

RAPPORTO DI PROVA SULL' INTEROPERABILITA' E LA SICUREZZA NEI SISTEMI RFID

**A cura del Laboratorio
sperimentale CNIPA**

Daniele Mongiello, Gabriele Bocchetta, Mauro Draoli

DATA DI EMISSIONE: aprile 2007

Abstract

Il presente rapporto tecnico illustra i risultati di una sperimentazione realizzata in collaborazione con i laboratori del CATTID (Centro per le Applicazioni della Televisione e delle Tecniche di Istruzione a Distanza) dell'Università "Sapienza" di Roma, nell'ambito delle attività del Gruppo di lavoro RFID del Cnipa.

L'attività sperimentale è stata specificatamente indirizzata alla verifica delle caratteristiche di interoperabilità e sicurezza negli ambienti RFID multivendor e multistandard tipici delle applicazioni della Pubblica Amministrazione. L'attività sperimentale ha dapprima affrontato l'affidabilità della lettura dei tag in ambienti multistandard, nonché in presenza di elementi ambientali sfavorevoli, quali l'esistenza di materiali interferenti, il movimento in velocità e l'interferenza di due antenne in lettura. Successivamente è stata valutata la robustezza dei tag ad attacchi "semplici", di tipo fisico e logico.

L'esperienza condotta in laboratorio, durata oltre sei mesi, ha portato all'acquisizione di elementi concreti circa la funzionalità e le prestazioni dell'RFID nelle situazioni di utilizzo tipiche. I risultati mostrano notevoli fluttuazioni delle prestazioni dei sistemi, in funzione delle caratteristiche tecniche degli apparati e di quelle ambientali di utilizzo.

Il presente rapporto illustra in modo sistematico i protocolli operativi ed i risultati degli esperimenti fin qui effettuati; esso viene messo a disposizione degli esperti e specialisti di settore, nel mondo accademico ed in quello della ricerca industriale, anche al fine di raccogliere osservazioni ed ulteriori contributi.

INDICE

| | | |
|-----------|--|-----------|
| 1. | OBIETTIVI DELLA SPERIMENTAZIONE | 4 |
| 2. | AFFIDABILITA' DELLA LETTURA IN AMBIENTI MULTISTANDARD | 5 |
| 2.1. | DESCRIZIONE DELL'ESPERIMENTO | 5 |
| 2.2. | RISULTATI | 6 |
| 3. | LETTURA DI TAG IN PRESENZA DI MATERIALI INTERFERENTI | 7 |
| 3.1. | DESCRIZIONE DELL'ESPERIMENTO | 8 |
| 3.2. | RISULTATI | 10 |
| 4. | ROBUSTEZZA ALL'INTERFERENZA TRA ANTENNE | 12 |
| 4.1. | DESCRIZIONE DELL'ESPERIMENTO | 12 |
| 4.2. | RISULTATI | 15 |
| 5. | ROBUSTEZZA AI PRINCIPALI ATTACCHI | 15 |
| 5.1. | FORZATURA DELLA PASSWORD DI KILL-COMMAND | 15 |
| 5.2. | RESISTENZA FISICA ALLE SCARICHE ELETTRICHE | 17 |
| 5.3. | RISULTATI | 18 |
| 6. | CONSIDERAZIONI CONCLUSIVE | 19 |

1. OBIETTIVI DELLA SPERIMENTAZIONE

I campi di applicazione della tecnologia RFID nella Pubblica Amministrazione sono molto vari, con esigenze molto eterogenee in termini di interoperabilità, di sicurezza e privacy. L'esistenza di diversi standard di comunicazione Tag/reader, alcuni dei quali proprietari (e.g. Tag-IT, I-CODE ecc.), la disponibilità di Tag con diverse prestazioni anche all'interno dello stesso standard (riconducibili ad esempio al particolare procedimento costruttivo) potrebbero vincolare alla scelta di una ben specifica tipologia di Tag, se non addirittura a quella di uno specifico produttore. Si pensi ad esempio ad un'applicazione in ambito sanitario in cui ciascun paziente deve essere identificato (e collegato ai suoi dati clinici) attraverso il proprio bracciale RFID in diverse unità sanitarie dislocate sul territorio: la compatibilità del Tag con i diversi lettori presenti sul territorio è fondamentale.

L'interoperabilità è quindi la principale e fondamentale caratteristica richiesta nei sistemi altamente distribuiti e cooperanti della Pubblica Amministrazione (e.g. unità sanitarie, magazzini doganali, tracciamento alimenti ecc.) e in cui in generale non esiste la possibilità del controllo centralizzato.

Pertanto, l'ambiente di riferimento per le sperimentazioni realizzate è, per quanto possibile, volutamente caratterizzato da dispositivi "multi-vendor". In questo tipo di scenario è lecito attendersi alcuni problemi di interoperabilità, legati principalmente alla parziale frammentazione degli standard tecnologici adottati per le comunicazioni ed è prevedibile anche una disomogeneità di prestazioni rispetto ai valori operativi dichiarati dai fornitori. In questo senso, l'osservazione dei valori effettivamente riscontrabili sul campo evidenzia fluttuazioni prestazionali non trascurabili, anche per dispositivi appartenenti ad una medesima classe funzionale e con fattori di forma simili. La cause di tali fluttuazioni potrebbero essere riconducibili a ragioni che possono essere le più varie e legate, ad esempio, allo specifico produttore, al particolare procedimento costruttivo e a fattori ambientali.

