# BASCPS: Behavioral Decision Making in Security Games for Protecting Multi-Defender Cyber Physical Systems

Mustafa Abdallah[1], Parinaz Naghizadeh[2], Ashish Hota[3], Issa Khalil[4], Timothy Cason[1], Saurabh Bagchi[1], and Shreyas Sundaram[1]

1: Purdue University; 2: Ohio State University; 3: Indian Institute of Technology, Kharagpur ; 4: Qatar Computing Research Institute

PURDUE UNIVERSITY

CRISP

## Introduction

- Cyber-physical systems (CPS), such as the power grid, consist of a large number of assets managed by multiple stakeholders (i.e., defenders)
- CPS defenders have to judiciously allocate their (often limited) security budget to reduce their security risks
- Particularly challenging for large-scale systems, i.e., with huge number of assets
- Security investments critically depend on:
  - How human decision-makers perceive the risk (probability) of being attacked successfully
  - Degree of interdependency among different CPS defenders

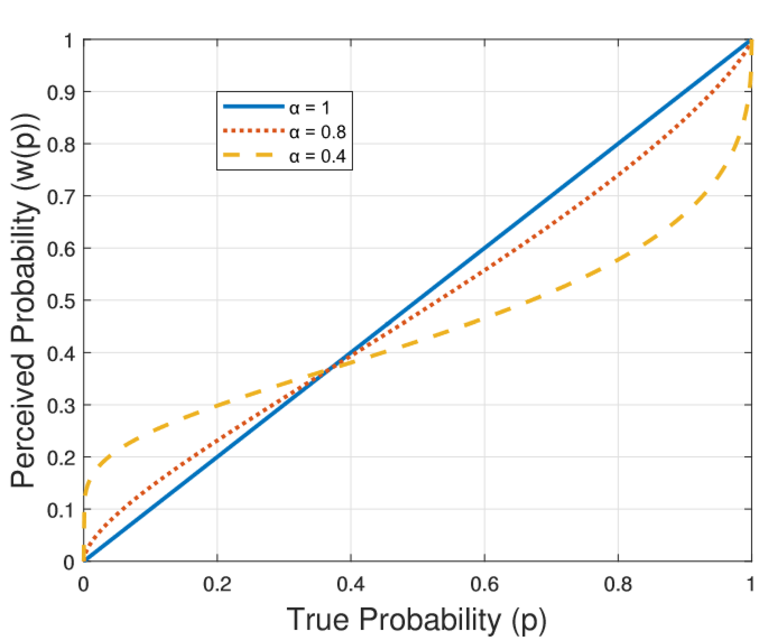
For a large-scale CPS systems, can we show the impacts of human's misperception of the risk on the optimal security investments allocated by human defenders and meeting security requirement of the system?

## Motivation

- Humans overweight low probabilities and underweight large probabilities
- Probability weighting functions transform true probabilities p into perceived probabilities $w(p)$
- Example: Prelec [1998] weighting function:

$$w(p) = \exp(-(-\ln(p))^{\alpha})$$

where parameter $\alpha \in (0,1]$




- The dashed lines shows the non-linear perception of the probability of successful attack by behavioral defender.
- The solid line gives the perception of rational defender who perceives the probability of attack in a true manner (correctly)
  - There is a cross-over point such that the true probability is the same as the perceived probability where probabilities greater than this point is underweighted and probabilities less than this point is over weighted
  - Therefore, BASCPS uses this probability weighting function to identify whether the defender is rational decision-maker or not

