A Cyber-Physical and Agent-Based Defense to False Data Injection Attacks on a SCADA System

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

Gabriela Hug-Glanzmann
Co-PI, Assistant Professor
Electrical and Computer Engineering, Carnegie Mellon University
Disclaimer

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. government or any agency thereof.
Additional Team Members

Soummya Kar
• Researcher, Assistant Research Professor
• Electrical and Computer Engineering, Carnegie Mellon University

David S. Kyle
• Research Programmer, Member of the Technical Staff
• Software Engineering Institute, Carnegie Mellon University

Kawa Cheung
• Research Assistant, MS Student
• Electrical and Computer Engineering, Carnegie Mellon University

Skyler B. Shatkin
• Research Assistant, MS Student
• Electrical and Computer Engineering, Carnegie Mellon University

Mayank K. Malu
• Research Programmer, MS Student
• Institute for Software Research, Carnegie Mellon University
Acknowledgements

• SEI Ultra-Large-Scale (ULS) System Research Initiative
  – http://www.sei.cmu.edu/uls/index.cfm
  – Linda Northrop

• High-Confidence Cyber-Physical Systems (CPS) Program
  – Mark Klein

• DoE Office of Electricity Delivery & Energy Reliability
  – Cybersecurity for Energy Delivery Systems (CEDS) Program
  – Carol Hawk
Research Problems

1. What is the security threat to the power grid posed by a compromised SCADA (Supervisory Control and Data Acquisition) system?
   – Consequence analysis on power system functions
   – Baseline for understanding how to regain control if attacked

2. Considerations of the architectural components of a SCADA and EMS (Energy Management System):
   – Which components need to be compromised?
   – How must they be compromised to perform an attack?
   – What are the implications for other components of the SCADA / EMS architecture?

3. If a SCADA system is subverted:
   – How can the extent of the subversion be identified and isolated?
   – How can the power system operator regain control?
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 ($m < 2N - 1$)
    - Perceived *observability* ($m \geq 2N - 1$), but
      - Incorrect and unsafe adjustments can be made
      - Based on misperceptions of system state due to FDI data
Technical Approach

• Focus on FDI attacks that create false sense of observable transmission grid state \( m \geq 2N - 1 \)
  – There are at least as many perceived usable measurements as state variables
  – Unobservability \( m < 2N - 1 \) will be addressed in the future

• Introduce autonomous software agents to model cyber-physical properties of the grid / EMS at their cyber-physical location

• Theoretically prove that for any and all vectors of FDI cyber-attack
  – The agents can autonomously detect it
  – Even if the agents may be compromised

• Validate proof by modeling and simulation

• Implement proof-of-concept on SCADA devices
Power grid operator’s perception should be as close to ground truth as possible.

Visualization of the Power Grid Operator’s Perception of Grid State

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

Agree with Measurements

Evaluate Locally

Disagree with Measurements

SCADA Agents
Five Models Studied in the Proposed SCADA Agent Protection System

1. Electrical Model
2. SCADA Model
3. SCADA Attack Model
4. SCADA Agent Model
5. SCADA Agent Attack Model
1. Electrical Model
2. SCADA Model

Control Center: Bad Data Detection, State Estimation

RTU-1

RTU-2

Bus

Bus

Line

Ground Truth
3. SCADA Attack Model

Control Center: Bad Data Detection, State Estimation

RTU-1

RTU-2

Ground Truth
4. SCADA Agent Model

Agent Model of the Control Center

Control Center: Bad Data Detection, State Estimation

Ground Truth

RTU-1

RTU-2

SCADA Agent-1

SCADA Agent-2

Line

Bus
5. SCADA Agent Attack Model

Control Center: Bad Data Detection, State Estimation

Agent Model of the Control Center

SCADA Agent-1

RTU-1

Bus

Line

SCADA Agent-2

RTU-2

Bus

Ground Truth
SCADA Agent Architecture

Other EMS Functions
- OPF
  - OPF-A
- CA
  - CA-A
- AGC
  - AGC-A

SCADA Agents of Other Areas
- Other Control Centers
  - OCC-A
- Distribution Grid
  - DG-A

Agent Model of the Control Center

Control Center: Bad Data Detection, State Estimation

SCADA Agent-1

SCADA Agent-2

RTU-1

RTU-2

Ground Truth

Bus

Line
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
Results to Date: A Cyber-Attack is Possible


- Three techniques for determining which measurements to attack
  - DC Model
    - Common in literature 2009 – present
    - Introduces detectable errors
  - AC Model
    - Based on Jacobian matrix
    - Introduced
  - Graph Theoretic Model
    - Extends AC Model for buses with no injections
    - Introduced

- Two techniques for determining measurement values
  - For an FDI-attack that falsifies observability
  - DC calculations – rapid but introduce detectable errors
  - AC calculations – non-linear, will not be detected
Take-Away Message

- Comprehensive power grid SCADA security requires a cyber-physical systems approach
  - Evaluate the threat with respect to its impact on properties of the power grid, not just the cybernetic infrastructure
  - Remedies should also focus on mitigating the impact of the threat, especially for cost-effective solutions to cyber-security.

- Knowledge to avert threat can be leveraged from multiple perspectives and sub-systems
  - Electrical properties, control theory, cybernetic properties
  - Leverage knowledge from other EMS functions
References

   http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6275516&isnumber=6275510
   http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06102319
3. ieRoadmap: interactive energy Roadmap to Achieve Energy Delivery Systems Cybersecurity,
   https://www.controlsystemsroadmap.net/Pages/default.aspx
   https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/roadmap.pdf
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

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

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