SAND2019-12885C

LDRD

Laboratory Directed Research and Development

# Cyber Physical Optimization Modeling

***Team Members***

*Anya Castillo*

*Bill Hart*

*Bryan Arguello*

*Cindy Phillips*

*Jared Gearhart*

***Presenter***

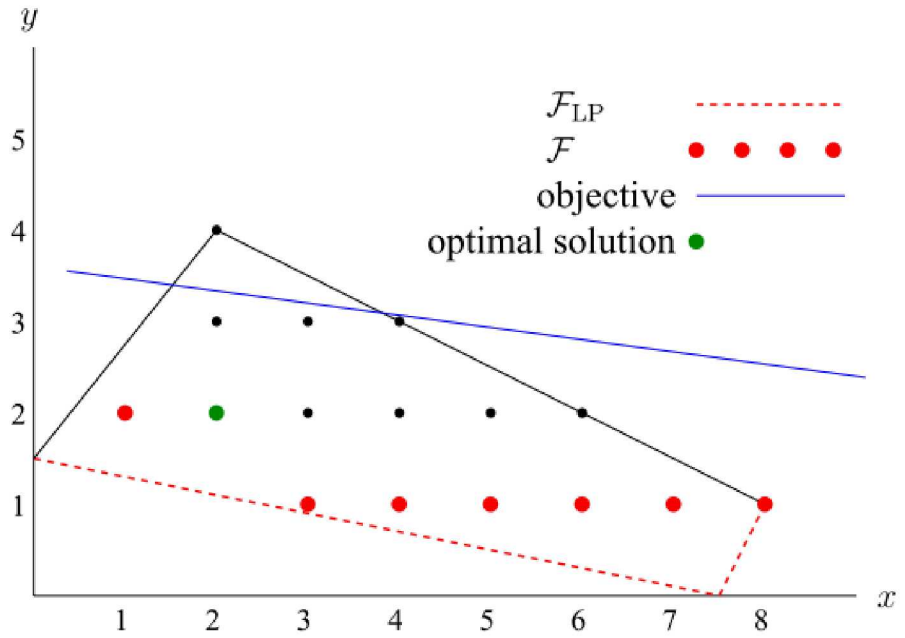
*Bryan Arguello*

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
  - Vulnerability Analysis
  - Intrusion Detection System Placement
  - Network Segmentation
- Emulytics Optimization
- Publications and External Engagements

# Bilevel Programming




Follower's decision

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

$$\text{s.t.} \quad y \in \operatorname{argmin}\{y :$$

$$\begin{aligned} -25x + 20y &\leq 30 \\ x + 2y &\leq 10 \\ 2x - y &\leq 15 \\ 2x + 10y &\geq 15 \\ y &\in \mathbb{Z}_+ \; \} \end{aligned}$$

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.

# Bilevel Programming Community

- I presented basic Pyomo Bilevel capabilities at the 2018 2nd International Workshop of Bilevel Programming


- We should plan to attend the 3rd International Workshop of Bilevel Programming in 2020 to be up-to-date on research and network with the experts. We have already begun some networking…

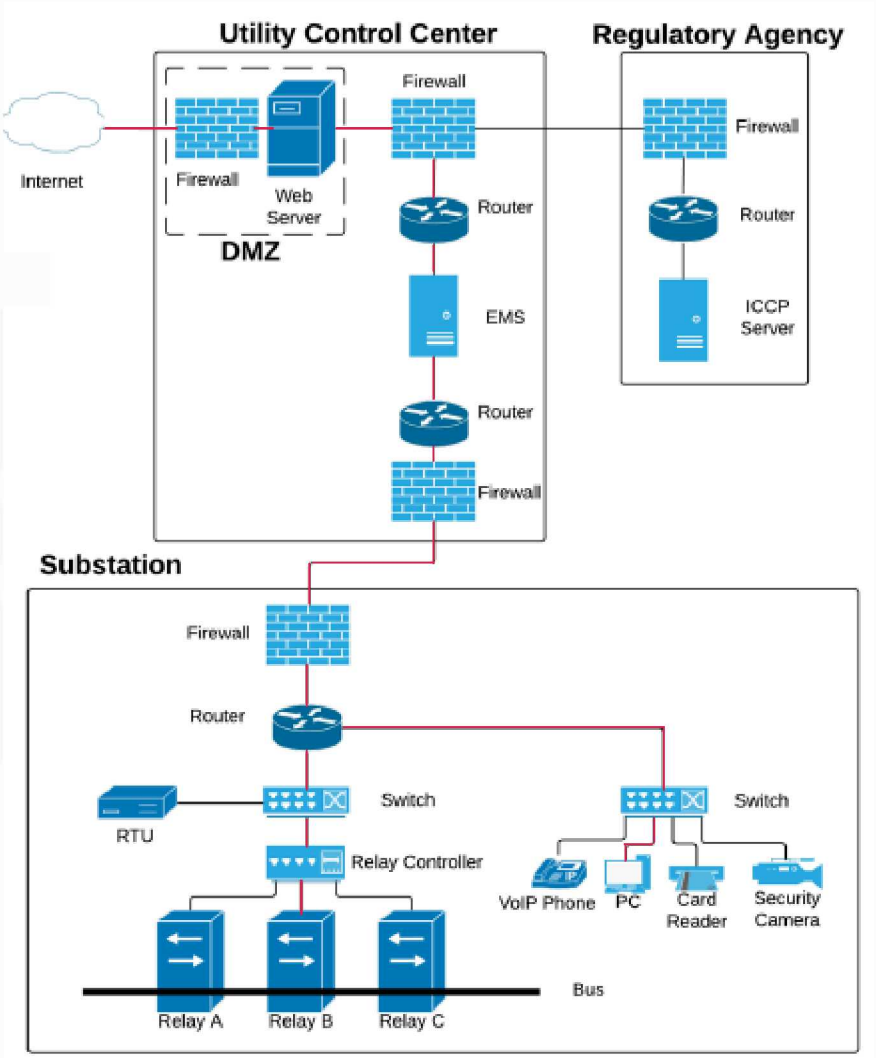
# Recent Advances in Bilevel Programming

- 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

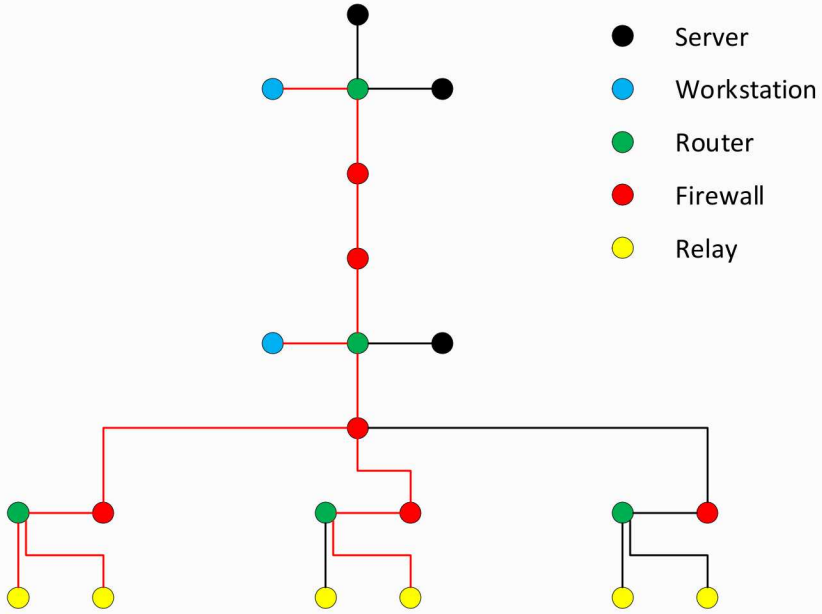
# Attacker Modeling




- Core modeling component is attacker modeling via cyber kill chains
- Elements of cyber kill chains
  - Sequence of hosts
  - Attacker access at hosts
  - Attacker actions at hosts
  - Network knowledge
  - Success probabilities
- Care must be taken in modeling cyber kill chains using optimization
  - Not enough detail => model may not be useful
  - Too much detail => model may be too difficult to solve

# Simple Topology Based Attack Model

- Communication network modeled as a graph where hosts are nodes and edges represent host connectivity
  - Does model:
    - This model only accounts for the sequence of host access obtained in a kill chain
  - Does not model:
    - Access type
    - Actions and network knowledge



# Simple Topology Based Attack Model

- Attack matrix:

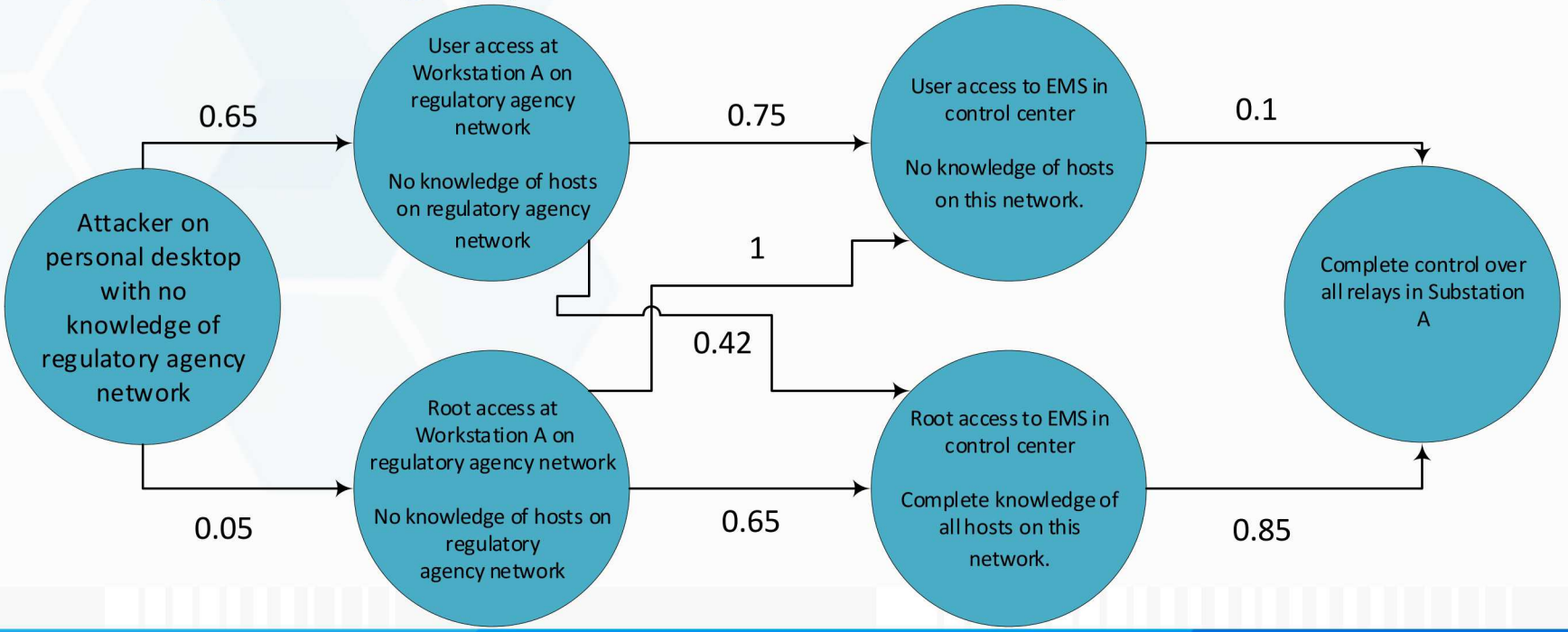
$P_{BA} = P(attacker\ can\ gain\ root\ access\ to\ A \mid attacker\ has\ root\ access\ to\ B)$

$$\begin{array}{c} \begin{matrix} A & B & C & D & E & F & G \end{matrix} \\ \begin{pmatrix} 1 & 0.65 & 0.60 & 0.55 & 0.50 & 0.50 & 0.50 \\ 0.65 & 1 & 0.75 & 0.70 & 0.65 & 0.65 & 0.65 \\ 0 & 0.75 & 1 & 0.85 & 0.80 & 0.80 & 0.80 \\ 0 & 0 & 0.85 & 1 & 0.95 & 0.95 & 0.95 \\ 0 & 0 & 0 & 0.95 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0.95 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0.95 & 1 & 1 & 1 \end{pmatrix} \begin{matrix} A \\ B \\ C \\ D \\ E \\ F \\ G \end{matrix} \end{array}$$

- Reachability matrix:
  - Replace nonzero entries with 1's

# Attack Graph Based Attack Model

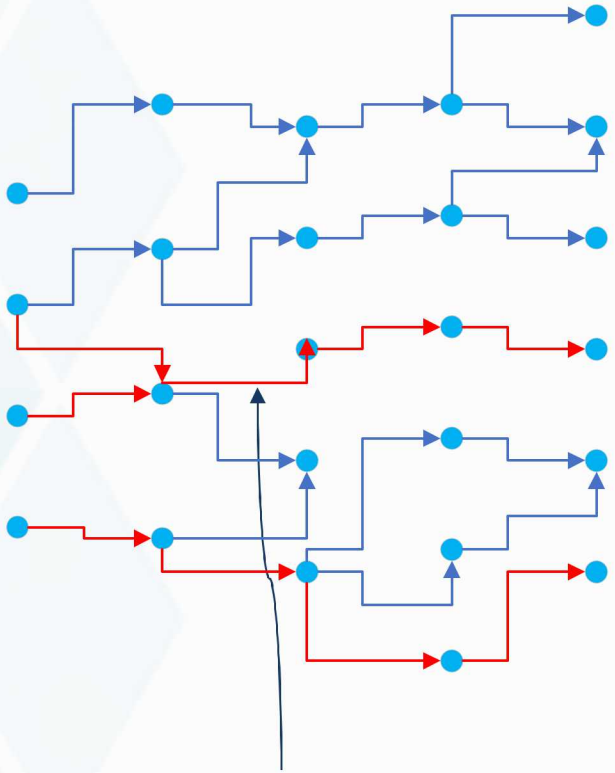
- Attack graph models cyber kill chains
  - Nodes are cyber states. Cyber states represent the stages of an attacker in a kill chain. They include any relevant information such as:
    - Host under attack
    - Host access
    - Current knowledge
  - Edges represent transitions between cyber states and hold probability of moving from origin cyber state to destination cyber state



# Attack Graph Based Attack Model

A slightly more complicated example:

Multiple attackers starting from multiple cyber states



Relays at multiple substations can be compromised

This transition can be used by two different cyber attacks. Possibly a coordinated attack.

# Attack Graph Based Attack Model

- Model gives fidelity as a choice
  - Attack graph can be as course as topology-based attack model
  - Each node can represent most/all cyber attack information leading to a detailed attack graph
- This approach is heavily dependent on SME input data
  - Relevant and likely cyber kill chains are needed for the whole communication network of interest
  - Probability needed between every two pairs of cyber states where a transition is probable
- Attack graph can be huge!
  - May include communication networks over various regulatory agencies, control centers, and substations

# Attacker-Defender Model

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

$s.t.$

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

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

$$x_e \le y_r$$

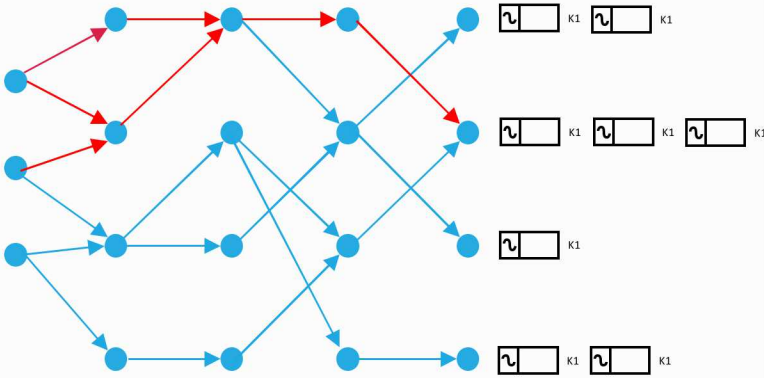
$$y_r \le \sum_{e\in\mathcal{T}_r} x_e$$

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

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

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

Attack Model




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

$s.t.$

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

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

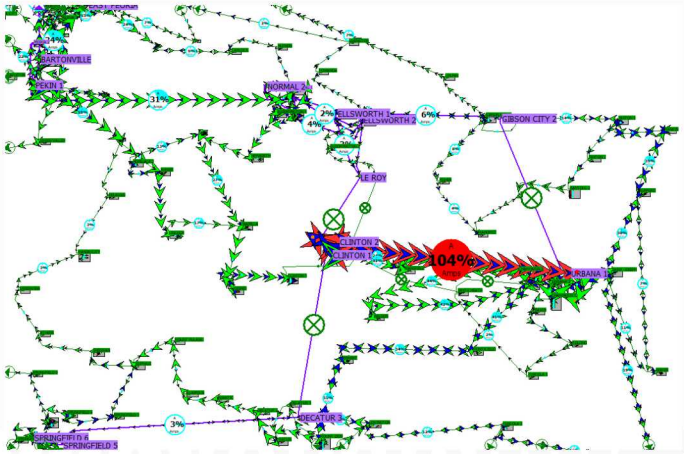
$$-S_k^{\max} \le p_k \le S_k^{\max}$$

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

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

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

Damage Control

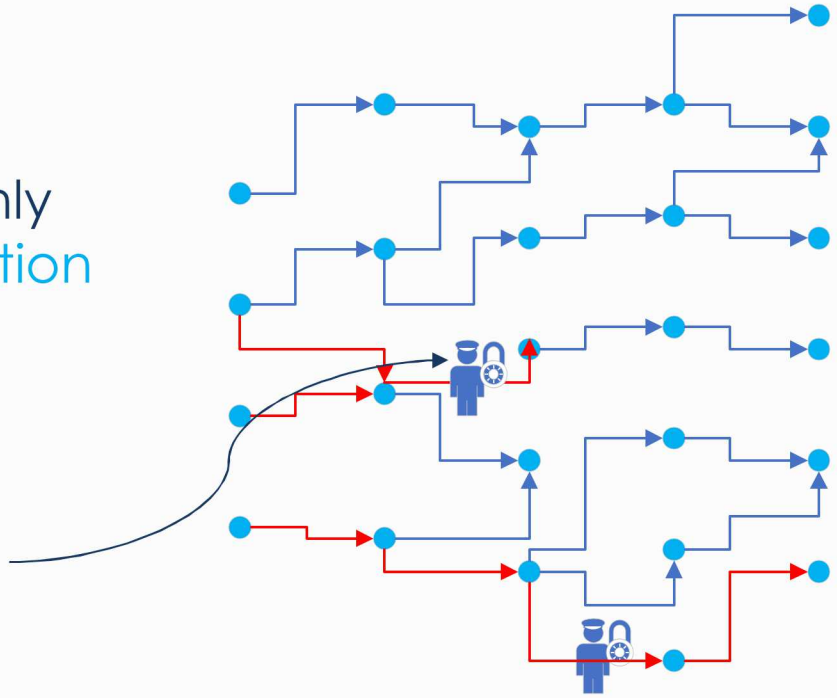


# Intrusion Detection System (IDS) Placement

- IDS are expensive, so they must be added to network sparingly

- They do not guarantee that an attack will be detected; they only increase the likelihood of detection

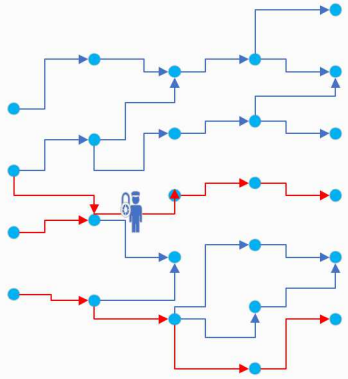
Strategic IDS placement that can mitigate two different attacks



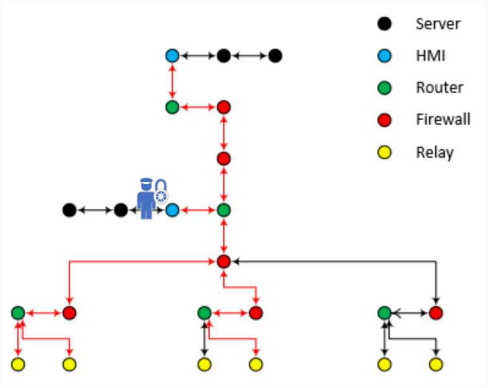
This IDS may not even detect the depicted attack

# IDS Placement Modeling

- IDS placement is a Designer-Attacker-Defender (DAD) type model.
  - The network designer decides where to optimally place IDS's.
  - After placement, the attacker executes optimal attack plan.
  - Control center defends using damage control (DC optimal power flow) to minimize unmet demand.

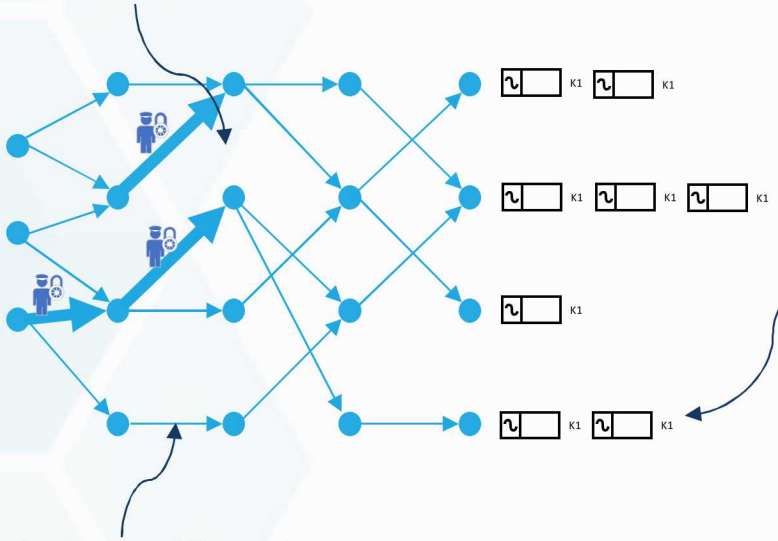


- From our vulnerability analysis modeling, we have choices with respect to attacker modeling



# IDS Placement Modeling

Placement of IDS's increase detection probabilities

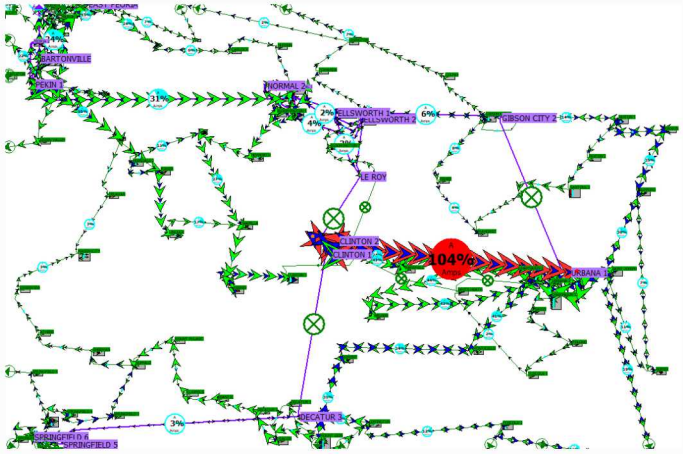


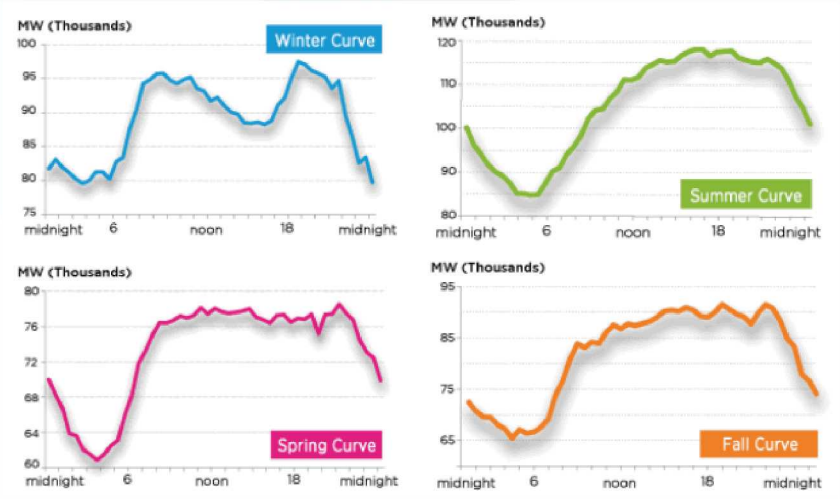

Loss metric such as controlled power capacity associated with each RTU

Each transition has a detection probability pre-IDS's placement

# Defender in IDS Placement Model

First model iteration includes no defender damage control via power flow




Such an approach allows the designer to consider seasonal load variation

# Intrusion Detection System Placement Model

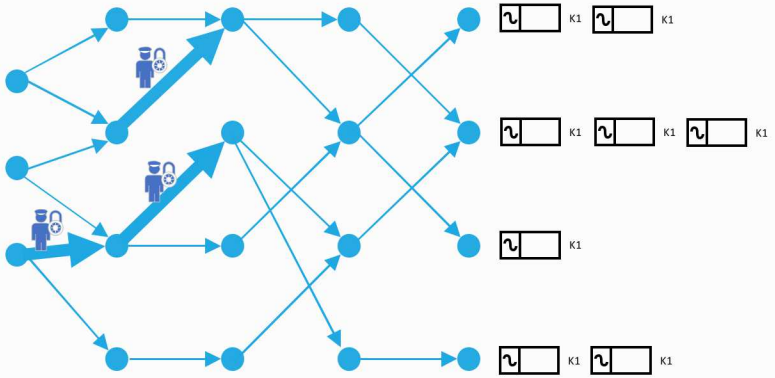
$$\min_{\boldsymbol{d}\in\{0,1\}^{|\mathcal{E}|},\boldsymbol{i}\in\{0,1\}^{|\mathcal{R}|}} \sum_{\omega\in\Omega} Pr(\omega)\gamma^{\omega}(\boldsymbol{d},\boldsymbol{i})$$

IDS Placement

$$\sum_{r\in\mathcal{R}} C_r^d i_r \le B^D$$

$$i_r \le d_e$$

$$\gamma^{\omega}(\boldsymbol{d},\boldsymbol{i}) = \max_{\boldsymbol{a},\boldsymbol{\alpha},\boldsymbol{z}} \sum_{s\in\mathcal{S}_f} L_s z_s$$




$$s.t.$$

$$\sum_{e\in\mathcal{E}} C_e^A(a_e+\alpha_e) \le B^A$$

$$\sum_{e\in\mathcal{E}_{F(s)}} (a_e+\alpha_e) = 1$$

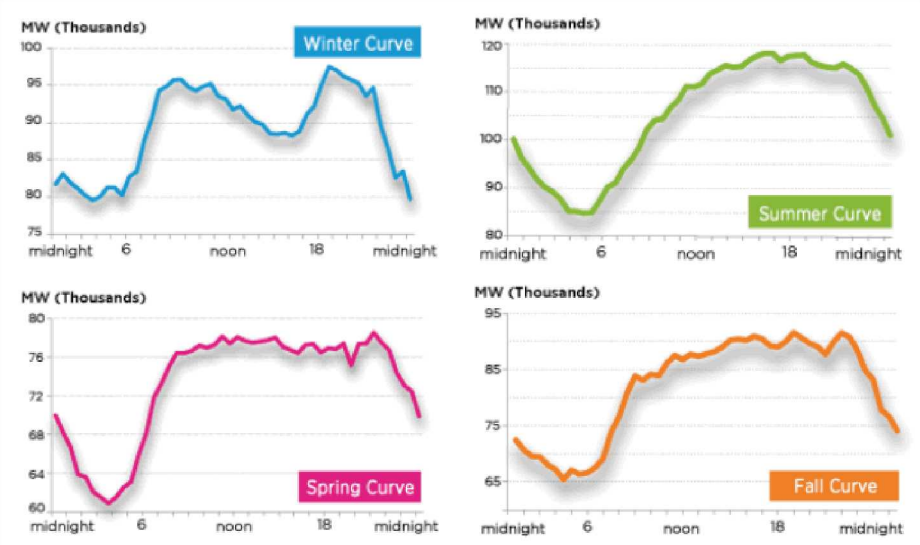
$$z_s - \sum_{e\in\mathcal{E}_{T(s)}} (P_e^{\omega}a_e + Q_e^{\omega}\alpha_e) = 0$$

$$\sum_{e\in\mathcal{E}_{F(s)}} (a_e+\alpha_e) - \sum_{e\in\mathcal{E}_{T(s)}} (P_e^{\omega}a_e + Q_e^{\omega}\alpha_e) = 0$$

$$0 \le a_e \le 1-d_e$$

$$0 \le \alpha_e \le d_e$$

Scenario-dependent Attacker

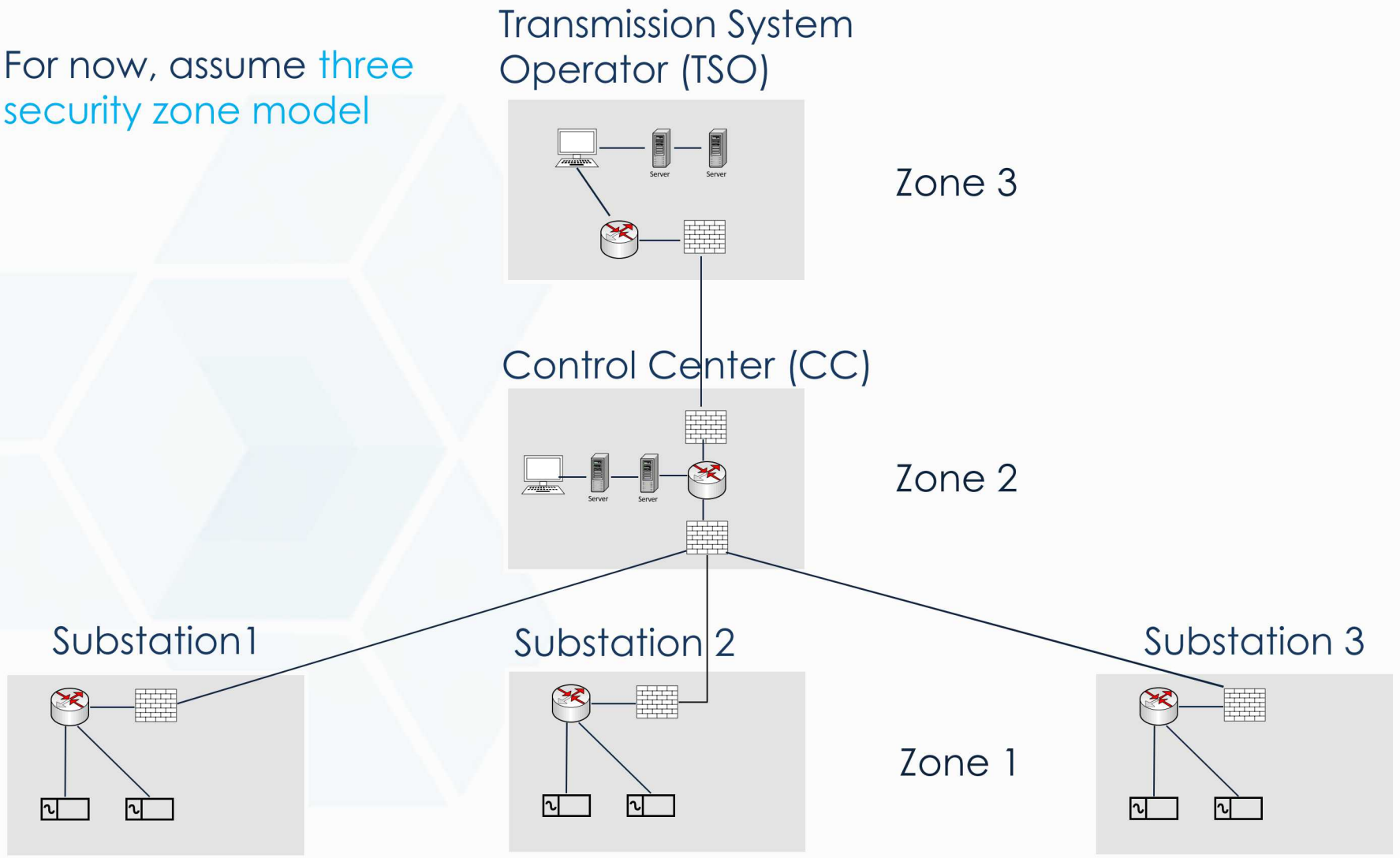


# Future Extensions of IDS Placement Model

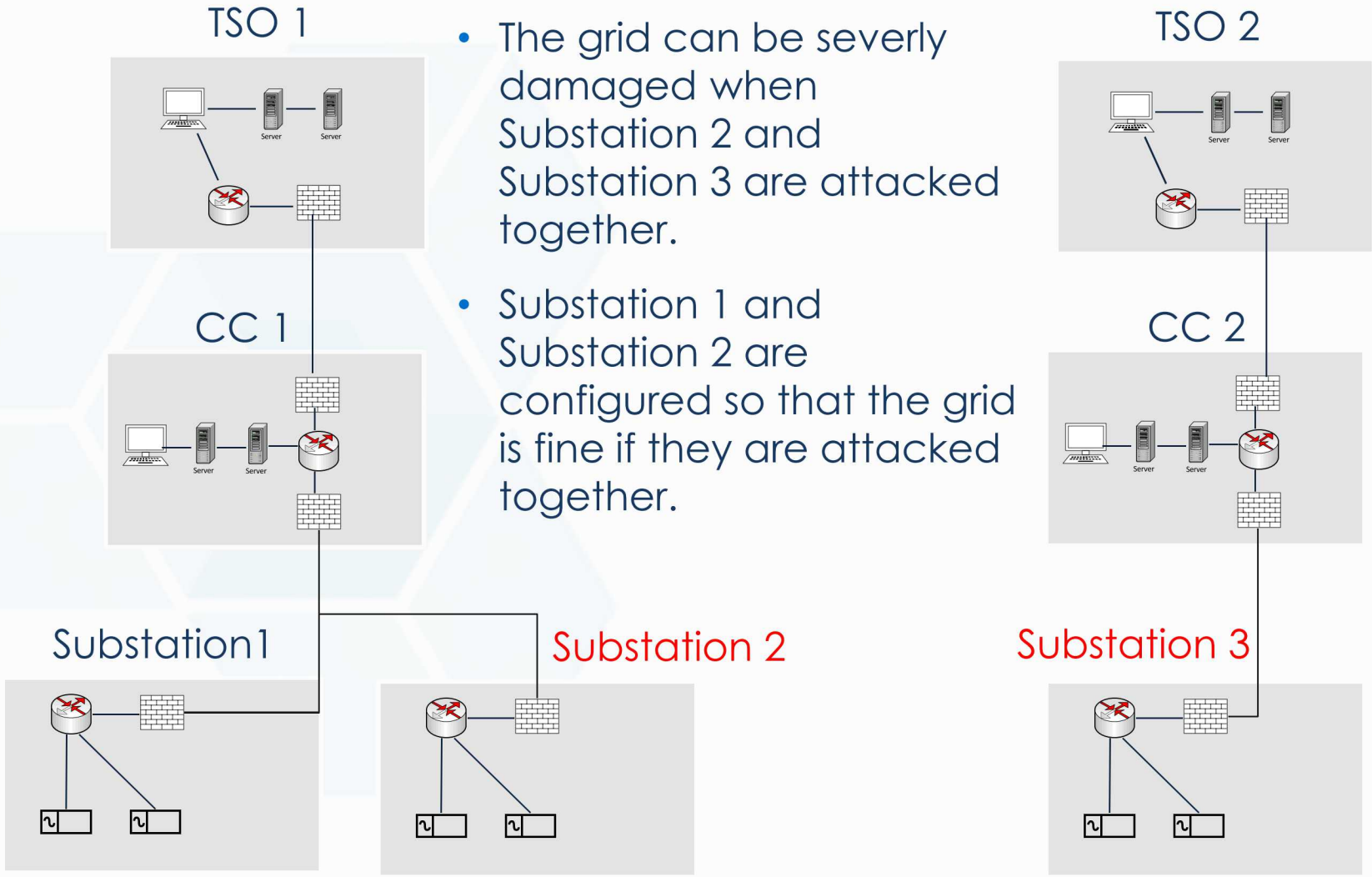
- Current model assumes attacker knowledge of where IDS's are placed
  - Designer places IDS's to increase particular intrusion detection probabilities
  - Attacker should not know where IDS's were placed and how probabilities changed
- Add power flow to allow damage control

# Network Segmentation Problem

For now, assume three security zone model



# Network Segmentation Problem




- The grid can be severly 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

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

$$s.t.$$

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

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

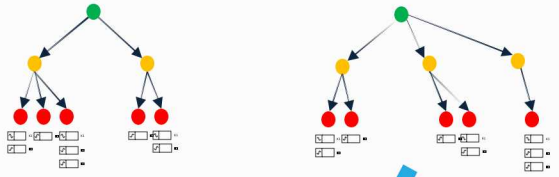
$$l_T = 3$$

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

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

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

Network Segmentation



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

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

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

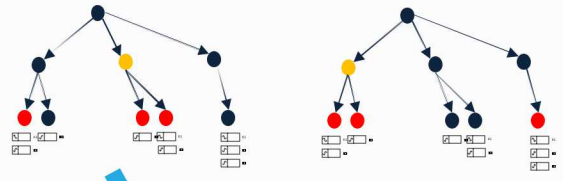
$$\delta_r = \sum_{e\in\mathcal{F}} x_{r,e} z_e$$

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

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

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

Attack Model



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

$$s.t.$$

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

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

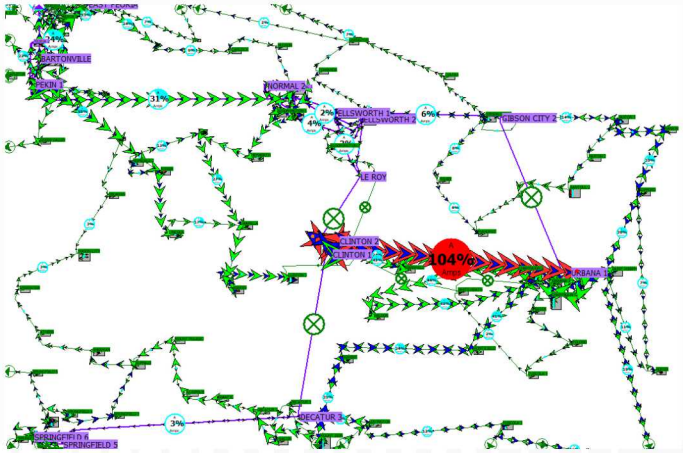
$$-S_k^{\max} \le p_k \le S_k^{\max}$$

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

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

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

Damage Control



# Future Extensions of Network Segmentation

- Not all zones are equal!
  - 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
  - Use caution when adding model detail. We must remember that these bilevel models are incredibly difficult to solve

- This model requires minimal SME input
  - Can add attacker detail

# Emulytics Optimization

- Network scanning optimization
  - Use optimization to pick optimal network scanning parameters
    - Number of nodes to scan in parallel
    - Probe delay
    - Number of retries
- Use worst-case analysis to help Emulytics team identify vulnerable loads and corridors
- Provide Emulytics team higher-fidelity power flow capability

# Conferences and External Engagements

- Presentations
  - Optimization work at INFORMS (October 2019)
  - In-progress paper at Resiliency Week (November 2019)
  - 2020 INFORMS Conference on Security (February 2020)
  - 3rd International Workshop of Bilevel Programming (2020)

- External Engagemenet
  - Santanu Dey and Emma Johnson at Georgia Tech
  - Kate Davis at Texas A&M
  - She'ifa Punla-Green at Rensselaer Polytechnic Institute

- Publications
  - Plenty of publishable material
  - Ramp up on publications in 2020