IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 23 February 2024, accepted 7 April 2024, date of publication 19 April 2024, date of current version 26 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3391305

RESEARCH ARTICLE

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

MD. REYA SHAD AZIM[1], (Graduate Student Member, IEEE), TIMOTHY CASON[2], (Senior Member, IEEE), AND MUSTAFA ABDALLAH[3], (Member, IEEE)

[1]Department of Electrical and Computer Engineering, Purdue School of Engineering and Technology, Indiana University–Purdue University Indianapolis (IUPUI), Indianapolis, IN 46202, USA
[2]Department of Economics, Purdue University, West Lafayette, IN 47907, USA
[3]Department of Computer and Information Technology, Purdue School of Engineering and Technology, Indiana University–Purdue University Indianapolis (IUPUI), Indianapolis, IN 46202, USA

Corresponding author: Mustafa Abdallah (mabdall@iu.edu)

This work was supported in part by AnalytixIN, Enhanced Mentoring Program with Opportunities for Ways to Excel in Research (EMPOWER); and in part by 1st Year Research Immersion Program (1RIP) Grant from the Office of the Vice Chancellor for Research at Indiana University–Purdue University Indianapolis.

ABSTRACT Interdependent systems, under the management of multiple decision-makers, confront rapidly growing cybersecurity threats. This paper delves into the realm of security decision-making within these complex interdependent systems managed by multiple defenders. Each defender assumes responsibility for safeguarding a specific subnetwork of the system against potential attacks. The relationships between these assets are depicted through an attack graph, where edges connecting assets signify that the compromise of one asset could expose vulnerabilities in another asset. These edges are associated with probabilities that represent the likelihood of a successful attack, which can be reduced through security investments by the defenders. Our approach involves modeling these systems using game-theoretic frameworks, accounting for the impact of bounded rationality and imperfect best-response behavior—as frequently observed in human decision-making within the domains of behavioral economics and psychology. We first establish the existence of quantal response equilibrium in our interdependent security games. We present illustrative examples to highlight the disparities between the solutions derived from the social optimal perspective and those arising from quantal response equilibrium. Subsequently, we analyze the inefficiency introduced by behavioral players with this type of bounded rationality in terms of the overall social cost of the system. We adapt a widely recognized metric to quantify the extent of this inefficiency, providing bounds and illustrating its exponential growth with an increase in the security budget. To assess our models, we employ a representative real-world interdependent system and compare the game-theoretic optimal investment strategies to those derived from a socially optimal standpoint.

INDEX TERMS Attack graphs, quantal response equilibrium, central planning, security games, cyber security, human decision-making, interdependent systems, quantal errors, risk assessment.

I. INTRODUCTION

Interdependent systems face an ever-increasing threat of sophisticated cyberattacks orchestrated by external adversaries. These attacks pose significant risks to critical infrastructures on a large scale [1], [2]. The primary objective behind such attacks is to gain control of vital assets within these systems [3]. In pursuit of this goal, attackers often exploit various vulnerabilities associated with each critical asset. Consequently, there have been numerous efforts to

The associate editor coordinating the review of this manuscript and approving it for publication was Lei Shu.

enhance the cybersecurity posture of these interdependent systems [4], [5], [6].

In this complex landscape, security executives responsible for managing these interdependent systems must make judicious allocations of their limited security budgets to mitigate security risks. This resource allocation problem is further complicated by the fact that large-scale systems comprise multiple interdependent subsystems, each overseen by different operators. Each operator prioritizes the security of their own subsystem, resulting in self-interested decision-making behavior. This inherent selfish behavior is a well-documented phenomenon in the literature on security resource allocation [7], [8], [9]. Prior work has considered such security resource allocation problems in interdependent systems via both decision- and game-theoretic settings in which the security risk faced by an operator (defender) depends on her security investments and the aggregate investments by other defenders [10], [11], [12].

Although there is a large body of security literature capturing security resource allocation problems in interdependent systems, most of the existing work has relied on *classical models* of decision-making (with few exceptions that explored the impact of human prospect-theoretic attitudes for interdependent security games [13], [14], [15], [16], [17], [18]), where all defenders and attackers are assumed to make fully rational risk evaluations, perceptions, and security decisions [11], [19]. On the contrary, behavioral economics and psychology have shown empirically that humans consistently deviate from these classical (fully rational) models of decision-making.

Notably, research in *behavioral economics and psychology* has shown that humans consistently make errors in choosing efficient (pure) strategies when making decisions [20]. In contrast to classical decision-making, the quantal response equilibrium takes into account the fact that human decision-makers may not always make perfectly rational decisions. Instead, it allows for decision-making where the players in a game may not always choose the best response with certainty, but their choices are probabilistic and influenced by factors such as noise and cognitive limitations. Many empirical studies have provided evidence for this class of behavioral models [21], [22], [23]. The effects of this quantal behavioral decision-making are relevant for evaluating security of interdependent systems in which decisions on implementing security controls are made through human decision-making, albeit with help from threat assessment tools [24], [25].

Most of existing research that has considered behavioral economics in security and privacy has the common theme of considering user choices regarding privacy and how people treat their own personal data [26] or entirely based on psychological studies [27]. There are a few exceptions that have leveraged mathematical analysis to predict the effect of behavioral decision-making on the players' investments in organizational contexts with interdependent systems [13], [14], [15], [16], [17], [18]. However, these works have only focused only on prospect-theoretic attitudes and do not consider quantal behavioral errors which is the focus of our work. Several prior works have shown such quantal response equilibrium for security problems, including defense of isolated targets [28], and Stackelberg security games with two players (one attacker and one defender) [29], [30], [31], [32], [33]. However, this class of games does not incorporate security externalities between multiple defenders and network interdependencies that are the focus of the current work.

In contrast to such studies, we consider general defense allocation schemes that can be applied to any system where failure scenarios are represented by an attack graph while modeling human behavioral decision-making. Our work introduces a rigorous framework that combines three important threads of human decision-making for distributed systems security research: game theory (modeled by multi-defender security games against external adversaries), interdependent systems (modeled by attack graphs), and behavioral economics (modeled by quantal response equilibrium).

Throughout our paper, we consider two classes of players.

A. BEHAVIORAL DEFENDERS

These defenders make security investment decisions subject to noise and probabilistically, as found in behavioral economics decision-making. They are assumed to make errors in choosing which pure security investment to allocate [22]. In particular, the probability of choosing any particular security investment profile is positively related to the payoff from that investment (in our setup, the lower the defender's cost, the better the investment profile).

B. NON-BEHAVIORAL (RATIONAL) DEFENDERS

These defenders make security investment decisions based on the classical economics models of perfectly rational decision-making. Thus, they correctly choose pure security investment strategies to minimize their expected cost function(s).

C. PROBLEM SETUP AND QUANTAL RESPONSE FOR INTERDEPENDENT SECURITY GAMES

We first model the effect that behavioral decision-making (quantal response) has on interdependent systems with multiple defenders. In these systems, each defender is responsible for defending a set of critical assets (i.e., a subnetwork of the whole network) against external adversaries. Due to the nature of interdependent systems, these external adversaries usually perform stepping-stone attacks to leverage vulnerabilities within the network in order to compromise critical targets. These stepping-stone attacks can be captured via the notion of *attack graphs*, which represent all possible attack paths that the adversary takes to reach critical assets within the system [19], [34].

We formulate such a scenario as a *behavioral interdependent security game*. We show that such a game has a quantal

response equilibrium (QRE). We calculate the QRE where the search strategy for each decision-maker adopts quantal response dynamics [21], [22]. We then show the difference under behavioral decision-making between the Pure-Strategy Nash Equilibrium (PNE) (with rational players), the socially optimal investment (with central planner), and the QRE (with behavioral players) via multiple motivating examples where we show the effect of behavioral level on the probability of deviating from rational behavior and the interdependent system's security level.

We then propose a new metric that we call *Price of Quantal Anarchy (PoQA)* to measure the inefficiency arising from the existence of behavioral players with quantal errors on the social cost of the interdependent system. In particular, we adapt the well-known price of anarchy concept [35] to our interdependent security game modeled by attack graphs and behavioral defenders (with quantal errors). The PoQA captures the degree of suboptimality resulting from quantal response equilibrium. We provide tight bounds for the PoQA and show a fundamental result that PoQA grows exponentially in the total security budget of the defenders. We then develop an algorithm to compute the QRE under many security investment strategies, in contrast to prior works [29], [30], [31], [32], [33] that only considered limited strategy space given their setup.

We finally evaluate our findings using an attack graph that represents a realistic interdependent system and attack paths through it. This system is a distributed energy resource (DER.1) [25] (modeled by the US National Electric Sector Cybersecurity Organization Resource (NESCOR)). In our evaluation, we show the effects of different parameters (e.g., financial loss values of system's assets and amount of security budget). In conducting our analysis, we address several domain-specific challenges in the context of security of interdependent systems. These include augmenting the attack graph with certain parameters such as sensitivity of edges to security investments (Eqn. (1)), the success attack probabilities (Section II-C), modifying quantal response formulation for our interdependent security games (Section III), and incorporating human behavioral errors in our formulations (Section III).

In summary, this paper makes the following contributions:

1) We propose a *security investment* model for human defenders of interdependent systems where defenders' assets have mutual interdependencies and attack scenarios are captured by attack graphs.
2) We show the effect of an important human behavioral error (probabilistic and noisy best response as modeled as quantal response equilibrium) on security resource allocation decision-making of human defenders for securing interdependent systems.
3) We introduce a metric for quantifying the level of inefficiency due to the existence of behavioral players. We give bounds on this level of inefficiency.

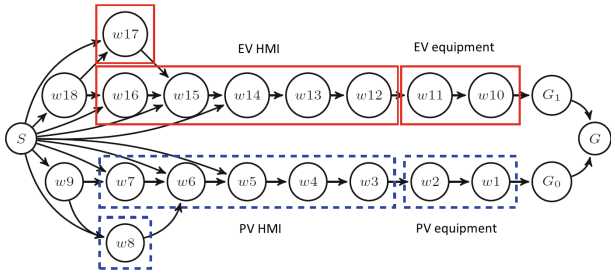


FIGURE 1. Attack Graph of DER interdependent System.

4) We illustrate the effects of *behavioral* errors of human decision-making on system security through a real-world interdependent system. We also analyze different system parameters that affect the security level of interdependent systems under our behavioral model.

The remainder of the paper is organized as follows. Section II provides background and preliminaries on interdependent security games and the main components for such games. Section III presents the proposed quantal response equilibrium framework and establishes the existence of QRE in interdependent security games. We provide motivational examples to explain the different aspects of QRE in Section IV. We measure the inefficiency of QRE and provide its bounds in Section V. Section VI provides our strategy pruning algorithm. We provide the evaluation of our framework on a real-world interdependent system in Section VIII provides the literature review. Section VII. Section IX provides the main discussion and limitations of current work. Finally, Section X concludes the paper and presents prospective future research directions.

II. BACKGROUND AND PROBLEM SETUP

We begin by presenting a background on interdependent security games, establishing a theoretical basis that can be used to model any multi-defender interdependent system. A motivating example for real-world interdependent system is shown in Figure 1. Then, a simple example of our setup is shown in Figure 2, which represents a system consisting of three interdependent defenders and an external attacker who seeks to exploit vulnerabilities within the network in order to reach and compromise critical targets [25]. We formalize the attacker and defenders' utilities, and actions in this section.

A. MOTIVATING APPLICATION FOR INTERDEPENDENT SECURITY GAMES

The security problems that we are addressing in this paper arise in a wide spectrum of applications. We briefly describe one example application here to motivate the main ideas in the paper. Our research goals are to understand the effect of behavioral errors for defenders (which is represented by quantal response equilibrium) in such application to provide a more efficient security resource allocation method in such

systems. We will also quantify the degree of inefficiency of behavioral security decision-makers and the effects of system parameters on the overall system security.

Application: Optimal Security Investments in Interdependent DER System. Consider the example of distributed energy resource (DER) network illustrated in Figure 10, based on the US National Electric Sector Cybersecurity Organization Resource (NESCOR) guidelines for electric grid [25]. In this example, there are two equipment critical assets: a photo voltaic (PV) generator and an electric vehicle (EV) charging station. Each equipment is accompanied by a human machine interface (HMI), the only gateway through which the equipment can be controlled. The DER failure scenario is triggered when the attacker gets access to the HMI. The vulnerability of the system may arise due to various reasons, such as hacking of the HMI, or an insider attack. Once the attacker gets access to the system, she changes the DER settings and gets physical access to the DER equipment which can cause serious physical damage to the system.

There are interdependencies between the various assets in the two subsystems, captured by an attack graph shown in Figure 1. An edge from one asset to another indicates that if the former asset is compromised by an attacker, the latter can also be subsequently compromised.

