

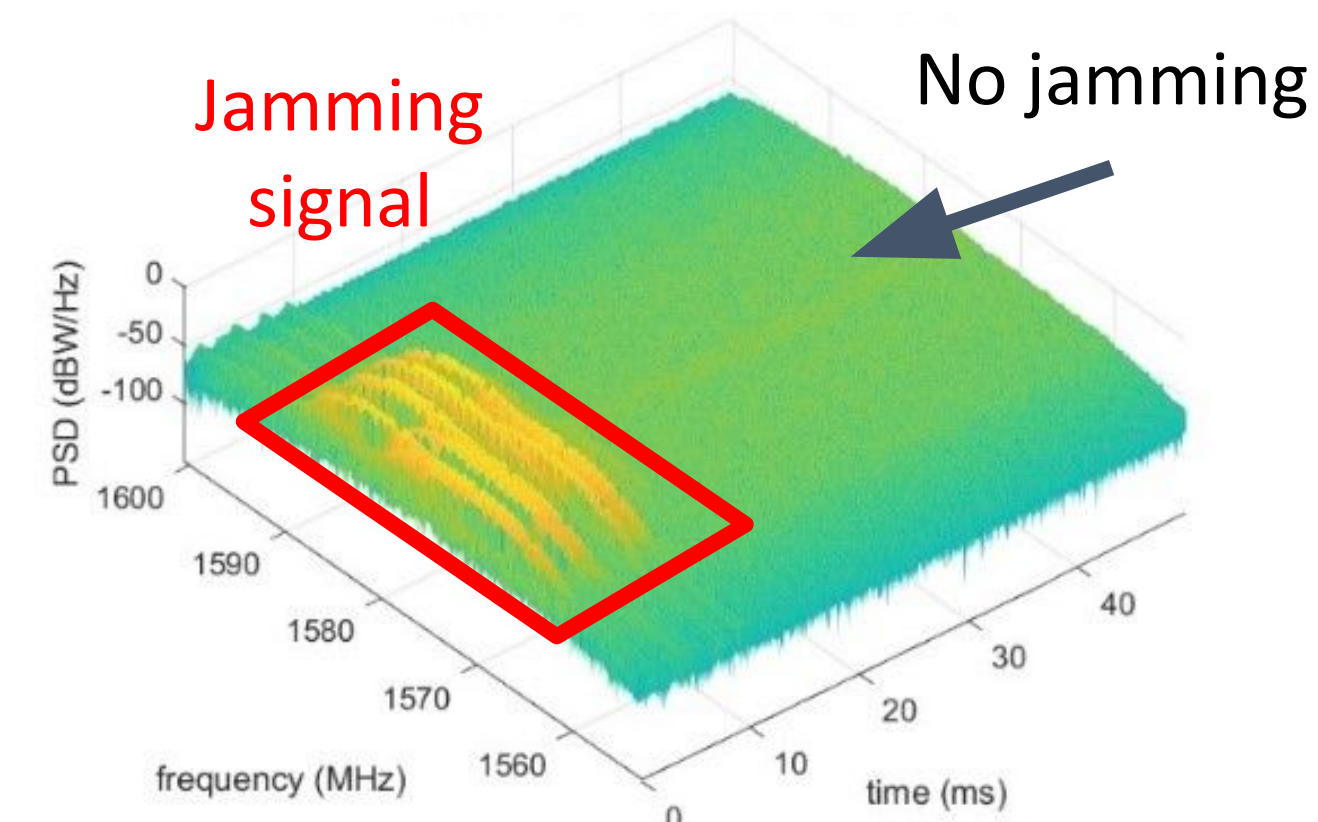


## Why does GPS jamming matter?

- What it is:** GPS jamming is the deliberate transmission of radio signals that interfere with or overpower legitimate signals from Global Positioning System (GPS) satellites, preventing receivers from determining accurate position, time, or velocity.
- How it works:** Jammers exploit the fact that GPS signals are very weak (~ -130 dBm) when they reach earth. By broadcasting stronger noise on the same frequencies, even small, inexpensive devices can disrupt reception over a localized area.
- Economic and societal effects:** Jamming can delay logistics, affect emergency response, and create cascading disruptions in supply chains and public services. Many critical systems, such as power grids, telecom networks, and financial systems, depend on GPS for precise timing. Jamming can potentially lead to outages or degraded performance.
- Legal status:** In many countries, including the U.S., operating or even selling GPS jammers is illegal due to the risk of widespread interference with essential services.



