Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter

Eric Horton, Jaya Preethi Mohan*, Prakash Ranganathan

School of Electrical Engineering and Computer Science

University of North Dakota, Grand Forks, ND-58202

INTRODUCTION

This research models a Global Positioning System (GPS) spoofing attack set-up, and investigation of defense mechanisms using available open-source software, and hardware.

The GPS spoofing attack and defense architecture is focused on application to a DJI Matrice 100 Quadcopter. Only the L1 (civilian) GPS frequency is used.

Key terms: GPS, Spoofing, DJI Matrice, Cyber attack, RF, Kalman Filter Model.

GPS SPOOFING ATTACK - SETUP

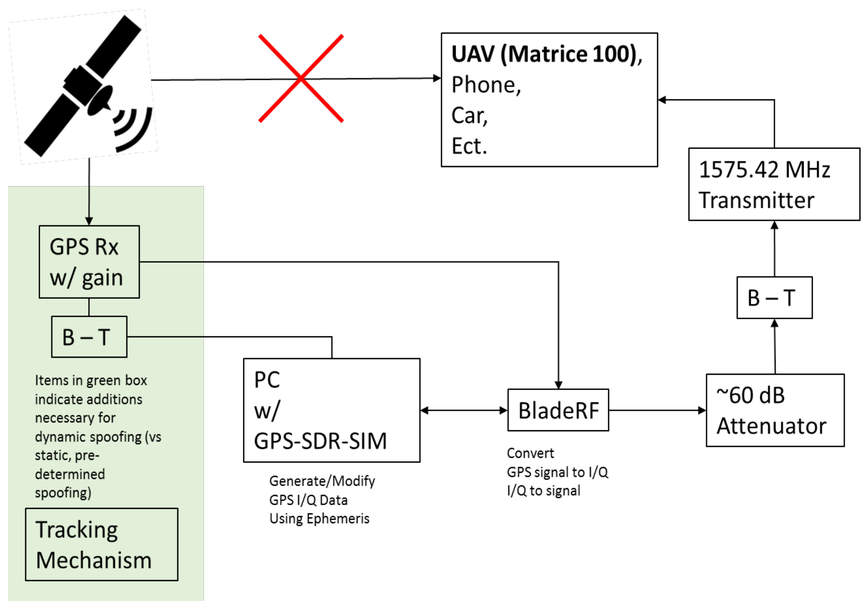

Figure 1 GPS Spoofing Attack Simulation

GPS SPOOFING DEFENSE- METHODS

UAV Sensors to GPS comparison (investigated)

- Accelerometer & Gyroscope
- Kalman Filter + Camera (work-in-progress)

Synthetic Antenna Array -- Movement (future work)

- Monitor Amplitude/Phase correlation of different PRNs

Signal to Noise Ratio (work-in-progress)

- Spoofing increase of SNR (carrier to noise)

Other Methods (future work)

- Absolute Power Monitoring (additional hardware)
- Power versus receiver movement (additional hardware)
- L1/L2 Comparison (additional hardware)

HARDWARE/SOFTWARE REQUIREMENTS

Hardware

- 1575.42 MHz Passive Garmin Antenna
- BladeRF Software Defined Radio
- Laptop running Windows
- 60dB attenuator
- 2 x Bias tee (1 for dynamic spoofing)
- Active GPS Antenna with LNA (dynamic spoofing)
- Matrice 100
- DJI Quadcopter to be spoofed
- Added ESP8266 Wifi module for communication.

Open-Source Software

- GPS-SDR-SIM
- GNSS-SDR (dynamic spoofing)
- DJI Onboard SDK
- Modified UDP socket for communication with Matrice 100 over Wifi.

GPS SPOOFED SNAPSHOT

Figure 2: GPS Spoofed Matrice 100 Data Output

Figure 3: Dynamic Spoofing Signal Generation

KALMAN FILTER MODELING

Only accelerometer/gyroscope vs GPS receiver simple comparison method currently implemented.

