Investigation of a GPS Spoofing Attack

College of Engineering & Mines
University of North Dakota
Rockwell Collins

School of Electrical Engineering & Computer Science
University of North Dakota

Eric Horton, Dr. Prakash Ranganathan, Electrical Engineering

ABSTRACT

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.

SPOOFING ATTACK HARDWARE/SOFTWARE

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

REFERENCES

[1] OSQZSS, "GPS-SDR-SIM," Github/Takuji Ebinuma, 2015. [Online]. Available: https://github.com/osqzss/gps-sdr-sim.

[2] T.TAKASU, "RTKLIB: An Open Source Program Package for GNSS Positioning," 2013. [Online]. Available: http://www.rtklib.com/.

[3] Nuand, "bladeRF," Nuand, 2016. [Online]. Available: https://github.com/Nuand/bladeRF.

[4] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," International Journal of Navigation and Observation, vol. Volume 2012, pp. Article ID 127072, 16 pages, 2012.

[5] H. Lin and Y. Qing, "GPS SPOOFING: Low-cost GPS simulator," in Defcon 23, Las Vegas, 2015.

[6] K. Wang, S. Chen and A. Pan, "Time and Position Spoofing with Open Source Projects," Mobile Security of Alibaba Group.

[7] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen and S. Capkun, "On the Requirements for Successful GPS Spoofing Attacks," in 18th ACM Conference on Computer and Communications Security, Chicago, 2011.

[8] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song and H. Li, "A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids," IEEE TRANSACTIONS ON SMART GRID, Vols. VOL. 6,, no. NO. 6, NOVEMBER 2015.

[9] CTTC, "GNSS-SDR," CTTC, 2016. [Online]. Available: http://gnss-sdr.org/project.

GPS SPOOFING ATTACK - SETUP

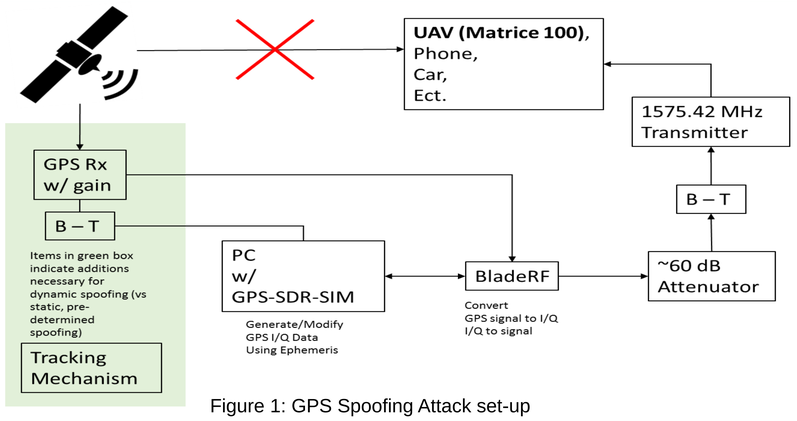

Figure 1: GPS Spoofing Attack set-up

ATTACK - RESULTS

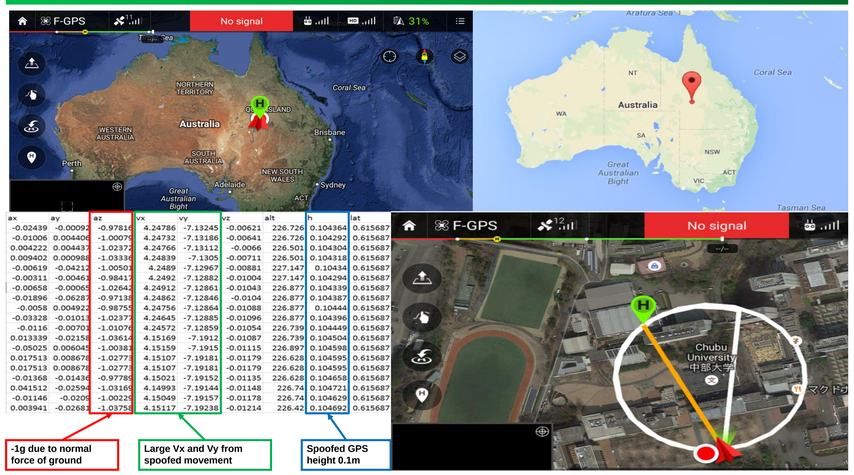

Figure 2: GPS Spoofed Matrice 100 Data Output

ATTACK – FUTURE WORK

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

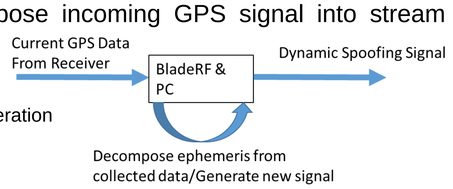

Figure 3: Dynamic Spoofing Signal Generation

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)

DEFENSE - RESULTS

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

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

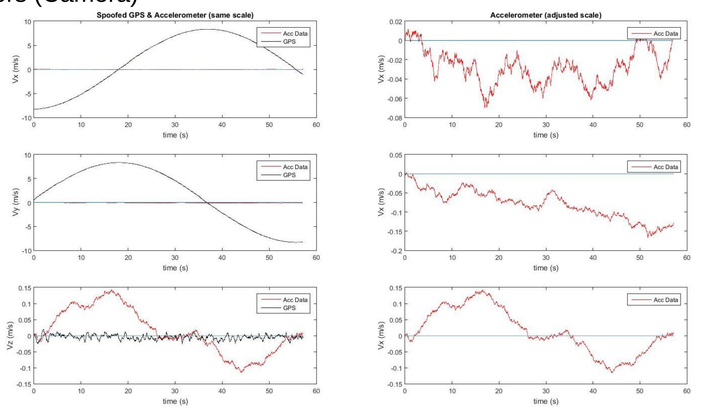

Figure 4: Accelerometer/Gyroscope vs Spoofed GPS Reciever

DEFENSE – FUTURE WORK

Begin implementation of signal to noise ratio measurements

- Requires decomposition of incoming GPS signal (GNSS-SDR)

Begin 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