CERIAS 2020 | PURDUE UNIVERSITY Discovery Park

Impacts of Behavioral Probability Weighting on Security Investments in Interdependent Systems

Mustafa Abdallah*, Parinaz Naghizadeh**, Ashish Hota^, Tim Cason+, Saurabh Bagchi*, Shreyas Sundaram*

* School of Electrical and Computer Engineering, Email: {abdalla0, sbagchi,sundara2}@purdue.edu

\+ Krannert School of Management, Email: cason@purdue.edu

** Electrical and Computer Engineering Department, Ohio State University Email: naghizadeh.1@osu.edu

^ Department of Electrical Engineering, Indian Institute of Technology (IIT), Kharagpur, Email: ahota@ee.iitkgp.ac.in

Motivation

- Cyber-physical systems, such as the power grid, consist of a large number of assets managed by multiple stakeholders.
- Security investments critically depend on how human decision-makers perceive the risk (probability) of being attacked successfully.
- This work:

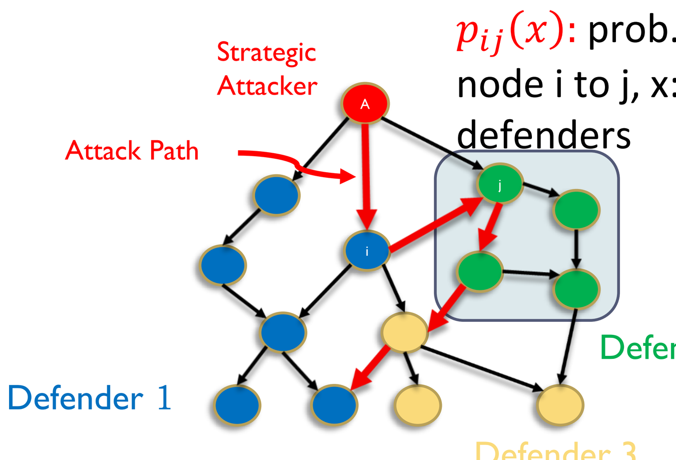
Rigorous investigation of the impacts of behavioral perceptions of security risk on security investment decisions made by defenders to protect their assets.

Game-Theoretic Formulation

- Consider a network of defenders where each defender has a limited security budget.
- Each defender has multiple valuable assets.
- **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

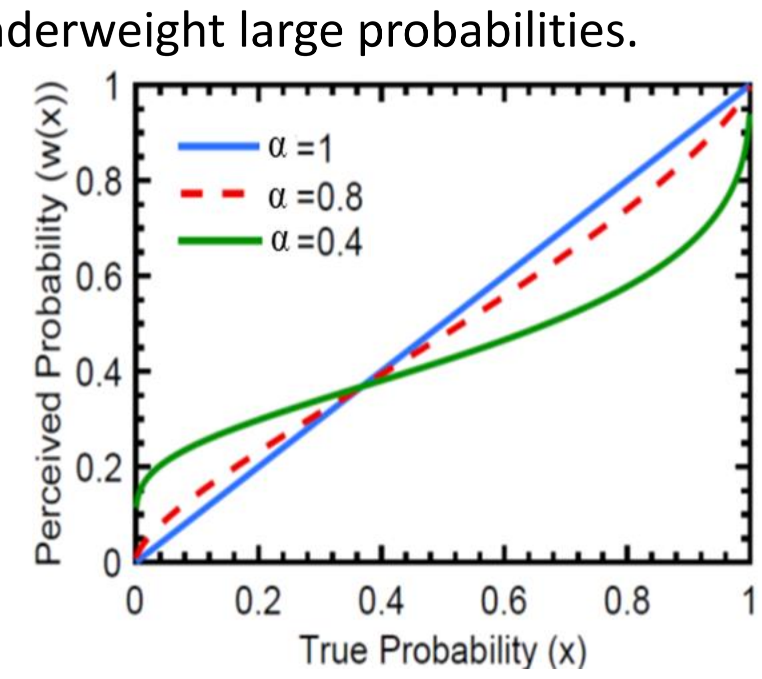
$$C_k(\mathrm{x}) \triangleq \sum_{u_m \in V_k} L_m \left(\max_{P \in \mathbb{P}_m} \prod_{(u_i,u_j)\in P} p_{ij}(\mathrm{x}) \right)$$

$p_{ij}(x)$: prob. attack spreads from node i to j, x: investment by all defenders



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: $w(x) = exp(-(-\ln x)^{\alpha});\ \alpha \in (0,1]$.

