\eta.num$ è empty in fine il tag manda n_t e β al reader. È da notare che β contenga η elementi, uno di questi è calcolato usando sk, mentre gli altri η-1 elementi sono calcolati usando $gk_i(1 \leq i \leq \eta -1)$.

Quando il reader riceve la risposta del tag, esamina le chiavi di gruppo associate ai nodi, cominciando dalla lista al livello più alto come descritto nell'algoritmo in Fig. 37.

All'inizio il puntatore punta al nodo v_0 in L_0, in L_1 ci sono k nodi (k=2) ed uno di loro ha la chiave di gruppo $v_i.key[1]$ ($v_i \in L_{i)}$) che è uguale alla chiave di gruppo usata per $\beta_1.hash$. Dopo aver trovato la chiave corrispondente usata per $\beta_1.hash$, il reader decodifica $\beta_1.num$ con la chiave. Poi il puntatore si muove da L_0 a L_1 e si sposta sulla destra di $\beta_1.num$.

Se il puntatore raggiunge la *tail* durante lo spostamento, viene fatto puntare alla *head* della stessa lista. Da notare che l'autenticazione usa lo spostamento a sinistra se percorre la skip list partendo dal basso mentre usa lo spostamento a destra se parte dal top. Indichiamo con v_i il nodo corrente dopo lo spostamento a destra di r_1, la lista L_2 ha k^2 nodi, ma soltanto k nodi $v_j(1 \leq j \leq i + k)$ devono essere esaminati, questo perché uno dei k nodi ha la chiave di gruppo per β_2.

Questo processo continua fino a quando il reader non raggiunge il livello più basso (bottom), dato che la chiave al livello L_η per un tag è unica, il reader identifica il tag da β_η. Il reader non esamina più di k chiavi ad ogni livello $1 \leq i \leq \eta$, dal momento che la skip list usa il metodo di ricerca di un albero bilanciato, se durante l'autenticazione il reader non è capace di trovare una chiave di gruppo ad ogni livello, la risposta del tag non è valida ed il reader trasmette il messaggio FAIL.

Algorithm 3 Authentication(n_r, n_t, β)

```
1: /* β = {β_1, β_2, ..., β_η}*/
2: v_0 ← head /* the pointer to the current node */
3: for j from 1 to η do
4:    /* Scan v.key[j] for k nodes from v_i */
5:    for m from 1 to k do
6:       /* Note that the base r_0 = empty */
7:       if H(v_i.key[j]||r_{j-1}||n_r||n_t) = β_j.hash then
8:          if j == η then
9:             Identify Tag t by the unique key v_i.key[j]
10:         else
11:            r ← D(v_i.key[j], β_j.num)
12:            v_i ← shift to the right by r
13:            j ← j + 1
14:         end if
15:      end if
16:      m ← m + 1
17:   end for
18:   if The key is not found for L_j then
19:      return FAIL
20:   end if
21: end for
22: return t
```

Figura 37 Algoritmo di Autenticazione.

Dimostriamo ora con un esempio come funziona l'autenticazione di un tag da parte di un reader (Fig.38)

