Motivations
- Data sharing amongst entities in electric grid is required for reliability.
- Successful cyber attacks on inter-area communications can have serious consequences and should be studied.
- Mimic outage and information sharing conditions that lead to Northeast blackout.

Objectives
- Introduce topology-targeted man-in-the-middle (MiM) communication attacks and study their consequences.
- Introduce MiM communication attacks on market coordination and study their consequences.
- Propose countermeasures for such attacks.

System Model

**EMS for Area 1**
- SCADA
- Local Topology Processing
- Local State Estimation
- Power Flow Calculation
- Local OPF Calculation
- Local generation dispatch plan

**EMS for Area 2**
- SCADA
- Local Topology Processing
- Local State Estimation
- Power Flow Calculation
- Local OPF Calculation
- Local generation dispatch plan

**Attack Model**

**Simulation & Results**
- Topology-targeted MiM attacks:
  - 5 possible long term outcomes of an attack after E0:
  - 1) Physical PF Overload
  - 2) Cyber PF Overload
  - 3) Not Converge; 4) No Violation; 5) Physical-cyber PF overload
- 373 total successful attack cases (69.08% of the total attack cases).
- MiM attacks on market coordination
- Potential consequences:
  1) OPF lack of convergence
  2) Lead to uneconomic and unreliable dispatch
  3) Attacker may make profit from such attack
- Countermeasures:
  - Understand the anomalies caused by attacks.
  - Test the attacks on a high fidelity distributed EMS platform.
  - Share external contingency list amongst areas.
  - Machine learning
  - Better operator training.