SAND2023-04388C

Sandia National Laboratories

Exceptional service in the national interest

A Covering Decomposition Algorithm for Power Grid Cyber-Network Segmentation

Emma Johnson, Jonathan Eckstein, Santanu Dey, Cindy Phillips, John Siirola

2023 SIAM Conference on Optimization

Sandia National Laboratories
U.S. DEPARTMENT OF ENERGY NNSA

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.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly artment of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY
NNSA

TRILEVEL INTERDICTION PROBLEM

Network Designer

Minimize load shed

Choose how to divide networks in communication system, respecting communication system structure and investment budgets

Cyber Attacker

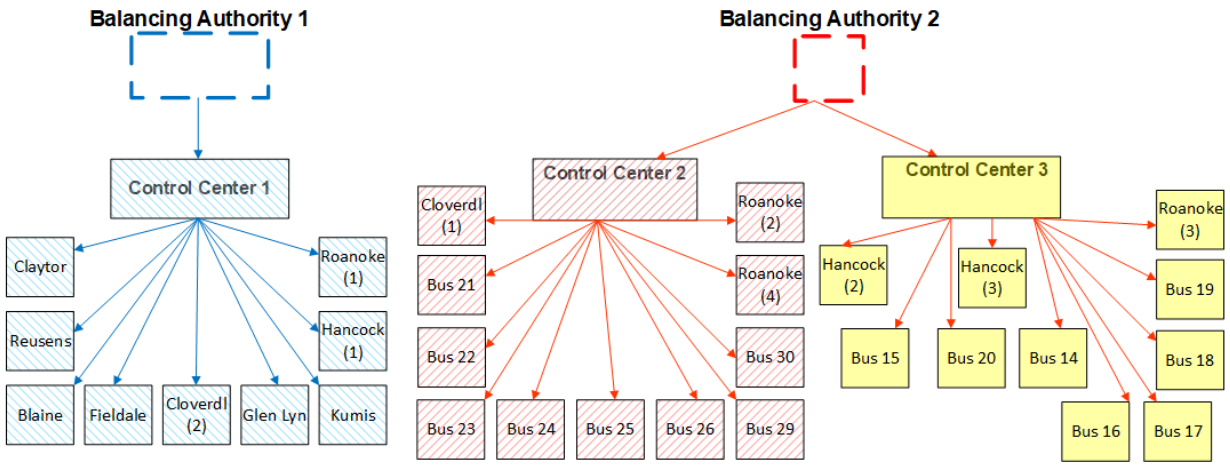
Maximize load shed by attacking subnetworks and compromising all components controlled by relays he accesses.

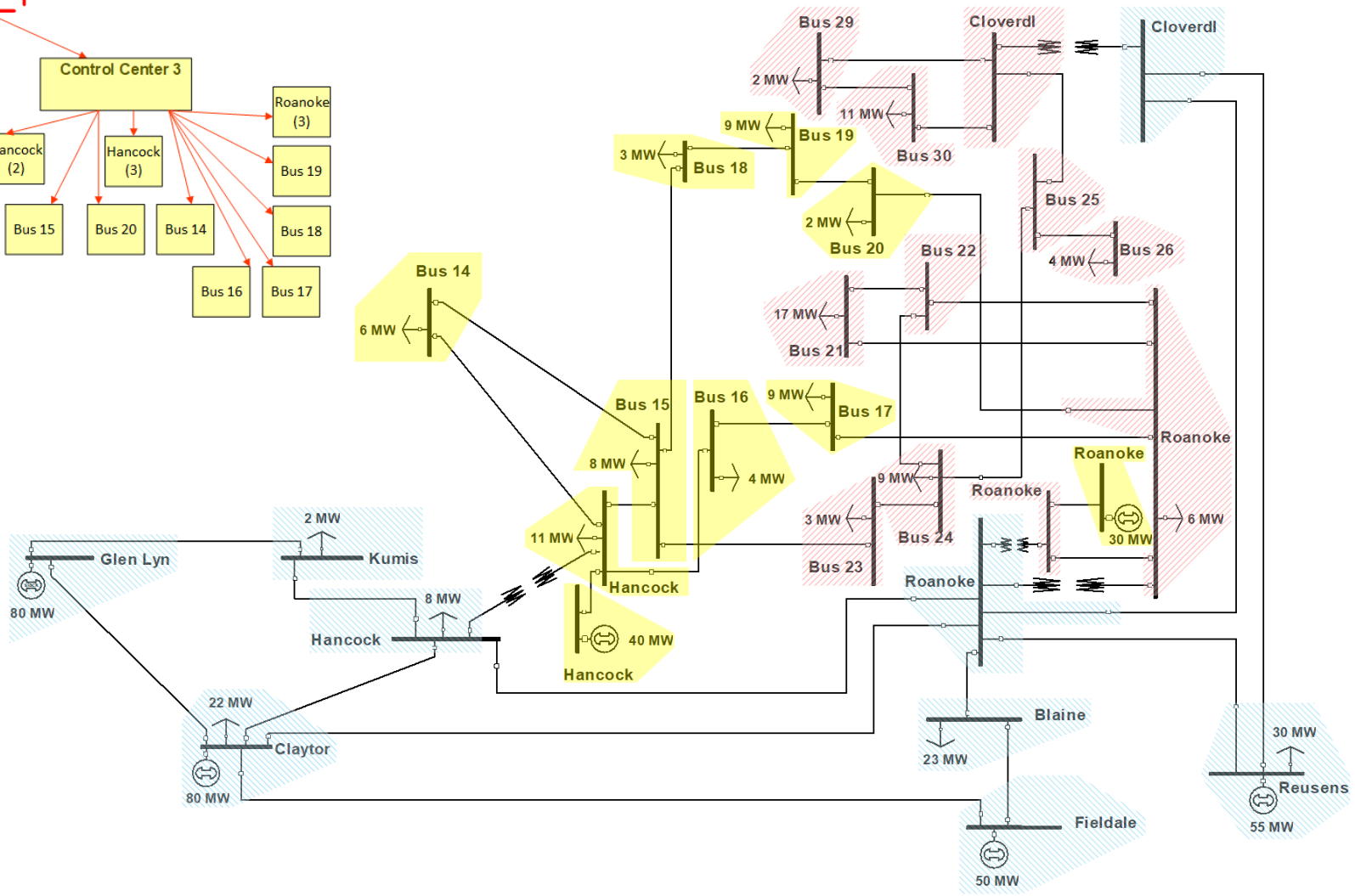
Defender

Redispatch on the remaining components, solving capacitated network flow and minimizing load shed.

EXAMPLE ATTACK

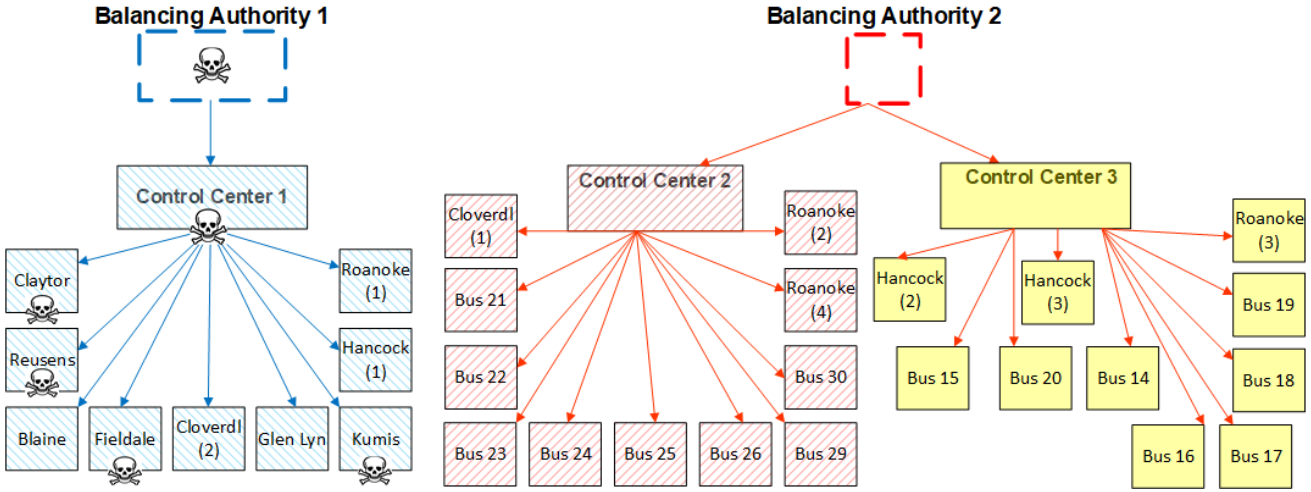
SCADA NETWORK



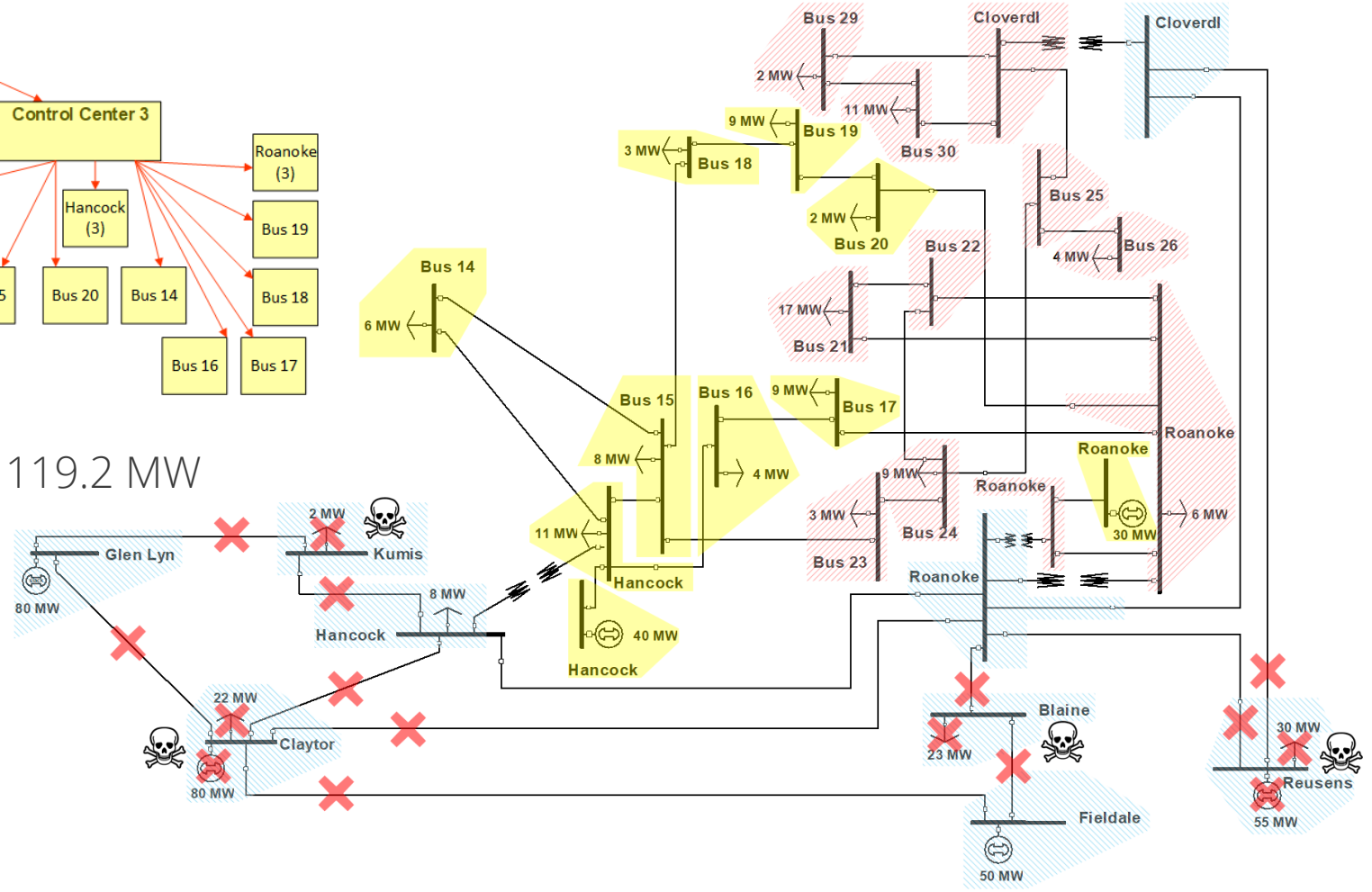


PRE-SEGMENTATION WORST-CASE ATTACK

Attack budget: 7



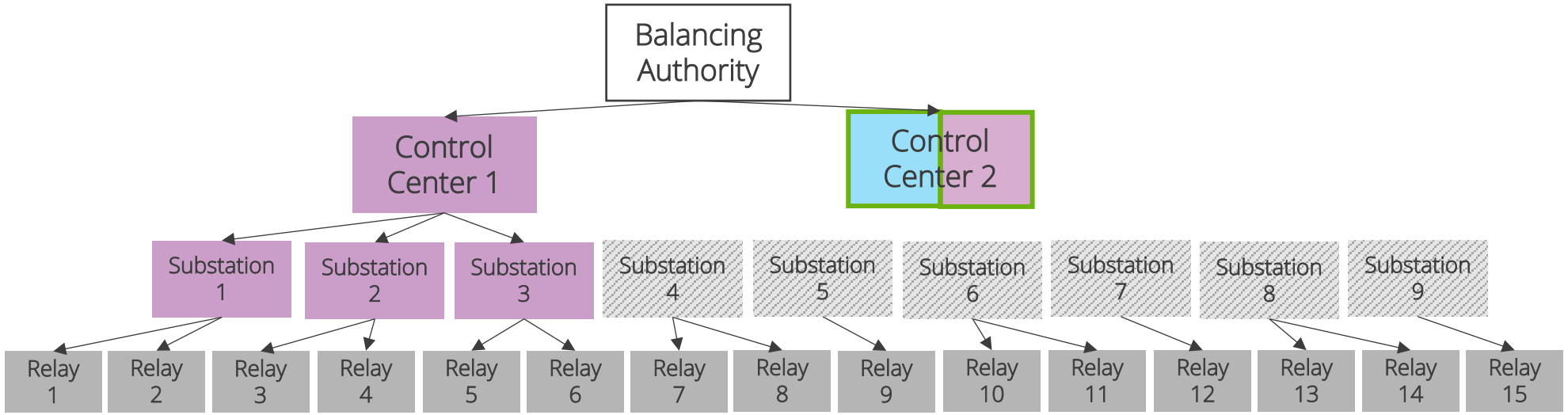
Total Load Shed: 119.2 MW



NETWORK DESIGNER DECISIONS

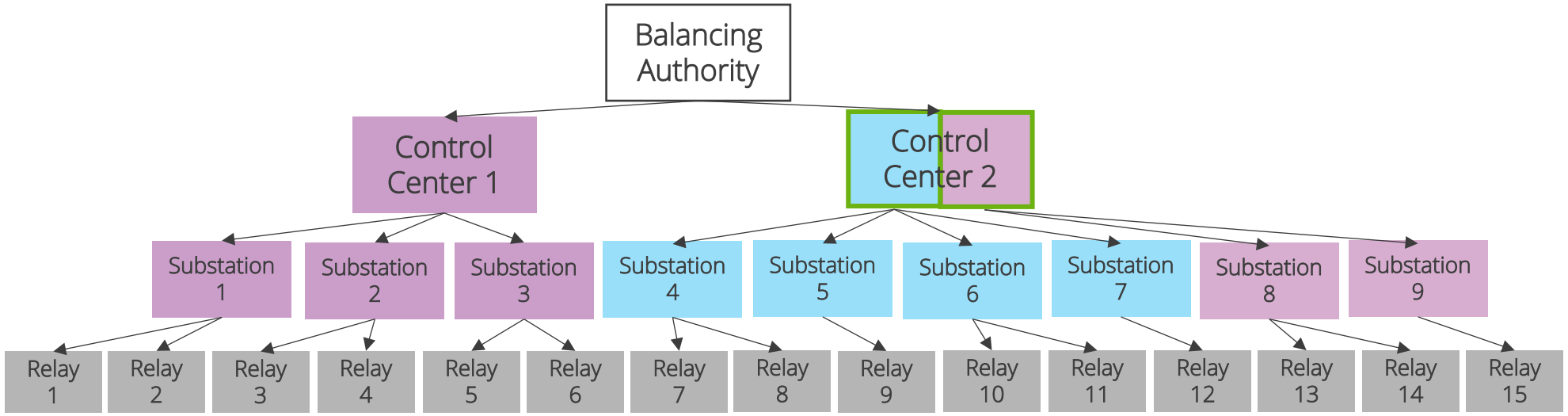
WHAT IS THE NETWORK DESIGNER ALLOWED TO DO?

- Divide a balancing authority, control center, or substation node:



WHAT IS THE NETWORK DESIGNER ALLOWED TO DO?

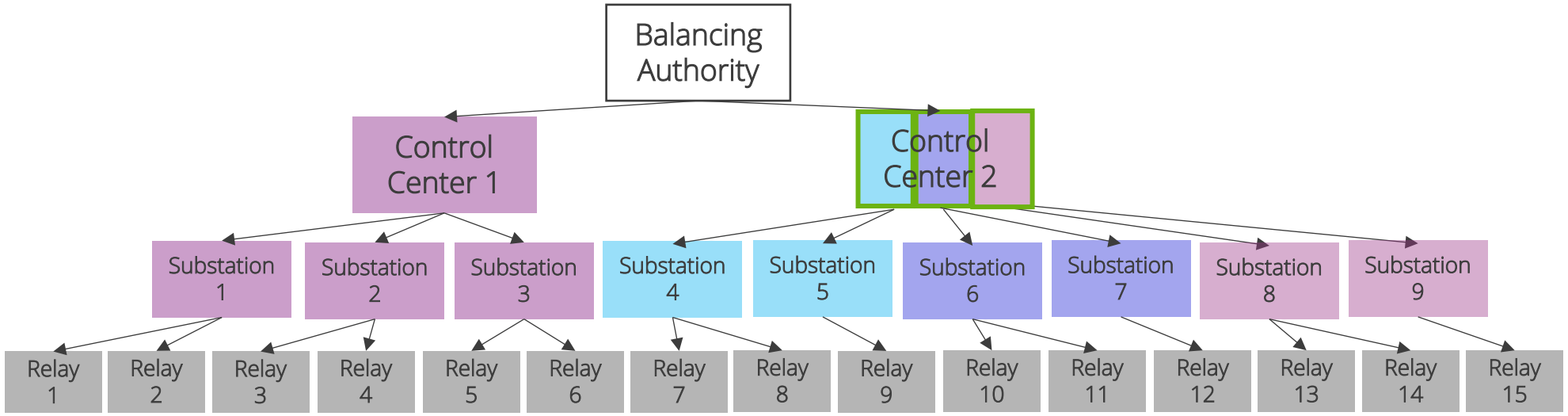
- Divide a balancing authority, control center, or substation node:



- Its children must be assigned to one of the subnetworks (but not to a new parent entity)

WHAT IS THE NETWORK DESIGNER ALLOWED TO DO?

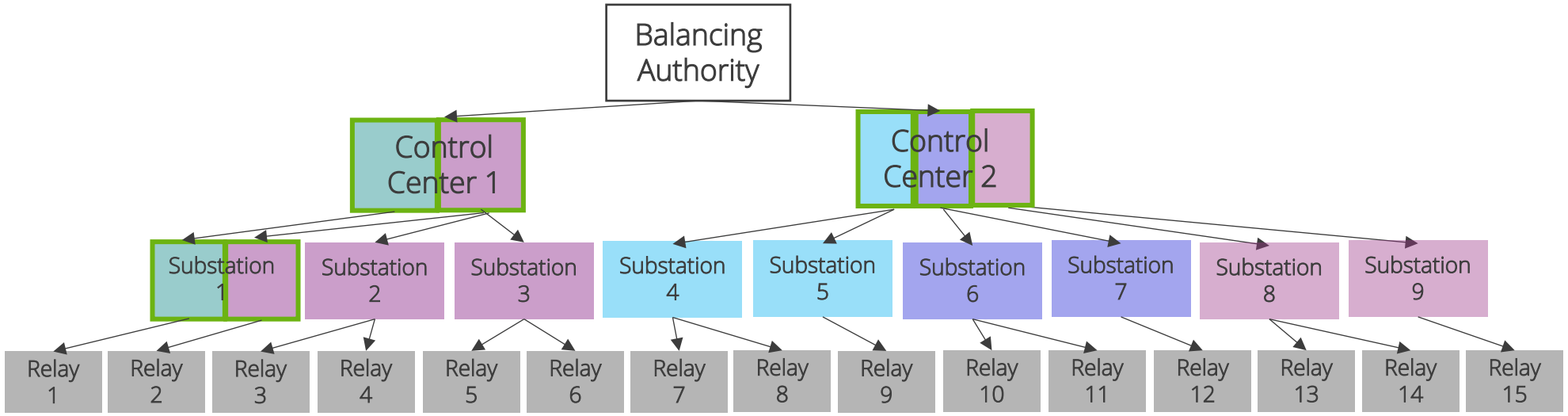
- Divide a balancing authority, control center, or substation node:



- Its children must be assigned to one of the subnetworks (but not to a new parent entity)
- This can be done more than once.

WHAT IS THE NETWORK DESIGNER ALLOWED TO DO?

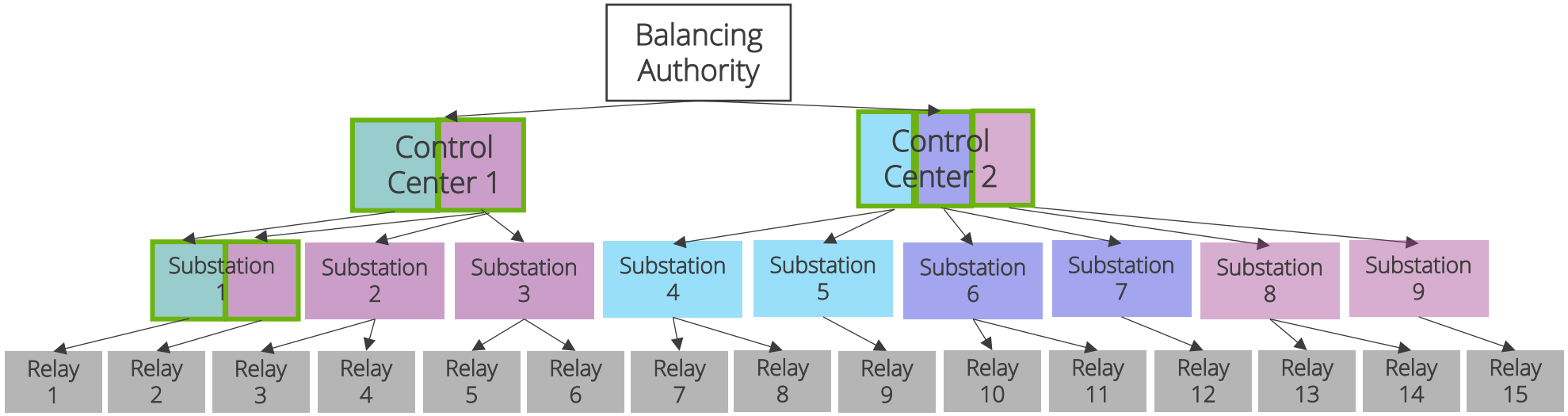
- Divide a balancing authority, control center, or substation node:



- Its children must be assigned to one of the subnetworks (but not to a new parent entity)
- This can be done more than once.
- When subdividing a substation, its subnetworks must have different parents.

