Time Synchronization Interval Attack: Impact and Detection

Jiecheng (Jeff) Zhao\textsuperscript{2}, Yilu Liu\textsuperscript{1,2}, Peter Fuhr\textsuperscript{2}, Marissa E. Morales Rodriguez\textsuperscript{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
  o Time stamp
  o Measurement accuracy and synchronization (through PPS)
  o 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

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

• For a small TSIA attack
  o Alternative timing source: GALileo, eLoran
  o Alternative timing distribution: PTP
  o 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

Frequency Deviation (Hz)

Time (h)
Conclusion

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


Questions?