Detection of Time Spoofing Attacks on GPS Synchronized Phasor Measurement Units

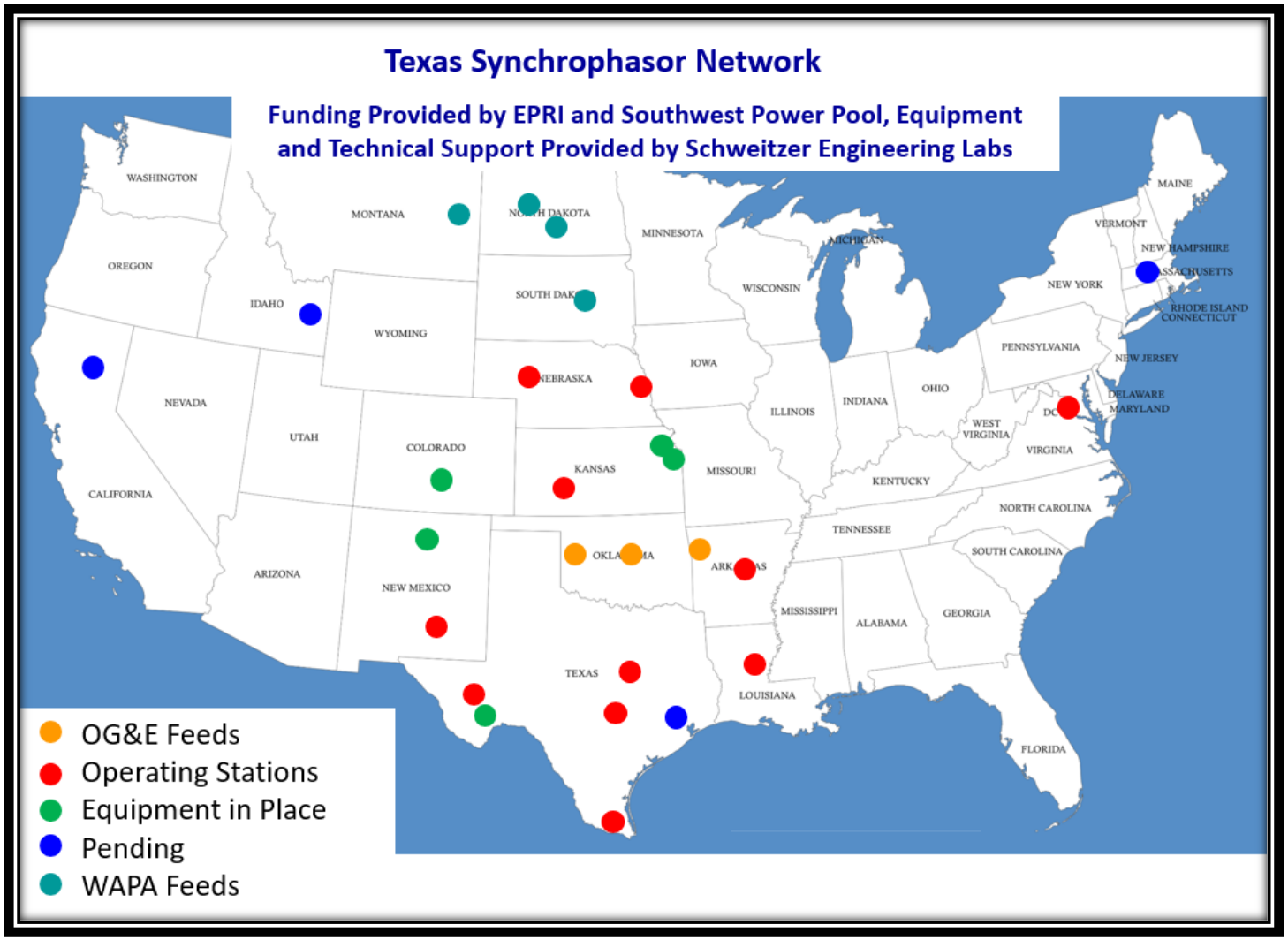
Andrew K. Mattei, Baylor University, Brazos Electric Cooperative

Dr. Mack Grady, Baylor University

P. Jay Caspary, Southwest Power Pool

Scott A. McBride, Idaho National Laboratories

Introduction



Outline

- Reality of Spoofing
- Frequency and The Grid
- Time Error Correction / Integrated Time Error
- Characteristics of Spoofing
- Simulating a Spoofing Attack
- Spoofed Data Graphs
- Transient Response
- Conclusions

What is “Spoofing”?

- Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security.

