Timing Vulnerabilities in Phasor Measurement Units

Rohan Chabukswar and Bruno Sinopoli
rchabuks@andrew.cmu.edu, brunos@ece.cmu.edu
Electrical and Computer Engineering

Phasor Measurement Units

"MRI of The Power System"
Power Grid Corporation of India Limited, on Schweitzer Engineering Laboratory's Synchrophasor System

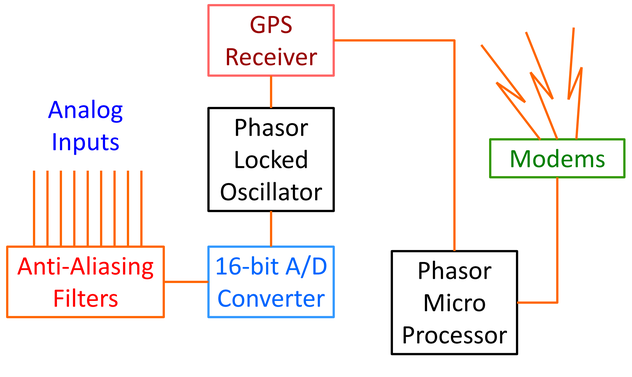
❖ Synchrophasors

- Voltage and current phasors measured synchronously at widely dispersed locations on power grid
- Can be compared in real time
- Improve upon traditional state estimation, calculated using unsynchronized data points collected every 2-4 seconds
- Can be used to provide a comprehensive dynamic overview of the system state in real-time, assess state of electrical system and manage power quality

❖ Phasor Measurement Units

- Invented in 1988 at Virginia Polytechnic Institute and State University, by Dr. Arun G. Phadke and Dr. James S. Thorp
- Output precisely time-stamped Synchrophasors
- One of the most important measuring devices in the future of power systems
- Used for:
  - Wide-area monitoring and control
  - High-precision state estimation
  - Forensic event analysis
  - Adaptive load shedding
- Synchrophasor system consists of Phasor Data Concentrators (PDCs) which collect data from several PMUs and communicate to the Supervisory Control and Data Acquisition (SCADA) system.

PMU Block Diagram



(Adapted from R.F. Nuqui, "State Estimation and Voltage Security Monitoring Using Synchronized Phasor Measurements", Doctorate Dissertation, Virginia Polytechnic Institute, Blacksburg, VA, July 2, 2001.)

Global Positioning System

❖ Accuracy Requirements

- For 60 Hz systems, PMUs must deliver between 10 and 30 synchronous reports per second depending on the application
- Accuracy of ±0.5 µS necessary for synchrophasor measurement
- Global Positioning System (GPS) provides necessary accuracy along with synchronization among geographically distant PMUs and PDCs

❖ Vulnerability

- PMUs are protected against loss of GPS signal, unintentional or otherwise — use internal reference clock for several seconds
- GPS broadcasts can be spoofed without jamming
- Practicality of GPS spoofing established by the work of Prof. Brumley et al, Carnegie Mellon University
- Attack involves fabricating a counterfeit signal from a GPS satellite, placing an antenna to ensure fake signal drowns out real one
- A properly orchestrated attack will change time-stamps on PMU measurements, causing a phase difference in State Estimation (SE)

❖ State Estimation Defense

- Bad Data Detection removes false measurements prior to SE
- Attack can only be successful if Bad Data Detection is evaded

Linear Analysis

❖ Assumption

- Measurements are linear functions of state
- Lines are reactive lossless and only reactive
- Voltage magnitudes are 1 pu — only phases need to be estimated
- Current injections at both ends of branch are equal and opposite
- Voltage phase differences are small

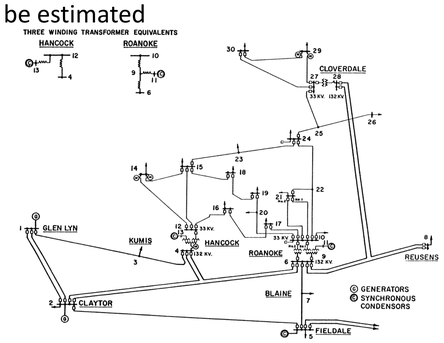
❖ Extent of Disruption

- Measurement Function: $\mathbf{y} = \mathbf{f}(\mathbf{x})$, Jacobian: $\mathbf{H} = \frac{\partial \mathbf{y}}{\partial \mathbf{x}}$
- State Estimation: $\hat{\mathbf{x}} = \left(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z}$
- Measurement Estimation: $\hat{\mathbf{z}} = \mathbf{H}\mathbf{x} = \mathbf{H}\left(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z} = \mathbf{K}\mathbf{z}$
- Residues (used for BDD): $\mathbf{r} = \mathbf{z} - \hat{\mathbf{z}} = \underbrace{\left(\mathbf{I} - \mathbf{K}\right)}_{\kappa}\mathbf{z}$
- Attacker wants to add attack vector **a** to measurements **z** — attack will fail if **a** is in null space of (**I**−**K**)
- All column vectors of **H** are in the null space of (**I**−**K**) — any linear combination of the columns is a valid attack vector
- Convex/Non-Convex Optimization gives desired attack vector

Non-linear System

❖ Failure of Linear Assumptions

- Lines are lossy, measurements are non-linear functions of state
- Unequal current injections increase possible measurements
- Voltage magnitudes must be estimated
- Systems are complex
- IEEE 30-bus system
- Shown in figure
- 30 Buses
- 41 Branches
- 59 States
- 224 Measurements



Simulation Results

❖ System Assumptions — IEEE 30 Bus System

- PMU on 10 out of 30 buses measure
  - Bus voltage magnitudes and phases
  - Current magnitudes and phases for all connected branches

❖ Attacker Assumptions

- Changes time on Bus 27 PMU by 6 µS

❖ Observations

- Without attack, 0 bad data, $\Delta V = 6\times10^{-5}$ pu, $\Delta\phi = 2\times10^{-3}$° (max)
- Under attack, 3 bad data, $\Delta V = 0.014$ pu, $\Delta\phi = 0.3$° (max)
- Max. change in active power estimate: 0.024 pu, 28%
- Max. change in reactive power estimate: 0.0700 pu, 104%

Conclusions & Future Work

❖ Effect of PMU Timing Attacks

- Attack on 1 PMU out of 10 can cause significant estimation error
- Estimation of active/reactive power can change widely, can cause:
  - Change Adaptive Load-Shedding Strategy
  - Change in Control Strategy
  - Change in Electricity Pricing

❖ Future Work

- Theoretically estimate disruptions
- Optimize attack vector — maximum damage, minimum detectability
- Perform hardware-in-the-loop simulations
- Improve detection scheme to prevent timing attacks

Electrical & Computer ENGINEERING

This research was supported by NSF Grant number CCF-042442, "Team for Ubiquitous Secure Technology (TRUST) and the US Army Research Office Grant number W911NF0910273, Perpetually Available and Secure Information Systems.