Given the interdependency network associated with the DER system, each defender in the network has to choose how much to invest in security on edges in order to reduce the probability that the physical equipment (PV for defender 1 and EV for defender 2) are compromised by the attacker. The security decisions made by a defender will depend on the investments made by the other defender, leading to a game-theoretic formulation of the resource allocation problem. The key questions that we seek to answer in this paper are: What is the effect of behavioral defenders with quantal error?; How to quantify the degree of inefficiency under behavioral decision-makers compared to socially optimal security investments?; and How does the system parameters affect the overall security level of the system (social cost) under behavioral error? Our framework in this paper revolves around encapsulating such scenario and providing answers to the above questions.

B. THREAT MODEL

We study security games consisting of an attacker and multiple defenders interacting through an attack graph $G = (V, \mathcal{E})$. The nodes V of the attack graph represent the assets in the system, while the edges $\mathcal{E}$ capture the attack progress between the assets. In particular, an edge from v_i to v_j, $(v_i, v_j) \in \mathcal{E}$, indicates that if asset v_i is compromised by the attacker, it can be used as a stepping stone to launch an attack on asset v_j. The baseline probability that the attacker can successfully compromise v_j given that it has compromised v_i, is denoted by the edge weight $p^0_{i,j} \in [0, 1]$. The baseline probability is the probability of successful compromise without any security investment on the edges for protecting the assets.[1] The attacker initiates attacks on the network from a source node v_s (or multiple source nodes), and aims to reach a target node $v_m \in V_k$, i.e., a critical node for defender D_k.

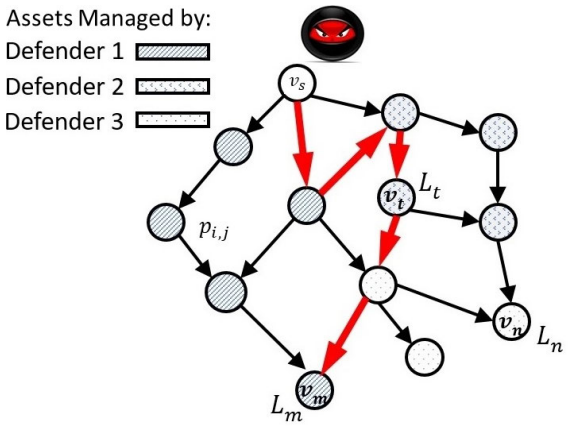


FIGURE 2. An outline of interdependent security framework. The connections between assets are depicted as edges. The objective of the attacker is to compromise critical assets by initiating stepping-stone attacks, commencing at node v_s. The red edges illustrate a potential attack path targeting asset v_m.

C. DEFENSE MODEL

Each defender $D_k \in \mathcal{D}$, where the set $\mathcal{D}$ denotes the set of all defenders in the system, has control of a subset of assets $V_k \subseteq V$. This is motivated by the fact that a large-scale interdependent system comprises a number of smaller subnetworks, each owned by a different stakeholder. 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. Specifically, if asset $v_m \in V_m$ is compromised by the attacker, any defender D_k for whom $v_m \in V_k$ suffers a financial loss $L_m \in \mathbb{R}_{>0}$. Note that L_m is a scalar value representing the financial loss of asset v_m is compromised. The higher the importance of the critical asset v_m, the higher the financial loss L_m if this asset is compromised.

To protect the critical assets from being reached through stepping-stone attacks, the defenders invest their resources in order to strengthen the security of the edges in the network. Specifically, let $x^k_{i,j}$ denote the investment of a defender D_k on edge $(v_i, v_j) \in \mathcal{E}$, and thus $x_{i,j} = \sum_{D_k \in D} x^k_{i,j}$ is the total investment on that edge by all eligible defenders. Then, the probability of successfully compromising v_j starting from v_i

[1] In practice, Common Vulnerability Scoring System (CVSS) [36] can be used for estimating initial probabilities of attack (for each edge in our setting). For example, [34] takes the access complexity submetric in the CVSS (which takes values in {low, medium, high}, representing the complexity of exploiting the vulnerability) and maps it to a probability of exploit (attack) success. The more complex it is to exploit a vulnerability, the less likely an attacker will succeed. Similarly, [37] provides methods and tables to estimate the probability of successful attack from CVSS metrics. We refer also to Section IX for more detailed discussion.

is given by $p_{i,j}(x_{i,j})$. In addition, let $s_{i,j} \in [1, \infty)$ denote the sensitivity of edge (v_i, v_j) to the total investment $x_{i,j}$. The edges that are easier to defend have a larger sensitivity (i.e., a faster decrease in attack success probability with investments).

1) DEFENSE STRATEGY SPACE

The defense strategy space of each defender $D_k \in \mathcal{D}$ is defined by

$$X_k := \{\mathbf{x}_k \in \mathbb{R}^{|\mathcal{E}|}_{\geq 0} \,|\, 1^T \mathbf{x}_k \leq B_k\}.$$

In words, X_k is the set of feasible security investments for defender D_k. It consists of all possible non-negative investments on the edges of the graph such that the sum of these investments is upper bounded by the defender's security budget B_k. This captures the real-world assumption of limited security resources for human security decision-makers. We denote any particular vector of investments by defender D_k as $\mathbf{x}_k \in X_k$. Each entry of $\mathbf{x}_k$ denotes the security investment on an edge within the attack graph of the interdependent system.

2) PROBABILITY OF SUCCESSFUL ATTACK

We let the probability of successfully compromising v_j starting from v_i be given by

$$p_{i,j}(x_{i,j}) = p^0_{i,j} \exp\Big(- s_{i,j} \sum_{D_k \in D} x^k_{i,j} \Big). \tag{1}$$

In other words, the likelihood of a successful attack on the edge (v_i, v_j) diminishes exponentially as the total investments made by all defenders on that edge increase. This probability function belongs to a category frequently examined in the field of security economics [9], [13], [18], [38].

D. COST MINIMIZATION

Let P_m be the set of all attack paths from v_s to v_m. The defender assumes the worst-case scenario, i.e., the attacker exploits the most vulnerable path to each target asset.[2] Mathematically, this can be captured via the following cost (total loss) function for defender D_k:

$$C_k(\mathbf{x}_k, \mathbf{x}_{-k}) = \sum_{v_m \in V_k} L_m \Big(\max_{P \in P_m} \prod_{(v_i, v_j) \in P} p_{i,j}(x_{i,j}) \Big). \tag{2}$$

Each defender $D_k \in \mathcal{D}$ chooses her security investments $\mathbf{x}_k := \{x^k_{i,j}\}_{(v_i,v_j)\in\mathcal{E}_k}$ to minimize her cost (total loss), given by (2) where $\mathbf{x}_{-k}$ is the vector of investments by defenders other than D_k. Such cost minimization is subject to her limited total security investment budget B_k (i.e., $\sum_{(v_i,v_j)\in\mathcal{E}} x^k_{i,j} \leq B_k$), and non-negativity of the investments, i.e., $x^k_{i,j} \geq 0$. It is easy to show that the total loss function (2) is convex in the investment $x_{i,j}$. Such convexity follows from the second derivative of the loss function in (2) with respect to $x_{i,j}$.

[2]Our formulation also encompasses scenarios where each defender contends with a distinct attacker who exploits the most susceptible (vulnerable) attack path leading to that defender's assets.

E. SECURITY GAME SETUP

After defining the threat and defense models and the main goals of players, we now primarily design a security investment decision-making model for interdependent systems that takes into account investments by all defenders.

1) GAME FORM

Our proposed interdependent security game will be formally defined as follows: $\Gamma = (\mathcal{D}, (X_k)_{k=1}^{|D|}, (C_k(\cdot))_{k=1}^{|D|})$ with $\mathcal{D} = \{D_1, D_2, \ldots\ldots, D_{|\mathcal{D}|}\}$ denoting the set of defenders protecting the assets of the interdependent system, $(X_k)_{k=1}^{|D|}$ are the sets of feasible security investments of all defenders, and $(C_k(\cdot))_{k=1}^{|D|}$ are the defenders' cost functions.

2) ATTACK ON INTERDEPENDENT SYSTEMS

In interdependent systems (such as cyber-physical systems), the adversaries exhibit various capabilities and employ different attack strategies concurrently, aiming to compromise different assets within the system. In Figure 2, where attackers traverse a sequence of nodes along the network edges until they reach their target asset. After all defenders have allocated their resources (or security investments), attackers select the path with the highest probability of success for compromising each target asset. This selection process is akin to identifying the most vulnerable path to the target asset. Such attack models, where attackers choose a single path to their target, have been studied in prior literature [8], [18]. To capture this scenario, given a set of security investments by defenders, the vulnerability of an asset v_m is defined as the maximum attack probability among all possible paths leading to that asset. Formally, the vulnerability of $v_m \in V$ is represented as:

$$\text{vulnerability}(v_m) = \max_{P \in P_m} \prod_{(v_i, v_j) \in P} p_{i,j}(x_{i,j}).$$

Here, P_m denotes the set of all directed paths from the entry node v_s to asset v_m, and $p_{i,j}(x_{i,j})$ is the conditional probability of successfully compromising v_j given that v_i has been compromised, as defined earlier.

3) DYNAMICS OF DEFENDERS' SECURITY GAME

Each defender D_k aims to minimize her expected cost, defined as the total loss incurred due to the highest probability of attack among all available paths to each of their critical assets. The expected cost for defender D_k is given by equation (2). As the attacker decides on the optimal attack paths to compromise critical assets, the objective of each defender $D_k \in \mathcal{D}$ is to strategically allocate her investment vector $\mathbf{x}_k$ within the budget constraints X_k to minimize the vulnerability of their assets, thereby reducing the expected cost of potential breaches.

The game dynamics can be explained as follows: the first defender D_1 allocates her investment vector $\mathbf{x}_1$ to minimize her cost $C_1(\mathbf{x}_1, \mathbf{x}_{-1})$, then defender D_2 allocates her investment vector $\mathbf{x}_2$ given investment vector of defender

D_1 to minimize her cost function $C_2(\mathbf{x}_2, \mathbf{x}_{-2})$. The same process is done by each defender following best response dynamics. Best response dynamics is a concept commonly used in game theory, particularly in the study of strategic interactions among decision-makers. It describes a process where each player in a game continuously adjusts their strategy to maximize their own payoff (here minimize the security cost), given the strategies chosen by the other players. In a best response dynamic, players iteratively update their strategies based on their perception of the strategies being employed by others. At each step, a player evaluates their available strategies (here, security investment vectors in X_k) and selects the one that yields the lowest cost, assuming the other players' strategies remain fixed.

This process of continual adjustment would eventually lead to the convergence of strategies towards a pure strategy Nash equilibrium (PNE), where no player has an incentive to unilaterally deviate from her strategy, given the strategies chosen by the other players.

4) EFFECT OF DEFENSE INVESTMENTS FROM SECURITY GAME ON SECURITY LEVEL OF INTERDEPENDENT SYSTEM

This game dynamics in interdependent systems have significant implications on the overall security posture of the system. In particular, defenders' investments on edges influence the probabilities of successful attacks on edges. The evolving nature of the gaming dynamics reflects the interactions between multiple defenders, shaping the resilience and vulnerability of the system over time. Another important part in the context of interdependent security games that in contrast to isolated systems, the edges of the attack graph of the interdependent systems can be common across different defenders (e.g., the red outgoing edge from v_s can be used to reach critical assets of the three defenders). Thus, there are externalities between defenders under their investments (i.e., one defender's cost can be reduced by other defender's investments on edges that belong to attack paths to that defender).

5) EXISTENCE OF PURE NASH EQUILIBRIUM

Having explained the best response dynamics of our game, we next show that such a game would reach a PNE. A profile of security investments by the defenders is said to be a PNE if no defender can decrease her cost by unilaterally changing her security investments. Under the probability of successful attack in (1), the interdependent security game possesses a pure strategy Nash equilibrium (PNE) since the feasible defense strategy space X_k is nonempty, compact, and convex for each defender $D_k \in \mathcal{D}$. Furthermore, for all $D_k \in \mathcal{D}$ and investment vector $\mathbf{x}_k$, the cost function $C(\mathbf{x}_k, \mathbf{x}_{-k})$ in (2) is convex in $\mathbf{x}_k \in X_k$. As a result, the interdependent security game is an instance of concave games, which always have a PNE [8], [39].

Having defined the interdependent security game setup, we next incorporate quantal response notion into our framework, which is the main focus of the current work.

III. QUANTAL RESPONSE EQUILIBRIUM

We start by presenting the proposed quantal response equilibrium framework and then establish the existence of QRE in interdependent security games.

A. BACKGROUND ABOUT QUANTAL RESPONSE

Quantal response equilibrium (QRE) is a solution concept in game theory which provides an equilibrium notion [40], [41] with bounded rationality [21], [22]. It provides a structural, statistical model of human operators where humans consistently make errors in choosing efficient strategies as shown in behavioral economics and psychology when modeling human decision-making [21], [22], [23]. In contrast to the deterministic and perfect best-response behavior of Nash equilibrium, in the QRE operators "better respond" and choose strategies that provide higher payoffs with a higher probability.

