Undetectable PMU Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation

Context

- Synchrophasor measurements are vulnerable to timing attacks:
  - GPS → Spoofing a GPS signal
  - PTP/White Rabbit → Inserting an asymmetric delay unknown to the protocol.
- Can we change the state of the network by just attacking the reference time of a subset of PMUs, undetectable by residual analysis?

System Model

- 1-ph direct-sequence model of a transmission network with \( N \) buses.
- Only PMU measurements (voltage or current).
- \( M \) measurements, measurement vector \( z \) in \( \mathbb{C}^N \).

Attack Model

- Attacker knows \( Y \) and \( H \) matrices.
- He manipulates \( p \) different time references with \( \alpha \), different attack-angles (\( i=1:p \)).
- The attacker applies each \( \alpha \) attack-angle to a subset of PMUs \( (A_i) \).

Results

We applied IoS equation to all possible combination of attack locations to discover undetectable spots

Undetectability

- We use state-of-the-art bad-data detection mechanisms (i.e., \( \chi^2 \) test, Largest Normalized Residual Test) to prove undetectability.
- The residuals are statistically the same before and after the attack.

Impact

- We deceive the network operator into believing that power flows have under- or overutilization.
- Up to 500% error in power-flow estimation

Comparison of the true apparent power flow in two lines and the estimated apparent power flow for the no-attack and attack scenarios

Comparison of \( p \)-values and CDFs of\( \chi^2 \)-values for the\( \chi^2 \) test applied to two attack locations: ideal location (in red), and lowest IoS performer location (in blue). New attack case is illustrated in gray.

References