TCIPG

Understanding and Mitigating the Impacts of GPS/GNSS Vulnerabilities

Secure GPS-based Timing for Power Systems

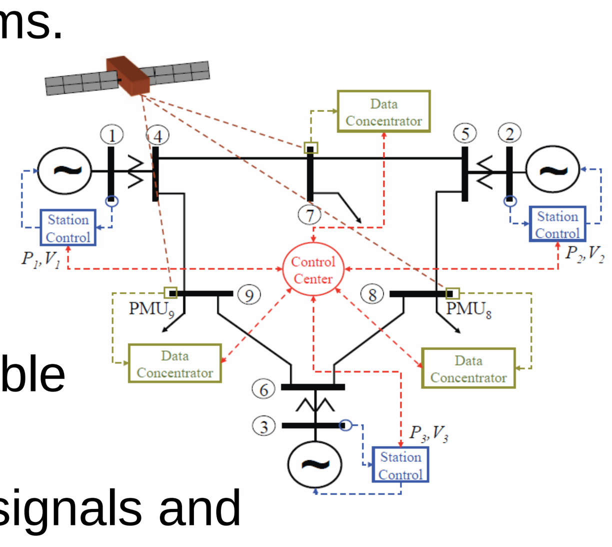
Daniel Chou, Liang Heng, Jonathan J. Makela, Alejandro Domínguez-García, and Grace X. Gao

GOALS

- Understand the timing and synchronization needs in power system applications.
- 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.

