Osservazioni Lotto - Gabriel

# Introduzione

* Ciò che è stato effettivamente implementato è un semplice schema PLA che sfrutta le proprietà fisiche (potenza, distanza e interferenza) del canale di trasmissione utilizzato per autenticare i messaggi trasmessi.

Lotto:

dovete spiegare in che modo queste proprietà fisiche vengono utilizzate per portare autenticazione.

Le proprietà sono del canale o del segnale? think about it...

Risposta:

Lo stato del canale influisce solo a livello di condizionamento dei parametri di simulazione, mentre è la potenza del segnale il parametro che influisce maggiormente, in particolare dato dalla potenza scelta del segnale e dalla forma d’onda che rappresenta un’ “impronta digitale” riconoscibile tra ricevitore e mittente, sfruttando la conoscenza condivisa delle soglie e dello schema di codifica. Il canale ha degli evidenti “disturbi” dati dal fading/interferenza/delay, variazioni attese in base al profilo delineato; se corrisponde a quello atteso, il messaggio è considerabile autentico.

# Sim.m

* Nello specifico, si è impostata una simulazione realistica nell’ambito delle distanze Bluetooth, coprendo una serie di messaggi mandati fino ad un massimo di 50 metri, impostando delle rate accettabili in termini di SNR sulle distanze, tra 30 e 10, andando a rappresentare un decadimento realistico del segnale qualora disturbato in termini di distanza effettiva.

Lotto:

cosa vuol dire decadimento realistico?

perchè 'qualora disturbato'? Aggiunge delle informazioni/condizioni aggiuntive per il quale è necessario questa specificazione?

Risposta

Il decadimento realistico intende che l'intensità del segnale diminuisce con l'aumentare della distanza tra il trasmettitore e il ricevitore. Questo è un fenomeno naturale nelle comunicazioni wireless, dove la potenza del segnale si attenua a causa della dispersione e delle perdite lungo il percorso, cercando di modellare una cosa più simile possibile alla realtà.

La presenza del disturbo è di interesse per aggiungere realismo alla simulazione, data la presenza dei rumori di fondo del canale, potenzialmente in grado di veicolare fonti di disturbi aggiuntive.

* Al fine di determinare l’autenticità o meno di un certo messaggio decodificato, si è ritenuto necessario impostare un numero massimo di bit permessi di errore sul segnale chiave/autenticazione.

Lotto

come avete scelto questo numero massimo?

Immagino abbiate fatto uno studio a riguardo, menzionate la cosa.

Risposta

La scelta del numero di bit massimi di errore è dato in primis dalla forma del segnale, dato ad onda quadra; questo permette una manipolazione più precisa dei suoi bit. Infatti, le soglie di distanza e di errore cercano di intervenire precisamente a livello di numero di bit, determinando la presenza di un numero di bit massimi come parametro di controllo e mantenimento delle singole soglie.

La scelta dei bit deriva inoltre dal controllo tramite distanza di Hamming; essendo il segnale unico analizzato inviato come mixato, la presenza di un controllo sul numero di bit permette, dopo ripetute simulazioni, di attivare un certo tipo di codifica piuttosto che un altro.

Siamo all’interno di un ambito simulativo, dunque la soglia di tolleranza è stata inserita come parametro di controllo al fine di rifinire, dopo alcune esecuzioni, tale soglia per verificare la correttezza o meno della trasmissione effettuata; ciò avviene in base alle prestazioni di sicurezza desiderate in primis.

# FA.m

* Per definire autentico un messaggio viene impostata una tolleranza di errore sui bit della chiave da rispettare per l’autenticazione stessa. Idealmente se il numero dei bit errati sulla chiave, calcolati tra l’output della decodifica e il pacchetto chiave originale, eccede questa tolleranza il messaggio non può essere dichiarato autentico e, per tale motivo, viene conteggiato come false alarm dato che, in questo contesto, supponiamo di inviare solamente messaggi autentici.

Lotto

come avete scelto questa tolleranza?