In the standard formulation of QRE (logit equilibrium), player's strategies are chosen according to the probability distribution:

$$\sigma_{kl} = \frac{\exp\big(\lambda EU_{kl}(\sigma_{-k})\big)}{\sum_l \exp\big(\lambda EU_{kl}(\sigma_{-k})\big)}, \tag{3}$$

where σ_{kl} is the probability of player k choosing strategy l. EU_{kl} is the expected utility to player k choosing strategy l under the belief that other players are playing according to the probability distribution σ_{-k}. Note that $\lambda \in [0, \infty)$ is the behavioral level of the players. The larger the value of λ, the more rational are the defenders.

B. QUANTAL RESPONSE IN OUR INTERDEPENDENT SECURITY GAME

In our interdependent security game logit equilibrium, the defender's security investment profiles would be chosen according to the probability distribution

$$\sigma_{kl} = \frac{\exp\big(-\lambda_k\, EC_{kl}(\sigma_{-k})\big)}{\sum_{\mathbf{x}_l \in X_k} \exp\big(-\lambda_k\, EC_{kl}(\sigma_{-k})\big)}, \tag{4}$$

where σ_{kl} is the probability of defender D_k choosing investment profile $\mathbf{x}_l \in X_k$, and EC_{kl} (σ_{-k}) is the expected cost of defender D_k of choosing investment strategy $\mathbf{x}_l$ under the belief that other players are playing according to the probability distribution σ_{-k} which is given by

$$EC_{kl}(\boldsymbol{\sigma}_{-k}) = \sum_{\mathbf{x}_j \in X_k} \sigma_{kj}\; C_k(\mathbf{x}_k, \mathbf{x}_{-k}).$$

Here, the probability of player D_k choosing $\mathbf{x}_l$ increases if the expected cost for defender D_k under that $\mathbf{x}_l$ decreases. Based on such quantal responses, our search seeks to find fixed points to achieve quantal response equilibrium $(\sigma_k^*, \sigma_{-k}^*)$ as in mean field theory [21]. In our evaluation, we show the effects of the non-negative parameter λ_k

which represents the rationality level of defender D_k. When $\lambda_k \to 0$, the defender becomes "completely non-rational (behavioral)" and chooses each investment profile with equal probability. As $\lambda_k \to \infty$, players become "perfectly rational" and the game approaches a Pure Strategy Nash equilibrium.

Remark 1: The subscript k in λ_k allows each defender in the interdependent Behavioral Security Game to have a different level of rationality. Throughout the rest of the paper, we will drop the subscript k when it is clear from the context. ■

C. GAME DYNAMICS IN QRE

QRE is a refinement of the Nash equilibrium concept, taking into account bounded rationality and stochasticity in players' decision-making processes. In interdependent security games, incorporating QRE adds another dimension to the strategic interactions between players. QRE allows for a more realistic representation of human decision-making, acknowledging that players may not always select the strictly optimal strategy but instead exhibit a degree of randomness or error in their choices. As defenders exhibit bounded rationality when allocating resources, considering factors such as uncertainty in attacker behavior, incomplete information, and cognitive biases, the inclusion of QRE enables a more nuanced analysis of how players' decisions are influenced by their perceptions of the game environment and the strategies employed by their counterpart. In our setup we use logit QRE where defenders' strategies are chosen probabilistically (according to (4)), with the likelihood of selecting a particular strategy influenced by its expected utility relative to other available strategies and a noise parameter λ representing the level of noise or randomness in decision-making. Defenders adopt mixed strategies, allocating resources based on cost function (2) and the stochastic nature of QRE introduces a level of uncertainty into players' decision-making, reflecting the inherent unpredictability of real-world cybersecurity scenarios [41].

One challenge we face here is that the strategy space X_k in our game contains many possible security investment vectors in contrast to the discrete strategies considered in prior work [29], [30], [31], [32]. To tackle this, we prune such vectors according to the expected cost to reduce the search space for the quantal response dynamics (via removing investment vectors that yield very high expected cost). We outline our main pruning algorithm in Section VI.

D. EXISTENCE OF A QUANTAL RESPONSE EQUILIBRIUM

We first establish the existence of a quantal response equilibrium (QRE) for the class of interdependent security games defined in Section III. Recall that a mixed strategy of profiles of security investments by the defenders is said to be a QRE when defenders assign probabilities to their available security investment profiles, representing the likelihood of selecting each profile. These probabilities are determined by the players' quantal response function (4), which describes how sensitive players are to the differences in expected costs between those different investment strategies.

TABLE 1. The security investment strategies for both defenders in our mathematical analysis example in Figure 3.

Strategy \ Edge Investment	$x_{s,1}$	$x_{s,2}$	$x_{1,3}$	$x_{2,3}$	$x_{3,t}$
X_1	0	0	0	0	10
X_2	2.5	2.5	2.5	2.5	0
X_3	5	5	0	0	0
X_4	2.5	2.5	0	0	5
X_5	0	0	2.5	2.5	5

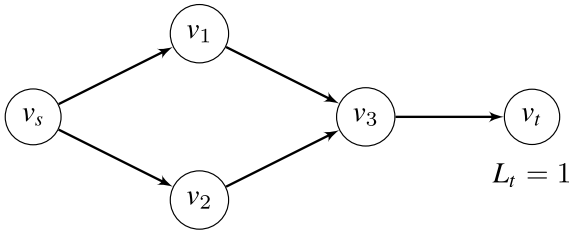


FIGURE 3. An attack graph for an interdependent security game instance with two defenders where both defenders seek to defend critical asset v_t which induces a unit loss for both defenders if compromised by the attacker (starting from v_s).

Proposition 1: Suppose the quantal response function for each defender $D_k \in \mathcal{D}$ is given by (4) and that the attack success function $p_{i,j}(x)$ is a twice-differentiable, convex, and decreasing function in x for all edges $(v_i, v_j) \in \mathcal{E}$. Then, the Interdependent Security Game possesses a quantal response equilibrium (QRE) when $\lambda_k \in [0, \infty)$ for each defender D_k.

Proof: The feasible defense strategy space X_k is nonempty, compact and convex for each defender D_k. Furthermore, for all $D_k \in \mathcal{D}$ and investment vectors $\mathbf{x}_{-k}$, the cost function $C_k(\mathbf{x}_k, \mathbf{x}_{-k})$ in (2) is convex in $\mathbf{x}_k \in X_k$. Thus, the logit quantal response function in (4) is interior, continuous, monotonic, and responsive [40]. Therefore, for all $D_k \in \mathcal{D}$, the logit quantal response function in (4) is a regular quantal response function [40]. As a result, the interdependent Security Game considered in our work in Section II possesses a quantal response equilibrium (QRE) [41]. ■

E. MATHEMATICAL ANALYSIS ILLUSTRATION OF FINDING QRE IN INTERDEPENDENT SECURITY GAMES

Having provided our quantal response model and shown the existence of QRE for our interdependent security game, we start by performing a mathematical quantal response analysis for a simplified example with two defenders with two strategies each to explain the concept of quantal response in our context. The goal of limiting the strategies in this mathematical analysis is to give the reader the main insight about how the QRE solution work when applied into our interdependent security games modeled

by attack graphs. We refer to Section V and Section VII that show our main mathematical results and experimental evaluation findings under continuous set of strategies, respectively.

Consider the attack graph of Figure 3, which has two defenders. Both defenders are protecting the critical asset v_t. We assume that defender D_1 has investment strategies X_1 and X_2, and defender D_2 has strategies X_3 and X_4 as shown in Table 1. The probability of successfully compromising v_j starting from v_i is given by (1) where $p_{i,j}(x_{i,j}) = \exp(-x_{i,j})$. To simply focus on the effect of quantal behavioral response, we consider $p^0_{i,j} = 1$ and sensitivity $s_{i,j} = 1$ in this example. We first show the joint defense strategies for both defenders. Then, we calculate the quantal response equilibrium of the defenders' joint strategies under different behavioral levels (i.e., different values of λ).

Recall that we consider a worst case scenario (as given by the cost function (2)). Suppose that each defender has a unit loss for the critical asset v_t (i.e., $L_t = 1$). The four joint defense strategies for the two defenders and the corresponding expected costs for both defenders would be given as follows:

	X_4	X_3
X_1	$\exp(-17.5), \exp(-17.5)$	$\exp(-15), \exp(-15)$
X_2	$\exp(-12.5), \exp(-12.5)$	$\exp(-10), \exp(-10)$

Let p be the probability that defender D_1 chooses investment strategy X_1 and q be the probability that defender D_2 chooses X_4. Then, the quantal response of defender D_1 to a given mixed strategy by defender D_2 (parameterized by q) is to choose investment strategy X_1 with probability p and X_2 with $(1-p)$. In particular, when applying the quantal response function in (4), such probabilistic choice of strategy X_1 would be given by

$$p = \frac{\exp(-\lambda \cdot (\exp(-17.5)q + \exp(-15)(1-q)))}{\exp(-\lambda \cdot (\exp(-17.5)q + \exp(-15)(1-q))) + \exp(-\lambda \cdot (\exp(-12.5)q + \exp(-10)(1-q)))}. \tag{5}$$

Similarly, the quantal response of defender D_2 to a given mixed strategy by defender D_1 (parameterized by p) would be to choose investment strategy X_4 with probability q and X_3 with $(1-q)$. The mixed strategy of defender D_2 is given by

$$q = \frac{\exp(-\lambda \cdot (\exp(-17.5)p + \exp(-12.5)(1-p)))}{\exp(-\lambda \cdot (\exp(-17.5)p + \exp(-12.5)(1-p))) + \exp(-\lambda \cdot (\exp(-15)p + \exp(-10)(1-p)))}. \tag{6}$$

Figure 4 shows the quantal response of the defenders under different behavioral levels. Such quantal response is given by the intersection of the two solid curves (red and blue lines), where each line shows the mixed strategy for one of the defenders. These solid curves are obtained by plotting the above equations (5) and (6). This figure shows the following insights. First, Figure 4a shows that each defender chooses randomly from the two defense strategies with equal probabilities when the defenders are highly behavioral (with very low λ, here $\lambda = 10$). Second, Figure 4c shows that as defenders become more rational (where λ increases), they choose better defense strategies (with lower cost). Finally, Figure 4d emphasizes that QRE achieves PNE (from best responses) for the given strategies for extremely high values of λ. We also show the evolution of the effect of behavioral level (λ) on the QRE solutions in Figure 4e. The mathematical analysis and graphical representation of this example show that the defenders act randomly when they are more behavioral (with low λ) and they act rationally (according to best response) when they are more rational (with high λ).

1) EFFECT OF BEHAVIORAL LEVEL (λ)

In our above example, each defender chooses two defense strategies from Table 1. We extend such example by considering five defense strategies instead of two (i.e., each defender can choose any of the five investment strategies in Table 1). Under such strategic choices, the QRE probabilities of choosing a particular investment strategy is similar for both defenders. However, when increasing the behavioral level (λ) of the defender, the defender becomes more rational and thus the QRE probabilities approach the best responses.[3] Figure 5 illustrates this relationship of QRE probabilities with different defender's behavioral levels.

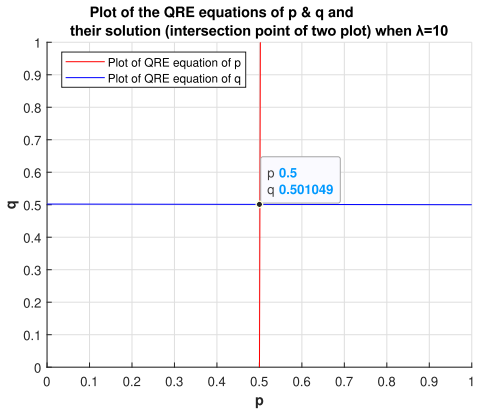
2) EFFECT OF FINANCIAL LOSS AMOUNT OF CRITICAL ASSET

We then measure the effect of increasing the amount of financial loss of the critical asset (i.e., increasing L_t). Figure 6a shows such an effect where the same defender (i.e., with same behavioral level) acts more rationally when the asset v_t has much higher financial loss. In particular, Figure 6a shows the QRE probabilities approach PNE choices faster (lower λ) when the financial loss of the critical asset is higher (red-colored line) compared to the case of lower loss (blue-colored line).

