GPS Spoofing alters the phasor timing making it appear as if a substation’s phase angle is inconsistent

• Current GPS clocks do not have a way of authenticating GPS signals
• Rely on a 1 pulse per second signal for timing
• Broadcasting a new pulse stronger than actual GPS allows attackers to change time

GPS Spoofing attacks on Phasor Measurement Unit (PMU)

• PMU’s measure voltage and current phasors at a substation
• Alter the reference time for phase angle estimation
• Introduce bias to phase angle measurements from attacked PMUs

GPS Spoofing is a comparatively easy attack to carry out

• Minimal required equipment
• Can be a few miles from substation
• Cost of components is less than $2000

How does this affect power grid control and protection, especially, smart algorithms?

A feature of GPS spoofing attacks is that all the phasor measurements collected from an attacked PMU will have the same phase angle offset

\[ \mathbf{Z}_i = \mathbf{Z}_i - \mathbf{Z}_{\text{atk}} \]

Where \( \mathbf{Z}_i \) is the Authentic PMU measurements from bus \( i \) and \( \mathbf{Z}_{\text{atk}} \) is the Spoofed PMU measurements from bus \( i \).

\[ \alpha = [\alpha_1, \alpha_2, \ldots, \alpha_K] \]: the angle offsets at all \( K \) PMUs induced by spoofing attack. Usually a small subset of PMUs are compromised, thus most entries of are zero, i.e., is a sparse vector.

We employ an iterative sparse optimization algorithm that leverages the knowledge of network topology and line parameters, to estimate the attack vector and correct PMU measurements.

RESULTS ON RTS-96 TEST CASE

Employing our attack-resilient data analytics, your system can:

• Effectively mitigate GPS spoofing attacks on PMU measurements
• Avoid having attacked PMU data affect control decisions
• Make use of PMU data for real time control & protection in a secure way

RESEARCH VISION

Develop attack-resilient data analytics for power system control and protection (that can isolate faults, mitigate damage, and recover lost components) in the presence of on-going GPS spoofing attacks.

OVERVIEW OF APPROACH

• PSSE handles the Dynamic Power System Simulation with standard Protection Devices (Distance, Overcurrent, Frequency trip, etc.)
• The Protection Control Module uses PMU data and simulation results to determine necessary protective and control actions
  o Best fit load shedding limits outage size
  o Determining protection settings in real-time makes the system more resilient reducing unnecessary line or generator disconnects
• The system requires accurate PMU data to avoid incorrect actions in the control systems
  o This is achieved through a Data Correction Module, which recovers PMU data that has been spoofed

IMPACT ON POWER GRID

Cooperation, support and guidance from industry partners in the following areas would benefit this research activity:

• Specifications or methods for coordinating real protection systems
• Alternative uses of phase angle in automated or semi-automated control systems
• Methods to evaluate power system protection performance and hardware validation

Contact: hagantr@oregonstate.edu, desilvas@oregonstate.edu, ecs@oregonstate.edu, jinsub.kim@oregonstate.edu

Activity webpage: https://cred-c.org/researchactivity/Analytics4GridOps