SAND2021-11823C

SECURE

Science and **E**ngineering of **C**yber security through **U**ncertainty quantification and **R**igorous **E**xperimentation

Trilevel Programming for Network Segmentation of Power System Cyber-Physical System

Team Members

Bryan Arguello (presenter)

Jared Gearhart

Cynthia Phillips

Georgia Tech Collaborators

Emma Johnson

Santanu Dey

Rutgers University Collaborator

Jonathan Eckstein

U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

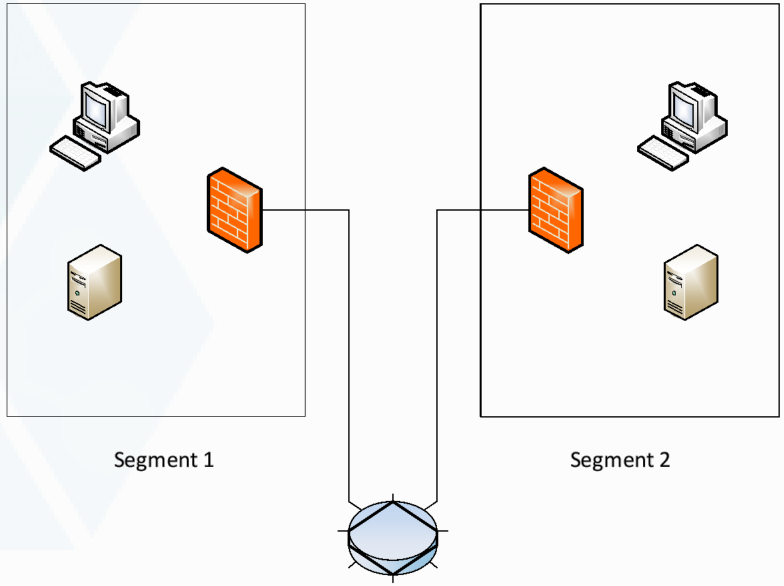
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Outline

- Motivation
- Model Description
- Solution Technique
- 9-Bus and 30 Bus Results
- Larger Cyber-Physical Systems

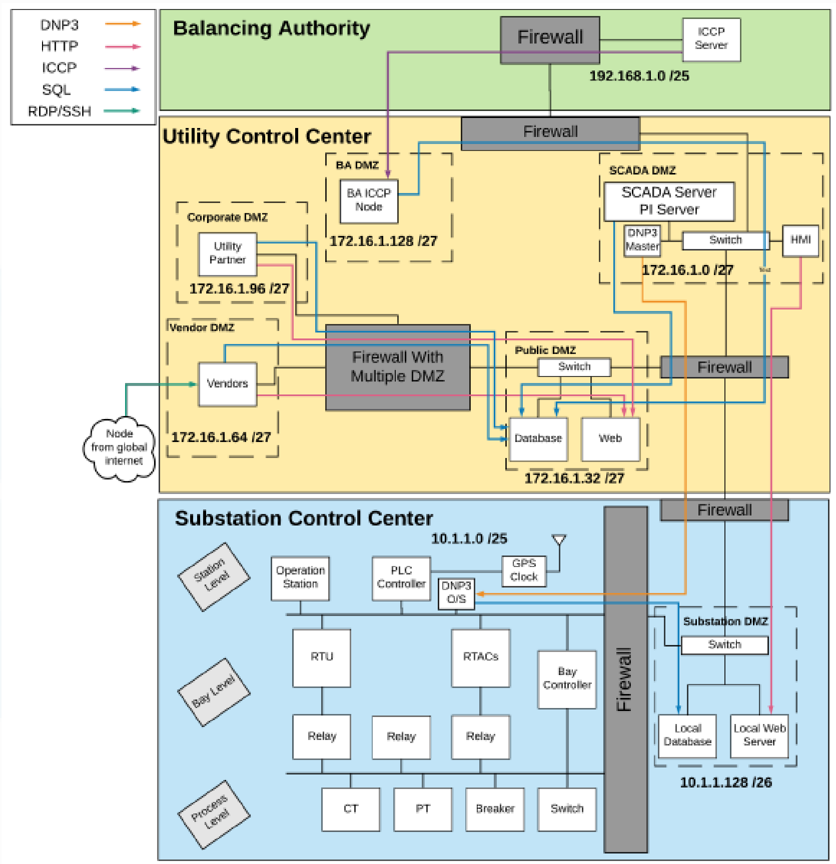
Network Segmentation

- Network segmentation involves
  - **dividing** a network into a set of sub-networks and
  - **enforcing communication rules** among network devices
- Improves security by limiting an attackers ability to pivot between workstations on network



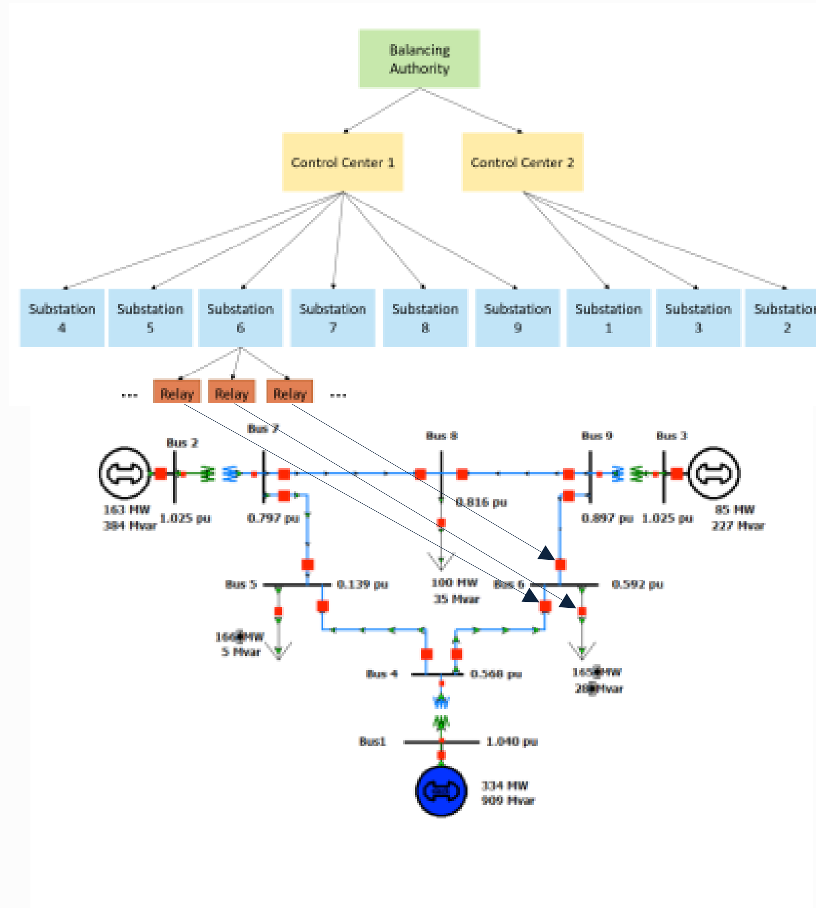
Power System Cyber-Physical Network

SCADA System



Gaudet, Nastassja, et al. "Firewall Configuration and Path Analysis for SmartGrid Networks." 2020 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR). IEEE, 2020.