WHAT IS THE NETWORK DESIGNER ALLOWED TO DO?

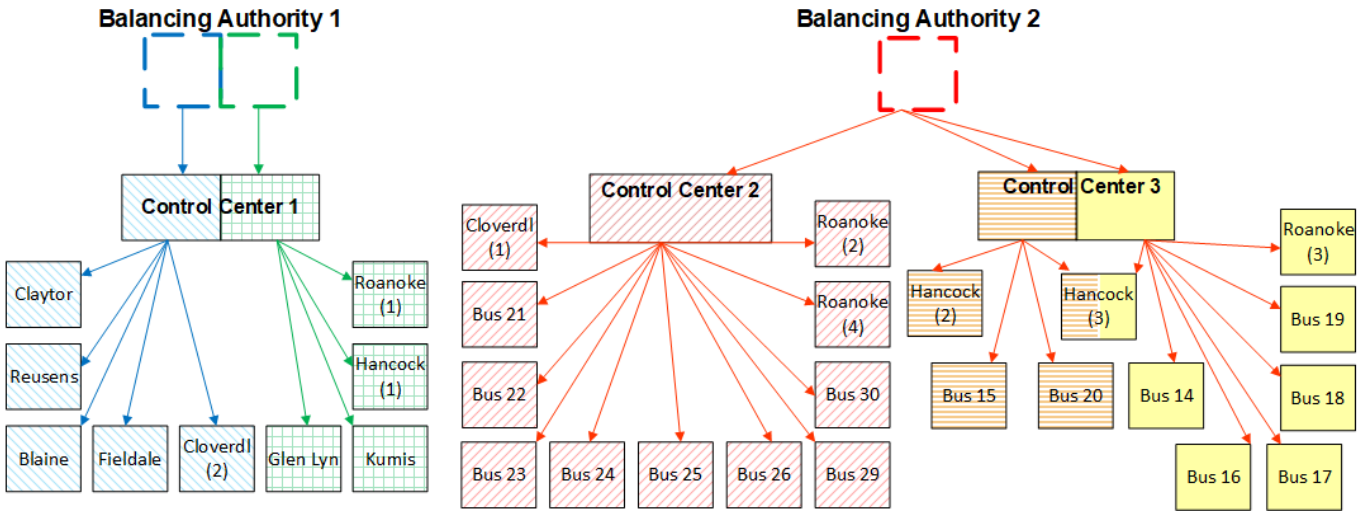
- Divide a balancing authority, control center, or substation node:

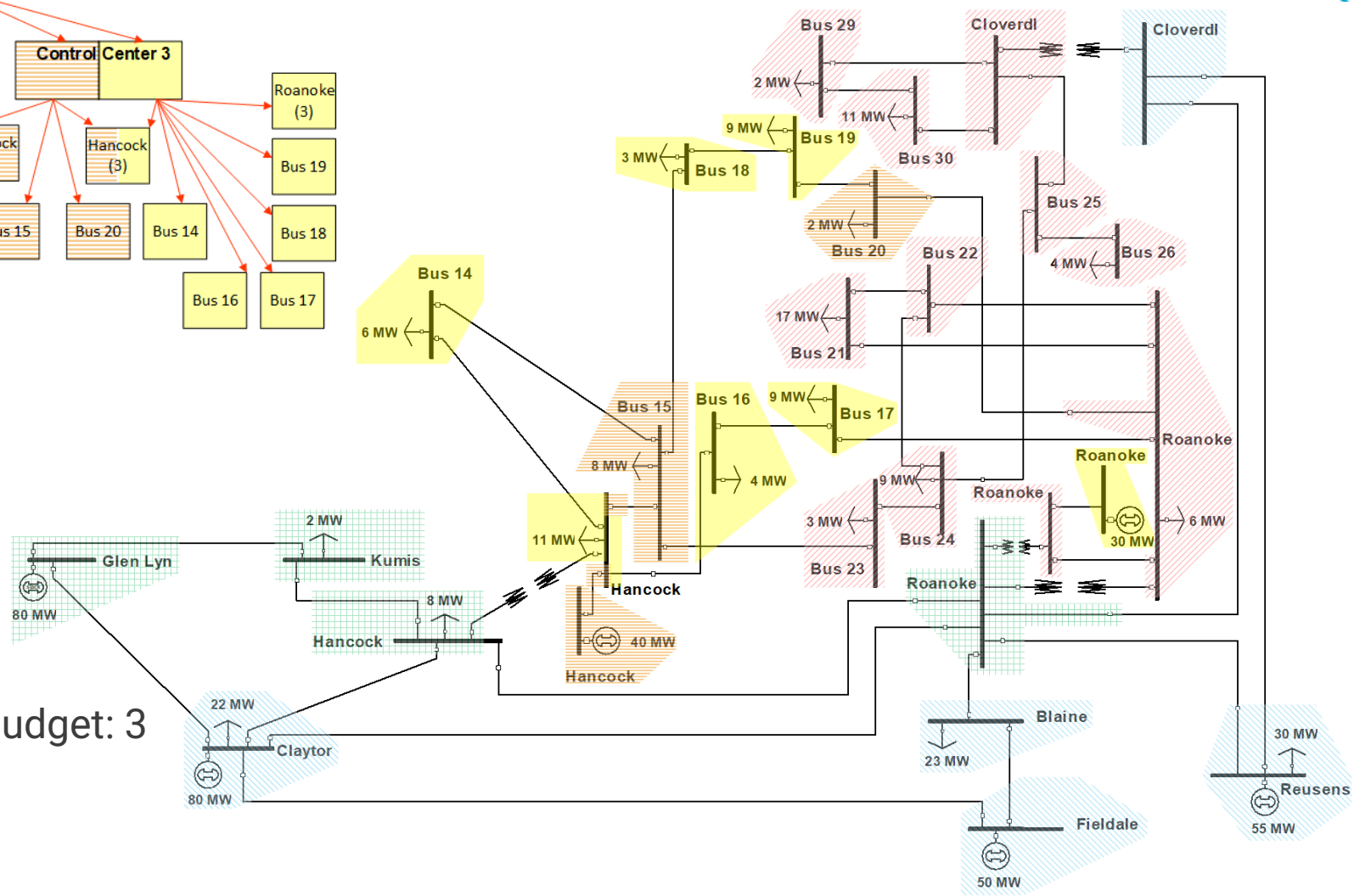


- Its children must be assigned to one of the subnetworks (but not to a new parent entity)
- This can be done more than once.
- When subdividing a substation, its subnetworks must have different parents.
- There are two budgets for number of new subnetworks, one for balancing authorities and control centers combined, the other for substations.

EXAMPLE NETWORK SEGMENTATION

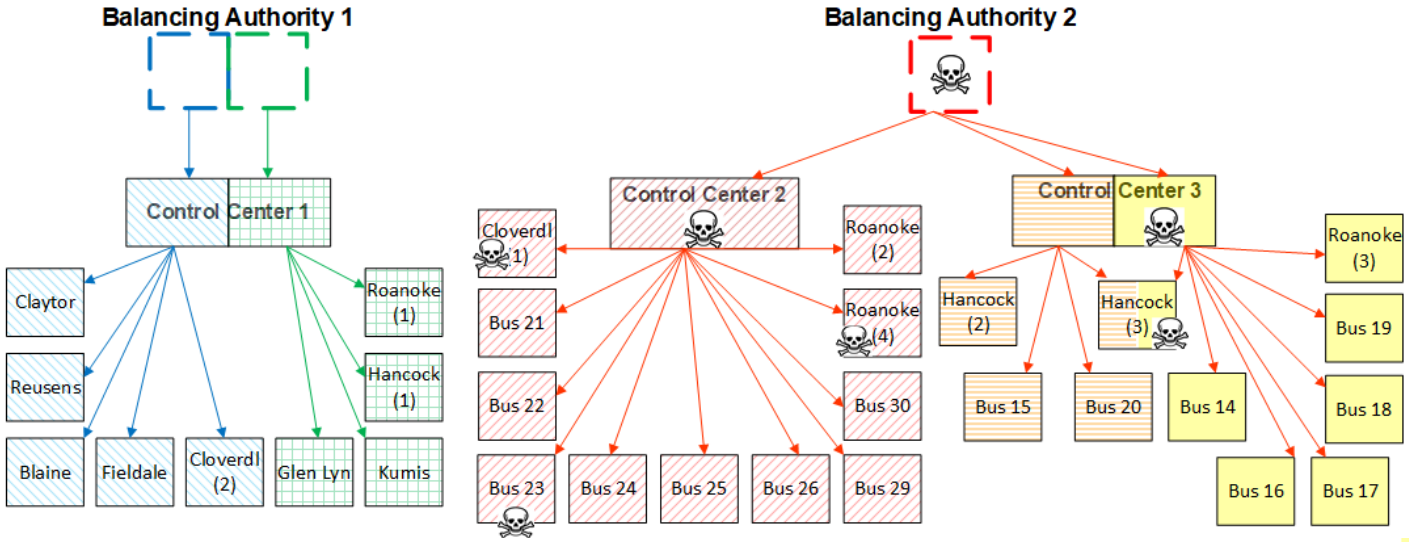
SEGMENTED SCADA NETWORK



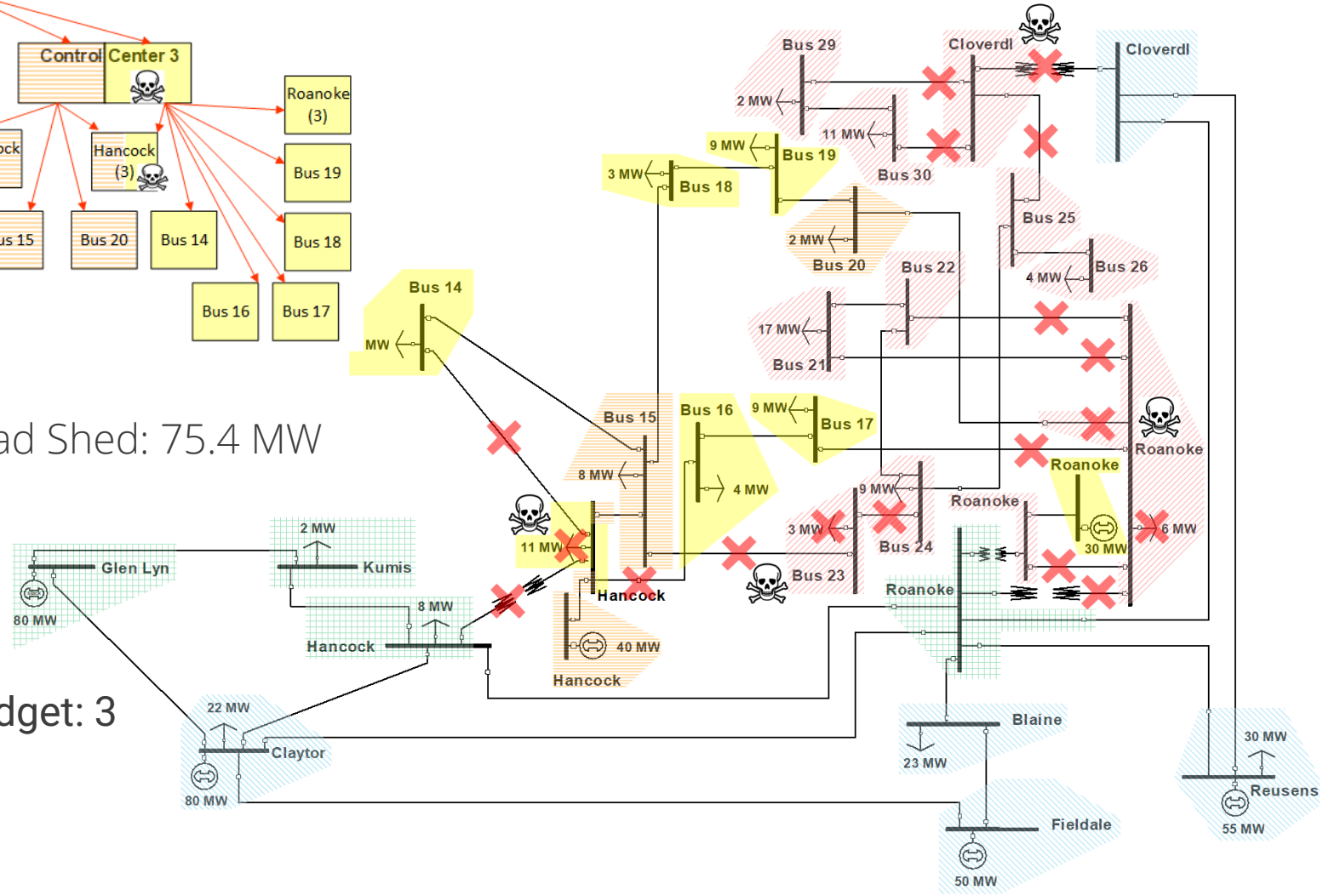


- Attack budget: 7
- Balancing Authority and Control Center budget: 3
- Substation budget: 1

WORST-CASE ATTACK ON SEGMENTED SCADA NETWORK



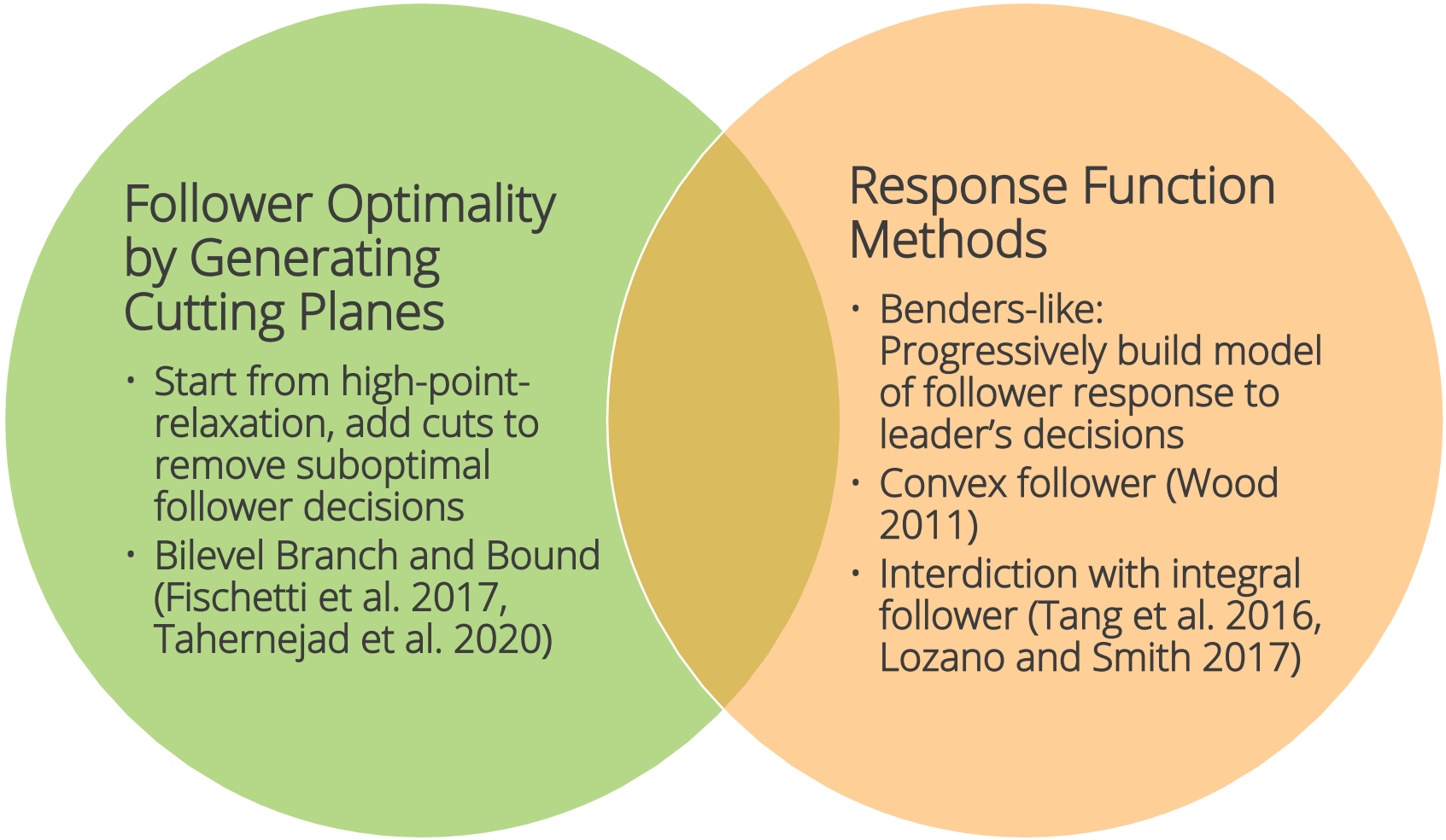
Total Load Shed: 75.4 MW



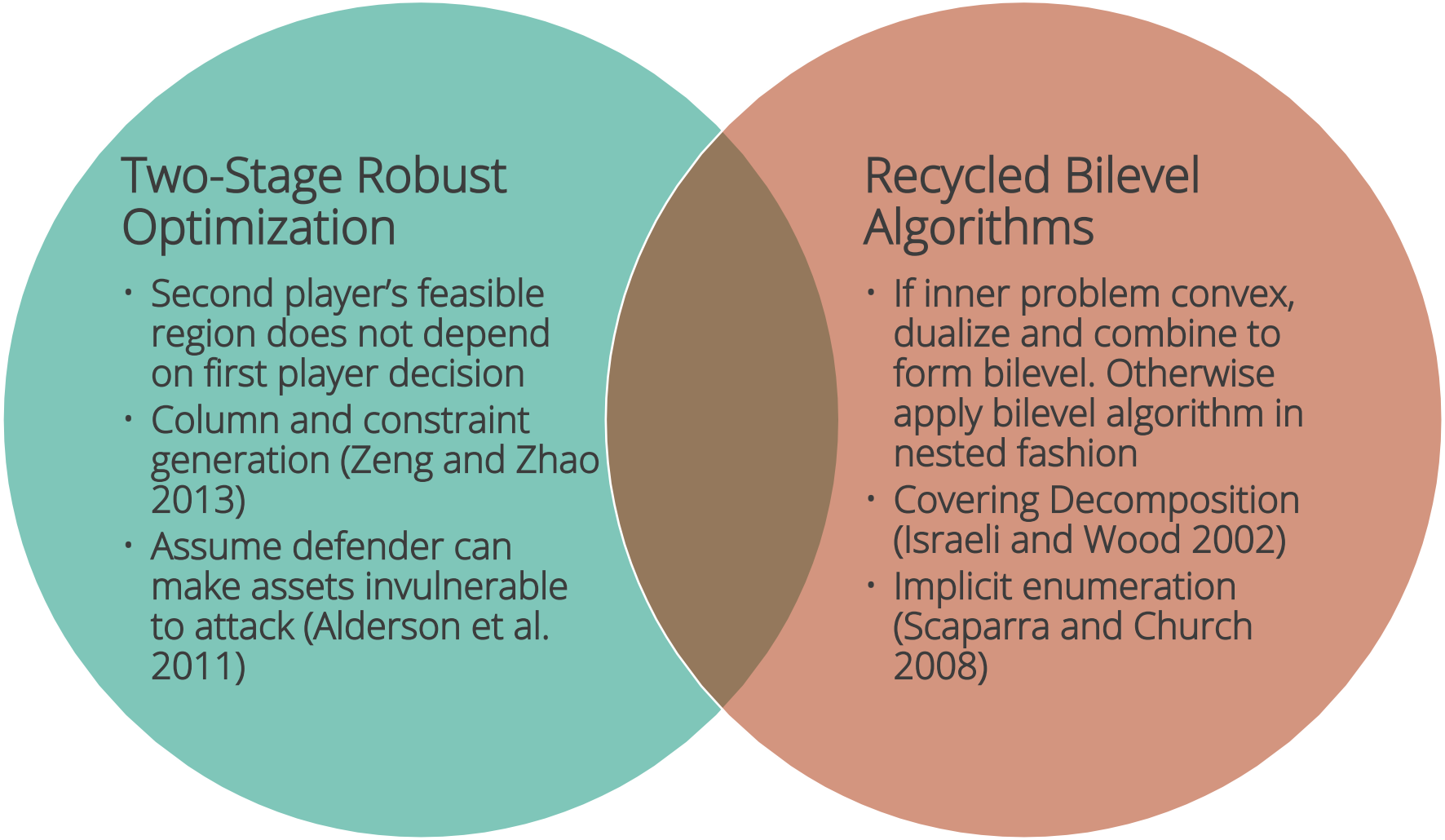
- Attack budget: 7
- Balancing Authority and Control Center budget: 3
- Substation budget: 1

SOLUTION METHODS

GENERAL BILEVEL ALGORITHMS

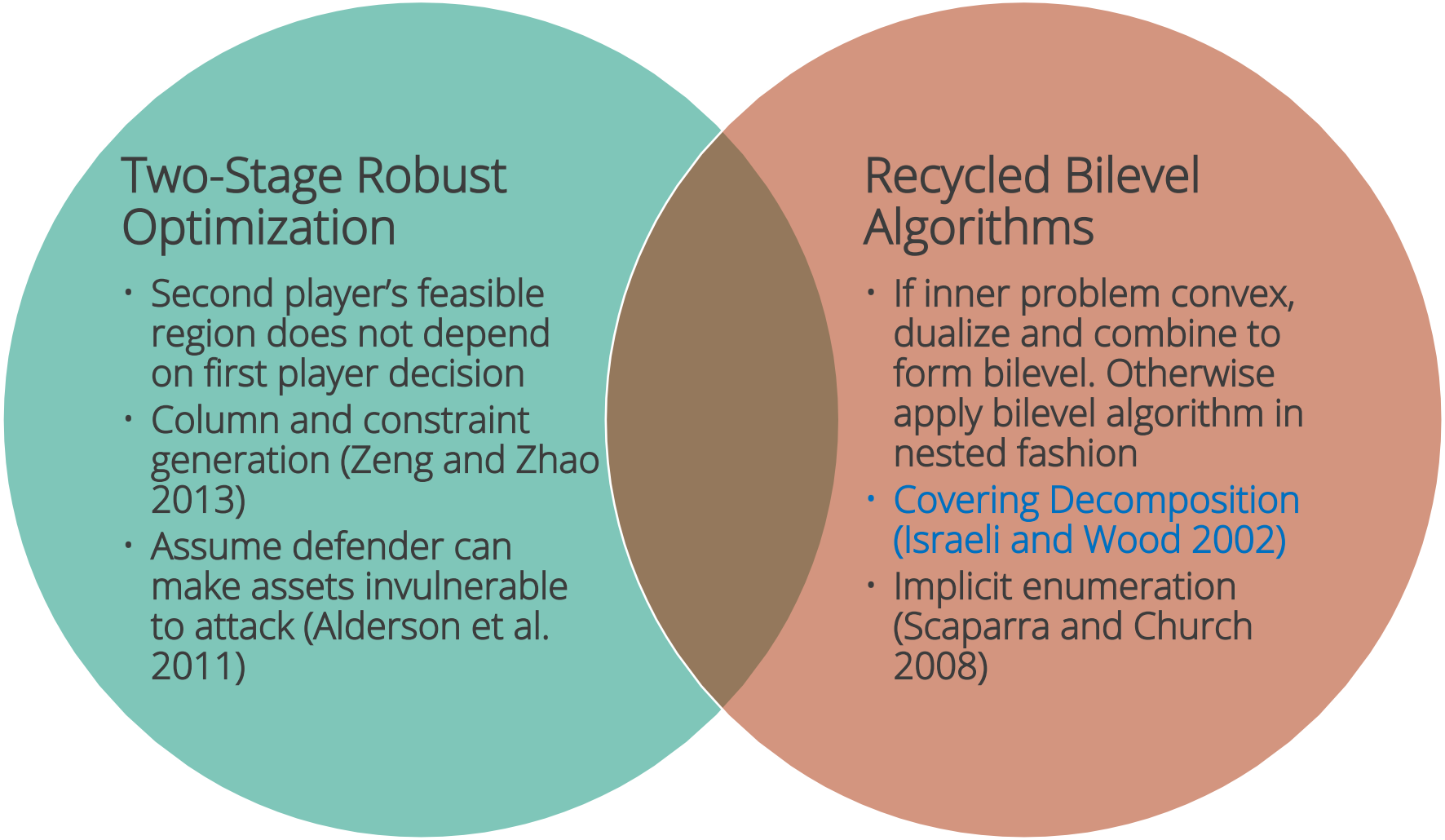


TRILEVEL INTERDICTION ALGORITHMS



Backwards sampling approach (Lozano and Smith 2017b)

TRILEVEL INTERDICTION ALGORITHMS



Backwards sampling approach (Lozano and Smith 2017b)

WE REMOVE TWO ASSUMPTIONS FROM PRIOR WORK

1. Designer can make assets invulnerable to attack

- Unrealistic: Designers really just make attackers' jobs harder (e.g., riskier, more expensive)
- Especially for cyberattack, no way to make a network impenetrable

2. Feasible region of attacker does not depend on designer decision

- This is a result of not assuming 1: If assets can be made invulnerable, they can be "attacked," but no damage is done in innermost problem.
- We need dependence because they designer (implicitly) changes the cost of the attacker's options, making some of them infeasible because they are too expensive

COVERING DECOMPOSITION ALGORITHM

Write general trilevel interdiction problem:

$$\min_{d \in D} \max_{a \in A(d)} \min_{x \in X(a)} f(x)$$

Where the following hold:

- Assumption 1: We have relatively complete recourse at every level. That is, given $d \in D$, $A(d) \neq \emptyset$, and given $a \in A(d)$, $X(a) \neq \emptyset$.
- Assumption 2: The set D is finite, as is $A(d)$ for all $d \in D$.
- Assumption 3: The function f is bounded below by some number. This can be any number, but we'll use 0 in this talk.

This means we can list all the attacks:

$$\{a^1, a^2, \dots, a^H\} = \bigcup_{d \in D} A(d)$$

Let the set of indices be $\overline{K} = \{1, 2, \dots, H\}$

COVERING DECOMPOSITION ALGORITHM

Then we can rewrite the trilevel problem as:

$$\nu = \min_{d \in D, \xi \in \mathbb{R}, \eta \in \mathbb{R}^H, x^1, \ldots, x^H \in \mathbb{R}^N} \xi$$

$$s.t. \quad \xi \geq \eta_k \qquad \forall k \in \overline{K}$$

$$\begin{bmatrix} \eta_k = f(x^k) \\ x^k \in X(a^k) \\ a^k \in A(d) \end{bmatrix} \vee \begin{bmatrix} \eta_k = 0 \\ a^k \notin A(d) \end{bmatrix} \quad \forall k \in \overline{K}$$

By our assumptions, we can write this as a MIP.

COVERING DECOMPOSITION ALGORITHM: LOWER BOUND

If we replace $\overline{K}$ with a set $K \subseteq \overline{K}$ then we have a relaxation and hence a lower bound on ν:

$$\nu \geq \min_{d \in D, \xi \in \mathbb{R}, \eta \in \mathbb{R}^H, x^1, \ldots, x^H \in \mathbb{R}^N} \xi$$

$$s.t. \quad \xi \geq \eta_k \qquad \forall k \in K$$

$$\begin{bmatrix} \eta_k = f(x^k) \\ x^k \in X(a^k) \\ a^k \in A(d) \end{bmatrix} \vee \begin{bmatrix} \eta_k = 0 \\ a^k \notin A(d) \end{bmatrix} \quad \forall k \in K$$

COVERING DECOMPOSITION ALGORITHM: UPPER BOUND

For any feasible design $d \in D$, we can get an upper bound on ν by calculating the worst-case attack on that design:

$$u(d) = \max_{a \in A(d)} \min_{x \in X(a)} f(x)$$

We know this isn't always an easy problem, but in our case we use a network flow restriction, which scales well in practice.

NETWORK FLOW RESTRICTION

Drop the only hard thing in DCOPF: Ohm's Law

- i.e., relax inner problem to capacitated network flow

- Totally unimodular constraint matrix ⇒ duals are bounded in absolute value by 1.
- We can linearize exactly, and the problem scales because of the moderate big-M values.

The result is a restriction of the original bilevel problem.

- We've lost nothing: All we had was a lower bound anyway because we don't know valid bounds on the dual variables of DCOPF!

$$\max_{\delta,u,v,w} \min_{f,p,l,\theta} \sum_{b\in\mathcal{B}} l_b$$

Attacker

$$\begin{aligned}
\text{s.t.} \quad & \sum_{r\in\mathcal{R}} \delta_r \le U && \\
& \sum_{r\in\mathcal{R}_k} \delta_r \ge 1 - v_k && \forall k \in \mathcal{K} \\
& \sum_{r\in\mathcal{R}_g} \delta_r \ge 1 - u_g && \forall g \in \mathcal{G} \\
& \sum_{r\in\mathcal{R}_b} \delta_r \ge 1 - w_b && \forall b \in \mathcal{B} \\
& \delta_r \le 1 - v_k && \forall k \in \mathcal{K}, r \in \mathcal{R}_k \\
& \delta_r \le 1 - u_g && \forall g \in \mathcal{G}, r \in \mathcal{R}_g \\
& \delta_r \le 1 - w_b && \forall b \in \mathcal{B}, r \in \mathcal{R}_b \\
& \delta_r \in \{0,1\} && \forall r \in \mathcal{R} \\
& v_k \in \{0,1\} && \forall k \in \mathcal{K} \\
& u_g \in \{0,1\} && \forall g \in \mathcal{G} \\
& w_b \in \{0,1\} && \forall b \in \mathcal{B}
\end{aligned}$$

Defender

$$\begin{aligned}
& \sum_{k\in\mathcal{K}_b^+} f_k - \sum_{k\in\mathcal{K}_b^-} f_k + \sum_{g\in\mathcal{G}(b)} p_g + l_b = D_b && \forall b \in \mathcal{B} \\
& \cancel{f_k \le B_k(\theta_{o(k)} - \theta_{d(k)}) + 2\pi B_k(1 - v_k)} && \forall k \in \mathcal{K} \\
& \cancel{f_k \ge B_k(\theta_{o(k)} - \theta_{d(k)}) - 2\pi B_k(1 - v_k)} && \forall k \in \mathcal{K} \\
& D_b(1 - w_b) \le l_b \le D_b && \forall b \in \mathcal{B} \\
& -\overline{F}_k v_k \le f_k \le \overline{F}_k v_k && \forall k \in \mathcal{K} \\
& \cancel{-\pi \le \theta_b \le \pi} && \forall b \in \mathcal{B} \\
& 0 \le p_g \le \overline{P}_g u_g && \forall g \in \mathcal{G} \\
& l_b \ge 0 && \forall b \in \mathcal{B}
\end{aligned}$$

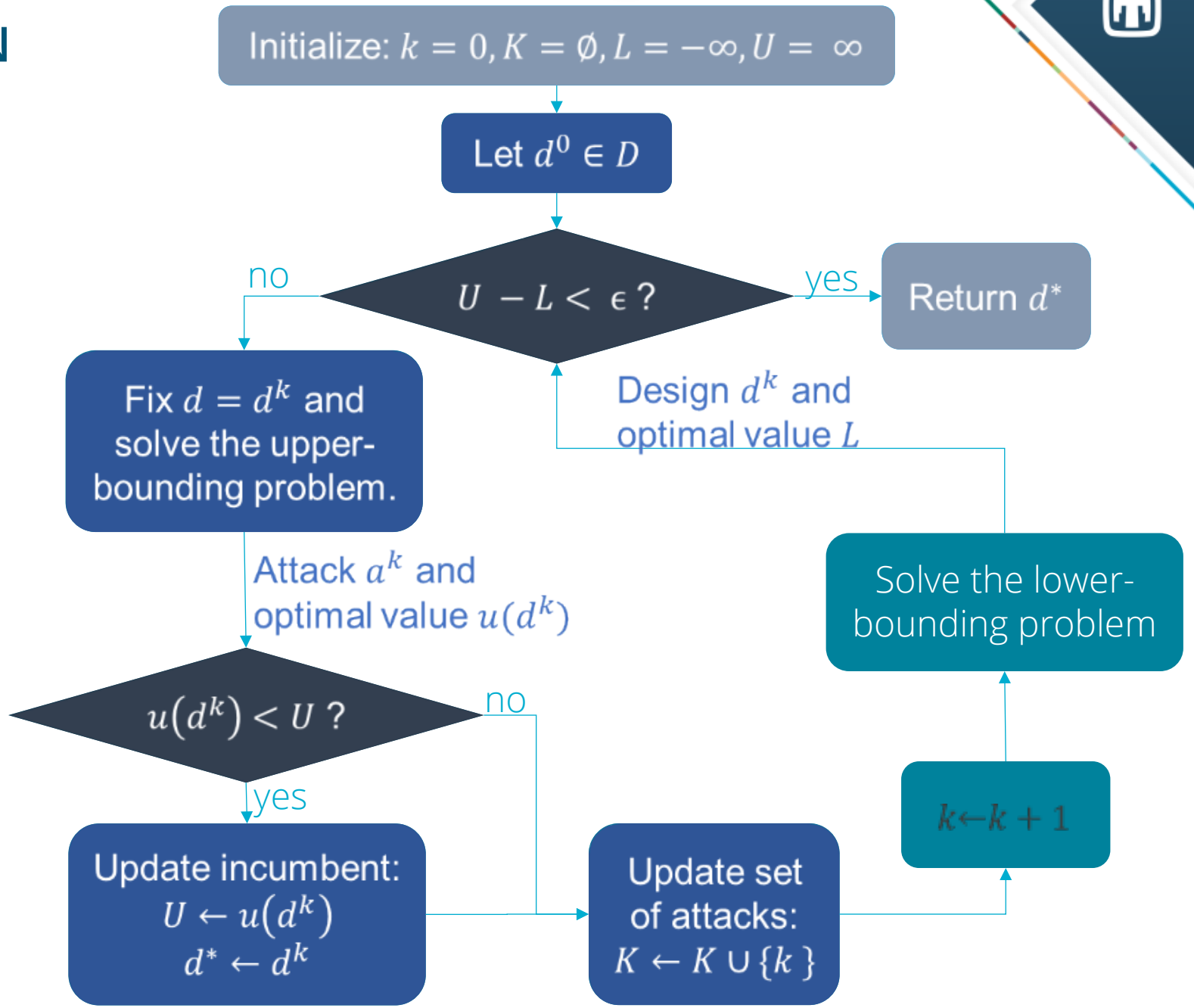
E.S. Johnson and S.S. Dey, "A Scalable Lower Bound for the Worst-Case Relay Attack Problem on the Transmission Grid," INFORMS Journal on Computing 2022 34:4, 2296-2312

COVERING DECOMPOSITION ALGORITHM, VERSION 1

Until bounds close, alternate between:

- Solving for a new design and a lower bound, and
- Finding the worst-case attack on that design and an upper bound

Proposition:
Under our assumptions, the algorithm converges in finite time with an ϵ-optimal solution d^*



THIS ISN'T COVERING DECOMPOSITION… YET

Observation:
In the covering decomposition algorithm from the previous slide, $L = 0$ until the iteration the algorithm terminates, and the returned solution will be exactly optimal regardless of the value of ϵ.

This is because the designer will choose the second disjunct for all k (i.e., block all the attacks) for as many iterations as he can:

$$\begin{bmatrix} \eta_k = f(x^k) \\ x^k \in X(a^k) \\ a^k \in A(d) \end{bmatrix} \vee \begin{bmatrix} \eta_k = 0 \\ a^k \notin A(d) \end{bmatrix} \quad \forall k \in K$$

The first iteration where this is impossible, the bounds will meet.

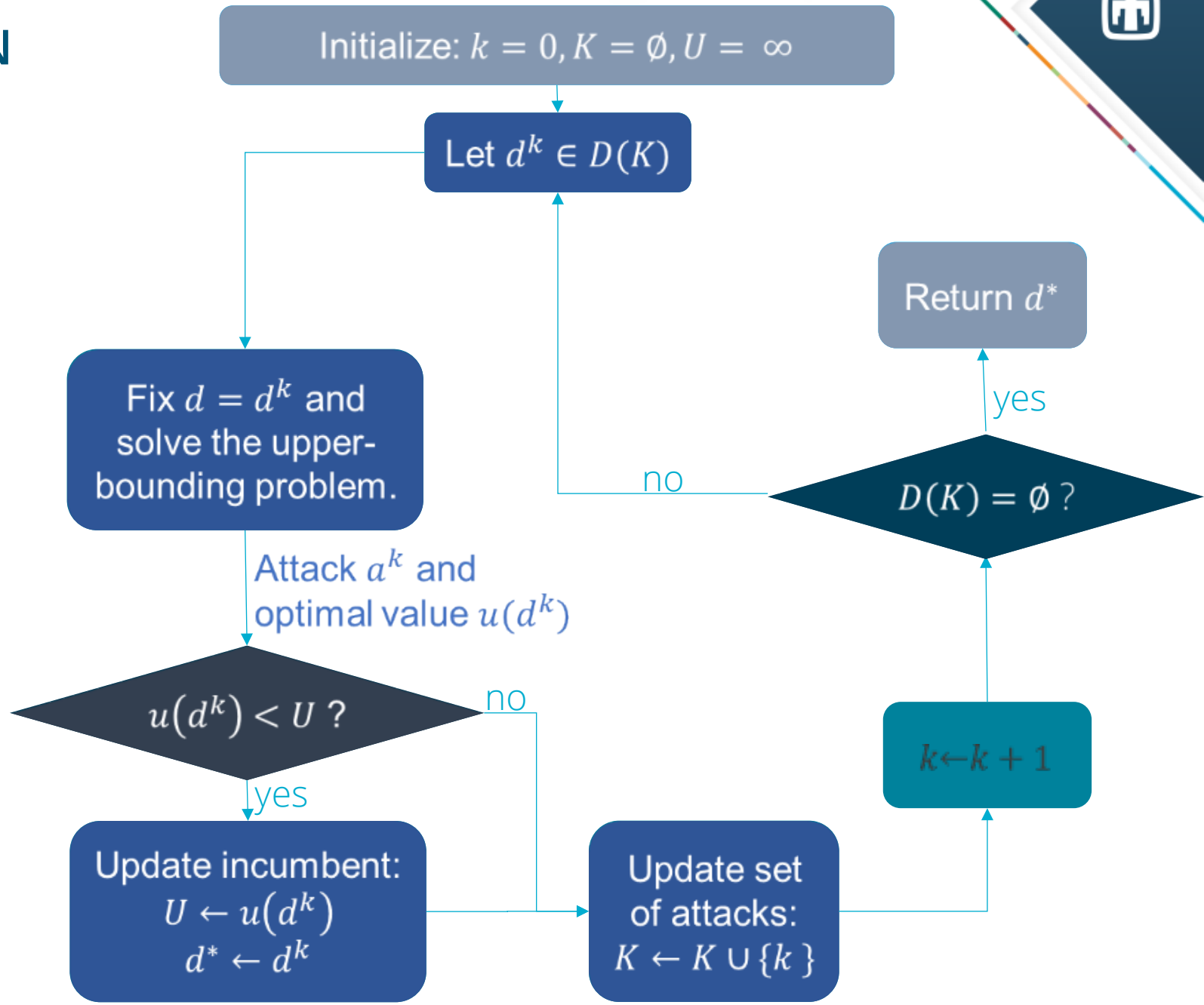
So we don't ever need to solve the disjunctive version…

Define $D(K) = \{d \in D : a^k \notin A(d) \forall k \in K\}$

COVERING DECOMPOSITION ALGORITHM, VERSION 2

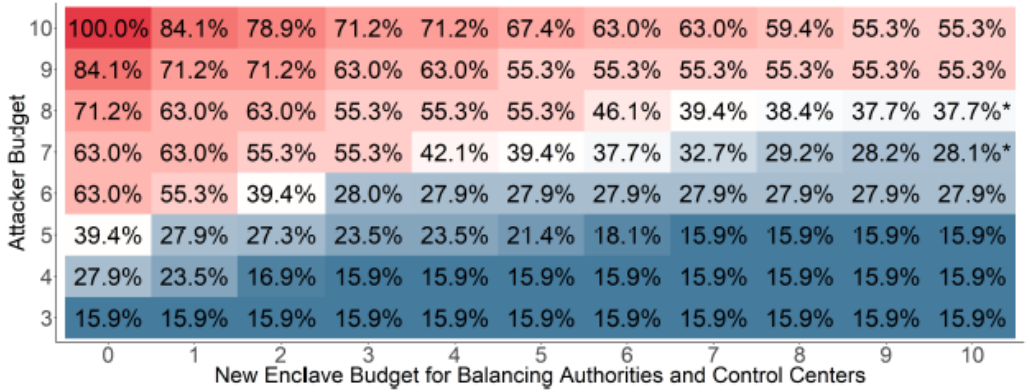
Until such a design does not exist, alternate between:

- Finding a design which blocks all the attacks generated so far
- Finding the worst-case attack on that design and an upper bound

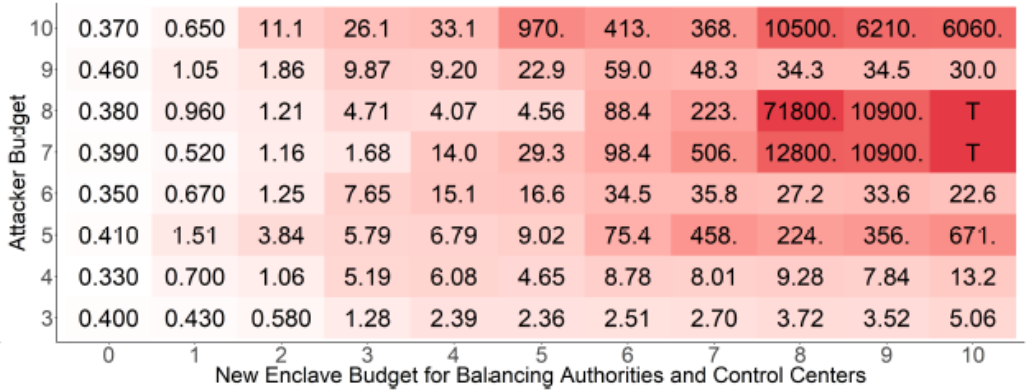


RESULTS

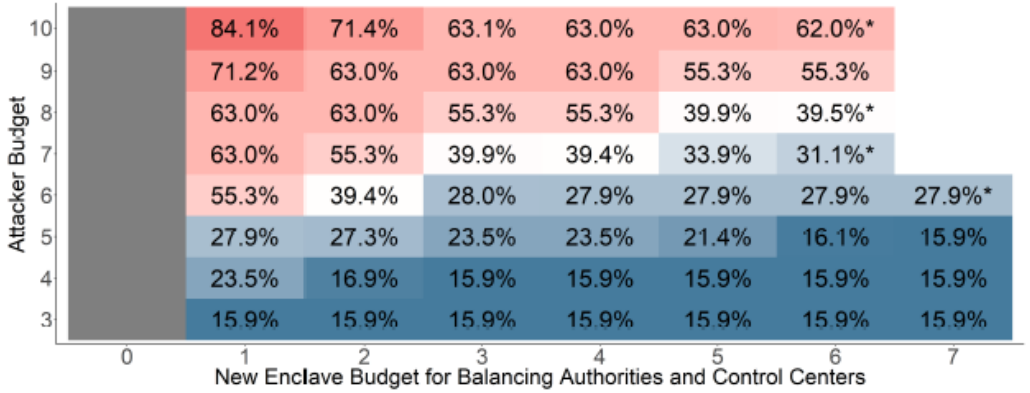
30-Bus Arguello et al. Topology: Percentage of Total Load Shed with 0 Added Substation Enclaves



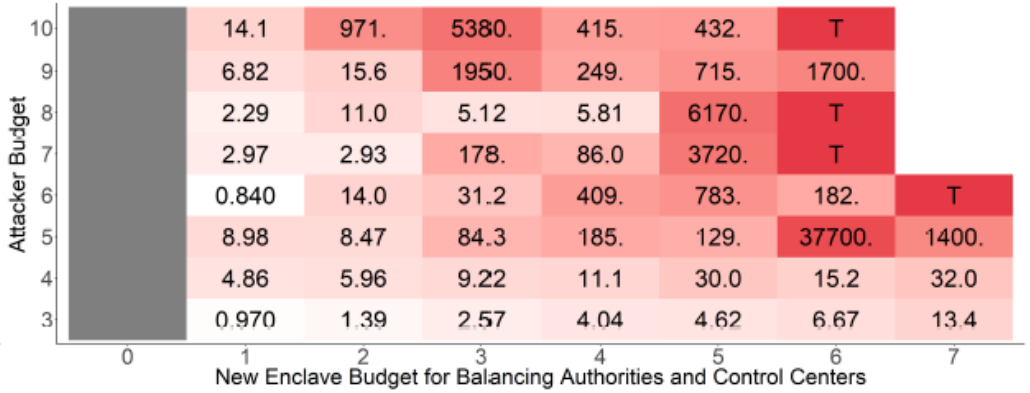
30-Bus Arguello et al. Topology: Computational Time with 0 Added Substation Enclaves



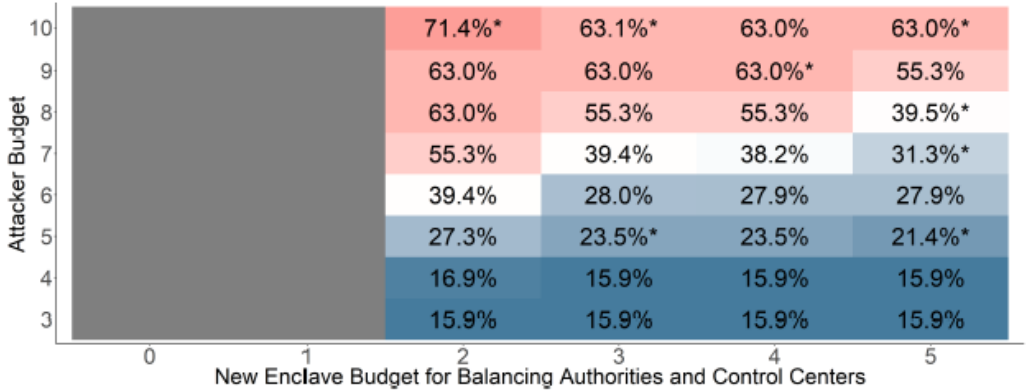
30-Bus Arguello et al. Topology: Percentage of Total Load Shed with 1 Added Substation Enclave



