Smart Grids Cyber System
Security: an Innovation Approach

Arturo Bretas
Department of Electrical and Computer Engineering
Outline

► Introduction
► State Estimation
► Smart Grids Cyber-Security
► Result
► Conclusions
Introduction

► Modern Power Systems:
► Energy monitoring systems
► Supervisory Control and Data Acquisition (SCADA) systems
► Phasor Measurement Units (PMUs)
► Smart Grids
  ► Smart meters
  ► Huge amount of data in real time
► Number of measurements > number of states
  ► Voltage magnitude and angle
  ► Inconsistent measurements
Introduction

► State of a system

► Smallest set of variables necessary to calculate any other variable

► For power systems: voltage angle and magnitude
State estimation

► Overview

Pre filtering: eliminates inconsistent data. Example: negative voltage magnitude

State estimator: obtains state. One method is Weighted Least Squares (WLS)

Errors: detect, identify and eliminate non-Gaussian errors

Topology: analyses electric network model. Example: switches (open or closed)

Observability: verifies if states can be obtained with available set of measurements
State estimation

- **WLS Algorithm:**
  - Initial state: \( V=1, \theta=0 \)
  - Update states:
    \[
    \Delta x^\nu = \left( H(x^\nu)^T W H(x^\nu) \right)^{-1} H(x^\nu)^T W \left[ z - h(x^\nu) \right]
    \]
    \[
    x^{\nu+1} = x^\nu + \Delta x^\nu
    \]
  - Verify convergence criteria
    \[
    \Delta x^{\nu+1} \leq \xi
    \]
  - Once it converges the residuals are calculated
    \[
    r = \left[ z - h(x^\nu) \right]
    \]
Smart Grids Cyber-Security

- Attacker
- State Estimator
- Bad Data Detection
- Contingency Analysis
- Optimal Power Flow
- Operator
- Power Grid

$z - h(x)$

$\hat{x}$

$\hat{\tau} = \tau - \hat{\tau}$

$u$
Error analysis

► Pre-filtering: identifies inconsistent measurement data
  ► Negative voltage magnitude, load buses having positive power injection…
► Pre-filtering cannot detect more subtle errors
► WLS-SE uses post-processing to detect errors based on statistical properties of residuals
► Most used tests: chi-square and highest normalized error
► Given that errors have a Gaussian behavior, this analysis aims at finding errors that do not have those characteristics
Error analysis

The sum of the squares of a Gaussian distribution of independent random variables having zero mean and standard deviation equal to one follow the chi-square distribution.

The value of $\chi^2_{a}$ is defined by a significance level (probability) or by degree of freedom (independence).
Error analysis

- Error detection:
  \[ J(x) = [z - h(x)]^T W[z - h(x)] = \sum_{i=1}^{m} \left( \frac{r_i}{\sigma_i} \right)^2 \]

- Residuals and errors are related by
  \[ r = z - h(x) = Se \]

- \( S \) is the sensitivity matrix (not a diagonal matrix)

- Error identification:
  - Using normalized error:
    \[ r_i^N = \frac{|z_i - h_i(x^*)|}{\sqrt{\Omega_{ii}}} = \frac{|r_i|}{\sqrt{S_{ii}R_{ii}}} \]

- R = W\(^{-1}\)
Innovation Approach

\[ CME_{mi} = r_{mi} \sqrt{1 + \frac{1}{II_{mi}^2}} \]

\[ II_{mi} = \sqrt{1 - K_{mi,mi}} / \sqrt{K_{mi,mi}} \]

\[ J'(\hat{x}) = (CME)W(CME)^T \]

\[ J'(\hat{x}) \geq \chi^2_{(nm,\alpha)} \]

\[ CME_{mi}^N = |CME_{mi}| / \sigma_{mi} \]
Case Study

i) Attack Scenario I: Multiple measurements errors in the IEEE 14-bus test system

Gross error of magnitude $\sigma$ added to measurement $Q:08-07 = 0.1762pu$ (reactive power flow from bus 8 to bus 7);

Gross error of magnitude $\sigma$ added to measurement $P:01-02 = 1.5689pu$ (active power flow from bus 1 to bus 2);

Gross error of magnitude $\sigma$ added to measurement $P:03 = -0.9420pu$ (active power injection at bus 3).
## Case Study

### Multiple Errors Processing

<table>
<thead>
<tr>
<th>Original Measurement</th>
<th>Measurement with Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q:08-07 = 0.1762</td>
<td>(Q:08-07) + 9σ = 0.1963</td>
</tr>
<tr>
<td>P:01-02 = 1.5689</td>
<td>(P:01-02) + 5σ = 1.6589</td>
</tr>
<tr>
<td>P:03 = -0.9420</td>
<td>(P:03) + 4σ = -0.9021</td>
</tr>
</tbody>
</table>

#### Processing Error Step 1

<table>
<thead>
<tr>
<th>Meas. with</th>
<th>CME^N</th>
<th>CNE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q:08-07 = 0.1962</td>
<td>2.1884</td>
<td>9.3760</td>
</tr>
</tbody>
</table>