- Source: https://www.techopedia.com/definition/5398/spoofing

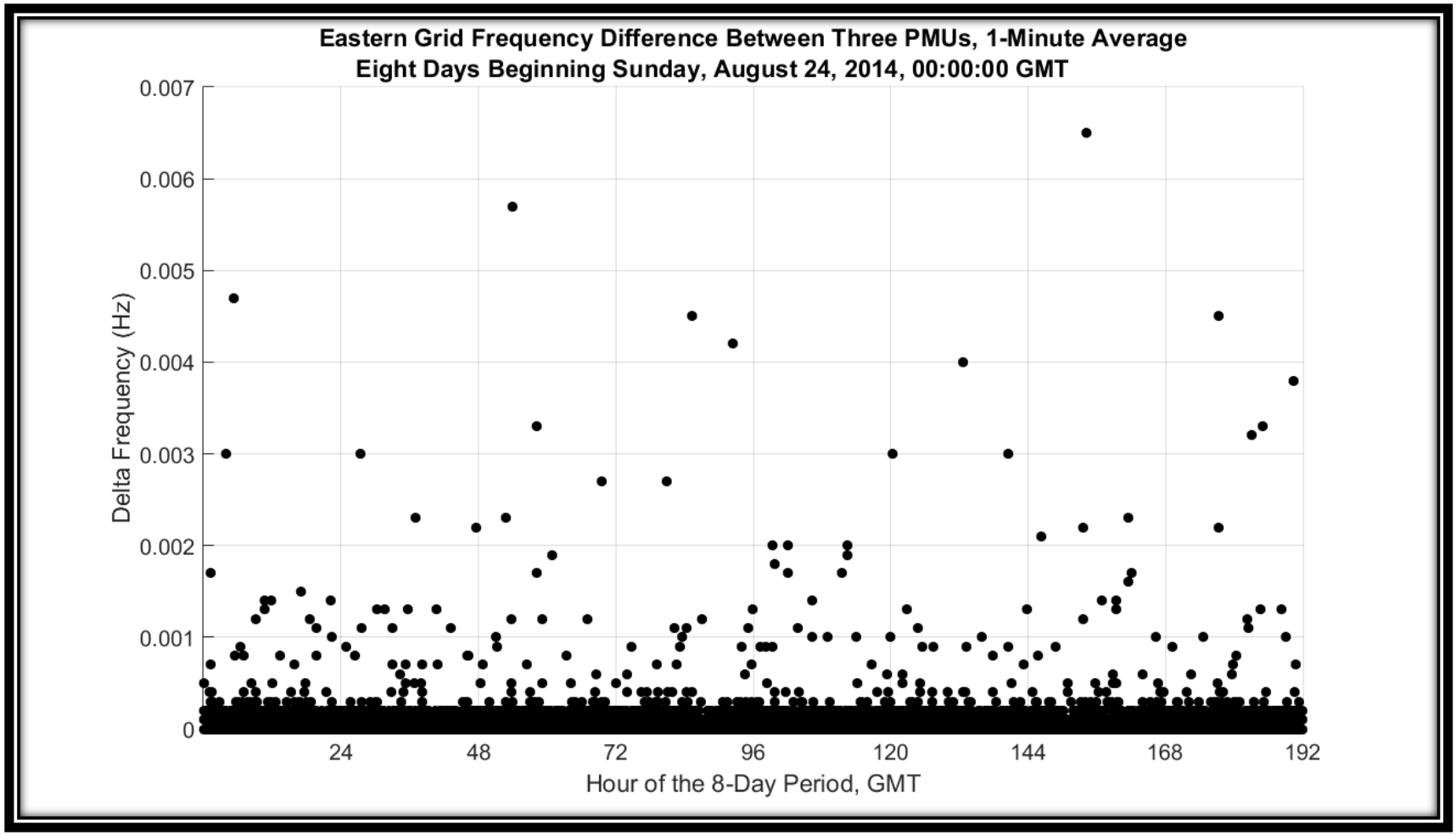
The Reality of GPS Spoofing

Spot the Antenna

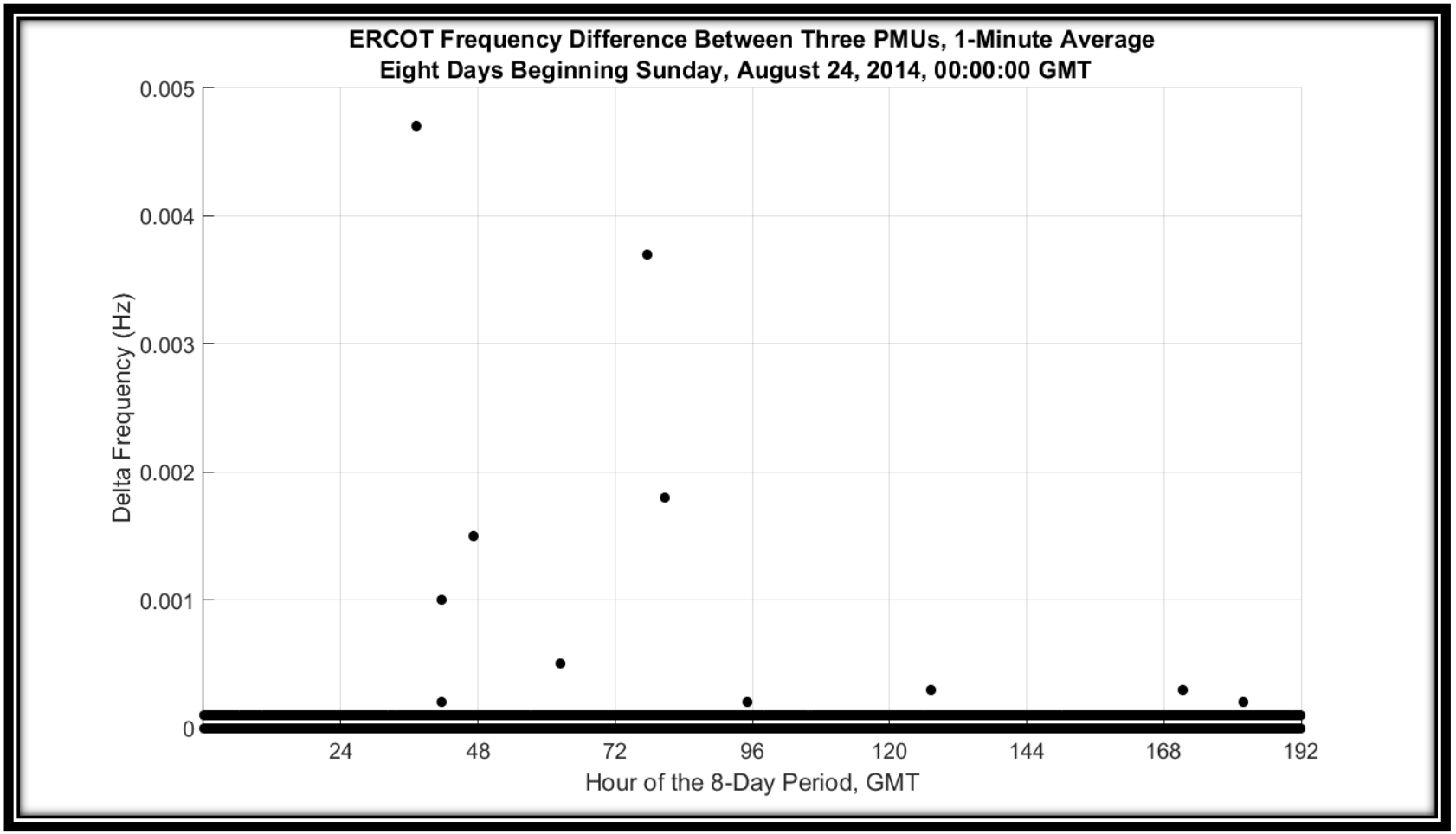
The Reality of GPS Spoofing

- Three Levels of Spoofing Devices
  1. Simplistic – Commercial signal generators
  2. Intermediate – Capable of generating false signals
  3. Sophisticated – Multiple synchronized false signal generators
- Most likely successful attack vector is the intermediate level of device