Nei test sono stati utilizzati dispositivi RFID progettati per il funzionamento in due diverse porzioni di spettro: elementi funzionanti in HF (13,56Mhz se non specificato diversamente) e UHF (868Mhz, in conformità con le attuali normative in materia).

Il piano di sperimentazione è stato organizzato in quattro serie di esperimenti:

1. misura dell'affidabilità della lettura e valutazione del livello di compatibilità tra lettori e Tag multistandard e multivendor;
2. misura dell'affidabilità della lettura di Tag in situazione "ideale" ed in presenza di materiali interferenti;
3. misura della capacità di lettura dei Tag in condizioni di interferenza tra lettori;
4. valutazione della robustezza dei Tag ad attacchi "semplici".

2. AFFIDABILITÀ DELLA LETTURA IN AMBIENTI MULTISTANDARD

L'esperimento è consistito nella verifica della capacità di un reader di leggere correttamente un insieme di Tag di diversi produttori. Tutti i sistemi utilizzati in questo esperimento operano in banda HF.

L'esperimento ha avuto i seguenti obiettivi specifici:

- misurare, in una situazione ideale, l'affidabilità di un reader nella lettura di un Tag;
- misurare la compatibilità, da parte di ciascun reader, nella lettura di Tag multistandard o multivendor;
- sperimentare la possibilità di sviluppare dei software che migliorino le prestazioni dei reader, come misurati al punto precedente.

Sono stati studiati, inoltre, i meccanismi che consentono di configurare la modalità di lettura di ciascun reader.

2.1. Descrizione dell'esperimento

Il test è stato effettuato utilizzando diversi reader commerciali. Nello specifico:

- antenna planare A, con controller esterno indipendente, interfaccia comandi vs PC su collegamento seriale (anno di produzione 2001);
- antenna Gate B, con controller esterno indipendente, interfaccia comandi vs PC su collegamento seriale (anno di produzione 2001);
- antenna planare C, con controller emulato via software e interfaccia comandi vs PC su collegamento USB (anno di produzione 2004);
- lettore portatile D, modello palmare ad antenna integrata con software di gestione proprietario (anno di produzione 2002);
- lettore portatile E, modello palmare ad antenna integrata con software di gestione realizzato su piattaforma WindowsCE (anno di produzione 2005);
- lettore portatile F, modello PC palmare con hardware di lettura su scheda SD e software di gestione realizzato su piattaforma WindowsCE (anno di produzione 2006).

I Tag selezionati per questo esperimento appartengono alle seguenti tipologie:

- I-Code 1
- I-Code SLI
- ISO 15693 – 18000-3
- TI Tag-It
- MiFare

L'insieme dei Tag utilizzato nell'esperimento, e pertanto appartenenti alle categorie sopra elencate, è detto nel seguito Tag-set.

Il setup dei test è consistito in:

- preparazione e test di funzionalità degli apparati, e specificatamente:
 - studio dell'interfaccia di gestione dello specifico reader;
 - predisposizione del firmware di controllo, ove fosse necessario;
- configurazione ambiente per l'interfaccia software di gestione, ove fosse necessario;
- sviluppo del software di lettura, ove possibile, per consentire in maniera automatica la lettura dell'intero Tag set;
- debugging e ottimizzazione.

La procedura di test per i singoli apparati è consistita in:

- selezione di una modalità di lettura;
- posizionamento del Tag-set nella zona di lettura "ideale";
- rilevazione dell'esito della lettura per ciascun Tag componente il set.

Sono stati effettuati, complessivamente, 21 test, dove per test si intende la lettura dell'intero Tag-set con uno dei reader selezionati. Il gruppo di test è stato effettuato in un periodo di 7 giorni, impegnando una media di 3 ore per lo svolgimento di ogni test.

2.2. Risultati

Prima di tutto, si osserva che tutti i reader in prova sono stati in grado di leggere correttamente i Tag per i quali erano configurati. Pertanto, tutti i reader hanno realizzato la funzione di lettura correttamente e secondo le aspettative.

Le valutazioni di interoperabilità hanno consistito nella verifica della capacità dei reader di modificare, con un'operazione manuale o automatica, la modalità (cioè lo standard) di lettura.

Pertanto, i lettori sottoposti a prova sono stati classificati come segue, sulla base della capacità di leggere Tag multiprotocollo:

- lettori monoprotocollo, incapaci cioè di commutare da una modalità di lettura ad un'altra;
- lettori multiprotocollo non adattativi: la commutazione da uno standard ad un altro avviene attraverso un comando manuale dell'operatore;
- lettori multiprotocollo, che utilizzano ciclicamente più protocolli per tentare di leggere i Tag.

Di conseguenza, con i lettori in dotazione al laboratorio ed il software fornito a corredo, solo in alcuni casi è stato possibile effettuare una lettura contemporanea dei diversi Tag senza un intervento diretto dell'operatore.

La maggior parte degli apparati di lettura, ed in particolar modo quelli prodotti precedentemente al 2001, non prevedono un supporto multiprotocollo o "hot-swap". Per gli apparati sottoposti a test in questo ambito ed in particolare per le due antenne di più vecchia produzione, la configurazione di una data modalità di lettura si realizza caricando il firmware e riavviando il controller (Apparati A e B). Questa operazione richiede l'intervento di un tecnico specializzato e può durare anche decine di secondi¹.

Per tutti i restanti reader è stato possibile sviluppare una semplice procedura software che configura ciclicamente la modalità di lettura dei Tag. È stato misurato il tempo necessario al reader per effettuare il cambio della modalità di trasmissione e riportare l'avvenuta lettura del Tag. Questo è risultato variabile da circa 2 secondi (modello C) fino a qualche frazione di secondo per il modello palmare ad antenna integrata (modello D), per il quale è stato quindi possibile realizzare un'applicazione, per quanto essenziale, in grado di consentire la lettura semi-contemporanea del Tag set mascherando la complessità sottostante.

Nei test condotti sui sei lettori utilizzati, solo in tre di questi è stata riscontrata una incompatibilità verso un tipo specifico di Tag. In particolare, per questi tre apparati, non è stato possibile reperire librerie software che consentissero la lettura di Tag di tipo MiFare. Va notato comunque che sono gli unici Tag appartenenti al set che comprendono funzionalità per la cifratura del canale on-air, adatti quindi ad applicazioni particolari.

Per i restanti lettori è sempre stato possibile reperire i componenti software necessari a consentire la lettura dell'intero Tag-set.

Dall'osservazione dei risultati è evidente che il progresso tecnologico degli ultimi quattro-cinque anni ha messo a disposizione pacchetti di sviluppo che permettono una personalizzazione rapida e flessibile secondo le proprie esigenze, offrendo trasparenza rispetto alle complessità tecnologiche. Apparati di costruzione antecedenti agli anni 2000-2001 risentono molto della frammentazione degli standard costruttivi e dei problemi di incomunicabilità relativi, fatto che può in parte essere ovviato tramite l'utilizzo di apparati di lettura di ultima generazione, più sofisticati dal punto di vista hardware.

3. LETTURA DI TAG IN PRESENZA DI MATERIALI INTERFERENTI

Questo gruppo di esperimenti ha avuto l'obiettivo di misurare la probabilità di errore nella lettura di Tag in funzione del tipo di imballaggio che li contiene. In particolare, sono state eseguite prove con i seguenti imballaggi:

- imballi vuoti (carta);

¹ Il caricamento del firmware sul controller si fa attraverso la connessione seriale del controller di antenna ad un PC

- imballi liquidi;
- imballi di metallo;
- Tetra-Pak.

Secondariamente, è stata misurata la distanza massima alla quale è possibile effettuare correttamente la lettura di un Tag, in funzione del tipo di imballaggio che lo contiene.

3.1. Descrizione dell'esperimento

Il test è stato effettuato utilizzando un'antenna in configurazione gate (A) ed un'antenna planare da tavolo (B). La *Figura 1* illustra lo scenario del test ed evidenzia il gate e l'antenna da tavolo.

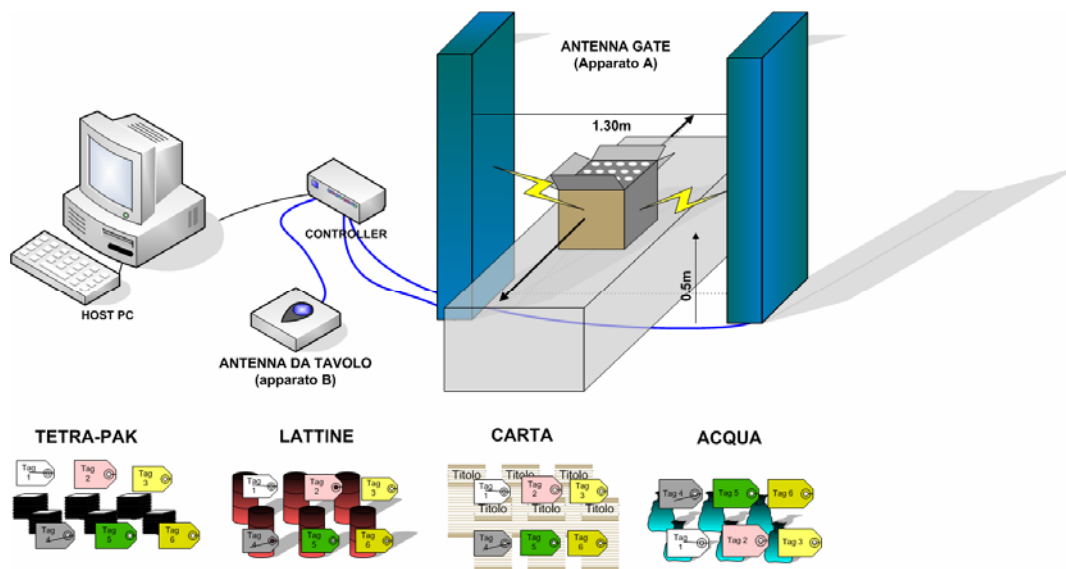


Figura 1: Schema dell'apparato sperimentale

Il setup della prova ha previsto:

- Selezione del Tag-set che comprende Tag conformi ai seguenti protocolli in dettaglio:
 - Tag I-Code 1
 - Tag I-Code SLI
- In particolare sono stati usati due Tag-set:
 - il Tag-set 1 è composto da 10 Tag di tre differenti produttori ed è stato utilizzato nelle prove con attraversamento del gate;

- il secondo è composto da 9 Tag, tutti differenti tra loro per dimensioni, forma e materiale costruttivo. Il Tag set 2 è stato utilizzato solo nelle prove di stima della distanza di lettura.
- Preparazione e test di funzionalità degli apparati:
 - posizionamento delle antenne del gate a 1,3m di distanza reciproca;
 - posizionamento dell'antenna planare in posizione verticale;
 - verifica di corretto funzionamento del firmware di controllo;
 - reinstallazione interfaccia software per i comandi, ove fosse necessario.