## Our Contributions: BASCPS

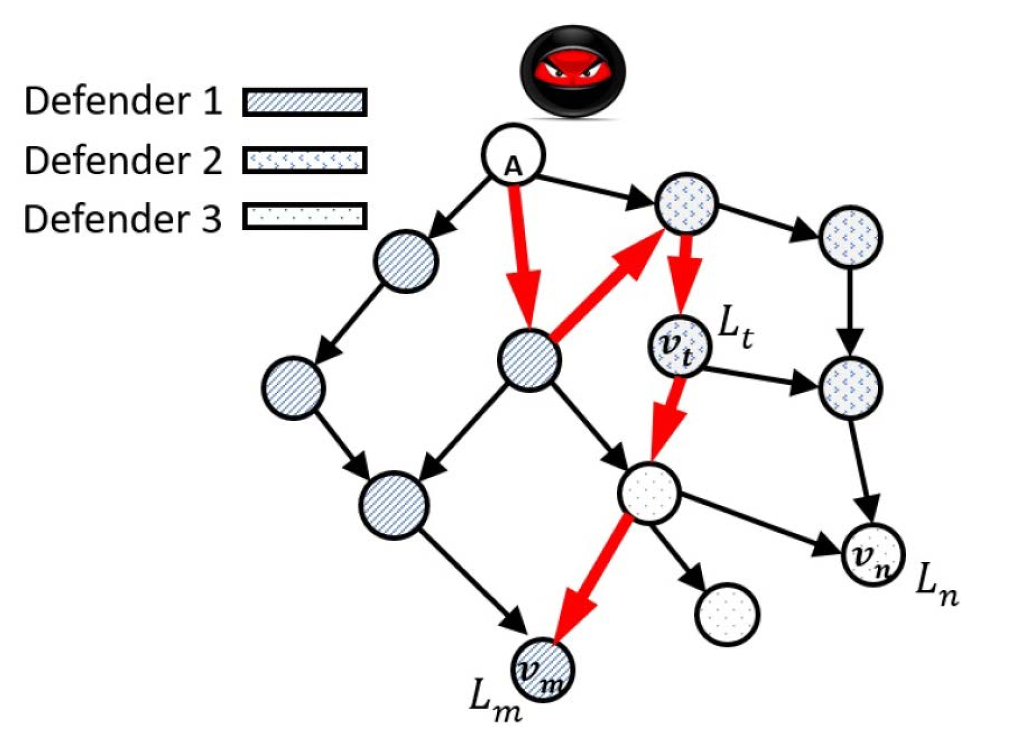
- Proposes a behavioral security game model for the study of security of multi-defender CPS where defenders' assets have mutual interdependencies
- Shows a rigorous investigation of the impacts of behavioral perceptions of security risk on security investment decisions made by defenders to protect their assets
- Analyzes the different parameters that affect the security of interdependent CPS under our behavioral model, such as the available security budget, types of defense mechanisms, degree of interdependency between defenders, and sensitivity of edges

## Model Overview

- **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

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

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



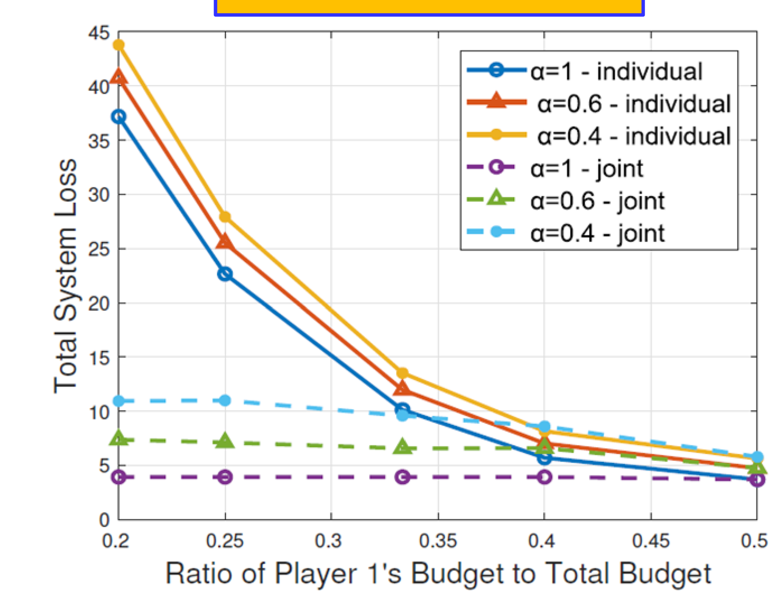

## Properties of Investments

- **Theorem:** The Behavioral Games possess a Pure Nash Equilibrium (PNE) for $0 < \alpha < 1$
- **Lemma: The** best response of Defender $D_k$ in the Behavioral Games can be computed by solving a convex optimization problem
- **Theorem:** For a non-behavioral (with $\alpha = 1$) 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 (with $0 < \alpha < 1$), 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