Behavioral Security Game:

- A game between different defenders in an interdependent network, where each player misperceives the attack probability on each edge.

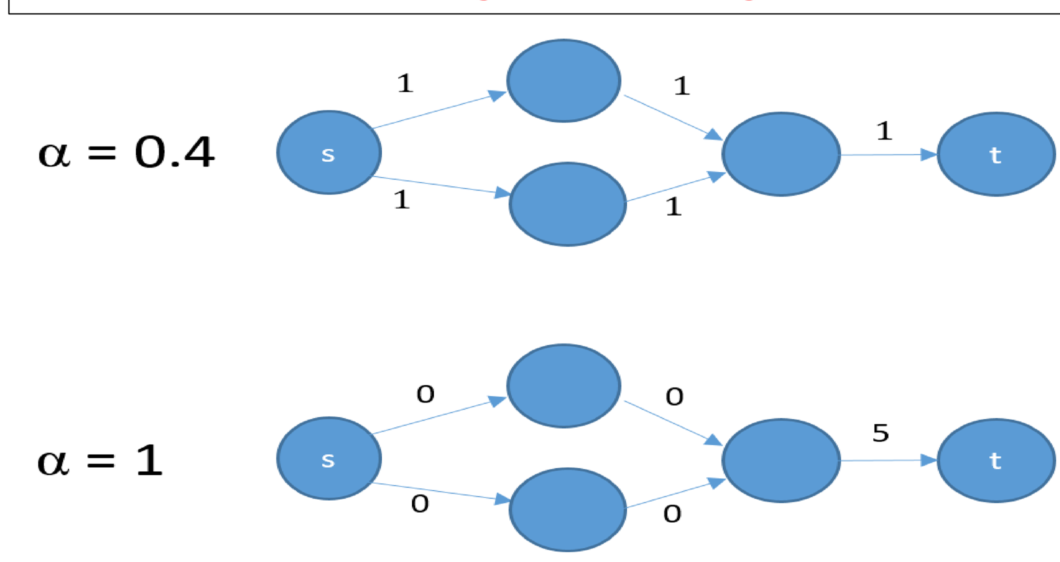
$$C_k(\mathrm{x}) \triangleq \sum_{u_m \in V_k} L_m \left(\max_{P \in \mathbb{P}_m} \prod_{(u_i,u_j)\in P} w(p_{ij}(\mathrm{x})) \right)$$

Properties of Security Investments

- **Theorem**: The Behavioral Games **possess a Pure Nash Equilibrium (PNE)** for 0 < α < 1.
- **Lemma**: The best response of Defender D_k in the Behavioral Security Games is computed by solving a **convex** optimization problem.
- **Theorem:** For a non-behavioral (i.e., with α=1) defender, it is sufficient to distribute all her investments only on a **Minimum Edge Cut** set in order to minimize her cost.
- **Proposition:** For a behavioral defender (i.e., with 0 < α < 1), investing entirely on the min edge cut **is not optimal from her perspective**. Thus, **she shifts a portion of her investments to other edge cuts**.