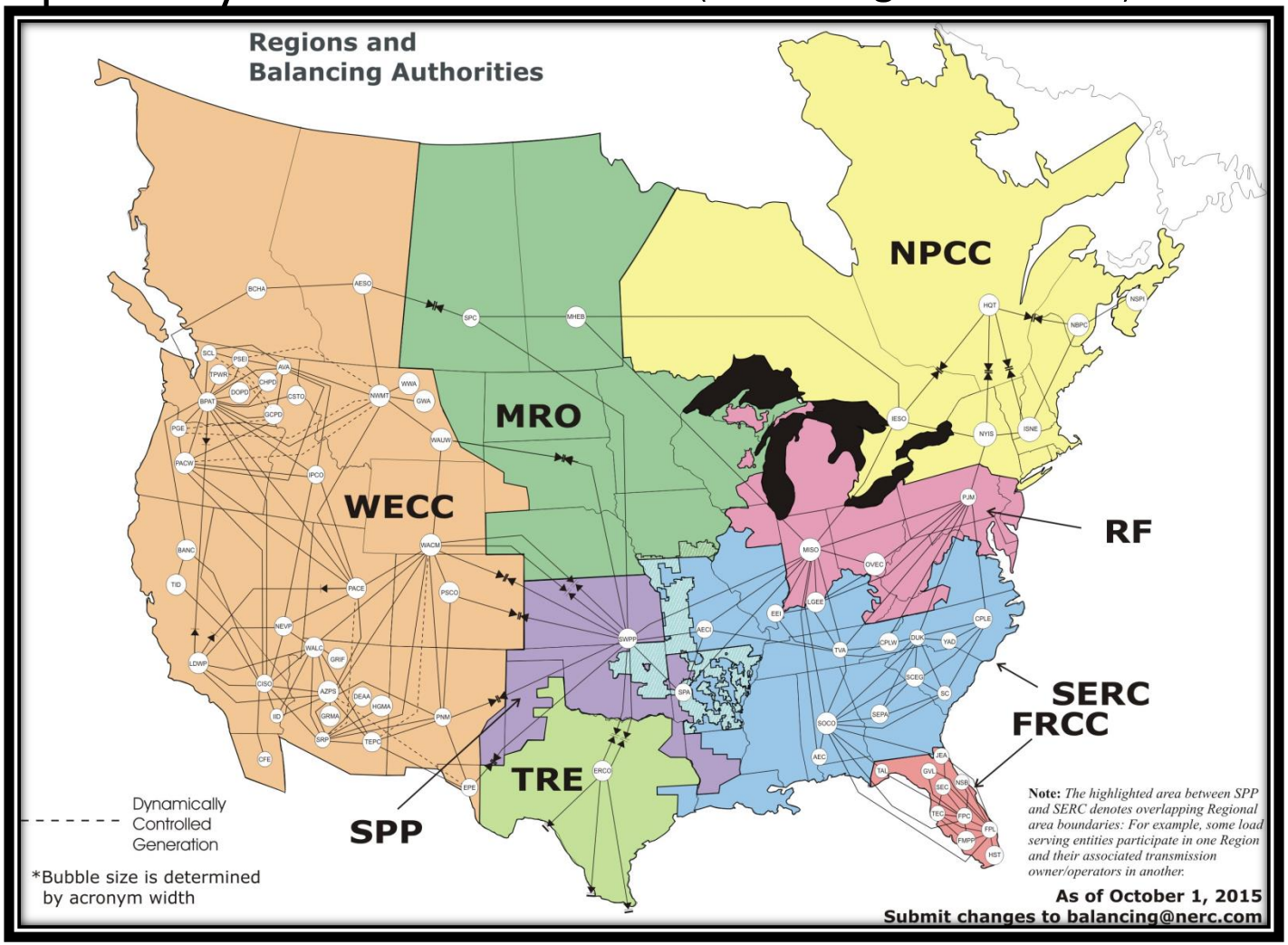
Frequency and The Grid (Eastern)



Frequency and The Grid (ERCOT)



Frequency and The Grid (Balancing Authorities)



Time Error Correction

$$60\ Hz\ \neq 60\ Hz$$

- Integrate frequency deviation over time
- NERC Definition: Accumulation of frequency error over a given period
- Synchrophasor: Sum of frequency error across *n* samples at given sample rate
- Control by different Balancing Authorities results in unique but consistent time errors for each B.A.

Integrated Time Error (ITE)

- ERCOT ITE < 0.01 seconds per minute across 4 PMUs (during chosen minute)
- ERCOT ITE difference from average < 2.7 µsec
- SPP ITE < 0.015 seconds per minute across 4 PMUs
- SPP ITE difference from average < 5.9 µsec
- Now we're on to something!

$$TimeError = \frac{\frac{\sum_{i=1}^{n} f_i}{n} - 60.000}{60} * \frac{n}{S_{RATE}}$$

Spoofing Characteristics

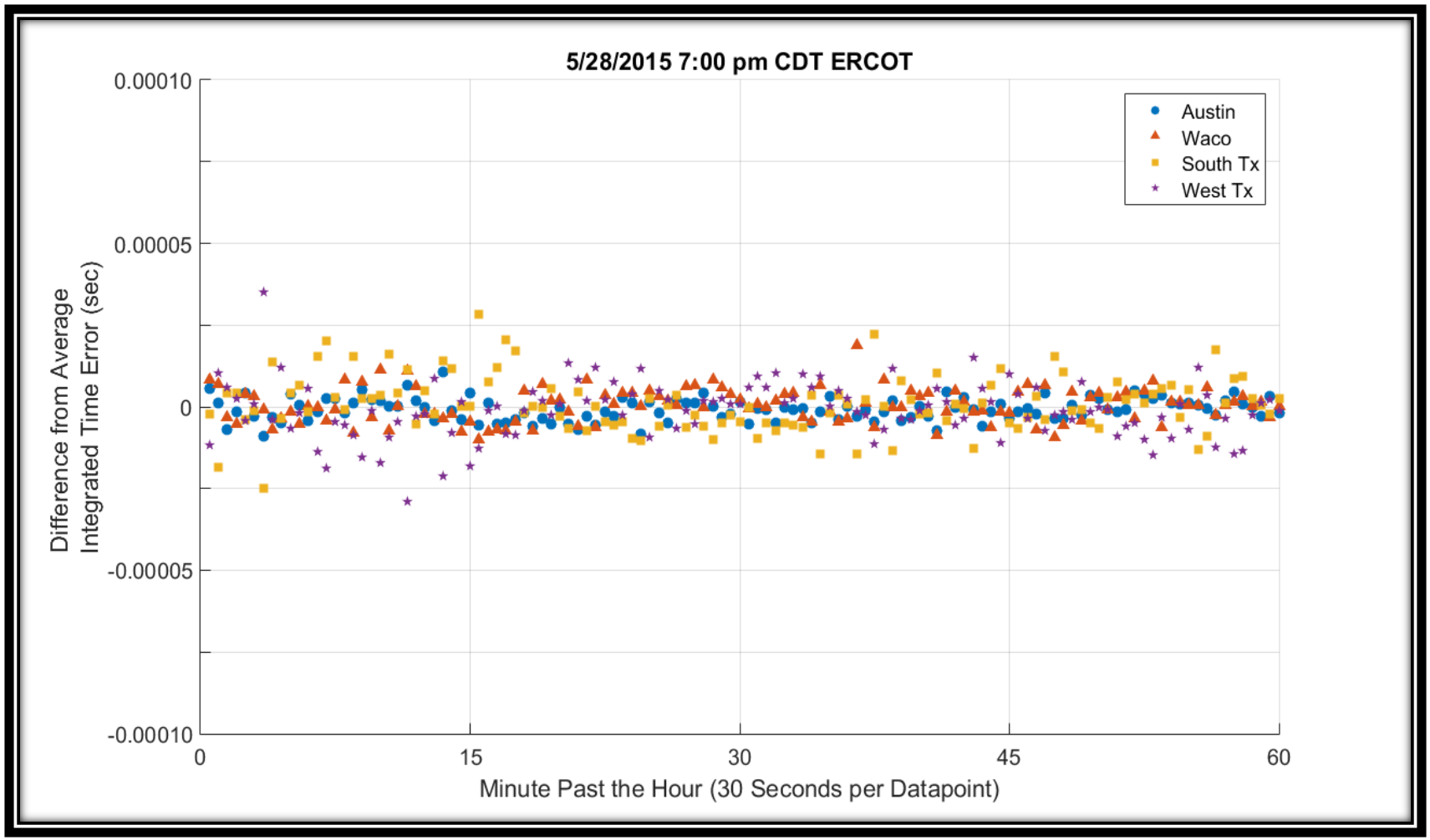
- A slight shift in GPS time…
  - Changes the calculated frequency
  - Changes the calculated phase angle

