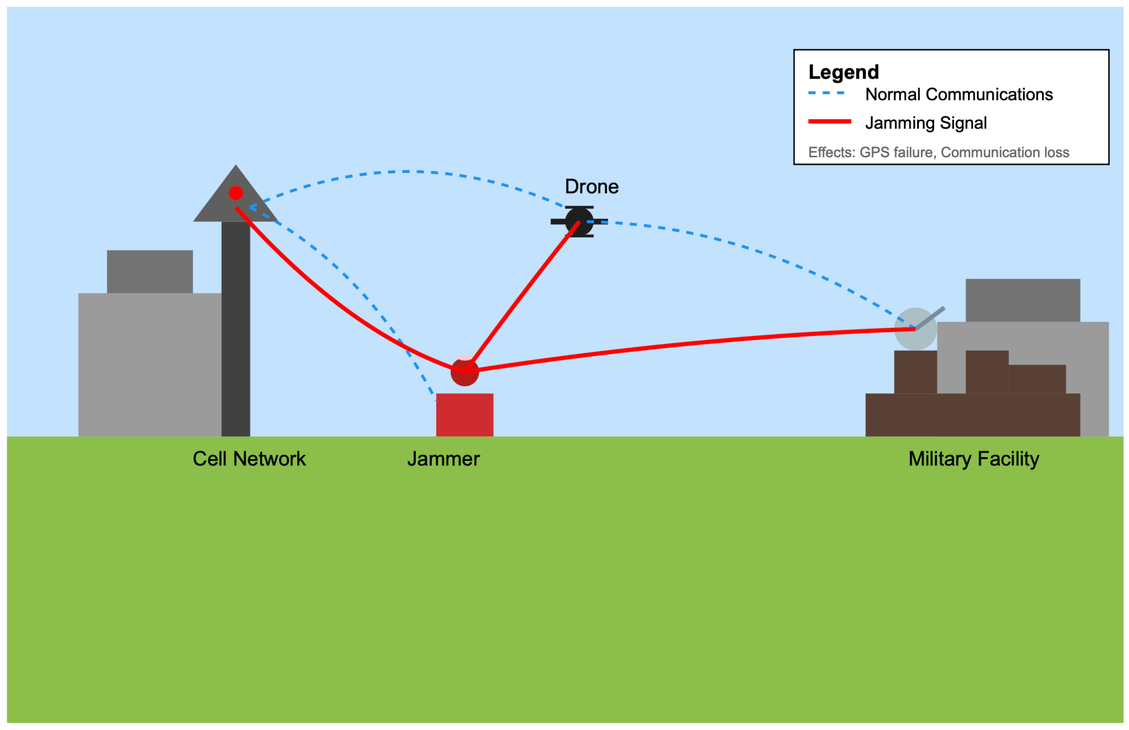
Frequency Hopping Spread Spectrum (FHSS)

