**Introduzione alla simulazione MATLAB**

La simulazione consente di studiare il comportamento di invio e ricezione di segnali wireless in ambito Bluetooth tramite trasmissioni parametrizzate, al fine di costruire un ambiente simulativo per lo studio di future implementazioni di schemi PLA con aggiunta di rumore artificiale per rendere il processo di autenticazione più efficace.

L’idea di base è avere un mittente e un ricevitore che mandano un segnale composto da chiave (autenticazione) e messaggio dati, mischiato con dei parametri di potenza noti all’interno del canale ed inviato ad una serie di distanze osservate ciascuna nell’ambito di interferenza accettabile per distanza (SNR - Signal-to-Noise Ratio).

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. Nell’ambito del ricevitore, il segnale viene decodificato sulla base di soglie di potenza (thresholds) fisse e variabili, che permettono di ottenere un’analisi più approfondita a livello di prestazioni sul canale e capire come rifinire i parametri stessi di simulazione per ottenere un messaggio il più possibile simile a quello originariamente inviato. I messaggi vengono definiti autentici se, dal risultato della decodifica utilizzata lato ricevitore, si ottiene un numero di bit errati (rispetto alla sequenza chiave originale generata) sulla chiave entro un certo limite prestabilito.

Sono state infine svolte alcune simulazioni in merito ai valori di FA e MD osservati sulla simulazione creata. In particolare, tramite questi ulteriori studi, si vuole comprendere la validità dei messaggi trasmessi all’interno della simulazione, comprendendo quanti messaggi falsi positivi (false alarm - messaggi veri che vengono interpretati come falsi) e falsi negativi (miss detection - messaggi falsi interpretati come veri).

Di seguito vengono illustrati i diversi file MATLAB che compongono l’intera simulazione.

**Sim.m**

La simulazione modella un sistema di comunicazione wireless che utilizza segnali di dati e di autenticazione combinati, con l’obiettivo l'analisi delle prestazioni del sistema in termini di Bit Error Rate (BER) per i segnali di dati e di autenticazione, al variare della distanza e del rapporto segnale-rumore (SNR).

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.

Successivamente, si è impostata la creazione dei due segnali dato e autenticazione come forma d’onda binaria, andando poi ad assegnare un valore di potenza prestabilito per

ciascuna, al fine di rilevare esattamente i “picchi” di potenza; specificamente, il segnale autenticazione assume picchi di potenza più bassi all’interno del segnale, per poter così analizzare il segnale composito i due in modo più preciso.

Questo risulta importante in fase di decodifica; infatti, viene impostato un metodo basato sulla concordanza/discordanza dei bit, al fine di variare correttamente segnale dato e autenticazioni ricevuti.

Sulla base di distanze e SNR variabili, viene simulato l’invio e la ricezione del segnale, a cui viene applicato del rumore bianco (AWGN) per simulare l’effetto del canale. In tale contesto, vengono testati due metodi di decodifica; a soglie fisse e a soglie variabili.

In particolare, le soglie variabili vengono impostate considerando quattro picchi sul segnale: alto-alto (valore massimo), basso-basso (valore minimo) e valori intermedi (medio-basso/medio-alto). Tali misurazioni sono variabili data la forma d’onda del segnale quando impostato un parametro di centro (center), definito per permettere di definire precisamente e così aggiornare questi valori di picco. Tale misurazione rifinisce in particolare i valori intermedi, considerando valore precedente e valore attuale (da valori teorici/predefiniti a valori calcolati).

Si ha poi la decodifica a soglie fisse, data sulla base del parametro di centro. In questo punto, viene definita la discordanza dei bit dato e autenticazione, per fare in modo i segnali ricevuti riflettano coerentemente due forme d’onda ricevute qualora mixate come avviene in origine.

Qualora il segnale ricevuto sia maggiore/uguale del parametro di centro, il segnale ricevuto in forma reale viene arrotondato alla soglia massima del segnale autenticazione (e il bit dato assume valore discorde); ciò consente di perfezionare la cattura del segnale entro le soglie, considerando possibili intervalli teorici di distanza. Viceversa, qualora il segnale ricevuto sia minore del parametro di centro, il segnale ricevuto in forma reale viene arrotondato alla soglia minima del segnale autenticazione (e il bit dato assume valore discorde).

Una volta ricevuti i segnali, tramite distanza di Hamming coi segnali originali è possibile determinare il numero di bit errati; ciò risulta particolarmente importante nella fase di calcolo delle soglie BER, calcolate sull’intero segnale e utili per il calcolo dei falsi allarmi e mancati rilevamenti.

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. Qualora il numero di bit errati sulla chiave ottenuti dalla decodifica standard (a soglie fisse) superi il suo valore soglia, allora entra in gioco la decodifica a soglie variabili, che permette di meglio interpretare e così rifinire l’errore entro un intervallo accettabile.

In questo caso, il segnale autenticazione è facente parte del picco alto/medio-alto oppure basso/medio-basso, assumendo come riferimento il segnale dato, realizzando così la discordanza in termini di bit. Il segnale assumerà un valore quando si trova nell’intervallo alto-alto e medio-basso e un altro valore nell’intervallo basso-basso e medio-alto, garantendo una decodifica corretta del segnale.

Anche per questa decodifica, viene controllato il numero di bit errati con distanza di Hamming. I valori di BER vengono poi inseriti all’interno di due matrici, al fine di calcolare il

tasso medio di BER, utile per le successive rilevazioni compiute negli altri file di simulazione, così calcolando correttamente i rate di FA e MD.

**FA.m**

La simulazione consente di andare a determinare e studiare il livello di affidabilità del sistema di trasmissione individuando il tasso di false alarm sul solo invio di messaggi autentici. Lo studio avviene sotto diverse configurazioni del sistema di trasmissione, variando distanza trasmettitore-ricevitore (1-50 metri) e il rapporto segnale rumore (10-30 dB).

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 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.

Lo studio del false alarm avviene tramite un ciclo for annidato che, per ogni distanza e per ogni rapporto segnale rumore (10-30 dB) genera N trasmissioni di messaggi differenti. Il FA viene calcolato come il rapporto (messaggi apparentemente non autentici)/N per ogni coppia (distanza,SNR) creando una matrice (FA\_matrix) che consente di visualizzare tali valori.

Il risultato finale osservato sulla base di diverse run è un tasso di FA pari allo 0% per tutte le coppie (distanza, SNR). Questo dato tuttavia non risulta così sorprendente in quanto l’algoritmo di decodifica variabile abbassa notevolmente il numero di errori sui bit chiave, ottenuti dall’algoritmo a soglie fisse, riuscendo sempre a restare al di sotto della soglia prestabilita. Questo ci ha portato a convalidare l’implementazione scelta per l’algoritmo di decodifica a soglie dinamiche.

**MD\_First\_Approach.m**

La simulazione consente di andare a determinare e studiare il livello di affidabilità del sistema di trasmissione individuando il tasso di missed detection sul solo invio di messaggi non autentici. Lo studio avviene sotto diverse configurazioni del sistema di trasmissione, variando distanza trasmettitore-ricevitore (1-50 metri) e il rapporto segnale rumore (10-30 dB).

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.

A differenza del caso di false alarm, in questo contesto si assume di ricevere sempre messaggi non autentici all’interno della stessa struttura for annidata descritta per il file “FA.m”. Si suppone che, dopo la generazione e l’invio di un nuovo messaggio, intervenga un man in the middle pronto a intercettare il messaggio, decodificarlo e trasmettere nuovamente. 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. Una volta ottenuta la sequenza codificata, l’attaccante trasmette al ricevitore originale la sequenza ricavata, utilizzando le potenze ricavate dai picchi del segnale originariamente inviato. A questo punto il ricevitore decodifica il messaggio ricevuto tramite i meccanismi a soglie fisse e dinamiche precedentemente descritti nelle precedenti simulazioni.

Per questo studio diviene quindi fondamentale andare ad osservare quanti dei messaggi intercettati dall'attaccante e reinviati vengono accettati dal sistema. Tali messaggi vengono quindi conteggiati come missed detection.

Lo studio della missed detection avviene tramite un ciclo for annidato che, per ogni distanza e per ogni rapporto segnale rumore (10-30 dB) genera N trasmissioni di messaggi differenti. La MD viene calcolata come il rapporto (messaggi interpretati come autentici)/N trasmissioni per ogni coppia (distanza,SNR) creando una matrice (MD\_matrix) che consente di visualizzare tali valori.

Il risultato finale osservato sulla base di diverse run è un tasso di MD pari allo 0% per tutte le coppie (distanza,SNR). Anche in questo caso il dato ottenuto non è così sorprendente in quanto conferma nuovamente la corretta implementazione dell’algoritmo di decodifica a soglie variabili. L’attacco simulato dall’attaccante risulta essere molto semplice ma allo stesso tempo molto naturale in quanto il man in the middle tenta di ricostruire il segnale binario inviato analizzando i picchi del segnale intercettato e utilizzando una sorta di decodifica a soglie fisse molto simile a quella implementata dal lato del ricevitore.

Questo risultato tuttavia ci ha portato a considerare un ulteriore scenario di possibile attacco, fonte di studio per un’ulteriore missed detection. Nel secondo approccio, che viene di seguito descritto, si suppone che l’attaccante abbia una conoscenza maggiore sul canale e sulla struttura dei messaggi inviati. Chiaramente questo per noi rappresenta il caso meno realisticamente probabile dato il livello di conoscenza che l’attaccante dovrebbe possedere, tuttavia si è ritenuto interessante valutare le prestazioni del sistema sottoponendolo ad un attacco molto mirato.

**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.

Nuovamente, l’attaccante cerca di decodificare il segnale dati i picchi alto/basso e livelli medi sui segnali, determinando il segnale autenticazione come segnale più piccolo in ampiezza rispetto al dato, emulando così il funzionamento della decodifica in modo similare a quella legittima; ciò che cambia è l’evidente guess da parte del possibile attaccante, così da combinare il segnale una volta data la decodifica delle soglie dinamiche così composte di potenza e autenticazione, mantenendo simile la logica di discordanza dei bit e garantire un segnale a forma d’onda quadra molto simile a quello legittimo.

In questo contesto, successivamente, si ha poi il ricevitore legittimo, in grado di decodificare il segnale nella maniera medesima presente all’interno del primo approccio di miss detection; decodifica a soglie fisse data l’impostazione del parametro di centro e attivazione della decodifica a soglie variabili una volta superati il numero di bit errati permessi sulla chiave, seguendo le logiche definite in precedenza.

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.