Robust and Secure GPS-based Timing for Power Systems

Algorithm and Validation of GPS-based Direct Timing Estimation for PMUs

Sriramya Bhamidipati, Yuting Ng and Grace Xingxin Gao

GOALS

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

BACKGROUND ON GPS-BASED TIME TRANSFER

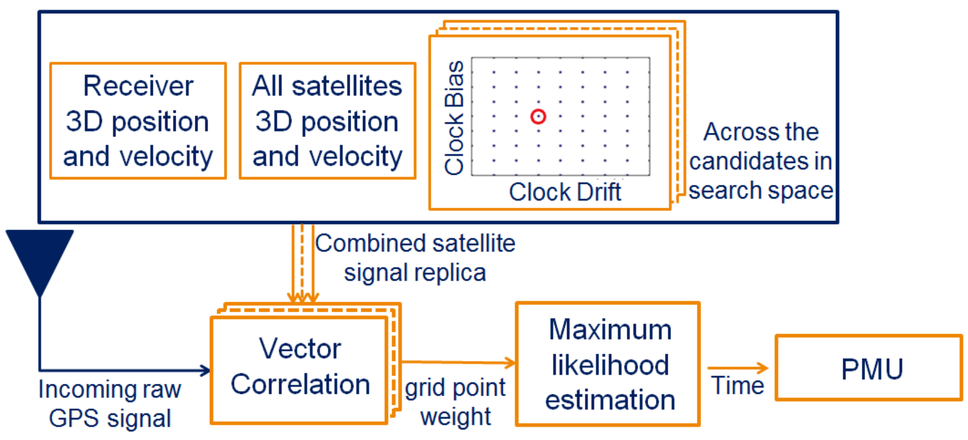
- GPS provides free accurate and precise time and frequency sources for power systems applications.
  - Time accuracy $\sim 100ns$, Frequency accuracy $\sim 1x10^{-12}$Hz.
- Civil GPS signals are susceptible to malicious attacks.
  - Civil GPS signals are weak and unencrypted, with their structures explicitly described in publicly available documents.
  - An attacker can broadcast counterfeit civil GPS signals and manipulate victim receivers' time and time drift solutions.
- Civil GPS-based timing equipment are not sufficiently robust to jamming, spoofing attacks and receiver errors.
  - Errors of up to 13 microseconds were observed for several hours during a GPS glitch on January 26 2016.
  - According to IEEE-C37.118.1, without other errors, maximum allowable phase angle error is $0.573°$ (~timing error of $26.5\ \mu s$).

OUR ROBUST GPS ALGORITHMS

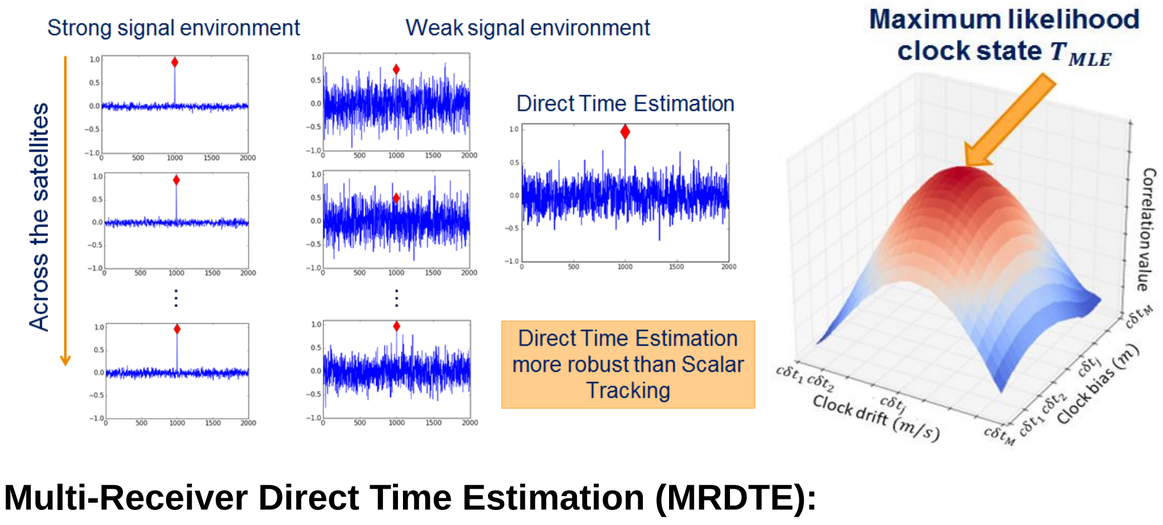
- Traditional GPS-based time transfer is a two-step process:
  - Acquire and track GPS signals per satellite individually to generate respective pseudorange and carrier phase.
  - Perform least-squares to obtain PVT solution from which UTC time is computed.
- The robust GPS algorithms developed in our lab:
  - No intermediate pseudorange measurements need to be estimated.
  - Leverage the static nature of the power grids to pre-determine 3D position an velocity of GPS receiver.
  - Works directly with timing parameters. Reduction in unknowns to be estimated from 8 $(x, y, z, c\delta t, \dot{x}, \dot{y}, \dot{z}, c\delta\dot{t})$ to 2 $(c\delta t, c\delta\dot{t})$.