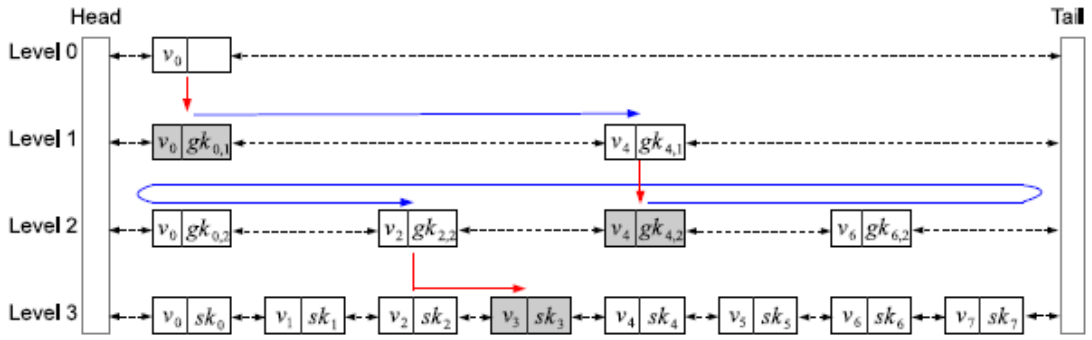

Figura 38 Esempio di autenticazione

Prendiamo in considerazione il tag 3 i cui parametri sono: sk_3, GK_3=$\{gk_{0,1}, gk_{4,2}\}$ e R = {1,3}, il messaggio di risposta β è il seguente:

$$\beta_1 = H(gk_{0,1}||n_t||n_r), E(gk_{0,1}, 1)$$

$$\beta_2 = H(gk_{4,2}||1||n_t||n_r), E(gk_{4,2}, 3)$$

$$\beta_3 = H(sk_3||3||n_t||n_r),\ empty$$

Il reader dopo aver ricevuto la risposta del tag n_t e β percorre la skip lists come mostrato

nella precedente figura. Per prima cosa il reader esamina $v_0.\text{key}[1]$ e $v_4.\text{key}[1]$ in L_1, cioè $gk_{0,1}$e $gk_{4,1}$, per paragonare il valore hash ottenuto con $\beta_1.\text{hash}$. Se la chiave $gk_{0,1}$funziona il reader applica $D(gk_{0,1}, \beta_1.\text{num})$ e ottiene r_1= 1, il reader si sposta a destra di 1, puntando su v_4.

Al livello 2 il reader esamina due nodi, dal momento che in questo esempio k=2, cioè $v_4.\text{key}[2]$ e $v_6.\text{key}[2]$, il reader convalida che $gk_{4,2}$ funziona per $\beta_2.\text{hash}$ e ottiene r_2= 3 da $\beta_2.\text{num}$. Questo processo continua fino a quando il reader non raggiunge la lista al livello più basso L_3.

Al livello 3 il reader esamina la chiave unica memorizzata a $v_2.\text{key}[3]$ e $v_3.\text{key}[3]$, il valore ottenuto dalla funzione hash con sk_3 si ottiene anche con $\beta_3.\text{hash}$, dato che v_3 corrisponde al tag 3, il reader conclude che la risposta arriva dal tag 3.

4.4.4 Key Update

I sistemi RFID sicuri dovrebbero periodicamente fare un update delle chiavi condivise per evitare gli effetti degli attacchi che sfruttano tag compromessi. Una soluzione pratica è aggiornare le chiavi di un tag dopo ogni autenticazione, cosicché un eventuale tag compromesso non possa fare uso delle chiavi ottenute per attaccare gli altri tag.

Nel protocollo RSLA, il reader prima aggiorna tutte le chiavi in tutte le skip list, poi aggiorna le informazioni sui tag durante il loro accesso. In altri, come [Lu2007] il reader prima aggiorna le chiavi del tag durante l'accesso e poi aggiorna le chiavi corrispondenti nell'albero.

4.4.5 System Maintenance

Nei sistemi RFID è naturale che alcuni tag vengano rimossi dal sistema o ne vengano aggiunti di nuovi. Il protocollo RSLA prevede delle funzioni di registrazione di nuovi tag e di rimozione dei tag non più necessari.

