Time Synchronization Interval Attack: Impact and Detection

Jiecheng (Jeff) Zhao[2], Yilu Liu[1,2], Peter Fuhr[2], Marissa E. Morales Rodriguez[2]

1. the University of Tennessee, Knoxville
2. Oak Ridge National Laboratory

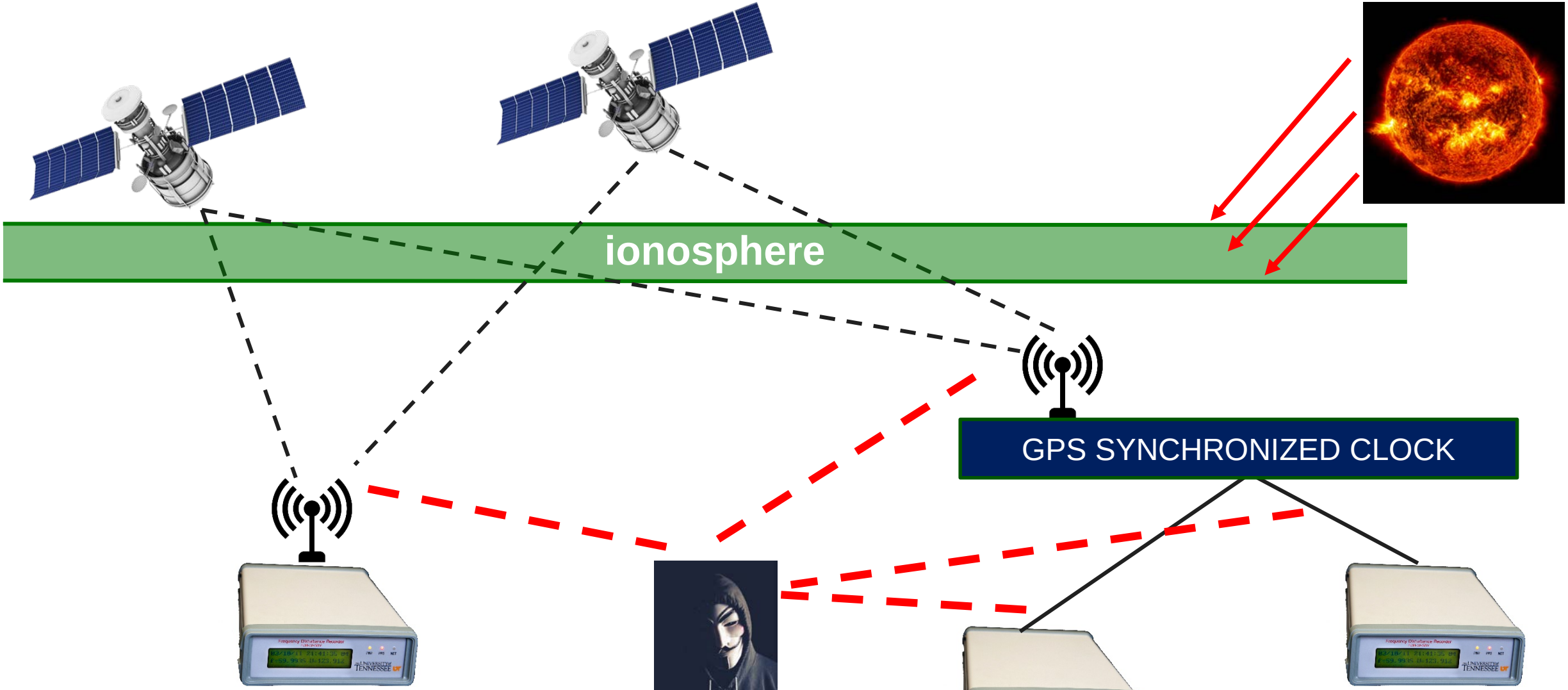
jzhao27@utk.edu

NASPI Work Group Meeting
Apr. 25, 2018

Motivation

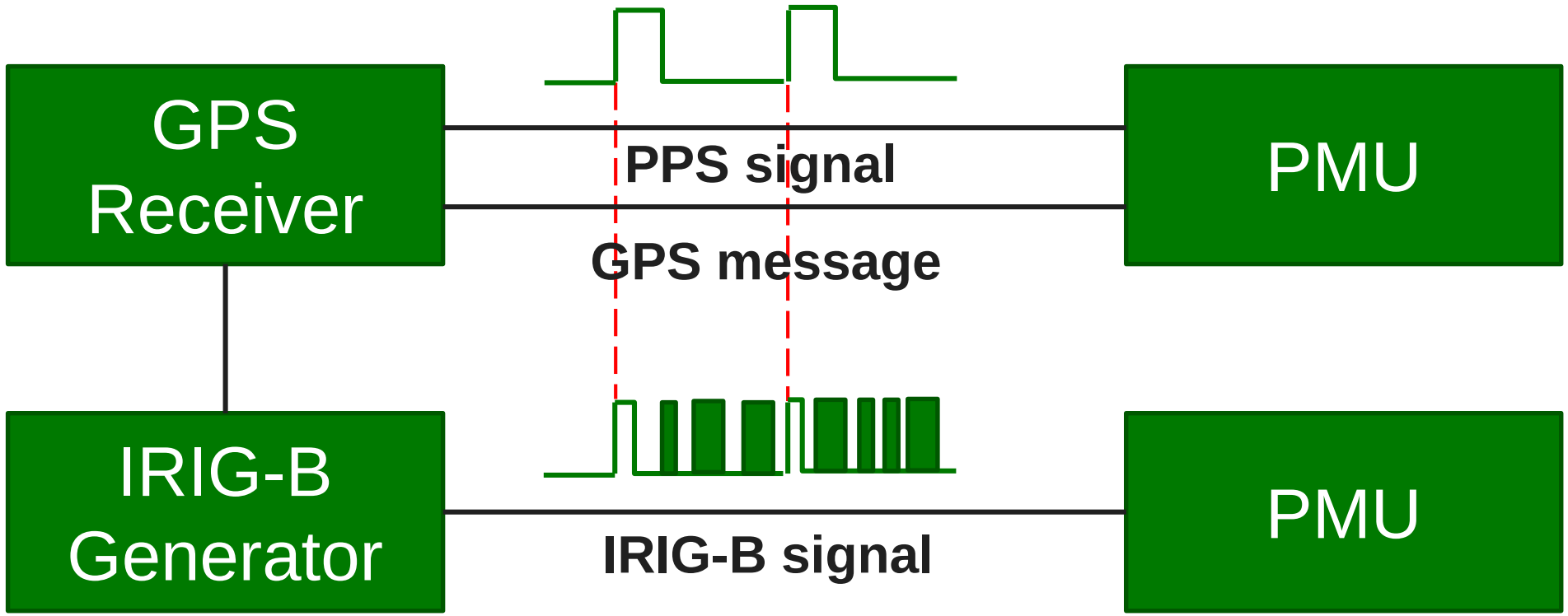
