THE OHIO STATE UNIVERSITY
COLLEGE OF ENGINEERING

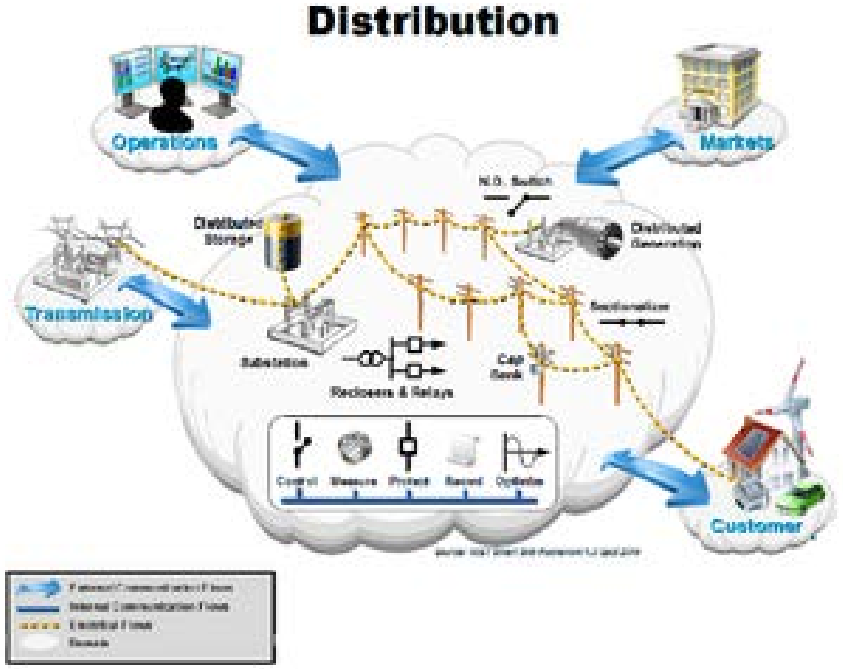
Attack Path Reconstruction from Consequence on Power Grids

with a focus on Monitoring Layer attacks

J.K. Wang Chris Moya
Wang.6536@osu.edu
Dept. of Electrical and Computer Engineering
The Ohio State University
Columbus, Ohio, USA

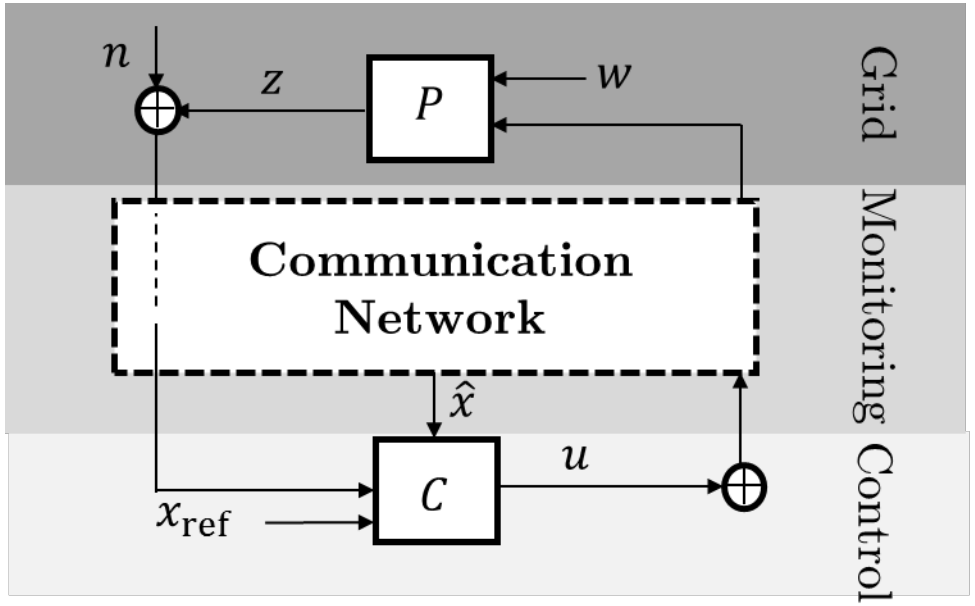
Motivation

- CPS structure of modern power grid.
  - **(Physical) grid**
    - including generators, power delivery equipment and lines, loads and protective devices;
  - **Control layer**
    - including central and local decision making units
  - **Monitoring layer**
    - including meters, actuators and hardware to store and transmit measurements