La procedura di test ha previsto:

- preparazione degli oggetti campione da utilizzare nelle singole prove. Nel dettaglio, i Tag sono stati applicati sui seguenti quattro materiali:
 - materiale non interferente (cartaceo);
 - sacchetti in plastica riempiti con acqua;
 - lattine da 33cl vuote e riempite con liquido acquoso;
 - Tetra-Pak riempiti con liquido acquoso;
- preparazione dell'imballo in cartone, delle dimensioni di 1m x 1m, in cui sono di volta in volta inseriti i Tag applicati sugli oggetti, descritti al punto precedente, come di seguito illustrato:
 - inserimento casuale dei Tag nella scatola, senza ricercare l'ortogonalità con l'asse delle antenne;
 - riposizionamento dei Tag, con lo stesso criterio, ad ogni passaggio;
 - viene imposta una distanza di almeno 10cm tra Tag per evitare interferenze reciproche;
 - percorso guida su cui far scorrere l'imballo posto ad 1 m da terra.
- passaggio dell'imballo per 12 volte in tutto, come di seguito:
 - velocità di attraversamento longitudinale del gate variabile tra 0,25 e 1,5 metri al secondo;
 - sei passaggi per direzione (“ingresso” e “uscita”):
- rilevazione dell'esito della lettura per ogni passaggio, attraverso la misura del rapporto tra il numero di Tag letti correttamente ed il numero totale di Tag appartenenti al Tag-set (denominato nel seguito tasso di successo).

- nei soli casi in cui il tasso di successo è risultato inferiore al 100%, si è proceduto come segue:
 - sono stati estratti tutti i Tag non letti, mantenendoli applicati all'imballo;
 - l'apparato di lettura B (antenna planare) è stato progressivamente avvicinato al Tag fino a raggiungere l'esito positivo della lettura;
 - è stata misurata e registrata la distanza massima alla quale la lettura è avvenuta correttamente.

Sono stati effettuati complessivamente 40 test (20 riguardanti le distanze di lettura e 20 riguardanti l'attraversamento del gate). I test sono stati effettuati in un periodo di 20 giorni, impegnando una media di 4 ore per lo svolgimento di ciascun test.

3.2. Risultati

È stato possibile osservare, tramite le prove eseguite, che l'impatto sulla trasmissione elettromagnetica dei materiali metallici e dei liquidi polari è fortemente distorsivo. La Figura 2 illustra il tasso di successo medio misurato utilizzando il Tag-set 1 e l'apparato di lettura A, in funzione del tipo di materiale su cui i Tag sono applicati. La media dei risultati si riferisce a 12 passaggi, con velocità diverse e nei due versi di attraversamento del gate, come precedentemente descritto.

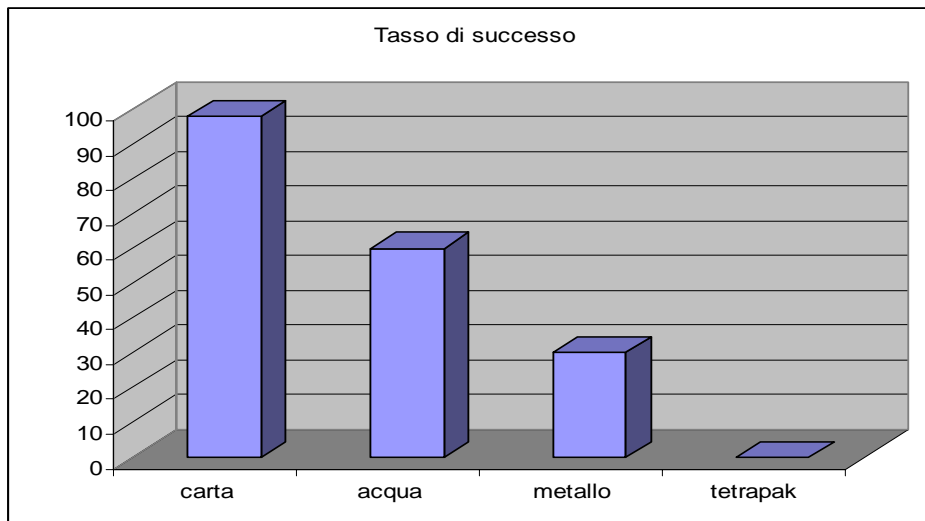


Figura 2: Tasso di successo su materiali interferenti (Tag-set 1)

Nelle condizioni ideali, in cui i Tag sono applicati su materiali elettromagneticamente non interferenti (carta), il tasso di successo è stato molto prossimo al 100%. Solo in alcuni passaggi non sono stati letti i Tag di dimensioni più piccole.

Nel caso in cui si sono utilizzati i Tag su oggetti (sacchetti di plastica) riempiti con acqua il tasso di successo, per lo stesso gruppo di Tag di riferimento, è sceso nei dodici passaggi, al 50-60%.

Un ulteriore peggioramento si è riscontrato nel caso di involucri metallici (lattine) con un 20-30% di Tag letti per passaggio e la comparsa di un primo passaggio con 0 Tag letti.

Infine, nella configurazione di test elaborata, si è arrivati all'inibizione quasi totale della lettura nel caso di involucri di Tetra-Pak.

Successivamente è stata misurata la massima distanza alla quale un Tag risulta leggibile da parte dell'antenna planare da tavolo (B), in funzione del materiale su cui il Tag è applicato. L'esperimento è stato realizzato su tutti i Tag appartenenti al Tag-set 2.