Corrected Measurement: Q:08-07 – CNE* = 0.1760pu  
(Correction Error = 0.1135%)

#### Processing Error Step 2

<table>
<thead>
<tr>
<th>Meas. with</th>
<th>CME^N</th>
<th>CNE</th>
</tr>
</thead>
<tbody>
<tr>
<td>P:01-02 = 1.6466</td>
<td>4.6720</td>
<td>4.7656</td>
</tr>
</tbody>
</table>

Corrected Measurement: P:01-02 – CNE* = 1.5663pu  
(Correction Error = 0.1657%)

#### Processing Error Step 3

<table>
<thead>
<tr>
<th>Meas. with</th>
<th>CME^N</th>
<th>CNE</th>
</tr>
</thead>
<tbody>
<tr>
<td>P:03 = -0.9033</td>
<td>2.4543</td>
<td>3.9560</td>
</tr>
</tbody>
</table>

Corrected Measurement: P:03 – CNE = -0.9418pu  
(Correction Error = 0.0212%)
Case Study

ii) Attack Scenario II: Simultaneous measurement error and parameter error in the IEEE 14-bus test system

Gross error of magnitude $-6\sigma$ added to measurement $P:04-09 = 0.1609\text{pu}$ (active flow from bus 4 to bus 9);

Error of 6% added to the parameters of the line 06-12.
## Case Study

### CME\textsuperscript{N} Descending List

<table>
<thead>
<tr>
<th>Measurement</th>
<th>II</th>
<th>CME\textsuperscript{N}</th>
<th>CNE</th>
</tr>
</thead>
<tbody>
<tr>
<td>P:04-09</td>
<td>2.9654</td>
<td>-5.8800</td>
<td>-6.2053</td>
</tr>
<tr>
<td>Q:12</td>
<td>0.4989</td>
<td>-5.8059</td>
<td>-13.0046</td>
</tr>
<tr>
<td>P:12-06</td>
<td>2.0719</td>
<td>4.7710</td>
<td>5.2976</td>
</tr>
<tr>
<td>Q:12-06</td>
<td>1.9688</td>
<td>4.0204</td>
<td>4.5093</td>
</tr>
<tr>
<td>Q:06-12</td>
<td>2.0766</td>
<td>-3.9147</td>
<td>-4.3450</td>
</tr>
<tr>
<td>Q:13</td>
<td>0.9701</td>
<td>-3.0646</td>
<td>-4.4012</td>
</tr>
</tbody>
</table>

Meas. with

<table>
<thead>
<tr>
<th>II</th>
<th>CME\textsuperscript{N}</th>
<th>CNE</th>
</tr>
</thead>
<tbody>
<tr>
<td>P:04-09 = 0.1509</td>
<td>2.9654</td>
<td>-5.8800</td>
</tr>
</tbody>
</table>

Corrected Measurement: P:04-09 – CNE\textsuperscript{*} = 0.1602
(Correction Error = 0.4351%)
# Case Study

## CME\textsuperscript{N} Descending List

<table>
<thead>
<tr>
<th>Measurement</th>
<th>II</th>
<th>CME\textsuperscript{N}</th>
<th>CNE</th>
</tr>
</thead>
<tbody>
<tr>
<td>P:12-06</td>
<td>2.0691</td>
<td>5.4585</td>
<td>6.0626</td>
</tr>
<tr>
<td>Q:12</td>
<td>0.4989</td>
<td>-5.0717</td>
<td>-11.3601</td>
</tr>
<tr>
<td>Q:12-06</td>
<td>1.9688</td>
<td>4.2039</td>
<td>4.7151</td>
</tr>
<tr>
<td>Q:06-12</td>
<td>2.0765</td>
<td>-2.7853</td>
<td>-3.0915</td>
</tr>
<tr>
<td>Q:13</td>
<td>0.9701</td>
<td>-2.6720</td>
<td>-3.8375</td>
</tr>
<tr>
<td>P:13-12</td>
<td>1.0450</td>
<td>1.9677</td>
<td>2.7235</td>
</tr>
</tbody>
</table>

## Parameters Correction

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Database Value</th>
<th>Erroneous Value</th>
<th>Corrected Value</th>
<th>Correction Error</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.5260</td>
<td>1.6175</td>
<td>1.5250</td>
<td>0.0655%</td>
</tr>
<tr>
<td></td>
<td>-3.1760</td>
<td>-3.3665</td>
<td>-3.1741</td>
<td>0.0598%</td>
</tr>
<tr>
<td></td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000%</td>
</tr>
</tbody>
</table>
Conclusions

• Innovation State Estimator: Extension/Enhancement of WLS;
• Initial Test Results are Encouraging;
• Capable to Detect, Identify and Correct Cyber-Attacks on Measurements and Parameters;
• Current Research on Topological Attacks and Physical Attacks.