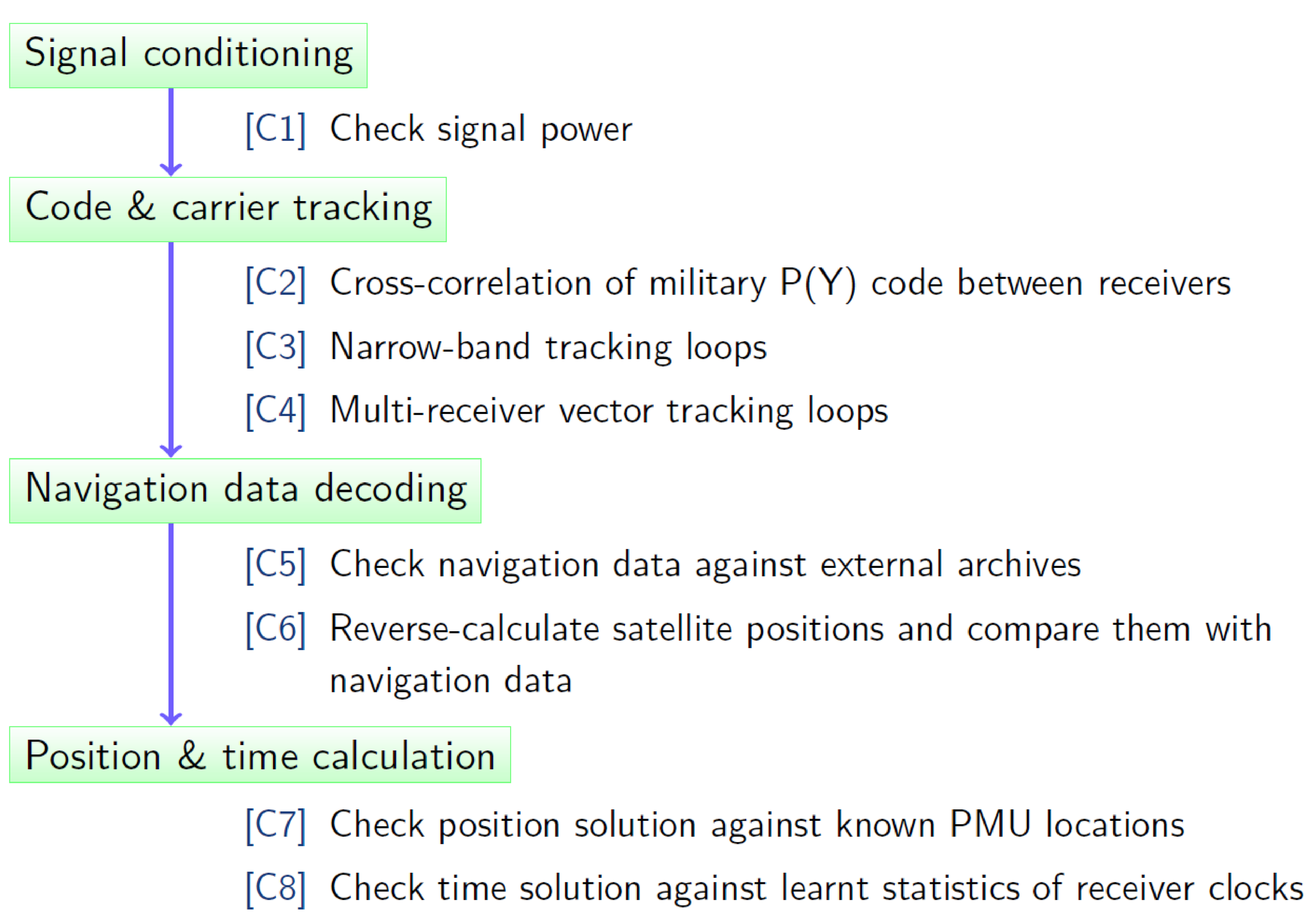
BACKGROUND

- GPS provides accurate timing for power systems.
  - ≤1μs accuracy.
  - Civil GPS signals 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' position & time solutions.