Risposta

La tolleranza è data da una serie di osservazioni, principalmente data dalle decodifiche adottate per entrambi i tipi di segnale; il segnale autenticazione, più piccolo in ampiezza/potenza del segnale dato, è un parametro da cui il segnale mixato dipende per poter definire l’ambito di decodifica e rigenerazione del segnale, essendo, specie nelle soglie variabili, impiegato come parametro intermedio per rifinire la rilevazione del segnale e garantire la corretta rilevazione di un bit.

In particolare, si è notato che la decodifica a soglie fisse risultava essere molto performante sul segnale dato, non rilevando particolari errori utili a decodificare il segnale; il numero di bit sul segnale di autenticazione è stato scelto per garantire un controllo più fine.

Si veda la risposta precedente per completamento logico, essendo lo stesso ragionamento.

* Il risultato finale osservato sulla base di diverse run è un tasso di FA pari allo 0% per tutte le coppie (distanza, SNR).

Lotto

Immagino quindi che per ogni possibile configurazione, la decodifica del messaggio di autenticazione sia sempre perfetta senza neanche un bit errato...?

La cosa mi risulta un po' strana nel caso in cui la mia soglia di tolleranza sia 0 (= nessun bit sbagliato per essere definito autentico) o 1 o 2.

Può essere, ma verificate...

Risposta

La rilevazione risulta essere efficace già nel metodo di decodifica a soglie fisse, dato che impostando l’ arrotondamento del segnale ricevuto ai picchi di potenza dipendenti dal parametro di centro, il segnale viene già arrotondato alle soglie di potenza previste; ciò è anche dovuto alla precisa ricombinazione del segnale dato ed autenticazione come previsto dalla singola simulazione (Sim.m).

Le soglie variabili intervengono nel caso di grosso scostamento dalla soglia di tolleranza; dato l’arrotondamento del segnale alle soglie di potenza individuate, il centro risulta essere il parametro più rilevante per aggiustare il segnale rilevato nel modo corretto.

# MD\_First\_Approach.m

* Si considerano, ugualmente al resto della simulazione, nuovamente segnali binari di lunghezza prestabilita mischiati con un pacchetto dati e un pacchetto chiave trasmessi a potenze differenti, con la potenza della chiave inferiore alla potenza di trasmissione del dato. I metodi per generare, unire e inviare tali segnali sono i medesimi descritti per il file “Sim.m”. Per definire non autentico un messaggio viene impostata una tolleranza di errore sui bit della chiave da rispettare per l’autenticazione stessa. Idealmente se il numero dei bit errati sulla chiave, calcolati tra l’output della decodifica e il pacchetto chiave originale, eccede questa tolleranza il messaggio non può essere dichiarato autentico.

Lotto

Quant'è questa tolleranza? e perchè proprio quel valore?

Anyway...non si era detto di provare una serie di valori di tolleranza e verificare le prestazioni di FA e MD per ognuno di questi valori?

Risposta

Non si è ritenuto necessario impostare un range in quanto i metodi di decodifica presenti sono già soddisfacenti, a parità di soglie di autenticazione, per rifinire la relativa percentuale d’errore, data la serie di simulazioni con diversi valori di tolleranza e l’efficacia delle decodifiche descritte.

Date le alte prestazioni dei sistemi di decodifica da noi implementati, in particolare relative all’algoritmo a soglie variabili, non si è ritenuto necessario implementare un meccanismo di controllo soglie FA threshold per cambiare le soglie di decodifica data l’alta prestazione raggiunta fin da subito.

* L’attaccante tenta quindi di decodificare il segnale originale analizzando i suoi picchi di potenza e utilizzando tali valori per decodificare la sequenza di bit inviata.

Lotto

Immagino quindi che l'attaccante non riesce MAI a decodificare correttamente giusto? Altrimenti, cade l'assunzione di "si assume di ricevere sempre messaggi non autentici".