Cyber-Physical Model



Outline

- Motivation
- Model Description
- Solution Technique
- 9-Bus and 30 Bus Results
- Larger Cyber-Physical Systems

Cyber-Physical Network Segmentation

Defender segments the SCADA system to limit the scope of the attacker

Operator observes the attack and redispatches power to minimize load shed

$$\min_{(x,y,q,t)\in\mathcal{D}} \max_{(\delta,z,u,v,w)\in\mathcal{A}(x,y)} \min_{(\theta,f,p,l)\in\mathcal{O}(u,v,w)} \sum_{d\in\mathcal{L}} l_d$$

Attacker attacks up to *N* segments on the defender-segmented SCADA and disables relays in compromised substations.

Rules

- Leaders make decisions in anticipation of optimal follower decisions
- Followers must adhere to decisions made by leaders

Network Segmentation Model

$$\mathcal{D}$$

$$\sum_{r \in \mathcal{R}} x_{e,r} \geq 1, \qquad \forall e \in \mathcal{E}(\mathcal{S}) \tag{2}$$

$$\sum_{e \in \mathcal{E}(\mathcal{S})} x_{e,r} = 1, \qquad \forall r \in \mathcal{R} \tag{3}$$

$$q_{s,e} \leq \sum_{r \in \mathcal{R}_s} x_{e,r}, \qquad \forall s \in \mathcal{S}, e \in \mathcal{E}_1(\mathcal{S}) \tag{4}$$

$$q_{s,e} \geq x_{e,r}, \qquad \forall s \in \mathcal{S}, r \in \mathcal{R}_s, e \in \mathcal{E}_1(\mathcal{S}) \tag{5}$$

$$Q_{s,e} \leq \sum_{r \in \mathcal{R}_s} x_{e,r}, \qquad \forall s \in \mathcal{S}, e \in \mathcal{E}_0(\mathcal{S}) \tag{6}$$

$$Q_{s,e} \geq x_{e,r}, \qquad \forall s \in \mathcal{S}, r \in \mathcal{R}_s, e \in \mathcal{E}_0(\mathcal{S}) \tag{7}$$

$$\sum_{e \in \mathcal{E}(A)} y_{e,f} = 1, \qquad \forall (A,B) \in \mathcal{Z}, f \in \mathcal{E}(B) \tag{8}$$

$$\sum_{n \in T} q_{n,e} = 1, \qquad \forall T \in \mathcal{T}, e \in \mathcal{E}_1(T) \tag{9}$$

$$t_{e,n} \leq \sum_{f \in \mathcal{E}_0(B)} y_{e,f} Q_{n,f} + \sum_{f \in \mathcal{E}_1(B)} y_{e,f} q_{n,f}, \quad \forall (A,B) \in \mathcal{Z}, e \in \mathcal{E}(A), n \in B \tag{10}$$

$$t_{e,n} \geq y_{e,f} Q_{n,f}, \qquad \forall (A,B) \in \mathcal{Z}, e \in \mathcal{E}(A), n \in B, f \in \mathcal{E}_0(B) \tag{11}$$

$$t_{e,n} \geq y_{e,f} q_{n,f}, \qquad \forall (A,B) \in \mathcal{Z}, e \in \mathcal{E}(A), n \in B, f \in \mathcal{E}_1(B) \tag{12}$$

$$t_{e,n} \leq Q_{m,e}, \qquad \forall (A,B) \in \mathcal{Z}, e \in \mathcal{E}_0(A), m \in A, n \in B_m \tag{13}$$

$$t_{e,n} \leq q_{m,e}, \qquad \forall (A,B) \in \mathcal{Z}, e \in \mathcal{E}_1(A), m \in A, n \in B_m \tag{14}$$

$$y_{e,f} \in \{0,1\}, \forall (e,f) \in (\mathcal{E}(\mathcal{C}) \times \mathcal{E}(\mathcal{S})) \cup (\mathcal{E}(\mathcal{B}) \times \mathcal{E}(\mathcal{C})) \tag{15}$$

$$x_{e,r} \in \{0,1\}, \qquad e \in \mathcal{E}(\mathcal{S}), \forall r \in \mathcal{R} \tag{16}$$

$$q_{n,e} \in \{0,1\}, \qquad \forall (n,e) \in \cup_{T \in \mathcal{T}} (T \times \mathcal{E}_1(T)) \tag{17}$$

$$t_{e,n} \in \{0,1\}, \quad \forall (e,n) \in (\mathcal{E}(\mathcal{C}) \times \mathcal{S}) \cup (\mathcal{E}(\mathcal{B}) \times \mathcal{C}) \tag{18}$$

Designer assignment model

$$\mathcal{A}(x,y)$$

$$\sum_{e \in \mathcal{E}} z_e \leq U \tag{22}$$

$$z_f \leq \sum_{e \in \mathcal{E}(A)} y_{e,f} z_e, \qquad \forall (A,B) \in \mathcal{Z}, \forall f \in \mathcal{E}(B) \tag{23}$$

$$\delta_r = \sum_{e \in \mathcal{E}(\mathcal{S})} x_{e,r} z_e, \qquad \forall r \in \mathcal{R} \tag{24}$$

$$v_k \leq (1 - \delta_r), \qquad \forall k \in \mathcal{K}, r \in \mathcal{R}_k \tag{25}$$

$$v_k \geq \sum_{r \in \mathcal{R}_k} (1 - \delta_r) - |\mathcal{R}_k| + 1, \qquad \forall k \in \mathcal{K} \tag{26}$$

$$w_g \leq (1 - \delta_r), \qquad \forall g \in \mathcal{G}, r \in \mathcal{R}_g \tag{27}$$

$$w_g \geq \sum_{r \in \mathcal{R}_g} (1 - \delta_r) - |\mathcal{R}_g| + 1, \qquad \forall g \in \mathcal{G} \tag{28}$$

$$u_d \leq (1 - \delta_r), \qquad \forall d \in \mathcal{L}, r \in \mathcal{R}_d \tag{29}$$

$$u_d \geq \sum_{r \in \mathcal{R}_d} (1 - \delta_r) - |\mathcal{R}_d| + 1, \qquad \forall d \in \mathcal{L} \tag{30}$$

