Understanding and Mitigating the Impacts of GPS/GNSS Vulnerabilities

Overview and Problem Statement

The Global Positioning System (GPS) is the mostly widely used example of what are more broadly known as Global Navigation Satellite Systems (GNSS). GPS provides precise location and time information to any receiver capable of receiving and decoding the timing signals from at least 4 satellites in the GPS constellation. The civilian GPS signal does not come with any authenticators and, given the relatively low signal strength, is vulnerable to intentional or malicious jamming from land-based transmitters. The application of GPS devices in the power sector can potentially have significant impact on the bulk electric system through their integration into synchronization devices such as Phasor Measurement Units (PMUs). Given that PMU technology is expected to transition to control applications in the future and that the primary time synchronization mechanism used by PMUs (today) is GPS, there is growing concern that a dependency on GPS will introduce a built-in vulnerability into the infrastructure.

Research Objectives

- Develop a hardware-based testbed capable of investigating the resiliency of various PMUs to known GPS spoofing attacks.
- Demonstrate the feasibility of an attack using that hardware setup.
- Investigate possible detection and mitigation schemes to harden PMUs to GPS spoofing attacks.
- Understand the timing and synchronization needs in power system applications.
- Develop a trustworthy GNSS-based timing source that is more spoofing-resilient than current GPS-based clocks.
- **Smart Grid Application Area:** This research will allow for a more secure and reliable power grid.

Technical Description and Solution Approach

- The synchronization of PMUs depends on GPS signals, which are unauthenticated.
- Multi-layer scheme for secure GPS-based timing: Investigate eight countermeasures in three layers: GPS raw signals layer; semi-processed signal layer; and fully processed signal layer.
- Use the fact that the GPS receivers are static to further improve the accuracy and robustness of GPS-based timing.
- Have multiple GPS receivers at different locations cross-check for anti-spoofing.
- Continue development of a GPS simulator using an NI PXI platform to be interfaced to the PMUs in the TCIPG testbed.

Results and Benefits

- Have investigated and implemented Position-Information-Aided Vector Tracking Loop, and have demonstrated:
    - Robustness against jamming with 5dB more noise tolerance compared with scalar tracking;
    - Capability of successfully detecting meaconing attacks;
    - Improvement of the accuracy of the timing solutions when compared with traditional scalar tracking (15 ns vs. 50 ns).
- Have explored cross-checking GPS military P(Y) codes among multiple GPS receivers at different locations, and have shown:
    - Anti-spoofing robustness grows exponentially with the number of cross-check receivers;

    - A modest number of low-cost unreliable receivers can outperform a high-end secure cross-check receiver.
- A hardware-based testbed is being created to investigate effects of spoofing on PMUs.
- **Technology Readiness Level:** Ongoing research.

Researchers

- Grace Gao, gracegao@illinois.edu
- Jonathan J. Makela, jmakela@illinois.edu
- Alejandro Domínguez-García, aledan@illinois.edu
- Daniel Chou, dchou3@illinois.edu