CERIAS

The Center for Education and Research in Information Assurance and Security

Computational and Behavioral Aspects of Network Security Games

Ashish R. Hota

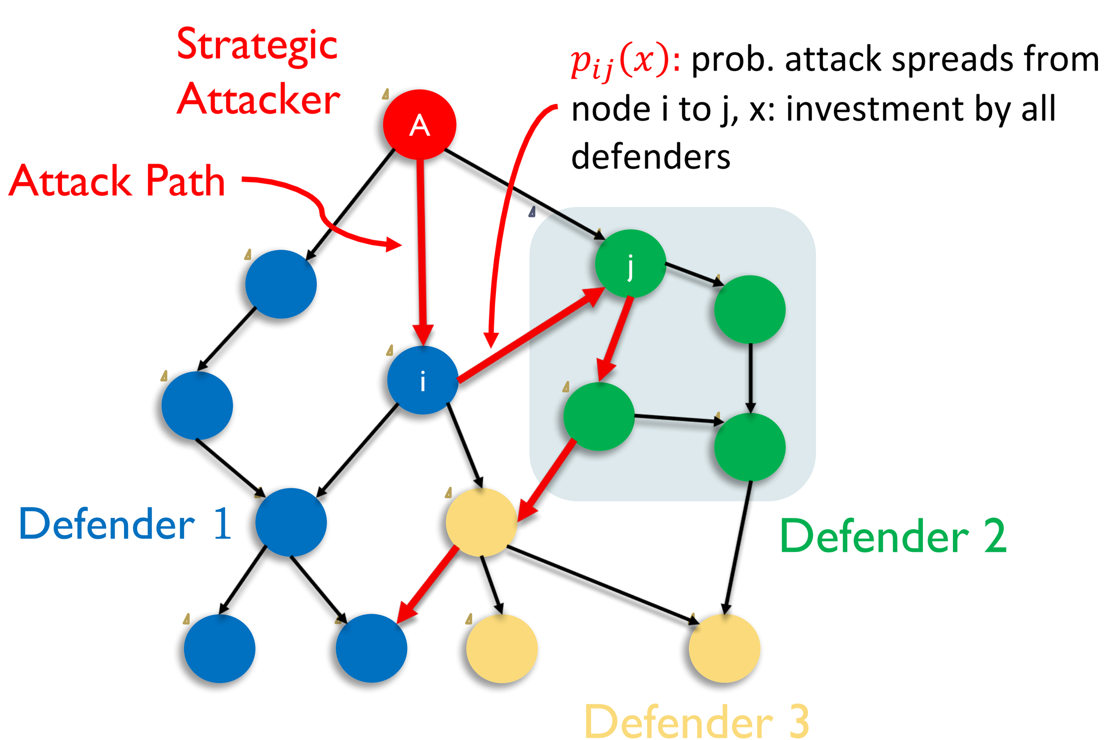
Joint work with: **Shreyas Sundaram (PhD Advisor),** Saurabh Bagchi, Abe Clements

School of Electrical and Computer Engineering, Email: ahota@purdue.edu

Decentralized Defense of Interdependent Assets in Large-Scale Networks

- Cyber-physical systems, such as the power grid, consist of a large number of assets managed by multiple stakeholders.
- Strategic attackers target valuable assets by exploiting interdependencies between them.

We develop a framework to compute optimal and game-theoretic security investments in large-scale networks.



- Security risk of an asset: probability of attack on the asset on the path that has the highest probability of success for the attacker.
- The cost of defender D_k is given by

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

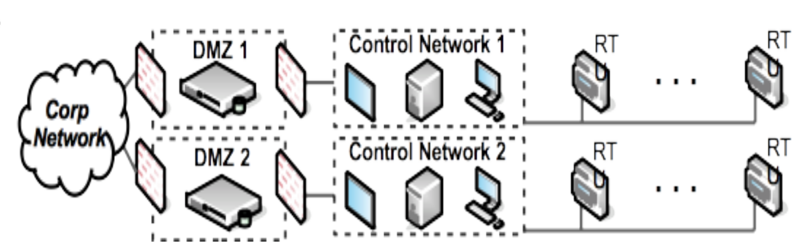
- Optimal security investments on the edges can be computed efficiently.

Theorem

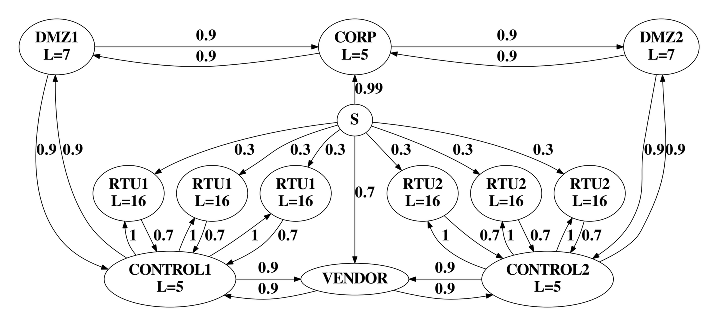
The best response of Defender D_k can be computed by solving a **convex** optimization problem.

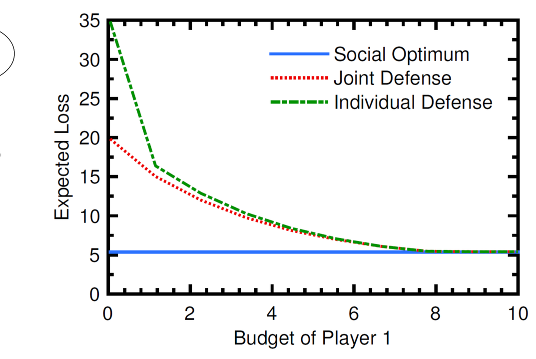
Case Study

- Consider the SCADA control system and interdependency network
- It consists of two subsystems managed by different entities.



- Assets are interdependent via a shared vendor.





- Plot compares social cost under centralized and decentralized investments.
- Total budget: 20
- Individual defense: Each player can assign resources within its subsystem.
- Joint defense: a player can defend anywhere in the network.

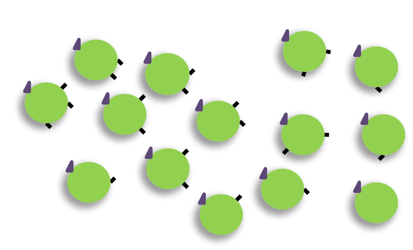
Observations
- Budget asymmetry leads to inefficient equilibrium.
- It is in the selfish interest for the player with a higher budget to defend certain assets of the other player.

Publication

A. R. Hota, A. Clements, S. Sundaram and S. Bagchi, "Optimal and Game-Theoretic Deployment of Security Investments in Interdependent Assets." Proceedings of GameSec, Conference on Decision and Game Theory for Security, New York, 2016.

Impacts of Behavioral Decision-Making on Security Investments in Networks

- Security risk of a node depends on its investment and the investments by its neighbors.

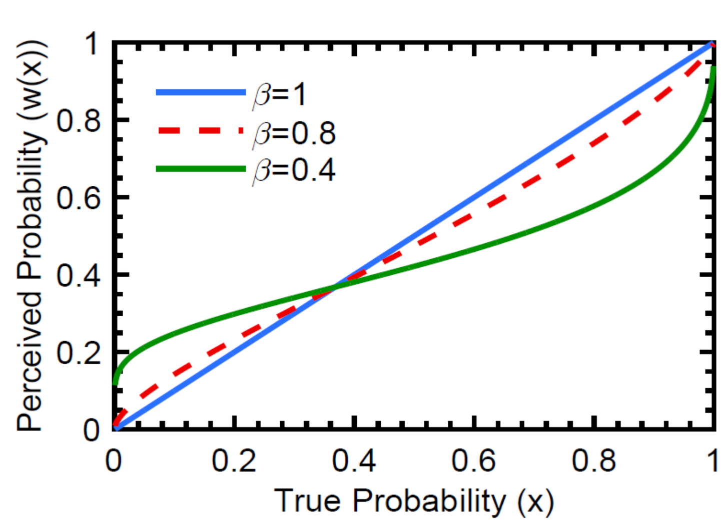


- Security investments critically depend on how human decision-makers perceive the risk (probability) of being attacked successfully.
- This work:

Rigorous investigation of the impacts of behavioral perceptions of security risk on selfish investment decisions.

Behavioral Perceptions of Probabilities

- Humans overweight low probabilities and underweight large probabilities.



- Probability weighting functions transform true probabilities x into perceived probabilities $w(x)$.
- Example: Prelec [1998] weighting function:
$$w(x) = \exp\left(-(-\ln x)^{\beta}\right)$$
where parameter $\beta \in (0,1]$.

Game-Theoretic Formulation

- Consider a network of agents.
- Node/Player i decides her personal security investment $s_i \in [0,1]$.
- **Total Effort Game**: Utility of player (node) i

True probability of successful attack

$$Eu_i = -L_i w_i \left(1 - \frac{s_i + \sum_{j \in N(i)} s_j}{d_i}\right) - c_i s_i,$$

Perceived probability of successful attack

where $N(i)$= neighbors of node i,

d_i = 1 + degree of node i

L_i: loss of player i when attacked

c_i: cost of security investment

Effects of Probability Weighting

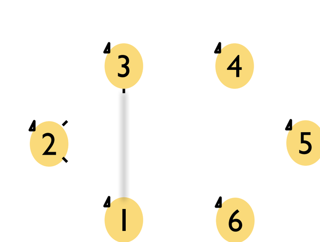
- The total effort game admits a pure Nash equilibrium (PNE) under heterogeneous weighting functions.
- Under true perceptions of probabilities, high degree nodes choose to invest 0, while behavioral users always choose a nonzero investment.
- **Behavioral perceptions are most beneficial when attack probability is high** (such as when the nodes in the network have a large number of neighbors).

Effects of Network Structure

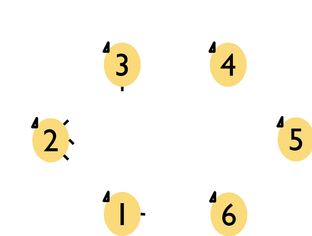
Theorem

Let $\mathbf{\Phi}^*$ be the expected fraction of nodes that are attacked successfully at a PNE.

1. Among all connected graphs with a given number of edges and nodes, Φ^* is **highest in degree-regular graphs.**
2. Among all connected graphs on n nodes, Φ^* is **smallest in the star graph**.
3. Among all connected graphs with a n nodes and e edges, Φ^* is **smallest in the quasi-complete graph $\mathbf{QC}(\boldsymbol{n}, \boldsymbol{e})$.**



Example: QC(6,3)



Example: QC(6,5)

Publications

1. A. R. Hota and S. Sundaram, "Interdependent Security Games under Behavioral Probability Weighting." Conference on Decision and Game Theory for Security, 2015.
2. A. R. Hota and S. Sundaram, "Optimal Network Topologies for Mitigating Security and Epidemic Risks." Allerton Conference on Communication, Control and Computing, 2016.
3. A. R. Hota and S. Sundaram, "Interdependent Security Games on Networks under Behavioral Probability Weighting." IEEE Transactions on Control of Network Systems (to appear).

CERIAS

PURDUE UNIVERSITY