Distributed Detection of Cyber Attacks against Power Grids

Hideaki Ishii
Dept. Computational Intelligence and Systems Science
Tokyo Institute of Technology

Workshop on Distributed Energy Management System
Waseda University
December 11th 2015
Acknowledgement

- Yacine Chakhchoukh (Tokyo Tech)
- Yasunori Isozaki (Tokyo Tech)
- Takashi Onoda (CRIEPI (Central Research Institute of Electric Power Industry), Japan)
- Isao Ono (Tokyo Tech)
- Yasuhiro Hayashi, Shinya Yoshizawa, and Yu Fujimoto (Waseda Univ.)

- EMS-CREST Project (Program Head: Masayuki Fujita)

Japan Science and Technology Agency
Cyber Security in Power Systems
Future Power Systems with More ICT

- More complex due to renewable generation sources and competitive electricity markets
- Real-time diagnostic and monitoring for stable operation and lowering cost
- Development of new energy management systems with ICT is necessary.
SCADA Systems

Supervisory Control & Data Acquisition (SCADA)

- To monitor/control, networks connect operator terminals and control devices.
- Physically operates the devices, and thus safety and security are critical.

Conventional Systems: Connection via isolated networks

Future Systems: Use general ICT techniques, Connection to business networks

Cyber security related issues
Importance of “Defense in Depth”

- Firewalls
- Virus Detection
- Authentication
- Encryption
- **Intrusion Detection**
  Monitor networks and detect malicious communication due to faults/attacks
Intrusion Detection in SCADA

ICT Systems for Business

- Known types of attacks: Apply established methods

SCADA Systems

- Known types and illegal communication:
  
  With sufficient data, detection may be possible

- However, if the communication is legal, but is intended to control devices, reliability and safety can be affected.

Conventional ICT-based detections are not enough!
Research Objective

Goal: To Detect Coordinated Attacks against SCADA Systems

- We must prevent malicious manipulation of control devices.
- What control information is useful for intrusion detection?

Model-Based Distributed Approach

- Construct models of the system under normal condition
- Detect when the system condition becomes abnormal

Comm. Network: Probabilistic model based

Integration of Detection Info

Power Grid: Dynamical model based
In This Talk

- Cyber security in power systems
- Objective of this research
- Transmission systems: Attacks against state estimation
- Distribution systems: Attacks against voltage regulation
Analysis of Attacks against State Estimation of Transmission Systems
State Estimation in the Power Grid

- Important for contingency analysis, load forecasting, control, and evaluating locational marginal pricing for power markets
- Evaluate bus voltage magnitudes and phase angles using measurements of power injection and power flows

IEEE 14 bus system
AC State Estimation

- Estimate the state (voltage magnitude and phase angles) from the measurements (active/reactive power, power flows)

\[ z = h(x) + e, \quad x \in \mathbb{R}^n, \quad z \in \mathbb{R}^m, \quad n < m \]

- \( h(\cdot) \): Nonlinear function

- \( e \): Gaussian noise with \( \mathbb{E}[e] = 0, \mathbb{Cov}[e] = R \)

- Estimated state via weighted least squares (WLS) after linearization:

\[
\hat{x}^{k+1} = \hat{x}^k + \left[ H^T(\hat{x}^k)R^{-1}H(\hat{x}^k) \right]^{-1}H^T(\hat{x}^k)R^{-1}(z - h(\hat{x}^k))
\]

- \( H \): Jacobian matrix of \( h(\cdot) \)

State Estimation: Linearized Method

- Linearized model with $\text{Cov}[e] = I$ after scaling:
  \[ z = H\hat{x} + e \]

- LS estimator: $\hat{x} = \arg \min ||z - H\hat{x}|| = \left[H^T H\right]^{-1} H^T z$

- Residual vector: $r = z - H\hat{x}$

- **Bad data detection**: To find outliers, it is common to analyze the residual of WLS: $z - h(\hat{x})$
  
  1. Chi-square test: Check if
  \[ \sum_{i=1}^{m} \frac{(z_i - h_i(\hat{x}))^2}{R_{ii}} > \chi^2_{m-n,p} \quad \Rightarrow \text{Bad data present!} \]
  
  2. Largest normalized residual test: Check if
  \[ \frac{|z_i - h_i(\hat{x})|}{\sqrt{R_{ii}S_{ii}}} > 3 \quad \Rightarrow \text{Remove } z_i \text{ and redo estimation} \]
False Data Injection Attacks

- Consider an attack as \( z_c = z + Hc \)
  
  = true measurement + false data

- Then, the estimated state becomes
  \[
  \hat{x}_c = \left[ H^T H \right]^{-1} H^T z_c = \hat{x} + c
  \]

- But the residue remains the same:
  \[
  r_c = z_c - H\hat{x}_c = (z + Hc) - (H\hat{x} + Hc) = r
  \]

- **Stealthy attack**: State is manipulated by \( c \), but residual is unchanged.