Conclusione

La sicurezza e la privacy sono tra i principali problemi che si devono affrontare con un sistema RFID. In questa tesi sono stati esaminati i sistemi che cercano di risolvere questi problemi, partendo da i più semplici ai più sofisticati, mettendone in risalto l'evoluzione.
Nel primo capitolo è stata esaminata la tecnologia impiegata per i tag e i reader, le potenzialità e le relative problematiche.
I sistemi RFID sono ormai usati ovunque ed hanno un impatto nella nostra vita quotidiana, essi sono uno dei building blocks dell'IoT (Internet of Things), che rappresenta uno dei paradigmi più importanti ed utilizza la conoscenza di differenti campi come le Telecomunicazioni, l'Informatica, l'Elettronica e le Scienze Sociali.
Nel secondo capitolo è stato trattato il processo dell'identificazione, durante il quale si presenta il problema della collisione: cioè diversi tag, che rispondono simultaneamente ad una interrogazione, possono collidere e interferire tra di loro. Il primo protocollo che ha affrontato questo problema è il protocollo "Aloha puro" seguito poi da altri protocolli Aloha più performanti come lo "Slotted Aloha", "Frame-Slotted Aloha", "Dynamic Frame-Slotted Aloha" fino ad arrivare al "Tree-Slotted Aloha" che, con una prestazione del 43%, è tra i protocolli più performanti.
La seconda parte del secondo capitolo tratta i protocolli tree based. Il protocollo Aloha (ad eccezione del TSA) non tenta di risolvere le collisioni nel momento che accadono, ma la rimanda nel tempo. Sono stati introdotti un tipo di algoritmi chiamati "Tree-Search algorithms" od anche "Collision Resolution Protocols" (CRP) che possono essere usati per la RFID arbitration e che cercano di risolvere le collisioni non appena si verificano. Questi protocolli sono gli Alberi Binari, Alberi binari dinamici e Query tree, questi ultimi hanno una prestazione del 37%.
Nel terzo capitolo sono stati descritti i vari tipi di attacco di cui sono oggetto i sistemi RFID e le contromisure che adottabili. Inoltre abbiamo trattato il problema della privacy e gli aspetti sociali dell'uso della tecnologia RFID. Determinati impieghi della RFID possono costituire una violazione del diritto alla protezione dei dati personali ed avere serie

ripercussioni sull'integrità e la dignità della persona.

Infine nel quarto capitolo è stato esaminato il problema dell'autenticazione, che è la tecnica che permette ad una parte (verifier) di certificare l'identità di un'altra parte (prover o claimant). L'autenticazione di reader e tag risolve molti dei problemi di sicurezza e privacy, i protocolli di autenticazione trattati sono gli "Hash Based", "Tree Based" e "Skip Lists Based". Quest'ultimi usano una struttura dati che potrebbe essere usata come un'alternativa agli alberi bilanciati.

Bibliografia

[Abra2002] Abraham C., V. Ahuja, A.K. Ghosh, P. Pakanati, Inventory Management using Passive RFID Tags: A Survey, Department of Computer Science, The University of Texas at Dallas, Richardson, Texas, pp. 1–16, October, 2002.

[Abr1970] Abramson N., “The ALOHA System - Another Alternative for Computer Communications,” pp. 281-285 in Proc. of the Fall Joint Computer Conference, (1970).

[Abr1977] Abramson N., “The Throughput of Packet Broadcasting Channels,” IEEE Trans. on Communications, **COM-25**(1) pp. 117-128 (January1977).

[Atzori2010] Atzori L. et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

[Avoin2007] Avoine G, L. Buttyan, T. Holczer, and I. Vajda, \Group-based Private Authentication," in Proceedings of the IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, 2007, pp. 1-6.

[Bagn2009] Bagnato G., Maselli G., Petrioli C., Vicari C., "Performance Analysis of Anti-Collision Protocols for RFID Systems", in Proceedings of the IEEE 69th Vehicular Technology Conference (VTC Spring 2009), 26-29 April 2009

[Bertse1992] Bertsekas, Dimitri and Gallager, Robert. Data Networks. Prentice-Hall, 1992

[Bonuc2006] Bonuccelli A.M. and Francesca Lonetti. Tree Slotted Aloha: a New Protocol for Tag Identification in RFID Networks. Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06).IEEE Computer Society

[Bonuc2007] Bonuccelli M.A., Francesca Lonetti , Francesca Martelli.Instant collision resolution for tag identification in RFID networks.Ad Hoc Networks 5 (2007) 1220–1232,Elsevier.

[Bonuc2015] Bonuccelli M.A., Francesca Martelli. Optimal Polling Protocol for Missing Tags Identification and Information Collection in RFID Systems 2015.

