J240332

UNDER $300 ANTI-DRONE GUN WITH GPS SPOOFING TECHNIQUE USING COTS

Pirada Techavijit*, Polkit Sukchalerm, Montawat Pitchsanupun, Natcha Kijatanath

*Corresponding Author: pirada.te@kmitl.ac.th

ABSTRACT

This research presents the development of a cost-effective anti-drone gun. The system utilizes Commercial Off-The-Shelf (COTS) components for scalability and rapid development. The system employs GPS spoofing using Software-Defined Radio (SDR) devices, offering a straightforward and energy-efficient solution compared to other complex anti-drone techniques. The prototype successfully manipulates coordinates, tricking commercial drones into autonomously landing in designated zones, showcasing a practical and resource-efficient approach to drone deterrence

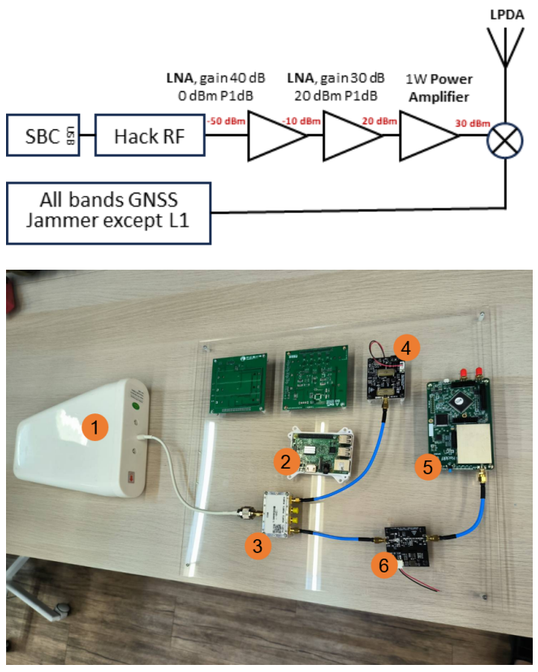
KEYWORDS

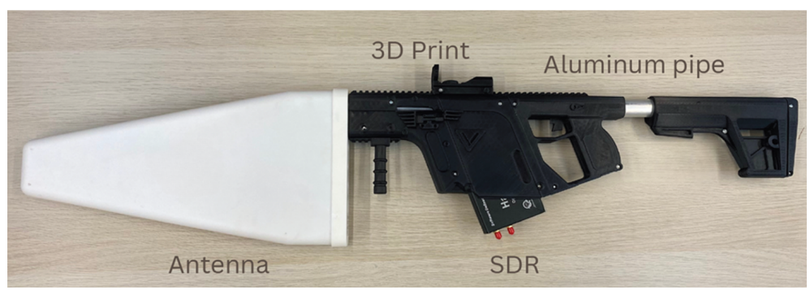
Anti-drone
UAV
GPS spoofing
Signal jamming

IMPLEMENTATION METHOD

In this research, **GPS Spoofing** is chosen to be the main technique as it requires less power and is less complex compared to other systems. Moreover, it poses a lower risk of harm to other objects in the sky.

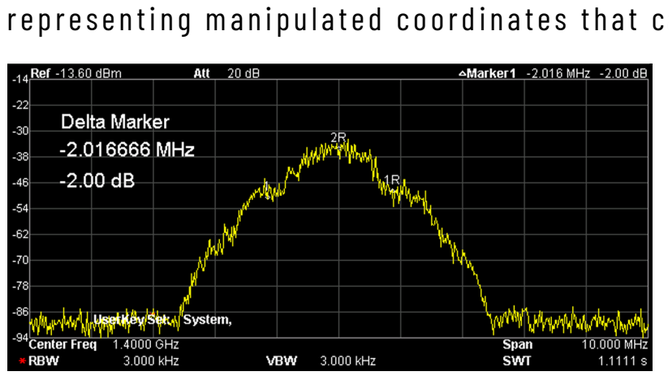
(1) Log-periodic antenna (LPDA): is a directional antenna that able to operate over a wide band of frequencies, suitable for emitting signals at various frequencies used by drones.
(2) Single board computer: This device controls the HackRF for emitting signals at the desired frequency. It can be a Raspberry Pi or any single board computer compatible with Windows OS.
(3) RF Combiner: An equipment that combines signals send to the LPDA for broadcasting.
(4) All band GNSS jammer except L1: This device generates signals interference across all GNSS frequency bands except L1 to prevent the GNSS module on the drone from receiving signals from real GNSS other than the anti-drone gun.
(5) HackRF: A wideband software-defined radio (SDR) transceiver capable of converting digital data into RF at the desired frequency.
(6) Pre-Amplifier and Power Amplifier (PA): Used to boost the signal amplitude emitted from the HackRF sufficiently to reach the drone.

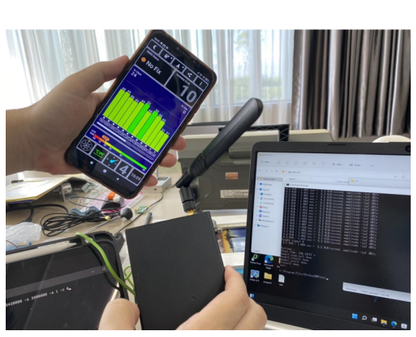




THE ANTI-DRONE GUN PROTOTYPE

GPS Spoofing will be generated by using the GPS-SDR-SIM software, which from a broadcast ephemeris file and can specify the location. and this research use an airport. The spoofed coordinates can be converted to RF using a software-defined radio (SDR) like HackRF. The resulting signals are specific to the L1 GPS part, operating at 1575.42 MHz, representing manipulated coordinates that can be user-defined.





BUDGET ON COMPONENT ON ANTI-DRONE GUN SYSTEM

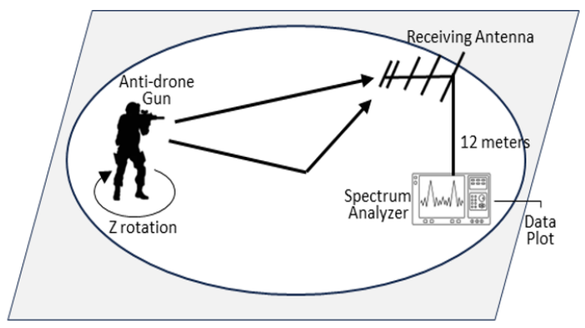
BUDGET ON COMPONENT ON ANTI-DRONE GUN SYSTEM

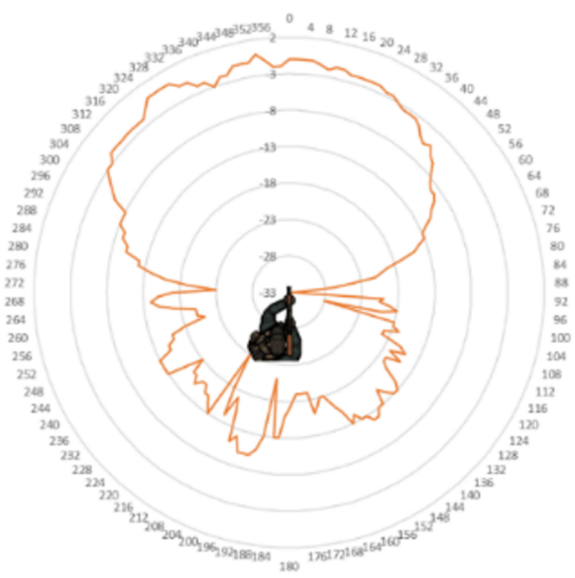
Component	Budget ($)
Structure: 3D Printers and aluminum pipe	13
HackRF	85
LPDA antenna	22
Pre-Amplifier & Power Amplifier	14
Single board computer	70
GNSS jammer	42
Combiner	16.75
Battery	20
Total	282.75

RESULT & CONCLUSION

RADIATION PATTERN TESTING

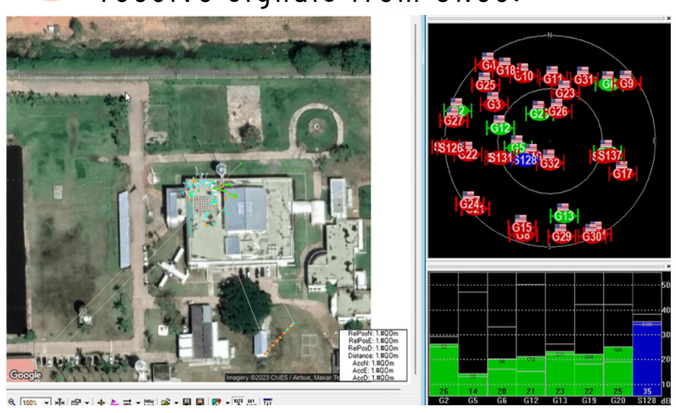
Measuring the radiation pattern of the signal transmission from the anti-drone gun is used for determining the direction, and characteristics of the propagated signal. The technique used in this paper is the open-area testing site (OATS) of the L-band frequency range. The testing setup includes the receiver situated above the ground at 12 meters, simulating a drone in the sky, and the anti-drone gun. The transmitter rotates from 0 to 360 degrees, while the receiver record signal strength amplitude in dBm from a spectrum analyzer, then plotted into a graph.
The radiation pattern is a 60- degree spread angle at the 3 dB beamwidth and a front-to-back ratio of -18 dB. This semi-directional propagation can cause signal interference and GPS spoofing over a wide angle, making it easier to aim the gun at the intended target. However, there may be risks of unintended interference with other devices, which is a factor that should be considered and improved upon in the future.





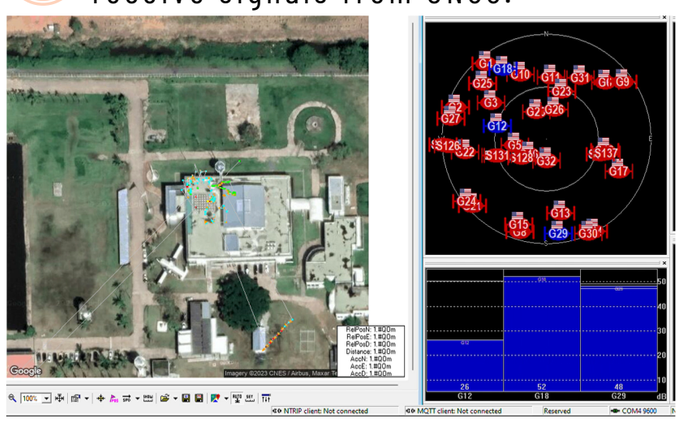
GPS SPOOFING RESULT

1 Enable the GNSS receiver module to receive signals from GNSS.



2 activate GPS spoofing from the anti-drone gun

3 The GNSS receiver fails to receive signals from GNSS.



This research discusses the design and development of a low-cost Anti-drone gun produced with Commercial Off-the-Shelf (COTS) components, utilizing GPS spoofing generated by Software-Defined Radio (SDR) in conjunction with LPDA. The system can counteract drone navigation systems through GPS by employing Spoofing-to-Signal (Sp/S) signal strength of 20 dB. It can induce GPS into a non-fixed state within 4 seconds and mislead the coordinates within 1 minute. In the experimentation phase, simulated misleading coordinates were created within an airport zone, causing immediate landing for commercial drones.

4 The receiver's coordinates change to the spoofed position.