- 1 degree of shift equals 0.0000463 Hz offset from 60 Hz
- Can you detect that, or is that in the noise?
- PMU Measurement resolution ~2 degrees

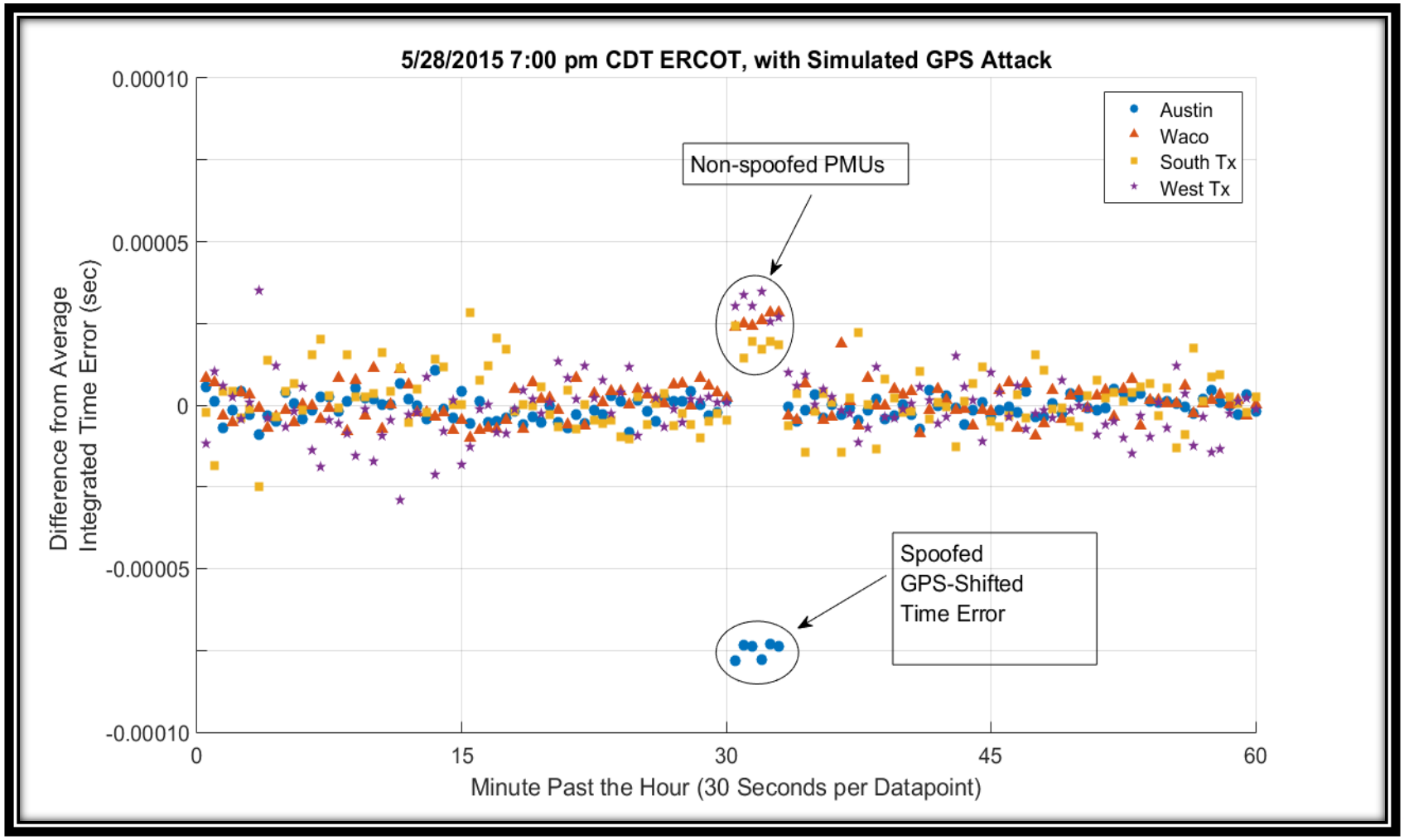
Simulating a Spoofing Attack

- Attack appears as either:
  - "Push", where $f_{new} > f_{actual}$ and attack phase angle is negative
  - "Pull", where $f_{new} < f_{actual}$ and attack phase angle is positive
- Simulated by scaling frequency of one PMU with a calculated angle of attack (ex: -4.2˚/min)