Motivation

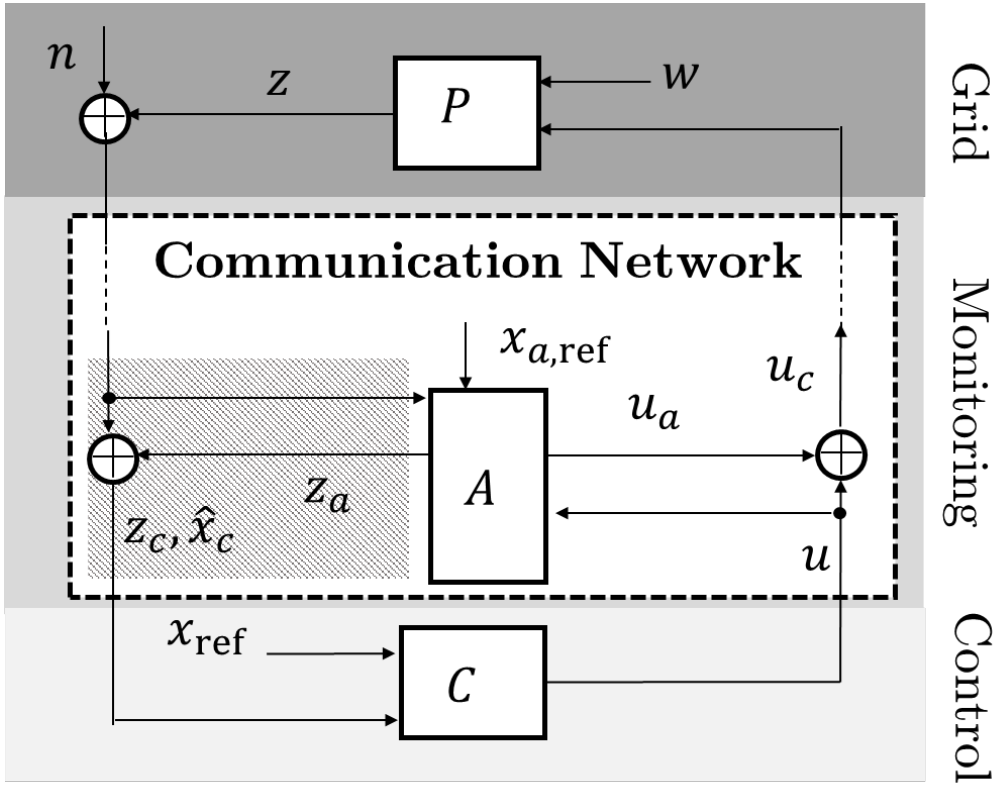
- Monitoring layer
  - **High impact**
    - Connecting a large number of devices over a wide area
    - Hovering over the control layer and the grid
  - **High vulnerability**
    - dedicated protection to individual devices practically impossible
    - nonproprietary cyber-space is resorted to important tasks, including electricity markets.



w system disturbance
n measurement noise
u operation command
z measurement
$\hat{x}$ estimated state
x_{ref} desired state

Motivation

- Measurement attacks
  - Model I: Covert control actions
    - False measurements are injected in order to cover the malicious control actions, while real attacks are launched on the control layer
    - replay attacks,
    - stealth attacks [Amin, 2012],
    - general covert attacks [Smith, 2011], [Teixeira, 2015]…

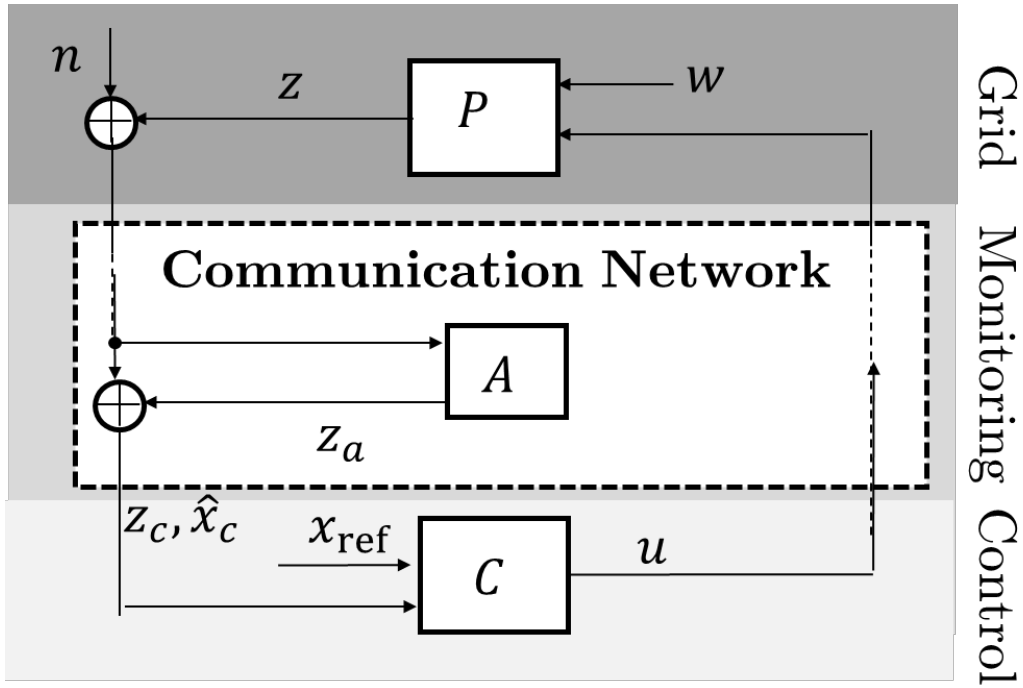


w system disturbance
n measurement noise
u operation command
z true measurement

z_a attacking measurement
z_c corrupted measurement
$\hat{x}_c$ corrupted estimated state
x_{ref} operator's desired state
$x_{a,\text{ref}}$ attacker's desired state

Motivation

- Measurement attacks
  - Model I: Covert control actions
  - Model II: Disabled alarms
    - The attacks that destroy the alarm function of the monitoring layer.
    - The formation of an attacker's action depends on the status of the physical grid.
    - Effect similar to causing "hidden failure."

