CERIAS

The Center for Education and Research in Information Assurance and Security

A Quantal Response Analysis of Human Decision-making in Interdependent Security Games Modeled by Attack Graphs

Md Reya Shad Azim[1], Timothy Cason[2], and Mustafa Abdallah[1]

[1]Purdue University in Indianapolis, [2]Purdue University, West Lafayette

azimm@purdue.edu, cason@purdue.edu, abdalla0@purdue.edu

Introduction

- Interdependent systems (e.g., **power grid** and **industrial control systems**) are increasingly vulnerable to sophisticated cyberattacks targeting critical infrastructure.
- These systems involves **multiple defenders** managing different **connected** subsystems.
- Defenders must **allocate their limited security budget efficiently** to reduce security risks.
- Traditional security models assume rational decision-makers, but **human decision-making** often **deviates due to cognitive limitations**.

Research Question:
For large-scale interdependent systems, what are the **impacts of human behavioral errors on security investments** allocated by human defenders and their **effects on the total system's security cost**?

Motivation

- Existing **security models rely on classical decision-making**, assuming perfect rationality, which does not align with real-world human behavior.
- Human defenders **exhibit bounded rationality and probabilistic decision-making**.
- Understanding **quantal response equilibrium (QRE) in interdependent security setup** can help **quantify inefficiencies in security investments** and improve security defense.

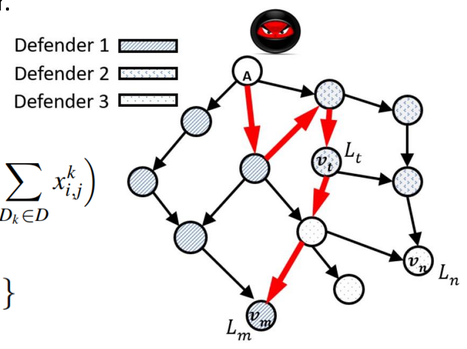
Our Contribution

- We introduce a **security investment model** for **human defenders** in interdependent systems modeled by **attack graphs**.
- We **develop a framework** incorporating **quantal response equilibrium** in order to model probabilistic security decision-making.
- We **quantify inefficiencies** arising **from bounded rationality** on system's security.

Background and Problem Setup

- **Threat & Defense Model:**
- We study security games consisting of **an attacker** and **multiple defenders** interacting through an attack graph G = (V, E).
- Attacker uses **stepping-stone** to launch an attack from source to target assets.
- Each defender $D_k \in D$ has control of a subset of assets $V_k \subseteq V$.
- Among all the assets in the network, a subset $V_m \subseteq V$ contains **critical assets**, the compromise of which entails a *financial loss* for the corresponding defender.
- The **cost of defender** D_k is given by

$$C_k(x_k, x_{-k}) \triangleq \sum_{v_m \in V_k} L_m \left(\max_{P \in \mathbb{P}_m} \prod_{(v_i,v_j)\in P} p_{ij}\,(x_{i,j}) \right)$$



- **Probability of Successful Attack**: $p_{i,j}(x_{i,j}) = p^0_{i,j} \exp\left(-s_{i,j} \sum_{D_k \in D} x^k_{i,j} \right)$
- **Defense Strategy Space:** $X_k := \{\mathbf{x}_k \in \mathbb{R}^{|\mathcal{E}|}_{\geq 0} \,|\, 1^T \mathbf{x}_k \leq B_k\}$

Quantal Response Equilibrium (QRE)

- **Quantal response equilibrium (QRE)** is a solution concept in game theory which provides an **equilibrium notion with bounded rationality**.
- It is a statistical tool to model **human errors** in choosing effective strategies.
- In our interdependent security game, we use *logit* QRE, where **defender's security investment profiles would be chosen according to the probability distribution**:

$$\sigma_{kl} = \frac{\exp(-\lambda_k\, EC_{kl}(\sigma_{-k}))}{\sum_{\mathbf{x}_l \in X_k} \exp(-\lambda_k\, EC_{kl}(\sigma_{-k}))}$$

where σ_{kl} is the **probability of defender D_k choosing investment profile** $x_l \in X_k$