[Burd2004] Burdet Luc André. RFID Multiple Access Methods,Seminar "Smart

Environments" ETH Zürich, Summer semester 2004.

[Cape1979] Capetanakis I.J., “Tree Algorithm for Packet Broadcast Channels,” IEEE Trans. on Information Theory, **IT-25**(5) pp. 505-515 (September1979).

[Chen2011] Chen S., M. Zhang, and B. Xiao, “Efficient information collection protocols for sensor-augmented rfid networks,” in INFOCOM, 2011 Proceedings IEEE, April 2011, pp. 3101–3109

[CoE2007] Comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europero e al comitato delle regioni: L'identificazione a radiofrequenza (RFID) in Europa: verso un quadro politico Bruxelles, 15.3.2007 COM(2007) 96 definitivo

[CoE2010] Risoluzione del Parlamento europeo sull'internet degli oggetti Strasburgo 15 giugno 2010 (2009/2224(INI))

Diaz2002] Diaz C., S. Seys, J. Claessens, and B. Preneel, \Towards Measuring Anonymity," in Privacy Enhancing Technologies Workshop (PET), 2002.

[Dimi2006] Dimitriou T., \A Secure and Efficient RFID Protocol that cold make Big Brother (partially) Obsolete," in Proceedings of the IEEE International Conference on Pervasive Computing and Communications, 2006, pp. 269-275.

[EPC2013] http://www.epc-rfid.info/

[EPCGLO] EPCglobal Network,Wikipedia

[Fink2010] Klaus Finkenzeller. RFID Handbook. John Wiley and Sons, 2003.

[Gara2005] "Etichette intelligenti" (Rfid): il Garante individua le garanzie per il loro uso - 9 marzo 2005.IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI.

[Hoqu2011] Hoque M.E., F. Rahman, and S. I. Ahamed, \AnonPri: An Efficient Anonymous Private Authentication Protocol," in Proceedings of the IEEE International Conference on Pervasive Computing and Communications, 2011, pp. 102-110.

[Impi2016] Inpinj Inc., http://www.impinj.com/.

[Jants2006] Jantscher M. and Peter H. Cole Jantscher . Security and Authentication Primer. Auto-ID Labs White Paper,2006.

[Juels2004] Juels, A. (2004). Minimalist Cryptography for Low-Cost RFID Tags. International Conference on Security in Communication Networks - SCN,

September 2004

[Juels2005] Juels, A. (2005). Attack on a Cryptographic RFID Device. RFID Journal, 28 Feb. 2005. Available at http://www.rfidjournal.com/article/articleview/1415/

[Juels2006] Juels, A. (2006). RFID Security and Privacy: A research Survey. IEEE Journal on Selected Areas in Communication. No 24 Vol 2, pp. 381 - 394, February 2006.

[Juels2003] Juels, A. ; Rivest, R. & Szydlo, M. (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. Conference on Computer and Communications Security – ACM CCS, October 2003

[Law2000] Law, Ching, Lee, Kayi and Siu, Kai-Yeung. Efficient Memoryless protocol for Tag Identification. In Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, pages 75-84. ACM, August 2000.

[Lee2005] S.R. Lee, Joo, C.W. Lee. “An Enhanced Dynamic Framed Slotted ALOHA Algorithm for RFID Tag Identification” In proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous’05), 2005.

[Leht2006] Lehtonen Mikko, et altri. A Review of RFID Product Authentication Techniques. Auto-ID Labs White Paper,2006.

[Li2010] Li T., S. Chen, and Y. Ling, “Identifying the missing tags in a large rfid system,” in Proceedings of the eleventh ACM international symposium on Mobile ad hoc networking and computing, ser. MobiHoc ’10. New York, NY, USA: ACM, 2010, pp. 1–10.

[Lu2007] Lu L., J. Han, L. Hu, Y. Liu, and L. M. Ni, "Dynamic Key-Updating: Privacy-Preserving Authentication for RFID Systems," in Proceedings of the IEEE International Conference on Pervasive Computing and Communications, 2007, pp.13-22.

