Obiettivo:

L'intero esperimento si basa sullo studiare il comportamento di segnali wireless trasmessi in un canale con precise configurazioni per le sue trasmissioni (potenza, distanza, SNR, soglie di FA desiderate).

L'obiettivo è quello di trovare una configurazione ideale che permetta di raggiungere la percentuale   
desiderata di FA per rendere sicure le trasmissioni nel canale. Il risultato finale sarà molto vicino   
al concetto di PLA dove l'obiettivo è quello di andare a costruire uno schema di trasmissione sicuro  
senza utilizzare alcuna tecnica crittografica ma solamente le proprietà del canale di trasmissione (stato del canale).

<https://www.sciencedirect.com/science/article/pii/S235286482200284X>

As a promising complement for upper-layer encryption authentication, Physical Layer Authentication (PLA) techniques utilize the unique physical layer characteristics in wireless communication, such as carrier frequency offset, channel impulse response, radio frequency fingerprint and received signal strength indicator to distinguish the legality of transmitter.

The accuracy of spoofing detection is reflected by two indicators, false alarm rate and miss detection rate, which are associated with the test threshold in the hypothesis test performed at the receiver and the attack probabilities of spoofers.

Linea logica:

* Numero di simulazioni
* Segnale di autenticazione
  + Due segnali (dato + autenticazione)
  + In forma binaria
* Threshold segnale dato
* Parametri di simulazione
  + SNR (come trovare i valori?)
  + Distanza
  + Target\_FA
    - epsilon = soglia di tolleranza
      * soglie più grandi = dato
      * soglie più piccole = chiave
    - “center”
* Definizione segnale inviato
  + Mix dati + autenticazione
* Generazione segnale ricevitore (autentico prima di decodificarlo)
  + for j in distance
    - for k in SNR
      * for i in range(1,N)
        + ricevitore = awgn(segnale\_generato, SNR)
        + bit per bit
      * calcolo BER medio