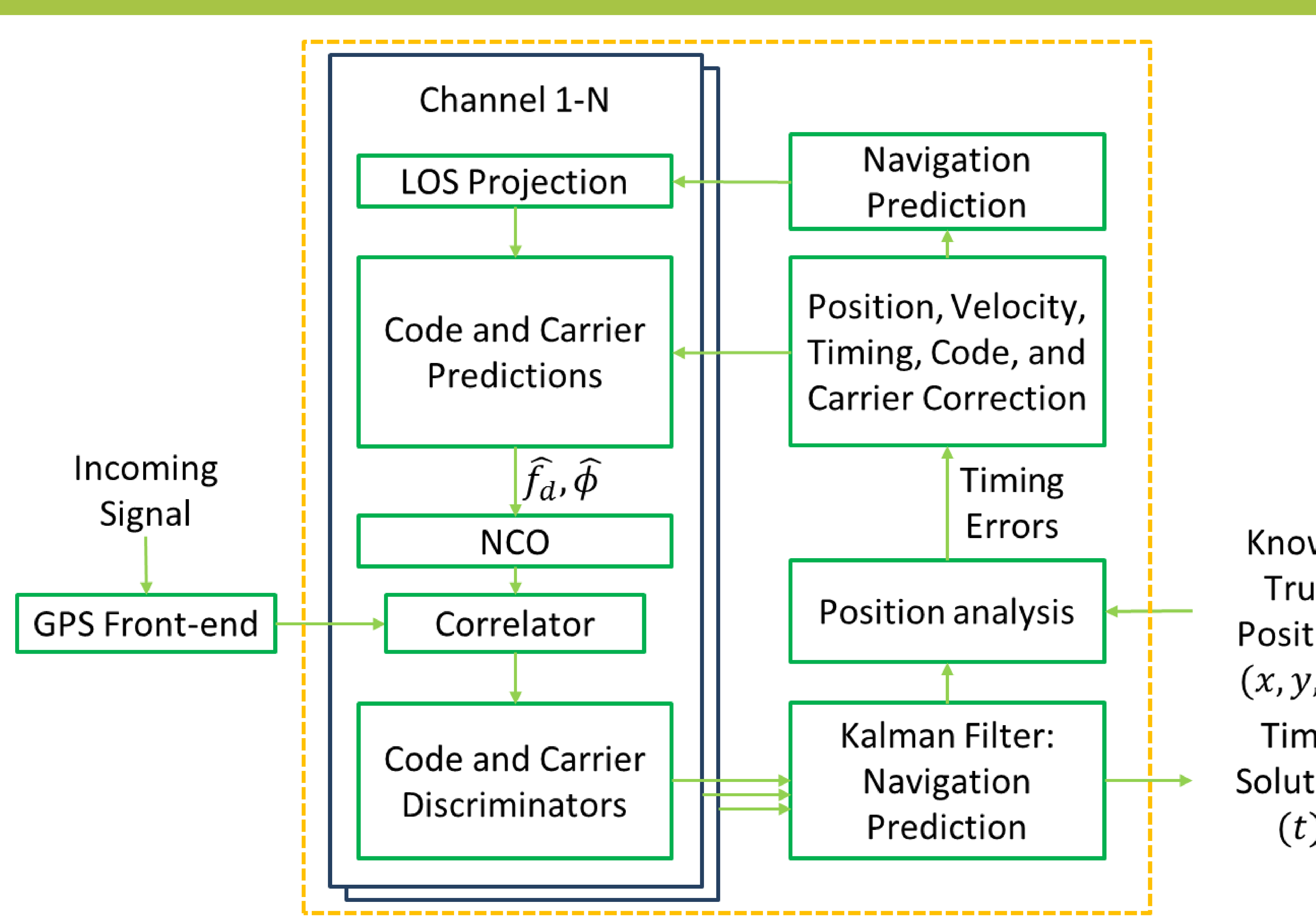
RESEARCH PLAN

- **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.



- **Investigation and development of countermeasures [C3, C4, C7]:**
  - 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 test-bed.

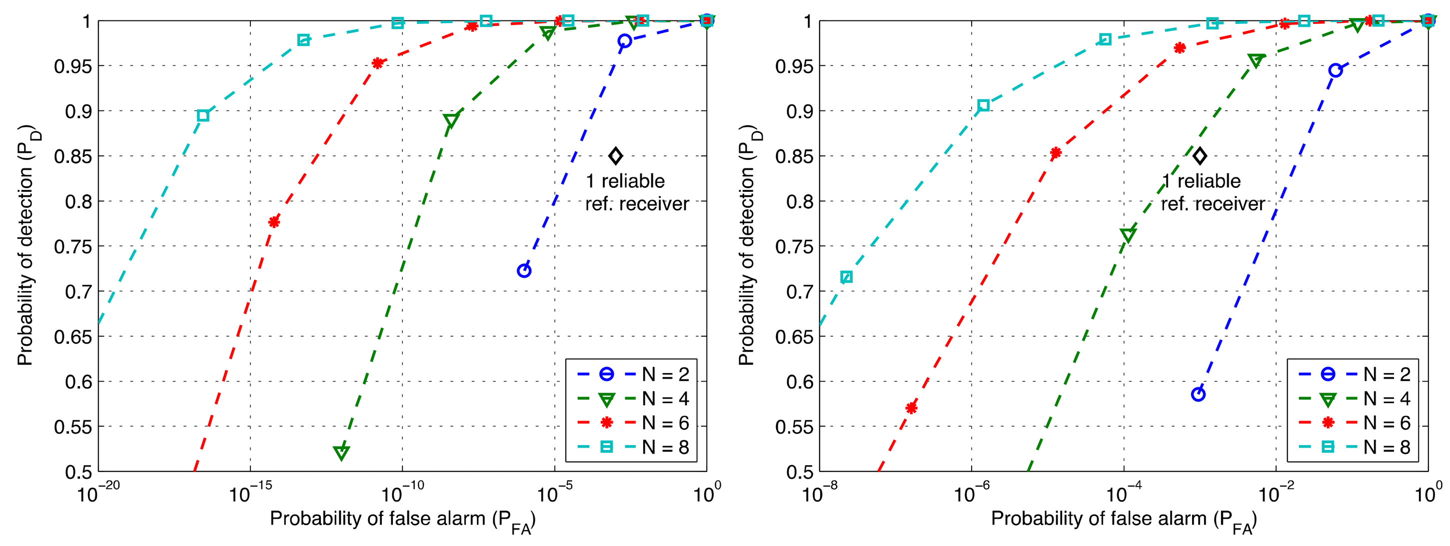
POSITION-INFORMATION-AIDED VECTOR TRACKING



CROSS-CHECKING GPS MILITARY P(Y) CODES

- Theoretical analysis shows that a modest number of reference receivers can achieve high spoofing detection performance, even if some of the receivers are unreliable or spoofed.

Assumption on pair-wise check performance: $\alpha = 0.001$ and $\beta = 0.15$.

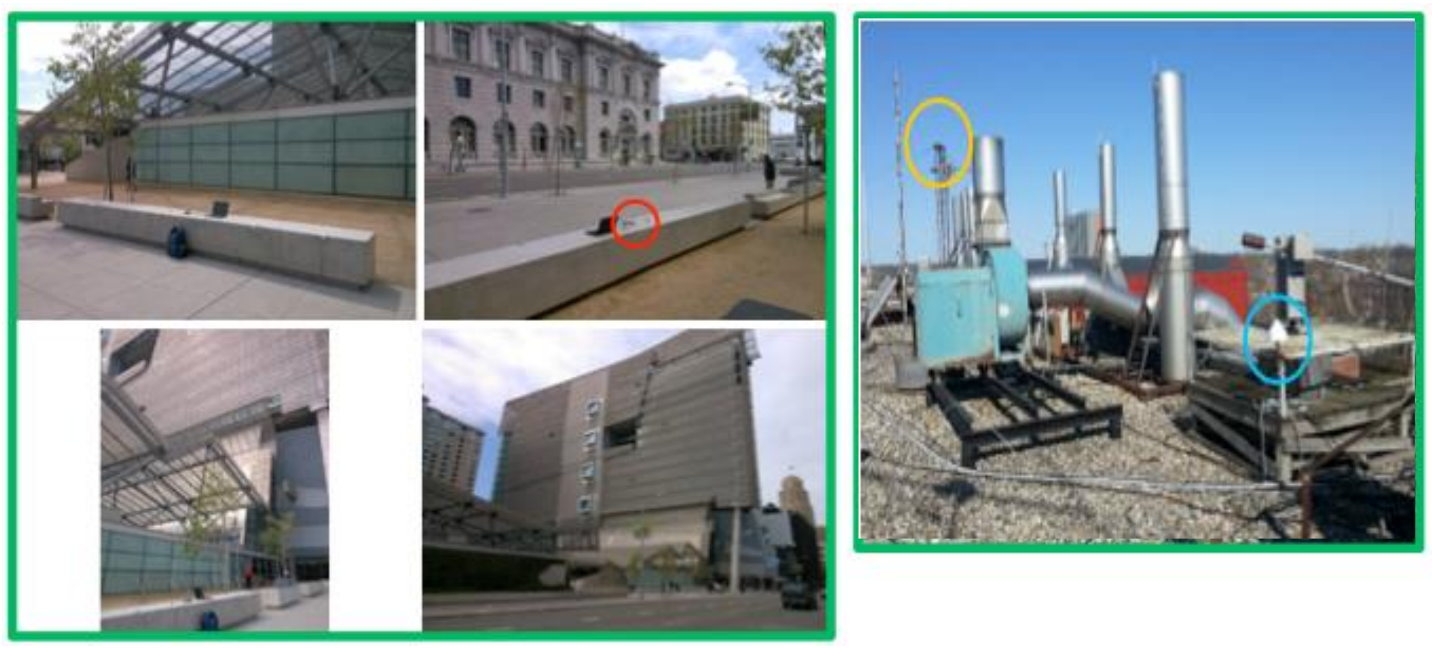


(a) Reliable reference receivers ($\gamma_1 = \gamma_2 = 0$)

