SAND2019-12887C

LDRD
Laboratory Directed Research and Development

Cyber Physical Optimization Modeling

Team Members

Anya Castillo

Bill Hart

Bryan Arguello

Cindy Phillips

Jared Gearhart

Presenter

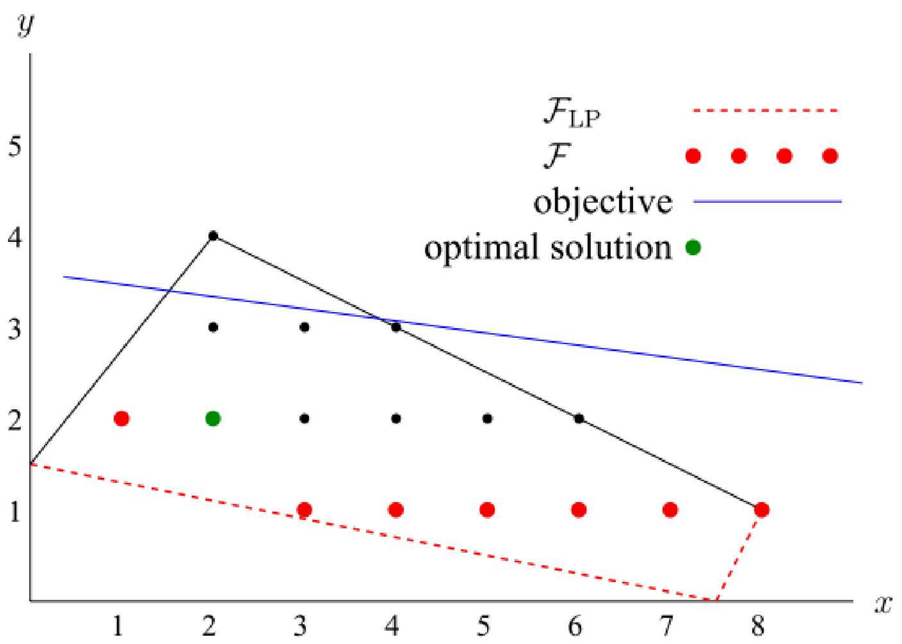
Bryan Arguello

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.

Optimization Thrust Outline

- Notes on Bilevel Programming
- Preliminary Cyber Physical Security Models
    - Worst Case Attacker Model
    - Stochastic Worst Case Attacker Model
    - Network Segmentation

Bilevel Programming



Follower's decision

$$\min_{x \in \mathbb{Z}_+} \; -x - 10y$$

$$\text{s.t.} \quad y \in \operatorname{argmin} \{ y : \begin{aligned} -25x + 20y &\le 30 \\ x + 2y &\le 10 \\ 2x - y &\le 15 \\ 2x + 10y &\ge 15 \\ y &\in \mathbb{Z}_+ \; \} \end{aligned}$$

Leader's decision

Figure 1: The feasible region of IBLP [Moore and Bard, 1990].

- Bilevel programs are very hard! NP-hard to be exact. In contrast to, say mixed-integer programming, there is no existing commercial technology for solving useful problems.

Mixed-Integer Programming vs Bilevel Programming

Mixed-Integer Programming (MIP)

- Major research began in late 1940's/early 1950's. By 1960's, commercially available solvers existed
- Mainstream commercial solver CPLEX invented in 1988. By the early 2000s—after incorporating academic research—it became a widely-used tool capable of solving real world problems
- Plethora of MIP research continues to improve solvers
- Solvers are so efficient that MIP is widely used for solving problems in many industries including energy, airline, health, finance, manufacturing

- **Bilevel Programming**
- Major research began in early 1980's
- No commercially available solvers exist to-date
- Up until the last few years, most progress on bilevel optimization has been on solving specific problems or classes of problems.

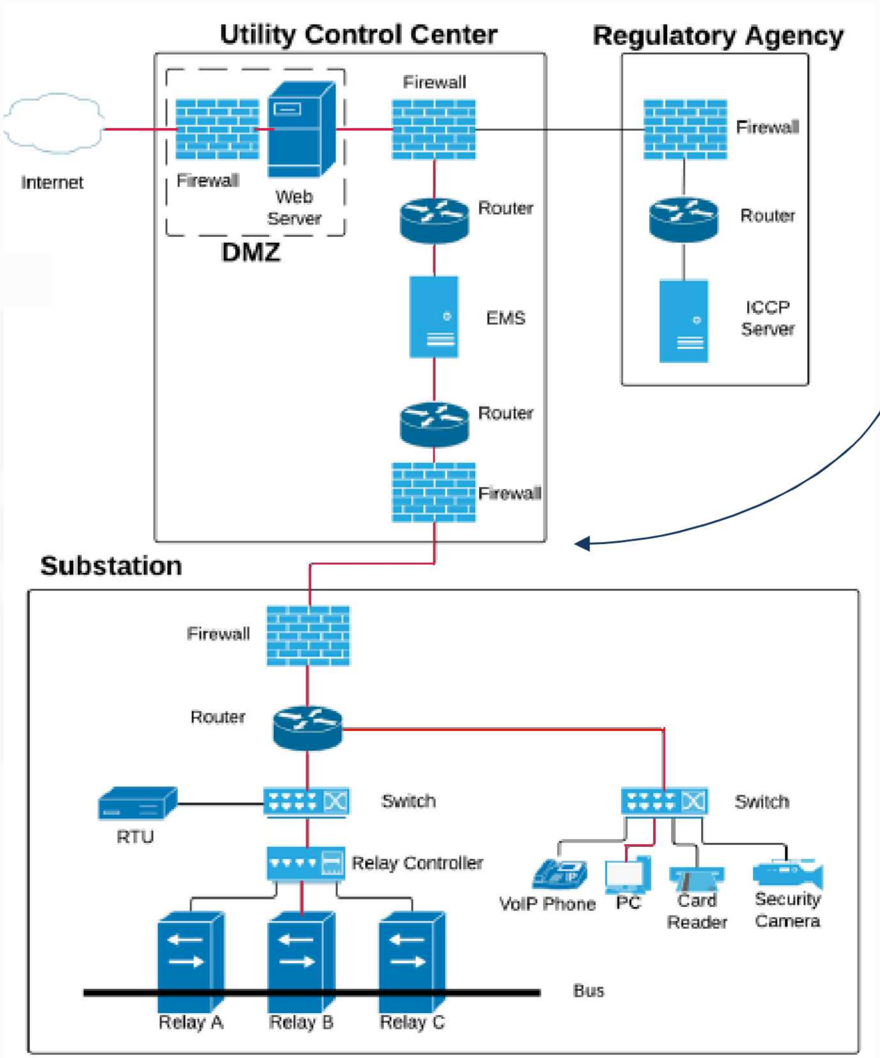
Recent Advances in Bilevel Programming

- Existing Software
  - MibS: Open-source bilevel programming branch-and-cut solver built using open-source COIN-OR software
  - CPLEX-based solver: European Academics (Fischetti, Ljubic, Monaci, and Sinnl) have developed solver based on their research for academic-use-only

- We would like to develop a similar solver built over Gurobi
  - We have Gurobi licenses
  - Greater control over software so we can add our own ideas into the solver

- General algorithms for solving hybrid discrete-continuous problems
  - "A projection-based reformulation and decomposition algorithm for global optimization of a class of mixed integer bilevel linear programs"
    - Coded by grad student intern She'ifa Punla
  - Academic Alliance partners at Georgia Tech interested in algorithms for solving these hard problems

Cyber Physical Attack Sequence Modeling

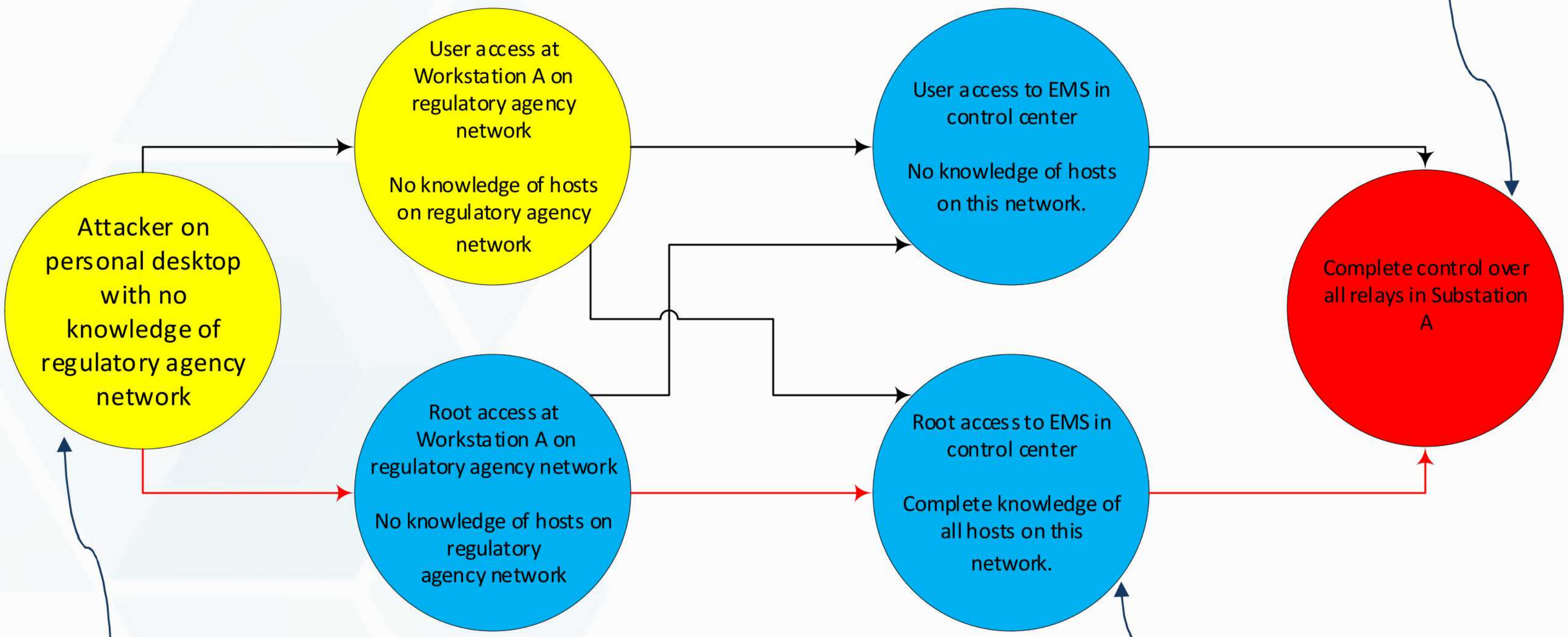


- Elements of cyber attack sequence
  - Sequence of hosts
  - Attacker access at hosts
  - Attacker actions at hosts
  - Network knowledge
  - Success probabilities
- Consider multiple attack sequences with some overlapping effort
- First question: while considering damage to the power grid, which attack sequences are most damaging?