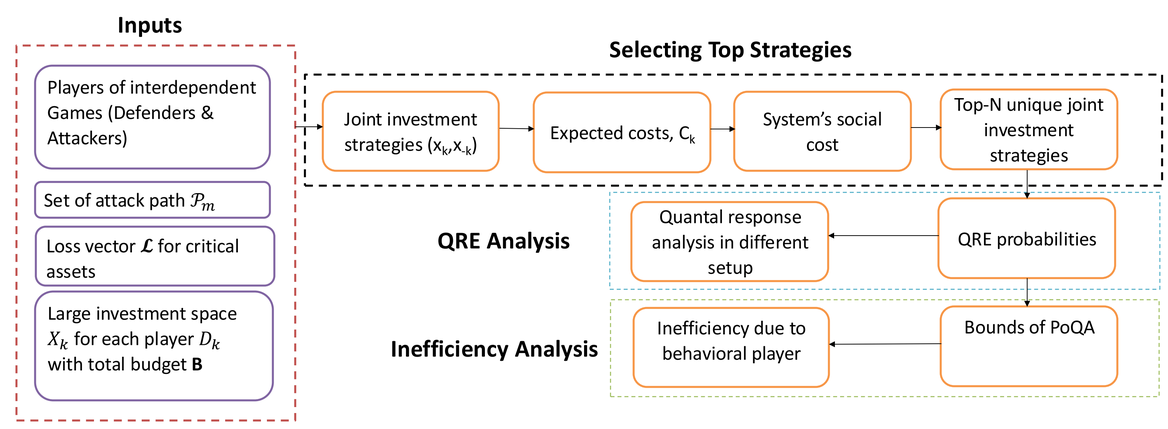
  - $EC_{kl}(\sigma_{-k})$ is the expected cost of defender D_k,
  - $\lambda \in [0, \infty)$

- We **introduce a metric to quantify the inefficiencies** of defenders' behavioral decision-making characterized by *quantal errors*

$$PoQA = \frac{\sum_{D_k \in \mathcal{D}} \left(\sum_{\mathbf{x}_l \in X^{\text{QRE}}_k} \sigma_{kl} \times EC_{kl}(\sigma_{-k}) \right)}{C(\mathbf{x}^*)}$$

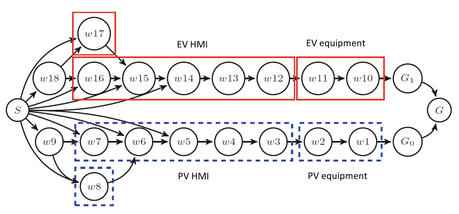
- PoQA is upper bounded by: $PoQA \leq \exp(B)$

Model Overview

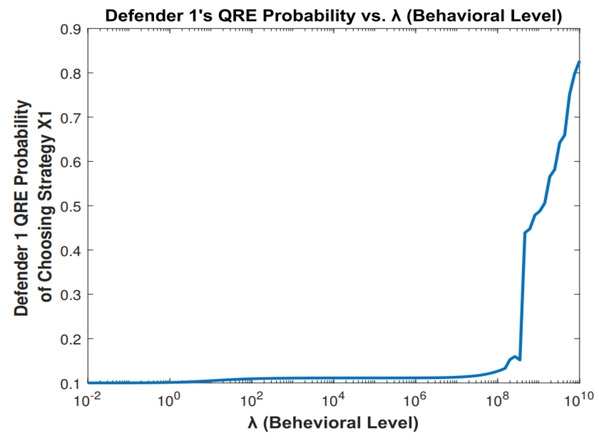


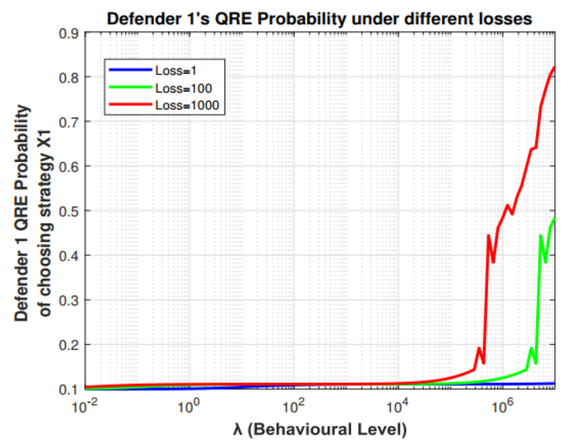
Overview of Quantal Response Analysis of Human Decision-making in Interdependent Security Games

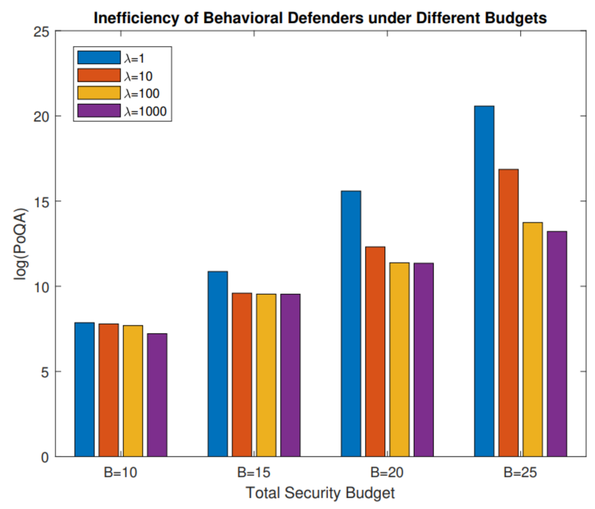
Main Results

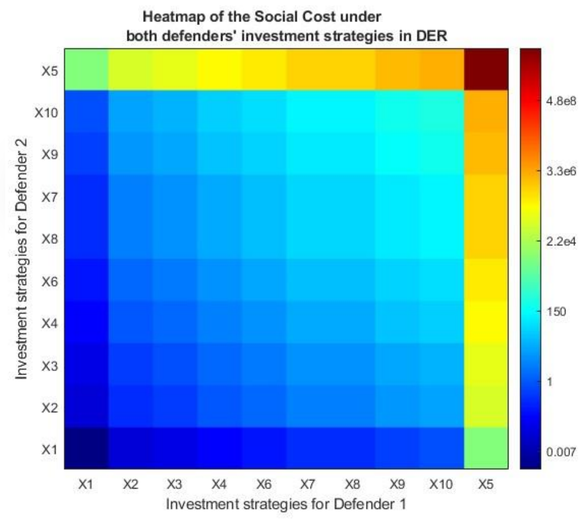


Strategy \ Edge Investment	$x_{1,0}$	$x_{2,1}$	$x_{3,2}$	$x_{4,3}$	$x_{5,4}$	$x_{6,5}$	$x_{7,6}$	$x_{9,7}$	$x_{s,9}$	$x_{s,5}$	$x_{s,6}$	$x_{s,7}$	$x_{s,8}$	$x_{9,8}$	$x_{8,6}$
X_1	15	0	0	0	0	0	0	0	0	0	0	0	0	0	0
X_2	2.5	2.5	2.5	2.5	2.5	2.5	0	0	0	0	0	0	0	0	0
X_3	0	3	3	3	3	3	0	0	0	0	0	0	0	0	0
X_4	0	0	3.75	3.75	3.75	3.75	0	0	0	0	0	0	0	0	0
X_5	0	0	0	0	0	15	0	0	0	0	0	0	0	0	0
X_6	2.14	2.14	2.14	2.1429	2.14	2.14	2.14	0	0	0	0	0	0	0	0
X_7	0	0	0	5	5	5	0	0	0	0	0	0	0	0	0
X_8	0	2.5	2.5	2.5	2.5	2.5	2.5	0	0	0	0	0	0	0	0
X_9	1.87	1.87	1.87	1.87	1.87	1.87	1.87	1.87	0	0	0	0	0	0	0
X_10	0	0	3	3	3	3	3	0	0	0	0	0	0	0	0









Key Takeaways

- Human defenders **do not always make perfectly rational security investment decisions**, leading to **suboptimal protection of interdependent systems**.
- The **introduction of QRE provides a more realistic approach** to modeling human security investments in interdependent systems.
- PoQA analysis reveals **that inefficiencies in security investments grow exponentially with defenders' security budget**, emphasizing the need for improved resource allocation.

Acknowledgement

This work is supported in part by AnalytixIN from Lilly Endowment, Enhanced Mentoring Program with Opportunities for Ways to Excel in Research (EMPOWER), and 1st Year Research Immersion Program (1RIP) grants from the office of the Vice Chancellor for Research at Indiana University-Purdue University Indianapolis.

PURDUE UNIVERSITY

CERIAS