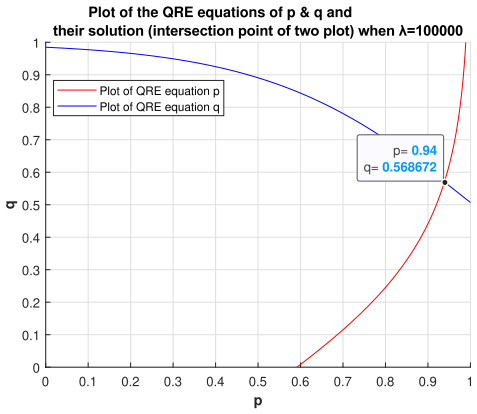
3) SOCIAL COST OF THE SYSTEM

Again, to consider a more complex setup extension of the example considered for mathematical illustration of finding QRE, we consider that both defenders have five possible strategies in Table 1 including the social optimum investment strategies. Here, the quantal response analysis yields the equilibrium approaching the social optimum solution for very high behavioral level. This QRE is given by the joint strategy of both defenders choosing X_1 investment profile. We show the social cost of all joint investment strategies in Figure 6b.

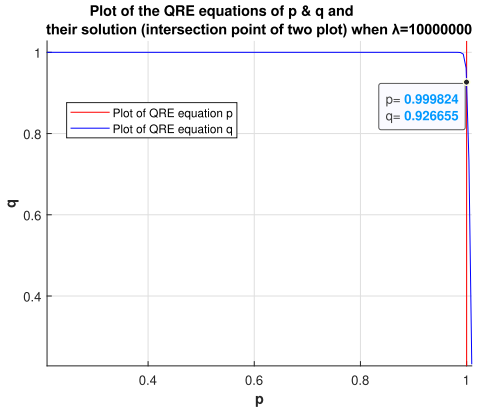
[3]Note that the five strategies outlined in Table 1 include the PNE in which defender D_1 chooses strategy X_1 and defender D_2 chooses strategy X_1. In this example, we perform the quantal analysis to study effects of behavioral level on QRE's probabilities and the relationship between QRE and PNE. Thus, we intentionally keep the PNE solution to our set of investment strategies to test whether QRE approach to PNE or not. In our experimental evaluation, we consider large set of investment strategies (see Section VII).



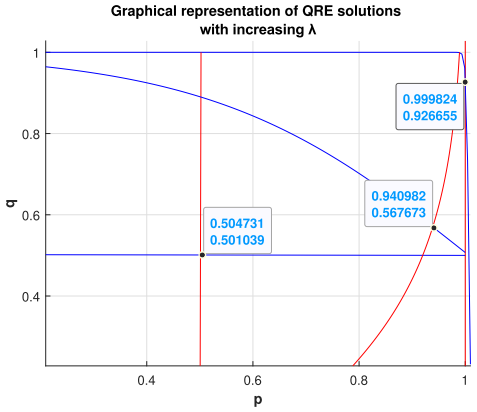
(a) Solution of p and q when $\lambda = 10$



(b) Solution of p and q when $\lambda = 100000$



(c) Solution of p and q when $\lambda = 10000000$



(d) Effect of behavioral levels on the QRE solutions

FIGURE 4. Quantal response analysis of two defenders with two investment strategies each on the attack graph of Figure 3 for our mathematical analysis illustration. We show the effect of behavioral level on the probability of choosing security investments.

It shows that the system under the social optimum (X_1, X_1) has the lowest social cost. We reemphasize that the QRE also approaches such social optimum with increasing λ for both defenders (as shown in Figure 5).

Remark 2: We emphasize that this is a special case where the social optimum is also the PNE. This is not guaranteed in our proposed interdependent security games with externalities across defenders. We show this intuition that social optimal can be different from PNE in interdependent security games in our motivational examples in Section IV. ■

IV. MOTIVATIONAL EXAMPLES

Having provided the game notations and the quantal response equilibrium, we now provide a couple of examples to evaluate the different aspects of QRE and its relationship with behavioral level, investment strategies, best response (or PNE) and socially optimal solutions.

Example 1: Consider the attack graph in Figure 7. Defender D_1 aims to defend asset v_1 and defender D_2 aims to defend asset v_2. Both defenders have unit loss for their critical assets (i.e., D_1 will have $L_1 = 1$ if asset v_1 is compromised and D_2 will have $L_2 = 1$ if asset v_2 is compromised). We consider symmetric security budget where we have $B_1 = B_2 = 10$. This attack graph is an instance of line graph

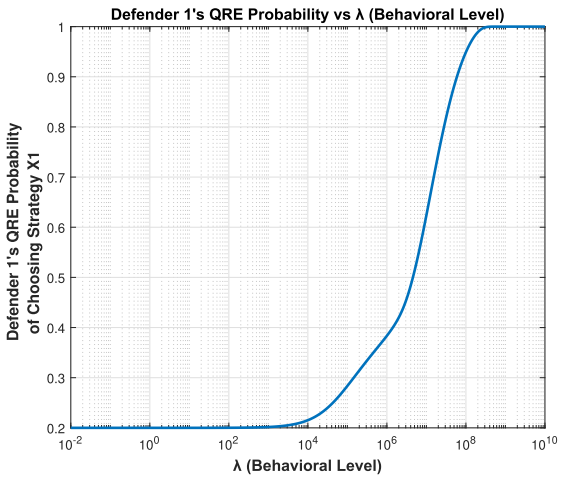
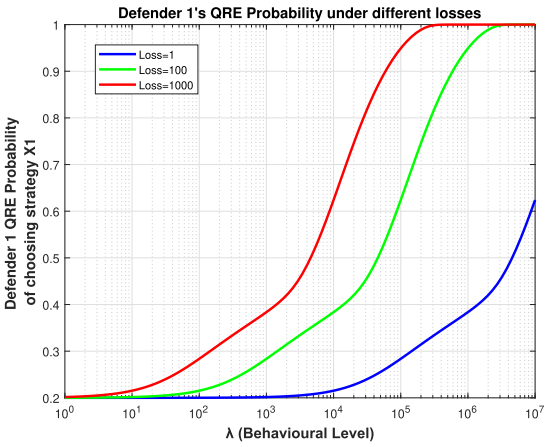
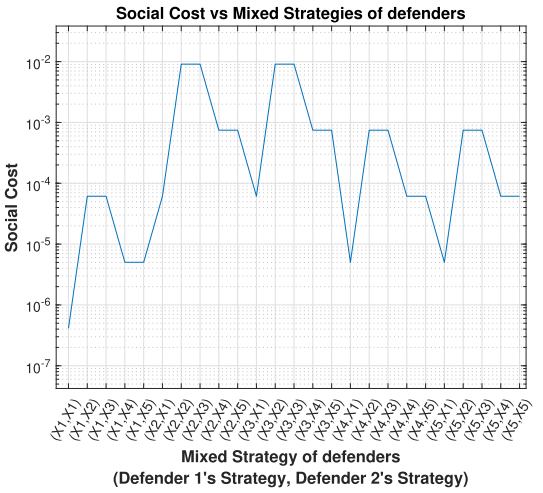


FIGURE 5. QRE probability of Defender's investment strategy with varying behavioral levels for the attack graph of Figure 3.



(a) QRE solutions under varying loss of critical asset



(b) Social Cost under defenders' mixed strategies

FIGURE 6. QRE probabilities evolution under different behavioral levels and the corresponding social costs for the interdependent security game instance considered in attack graph of Figure 3.

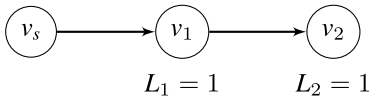
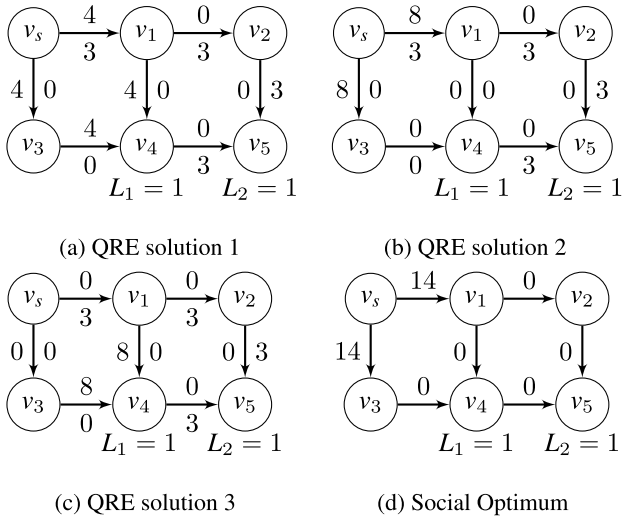


FIGURE 7. The line attack graph of interdependent security game instance considered in Example 1.

where we have only one attack path to all critical assets. Thus, defenders' budgets are allocated along this one path $(v_s - v_1 - v_2)$. Here, defender D_1 has only one strategy which is to invest all her budget on the incoming edge to her critical asset v_1, i.e., the edge (v_s, v_1). Thus, defender D_1 has only one strategy to choose from, hence the probability of choosing that strategy would be given by $p = 1$. On the other hand, defender D_2 can choose investment strategies from different possible strategies which are $(10, 0)$, $(0, 10)$, and $(x_{s,1}^2, x_{1,2}^2)$ where $x_{s,1}^2 + x_{1,2}^2 = 10$. Under joint defense strategies, defender D_2 would have expected costs of e^{-20}, e^{-20}, and e^{-20} under these three joint defense strategies, respectively.



(a) QRE solution 1 (b) QRE solution 2

(c) QRE solution 3 (d) Social Optimum

FIGURE 8. Attack graph of Example 2 with investment instances for QRE solutions ((a), (b), and (c)) and corresponding socially optimal solution ((d)). The numbers above/left and below/right of the edges represent investments by D_1 and D_2, respectively.

The probability of choosing strategy $(10, 0)$ by defender D_2 under joint defense strategy would be

$$q = \frac{\exp(-\lambda \cdot \exp(-20))}{3 \times \exp(-\lambda \cdot \exp(-20))} = \frac{1}{3}.$$

Note that for defender D_2 choosing any of the aforementioned three strategies will have the same probability of $\frac{1}{3}$. The QRE probabilities in this example do not change with respect to defenders' behavioral level. This is because in this example any one of the joint investment strategies will correspond to one PNE, i.e., defender D_2 can choose any of the three investment strategies since all of them will yield the same expected cost (as shown from identical expected cost values above). Under joint defense strategy, defender D_1 have expected costs of e^{-20}, e^{-10}, and $e^{-(10+x_{s,1}^2)}$ respectively for defender D_2's aforementioned strategies. In contrast to QRE and PNE, note here that the socially optimal solution would be unique which is given by investing all 20 defense units on the edge (v_s, v_1). Thus, one of the joint strategies (where D_1 allocates $(10, 0)$ and D_2 allocates $(10, 0)$) is a social optimum while the other two joint strategies are not since they yield higher social cost.

Example 2: Consider the attack graph of Figure 8. Defender D_1 aims to defend asset v_4, and defender D_2 wishes to defend asset v_5. For simplicity, suppose that D_1 has a budget $B_1 = 16$ and D_2 has $B_2 = 12$. Table 2 shows the top five investment strategies by each defender. Let the probability of successful attack on each edge (v_i, v_j) be given by $p_{i,j}(x_{i,j}) = e^{-x_{i,j}}$ (assuming $p_{i,j}^0 = s_{i,j} = 1$). Figure 8 shows the difference between QRE and social optimum solutions. For the QRE solution, defender D_1 chooses investment strategy X_1, X_3, X_4, and X_5 with equal probability each when λ approaches infinity. This choice arises from the fact that all of these strategies would yield the same cost for

TABLE 2. Top investment strategies for Defender D_2.

(a) Top investment strategies for defender D_1

Strategy \ Edge Investment	$x_{s,1}$	$x_{s,3}$	$x_{1,2}$	$x_{1,4}$	$x_{3,4}$	$x_{2,5}$	$x_{4,5}$
X_1	4	4	0	4	4	0	0
X_2	1	5	0	5	5	0	0
X_3	8	8	0	0	0	0	0
X_4	0	0	0	8	8	0	0
X_5	6	6	0	2	2	0	0

(b) Top investment strategies for Defender D_2

Strategy \ Edge Investment	$x_{s,1}$	$x_{s,3}$	$x_{1,2}$	$x_{1,4}$	$x_{3,4}$	$x_{2,5}$	$x_{4,5}$
X_1	0	0	4	0	0	4	4
X_2	4	0	3.14	0	0	3.14	1.72
X_3	0	0	0	0	0	6	6
X_4	3	0	3	0	0	3	3
X_5	6	6	0	0	0	0	0

D_1 at the QRE (as shown in Figure 8). This cost for defender D_1 would be given by $\max(\exp(-8), \exp(-11)) = \exp(-8)$. On the other hand, defender D_2 would choose X_4 at the QRE when λ approaches infinity. Similarly, the cost of defender D_2 would be $\exp(-11)$ under any of the four possible joint strategies.

For the social optimum, the central planner would divide all the budget (given by $B_1 + B_2$) on the minimum edge cut (edges (v_s, v_1) and (v_s, v_3)). Note that the social cost under the social optimum will be given by $e^{-14} + e^{-14}$, while the social cost under the QRE (when λ approaches infinity) will be given by $e^{-11} + e^{-8}$. We also show the evolution of QRE probabilities of defenders' investment strategies with varying behavioral level (λ) in Figure 9.

