MULTI-AGENT SYSTEM FOR DETECTING FALSE DATA INJECTION ATTACKS AGAINST THE POWER GRID

Esther M. Amullen\textsuperscript{1}, Hui Lin\textsuperscript{2}, Zbigniew Kalbarczyk\textsuperscript{2}
\textsuperscript{1}Tennessee State University, \textsuperscript{2}University of Illinois at Urbana-Champaign
\textsuperscript{1}eamullen@my.tnstate.edu, \textsuperscript{2}{hlin33, kalbarcz}@illinois.edu

1. MOTIVATION
- In the power grid, control decisions and subsequent actions that directly impact the operation of the power grid are made based on estimation data obtained from the state estimator.
- False Data Injection (FDI) attacks are cyber attacks that target measurement data used for state estimation.
- FDI attacks modify sensor readings obtained from measuring equipment with the aim of misleading the control center.
- An attacker who knows the topology of the power grid can craft an attack that bypasses existing bad data detection schemes.
- We propose a multi-agent system for accurate and timely detection of FDI attacks.

2. CHALLENGES
- Substations have access to a limited amount of information to accurately determine state.
- Determining states for substations locally introduces singularities in power flow computation.
- Deploying agents across the network requires developing new functional relationships among substations to determine power flow.
- New functional relationships developed need to be mapped onto the entire power network.

3. CYBER STRUCTURE OF THE POWER GRID

4. MULTI-AGENT SYSTEM ARCHITECTURE
- Software based agents are created for each substation.
- Each agent collects measurements from its substation, shares this data with other agents and the control center periodically.
- Using Shared measurements, agents can
  - build subsystems of the power grid,
  - determine state estimates at these subsystems
  - identify discrepancies in state estimate results

5. FORMAL ANALYSIS
- Threat Model: For a power network, the correlation between the measurement vector $z$ and the state estimate $\hat{x}$ is given by $z = Hx + e$ where $H$ is the topology matrix.
- Attackers compromise measurements delivered to the control center by injecting an FDI attack vector $\hat{a}$ such that $\hat{z}_i = Hx_i + e_i + \hat{a}_i$.
- The FDI attack is designed to bypass bad data detection for the whole power grid. In addition, Measurement data exchanged by substations can be compromised.
- Detection: The FDI attack is undetectable if there is a vector $c$ such that $\hat{a}^T H c = 0$. For a substation, the agent $A_i$ computes a measurement vector $\hat{z}_i$ and state vector $\hat{x}_i$ from $\hat{z}_i = H_i \hat{x}_i + e_i$.
- The FDI attack must satisfy the condition $\hat{d}_i = H_i c_i$ at each substation along with $\hat{a} = H c$ to remain undetectable.
- The attack is detected if the condition $\hat{d}_i = H_i c_i$ is not satisfied for at least one agent.

6. EXPERIMENTAL EVALUATION
- The figures below show the distribution of agents for a 9-bus system.
- Injection: Inject false data $\hat{a}$ into the system by selecting an arbitrary vector $c = [0 1 2 0 0 0 0 0]^T$. Computing $\hat{a} = Hc$, and $\hat{d} = H[c]^T$, conditions for FDI are tested. For some agents (4, 5, 6, 7, 8, 9), this condition does not hold making the attack detectable by our proposed agent-based detection technique.

7. FUTURE WORK
- Enhancing this technique to identify compromised measurements
- Evaluate the approach with a physical system