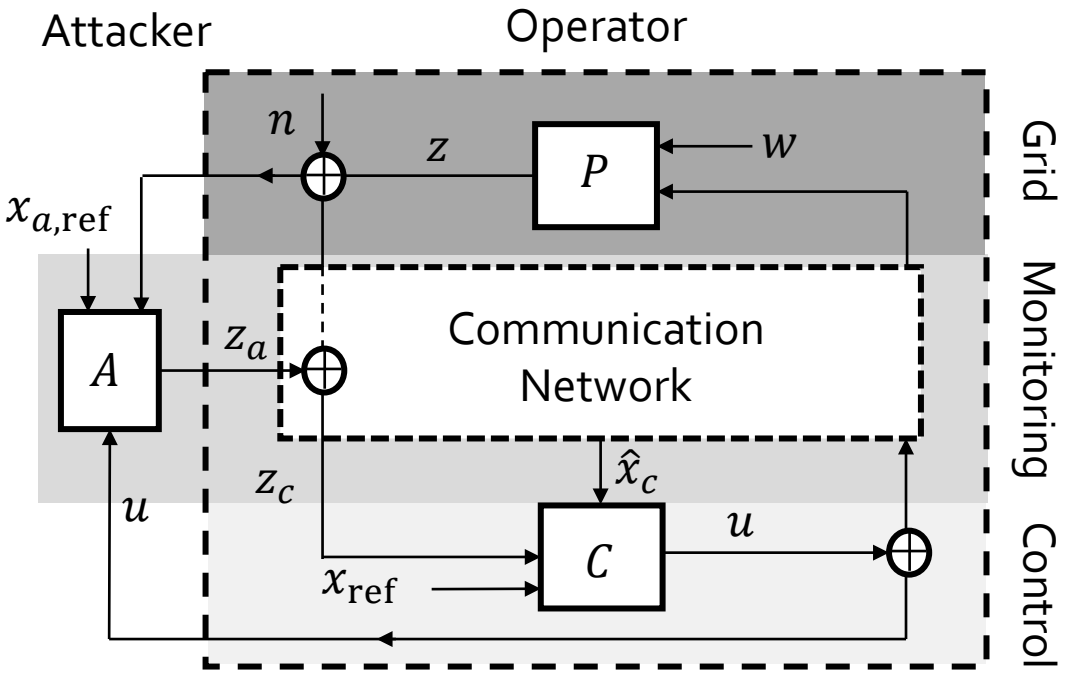


w system disturbance
n measurement noise
u operation command
z true measurement

z_a attacking measurement
z_c corrupted measurement
$\hat{x}_c$ corrupted estimated state
x_{ref} operator's desired state
$x_{a,\text{ref}}$ attacker's desired state

Motivation

- Measurement attacks
  - Model I: Covert control actions
  - Model II: Disabled alarms
  - Model III: State estimator cheater
    - inject false measurements that can bypass the detection of state estimators [Liu & Ning, 2011], [Kim & Tong, 2014], [Li & Scaglione, 2013]