- Performance of PMUs relies on timing source
  - Time stamp
  - Measurement accuracy and synchronization (through PPS)
  - Data availability
- GPS is the main timing source for PMUs
- GPS is vulnerability to interference, system failure, and cyber-attack

Vulnerability of GPS Timing



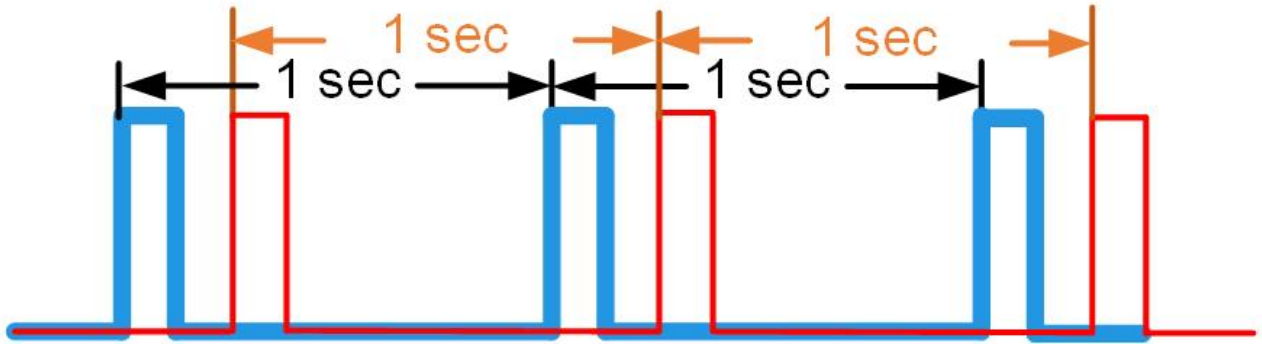
Pulse Per Second (PPS)