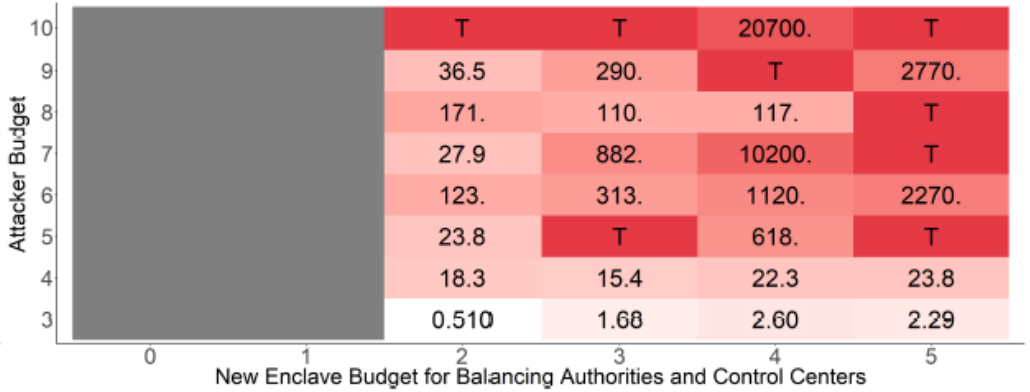
30-Bus Arguello et al. Topology: Computational Time with 1 Added Substation Enclave



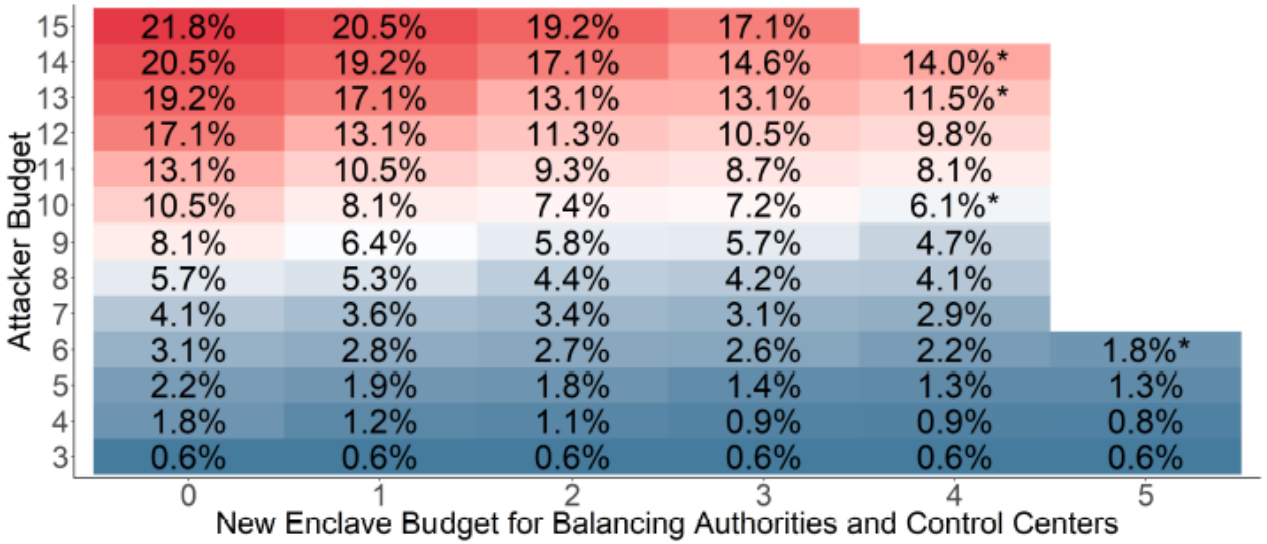
30-Bus Arguello et al. Topology: Percentage of Total Load Shed with 2 Added Substation Enclaves



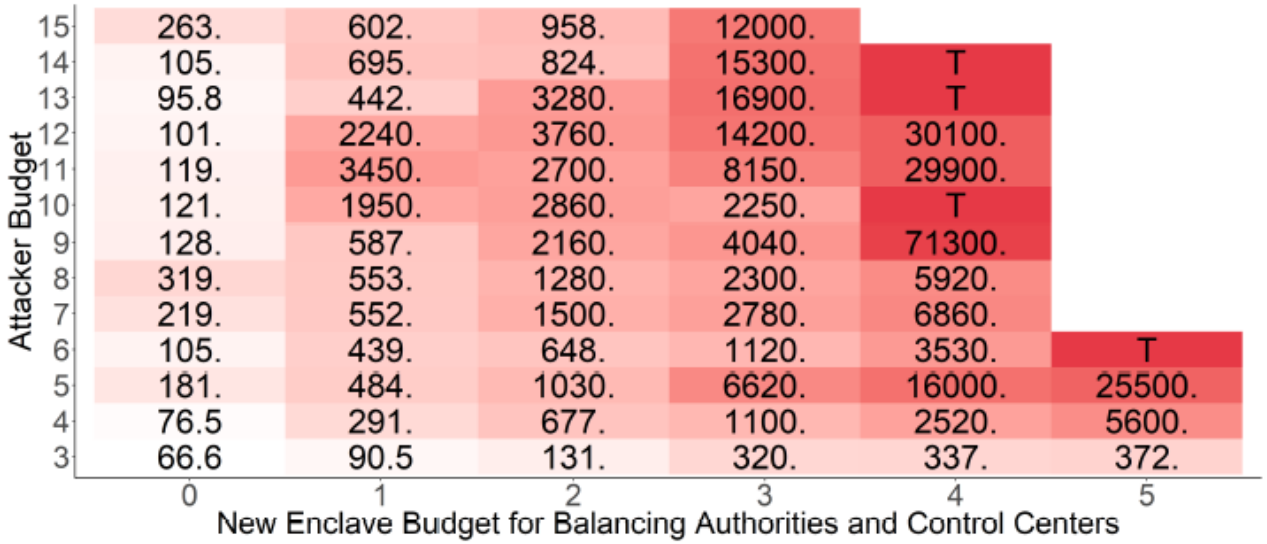
30-Bus Arguello et al. Topology: Computational Time with 2 Added Substation Enclaves



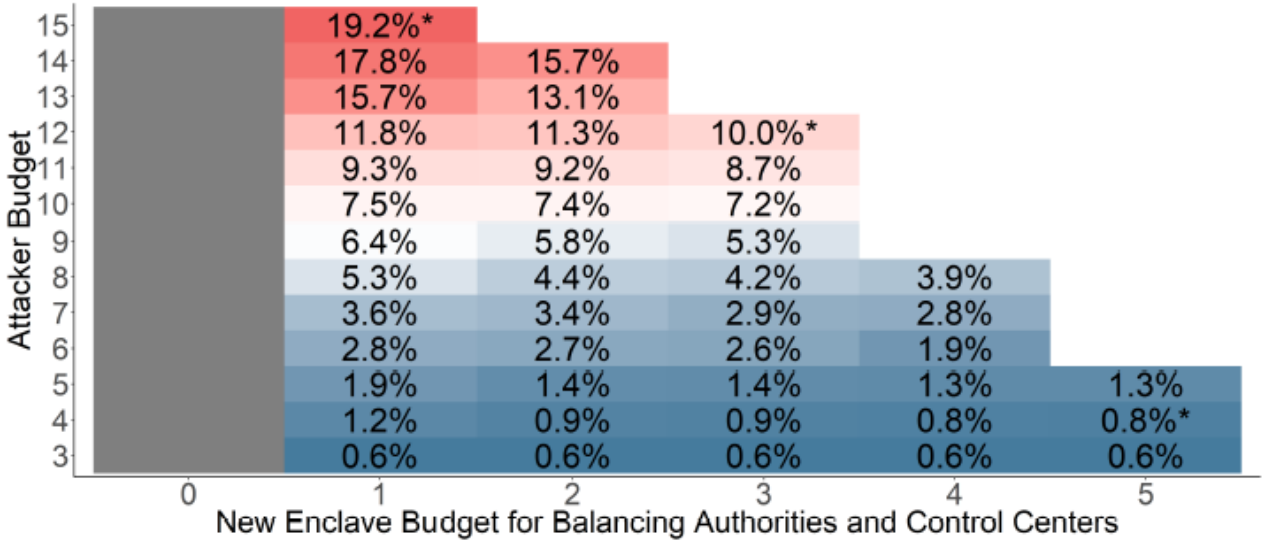
2000-Bus Case with 2 BAs and 5 CCs: Percentage of Total Load Shed with 0 Added Substation Enclaves



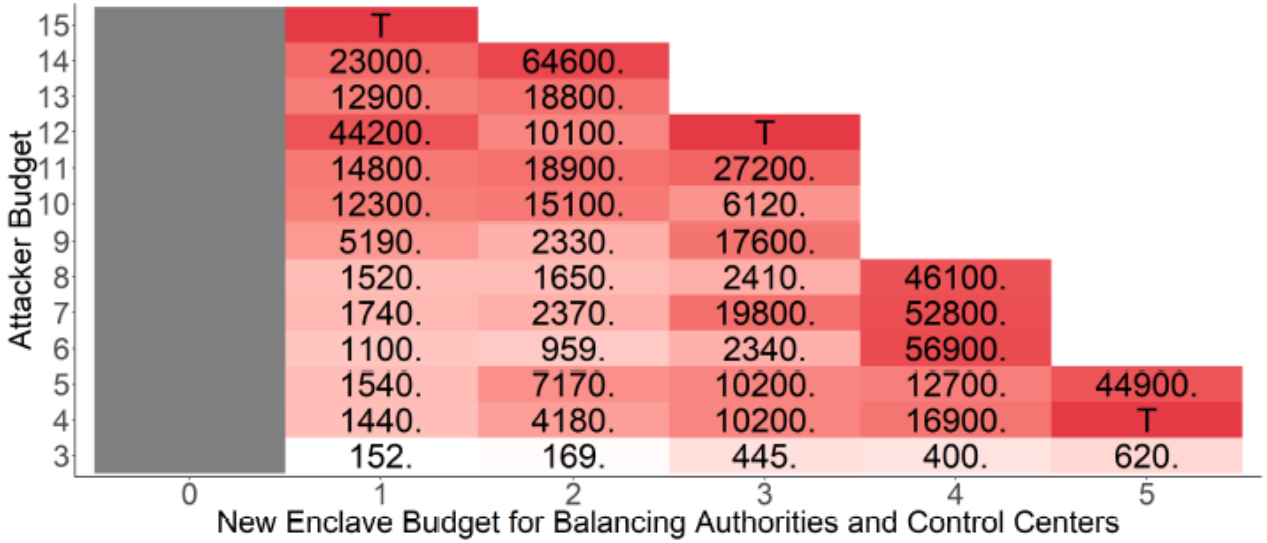
2000-Bus Case with 2 BAs and 5 CCs: Computational Time with 0 Added Substation Enclaves



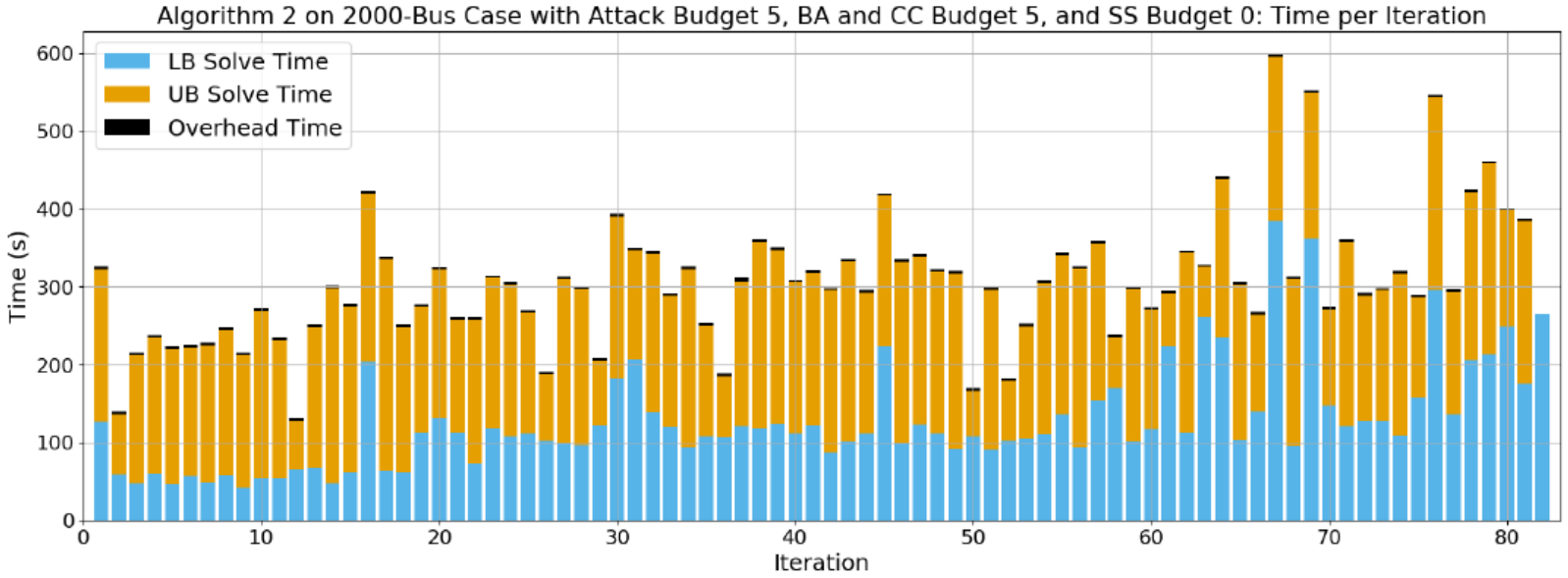
2000-Bus Case with 2 BAs and 5 CCs: Percentage of Total Load Shed with 1 Added Substation Enclave

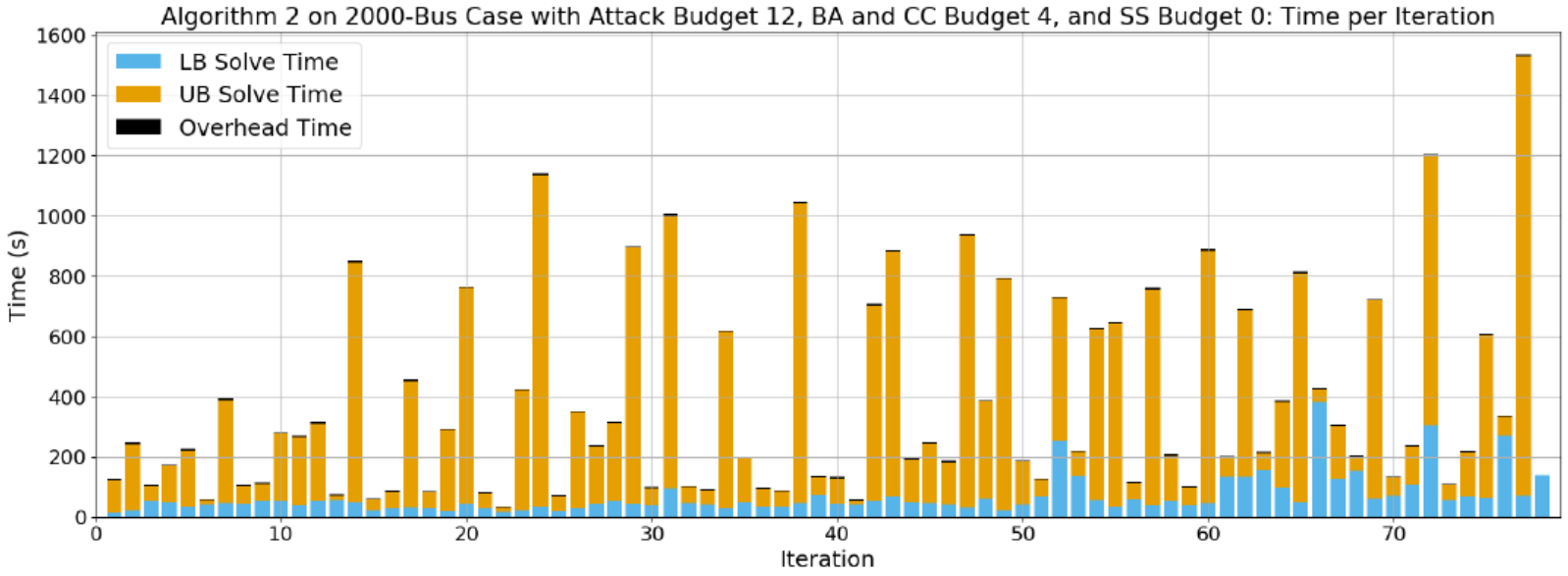


2000-Bus Case with 2 BAs and 5 CCs: Computational Time with 1 Added Substation Enclave

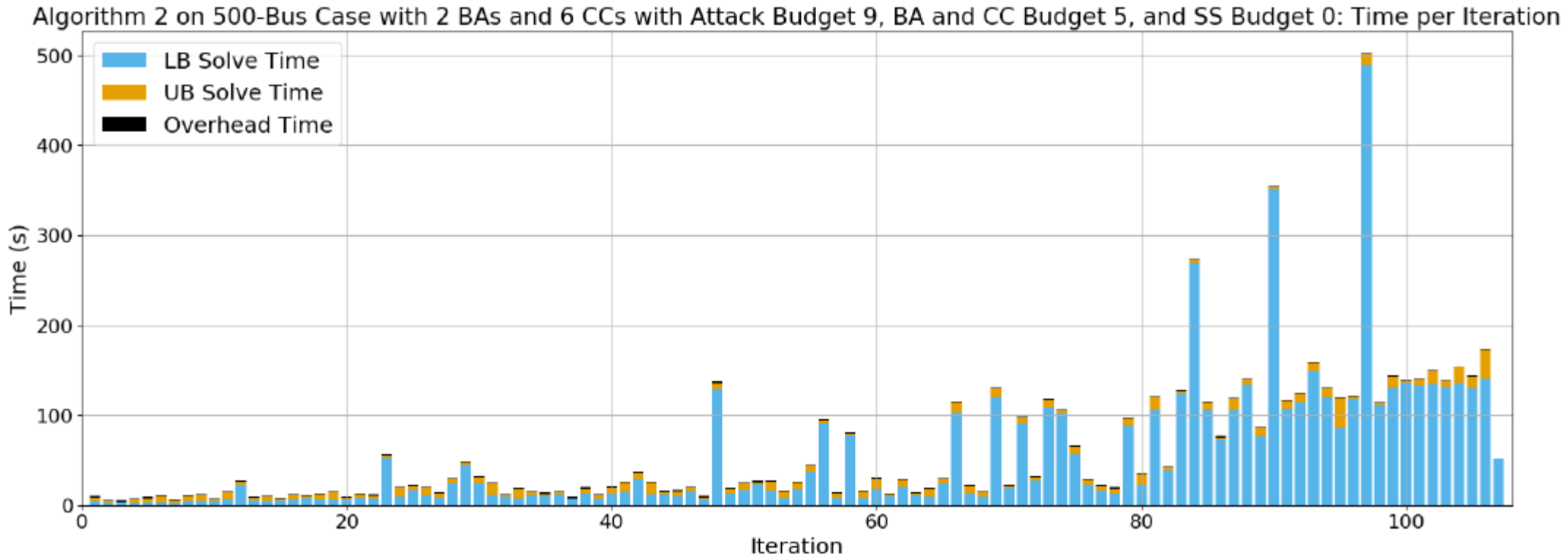


ALGORITHM PERFORMANCE: 2000-BUS CASE





ALGORITHM PERFORMANCE: 500-BUS CASE



CONCLUSIONS

The covering decomposition algorithm is scalable for realistic grids and moderate attacker and defender budgets

Increases in the substation budget do not help the network designer significantly, and come at high computational cost

Preprint available on optimization online: https://optimization-online.org/?p=18421

FUTURE DIRECTIONS

Solving the feasibility problem with a MIP solver is likely misguided: Trying constraint programming makes sense

For very large networks, the attacker problem is also still difficult. Benders decomposition or other techniques from bilevel optimization might be beneficial

Version 1 of the algorithm could provide nontrivial lower bounds for problems where solving the disjunctive problem was reasonable (and if the algorithm and/or initialization was modified to include suboptimal attacks.) This could allow terminating early, with a gap.

REFERENCES

D. Alderson, G. Brown, M. Carlyle, and R.K. Wood, "Solving defender-attacker-defender models for infrastructure defense," *Operations Research, Computing, and Homeland Defense, Proceedings of the 12th INFORMS Computing Society Conference,* Ed. by R.K. Wood and R.F. Dell. Hanover, MD: INFORMS, pp. 28-49, 2011.

B. Arguello, E.S. Johnson, and J.L. Gearhart, "A trilevel model for segmentation of the power transmission grid cyber network," Technical report 2108.10958. ArXiv, 2021.

M. Fischetti, I. Ljubić, M.Monaci, and M. Sinnl, "A new general-purpose algorithm for mixed-integer bilevel linear programs," *Operations Research,* vol. 65, no. 6, pp. 1615-1637, 2017

E. Israeli and R.K. Wood, "Shortest-path network interdiction," *Networks,* vol. 40, no. 2, pp. 97-111, 2002

L. Lozano and J.C. Smith, "A value-function-based exact approach for the bilevel mixed-integer programming problem," *Operations Research,* vol.65, no. 3, pp. 768-786, 2017.

L. Lozano and J.C. Smith, "A backward sampling framework for interdiction problems with fortification," *INFORMS Journal on Computing,* vol. 29, no. 1, pp. 123-139, 2017.

P.A. Ruiz, J.M. Foster, A. Rudkevich, and M.C. Caramanis, "Tractable transmission topology control using sensitivity analysis," *IEEE Transactions on Power Systems,* vol. 27, no. 3, pp. 1550-1559, 2012.

J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Transactions on Power Systems,* vol. 19, no. 2, pp. 905-912, 2004.

M.P. Scaparra and R.L. Church, "A bilevel mixed-integer program for critical infrastructure protection planning," *Computers & Operations Research,* vol. 35, no. 6, pp. 1905-1923, 2008.

S. Tahernejad, T.K. Ralphs, and S.T. DeNegre, "A branch-and-cut algorithm for mixed integer bilevel linear optimization problems and its implementation," *Mathematical Programming Computation,* vol. 12, no. 4, pp.529-568, 2020.

Y.Tang, J.-P. Richard, and J.C. Smith, "A class of algorithms for mixed-integer bilevel min-max optimization," *Journal of Global Optimization,* vol. 66, no. 2, pp. 225-262, 2016.

R.K. Wood, "Bilevel network interdiction models: formulations and solutions," *Wiley Encyclopedia of Operations Research and Management Science.* Ed. by J.J. Cochran, L.A. Cox Jr., P. Keskinocak, J.P. Kharoufeh, and J.C. Smith. New York: John Wiley & Sons, 2011.

D. Yue, J. Gao, B. Zeng and F. You, "A projection-based reformulation and decomposition algorithm for global optimization of mixed integer bilevel linear programs," *Journal of Global Optimization,* vol. 73, pp. 27-57, 2019.

B. Zeng and L. Zhao, "Solving two-stage robust optimization problems using a column-and-constraint generation method," *Operations Research Letters,* vol. 41, no. 5, pp. 457-461, 2013.