Attacker precedence-based selection model

$$\mathcal{O}(u,v,w)$$

$$\sum_{k \in \{k' | d(k') = s\}} f_k - \sum_{k \in \{k' | o(k') = s\}} f_k + \sum_{g \in \mathcal{G}_s} p_g = \sum_{d \in \mathcal{L}_s} (D_d - l_d) \qquad \forall s \in \mathcal{S} \tag{31}$$

$$f_k = B_k v_k (\theta_{o(k)} - \theta_{d(k)} - \Theta_k) \qquad \forall k \in \mathcal{K} \tag{32}$$

$$-\overline{F}_k \leq f_k \leq \overline{F}_k \qquad \forall k \in \mathcal{K} \tag{33}$$

$$0 \leq p_g \leq w_g \overline{P}_g \qquad \forall g \in \mathcal{G} \tag{34}$$

$$(1 - u_d) D_d \leq l_d \leq D_d \qquad \forall d \in \mathcal{L} \tag{35}$$

$$-\pi \leq \theta_s \leq \pi \qquad \forall s \in \mathcal{S} \tag{36}$$

DCOPF operator model

Network Segmentation Model

$$\mathcal{D}$$

$$\sum_{r \in \mathcal{R}} x_{e,r} \geq 1, \qquad \forall e \in \mathcal{E}(\mathcal{S}) \tag{2}$$

$$\sum_{e \in \mathcal{E}(\mathcal{S})} x_{e,r} = 1, \qquad \forall r \in \mathcal{R} \tag{3}$$

$$q_{s,e} \leq \sum_{r \in \mathcal{R}_s} x_{e,r}, \qquad \forall s \in \mathcal{S}, e \in \mathcal{E}_1(\mathcal{S}) \tag{4}$$

$$q_{s,e} \geq x_{e,r}, \qquad \forall s \in \mathcal{S}, r \in \mathcal{R}_s, e \in \mathcal{E}_1(\mathcal{S}) \tag{5}$$

$$Q_{s,e} \leq \sum_{r \in \mathcal{R}_s} x_{e,r}, \qquad \forall s \in \mathcal{S}, e \in \mathcal{E}_0(\mathcal{S}) \tag{6}$$

$$Q_{s,e} \geq x_{e,r}, \qquad \forall s \in \mathcal{S}, r \in \mathcal{R}_s, e \in \mathcal{E}_0(\mathcal{S}) \tag{7}$$

$$\sum_{e \in \mathcal{E}(A)} y_{e,f} = 1, \qquad \forall (A,B) \in \mathcal{Z}, f \in \mathcal{E}(B) \tag{8}$$

$$\sum_{n \in T} q_{n,e} = 1, \qquad \forall T \in \mathcal{T}, e \in \mathcal{E}_1(T) \tag{9}$$

$$t_{e,n} \leq \sum_{f \in \mathcal{E}_0(B)} y_{e,f} Q_{n,f} + \sum_{f \in \mathcal{E}_1(B)} y_{e,f} q_{n,f}, \quad \forall (A,B) \in \mathcal{Z}, e \in \mathcal{E}(A), n \in B \tag{10}$$

$$t_{e,n} \geq y_{e,f} Q_{n,f}, \qquad \forall (A,B) \in \mathcal{Z}, e \in \mathcal{E}(A), n \in B, f \in \mathcal{E}_0(B) \tag{11}$$

$$t_{e,n} \geq y_{e,f} q_{n,f}, \qquad \forall (A,B) \in \mathcal{Z}, e \in \mathcal{E}(A), n \in B, f \in \mathcal{E}_1(B) \tag{12}$$

$$t_{e,n} \leq Q_{m,e}, \qquad \forall (A,B) \in \mathcal{Z}, e \in \mathcal{E}_0(A), m \in A, n \in B_m \tag{13}$$

$$t_{e,n} \leq q_{m,e}, \qquad \forall (A,B) \in \mathcal{Z}, e \in \mathcal{E}_1(A), m \in A, n \in B_m \tag{14}$$

$$y_{e,f} \in \{0,1\}, \forall (e,f) \in (\mathcal{E}(\mathcal{C}) \times \mathcal{E}(\mathcal{S})) \cup (\mathcal{E}(\mathcal{B}) \times \mathcal{E}(\mathcal{C})) \tag{15}$$

$$x_{e,r} \in \{0,1\}, \qquad e \in \mathcal{E}(\mathcal{S}), \forall r \in \mathcal{R} \tag{16}$$

$$q_{n,e} \in \{0,1\}, \qquad \forall (n,e) \in \cup_{T \in \mathcal{T}} (T \times \mathcal{E}_1(T)) \tag{17}$$

$$t_{e,n} \in \{0,1\}, \quad \forall (e,n) \in (\mathcal{E}(\mathcal{C}) \times \mathcal{S}) \cup (\mathcal{E}(\mathcal{B}) \times \mathcal{C}) \tag{18}$$

Designer assignment model

$$\mathcal{A}(x,y)$$

$$\sum_{e \in \mathcal{E}} z_e \leq U \tag{22}$$

$$z_f \leq \sum_{e \in \mathcal{E}(A)} y_{e,f} z_e, \qquad \forall (A,B) \in \mathcal{Z}, \forall f \in \mathcal{E}(B) \tag{23}$$

$$\delta_r = \sum_{e \in \mathcal{E}(\mathcal{S})} x_{e,r} z_e, \qquad \forall r \in \mathcal{R} \tag{24}$$

$$v_k \leq (1 - \delta_r), \qquad \forall k \in \mathcal{K}, r \in \mathcal{R}_k \tag{25}$$

$$v_k \geq \sum_{r \in \mathcal{R}_k} (1 - \delta_r) - |\mathcal{R}_k| + 1, \qquad \forall k \in \mathcal{K} \tag{26}$$

$$w_g \leq (1 - \delta_r), \qquad \forall g \in \mathcal{G}, r \in \mathcal{R}_g \tag{27}$$

$$w_g \geq \sum_{r \in \mathcal{R}_g} (1 - \delta_r) - |\mathcal{R}_g| + 1, \qquad \forall g \in \mathcal{G} \tag{28}$$

$$u_d \leq (1 - \delta_r), \qquad \forall d \in \mathcal{L}, r \in \mathcal{R}_d \tag{29}$$

$$u_d \geq \sum_{r \in \mathcal{R}_d} (1 - \delta_r) - |\mathcal{R}_d| + 1, \qquad \forall d \in \mathcal{L} \tag{30}$$