- PPS is the synchronized signal for PMU
- Determines the sampling point(s) and interval



Time Synchronization Attack: PPS Shifting

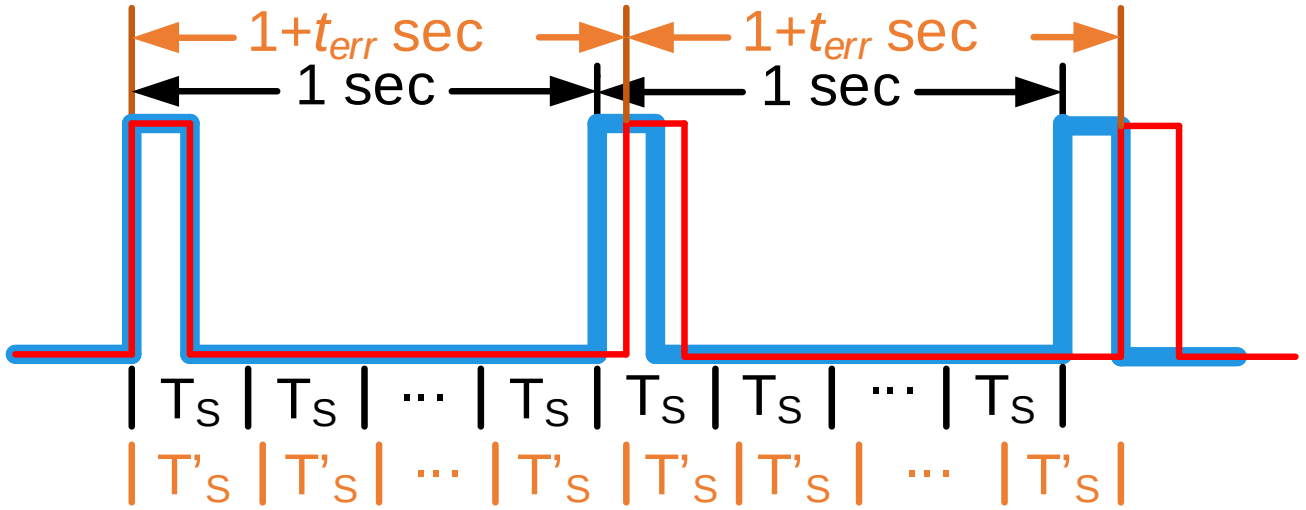
- PPS shifting: a constant PPS error



- Phase angle: constant error proportional to the shift
- Frequency: no influence

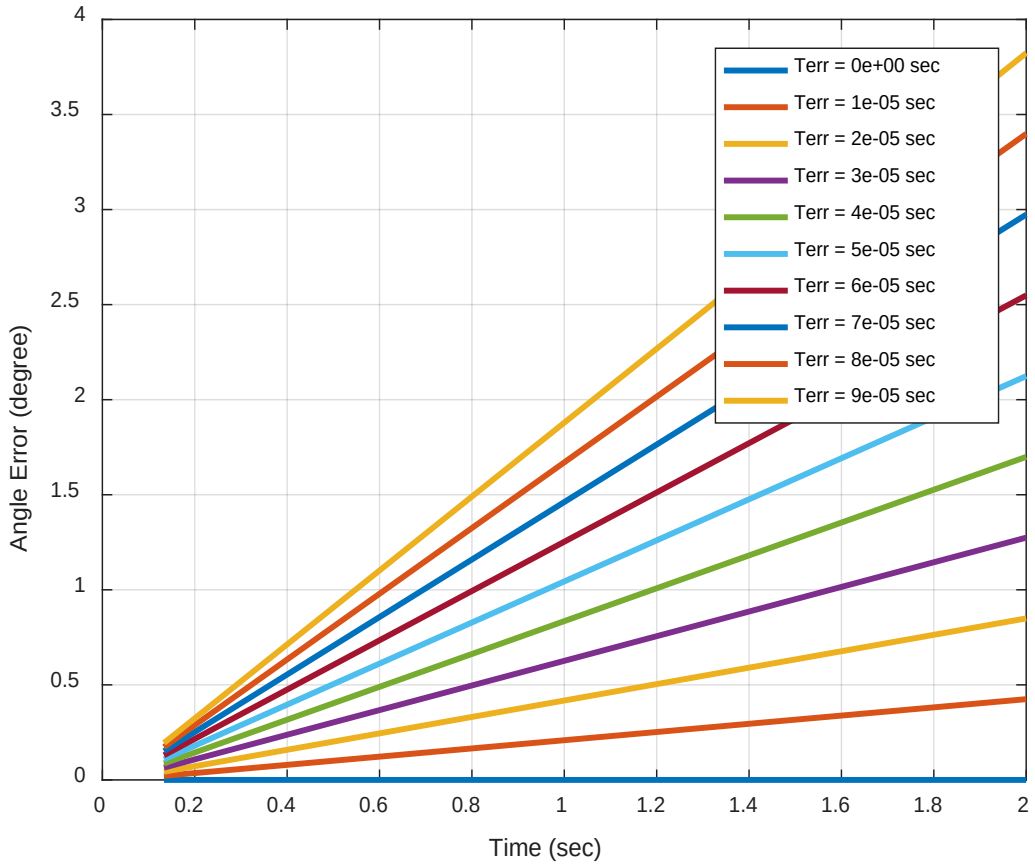
Time Synchronization Interval Attack (TSIA)