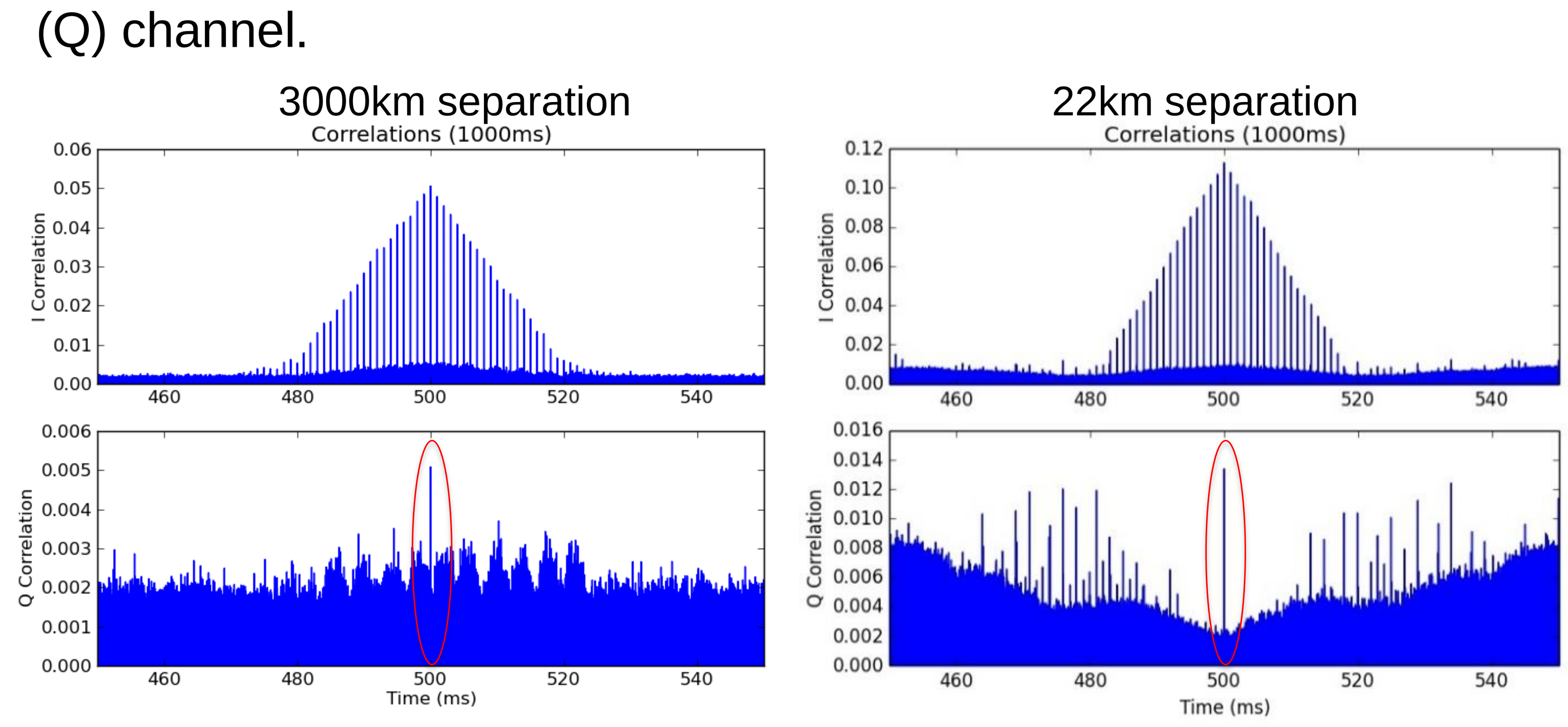
(b) Unreliable reference receivers ($\gamma_1 = \gamma_2 = 0.1$)