Attacker precedence-based selection model

$$\mathcal{O}(u,v,w)$$

$$\sum_{k \in \{k' | d(k')=s\}} f_k - \sum_{k \in \{k' | o(k')=s\}} f_k + \sum_{g \in \mathcal{G}_s} p_g = \sum_{d \in \mathcal{L}_s} (D_d - l_d) \qquad \forall s \in \mathcal{S} \tag{31}$$

$$f_k = B_k v_k (\theta_{o(k)} - \theta_{d(k)} - \Theta_k) \qquad \forall k \in \mathcal{K} \tag{32}$$

$$-\overline{F}_k \leq f_k \leq \overline{F}_k \qquad \forall k \in \mathcal{K} \tag{33}$$

$$0 \leq p_g \leq w_g \overline{P}_g \qquad \forall g \in \mathcal{G} \tag{34}$$

$$(1 - u_d) D_d \leq l_d \leq D_d \qquad \forall d \in \mathcal{L} \tag{35}$$

$$-\pi \leq \theta_s \leq \pi \qquad \forall s \in \mathcal{S} \tag{36}$$

DCOPF operator model

Results in the coming slides will clarify the model

Outline

- Motivation
- Description
- Solution Technique
- 9-Bus and 30 Bus Results
- Larger Cyber-Physical Systems

A Naïve Solution Technique for Small Systems

- Step 1: Linearize bilinear terms using **McCormick Relaxation**

$$z_f \leq \sum_{e \in \mathcal{E}(A)} y_{e,f} z_e \qquad f_k = B_k v_k(\theta_{o(k)} - \theta_{d(k)} - \Theta_k)$$

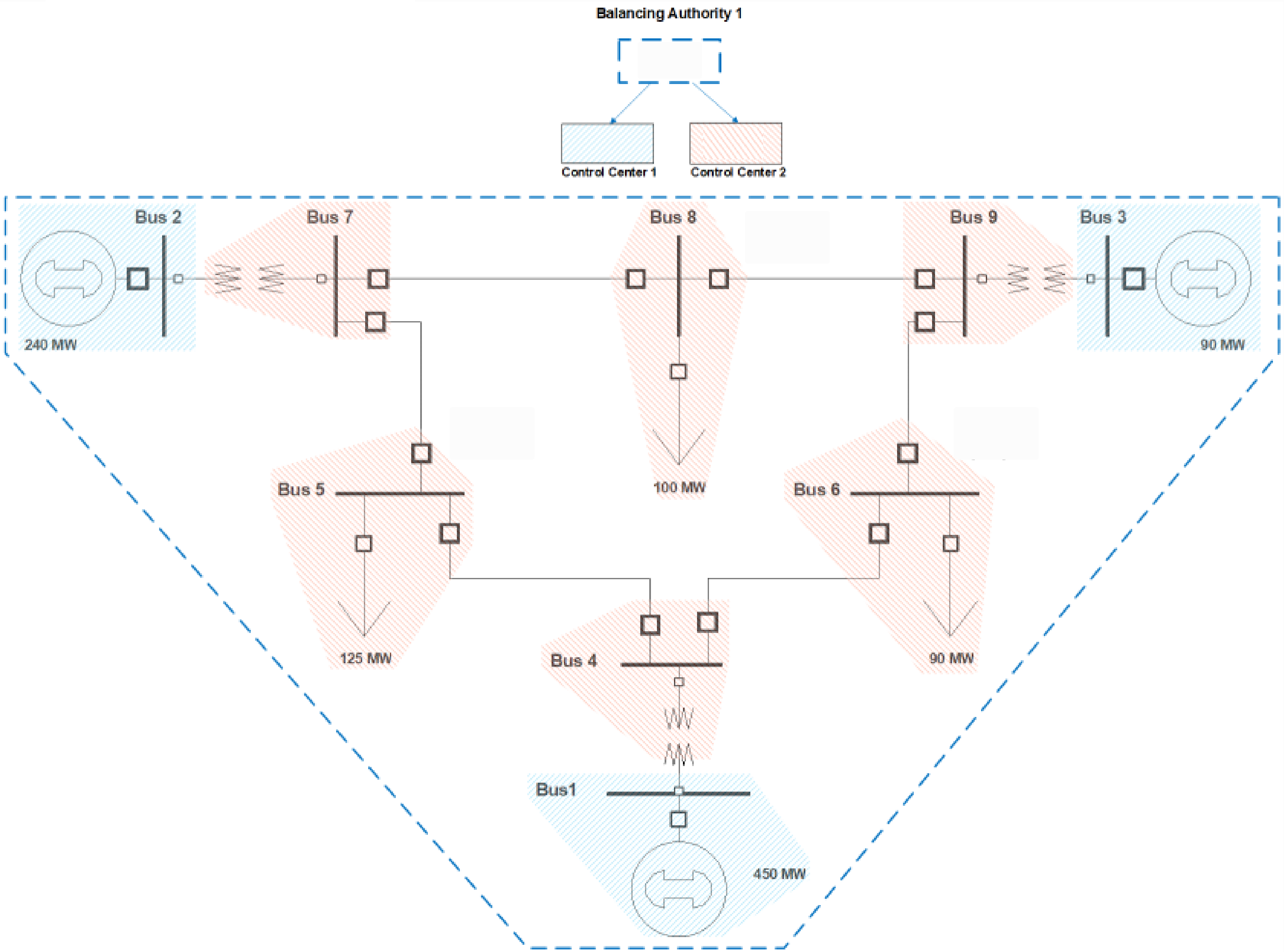
- Step 2: **Dualize** third (operator) model and **reduce** attacker and dualized operator into a single max model, transforming the trilevel model into a bilevel min-max model.
  - Note that the combined max model has binaries, so it cannot be dualized.

- Step 3: Use **bilevel branch-and-bound** to solve mixed bilevel model
  - Apply branch-and-bound to high-point relaxation (constraints from both levels with leader objective) and obtain cuts to remove follow-suboptimal solutions through callbacks.
  - **Fischetti et. al.** has made their CPLEX-based academic solver available for research purposes.
  - MibS is open-source and uses COIN-OR framework.

