

Beamforming Phased Array for GPS Spoofing

Adam Chapman (EE)
Noel Hwang (EE)
Alec Koudijs (CS)

Context

Drones have fallen into the wrong hands. These unmanned aerial vehicles have been increasingly used for illicit activities and pose a threat to national security.

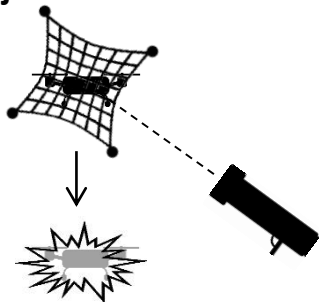
Problem

Current countermeasures give an inadequate level of control over rogue drones, which can result in collateral damage.

Jamming

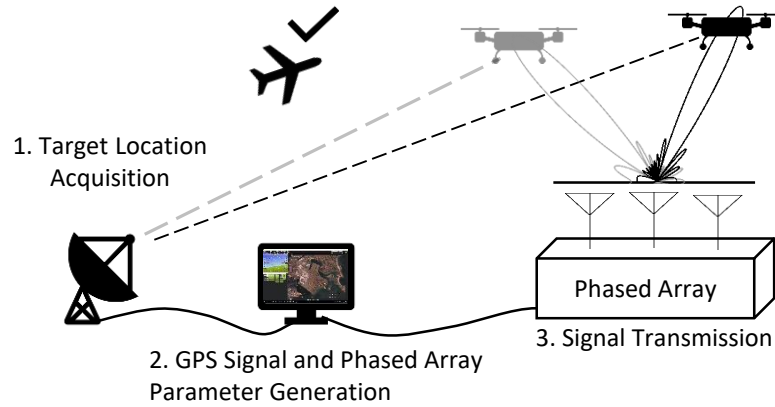


Projectiles



Our Solution

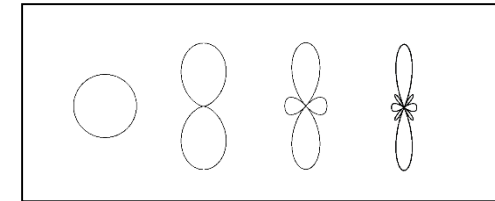
We exploit GPS vulnerabilities found in many commercially available drones to redirect targets for safe containment. Further, by using a phased array to transmit the spoofing GPS signal, we can limit the scope of the attack to the desired target and avoid fratricide.



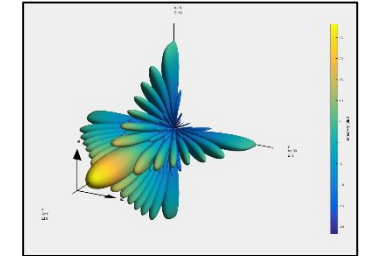
The simulated flight path of a spoofed drone over Boston Logan International Airport.
Left: (Purple) Spoofed location experienced by the Drone, (Black) Position Data from Real GPS satellites, (Yellow) Programmed flight path.
Right: (Pink) Overlay of actual flight path of the drone.

What is a Phased Array?

A phased array is an array of transmitting or receiving elements, such as speakers, microphones, or antennae. By utilizing multiple elements, the array is capable of spatially restricting radiation (**beamforming**). Adjusting the phase or time delays to the individual elements enables beamsteering, in which the direction of greatest radiation or reception can be aimed.



Radiation patterns for linear arrays consisting of one, two, three, and five omnidirectional radiators



Radiation pattern for a planar array

What is GPS Spoofing?

GPS spoofing is the process of taking over a receiver by transmitting false GPS signals. Once the satellite signals are replaced with the spoofer's signals, the spoofer may adjust the timing of each one, resulting in a new position being reported by the receiver.

- 1) Normal GPS Reception
- 2) Spoofing Signal Locked On
- 3) False Location Acquired

