* Autenticazione in ambito Bluetooth

Immagine che contiene linea, Diagramma, numero, Carattere

Descrizione generata automaticamenteFacciamo conto di iniziare il sampling dei segnali

Immagine che contiene linea, Diagramma, Carattere, numero

Descrizione generata automaticamenteSampling segnali funziona così:

Questo è il segnale con cui comunichiamo trasmettendo tra i devices. La parte di autenticazione lavora con lo stesso principio e da qui calcoliamo un MAC di autenticazione (può essere calcolato oppure la chiave stessa condivisa – al momento non ci interessa il valore).

Immagine che contiene testo, linea, Diagramma, Carattere

Descrizione generata automaticamenteCodifichiamo il segnale a livelli di ampiezza. Vediamo un esempio di come funziona il sampling in questo contesto. Questi sono i bit di autenticazione, mentre sopra abbiamo il segnale:

Il segnale risultante è la sovrapposizione dei due segnali nei device.

Immagine che contiene linea, Diagramma, diagramma

Descrizione generata automaticamenteIl sampling dei segnali procede in questo modo, tra concordi e discordi. Questo è il segnale che realmente buttiamo fuori.

Il ricevitore è sempre in grado di interpretare correttamente il segnale. Per la decodifica del segnale vero e proprio, ogni volta che il bit è maggiore di zero, il bit del segnale sarà 1 e viceversa.

Abbiamo quattro possibilità, in particolare quando siamo nei bit negativi:

Immagine che contiene linea, Diagramma, diagramma

Descrizione generata automaticamente

Se siamo sotto la potenza nominale, i bit erano discordi, viceversa erano concordi. Se ci mettiamo dal punto di vista di un attaccante, non ci sta nessun processing o conoscenza segreta tra trasmettitore e ricevitore, per un possibile attaccante ci sta lo stesso possibilità di fare una codifica.

Immagine che contiene linea, Diagramma, diagramma

Descrizione generata automaticamenteImmagine che contiene linea, Diagramma, diagramma

Descrizione generata automaticamenteL’idea è di aggiungere del rumore al segnale finale (che è la somma dei due segnali) portando le due ampiezze entro un certo range):

Immagine che contiene linea, Diagramma, diagramma

Descrizione generata automaticamenteI segnali sono tutti allo stesso livello, ma immaginiamo che invece abbiamo aggiunto del rumore al segnale azzurro. Se vedo tutti i segnali presenti nel bound, io non so se il valore è stato generato dalla combinazione dei valori (ora abbiamo tre valori: bit segnale, autenticazione, rumore).

Immagine che contiene linea, Diagramma, diagramma

Descrizione generata automaticamenteDecido di fare il flip dei valori presenti e da attaccante non posso più fare inferenza diretta con i bit del segnale con i bit di autenticazione (rumore di cui io non sono a conoscenza).

Immagine che contiene testo, linea, Carattere, Diagramma

Descrizione generata automaticamenteStrutturiamo ora il messaggio con una serie di pezzi, normalmente riconoscibili. Indichiamo al ricevitore il rumore che è stato aggiunto:

Il tutto è criptato e l’attaccante non riesce a vedere il rumore e se la criptazione può riuscire a fare questa cosa.

Migliore soluzione introducendo la miglior efficienza con meno overhead.

Dal segnale viola accetta il messaggio se e solo se i bit di autenticazione corrisponde ai bit attesi. La sicurezza di questo protocollo.

Immaginiamo questa situazione, con Eve che fa sniffing del messaggio così com’è. Se non viene modificato il segnale, assumendo che il canale di comunicazione sia fatto così:

Immagine che contiene calligrafia, linea, Carattere, Diagramma

Descrizione generata automaticamente

Immagine che contiene calligrafia, linea, Carattere, Diagramma

Descrizione generata automaticamenteIl segnale viene ricevuto in forma modulata – più distante sono dal segnale, minore è la potenza del segnale e diminuisce in modo quadratico rispetto alla distanza.

Immagine che contiene diagramma, schizzo, linea, calligrafia

Descrizione generata automaticamenteIl segnale assume forma sferica e così la potenza:

Ci possono essere problemi sul canale dovuti a:

* distanza
* interferenza
  + Se ci sono altri segnali che usano la stessa frequenza (2.4 Ghz), il segnale sarà nullo
  + Ci può essere interferenza distruttiva (caso sopra) oppure concordi (interferenza costruttiva)
* multipath (come visibile dalla figura)
  + Quando sono tra A e B, il segnale viene inviato a 360 gradi.
  + Un segnale arriva diretto e rimbalza tra oggetti per poi essere riflesso tra ostacoli
  + Immagine che contiene schizzo, Line art, bianco, disegno al tratto

    Descrizione generata automaticamenteImpossibile avere un segnale dritto per dritto

Immagine che contiene calligrafia, Carattere, linea, testo

Descrizione generata automaticamenteQuando un segnale viene rappresentato, si usano i numeri complessi (rappresentazione polare dei numeri primi), ad esempio come segue:

Immagine che contiene calligrafia, diagramma, linea, testo

Descrizione generata automaticamenteSe il segnale rimbalza, aumenta la fase e quindi è possibile che si inverta in un senso polare/coordinate goniometriche. Vediamo il tipo di frequenze usate:

In questo modo, il segnale viene riflesso e il canale è lo stesso può essere soggetto a reply attack. Assumiamo che Alice non sia in grado di bloccare il segnale.