- Residual analysis in bad data detection is not effective.

L. Xie, Y. Mo, and B. Sinopoli (2010), ...
Attacks on the Measurement Function

- We consider attacks on the Jacobian matrix:

\[ H_c = H + \delta H \]  \hspace{1cm} \text{(called leverage points)}

- by modifying network topology estimates at SCADA, or
- by changing line parameter values

- Our approach is based on
  - Robust estimation methods
  - Decomposition of the grid

Robustness against Outliers

- If some measurements don’t follow theoretical assumptions, estimation performance can degrade severely.
- Robustness must be enhanced against outliers.
- Outliers in matrix $H$ can result in biased WLS estimates.
  - Not detectable from the residuals

$$z = Hx + e$$
Robust Statistics Methods

- **Least trimmed squares (LTS)**

  Minimizes the squared residuals by ignoring an $\alpha$-portion as

  $$
  \hat{x} = \arg \min_x \sum_{i=1}^{\lfloor (1-\alpha)m \rfloor + 1} r_i^2(x)
  $$

  where $\alpha \in (0, 1)$ and

  $$
  r_{(1)}^2(x) \leq r_{(2)}^2(x) \leq \cdots \leq r_{(m)}^2(x)
  $$

- **Least median of squares (LMS)**

  Minimizes sample median $r_{([m/2])}^2$ of the squared residuals

  **How robust are they in power systems?**


  Y Wng, R. Negi, Q. Liu, and M. Ilic (2011)
Breakdown Points (BDPs) of Estimators

- **Maximum** ratio of # outliers over # measurements tolerable for estimation
- Determined by the minimum # measurements that, if removed, leaves one remaining measurement critical.
  - BDP of LS = 0
  - BDP of LTS and LMS < \((m - n)/2m\), Asymptotically goes to 0.5

**Attack scenario 1 (Masked attack)**

- Attacker modifies entries more than the BDP \(\Rightarrow\) Estimate is affected
- Difficult to detect from the residuals
Decomposition of the Grid

- Power systems are very sparse: BDPs are small for large systems.
- Our approach: Decompose the grid into islands/subsystems
- IEEE 14 bus system: Decomposed into 8 islands (7 cyclic and 1 radial):
Scenarios for Stealthy Attacks

**Theorem:** If the attack satisfies $\text{Im} \delta H \subset \text{Im} H$, then

$$\|S_c \delta P\| = \cos \gamma = 0, \text{ that is, } E[r_c] = 0. \quad (\text{Scenario 2: Stealthy attack})$$

**Example:** Take $\delta H^{(i)}$ as

(i) the $i$th column is a scalar multiple of that of $H$:

$$\delta H^{(i)}(:, i) = c \cdot H(:, i)$$

(ii) the rest are zero.

Then, the estimated state is

$$\hat{x}_c(i) = \frac{1}{1 + c} \hat{x}(i)$$

This attack requires modifying all $\ell_i$ nonzero entries of $H(:, i)$.

- Power systems are sparse, so this type of attacks can be done locally.
Different Scenarios against LTS

Proposition:

- If more than \((\ell_i \times \text{BDP})\) entries of \(H(:,i)\) are modified
  
  \[ \text{State estimate is affected. \hspace{4mm} (Scenario 1: Masked attack)} \]

- If more than \((\ell_i \times (1-\text{BDP}))\) entries of \(\delta H^{(i)}(:,i) = c \cdot H(:,i)\) are used

  \[ \hat{x}_c(i) = \frac{1}{1 + c} \hat{x}(i) \hspace{4mm} (\text{Scenario 2: Stealthy attack)} \]

Good data will be treated as bad and thus ignored!

![Graph showing danger level vs. number of attacks.](image)
Simulation Results

- IEEE 14 bus system with 123 measurements

- Two methods: (i) Least trimmed squares (LTS) with decomposition
  BDPs at 0.1/0.25 for each island

  (ii) Residual analysis (RA): Common in practice
(1) Random Attacks on $H$

- Random changes in matrix $H$ (8 entries) and measurement $z$ (1 entry)
- LTS is robust, but RA is very vulnerable.