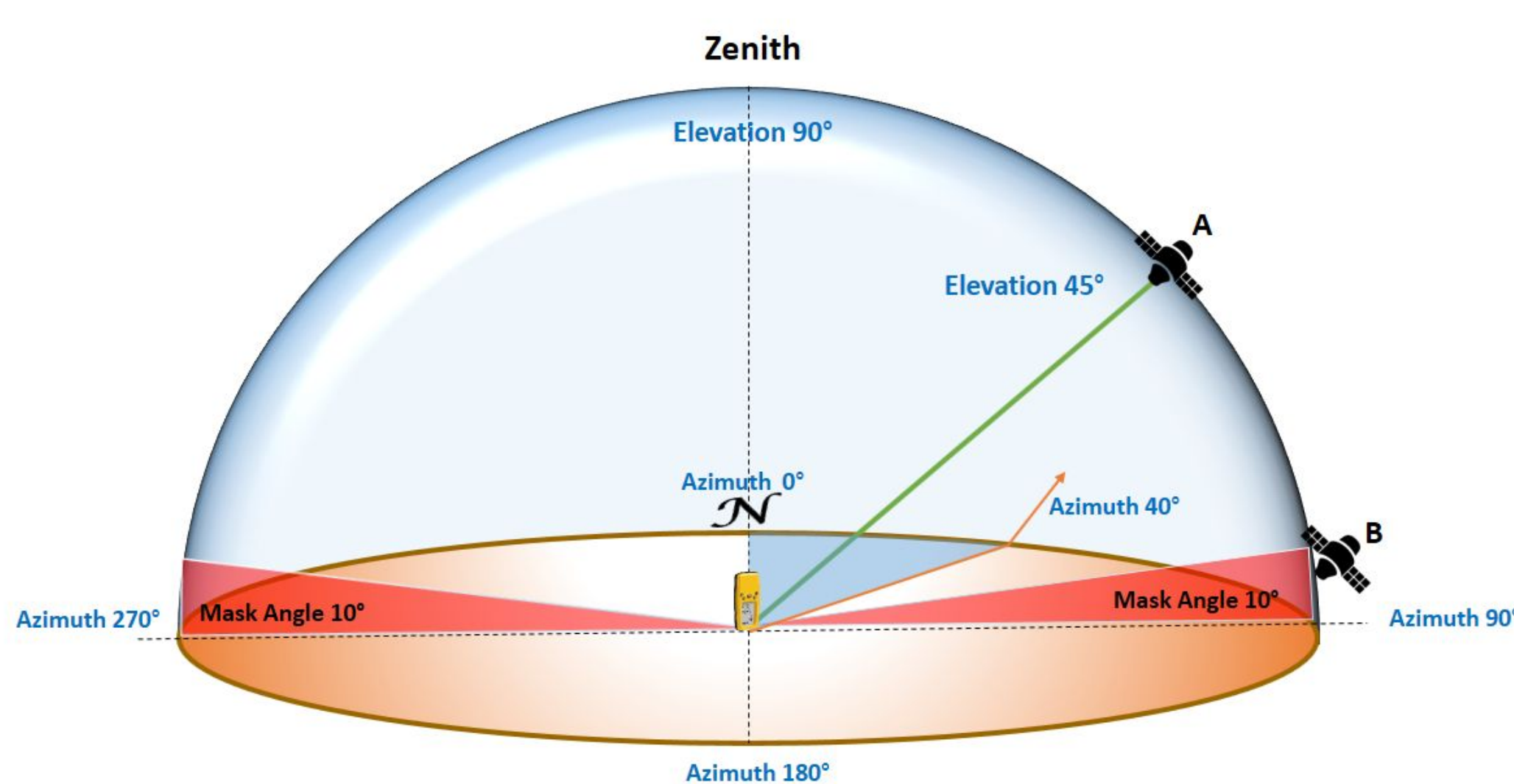
Example of low-cost handheld jamming device



Spectrogram showing GPS L1 (1575.42 ± 7.6725 MHz) band with and without jamming

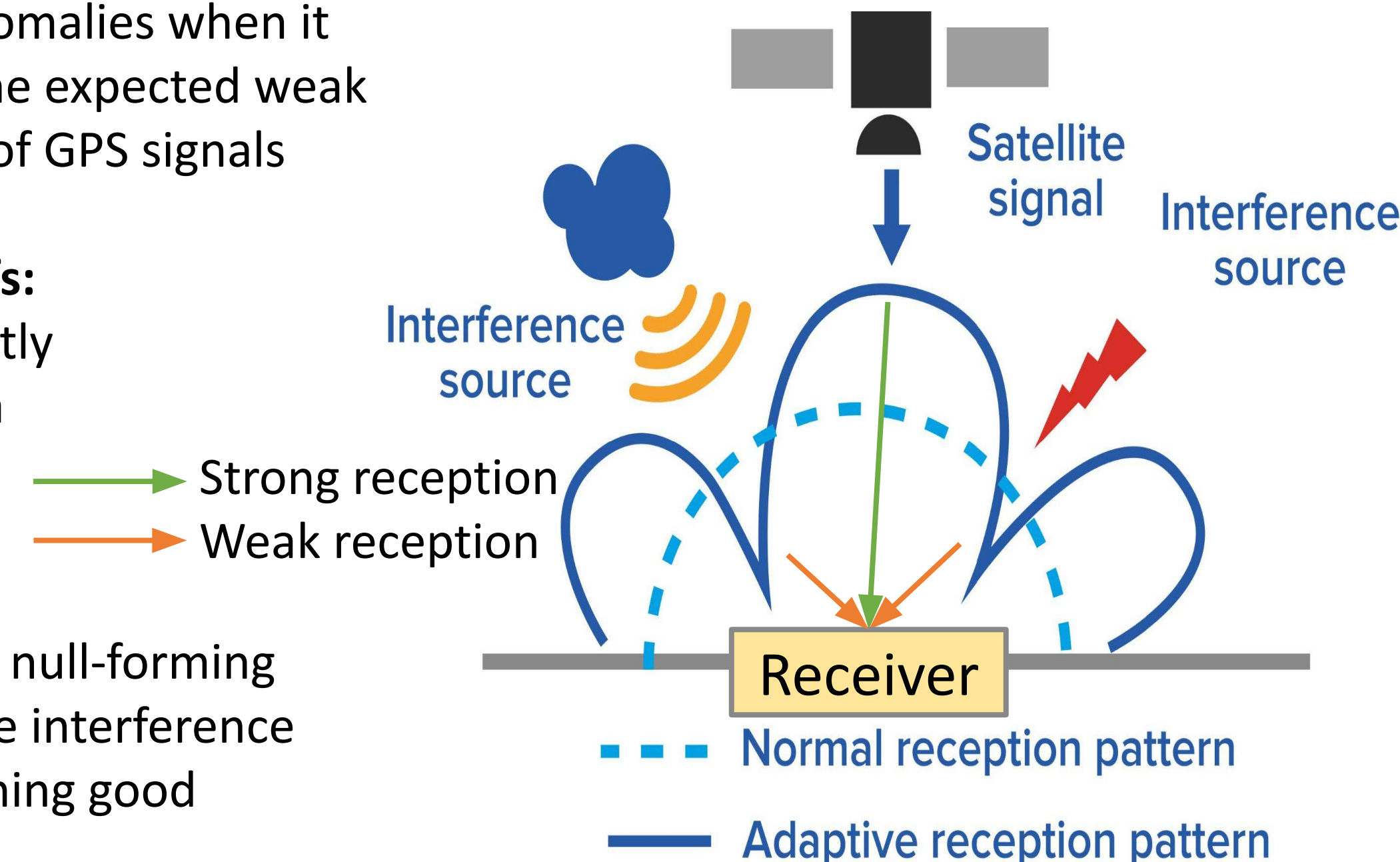
## Problem Statement

Low-cost wideband jammers can overwhelm GPS signals, preventing receivers from **maintaining a reliable position fix**. This project focuses on the elimination of jamming interference to ensure a continuously working GPS system. This issue **impacts critical users** such as transportation, emergency services, defense, and autonomous technologies, where jamming—both accidental and intentional—can **disrupt navigation and safety**. A robust, low-cost solution is needed to maintain GPS functionality in these environments.



## Proposed Solution: Adaptive Nulling with CRPA

- What CRPA is:** A Controlled Reception Pattern Antenna (CRPA) is a multi-element antenna system designed to protect receivers from interference, especially jamming and spoofing.
- Multiple antenna elements:** Instead of a single antenna, the proposed CRPA uses an array (4 elements). This allows the system to compare signals arriving from different directions and process them intelligently.
- Adaptive nulling:** The core anti-jamming feature where the CRPA electronically creates “nulls” (directions of very low reception) toward a jammer, suppressing interference while keeping satellite signals intact.
- Jamming detection:** GPS jamming can be detected by monitoring the received signal power and flagging anomalies when it significantly exceeds the expected weak baseline levels typical of GPS signals at Earth's surface.
- Performance trade-offs:** Creating nulls can slightly reduce overall antenna gain or distort the reception pattern (affecting GPS reception strength), so null-forming algorithm must balance interference rejection with maintaining good satellite coverage.



## Adaptive Nulling

- Forming reception pattern:** The receiver applies adjustable phase shifts (time delays) to each antenna channel before combining them, which shapes the overall reception pattern as signals coming from different directions interfere constructively or destructively.
- Interference estimation:** The reception pattern, termed array factor (AF) is calculated by combining the phase factors for each antenna channel as:

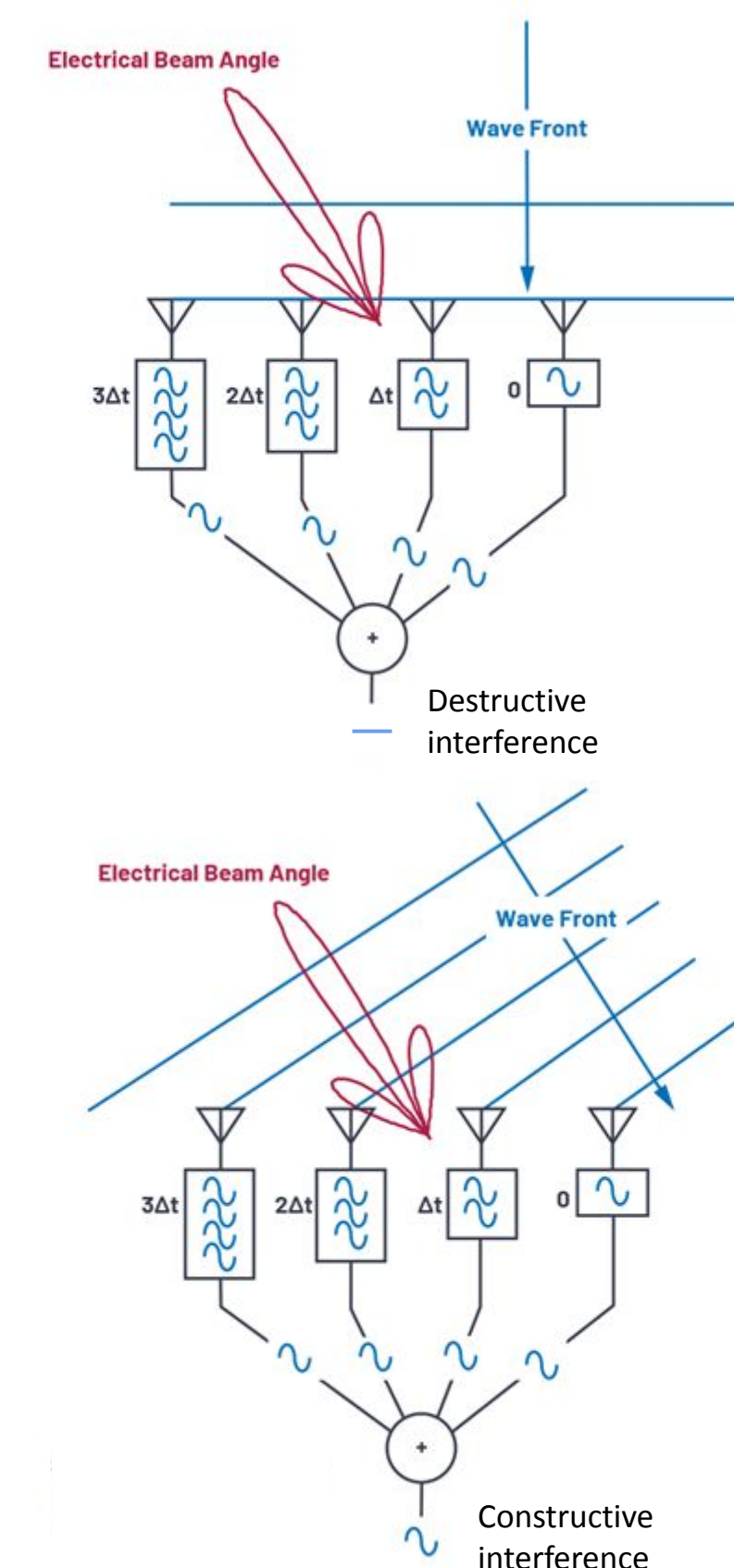
$$AF(\theta, \phi) = \sum_{m=0}^1 \sum_{n=0}^1 e^{j[kd(m \sin \theta \cos \phi + n \sin \theta \sin \phi) + \phi_{m,n}]}$$

where

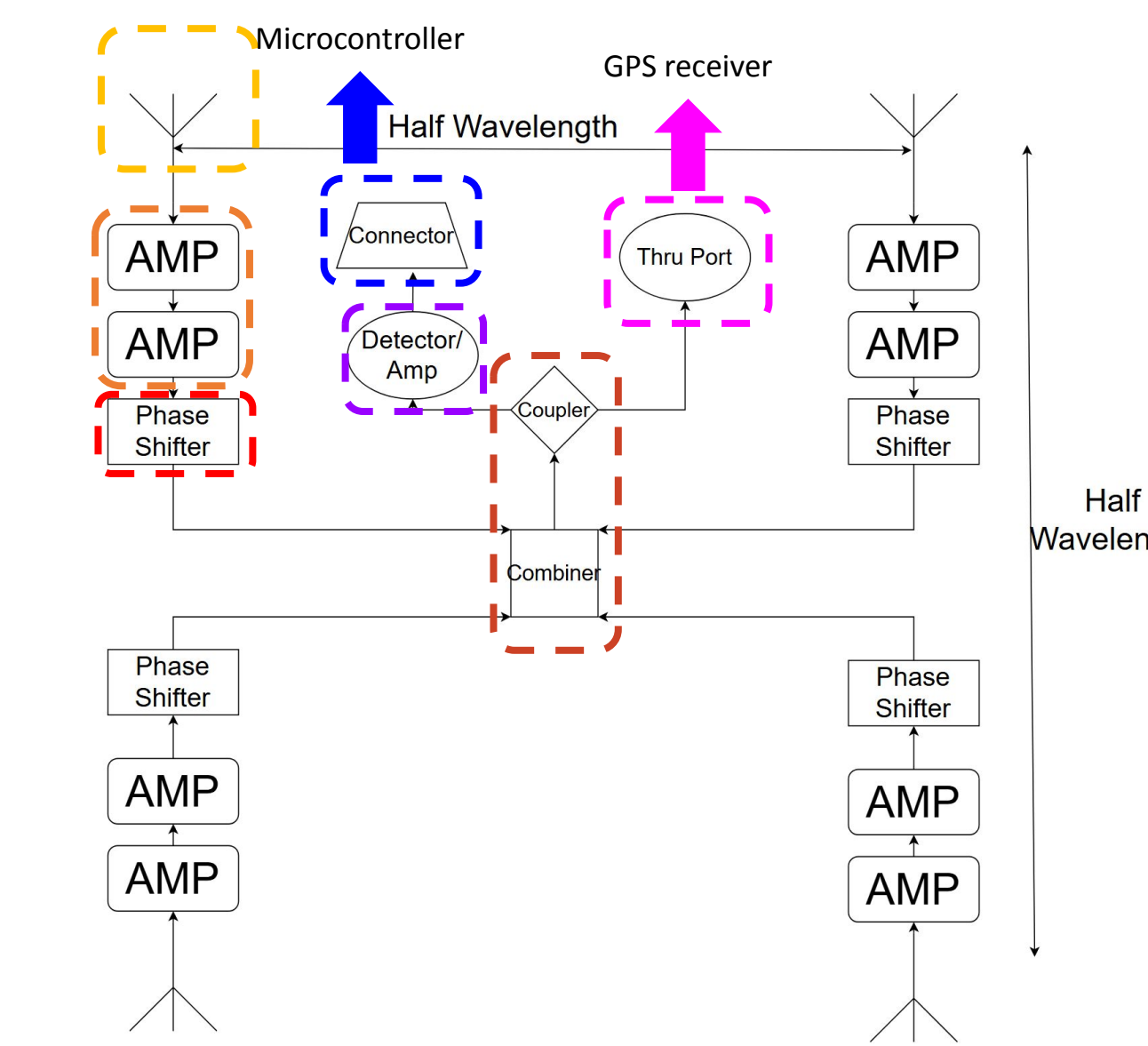
- $m, n$  : antenna index in the  $x$ - and  $y$ -directions
- $k$  : wave number ( $2\pi/\lambda$ ) where  $\lambda$  is the wavelength
- $d$  : distance between two adjacent antennas
- $\theta$  : elevation angle
- $\phi$  : azimuth angle
- $\phi_{m,n}$  : phase shifter phase for antenna at  $(m, n)$

A genetic algorithm search for the phase factor combinations to produce nulls with a resolution of 5° in the azimuth and 5° in the elevation. A codebook containing the different combinations of phase shift values and corresponding null elevation and azimuth angles.

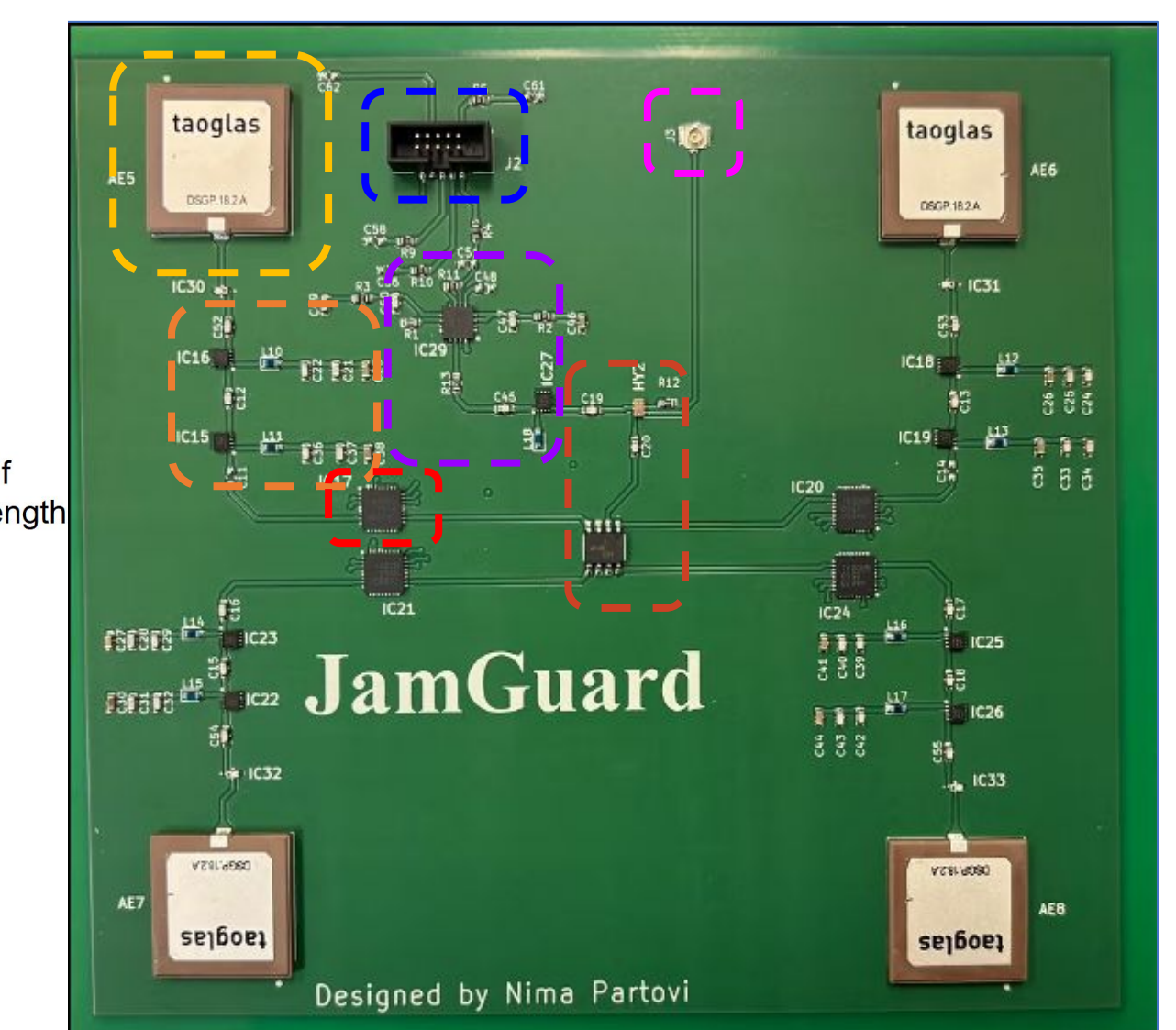
- Continuous adaptation:** The phase factors are updated in real time as the environment changes, allowing the nulls to track interference sources dynamically.
- Hardware integration:** Received signal power is continuously monitored for any jamming. When jamming is detected, a microcontroller uses the precomputed codebook and applies the phase values in sequence to steer the null until the interference is suppressed.



## Design and Measurements



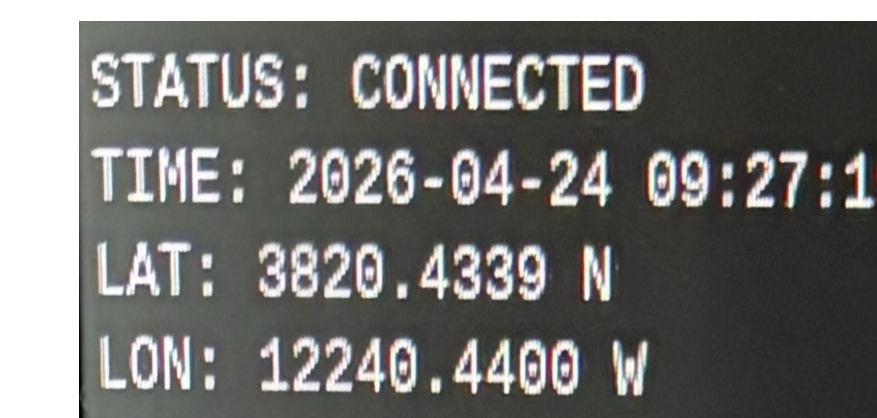
System block diagram



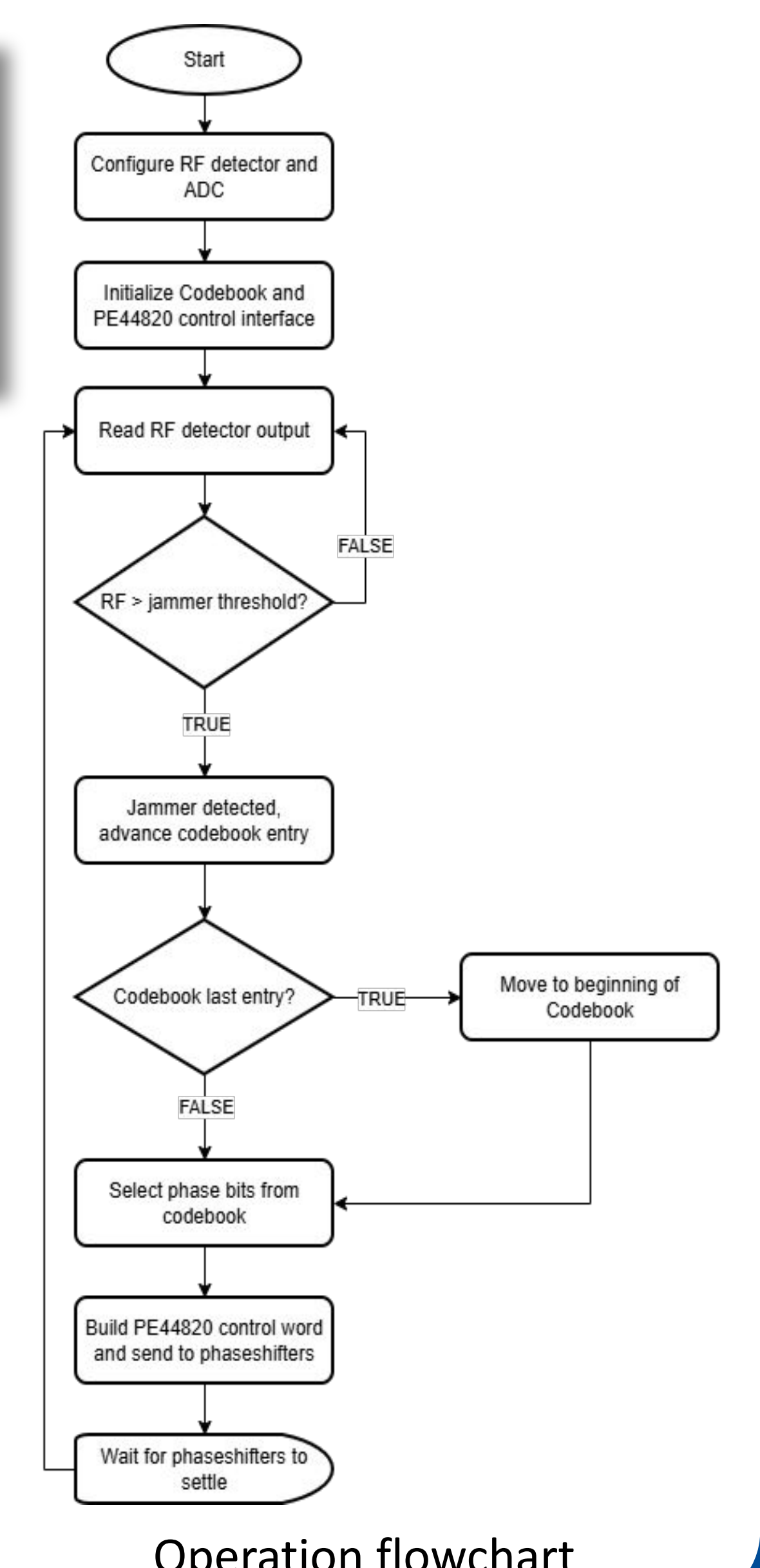
Fabricated Jam Guard PCB



Output impedance measurement



GPS connectivity test



Operation flowchart

## Future Work

- Perform testing in real-world environments (near interference sources)
- Improve impedance matching to achieve true 50 Ω across RF chain
- Miniaturize PCB board for increased mobility
- Further develop system for multi-jammer scenarios
- Expand to combat GPS spoofing and meaconing

## Acknowledgements

We want to acknowledge funding from the Center for Environmental Inquiry (CEI) at Sonoma State University: **The Norwick Memorial Fund**