False Data Injection Attacks: Feasibility of Limited Knowledge Attacks and Scalability of Attacks on Large Power Systems

Lalitha Sankar

Arizona State University

(lsankar@asu.edu)

PSERC Webinar
September 5, 2017

Industry Advisors

- Mark Westendorf (MISO)
- Evangelos Farantatos (EPRI)
- Galen Rasche (EPRI)
- Reynaldo Nuqui (ABB)
- George Stefopoulos (NYPA)
- Sharon Xia (ALSTOM)
- Eugene Litvinov (ISONE)
- Harvey Scribner (SPP)
- Benjamin Kropowski (NREL)
- Maurice Martin (NREL)
- Erfan Ibrahim (NREL)
- Reid Fudge (Tristate GT)
- Brandon Aguirre (Tristate GT)

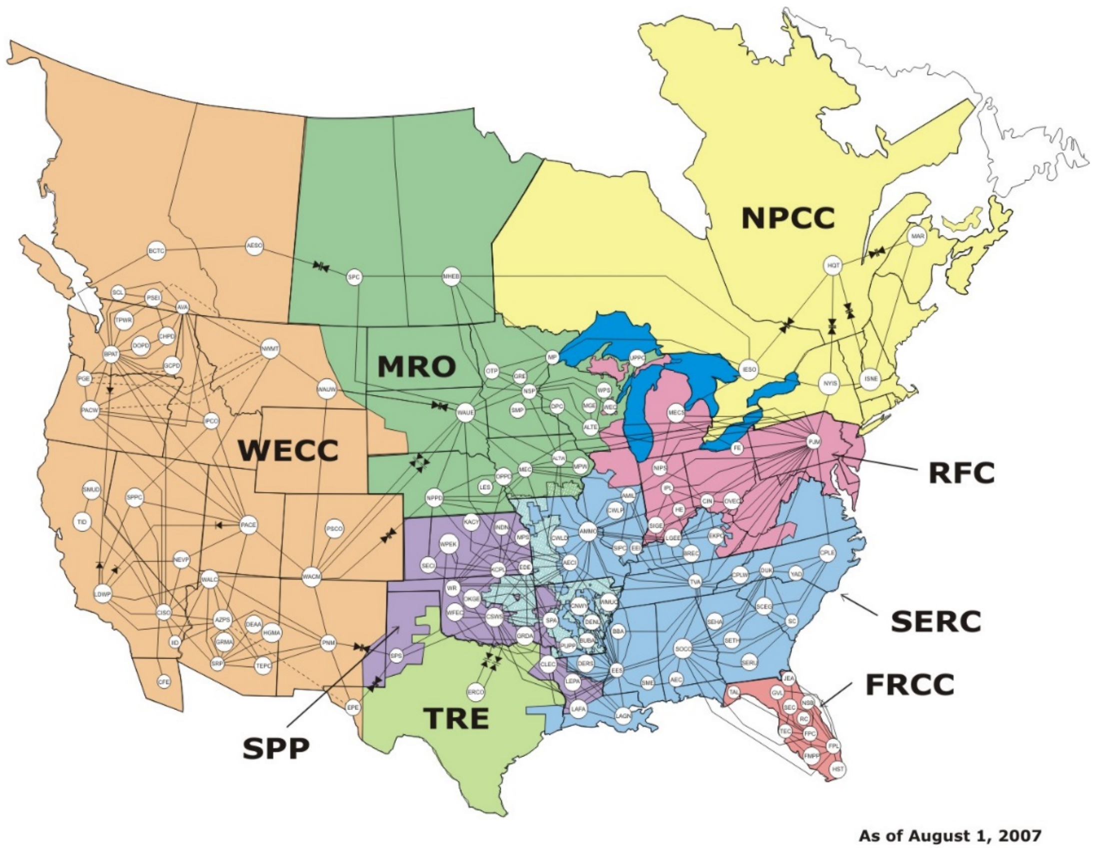
Content

- Electric Power System: Introduction
- Cyber-attacks on the Grid
- Approach:
  - Java-based software verification platform
  - False data injection (FDI) attacks
- Ongoing Work

Electric Power System

North American Electric Power Grid

US is 18% of world consumption as of 2015.

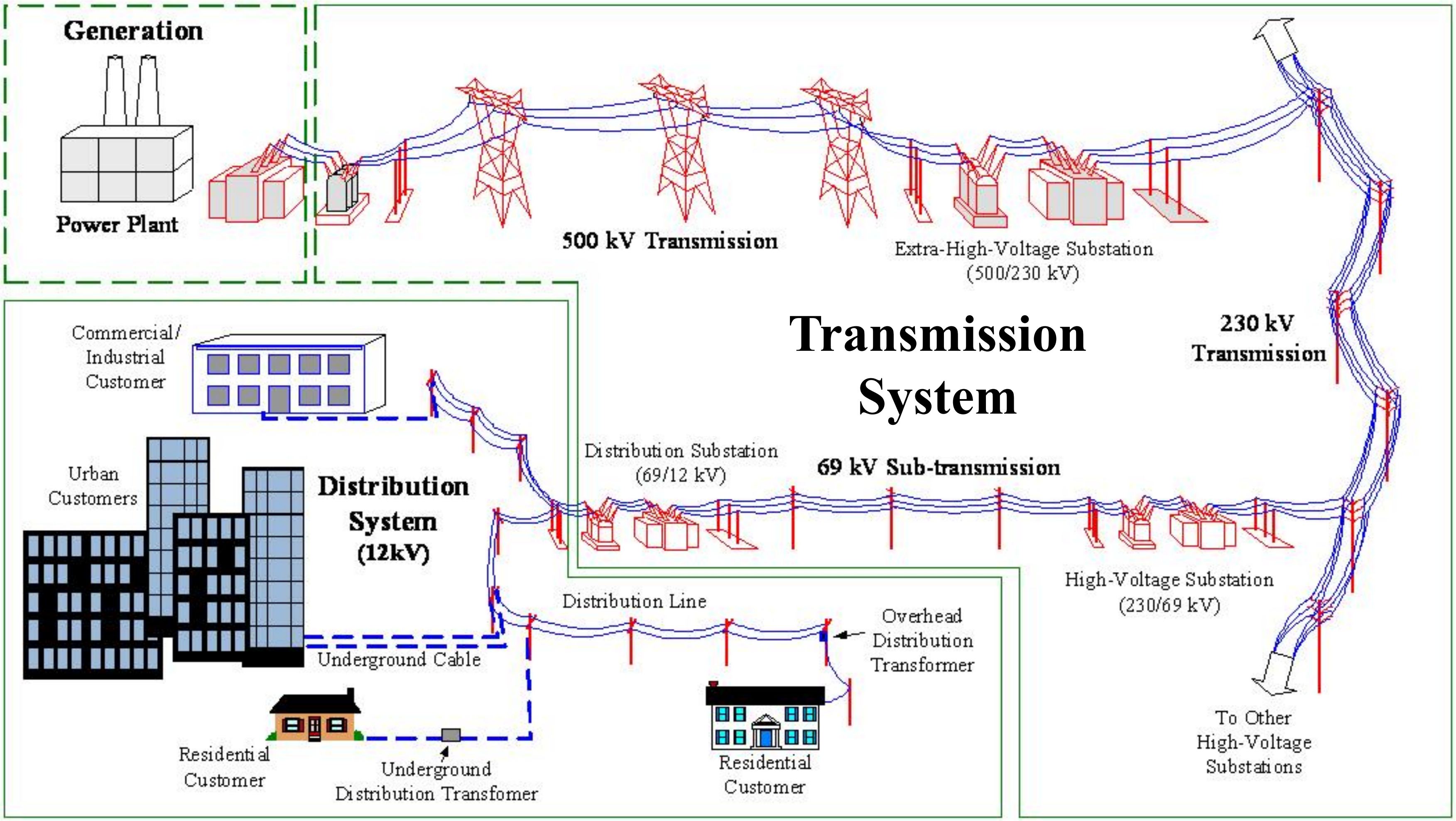


- 3200 electric utility companies
- 17,000 power plants
- 800 GW peak demand
- 165,000 miles of high-voltage lines
- 140 million meters
- $ 1 trillion in assets

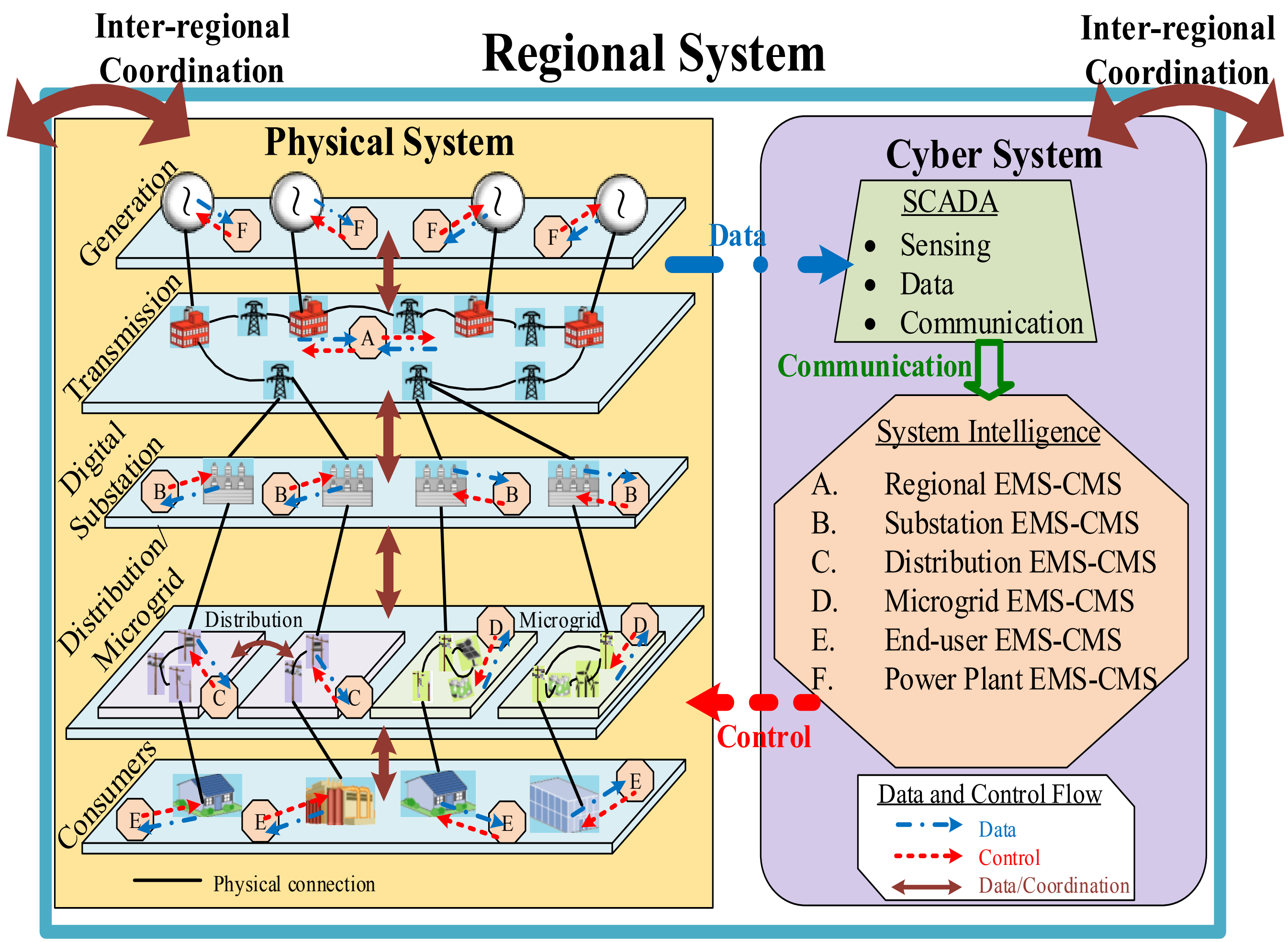
D. Wollman, "Accelerating Standards and Measurements for the Smart Grid," National Institute of Standards and Technology (NIST), U.S. Department of Commerce. [Online] https://www.superlectures.com/icassp2011/downloadFile.php?id=322&type=slides&filename=accelerating-standards-and-measurements-for-the-smart-grid

Electric Power System

Generation, transmission, and distribution model

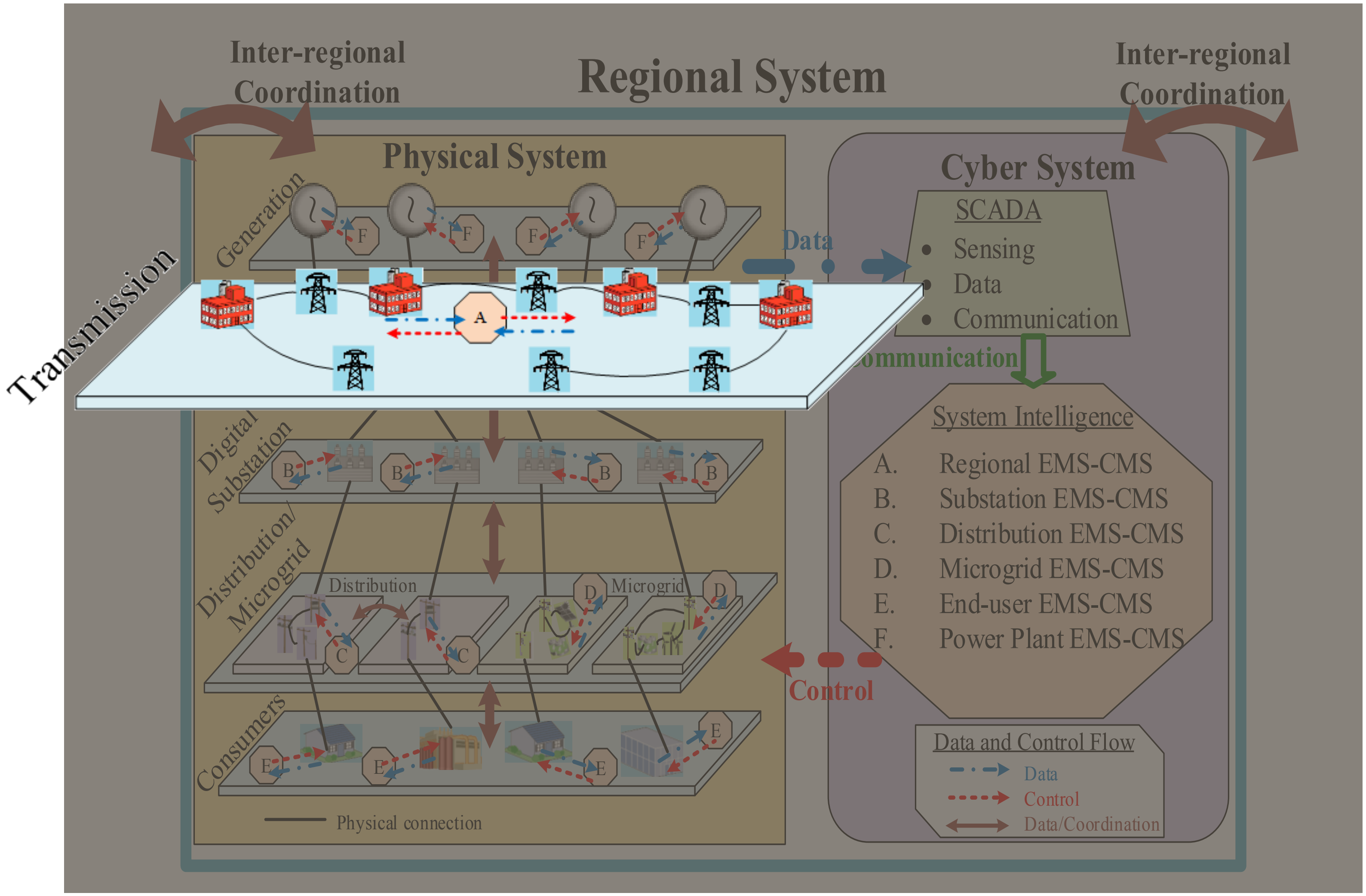


Hierarchical Cyber-physical Power System



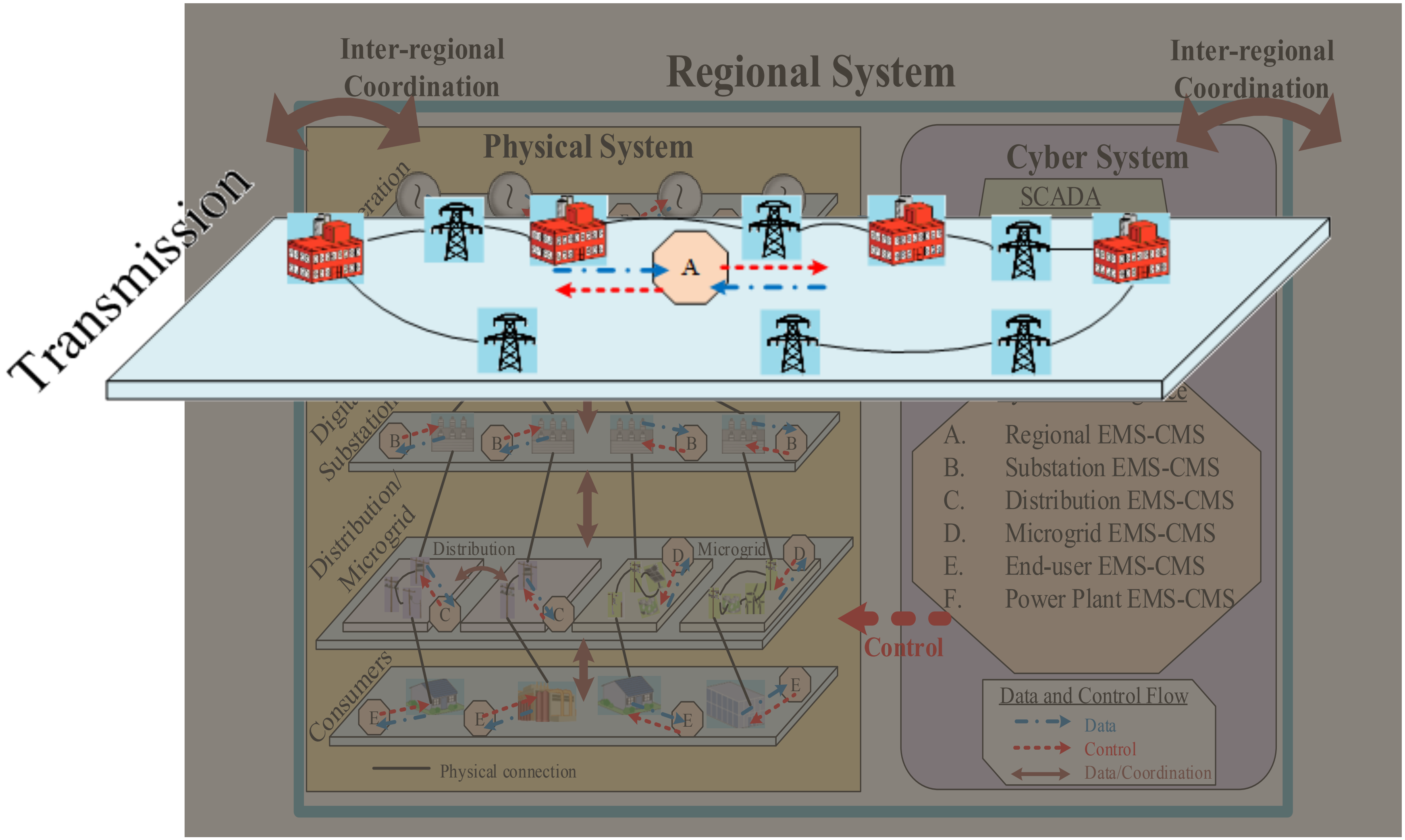
Hierarchical Cyber-physical Power System

Hierarchical Cyber-physical Power System



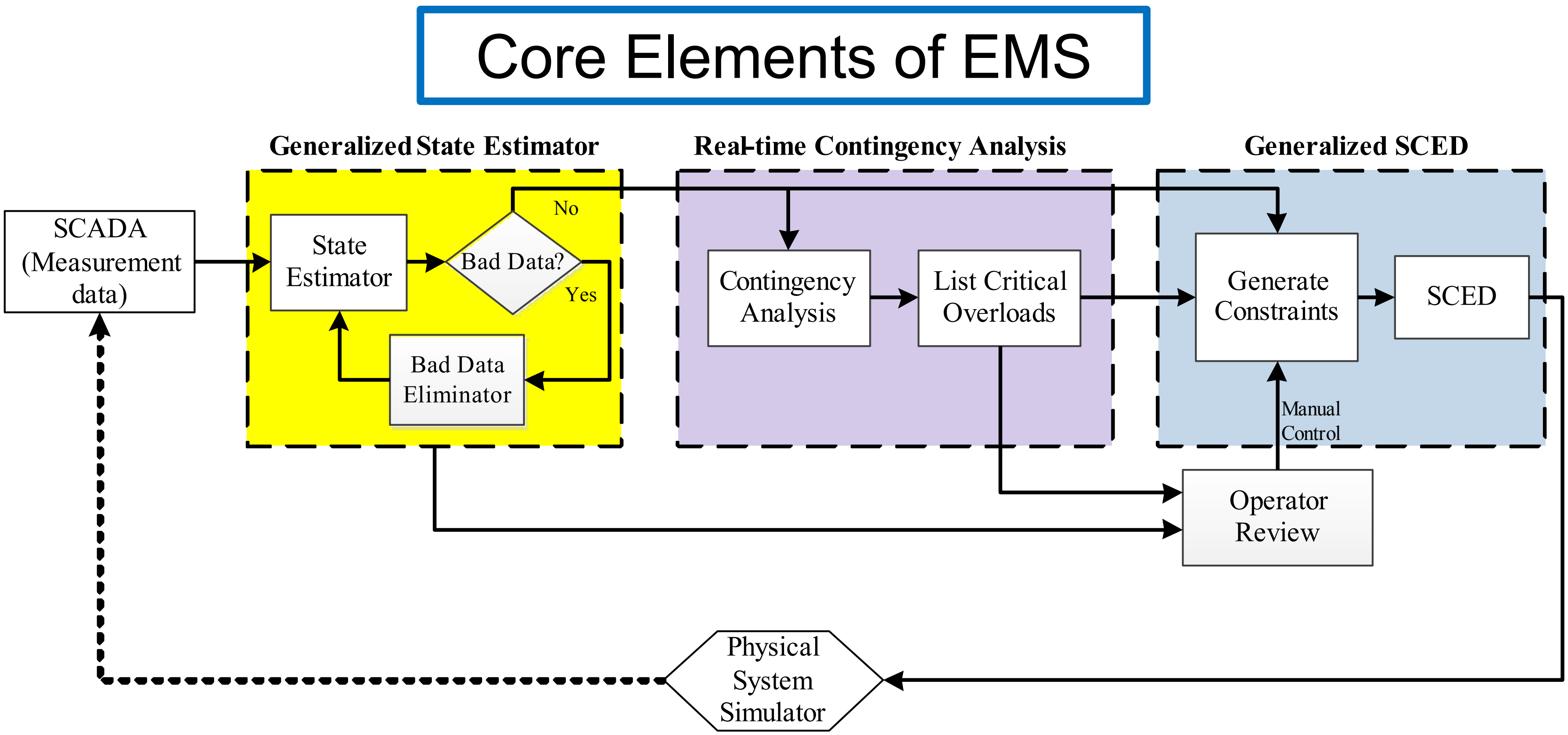
Hierarchical Cyber-physical Power System

Hierarchical Cyber-physical Power System



Hierarchical Cyber-physical Power System

Energy Management System (EMS)

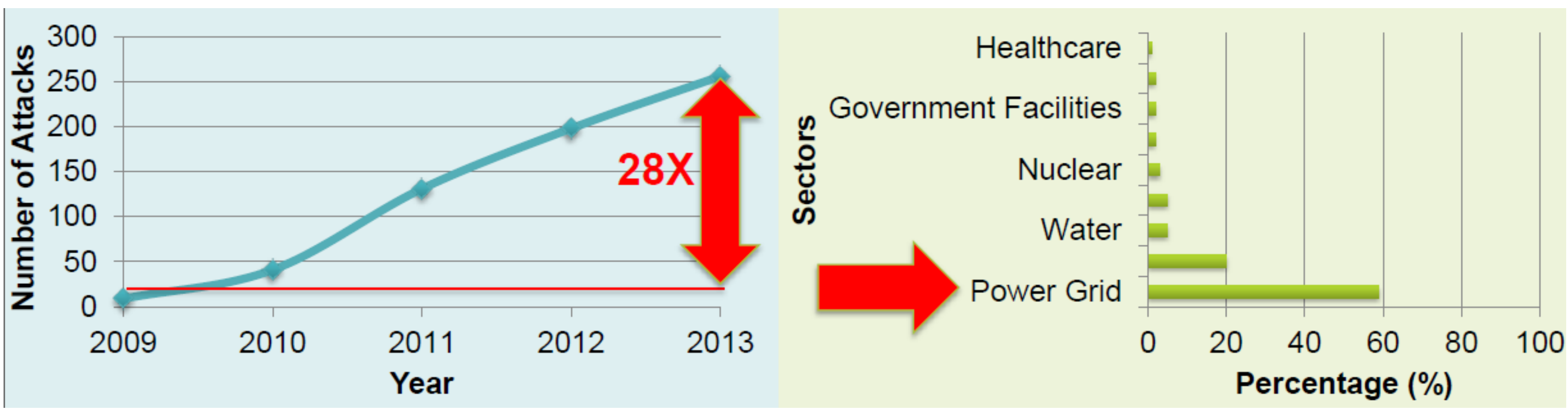


Cyber-attacks on the Grid

Cyber-attacks on the Grid

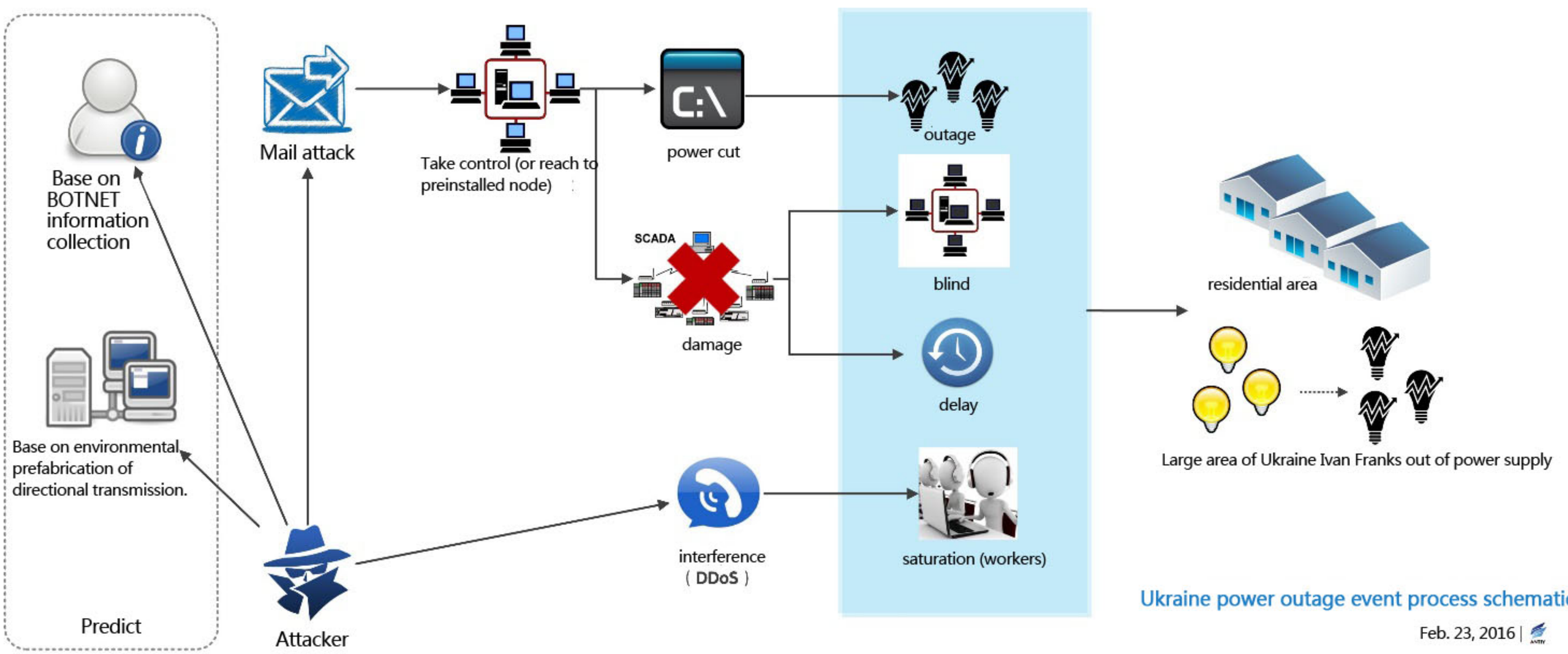
- Electric power system is vulnerable to cyber attacks
  - Stuxnet malware attacks SCADA systems in Germany in 2010
  - Ukraine power grid attacks in 2015

- DHS recorded 161 cyber attacks on the energy sector in 2013, compared to 31 in 2011



Ukraine Cyber Attack

- Cyber attack against Ukraine power grid illuminated the urgency of prognosis of cyber attacks on open-source EMS platform



Antiy Labs, “Comprehensive analysis report on Ukraine power system attacks,” March 2016. [Online]. Available: http://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks/

Motivation

- What is the motive for attacking the electric power system?
  - Financial, social, political
- Financial damage akin to credit card theft can be achieved by manipulating electricity markets
  - Unclear if sophisticated cyber-attacks on the electric grid is required
- Attacks need to create significant change in production and flow of electrical power to cause large scale damage
- Can cascading outages and failures be achieved by intelligent attacks on the cyber-infrastructure of electric power systems?
  - Physical attacks on the grid not considered

Approach

Two-Pronged Approach

Theoretical Work

- Analyze potential attacks
- Characterize system vulnerabilities
- Develop countermeasure algorithms

IMPLEMENT

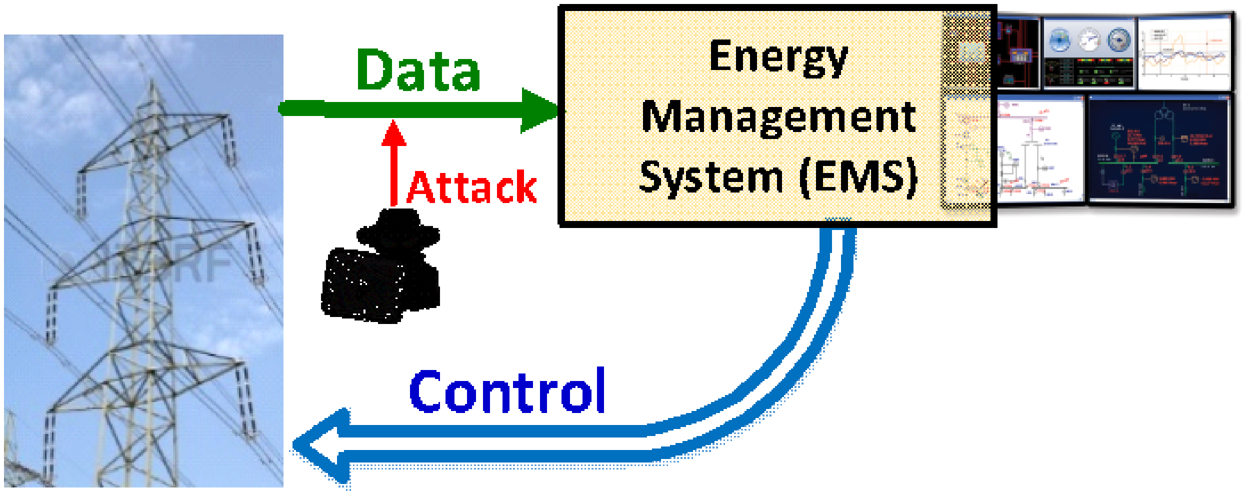
VERIFY

Simulation Platform

- Java-based, high-fidelity EMS (Energy Management System) simulation
- Simulate attacks and system response on large scale systems

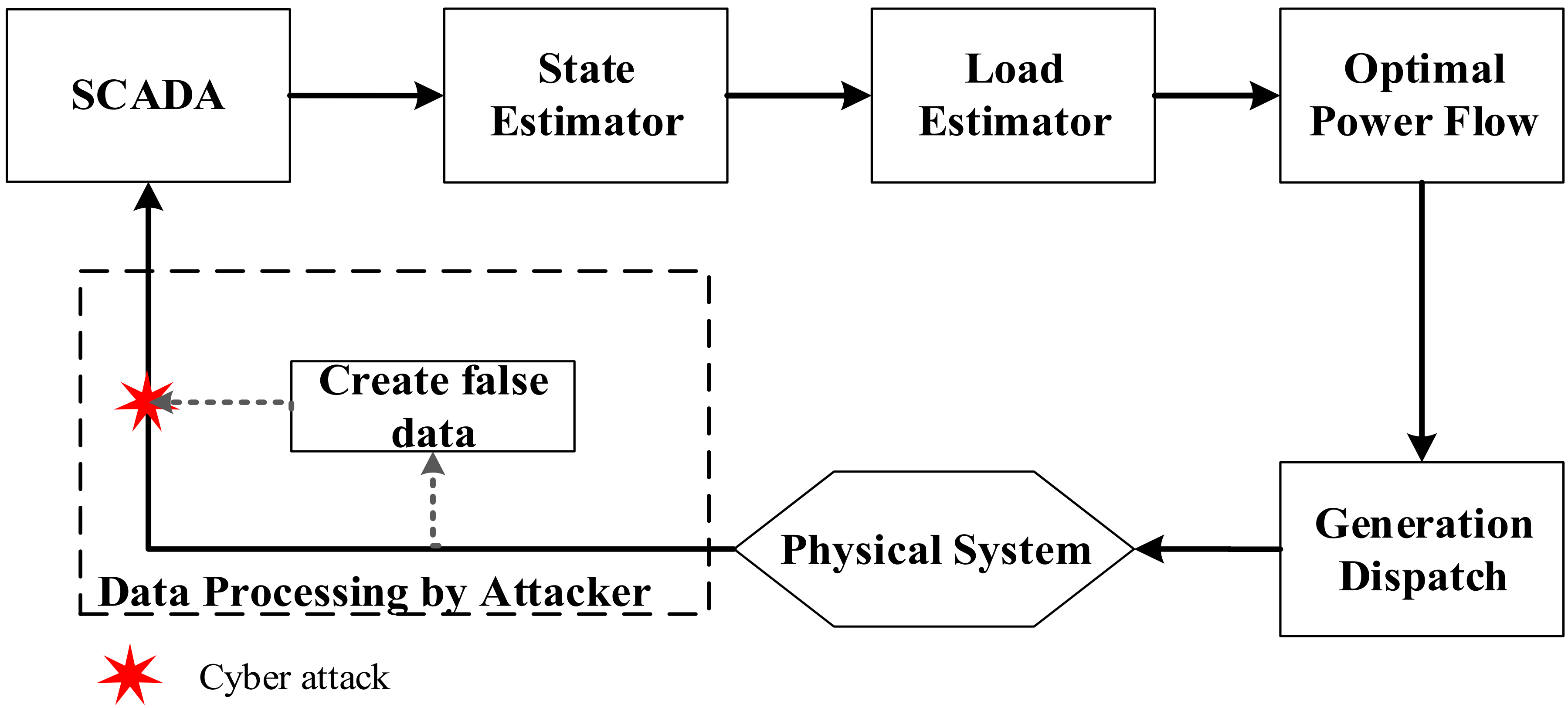
Project jointly funded by NSF and DHS, as well as PSERC (S.72)

False Data Injection (FDI) Attack



- Knowing system configuration, attacker can inject malicious data (measurements) without detection by existing techniques for bad data detection
- Requires attacker to have access to remote terminal units (RTUs) or a control center
- Replace actual data packets with carefully constructed malicious data packets and impersonate a valid data source

System and Attack Model



State of Art

- Liu *et al.* introduce FDI attacks on DC state estimation (SE) and demonstrate that FDI attacks cannot be detected by bad data detector [1]

- Hug and Giampapa demonstrate that FDI attacks on AC SE requires both system topology and state knowledge [2]

- Liang *et al.* demonstrate that FDI attacks can lead to overflow in physical system which cannot be detected in cyber layer [3]

- Yuan *et al.* introduce a two-stage optimization problem to determine the most damaging FDI attacks that can maximize optimization costs [4]

---

[1]. Y. Liu, P. Ning, and M. K. Reiter, False data injection attacks against state estimation in electric power grids," in Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS '09, (Chicago, Illinois, USA), pp. 21-32, 2009.

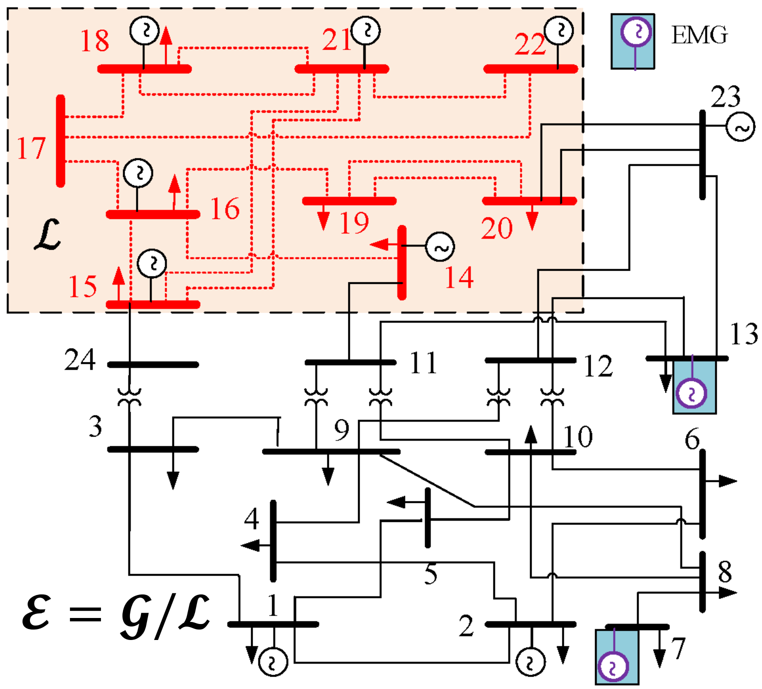
[2]. G. Hug and J. A. Giampapa, Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1362-1370, 2012.

[3]. J. Liang, O. Kosut, and L. Sankar, Cyber-attacks on ac state estimation: Unobservability and physical consequences," in IEEE PES General Meeting, (Washington, DC), July 2014.

[4]. Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," Smart Grid, IEEE Transactions on, vol. 2, no. 2, pp. 382–390, June 2011.

Our Contributions

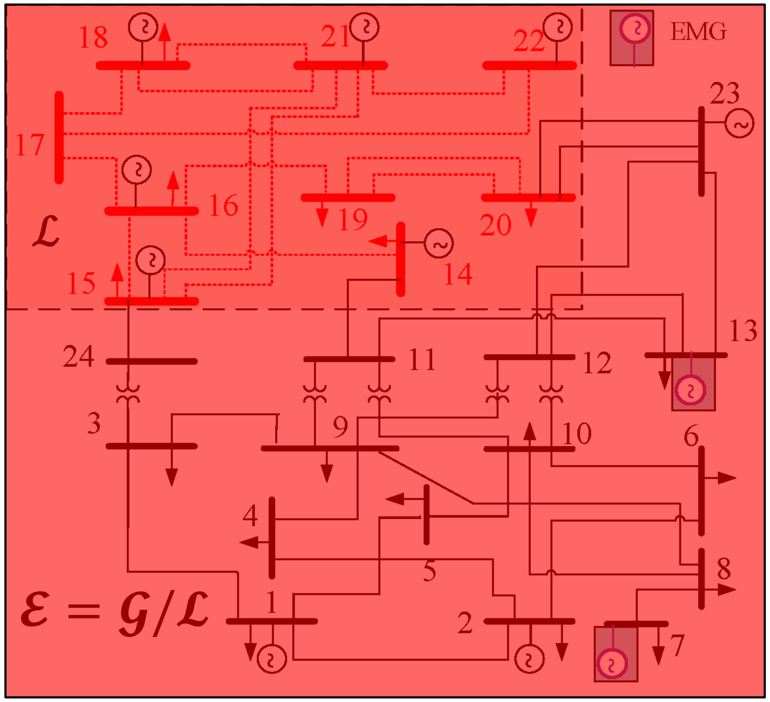
- Assume the attacker has control in a subnetwork $\mathcal{L}$



EMG: external marginal generators

Our Contributions

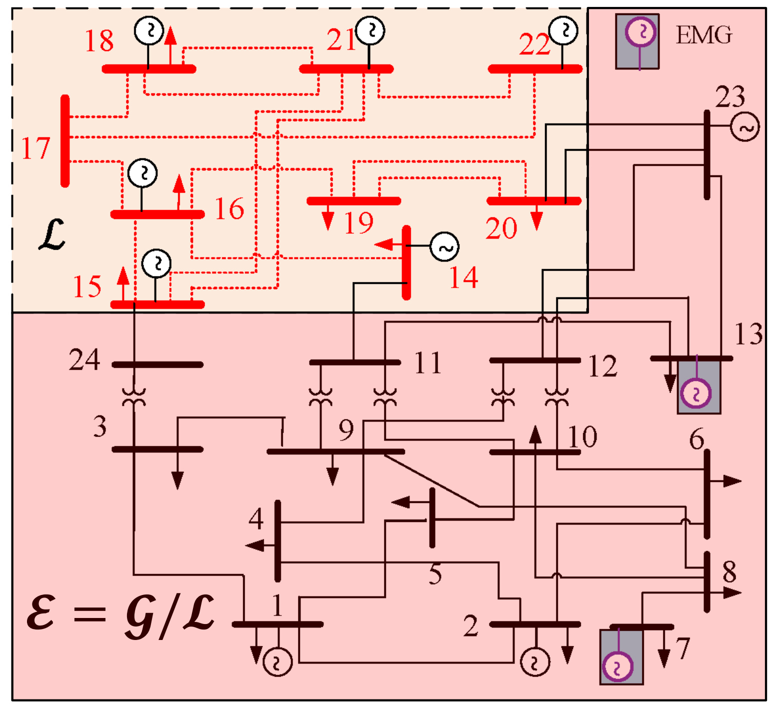
- Assume the attacker has control in a subnetwork $\mathcal{L}$
  - Model 1: The attacker has full knowledge of the whole system



EMG: external marginal generators

Our Contributions

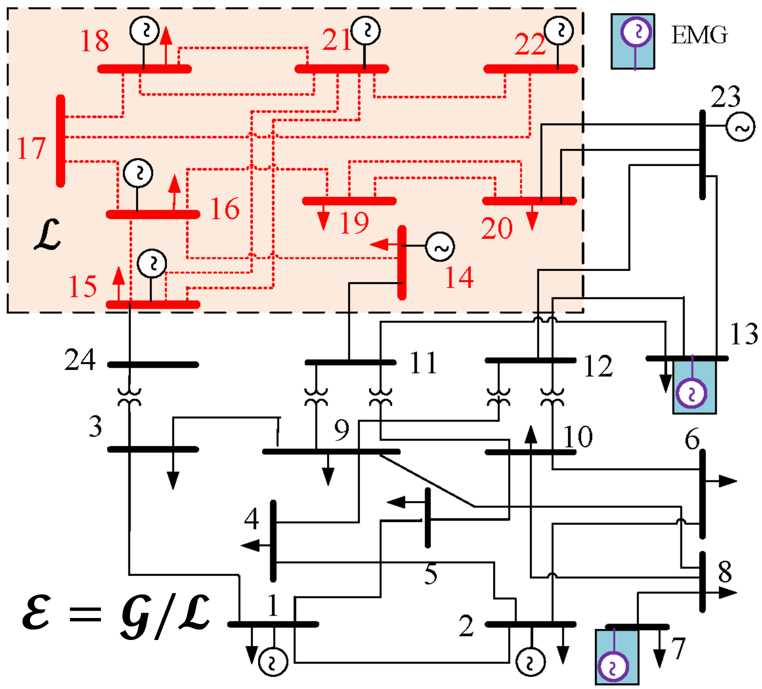
- Assume the attacker has control in a subnetwork $\mathcal{L}$
  - Model 1: The attacker has full knowledge of the whole system
  - Model 2: The attacker has full knowledge of $\mathcal{L}$ but limited knowledge of $\mathcal{E}$



EMG: external marginal generators

Our Contributions

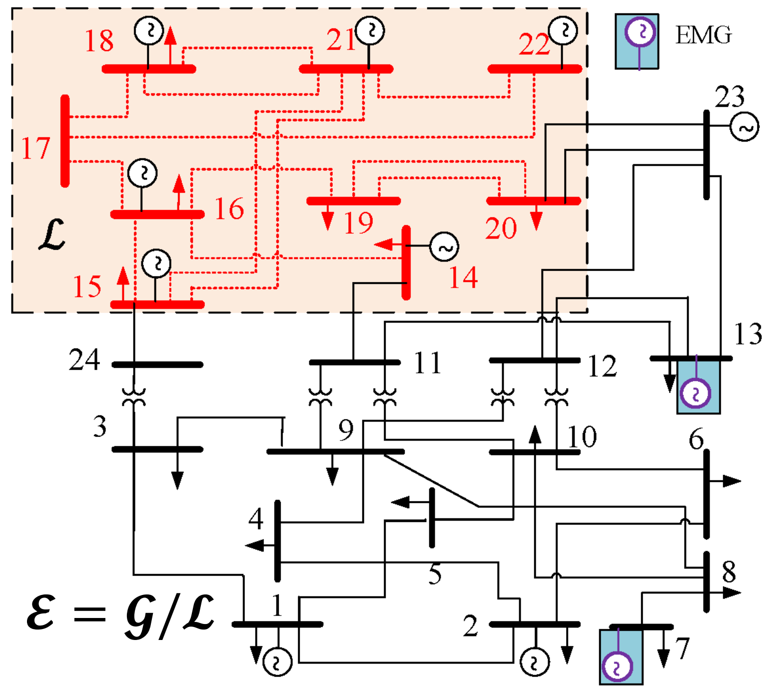
- Assume the attacker has control in a subnetwork $\mathcal{L}$
  - Model 1: The attacker has full knowledge of the whole system
  - Model 2: The attacker has full knowledge of $\mathcal{L}$ but limited knowledge of $\mathcal{E}$
  - Model 3: The attacker has full knowledge of $\mathcal{L}$ but no knowledge of $\mathcal{E}$



EMG: external marginal generators

Our Contributions

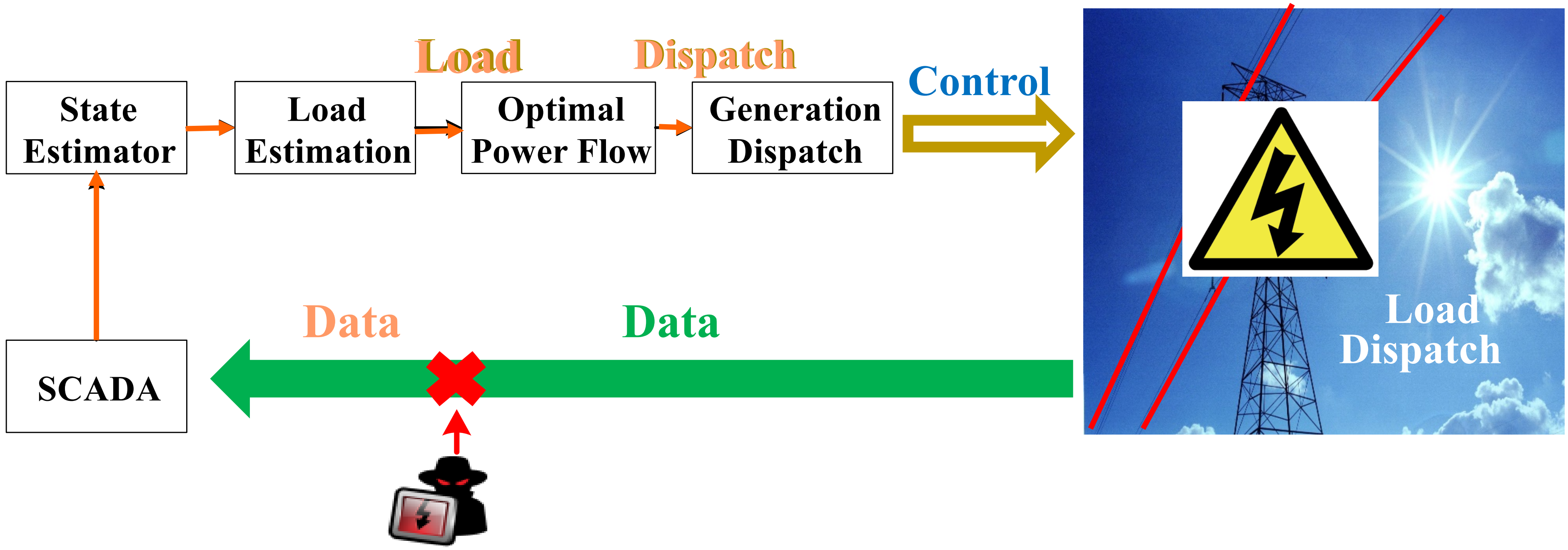
- Assume the attacker has control in a subnetwork $\mathcal{L}$
  - Model 1: The attacker has full knowledge of the whole system
  - Model 2: The attacker has full knowledge of $\mathcal{L}$ but limited knowledge of $\mathcal{E}$
  - Model 3: The attacker has full knowledge of $\mathcal{L}$ but no knowledge of $\mathcal{E}$



EMG: external marginal generators

- Assess power system vulnerability to FDI attacks with all three models

Worst-case Line Overflow FDI Attacks



Joint work with Jingwen Liang and Oliver Kosut

J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Transactions on Power Systems*, vol. PP, no. 99, pp. 1–9, 2016.

Worst-case Line Overflow Attacks

- The knowledge (K1) and capability (C1) of the attacker:

K1
i. The topology of the entire power system $\mathcal{G}$
ii. The cost, capacity, and operational status of generators in $\mathcal{G}$
iii. The historical load data in $\mathcal{G}$

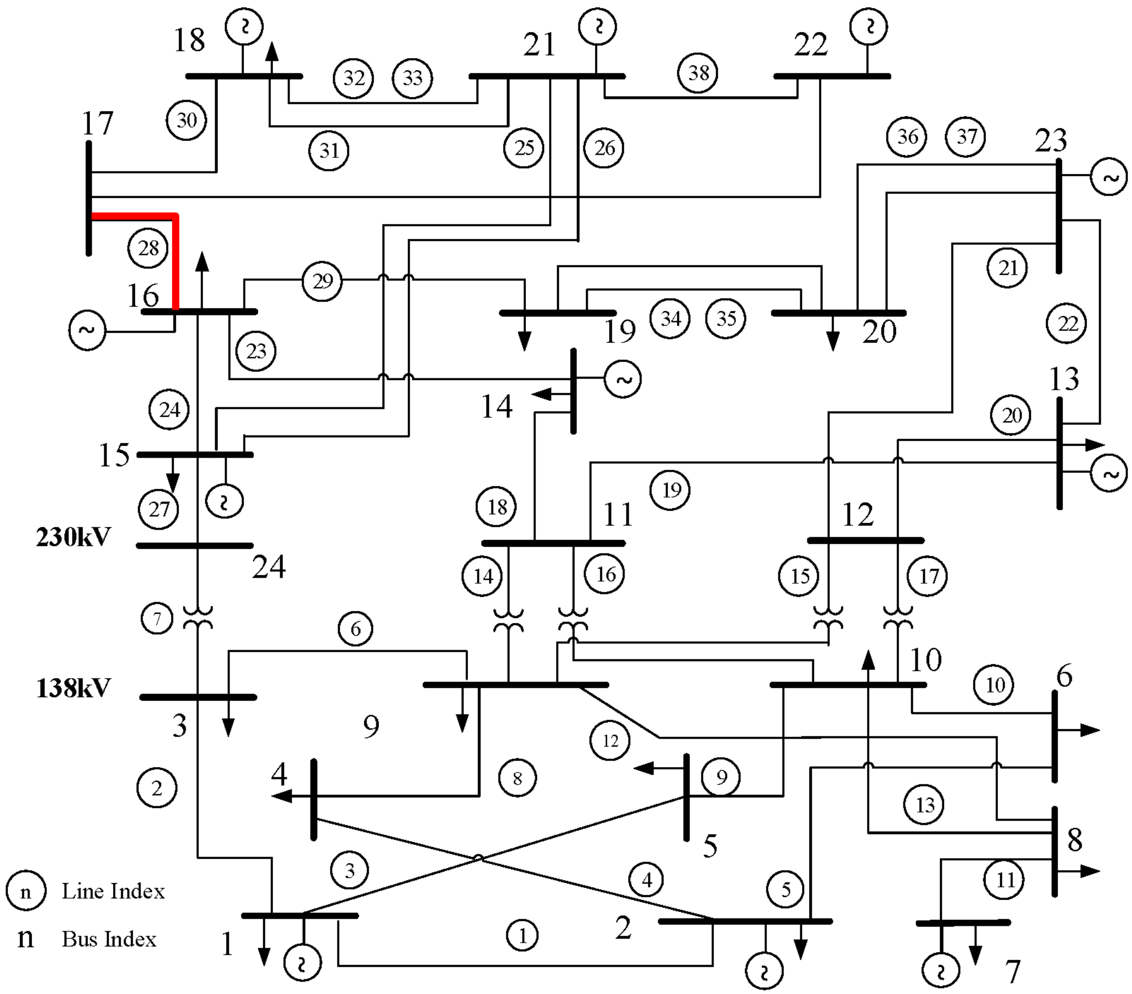
C1 Access and modify measurements inside a small area $\mathcal{S}$, $\mathcal{S} \subseteq \mathcal{G}$

- Attack implementation via sub-graph

The attacker replaces several measurements inside $\mathcal{S}$ with counterfeits:

$$\bar{z}_i = \begin{cases} z_i\ , & i \notin \mathcal{J}_\mathcal{S} \\ h_i(\hat{x} + c)\ , & i \in \mathcal{J}_\mathcal{S} \end{cases}$$

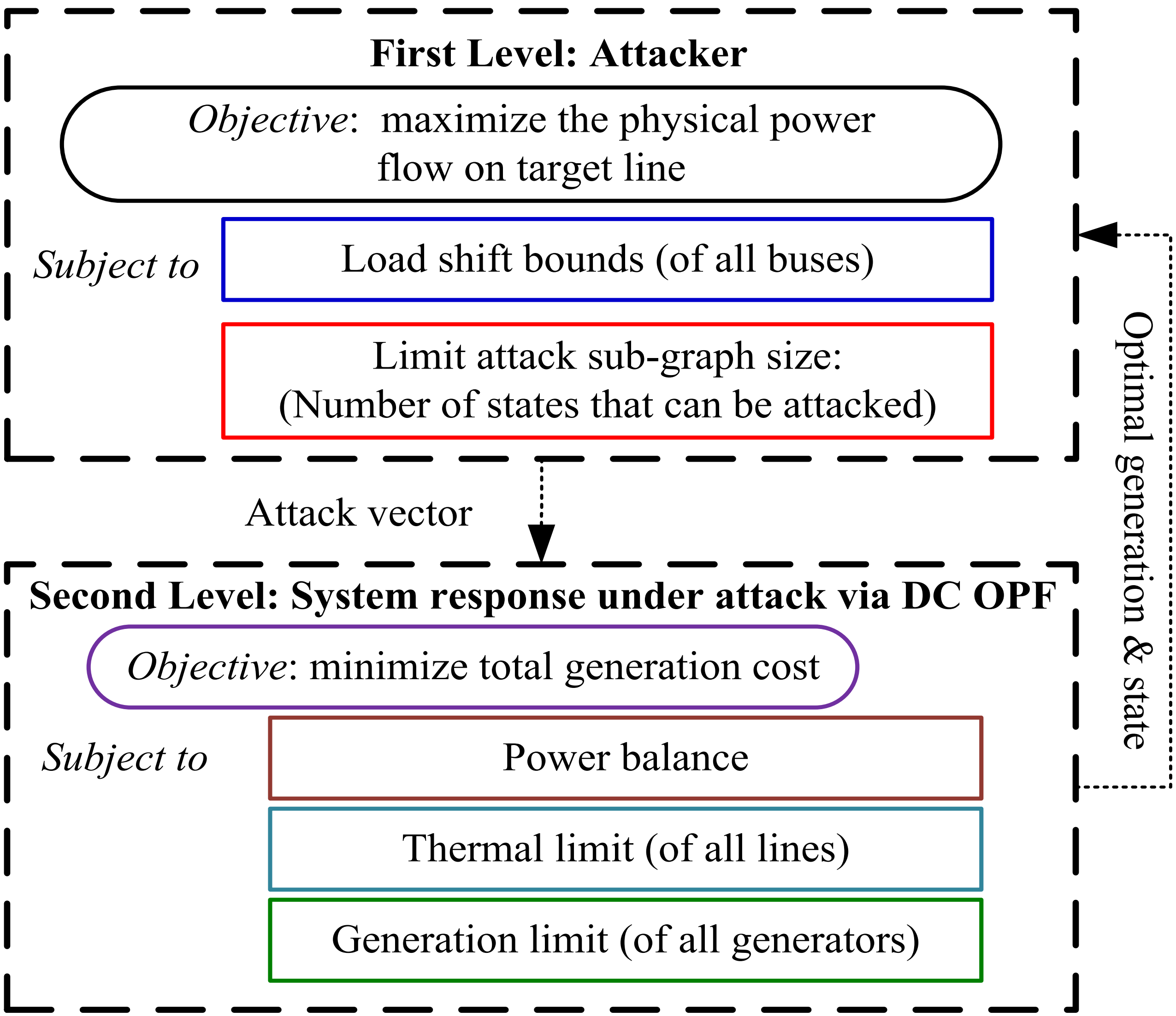
Worst-case Line Overflow Attacks



- Pick a target line
- Change measurements to maximize the power flow on target line after re-dispatch
- With limited attack size
- With limited load shift

How to find such an attack?

