**PLA (PHYSICAL LAYER AUTHENTICATION)**

IDEA: verificare l'autenticità del messaggio inviato andando a sfruttare le proprietà fisiche della rete.

Ricezione e generazione del segnale non sono componenti univoche, se ricevo un messaggio, questo può essere generato anche in maniera legittima ma questo non assume che il messaggio non possa essere intercettato e re-inviato da terze parti.

=> Applicazione nei sensori: siamo sicuri che una certa misurata ricevuta è corretta? Es. misure di temperatura, ecc.

Per proteggerci da questi scenari si va a intervenire sullo strato fisico della rete => proteggere la corretta ricezione del messaggio.

POSSIBILITA’ DI PROGETTO:

**1**) **lavorare sulle proprietà del segnale**: sfrutto la randomicità del segnale in modo che esso non sia replicabile tra l'attaccante e il ricevitore. Il segnale può essere manipolato aggiungendo, ad esempio, una fase.

2) ML: RF-finger-printing

**APPROCCIO BASATO SULLE PROPRIETA’ FISICHE DELLA RETE**

Contesto di studio: device authentication in ambito bluetooth.

Immagine che contiene linea, Diagramma, numero, Carattere

Descrizione generata automaticamenteFacciamo conto di iniziare il sampling dei segnali

Codifichiamo il segnale con 2 valori di bit:

- ampiezza = 1 🡪 bit = 1

- ampiezza = -1 🡪 bit = 0

Immagine che contiene linea, Diagramma, Carattere, numero

Descrizione generata automaticamenteOttenendo:

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 (supponiamo di aumentare la potenza A=2). Il nuovo segnale rappresenta i bit di autenticazione, mentre sopra abbiamo il segnale standard:

**Il segnale risultante è la sovrapposizione dei due segnali**.

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 emesso.

**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 è presente nessuna conoscenza segreta tra trasmettitore e ricevitore**.

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**, il quale corrisponderà alla somma dei due segnali precedenti + aggiunta di rumore:

Ora abbiamo tre valori distinti che compongono il segnale: bit segnale, bit autenticazione e bit rumore.

L’idea è quella di comunicare al ricevitore il rumore aggiunto in modo che lo possa rimuovere per decodificare il segnale originale. Chiaramente dobbiamo proteggere questa informazione.

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. Migliore soluzione introducendo la miglior efficienza con meno overhead.

Il destinatario riceverà il messaggio se e solo se i bit di autenticazione erano quelli che si aspettava.

**PRIMO PUNTO DI STUDIO:** **La criptazione è sufficiente come metodo di sicurezza o è necessario anche il rumore?**

Come aggiungiamo questo rumore?

- attraverso la CSI (Channel State Information)

- in un modo tale che esso sia dipendente dal canale di trasmissione usato per inviare il messaggio. In questo modo il destinatario riuscirà sempre a capire se un messaggio è autentico o meno 🡺 se terze parti vogliono comunicare con il destinatario dovranno instaurare un nuovo canale di comunicazione; pertanto, la decodifica di un messaggio che proviene dal nuovo canale non sarà valida perché porterà ad un’autenticazione diversa.

**Immagine che contiene testo, Carattere, calligrafia, linea

Descrizione generata automaticamente**

Il parametro h è condizionato da:

- distanza e ostacoli

- interferenza (altri segnali sulla stessa frequenza)

- multipath (inteferenza dovuta a segnali riflessi)

Per stimare il valore di h, dobbiamo trasmettere dei segnali pilota e dobbiamo definire una mappa del segnale ricevuto, ottenendo così il canale finale.

Immagine che contiene Carattere, linea, numero, tipografia

Descrizione generata automaticamenteNota: se usiamo piu frequenze per trasmettere, dobbiamo ripetere questa procedura (CSI) per ogni frequenza 🡪 possiamo usare una sintassi che coinvolge le matrici:

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

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

Immagine che contiene calligrafia, linea, Carattere, Diagramma

Descrizione generata automaticamente

Immagine che contiene diagramma, linea, calligrafia, schizzo

Descrizione generata automaticamenteIl segnale assume forma sferica e così la potenza (P potenza (azione del canale), d distanza, pi-greco):

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.
  + È impossibile avere un segnale dritto da A a B. Il segnale rimbalza contro degli ostacoli e crea diversi path che raggiungono B. Il segnale finale sarà la somma di questi multipath (NB: quando un segnale rimbalza su un oggetto la sua fase cambia).

Immagine che contiene schizzo, Line art, bianco, disegno al tratto

Descrizione generata automaticamente

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

Immagine che contiene calligrafia, Carattere, linea, testo

Descrizione generata automaticamente

Se 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:

Immagine che contiene calligrafia, diagramma, linea, testo

Descrizione generata automaticamente

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 (procedura CSI). 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 (h) mi permetta di riottenere la stessa incognita (x). In questo modo, da un valore precedente, riesco a riottenere il segnale e l’autenticazione.

L’azione del canale non legittimo (AE che si interpone tra AB) fa sì che se A toglie il rumore, non è più in grado di autenticare quel segnale perché quel segnale apparteneva ad un canale diverso su cui B aveva aggiunto del rumore 🡺 il rumore, infatti, dipende dal canale di appartenenza.

Immagine che contiene calligrafia, linea, Carattere, testo

Descrizione generata automaticamente

**Il 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.

**Immagine che contiene linea, Diagramma, diagramma, testo

Descrizione generata automaticamente**

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

Alice riceve il segnale, sapendo che l’anti-azione 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:

Assumeremo 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 linea, Diagramma, diagramma

Descrizione generata automaticamente

Immagine che contiene calligrafia, linea, Carattere, schizzo

Descrizione generata automaticamentePer 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):

**SECONDO PUNTO DI STUDIO: in base a cosa aggiungiamo il rumore? In base all’azione del canale?**

**CONSIDERAZIONI FINALI**

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