- Kalman filter implemented, minor improvement without additional sensors (Camera)

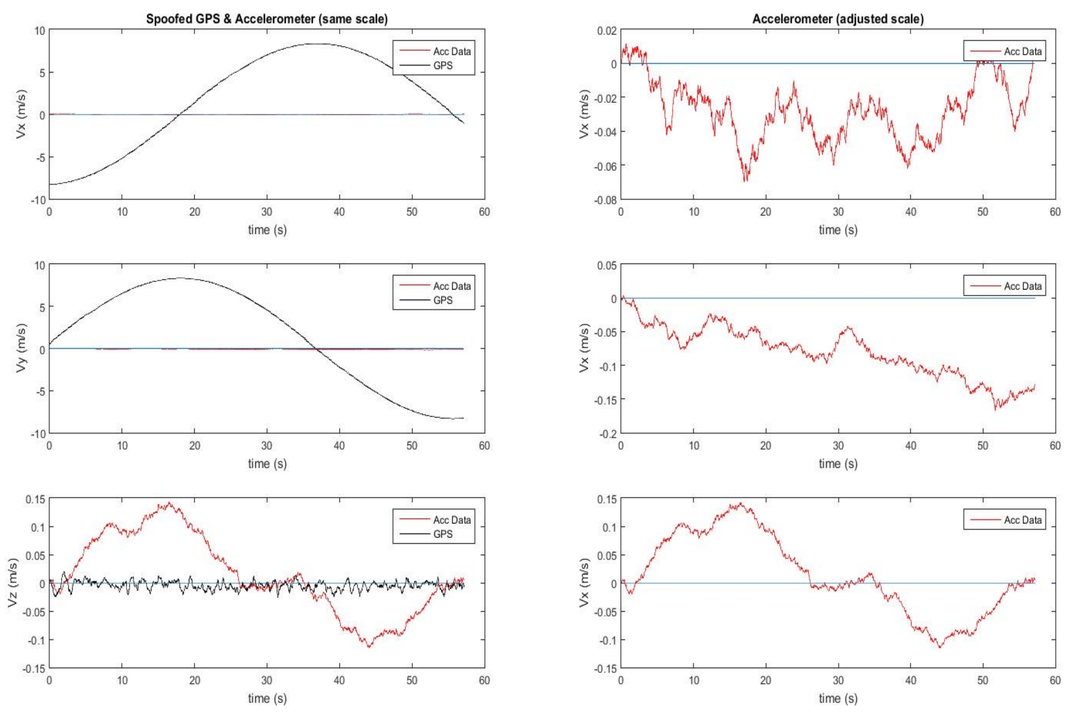

Figure 4 Kalman Filter Modeling Results

DEFENSE – FUTURE WORK

Implementation of signal to noise ratio measurements. Requires decomposition of incoming GPS signal (GNSS-SDR).Correlation measurement between signal parameters when moving (synthetic antenna array). Requires decomposition of incoming GPS signal (GNSS-SDR). Expand upon sensor comparison

- Kalman filter than includes camera movement approximation.
- Create dynamic spoofing setup using static spoofing building blocks
- Modify GPS-SDR-SIM software to generate continuous I-Q data output
- Create real time pipe from GPS-SDR-SIM output to BladeRF.
- Use GNSS-SDR to decompose incoming GPS signal into stream for GPS-SDR-SIM input.

CITATION

Horton, Eric, and Prakash Ranganathan. "Development of a GPS spoofing apparatus to Quadcopter." The Journal of Global Positioning Systems 16, no. 1 (2018): 1-11. attack a DJI Matrice 100 .

*Poster creator (Non Author)

CONTACT

Jaya Preethi Mohan
Master of Science in Computer Science Student
School of Electrical Engineering and Computer Science
Email:jayapreethi.mohan@und.edu

DATA, ENERGY, CYBER AND SYSTEMS

School of Electrical Engineering & Computer Science
UNIVERSITY OF NORTH DAKOTA