Outline

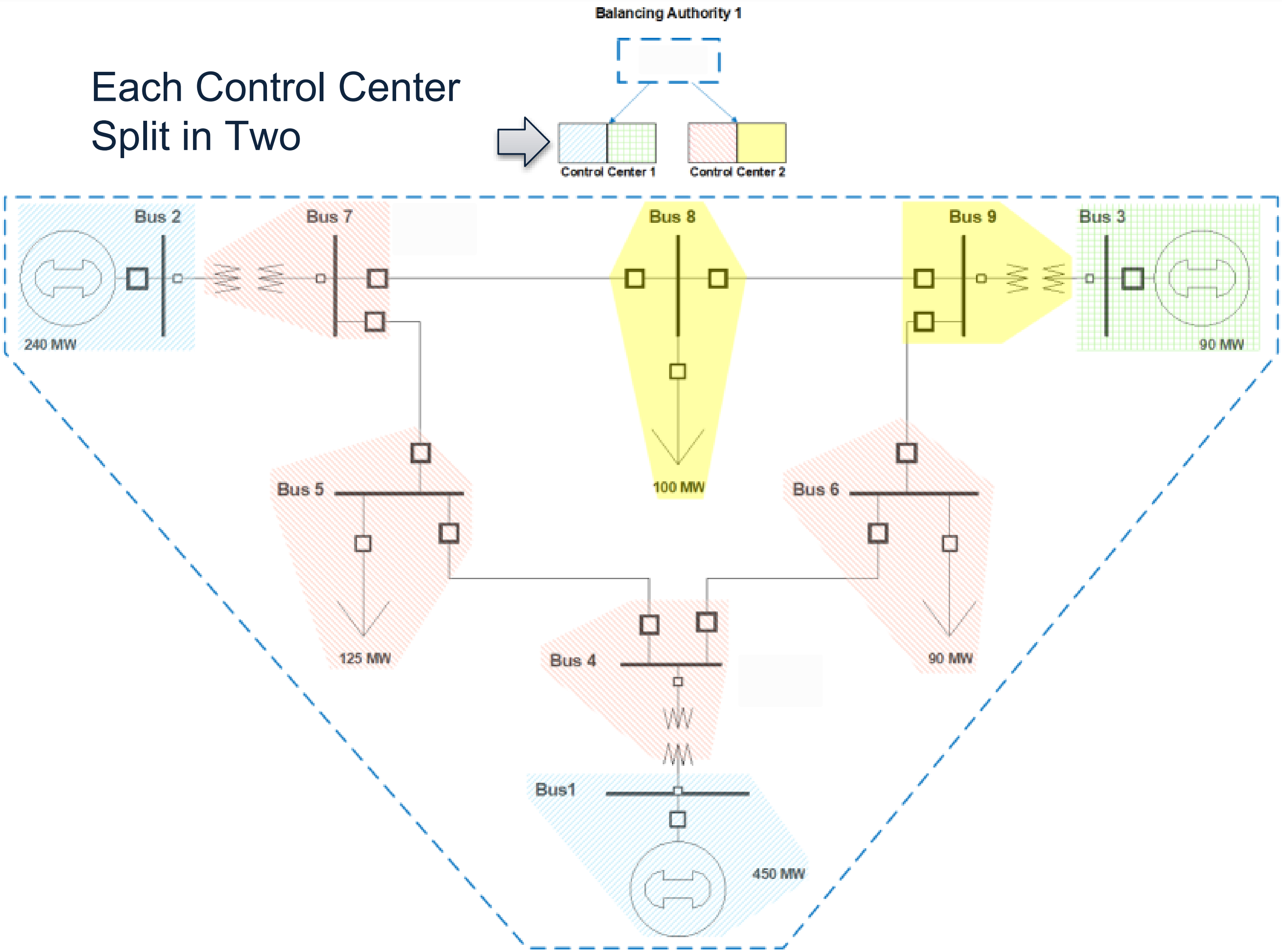
- Motivation
- Model Description
- Solution Technique
- 9-Bus and 30 Bus Results
- Larger Cyber-Physical Systems

9-bus System Before Segmentation

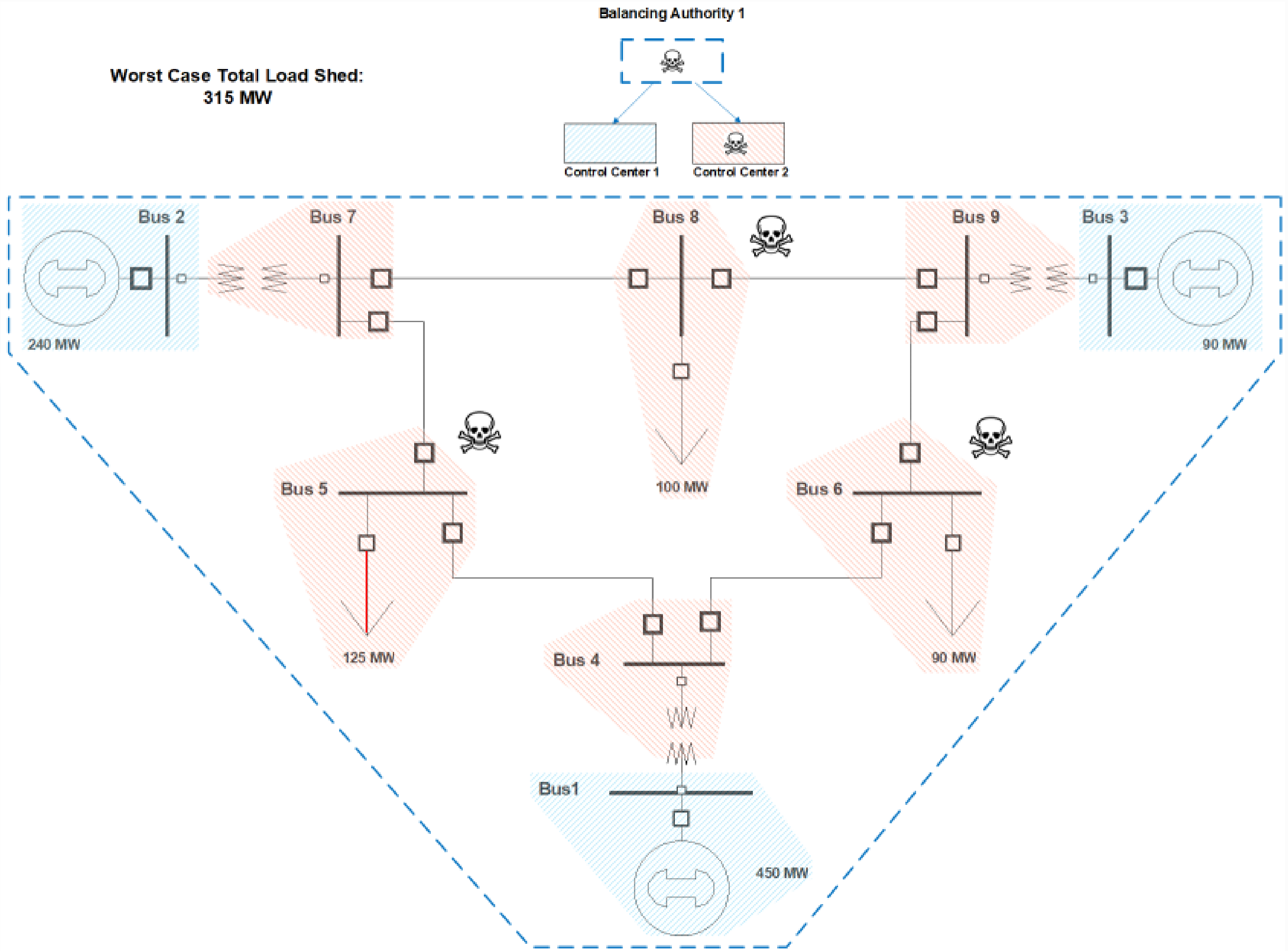


9-bus After Segmentation

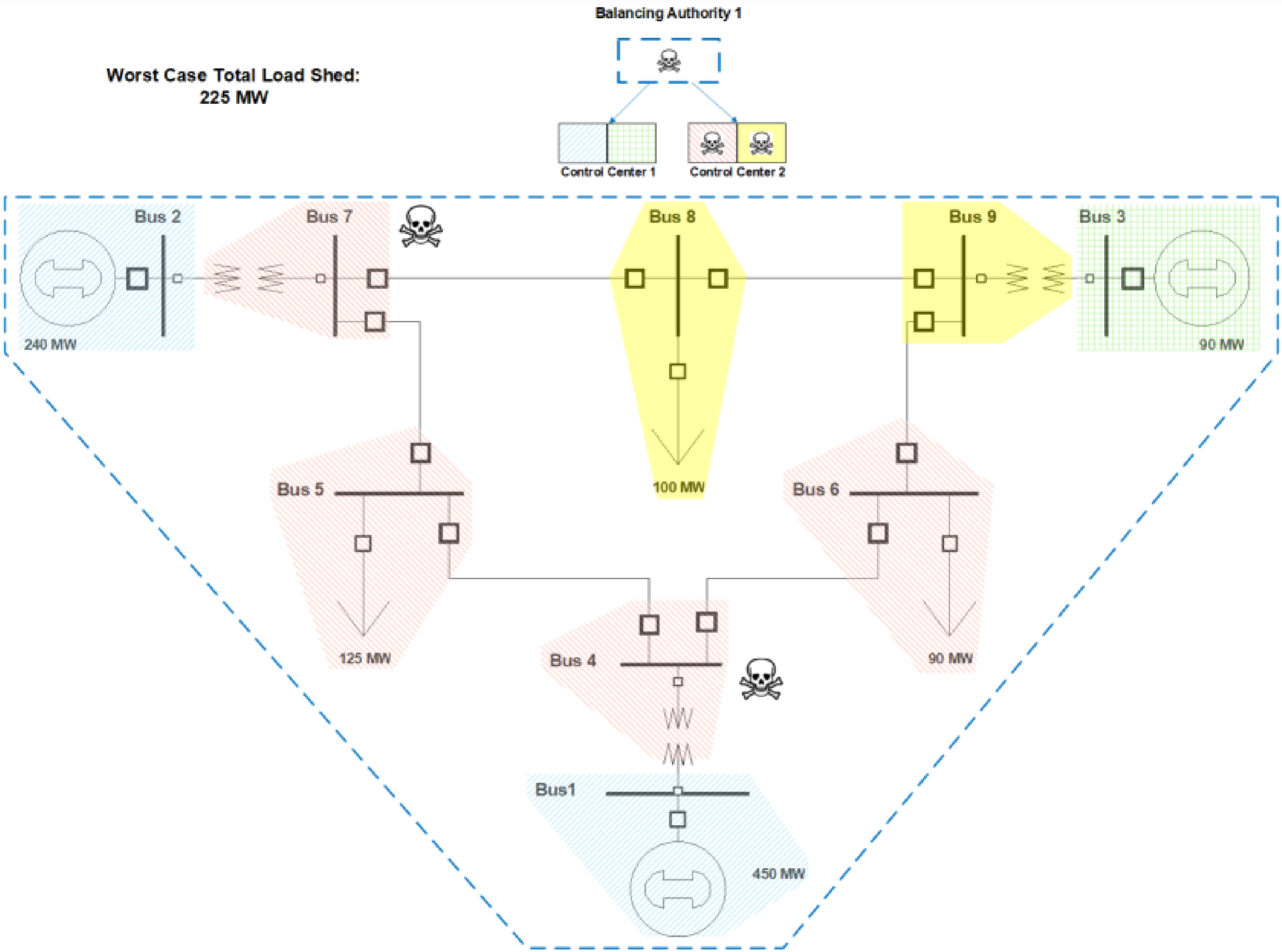
Each Control Center Split in Two



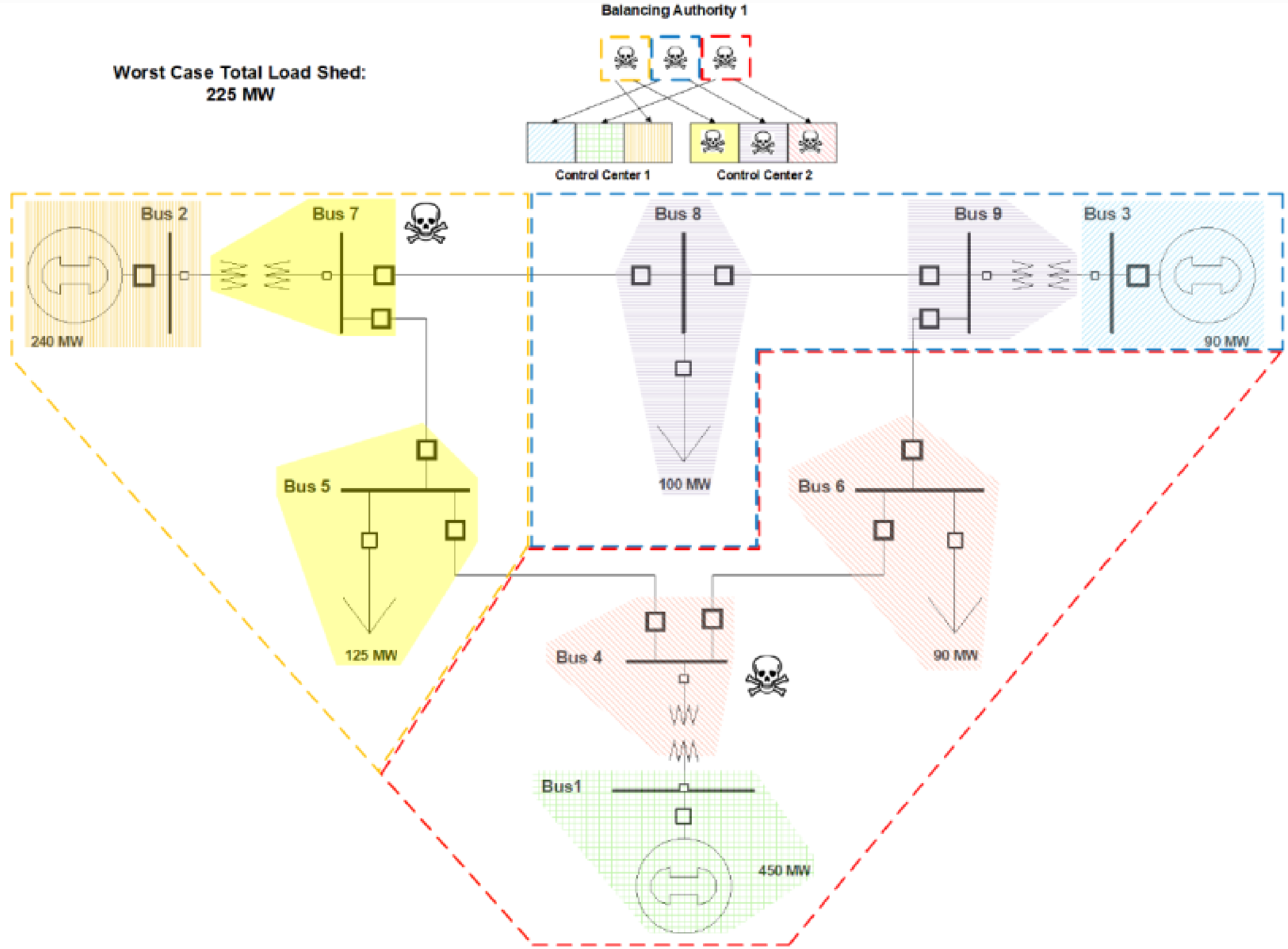
9-bus (Attacker Budget = 5) Before Segmentation



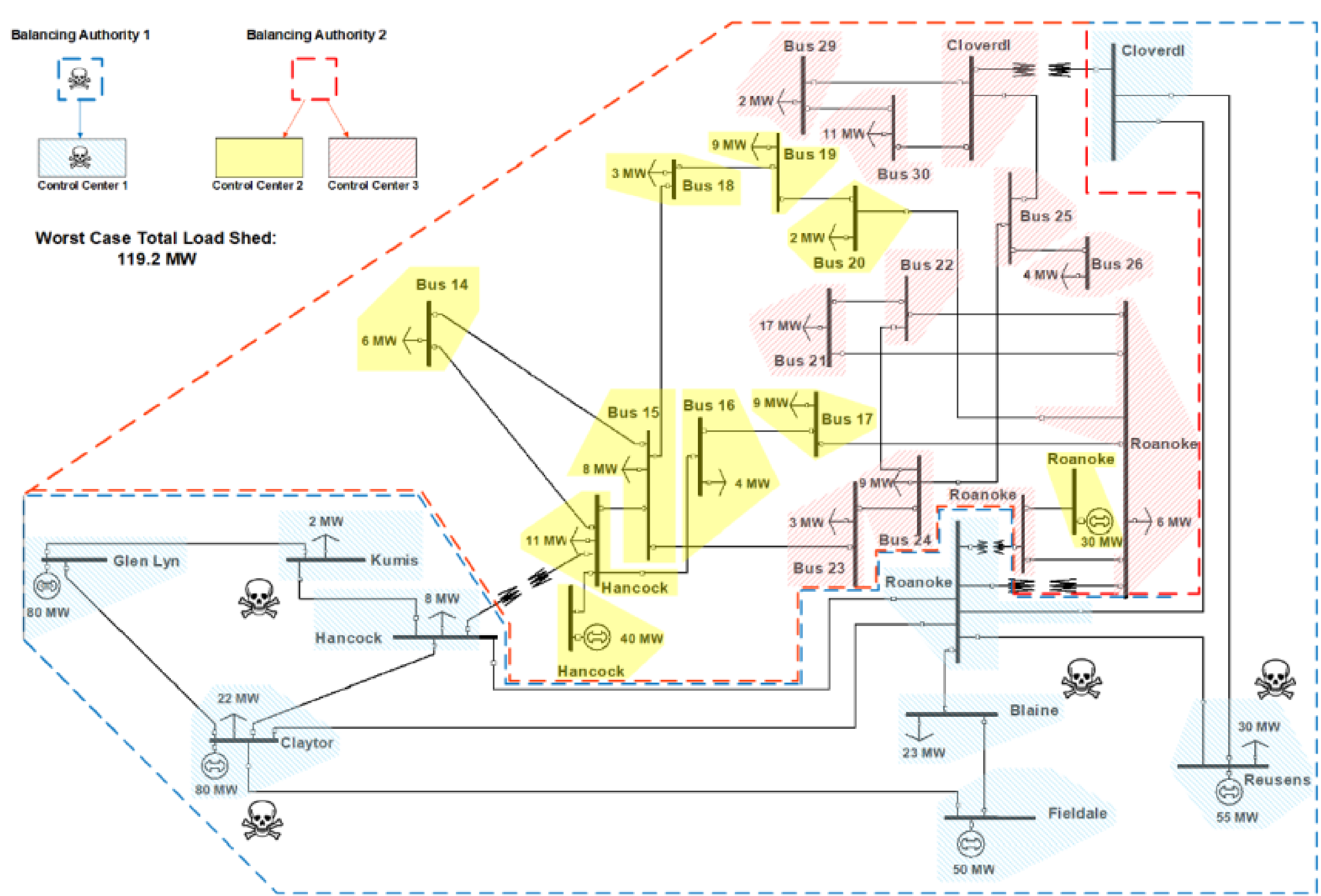
9-bus (Attacker Budget=5) After Segmentation