Direct Time Estimation (DTE):

- Direct time estimation is a novel signal processing technique that evaluates a pre-generated set of clock candidates using the principle of maximum likelihood estimation.



- This algorithm computes non-coherent summation across satellites which improves the signal-to-noise ratio of the system.

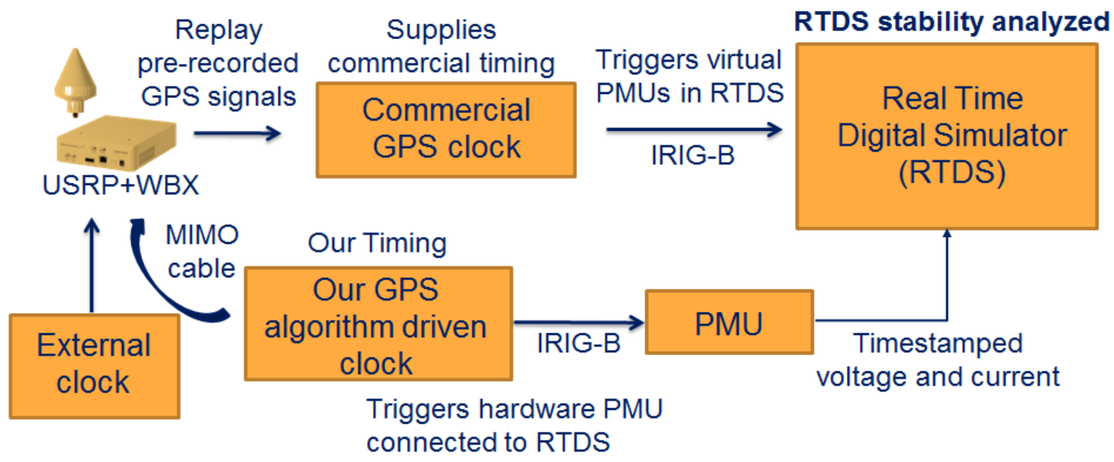


Multi-Receiver Direct Time Estimation (MRDTE):

- An extension of DTE known as Multi-Receiver Direct Time Estimation (MRDTE) is developed to incorporate multiple receivers.
  - Geographical diversity of multiple receivers is taken into account so as to further improve the robustness against timing attacks.
  - All the receivers are triggered by a common external clock.