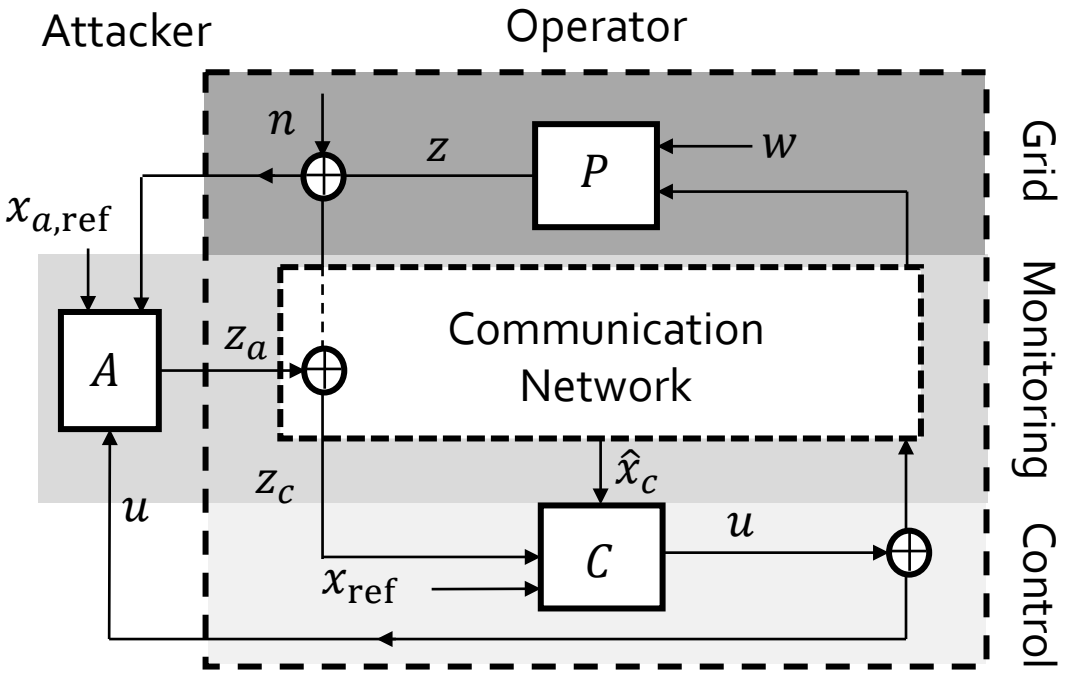


w system disturbance
n measurement noise
u operation command
z true measurement

z_a attacking measurement
z_c corrupted measurement
$\hat{x}_c$ corrupted estimated state
x_{ref} operator's desired state
$x_{a,\mathrm{ref}}$ attacker's desired state

Motivation

- Measurement attacks
  - Model I: Covert control actions
  - Model II: Disabled alarms
  - Model III: State estimator cheater → Monitoring Layer (ML) attack
- (**ML attacks**) inject falsified measurements $\boldsymbol{z_a}$ to *manipulate* decision-making processes $\boldsymbol{u}$ to accomplish the attacking goal $\boldsymbol{x}_{\mathrm{a,ref}}$.

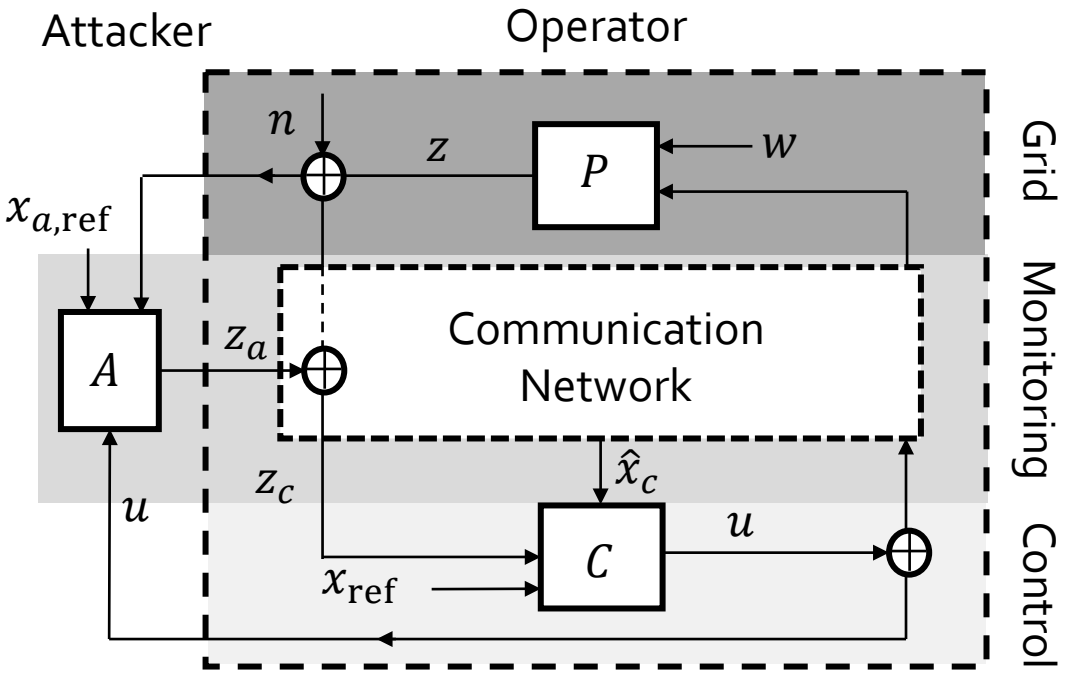


w system disturbance
n measurement noise
u operation command
z true measurement

z_a attacking measurement
z_c corrupted measurement
$\hat{x}_c$ corrupted estimated state
x_{ref} operator's desired state
$x_{a,\mathrm{ref}}$ attacker's desired state

Motivation

- Existing studies' methodology:
  - $\max|\boldsymbol{z} - \boldsymbol{z_a}|_p$.
- Deficiency:
  - An attacker's goal would not be injecting maximum erroneous measurements, but causing intended physical consequences on the grid.
- Research Goal: investigating models of ML attacks based on an attacker's motivation



w system disturbance
n measurement noise
u operation command
z true measurement

z_a attacking measurement
z_c corrupted measurement
$\hat{x}_c$ corrupted estimated state
x_{ref} operator's desired state
$x_{a,\text{ref}}$ attacker's desired state

Outline

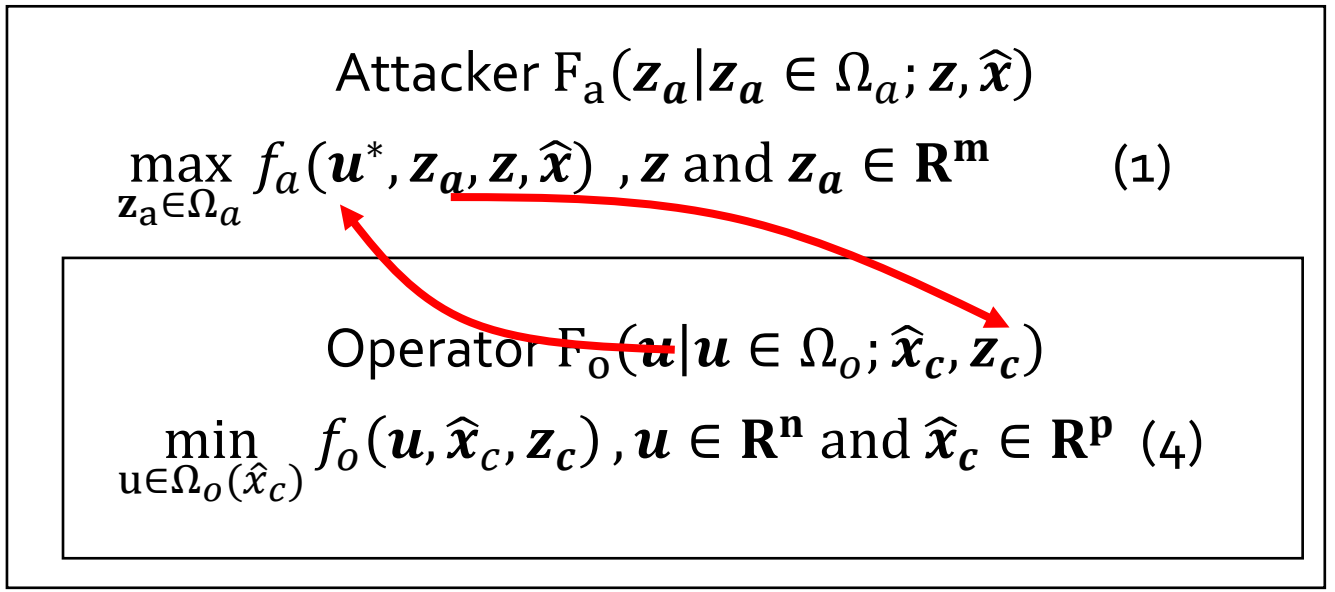
- ~~Motivation~~
- Methodology
- Numerical examples
- Implications

Methodology

- Attacking principle:
  - (**ML attacks**) inject falsified measurements $\boldsymbol{z_a}$ to *manipulate* decision-making processes $\boldsymbol{u}$ to accomplish the attacking goal $\boldsymbol{x}_{\mathrm{a,ref}}$.
- Problem statement:
  - Find $\boldsymbol{z_a}$ (on monitoring layer) that induces $\boldsymbol{u}$ (on control layer) that results $\boldsymbol{x}_{\mathrm{a,ref}}$ (on grid).
- Challenge: complex system
  - Large set of variables
  - Grid dynamics

Methodology

- Assumption:
  - one-step false measurement injection (zero-day attack).
  - Operation objective under manipulation is known.
- Problem form:
  - Bi-level optimization
  - corrupted measurement $\boldsymbol{z_c}$
    - $\boldsymbol{z_c} = \boldsymbol{z} + \boldsymbol{z_a}$
  - Manipulated decision $\boldsymbol{u}^*$
    - $\boldsymbol{u}^* = \arg\left\{\min_{\mathrm{u}} f_o(\boldsymbol{u}, \hat{\boldsymbol{x}}_c)\right\}$



Methodology

- Problem structure
  - Attacker's feasible set $\Omega_a(\boldsymbol{z})$
    - attacker's accessibility to the network and condition to bypass bad data detection in SCADA and EMS
  - Conditions defined in prior works [Liu and Ning, 2011]:
    - Scenario I- Limited access to meters.
    - Scenario II-Limited resources available to compromise meters.

$$\textbf{Attacker } \mathrm{F_a}(\boldsymbol{z_a}|\boldsymbol{z_a} \in \Omega_a; \boldsymbol{z}, \hat{\boldsymbol{x}})$$

$$\max_{\mathbf{z_a} \in \Omega_a} f_a(\boldsymbol{u}^*, \boldsymbol{z_a}, \boldsymbol{z}, \hat{\boldsymbol{x}}) \text{ , } \boldsymbol{z} \text{ and } \boldsymbol{z_a} \in \mathbf{R^m} \quad (1)$$

$$\textbf{Operator } \mathrm{F_o}(\boldsymbol{u}|\boldsymbol{u} \in \Omega_o; \hat{\boldsymbol{x}}_c, \boldsymbol{z}_c)$$

$$\min_{\mathrm{u} \in \Omega_o(\hat{x}_c)} f_o(\boldsymbol{u}, \hat{\boldsymbol{x}}_c, \boldsymbol{z}_c), \boldsymbol{u} \in \mathbf{R^n} \text{ and } \hat{\boldsymbol{x}}_c \in \mathbf{R^p} \quad (4)$$

Methodology

- Problem structure
  - Operator's feasible set $\Omega_o(\hat{\boldsymbol{x}}_c, \boldsymbol{z}_c)$
    - operation feasible region defined by system states
    - E.g. security constrained optimal power flow.

$$\textbf{Attacker } \mathrm{F_a}(\boldsymbol{z_a} | \boldsymbol{z_a} \in \Omega_a; \boldsymbol{z}, \hat{\boldsymbol{x}})$$

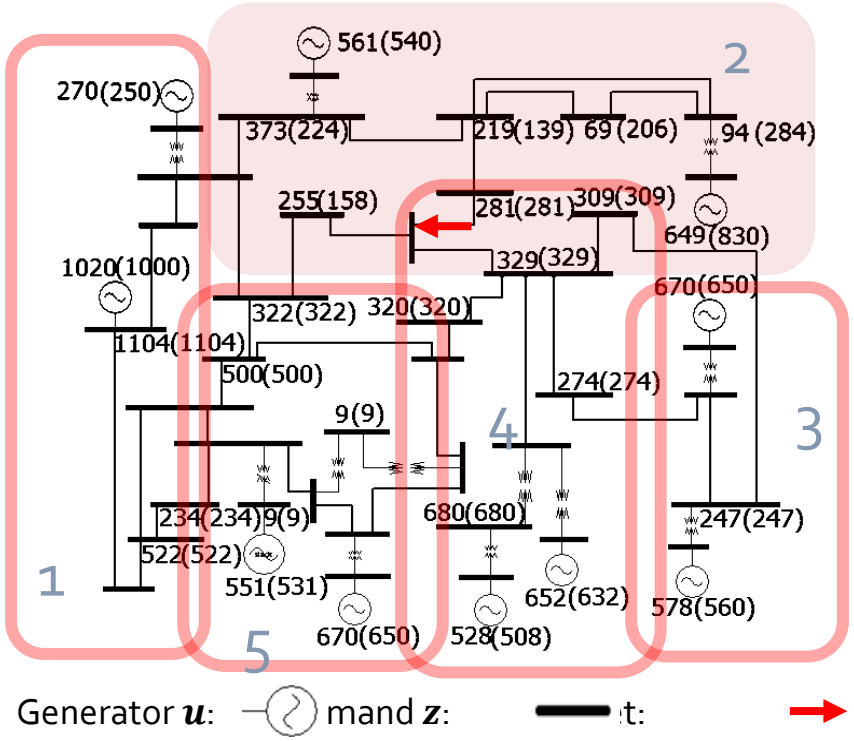
$$\max_{\mathbf{z_a} \in \Omega_a} f_a(\boldsymbol{u}^*, \boldsymbol{z_a}, \boldsymbol{z}, \hat{\boldsymbol{x}}) \ , \boldsymbol{z} \text{ and } \boldsymbol{z_a} \in \mathbf{R^m} \qquad (1)$$

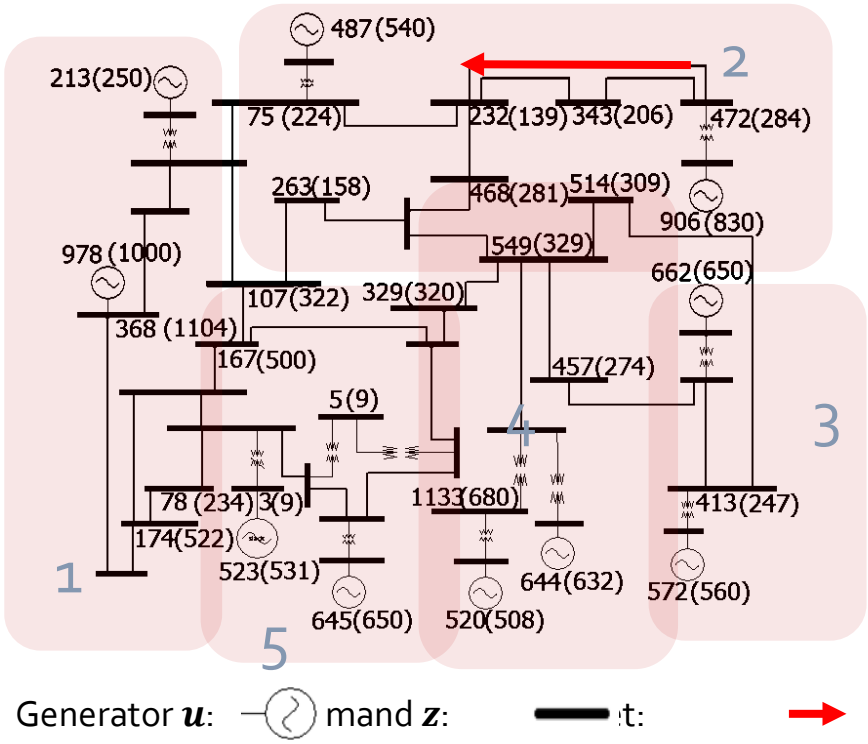
$$\textbf{Operator } \mathrm{F_o}(\boldsymbol{u} | \boldsymbol{u} \in \Omega_o; \hat{\boldsymbol{x}}_c, \boldsymbol{z}_c)$$

$$\min_{\mathrm{u} \in \Omega_o(\hat{x}_c)} f_o(\boldsymbol{u}, \hat{\boldsymbol{x}}_c, \boldsymbol{z}_c), \boldsymbol{u} \in \mathbf{R^n} \text{ and } \hat{\boldsymbol{x}}_c \in \mathbf{R^p} \quad (4)$$

Numerical Example I

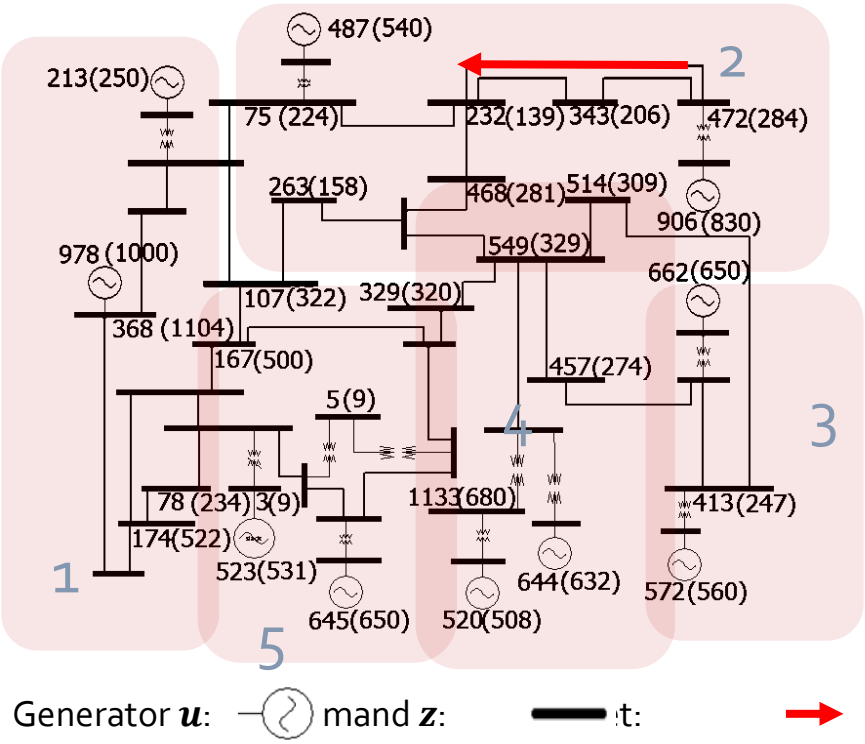
- IEEE 39-bus system, 5 substations
  - **Attacker's goal:** Congest transmission lines
  - **Manipulated operation:** security constrained OPF
  - $\boldsymbol{z}, \boldsymbol{u}(MW)$





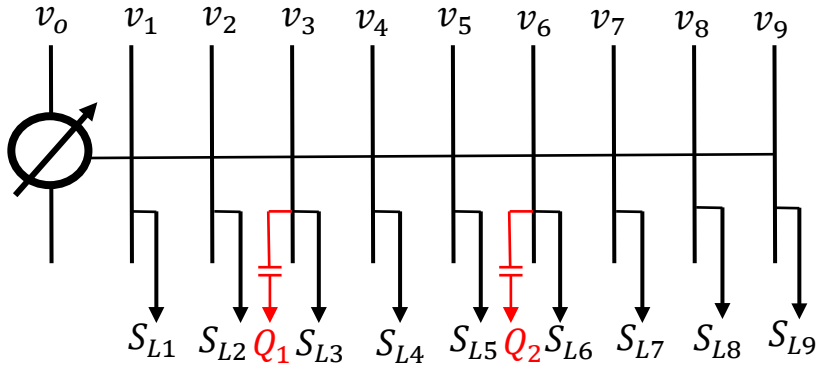
Numerical Example I

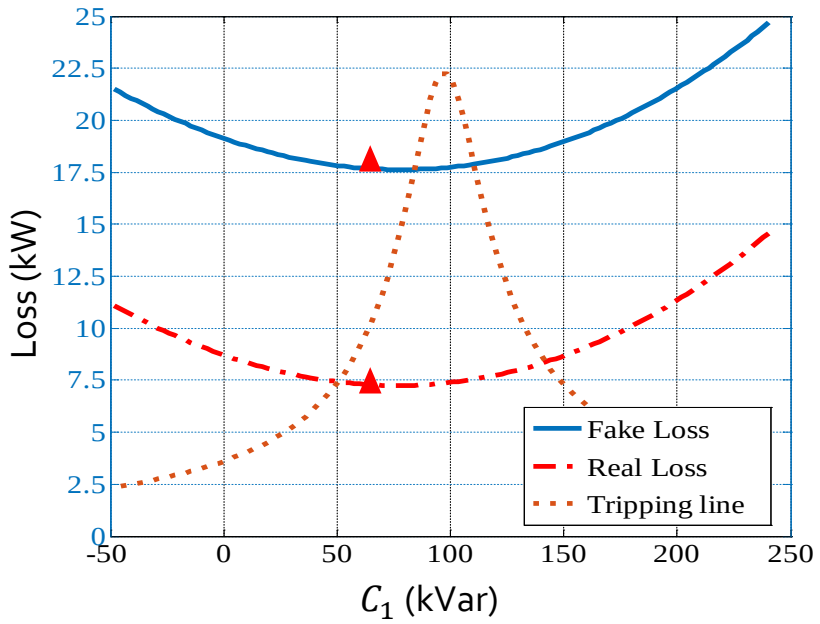
- Implication
  - No guarantee that a Play Safe [in game theory] operation strategy is always available (versus [Zhu, 2011]).
  - The correlation pattern of attacks depends on the system topology and original bus power injections.

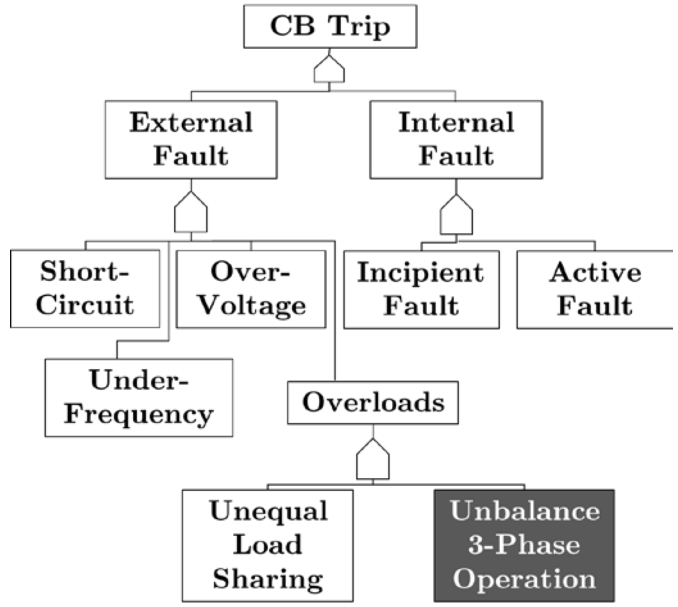


Numerical Example II

- Radial distribution system (IEEE-9 bus system)
  - **Attacker's goal:** disrupting regional supply
  - **Manipulated operation**: Volt/Var management on the distribution system.
- Attacking outlet:
  - Tripping protection on substation transformer.

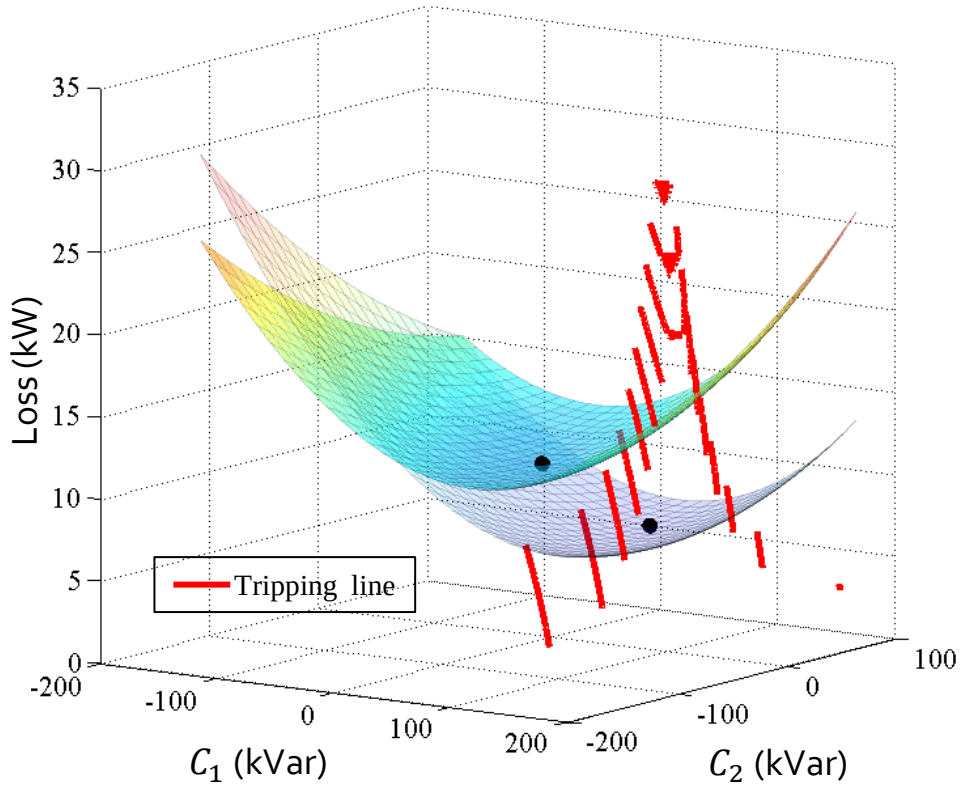






Numerical Example II

- Implications
  - Attack can be defended by trading off operation goals.
  - Effective trading off can be found (indicated by dual variables in the example).



Questions?

Wang.6536@osu.edu