Il grafico seguente (Figura 3) indica, in ascissa, la dimensione fisica di ciascuno dei Tag oggetto dell'esperimento, in ordine crescente. L'asse delle ordinate misura la variazione percentuale della distanza di lettura rispetto a quella ideale misurata quando il Tag è applicato su materiale cartaceo. Ciascuna delle tre curve illustra pertanto la degradazione della distanza di lettura quando il Tag è applicato rispettivamente a contatto con materiale acquoso, metallo e tetrapak. L'osservazione mostra che la riduzione della portata rispetto al caso ideale (imballo vuoto contenente i soli Tag) è dell'ordine del 10% circa per Tag applicati su oggetti contenenti acqua (ed indipendentemente dalle dimensioni del Tag), varia tra il 40% ed il 100% per involucri metallici e, nel caso del Tetra-Pak, provoca una "inibizione" vera e propria della lettura della gran parte dei Tag² con dimensione inferiore 5mm x 5mm.

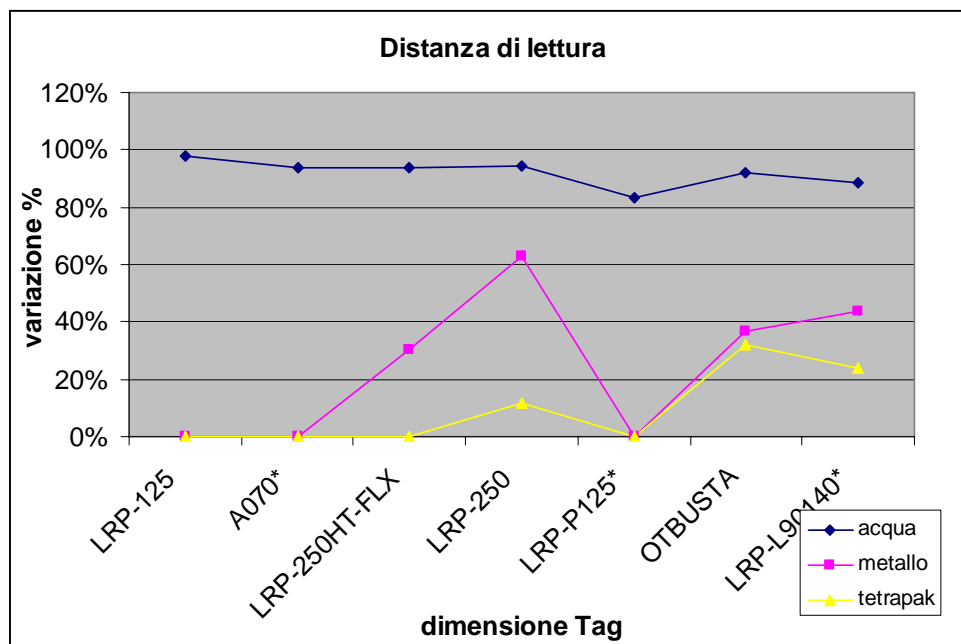


Figura 3 - Degradazione della distanza di lettura per materiali

Anche la velocità di attraversamento del gate ha avuto un effetto di degradazione sensibile delle prestazioni misurate. Una lettura completa del set, pertanto senza errori, è stata possibile unicamente nel caso ideale (Tag applicati su carta) e con velocità non superiori a circa 1 m/s.

² Esistono Tag appositamente costruiti per l'utilizzo su materiali speciali, quali il Tetrapak, che non sono stati inclusi nei Tag-set oggetto della sperimentazione

La conclusione è che, in scenari simili a quello di prova, il disturbo dovuto alla presenza di materiali specifici comporta un forte degradamento del tasso di successo nella lettura automatizzata. Di contro, in scenari di lettura in cui non siano coinvolti elementi elettromagneticamente non trasparenti, lo stesso sistema può funzionare con buoni livelli prestazionali.

In conclusione, si può affermare che, in fase di progettazione, debbono essere tenute in conto nell'ordine:

- le condizioni ambientali di utilizzo della tecnologia RFID, con specifico riferimento primariamente alla natura dei materiali su cui i Tag sono apposti;
- la velocità di movimento degli oggetti "taggati" quando attraversano le zone di lettura;
- la dimensione e le caratteristiche fisiche dei Tag utilizzati.

4. ROBUSTEZZA ALL'INTERFERENZA TRA ANTENNE

L'esperimento ha avuto l'obiettivo di misurare la probabilità di errore nella lettura di un Tag da parte di un lettore di riferimento, quando è presente un lettore interferente.

A tale scopo è stato posto sotto osservazione il comportamento di un reader palmare HF quando nelle vicinanze è presente un'antenna Gate funzionante alla medesima frequenza. In questo scenario, è stata misurata la massima distanza di lettura di Tag passivi da parte dell'apparato HF con antenna Gate in prossimità del reader palmare HF funzionante in modalità CR (Continuos Reading).

4.1. Descrizione dell'esperimento

Questo test è stato realizzato per valutare sperimentalmente quanto segue:

- la riduzione della massima distanza di lettura di un Tag HF passivo a 13,56MHz, posto nel campo generato da due reader interferenti, rispetto ad una situazione di non interferenza;
- la minima distanza a cui due reader, in condizioni di interferenza reciproca, sono in grado di operare entrambi correttamente.

