SCADA Resilience via Autonomous Cyber-Physical Agents

Joseph Andrew Giampapa
PI, Senior Member of Technical Research Staff
Software Engineering Institute

Gabriela Hug-Glanzmann
Soummya Kar
Co-PIs, Assistant Professors
Electrical and Computer Engineering

Carnegie Mellon University
Pittsburgh, PA 15213

Tuesday, 4 February 2014
Disclaimer

Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.


DM-0000954
Advisors from Industry

Kevin Ding
CenterPoint Energy
Houston, TX

Valentine Emiseh
CenterPoint Energy
Houston, TX

Dong Wei
Siemens Corporation
Princeton, NJ
Outline

• False Data Injection (FDI) Attack
• Three Types of FDI Attack
• Illustrative Example
• Autonomous Cyber-Physical Agent Architecture
• References
• Discussion
Cyber-Threat: False Data Injection (FDI) Attack

- Single-most critical EMS function is *state estimation*
  - Process is *central* to a grid control center
  - Receives noisy remote sensor data
  - Identifies and discards *bad data*
  - Determines *state variables* of the grid for power flow calculations
  - Based on this data, power grid operations are determined

- False Data Injection
  - Falsifies data that is input to state estimation
  - Has two potential impacts on operator’s perception of grid state:
    - Loss of *observability* of power grid state
    - Perceived *observability*, but
      - Incorrect and unsafe adjustments can be made
      - Based on misperceptions of system state due to FDI data
Outline

• False Data Injection (FDI) Attack
• Three Types of FDI Attack
• Illustrative Example
• Autonomous Cyber-Physical Agent Architecture
• References
• Discussion
Three Types of FDI Attacks

1. Sensor Attack
2. SCADA Communications Attack
3. Attack on Control Center Centralized Database

- Each type of attack is detectable and/or identifiable in isolation
  - Combinations of attacks are not yet considered
Schematic of Attacks

- Sensor Attack
- SCADA Communications Attack
- Database Attack
Sensor Attack

• With complete sensor agent coverage
  • We can detect and identify an attacked sensor.
  • Complete: one agent per sensor, one sensor per bus
  • As long as the set of non-attacked measurements constitute an observable set of measurements.
• Caveat: most grids do not deploy complete sensor coverage.
• For a specific grid, observability analysis will need to be performed before guarantees can be made.
SCADA Communications Attack

- We can *detect* the presence of an attack
  - It can be *localized* if the communications topology is radial
    - All sensors communicate directly with the control center
  - And if the sensors from which the readings are made are from an observable set of measurements
- In the event of non-radial communications topology:
  - Localization of attack will depend and need to be analyzed per segment
  - Assurance claims can still be made that inform area of compromise.
Database Attack

- An FDI attack can be *detected* and *localized* to DB
  - Via distributed state estimation performed by the agents
  - Assuming that all communications are secure, and that we have an
  - Observable set of measurements from the sensors
Outline

• False Data Injection (FDI) Attack
• Three Types of FDI Attack
• Illustrative Example
• Autonomous Cyber-Physical Agent Architecture
• References
• Discussion
Illustrative example

Consider an attack on line 17 to induce a load shed situation targeting bus 17 …
Illustrative example: FDI

Impact on the Line 17:

<table>
<thead>
<tr>
<th>Line 17</th>
<th>Line Number</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Detection likely?</th>
<th>Mismatch (Std Dev)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>No</td>
<td>18.990</td>
</tr>
<tr>
<td>Pline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>No</td>
<td>18.690</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>No</td>
<td>3.469</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>No</td>
<td>4.840</td>
</tr>
</tbody>
</table>

Legend:

- **V** Voltage magnitude measurement
- **P** Active power injection measurement
- **Q** Reactive power injection measurement
- **p** Active power flow measurement
- **q** Reactive power flow measurement

Undetected; Mismatch = [ 0 , 3 x Std Dev ]
Undetected; Mismatch = ( 3 x Std Dev , 6 x Std Dev ]
Undetected; Mismatch > 6 x Std Dev
Detected
Illustrative example: FDI

Observations:
The extent of the impact diminishes with distance from the point of attack, e.g. line 17.

