GPS Multi-Receiver Joint Direct Time Estimation and Spoofer Localization
Sriramya Bhamidipati and Grace Xingxin Gao

GRID VULNERABILITY TO SPOOFING ATTACKS

- GPS provides accurate and precise time synchronization for PMUs to perform wide area monitoring and control
  - GPS time accuracy ~100 ns and frequency accuracy ~10^-12 Hz
- According to IEEE-C37.118.1, to maintain grid stability, the maximum allowable phase angle error is 0.573° (~timing error of 26.5 µs)
- Civil GPS signals are susceptible to malicious spoofing attacks
  - The received signal power is as low as ~130 dBm; the civil signal structure is unencrypted and known to the public
  - An attacker broadcasts counterfeit civil GPS signals and manipulate victim receivers’ time and time drift solutions
- Incidents of GPS spoofing attacks reported in the recent past
  - In 2017, around 20 maritime vessels near the coast of Novorossyssk, Russia were effected by a mass spoofing attack
  - At the ION GNSS+ 2017, numerous devices reported incorrect time and position due to accidental spoofing caused by a leaky simulator

REALISTIC MODEL SIMULATIONS

- Simulated meaconing causing 30 µs time delay is added to authentic data collected in open sky
- Geometry of multiple receivers comply with the Ameren Illinois Power Substation, Kansas, IL
- Our Joint Filter demonstrates spoofer localization to within 3 m and accuracy of GPS time to within 1.5 µs

RESEARCH GOALS

- Address the GPS vulnerability by investigating spoofing attacks that adversely affect PMU accuracy
- Devise algorithms to counteract these attacks, thereby enabling the adoption of GPS/GNSS synchronized PMUs while advancing power grid resiliency

OUR ARCHITECTURE

Key aspects:
- Multiple receivers
  - Geographical diversity
  - Known receiver positions
- Direct Time Estimation (DTE)
  - Directly works in the timing domain
  - Detects spoofing attacks
- Joint Particle and Kalman Filter
  - Locates the ground spoofer

Geographically distributed receivers within power substation

MULTIPLE PEAK VECTOR CORRELATION

- Grid points in the 2-D search space represent the pre-generated clock bias and clock drift candidates
- At each receiver, the presence of multiple significant peaks during vector correlation indicate spoofing attack

OUR RESEARCH RESULTS

- Simulated meaconing causing 30 µs time delay is added to authentic data collected in open sky
- Geometry of multiple receivers comply with the Ameren Illinois Power Substation, Kansas, IL
- Our Joint Filter demonstrates spoofer localization to within 3 m and accuracy of GPS time to within 1.5 µs

IMPACT ON POWER GRID

Performance benefits:
- By implementing our algorithm, the power system would:
  - Provide synchronized phasor measurements up to 100 ns accuracy
  - Reduce the system risks against external timing attacks
  - Ensure continued robust performance even in degraded scenarios.
- Elevate the maturity of wide area monitoring for future power grids

Business benefits:
- Minimal added hardware and infrastructure costs
- Increased timing resilience and precise time synchronization

CONTACTS

- Contact: gracegao@illinois.edu, sbhamid2@illinois.edu

CONCLUSION

- Robust and Secure GPS-based Timing for Power Systems
- GPS Multi-Receiver Joint Direct Time Estimation and Spoofer Localization
- Key aspects: multiple receivers, direct time estimation, joint particle and kalman filter
- Research goals: address GPS vulnerability, devise countermeasure algorithms
- Architecture: multiple receivers, direct time estimation, joint particle and kalman filter
- Results: spoofing attack detection, localization, GPS timing accuracy improvement
- Impact: enhanced grid stability, reduced system risks, improved performance
- Collaboration opportunities: industry partners, additional research collaboration

ACKNOWLEDGMENTS

- Funding support from the U.S. Department of Energy and Homeland Security
- Research contributions from Sriramya Bhamidipati and Grace Xingxin Gao