Per effettuare le prove è stato posto un lettore palmare, in modalità lettura continua, nel campo generato da un lettore con una singola antenna appartenente ad una configurazione a Gate. Quest'ultima è configurata per inviare una richiesta di lettura con tempi di interlettura di: 100ms, 200ms, 300ms. La Figura 4 illustra lo scenario della prova.

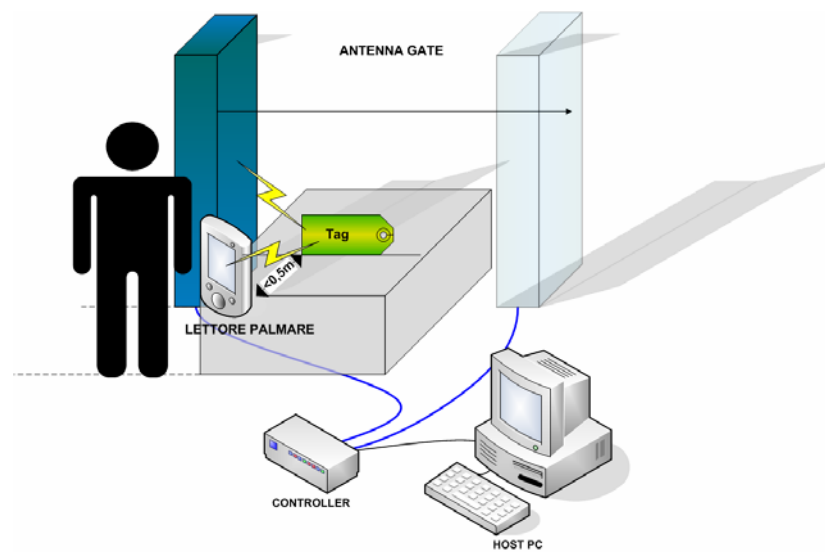


Figura 4: Schema dell'apparato sperimentale per la valutazione dell'interferenza

Il test è stato eseguito utilizzando i seguenti Tag a 13,56 MHz:

- Tag i-code SLI II
- Tag ISO 15693

e i seguenti apparati:

- controller con singola antenna di Gate (nel seguito R1), ERP 500mW;
- reader palmare (nel seguito R2) in modalità CR;
- asta graduata per la misurazione delle distanze.

La procedura di test è stata eseguita separatamente per i Tag indicati sopra (punti 1 e 2), per i seguenti tempi di interlettura³ del reader R1:

- $t_{il}=300$ ms
- $t_{il}=200$ ms
- $t_{il}=100$ ms

per le seguenti distanze tra R1 e R2:

- $distanza(R1,R2)=10$ cm

³ Il tempo di interlettura misura l'intervallo di tempo che intercorre tra due successivi invii del segnale di interrogazione (detto anche intervallo di polling). Lo stato di Continuous Reading, per l'apparato palmare utilizzato, corrisponde ad un intervallo di interlettura pari a 50 ms.

- distanza(R1,R2)=20 cm
- distanza(R1,R2)=30 cm
- distanza(R1,R2)=40 cm

Procedura di test:

- misura della massima distanza tra i due apparati in cui è possibile ottenere una lettura corretta tramite l'apparato R1 con tempo di interlettura fissato;
- misura della massima distanza tra i due apparati in cui è possibile ottenere una lettura corretta tramite palmare R2 in modalità lettura continua;
- posizionamento degli apparati R1 e R2 in condizione di massima interferenza e distanza(R1,R2) fissa;
- posizionamento del Tag tra gli apparati, il Tag è stato posto tra i due apparati R1 e R2 con l'orientamento dell'antenna più favorevole alla lettura, variando la distanza:
 - distanza(Tag,R1);
 - distanza(Tag,R2) = distanza(R1,R2)-distanza(Tag,R1) con scarti di 5 cm partendo dal lettore R1;
- verifica dell'avvenuta lettura del Tag da parte dei lettori R1 e R2.

Per tutti i test è stato definito un sistema di riferimento in cui la posizione del lettore R1 è stata presa come punto di riferimento (coordinata X=0) per la misura delle distanze. A tale scopo è stata posizionata un'asta graduata perpendicolarmente al piano dell'antenna del lettore R1 in coincidenza dell'asse centrale dell'antenna stessa. La distanza tra R1 e R2 è stata variata mantenendo fissa la posizione di R1.

Sono stati eseguiti i test con i seguenti setup sperimentali:

- reader palmare in CR, controller con antenna Gate e tempo di interlettura 300ms, distanza tra i lettori: 10-20-30-40 cm per un totale di 60 letture;
- reader palmare in CR, controller con antenna Gate e tempo di interlettura 200ms, distanza tra i lettori: 10-20-30-40 cm per un totale di 60 letture;
- reader palmare in CR, controller con antenna Gate e tempo di interlettura 100ms, distanza tra i lettori: 10-20-30-40 cm per un totale di 60 letture.

Sono stati effettuati, complessivamente, 6 test (2 per ogni tipo di setup sperimentale, utilizzando rispettivamente Tag i-code SLI II e Tag ISO 15693).

4.2. Risultati

Il primo risultato è che, seppure in presenza di campi d'interferenza reciproca ed azioni di lettura concorrenti, gli apparati Reader, anche se caratterizzati da livelli di potenza elettromagnetica molto diversi (e quindi da una diversa capacità di "controllare" il Tag), riescono comunque a leggere il valore corretto dell'Id del Tag.