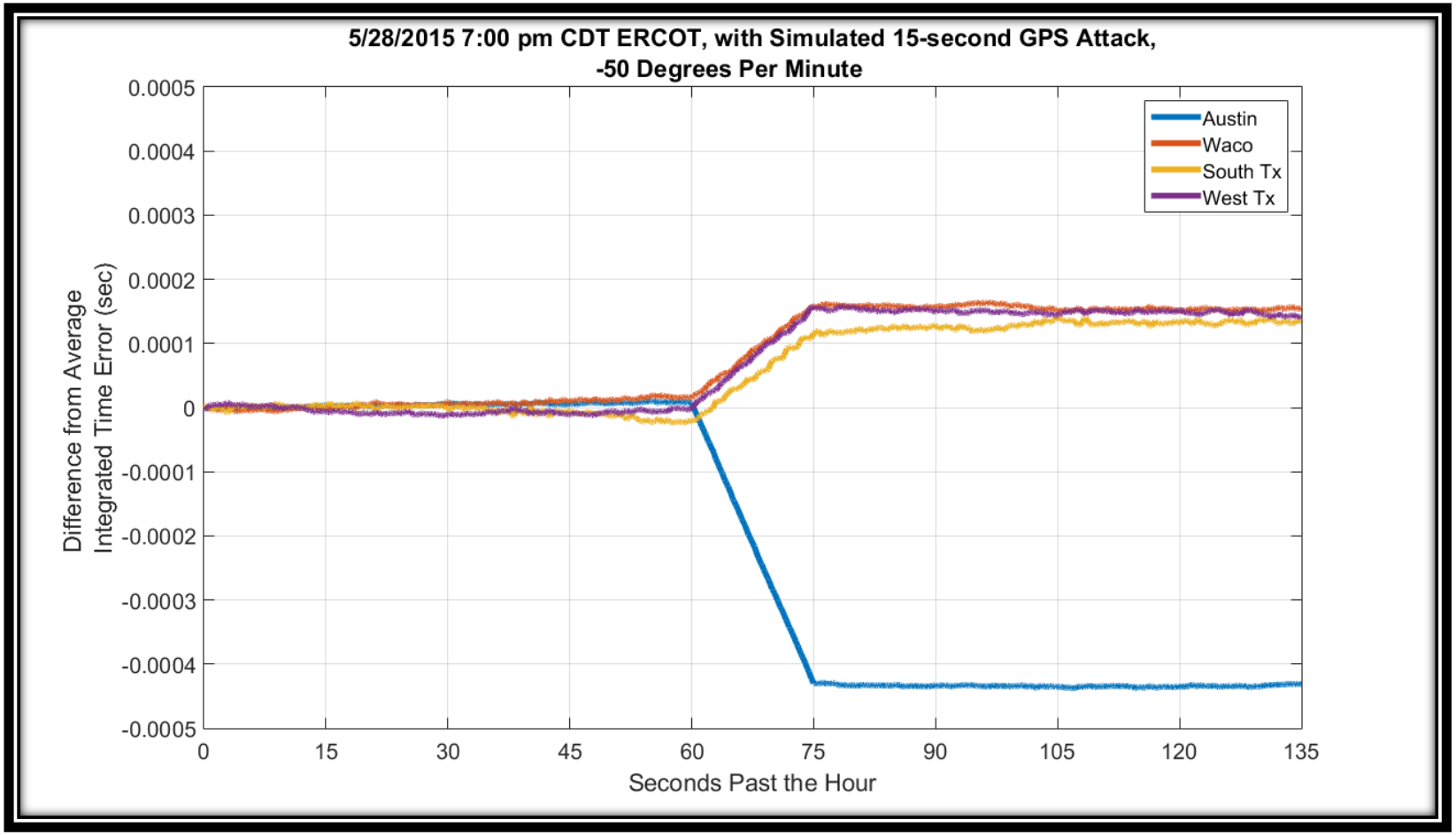
Normal Mode Data – 30 sec avg



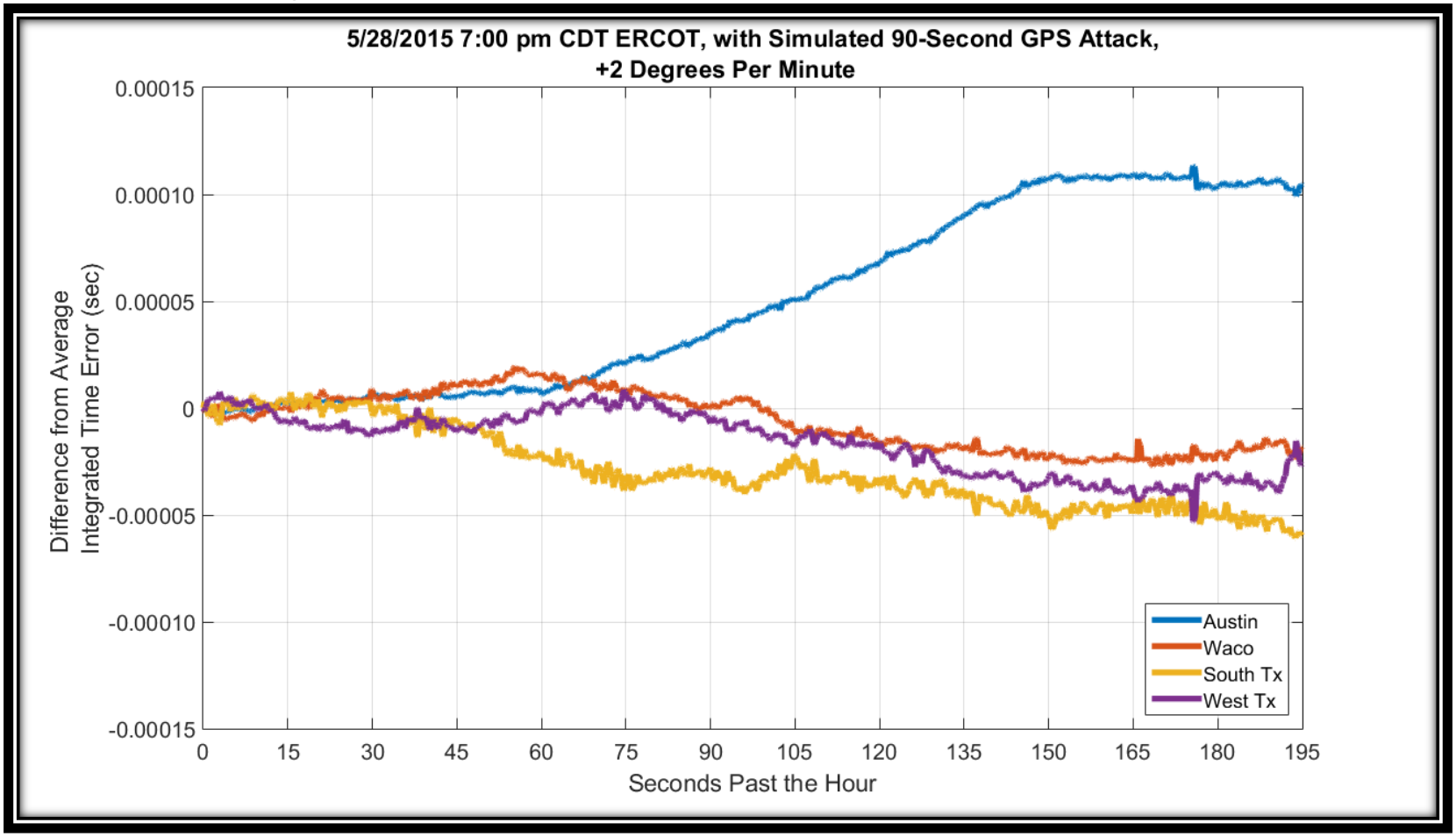
Spoofed Data – 30 sec avg, -4.2˚/min



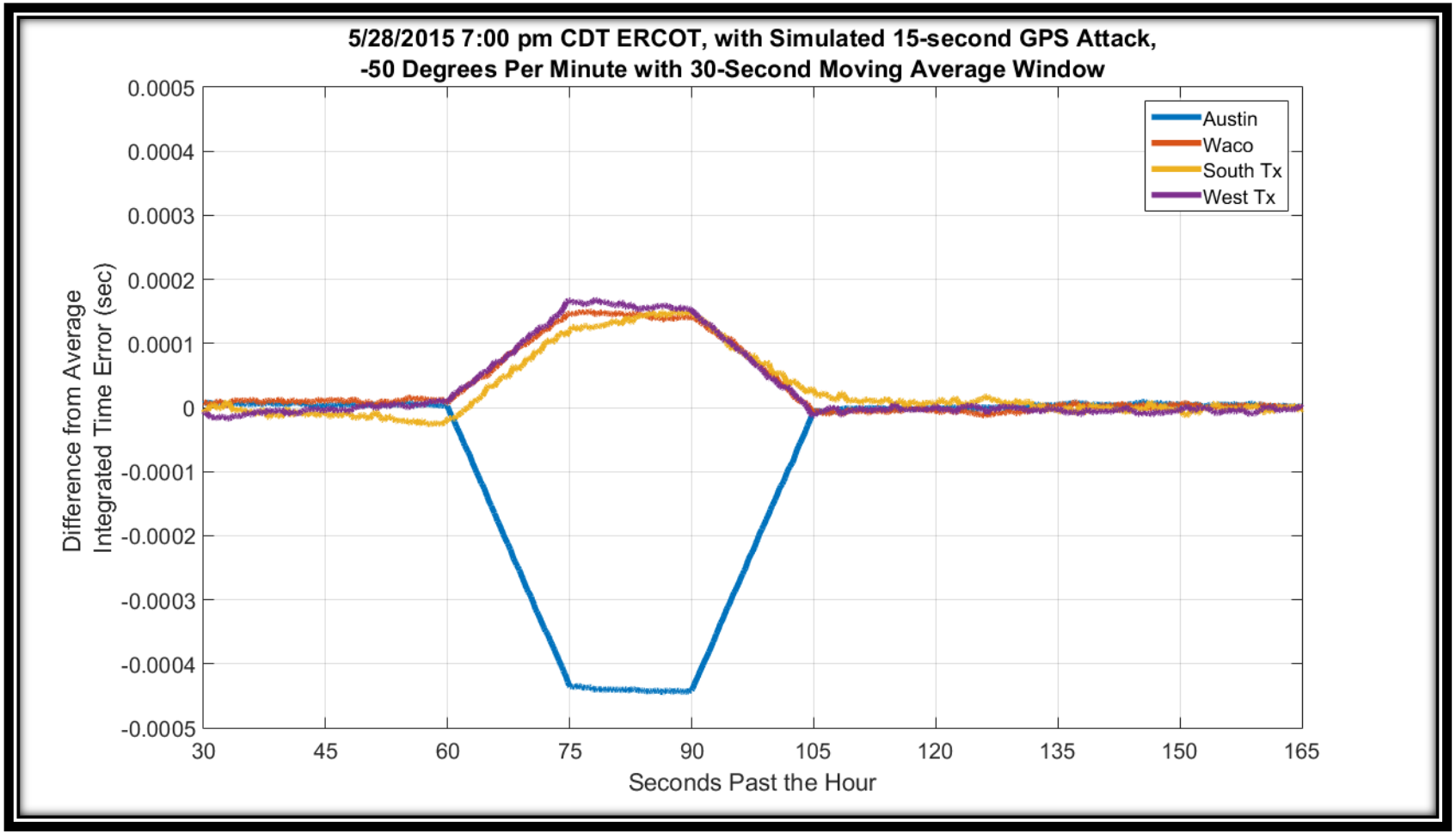
Aggressive Spoof, continuous ITE sum



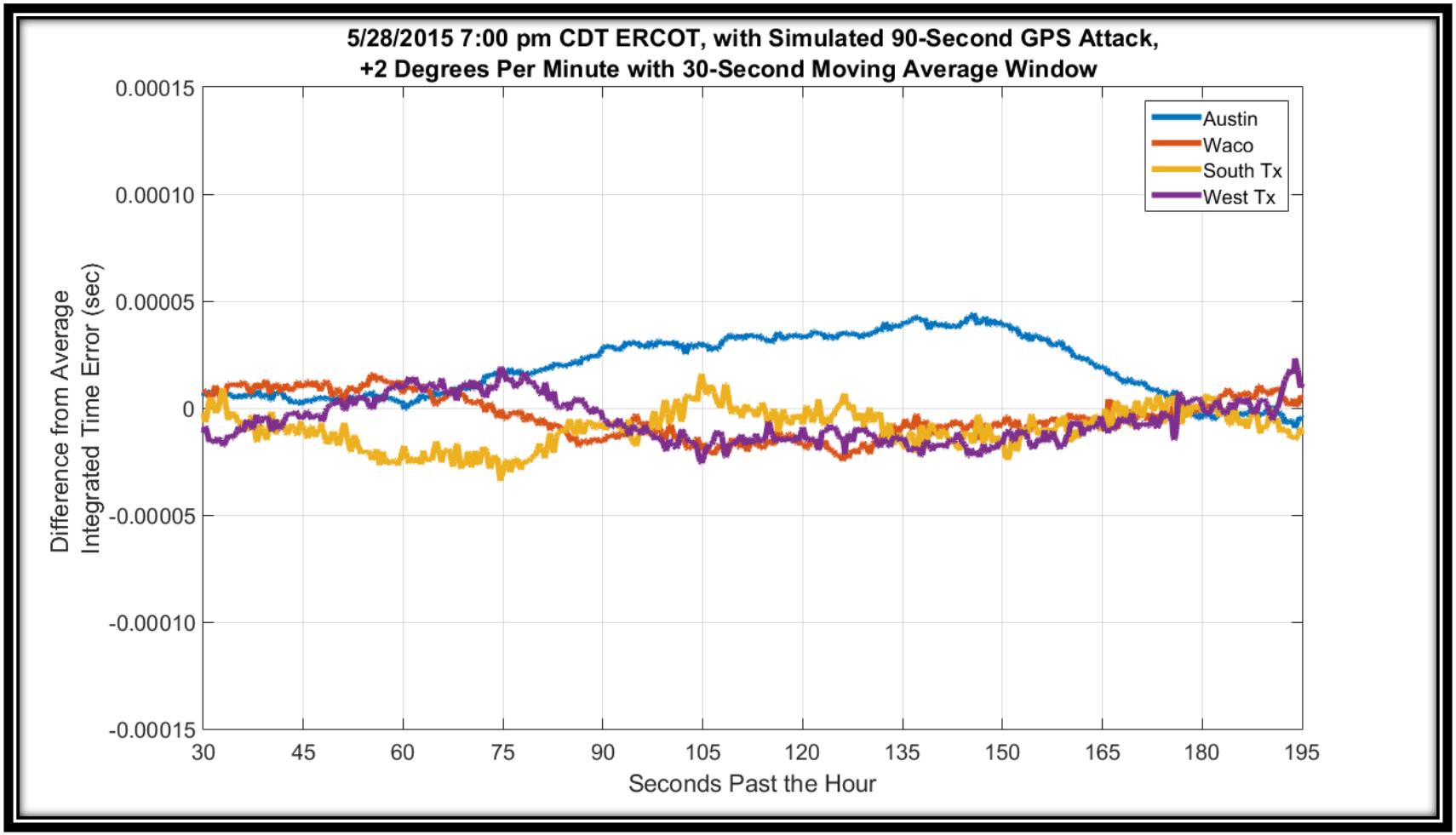
