Implications of Cyber Attacks on Distributed Power System Operations

Jiazi Zhang, Lalitha Sankar and Kory W. Hedman

jzhan188@asu.edu, lalithasankar@asu.edu and kory.hedman@asu.edu
School of Electrical, Computer, and Energy Engineering | Arizona State University

21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2014 Grid of the Future Symposium

Content

- Motivation and Objectives
- System Model
- Attack Model
- Simulation and Results
- Conclusion and Countermeasures

Motivation and Objectives

Motivation:

- ➢ 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.
- ➢ Mimicking outage and information sharing conditions that led to the Northeast blackout in 2003.

Objectives:

- ➢ Introduce a class of topology-targeted man-in-the-middle communication attacks.
- ➢ Study attack consequences using a time progression model for cyber operations.
- ➢ Propose countermeasures for such attacks.

System Model

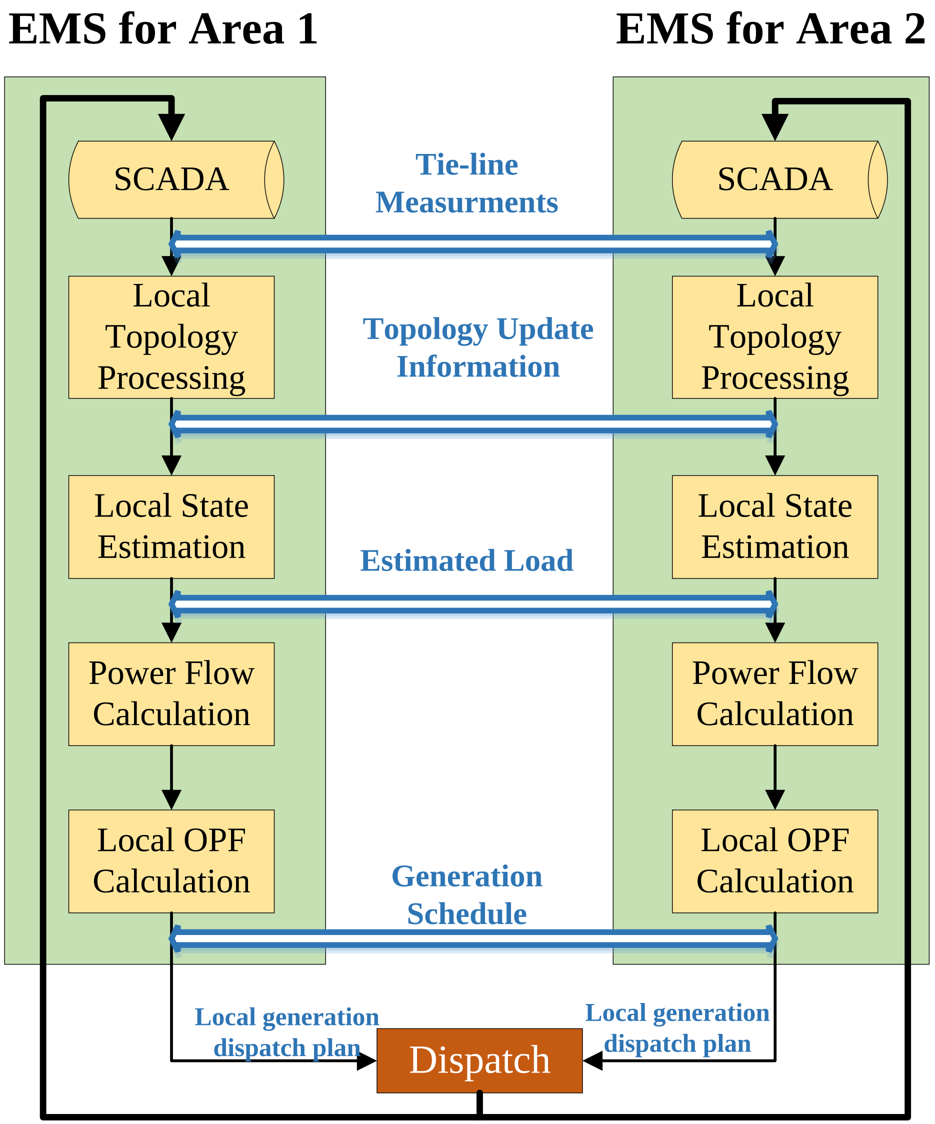


Fig.1 Computational units and data interactions between two areas of the network

System Model

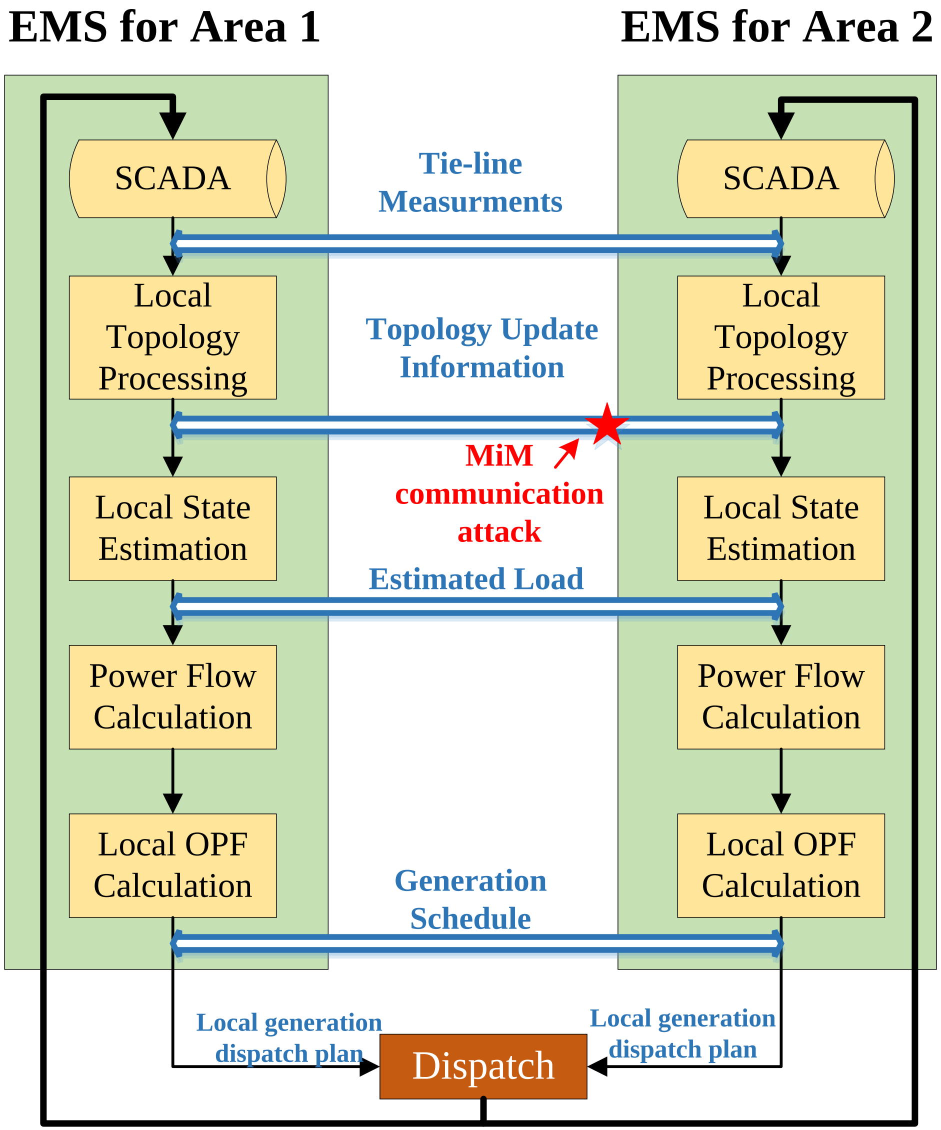
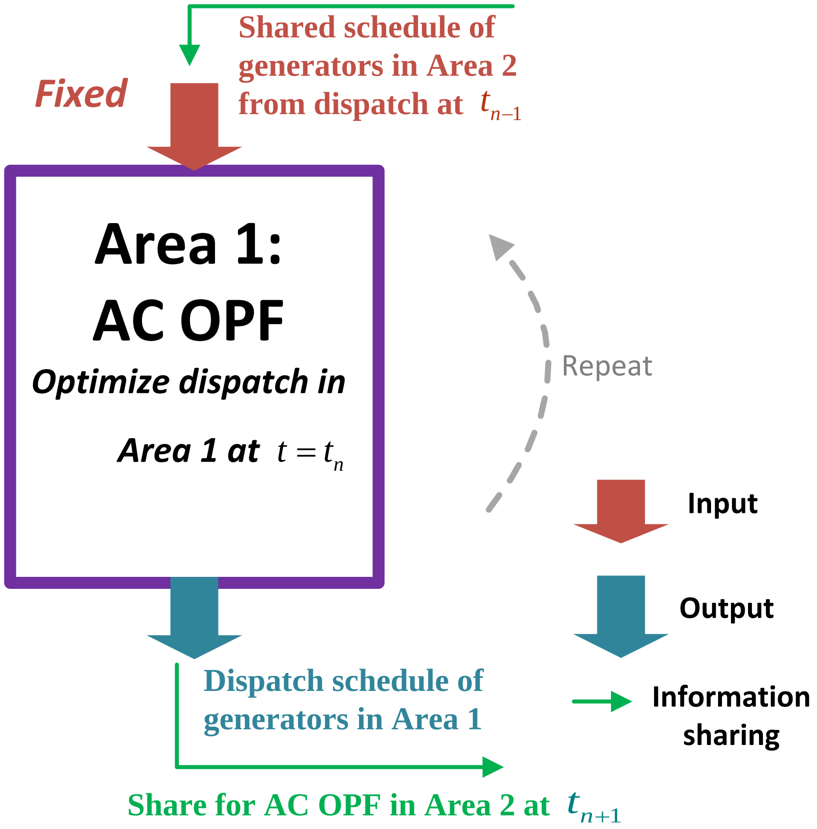


Fig.1 Computational units and data interactions between two areas of the network

System Model

Computational models

➢ Optimal Power Flow:



Shared schedule of generators in Area 2 from dispatch at t_{n-1}
Fixed
Area 1:
AC OPF
Optimize dispatch in Area 1 at $t = t_n$
Repeat
Input
Output
Information sharing
Dispatch schedule of generators in Area 1
Share for AC OPF in Area 2 at t_{n+1}

Fig.2 Optimal power calculation unit for area 1

For area i :

- Perform OPF with whole network topology;
- Optimize dispatch of generators only in area i;
- Fix generation schedule shared from neighboring area.

Attack Model

- **Attacker capability:** the attacker has access to the data being shared between areas and can corrupt the data:

1) Participate in creating a line outage in one area/ be aware of such an outage

2) Corrupt the topology information shared with the other area.

- **Modeling human error:**

  1) Contingency communication delays

  2) Line switch miscommunications

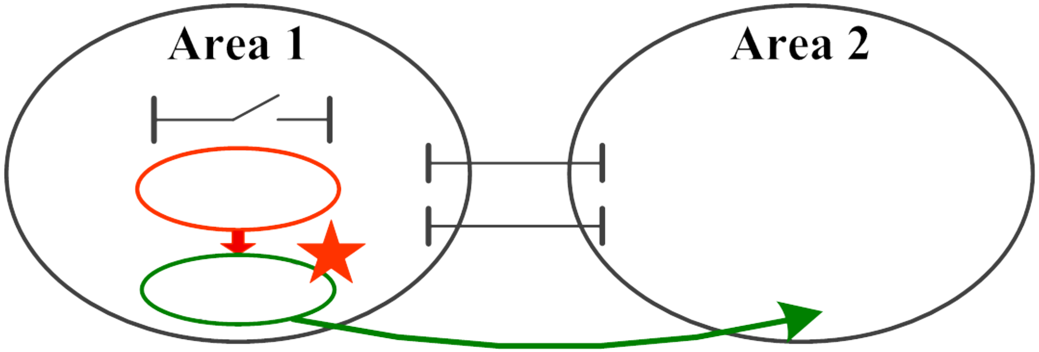
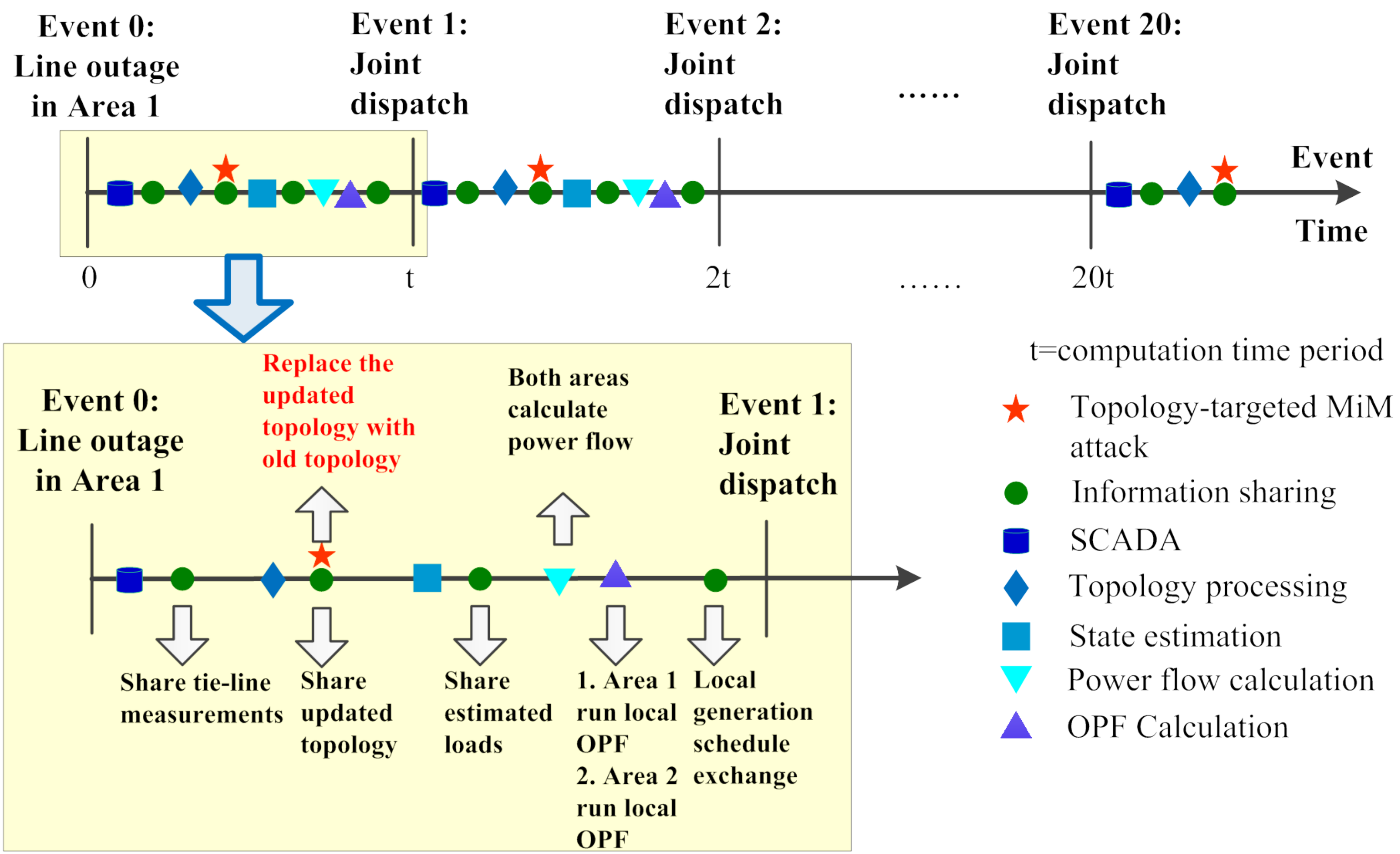


Fig. 3 Topology-targeted MiM Attack Model

- In Area 1 Line *i* outage happens
- Area 1 updates the topology (s_i=0) and communicates with Area 2
- Attacker access to the topology communication, replace the updated topology with the old topology
- Area 2 now has false topology information (s_i=1)

Attack Model



Event 0: Line outage in Area 1

Event 1: Joint dispatch

Event 2: Joint dispatch

……

Event 20: Joint dispatch

Event

Time

0

t

2t

……

20t

Event 0: Line outage in Area 1

Replace the updated topology with old topology

Both areas calculate power flow

Event 1: Joint dispatch

Share tie-line measurements

Share updated topology

Share estimated loads

1. Area 1 run local OPF
2. Area 2 run local OPF

Local generation schedule exchange

t=computation time period

- ★ Topology-targeted MiM attack
- ● Information sharing
- ▮ SCADA
- ◆ Topology processing
- ■ State estimation
- ▼ Power flow calculation
- ▲ OPF Calculation

Fig.4 Time progression model

Simulation and Results

Test system:

MiM Attack:

- ➢A line outaged in one area
- ➢A line congested prior to the attack in the other area.
- ➢Replace updated topology with old topology

- ➢All possible choice of line outage in one area and congested line in the other area are exhaustively tested.

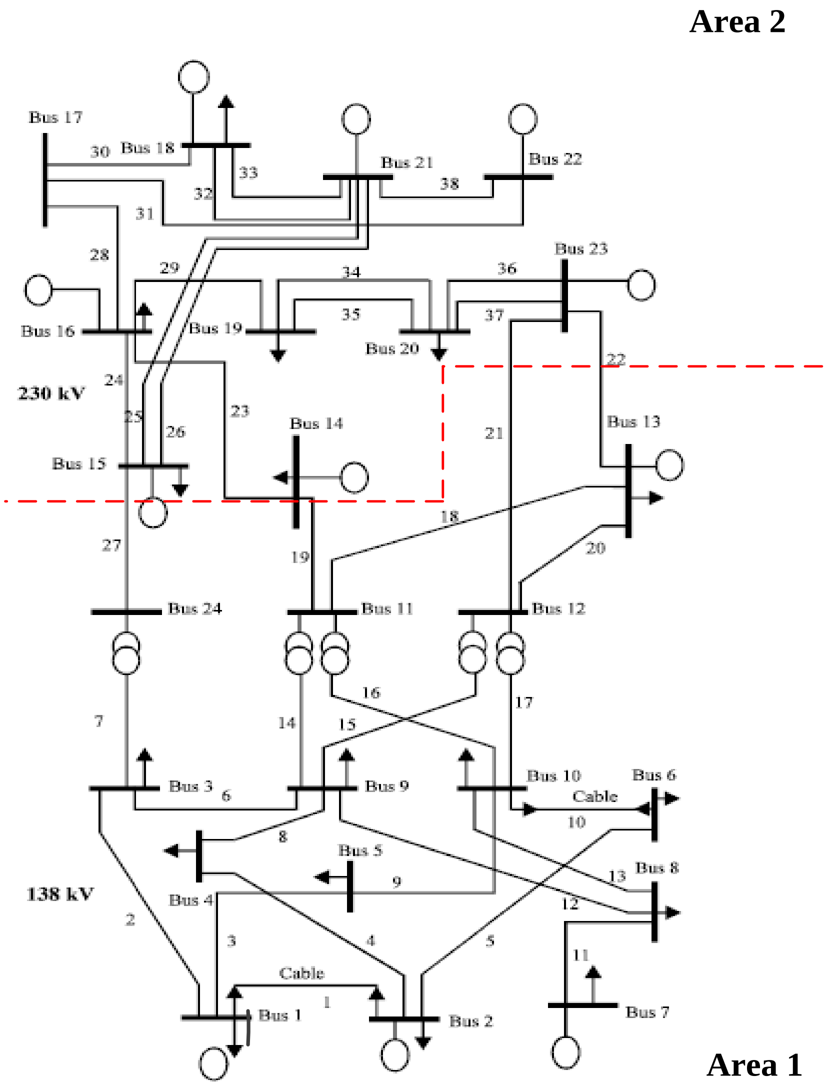


Fig. 5 An IEEE RTS 24-bus divided into two areas

Simulation and Results

Overall statistics:

Feasible Case	Physical PF Overload	Cyber PF Overload	Not Converge	Undetectable cases
540	35.19%	24.44%	17.41%	22.96%

PF: Power flow

Table 1. System behavior with sustained attack

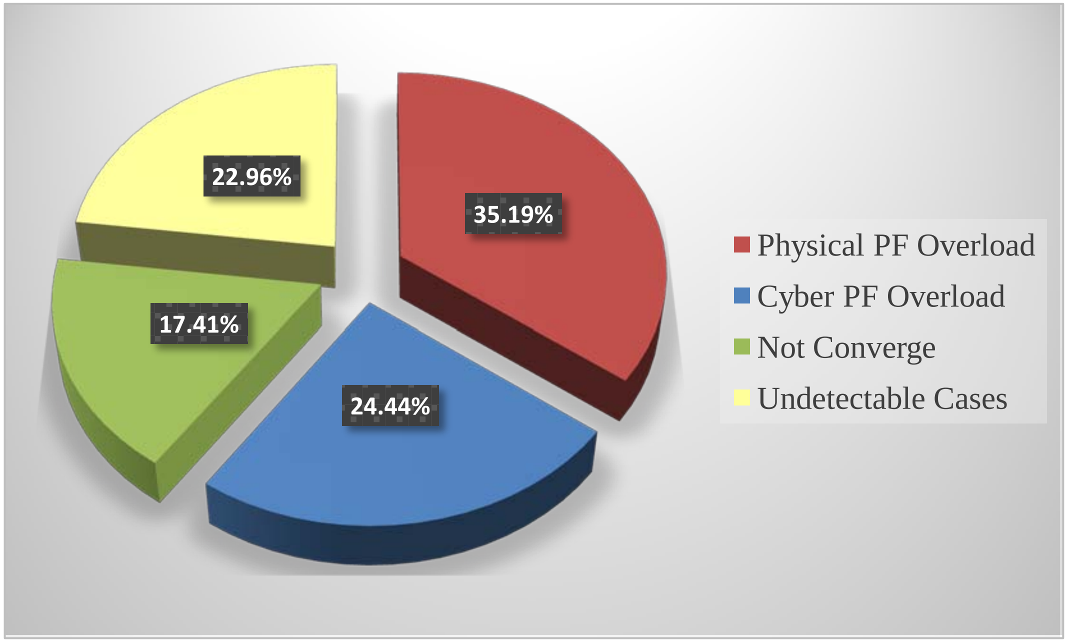
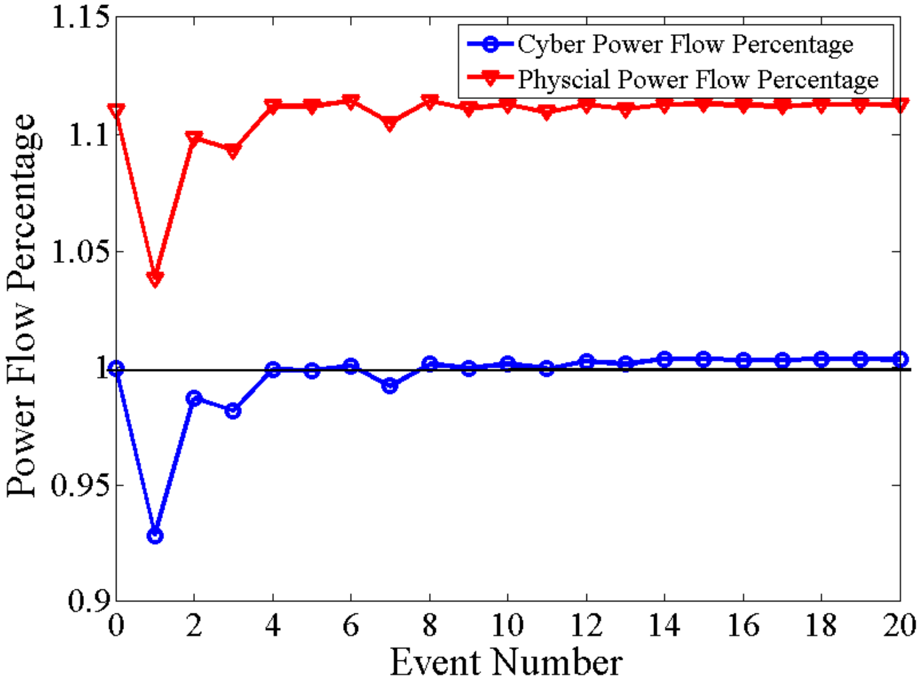


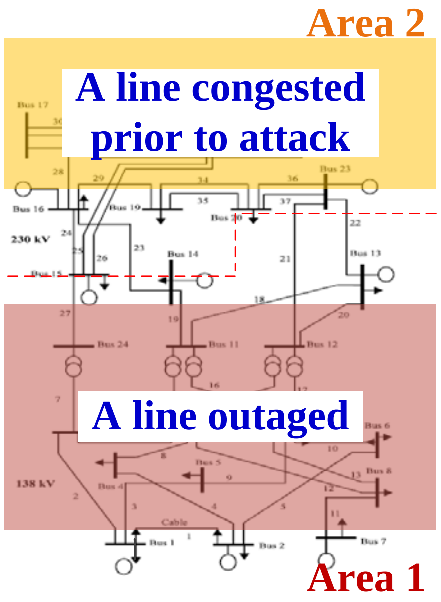
Fig. 6 Pie chart for statistic simulation results of the test system

Simulation and Results

Disparities:

- 1) Physical PF Overload (*successful attack*)
  - For area with false topology, monitoring the cyber power flow cannot reflect the severity of the physical overload.





Area 2

A line congested prior to attack

A line outaged

Area 1

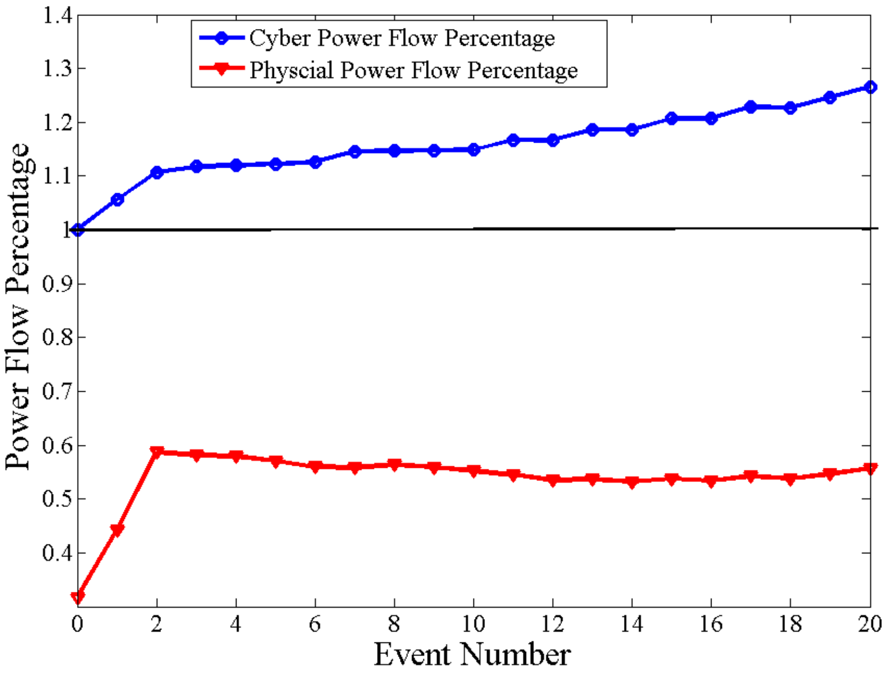
Fig.7 Physical PF Overload case: Power flow on prior congested line #24 (area 2) when line #3 (area 1) is outaged.

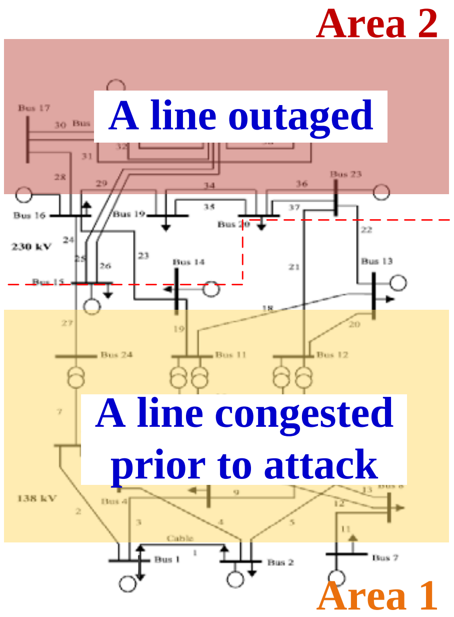
Simulation and Results

Disparities:

2) Cyber PF Overload Violation (*successful attack*)

- Can cause mis-operation such as throttling up other nearby sources or load shedding.





Area 2

A line outaged

A line congested prior to attack

Area 1

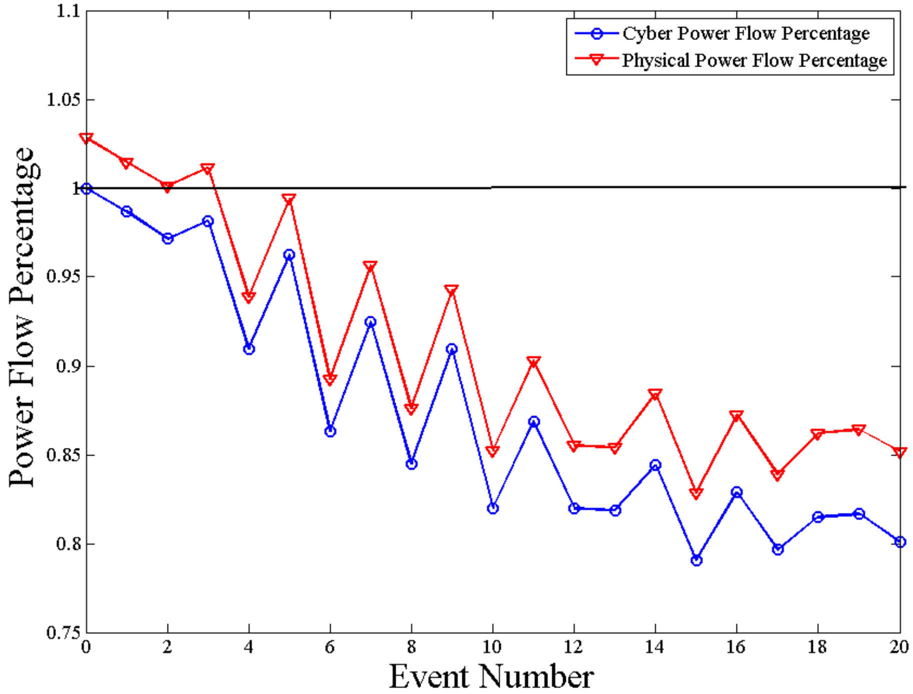
Fig.8 Cyber PF Overload Violation case: Power flow on prior congested line #14 (area 1) when line #23 (area 2) is outaged.

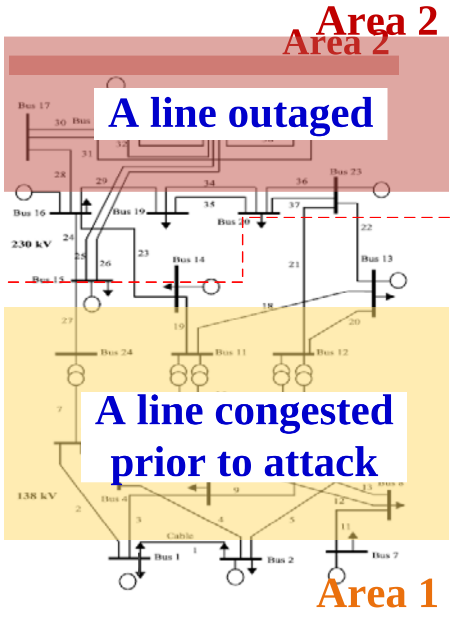
Simulation and Results

Disparities:

3) Undetectable cases (***unsuccessful attack***)

- Power flow reduce below 100% after few events
- No further problem happened





Area 2

Area 2

A line outaged

A line congested prior to attack

Area 1

Fig.9 Undetectable case: Power flow on prior congested line #9 (area 1) when line #29 (area 2) is outaged.

Simulation and Results

Disparities:

4) PF Not Converge (***successful attack***)

- Cannot find feasible OPF solution for one area
- Require distributed OPF algorithm (joint OPF calculation) between two areas

Result summary:

- For test system, there are 416 total successful attack cases, which is 77.04% of the total attack cases.
- Total critical attack cases (physical power flow > 105%) are 53, which is 9.81% of the total attack cases.
- This result demonstrates the vulnerability of the topology-targeted MitM attack.

Conclusion and Countermeasures

- Demonstrate the time consequences of a new class of man-in-the-middle distributed communication attacks.
- Show that such attacks can lead to serious consequences if active intervention is not present.

Countermeasures:

Build a more interactive distributed processing platform:

(a) enable real-time coordination of OPF calculation between areas;

(b) create and share external contingencies lists.

THANK YOU!

ANY QUESTIONS?

Jiazi Zhang
jzhan188@asu.edu