Remark 3: Our analysis in the motivational examples considered limited strategies to showcase the main insights about security resource allocation problem in interdependent systems with multiple defenders and the effect of behavioral level on this problem and arising defender's costs. However, our theoretical analysis and experimental evaluation (in the next two sections) consider many investment strategies. ■

V. MEASURING INEFFICIENCY OF QRE: THE PRICE OF QUANTAL RESPONSE

The notion of Price of Anarchy (PoA) is commonly utilized to assess the inefficiencies of a Nash equilibrium when compared to the socially optimal outcome [35]. More precisely, the Price of Anarchy is the measure of the highest total system cost at a Pure Nash Equilibrium (PNE) relative to the total system cost at the socially optimal state.

In our specific context, we aim to establish a metric that accounts for inefficiencies in the equilibrium resulting from the individual strategic behaviors of defenders and their behavioral decision-making characterized by quantal errors. Therefore, we introduce the concept of Price of Quantal Anarchy (PoQA), which quantifies the ratio of the total true expected cost of the system when considering defenders' behavioral choices at the quantal response equilibrium (QRE) in comparison to the total true expected cost at the

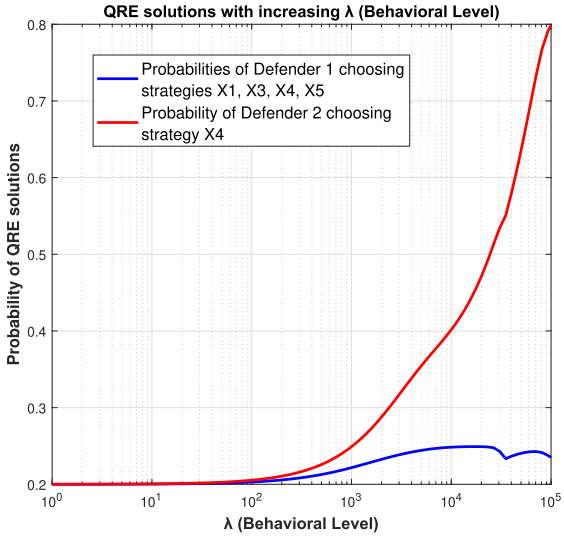


FIGURE 9. QRE probabilities of defenders' investment strategies with varying behavioral levels for Example 2.

socially optimal solution, determined by a non-behavioral (or rational) social planner.

Specifically, we define $C(\mathbf{x}) \triangleq \sum_{D_k \in \mathcal{D}} C_k(\mathbf{x})$, where C_k (defined in (2)) is the true expected cost faced by defender D_k under the investment vector $\mathbf{x}$. Let X_k^{QRE} denotes the set of all investments that constitute a QRE for defender D_k. We now define the Price of Quantal Anarchy as

$$PoQA = \frac{\sum_{D_k \in \mathcal{D}} \left(\sum_{\mathbf{x}_l \in X_k^{\text{QRE}}} \sigma_{kl} \times EC_{kl}(\sigma_{-k}) \right)}{C(\mathbf{x}^*)}, \quad (7)$$

where each expected cost $EC_{kl}(\sigma_{-k})$ in the numerator for a defender $D_k \in \mathcal{D}$ under investment profile $\mathbf{x}_l$ is weighted with the probability of choosing that investment vector by defender D_k in the QRE (given by σ_{kl}). Furthermore, $\mathbf{x}^*$ denotes the investments at the social optimum (computed by a non-behavioral social planner with access to the sum of all defenders' budgets). Mathematically, let $X^{\text{Soc}} := \{\mathbf{x}^* \in \mathbb{R}_{\geq 0}^{|\mathcal{D}||\mathcal{E}|} | \mathbf{1}^T \mathbf{x}^* \leq \sum_{D_k \in \mathcal{D}} B_k\}$, i.e., X^{Soc} is the set of all feasible investments by the social planner. Thus, the social optimal would be given by

$$\mathbf{x}^* \in \underset{\mathbf{x} \in X^{\text{Soc}}}{\operatorname{argmin}} C(\mathbf{x}). \quad (8)$$

In our evaluation, we also refer to the PoQA as the "inefficiency" of the QRE. We emphasize that the cost in the denominator of (7) is the sum of the expected costs of the defenders under social optimum.

A. BOUNDS ON THE POQA

We now establish upper and lower bounds on the PoQA. We first show that the PoQA is bounded if the total budget is bounded (regardless of the defenders' behavioral levels).

Proposition 2: Suppose the total budget available to all defenders is denoted as B, and the probability of a successful

attack on each edge $(v_i, v_j) \in \mathcal{E}$ *is determined by* $p_{i,j}(x_{i,j}) = e^{-x_{i,j}}$. *Thus, for any given attack graph and any set of quantal behavioral levels* λ_k, *it holds that* $PoQA \leq \exp(B)$.

Proof: We start with the numerator of the PoQA in (7) (the total true expected cost at the QRE). Recall that each defender D_k incurs a financial loss L_m for each successfully compromised asset v_m. Thus, the worst case true expected cost under any QRE is upper bounded by $\sum_{D_k \in \mathcal{D}} \sum_{v_m \in V_k} L_m$ (i.e., the sum of financial losses of all assets).

On the other hand, the denominator (the social optimum true expected cost) is lower bounded by $\left(\sum_{D_k \in \mathcal{D}} \sum_{v_m \in V_k} L_m \right) \exp(-B)$ (which can only be achieved if every asset has all of the budget B, invested by a social planner, on the edges constituting its attack path). Thus, we have

$$C(\mathbf{x}^*) \geq \left(\sum_{D_k \in \mathcal{D}} \sum_{v_m \in V_k} L_m \right) \exp(-B).$$

Substituting these bounds into (7), we obtain $PoQA \leq \exp(B)$. This concludes the proof. ∎

Next, we show that the upper bound on PoQA obtained in Proposition 2 is asymptotically tight.

Proposition 3: For all $B > 0$ *and* $\epsilon > 0$, *there exists an instance of the interdependent Security Game with total budget* B *such that the PoQA is lower bounded by* $(1 - \epsilon)\exp(B)$.

Proof: Consider the attack graph in Figure 10, where the probability of a successful attack on each edge (v_i, v_j) is given by (1) with $p^0_{i,j} = 1$. This graph contains K defenders, and each defender D_k is responsible for defending target node v_k. Assume the total security budget B is divided equally between the K players (i.e., each player has security budget $\frac{B}{K}$). Let the first node have loss equal to $L_1 = K$, and the other $K - 1$ nodes have loss $\frac{1}{K-1}$. Then, the socially optimal solution would put all the budget B on the first edge (v_s, v_1), so that all nodes have the probability of successful attack given by $\exp(-B)$. Thus, the denominator of (7) is $\sum_{i=1}^{K} L_i \exp(-B) = (K + 1)\exp(-B)$.

We now characterize a lower bound on the cost under a PNE (i.e., the numerator of (7) with very high λ). Specifically, consider the investment profile where each defender D_k puts their entire budget $\frac{B}{K}$ on the edge coming into their node v_k. We claim that this is a PNE. To show this, first consider defender D_1. Since investments on edges other than (v_s, v_1) do not affect the probability of successful attack at node v_1, it is optimal for defender D_1 to put all her investment on (v_s, v_1).

Now consider defender D_2. Given D_1's investment on (v_s, v_1), defender D_2 has to decide how to optimally spread her budget of $\frac{B}{K}$ over the two edges (v_s, v_1) and (v_1, v_2) in order to minimize her cost function (2). Thus, D_2's optimization problem, given D_1's investment, is

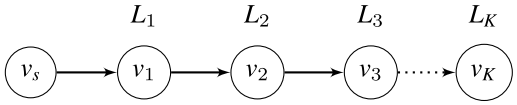


FIGURE 10. An attack graph where the PoQA grows exponentially in the sum of defenders' security budgets.

$$\underset{x^2_{s,1}+x^2_{1,2}=\frac{B}{K}}{\text{minimize}}\ e^{-\left(\frac{B}{K}+x^2_{s,1}-x^2_{1,2}\right)}. \tag{9}$$

One optimal solution of (9) would be to put all $\frac{B}{K}$ into $x^2_{1,2}$ and zero on $x^2_{s,1}$. Continuing this analysis, we see that if defenders $D_1, D_2, \ldots, D_{k-1}$ have each invested $\frac{B}{K}$ on the edges incoming into their nodes, it is optimal for defender D_k to also invest their entire budget $\frac{B}{K}$ on the incoming edge to v_k. Thus, investing $\frac{B}{K}$ on each edge is a PNE.

The numerator of the PoQA under this PNE (which is QRE with very high λ) is lower bounded by $L_1 \exp\left(-\frac{B}{K}\right) = K \exp\left(-\frac{B}{K}\right)$. Thus, PoQA is lower bounded by

$$PoQA \geq \frac{K \exp\left(-\frac{B}{K}\right)}{(K+1)\exp(-B)} = \frac{K \exp\left(-\frac{B}{K}\right)}{(K+1)} \exp(B).$$

As the length of the chain in Figure 10 grows, we have

$$\lim_{K \to \infty} \frac{K \exp\left(-\frac{B}{K}\right)}{(K+1)} = 1.$$

Thus, for every $\epsilon > 0$, there exists K large enough such that the PoQA in the line graph with K nodes is lower bounded by $(1 - \epsilon)\exp(B)$. ∎

We emphasize that the upper bound established in Proposition 2 remains independent of the interdependent system's network configuration, the count of defenders, and their level of quantal behavioral level. In Proposition 3, we demonstrate that the upper bound determined in Proposition 2 is precise, meaning it cannot be diminished unless further game-specific conditions are considered. However, for each specific interdependent security game instance, we can directly calculate the degree of inefficiency, which will be contingent on the system's structure and other pertinent parameters specific to that instance (as will be shown in our evaluation in Section VII).

Having established the existence of QRE in our interdependent security game and provided mathematical bounds on the inefficiency under the existence of behavioral defenders (with quantal errors), we next show our pruning algorithm for finding QRE under many security investment strategies in our interdependent security game.

VI. FINDING QRE UNDER MANY SECURITY INVESTMENT STRATEGIES IN INTERDEPENDENT SECURITY GAMES

We now provide the details of our algorithm that aims at pruning investment strategies and select the most efficient ones for calculating QRE for interdependent systems with multiple defenders. Recall that any defender $D_k \in \mathcal{D}$ can allocate her security budget B_k in numerous ways via

spreading that budget on the edges incoming to her critical assets $\forall v_m \in V_k$.

In Algorithm 1, we prune these many investment strategies to elect the most promising ones (i.e., that yield lowest social costs for the interdependent system). The main inputs for our algorithm are security budgets of the defenders ($B_k \; \forall D_k \in \mathcal{D}$), all attack paths associated with critical assets for defender ($\mathcal{P}_m \; \forall v_m \in V_k$), and loss vectors that have the estimated financial losses when successfully compromising these assets. Our goal is to find a set of security investment strategies which have lowest social costs under the notion that the attacker exploits the most vulnerable path for each critical asset. To do this, we first create a large defense strategy space X_k for each defender $D_k \in \mathcal{D}$ which contains many investment strategies where the budget B_k is first allocated on only one edge, then splitting the budget equally in an incremental manner across the edges up to all edges of the attack paths. After getting this large strategy space, we create a joint defense strategy space considering all the possible combinations of investment strategies from previous step.

We then calculate the expected cost for each defender $D_k \in \mathcal{D}$ using equation (2) under these joint defense investments. After calculating individual costs in previous step, we then calculate social costs by summing expected costs of all defenders. We next sort these social costs in an ascending order. While pruning our strategies, we only keep strategies with unique total costs. In other words, if we have many investment strategies with the same social cost, we take only one strategy from these equivalent strategies and prune the other equivalent strategies (with identical social cost). This is intuitive since these joint investment strategies with the same social cost are equivalent joint investment strategies to each other from the perspective of securing the whole interdependent system.

From that sorted unique joint strategies, we start selecting the top-N security investment strategies that have the lowest social costs and end this process when we get our desired N investment strategies. Finally, we compute QRE via applying quantal response function in (4) on the selected top-N investment strategies from our algorithm.

Algorithm 1 Strategy Pruning and QRE Calculation for Interdependent Systems With Multiple Defenders

Input: Security budget $B_k \; \forall D_k \in \mathcal{D}$, Set of attack paths $\mathcal{P}_m \; \forall v_m \in V_k$, Loss vector of critical assets $\mathbf{L}$, Num. of top investment strategies N

Output: Top-N joint investment strategies and corresponding QRE probabilities

1) For each defender $D_k \in \mathcal{D}$, create an investment strategy space X_k for defender D_k by spreading her budget B_k across edges of the attack paths in $\mathcal{P}_m$.
2) Compute joint investment strategies $(\mathbf{x}_k, \mathbf{x}_{-k})$ of defenders using all combinations of investment strategies for each defender $D_k \in \mathcal{D}$ from step 1.
3) Create a cost vector for each defender D_k by calculating expected costs $C_k(\mathbf{x}_k, \mathbf{x}_{-k})$ for all joint investment strategies using equation (2), $\mathcal{P}_m$, and $\mathbf{L}$.
4) Calculate system's social costs by summing expected costs of defenders for each joint defense strategy.
5) Sort social costs from step 4 in ascending order.
6) Keep joint strategies with unique social costs and prune equivalent joint investment strategies.
7) Select top-N unique joint investment strategies from step 6 that have the best (lowest) social costs.
8) Compute QRE using quantal response function in equation (4) for the top-N joint investment strategies.

return Top-N investments and their QRE probabilities

VII. EVALUATION

We now evaluate our setup with a realistic interdependent system. Our evaluation aims to answer the following questions:

- What is the effect of behavioral players (with quantal errors) on the overall security level of the system?
- How to quantify the degree of inefficiency under behavioral decision-makers compared to socially optimal security investments?
- How does each system parameter affect the overall security level of the system (social cost) with behavioral decision-making?

A. DATASET DESCRIPTION

We use a real-world interdependent system to evaluate our setups. Specifically, we consider the popular interdependent system of DER.1 [25]. In this system, nodes represent the progression of attack steps (e.g., unauthorized control of a physical generator in DER.1).

We give a brief explanation of this system and its associated failure scenarios below. We leverage the CyberSage tool [25] which maps system's failure scenarios into an attack graph given the workflow of that system, security goals, and attacker's model.

DER.1 System Description: The Technical Working Group of the US National Electric Sector Cybersecurity Organization Resource (NESCOR) has introduced a framework aimed at assessing the cybersecurity risks associated with potential cyber attacks on the electric grid. Within this framework, a distributed energy resource (DER) is defined as a cyber-physical system composed of various entities, including generators, storage devices, and electric vehicles, all integrated into the smart energy distribution system. Among the identified failure scenarios, DER.1 has been identified as the most precarious, according to NESCOR's ranking [25].

In Figure 1, two pivotal equipment assets are highlighted: a PhotoVoltaic (PV) generator and an electric vehicle (EV) charging station. Each piece of equipment is equipped with

TABLE 3. Best 10 (top-10) security investment strategies for defender D_1 for the attack graph of DER system in Figure 1.

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

a Human Machine Interface (HMI), serving as the sole gateway for controlling the respective equipment. The DER.1 failure scenario unfolds when an attacker gains access to the HMI. Subsequently, the attacker manipulates the DER settings and physically accesses the DER equipment to ensure continued power provision even during a power system fault. This malicious action has the potential to inflict severe physical damage on the system, leading to significant financial losses. On the worst scenario, such attack can result in the electrocution of a utility field crew member.

B. EXPERIMENTAL SETUP

The simulations are based on our proposed game-theoretic models in Section II and quantal response models in Section III with the following parameters. The DER system has two defenders. For DER, we have the financial losses $L_i = L = \$10, \forall i$ for the critical assets (G_0 for defender D_1 and G_1 for defender D_2).

We used the probability of successful attack function in (1) in our simulations. We consider baseline probabilities of successful attack on edges (i.e., without any security investment) to be the same to avoid its bias on the simulation results.[4] We consider a range of the behavioral level λ such that $\lambda \in [1, \infty)$, which is consistent with prior human subject experimental studies on quantal responses [21], [22]. We consider symmetric behavioral level (λ) for both defenders. We consider a symmetric security budget across the defenders (unless otherwise stated). Each defender has a security budget of 15. For Quantal Response Equilibrium (QRE), we run the quantal response dynamics to calculate the QRE while the social optimal is found using equation (8) defined in Section V. To compute the PNE for comparisons, we followed the best response dynamics notion to calculate the optimal investments of each player at the PNE.

C. EVALUATION RESULTS

We now summarize the main findings of our evaluation.

[4]Our model can also support different baseline probabilities of successful attack on different edges. To estimate these baseline probabilities on each edge, we can create a table of CVE-IDs (from real vulnerabilities reported in the CVE database for 2000-2020). We can then follow [34] to convert the main attack's metrics to a baseline probability of successful attack.

1) PRUNING OF INVESTMENTS

In the DER experimental setup, we started with choosing randomly 120 investment strategies for each defender. We then perform pruning to get the top-10 unique investment strategies (according to Algorithm 1). Recall that this pruning is done according to the lowest social cost under considering both defenders' combined investments (joint investments). We observe that the social cost is lowest when both defenders invest all of their budgets only on the min-cut (common) edges (i.e., edges that are common on all attack paths). For the DER system, these edges are (w_5, w_4), (w_4, w_3), (w_3, w_2), (w_2, w_1), and (w_1, G_0) for defender D_1. Similarly, the min-cut edges for defender D_2 are (w_{14}, w_{13}), (w_{13}, w_{12}), (w_{12}, w_{11}), (w_{11}, w_{10}), and (w_{10}, G_1).

2) QRE ANALYSIS AND EFFECT OF BEHAVIORAL LEVEL

We then perform the QRE analysis with these top-10 investment strategies (shown in Table 3). Our QRE analysis shows that rational defenders (with very high λ) get quantal response equilibrium approaching best response solution (PNE). Figure 11 shows the evolution of QRE towards best strategy under different quantal behavioral levels. This also validates our findings in our aforementioned mathematical analysis (in Section III) and both motivational examples.

3) EFFECT OF FINANCIAL LOSS OF CRITICAL ASSETS

We then vary the financial loss of the critical assets (G_0 and G_1 for defenders D_1 and D_2, respectively). We consider three loss levels to test the effect of loss on the QRE solution under different behavioral levels. Figure 12 shows this experiment where it shows that when facing higher losses behavioral defenders would have a higher probability of choosing the best investment strategy (X_1) under the same behavioral level (λ). The intuition here is that the difference in the expected cost of best investment strategy and other strategies is higher under higher financial losses and thus the quantal behavioral error will have lower effect in these cases with higher losses, particularly for more rational players (with higher λ).

4) INEFFICIENCY OF BEHAVIORAL PLAYERS

We now measure the inefficiency due to behavioral players with quantal errors by measuring PoQA from (7). Figure 13

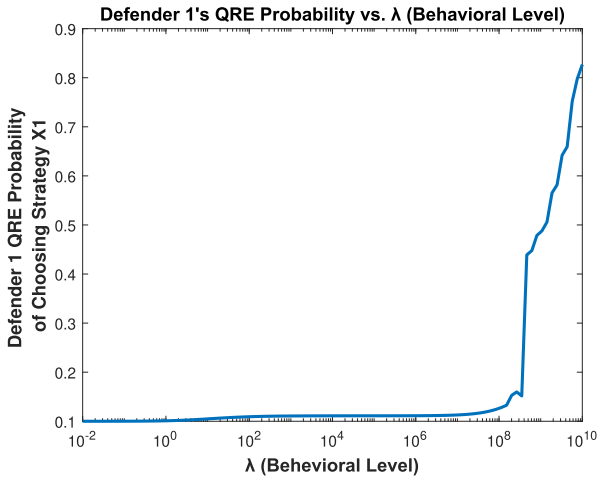


FIGURE 11. QRE probability of defender's investment strategy with varying behavioral levels for the DER system.

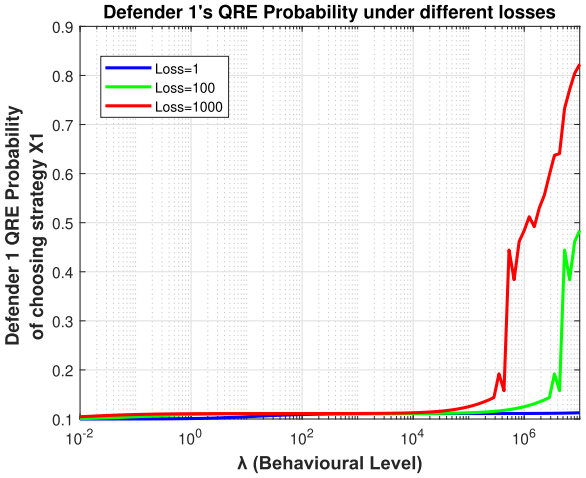


FIGURE 12. The probability of best investment strategy at QRE of DER system under varying the financial loss of critical asset.

shows the logarithm of the value of this metric as we vary λ (taken to be the same for both defenders) from 1 (highly behavioral) to 1000 (low-behavioral) for different values of the total security budget B. Figure 13 shows that the inefficiency due to behavioral decision-making becomes exacerbated as the total budget B increases (which is consistent with our finding in Proposition 2). For example, the difference between the PoQA with highly behavioral defenders ($\lambda = 1$) and that with low behavioral defenders ($\lambda = 1000$) under higher security budget ($B = 25$) is much higher compared to that difference under lower budget ($B = 10$). The reason for such increase in inefficiency is two-fold. First, selfish defenders do not invest security resources on edges of other defenders. Second, as security budget increases, behavioral defenders shift higher amounts of their budget to the non-common (non-critical) edges in the DER network in contrast to the social optimal that has all the budget only on the min-cut edges.

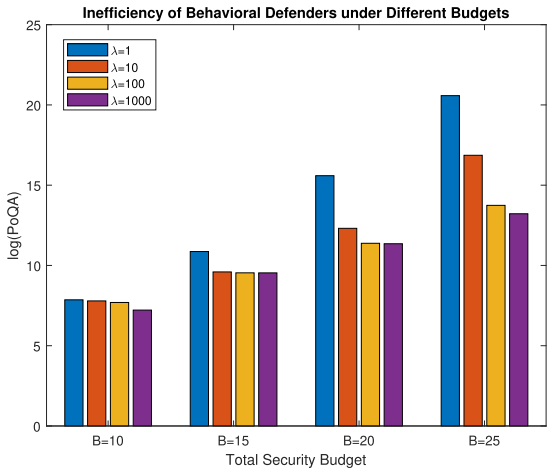


FIGURE 13. The inefficiency (PoQA) of behavioral defenders with different behavioral levels and different security budgets. For better readability, we show the logarithm of inefficiency.

5) SOCIAL COSTS

Figure 14 demonstrates the heatmap of social cost (which is the sum of the costs of the two defenders) under the top-10 unique security investment strategies. It shows that the PNE (defender D_1 allocating all her defense budget on the incoming edge (w_1, G_0) to her critical asset G_0 and defender D_2 allocating all her defense budget on the incoming edge (w_{10}, G_1) to her critical asset G_1) has the lowest social cost across these different joint investment strategies (on the lower left corner of the heatmap). Note that this PNE is the QRE at very high behavioral level λ. This is shown by the darkest blue-colored square in this heat map. On the other hand, distributing the budget between common edges (that belong to all attack paths to critical assets) and non-common edges (that belongs to few attack paths) yield worse social cost. This is shown by the light blue-colored squares in this heat map. Finally, allocating all investments on non-common edges and leaving common edges with zero investments would lead to the highest social cost (shown with orange- and red-colored squares in the heatmap).

Numerically, we see that the gain for society (represented by the ratio of the social cost under worst joint investment strategy here (X_5, X_5) to the social cost under the PNE (X_1, X_1)) is 1.0526 exp(13) for DER. This result shows that the social cost under optimal security allocations is much lower than that under non-optimal allocations and the gap is higher for highly behavioral defenders (that have different QRE from PNE and allocate more investments on non-important edges).

6) COMPUTATIONAL EFFICIENCY OF QRE

We finally show the required computational time to compute QRE in Figure 15 under our two setups which are: with strategy-pruning (Algorithm 1), and without strategy pruning. Although both scenarios achieve PNE under rational decision-making (high λ), the strategy-pruning has 33.85X

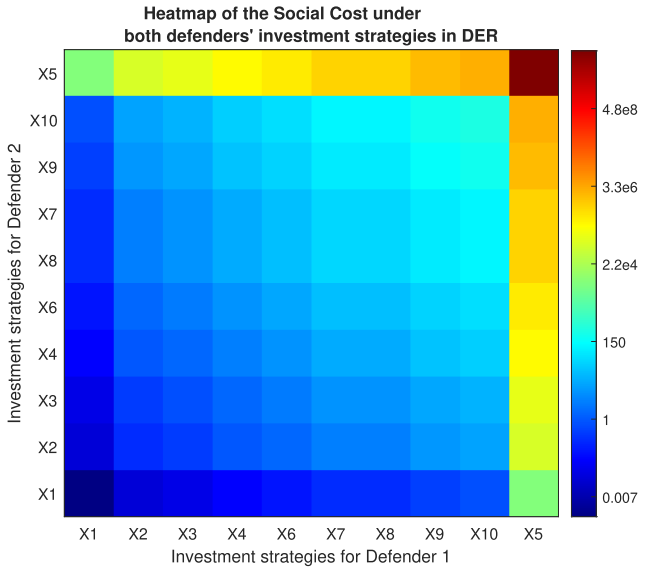


FIGURE 14. The heat map of social costs for the DER system under the top-10 unique security investment strategies.

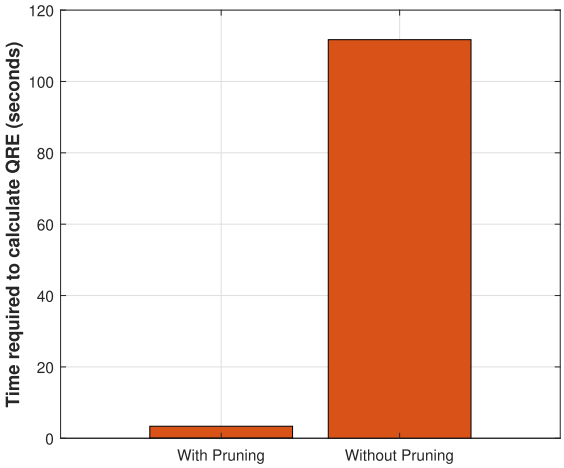


FIGURE 15. A comparison of the required time (seconds) to compute the QRE with strategy-pruning vs. without pruning.

reduction in QRE computation time. which shows the potential application of the proposed framewok for large-scale systems.

In sum, our evaluation results show the importance of understanding human behavioral error (quantal error) and its effect on security level of the interdependent system. The evaluation also shows the importance of quantifying the effect of different resource allocations when doing risk assessment of interdependent systems.

VIII. RELATED WORK

A. GAME-THEORETIC MODELING OF SECURITY

Game theory has found application in describing the interactions between attackers and defenders and their impact on system security. A prevalent model in this context involves two-player games, where a single attacker seeks to compromise a system controlled by a single defender [42], [43]. In some instances, game-theoretic models have been extended to explore the dynamics between a defender and one or more attackers engaged in Distributed Denial of Service (DDoS) attacks, as evidenced in [44]. Additionally, game-theoretic frameworks have been proposed for investigating the security of critical infrastructure, as discussed in the survey [11]. What sets our work apart from the aforementioned literature is our focus on behavioral decision-making models. Unlike most existing research, which primarily revolves around classical game-theoretic models of rational decision-making, we analyze models that account for the behavioral aspects of decision-making (particularly on the noisy decisions of human decision-makers, modeled using the logit QRE for interdependent security games).

B. SECURITY GAMES ON INTERDEPENDENT SYSTEMS

A large body of literature has been developed to explore security decision-making in interdependent systems (see [11], [45] for a review), including single defender for network security [44], [46], [47], [48], and multiple defenders in specific interdependent security games [10], [12], [49], [50] and critical infrastructure security [51], [52]. However, these works have been proposed under the common assumption that the players are entirely rational and optimal decision-makers. The impact of human prospect-theoretic attitudes has been studied in several classes of interdependent security games, including drone delivery systems [14], unmanned aerial vehicle assisted network operation [16], and in prior work on network defense [17] and mechanism-based games [18].

However, these investigations have several limitations, including choosing a specific game where each defender has ownership of a single asset, modeling each player via a binary strategy in which she either defends her asset or not, and not considering different interdependent attack paths among different defenders using attack graphs.

C. QUANTAL RESPONSE EQUILIBRIUM

The majority of prior works in security resource allocation for interdependent systems have considered the pure strategy Nash equilibrium (PNE) solution concept in which the search strategy for the best resource allocation for each decision-maker adopts best response dynamics [18], [48], [49], [51]. However, behavioral economics and psychology has shown that humans have errors in choosing which pure strategy to select in real-world scenarios [21], [22], [23]. Such a process can be modeled using quantal functions (such as the logit function [22]) where the human chooses each strategy with a probability that is positively related to the payoff from that strategy. This process typically leads to quantal response equilibrium. There are several prior works that have shown such quantal response equilibrium for security problems, including defense of isolated targets [28], and Stackelberg security games with two players (one attacker

and one defender) [29], [30], [31], [32], [33]. However, this class of games does not incorporate security externalities between multiple defenders and network interdependencies.

D. HUMAN BEHAVIOR IN SECURITY AND PRIVACY

A noticeable departure from traditional economic models in the realm of security and privacy is exemplified by [26], which delves into the impact of behavioral decision-making on an individual's choices concerning personal privacy. Recognizing the significance of similar models in the domain of system security, prior research [53] has highlighted the importance of such considerations. Some previous works have explored models derived from behavioral economics within the context of security applications [27], [54]. It is worth noting that these studies relied primarily on insights from psychological studies [27] and human subject experiments [54], primarily focused on end-users.

Our approach is distinguished from these prior works in several ways. We employ a rigorous mathematical model to analyze the quantal behavior of defenders. Additionally, we model the interactions among multiple defenders, as opposed to the singular defender in these previous studies. Furthermore, we consider interdependent assets, in contrast to binary decisions related to isolated assets, as seen in those studies. To the best of our knowledge, notable exceptions to the existing body of literature that provide a theoretical treatment of behavioral decision-making in specific classes of interdependent security games are [8], [13], [14], and [55]. However, it is important to note that these studies do not encompass the broader spectrum of realistic attack scenarios and types that our work explores. Moreover, they do not examine the quantal response behavior exhibited by defenders, which is a focal point of our research. Instead, their focus is on prospect-theoretic behavior of defenders.

IX. LIMITATIONS AND DISCUSSION

A. ESTIMATION OF BASELINE PROBABILITIES OF SUCCESSFUL ATTACK

One challenging issue with any security resource allocation framework is the estimation of the attack success probabilities. In our setup, the initial probabilities of successful attack on the edges of the attack graph can be estimated via the Common Vulnerability Scoring System (CVSS) scores [36], that measure how a vulnerability (that corresponds to a CVE entry [56]) is exploited (successfully attacked). This CVE entry is composed of the following three access metrics:

- Access Vector (AV), which measures whether or not the vulnerability is exploited locally or remotely.
- Access Complexity (AC), which measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system.
- Authentication (AU), which measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability successfully.

TABLE 4. Baseline probability of successful attack for vulnerabilities in DER.1 system.

Vulnerability (CVE-ID)	Edge(s)	Attack Vector	Score
DER.1 application			
Physical access (CVE-2017-10125)	(w_9, w_7),(w_{18}, w_{16})	Physical	0.71
Network access (CVE-2019-2413)	(w_9, w_8),(w_{18}, w_{17})	Network	0.61
Software access (CVE-2018-2791)	(w_7, w_6),(w_8, w_6)	Network	0.82
Sending cmd (CVE-2018-1000093)	(w_6, w_5),(w_{15}, w_{14})	Network	0.88

There are multiple previous works [34], [37] that have provided clearly defined mathematical models that can be used to convert CVSS metrics to initial probability of successful attack. Specifically, the work [34] has taken the Access Complexity (AC) sub-metric in CVSS and mapped it to a probability of exploit (attack) success. The AC metric takes values in {low, medium, high} indicating the complexity of exploiting the vulnerability. For instance, the authors used the mapping $\{low \longrightarrow 0.9, medium \longrightarrow 0.6, high \longrightarrow 0.2\}$. Note that the more complex it is to exploit a vulnerability, the less likely an attacker will succeed. Moreover, the work in [37] has estimated the probability of successful attack from CVSS as a combination of the three defined metrics (i.e., Access Complexity (AC), Attack vector (AV), and Authentication (AU)) as follows, $p^0_{i,j} = AV_{i,j} \times AU_{i,j} \times AC_{i,j}$ (we refer to tables in [37] which contain numerical values corresponding to the different values of each metric).

In our setting, based on our adversary model (where the attacker picks the path with the highest probability of success), the probability of a node v_m being successfully attacked (i.e., its vulnerability) is given by $\max_{P \in \mathcal{P}_m} \prod_{(v_i,v_j)\in P} p_{i,j}(x_{i,j})$ (the highest probability of attack among all paths available for attack).

Estimation of Baseline Probabilities of Successful Attack Example for DER: We show the estimation of baseline probability of successful attack for DER system in Table 4. The first column represents the vulnerability CVE-ID (from real-world vulnerabilities reported in CVE database). The second column represents the corresponding edge(s) in the attack graph. The third column represents the attack vector type (physical, local, or network). The fourth column is the score generated following the seminal work [34].

B. QUANTAL RESPONSE OF ATTACKER

Throughout this paper, we operate under the assumption that defenders have quantal errors in choosing the best security investment strategies for interdependent security game proposed in our work. To give complete treatment of such an effect on defense, we assumed that the attacker is non-behavioral (rational). This also gives worst case estimate of security level of the system under human errors. However, it is essential to acknowledge that attackers can exhibit behavioral traits as well. Our assumption of a non-behavioral attacker is made to assess the worst-case scenario for system

vulnerability since a behavioral attacker might not always choose attack paths of true highest vulnerability due to quantal errors. By focusing on the behavioral aspect of the defenders, we aim to unravel the effects of quantal errors. This prompts an intriguing question: ''How can rational defenders manipulate a behavioral attacker with quantal errors into selecting attack paths with reduced likelihood of success to enhance the overall security of the target system?''

C. QUANTAL RESPONSE FOR DIFFERENT CLASSES OF SECURITY GAMES

In this paper, we have explored the quantal response analysis for security decision-making by behavioral defenders of interdependent security systems using attack graphs. One potential area to expand our quantal response analysis model is by determining equilibrium in other types of security games. In particular, characterizing defense resource allocation in other classes of security games, such as sequential attacker-defender games, could be a potential extension. Also, the real-world interactions between the attackers and defenders in simultaneous strategic games can be explored using the proposed QRE model. While previous works have addressed security issues in these classes of security games using either classical models [13], [14], [15], [16], [17], [18] or prospect-theoretic behavioral biases [16], [17], [18], quantal response analysis can enhance the network security by considering quantal errors and uncertainties of players in various types of security games, quantifying the arising security level of interdependent systems under such quantal errors, and guiding decision-makers towards avoiding such noisy and non-optimal decisions.

X. CONCLUSION

We presented a *security investment* model for defenders of interdependent systems where defenders' assets have mutual interdependencies. We modeled stepping-stone attacks by the notion of *attack graphs*. The proposed security game model captures the existence of behavioral players that have quantal behavior (where they have errors in choosing the best investment strategies). We showed that such a game has a quantal response equilibrium (QRE). We then adapted the price of anarchy and introduced a new metric that we called price of quantal anarchy (PoQA) to measure the inefficiency arising from the existence of behavioral players with quantal errors on the social cost of the interdependent system. We provided rigorous bounds for such inefficiency metric. We then developed an algorithm to compute the QRE under many security investment strategies by pruning non-efficient strategies based on the social cost of the system. This algorithm is particularly useful for large-scale systems with many possible security investment strategies. We then evaluated the effects of *behavioral* quantal errors of human decision-makers on overall system's security through a real-world interdependent system and identified different system parameters that affect the overall system's security for our security game model. The insights gained from this analysis are useful for configuring real-world systems with optimal parameter choices and guiding behavioral decision-makers toward socially optimal allocations and rational decision-making that can eventually lead to improvements in interdependent systems' security.

There are multiple prospective avenues for future research, including studying heterogeneous types of behavioral players and their resulting impacts, exploring environments in which adversaries have also quantal behavior, and evaluating our findings empirically via human subject experiments.

Building on our current study, these fruitful directions of future research can help in mitigating the effects of behavioral decision-makers in real-world systems.

REFERENCES

[1] I. Week. (Jan. 2021). *The 10 Biggest Cyber Security Attacks of 2020*. Accessed: Oct. 1, 2023. [Online]. Available: https://searchsecurity.techtarget.com/news/252494362/10-of-the-biggest-newlinecyber-attacks

[2] J. Robertson and W. Turton. (2021). *Colonial Pipeline Ransomware Attack*. Accessed: Oct. 30, 2023. [Online]. Available: https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-newlinestole-data-thursday-ahead-of-pipeline-shutdown

[3] A. Humayed, J. Lin, F. Li, and B. Luo, ''Cyber-physical systems security—A survey,'' *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[4] J. Ding, Y. Atif, S. F. Andler, B. Lindström, and M. Jeusfeld, ''CPS-based threat modeling for critical infrastructure protection,'' *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 45, no. 2, pp. 129–132, Oct. 2017.

[5] A. B. Sharma, F. Ivančić, A. Niculescu-Mizil, H. Chen, and G. Jiang, ''Modeling and analytics for cyber-physical systems in the age of big data,'' *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 41, no. 4, pp. 74–77, Apr. 2014.

[6] NREL. (2021). *Cybersecurity Threat Evaluation on Renewable Energy Systems*. Accessed: Feb. 1, 2022. [Online]. Available: https://www.nrel.gov/news/program/2021/nrel-joins-industry-in-leading-cybersecurity-threat-evaluation-for-us-wind-fleet.html

[7] E. Koutsoupias and C. Papadimitriou, ''Worst-case equilibria,'' *Comput. Sci. Rev.*, vol. 3, no. 2, pp. 65–69, May 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013709000203

[8] M. Abdallah, P. Naghizadeh, A. R. Hota, T. Cason, S. Bagchi, and S. Sundaram, ''Behavioral and game-theoretic security investments in interdependent systems modeled by attack graphs,'' *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 4, pp. 1585–1596, Dec. 2020.

[9] L. A. Gordon and M. P. Loeb, ''The economics of information security investment,'' *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.

[10] D. Shishika and V. Kumar, ''A review of multi agent perimeter defense games,'' in *Proc. Int. Conf. Decis. Game Theory Secur.* Cham, Switzerland: Springer, 2020, pp. 472–485.

[11] A. Laszka, M. Felegyhazi, and L. Buttyan, ''A survey of interdependent information security games,'' *ACM Comput. Surv.*, vol. 47, no. 2, pp. 1–38, Jan. 2015.

[12] T. Alpcan and T. Baar, *Network Security: A Decision and Game-Theoretic Approach*, 1st ed. New York, NY, USA: Cambridge Univ. Press, 2010.

[13] A. R. Hota and S. Sundaram, ''Interdependent security games on networks under behavioral probability weighting,'' *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 262–273, Mar. 2018.

[14] A. Sanjab, W. Saad, and T. Basar, ''Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[15] M. Abdallah, D. Woods, P. Naghizadeh, I. Khalil, T. Cason, S. Sundaram, and S. Bagchi, ''Morshed: Guiding behavioral decision-makers towards better security investment in interdependent systems,'' in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, May 2021, pp. 378–392.

[16] P. Vamvakas, E. E. Tsiropoulou, and S. Papavassiliou, ''Exploiting prospect theory and risk-awareness to protect UAV-assisted network operation,'' *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–20, Dec. 2019.

[17] D. Woods, M. Abdallah, S. Bagchi, S. Sundaram, and T. Cason, "Network defense and behavioral biases: An experimental study," *Experim. Econ.*, vol. 25, no. 1, pp. 254–286, Feb. 2022.
[18] M. Abdallah, D. Woods, P. Naghizadeh, I. Khalil, T. Cason, S. Sundaram, and S. Bagchi, "TASHAROK: Using mechanism design for enhancing security resource allocation in interdependent systems," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2022, pp. 249–266.
[19] G. Modelo-Howard, S. Bagchi, and G. Lebanon, "Determining placement of intrusion detectors for a distributed application through Bayesian network modeling," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*. Cham, Switzerland: Springer, 2008, pp. 271–290.
[20] S. Dhami, *The Foundations of Behavioral Economic Analysis*. London, U.K.: Oxford Univ. Press, 2016.
[21] S. P. Anderson, J. K. Goeree, and C. A. Holt, "Noisy directional learning and the logit equilibrium," *Scandin. J. Econ.*, vol. 106, no. 3, pp. 581–602, Oct. 2004.
[22] Q. Zhuang, Z. Di, and J. Wu, "Stability of mixed-strategy-based iterative logit quantal response dynamics in game theory," *PLoS ONE*, vol. 9, no. 8, Aug. 2014, Art. no. e105391.
[23] B. J. Morgan, *Analysis of Quantal Response Data*, vol. 46. Boca Raton, FL, USA: CRC Press, 1992.
[24] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proc. IEEE Symp. Secur. Privacy*, May 2002, pp. 273–284.
[25] S. Jauhar, B. Chen, W. G. Temple, X. Dong, Z. Kalbarczyk, W. H. Sanders, and D. M. Nicol, "Model-based cybersecurity assessment with NESCOR smart grid failure scenarios," in *Proc. IEEE 21st Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Nov. 2015, pp. 319–324.
[26] A. Acquisti, "Nudging privacy: The behavioral economics of personal information," *IEEE Secur. Privacy*, vol. 7, no. 6, pp. 82–85, Nov. 2009.
[27] R. Anderson, "Security economics: A personal perspective," in *Proc. 28th Annu. Comput. Secur. Appl. Conf.*, Dec. 2012, pp. 139–144.
[28] J. Zhang, Y. Wang, and J. Zhuang, "Modeling multi-target defender-attacker games with quantal response attack strategies," *Rel. Eng. Syst. Saf.*, vol. 205, Jan. 2021, Art. no. 107165.
[29] R. Yang, C. Kiekintveld, F. Ordóñez, M. Tambe, and R. John, "Improving resource allocation strategies against human adversaries in security games: An extended study," *Artif. Intell.*, vol. 195, pp. 440–469, Feb. 2013.
[30] A. X. Jiang, T. H. Nguyen, M. Tambe, and A. D. Procaccia, "Monotonic maximin: A robust Stackelberg solution against boundedly rational followers," in *Proc. Int. Conf. Decis. Game Theory Secur.*, Fort Worth, TX, USA. Cham, Switzerland: Springer, Nov. 2013, pp. 119–139.
[31] D. Kar, F. Fang, F. D. Fave, N. Sintov, and M. Tambe, "'A game of thrones' when human behavior models compete in repeated Stackelberg security games," in *Proc. Int. Conf. Auto. Agents Multiagent Syst.*, 2015, pp. 1381–1390.
[32] M. Brown, W. B. Haskell, and M. Tambe, "Addressing scalability and robustness in security games with multiple boundedly rational adversaries," in *Proc. Int. Conf. Decis. Game Theory Secur. (GameSec)*, Los Angeles, CA, USA, Nov. 2014, pp. 23–42.
[33] T. Nguyen, R. Yang, A. Azaria, S. Kraus, and M. Tambe, "Analyzing the effectiveness of adversary modeling in security games," in *Proc. AAAI Conf. Artif. Intell.*, vol. 27, no. 1, 2013, pp. 718–724.
[34] J. Homer, S. Zhang, X. Ou, D. Schmidt, Y. Du, S. R. Rajagopalan, and A. Singhal, "Aggregating vulnerability metrics in enterprise networks using attack graphs," *J. Comput. Secur.*, vol. 21, no. 4, pp. 561–597, Sep. 2013.
[35] T. Roughgarden, "The price of anarchy is independent of the network topology," *J. Comput. Syst. Sci.*, vol. 67, no. 2, pp. 341–364, Sep. 2003.
[36] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Secur. Privacy Mag.*, vol. 4, no. 6, pp. 85–89, Nov. 2006.
[37] H. Zhang, F. Lou, Y. Fu, and Z. Tian, "A conditional probability computation method for vulnerability exploitation based on CVSS," in *Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2017, pp. 238–241.
[38] M. Abdallah, T. Cason, S. Bagchi, and S. Sundaram, "The effect of behavioral probability weighting in a sequential defender-attacker game," in *Proc. 59th IEEE Conf. Decis. Control (CDC)*, Dec. 2020, pp. 3255–3260.
[39] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave N-Person games," *Econometrica*, vol. 33, no. 3, p. 520, Jul. 1965.
[40] J. K. Goeree, C. A. Holt, and T. R. Palfrey, "Regular quantal response equilibrium," *Experim. Econ.*, vol. 8, no. 4, pp. 347–367, Dec. 2005.
[41] R. D. McKelvey and T. R. Palfrey, "Quantal response equilibria for normal form games," *Games Econ. Behav.*, vol. 10, no. 1, pp. 6–38, Jul. 1995.
[42] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, Jan. 2010, pp. 1–10.
[43] T. Alpcan and T. Basar, "An intrusion detection game with limited observations," in *Proc. 12th Int. Symp. Dyn. Games Appl.*, vol. 26, 2006, pp. 1–9.
[44] G. Yan, R. Lee, A. Kent, and D. Wolpert, "Towards a Bayesian network game framework for evaluating DDoS attacks and defense," in *Proc. ACM Conf. Comput. Commun. Secur.*, Oct. 2012, pp. 553–566.
[45] S. Rass and S. Schauer, *Game Theory for Security and Risk Management*, vol. 10. Cham, Switzerland: Springer, 2018, p. 978.
[46] Z. Xu and J. Zhuang, "A study on a sequential one-defender-n-attacker game," *Risk Anal.*, vol. 39, no. 6, pp. 1414–1432, Jun. 2019.
[47] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of DDoS attacks against Bitcoin mining pools," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Cham, Switzerland: Springer, 2014, pp. 72–86.
[48] M. Nasr, S. Farhang, A. Houmansadr, and J. Grossklags, "Enemy at the gateways: Censorship-resilient proxy distribution using game theory," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2019, pp. 1–15.
[49] A. R. Hota, A. Clements, S. Sundaram, and S. Bagchi, "Optimal and game-theoretic deployment of security investments in interdependent assets," in *Proc. Int. Conf. Decis. Game Theory Secur.*, 2016, pp. 101–113.
[50] K. C. Nguyen, T. Alpcan, and T. Basar, "Stochastic games for security in networks with interdependent nodes," in *Proc. Int. Conf. Game Theory Netw.*, May 2009, pp. 697–703.
[51] L. Perelman and S. Amin, "A network interdiction model for analyzing the vulnerability of water distribution systems," in *Proc. 3rd Int. Conf. High Confidence Netw. Syst.*, Apr. 2014, pp. 135–144.
[52] F. Chaoqi, G. Yangjun, Z. Jilong, S. Yun, Z. Pengtao, and W. Tao, "Attack-defense game for critical infrastructure considering the cascade effect," *Rel. Eng. Syst. Saf.*, vol. 216, Dec. 2021, Art. no. 107958.
[53] L. F. Cranor, "A framework for reasoning about the human in the loop," in *Proc. 1st Conf. Usability, Psychol., Secur.*, 2008, pp. 1–15.
[54] E. M. Redmiles, M. L. Mazurek, and J. P. Dickerson, "Dancing pigs or externalities: Measuring the rationality of security decisions," in *Proc. ACM Conf. Econ. Comput.*, Jun. 2018, pp. 215–232.
[55] A. Sanjab, W. Saad, and T. Basar, "A game of drones: Cyber-physical security of time-critical UAV applications with cumulative prospect theory perceptions and valuations," *IEEE Trans. Commun.*, vol. 68, no. 11, pp. 6990–7006, Nov. 2020.
[56] R. A. Martin, "Managing vulnerabilities in networked systems," *Computer*, vol. 34, no. 11, pp. 32–38, 2001.

MD. REYA SHAD AZIM (Graduate Student Member, IEEE) received the B.Sc. degree in electrical and electronic engineering from Chittagong University of Engineering and Technology (CUET), Bangladesh. He is currently pursuing the master's degree with the Department of Electrical and Computer Engineering, Indiana University–Purdue University Indianapolis (IUPUI). He is also a Research Assistant focusing on game theory and cyber security in cyber-physical systems. He has an industrial experience of 12 years on instrumentation and control at Nuclear Power Plants, System Protection and Testing-Commission in national grids, and several power plants' switchgear and control system installation and commissioning. He has hands-on experience in the implementation of automation and control systems and equipment at the industrial level. His previous academic and professional experiences have inspired him to pursue higher study and research on automation and control integrated with machine learning and artificial intelligence.

TIMOTHY CASON (Senior Member, IEEE) received the Ph.D. degree in economics from the University of California at Berkeley, Berkeley, CA, USA, in 1991. He was an Assistant and Associate Professor with the University of Southern California, before joining Purdue University, in 1998. He is currently a Distinguished Professor and the Robert and Susan Gadomski Chair of Economics with Purdue University, West Lafayette, IN, USA. His research interests include experimental and behavioral economics, environmental economics, and industrial organization, including applied research in market design, environmental regulation, and antitrust. He is a former Co-Editor of the *Journal of Public Economics* and a past Editor of the *Journal of Behavioral and Experimental Economics*. He has also served on numerous other editorial boards. He has served as the President of the Economic Science Association, from 2009 to 2011, which is the international society of experimental economists. He is a fellow of the Society for the Advancement of Economic Theory and a Fulbright Commission Senior Scholar. He was a recipient of dozens of grants, awards, and fellowships.

MUSTAFA ABDALLAH (Member, IEEE) received the M.Sc. degree in engineering mathematics from the Faculty of Engineering, Cairo University, and the Ph.D. degree from the Elmore Family School of Electrical and Computer Engineering, Purdue University. He is currently an Assistant Professor with the Purdue School of Engineering and Technology, Indiana University–Purdue University Indianapolis (IUPUI). His research interests include game theory, human decision-making, explainable AI, and machine learning with applications, including network security and autonomous driving systems. He has several industrial research experiences, including internships with Adobe Research, and a Principal, and a five-year machine learning research experience with RDI (a leading machine learning company in Egypt). His research contribution is recognized by receiving the Purdue Bilsland Dissertation Fellowship and having many publications in top IEEE/ACM journals and conferences. He was a recipient of the M.Sc. Fellowship from the Faculty of Engineering, Cairo University, in 2013.