Using Synchrophasor Measurements to Detect Cyber Attacks on Distribution Grids

2017-3-22 NASPI Meeting

Alex McEachern, Power Standards Lab
Alex@PowerStandards.com
Sean Peisert, Lawrence Berkeley National Lab
C.P. McParland, Lawrence Berkeley National Lab

All errors attributed to Alex, all good ideas attributed to Sean and Chuck, due to Alex's scheduling problems making it impossible for Sean and Chuck to review.

Background on grid cyberattacks (1)

- Policy / political background
  - Hackers
  - State-sponsored adversaries
    - Avoiding acts of war
    - Requirements for “Proportional Response”
    - Detection / monitoring is critical element

This slide: Alex McEachern, not co-authors…

Background on grid cyberattacks (2)

- Technical background
  - Self-destructive nature of the grid
    - It's a closer match with explosives factory than with internet
  - Types of attacks
    - Change the state of a switch, and lie about its state
    - Change the control algorithm in an intelligent grid device
  - Nature of engineers
    - Risk averse
    - Tests and rehearsals (aligns with policy)
    - Rehearsals must
      - have no functional effect (policy)
      - Be confirmable (technical)

This slide: Alex McEachern, not co-authors…

Background on grid cyberattacks (3)

- Nature of cyber defense at utilities
  - "t present, focused on attacks against digital relays and specific commands, not necessarily the effects of those commands
  - Opportunity to add physics-based detection
    - Volts, amps, impedance, synchrophasors…
    - Physics detection informs & narrows bit/packet detection targets
  - Still in organization silos – how do we overcome?
  - Still focused on generation/transmission – how do we include distribution and end-use?

Microsynchrophasors to detect distribution grid cyber attacks

This research was supported in part by the Director, Office of Science, and the Director, Office of Electricity Delivery and Energy Reliability, Cybersecurity for Energy Delivery Systems program, of the U.S. Department of Energy, under contract DE-AC02-05CH11231.

Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the sponsors of this work.

Microsynchrophasors to detect distribution grid cyber attacks (1)

- Use dispersed microPMUs to report actual grid configuration
- Compare actual grid configuration to intended grid configuration
- Difference indicates possible attack
- Example: Source impedance of a distribution feeder, and substation bus-tie switch attack

(patent issued)

Microsynchrophasors to detect distribution grid cyber attacks (2)

- Use microPMUs to reverse-engineer the control algorithm parameters in intelligent grid devices
  - Continuous, automated reverse-engineering
  - Example: Tap changing regulators (upstream)
  - Example: Capacitor switches (downstream)
- If control parameters change abruptly, possible attack…

A couple of notes (1)

- Algorithms rely on secure and reliable data communication
  - PMU data is always vulnerable to replay-type attacks
  - Secure microPMU communication is being actively investigated
  - Does not necessarily use the utility comms systems
- May not require synchrophasor measurements…
  - Very high resolution magnitudes, combined with precision time stamps, may be enough in some cases

A couple of notes (2)

- The most useful information is seen during non-steady-state grid conditions.

- New technique to use ordinary, in-use distribution transformers for ultra-precise measurements of distribution-level microsynchrophasors (patent pending)

A couple of notes (3)

- Practical availability of the concept, and the underlying technology
  - PSL has developed the sensor
  - LBNL & partners (ASU, PSL, etc…) have developed the methodology to detect capacitor bank switches + transformer tap changes
  - Ready to test at utilities – tests planned over next few months.

Conclusions

- Distribution grid cyber attacks are happening.
- Detecting rehearsals of these attacks aligns with policy and technical goals, especially for attacks originated by state adversaries.
- Microsynchrophasor measurements show promise for detecting distribution grid cyber attack rehearsals.

Using Synchrophasor Measurements to Detect Cyber Attacks on Distribution Grids

2017-3-22 NASPI Meeting

Alex McEachern, Power Standards Lab
Alex@PowerStandards.com
Sean Peisert, Lawrence Berkeley National Lab
C.P. McParland, Lawrence Berkeley National Lab

All errors attributed to Alex, all good ideas attributed to Sean and Chuck, due to Alex's scheduling problems making it impossible for Sean and Chuck to review.