Immagine che contiene linea, Diagramma

Descrizione generata automaticamente

Alice e Bob si scambieranno dei messaggi pilota per spiare il canale. Stimando il canale, il rumore aggiunto al segnale sarà dipendente dal canale tra Alice e Bob. In questo modo, con l’assunzione di prima, il rumore non può più essere valido.

Immagine che contiene testo, calligrafia, Carattere, linea

Descrizione generata automaticamenteQuello che vogliamo è che l’azione del canale mi permetta di riottenere la stessa incognita. In questo modo, da un valore precedente, riesco a riottenere il segnale e l’autenticazione.

Il rumore tolto da una parte non era quello della stima e quindi deve ritornare un valore diverso da quello iniziale. Rilassiamo il vincolo e vogliamo che, se il segnale autenticato viene ricevuto, il canale essendo diverso, l’errore, per quanto qualcuno conosca il contesto, se viene tolto, dato il canale diverso, si ottiene un messaggio che verifica non essere più in grado di autenticare.

Immagine che contiene calligrafia, linea, Carattere, testo

Descrizione generata automaticamente

Immagine che contiene linea, Diagramma, diagramma, testo

Descrizione generata automaticamenteIl rumore è dipendente dal canale e, quando non si ha più lo stesso canale, si capisce che la comunicazione non è più valida. Uno dei partecipanti capisce che la trasmissione è diversa perché il canale non legittimo fa in modo che il segnale sia diverso da quello della trasmissione iniziale. In questo modo, non potrà più verificare l’autenticazione iniziale nello stesso modo.

Immaginiamo di mappare il messaggio col canale legittimo, con la possibile aggiunta di rumore sul segnale mappato.

Alice riceve il segnale, sapendo che l’antiazione del canale è una traslazione del segnale. Dovrà quindi spostare quello che fa il canale in senso dimensionale.

Immagine che contiene linea, diagramma, Diagramma

Descrizione generata automaticamenteImmagine che contiene linea, Diagramma, diagramma

Descrizione generata automaticamenteOra sa qual è il segnale artificiale raggiunto da Bob e per ricostruirlo, partendo dal segnale rumoroso, ha tolto l’azione del canale che pensa essere per Bob, e questa non è la stessa di prima e rimuove il canale artificiale:

Immagine che contiene linea, Diagramma, diagramma, Carattere

Descrizione generata automaticamenteDal segnale, cerchiamo di capire dove sta l’autenticazione e poi calcolo il MAC. Se capito “nello spazio” bene, se capito fuori non tanto:

Immagine che contiene linea, Diagramma, diagramma

Descrizione generata automaticamenteAssumeremo come threat model un segnale più semplice e poi studiamo come si comporta il meccanismo. Il messaggio sarà rumoroso e il caso peggiore è quando Eve è vicina a Bob. In quel caso, si considera che ci siano situazioni di rumore bianco – non è rimuovibile.   
In questo caso, ciò che conta nella comunicazione è il signal to noise ratio:

Immagine che contiene calligrafia, linea, Carattere, schizzo

Descrizione generata automaticamente

Per colpa della rilevazione, siamo sotto al segnale misurato e non riesco a decodificare correttamente. Non ci interessa la potenza ma questo ratio (quanto pulito è il segnale rispetto al rumore). Questo il calcolo:

Immagine che contiene linea, calligrafia, Diagramma, Carattere

Descrizione generata automaticamenteIl segnale ha un certo rumore e qui abbiamo il rumore bianco (white gaussian noise):

Design del protocollo e poi ci aiutiamo con lui. Simulazione software intanto poi in base a quanto veloci lavorare, pensiamo se fare un testband più reale in base al tempo e tutto il resto.

* Rivedere bene questi concetti (in base anche agli appunti di Alessandro)
* Buttarci giù un’idea di come simulare
* Meeting tra Natale e Capodanno per allinearci sull’impostazione della simulazione
* Ci può dare qualche dritta implementativa (azione del canale, generazione segnale, etc.)

Matlab/Python/C++/Java

Simulazione in Matlab per il progetto

Introdursi su cosa è stato fatto in Bluetooth lato Physical Layer – related work del paper

Approfondire di più i paper di Alessandro