EXPERIMENTAL RESULTS

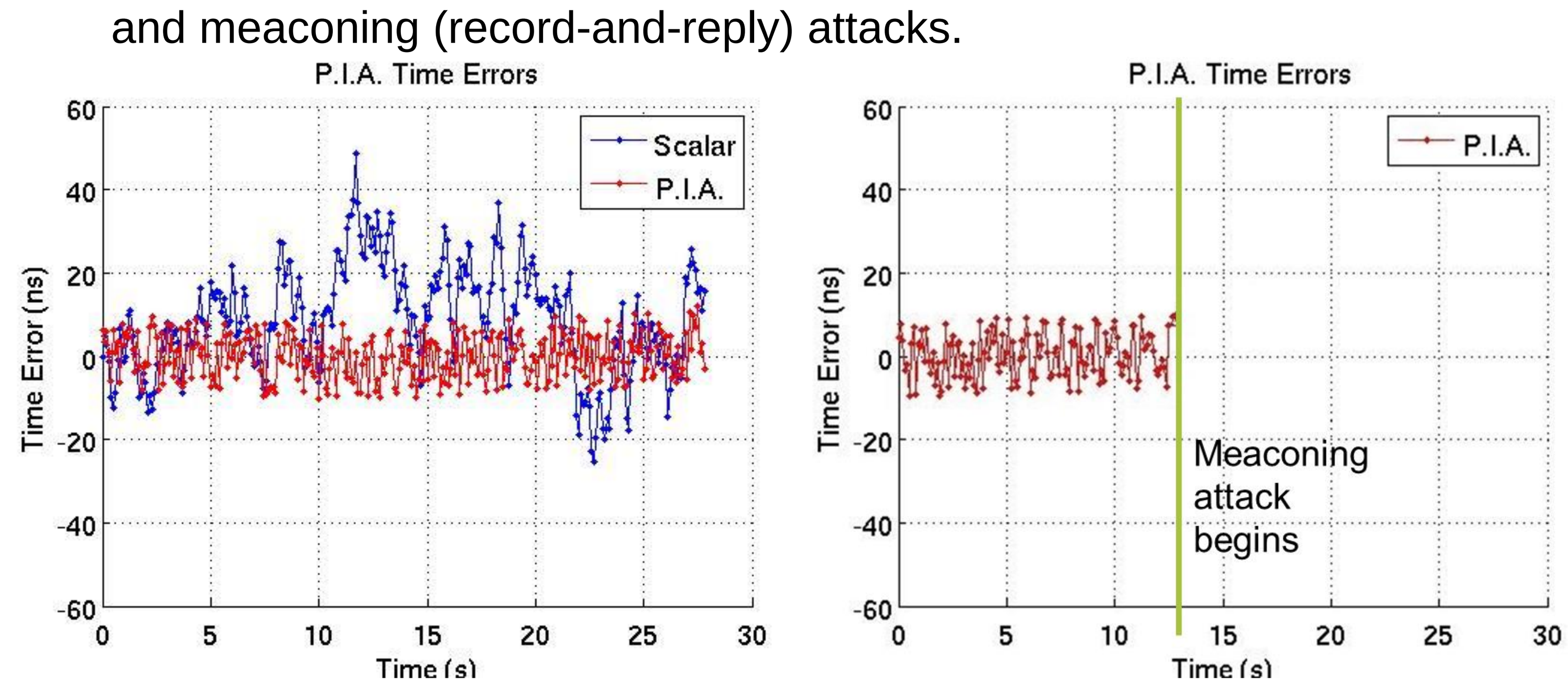
- Conducted the experiments and field tests at San Francisco, CA; Rantoul, IL; and UIUC (Everitt Lab).



- Cross-correlating snippets between the user receiver and a cross check receiver can successfully detect military P(Y) codes in the quadrature (Q) channel.



- Position-information-aided vector tracking is robust against jamming and meaconing (record-and-reply) attacks.



CONCLUSION

- Position-Information-Aided Vector Tracking Loop:
  - Robust against jamming (5dB more noise tolerance compared with scalar tracking).
  - Can successfully detect meaconing attacks.
  - Improves the accuracy of the timing solutions when compared with traditional scalar tracking (15 ns vs. 50 ns).
- 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.

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG
UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T