![Graph showing comparisons between LTS, RA, and clean data across bus numbers and magnitude/angle values.](image-url)
(2) Stealthy Attacks on Phase Angle at Bus 2

- The measurement function is altered as

\[ h_c(x) = h(x) + \delta H^{(1)}x \]

- Even LTS is vulnerable against such coordinated attacks.

![Graph showing error only at specific bus number](image-url)
(2) Stealthy Attacks on Phase Angle at Bus 2

- Attacker has access to island 1 only.
- 21 measurements (9 active power flows/injections)
- LTS with BDP = 0.25 $\Leftrightarrow$ Up to 2 attacks

Estimate of phase angle of bus 2: Average and standard deviation of 100 runs

<table>
<thead>
<tr>
<th># of attacks</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTS</td>
<td>-6.38 (0.7)</td>
<td>-3.01 (2.49)</td>
<td>-1.33 (0.10)</td>
<td>-1.25 (0.09)</td>
</tr>
<tr>
<td>RA</td>
<td>-1.92 (1.14)</td>
<td>-4.03 (2.07)</td>
<td>-1.25 (0.29)</td>
<td>-1.10 (0.16)</td>
</tr>
</tbody>
</table>

Scenario 1:
Estimates are unreliable
> 2 attacks

Scenario 2:
States are controlled
> 9-2 = 7 attacks
Stealthy attacks in $H$ are challenging

Potential solutions

- Increase # of measurements and make them secure
- Use multiple estimators with different BDPs
  
  Y. Chakhchoukh and H. Ishii (IEEE Trans Power Syst, 2016)

- Look at data variations in time

Dynamical approach for distributed detection of attacks

H. Nishino & H. Ishii (2014)
Attack Detection at Voltage Regulation of Distribution Systems
Substations regulate voltage to keep it within admissible range at consumers.

PVs can cause inverse currents, resulting in complex voltage profiles.

A. Teixeira, G. Dan, H. Sandberg, R. Berthier, R. Bobba, and A. Valdes (2014)
Centralized Voltage Regulation

- One solution: Centralized control using measurements from switches
- More sensors can enhance control, but cyber security issues can arise.

Elkhatib, El-Shatshat, & Salama (2011), Yoshizawa, Hayashi, Tsuji, & Kamiya (2012)
Model of the Distribution System

- Small-scale residential area in Japan
- High voltage loads: Nodes 3, 5, 8, 9, 11, 13, 14
- Low voltage loads: 435 houses in total
- Assumed each house with PV generation

Diagram:

- 6750/105V
- 6600/105V
- LRT
- Load
- IT switch

Graphs:

- Power generated at PVs
- Low voltage load
The tap at LRT is switched as loads become higher: Morning & Evening

In the presence of PVs, voltage becomes high during the day time

Profiles in the evening/night are similar.
Algorithm to Detect Sensor Value Falsification

1. Voltage in the admissible range
   - Smaller in downstream
   - Void when PVs are active

2. Order among nodes
   - Smaller in downstream
   - Void when PVs are active

3. Change rates

4. Lower bound on differences

Without PVs

1. Voltage in the admissible range
The simple algorithm can detect attacks on one or two nodes.

However, attacks are still possible.

Example (Without PV): Attacks at Five Nodes

1. To cancel upward tap change
2. To avoid detection

Sensor values: Normal
Actual values: Undervoltage
Example (With PVs): Attacks at five nodes

- Attacks at 1-2 nodes can be all detected by the algorithm.
- With 3 or more attacks, tap changes can be suppressed.
- Compared to no PV case: More complicated, but similar damages.

1. To cancel upward tap change
2. To induce downward tap change
3. To avoid detection

Sensor values: Normal
Actual values: Undervoltage
Effectiveness of the Algorithm

- Attacks on one or two nodes can be prevented.
- No difference between with/without PVs
Discussion

- Simple algorithm for attack detection can be useful.
- Steps can be added to enhance detection.
- Further research:
  - Study the case with PV output regulation

PVs reduce outputs!

To induce tap changes upwards
Conclusion

- Distributed detection of cyber attacks in power systems EMS
- System theoretic approaches based on models
  - Transmission Systems: Robust state estimation
  - Distribution Systems: Centralized voltage control
- New area of research with a lot of potential collaborations
- Networked control in a broad sense, with specific control applications
References