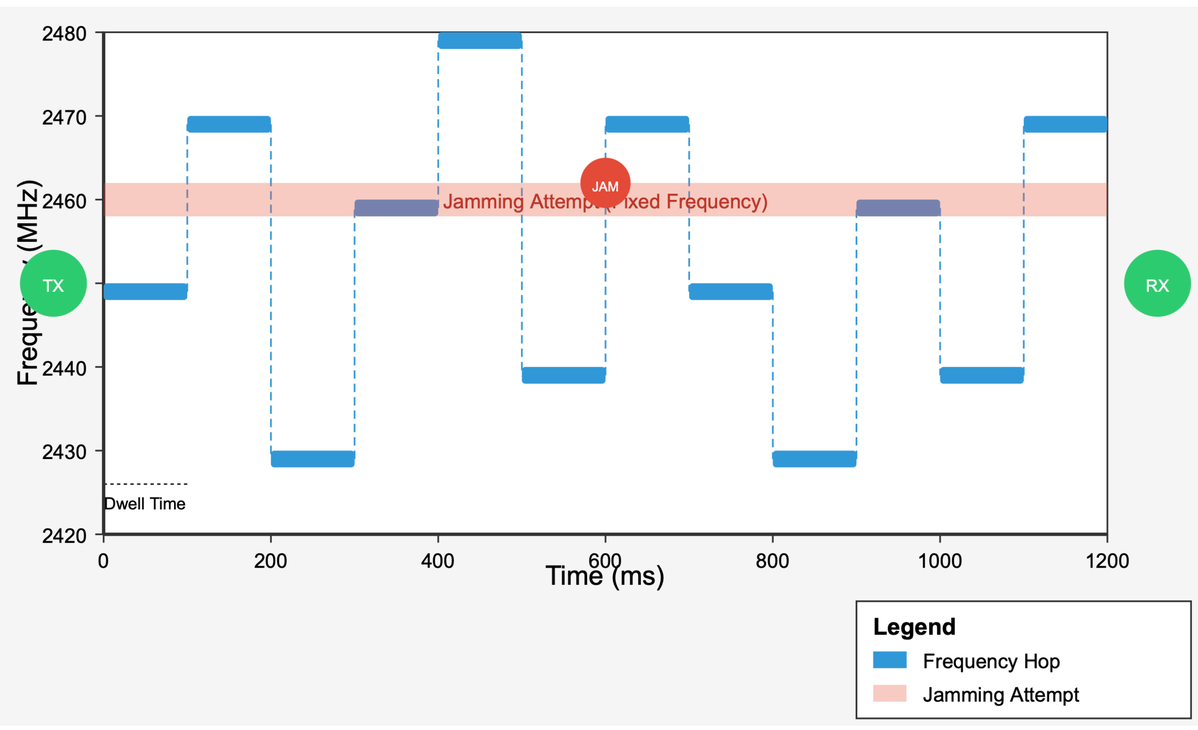
Wednesday, April 23, 2025 11:00 AM

THE CHALLENGE



An intruder sends a signal at the same frequency of the communication system to interfere with radio frequency. For example, someone could jam GPS signals preventing your devices from displaying your route accurately.

THE SOLUTION : FHSS



FHSS, a spread-spectrum technique where the Transmitter (Tx) rapidly switches frequencies in a pseudorandom sequence known to both Tx and Receiver (Rx).

SIMULATION PARAMETERS

* 10 frequencies from 2.4 GHz to 2.6 GHz (ISM band)
* Slow hopping : One freq. per bit duration (1ms)

MATHEMATICAL MODEL

The Tx'd signal for the n^{th} hop interval is :-

$$s(t) = A \cdot \cos(2\pi f_n t + \phi) \cdot d(t)$$

where,

$f_n \in \{f_1, f_2, \ldots, f_N\}$ → hopping frequencies
$d(t) \in \{0, 1\}$ → digital data
ϕ → phase (assumed constant)

Hopping sequence is pseudorandom but synchronized between the Tx and Rx.

WHY FHSS ?

1. Resistant to narrowband interference / jamming
   i.e., if one frequency is jammed, only a few bits are lost.
2. Low probability of interception
   Without knowing the hopping sequence, an eavesdropper cannot reconstruct the signal.

XOR OPERATION

The simulation uses a simple XOR encryption (Symmetric key cryptography) :

$$C = P \oplus K$$

C : ciphertext bit, P : plaintext bit, ⊕ : bitwise XOR, K : key bit

Lets implement 2 key generation approaches :-

1. Random key
   Provides perfect secrecy when key length ≥ plaintext length and used only once.
2. Repeating key
   More vulnerable as the pattern repeats, making cryptanalysis easier.

Real-World Issue : Random key

- for long messages, the key also becomes very large.
- each key must be used exactly once and then discarded, requiring extensive key management.

- In real-world implementations of frequency hopping systems (like bluetooth or military radios), they typically use shorter shared keys and deterministic algorithms to generate the hopping sequences rather than truly random keys.

⇒ Decryption : It works the same way.

$$P = C \oplus K$$

JAMMING MODEL

Let's implement a barrage jamming model where :

- A jammer transmits noise across a specific bandwidth (B_j).
- Jamming occurs when the hop frequency falls within the jammer bandwidth.

i.e frequency, f_n is jammed if $|f_n - f_j| \leq \frac{B_j}{2}$