Slow Spoof, continuous ITE sum



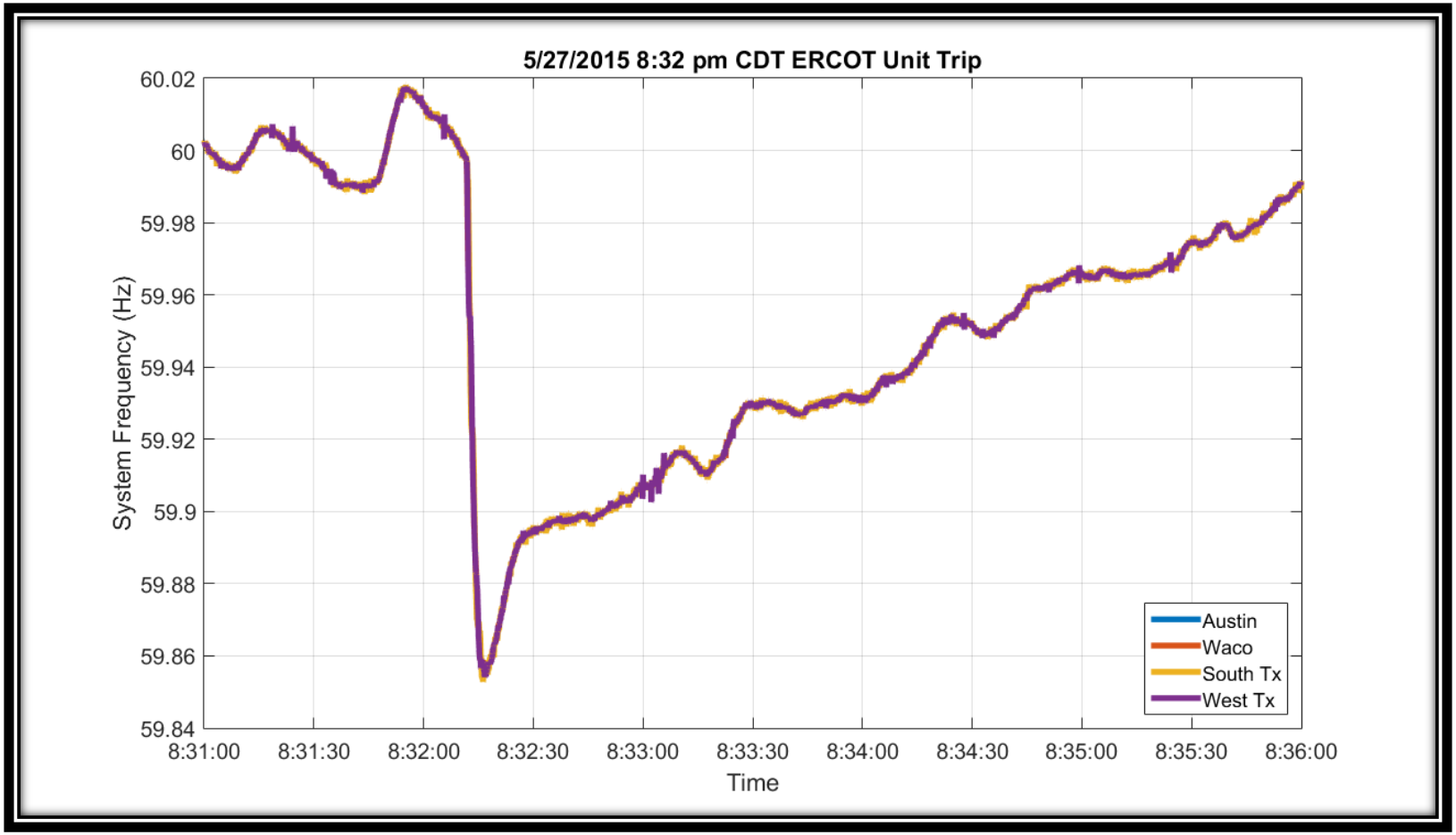
Aggressive Spoof, sliding window



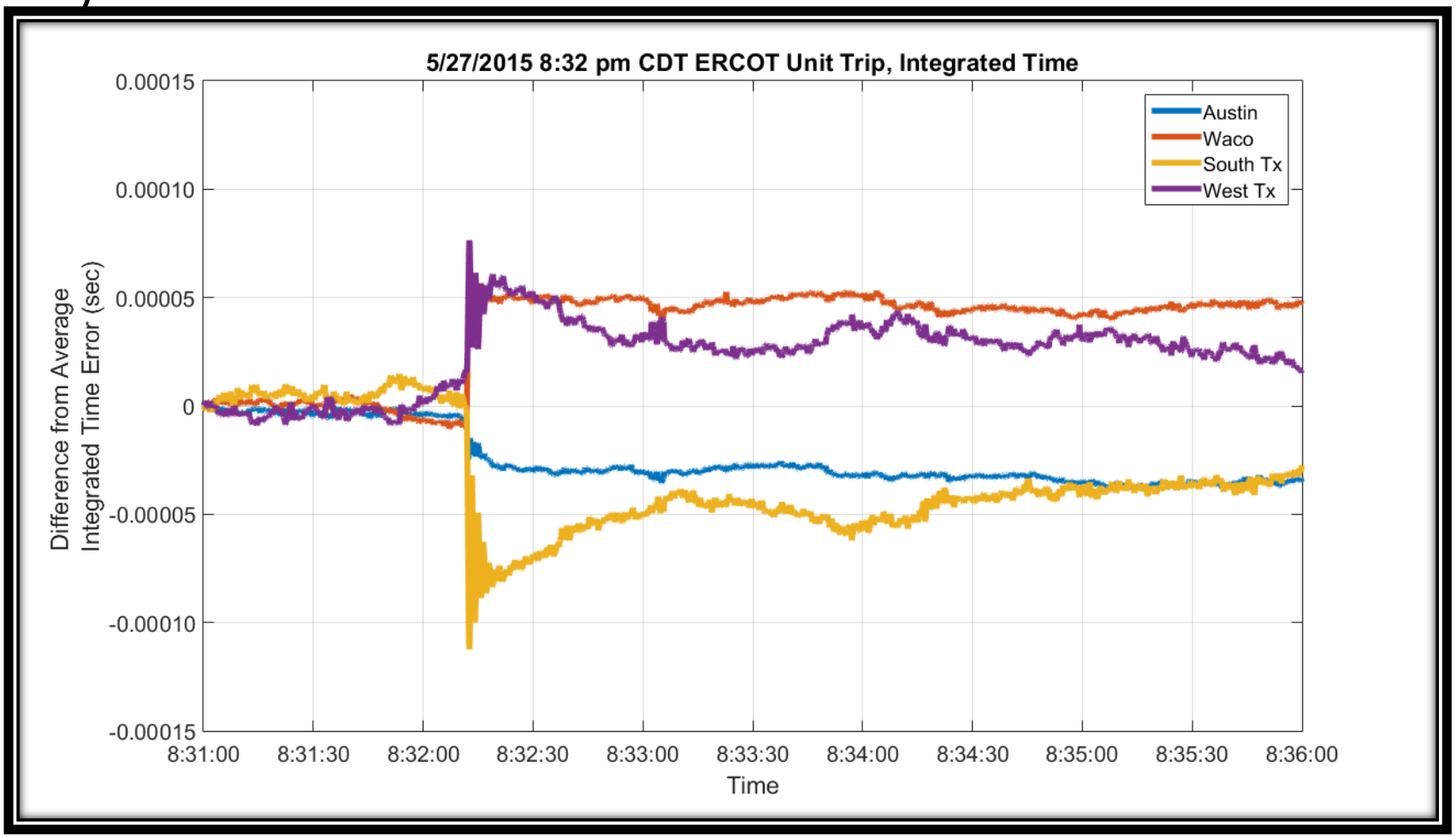
Slow Spoof, sliding window



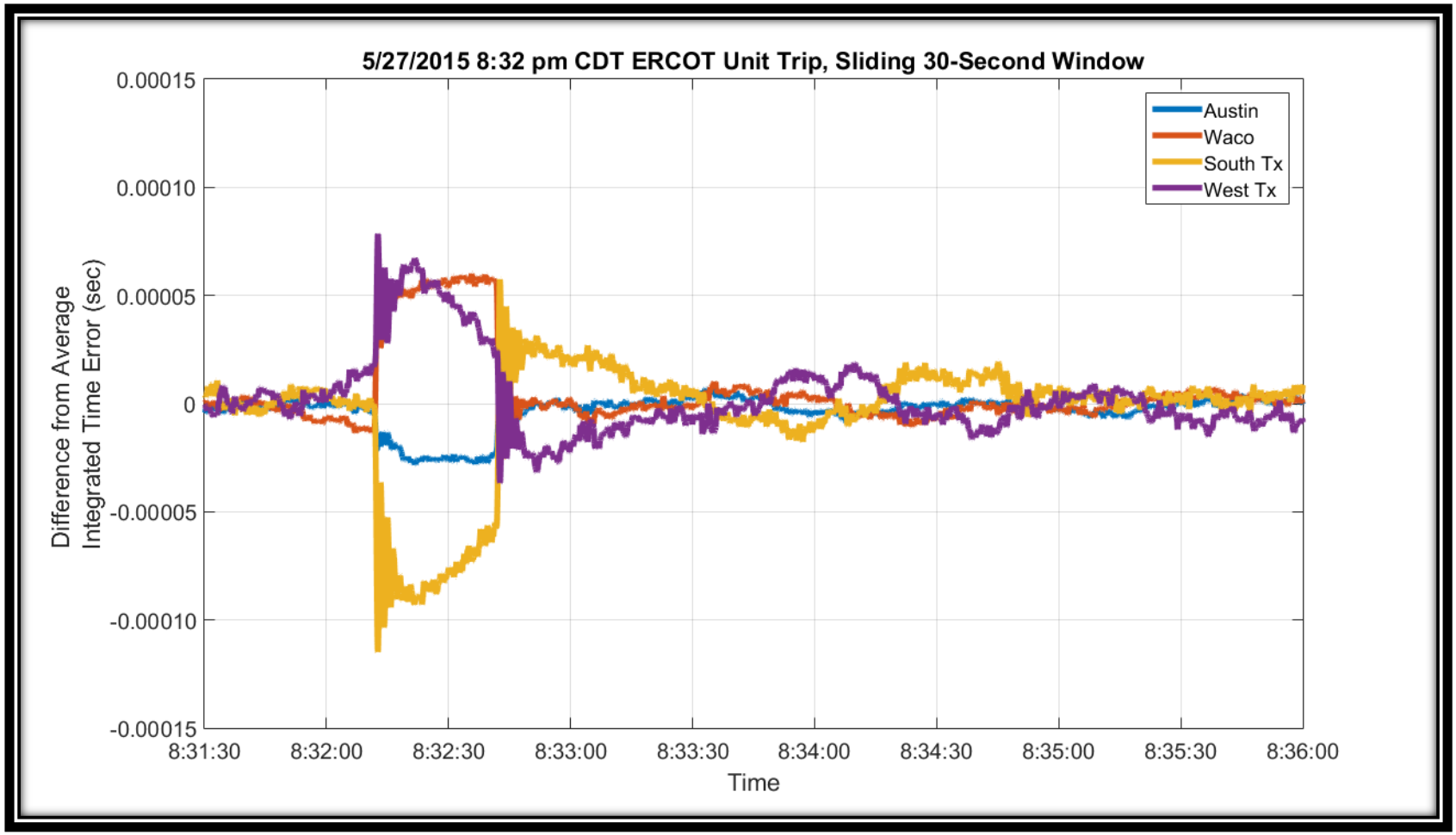
What happens when?



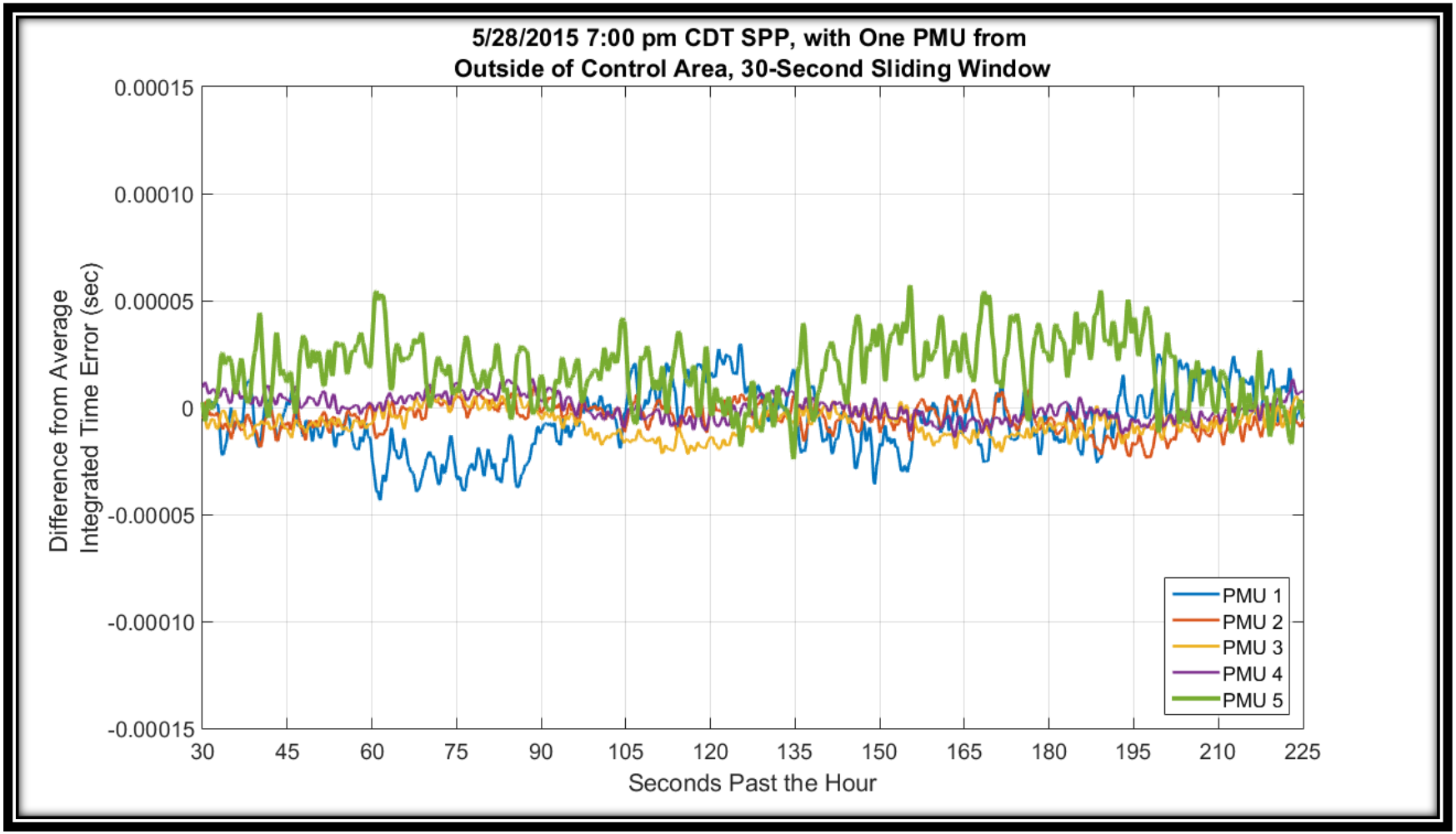
System Transients



System Transients



Outside of Control Area?



Conclusions

- Replacing GPS clocks with spoof-resistant units is not practical for many organizations
- PMU grouping is based on control area
- Applying simple algorithms to frequency measurements can detect GPS spoofing and clock anomalies
- These tunable algorithms may be implemented in phasor data concentrators
- Can this be defeated?
- Resolution of measurement needs testing.

Questions / Comments?

Thank you.