MULTI-AGENT SYSTEM FOR DETECTING

FALSE DATA INJECTION ATTACKS AGAINST THE POWER GRID

Esther M. Amullen, Hui Lin, Zbigniew Kalbarcyzk

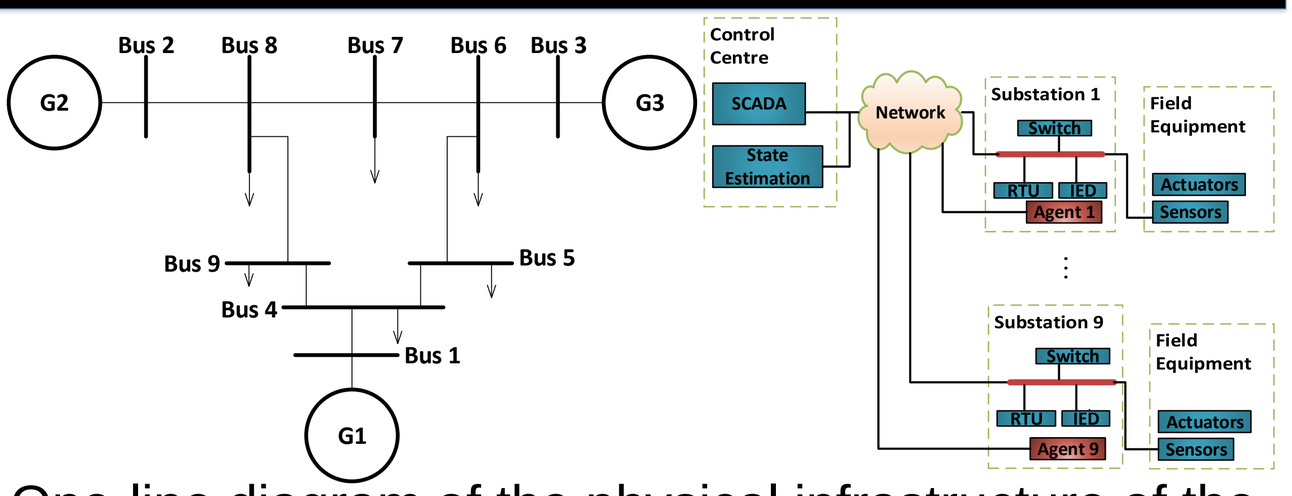
OBJECTIVES

- Provide accurate and timely detection of false data injection attacks in the power grid.
- Use software implemented agents distributed. across substations to:
  - ✓ Facilitate state information exchange among substations.
  - ✓ Ensure scalability of the solution.
- Evaluate the approach using a simulated example.

CHALLENGES

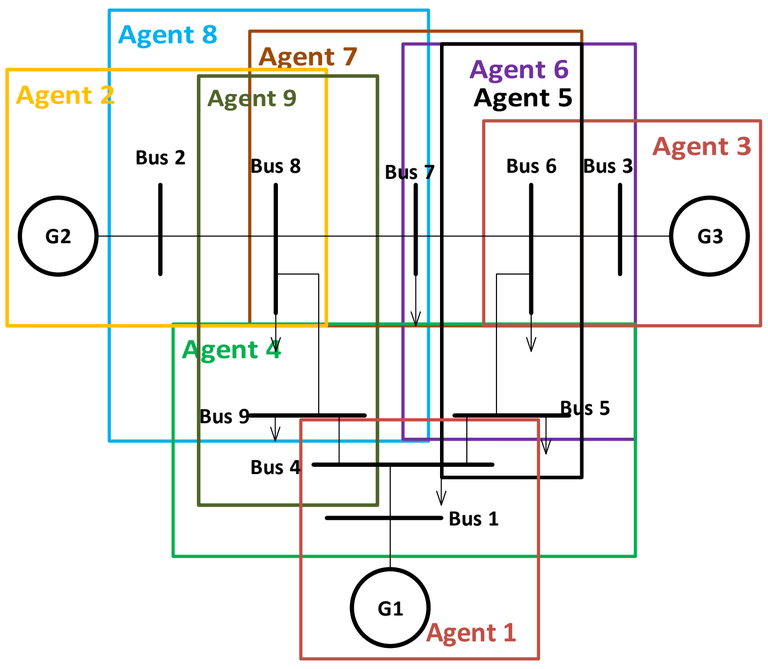
- Substations have access to a limited amount of information to accurately determine state.
- Determining states for substations locally introduces singularities in power flow computation.
- Deploying agents across the network requires developing new functional relationships among substations to determine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

CYBER AND PHYSICAL SYSTEM STRUCTURE



One-line diagram of the physical infrastructure of the IEEE 9-bus system and its communication infrastructure.

SOFTWARE-BASED DETECTION AGENTS FOR FDI ATTACKS



- The figure shows the distribution of agents for a 9-bus system.
- An agent is assigned per substation.

APPROACH

- The topology of the 9-bus system is described by matrix H.
- Detection agents are created for each substation(Bus);
- Grouping interconnected substations into subnetworks results into new topologies H'_i;
- The detection agents are software based each defined by H'_i. For agent i,

$$H'_i = \begin{bmatrix} A'^T_i D'_i A'_i \\ D'_i A'_i \\ -D'_i A'_i \end{bmatrix} H = \begin{bmatrix} A^T DA \\ DA \\ -DA \end{bmatrix}$$

-A is the Network connectivity matrix

-D is a diagonal matrix of all line admittances

- Using H'_i, agent i determines the state of substation i and shares this state information with the neighboring substations.
- For all measurement data sent to the control center, each agent compares these measurements with its local estimates and communicates any discrepancies.

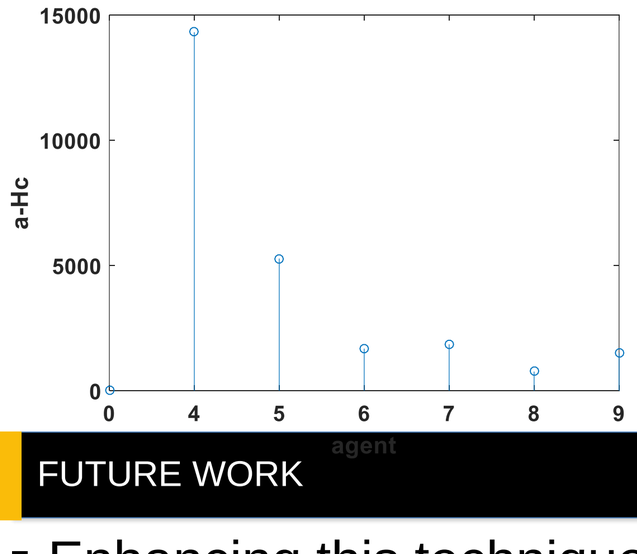
EVALUATION

- Injection: Inject false data a into the system by selecting an arbitrary vector c and computing $a = Hc$

$c = [0\ -1\ 2\ 0\ 0\ 0\ 0\ 0]^T$

$a = [0\ -10.9\ 5.9\ 34.1\ 0\ 0\ -16\ 0\ 16\ 34.1\ -10.9\ 16.8\ -40\ .-16\ 0]^T$

- Detection: An FDI attack is undetectable by the whole grid state estimator if $a - Hc = 0,$
- Augmenting the injected attack to obtain $c'_i, a'_i = H'_i c'_i$ is computed. Agents check the condition $a'_i - H'_i c'_i = 0,$ if the condition holds for all agents, the attack is undetectable.
- 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 false data injections but actual measurements targeted are not known

REFERENCES

- Liu, Yao, Peng Ning, and Michael K. Reiter. "False data injection attacks against state estimation in electric power grids." ACM Transactions on Information and System Security 14.1 (2011).

FUTURE WORK

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

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency.

INFORMATIONTRUST INSTITUTE