Key Insight

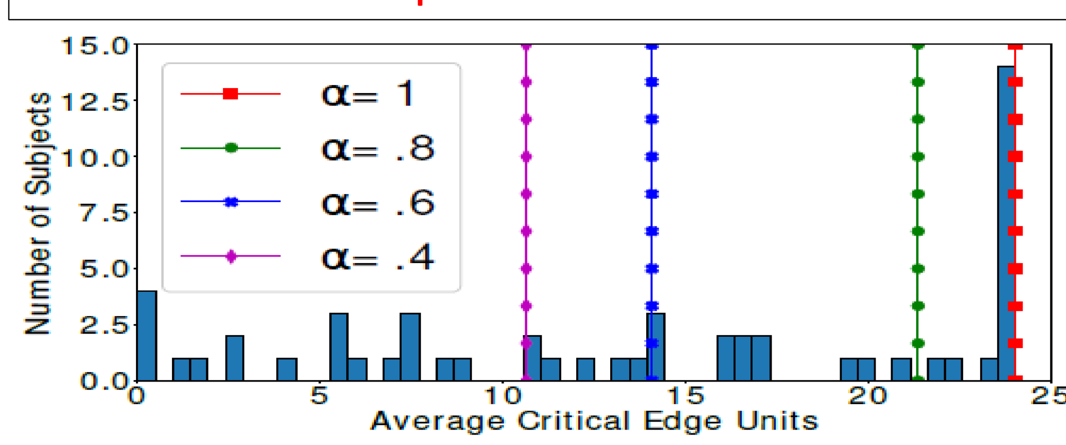
- The non-behavioral player **(i.e., $\alpha = 1$)** puts all her budget **B = 5** on the min cut (i.e., common) edge while behavioral player **(i.e., $0 < \alpha < 1$)** distributes the budget on all edges.

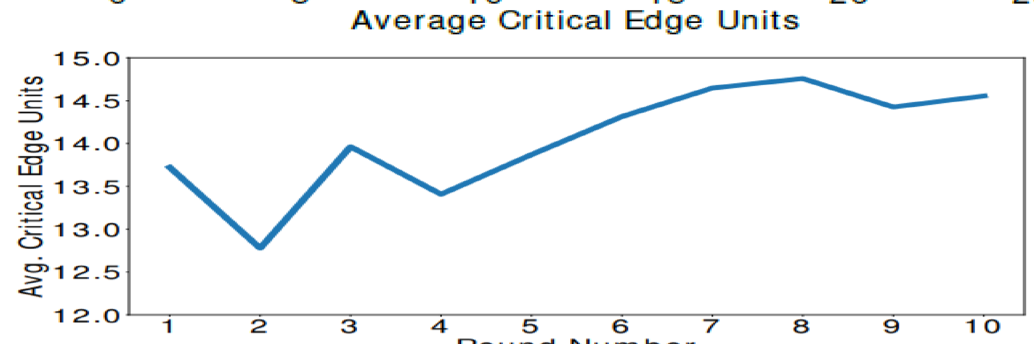


Human Subject Experiments

A) Probability Weighting Bias

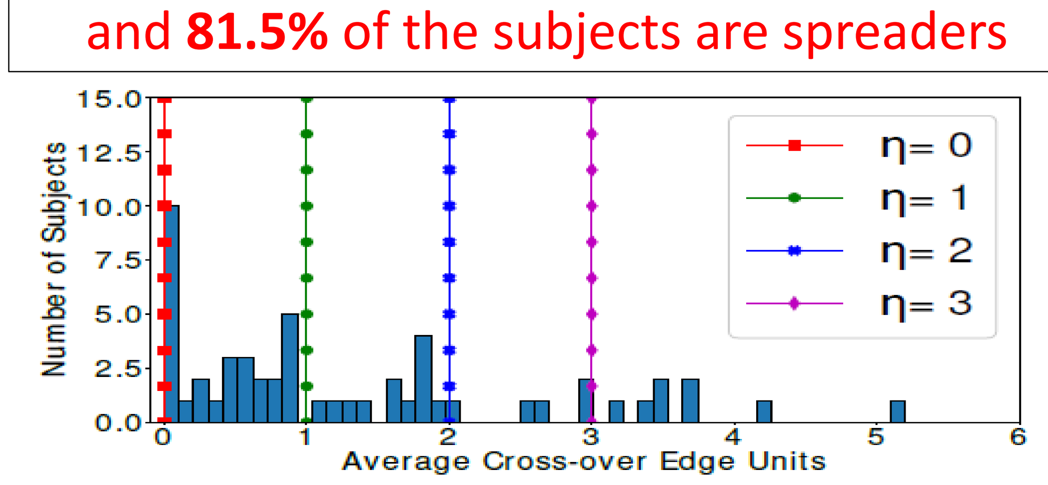
- **24%** of the subjects are rational and **76%** of the subjects are behavioral
- **45.45%** exhibit no learning across rounds and **34.10%** improve their investments.





B) Spreading Heuristics Bias

- **18.5%** of the subjects are non-spreaders and **81.5%** of the subjects are spreaders

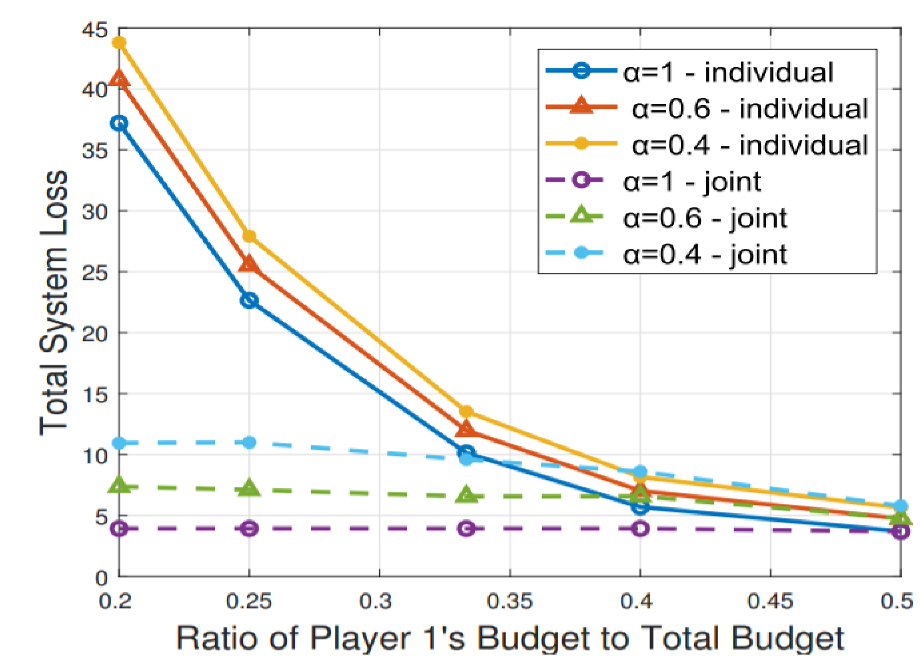


Evaluation

- We evaluate our model on two interdependent CPS:
  - Distributed energy resource (DER)
  - SCADA industrial control system (NIST)

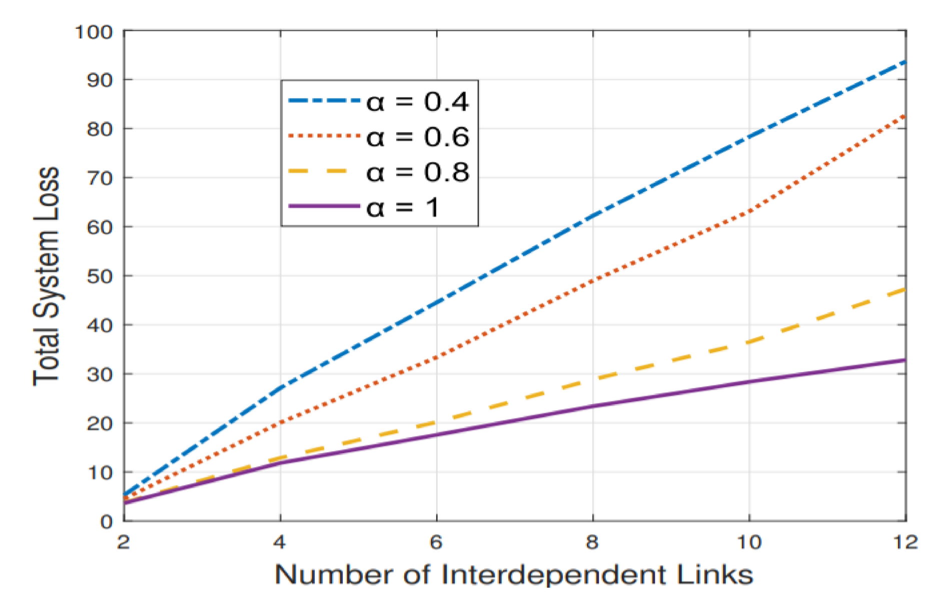
Defense Mechanism Type

- The advantage of joint defense is higher under asymmetric budget allocation among the defenders
- 88.5% reduction in total loss if both defenders are rational with 20:80 distribution of budget



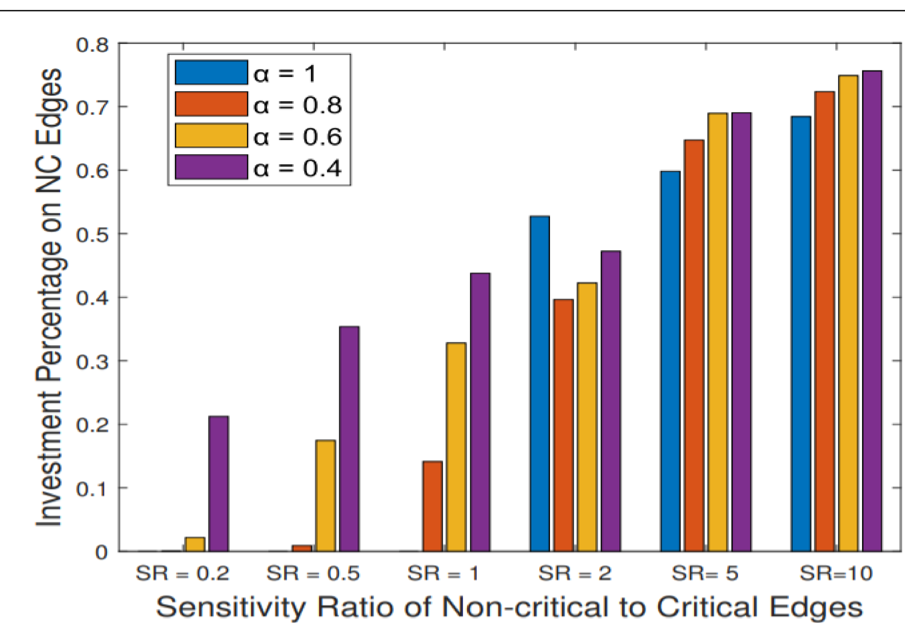
Degree of Interdependency

- **500%** relative increase in total system loss if both defenders are rational
- **1230%** relative increase in total system loss if both defenders are highly behavioral



The Sensitivity of Edges to investments

- The higher the sensitivity of the edge to investment, the more the defender invest on non-critical edges, but the increase is slower for behavioral defender.



Publications

1. M. Abdallah, P. Naghizadeh, A. Hota, T. Cason, S. Bagchi, and S. Sundaram, "Impacts of Behavioral Probability Weighting on Security Investments in Interdependent Systems." IEEE Transactions on Control of Network Systems (TCNS), 2020.
2. M. Abdallah, P. Naghizadeh, I. Khalil, T. Cason, S. Sundaram, and S. Bagchi, "Guiding Behavioral Decision Making in Security of interdependent systems "submitted to ASIA Conference on Computer and Communications Security (ASIACCS), 2021.