Mismatch = [0, 3 x Std Dev] Mismatch = (3 x Std Dev, 6 x Std Dev] Mismatch > 6 x Std Dev
Illustrative example: FDI

State Estimation Program

Measurements

State Estimation

Bad Data Detection

Bad Data Identification

Bad Data

No

Yes

Estimates

Line 17

<table>
<thead>
<tr>
<th>Type</th>
<th>Line Number</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Measurements (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>0.453</td>
</tr>
<tr>
<td>Pline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>-0.448</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>0.072</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>-0.081</td>
</tr>
</tbody>
</table>
Illustrative example: FDI

Measurement Model:

\[
\text{Measurement} = \text{Ground Truth} + \text{Random Error} + \text{FDI}
\]

where
- **Ground Truth**: Actual physics of grid
- **Random error**: Gaussian noise \( \sim N(0, \text{Std Dev}) \)
- **Std Dev**: Sensor precision
- **FDI**: Highly structured error

### Line 17

<table>
<thead>
<tr>
<th>Type</th>
<th>Line Number</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Measurements (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>0.453</td>
</tr>
<tr>
<td>Pline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>-0.448</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>0.072</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>-0.081</td>
</tr>
</tbody>
</table>
Illustrative example: FDI

State Estimation Program

Measurements

Bad Data Detection

State Estimation

Bad Data Identification

Bad Data

Yes

No

Estimates

Line 17

<table>
<thead>
<tr>
<th>Type</th>
<th>Line Number</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Measurements (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>0.453</td>
</tr>
<tr>
<td>Pline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>-0.448</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>0.072</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>-0.081</td>
</tr>
</tbody>
</table>

Measurement Model:

<table>
<thead>
<tr>
<th>Ground Truth (p.u.)</th>
<th>FDI (p.u.)</th>
<th>Random Error (p.u.)</th>
<th>Std Dev (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.301</td>
<td>1.448E-01</td>
<td>7.111E-03</td>
<td>8.000E-03</td>
</tr>
<tr>
<td>-0.299</td>
<td>-1.501E-01</td>
<td>5.538E-04</td>
<td>8.000E-03</td>
</tr>
<tr>
<td>0.100</td>
<td>-3.176E-02</td>
<td>4.011E-03</td>
<td>8.000E-03</td>
</tr>
<tr>
<td>-0.120</td>
<td>3.440E-02</td>
<td>4.323E-03</td>
<td>8.000E-03</td>
</tr>
</tbody>
</table>

FDIs are large relative to Std Devs. Unlike Gross Errors, FDIs are strategically designed using the attacker’s knowledge of the grid.
Illustrative example: FDI

State Estimation Program

Measurements

State Estimation

Bad Data Detection

Bad Data Identification

Attack Measurements

Estimates

<table>
<thead>
<tr>
<th>Line 17</th>
<th>Type</th>
<th>Line Number</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Measurements (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td></td>
<td>0.453</td>
</tr>
<tr>
<td>Pline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td></td>
<td>-0.448</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td></td>
<td>0.072</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td></td>
<td>-0.081</td>
</tr>
</tbody>
</table>

Estimation Results:
Illustrative example: FDI

State Estimation Program

Measurements

Attack Measurements

Bad Data Detection

Bad Data Identification

State Estimation

Estimates

Line 17

<table>
<thead>
<tr>
<th>Type</th>
<th>Line Number</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Measurements (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>0.453</td>
</tr>
<tr>
<td>Pline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>-0.448</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>0.072</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>-0.081</td>
</tr>
</tbody>
</table>

Estimation Results:

<table>
<thead>
<tr>
<th>Estimates (p.u.)</th>
<th>Residuals (p.u.)</th>
<th>Weighted Residuals (p.u.)</th>
<th>Ground Truth (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.453</td>
<td>1.080E-07</td>
<td>1.350E-05</td>
<td>0.301</td>
</tr>
<tr>
<td>-0.448</td>
<td>1.370E-07</td>
<td>1.713E-05</td>
<td>-0.299</td>
</tr>
<tr>
<td>0.072</td>
<td>3.774E-07</td>
<td>4.718E-05</td>
<td>0.100</td>
</tr>
<tr>
<td>-0.081</td>
<td>7.335E-07</td>
<td>9.169E-05</td>
<td>-0.120</td>
</tr>
</tbody>
</table>

Estimates and measurements agree perfectly, but there are huge discrepancies when compared Ground Truth.
Illustrative example: FDI

State Estimation Program

Measurements

Attack Measurements

<table>
<thead>
<tr>
<th>Line 17</th>
<th>Type</th>
<th>Line Number</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Measurements (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td></td>
<td>0.453</td>
</tr>
<tr>
<td>Pline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td></td>
<td>-0.448</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td></td>
<td>0.072</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td></td>
<td>-0.081</td>
</tr>
</tbody>
</table>

Estimation Results:

<table>
<thead>
<tr>
<th></th>
<th>Estimates (p.u.)</th>
<th>Residuals (p.u.)</th>
<th>Weighted Residuals (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pline</td>
<td>0.453</td>
<td>1.080E-07</td>
<td>1.350E-05</td>
</tr>
<tr>
<td>Pline</td>
<td>-0.448</td>
<td>1.370E-07</td>
<td>1.713E-05</td>
</tr>
<tr>
<td>Qline</td>
<td>0.072</td>
<td>3.774E-07</td>
<td>4.718E-05</td>
</tr>
<tr>
<td>Qline</td>
<td>-0.081</td>
<td>7.335E-07</td>
<td>9.169E-05</td>
</tr>
</tbody>
</table>

Random Error:

<table>
<thead>
<tr>
<th>Std Dev (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.000E-03</td>
</tr>
<tr>
<td>8.000E-03</td>
</tr>
<tr>
<td>8.000E-03</td>
</tr>
<tr>
<td>8.000E-03</td>
</tr>
</tbody>
</table>

Residuals practically insignificant compared to Std Devs.
Illustrative example: FDI

State Estimation Program

- Measurements
- Attack Measurements

Bad Data Detection

Bad Data Identification

Yes

No

Estimates

<table>
<thead>
<tr>
<th>Line 17</th>
<th>Type</th>
<th>Line Number</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Measurements (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td></td>
<td>0.453</td>
</tr>
<tr>
<td>Pline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td></td>
<td>-0.448</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td></td>
<td>0.072</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td></td>
<td>-0.081</td>
</tr>
</tbody>
</table>

Estimation Results:

<table>
<thead>
<tr>
<th>Estimates (p.u.)</th>
<th>Residuals (p.u.)</th>
<th>Weighted Residuals (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.453</td>
<td>1.080E-07</td>
<td>1.350E-05</td>
</tr>
<tr>
<td>-0.448</td>
<td>1.370E-07</td>
<td>1.713E-05</td>
</tr>
<tr>
<td>0.072</td>
<td>3.774E-07</td>
<td>4.718E-05</td>
</tr>
<tr>
<td>-0.081</td>
<td>7.335E-07</td>
<td>9.169E-05</td>
</tr>
</tbody>
</table>

Random Error:

<table>
<thead>
<tr>
<th>Weighted Residuals (p.u.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.801E-01</td>
</tr>
<tr>
<td>1.762E-01</td>
</tr>
<tr>
<td>5.206E-01</td>
</tr>
<tr>
<td>5.059E-01</td>
</tr>
</tbody>
</table>

Weighted residuals are practically insignificant compared to the Random Error case.
No bad data detected => DANGER !!!
Illustrative example: FDI

Summary of results:
• If bad data detection is tuned to data with assumed random error distribution, then
  • FDI data will likely not be detected if it is highly structured
  • Because the weighted residual of the FDI data is much less than that of the random error.