[Luo2012] Luo W., S. Chen, T. Li, and Y. Qiao, “Probabilistic missing-tag detection and energy-time tradeoff in large-scale rfid systems.” in Proceedings of the Thirteenth International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc ’12), Hilton Head Island, South Carolina U.S.A., June 2012, pp. 95–104.

[Mase2008] G. Maselli, C. Petrioli, and C. Vicari,Dynamic Tag Estimation for Optimizing Tree Slotted Aloha in RFID Networks,ACM MSWIM 2008, Vancouver, [J. Canada.

[Mass1981] Massey J., “Collision resolution algorithms and random-access communication,”Multi-Users Communication Networks, CISM Courses and Lectures, no. 256, pp. 73–137, 1981.

[Men2006] Menezes, A., van Oorschot, P. and Vanstone, S.; Handbook of Applied Cryptography;CRC Press; Boca Raton; 1996.

[Metc1976] Metcalfe R.M. and David R. Boggs (July 1976). "Ethernet: Distributed Packet Switching for Local Computer Networks". Comm. of the ACM 19 (7).

[Molna2004] Molnar D. and D. Wagner, \Privacy and Security in Library RFID Issues, Prac-tices, and Architectures," in Proceedings of the ACM Conference on Computer and Communications Security, 2004, pp. 210-219.

[Rana2006] Ranasinghe D. C.. A Low Cost Solution to Authentication in Passive RFID Systems.Auto-ID Labs White Paper,2006.

[Pugh1990] Pugh W., "Skip Lists: A Probabilistic Alternative to Balanced Trees," Commu-nications of the ACM, vol. 33, no. 6, pp. 668-676, 1990.

[Rieb2006] Rieback, M. R.; Crispo, B. & Tanenbaum, A. S. (2006b). Is your cat infected with a computer virus? Proc. of the 4th Annual IEEE International Conference on Pervasive Computing and Communication, pp. 169-179, ISBN: 0-7695-2518-0, 13-17 March 2006, Pisa, Italy.

[Rom1990] Rom R. . Multiple access protocols: performance and analysis Springer-Verlag New York, Inc.New York, NY, USA©1990

[Rott2009] Rotter P. . Security and Privacy in RFID Applications,Development and Implementation of RFID Technology, Book edited by: Cristina TURCU, February 2009, I-Tech, Vienna, Austria

[Saka2013] Sakai Kazuya . Security and Privacy in Large-Scale RFID Systems. Dissertation Presented in Partial Fulllment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of The Ohio State University, 2013.

[Talo2008] Paolo Talone,et al. RFID Fondamenti di una tecnologia silenziosamente pervasiva, Fondazione Ugo Bordoni,2008.

[Tuyls2006] Tuyls, P. & Batina, L. (2006). RFID-tags for anti-counterfeiting, In D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006, Vol. 3860 of LNCS, pp.115-131, Springer-Verlag, ISSN: 0302-9743, San Jose, CA, USA.

[Xiao2008] Xiao Q. . RFID Technology, Security Vulnerabilities, and Countermeasures, Supply Chain; The Way to Flat Organisation, Book edited by: Yanfang Huo and Fu Jia, December 2008, I-Tech, Vienna, Austria

[WEI2003] Weis, S., Sarma, S., Rivest, R. and Engels, D.; Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems; in Proceedings of the First International Conference on Security in Pervasive Computing; Springer Lecture Notes in Computer Science; Volume 2802; Pages 201-212; 2003.

[Wel2009] E. Welbourne, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the internet of things using RFID." IEEE Internet Computing, vol. 13, no. 3, pp. 48–55, May 2009.

[Wikipedia] https://it.wikipedia.org/wiki/ALOHAnet

[Zhou2004] Zhou F., C. Chen, D. Jin, C. Huang, H. Min, Evaluating and optimizing power consumption of anti-collision protocols for applications in RFID systems, in: Proceedings of the International Symposium on Low Power Electronics and Design 2004 (ISLPED '04), New York, NY, USA, 2004, pp. 357–362.