Optimization for Worst-case Attacks



Optimization for Worst-case Attacks

One level mixed-integer linear program (MILP)

Objective: maximize the physical power flow on target line

Subject to

Load shift bounds (of all buses)

Limit attack sub-graph size:
(Number of states that can be attacked)

Karush-Kuhn-Tucker (KKT) conditions of the second level DCOPF problem

$$\|c\|_0 \le N_0 \xrightarrow{\text{Relaxed}} \|c\|_1 \le N_0 \rightarrow c \le s, -c \le s, \sum s \le N_1$$

Optimization for Worst-case Attacks

One level mixed-integer linear program (MILP)

Objective: maximize the physical power flow on target line

Subject to

Load shift bounds (of all buses)

Limit attack sub-graph size:
(Number of states that can be attacked)

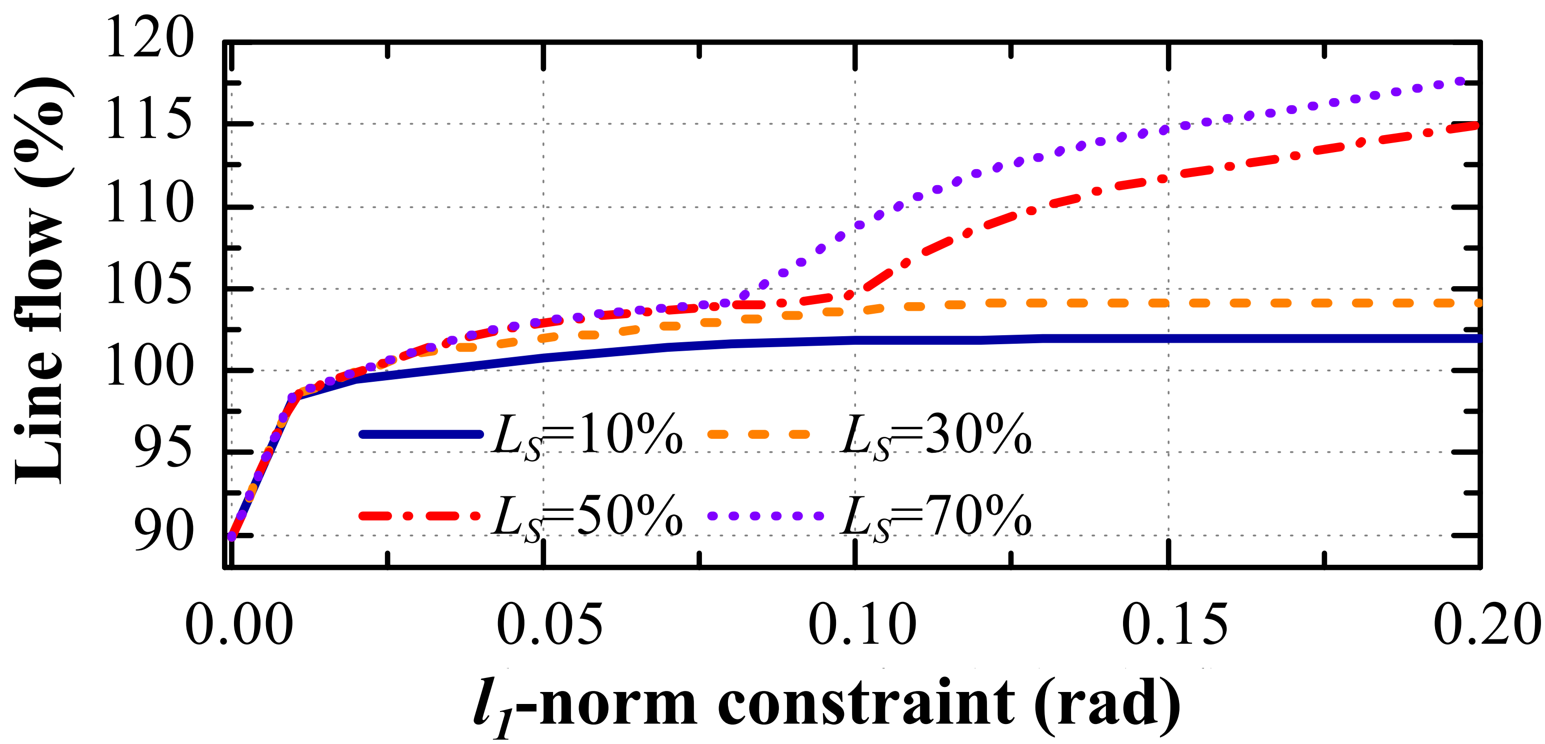
Karush-Kuhn-Tucker (KKT) conditions of the second level DCOPF problem

Complementary slackness condition for $x \leq x^{\max}$, dual variable α

$$\alpha(x - x^{\max}) = \mathbf{0} \rightarrow \begin{cases} \alpha \leq M\delta_{\alpha} \\ x^{\max} - x \leq M(1 - \delta_{\alpha}) \\ \delta_{\alpha} \in \{0,1\} \end{cases}$$

Numerical Results

- Test on IEEE 24-bus RTS system

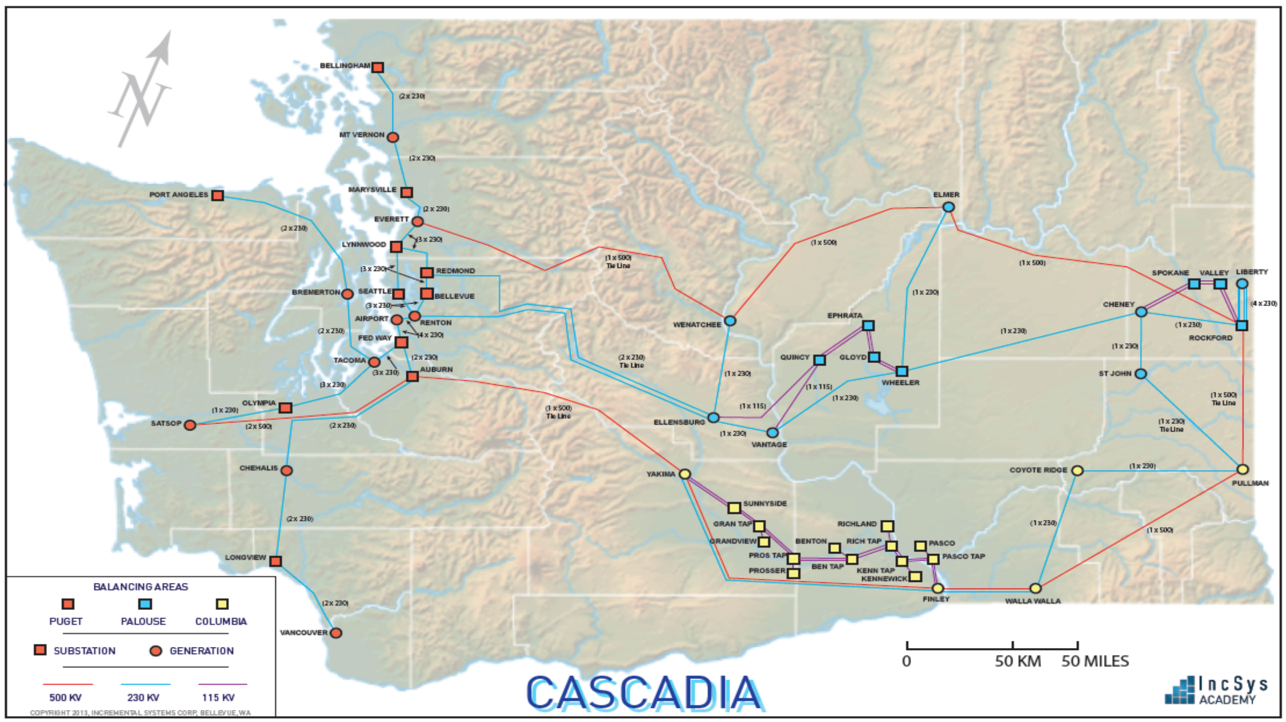


Java-based High-fidelity EMS Simulation Platform

Joint work with IncSys and Powerdata

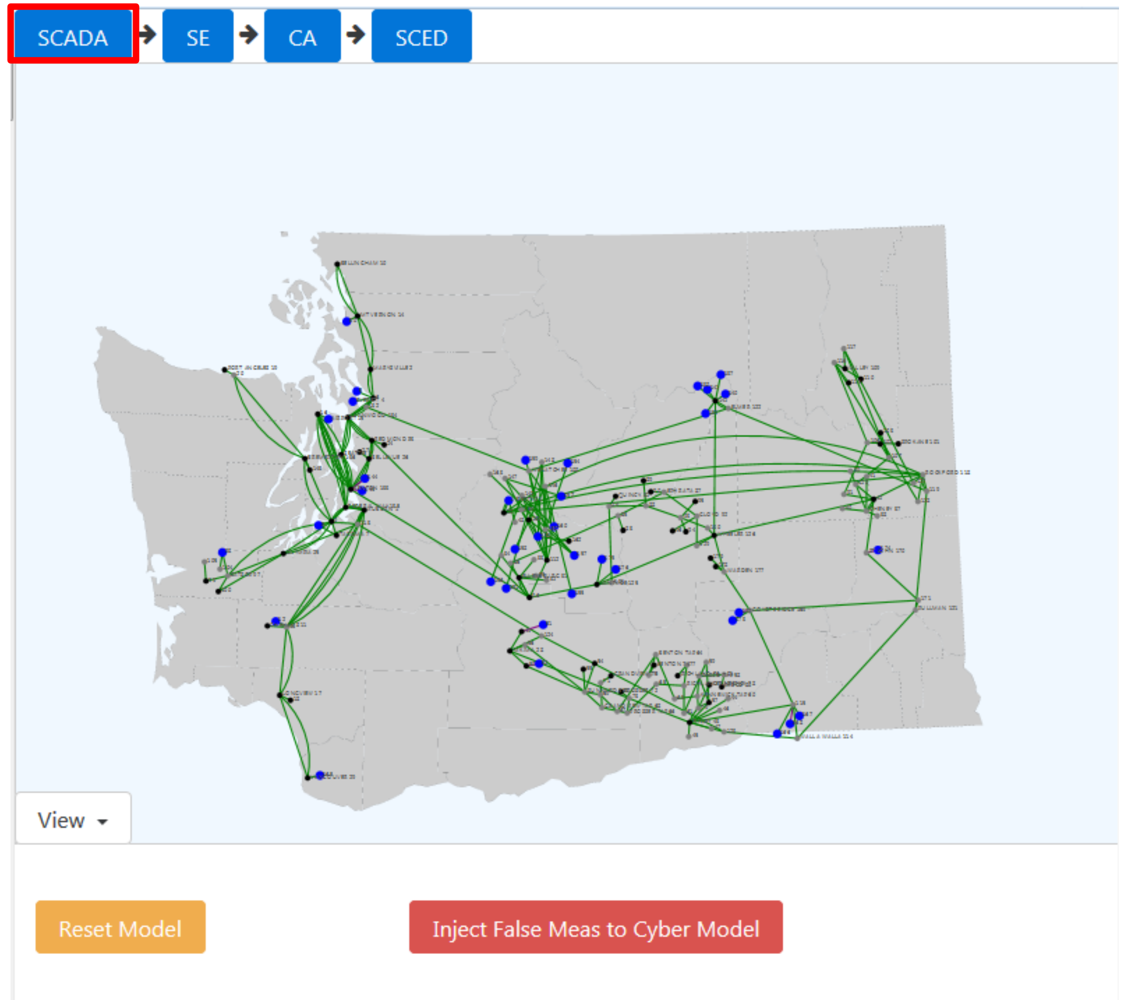
Test System - Cascadia System

- 179 buses, 121 lines, 125 transformers, 37 generators and 72 loads
- Synthetic model of the power grid of Washington state



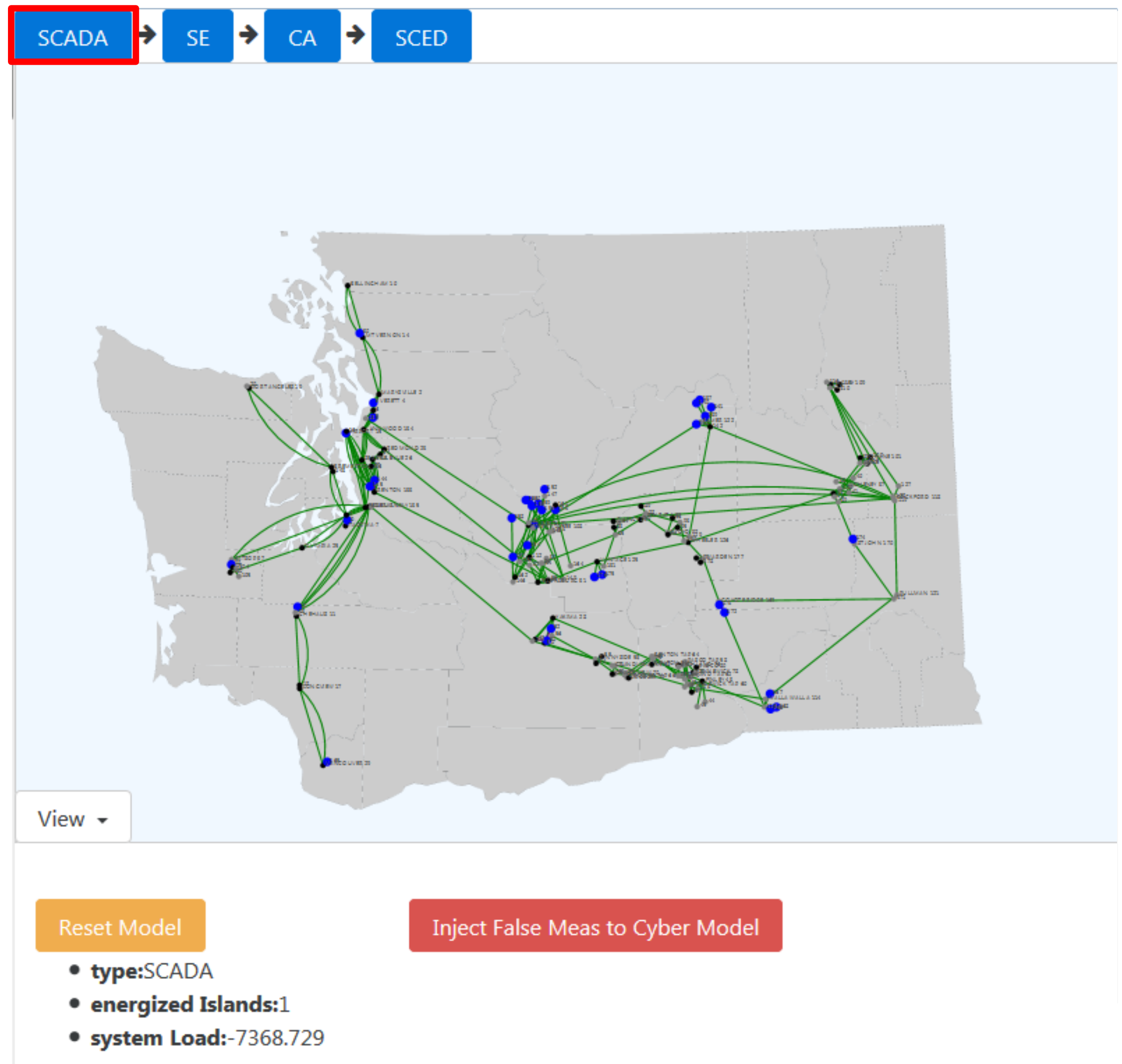
EMS Platform

- SCADA:



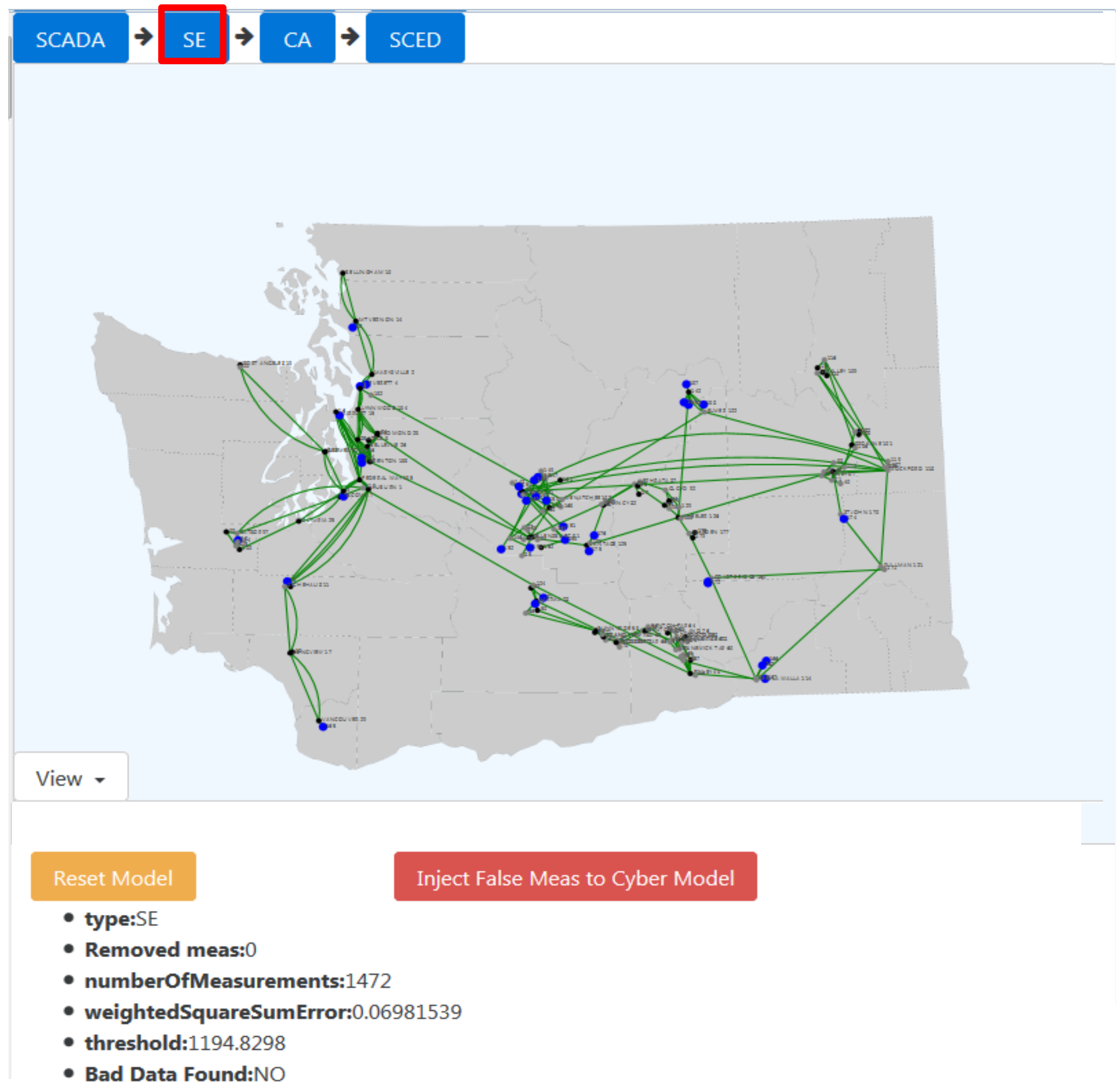
EMS Platform

- SCADA:
  - Collect measurements



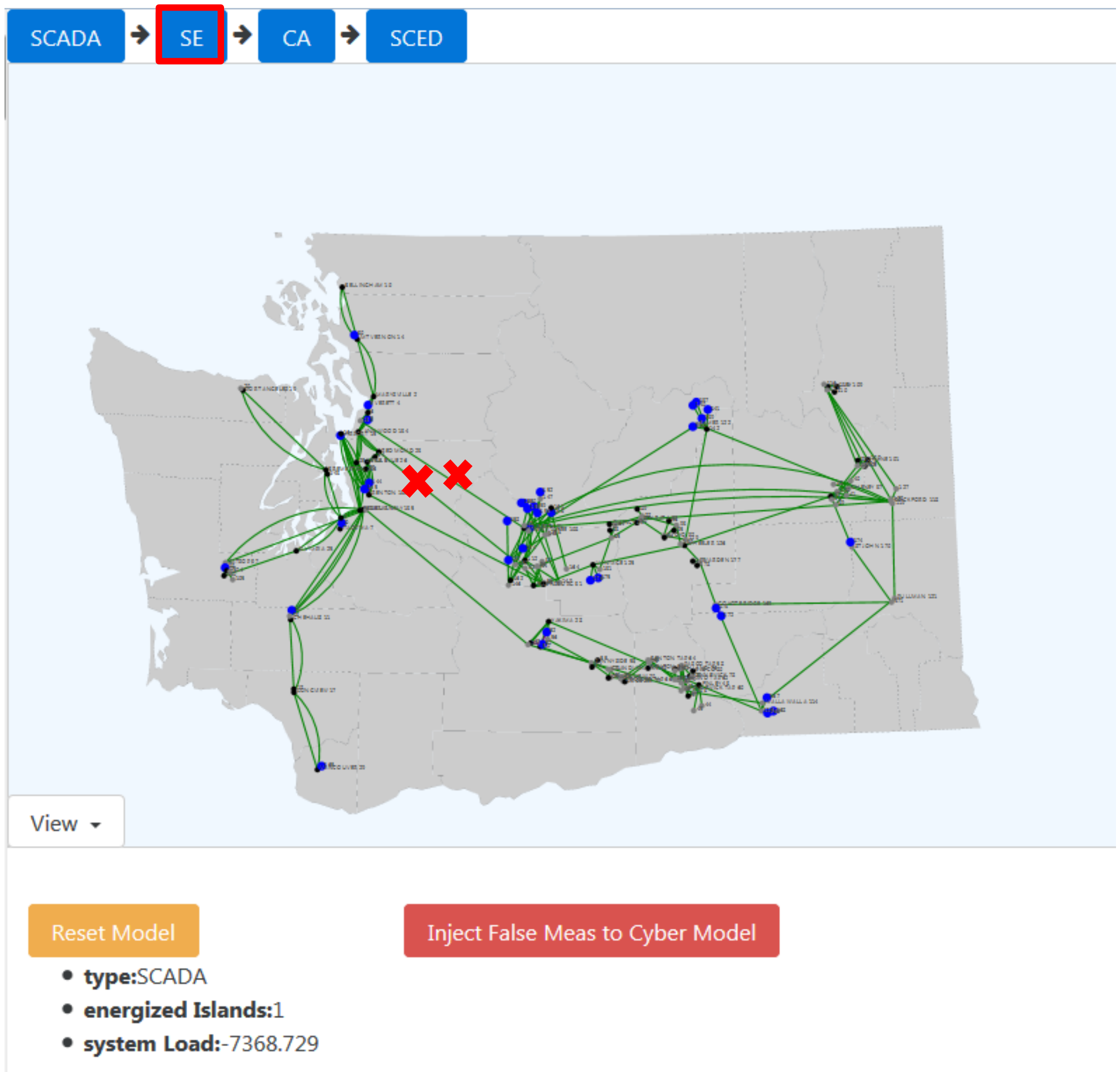
EMS Platform

- SCADA:
  - Collect measurements
- AC State Estimator:
  - Estimate states utilizing measurements



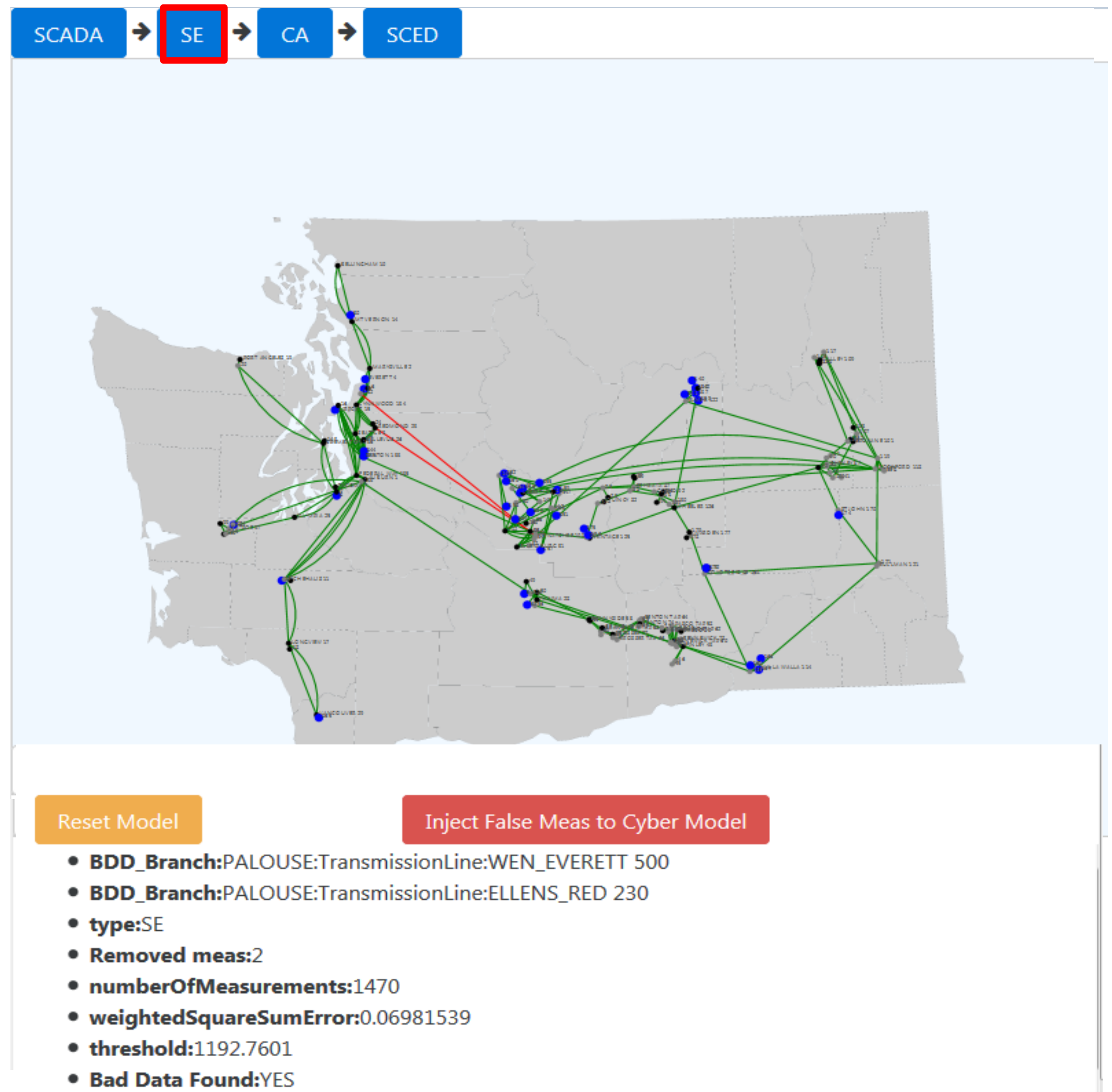
EMS Platform

- SCADA:
  - Collect measurements
- AC State Estimator:
  - Estimate states utilizing measurements
  - Filter bad data



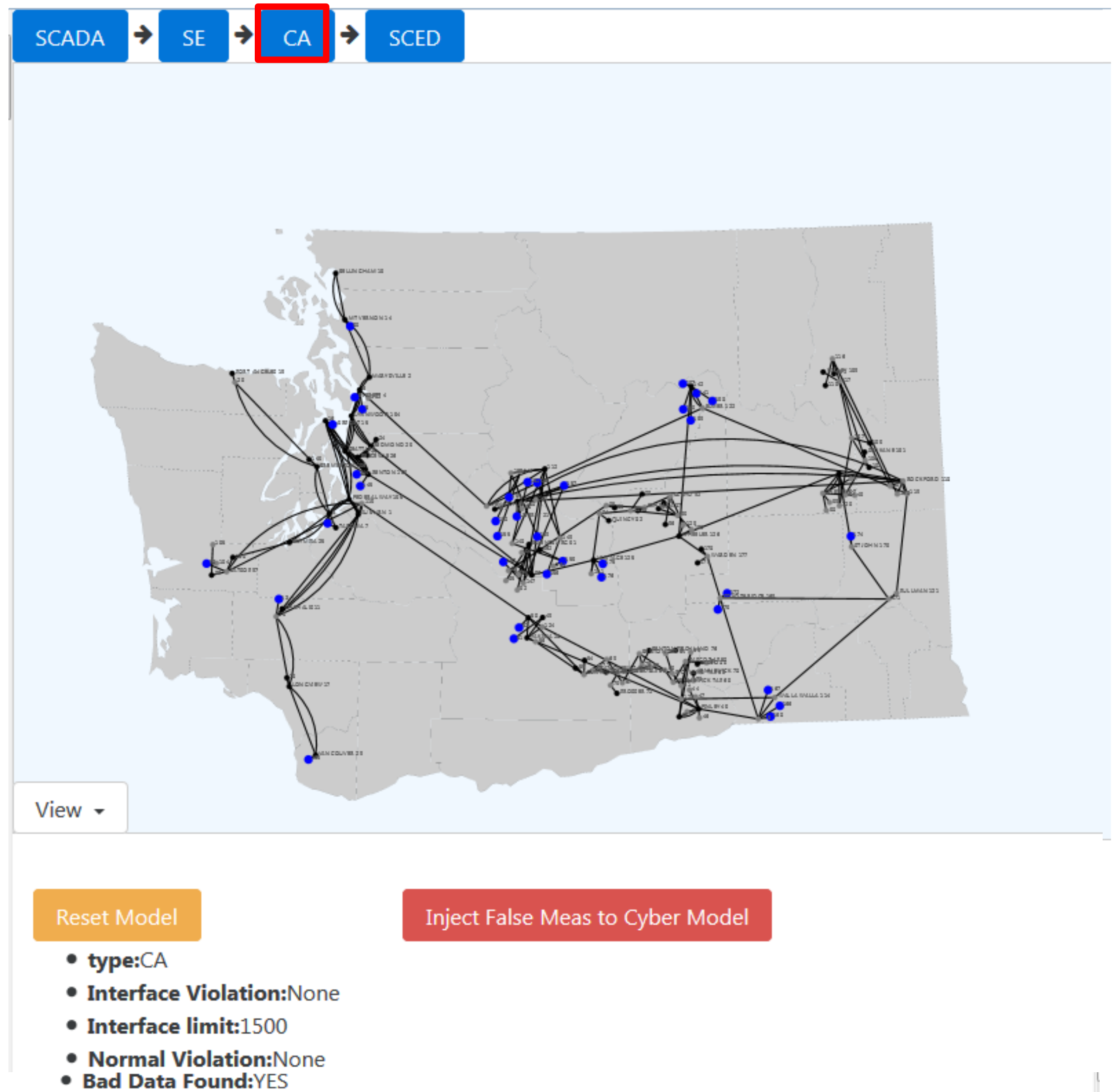
EMS Platform

- SCADA:
  - Collect measurements
- AC State Estimator:
  - Estimate states utilizing measurements
  - Filter bad data



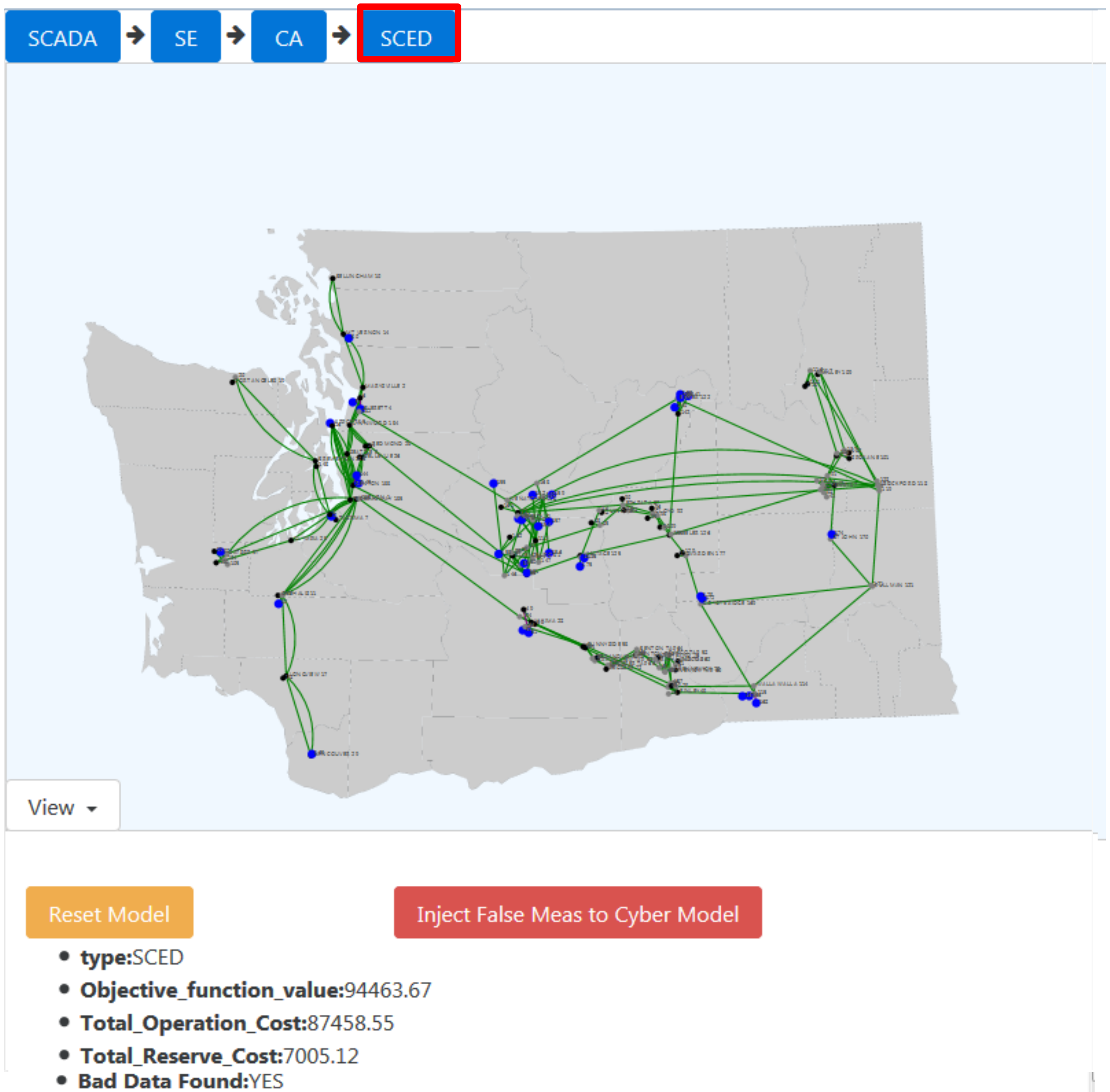
EMS Platform

- SCADA:
  - Collect measurements
- AC State Estimator:
  - Estimate states utilizing measurements
  - Filter bad data
- Contingency Analysis
  - Perform N-1 line outage contingency analysis
  - List critical line and interface violations
  - Add security constraints to monitor critical lines in security constraint economic dispatch (SCED)



