Market-Level Defense Against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations

2020 CURENT NSF/DOE Site Visit and Industry Conference
Virtual
Nov. 2020

Qiwei Zhang
Fangxing (Fran) Li
The University of Tennessee, Knoxville
Market-Level Defense Against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations

Background and motivation:
- Traditional cyberattack strategies on the power market only consider bypassing bad data detections.
- Our analysis shows that abnormal locational marginal prices (LMPs) can be an easy-to-detect signal of attacks.
- Based on the relationship of market cyberattacks and price signals, a market-level defense strategy is proposed, and a new LMP-disguising attack strategy is discussed.

Abnormal LMP Step Changes
- Why traditional attack strategies lead to abnormal LMP step changes:
  1) the resulting new congestion pattern may fall outside of the normal congestion pattern at the current loading level.
  2) the compromised LMPs are not consistent with previous periods when the system loading changes smoothly.

Conclusions:
- Even if state estimation level detection mechanisms are bypassed, cyberattacks can easily be detected by market-level behavior, such as abnormal price signals.
- By analyzing CLLs of LMPs, we construct a market-level defense analysis method to help operators identify attacks.
- An LMP-disguising attack strategy is developed to disguise the compromised LMPs as normal LMPs, which can bypass both bad data detection and market-level detection.

Detecting abnormal LMPs

Fig. 1 Detection procedures
The market-level defense library

<table>
<thead>
<tr>
<th>Algorithm BC</th>
<th>Function build_contingency (risky CLLs, x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>All risky CLLs</td>
</tr>
<tr>
<td>Output</td>
<td>Contingency library</td>
</tr>
<tr>
<td>1</td>
<td>For each risky CLL do</td>
</tr>
<tr>
<td>2</td>
<td>Solve the market-clearing model</td>
</tr>
<tr>
<td>3</td>
<td>For each possible combination do</td>
</tr>
<tr>
<td>4</td>
<td>Record target lines in this combination</td>
</tr>
<tr>
<td>5</td>
<td>For each target line i do</td>
</tr>
<tr>
<td>6</td>
<td>Remove i⁻th line flow limit</td>
</tr>
<tr>
<td>7</td>
<td>End for</td>
</tr>
<tr>
<td>8</td>
<td>Solve the market-clearing model</td>
</tr>
<tr>
<td>9</td>
<td>Record CLLs, congestion patterns, and LMPs</td>
</tr>
<tr>
<td>10</td>
<td>Add the recorded value to the library</td>
</tr>
<tr>
<td>11</td>
<td>End for</td>
</tr>
<tr>
<td>12</td>
<td>End for</td>
</tr>
<tr>
<td>13</td>
<td>Return the library</td>
</tr>
</tbody>
</table>

The LMP-disguising attack

![Diagram of LMP-disguising attack]

- Target period t
- Next period t+1
- LMP2
- True LMP
- LMP2
- Delay attacked LMP
- Example 1
- LMP3
- LMP2
- Traditional compromised LMP
- Example 2
- Loading level
- CLLs
Market-Level Defense Against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations

PJM 5-bus system test case

IEEE 118-bus test case

Profitability analysis
Acknowledgements

This work made use of Engineering Research Center shared facilities supported by the Engineering Research Center Program of the National Science Foundation and the Department of Energy under NSF Award Number EEC-1041877 and the CURENT Industry Partnership Program.

The primary sponsor of this research work is RTRC.