## Evaluation

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

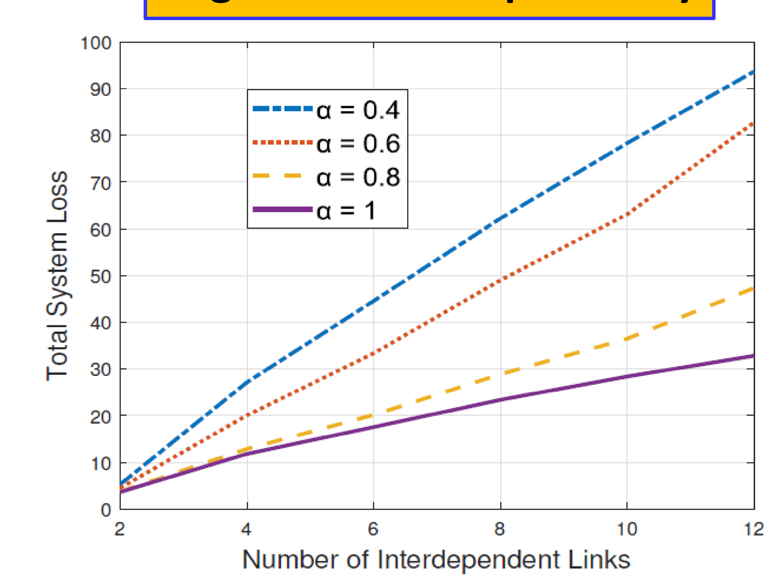
### Defense Mechanism




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

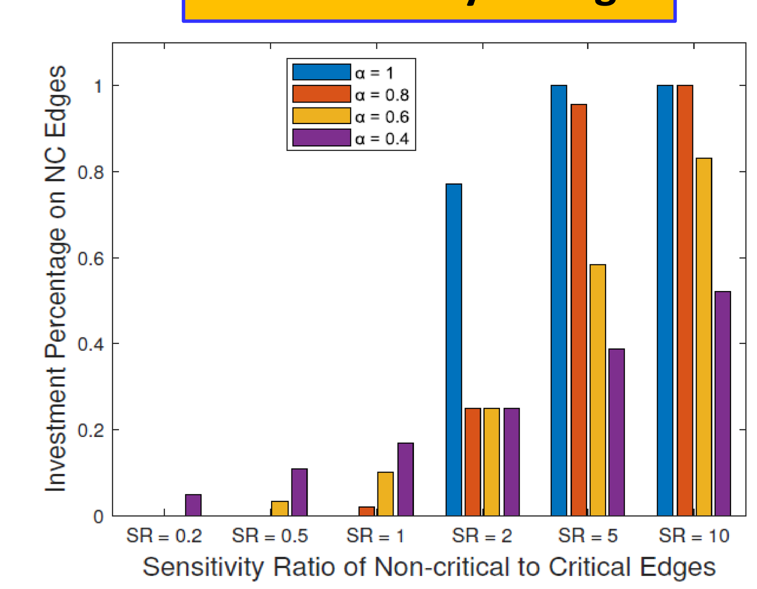
### Degree of Interdependency




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

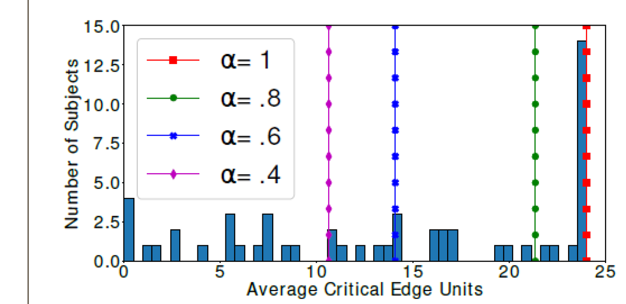
### The Sensitivity of Edges

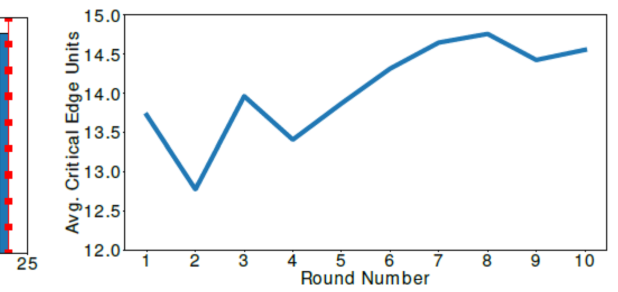



As SR increases, all defenders invest more on NC edges, but the increase is slower for behavioral defenders.