Tuttavia, l'esperienza ha mostrato che, in ambienti in cui siano presenti più sistemi di lettura RFID indipendenti e di diversa tipologia, ad esempio quando alle postazioni fisse si aggiungano apparati per letture in mobilità, i problemi di interferenza sono evidenti:

- la riduzione della portata del lettore portatile utilizzato nei test quando posto a meno di un metro dall' apparato più potente, come il gate utilizzato, è consistente e misurata nell'ordine del 50%;
- durante la sperimentazione sono state rilevate delle "letture incerte" nella zona di sovrapposizione dei campi elettromagnetici generati dai due reader che quindi interferiscono reciprocamente. La visualizzazione dell'Id del Tag, sebbene decifrabile, risulta instabile e intermittente mentre in modalità CR dovrebbe rimanere statica e fissa sul display;
- al di sotto dei 0,5 m di distanza tra i due lettori il dispositivo meno potente, quello palmare, non riesce più a leggere correttamente i Tag selezionati.

5. ROBUSTEZZA AI PRINCIPALI ATTACCHI

L'esperimento ha avuto l'obiettivo di valutare la robustezza dei Tag ad alcuni semplici attacchi di tipo logico e fisico. Le prove sono state suddivise in due gruppi con differenti finalità sperimentali relative a:

- sicurezza logica: forzatura della password a protezione del kill-command deputata alla disattivazione del Tag;
- sicurezza fisica: disattivazione/danneggiamento del Tag per mezzo di impulsi elettrici diretti e di impulsi elettromagnetici.

5.1. Forzatura della password di kill-command

Il kill-command è un particolare comando che provoca la disattivazione permanente e definitiva del Tag a cui esso viene inviato.

I Tag utilizzati nelle prove eseguite in laboratorio sono conformi alle specifiche EPCGlobal C1G1. Questo tipo di Tag, in una configurazione minimale, ha una memoria interna di 128bit, di cui 96 sono destinati a contenere l'Id di identificazione, 8bit/16bit contengono la password di kill, 16bit un CRC calcolato secondo CCITT CRC-16 ed i restanti 8bit un lock-code opzionale il cui scopo è rendere "opache" alcune zone di memoria. La kill command key dei Tag UHF C1G1 utilizzati per i test è

costituita da una stringa lunga 2 byte, precedentemente registrata in una speciale area di memoria. Una chiave di soli 2 byte significa che vi possono essere al massimo 2^{16} ovvero 65536 chiavi.

Visto il limitato range di valori che la chiave di protezione può assumere, la sicurezza garantita a fronte di un “attacco di forza bruta” mirato alla disattivazione dei Tag tramite un reader “intruso” è, relativamente, piuttosto debole.

Le specifiche EPCGlobal C1G2 prevedono invece che sui Tag sia memorizzata una password statica di 32bit che inibisce l'esecuzione del kill command. Viene inoltre aggiunto un meccanismo di protezione della memoria, opzionale, con una ulteriore password di 32bit che il reader dovrà fornire per avere diritti di lettura/scrittura sul Tag in determinate aree.

La protezione offerta per questa versione delle specifiche EPC, che prevede password statiche per un gruppo omogeneo di Tag esposti ad un attaccante determinato, è sicuramente migliore in quanto richiede range temporali di gran lunga superiori (2^{32} ovvero circa 16M di chiavi possibili).

I test di sicurezza logica sono stati effettuati con l'ausilio di un dispositivo di lettura UHF composto da:

- due antenne di lettura formato “patch” delle dimensioni di 40x40cm;
- controller separato per entrambe le antenne con collegamento USB.

Le prove di laboratorio hanno richiesto lo sviluppo di una semplice applicazione in linguaggio Java per la generazione ricorsiva delle password e del tentativo di attacco mediante kill-command. A tale scopo si è fatto uso dello SDK (Software Development Kit) a corredo, che include le librerie software di gestione degli apparati di trasmissione e il supporto per i protocolli relativi ai Tag utilizzati⁴.

Il setup della prova ha previsto:

- setup della macchina di sviluppo;
- studio del pacchetto SDK: Vendor 1 SDK Java
- scelta dei Tag da porre in test, in dettaglio:
 - EPC C1G1
 - EPC C1G2⁵
- realizzazione del codice necessario;
- debugging e ottimizzazione.

⁴ Lo studio e la codifica del software che realizza la ricerca esaustiva delle password è stata condotta con l'ausilio del personale tecnico della casa costruttrice dell'apparato di lettura Parte del listato relativo al codice utilizzato proviene da codice già realizzato internamente al CATTID per altre sperimentazioni sulle stesse tecnologie

⁵ Pur avendo inserito nello scenario di test questa tipologia di Tag, in fase di set up delle strumentazioni, si è riscontrata la mancanza delle librerie di controllo funzionanti che non hanno consentito la corretta esecuzione del codice di ricerca della password di kill command

La procedura di test ha previsto:

- posizionamento dei Tag in zona di lettura;
- lettura del Tag prima dell'esperimento;
- avvio del ciclo di scansione delle password possibili per l'invio e l'esecuzione del comando di Kill;
- lettura del Tag per verificarne l'eventuale disattivazione.

5.2. Resistenza fisica alle scariche elettriche

L'esperimento ha l'obiettivo di misurare la robustezza dei Tag alla scarica elettrica indotta da una batteria di condensatori caricati attraverso una rete elettrica appositamente realizzata e alla scarica elettrica indotta da dispositivo piezoelettrico. I Tag selezionati sono tutti operanti a 13.56 MHz.

