Semantic Security Analysis of SCADA Networks to Detect Malicious Control Commands in Power Grids

Hui Lin,
Adam Slagell, Zbigniew Kalbarczyk,
Peter W. Sauer, and Ravishankar K. Iyer
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Control-related Attacks in SCADA

• Control-related attacks: an attacker can exploit system vulnerabilities and use a maliciously crafted control command to cause a wide range of system changes
  – Hard to detect based solely on states of physical components
    • Classical state estimation analysis usually covers $N-1$ contingencies, hence cannot cover high-order changes
    • Measurements can be compromised during network communications
  – Hard to detect based solely on network activities
    • Malicious commands do not need to generate network anomaly
Attack Model

- Not trust “intelligent” devices
  - Personal computers in control centers
  - Intelligence field devices in substations
  - Control network
- Trust measurements of power usage, current, and voltage directly obtained from sensing devices (or sensors) in substations
  - Concurrent physical accesses to and tampering with a number of distributed sensors is not practical
### Attack Case Scenario

**Attack Entry Points**

- Insider Access
- Remote Access

**State Estimation & Contingency Analysis**

**Data Historian**

**Installed Malware in Substations**

**Access Control Center**

**Access Field Devices**

---

**Option 1:** Attackers learn network topology, estimate system states, and determine attack strategy, e.g., opening transmission lines to open.

**Option 2:** Open lines at random when systems operate under high generations or load demands.

---

**Attack Preparation Stage**

1. Generate legitimate but malicious network packets (a sample DNP3 packet to open 4 breakers simultaneously):

   CB 04 0C 28 04 00 01 04 … 03 04 … 05 04 … 06 04 …

   **IP + TCP Headers**

   **DNP3 Headers**

   **Device Index**

   **Control Code**

   **Four Control Relay Objects**

2. To hide system changes, intercept and/or alter the network packets sent to the control center in response to the commands.

---

**Attack Execution Stage**
Semantic Analysis Framework

Control Center

SCADA Master

IDS Instance #1

State Estimation & Contingency Analysis

Substation

DNP3 Slave

IDS Instance #2

Actuators & Sensors

Measurements: power usage, current, and voltage

Control Commands

1) Commands issued to the remote site
2) Measurements obtained from sensors

Generated Alerts

Semantic Analysis Framework
Semantic Analysis Framework (cont’d)

- **IDS at the control center:**
  - Distinguish critical commands from non-critical ones, e.g., commands that can change system states instantly
  - Collect measurements from all substations
  - Include state estimation & contingency analysis components to estimate the execution consequence of the command

- **IDS at the remote substation**
  - Use local IDS to obtain measurements directly from sensors (trusted in our threat model)
  - Validate measurements or commands are not corrupted at other locations
Evaluation

• The evaluation includes:
  – The effects of malicious commands on power systems
  – Performance of semantic analysis

• The test-bed configuration
  – An Intel i3 (3.07 GHz) quad-core and 4 GB RAM, running Ubuntu 10.04 OS
  – Implement SCADA master and DNP3 slave by DNP3 open source library
  – Use Matpower, an open source Matlab toolbox, to analyze control commands
Generation of Synthetic Network Traffic

- SCADA master issues DNP3 network packets to change power system states
  - The traffic includes network packets, representing *read*, *write*, and *execute* commands
  - Include the maliciously crafted commands
  - IEEE 30-bus system is analyzed

<table>
<thead>
<tr>
<th>Cmd Type</th>
<th>Description</th>
<th>Event Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Read</strong></td>
<td>Request to read (i) static data and (ii) event data from relays</td>
<td>Periodic event with interval of 1 second</td>
</tr>
<tr>
<td><strong>Write</strong></td>
<td>Request to (i) update the static configuration file and (ii) open/close an application in a relay</td>
<td>Poisson process with average command arrival interval of 50 seconds</td>
</tr>
<tr>
<td><strong>Execute</strong></td>
<td>Request to open/close a breaker of a relay</td>
<td>Poisson process with average command arrival interval of 100 seconds</td>
</tr>
</tbody>
</table>
IEEE 30-bus System

- **Generator**: Black circle
- **Load**: Triangle symbol
- **Bus #**: Each bus can represent a substation

Diagram showing the connectivity and flow between various buses.
Define System Perturbation and Security Metrics

- System perturbation to emulate potential attacks
  - Increase generation (at bus 2, 13, 22, 23, and 27) by 50%
  - Increase all load demands by 50%
  - Open 3 transmission lines at random
  - All changes simultaneously

- Check line status
  - Voltage drop limits
    - $V_R / V_S < 5\%$
  - Steady-state stability limits
    - $P_{\text{line}} < P_{\text{max}}$

- Use the number of insecure lines as security metrics

```
Malicious System Changes
↓
State Estimation
↓
Check Line Status

Within Steady-state Limit?
<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

secure  insecure  secure
```
Effect of System Changes

- We can always find an attack strategy to put a system into insecure states
- A smart attacker can reduce the chance of detection:
  - Select vulnerable time (with high power generation) to open a few transmission lines
Performance Evaluation

• Performance of semantic analysis does not affect power system normal operations

• The execution time of the semantic analysis consists of two parts:
  – *Network analysis latency*: intercept control commands, extract their parameters and deliver them to contingency analysis
  – *Contingency analysis latency*: execute the contingency analysis to estimate the execution consequence of the command
Conclusion

• Analyze the impact of control-related attack in power grid
  – The network IDS is used to monitor and extract SCADA-related network semantic
  – Augment the IDS with power flow assessment tools to estimate the execution consequence of a command

• In future work, we will focus on preemptive analysis on both cyber and physical knowledge from power grid
  – Physical damages is hard to reverse
  – Investigate appropriate responses, i.e., postpone the command? Or reverse the command?
Thanks!