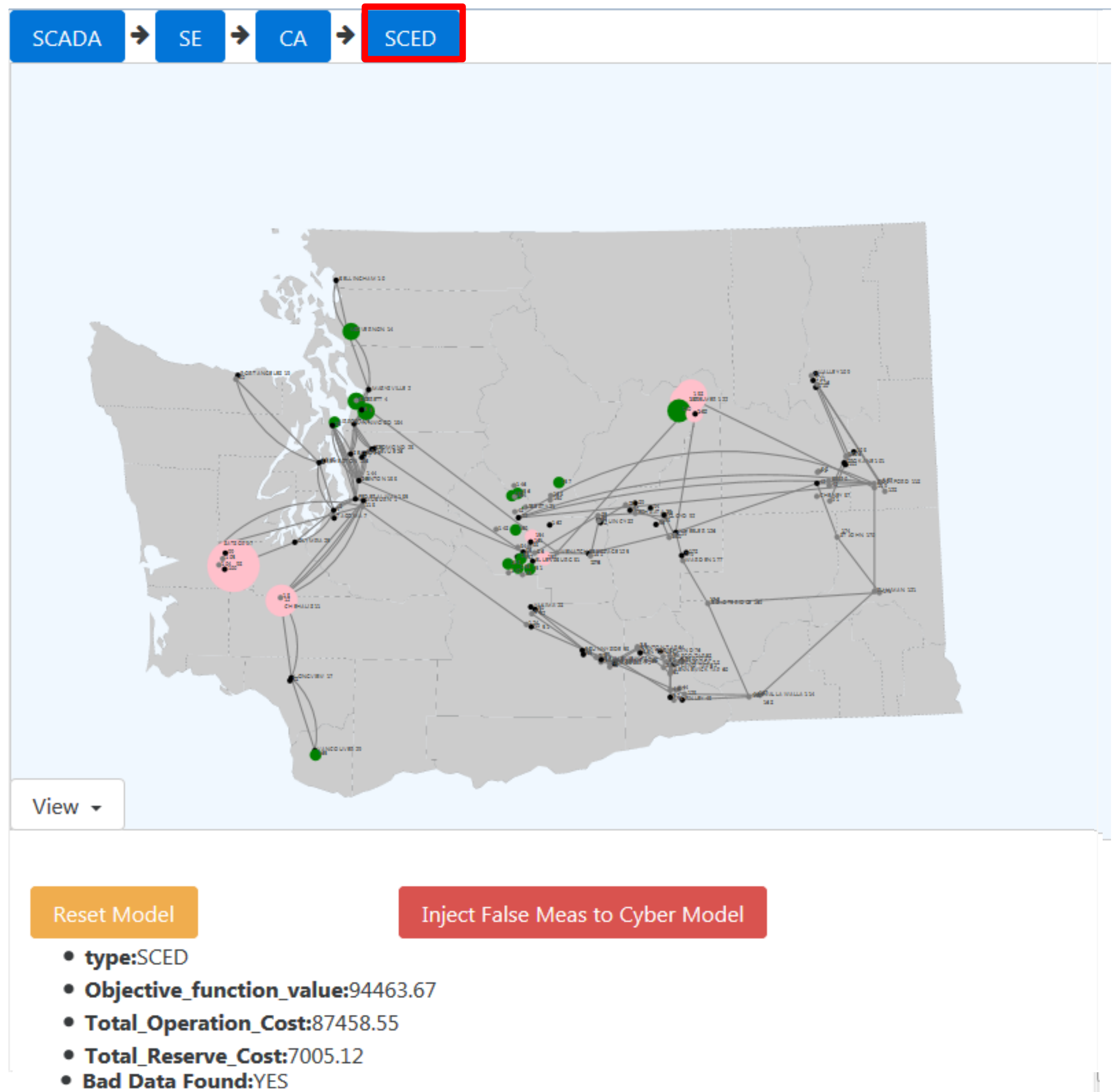
EMS Platform

- SCADA:
  - Collect measurements
- AC State Estimator:
  - Estimate states utilizing measurements
  - Filter bad data
- Contingency Analysis
  - Perform N-1 line outage contingency analysis
  - List critical line and interface violations
  - Add security constraints to monitor critical lines in security constraint economic dispatch (SCED)
- Security Constrained Economic Dispatch (SCED)



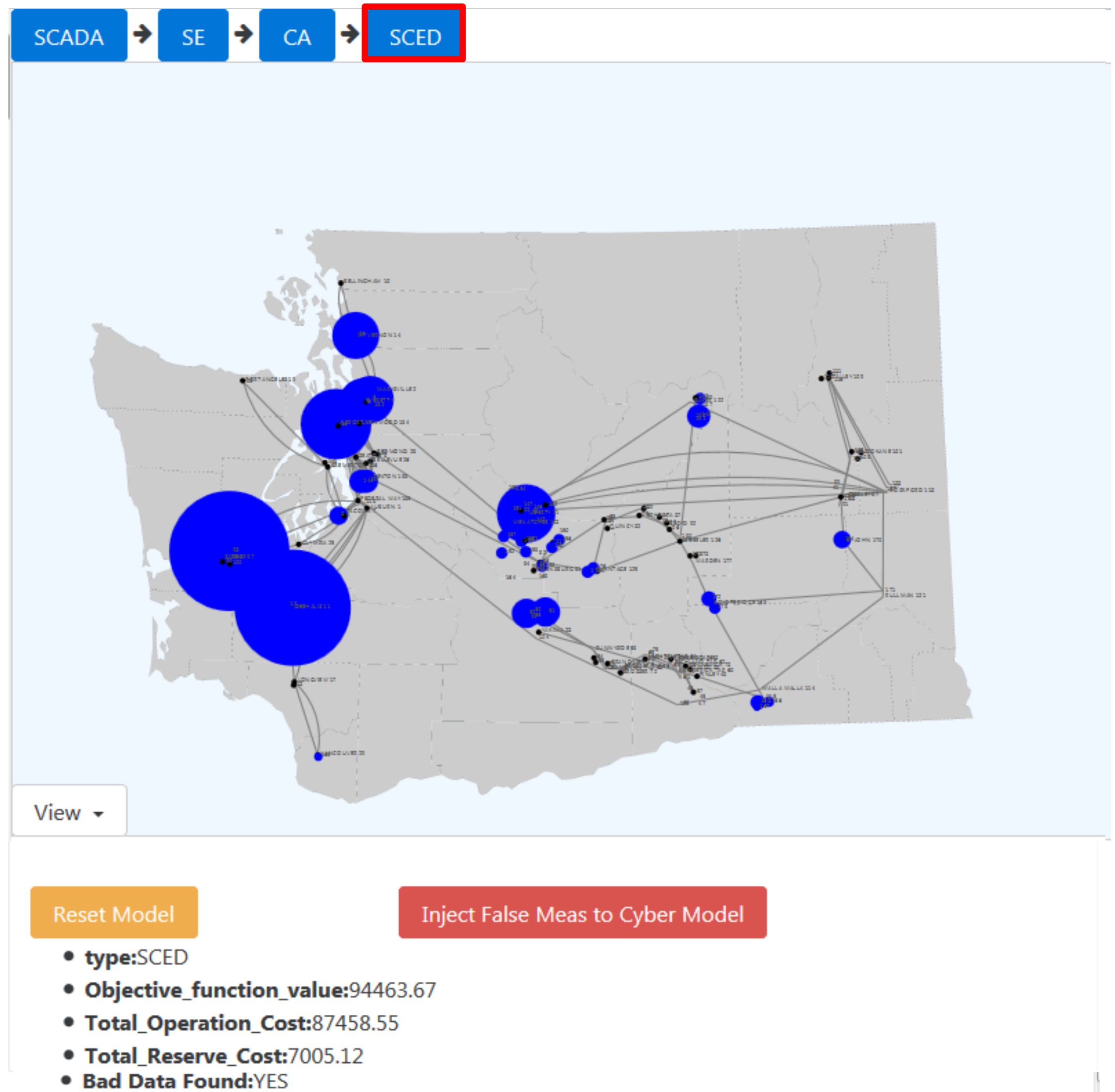
EMS Platform

- SCADA:
  - Collect measurements
- AC State Estimator:
  - Estimate states utilizing measurements
  - Filter bad data
- Contingency Analysis
  - Perform N-1 line outage contingency analysis
  - List critical line and interface violations
  - Add security constraints to monitor critical lines in security constraint economic dispatch (SCED)
- Security Constrained Economic Dispatch (SCED)
  - Perform economic dispatch to minimize operation costs under security constraints



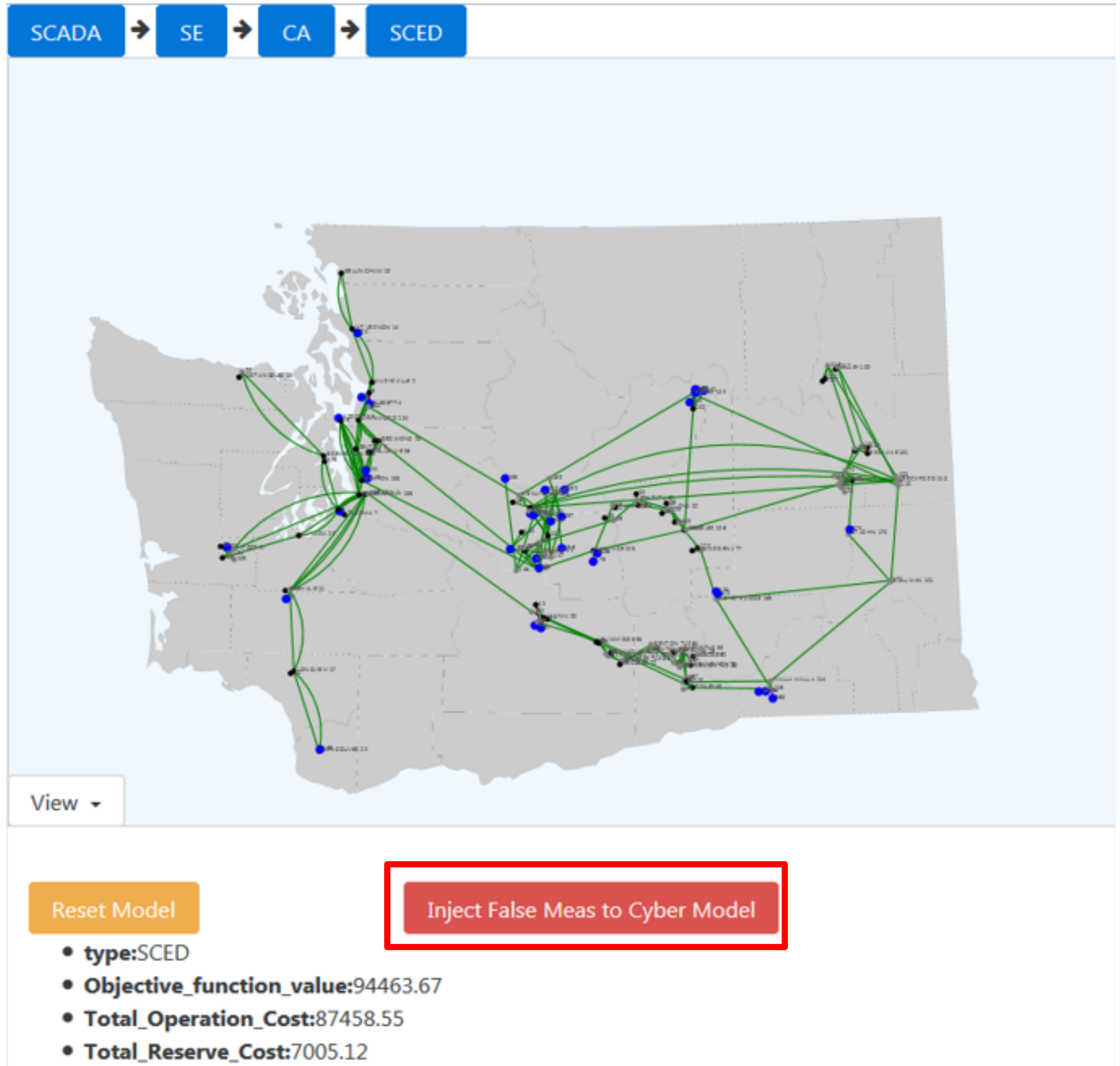
EMS Platform

- SCADA:
  - Collect measurements
- AC State Estimator:
  - Estimate states utilizing measurements
  - Filter bad data
- Contingency Analysis
  - Perform N-1 line outage contingency analysis
  - List critical line and interface violations
  - Add security constraints to monitor critical lines in security constraint economic dispatch (SCED)
- Security Constrained Economic Dispatch (SCED)
  - Perform economic dispatch to minimize operation costs under security constraints



FDI Attack

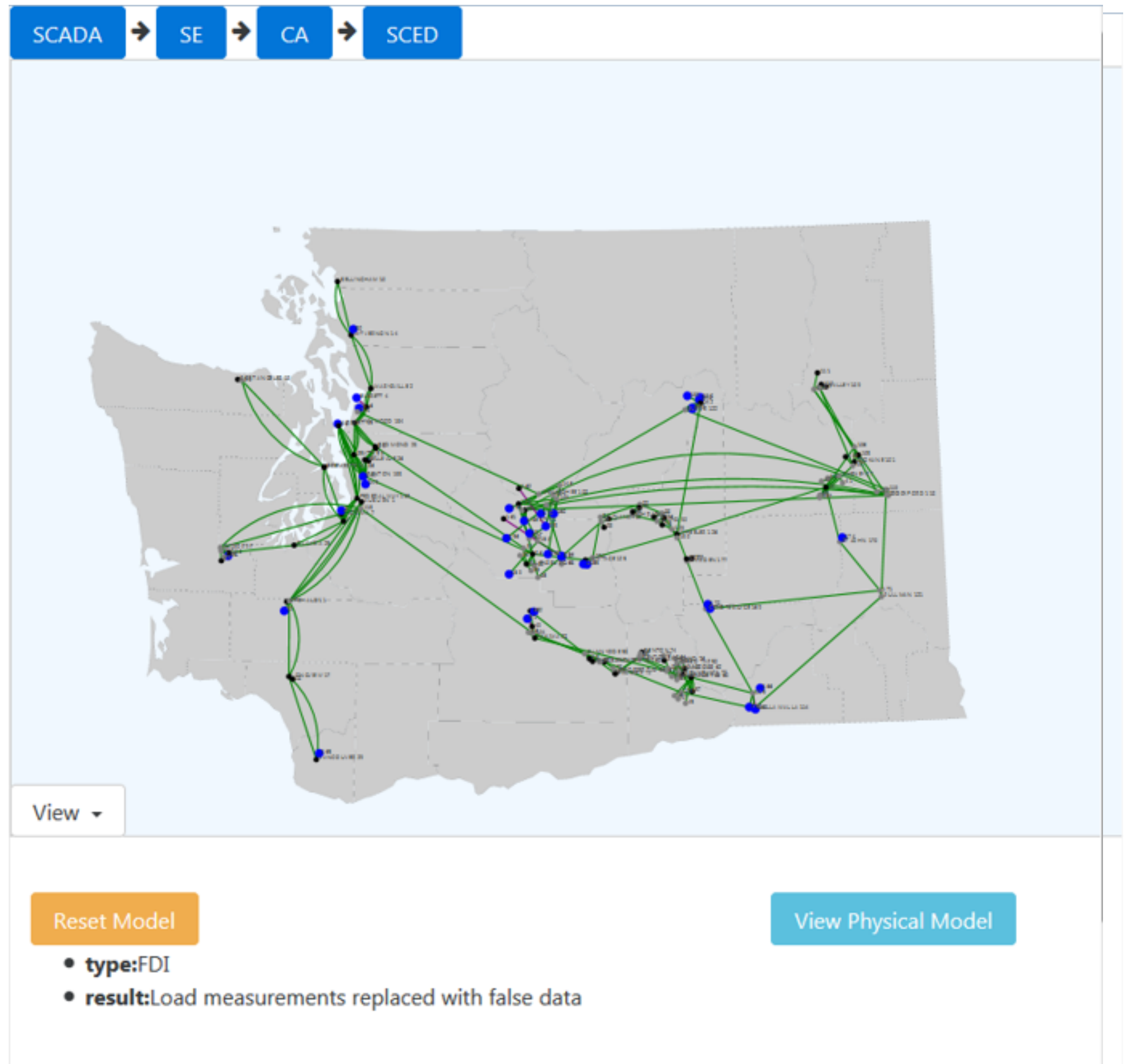
- **Inject false measurements in SCADA**



FDI Attack

- **Inject false measurements in SCADA**

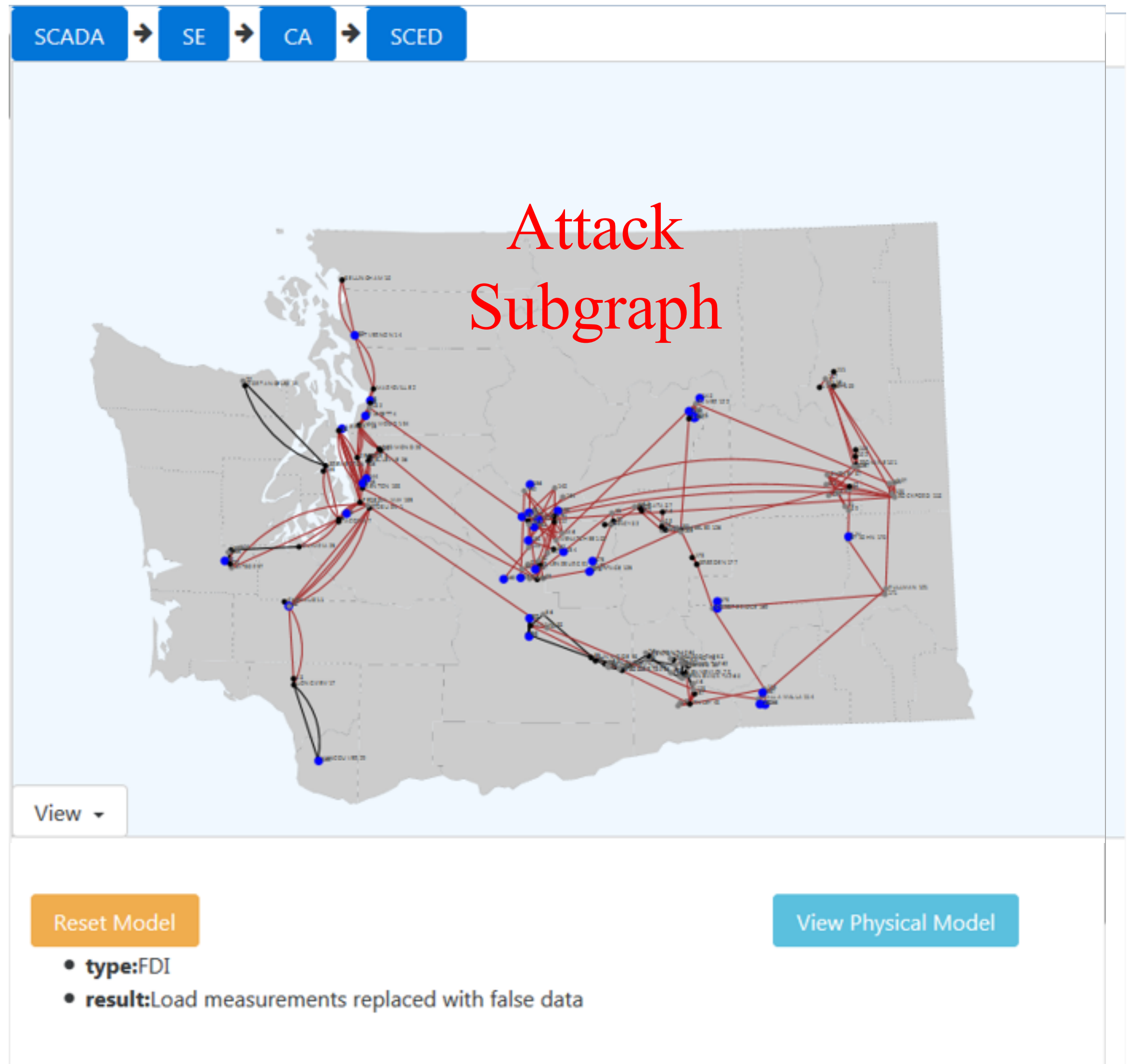
In the cyber system:



FDI Attack

- **Inject false measurements in SCADA**

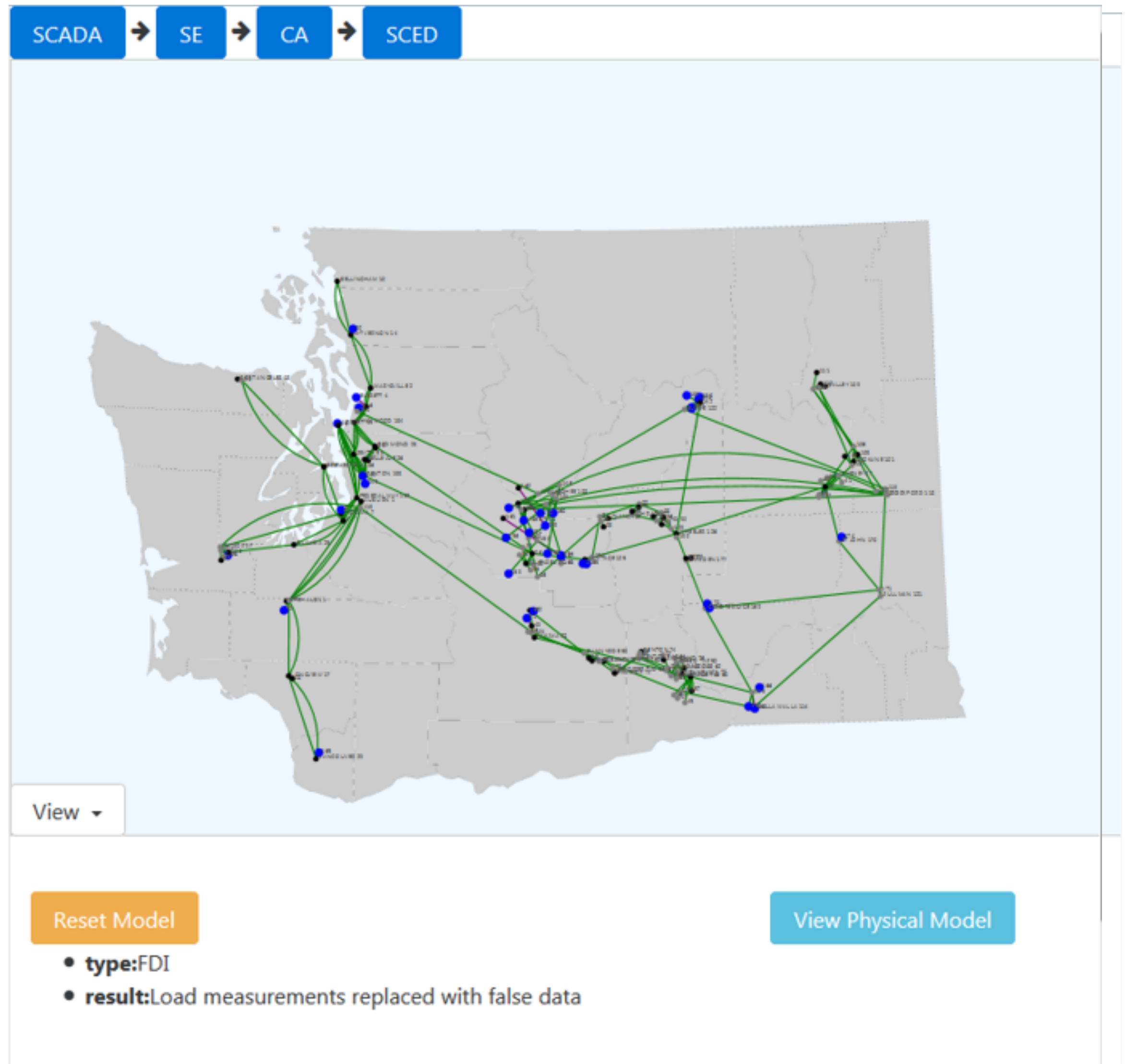
In the cyber system:



FDI Attack

- **Inject false measurements in SCADA**

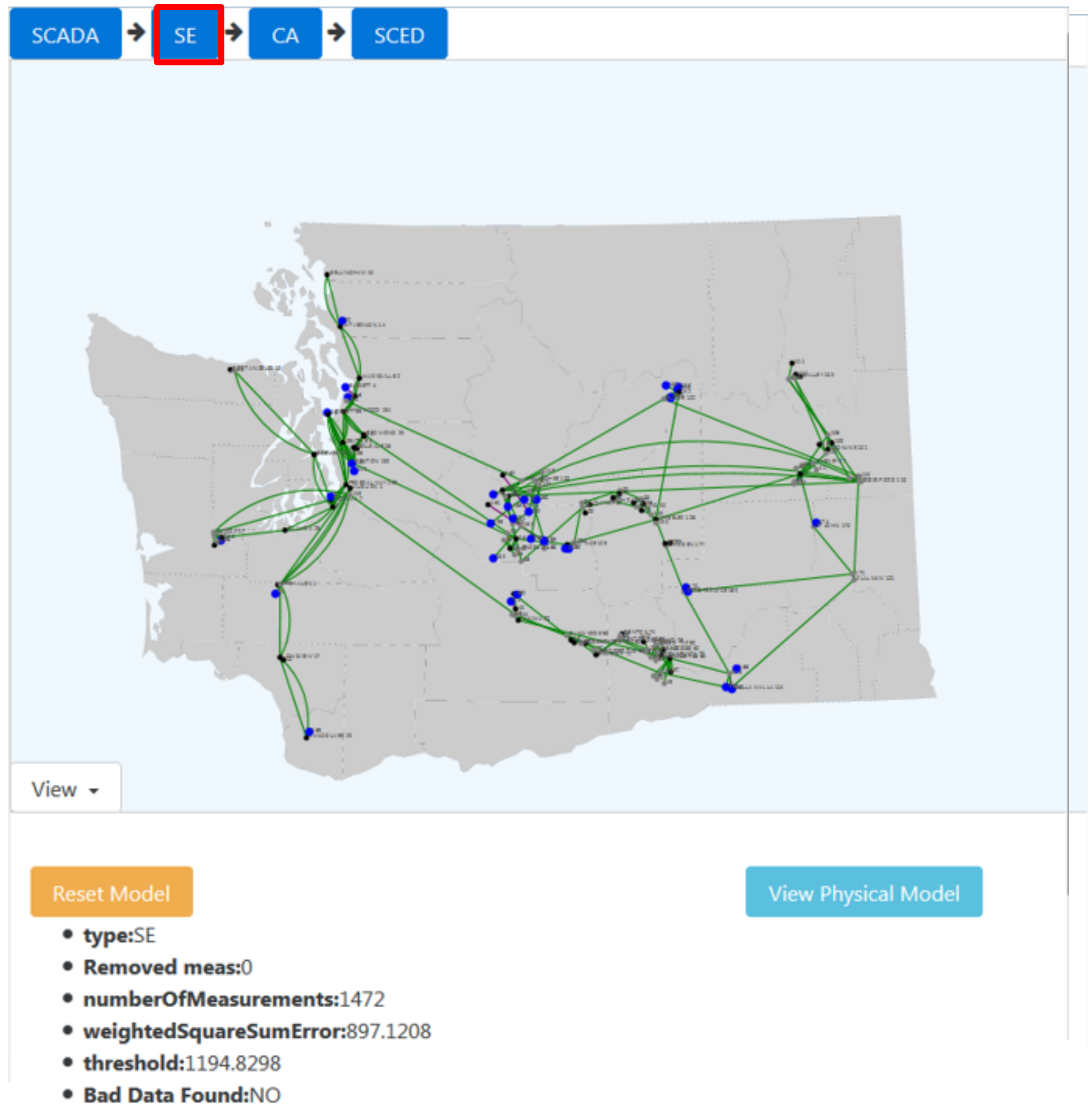
In the cyber system:



FDI Attack

- **Inject false measurements in SCADA**

In the cyber system:

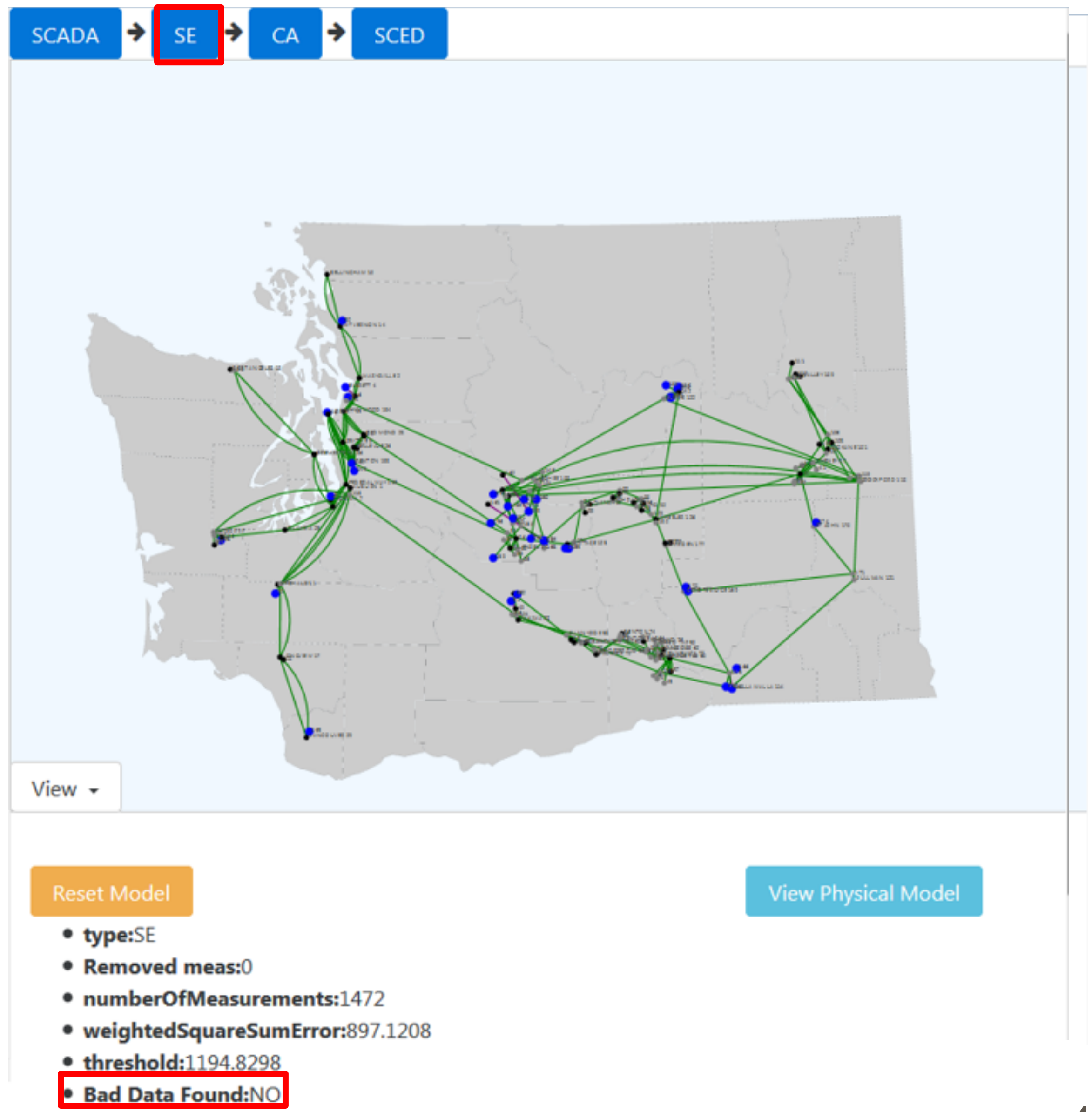


FDI Attack

- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector

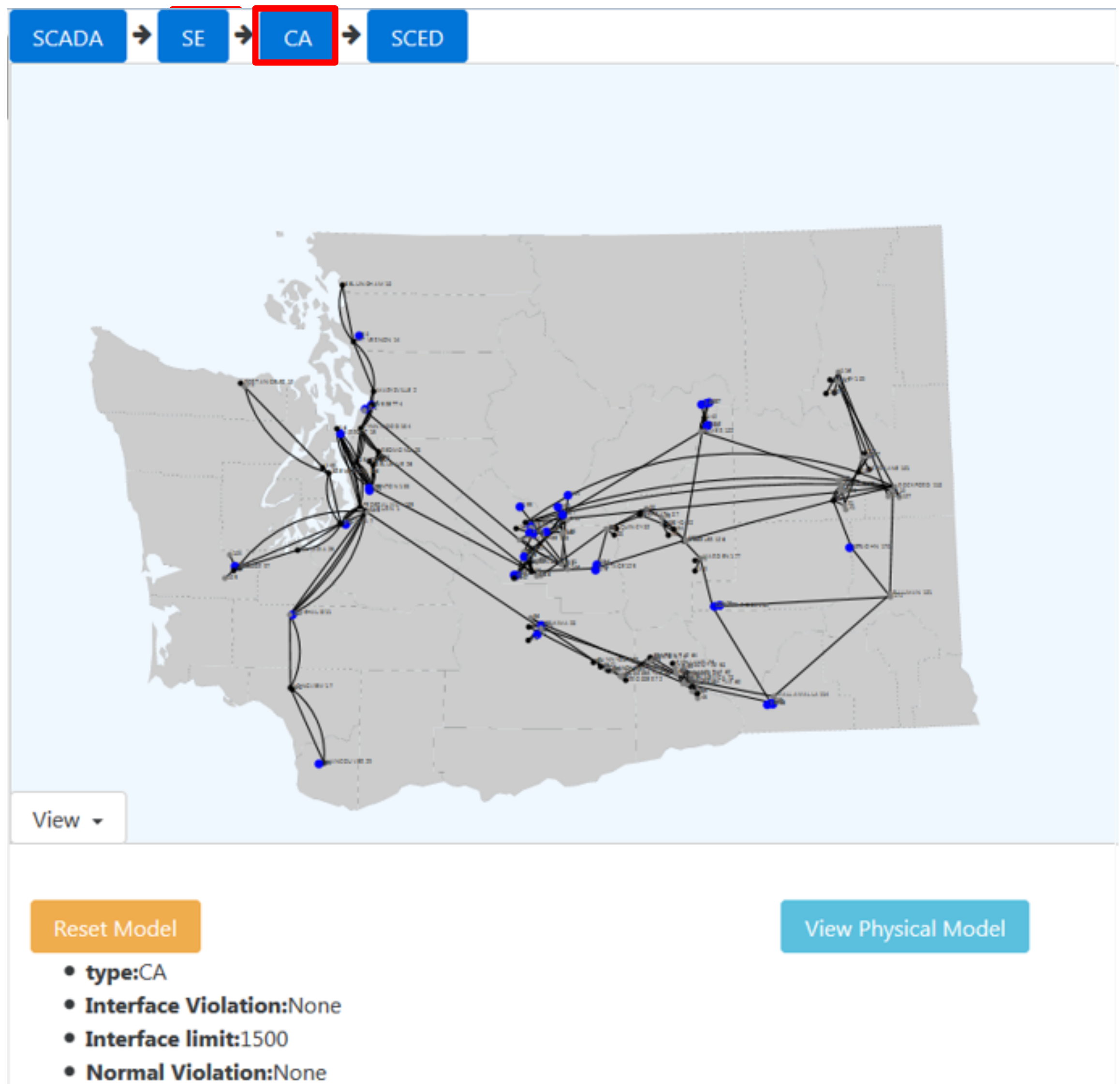


FDI Attack

- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector

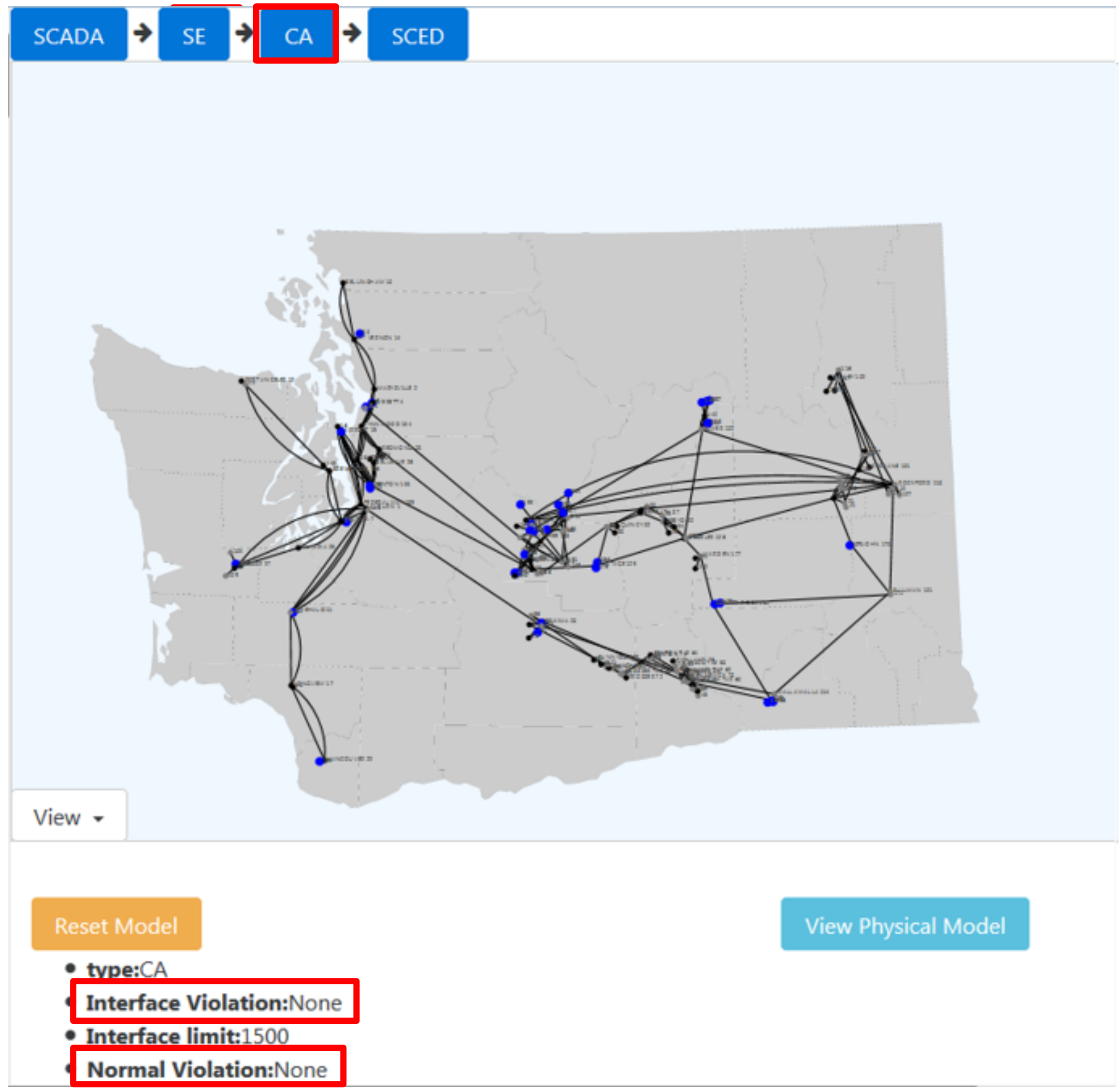


FDI Attack

- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector
- No post-contingency violation is found!
- No security constraints are added in SCED!!

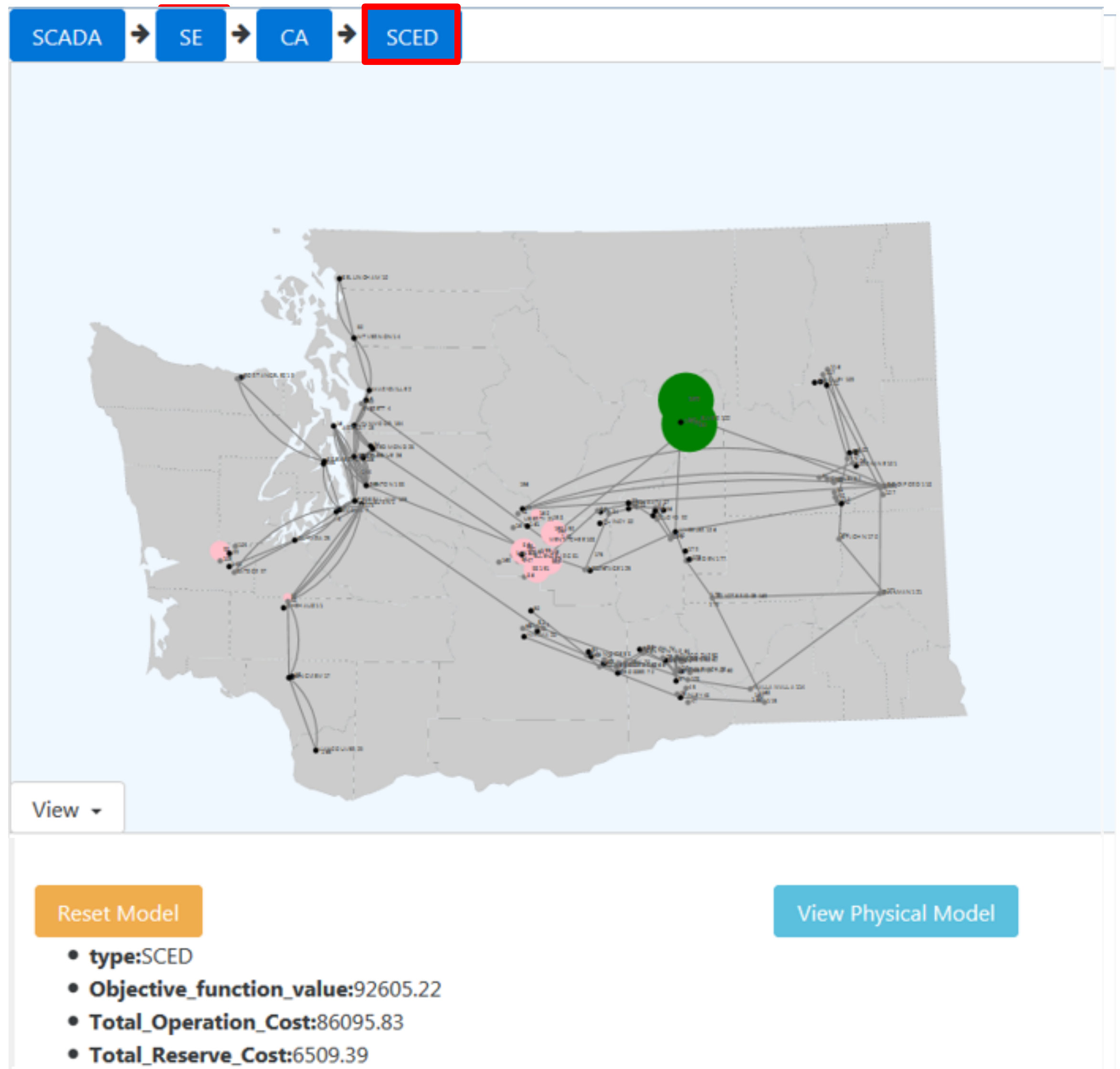


FDI Attack

- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector
- No post-contingency violation is found!
- No security constraints are added in SCED!!
- Several generators re-dispatch due to the false load



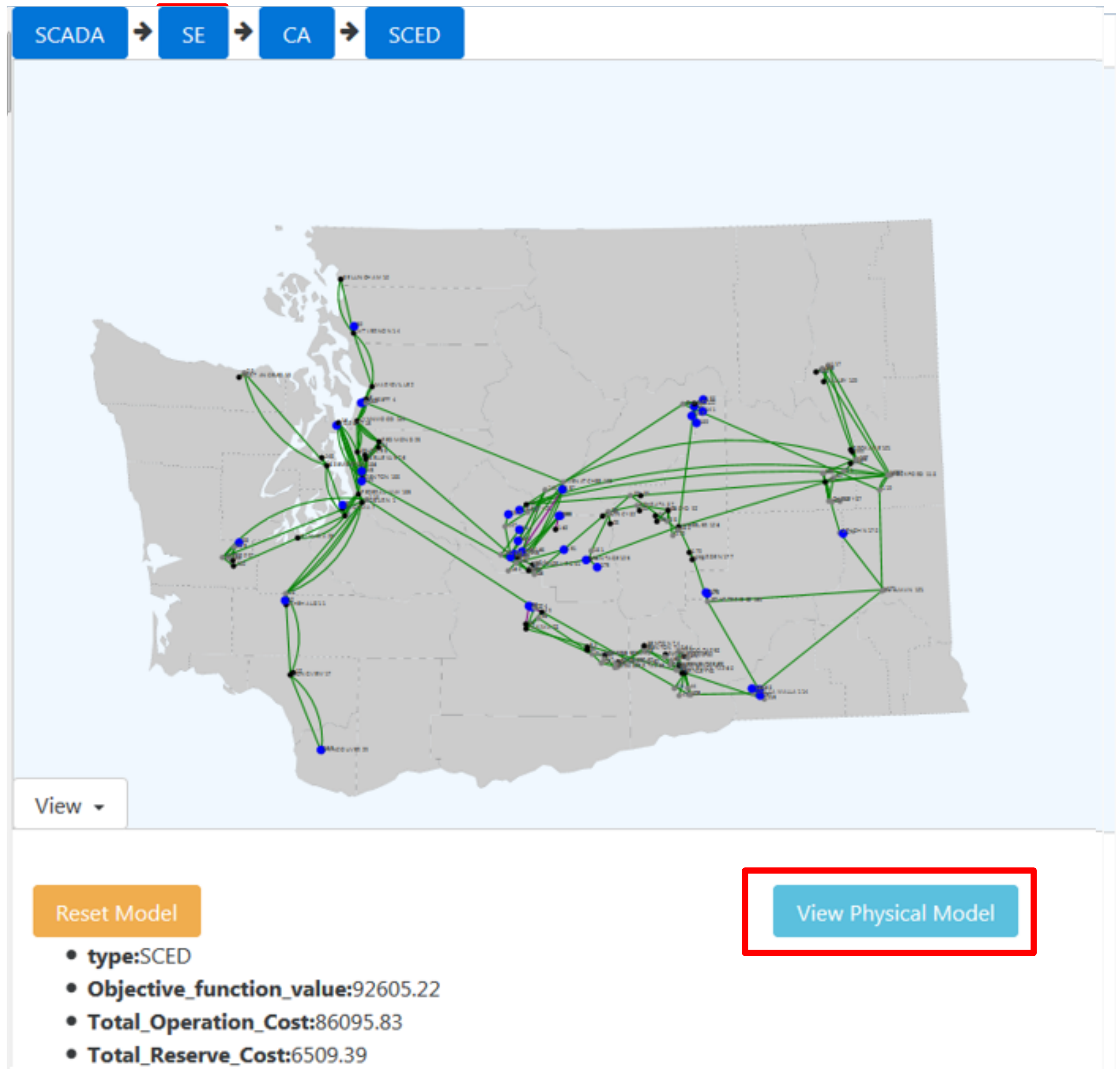
FDI Attack

- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector
- No post-contingency violation is found!
- No security constraints are added in SCED!!
- Several generators re-dispatch due to the false load

In the physical system:



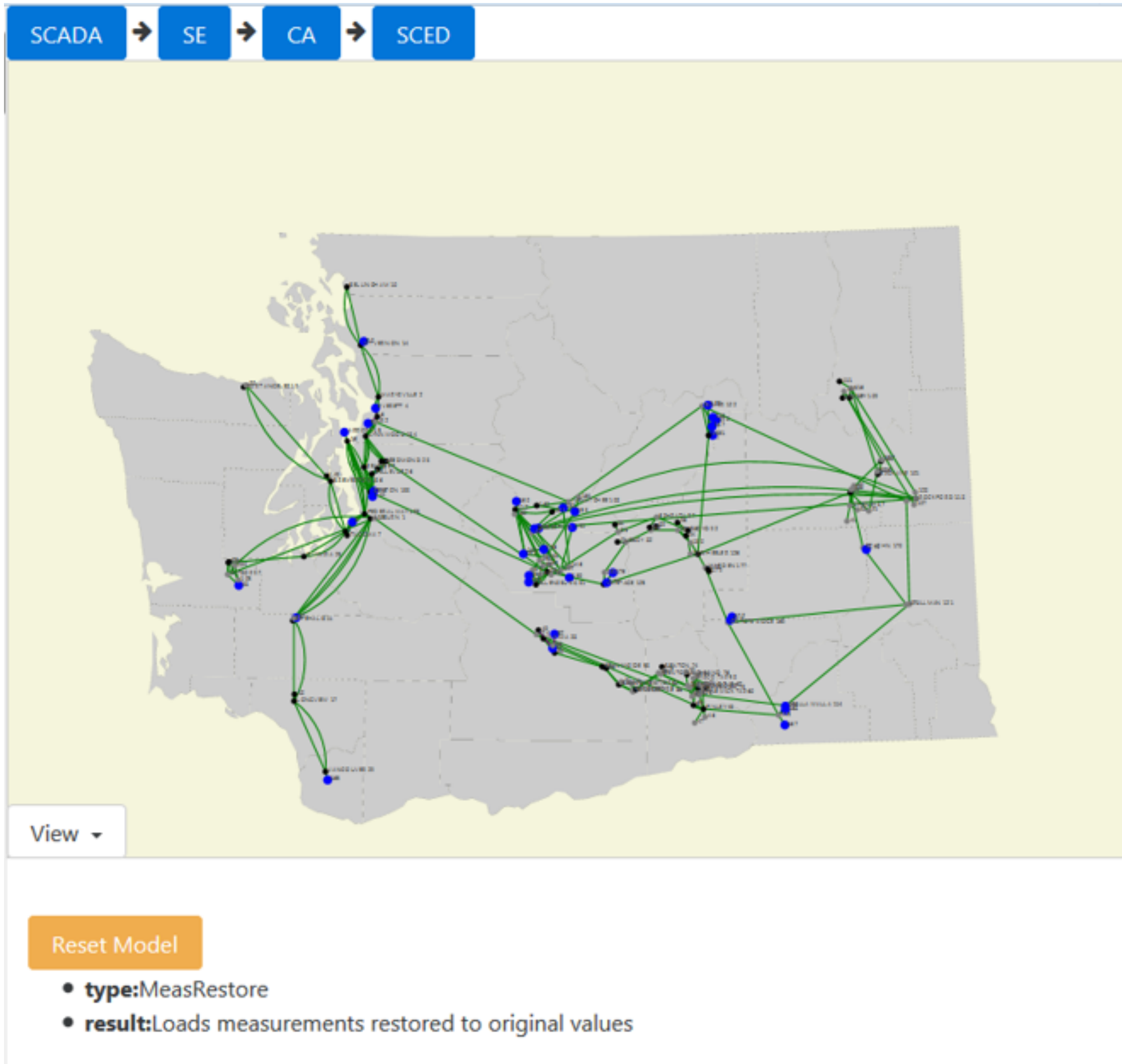
FDI Attack

- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector
- No post-contingency violation is found!
- No security constraints are added in SCED!!
- Several generators re-dispatch due to the false load

In the physical system:



FDI Attack

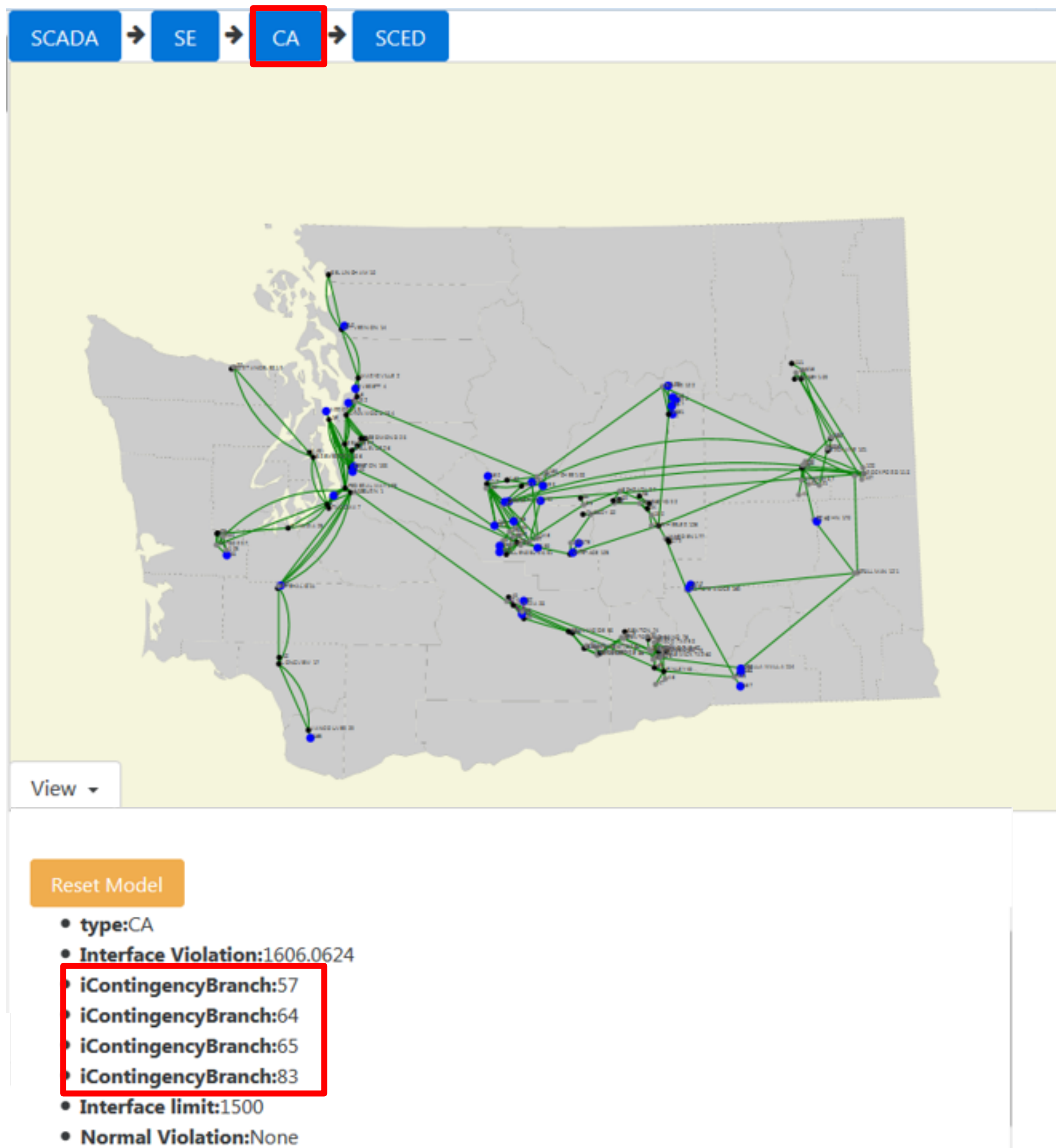
- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector
- No post-contingency violation is found!
- No security constraints are added in SCED!!
- Several generators re-dispatch due to the false load

In the physical system:

- Four post-contingency interface violations are unobservable in the cyber system!



FDI Attack

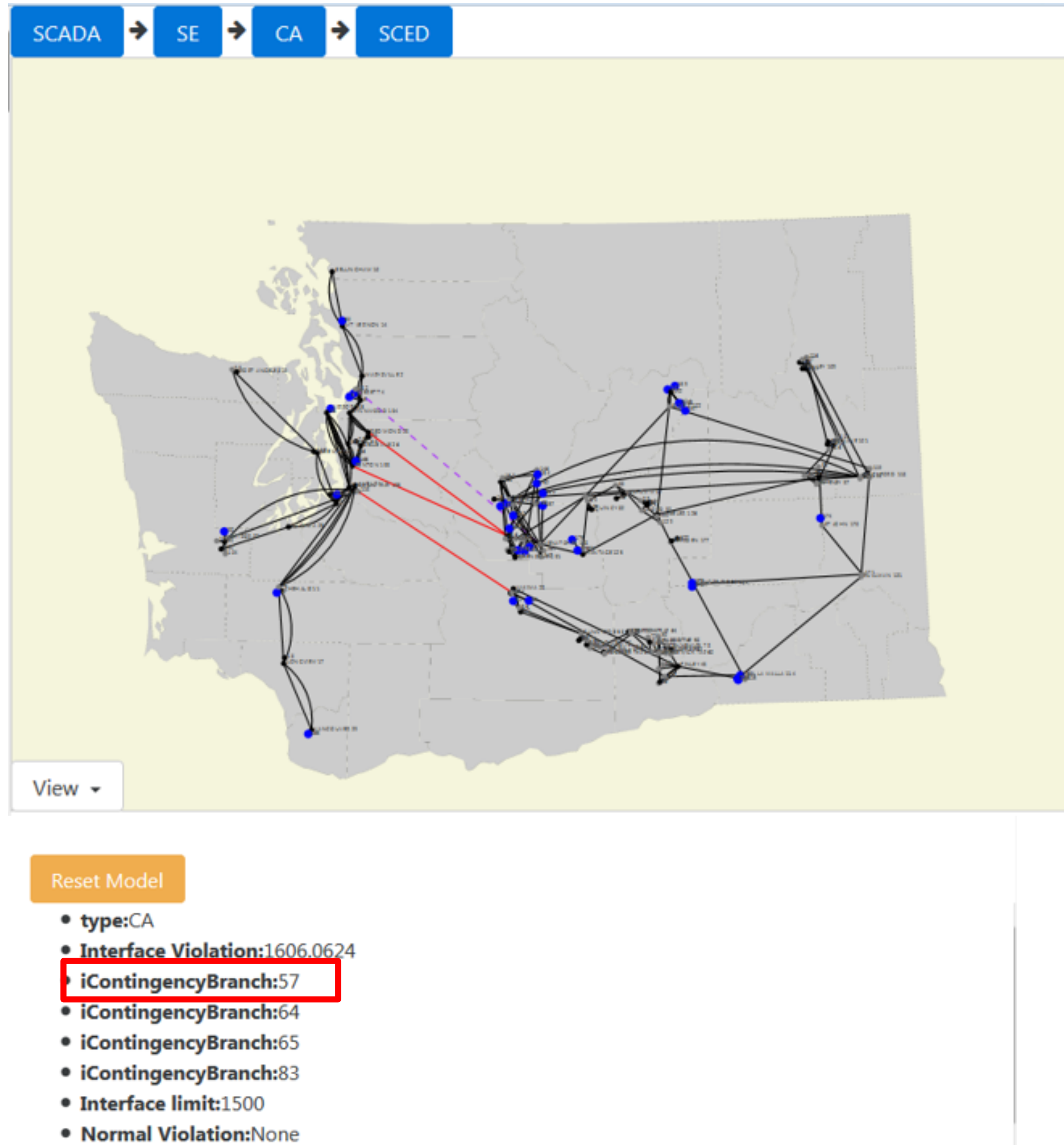
- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector
- No post-contingency violation is found!
- No security constraints are added in SCED!!
- Several generators re-dispatch due to the false load

In the physical system:

- Four post-contingency interface violations are unobservable in the cyber system!



FDI Attack

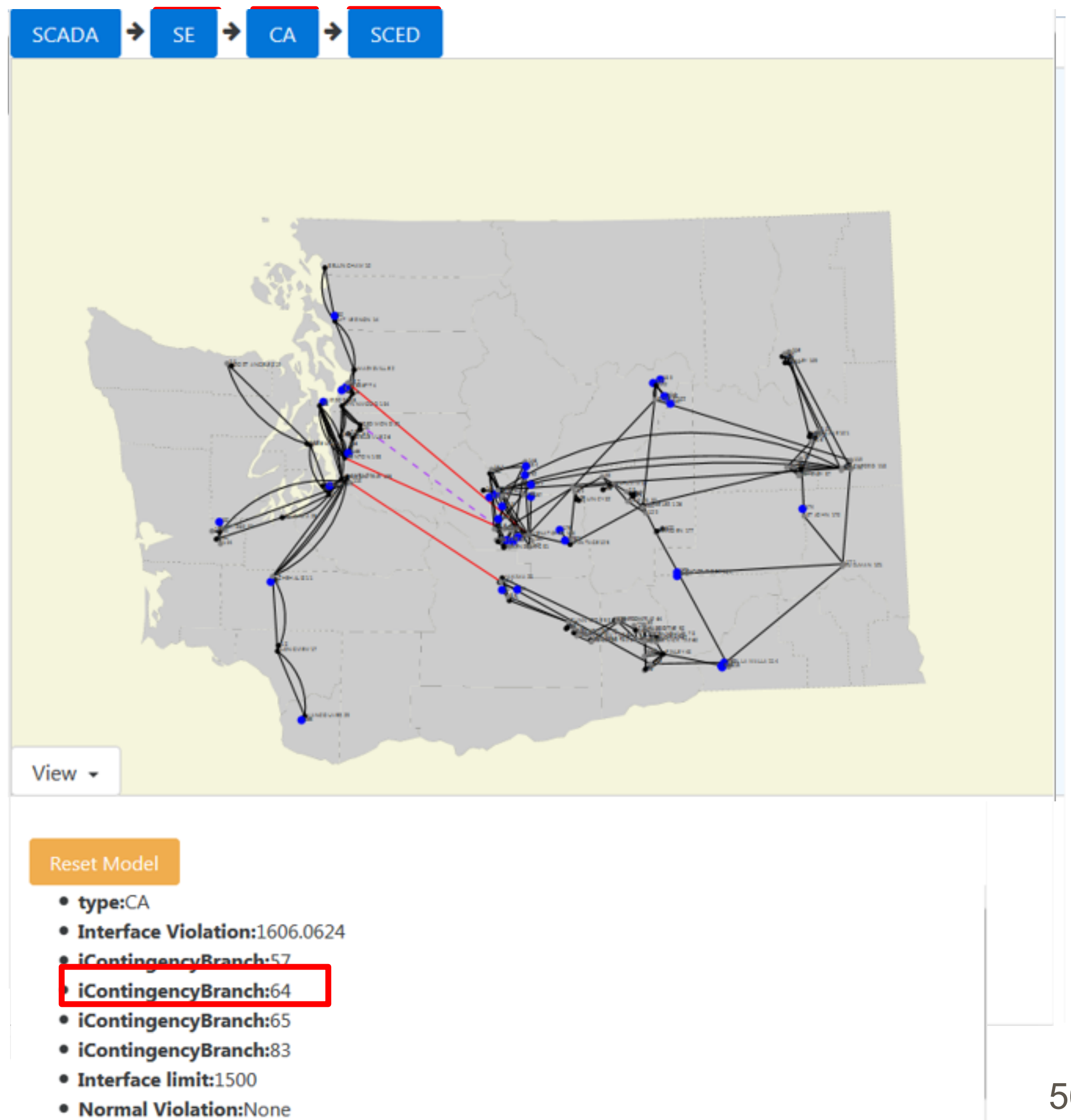
- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector
- No post-contingency violation is found!
- No security constraints are added in SCED!!
- Several generators re-dispatch due to the false load

In the physical system:

- Four post-contingency interface violations are unobservable in the cyber system!



FDI Attack

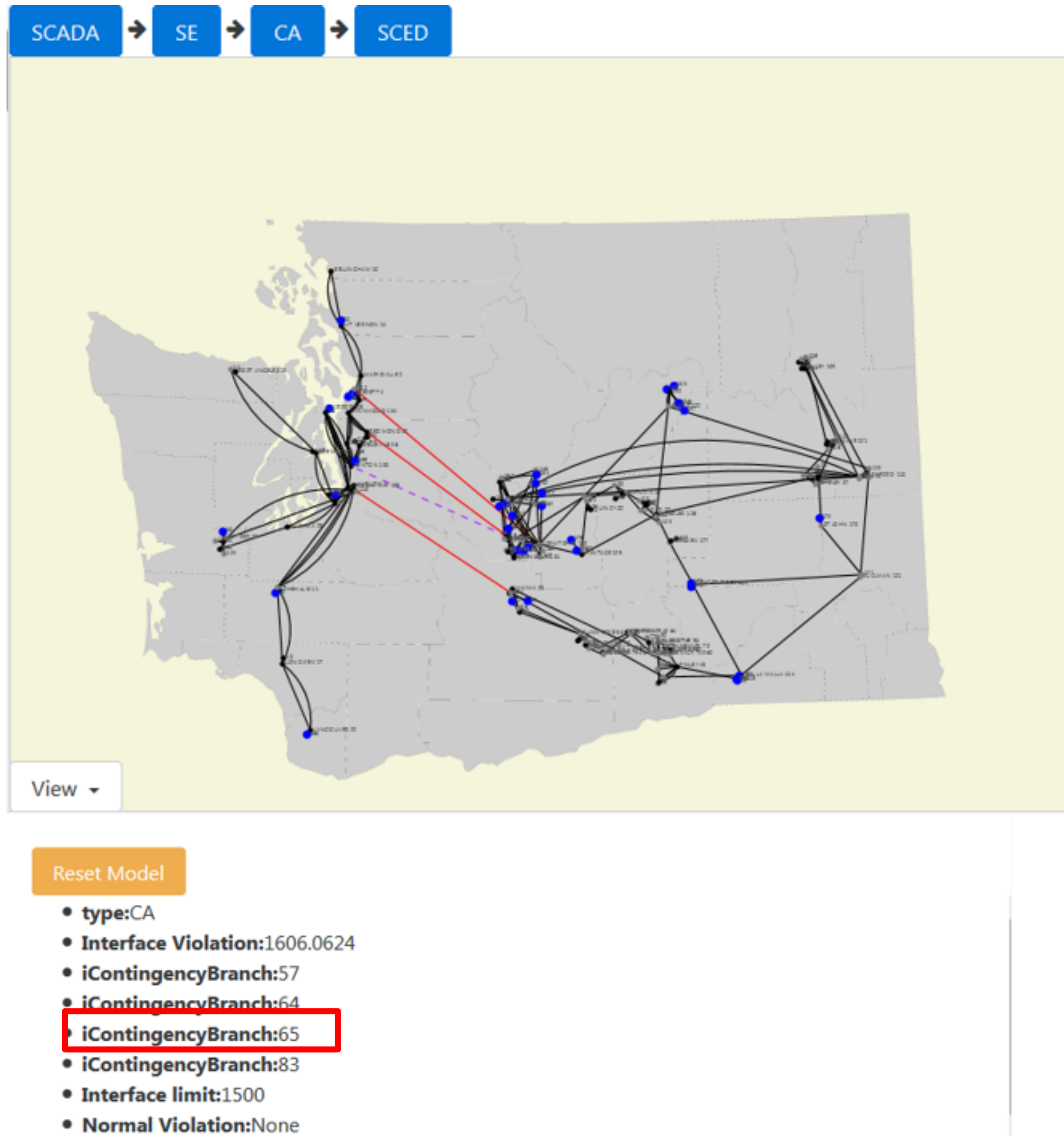
- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector
- No post-contingency violation is found!
- No security constraints are added in SCED!!
- Several generators re-dispatch due to the false load

In the physical system:

- Four post-contingency interface violations are unobservable in the cyber system!



FDI Attack

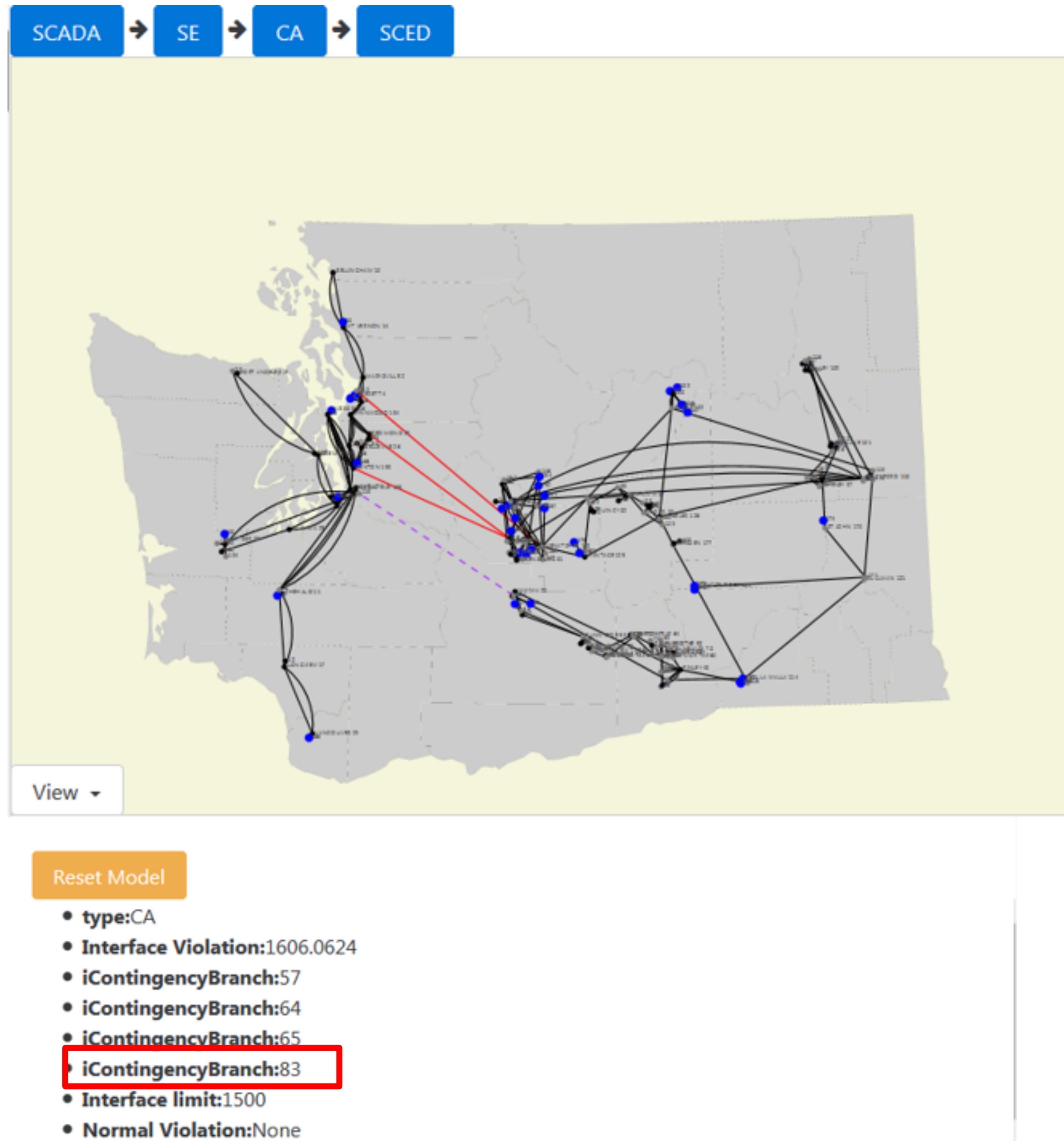
- **Inject false measurements in SCADA**

In the cyber system:

- This attack cannot be detected by bad data detector
- No post-contingency violation is found!
- No security constraints are added in SCED!!
- Several generators re-dispatch due to the false load

In the physical system:

- Four post-contingency interface violations are unobservable in the cyber system!



Discussion

- Typically, the attacker is assumed to have complete knowledge of the system
- What if the attacker's information is limited to a sub-network?
- We introduce a class of *limited information FDI attacks*

- FDI attack model: bi-level optimization problem that is then converted to single-level mixed integer linear programming (MILP)
- Such a modification introduces a large number of binary variables
- Problem is intractable for large power systems
- Can we evaluate the vulnerability of large-scale system to FDI attacks?
- We introduce *scalable optimization* methods to address this problem

FDI Attacks with Limited External Network Information

J. Zhang, Z. Chu, L. Sankar and O. Kosut, "False data injection attacks on power system state estimation with limited information," *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, USA, 2016, pp. 1-5.
J. Zhang, Z. Chu, L. Sankar and O. Kosut, "Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems?" *IEEE Transactions on Power Systems, under review*. [Online] https://arxiv.org/abs/1703.07500

Limited Information

The knowledge (K2) and capabilities (C2) of the attacker:

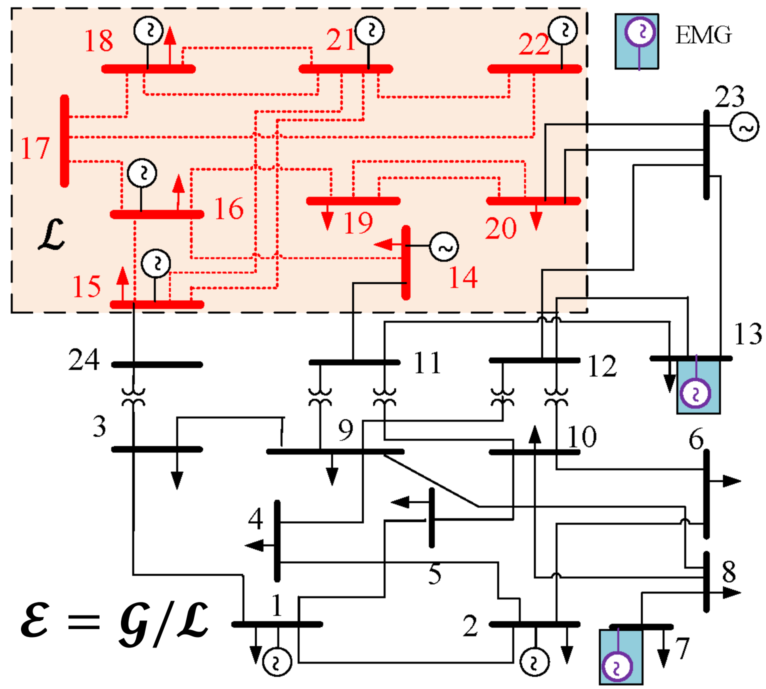
K2(a) Perfect knowledge inside a subnetwork $\mathcal{L}$:

i. the topology
ii. the cost, capacity, and status of generators
iii. the historical load data

K2(b) Knowledge outside $\mathcal{L}$ (possibly inaccurate):

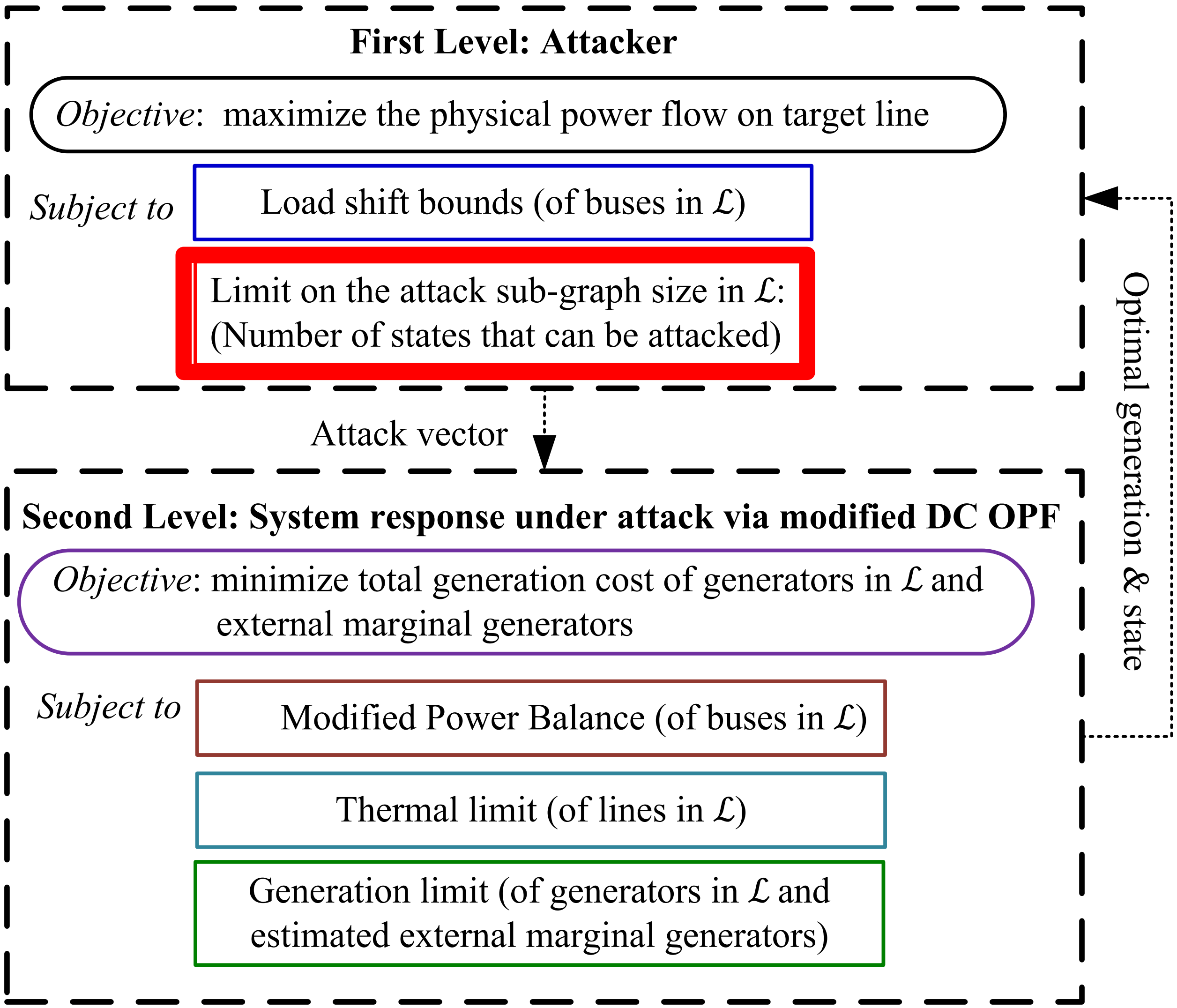
i. the power transfer distribution factor (PTDF) of $\mathcal{G}$
ii. status, capacity and cost of only marginal generators

C2 Access and modify measurements inside a small area $\mathcal{S}$, $\mathcal{S} \subseteq \mathcal{L}$



EMG: external marginal generators

Optimization for Worst-case Attacks



Optimization for Worst-case Attacks

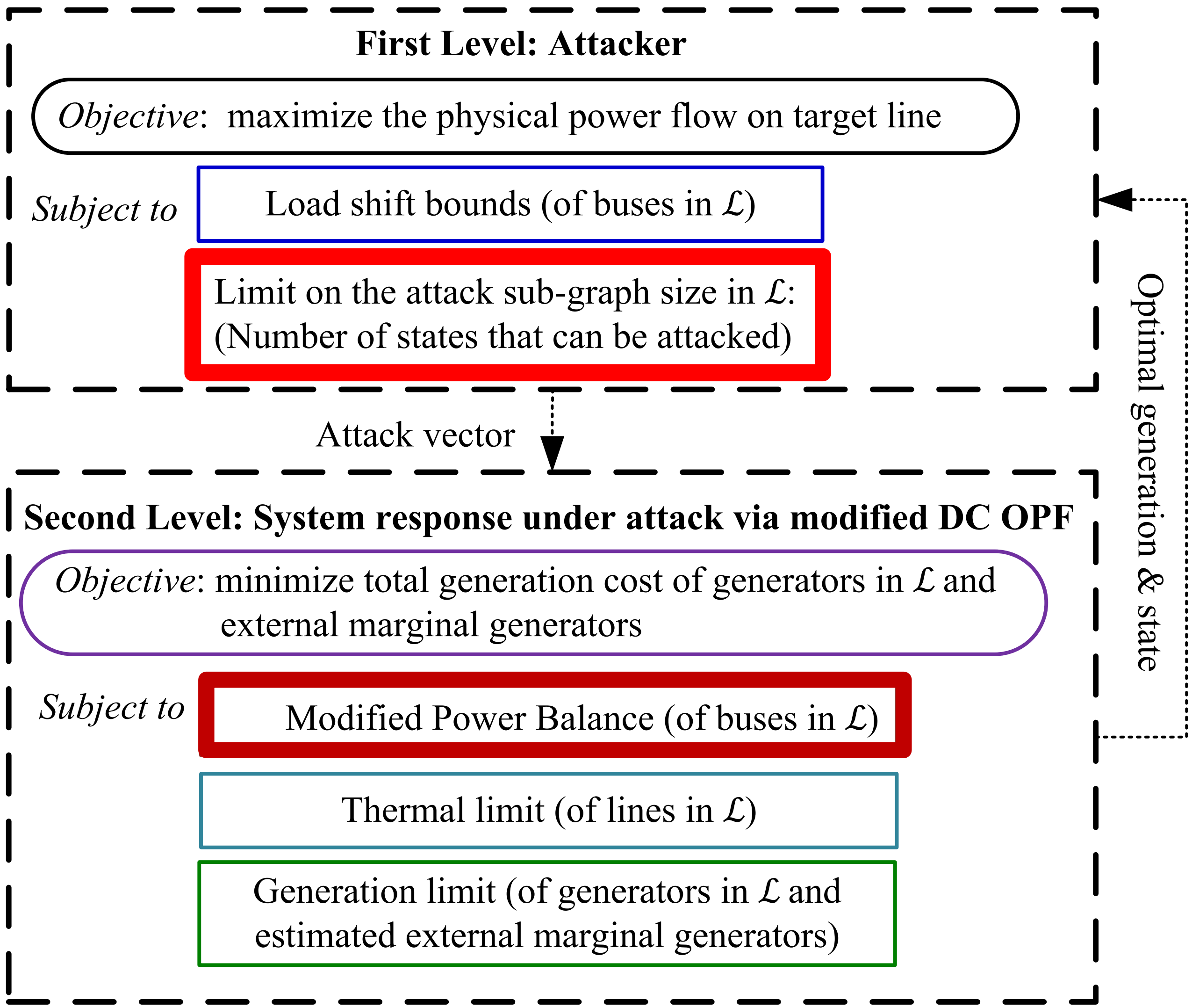
Modifications due to limited information:

- Attack vector is limited only inside $\mathcal{L}$

Limit on the attack sub-graph size:
(Number of states that can be attacked)

- Only states inside $\mathcal{L}$ can be changed
- States on boundary buses remain unchanged

Optimization for Worst-case Attacks



Optimization for Worst-case Attacks

Modifications due to limited information:

- Power balance constraints in $\mathcal{L}$ is modified as

> - Power balance of internal buses in $\mathcal{L}$ remain unchanged
> - Power balance of boundary buses in $\mathcal{L}$:
>
> *Generation* – Σ *Power flow in* $\mathcal{L}$ – Σ *Injection from* $\mathcal{E}$ = *Load*
>
> Estimated PTDF and external marginal generation are utilized to calculate injection from $\mathcal{E}$

Discussion

- Compared to perfect information attacks, limited information attack optimization may only lead to sub-optimal attack vector

- The estimated consequences may be inaccurate due to
  - Congested lines in $\mathcal{E}$
  - Wrong external marginal generators (EMG)
  - Wrong PTDF

- However, such limited inaccurate attacks can still cause damage to a congested system

Illustration of Results

Test system: IEEE 24-bus RTS

- Perfect information attacks **(Global case)**
- Limited information attacks:
  - External information is perfect (**Perfect local case**)
  - Inaccurate external information
    - **Case 1**: Lack of knowledge of congested lines in $\mathcal{E}$
    - **Case 2**: Wrong external marginal generators (EMG)
    - **Case 3**: Wrong PTDF

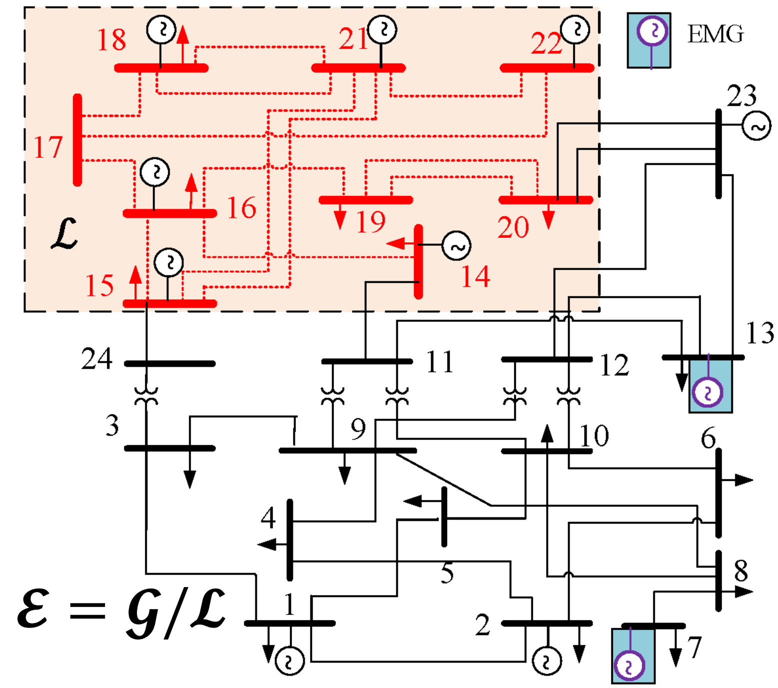
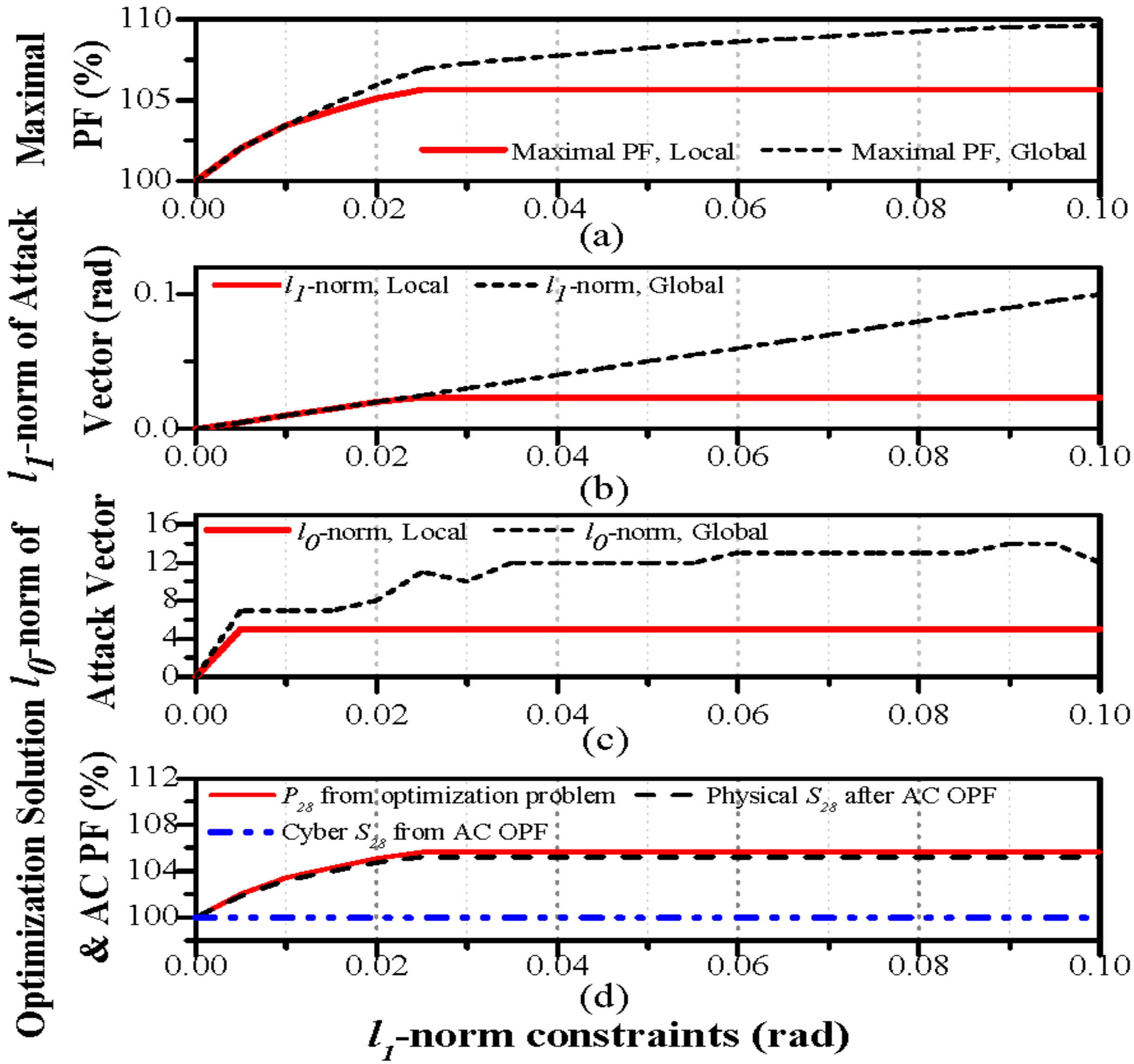


Illustration of Results

Global case vs. Perfect local case



Target line 28

Illustration of Results

Perfect information vs. inaccurate external information

Case	Actual Physical PF	Computed Physical PF
Perfect Case	105.64%	105.64%
Case 1	104.60%	105.64%
Case 2	104.82%	105.95%
Case 3	104.95%	105.90%

Case 1: Lack of knowledge of congested lines in $\mathcal{E}$
Case 2: Wrong external marginal generators (EMG)
Case 3: Wrong PTDF

No External Network Information

- Designing FDI attacks with limited external network information still requires partial information in external network

- What if the attacker has no information in external network?

- Can attacker take advantage of the historical data to overcome limited information?

No External Network Information

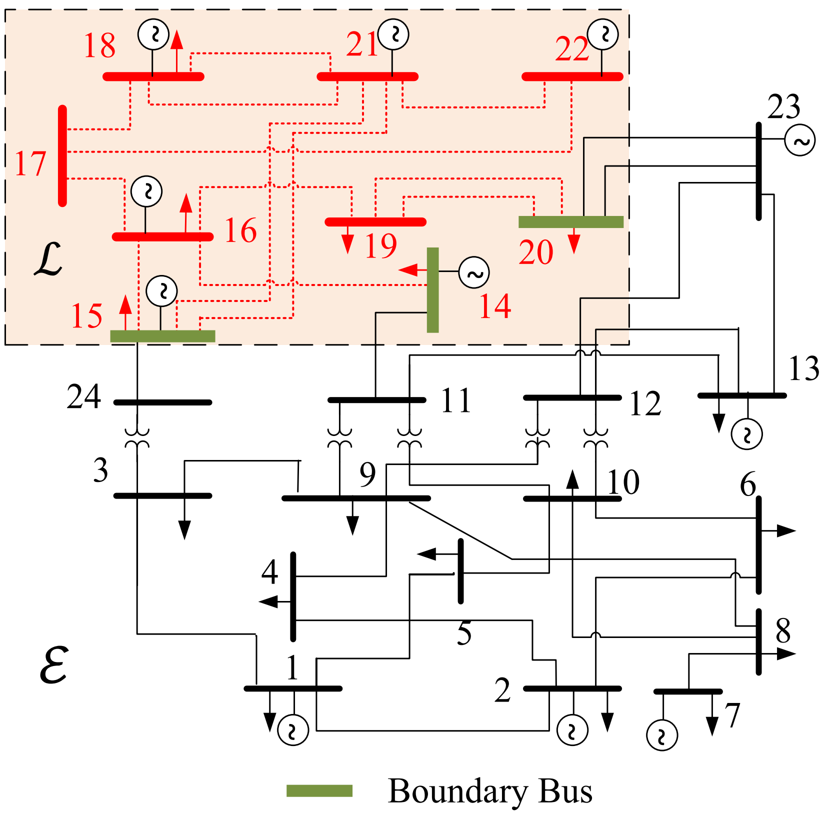
The knowledge (K3) and capabilities (C3) of the attacker:

K3 Perfect knowledge inside a subnetwork $\mathcal{L}$:

i. the topology
ii. the historical data of generators including cost, capacity, and status
iii. the historical load data
iv. the locational marginal price (LMP)

C3 Access and modify measurements inside a small area $\mathcal{S}$, $\mathcal{S} \subseteq \mathcal{L}$

Reformulate System Power Flow with Localized Information



For lines in $\mathcal{L}$:

$$P = K\left(GP_G - P_D\right)$$

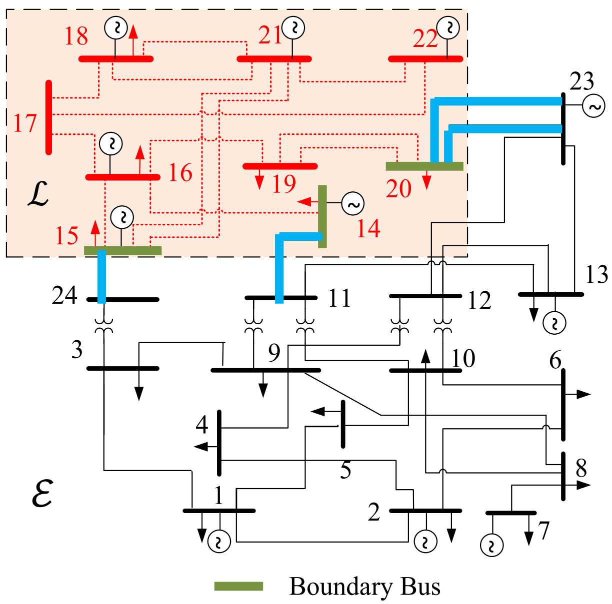
– K is the PTDF matrix of the entire network

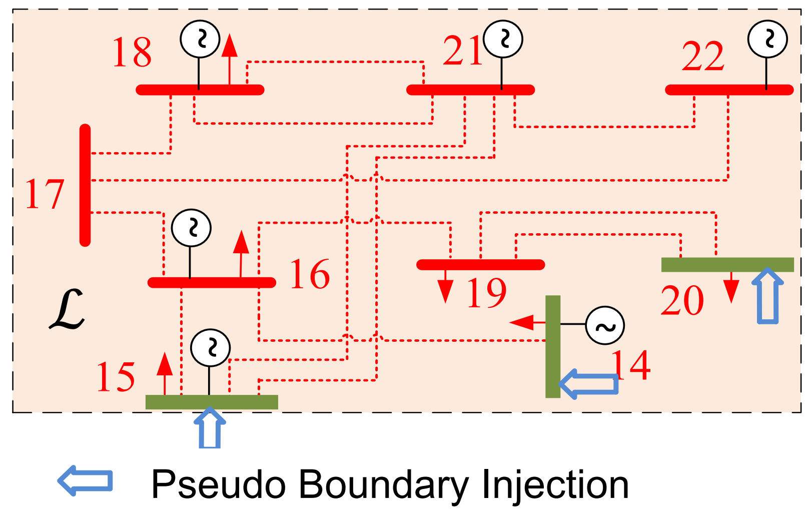
$$P = K^{\mathcal{L}}\left(G_{\mathcal{L}}P_G - P_{D,\mathcal{L}}\right) + \boxed{K^{\mathcal{E}}\left(G_{\mathcal{E}}P_G - P_{D,\mathcal{E}}\right)}$$

Unknown to attacker!!

- P is the vector of real power flow
- P_G is the vector of real generation output
- P_D is the vector of real power load
- G is the generator-to-bus connectivity matrix

Reformulate System Power Flow with Localized Information





$$\bar{P}_{I,i} = \sum_{k \in \mathbb{W}_i^{\mathcal{E}}} P_k$$

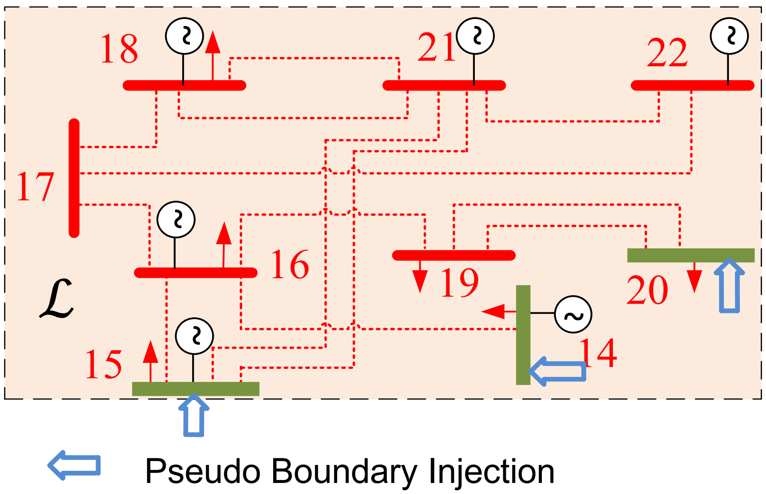
- Introduce pseudo-boundary injections

$$\bar{P} = \bar{K}(\bar{G}\bar{P}_G - \bar{P}_D) - \bar{K}^{\mathcal{B}}\bar{P}_{I,\mathcal{B}}$$

  – $\overline{(\cdot)}$ represents vector or matrix computed only within the attack sub-network $\mathcal{L}$

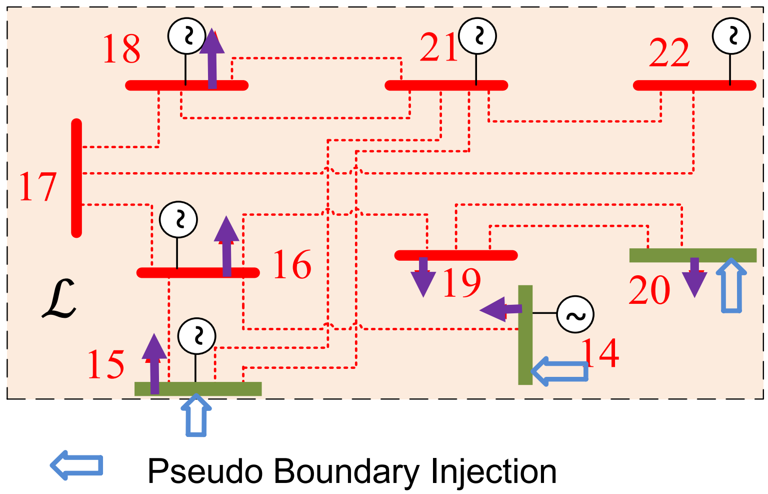
Multiple Linear Regression Model

- Pseudo-boundary injections depends on both power injections in $\mathcal{L}$ and $\mathcal{E}$



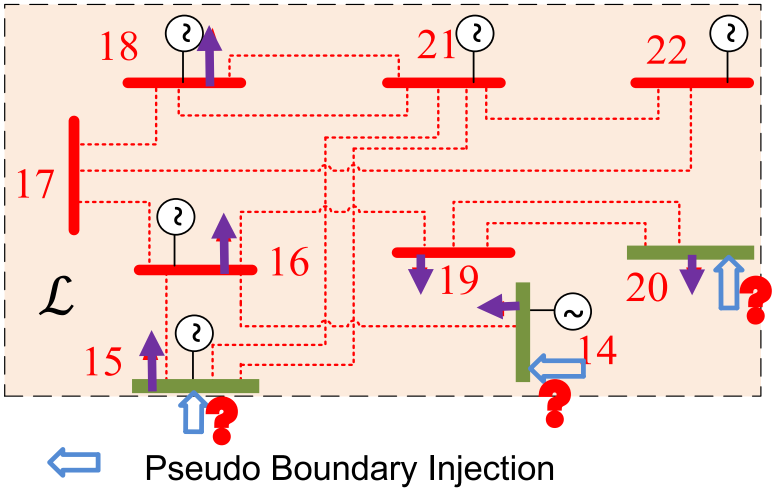
Multiple Linear Regression Model

- Pseudo-boundary injections depends on both power injections in $\mathcal{L}$ and $\mathcal{E}$
- The attacker cannot accurately estimate the system re-dispatch after attack with real-time information in $\mathcal{L}$.



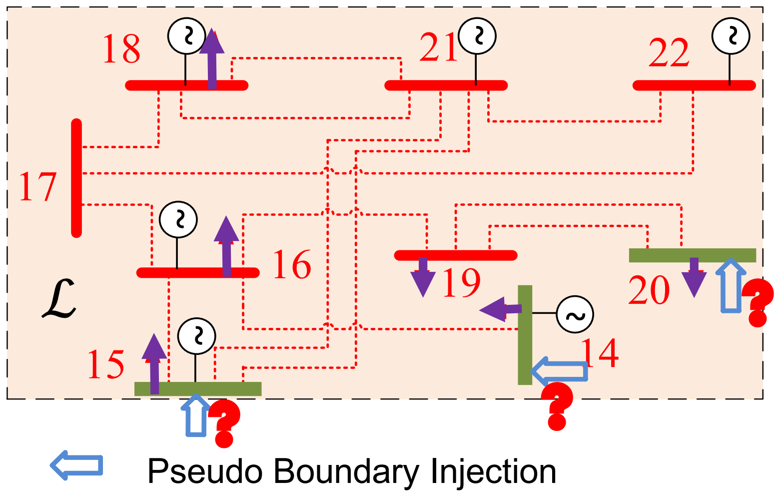
Multiple Linear Regression Model

- Pseudo-boundary injections depends on both power injections in $\mathcal{L}$ and $\mathcal{E}$
- The attacker cannot accurately estimate the system re-dispatch after attack with real-time information in $\mathcal{L}$.



Multiple Linear Regression Model

- Pseudo-boundary injections depends on both power injections in $\mathcal{L}$ and $\mathcal{E}$
- The attacker cannot accurately estimate the system re-dispatch after attack with real-time information in $\mathcal{L}$.
- Attacker can learn a functional relationship between pseudo-boundary injections and power injections inside $\mathcal{L}$ from historical data

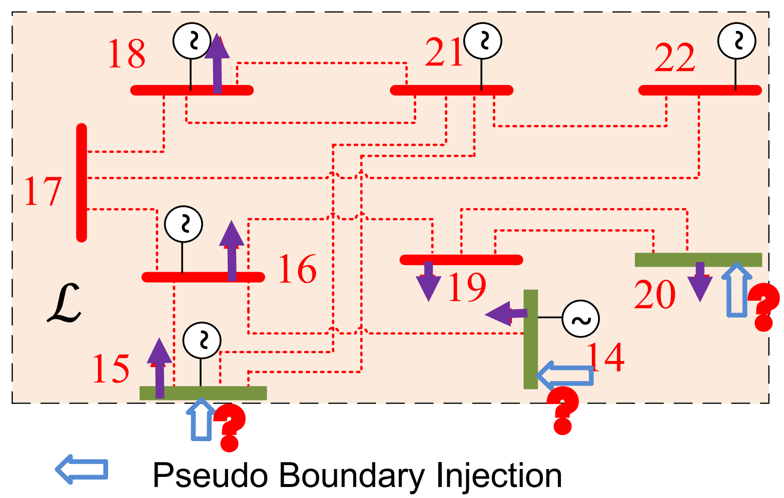


Multiple Linear Regression Model

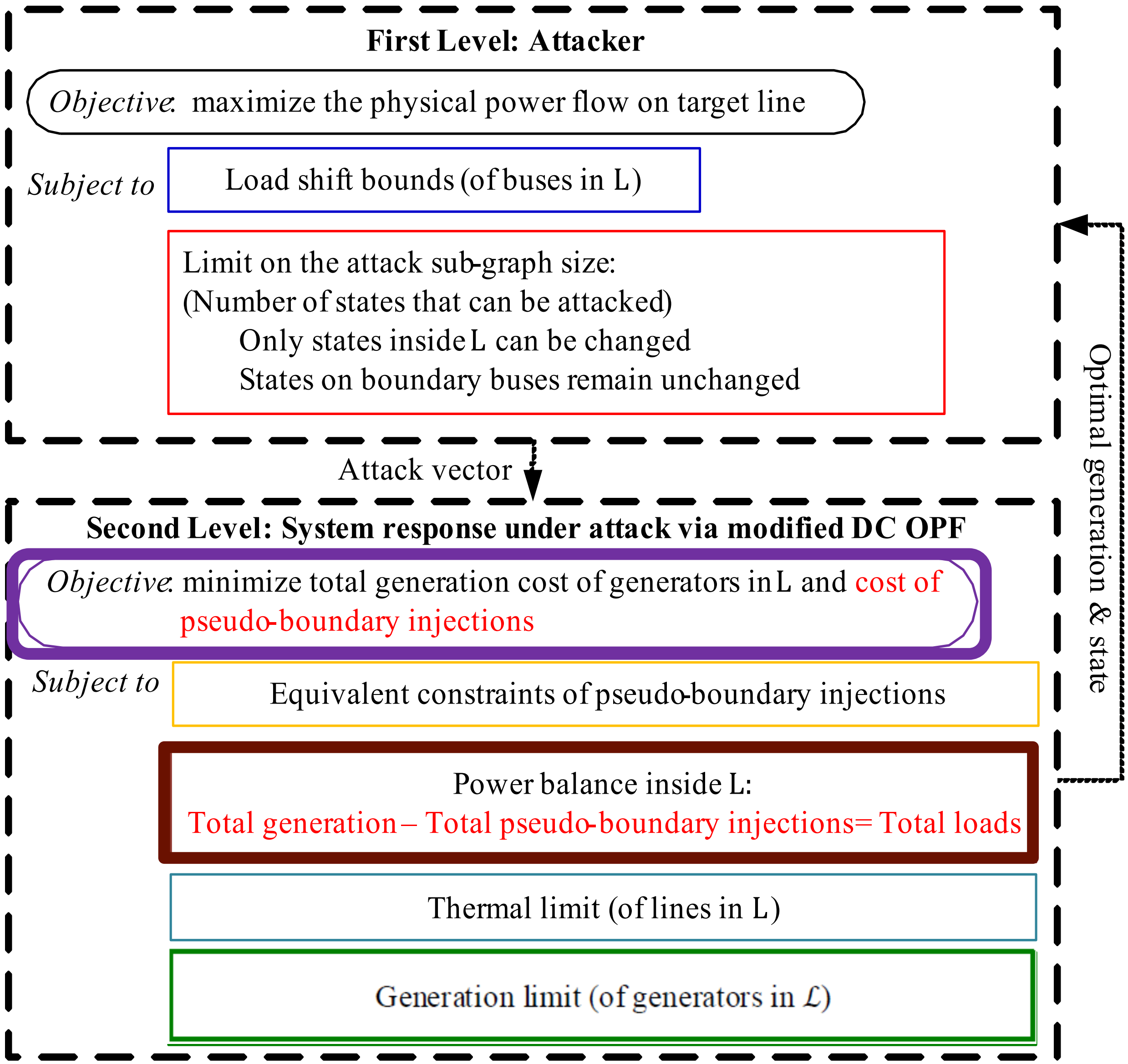
- Pseudo-boundary injections depends on both power injections in $\mathcal{L}$ and $\mathcal{E}$
- The attacker cannot accurately estimate the system re-dispatch after attack with real-time information in $\mathcal{L}$.
- Attacker can learn a functional relationship between pseudo-boundary injections and power injections inside $\mathcal{L}$ from historical data
- The attacker can then predict the pseudo-boundary injections as

$$\hat{\bar{\bar{P}}}_{I,\mathcal{B}} = \hat{F}\left(\bar{G}\bar{P}_G - \bar{P}_D\right) + \hat{f}_0$$

  - $\hat{F}$ is the linear coefficient matrix
  - $\hat{f}_0$ is the constant

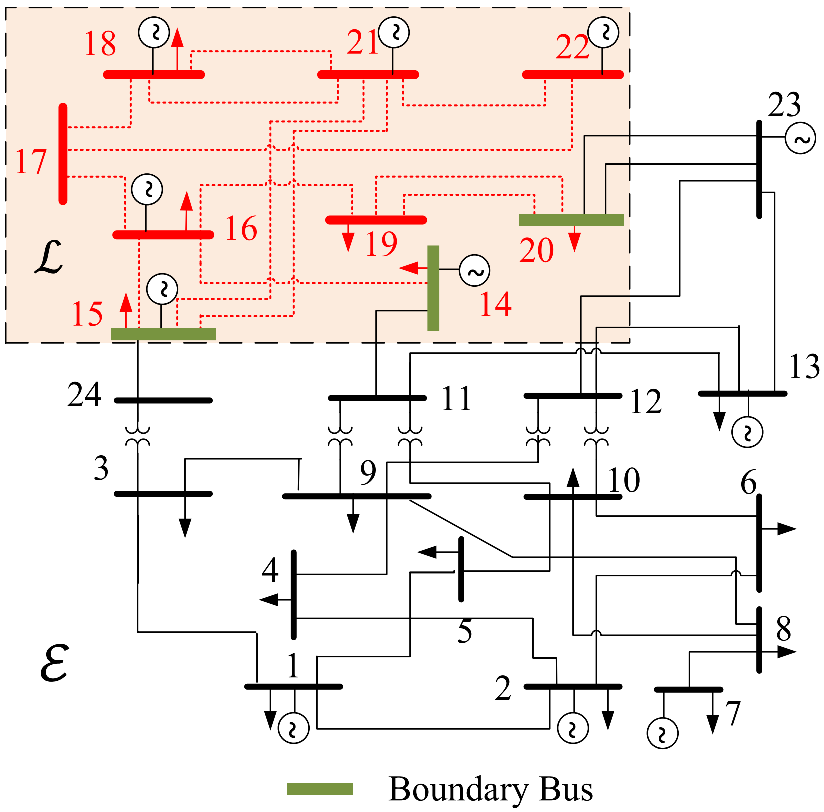


Optimization for worst-case attacks



Historical Data Analysis

- **Scenario 1 - Constant Loads in $\mathcal{E}$:**
  In each instance of data:

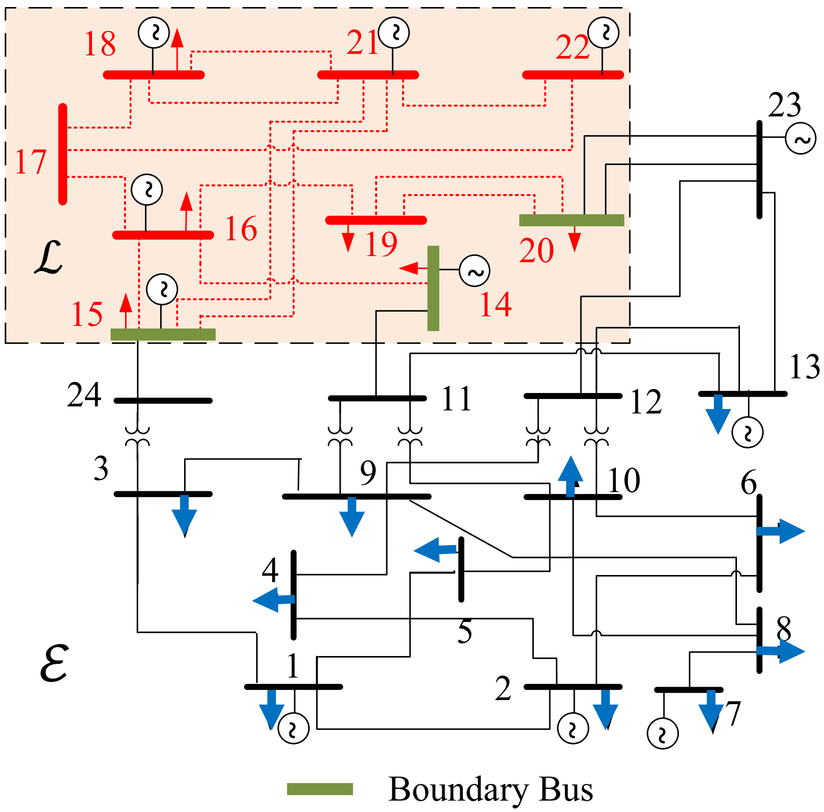


Historical Data Analysis

- **Scenario 1 - Constant Loads in $\mathcal{E}$:**

  In each instance of data:

  - loads in $\mathcal{E}$ remain unchanged
  - loads in $\mathcal{L}$ varies as a percent p of the base load, where p is independent $\mathcal{N}(0; 10\%)$.

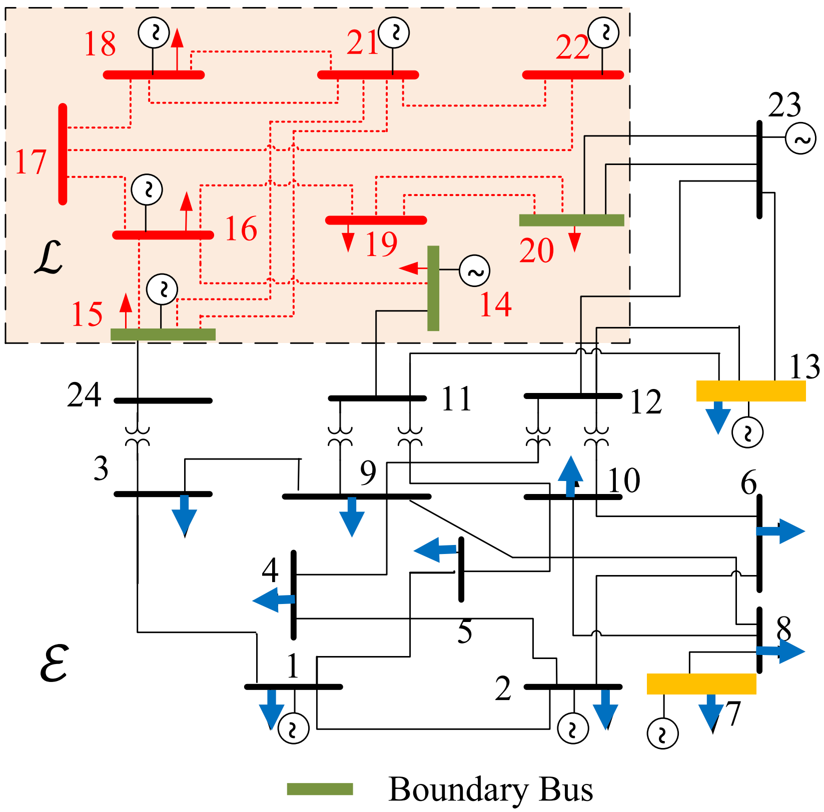


Historical Data Analysis

- **Scenario 1 - Constant Loads in $\mathcal{E}$:**

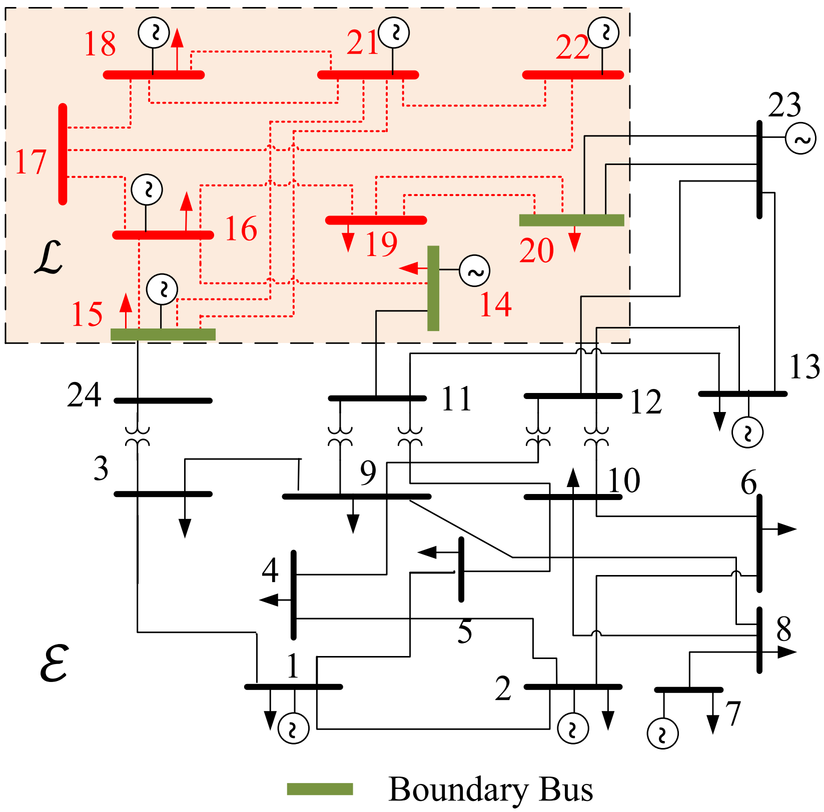
  In each instance of data:

  - loads in $\mathcal{E}$ remain unchanged
  - loads in $\mathcal{L}$ varies as a percent p of the base load, where p is independent $\mathcal{N}(0; 10\%)$.



Historical Data Analysis

- **Scenario 1 - Constant Loads in $\mathcal{E}$:**
  In each instance of data:
  - loads in $\mathcal{E}$ remain unchanged
  - loads in $\mathcal{L}$ varies as a percent p of the base load, where p is independent $\mathcal{N}(0;\ 10\%)$.
- **Scenario 2 - Varying Loads in the whole network $\mathcal{G}$:**



Historical Data Analysis

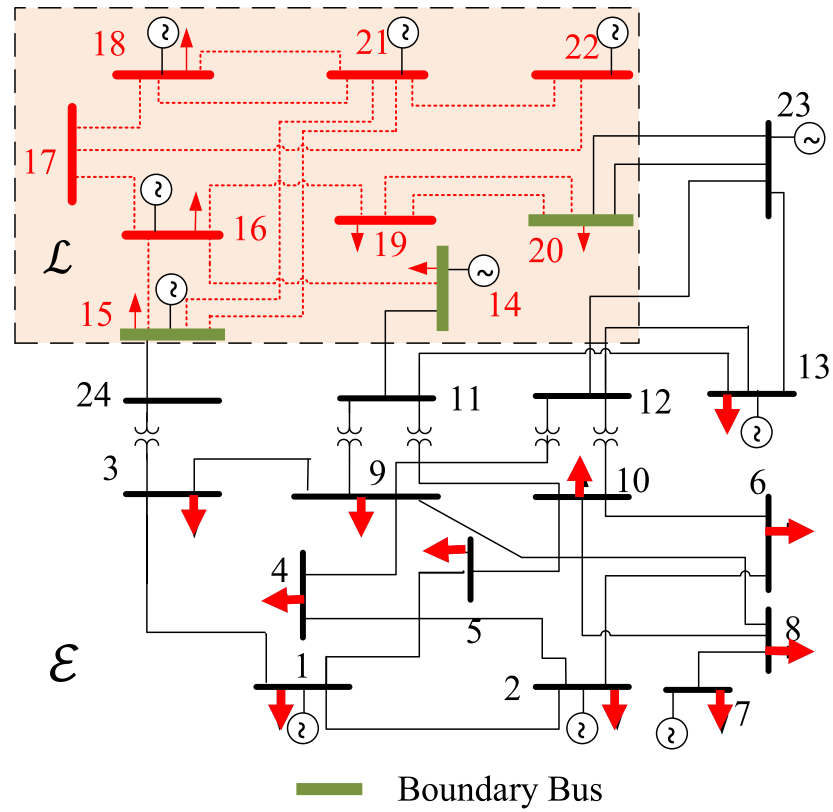
- **Scenario 1 - Constant Loads in $\mathcal{E}$:**

  In each instance of data:

  - loads in $\mathcal{E}$ remain unchanged
  - loads in $\mathcal{L}$ varies as a percent p of the base load, where p is independent $\mathcal{N}(0; 10\%)$.

- **Scenario 2 - Varying Loads in the whole network $\mathcal{G}$:**

  In each instance of data, both loads in $\mathcal{L}$ and $\mathcal{E}$ varies as a percent p of the base load, where p is independent $\mathcal{N}(0; 10\%)$.



Historical Data Analysis

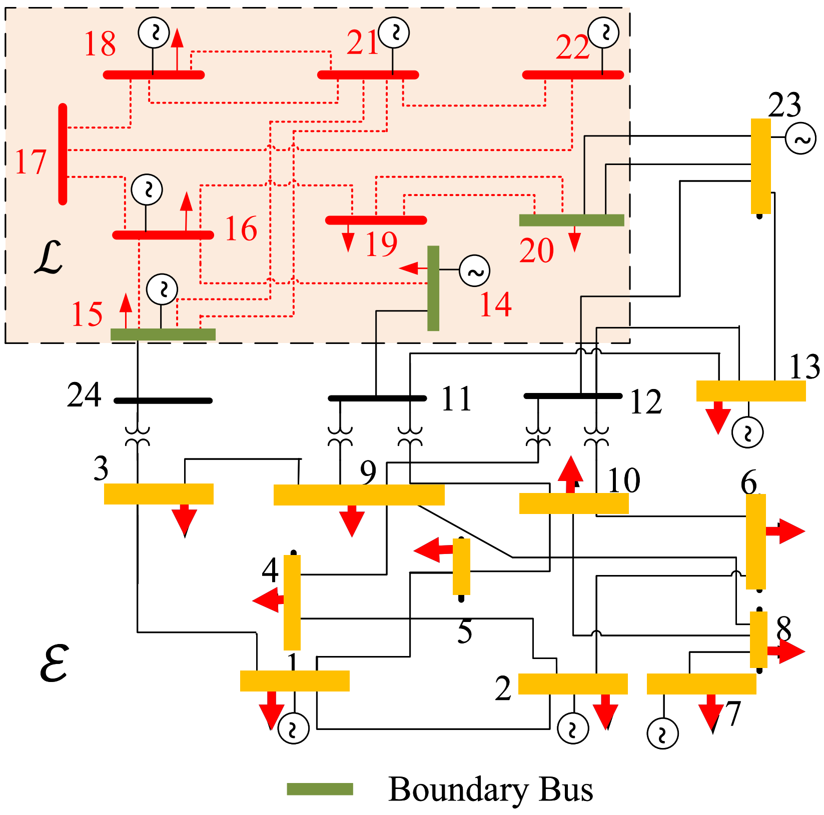
- **Scenario 1 - Constant Loads in $\mathcal{E}$:**

  In each instance of data:

  - loads in $\mathcal{E}$ remain unchanged
  - loads in $\mathcal{L}$ varies as a percent p of the base load, where p is independent $\mathcal{N}(0; 10\%)$.

- **Scenario 2 - Varying Loads in the whole network $\mathcal{G}$:**

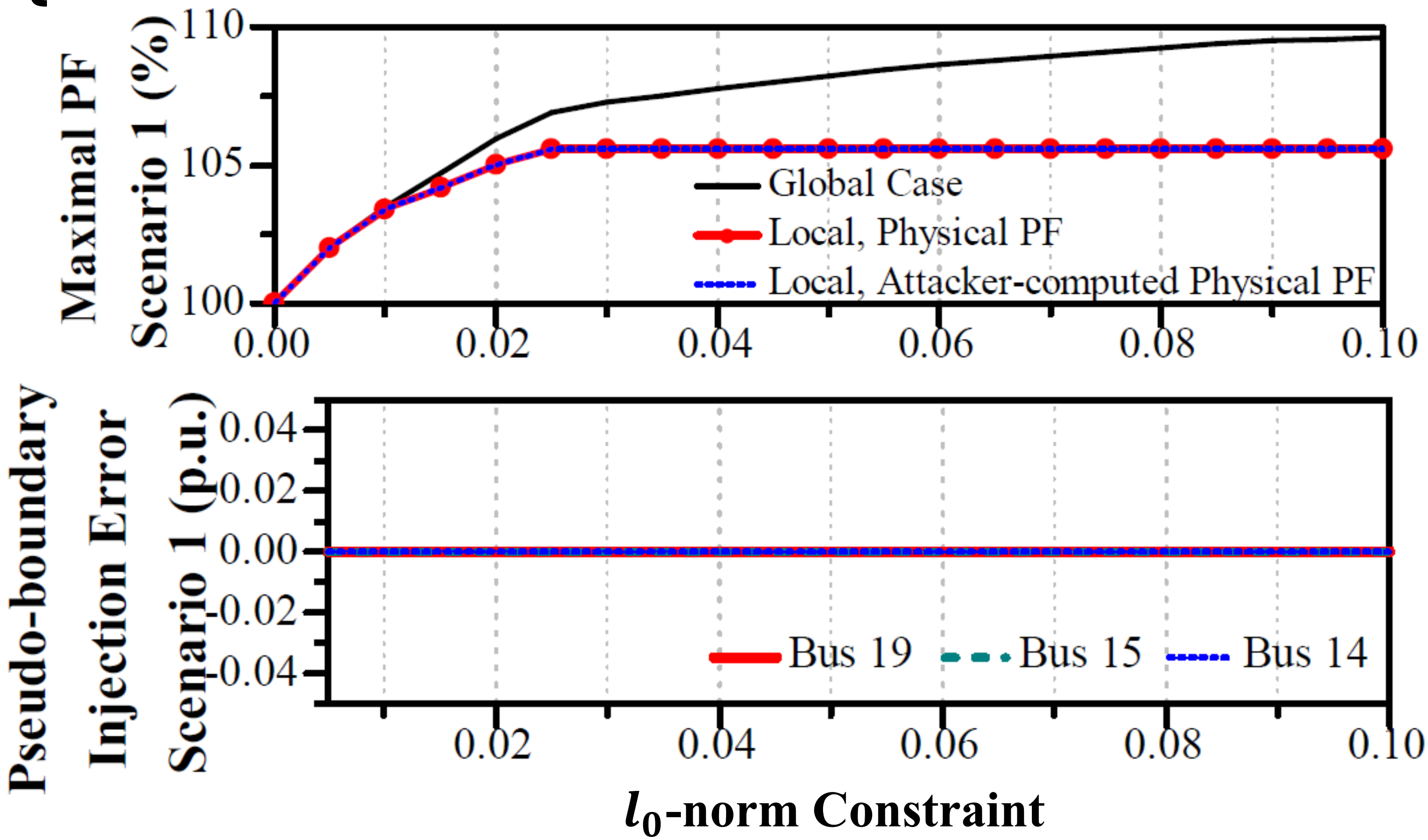
  In each instance of data, both loads in $\mathcal{L}$ and $\mathcal{E}$ varies as a percent p of the base load, where p is independent $\mathcal{N}(0; 10\%)$.



IEEE 24-bus System

Scenario 1: Constant Loads in $\mathcal{E}$

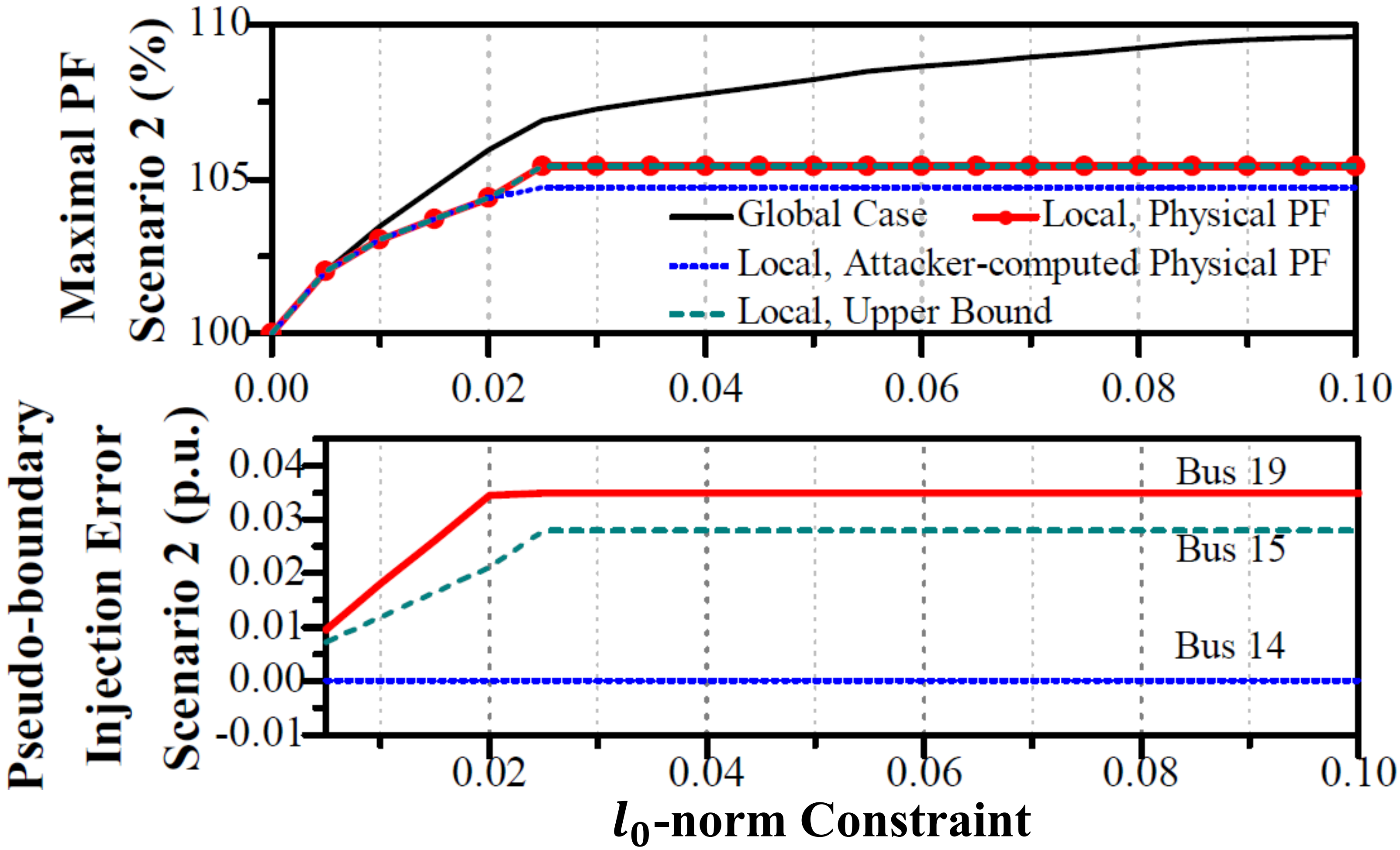
Target line 28



IEEE 24-bus System

Scenario 2: Varying Loads in the whole network $\mathcal{G}$

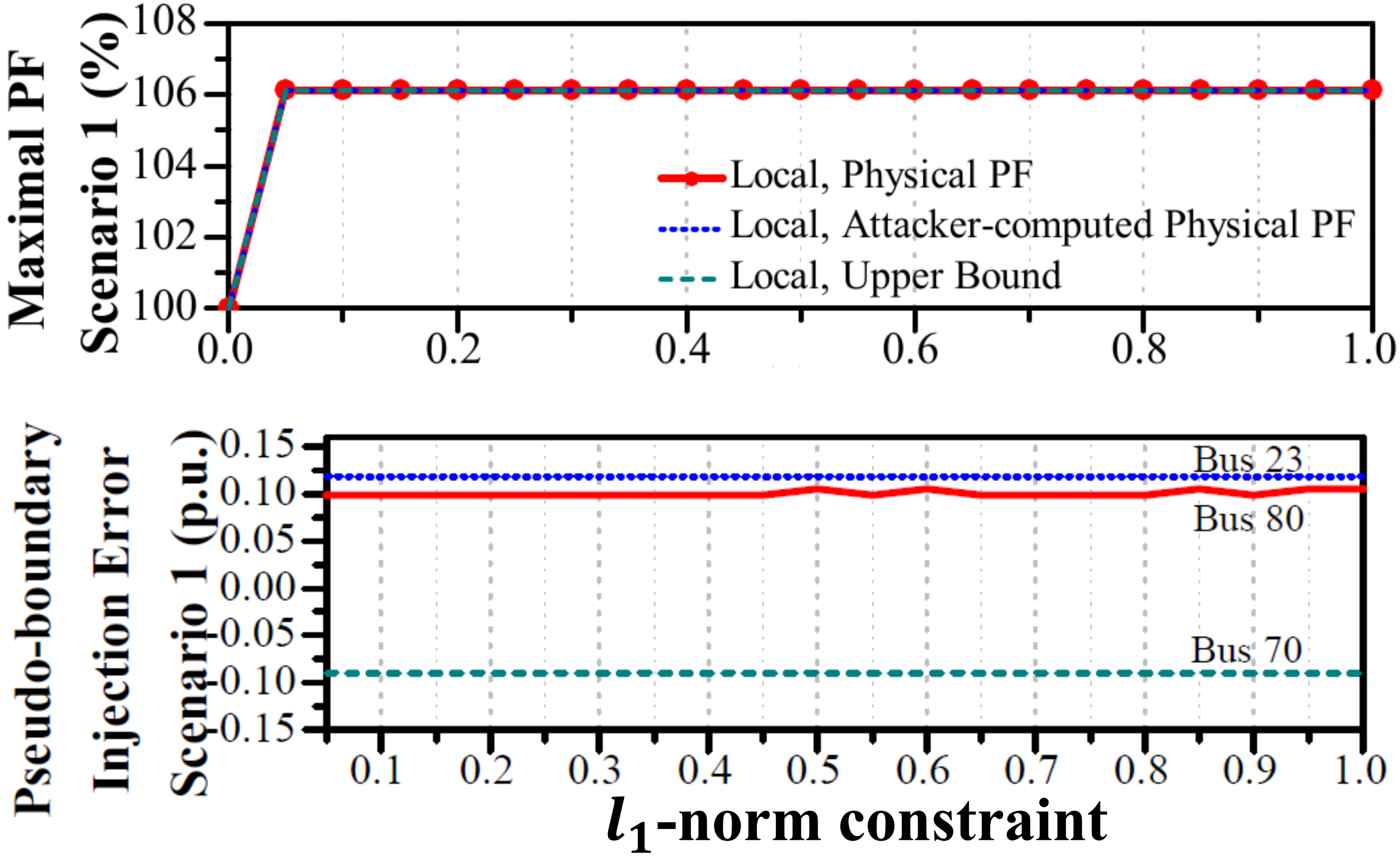
Target line 28



IEEE 118-bus System

Scenario 1: Constant Loads in $\mathcal{E}$

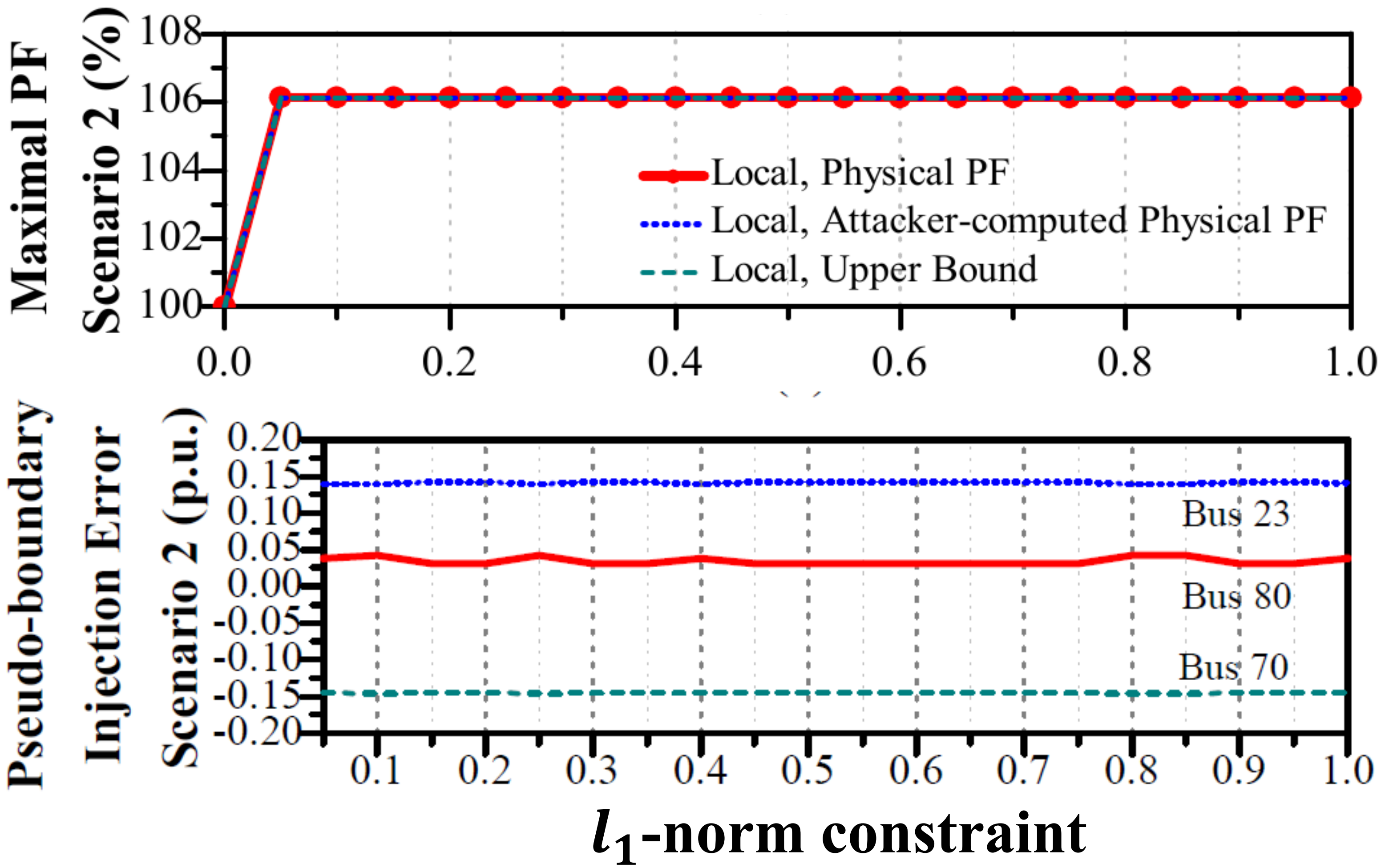
Target line 5



IEEE 118-bus System

Scenario 2: Varying Loads in the whole network $\mathcal{G}$

Target line 28



FDI Attacks via Scalable Optimization

Still vulnerable?

Joint work with Zhigang Chu, Jiazi Zhang, and Oliver Kosut

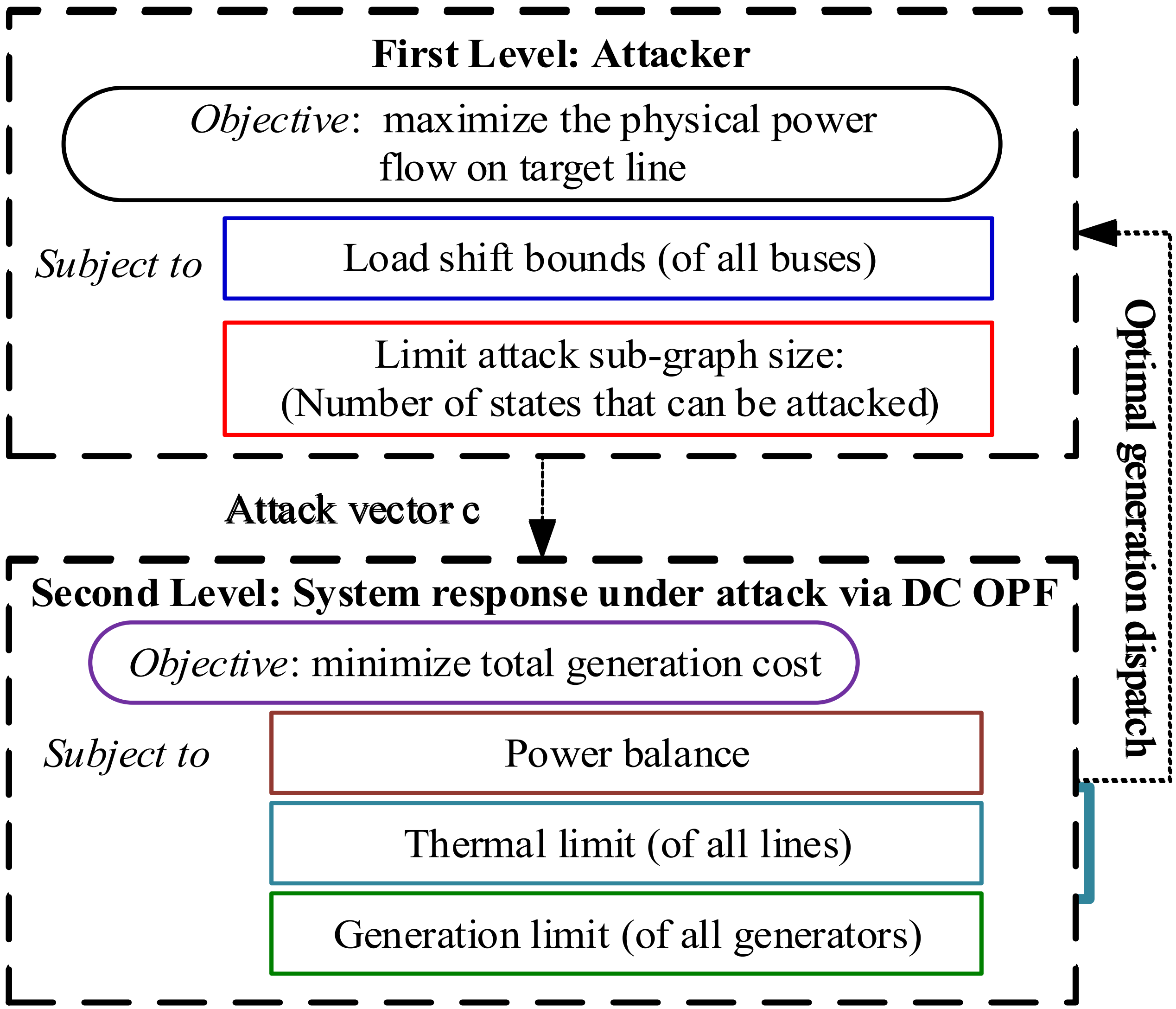
Z. Chu, J. Zhang, O. Kosut, and L. Sankar, "Evaluating Power System Vulnerability to False Data Injection Attacks via Scalable Optimization," *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Sydney, 2016, pp. 1-6.

Z. Chu, J. Zhang, O. Kosut, and L. Sankar, "Vulnerability Assessment of Large-scale Power Systems to False Data Injection Attacks," *IEEE Transaction on Power systems,* under review. [Online] https://arxiv.org/abs/1705.04218

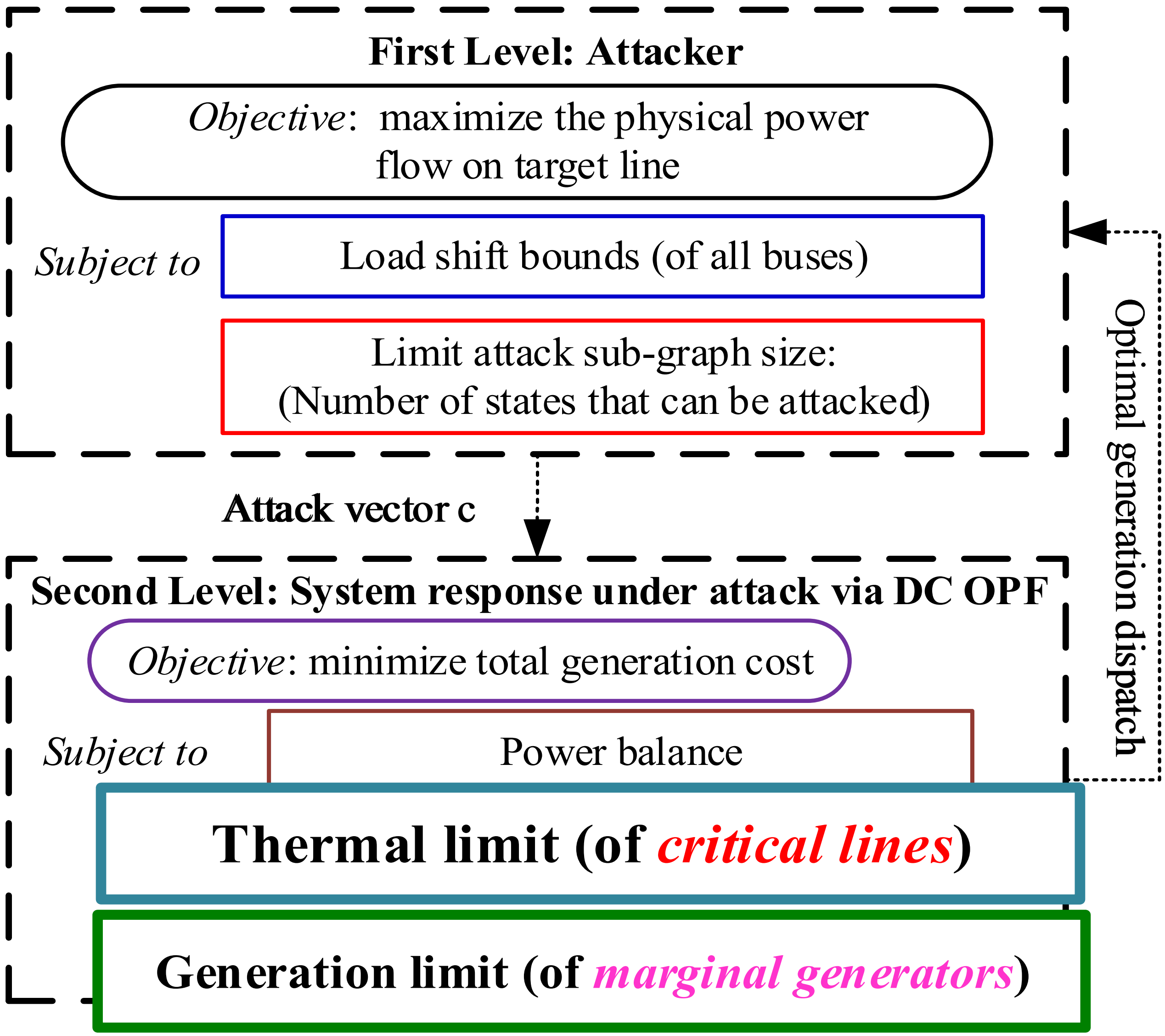
Attack Optimization Problem on Large-scale Power Systems

- The number of binary variables increases with the size of the network
  - Large number of transmission lines and generators
  - Hard to solve the optimization problem due to numerical challenges
- Four computationally efficient algorithms

Algorithm1: Row Generation



Algorithm2: Row & Column Generation



Algorithm 3: Cyber-physical Difference Maximization

Step 1: Solve the following optimization problem

Objective: maximize *the difference between physical and cyber power flow* on target line

Subject to

Load shift bounds (of all buses)

Limit attack sub-graph size:
(Number of states that can be attacked)

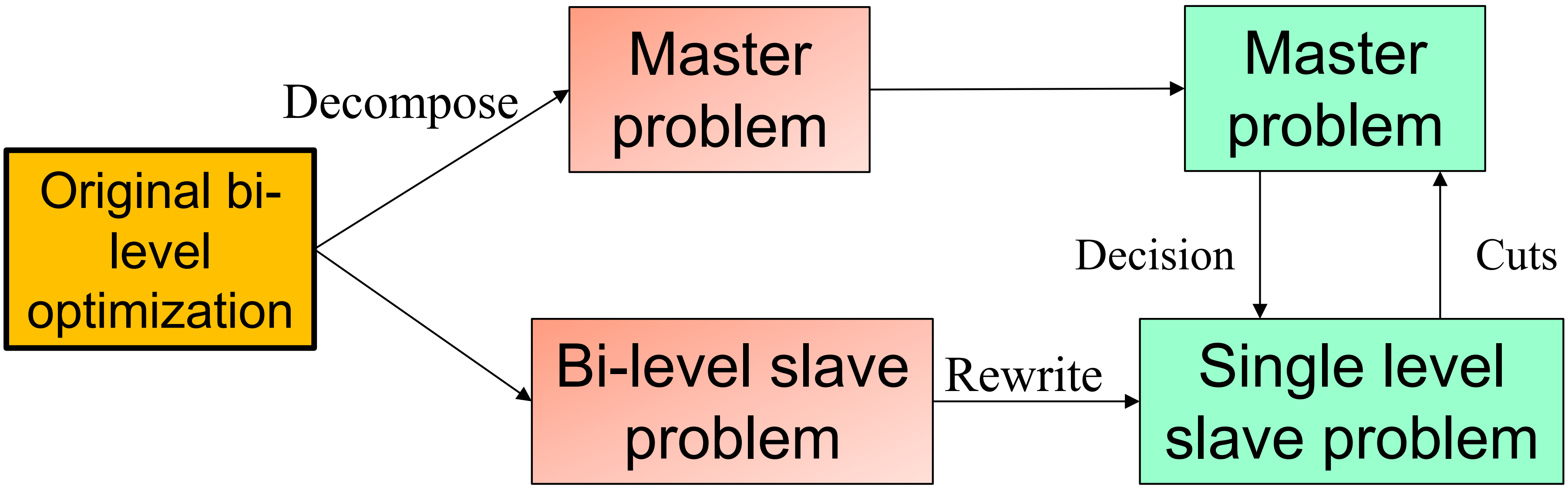
Attack Vector

Obtain upper bound = Objective + Rating

Step 2: Re-run DCOPF with attack vector

Obtain lower bound = Resulting physical power flow

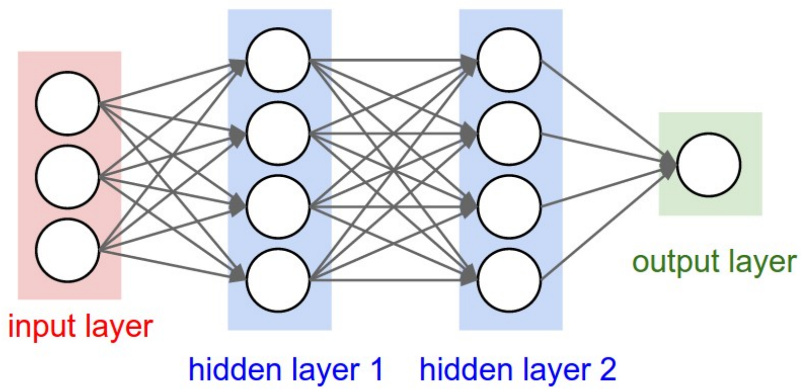
Algorithm 4: Modified Benders' Decomposition



- Iteratively solve the master problem and single level slave problem until convergence
- Due to the non-convexity of the original bi-level linear program, the solution of MBD, is a lower bound.

Ongoing Work

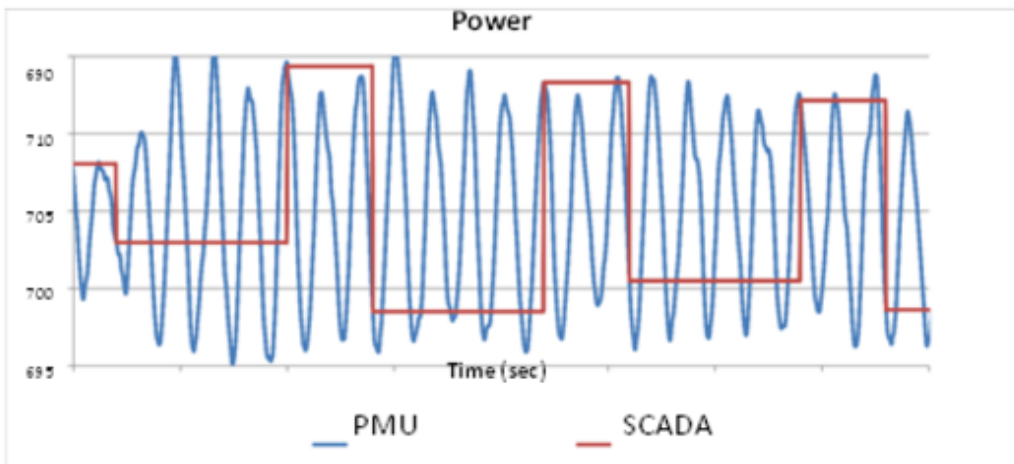
- Data-driven machine learning based attack detection



Ongoing Work

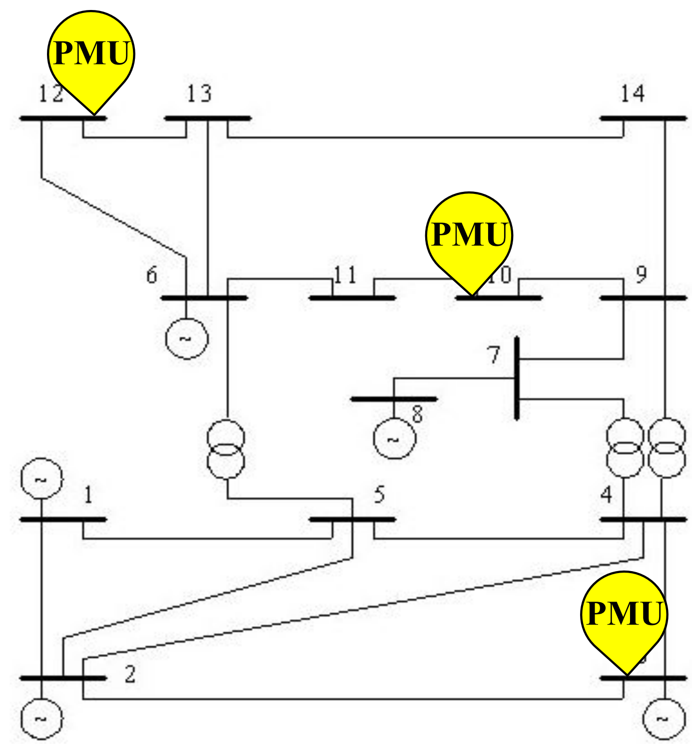
- Data-driven machine learning based attack detection

- Vulnerability analysis of PMU data



Ongoing Work

- Data-driven machine learning based attack detection
- Vulnerability analysis of PMU data
- Attack detection with PMUs



Team Profile: ASU

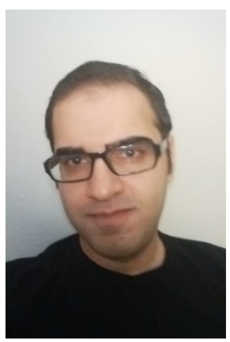
Dr. Lalitha Sankar
PI

Dr. Kory Hedman
Co-PI

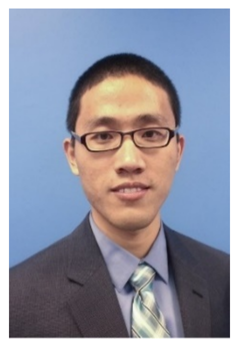
Dr. Oliver Kosut
Co-PI

Jiazi Zhang
Graduate Student

Zhigang Chu
Graduate Student



Roozbeh Khodadadeh
Graduate Student



Xingpeng Li
Graduate Student

Andrea Pinceti
Graduate Student

Funded by NSF-DHS & PSERC

Team Profile: IncSys

Dr. Robin Podmore
IncSys

Chris Mosier
PowerData

Fabiola Robinson
PowerData

- Mission: Help organizations of all sizes train and prepare the world's finest system operators to ensure the reliability of the bulk power system.
- Product: PowerSimulator™

ARIZONA STATE UNIVERSITY

IncSys

POWERDATA

PSERC

Funded by NSF-DHS & PSERC

Questions?

Lalitha Sankar

(lsankar@asu.edu)