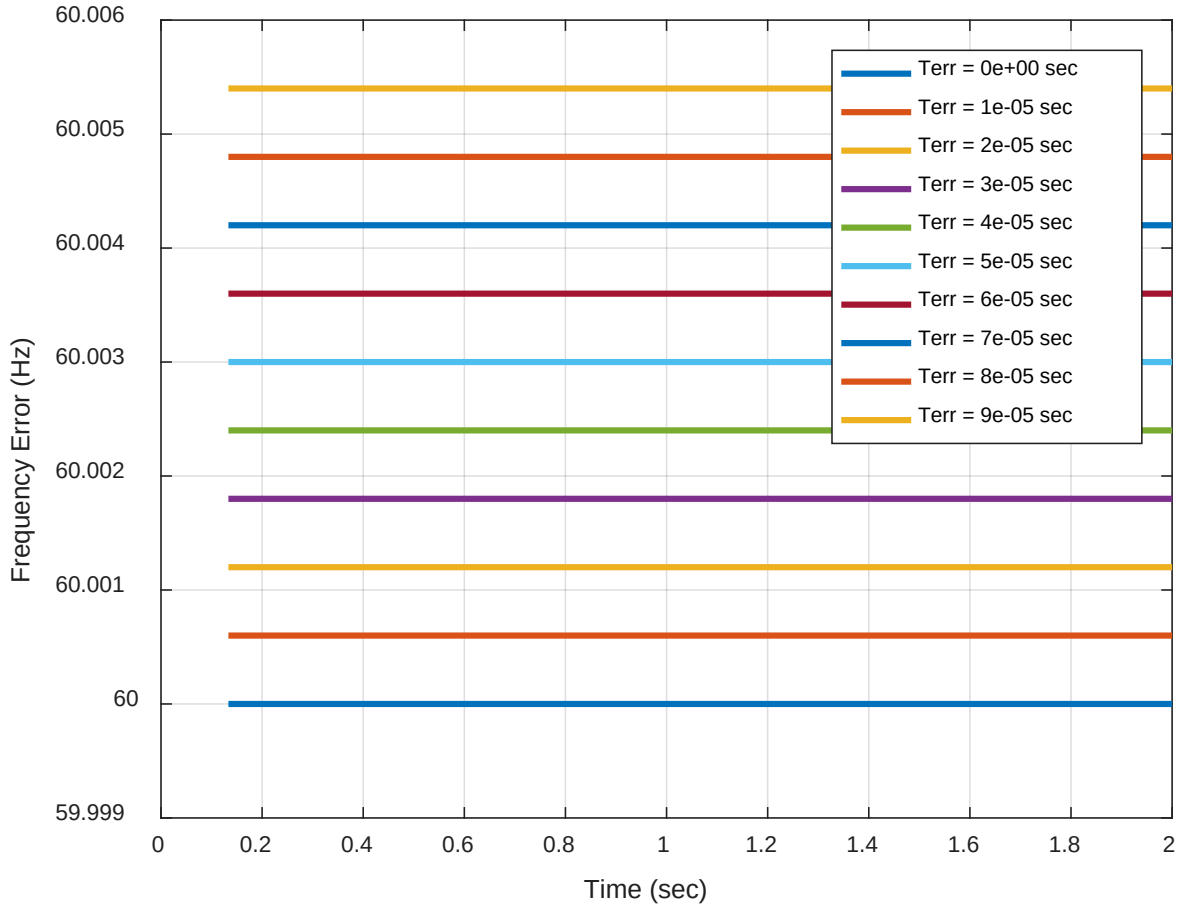
- Change the interval of PPS



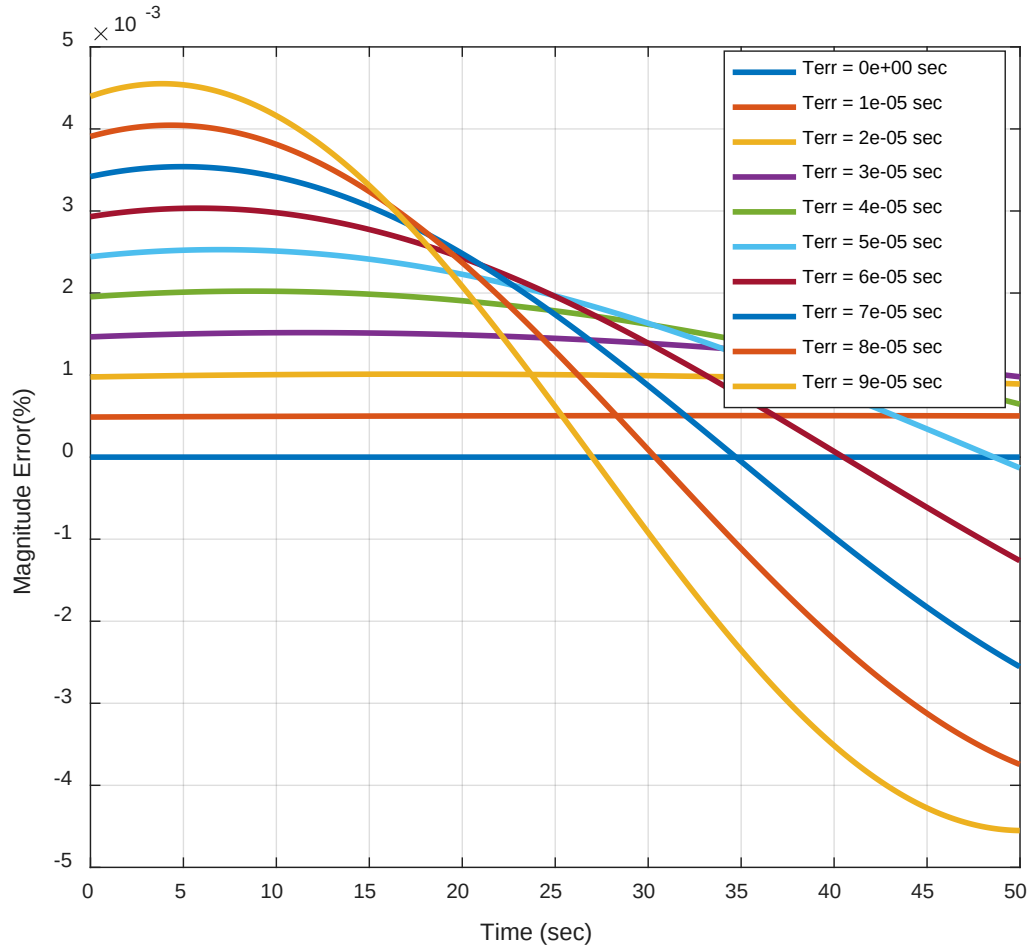
- Synchronization influenced and sampling rate changed
- Impact magnitude, angle, frequency

Constant Attack (error from 10 us to 90 us)





Constant Attack (error from 10 us to 90 us)

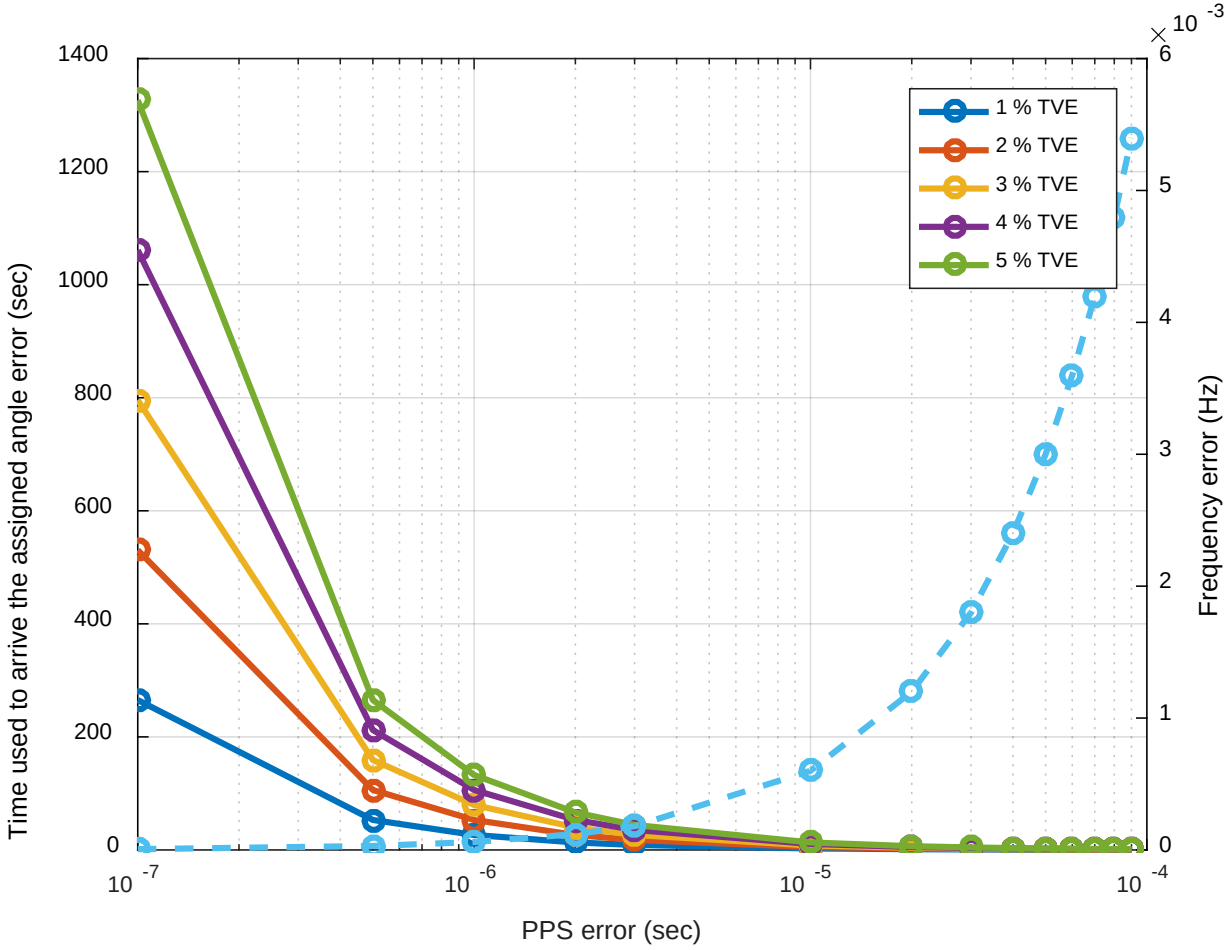


- **Phase angle error**: error increases with time, skew rate mainly depending on the PPS error (major impact)
- **Frequency error**: step change, step mainly depending on the PPS error (moderate impact)
- **Magnitude**: sinusoidal wave, whose magnitude and frequency depends on the PPS error (minor impact)

Impact

Application	Impact	Comments
Phase angle monitoring [1]	2.7° error causes 12% power flow error (NORDIC)	Depends on the power grid
Anti-islanding protection (angle-based) [1]	8° for 10 cycles activates protection scheme (IEEE 9-Bus system)	Larger mismatch accelerates the action
Oscillation damping control [1]	10.73° error increases 13% over shoot and 15.4% setting time 35.6° error causes negative damping (Kundur system model)	Smaller error, though may not cause negative damping, increases overshoot and setting time
Line fault detection and location [2]	20° error: 50 km error (3Φ-G) 10° error: 220 km error (L-G) 10° error: 50 km error (L-L)	Transmission line dependent
Voltage stability [2]	Decrease the active power delivered margin 10° error: from 7.8 p.u. to 0.8 p.u.	Misleads the system to implement wrong actions of voltage stabilization
Event location (TDOA based) [2]	1 sec error causes 35 km	

Comparison



- When PPS error is large
  - Phase angle error increases very fast
  - Frequency error is also large
  - Frequency can be used to detect the attack
- When PPS error is small
  - Phase angle error slowly increases
  - Frequency error is very small
  - Sophisticated attacker may choose this strategy
  - May rely on angle to detect the attack

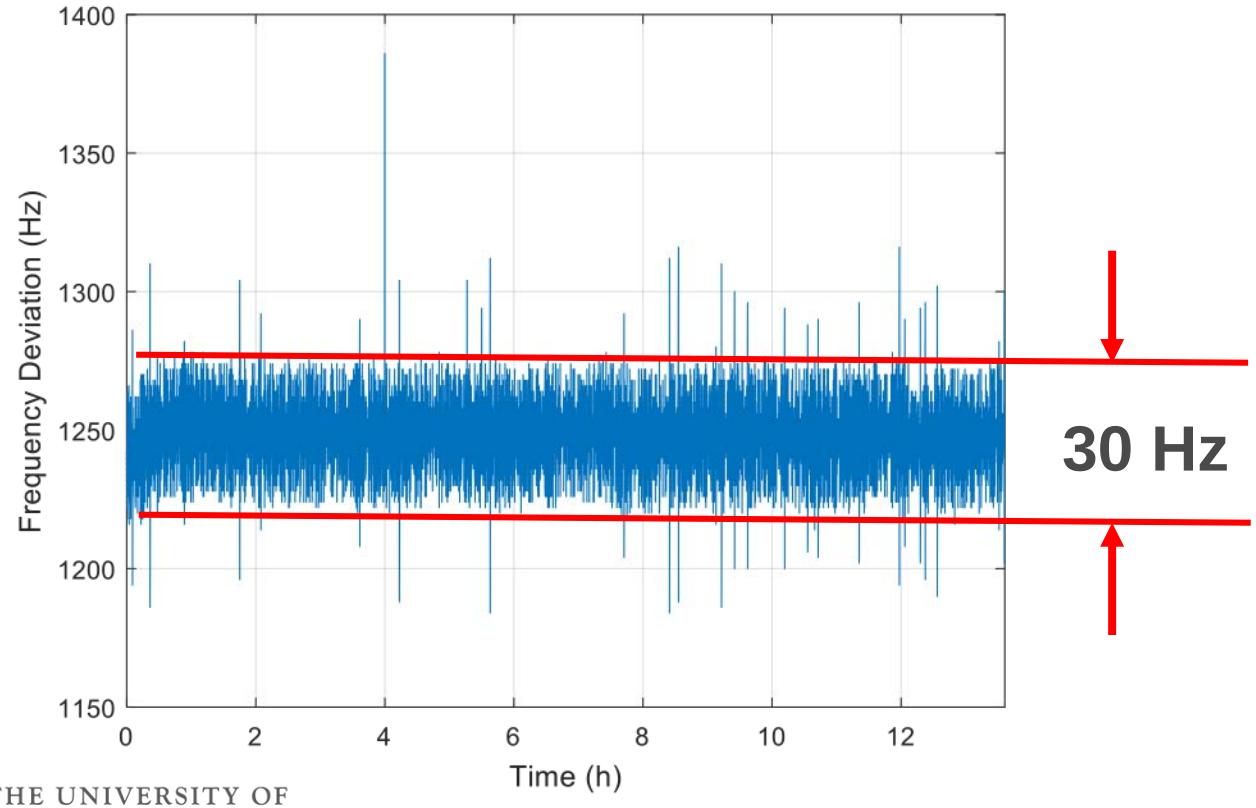
TSIA Attack Detection

- For a large TSIA attack
  - Drift of angle difference
  - Step change and deviation of frequency

- For a small TSIA attack
  - Alternative timing source: GALLEO, eLoran
  - Alternative timing distribution: PTP
  - Local oscillator

TSIA Attack Detection

- An oscillator inside the PMU to inspect the PPS interval
- Capable to detect TSIA attack of 1 us and above



Test of a 40 MHz Oscillator inside PMU

Conclusion

- TSIA could be used as sophisticated attack
- Influence phase angle, frequency, and magnitude
- Impact PMU based applications
- Multiple detection methods

References

[1] M. S. Almas, L. Vanfretti, R. S. Singh, and G. M. Jonsdottir, "Vulnerability of Synchrophasor-based WAMPAC Applications' to Time Synchronization Spoofing," *IEEE Trans. Smart Grid,* vol. PP, pp. 1-1, 2017.

[2] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis," *IEEE Trans. Smart Grid,* vol. 4, pp. 87-98, 2013.

Questions?