

### 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).



### MATHEMATICAL MODEL

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

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

where,

$f_n \in \{f_1, f_2, \dots, f_N\} \rightarrow$  hopping frequencies

$d(t) \in \{0, 1\} \rightarrow$  digital data

$\phi \rightarrow$  phase (assumed constant)

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

### WHY FHSS ?

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