Se questo non è ciò che succede, allora bisogna cambiare, perchè in realtà il messaggio è stato autenticato con la chiave corretta. Che poi sia l'attaccante a generare questo messaggio non conta, perchè comunque la chiave è corretta. Piuttosto, questo va a studiare la resistenza del protocollo da decodifica da parte di terzi non autorizzati e quanto è probabile che siano in grado di ricavare la chiave di autenticazione. Assicuratevi che i messaggi che inviate NON siano autentici

Risposta

Di fatto, la decodifica non risulta corretta, confermando la validità del nostro approccio. Il messaggio non autentico garantisce che il messaggio sia effettivamente diverso dall’originale; all’interno della simulazione viene infatti generato casualmente con dei bit “flippati” secondo un intervallo casuale, determinando quindi l’inefficacia da parte dall’attaccante nella decodifica e successiva reinterpretazione. Infatti, come evidenziato da metodi precedenti, il segnale autentico viene determinato efficacemente dato il controllo “preciso” svolto dai metodi di decodifica e il sistema si rivela in grado di resistere all’errore sia in caso di messaggio diverso che di decodifica non autorizzata.

* Il risultato finale osservato sulla base di diverse run è un tasso di MD pari allo 0% per tutte le coppie (distanza,SNR).

Lotto

Cioè, è sempre in grado di distinguere che il messaggio sia non-autentico anche se cambio un solo bit di autenticazione?

Mi sembra strano, ma come prima, controllate.

Risposta

Nuovamente, l’efficacia della rilevazione viene data dalla decodifica, in grado di rilevare molto precisamente, date le soglie di potenza presenti, gli errori sul dato, che tendono gradualmente a rifinirsi in media assestandosi a valori medi di BER. Infatti, data la diversità del segnale trasmesso, il segnale non autentico viene sempre rilevato con precisione, garantendo la corretta rilevazione e codifica anche nel caso di variazioni minime sul bit autenticazione.

* Chiaramente questo per noi rappresenta il caso meno realisticamente probabile dato il livello di conoscenza che l’attaccante dovrebbe possedere…

Lotto

Assolutamente no! Quando definiamo il threat model, dobbiamo sempre assumere l'attaccante più potente possibile, e.g., che abbia piena conoscenza di come funziona il sistema di comunicazione analizzato.

La sicurezza del sistema si basa quindi sulla segretezza di certi parametri, la chiave nel nostro caso.

Risposta

(Qua direi che va rivista come scritta, visto che nel Second Approach, di fatto, dando in mano più parametri possibile tutto funziona; semplicemente direi solo sopra così: “Si è tentato di seguire un approccio naif, in cui assumiamo che l’attaccante non sia sufficientemente potente da avere a sufficienza informazioni precise sul segnale dato/autenticazione; per questo motivo, si è scelto di utilizzare il secondo approccio di miss detection e rilevazione”)

# MD\_Second\_Approach.m

* Sulla base del primo approccio del conteggio delle miss detection, la seconda simulazione è stata impostata con il fine di considerare nuovamente i parametri simulativi della singola simulazione Sim e, sulla logica del primo approccio di rilevazione, si è tentato di fornire maggior conoscenza ad un possibile attaccante MITM. In questo caso, infatti, l’attaccante sa la struttura del messaggio originale, composto da messaggio chiave/autenticazione e messaggio normale e, sulla base di queste, impostare una decodifica basata sulle soglie dinamiche del segnale, date sempre dai picchi come per le simulazioni precedenti.

Lotto

Immagino quindi che nello scenario precedente l'attaccante utilizzasse approccio a soglie fisse..?

Se così, sistemate sopra perchè non chiaro.

Risposta

Corretto, sistemiamo

* In questo caso, il principale interesse è volto al risultato della citata matrice di miss detection MD\_matrix. Qui, infatti, i valori di miss detection rilevano valori altalenanti, compresi in media dopo una serie di rilevazioni tra il 20 e il 30/35%, confermando l’efficacia dell’approccio evidenziato. In questo modo, è possibile notare che un attaccante può inserirsi all’interno del meccanismo di decodifica, in tal modo non venendo rilevato (ma, essendo un ambito simulativo, si è in grado di “accorgersi” dell’interpretazione errata dei messaggi, dando dei dati utili per correggere i parametri di partenza della simulazione). Con codifica/decodifica “vicine” tra di loro per logica, si evidenzia come la simulazione si mantiene solidamente in grado di rilevare i messaggi errati interpretati come legittimi, confermando infine la validità della rilevazione compiuta e descritta nei suoi vari approcci.

Lotto

cosa vuol dire?

Risposta

Corretto, sistemiamo