Robust and Secure GPS-based Timing for Power Systems

GPS-Based Direct Timing Estimation for PMUs

Yuting Ng, Arthur Hsi-Ping Chu, Sriramya Bhamidipati, 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 testbed 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 ~100ns.
  - Frequency accuracy ~$1x10^{-12}$.
- 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 is not sufficiently robust to jamming, spoofing attacks, and receiver errors.
  - Global users of civil GPS-based timing equipment reported timing errors of up to 13 microseconds for several hours during a GPS glitch on January 26, 2016.

ANALYSIS OF JANUARY 26 GPS TIMING ANOMALY

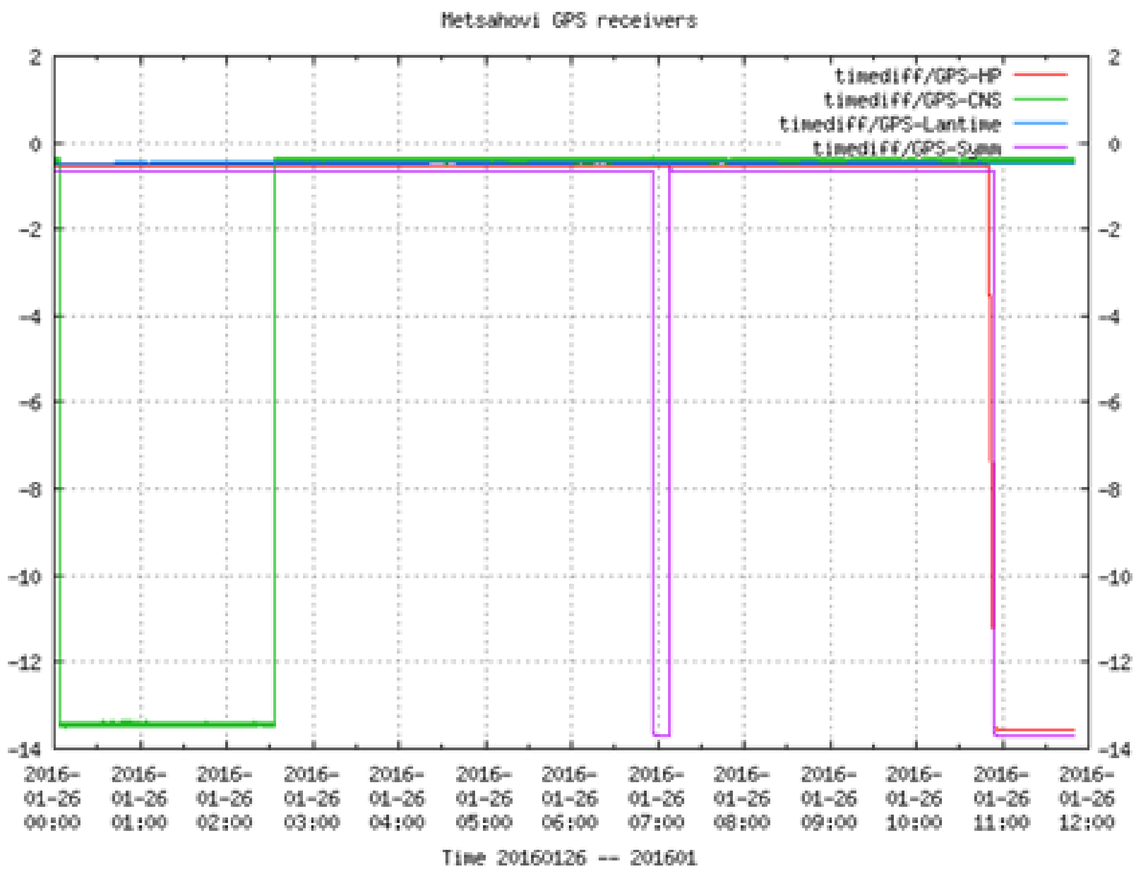


Figure source: Metsähovi Radio Observatory

- Analyzed GPS observations and navigation messages from Trimble NetR9 base station receiver located on the roof of Talbot Laboratory in Urbana, IL on Jan. 26, 2016, 00:00:00–23:59:59 UTC.
- Timeline of events:
  - 08:00 UTC: reports of timing anomaly from global users.
  - 16:00 UTC: issue identified and resolved; global users continue to experience timing errors for several hours.
- Affected satellites: 2, 6, 7, 9, 23.
- Cause of timing anomaly:
  - Universal Time Coordinated (UTC) correction parameters were incorrectly uploaded onto affected satellites.
  - UTC correction parameters affected.

