GPS Spoofing Impact Analysis and Detection Techniques

10/29/19

Colin Ponce

Cyber and Infrastructure Resilience

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) sponsored the production of this material under DHS Contract Number HSHQPM-17-X-00140 and DOE Contract Number DE-AC52-07N427344 for the management and operation of Lawrence Livermore National Laboratory.

Lawrence Livermore National Laboratory

GPS Signals and Precision Timing

- GPS receivers can use GPS signals to acquire four pieces of information:
  - x, y, z coordinates.
  - **Time.**

- GPS-based timing has < 100 ns of precision.

- GPS signals are ubiquitous, GPS receivers are cheap.
  - Used for timing in many PMUs.

GPS Spoofing

- **Also cheap:** radio transmitters that can broadcast in the GPS frequency range.
- **GPS Spoofing:** Sending a false signal that imitates a real GPS signal.
- If a GPS receiver locks onto the false signals, can fool the GPS receiver into believing an incorrect time or location.

What impacts can GPS spoofing attacks have on the transmission grid?

Quantities Affected by GPS Spoofing

Type of Quantity	Affected by GPS Spoofing Attacks?
Phase Angle	Yes
Frequency	No
ROCOF	No
Voltage Magnitude	No
Current Magnitude	No

Characterizing Impact

- **No Impact:**
  - No detectable change to operating parameters.
- **Low Impact:**
  - Detectable changes, but operating parameters are still within normal range.
- **Medium Impact:**
  - One or more operating parameters shift outside normal range.
  - Equipment or lines can trip offline, but no loss of load.
- **High Impact:**
  - Loss of load, possible cascading effects.

Operating parameters:

Voltage magnitude, frequency, load, equipment operability.

Phase Drift Attacks On Relays

Using a GPS spoofing attack to bias an angle-based relay's estimation of a power signal's phase angle θ.

Tested using our hardware-in-the-loop laboratory:

- Fed a false timing signal to a transmission relay.
- Timing bias induces a phase angle bias.

- **Sufficient timing bias causes a relay to trip incorrectly.**

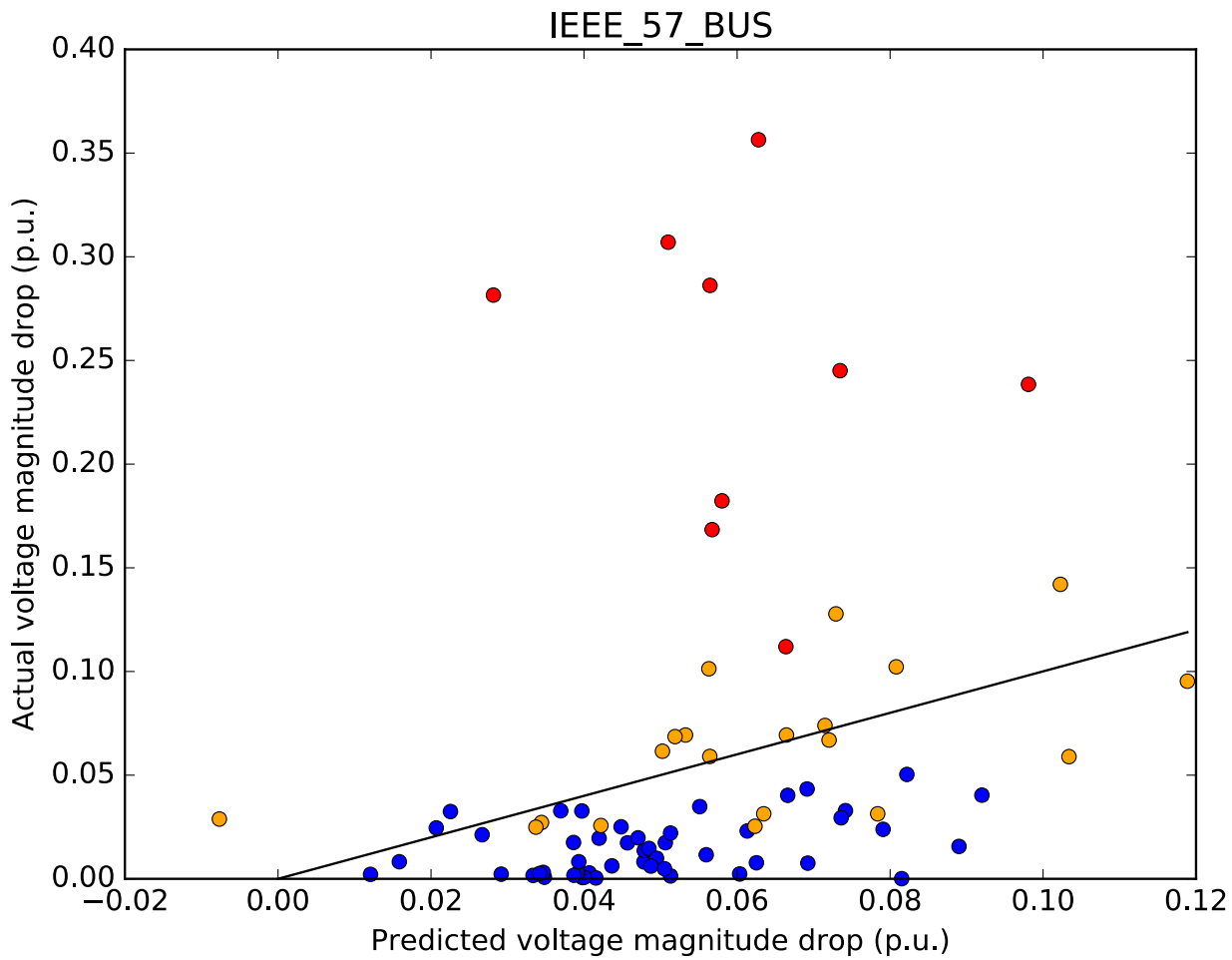
What are the Effects of Phase Drift Attacks?

- Phase drift attacks can cause relays to trip when they shouldn't.
- Causing relays *not* to trip when they *should* is also possible, but less likely.

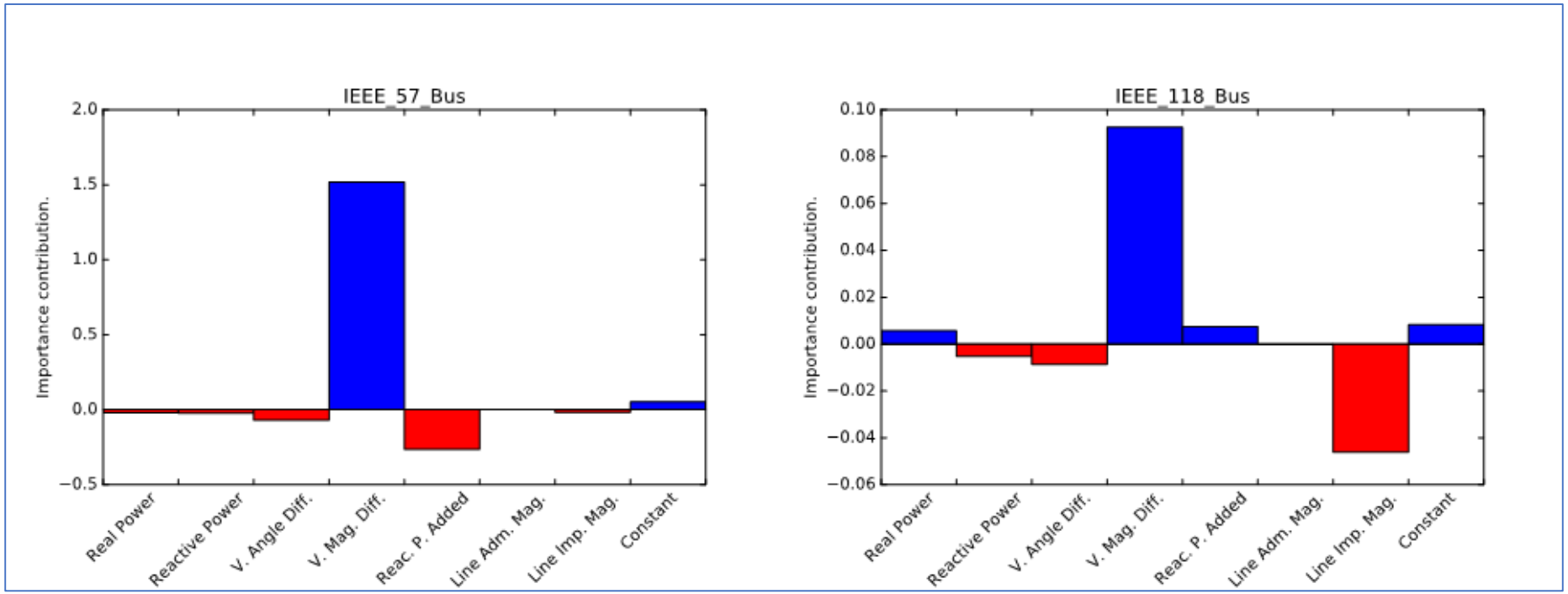
- Focus on inducing trips:
  - What effects can it have?
  - What transmission line properties make them the best targets?

- **Simulate** effects of line tripping on standard test models.
- Perform linear regression to identify important line properties.

Possible Impacts of a Phase Drift Attack

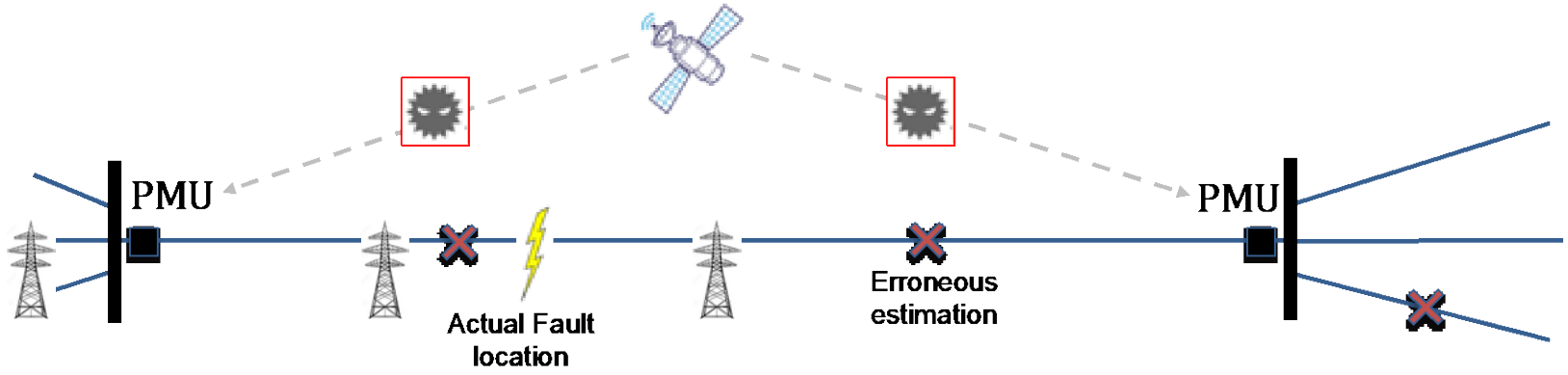


Line Properties Resulting in Big Impact



Conclusion: Phase drift attacks can have a **medium** to **high** impact on the grid, especially when the voltage magnitude difference across a line is large.

Fault Location

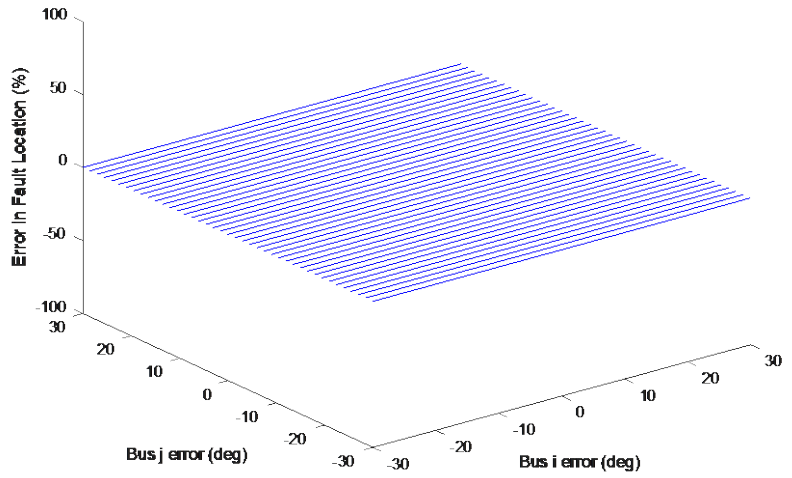


Challenging to locate faults **quickly for repairs** along 100's of km of lines.

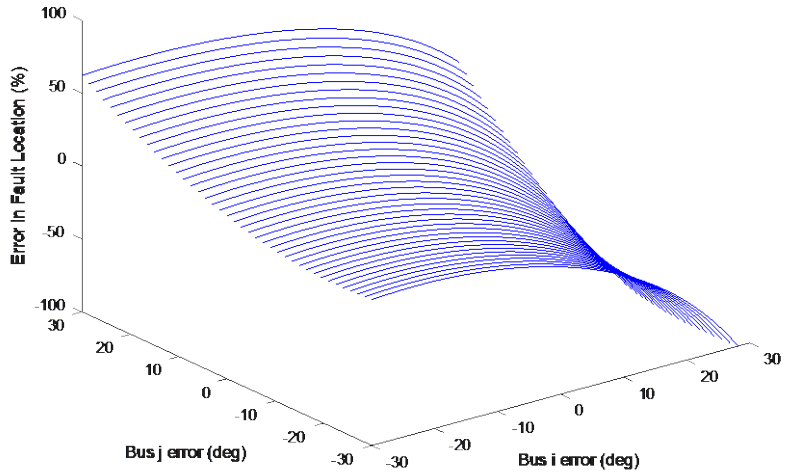
One-sided method: $$m \approx \frac{(V_{i,real}-V_{i,imag})}{r_{ij}(I_{i,real}-I_{i,imag})-x_{ij}(I_{i,real}+I_{i,imag})}$$

Two-sided method: $$m = \frac{(V_{i,real}-V_{i,imag})-(V_{j,real}-V_{j,imag})+r_{ij}(I_{j,real}-I_{j,imag})-x_{ij}(I_{j,real}+I_{j,imag})}{r_{ij}(I_{i,real}-I_{i,imag})-x_{ij}(I_{i,real}+I_{i,imag})+r_{ij}(I_{j,real}-I_{j,imag})-x_{ij}(I_{j,real}+I_{j,imag})}$$

Percent Error in Fault Location from Phase Angle Errors



One-sided method



Two-sided method

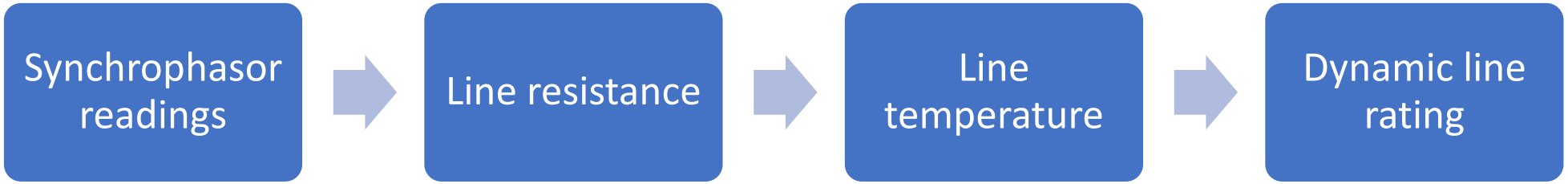
Conclusion: GPS spoofing attacks have **no impact** to **medium impact** (mostly from sending repair crews to the wrong location), depending on the fault location method used.

Dynamic Line Rating (DLR)

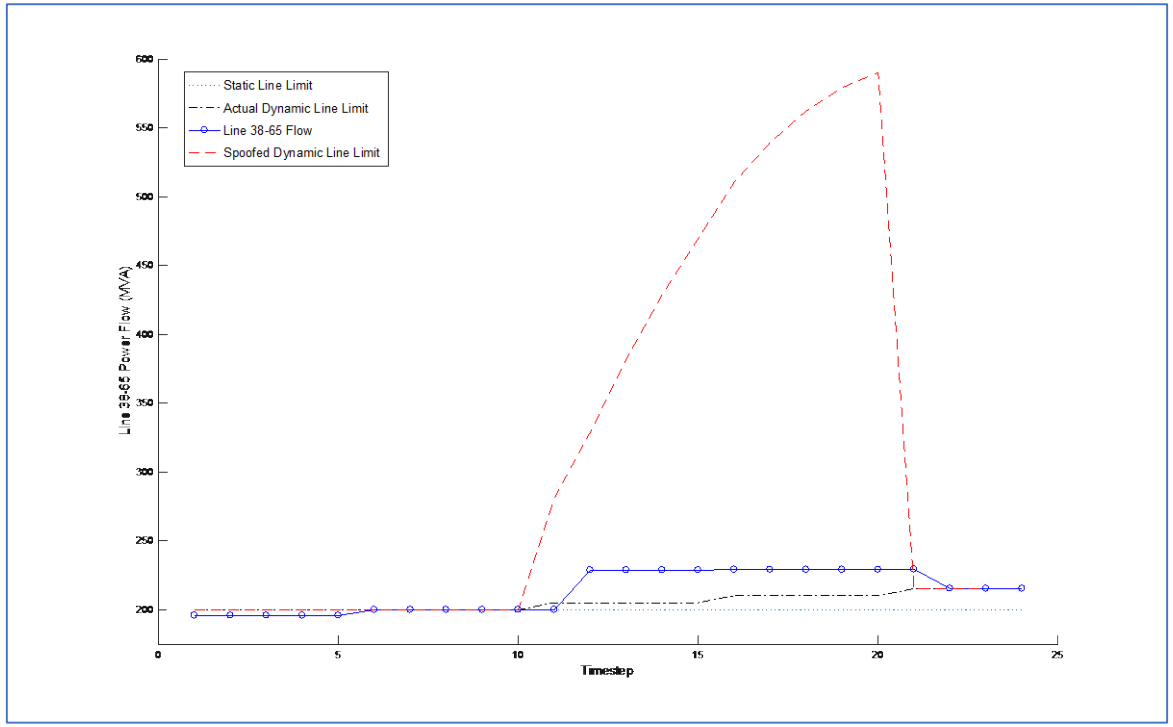
Line rating: Maximum capacity of a line to carry power.

Static line rating: Determined a priori by manufacturer.

Dynamic line rating: Takes into account real-time conditions such as temperature.



Actual DLR, Spoofed DLR, and Power Flow



Conclusion: GPS spoofing attacks can have **medium** to **high** impact on dynamic line rating calculations, as they can result in damage to lines and possible cascading effects.

GPS Spoofing Detection

GPS Spoofing Detection

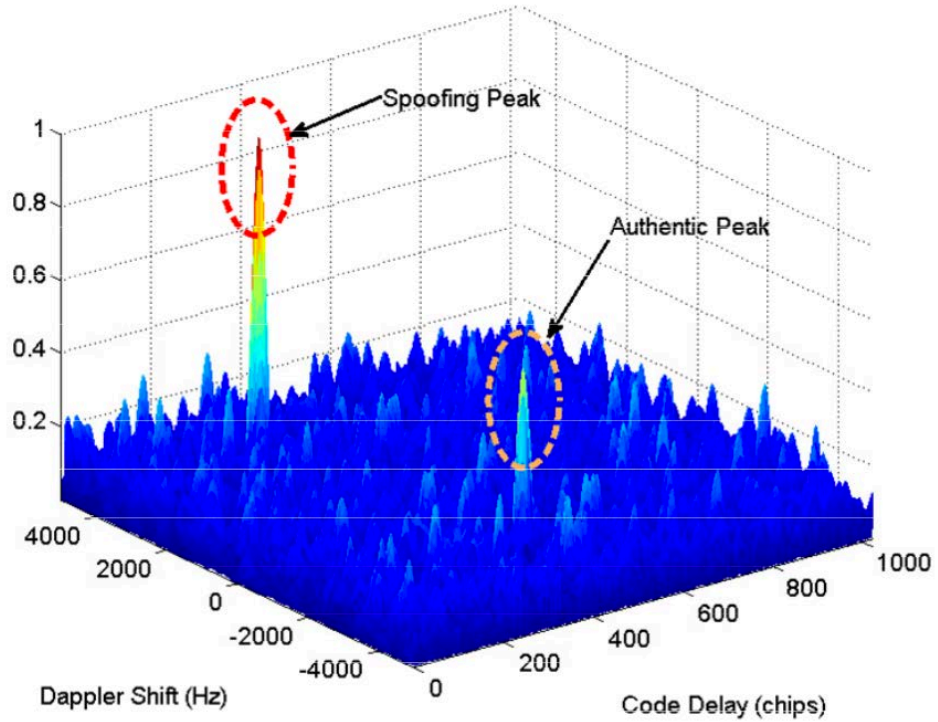
Two approaches:

1. Look for hints in the raw GPS signal known to be associated with spoofing.

2. Data fusion. You typically have available multiple sources of data, one of which is GPS, that are all correlated. Look for anomalous data configurations.

Hints in the Raw GPS Signal

- GPS signals are very weak—typically between -125 dBM and -130 dBM.
  - A significantly stronger GPS signal is suspicious.
- GPS signal acquisition searches through different signal frequencies and phase offsets for a best-match.
  - If a spoofing signal is present, two good matches will appear near each other.



Jafarnia-Jahromi et. al., "Spoofing Countermeasure for GNSS Receivers", *4th Intern. Colloq. on Scientific and Fundamental Aspects of the Galileo Program, 2013*

Data Fusion

- You typically have available multiple sources of data, one of which is GPS, that are all correlated.

- Examples:
  - If another timing source is available, these are clearly correlated.
    - Even lower-precision clocks will still have meaningful correlation!
  - Frequency and voltage magnitude are correlated, both sag under heavy load.
    - What if **just** the frequency sags?

Wide Area Data Fusion

- Data is correlated not just on a single device, but across devices.
- Can look directly at timing correlations between devices, but unless your network is Precision Time Protocol-enabled, correlation is likely weak.
- However, **time-stamped power grid data** is highly correlated.
  - E.g. phase angles between two ends of a transmission line.
- Can analyze wide area data for timing anomalies.
- **Disadvantage:** More sources of data implies more possible types of anomalies – not just GPS spoofing.

Thank you

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) sponsored the production of this material under DHS Contract Number HSHQPM-17-X-00140 and DOE Contract Number DE-AC52-07N427344 for the management and operation of Lawrence Livermore National Laboratory.