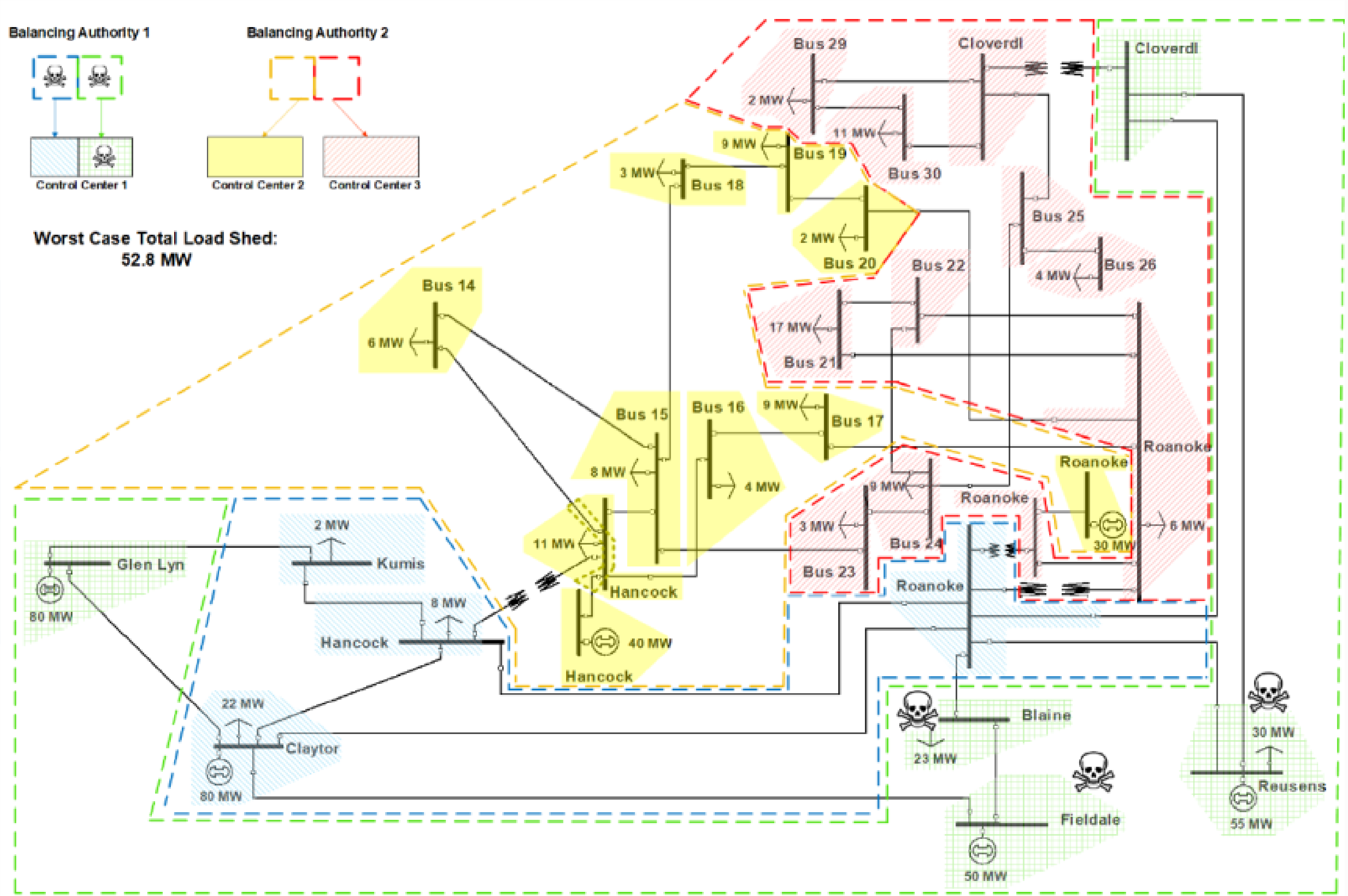
9-bus (Attacker Budget = 8) After Segmentation



30-bus (Attacker Budget = 6) Before Segmentation



30-bus (Attacker Budget = 6) After Segmentation



Outline

- Motivation
- Brief Model Description
- Solution Technique
- 9-Bus and 30 Bus Results
- Larger Cyber-Physical Systems

Scaling to Larger Systems

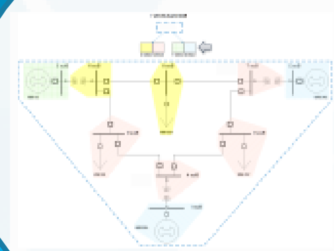
- Bilevel branch-and-bound is ineffective for **interdiction** models.
  - Follower and leader objectives are the same.
  - This leads to **weak dual bounds**.
  - Does not scale well for larger power systems than the 30-bus test case.

- Partnered with Emma Johnson and Santanu Dey (Georgia Tech), Jonathan Eckstein (Rutgers), and Cynthia Phillips (Sandia) to develop **decomposition algorithm for trilevel interdiction**.
  - Based on the **Covering Decomposition Algorithm** for bilevel programming by Israeli and Wood (2002)

A Trilevel Decomposition Algorithm

$$\min_{(x,y,q,t)\in\mathcal{D}} \; \min_{(\theta,f,p,l)\in\mathcal{O}(u,v,w)} \sum_{d\in\mathcal{L}} l_d$$

Network design that can block all discovered worst-case attacks is passed to attacker subproblem



Worst-case attack is returned to master

$$\max_{(\delta,z,u,v,w)\in\mathcal{A}(x,y)}$$

Large-scale Results

- Can solve small instances far more quickly with trilevel decomposition than with the bilevel branch-and-bound approach.

- To further help with scaling, the DC optimal power flow was simplified to **capacitated network flow**
  - Relaxing B-theta constraint has empirically been shown to yield high-quality lower bounds for the inner two problems (Johnson and Dey 2021)
  - Can solve:
    - **500-bus** system with a SCADA system that communicates with the whole grid.
    - **2000-bus** synthetic system with a SCADA system that communicates with 30 buses.

References

- Arguello, B., Johnson, E. S., & Gearhart, J. L. (2021). A Trilevel Model for Segmentation of the Power Transmission Grid Cyber Network. *arXiv preprint arXiv:2108.10958*
- Johnson, E.S., Dey, S.S., Eckstein, J., Phillips, C.A., & Siirola, J.D. (2021). A Covering Decomposition Algorithm for Power Grid Cyber-Network Segmentation. In Review
- Fischetti, M., Ljubić, I., Monaci, M., & Sinnl, M. (2017). A new general-purpose algorithm for mixed-integer bilevel linear programs. *Operations Research*, *65*(6), 1615-1637.
- Tahernejad, S., Ralphs, T. K., & DeNegre, S. T. (2020). A branch-and-cut algorithm for mixed integer bilevel linear optimization problems and its implementation. *Mathematical Programming Computation*, *12*(4), 529-568.
- Motto, A. L., Arroyo, J. M., & Galiana, F. D. (2005). A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat. *IEEE Transactions on Power Systems*, *20*(3), 1357-1365.E. Israeli and R.K. Wood, "Shortest-path network interdiction," *Networks* 40(2): 97-111, 2002
- E.S. Johnson and S.S. Dev. "A scalable lower bound for the worst-case relav attack problem on the transmission grid," Technical report 2105.020801, ArXiv, 2021
- B. Hua. R. Baldick. R.K. Wood. "Interdiction of a mixed-integer linear system," Preprint 2019 -01-7103, Optimization Online, 2019

Thank you!