La robustezza è stata valutata andando a verificare il corretto funzionamento dei Tag colpiti da una scarica ed ispezionando a vista la presenza di ustioni sul packaging. Il Tag si ritiene funzionante dopo la scarica se viene correttamente letto dal reader e se il valore dell'identificativo letto coincide con quello letto prima della scarica.

Il test è stato eseguito utilizzando i seguenti Tag:

- Tag Vendor 1 ISO 15693 ICODE SL2 (5x5 cm);
- Tag Vendor 2 ISO 15693 (8,5x5,5 cm);
- Tag Vendor 3 ISO 15693 (8x2,5 cm);
- Tag Vendor 4 ISO 15693 ICODE SL2 (7,5x4,5 cm);
- Tag Vendor 5 ISO 15693 (8x5 cm);

e i seguenti apparati e dispositivi:

- reader palmare utilizzato per eseguire letture dei Tag elencati sopra;
- dispositivo piezoelettrico;
- condensatori con capacità singola di 4700 μ F;
- alimentatore 13,8 V DC 3A;
- breadboard e componenti elettrici aggiuntivi per la realizzazione del circuito di carica dei condensatori.

Le prove sono state eseguite con apparati di scarica "portatili", ossia di dimensioni contenute, di facile realizzazione e con alimentazione portatile. Si consideri che i circuiti a condensatori realizzati allo scopo possono essere efficacemente alimentati a batteria.

La procedura di test ha previsto:

- realizzazione dei circuiti di scarica con capacità:
 - A. $C=4700 \mu\text{F}$;
 - B. $C=9400 \mu\text{F}$;
 - C. $C=14100 \mu\text{F}$.
- selezione sul reader dello standard di lettura del Tag sotto test;
- lettura e registrazione dell'identificativo del Tag prima del test;
- scarica elettrica sul packaging del Tag in prossimità del chip, attraverso conduttori a punta che prelevano la carica:
 - ai capi della batteria di condensatori (circuiti A,B,C);
 - dal dispositivo piezoelettrico;
- lettura del Tag dopo la scarica per verificarne il funzionamento.

5.3. Risultati

L'esperimento di attacco tramite kill-command ha sempre avuto successo. Relativamente ai Tag C1G1 l'attacco è stato portato a compimento in un massimo di circa 5800 secondi circa (su un tempo massimo teorico di 6030 secondi circa, ottenuto considerando un tempo di esecuzione complessivo del singolo comando di circa 90ms moltiplicato per il totale delle chiavi possibili).

Per i test riguardanti i Tag C1G2, per problemi emersi con il tool di sviluppo del codice, è stato possibile affrontare solo uno studio approssimato dei tempi di successo attesi per la ricerca della password di kill. Tale studio, prendendo in considerazione le stesse modalità di esecuzione e password di 4 Byte, ha indicato comunque un tempo di esecuzione massimo di molto superiore⁶.

Pertanto, l'utilizzo di Tag UHF EPC C1G1 e G2 in applicazioni in cui siano coinvolti dati sensibili su scenari aperti o comunque non "supervisionati" è una scelta da valutare con attenzione⁷.

Nella composizione del Tag-set per la sperimentazione sulla sicurezza fisica, sono stati selezionati i Tag maggiormente diffusi nelle applicazioni RFID, ossia Tag ad alimentazione passiva ed a basso costo.

Il Tag set utilizzato per questa sperimentazione ha evidenziato una rilevante robustezza all'induzione di scariche elettriche indotte dagli apparati utilizzati. In particolare nelle prove eseguite,

⁶ Va tenuto conto, comunque, che la sicurezza assicurata da un sistema che si affidi unicamente a chiavi simmetriche resta comunque bassa. In letteratura sono state dimostrate tecniche di analisi del segnale riflesso dal Tag che permettono la ricostruzione corretta di parte delle sequenze numeriche inviate on-air in chiaro

⁷ Sulla base delle specifiche sulla password di identificazione dei reader per la scrittura sono state proposte soluzioni basate su un servizio directory per le chiavi di lettura

pur in presenza di ustioni e segni permanenti sulla pellicola di protezione dei Tag, essi hanno continuato a funzionare correttamente.

6. CONSIDERAZIONI CONCLUSIVE

L'esperienza in laboratorio e l'approccio sperimentale hanno consentito di acquisire elementi di conoscenza utili alla definizione di un percorso di introduzione ed utilizzo della nuova tecnologia RFid nella Pubblica Amministrazione. A tale scopo, i risultati dell'attività sperimentale sono stati posti all'attenzione del Gruppo di lavoro sull'RFid del Cnipa.

L'esperienza condotta in laboratorio, durata oltre sei mesi, ha portato all'acquisizione di elementi concreti circa la funzionalità e le prestazioni dell'RFID nelle situazioni di utilizzo tipiche. I risultati mostrano notevoli fluttuazioni delle prestazioni dei sistemi, in funzione delle caratteristiche tecniche degli apparati e di quelle ambientali di utilizzo, e di cui si dovrebbe tenere in conto nella progettazione dei servizi per la Pubblica amministrazione.

Le attività svolte in laboratorio non possono certamente considerarsi concluse, né i risultati esaustivi. Il presente rapporto illustra in modo sistematico i protocolli operativi ed i primi risultati degli esperimenti fin qui effettuati; esso viene messo a disposizione degli esperti e specialisti di settore, nel mondo accademico ed in quello della ricerca industriale, anche al fine di raccogliere osservazioni ed ulteriori contributi.