Obiettivo:

The whole experiment is based on studying the behavior of wireless signals transmitted in a channel with precise configurations for its transmissions (power, distance, SNR, desired FA thresholds).

The goal is to find an ideal configuration that allows the desired percentage of AF to be achieved to make the transmissions in the channel safe. The final result will be very close to the concept of PLA where the goal is to build a secure transmission scheme without using any cryptographic technique but only the properties of the transmission channel (channel state).

<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