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

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

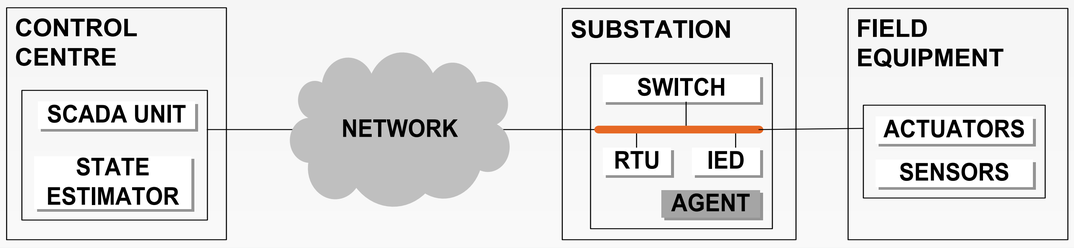
1. MOTIVATION

- 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.
- Soft-ware implemented agents are distributed across substations to
  - ✓ facilitate exchange of measurement data and state variables among substations
  - ✓ detect disparities between state variables at the substation and whole grid state variables.
  - ✓ ensure scalability of the solution.

2. CHALLENGES

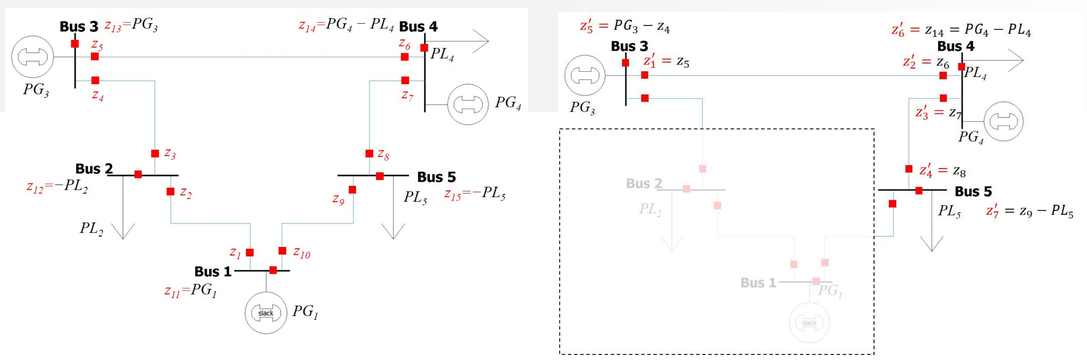
- Substations have access to a limited amount of information to accurately determine state.
- Determining states for substations locally introduces singularities in power flow computation.
- Deploying agents across the network requires developing new functional relationships among substations to determine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



Procedure: generate sub-system for agent at bus *i*

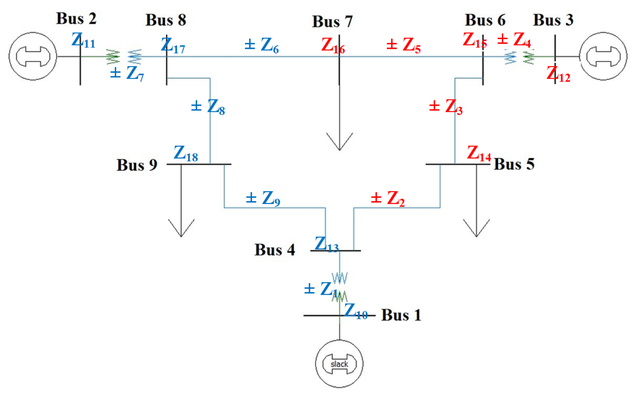
(1) Include bus *i* and its neighboring buses;
(2) Include the transmission lines that connect the buses selected at (1);
(3) Keep unchanged the real power flow measurements at the sending and receiving end of selected transmission lines;
(4) **For** bus $j \neq i$
(5) **For** transmission line *k* not selected at (2)
(6) **If** Power *P* at line *k* is delivered into bus *j*
(7) Increase power injection at bus *j* by *P*
(8) **Else**
(9) Decrease power injection at bus *j* by *P*
(10) **EndIf**
(11) **EndFor**
(12) **EndFor**

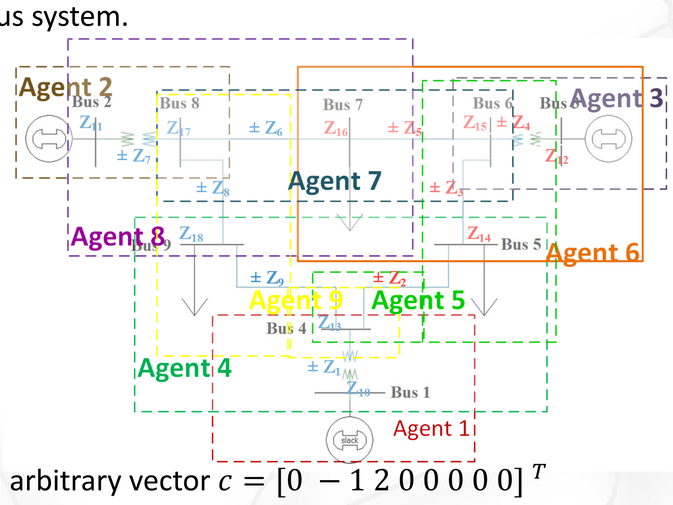
5. FORMAL ANALYSIS

- Threat Model: For a power network, the correlation between the measurement vector z and the state estimate 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 a such that $z_a = Hx + e + a$.
- 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 $a - Hc = 0$. For a substation, the agent A_i computes a measurement vector z_i' and state vector x_i' from $z_i' = H_i' x_i' + e_i'$
- The FDI attack must satisfy the condition $a' = H_i' c_i'$ at each substation along with $a = Hc$ to remain undetectable.
- The attack is detected if the condition $a' = H_i' c_i'$ is not satisfied for at least on agent.

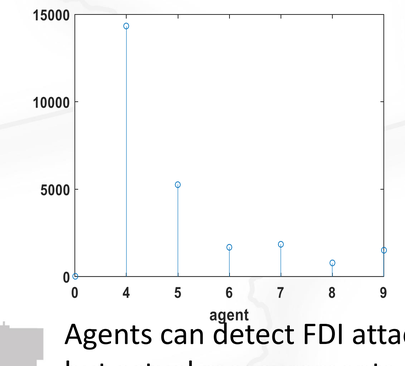
6. EXPERIMENTAL EVALUATION

- The figures below show the distribution of agents for a 9-bus system.

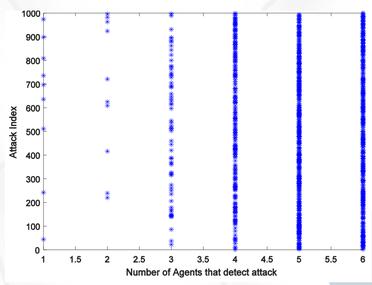




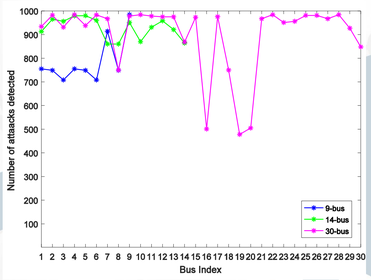
- Injection: Inject false data a into the system by selecting an arbitrary vector $c = [0\ -1\ 2\ 0\ 0\ 0\ 0\ 0]^T$
- Computing $a = Hc$, and $a' = H_i' c_i'$, conditions for FDI are tested. For some agents $(4, 5, 6, 7, 8, 9)$, this condition does not hold making the attack detectable by our proposed agent-based detection technique.



Agents can detect FDI attacks but actual measurements targeted are not known



1000 undetectable FDI attacks for the whole grid can be detected by at least one agent.



Probability that an agent successfully detects an FDI for the 9-bus, 14-bus and 30-bus system

7. FUTURE WORK

- Enhancing this technique to identify compromised measurements
- Evaluate the approach with a physical system

HoTSoS *Symposium and Bootcamp*
HOT TOPICS *in the* **SCIENCE OF SECURITY**
APRIL 4-5, 2017 | HANOVER, MARYLAND

8. ACKNOWLEDGEMENT

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141.