Affected UTC correction parameters	Feb. 22, 2016 (for comparison)	Jan. 26, 2016 (incorrect)
A0: constant term of correction polynomial	3.7 ns	-13.7 µs
WN_t: UTC reference week number	1885	0
T_{ot}: UTC reference time	319488	0

Table generated from ephemerides logged by Trimble NetR9. Values were in error for the entire day.

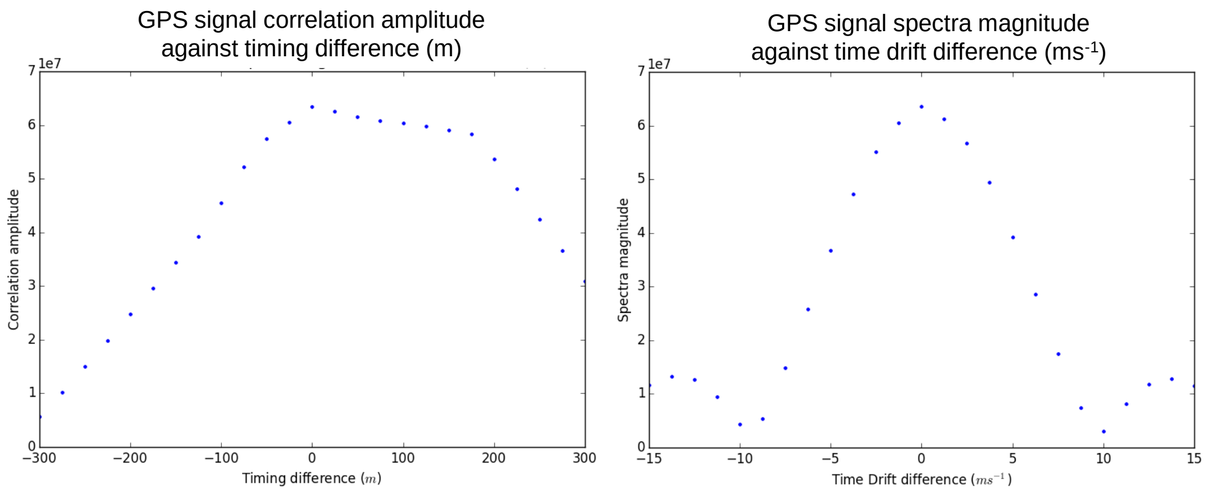
- Certain civil GPS receivers in the CORS network were unaffected.

GPS-BASED DIRECT TIMING ESTIMATION

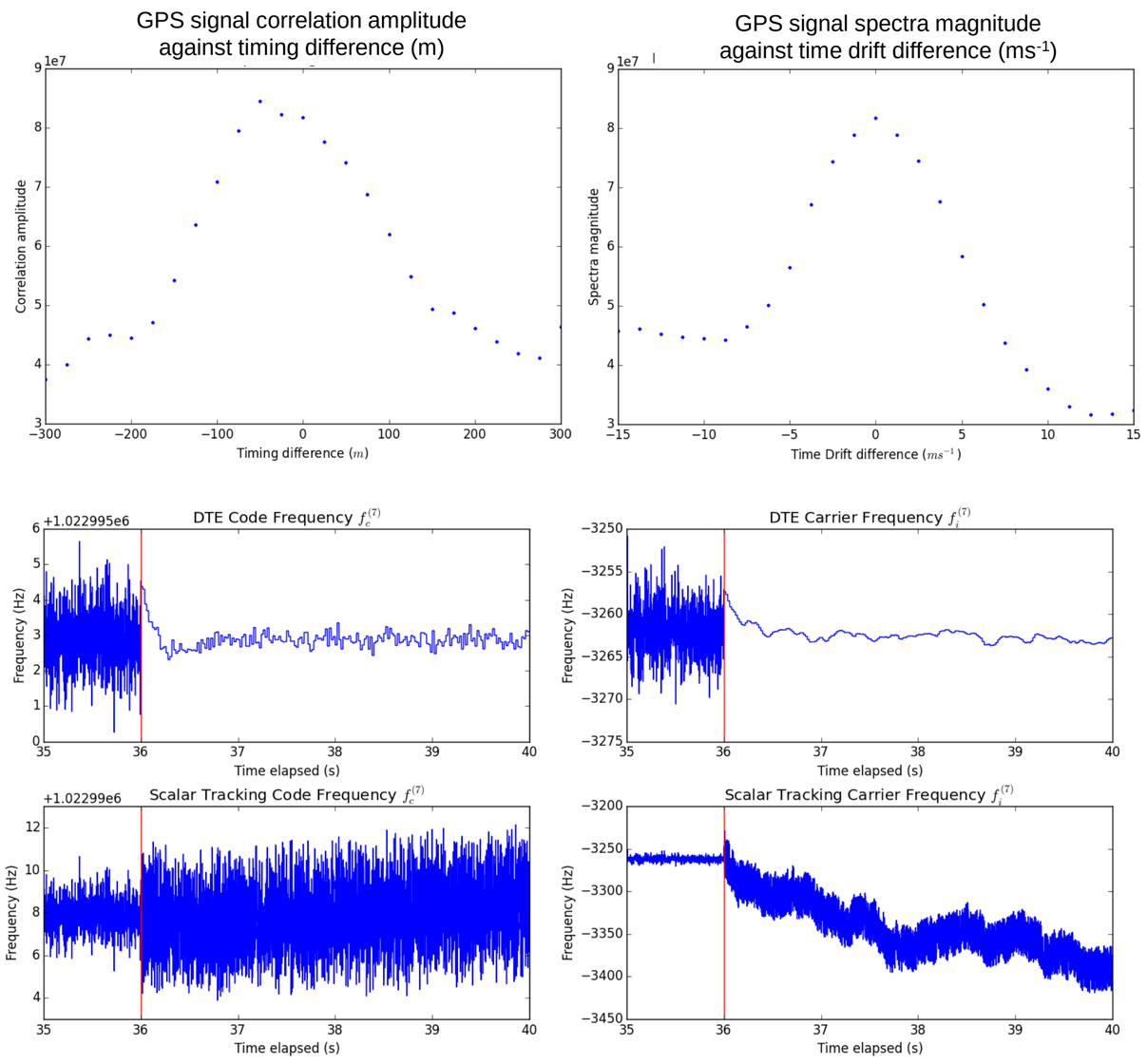
- Traditional GPS-based time transfer is a two-step process:
  - Acquire and track GPS signals per satellite.
  - Generate GPS measurements, pseudorange, and carrier phase per satellite; then perform least-squares to estimate time and time drift.
- Our method, Direct Timing Estimation (DTE), is a one-step process:
  - Directly search for the time and time drift parameters that most likely led to the received GPS signal.
  - Based on the following two assumptions:
    - Received GPS signal is intimately governed by the underlying parameters of receiver position, time, velocity, and time drift.
    - Receiver position and velocity can be accurately surveyed ahead of time for static PMUs used in power system applications.

RESEARCH RESULTS

- DTE is robust to and provides visual representation of spoofing attack:



  - GPS signal correlation amplitude peak shows accurate time under a spoofing attack in which a meaconing signal of gain G = 0.85, with a delay of 0.6 microseconds corresponding to 180 m, is broadcast on top of the original, authentic signal.
  - GPS signal spectra magnitude plot is unaffected, as the meaconing signal does not contain a difference in time drift.
- DTE is robust to and provides visual representation of jamming attack:



CONCLUSION

- Direct Timing Estimation (DTE) is more robust to jamming, spoofing, and receiver errors than traditional GPS processing methods are.
  - DTE utilizes information from the entire raw GPS signal; traditional methods discard remaining information in raw signal after determining intermediate measurements.
  - DTE is able to continue tracking the original, authentic GPS signal under weak, jammed, and spoofed scenarios to a greater degree than traditional GPS processing methods can.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY