# MULTI-AGENT SYSTEM FOR DETECTING CONTROL-RELATED ATTACKS IN POWER GRIDS

Esther M. Amullen, Hui Lin, Zbigniew T. Kalbarczyk

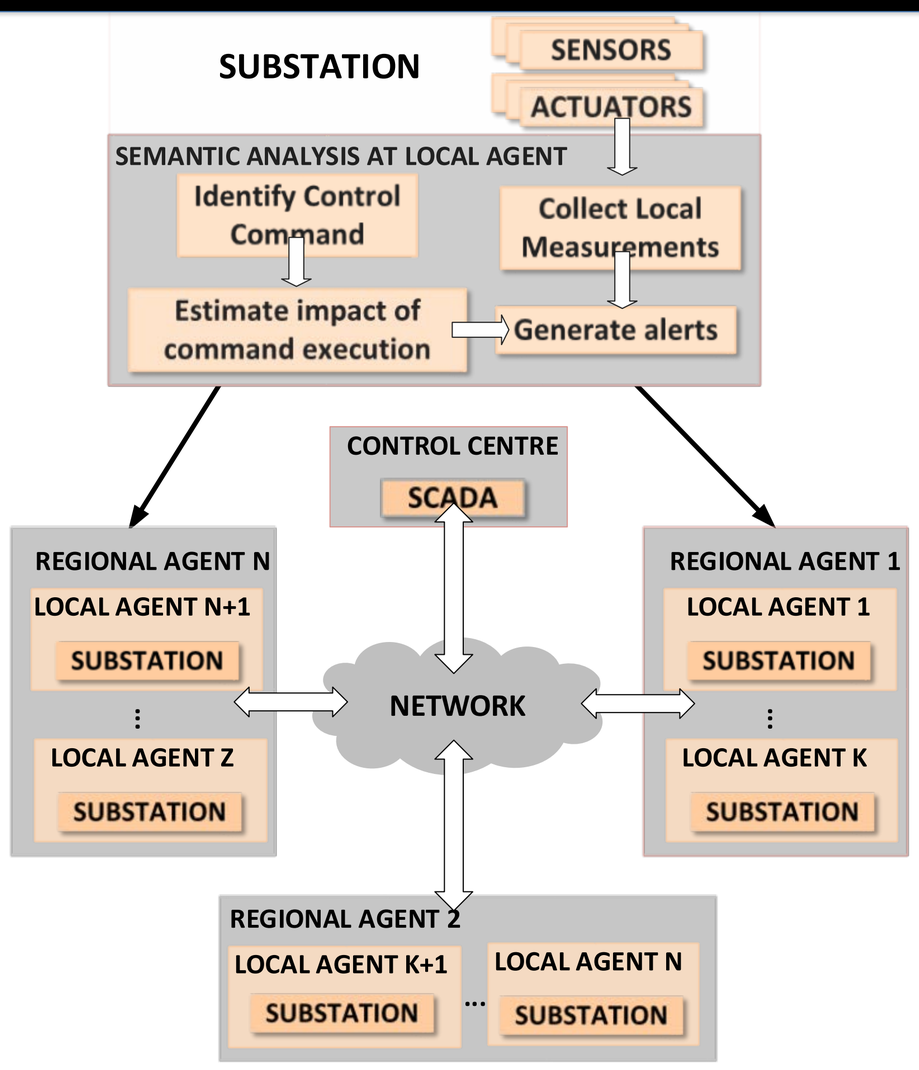
## 0BJECTIVES

- Monitor and detect control-related attacks in power grid SCADA
  - An attacker who knows the syntax and payload of SCADA control commands can create maliciously crafted commands and put the power network in an insecure state
- Develop a distributed semantic analysis framework employing a multi-agent system for detecting control-related attacks
  - Two-level hierarchy of software implemented agents
    - ✓local agents deployed across substations to facilitate exchange of measurement data and state variables among substations
    - ✓regional agents facilitate exchange of measurement data and state variables among agents.
- Evaluate the distributed semantic analysis framework approach using the IEEE 24 bus power system

## RESEARCH CHALLENGES

- Detect malicious control commands and allow for timely response while still meeting the strict timing requirements of the power grid
- Local agents have access to limited information acquired from adjacent substations regarding the overall state of the grid
- Local agents need to determine system state based on partial information;
- Regional agents need to provide local agents with updated state information from remote local agents with minimal latency.
- A mathematical model that relates power flow among local agents, regional agents and the overall grid has to be defined.

## DISTRIBUTED SEMANTIC ANALYSIS FRAMERWORK




- Regional agents partition the network into N areas each with k local agents and substations
- Each local agent monitors control traffic at its substation along with adjacent substations to identify control commands
- For critical control commands, local agents extract command semantics and run *a look ahead power flow analysis (LAP)* to estimate the impact of executing the command on the state of the power grid
- LAP analysis is adapted to execute within a fraction of the time it takes for the AC power flow analysis to converge to a solution

**References:**
[1] H. Lin; A. Slagell; Z. Kalbarczyk; P. Sauer; R. Iyer, "Runtime Semantic Security Analysis to Detect and Mitigate Control-related Attacks in Power Grids," in IEEE Transactions on Smart Grid , vol.PP, no.99, pp.1-1
[2] Esther Amullen, Hui Lin, Zbigniew Kalbarczyk, and Lee Keel. 2016. Multi-agent System for Detecting False Data Injection Attacks Against the Power Grid. In Proceedings of the 2nd Annual Industrial Control System Security Workshop (ICSS '16). ACM, New York, NY, USA, 38-44.

## MULT-AGENT SYSTEM ARCHITECTURE

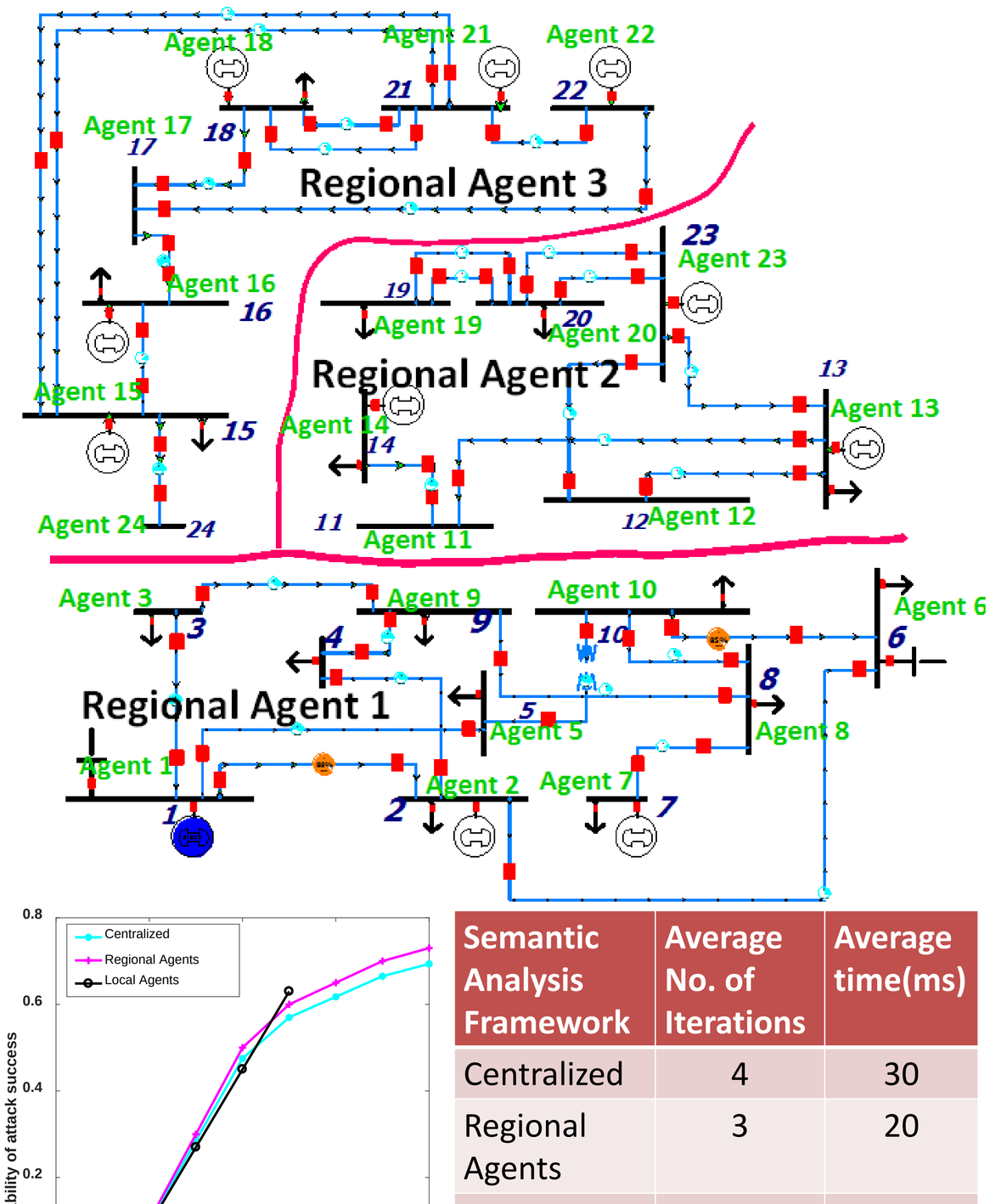
- Local agents
  - provide local (within a substation) communication and computation [2]
- Regional Agents
  - connect local agents located at substations based on geographic location and transmission line connectivity.
  - enable local agents run rapid power flow analysis to reduce latency and provide updated state information from other local agents
- The power grid is represented as a graph G={V, E}, with vertices V (buses) and edges E (line impendences). The *L-bounded Graph Partition Method* is used to establish subgraphs of the main power system

**Procedure** for defining regions

- **Input**: The number of regions k, the adjacency matrix $A=\{a_{i,j}\}$ (where the weighted edge $a_{i,j}$ represents the impendence of the transmission line and is nonzero when bus i and bus j are directly connected). **Output**: Desired regions 1, 2, …, k
  - (1) Create a normalized symmetric matrix A' from the matrix A
  - (2) Calculate the eigenvalues of A' and determine the largest k
  - (3) Use the eigenvalues from (2) and k as input to the expectation maximization clustering algorithm to determine vertices
  - (4) Generate adjacency matrices for each region k

## EXPERIMENTAL EVALUATION

- IEEE 24-bus power network is used to evaluate the distributed semantic analysis framework. 24 local agents and 3 regional agents are defined.







The regional and local agents detect attacks on transmission links along with the system

| Semantic Analysis Framework | Average No. of Iterations | Average time(ms) |
|---|---|---|
| Centralized | 4 | 30 |
| Regional Agents | 3 | 20 |
| Local Agents | 1 | 10 |

The regional and local agents run the look ahead power flow analysis with lower latency

## FUTURE WORK

- Optimize the distributed semantic analysis framework to further reduce detection time
- Implement a distributed intrusion mechanism at local agents and regional agents

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