Attack Graph

A simple example with 6 attack sequences…

Terminal nodes inflict damage on grid if reached



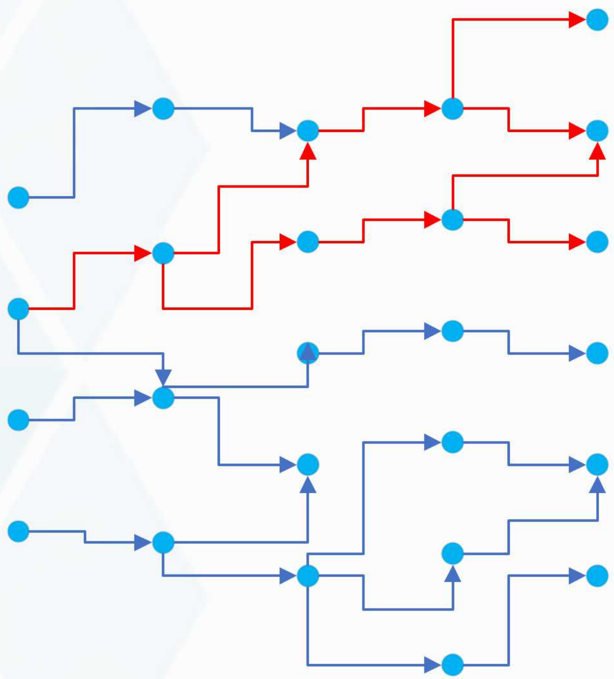
Attack sequences can only start at Initial nodes

Intermediate nodes can only be reached if at least one predecessor node is reached

Attack Graph Based Attack Model

A slightly more complicated example:

Multiple initial nodes possibly from multiple communication networks



Relays at multiple substations can be compromised and allow attacker to open loads, generators, or lines

Combining kill chains into a single graph allows for analysis of efficient coordinated attacks

Worst-Case Attacker Model

$$\max_{x,y,u,v,w,z} \gamma(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}, \boldsymbol{z})$$

$s.t.$

$$\sum_{e \in \mathcal{T}} D_e x_e \leq B$$

$$x_{e'} \leq \sum_{e \in \mathcal{T}_r} x_e$$

$$x_e \leq y_r$$

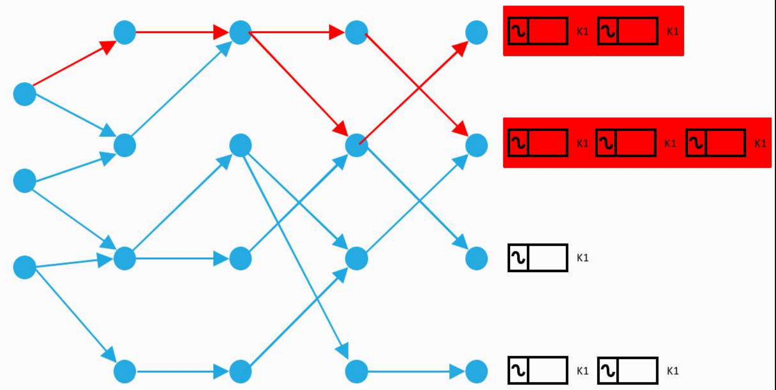
$$y_r \leq \sum_{e \in \mathcal{T}_r} x_e$$

$$\sum_{r \in \mathcal{R}_l} (1 - y_r) - |\mathcal{R}_l| + 1 \leq u_l \leq (1 - y_r)$$

$$\sum_{r \in \mathcal{R}_k} (1 - y_r) - |\mathcal{R}_k| + 1 \leq v_k \leq (1 - y_r)$$

$$\sum_{r \in \mathcal{R}_g} (1 - y_r) - |\mathcal{R}_g| + 1 \leq w_g \leq (1 - y_r)$$

Attack Model



$$\gamma(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}, \boldsymbol{z}) = \min_{\boldsymbol{\theta}, \boldsymbol{p}, \boldsymbol{p}^{\boldsymbol{G}}, \boldsymbol{p}^{\boldsymbol{L},S}} \sum_{b \in \mathcal{B}} p_b^{L,S}$$

$s.t.$

$$p_k = v_k B_k(\theta_{o(k)} - \theta_{d(k)} - \Theta_k)$$

$$\sum_{g \in \mathcal{G}_b} p_g^G - \sum_{k \in \{k' | o(k') = b\}} p_k + \sum_{k \in \{k' | d(k') = b\}} p_k = \sum_{l \in \mathcal{L}_b} P_l^L - p_b^{L,S}$$

$$-S_k^{\max} \leq p_k \leq S_k^{\max}$$

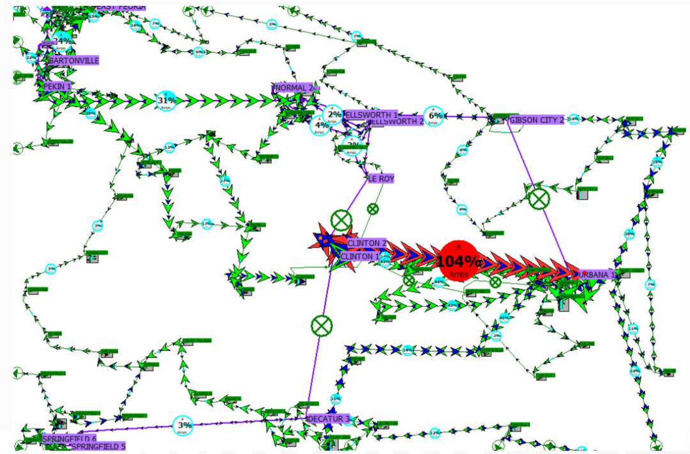
$$w_g P_g^{G,min} \leq p_g^G \leq w_g P_g^{G,max}$$

$$\sum_{l \in \mathcal{L}_b} (1 - u_l) P_l^L \leq p_b^{L,S} \leq \sum_{l \in \mathcal{L}_b} P_l^L$$

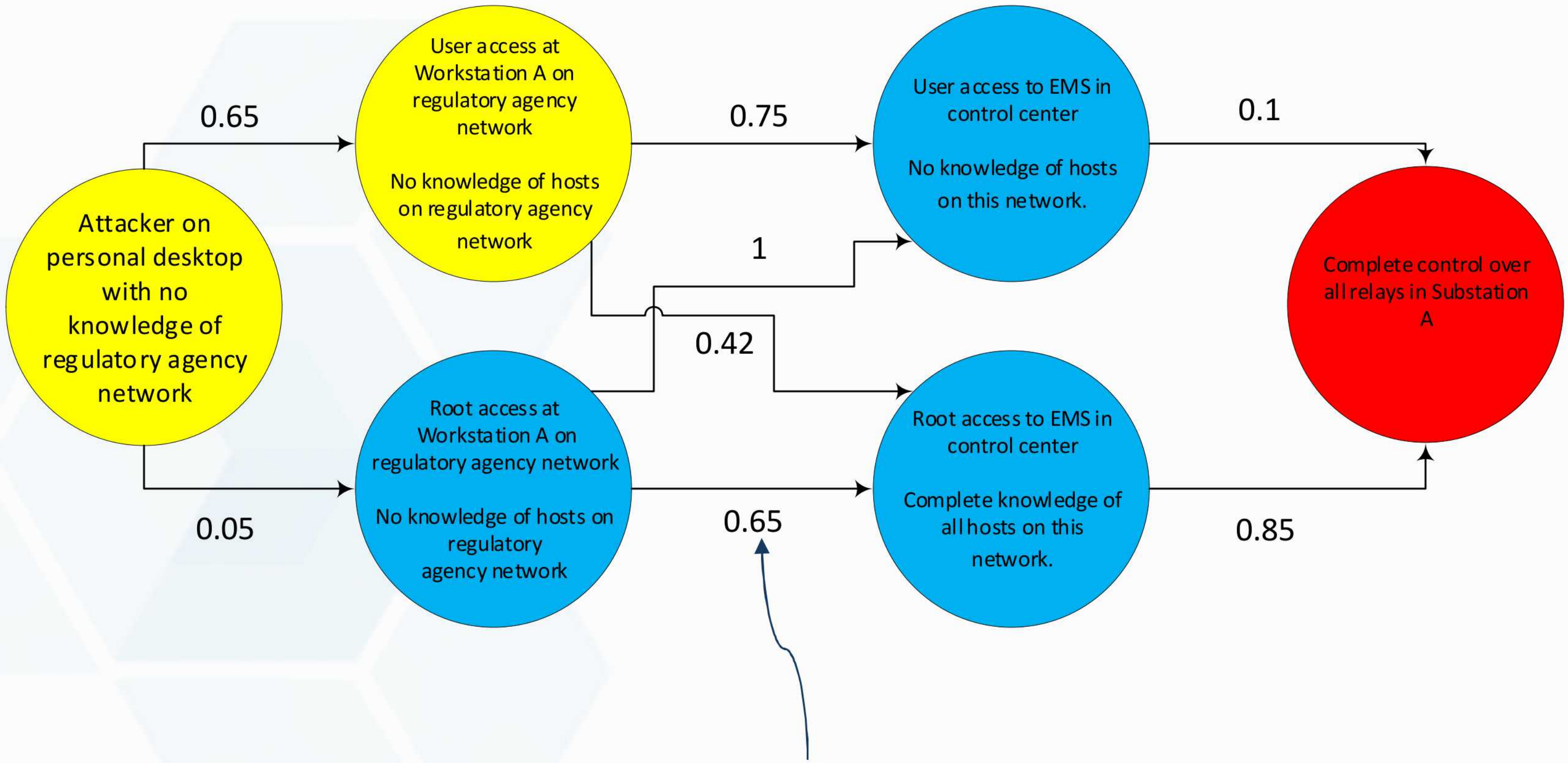
$$-\pi \leq \theta_b \leq \pi$$

Damage Control

Optimal Power Flow



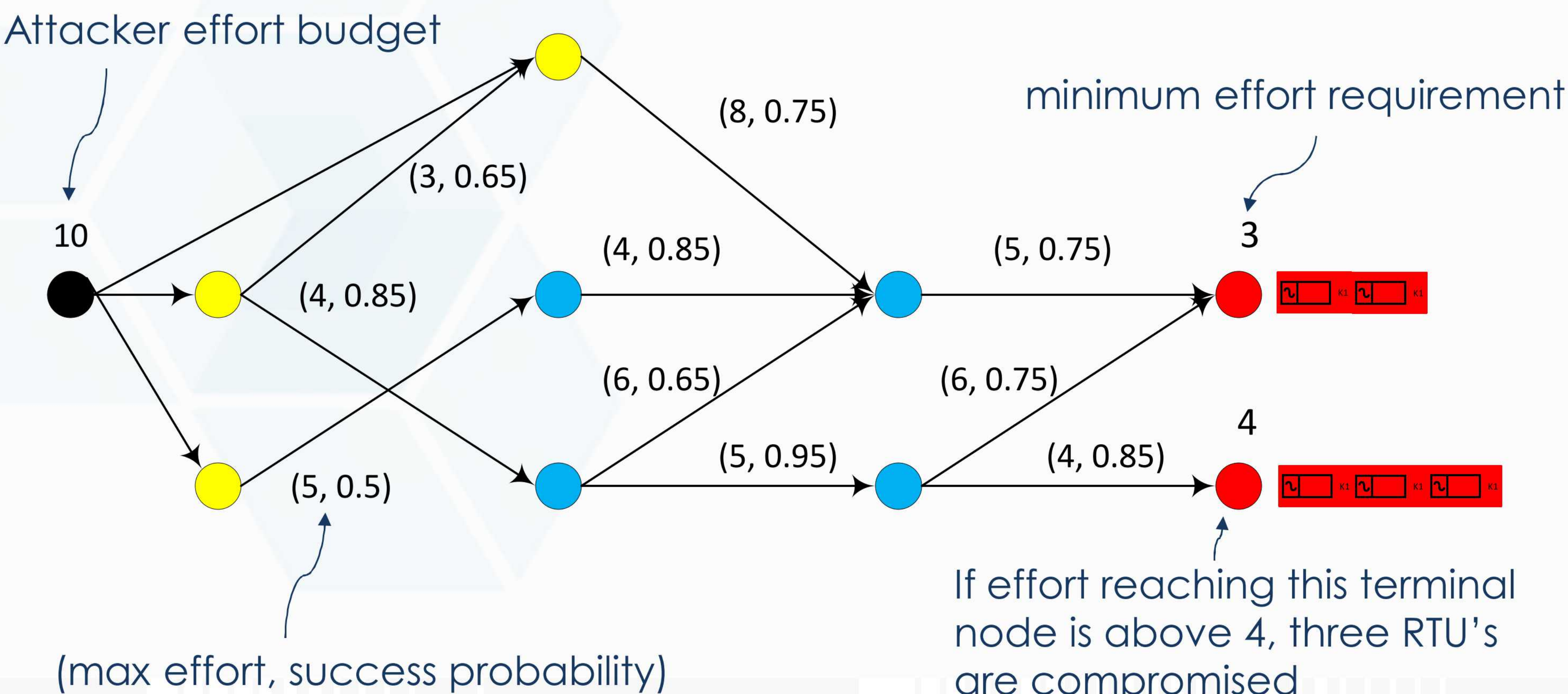
Stochastic Attack Graph



Now let's add edge probabilities to model difficulty in moving between nodes

Stochastic Attack Graph Based Attack Model

- Use maximum flow with multiple sinks
- Interpret flow as “effort”
- Edge probabilities cause effort leaking
- Generalize max flow by considering power grid reaction to attack…



Stochastic Worst-Case Attack Model

$$\max_{a,z,\delta,u,v,w} \gamma(u,v,w)$$

$s.t.$

$$\sum_{e\in\mathcal{E}_{F(s)}} a_e = B$$

Stochastic Attack Model →

$$z_s = \sum_{e\in\mathcal{E}_{T(s)}} P_e^{\omega} a_e$$

$$\sum_{e\in\mathcal{E}_{F(s)}} a_e = \sum_{e\in\mathcal{E}_{T(s)}} P_e^{\omega} a_e$$

$$a_e \le u_e$$

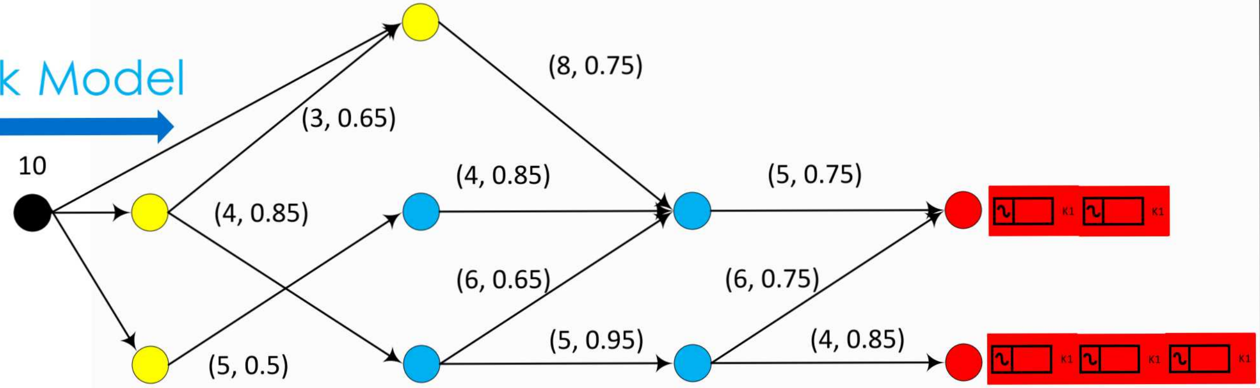
$$t_s \delta_r \le z_s$$

$$\sum\nolimits_{r\in\mathcal{R}_l} (1-y_r) - |\mathcal{R}_l| + 1 \le u_l \le (1-y_r)$$

$$\sum\nolimits_{r\in\mathcal{R}_k} (1-y_r) - |\mathcal{R}_k| + 1 \le v_k \le (1-y_r)$$

$$\sum\nolimits_{r\in\mathcal{R}_g} (1-y_r) - |\mathcal{R}_g| + 1 \le w_g \le (1-y_r)$$

$$\gamma(u,v,w) = \min_{\theta,p,p^G,p^{L,S}} \sum\nolimits_{b\in\mathcal{B}} p_b^{L,S}$$



$s.t.$

Damage Control →

$$p_k = v_k B_k(\theta_{o(k)} - \theta_{d(k)} - \Theta_k)$$

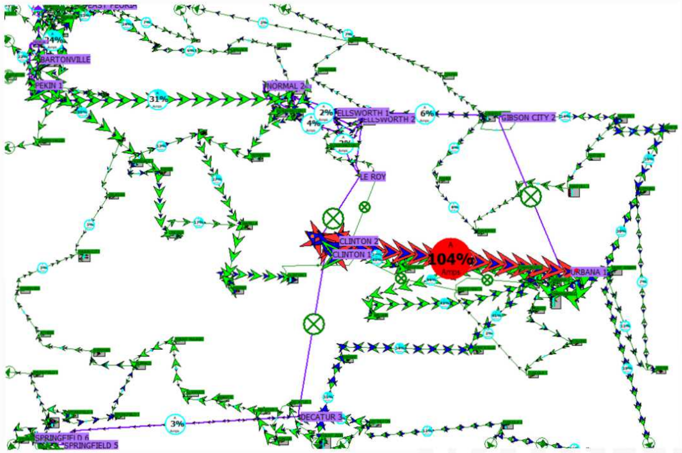
$$\sum\nolimits_{g\in\mathcal{G}_b} p_g^G - \sum\nolimits_{k\in\{k'|o(k')=b\}} p_k + \sum\nolimits_{k\in\{k'|d(k')=b\}} p_k = \sum\nolimits_{l\in\mathcal{L}_b} P_l^L -$$

$$-S_k^{\max} \le p_k \le S_k^{\max}$$

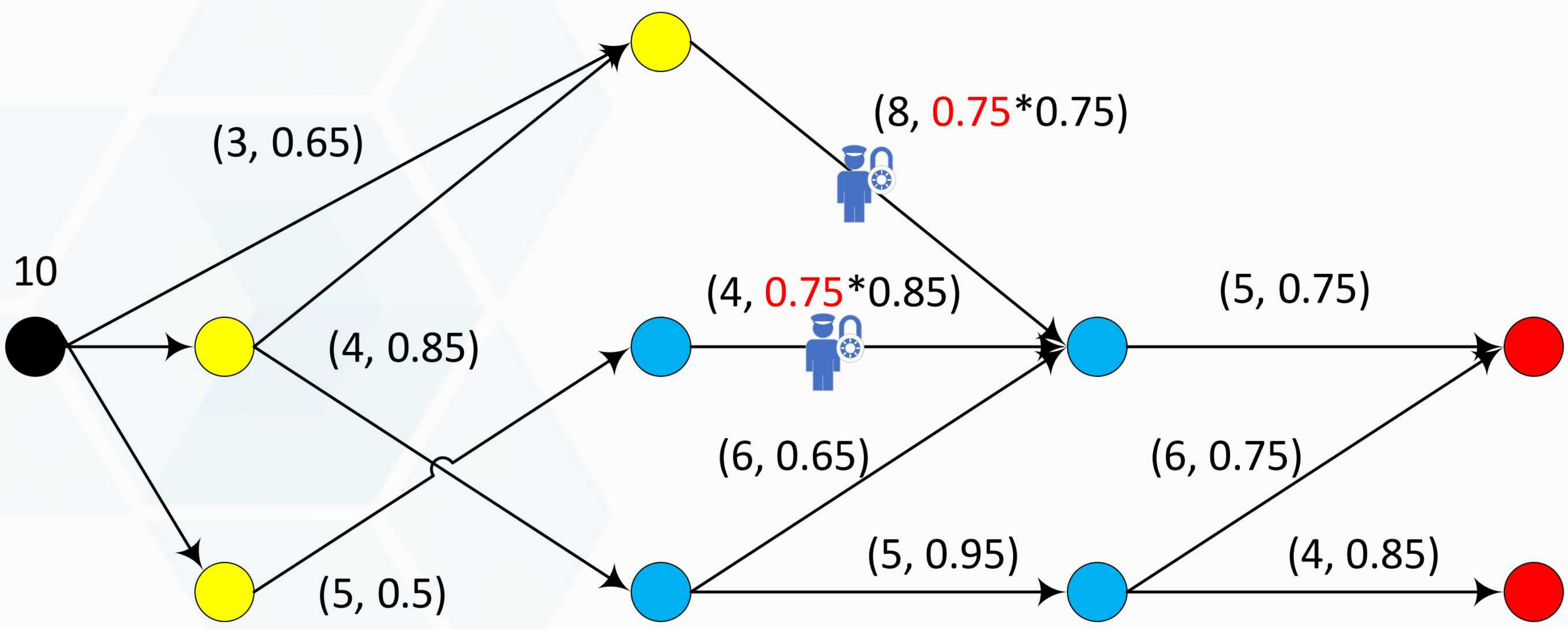
$$w_g P_g^{G,min} \le p_g^G \le w_g P_g^{G,max}$$

$$\sum\nolimits_{l\in\mathcal{L}_b} (1-u_l) P_l^L \le p_b^{L,S} \le \sum\nolimits_{l\in\mathcal{L}_b} P_l^L$$

$$-\pi \le \theta_b \le \pi$$

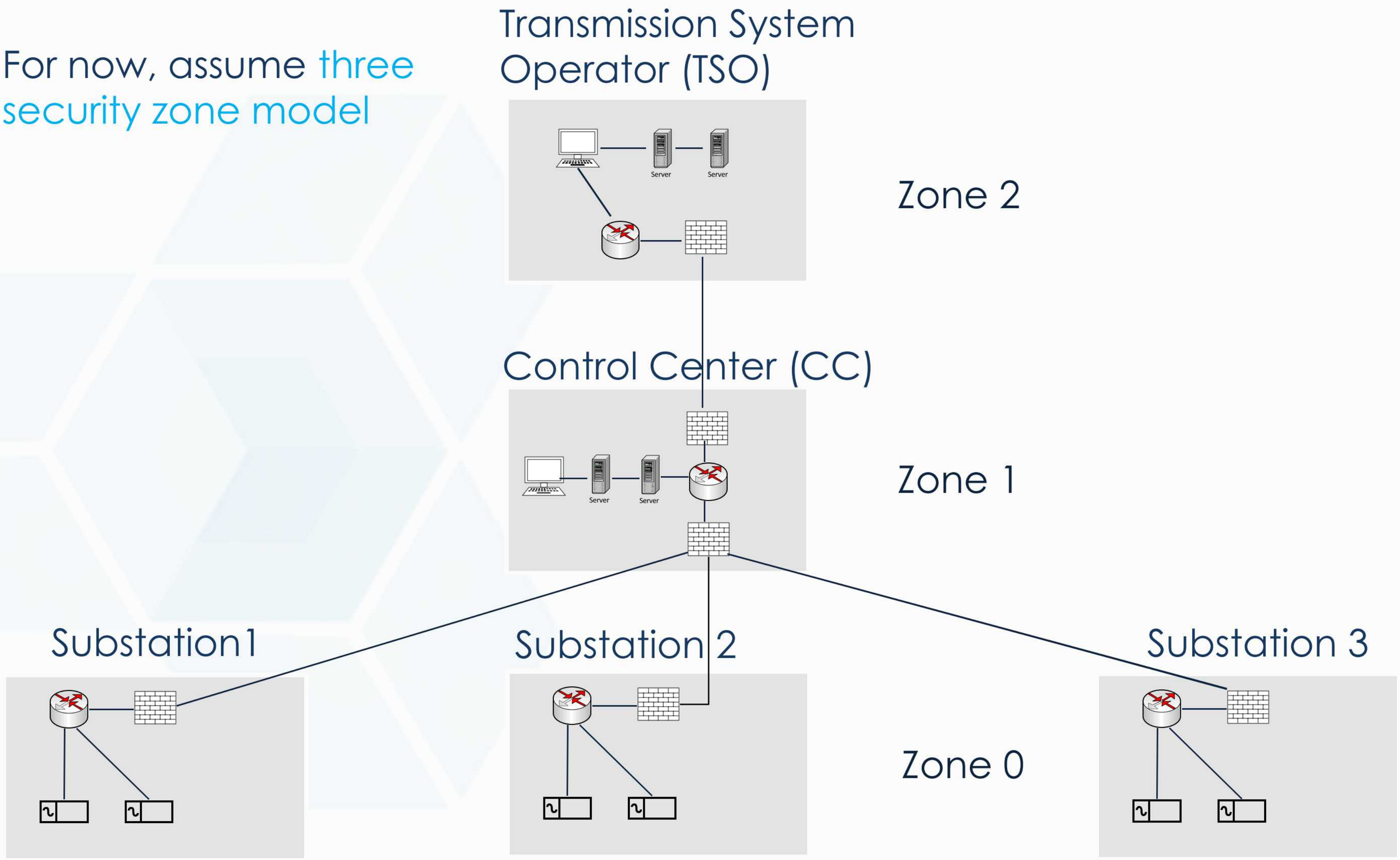


Intrusion Detection System Placement

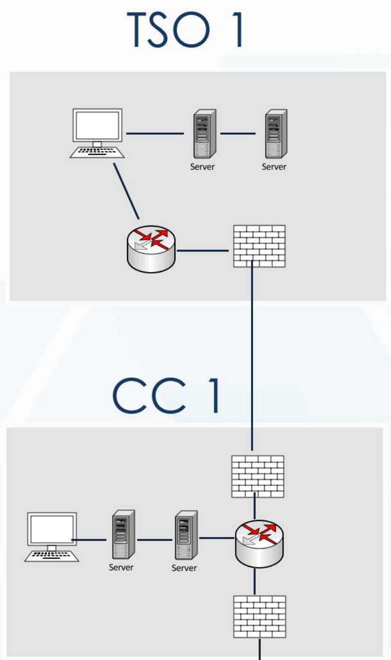


Network Segmentation Problem

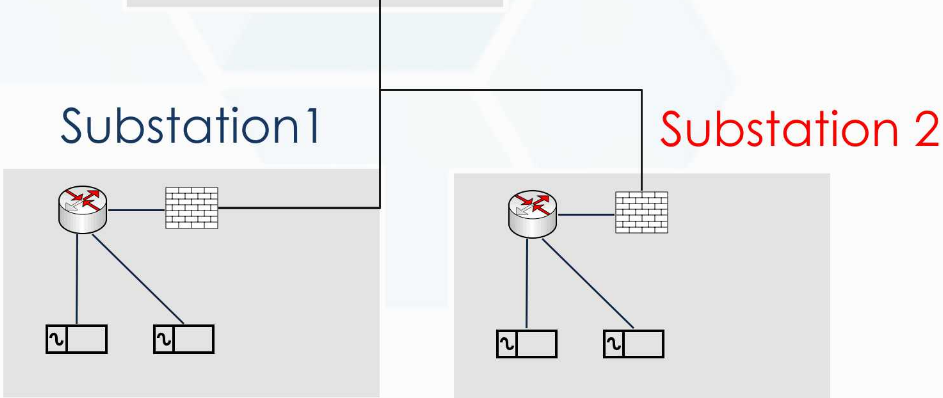
For now, assume three security zone model

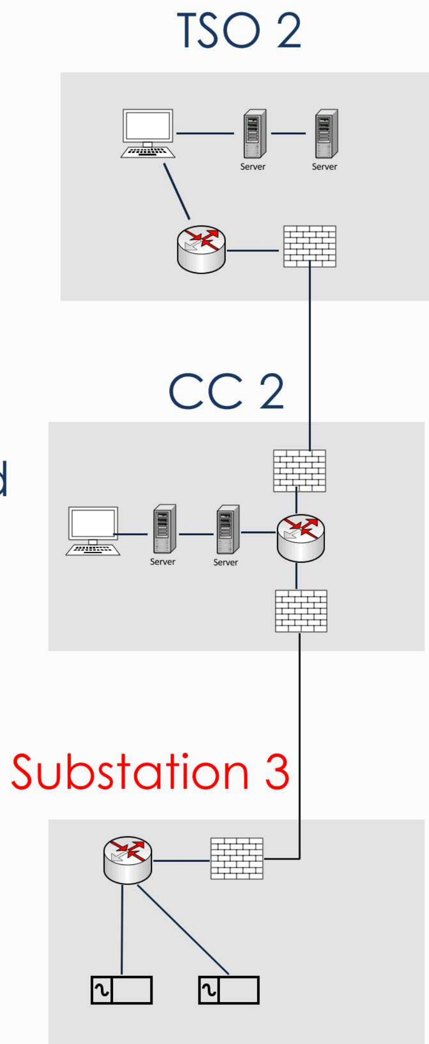


Network Segmentation Problem



- The grid can be severely damaged when Substation 2 and Substation 3 are attacked together.
- Substation 1 and Substation 2 are configured so that the grid is fine if they are attacked together.





Network Segmentation Model

$$\min_{x,y} \gamma(x,y)$$

s.t.

$$\sum_{f\in\mathcal{F}-\{T\}} x_{r,f} = 1$$

$$\sum_{\{f>e\}} y_{e,f} = 1$$

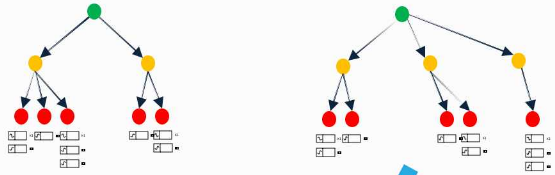
$$l_T = 3$$

$$l_f \le 2(1-\sum_{r\in\mathcal{R}} x_{r,f})$$

$$l_f \ge y_{e,f}(l_e+1)$$

$$l_e \le y_{e,f}(l_f-1) + 2(1-y_{e,f})$$

Network Segmentation



$$\gamma(x,y) = \max_{z,\delta} \lambda(u,v,w)$$

$$\sum_{e\in\mathcal{F}} z_e \le B$$

$$z_e \le \sum_{f>e} y_{e,f} z_f + y_{e,T}$$

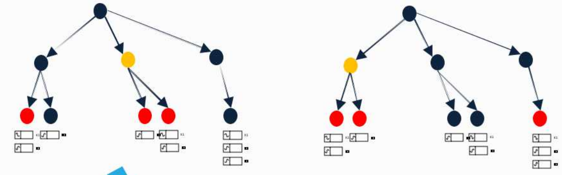
$$\delta_r = \sum_{e\in\mathcal{F}} x_{r,e} z_e$$

$$\sum_{r\in\mathcal{R}_k} (1-\delta_r) - |\mathcal{R}_k| + 1 \le v_k \le (1-\delta_r),$$

$$\sum_{r\in\mathcal{R}_l} (1-\delta_r) - |\mathcal{R}_l| + 1 \le u_l \le (1-\delta_r),$$

$$\sum_{r\in\mathcal{R}_l} (1-\delta_r) - |\mathcal{R}_l| + 1 \le w_g \le (1-\delta_r),$$

Attack Model



$$\lambda(u,v,w) = \min_{\theta,p,p^G,p^{L,S}} \sum_{b\in\mathcal{B}} p_b^{L,S}$$

s.t.

$$p_k = v_k B_k(\theta_{o(k)} - \theta_{d(k)} - \Theta_k)$$

$$\sum_{g\in\mathcal{G}_b} p_g^G - \sum_{k\in\{k'|o(k')=b\}} p_k + \sum_{k\in\{k'|d(k')=b\}} p_k = \sum_{l\in\mathcal{L}_b} P_l^L - p_b^{L,S}$$

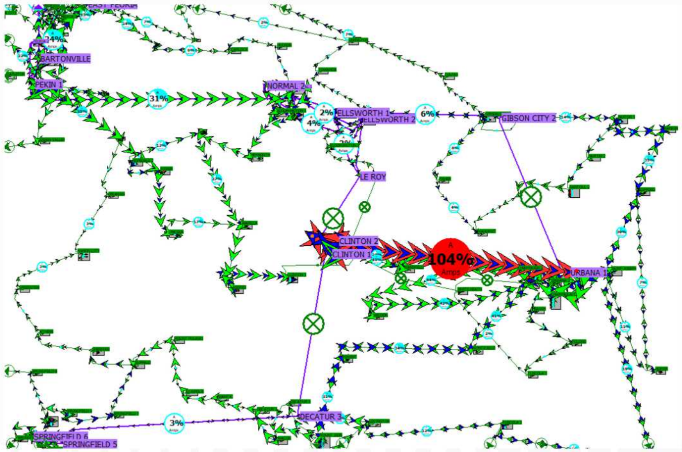
$$-S_k^{\max} \le p_k \le S_k^{\max}$$

$$w_g P_g^{G,max} \le p_g^G \le w_g P_g^{G,max}$$

$$\sum_{l\in\mathcal{L}_b} (1-u_l) P_l^L \le p_b^{L,S} \le \sum_{l\in\mathcal{L}_b} P_l^L$$

$$-\pi \le \theta_b \le \pi$$

Damage Control



Future Extensions of Network Segmentation

- Network segmentation pricing
  - Assign a cost to each subnet that depends on security zone
  - Use a budget to limit the overall cost of network segmentation

- If necessary, add subnet detail so that a subnet is more than just a node. Preferably don't since this model requires minimal SME data.
  - Use caution when adding model detail. We must remember that these bilevel models are incredibly difficult to solve