Understanding and Mitigating the Impacts of GPS/GNSS Vulnerabilities

T. W. Gehrels, X. Jiang, J. J. Makela, A. D. Domínguez-García, G. Gao, and R. Bobba

GOALS

- Model, test, and demonstrate the maximum clock offset achievable on a GPS receiver because of a spoofing attack.
- Demonstrate current vulnerabilities of PMUs and GPS receivers to spoofing attacks.
- Develop techniques for detection and mitigation of attacks on GPS receivers used for PMU reference clock.
- Develop GPS receiver software/hardware designed for PMU applications resulting in added robustness against attacks.

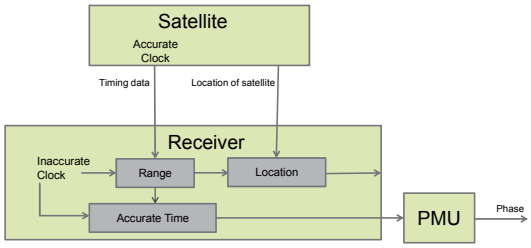
FUNDAMENTAL QUESTIONS/CHALLENGES

- How to design scalable, application-specific GPS receiver software and hardware that take advantage of the additional information available from the PMU network.
- Which techniques are effective at detecting each type of attack on GPS receivers?
- What are the consequences of GPS spoofing attacks on the electrical grid, and how could such attacks be mitigated?

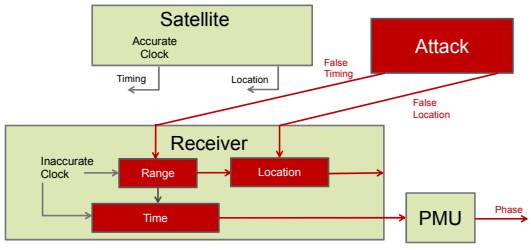
RESEARCH PLAN

- **Data-level spoofing attack optimization:**
  - Derive the changes to the GPS signal data and timing that will maximize the receiver clock offset while keeping changes to receiver perceived position bounded via nonlinear constrained minimization.
- **Attack demonstration:**
  - Generate a false GPS signal using GPS simulator software and hardware in order to demonstrate that receivers will accept the signal as authentic.
  - Demonstrate that a receiver will accept changes to the signal data that do not meet the GPS signal specifications.
  - Demonstrate that a significant receiver clock offset can be introduced via changes to the signal data.

Normal operation

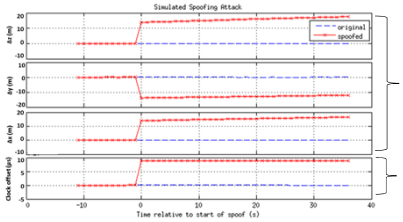


Attack impact



RESEARCH RESULTS

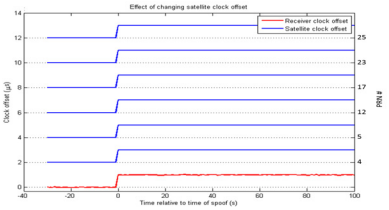
- Maximization of clock bias determined based on user-defined constraints to change in receiver position and data value.



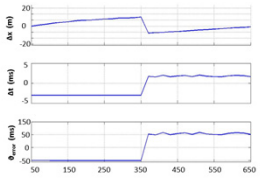
Receiver position bounded to ±15 m change at time of spoof

Change to clock offset maximized at time of spoof (given bounds).

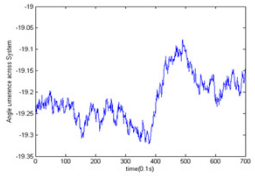
- Implementation of spoofing attack shows that GPS receiver will accept inauthentic signals, and receiver clock offset can be manipulated.



- Receiver clock offset will result in error in PMU phase angle calculation.



Navigation solution with 4 satellites: Clock offset of 8ms leads to the PMU measurement of phase information shifted by half cycle.



Normal angle difference across system: critical angle difference is 45° with 30% margin

BROADER IMPACT

- This research will help accomplish the smart grid vision by providing powerful tools for engineering more reliable and more responsive electrical energy systems.
- The spoofing detection algorithms developed will make the current power system more robust to attacks.
- The methods and tools developed will also help to broaden understanding of cyber-physical systems.

FUTURE EFFORTS

- GPS receiver design, spoofing attack detection and mitigation for PMUs:
  - Design a GPS receiver that uses a multilayer defense scheme to detect and mitigate effects of spoofing.
  - Use PMU communication network to authenticate and verify received data.
  - Consider impact of spoofing attacks on cyber-based control strategies that are likely to become pervasive in distributed systems.
- Identify the impact of PMU timing error on overall system performance when phasor measurements are used in real-time control applications.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T