GOALS

- Investigate possible detection and mitigation schemes to harden PMUs against spoofing, jamming, and receiver errors.
- Develop a hardware-based test-bed capable of investigating the resiliency of various PMUs to known GPS spoofing attacks.
- Develop a trustworthy GNSS-based timing source that is more spoofing-resilient than current GPS-based clocks.

BACKGROUND

- GPS provides accurate time and frequency sources for power systems applications.
  - Time accuracy ~100ns
  - Frequency accuracy ~1x10^{-12}
  - Civil GPS signals are freely available.
  - GPS receivers are inexpensive.
- Civil GPS signals are unencrypted, with their structures explicitly described in publicly available documents.
- An attacker can broadcast counterfeit GPS signals and manipulate victim receivers’ time and frequency solutions.

RESEARCH PLAN

- Multi-layer scheme for secure GPS-based timing:
  - Investigate eight countermeasures in three signal layers: GPS raw signals; semi-processed signals; and processed signal.

  Signal conditioning:
  - Check signal power
  - Cross-correlation of military P(Y) code between receivers
  - Narrow-band tracking loops
  - Multi-receiver vector tracking loops

  Navigation data decoding:
  - Check navigation data against external archives
  - Reverse-calculate satellite positions and compare them with navigation data

  Position & time calculation:
  - Check position solution against known PMU locations
  - Check time solution against learnt statistics of receiver clocks

- Investigation and development of countermeasure [C2]:
  - Use the fact that the publicly-known C/A signal and encrypted P(Y) signal are quadrature-modulated onto the same carrier. Encrypted P(Y) signal is used for cross-correlation spoofing detection.

- Investigation and development of countermeasures [C3, C4, C7]:
  - Use the fact that the GPS receivers are static at known locations to further improve the accuracy and robustness of GPS-based solutions.
  - Cross-check against multiple GPS receivers at different locations.
  - Investigate the impacts of attacks on a PMU’s time source using the real-time digital simulator (RTDS) in the TCIPG testbed.

MULTI-RECEIVER POSITION-INFORMATION-AIDED VECTOR TRACKING

- Cross-checking GPS military P(Y) codes:
  - Theoretical analysis shows that a modest number of receivers can achieve high spoofing detection performance, even if some of the receivers are unreliable or spoofed.

  Assumption on pairwise check performance: \( \alpha = 0.001 \) and \( \beta = 0.15 \).

  (a) Reliable reference receivers
  (b) Unreliable reference receivers

  \[ \gamma_1 \approx \gamma_0 = 0 \]
  \[ \gamma_1 \approx \gamma_0 = 0.1 \]

EXPERIMENTAL RESULTS

[C2] Conducted experiments at San Francisco, CA; Rantoul, IL; and UIUC. Successfully detected military P(Y) codes in the quadrature channel when cross-correlating snippets between two reliable receivers.

[C3, C4, C7] Conducted experiments using 4 GPS antennas placed at approximately 10m radius. Demonstrated additional 7dB of noise tolerance compared to the traditional scalar tracking approach, and capability of detecting data-level spoofing as well as meaconing attacks.

Investigation of the impacts of attacks on a PMU’s time source using the real-time digital simulator (RTDS) in the TCIPG testbed.

CONCLUSION

- Cross-checking GPS military P(Y) codes:
  - 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.

- Multi-Receiver Position-Information-Aided Vector Tracking:
  - Robust against jamming (additional 7dB of noise tolerance compared to the traditional scalar tracking).
  - Successfully detects data-level spoofing and meaconing attacks.
  - Improves the accuracy of the timing solutions when compared with traditional scalar tracking (1.5ns vs. 7ns).

- Investigation of the impacts of attacks on a PMU’s time source:
  - Voltage phase becomes increasingly unsynchronized. The phase difference increases the longer the spoofing attack is in place.