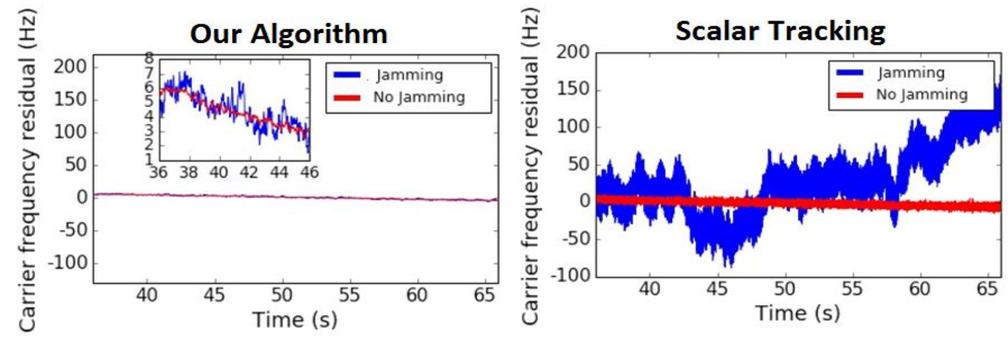
VALIDATION OF GPS-BASED TIMING FOR PMU

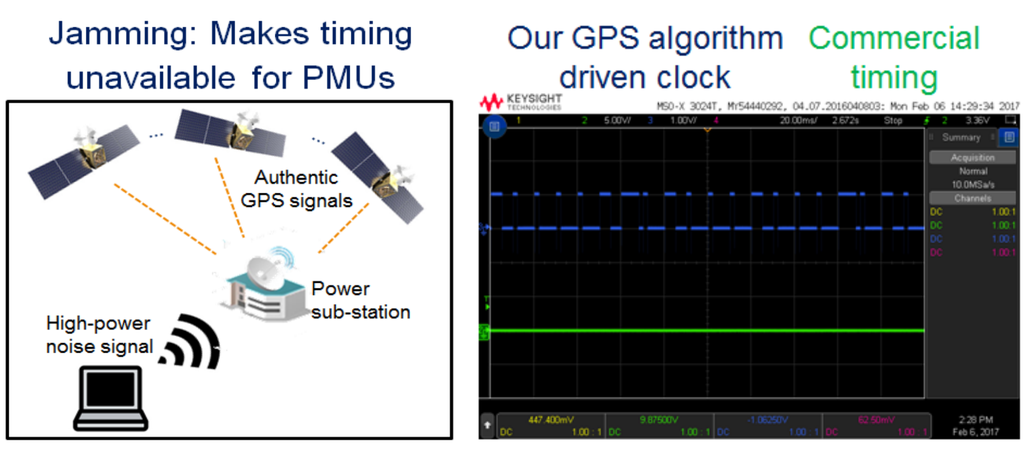
- Experimental validation of our robust GPS-based timing on PMUs involves two threads:
  - The GPS signals are given as input to the commercial clocks which supply IRIG-B timing signals to virtual PMUs in RTDS setup.
  - Our GPS algorithm driven clock takes the GPS signals to generate timing signals which are supplied to the hardware PMU connected to the RTDS setup.
- Synchronization of the threads is done using an external clock (Chip Scale Atomic Clock) and MIMO cable.



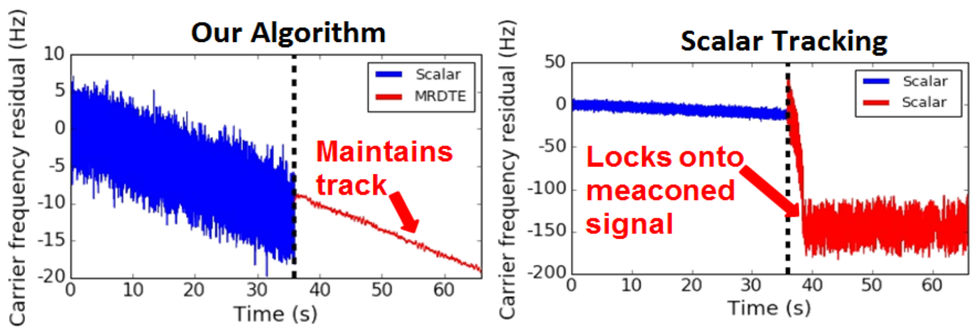
RESEARCH RESULTS

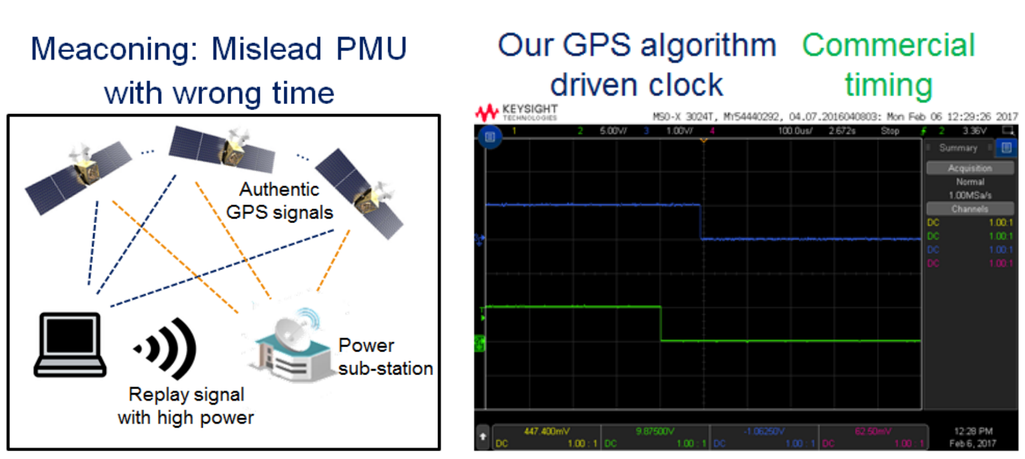
- Under $25dB$ of added Jamming above noise floor, the commercial clock lost track while our Direct Time Estimation driven clock is robust.





- Under Spoofing attack which broadcasts a meaconed signal of delay $100\mu s$ and $20db$ higher power, the commercial clock locks on spurious signal while Direct Time Estimation tracks the authentic signal.





CONCLUSION

- Our GPS algorithms utilize the entire information in the raw signal whereas the traditional methods discard the remaining information in raw signal after determining intermediate measurements.
- Experimental tests validate the increased robustness of our GPS algorithms against jamming, spoofing and receiver errors as compared to traditional GPS processing methods.

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY