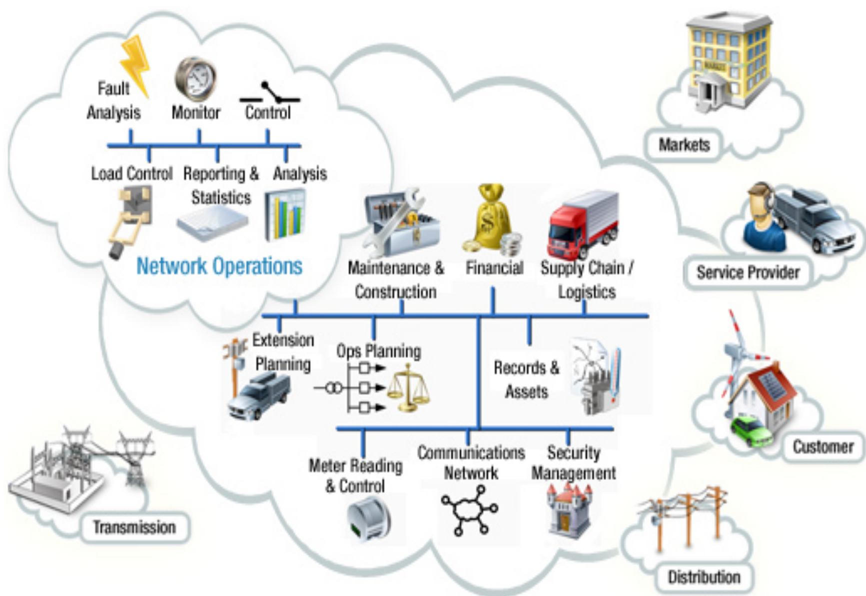
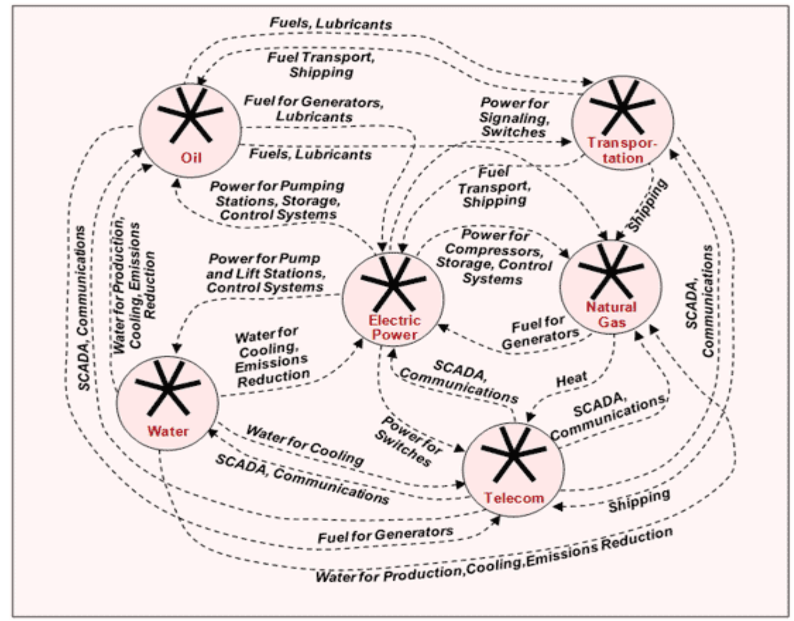
Optimal and Game-Theoretic Deployment of Security Investments in Interdependent Assets

Ashish R. Hota, Abraham A. Clements, Shreyas Sundaram and Saurabh Bagchi
School of Electrical and Computer Engineering
Purdue University

Challenge

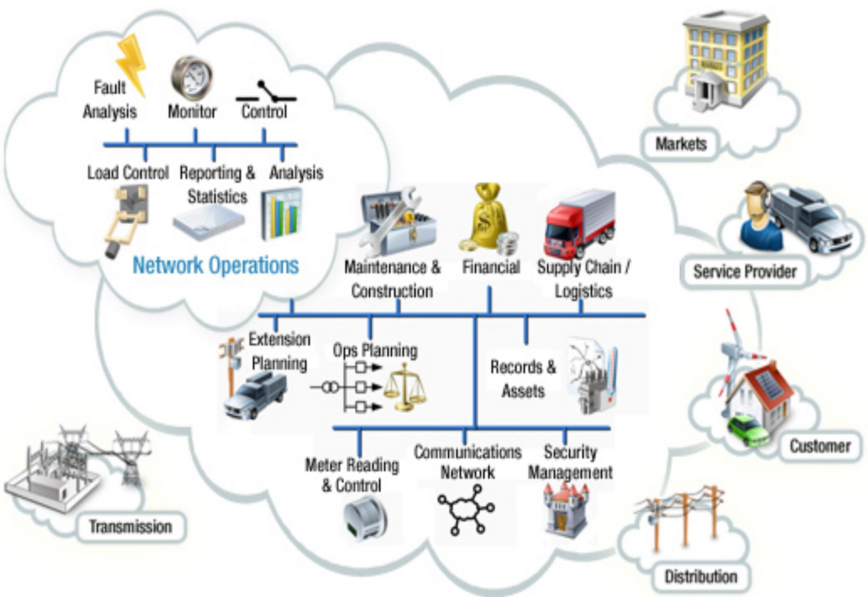


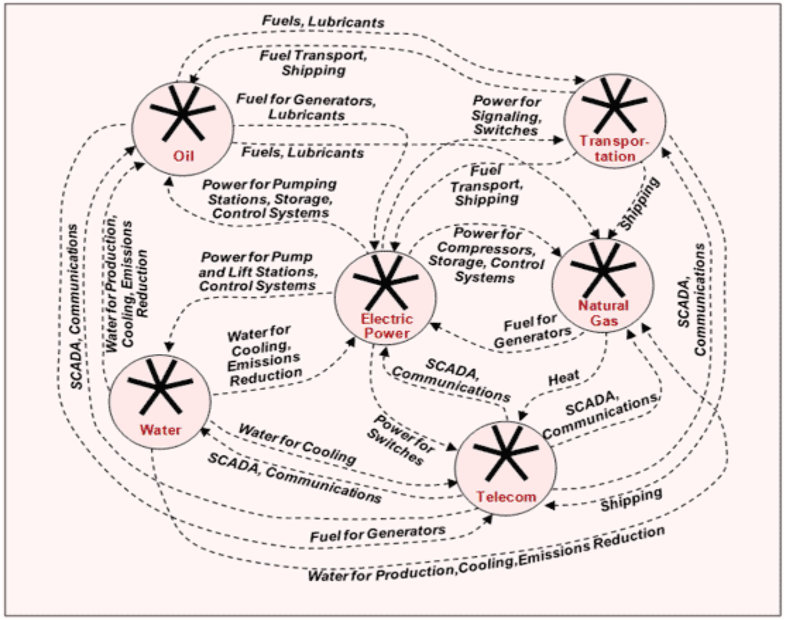


- Modern critical infrastructures have a large number of assets, managed by multiple stakeholders.
- The security of these complex systems depends critically on the interdependencies between these assets.

Image credits: sgip.org, USC.

Contribution





We propose a systematic framework for optimal and strategic allocation of defense resources in interdependent large-scale networks.

Image credits: sgip.org, USC.

Related Work

- Interdependent Security Games: each node is a decision-maker.
  - [Laszka et. al., ACM CSUR 2014, Hota and Sundaram, GameSec 2015, …]

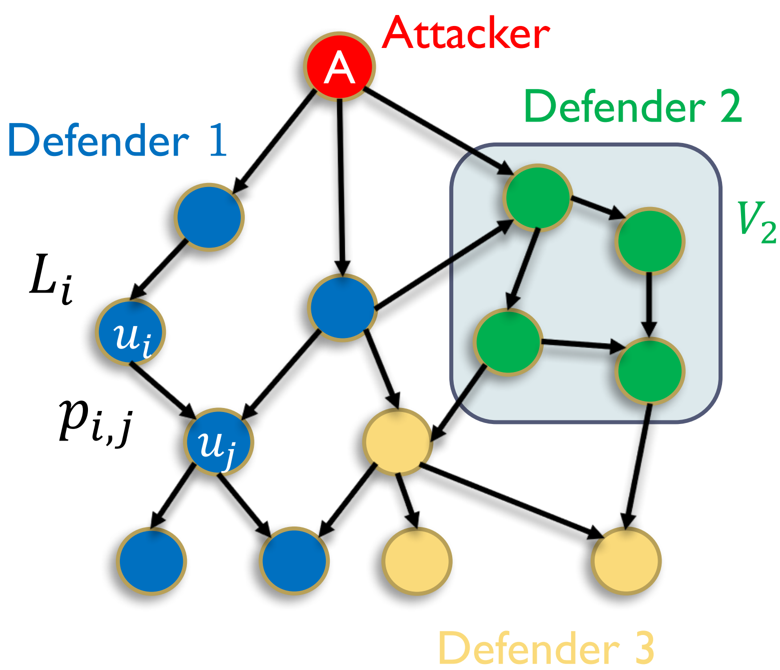
- Two player attacker-defender games
  - Stackelberg Security Games [Jain et. al., AAMAS 2013, …]
  - Colonel Blotto Games [Gupta et. al., GameSec 2014, …]
  - Network Interdiction Games [Israeli and Wood, Networks 2002, …]

- Our framework captures externalities between the above two extremes.
  - Multiple defenders, each responsible for a set of assets.
  - The assets that belong to multiple defenders are interdependent.

- Closely related work:
  - Multidefender Security Game [Lou et. al., 2016]

Interdependency Graph

- A directed graph where each node represents an asset in a networked system.
- Multiple defenders, denoted by the set D, each responsible for a subset of assets.
- When an asset u_i is compromised, it can be used to attack asset u_j if (u_i, u_j) is an edge.
- $p_{i,j}^0 \in (0,1]$: the probability of the above attack being successful. Independent across edges.
- $L_i \geq 0$: loss experienced by the defender if asset u_i is attacked successfully.



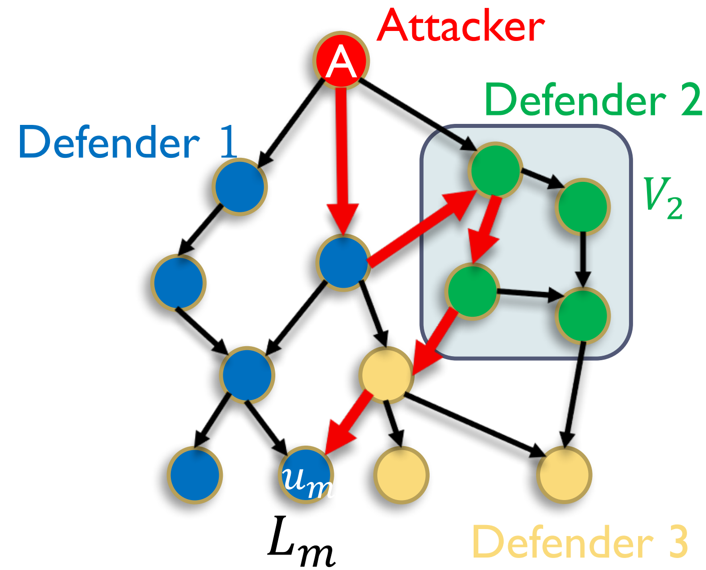
Attack Probability

- Defense strategies reduce the attack probabilities of the edges.

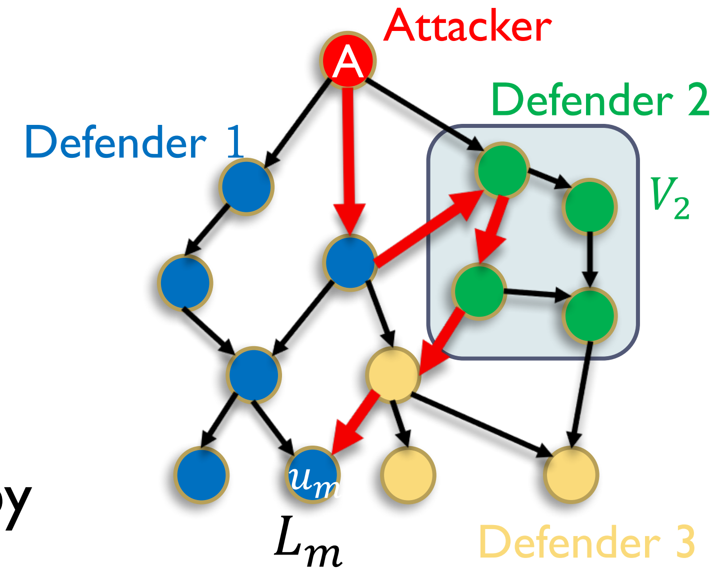
- Joint strategy profile
  $$\mathrm{x} = (\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_{|D|}),$$
  where each x_k drawn from a convex and compact subset of $\mathbb{R}^{\mathrm{q}_\mathrm{k}}$.

- Let $\mathbb{P}_m$: set of paths from A to u_m

- The attack probability on a node u_m due to a given path $P \in \mathbb{P}_m$ is
  $$\prod_{(u_i, u_j) \in P} p_{i,j}(\mathrm{x})$$



Cost of a Defender



- The cost of a defender D_k is given by

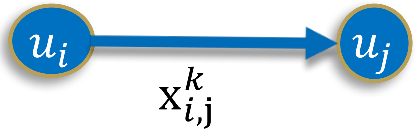
$$C_k(\mathrm{x}) \triangleq \sum_{u_m \in V_k} L_m \left(\max_{P \in \mathbb{P}_m} \prod_{(u_i, u_j) \in P} p_{i,j}(\mathrm{x}) \right)$$

- Captures the notion of "weakest link."

Defense Strategies

- $x^k_{i,j}$: defense allocation by defender D_k on edge (u_i, u_j).

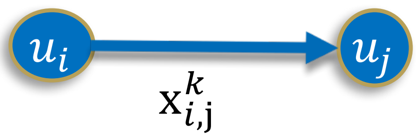
- Multiple defenders can potentially assign defense resources on a single edge.



Defense Strategies

- $\mathrm{x}_{i,\mathrm{j}}^{k}$: defense allocation by defender D_k on edge (u_i, u_j).
- Multiple defenders can potentially assign defense resources on a single edge.

<u>More Generally:</u>

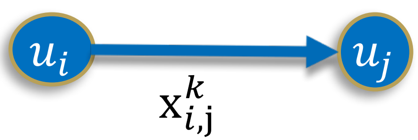


- Let $\mathrm{T_k}: \mathbb{R}^{q_\mathrm{k}} \rightarrow \mathrm{R}^{|\mathrm{E}|}$ be a linear map that transforms defense strategy of defender D_k, denoted by $\mathrm{x_k}$, to the edges of the graph.
- $[\mathrm{T_k x_k}]_{i,j}$: defense allocation by defender D_k on edge (u_i, u_j).

Defense Strategies

- $x_{i,j}^{k}$: defense allocation by defender D_k on edge (u_i, u_j).
- Multiple defenders can potentially assign defense resources on a single edge.

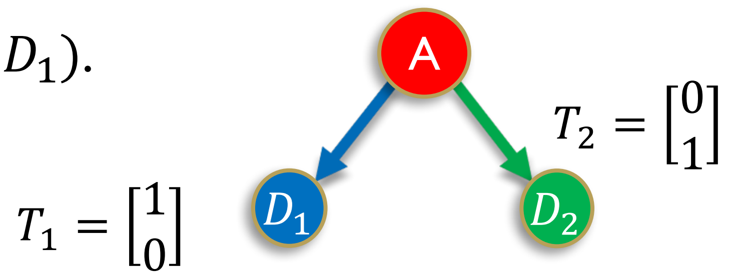
<u>More Generally:</u>



- Let $T_k: \mathbb{R}^{q_k} \rightarrow R^{|E|}$ be a linear map that transforms defense strategy of defender D_k, denoted by x_k, to the edges of the graph.

<u>Example: Edge-based defense strategy</u>

- Defender D_1 can only defend the edge (A, D_1).
- D_2 only defends (A, D_2).
- x_1 and x_2 are scalars.



Transformation of Probabilities

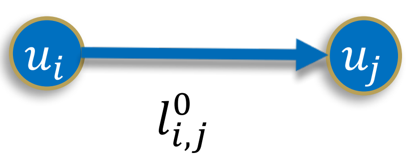
- Define the length of an edge (i, j) as $l_{i,j}^{0} \triangleq -\log\left(p_{i,j}^{0}\right) \in [0, \infty)$

- Under a joint defense strategy, the modified length is given by

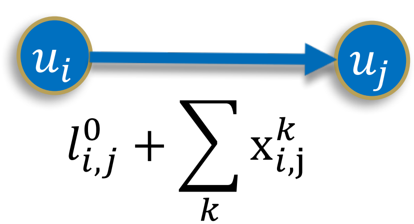
$$l_{i,j}(\mathrm{x}) \triangleq l_{i,j}^{0} + \sum_{k} \mathrm{x}_{\mathrm{i,j}}^{k}$$

$$= l_{i,j}\left(\mathrm{x}_{-\mathrm{k}}\right) + \mathrm{x}_{\mathrm{i,j}}^{k}$$

Initial length



Length under joint defense strategy x



Transformation of Probabilities

- Define the length of an edge (i, j) as $l_{i,j}^0 \triangleq -\log\left(p_{i,j}^0\right) \in [0, \infty)$

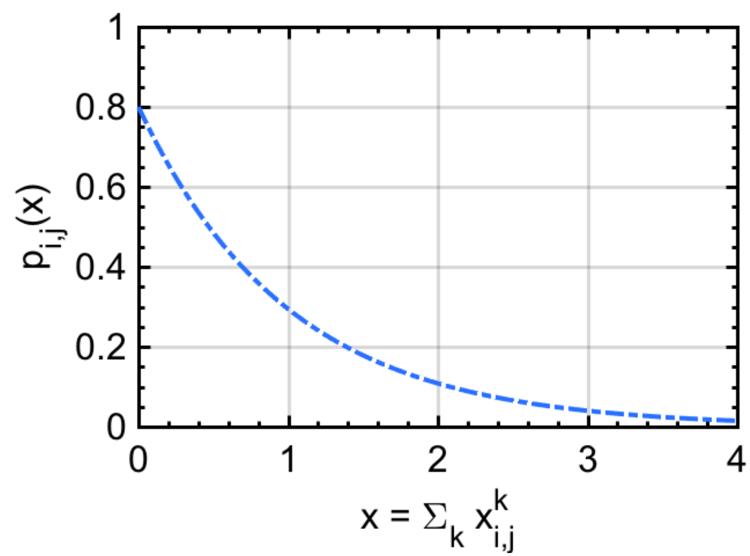
- Under a joint defense strategy, the modified length is given by

$$l_{i,j}(\mathrm{x}) \triangleq l_{i,j}^0 + \sum_k \mathrm{x}_{i,\mathrm{j}}^k$$

- Equivalently

$$p_{i,j}(\mathrm{x}) \triangleq p_{i,j}^0 \exp\left(-\sum_k \mathrm{x}_{i,\mathrm{j}}^k\right)$$

- Satisfies the assumptions in the Gordon-Loeb model.



Observation

- The attack probability on a node u_m due to a given path $P \in \mathbb{P}_m$ is

$$\prod_{(u_i,u_j)\in P} p_{i,j}(\mathrm{x}) = \exp\left(-\sum_{(u_i,u_j)\in P}\left[l_{i,j}^0 + \sum_k \mathrm{x}_{i,j}^k\right]\right)$$

- Path with the highest attack probability has the smallest length.

Equilibria in the Multidefender Game

The cost of Defender D_k can be stated as

$$C_k(\mathrm{x_k}, \mathrm{x_{-k}}) \triangleq \sum_{u_m \in V_k} L_m \left(\max_{P \in \mathbb{P}_m} \prod_{(u_i, u_j) \in P} p_{i,j}(\mathrm{x}) \right)$$

$$= \sum_{u_m \in V_k} L_m \underbrace{\exp\left(- \min_{P \in \mathbb{P}_m} \overbrace{\sum_{(u_i, u_j) \in P} l_{i,j}(\mathrm{x_{-k}}) + \mathrm{x}_{i,j}^{k}}^{\text{Affine in } \mathrm{x_k} \text{ for given } \mathrm{x_{-k}}} \right)}_{\text{Convex in } \mathrm{x_k} \text{ for given } \mathrm{x_{-k}}}$$

Equilibria in the Multidefender Game

The cost of Defender D_k can be stated as

$$C_k(\mathrm{x_k}, \mathrm{x_{-k}}) \triangleq \sum_{u_m \in V_k} L_m \left(\max_{P \in \mathbb{P}_m} \prod_{(u_i,u_j) \in P} p_{i,j}(\mathrm{x}) \right)$$

$$= \sum_{u_m \in V_k} L_m \underbrace{\exp\left(- \min_{P \in \mathbb{P}_m} \overbrace{\sum_{(u_i,u_j) \in P} l_{i,j}(\mathrm{x_{-k}}) + \mathrm{x}_{i,j}^{k}}^{\text{Affine in } \mathrm{x_k} \text{ for given } \mathrm{x_{-k}}} \right)}_{\text{Convex in } \mathrm{x_k} \text{ for given } \mathrm{x_{-k}}}$$

Theorem

The multidefender game is an instance of *concave game* [Rosen, Econometrica, 1965] and a pure Nash equilibrium exists.

Computing Best Response

Theorem
The best response of Defender D_k can be computed by solving the following convex optimization problem.

$$\min_{\mathrm{y} \in \mathbb{R}_+^{|V|}, \mathrm{x} \in \mathbb{R}_+^{|q_k|}} \sum_{u_m \in V_k} L_m e^{-\mathrm{y}_m}$$

s.t. $\mathrm{y}_j - \mathrm{y}_\mathrm{i} - \mathrm{x}_{i,\mathrm{j}}^k \leq l_{i,j}(\mathrm{x}_{-\mathrm{k}}), \forall$ edge (u_i, u_j)

$$\mathrm{y}_a = 0$$

$$1^T \mathrm{x}_k \leq B_k$$

Budget constraint

y_m: feasible potential of node u_m, at most the length of the shortest path from node u_a

y_a: potential of attacker node

$$\mathrm{y}_j \leq \mathrm{y}_\mathrm{i} + \sum_k \mathrm{x}_{i,\mathrm{j}}^k$$

Computing Best Response

Theorem

The best response of Defender D_k can be computed by solving the following convex optimization problem.

$$\min_{\mathrm{y}\in\mathbb{R}_+^{|V|},\mathrm{x}\in\mathbb{R}_+^{|q_k|}} \sum_{u_m\in V_k} L_m e^{-\mathrm{y}_m}$$

s.t. $\mathrm{y}_j - \mathrm{y}_\mathrm{i} - \mathrm{x}_{i,\mathrm{j}}^k \leq l_{i,j}(\mathrm{x}_{-\mathrm{k}}), \forall$ edge (u_i, u_j)

$$\mathrm{y}_a = 0$$

$$1^T \mathrm{x}_k \leq B_k$$

y_m: feasible potential of node u_m, at most the length of the shortest path from node u_a

- When the graph does not have a cycle of negative length, a feasible potential exists and the potential at every node is equal to the length of the shortest path from the source [Cook et al, 1998].

Observation

- Given the defense strategies of other players, a player can compute her best response efficiently.

- A social planner can efficiently compute optimal defense allocations over the entire network.

Computing Nash Equilibrium

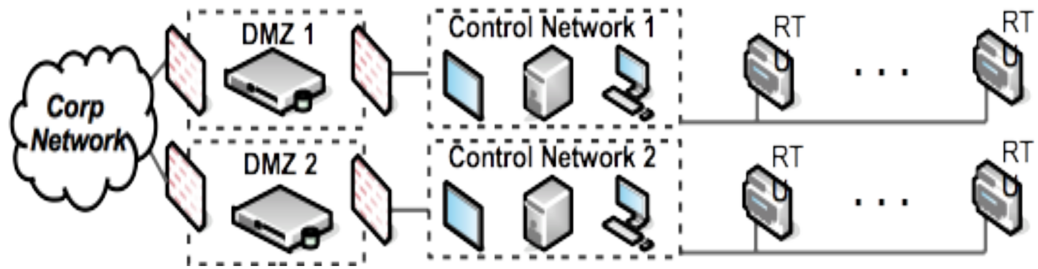
- Expected loss of a player in the original formulation is non-differentiable.

- In the modified convex formulation, the constraints of a player depend on the strategies of other players.
  - Leads to a Generalized Nash Equilibrium Problem.
  - When each player values a single asset in the network, equilibrium strategies can be computed by solving a Linear Complementarity Problem [Sreekumaran, Hota and others, arxiv:1503.01100, 2015].

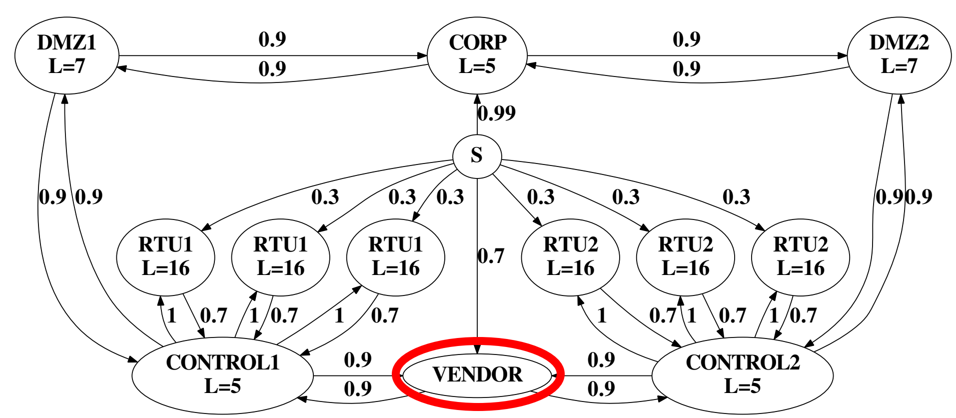
- In this work, we compute Nash equilibrium strategies by iteratively computing the best responses of the players.

Case Studies

Example – 1: SCADA Network

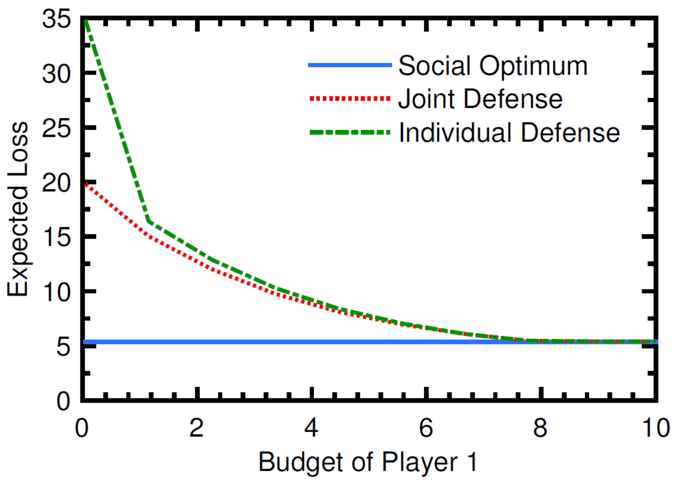


- Two interdependent control subsystems.
- Shared corporate network.
- Common vendor for remote terminal units (RTUs).

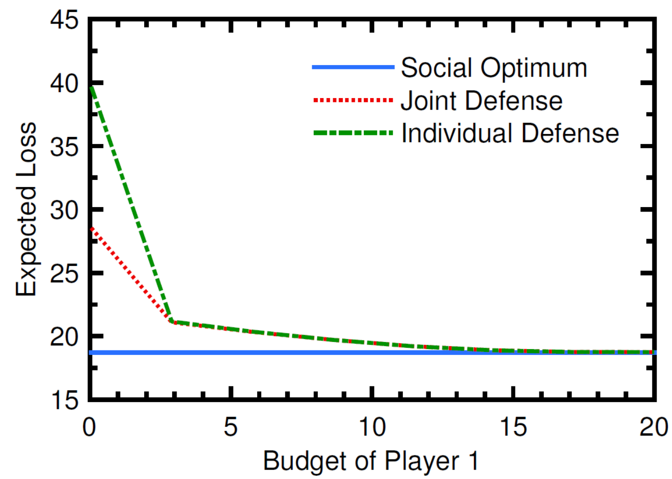


Expected Loss at Equilibrium

3 RTUs



30 RTUs



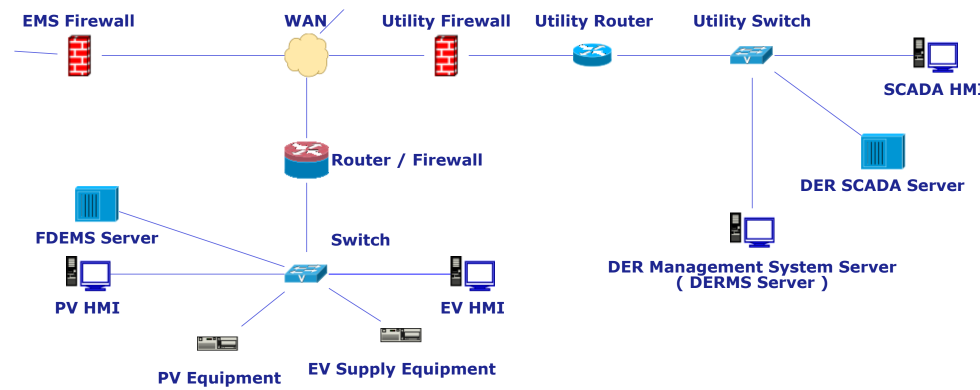
- Total budget: 20 and 40, respectively.
- Edge-based defense.
- Individual defense: Each player can assign resources within its subsystem.
- Joint defense: a player can defend anywhere in the network.

When the budgets are asymmetric, it is in the selfish interest for the player with a higher budget to defend certain assets of the other player.

Example – 2: Distributed Energy Resource

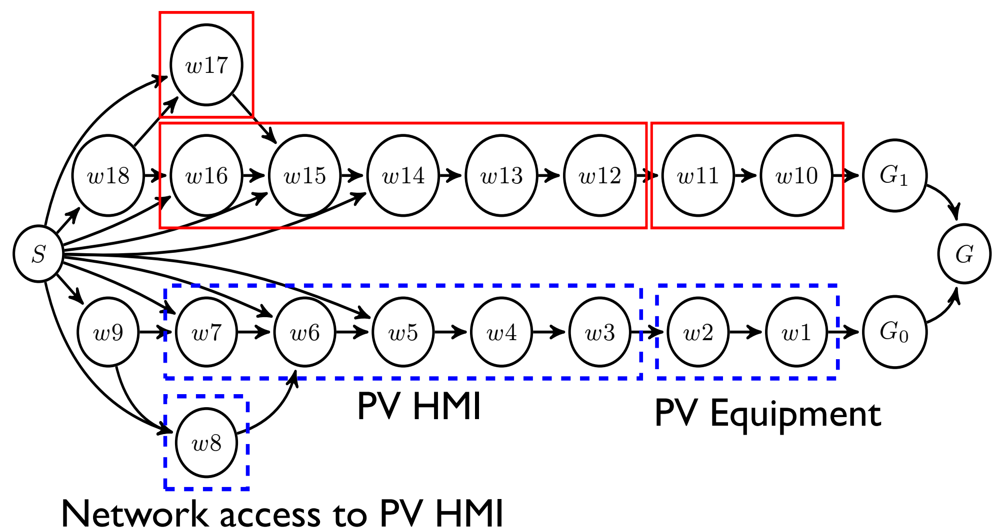
- Instance of NESCOR failure scenario:

  Attacker tries to gain access to the DER so that it does not trip during low voltage.



- Example network borrowed from [Jauhar et. Al., PRDC 2015.]

- Each node corresponds to an attack step.

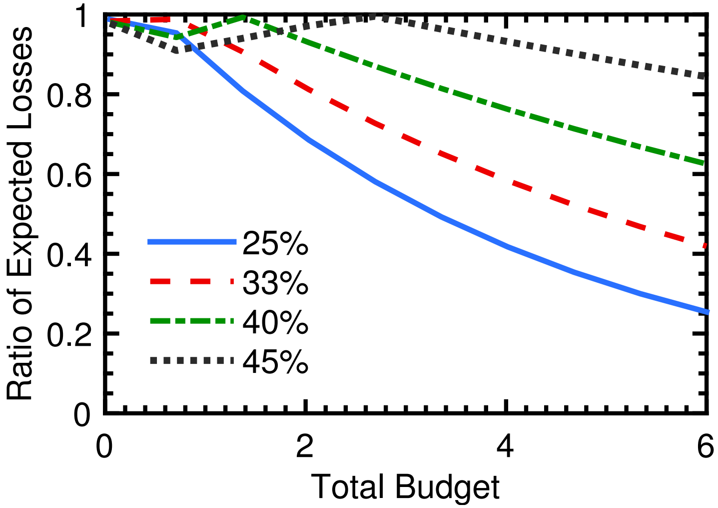


Inefficiency of Equilibrium Investments

- We plot $\frac{\text{Minimum Total Cost}}{\text{Total Cost at a Nash Equilibrium}}$ against the total budget.

- Inefficiency increases when
  a. total budget increases, and
  b. difference in the budgets of the players increases.

- Similar trends for both edge-based and node-based defenses.



Percentage denotes the fraction of total budget that belongs to the PV defender.

Summary and Conclusion

- Proposed a general framework to compute optimal and game-theoretic defense allocation under network interdependencies.

- Demonstrated its applications in industrial control systems and the smart grid.

- Future work:

  - Analytical investigations on the equilibrium computation problem
  - Theoretical bounds on Price of Anarchy
  - Validation of this approach in large-scale practical problems

Thank you!