### Human Subject Experiments

#### A) Probability Weighting Bias

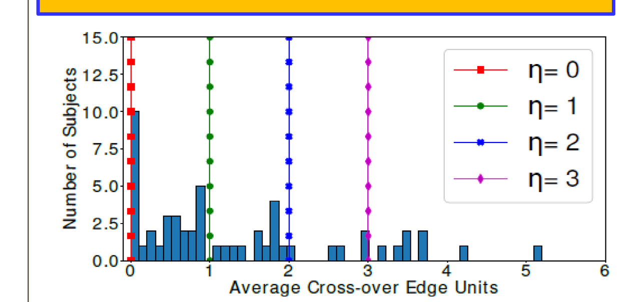


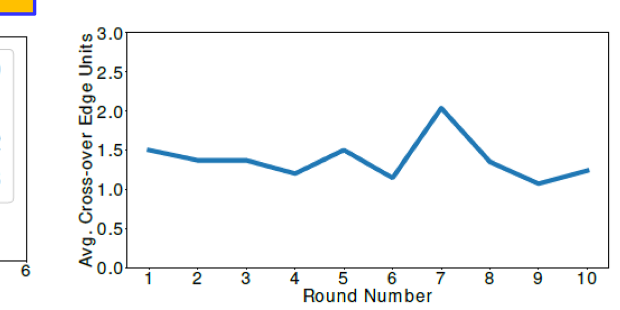




24% of the subjects makes rational decisions
76% of the subjects are behavioral

20.45% makes worse decisions in later rounds, 45.45% exhibits no learning across rounds, 34.10% improves their investments.

#### B) Spreading Heuristics Bias



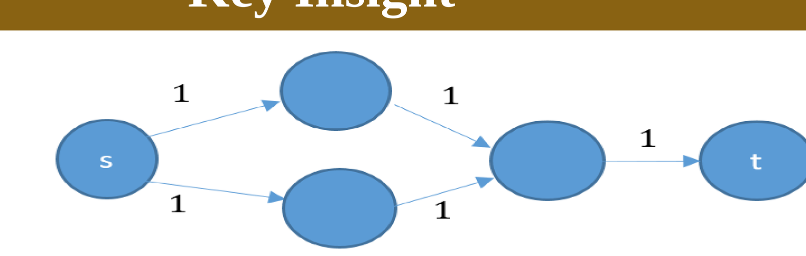




18.5% of the subjects are non-spreaders
81.5% of the subjects are spreaders

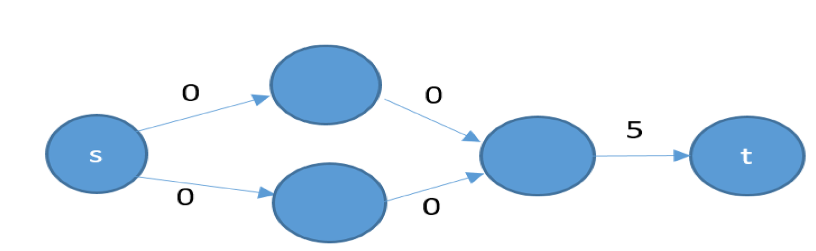
This shows the average of subjects' investments on the crossover edge in each round, which shows a weak downward trend.

## Key Insight

$\alpha = 0.4$




$\alpha = 1$




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

## Prior Work

- Majority of existing work has focused on classical game theoretic models of rational decision making on large scale systems modelled by attack graphs [Sheyner-IEEE Security and Privacy 02], while we [Abdallah-ACC 19] analyze behavioral models of decision making in these systems
- A notable departure from classical economic models within the security and privacy literature is in [Acquisti-IEEE Security and Privacy 09], which identifies the effects of behavioral decision making on individual's personal privacy choices.
- The problem of security resource allocation for smart city infrastructures and water distribution networks [Perelman-HiCons14] was studied. However, this work has not taken into account the interdependencies between multiple defenders.
- [Hota-TCNS18]: provides a theoretical treatment of behavioral decision making in certain specific classes of interdependent security games. That research, however, does not consider the more realistic attack scenarios and systems that we consider here.

## Acknowledgments

This work is supported by NSF SaTC grant CNS-1718637, and Purdue WHIN center. Any opinions, findings, and conclusions or recommendations expressed here are those of the authors and do not necessarily reflect the views of the funding agencies.

## References

[1] Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, and Jeannette M Wing. "Automated generation and analysis of attack graphs". In IEEE Symposium on Security and Privacy, pp. 273-284, IEEE, 2002.

[2] Mustafa Abdallah, Parinaz Naghizadeh, Ashish Hota, Timothy Cason, Saurabh Bagchi, and Shreyas Sundaram, "Impacts of Behavioral Probability Weighting on Security Investments in Interdependent Systems." American Control Conference (ACC), pp. 5260-5265, 2019.

[3] Alessandro Acquisti. "Nudging privacy: The behavioral economics of personal information." IEEE security and privacy, 2009.

[4] Lina Perelman and Saurabh Amin. "A network interdiction model for analyzing the vulnerability of water distribution systems." In Proceedings of the 3rd international conference on High confidence networked systems, pp. 135-144, ACM, 2014.

[5] Ashish R. Hota and Shreyas Sundaram. "Interdependent Security Games on Networks Under Behavioral Probability Weighting." In IEEE Transactions on Control of Network Systems, vol. 5, no. 1, pp. 262-273, 2018.