AN INTEGRATED GENERATIVE ADVERSARIAL NETWORK FOR IDENTIFICATION AND MITIGATION OF CYBER-ATTACKS IN WIDE-AREA CONTROL

Jishnudeep Kar and Aranya Chakrabortty
FREEDM System Center,
North Carolina State University, Raleigh, NC

Introduction

Denial of service (DoS) and false data injection (FDI) attacks are very common in wide-area network. About DoS
- The communicating servers are jammed with malicious request
- Server becomes unable to respond to legitimate requests.
About FDI
- The data shared over the network is corrupted by adding bias.
- This could cause controllers and operators to actuate wrong control actions which may cause closed-loop instability.

Objective

False Data Injection Attacks – Detection and localization

- IEEE 68 bus system has 16 machines.
- Attacked links are shown by red lines.
- Communication delays are as follows:
  - Local = 0 ms,
  - Intra-area = 30ms,
  - Inter-area = 60ms.
- Training data consists of 5000 operating points obtained by load changes at several buses.

Results

- Neural network-based methods benefit in not requiring the actual model to ensure resiliency during a cyber-attack.
- Can be implemented in a decentralized manner ensuring model privacy.
- Proposed GAN based method work effectively to both localize and mitigate both FDI and DoS cyber-attacks.
- Future Work: Large changes in operating points, non-linear controller

Results (contd.)

Denial of Service Attacks – Closed-Loop Resiliency

- IEEE 68 bus system has 16 machines.
- Attacked links are shown by red lines.
- Communication delays are as follows:
  - Local = 0 ms,
  - Intra-area = 30ms,
  - Inter-area = 60ms.
- Training data consists of 5000 operating points obtained by load changes at several buses.

Conclusions

References