• The negative consequences of the FDI attack:
  • Data that would normally be rejected (cf. Mismatch (Std Dev)) is accepted as good.
  • Control center operator will be making decisions based on wrong perception of operating state.

• Two types of mismatches, below, illustrate this:
  1. Mismatch = Estimated_{FDI} – Ground Truth [p.u.]
  2. Mismatch = Estimated_{FDI} – Ground Truth [Std Dev]

<table>
<thead>
<tr>
<th>Line 17</th>
<th>Type</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Weighted Residual_{FDI} (p.u.)</th>
<th>Weighted Residual_{Random} (p.u.)</th>
<th>Detection likely?</th>
<th>Estimated_{FDI} (p.u.)</th>
<th>Ground Truth (p.u.)</th>
<th>Std Dev (p.u.)</th>
<th>Mismatch (p.u.)</th>
<th>Mismatch (Std Dev)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>1.350E-05</td>
<td>7.801E-01</td>
<td>No</td>
<td>0.453</td>
<td>0.301</td>
<td>8.000E-03</td>
<td>0.152</td>
<td>18.990</td>
</tr>
<tr>
<td>Pline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>1.713E-05</td>
<td>1.762E-01</td>
<td>No</td>
<td>-0.448</td>
<td>-0.299</td>
<td>8.000E-03</td>
<td>0.150</td>
<td>18.690</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>1</td>
<td>17</td>
<td>4.718E-05</td>
<td>5.206E-01</td>
<td>No</td>
<td>0.072</td>
<td>0.100</td>
<td>8.000E-03</td>
<td>0.028</td>
<td>3.469</td>
</tr>
<tr>
<td>Qline</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>9.169E-05</td>
<td>5.059E-01</td>
<td>No</td>
<td>-0.081</td>
<td>-0.120</td>
<td>8.000E-03</td>
<td>0.039</td>
<td>4.840</td>
</tr>
</tbody>
</table>
Outline

- False Data Injection (FDI) Attack
- Three Types of FDI Attack
- Illustrative Example
- Autonomous Cyber-Physical Agent Architecture
- References
- Discussion
Architectural Rationale

• Do not modify centralized state estimation functions with security enhancements
  • It is an optimized process for current operations
  • Early and widespread adoption is desired
    • Interoperability with legacy systems
    • Low-interference with current operations
    • Minimize startup and implementation costs

• Overlay distributed state estimation (DSE) verification for security
  • If DSE can be conducted autonomously by software agents
  • FDI attacks on centralized state estimation can be detected by distributed agents
  • Power system is a closed system
    • There is always knowledge elsewhere that can be leveraged
Schematic of Attacks

- Sensor Attack
- SCADA Communications Attack
- Database Attack

Ground Truth

Control Center:
Bad Data Detection, State Estimation

RTU-1
RTU-2

Bus
Line
Bus
Detection Even if Agents Are Compromised
Test Bed & Data Flow

Visualization of the Power Grid's Ground Truth

Measure

Measured State

FDI Cyber-Attack State

Temporary Data Store

Estimate State

Bad Data

Estimated State

Topologically-Motivated Errors

Power grid operator's perception should be as close to ground truth as possible.

SCADA Agents

Agree with Measurements

Evaluate Locally

Disagree with Measurements

Visualization of the Power Grid Operator's Perception of Grid State
Outline

• False Data Injection (FDI) Attack
• Three Types of FDI Attack
• Illustrative Example
• Autonomous Cyber-Physical Agent Architecture
• References
• Discussion
References


http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6275516&isnumber=6275510


http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06102319


Outline

- False Data Injection (FDI) Attack
- Three Types of FDI Attack
- Illustrative Example
- Autonomous Cyber-Physical Agent Architecture
- References
- Discussion
Contact Information

Joseph Andrew Giampapa
Senior Member of the Research Technical Staff
Research, Technology, and Systems Solutions (RTSS) Program
Telephone: +1 412-268-6379
Email: garof@sei.cmu.edu

Web
www.sei.cmu.edu
www.sei.cmu.edu/staff/garof

U.S. Mail
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA