Towards Attack Resilient Data Analytics for Power Grid Operations

Travis Hagan, Shashini De Silva, Galpottage Dilan Senaratne, Arezoo Rajabi, Eduardo Cotilla-Sanchez, Jinsub Kim

GPS SPOOFING ATTACKS ON POWER SYSTEMS

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

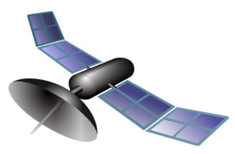
GPS Spoofing attacks on Phasor Measurement Unit (PMU)

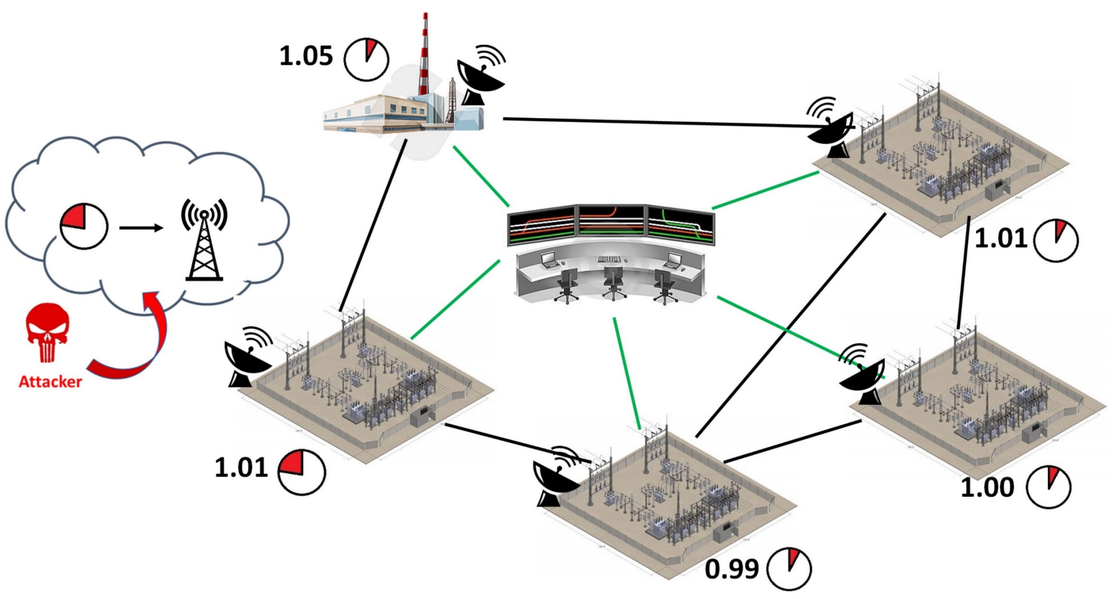
- PMU's measure voltage and current phasors at a substation
- Alter the reference time for phase angle estimation
- Introduce bias to phase angle measurements from attacked PMUs

GPS Spoofing is a comparatively easy attack to carryout

- 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?

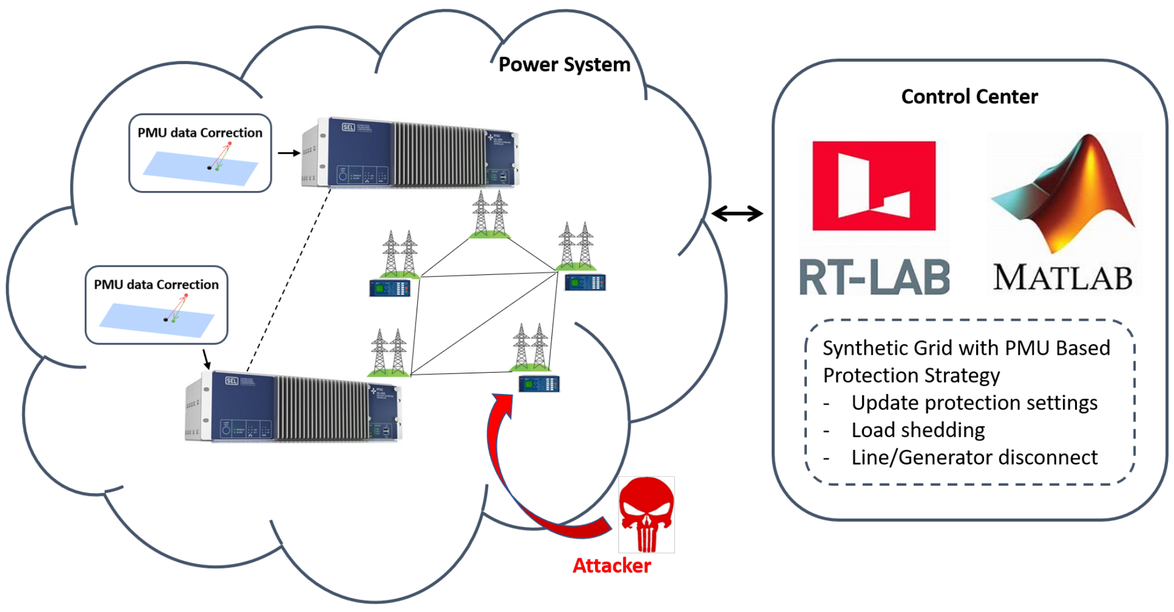




RESEARCH VISION

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

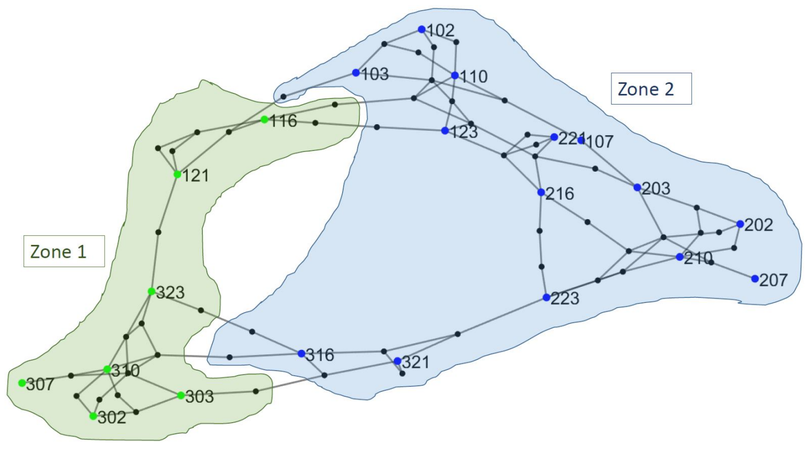


- Each Real Time Automation Controller (RTAC) corrects data in the vicinity
- A high speed connection allows the RTACs to work together to provide wider visibility and correct attacked PMUs between them
- The Control Center uses PMU data and simulation results to determine necessary protective and control actions
  - Best fit load shedding limits outage size
  - 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
  - This is achieved through a Data Correction Module, which recovers PMU data that has been spoofed

DECENTRALIZED PMU DATA CORRECTION

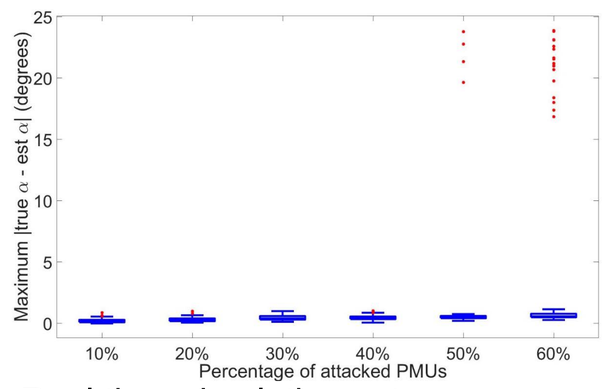
A feature of GPS spoofing attacks is that all the phasor measurements collected from *an* attacked PMU will have the same phase angle offset

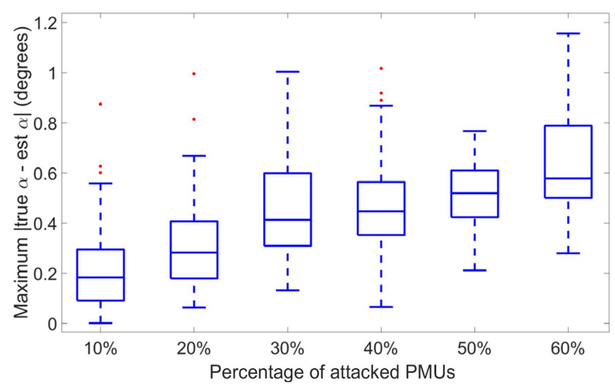
- Effect of the attack on the i^{th} PMU : $\bar{\mathbf{z}}_i = e^{j\alpha_i}\mathbf{z}_i$
  - $\mathbf{z}_i$ - Authentic PMU measurements from bus i
  - α_i - Phase angle offset in bus i
  - $\bar{\mathbf{z}}_i$ - Spoofed PMU measurements from bus i
- $\boldsymbol{\alpha} = [\alpha_1; \alpha_2; \ldots; \alpha_K]$ - sparse vector
- We identify zones in the power network that can perform PMU data correction locally.
- We prove that sparse attack is locally identifiable if the number of spoofed PMUs is less than half of the total number of PMUs in the zone.



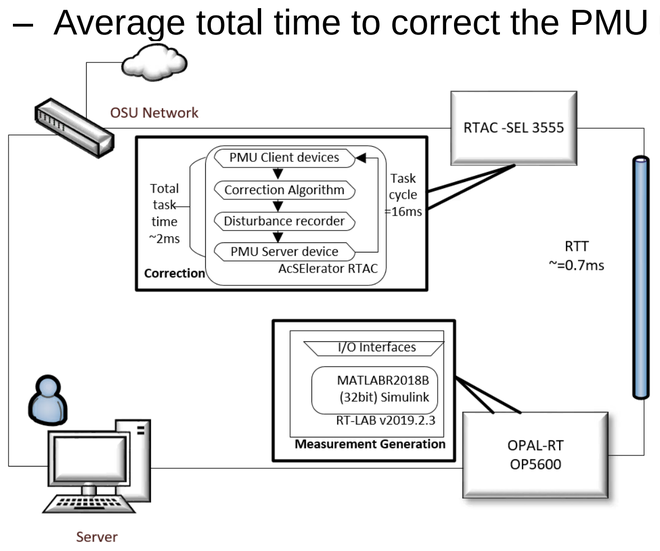
RESULTS ON RTS-96 TEST CASE

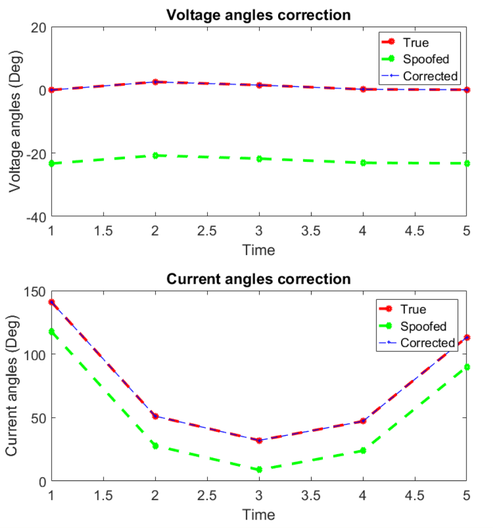
- Simulation results – RTS 96 Zone 2





- Real time simulation setup
  - Average total time to correct the PMU measurements is 2.7 ms





IMPACT ON POWER GRID

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

COLLABORATION OPPORTUNITIES

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, desilvas, senaratg, rajabia, ecs and jinsub.kim} @oregonstate.edu

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

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY